Hewlett Packard
Enterprise

HPE Storage Operations Manager

Software Version: 10.20
Windows® and Linux® operating systems

Deployment 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.

 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

Chapter 1: About this Guide

This guide contains information and best practices for administering SOM. This guide is for an expert system administrator or HPE support engineer with experience in deploying and managing SOM installations. Read this guide before you start installing SOM.

Note: This document is updated as new information becomes available. 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

For more information, see "Documentation Updates" on page 3.

Chapter 2: Planning an SOM Deployment

Planning the deployment is a critical activity to ensure that the SOM server can manage your storage environment effectively. Use the following guidelines for planning a successful deployment of SOM in your environment:

- **Sizing the SOM management server**
  The size of the environment you want to manage decides how the servers should be sized and configured. To decide the SOM management server configuration that is suitable for your environment, see the "Performance and Sizing for the SOM Management Server" in the *SOM Support Matrix*.
- **Gather the system pre-requisites**
  Ensure that all the system pre-requisites are met before attempting to install SOM. Not meeting system requirements could result in an installation failure. For information about installation pre-requisites, see "Planning for Installation" in the *SOM Interactive Installation Guide*.
- **Check the firewall port configuration**
  The SOM management server uses various ports for communicating with the managed environment, the SOM console, and the SOM reporting server. The port configuration is largely decided by the proxy configuration of the managed devices. Ensure that the required configurations are enabled in the firewall configuration before starting the product installation. This will remove delays in discovering the managed environment once the product is deployed. For port configuration details, see "Ports and Firewall " on page 49.
- **Plan Tenancy**
  If you plan to have multiple tenants in your environment, it is a good idea to configure tenants before you start discovering your environment. You can associate the tenants to a discovery address. Elements discovered via this discovery address will automatically get associated with the configured tenant. It is easier to configure tenants before discovery as compared to moving elements to tenants after discovery. For information about planning tenants, see "Recommendations for Planning Tenants" on page 130.
- **Plan your Node Groups**
  In SOM, many of the management primitives such as data collection and monitoring policies are applied to groups of elements instead of to individual elements. This means that group definitions can be created in advance, and then the discovery process distributes the elements across different groups accordingly. For information about node group creation, see "Recommendations for Planning Node Groups" on page 58.
- **Determine the Data Collection Policies**
  Data collection policies can be pre-defined and applied to node groups before discovering your environment. After the elements are discovered, they will be categorized into the groups as described in "Planning your Node Groups" and then appropriate policies are applied to them. For example, if you follow a convention of naming all windows hosts as 'win*', you can create a group definition based on that and

apply a data collection policy with a custom freshness as required. This is a onetime definition and thereafter, as your windows hosts get discovered, they are already covered by data collection policies without additional administration overheads.

Also, you may want to set the level of data to collect for elements in your environment. By default, the system is configured NOT to collect all data on all devices in the environment. If you want to collect deeper data for a set of devices, you can configure this using the Data Collection Control feature. By planning this in advance you can avoid additional data collection cycles to get more data.

For information about best practices on data collection policies, see "Recommendations for Data Collection Policies" on page 65

- **Configure Performance Monitoring**
  As a general rule, wait for one data collection to complete in your environment for all (or a majority) of devices before configuring monitoring policies. You can refer to the Collection Status Dashboard to monitor the number of running collections. In large environments, configuring monitoring policies can overlap with the data collection process and might result in missing statistics. For information about best practices on creating monitoring policies, "Recommendations for Monitoring Performance " on page 66.
- **Decide your host discovery strategy – Rule-based inference/Agentless/Agent**
  Host discovery needs to be planned carefully, since they add the maximum bulk in terms of the number of elements discovered. SOM uses the following mechanisms to discover hosts in your environment:
  a. Rule-based inference – Use the configurations in your environment like Zones, Zone Aliases, and Host Security Groups to understand the distribution of storage to the hosts.
  b. Agentless discovery of hosts – Discover hosts without deploying agents on them by using mechanisms like WMI, SSH, or native API (for example, VMWare).
  c. Discovery by deploying agents on hosts – Deploy agents on hosts to discover hosts.

  Typically, agent deployment incurs administrative overheads. At the same time, agents provide the maximum depth of information on a host.

  To reduce this administrative overhead, you can use a combination of the methods listed above. Rule-based inference can be configured in your environment as soon as you have discovered your switches (fabric) and storage systems. Use the presented storage views and reports to understand the storage distribution in your environment. Once you understand the distribution of storage in your environment, you will be able to identify the top hosts that are consuming storage in your environment and then decide to discover them using agentless or agent based mechanism for further analysis.

  The choice between agentless discovery or agent-based discovery is driven by the depth of information you require on the host.

  For information on details about host discovery, see"Host Discovery" on page 60.
- **Configure the SOM reporting server**
  HPE Operations Bridge Reporter (OBR) is the reporting engine for SOM and needs to be installed on a separate server. Ensure that the ports for communication between SOM and OBR are available. For information about the required port, see "Ports and Firewall " on page 49.

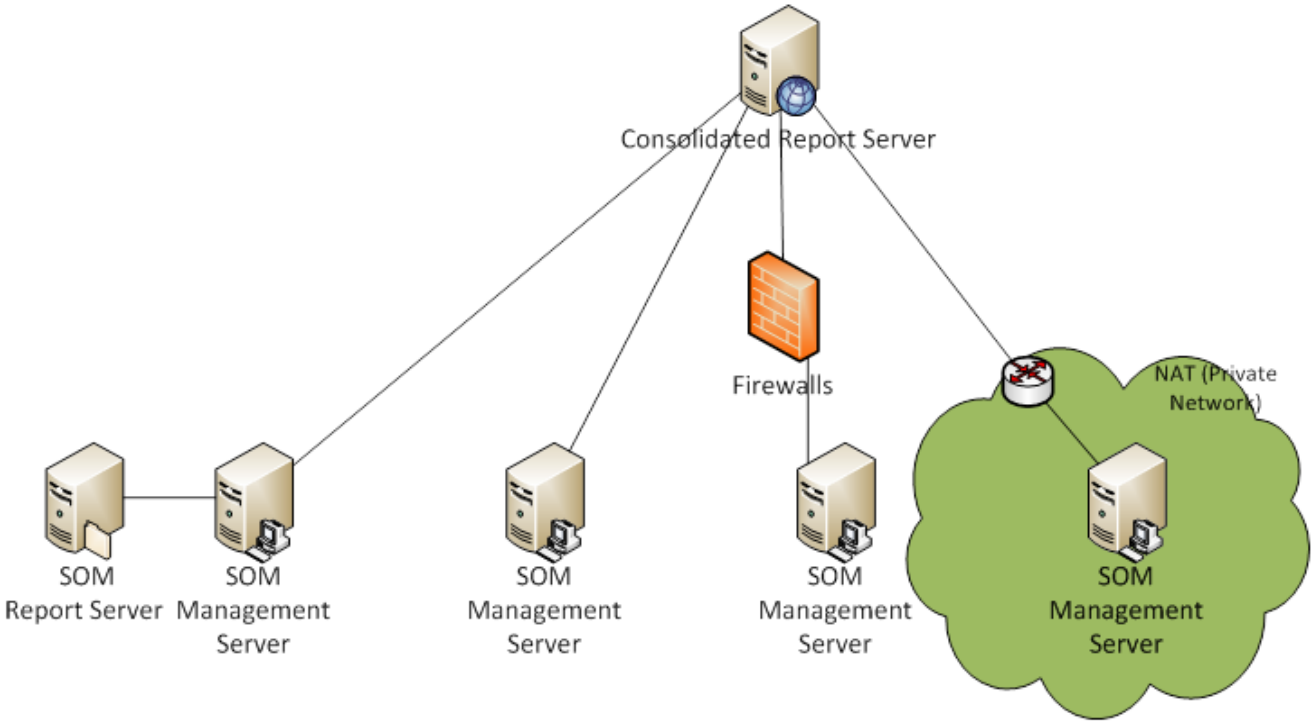
For information about sizing the SOM reporting server to suit your environment, see "Performance and Sizing for the SOM Reporting Server" in the *SOM Support Matrix*.

After installing the SOM reporting server and deploying the SOM content packs, you must configure certificates for enabling file transfer between the SOM management server and the SOM reporting server. See the appropriate chapter for configuring connections between the SOM management server and the SOM reporting server in the *Reports Guide*.

SOM Deployment Architecture

SOM can be deployed in different configurations and environments. In large environments, it may be necessary to deploy more than one SOM management server. In this case, you can have one consolidated SOM reporting server to which multiple SOM management servers can send data. In a consolidated reporting environment, it is also possible to deploy a local SOM reporting server that connects to one of the SOM management servers. In this case, the SOM management server sends data to both the local SOM reporting server and the consolidated SOM reporting server as shown in the diagram.

Consolidated report architecture can also be used to discover specific isolated infrastructure behind a firewall or NAT boundary. In this case, the SOM management server must be behind the firewall or NAT boundary and the communication between the SOM management server and the SOM reporting server must be configured across the firewall or NAT boundary.



Chapter 3: Planning Licenses

The HPE Storage Operations Manager restricts the number of elements it manages through licenses. Licensing is based on Managed Access Ports (MAP) count. Refer to the MAP Count Calculation table for details.

Key points on SOM licensing:

- SOM identifies the licensed MAP count (available capacity) limit from the installed license. SOM calculates the MAP count consumption (used capacity) based on the discovered elements in your environment. If the used capacity exceeds the available capacity, SOM will prevent discovery of further elements. In such a case if you attempt to discover an element, you will receive an error “License capacity exceeded.” However, there is no restriction on discovery for a valid temporary Instant-On license.
- Only one type of license is active at a time. You cannot have a mix of Premium and Ultimate-Perf license types. If both SOM Premium license and SOM Ultimate-Perf are installed, then Ultimate-Perf supersedes the Premium license. Available capacity is derived from the superseded license.
- You need SOM Ultimate-Perf license to collect performance metrics from devices that support performance collection. The current release of SOMallows configuring and collecting performance metrics from 25 devices simultaneously by a single instance of the management server.
- You can extend the licensed MAP count (available capacity) by procuring additional licenses. Available capacity will be aggregated and refreshed after installation of new licenses. However, the license capacity for performance is not aggregated and is fixed to 25 devices by a single instance of the management server.

License Types

There are three types of licenses available with the current release of SOM.

License Type	Validity	Supports Performance
SOM Instant-on	60 days	Yes
SOM Premium	Unlimited	No
SOM Ultimate-Perf	Unlimited	Yes

Temporary Instant-On License

When you install HPE Storage Operations Manager, it comes with a temporary Instant-On license. The temporary Instant-On license is valid for 60 days. You should obtain and install a permanent license as soon as possible to continue using SOM.

Obtaining and Installing a New License

To request a permanent license, gather the following information:

- The Entitlement Certificate, which contains the HPE product number and order number
- The IP address of one of the SOM management servers
- Your company or organization information

You can install the permanent license using the Autopass user interface or the command line interface.

Install a Permanent License from the Command Line

To install the license at a command prompt on the SOM management server, enter the following command:

```
somlicensemanager.ovpl SOM -install <path_of_license_file>
```

where <path_of_license_file> is the location where the license file is stored.

Install a Permanent License using Autopass

To install a permanent license, follow these steps:

1. At the command prompt, enter the following command to open the Autopass user interface:
   `somlicensemanager.ovpl SOM -gui`
2. On the left pane of the Autopass window, click **License Management**.
3. Click **Install License Key**.
4. Click **Install/Restore License Key**.
5. Browse to the location where the license key is stored.
6. View file content.
7. Select the license and click **Install**.

Extend a Licensed Capacity

To extend the licensed capacity, purchase and install an additional SOM Premium or SOM Ultimate Perf license.

Contact your HPE Sales Representative or your Authorized Hewlett Packard Enterprise Reseller for information about the SOM licensing structure. To obtain additional license keys, go to the HPE License Key Delivery Service:

https://h30580.www3.hpe.com/poeticWeb/portalintegration/hppWelcome.htm

Viewing License Information

1. From the SOM console, click **Help** > **System Information** > **View Licensing Information**.
2. Look for the value shown in the **Consumption** field. This is the number of MAPs that SOM is currently managing (used capacity).

Viewing Consumed MAP Count for Each Element

You can view the number of MAPs consumed by each element being managed by SOM. This information is displayed in the **MAP Count** field in the Analysis Pane of each element in the Inventory views.

MAP Count Calculation

Element	Description	Number of MAPs	Comments
Hosts	Host with a single port HBA Host with a dual port HBA	1 MAP 2 MAPs	No additional counting for CIM Extension.
	Host without FC ports	1 MAP	
	Host with one iSCSI network card port	1 MAP	
	Host with no FC port and no iSCSI network card port with CIM Extension.	1 MAP	
	Standalone server with no FC HBA discovered through CIM Extension.	1 MAP	
	Windows server agentless discovery	1 MAP at a minimum or 1 MAP per FC HBA	

Element	Description	Number of MAPs	Comments
	through Windows Management Instrumentation (WMI)	port.	
	Linux server agentless discovery through SSH	1 MAP at a minimum or 1 MAP per FC HBA port.	
	AIX agentless discovery through SSH	1 MAP at a minimum or 1 MAP per FC HBA port.	
	Solaris agentless discovery through SSH	1 MAP at a minimum or 1 MAP per FC HBA port.	
Virtual Servers	VMware ESX servers	1 MAP at a minimum or 1 MAP per FC HBA port.	Five ESX servers with two dual-ported HBAs count as 10 MAPs (5*2=10)
	Each FC port on a virtual server	1 MAP	Virtual servers are treated like physical hosts.
	A virtual server without FC ports.	1 MAP	The software assumes one MAP.
Virtual Machines	A virtual machine if it is running VMTools irrespective whether it was discovered through its virtual server or its VirtualCenter	1 MAP	
	A virtual machine with an installed CIM Extension regardless if VMTools is running.	1 MAP	
	Each VMware Virtual Machine Guest OS discovered directly through WMI (Windows)	1 MAP	A VMware Virtual Machine Guest OS discovery through VMTools, and subsequently discovered

Element	Description	Number of MAPs	Comments
	or SSH (Linux), or CIM Extension		through agentless WMI or CIM Extension counts as only 1 MAP.
Switches	Each port on a switch Physical switches, all ports are counted as MAPs.	1 MAP	• All switch ports with GBICS installed are counted as MAPs. • ISL links are not counted as MAPs. • If the Switch port is not licensed then it's not counted as MAP. • When GBIC is not there or if the port is not licensed, SOM does not discover these port numbers. Only ports that are discovered are counted as MAPs.
Isilon		No. of nodes * 5 MAPs	
HPE XP / P9500 External Storage	Each port	1 MAP	All backend ports count as MAPs.
EVA, 3PAR, EMC VNX/CLARiiON, DMX/VMAX, VPLEX, HUS/USP	Each port	1 MAP	All backend ports count as MAPs.
NetApp 7-Mode		5 MAPs	Only single node supported.
NetApp C-Mode Logic		No. of nodes * 5 MAPs	
EMC VNX Filer		5 MAPs	
EMC Data Domain Storage Systems	EMC Data Domain System	5 MAPs + No. of FC ports * 1 MAP	
	EMC Data Domain Virtual Edition	5 MAPs	

Element	Description	Number of MAPs	Comments
Block Storage Systems	Block Storage System without FC ports	20 MAPs	

Chapter 4: CIM Extensions

The Common Information Model (CIM) standard specifies a structure of information about managed elements. CIM provides for consistent data structure and access regardless of device vendor. CIM is maintained by the Distributed Management Task Force (DMTF).

The Storage Management Initiative Specification (SMI-S) enables consistent management of heterogeneous storage elements. SMI-S is based on the Common Information Model (CIM) and Web-Based Enterprise Management (WBEM) standards for accessing management information over HTTP. SMI-S is maintained by the Storage Networking Industry Assocation (SNIA).

A SOM CIM Extension is a collection agent that runs on a storage host to gather information about that host. SOM communicates with the CIM Extension while discovering and managing the host.

For SOM to obtain information from the host, the CIM Extension must be running. The CIM Extension starts automatically after installation and whenever the host boots. On an HP-UX host, the CIM Extension uses `/sbin/rc2.d` scripts.

SOM can manage some storage hosts using an agentless process. The agentless approach, however, limits the information that is available to SOM. For more information, see the *SOM Device Support Matrix*.

The default location of the CIM Extension is:

- *Windows*: `<Drive:>\Program Files (x86)\APPQcime\CimExtensions`
- *UNIX or Linux*: `/opt/APPQcime/`

Installing CIM Extensions

A CIM Extension communicates with a host bus adapter (HBA) using the fibre channel host bus adapter application programming interface (FC-HBA API) created by the Storage Network Industry Association (SNIA). The SOM management server only supports communication with HBAs that are compliant with the HBA API. For more information about the HBA API, see the SNIA web page: http://www.snia.org.

The `hbatest` program on the SOM installation media outputs the name and number of all HBAs on the host that support the FC-HBA API. In some instances, `hbatest` might report that it cannot find an HBA driver even though an HBA driver is installed. In this case, try installing a different, SNIA-compliant version of the HBA driver.

The SOM installation media includes operating system-specific CIM Extensions in the `CIMExtensionsCD1` directory.

To install a CIM Extension

1. Verify that at least one host bus adapter (HBA) on the host supports the FC-HBA API. Follow the procedures that apply to your environment:
   - "Verify FC-HBA API Support on a Windows Host" on the next page
   - "Verify FC-HBA API Support on an HP-UX Host" on the next page
   - "Verify FC-HBA API Support on a Linux Host" on page 22
   - "Verify FC-HBA API Support on a Solaris Host" on page 22
   - "Verify FC-HBA API Support on an IBM AIX Host" on page 23
2. Verify that port 4673 is available on the host and reachable by the SOM management server.

   Alternatively, identify a different port for the CIM Extension. After installation, configure the CIM Extension to use that port as described in "Change the CIM Extension Port Number" on page 35.
3. Install the CIM Extension software on the host. Follow the procedures that apply to your environment:
   - "Install the CIM Extension Software on a Windows Host" on page 24
   - "Install the CIM Extension Software on an HP-UX Host" on page 24
   - "Install the CIM Extension Software on a Linux Host" on page 25
   - "Install the CIM Extension Software on a Solaris Host" on page 27
   - "Install the CIM Extension Software on an IBM AIX Host" on page 28

Tip: If your security environment requires that you customize the CIM Extensions or the CIM Extension installation process, you might need to use a third-party tool to deploy CIM Extensions. Third-party tools are commonly used in large environments that require the use of a request for change (RFC) process.

Verify FC-HBA API Support on a Windows Host

To verify that at least one host bus adapter on a Windows host supports the FC-HBA API

1. In a command window, change to the `CimExtensionsCD1/Windows/tools` directory on the SOM installation media.
2. Enter the following command:

   `hbatest.exe -v`

   The beginning of the command output should be similar to the following example:

   ```
   hbaapi.dll, version XXXXXXXXXXXXXX will be used to get HBA information.
   HBA API Library version is 2
   hbatest build date: Jun 26 2014:20:14:26
   Number of HBA's is 2
   ****************************************
   ```

   After the header, the command output lists each HBA present on the host.

Return to the installation procedure.

Verify FC-HBA API Support on an HP-UX Host

To verify that at least one host bus adapter on an HP-UX host supports the FC-HBA API

1. Go to the `CimExtensionsCD1/HPUX/tools` directory on the SOM installation media.
2. Run the following command:

   `./hbatest`

   The program runs its diagnostics.

HP SNIA adapters AXXXXA come from fileset FC-FCD, FC-TACHYON-TL. Unless separated purposely during the installation of the operating system, filesets are there by default. To view the location of the library, enter the following at the command prompt:

`more /etc/hba.conf`

The `hba.conf` file includes the following lines:

```
com.hp.fcms32 /usr/lib/libhbaapihp.sl #32 bit lib names end in 32
com.hp.fcms64 /usr/lib/pa20_64/libhbaapihp.sl #64 bit lib names end in 64
com.hp.fcd32 /usr/lib/libhbaapifcd.sl
com.hp.fcd64 /usr/lib/pa20_64/libhbaapifcd.sl
```

Return to the installation procedure.

Verify FC-HBA API Support on a Linux Host

To verify that at least one host bus adapter on a Linux host supports the FC-HBA API

1. Go to the `CimExtensionsCD1/linux/tools` directory on the SOM installation media.
2. Run the following command:

   `./hbatest`

   The program runs its diagnostics.

Driver Information for Verifying Emulex SNIA Adapters (Red Hat Linux Only)

The Emulex driver does not contain the library that is required by the SOM management server. You must install Emulex OneCommand Manager software so that the management server can discover hosts configured with OneCommand Manager and the HBATool can detect the Emulex host bus adapter.

After you install the OneCommand Manager software, you can find the location of the libraries in the `/etc/hba.conf` file.

To view the `hba.conf` file on a Linux host, run the following command:

`cat /etc/hba.conf`

The output lists the library name and then the path, as shown in the following examples:

- Linux 64-bit host Emulex driver example output

  ```
  com.emulex.emulexapilibrary /usr/lib64/libemulexhbaapi.so
  com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
  ```

  Note: The OneCommand Manager CLI must be used for IA64 Linux.

- Linux 32-bit host Emulex driver example output

  ```
  com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
  ```

Return to the installation procedure.

Verify FC-HBA API Support on a Solaris Host

To verify that at least one host bus adapter on a Solaris host supports the FC-HBA API

1. Go to the `CimExtensionsCD1/Solaris/tools` directory on the SOM installation media.
2. Run the following command:

   `./hbatest`

   The program runs its diagnostics.

Depending on the driver and version of the operating system, the SNIA API library might be installed with the driver or its utility program provided by the vendor.

To find the API library, type the following command:

```
more /etc/hba.conf
```

The following are examples of the library names and paths:

Emulex

```
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
com.emulex.emulexapilibrary /usr/lib/sparcv9/libemulexhbaapi.so
```

JNI

```
JniHbaLib /opt/JNIsnia/Solaris/Jni/32bit/JniHbaLib.so
JniHbaLib /opt/JNIsnia/Solaris/Jni/64bit/JniHbaLib.so
```

SUN Branded

```
com.sun.fchba /usr/lib/libsun_fc.so.1
com.sun.fchba64 /usr/lib/sparcv9/libsun_fc.so.1
```

Return to the installation procedure.

Verify FC-HBA API Support on an IBM AIX Host

To verify that at least one host bus adapter on an AIX host supports the FC-HBA API

1. Go to the `CimExtensionsCD1/Aix/tools` directory on the SOM installation Media.
2. Enter the following at the command prompt:

   `./hbatest`

   The program runs its diagnostics.

IBM Adapters FCXXXX SNIA comes from the package `devices.common.IBM.fc.hba-api`. To find its library, enter the following at the command prompt:

`more /etc/hba.conf`

The `hba.conf` file includes the following lines:

```
com.ibm.df1000f7 /usr/lib/libHBAAPI.a
com.ibm.df1000f9 /usr/lib/libHBAAPI.a
```

Return to the installation procedure.

Install the CIM Extension Software on a Windows Host

You must have administrator privileges to install the the CIM Extension on a Windows host.

If a firewall is enabled on the Windows host, open the CIM Extension port before installing the CIM Extension. The default CIM Extension port is 4673. For information about configuring the Windows firewall, see the documentation for the Microsoft Windows operating system.

The Windows CIM Extension can be installed interactively or in silent mode. Use silent mode to install the Windows CIM Extension with the default settings and no user intervention.

Interactive Mode

To install the CIM Extension using interactive mode, follow the procedure below:

1. Log on to the Windows host as a user with administrator privileges.
2. Insert the SOM installation media into the DVD drive.
3. In Windows Explorer, change to the `CimExtensionsCD1\Windows` directory, and then double-click `InstallCIMExtensions.exe`.
4. Follow the instructions on the screen.

Silent Mode

To install the CIM Extension using silent mode, follow the procedure below:

1. Verify that no other programs are running.
2. Remove the previous version of the CIM Extension as described in "Remove the CIM Extension from a Windows Host" on page 44.
3. Log on to the Windows host as a user with administrator privileges.
4. Insert the SOM installation media into the DVD drive.
5. In a command window, change to the following directory:

   ```
   CimExtensionsCD1\Windows
   ```

6. Enter the following command:

   ```
   InstallCIMExtensions.exe -i silent
   ```

Return to the installation procedure.

Install the CIM Extension Software on an HP-UX Host

The following instructions apply to a local installation of the CIM Extension.

You must install the CIM Extension for HP-UX to the default directory. If there are space issues, such as large CIM Extension binary files, create a symbolic link to a folder with more space.

To install the CIM Extension, follow the procedure below:

1. Log on to the HP-UX host as the `root` user.
2. Insert the SOM installation media into the DVD drive.
3. Create the `/DVD` directory by running the following command:

   `mkdir /DVD`
4. Mount the SOM installation media by enter the following at the command prompt:

   `mount /dev/dsk/c#t#d#  /DVD`

   In this instance, the c, t, and d numbers correspond to DVD device numbers.

   To find out c#t#d# for your DVD drive, run the **`ioscan -fnC disk`** command on the HP-UX host.
5. Run the following command:

   `swinstall -x mount_all_filesystems=false -s /DVD/HPUX/APPQcime.depot APPQcime`

   The installation is complete when a message similar to the following appears:

   `analysis and execution succeeded`
6. Unmount the DVD by running the following command:

   `umount /DVD`

   In this instance, `/DVD` is the name of the directory where you mounted the DVD.

Return to the installation procedure.

Install the CIM Extension Software on a Linux Host

The following instructions apply to a local installation of the CIM Extension.

The installation is a two-step process where a “requires” rpm is run to check for dependencies, and then the full rpm is installed.

You must install the CIM Extension for Linux to the default directory. If there are space issues, such as large CIM Extension binary files, create a symbolic link to a folder with more space.

To install the CIM Extension

1. Log on to the Linux host as the `root` user.
2. Insert the SOM installation media into the DVD drive.
3. Change to the `CIMExtensionCD1/linux/requires_rpm` directory on the SOM installation media.

   `cd /DVD/linux/requires_rpm`

   In this instance, `/DVD` is the name of the DVD drive.
4. Use the appropriate "requires” rpm from the following list for the version of your operating system.

Operating System	RPM
Red Hat versions 5 and 6	
32-bit and 64-bit (Red Hat 5) on x86_64	RedHat<version>/APPQcime--Requires- <Version>-<Release>.i386.rpm
IA64-based Red Hat 5 and Red Hat 6 installations	SUSE<version>/APPQcime-Requires-<Version>-<Release>.ia64.rpm
32-bit (Red Hat 6) on x86_64	RedHat<version>/APPQcime--Requires- <Version>-<Release>.i386.rpm
64-bit (Red Hat 6) on x86_64	RedHat<version>/APPQcime--Requires- <Version>-<Release>.x86-64.rpm
SUSE 11 and 12	
32-bit and 64-bit on x86_64	SUSE<version>/APPQcime-Requires-<Version>-<Release>.i386.rpm
IA64	SUSE<version>/APPQcime-Requires-<Version>-<Release>.ia64.rpm

After running the “requires” rpm, you will get one or more dependency errors. A dependency on the rpm package APPQcime is expected, for example:

`APPQcime is needed by APPQcime-Requires-9.4.0-224.i386.rpm`

If you get an additional dependency error, you must install the required packages before continuing.

5. If you get only the one expected dependency-error after running the “requires” rpm, run the following command:

   `rpm -idvh <rpm_package_name>`

   In this instance `<rpm_package_name>` is the name of the rpm package listed in the following table.

Operating System	RPM
64-bit Red Hat versions 6 and later	APPQcime-<Version>-<Release>-x86_64.rpm
• Red Hat 32-bit installations on x86 • 64-bit installations earlier than Red Hat version 6 • SUSE installations on x86 or x64	APPQcime-<Version>-<Release>-i386.rpm

Operating System	RPM
(Red Hat and SUSE Linux) IA64-based installations	APPQcime-<Version>-<Release>-ia64.rpm

The following output is displayed:

```
Preparing... ########################################### [100%]
1:APPQcime ########################################### [100%]
```

The installation is done when you are returned to the command prompt.

6. *Optional*. Verify that the packages were installed:

```
rpm -qa | grep APPQcime-Requires
rpm -qa | grep APPQcime
```

Return to the installation procedure.

Install the CIM Extension Software on a Solaris Host

The following instructions apply to a local installation of the CIM Extension.

You must install the CIM Extension for Solaris to the default directory. If there are space issues due to large CIM Extension binary files, create a symbolic link to a folder with more space.

Prerequisites

- SOM requires certain packages and patches to discover a Solaris host. The CIM Extension installer checks for the following packages and verifies that the Solaris operating system is installed.

  The core set `SUNWCreq` is required. If the core environment packages are installed, the following packages must be installed manually on a Solaris host:

  - `SUNWlibC` – Sun Workshop Compilers Bundled libC
  - `SUNWlibCf` – SunSoft WorkShop Bundled libC (cfront version)
  - `SUNWlibCx` – Sun Workshop Bundled 64-bit libC
- Verify that the latest Oracle patches are installed.
- The server must be running sh, ksh, or bash shell.

To install a CIM Extension:

1. Log on to a Solaris host as the `root` user.
2. Copy the following file to the local host server:
   - For Windows: `Software_HPE_Storage_Operations_Manager_<version_number>_<SKU_number>.zip`

- For Linux: `Software_HPE_Storage_Operations_Manager_<version_number>_<SKU_number>.tar.gz`

3. Extract the contents of the file:
   - For Windows: Right-click the file and then select **Extract All**
   - For Linux: Run the following command:

   `tar -zxvf Software_HPE_Storage_Operations_Manager_<version_number>_<SKU_number>.tar.gz`
4. Change to either one of the directories:
   - For SPARC - `CimExtensionsCD1/Solaris`
   - For x86 - `CimExtensionsCD1/Solaris-x86`
5. Type the following command:

   `pkgadd -d APPQcime.pkg`
6. When prompted for the installation directory, type the path of the default directory (`/opt`), and then press **Enter**.
7. To continue the installation, press **y**.

   The CIM Extension installation is complete.
8. To quit the installer, press **q**.

Return to the installation procedure.

Install the CIM Extension Software on an IBM AIX Host

The following installation steps assume you know how to use the AIX System Management Interface Tool (SMIT). If you are unfamiliar with SMIT, see the documentation that accompanies the AIX host.

You must install the CIM Extension for IBM AIX to the default directory. If there are space issues, such as large CIM Extension binary files, create a symbolic link to a folder with more space.

To install the CIM Extension on an IBM AIX host, use the `installp -aX -d /cime_location/APPQcime.bff` command. In this instance cime_location is the directory where the cime install file for AIX is copied.

Use the following steps to install the CIM Extension on an AIX host:

1. Log on to an AIX host as the `root` user.
2. Copy the following file to the local host server:

- For Windows: `Software_HPE_Storage_Operations_Manager_<version_number>_<SKU_number>.zip`
- For Linux: `Software_HPE_Storage_Operations_Manager_<version_number>_<SKU_number>.tar.gz`

3. Extract the contents of the file:
   - For Windows: Right-click the file and then select **Extract All**
   - For Linux: Run the following command:

   `tar -zxvf Software_HPE_Storage_Operations_Manager_<version_number>_<SKU_number>.tar.gz`
4. Change to the `CIMExtensionCD1/aix directory`.

   `cd CIMExtensionCD1/aix`
5. Enter the following at the command prompt:

   `smit-C`
6. Select **Software Installation and Maintenance**.
7. Select **Install and Update Software**.
8. Select **Install Software**.
9. For INPUT device/directory for software, enter the following:

   `CIMExtensionCD1/aix`
10. Activate the list command (**Esc+4**), and then select the following:

    `APPQcime`
11. Press **Enter**
12. Complete the following:
    - Turn on Monitoring.
    - Start the CIM Extension (see "Starting a CIM Extension Manually" on page 42).

Return to the installation procedure.

Upgrading the CIM Extension Software

You must upgrade your CIM Extensions to obtain the latest functionality.

To upgrade the CIM Extension software on the host follow the procedures that apply to your environment:

- "Upgrade the CIM Extension Software on a Windows Host" on the next page
- "Upgrade the CIM Extension Software on an HP-UX Host" on the next page
- "Upgrade the CIM Extension Software on a Linux Host" on the next page

Upgrade the CIM Extension Software on a Windows Host

You must have administrator privileges to upgrade the CIM Extension on a Windows host.

The following instructions apply to a local installation of the CIM Extension.

To upgrade the CIM Extension, follow the procedure below:

1. Install the new CIM Extension software from the SOM installation media as described in "Install the CIM Extension Software on a Windows Host" on page 24.

   Note: To upgrade the CIM Extension software on windows hosts, you need not uninstall the existing CIM Extension software. You can continue to install the new version on the existing software version.

Upgrade the CIM Extension Software on an HP-UX Host

The following instructions apply to a local installation of the CIM Extension.

To upgrade the CIM Extension, follow the procedure below:

1. Uninstall the existing CIM Extension software as described in "Remove the CIM Extension from an HP-UX Host" on page 45.
2. Install the new CIM Extension software from the SOM installation media as described in "Install the CIM Extension Software on an HP-UX Host" on page 24.

Upgrade the CIM Extension Software on a Linux Host

The following instructions apply to a local installation of the CIM Extension.

To upgrade the CIM Extension, follow the procedure below:

1. Uninstall the existing CIM Extension software as described in "Remove the CIM Extension from a Linux Host" on page 45.
2. Install the new CIM Extension software from the SOM installation media as described in "Install the CIM Extension Software on a Linux Host" on page 25.

Upgrade the CIM Extension Software on a Solaris Host

The following instructions apply to a local installation of the CIM Extension.

To upgrade the CIM Extension, follow the procedure below:

1. Uninstall the existing CIM Extension software as described in "Remove the CIM Extension from a Solaris Host" on page 46.
2. Install the new CIM Extension software from the SOM installation media as described in "Install the CIM Extension Software on a Solaris Host" on page 27.

Upgrade the CIM Extension Software on an IBM AIX Host

The following instructions apply to a local installation of the CIM Extension.

To upgrade the CIM Extension, follow the procedure below:

1. Uninstall the existing CIM Extension software as described in "Remove the CIM Extension from an IBM AIX Host" on page 46
2. Install the new CIM Extension software from the SOM installation media as described in "Install the CIM Extension Software on an IBM AIX Host" on page 28

Configuring a CIM Extension

The `cim.extension.parameters` file determines the CIM Extension behavior. The CIM Extension reads this file at startup.

The `cim.extension.parameters-sample` file provides a template configuration.

These files are located in the following directory:

- *Windows*: `[Installation_Directory]\CimExtensions\conf`
- *UNIX/Linux*: `/opt/APPQcime/conf`

The default behavior of a CIM Extension is as follows:

- The SOM management server must use the administrator or root account on the host for communications with the CIM Extension.
- The CIM Extension sends and receives communications on port 4673.
- The CIM Extension listens on the loopback address of the host.

To change this behavior, create the `cim.extension.parameters` file by copying and customizing the provided template file (`cim.extension.parameters-sample`).

To configure the CIM Extension

1. Log on to the host as a user with administrator or root privileges.
2. Change to the CIM Extension configuration directory:
   - *Windows*: `[Installation_Directory]\CimExtensions\conf`
   - *UNIX/Linux*: `/opt/APPQcime/conf`
3. Save a copy of the `cim.extension.parameters-sample` file as `cim.extension.parameters` in the same directory.
4. In a text editor, edit the `cim.extension.parameters` file as required.

   For information about commonly changed parameters, see the table of CIM Extension parameters.

   For information about configuring log files, see "Log File Properties" on page 41.
5. Save and close the file.
6. Restart the CIM extension.
   - *Windows*:

     Restart the AppStorWin32Agent service from the **Services** window or reboot the host.

     Note: To restart the AppStorWin32Agent service, you can also use the following commands at the command prompt:

     ```
     [Installation_Directory]\CimExtensions\tools\net stop AppStorWin32Agent
     [Installation_Directory]\CimExtensions\tools\net start AppStorWin32Agent
     ```

   - *UNIX/Linux*:

     ```
     /opt/APPQcime/tools/stop
     /opt/APPQcime/tools/start
     ```

Commonly Configured CIM Extension Parameters

Parameter	Description
`-users`	Restricts the discovery of the host to a list of valid host users. Each user defined in this parameter must be a valid existing user on the host, and the user name must match one of the user names used on the discovery page to discover the host for authentication to occur. The user does not need to have root authority. Use a colon (`:`) to separate multiple users. The format of the user name depends on the operating system: • *Windows*: Specify the domain name and the user name, for example: `-users domain_name\user_name` • *UNIX*: Specify the user name without the domain name, for example:

Parameter	Description
	`-users user_name` For more information, see "Restrict the Users Who Can Discover the Host" on the next page.
`-credentials <username>:<password>`	Specifies a user name and password on the host to facilitate communication between the SOM management server and the managed host. This configuration eliminates the need to use the local operating system user/password database for credential verification. This user name / password pair is known only to the CIM Extension and does not identify a real user on the host. The specified account name might not exist on the host. The `-users` parameter always takes precedence over the `-credentials` parameter. To use the `-credentials` parameter when the `-users` parameter has been added to the `cim.extension.parameters` file, comment out the `-users` parameter by inserting the number sign character (#) at the beginning of the `-users` line.
`-mgmtServerIP <ip address>`	Restricts the CIM Extension to listen only to the specified SOM management servers. Use commas to separate multiple address values. For example: `-mgmtServerIP 127.0.0.1,192.168.0.1`
`-port <new port>`	Specifies the port that the CIM Extension accesses. For example: `-port 1234` See "Change the CIM Extension Port Number" on page 35.

`-on <ip address1>`
`-on <ip address2:port>`
	For multi-homed systems, restricts the CIM Extension to listen only on designated IP address.
	Use multiple entries for multiple addresses. For example:
	`-on <15.218.125.12>`
	`-on <15.218.125.123:5432>`
	See "Configure the CIM Extension to Listen on a Specific IP Address" on page 36.

Linux only. For command line help about CIM Extension configuration, run the following command:

`/opt/APPQcime/tools/start -help`

Restrict the Users Who Can Discover the Host

The `-users` parameter increases security by restricting access to the CIM Extension. When you use the SOM management server to discover the host, provide one of the user names that was specified in the `-users` parameter.

To use the management server to discover a host without using the root account, provide the password to another valid user account with fewer privileges on the host.

First, add the user to the parameters file. Next, log on to the management server, access the Discovery page, and provide the user name and password for jsmythe. Only the user name and password for jsmythe can be used to discover the host.

To add a user to the parameters file

1. Backup the `cim.extension.parameters` file to a location outside the CIM Extension installation directory:
   - *Windows*: `[Installation_Directory]\CimExtensions\conf\cim.extension.parameters`
   - *UNIX/Linux*: `/opt/APPQcime/conf/cim.extension.parameters`
2. In a text editor, open the `cim.extension.parameters` file.
3. Add the following line:

   ```
   -users myname
   ```

   In this instance, myname is a valid user name on the host.

   To enter multiple users, separate them with a colon; for example, `-users myname:jsymthe`.
4. Save the file.
5. Restart the CIM extension.
   - *Windows*:

     Restart the AppStorWin32Agent service from the **Services** window or reboot the host.

     > **Note:** To restart the AppStorWin32Agent service, you can also use the following commands at the command prompt:
     >
     > **`[Installation_Directory]\CimExtensions\tools\net stop AppStorWin32Agent`**
     > **`[Installation_Directory]\CimExtensions\tools\net start AppStorWin32Agent`**

   - *UNIX/Linux*:

     `/opt/APPQcime/tools/stop`
     `/opt/APPQcime/tools/start`

Change the CIM Extension Port Number

By default, the CIM Extension uses port 4673. If this port is already in use, change the CIM Extension port as follows:

1. Back up the CIM Extension configuration directory to a location outside the CIM Extension installation directory:
   - *Windows*: `[Installation_Directory]\CimExtensions\conf`
   - *UNIX/Linux*: `/opt/APPQcime/conf`
2. In a text editor, open the `cim.extension.parameters` file.
3. Add the following line:

   `-port <port_number>`

   Replace *<port_number>* with the port number to use.
4. Save the file.
5. Restart the CIM extension.
   - *Windows*:

     Restart the AppStorWin32Agent service from the **Services** window or reboot the host.

     Note: To restart the AppStorWin32Agent service, you can also use the following commands at the command prompt:

     `[Installation_Directory]\CimExtensions\tools\net stop AppStorWin32Agent`
     `[Installation_Directory]\CimExtensions\tools\net start AppStorWin32Agent`
   - *UNIX/Linux*:

     `/opt/APPQcime/tools/stop`
     `/opt/APPQcime/tools/start`
6. Update the SOM management server with the new port number for this host.
   a. Open the **Discovery Addresses** form (**Configuration > Discovery > Discovery Addresses**) for this host.
   b. In the **IP Address** box, enter the IP address with a colon followed by the new port number. For example:

      `192.168.1.2:1234`

      In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

      If you already added the host to the discovery list (**Configuration > Discovery > Discovery Address**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configure the CIM Extension to Listen on a Specific IP Address

To configure the CIM Extension to listen on a specific IP address

1. Back up the CIM Extension configuration directory to a location outside the CIM Extension installation directory:
   - *Windows*: `[Installation_Directory]\CimExtensions\conf`
   - *UNIX/Linux*: `/opt/APPQcime/conf`
2. In a text editor, open the `cim.extension.parameters` file.
3. For each IP address to listen on, add the following line:

   `-on <IP_address>`

   Replace *<IP_address>* with one IP address. Optionally, add a port. For example, to listen on port 3456 of IP address 192.168.2.2, use the following text:

   `-on 192.168.2.2:3456`
4. Save the file.
5. Restart the CIM extension.
   - *Windows*:

     Restart the AppStorWin32Agent service from the **Services** window or reboot the host.

     > **Note:** To restart the AppStorWin32Agent service, you can also use the following commands at the command prompt:
     >
     > **`[Installation_Directory]\CimExtensions\tools\net stop AppStorWin32Agent`**
     > **`[Installation_Directory]\CimExtensions\tools\net start AppStorWin32Agent`**

   - *UNIX/Linux*:

     `/opt/APPQcime/tools/stop`
     `/opt/APPQcime/tools/start`
6. Update the SOM management server with the new port number for this host.
   a. Open the **Discovery Addresses** form (**Configuration > Discovery > Discovery Addresses**) for this host.
   b. In the **IP Address** box, enter the IP address with a colon followed by the new port number. For example:

      `192.168.1.2:1234`

      In this instance, 192.168.1.2 is the IP address of the host, and 1234 is the new port number.

If you already added the host to the discovery list (**Configuration > Discovery > Discovery Address**) on the management server, you must remove it and then re-add it. You cannot have more than one listing of the host with different ports.

Configuring CIM Extensions to Run Behind Firewalls (UNIX Only)

To discover a host behind a firewall, use the following table as a guideline. Assume the management server wants to discover HostA, which has three network interface cards on three separate networks with three separate IP addresses: 10.250.250.10, 172.31.250.10, and 192.168.250.10. The following table presents configuration options.

- The “Manual Start Parameters for CIM Extensions” column provides the values you would enter to start the CIM Extension manually on the host. For more information about how to start a CIM Extension manually, see "Starting a CIM Extension Manually" on page 42.
- The “If Mentioned in cim.extension.parameters” column provides information about modifying the `cim.extension.parameters` file (see "Change the CIM Extension Port Number" on page 35).
- The “Step 1 Discovery and RMI Registry Port” column provides information about the IP addresses that are required for the discovery list. The CIM Extension uses the RMI registry port. When a port other than 4673 is used for the CIM Extension, the port must be included in the discovery IP address; for example, 192.168.1.1:1234. In this instance, 192.168.1.1 is the IP address of the host, and 1234 is the port the CIM Extension uses.

Troubleshooting Firewalls

Configuration	Manual Start Parameters for CIM Extension	If mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
Firewall port 4673 opened between host and management server.	start		10.250.250.10 *OR* 172.31.250.10 *OR* 192.168.250.10 Communication Port: 4673
Firewall port 1234 opened between host and management server.	start -port 1234	-port 1234	10.250.250.10:1234 *OR* 172.31.250.10:1234 *OR* 192.168.250.10:1234 Communication

Troubleshooting Firewalls, continued

Configuration	Manual Start Parameters for CIM Extension	If mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
			Port: 1234
Firewall port 4673 opened between host and management server on the 172.31.250.x subnet.	start -on 172.31.250.10	-on 172.31.250.10	172.31.250.10 Communication Port: 4673
Firewall port 1234 opened between host and management server on the 192.168.250.x subnet.	start -on 192.168.250.10:1234	-on 172.31.250.10:1234	172.31.250.10:1234 Communication Port: 1234
With 3 firewall ports opened on different ports respectively 1234, 5678, 9012.	start -on 10.250.250.10:1234 -on 172.31.250.10: 5678 -on 192.168.250.10: 9012	-on 10.250.250.10:1234 -on 172.31.250.10: 5678 -on 192.168.250.10: 9012	10.250.250.10:1234 *OR* 172.31.250.10:5678 *OR* 192.168.250.10:9012 Communication Port: 1234, 5678, 9012
With firewall port 4673 opened between host and management server. NAT environment,	start		172.16.10.10 Communication Port: 4673

Troubleshooting Firewalls, continued

Configuration	Manual Start Parameters for CIM Extension	If mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches the other side of the firewall.			
With firewall port 1234 opened between a host and management server. NAT environment, where 10.250.250.10 subnet is translated to 172.16.10.10 when it reaches the other side of the firewall.	start -port 1234	-port 1234	172.16.10.10 Communication Port: 1234
With 3 firewall ports opened on different ports respectively 1234, 5678, 9012. NAT environment, where all 3 NICs are translated to different 172.16.x.x	start -on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012	-on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012	172.16.10.10:1234 *OR* 172.16.20.20:5678 *OR* 172.16.30.30:9012 Communication Port: 1234, 5678, 9012

Troubleshooting Firewalls, continued

Configuration	Manual Start Parameters for CIM Extension	If mentioned in cim.extension.parameters	Step 1 Discovery and RMI Registry Port
subnets.			
False DNS or IP is slow to resolve.		jboss.properties, cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	Any IP that is reachable Communication Port: 4673
No DNS, never resolve.		jboss.properties cimom.Dcxws.agency.firstwait=200000 cimom.Dcxws.agency.timeout=200000	Any IP that is reachable Communication Port: 4673
No firewall. Discover with a non-existent user for security reasons.	start -credentials string1:string2 In this instance, string1 is supplied in discovery as the “username” and string2 is supplied as the “password”.	-credentials username:password	Specify username and password in the discovery list. Communication Port: 4673
With 3 firewall ports opened on different ports, respectively 1234, 5678, 9012. Discover with a nonexistent user for security reasons.	start -on 10.250.250.10:1234 -on 172.31.250.10:5678 -on 192.168.250.10:9012 -credentials string1:string2 In this instance, string1 is supplied in discovery as the “username” and string2 is supplied as the “password”.	-on 10.250.250.10:1234 -on 172.31.250.10: 5678 -on 192.168.250.10: 9012 -credentials username:password	10.250.250.10:1234 *OR* 172.31.250.10:5678 OR 192.168.250.10:9012 Specify username and password in the discovery list. Communication Port: 1234, 5678, 9012

Log File Properties

The `cim.extension.parameters` file contains the following properties for each log file:

- `<log name>.log.File` – Sets the name of the log file.
- `<log name>.log.MaxFileSize` – Sets the maximum file size in MB.
- `<log name>.log.MaxBackupIndex` – Sets the maximum number of files created before the files are overwritten.

The default location of the CIM Extension log files is:

- *Windows*: [*Installation_Directory*]\CimExtensions\tools
- *Linux*: /opt/APPQcime/tools

Log files roll over upon reaching the configured size. Each log consists of a configured number of files.

For example, the `cxws.log` file collects most of the CIM Extension logging information. The CIM Extension appends start time, stop time, and unexpected error conditions to the existing `cxws.log` file. The default `cxws.log` file configuration in the `cim.extension.parameters` file is as follows:

```
-D cxws.log.File=cxws.log
-D cxws.log.MaxFileSize=30MB
-D cxws.log.MaxBackupIndex=3
```

By default, the `cxws.log` file rolls over each time it becomes larger than 30 MB. The `cxws.log` file is renamed `cxws.log.1`, and a new `cxws.log` file is created. When the `cxws.log` file rolls over again,`cxws.log.1` is renamed `cxws.log.2`, the `cxws.log` file is renamed `cxws.log.1`, and a new `cxws.log` file is created and so on for a maximum of three backup log files:

- `cxws.log`
- `cxws.log.1`
- `cxws.log.2`
- `cxws.log.3`

Finding the Version of a CIM Extension

To find the version number of a CIM Extension

- *Windows*: In the **Programs and Features** control panel, examine the value in the **Status** column for the AppStorWin32Agent service.
- *UNIX or Linux*: Run the following command:

  /opt/APPQcime/tools/status

To find the version number of a CIM Extension, run the following command:

/opt/APPQcime/tools/start -version

The output displays the CIM Extension version number and build date. For example:

```
Starting CIM Extension for HP-UX
CXWS for mof/cxws/cxws-HPUX.mof
CXWS version x.x.x.x, built on Fri 12-March-xxxx 12:29:49 by dmaltz
```

Checking the Status of a CIM Extension

To determine the status of a CIM Extension

- *Windows*: In the **Services** window, examine the value in the **Status** column for the AppStorWin32Agent service.
- *UNIX or Linux*: Run the following command:

  /opt/APPQcime/tools/status

Starting a CIM Extension Manually

The SOM management server can only gather information about a host when the installed CIM Extension is running.

You must have administrator or root privileges to start a CIM Extension. The CIM Extension only provides the information within the privileges of the user account that started the CIM Extension. Only administrator or root has enough privileges to provide the information the management server needs. If you do not start the CIM Extension with administrator or root privileges, the management server display messages similar to the following:

```
Data is late or an error occurred.
```

To start a CIM Extension

- *Windows*: Start the AppStorWin32Agent service from the **Services** window.

  Note: To start the AppStorWin32Agent service, you can also use the following command at the command prompt:

  [Installation_Directory]\CimExtensions\tools\net start AppStorWin32Agent

- *Linux*: Run the following command:

  /opt/APPQcime/tools/start

  Tip: You can use any of the options in the table of CIM Extension parameters when starting a CIM Extension from the command line.

Stopping a CIM Extension

The management server can only gather information about a host when the installed CIM Extension is running.

You must have administrator or root privileges to stop a CIM Extension.

To stop a CIM Extension, follow the procedure below:

- *Windows*: Stop the AppStorWin32Agent service from the **Services** window.

  Note: To stop the AppStorWin32Agent service, you can also use the following command at the command prompt:

  `[Installation_Directory]\CimExtensions\tools\net stop AppStorWin32Agent`

- *Linux*: Run the following command:

  `/opt/APPQcime/tools/stop`

Customize JVM Settings for a CIM Extension

To customize the Java virtual machine (JVM) configuration for a CIM Extension, create the `wrapper.user` file by copying and customizing the provided template file (`wrapper.user-sample`). Place the configuration file in the following directory:

- *Windows*: [*Installation_Directory*]\CimExtensions\conf
- *UNIX/Linux*: /opt/APPQcime/conf

The CIM Extension retains and uses the customized `wrapper.user` file after each future upgrade of the CIM Extension.

To configure a CIM Extension JVM

1. Log on to the host as a user with administrator or root privileges.
2. Change to the CIM Extension configuration directory:
   - *Windows*: [*Installation_Directory*]\CimExtensions\conf
   - *UNIX/Linux*: /opt/APPQcime/conf
3. Save a copy of the `wrapper.user-sample` file as `wrapper.user` in the same directory.
4. In a text editor, edit the file `wrapper.user` file according to the comments in the file.
5. Save and close the file.

6. Restart the CIM extension.
   - *Windows*:

     Restart the AppStorWin32Agent service from the **Services** window or reboot the host.

     Note: To restart the AppStorWin32Agent service, you can also use the following commands at the command prompt:

     ```
     [Installation_Directory]\CimExtensions\tools\net stop AppStorWin32Agent
     [Installation_Directory]\CimExtensions\tools\net start AppStorWin32Agent
     ```

   - *UNIX/Linux*:

     ```
     /opt/APPQcime/tools/stop
     /opt/APPQcime/tools/start
     ```

Removing CIM Extensions

To remove a CIM Extension from a host, follow the applicable procedure:

- "Remove the CIM Extension from a Windows Host" below
- "Remove the CIM Extension from an HP-UX Host" on the next page
- "Remove the CIM Extension from a Linux Host" on the next page
- "Remove the CIM Extension from a Solaris Host" on page 46
- "Remove the CIM Extension from an IBM AIX Host" on page 46

Remove the CIM Extension from a Windows Host

If you remove a CIM Extension from a Windows host where there is a service that is using WMI (such as Microsoft Exchange), you will see a message that the WMI service could not be stopped. Continue with the removal of the CIM Extension, and then reboot the host after the removal process completes.

To remove the CIM Extension from a Windows host

1. Log on to the Windows host as a user with administrator privileges.
2. Open the **Programs and Features** or the **Add or Remove Programs** control panel.
3. In the list of installed programs, right-click **Windows CIM Extension**, and then click **Uninstall**.
4. Follow the instructions on the screen.
5. After the uninstaller completes, delete the CIM Extension installation directory.

   The default location is:

   `<Drive:>\Program Files (x86)\APPQcime\CimExtensions`
6. It is recommended to reboot the host.

Remove the CIM Extension from an HP-UX Host

To remove the CIM Extension from an HP-UX host

1. Log on to the HP-UX host as the `root` user.
2. Stop the CIM Extension by running the following command:

   `/opt/APPQcime/tools/stop`
3. To ensure that you are not in the `/opt/APPQcime` directory, change to the root directory.
4. Run the following command:

   `swremove APPQcime`

   Expected output is similar to the following example:

   ```
   * Beginning Execution
   * The execution phase succeeded for hpuxqaX.dnsxxx.com:/".
   * Execution succeeded.
   ```
5. To remove the `APPQcime` directory, run the following command:

   `rm -r /opt/APPQcime`

Remove the CIM Extension from a Linux Host

To remove the CIM Extension from a Linux host

1. Log on to the Linux host as the `root` user.
2. Stop the CIM Extension by running the following command:

   `/opt/APPQcime/tools/stop`
3. Uninstall the "requires" rpm. For example:

   `rpm –e APPQcime-Requires-XX-224`
4. Uninstall the CIM Extension:

   `rpm -e APPQcime`

   Note: In case of RHEL7 host, this command might display a warning message that the file does not exist. Ignore this warning message as this an issue specific to RHEL7 kernel.
5. To remove the `APPQcime` directory, run the following command:

   `rm -r /opt/APPQcime`

Remove the CIM Extension from a Solaris Host

To remove the CIM Extension from a Solaris host

1. Log on to the Solaris host as the `root` user.
2. Stop the CIM Extension by running the following command:

   `/opt/APPQcime/tools/stop`
3. To ensure that you are not in the `/opt/APPQcime` directory, change to the root directory.
4. Type the following command:

   `pkgrm APPQcime`
5. To remove the CIM Extension, type `y`.
6. To remove the `APPQcime` directory, run the following command:

   `rm -r /opt/APPQcime`

Remove the CIM Extension from an IBM AIX Host

To remove the CIM Extension from an IBM AIX, run the `installp -u APPQcime` command at the command prompt or follow the procedure below:

1. Make sure **preview** is set to **No**. See the AIX documentation for more information.
2. Stop the CIM Extension as described in "Stopping a CIM Extension" on page 43.
3. Enter the following at the command prompt:

   `smit-C`
4. Select **Software Installation and Maintenance**.
5. Select **Software Maintenance and Utilities**.
6. Select **Remove Installed Software**.
7. In the SOFTWARE name, press **Esc+4** and select:

   `APPQcime`
8. On the same page you selected APPQcime, select **No** for Preview by pressing the **Tab** key.
9. Press **Enter** to remove the software.
10. To remove the `APPQcime` directory, run the following command:

    `rm -r /opt/APPQcime`

Troubleshooting CIM Extensions

The following topics describe some common approaches to troubleshooting a CIM Extension:

- "Agent Service Does Not Start (Windows Only)" below
- "CIM Extension Hangs Because of Low Entropy (Linux Only)" below

Agent Service Does Not Start (Windows Only)

The CIM agent service, `AppStorWin32Agent`, might not start after you install the agent on a Windows Server 2003/2008 R2 IA64 platform.

This issue appears if the JVM exits because of a memory allocation issue during the start of the agent on Intel® Itanium®-based computers.

To resolve this issue:

1. Open the following file in a text editor:

   `[Installation_Directory]\CimExtensions\conf\wrapper.user`
2. Decrease the value of the property `wrapper.java.maxmemory`. For example, if the current value is 1024, reduce the value to 512.
3. Restart the AppStorWin32Agent service from the **Services** window or reboot the host.

> **Note:** To restart the AppStorWin32Agent service, you can also use the following command at the command prompt:
>
> ```
> [Installation_Directory]\CimExtensions\tools\net stop AppStorWin32Agent
> [Installation_Directory]\CimExtensions\tools\net start AppStorWin32Agent
> ```

CIM Extension Hangs Because of Low Entropy (Linux Only)

At times, the Linux CIM Extension might hang on startup due to low entropy.

The Linux kernel uses keyboard timings, mouse movements, and IDE timings to generate entropy for `/dev/random`. Entropy gathered from these sources is stored in an “entropy pool,” and random values returned by `/dev/random` use this pool as a source. This means that `/dev/random` does not return any values if the entropy counter is too low, and programs reading from `/dev/random` are blocked until there is enough collected entropy. This behavior can happen on servers with no keyboards, no mice, and no IDE disks.

1. To determine whether the Linux agent is hung due to this problem, run the following command:

   `kill -3 java_process_id`

In this instance, java_process_id is the process ID of the Java process for the Linux agent. It is not the process ID returned by the `status` command.

The preceding command generates the stack trace, which should be similar to the following example:

```
INFO | jvm 1 | 2006/11/22 10:56:58 | at java.security.SecureRandom.next(Unknown
Source)
INFO | jvm 1 | 2006/11/22 10:56:58 | at java.util.Random.nextInt(Unknown Source)
INFO | jvm 1 | 2006/11/22 10:56:58 | at
com.sun.net.ssl.internal.ssl.SSLContextImpl.engineInit(Unknown Source)
INFO | jvm 1 | 2006/11/22 10:56:58 | at javax.net.ssl.SSLContext.init(Unknown Source)
INFO | jvm 1 | 2006/11/22 10:56:58 | at
com.appiq.cxws.agency.agent.AgentMessageDispatcher.
createServerSocket(AgentMessageDispatcher.java:1
INFO | jvm 1 | 2006/11/22 10:56:58 | at
com.appiq.cxws.agency.agent.AgentMessageDispatcher.
startAccepting(AgentMessageDispatcher.java:74)
```

2. To fix the problem, in the `/opt/APPQcime/conf/wrapper.conf` file, in the Java Additional Properties section, search for the property, `wrapper.java.additional.N=-Djava.security.egd=file:/dev/random` and change `random` to `urandom`.

   After the change, the property should be similar to:

   `wrapper.java.additional.`*`N`*`=-Djava.security.egd=file:/dev/urandom`

3. Restart the CIM Extension:

   `/opt/APPQcime/tools/stop`
   `/opt/APPQcime/tools/start`

Chapter 5: Configuration

This chapter contains an introduction to concepts, initial configurations required, defaults provided by SOM, some best practices and planning information that will help you implement SOM in your environment.

Ports and Firewall

The SOM management server uses various ports for communicating with the managed environment, the SOM console, and the SOM reporting server. The port configuration is largely decided by the proxy configuration of the managed devices. Ensure that the required configurations are enabled in the firewall configuration before starting the product installation. This will remove delays in discovering the managed environment once the product is deployed.

The following table shows the ports SOM used on the management server.

Legend	
I/O	The port must be opened on both SOM server and the target device.
O	The port must be opened on the target device.
I	The port must be opened on the source server; for example, the SOM management server.

Ports Used on the SOM Management Server

Port	Type	Name	Purpose	Change Configuration	In/Out
80	TCP	nmsas.server.port.web.http	Default HTTP port used for Web UI and Web Services; after this port is open, it becomes bi- directional.		I/O
443	TCP	nmsas.server.port.web.https	Default secure HTTPS port (SSL); used for Web UI and Web Services.	Modify the nms-local.properties file	
1098	TCP	nmsas.server.port.naming.rmi	• Used by SOM command line tools to communicate with a variety of services used by	Modify the nms-local.properties file	

Ports Used on the SOM Management Server, continued

Port	Type	Name	Purpose	Change Configuration	In/Out
			SOM • HPE recommends configuring the system firewall to restrict access to these ports to localhost only		
1099	TCP	nmsas.server.port.naming.port	• Used by SOM command line tools to communicate with a variety of services used by SOM. • HPE recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the nms-local.properties file	
3873	TCP	nmsas.server.port.remoting.ejb3	• Used by SOM command line tools to communicate with a variety of services used by SOM. • HPE recommends configuring the system firewall to restrict access to these ports to localhost only	Modify the nms-local.properties file	
4444	TCP	nmsas.server.port.jmx.jrmp	• Used by SOM command line tools to communicate with a variety of services used by SOM. • HPE recommends configuring the system firewall to restrict access to these ports to localhost only.	Modify the nms-local.properties file	
4445	TCP	nmsas.server.port.jmx.rmi	• Used by SOM command line tools to communicate with a variety of services used by	Modify the nms-local.properties file	

Ports Used on the SOM Management Server, continued

Port	Type	Name	Purpose	Change Configuration	In/Out
			SOM. • HPE recommends configuring the system firewall to restrict access to these ports to localhost only		
4446	TCP	nmsas.server. port.invoker.unified	• Used by SOM command line tools to communicate with a variety of services used by SOM. • HPE recommends configuring the system firewall to restrict access to these ports to localhost only.	Modify the nms-local.properties file	
4712	TCP	nmsas.server. port.ts.recovery	Internal transaction service port .	Modify the nms-local.properties file	
4713	TCP	nmsas.server. port.ts.status	Internal transaction service port.	Modify the nms-local.properties file	
4714	TCP	nmsas.server. port.ts.id	Internal transaction service port.	Modify the nms-local.properties file	
5432	TCP	com.hp.ov.nms. postgres.port	This PostgreSQL port is the port the embedded database listens on for this SOM management server.	Modify the nms-local.properties file	
8886	TCP	OVsPMD_MGMT	SOM ovspmd (process manager) management port.	Modify the /etc/services file	
8887	TCP	OVsPMD_REQ	SOM ovsmpd (process manager) request port.	Modify the /etc/services file	
8989	TCP	com.hp.ov.nms. events.action.server.port	Enables the action server port to be configurable.	Modify the nnmaction.properties file	

Ports Used for Communication Between the SOM Management Server and Other Systems

Port	Type	Purpose	Client, Server	In/Out
80	TCP	Default HTTP port for SOM; used for Web UI and Web Services.	Server	
80	TCP	Default HTTP port for SOM connecting to other applications. The actual port depends on SOM configuration.	Client	
389	TCP	Default LDAP port.	Client	
443	TCP	Default secure HTTPS port for SOM connecting to other applications; the actual port depends on SOM configuration. Default HTTPS port forHPE OMi on Windows.	Client	
443	TCP	Default secure HTTPS port; used for Web UI and Web Services .	Server	
636	TCP	Default secure LDAP port (SSL).	Client	
135	TCP	psexec port, Windows Agentless on the management server.	Server	
445	TCP	psexec port, Windows Agentless on the management server.	Server	
139	TCP	winexe port, Windows Agentless on the management server.	Server	
383	TCP	LCore communication port on CMS used for communication with the SOM reporting server.	Server	
5433	TCP	Receive analytics data from the SOM reporting server.	Client	I

Device Specific Ports used by SOM

Device	Device Interface	Port (SOM Outbound/Device Inbound)
Storage		
HPE 3PAR*	SMI-S	22, 5989
HP EVA	SMI-S	5989
HPE StoreEasy Storage	WMI	135, 445
HPE XP	RMI-API	1099, 51099, 51100
NetApp 7 Mode, NetApp	ONTAP API	443

Device Specific Ports used by SOM, continued

Device	Device Interface	Port (SOM Outbound/Device Inbound)
Cluster Mode		
Hitachi AMS, Hitachi Unified Storage, Hitachi VSP	XML	1099, 2001, 51099, 51100
IBM SAN Volume Controller*, IBM Storwize V7000*, IBM XIV	SMI-S	5989
EMC CLARiiON*, EMC VNX Block*, EMC Symmetrix*	SMI-S	5989
EMC VNX Filer*	XML API	443
EMC VPLEX	REST API	443
EMC Isilon	SSH	22
Switches		
Brocade Switch*	SMI-S	5989
Cisco Switch*	SNMP v2, v3	161
Hosts		
HP-UX	SSH (Agentless)	22
	CIM Extension	4673
IBM AIX	SSH (Agentless)	22
	CIM Extension	4673
IBM HMC	SSH (Agentless)	22
Red Hat Enterprise Linux (RHEL)	SSH (Agentless)	22
	CIM Extension	4673
Solaris host	SSH (Agentless)	22
	CIM Extension	4673

Device Specific Ports used by SOM, continued

Device	Device Interface	Port (SOM Outbound/Device Inbound)
SuSE Linux	SSH (Agentless)	22
	CIM Extension	4673
Windows Agentless (for Windows Management Server)	WMI (Agentless)	135, 445
Windows Agentless (for Linux Management Server)	WMI (Agentless)	139
Windows Host	CIM Extension	4673

Note: * Incidents supported for these devices.

Note: For devices with Incident support, the device inbound port is 161 and SOM inbound port is 162.

Node Groups

A Node Group is a collection of nodes (elements) or child node groups that have the same device filter criteria. After discovery elements are automatically assigned to node groups based on predefined attributes.

Node groups can be used for any or all of the purposes:

- For categorization that enables you to identify basic categories in the system, such as hosts, storage systems, switches, and fabrics.
- Categorization enables you with easier monitoring and administration. It helps you apply settings to a group and avoid dealing with elements on an individual basis. For example, you can implement a data collection policy on a node group rather than on individual elements.
- As a primary filtering technique for customizing different views.
- User access control to limit access to a set of nodes through security mappings.

Default Node Groups

SOM provides the following default node groups. These are configured with specific information about your management domain. You can change them to meet your needs.

- All Elements
- FC Fabrics
- FC Switches
- Hosts
- Storage Systems

These are based on device categories derived from the system object ID during the discovery process.

Node Group Membership

You can create additional node groups based on your environment and requirements. You can define attributes to determine node group membership.

Each node group is defined using one or more of the following options:

- "Device Filters" below
- "Additional Filters" below
- "Additional Nodes" on the next page
- "Child Node Groups" on the next page

Device Filters

Device filters provide categories such as device category, vendor, family, or device profile. Nodes must match at least one specification to belong to the node group.

During discovery, SOM collects direct information through SNMP queries and derives other information from that through device profiles. By gathering the system object ID, SOM can index through the correct device profile to derive the following information:

- Vendor
- Device category
- Device family within the category

These derived values, in addition to the device profile itself, are available for use as filters. For example, you can group all objects from a specific vendor, regardless of device type and family. Or you can group all devices of a type such as router, across vendors.

Additional Filters

With this option you can specify additional filters using Boolean expressions based on a list of object attributes.

Use the additional filters editor to create custom logic to match fields including:

- tenantName (Name)
- securityGroupName (Security Group)
- sysName (System Name)
- sysLocation (System Location)
- sysContact (System Contact)
- hostname (Hostname, case-sensitive)
- hostedIPAddress (Address)
- mgmtIPAddress (Management Address)
- nodeName

Filters can include the AND, OR, NOT, EXISTS, NOT EXISTS, and grouping (parentheses) operations. See "Specify Node Group Additional Filters" in the SOM Online help for more information.

Additional Nodes

This option enables you to add additional nodes to the node group regardless of any filters.

It is better to use Additional Filters to qualify nodes for node groups. If the environment contains critical devices that are too difficult to qualify using filters, add them to a group by individual host name. Add nodes to a node group by individual host names only as a last option.

Child Node Groups

Enables you to add node groups to the node group to establish hierarchical containers. Child node groups are treated similarly as additional nodes.

Node Groups Evaluation

SOM evaluates each discovered node to determine its node group membership using the following criteria:

- Any node that matches one or more entries (if any exist) on the Device Filters tab and the filter specified on the Additional Filters tab is a member of the node group.
- All nodes specified on the Additional Nodes tab are members of the node group.
- All nodes that are members of at least one node group specified on the Child Node Groups tab are members of the node group.

Group Overlap

Regardless of the intended uses for group definitions, the first step is to define which nodes are members of a group. Because you can create groups for different purposes, each object can be included in multiple groups. Consider the following example:

- You might want to group all HPE 3PAR arrays into single group using the Device Profile filter.
- Top elements are automatically assigned to the default node group of Storage Systems.
- You might want to collect data from all storage arrays regardless of device vendor or device family.

The 3PAR array with an IP address 10.10.10.3 would qualify for all three groups. You want to find the balance between having a usably rich set of groups available for configuration and viewing, and overloading the list with superfluous entries that will never be used.

Hierarchies/Containment

You can create simple, reusable, atomic groups and combine them hierarchically for monitoring or visualization. Using hierarchical containers for nodes greatly enhances map views by providing cues about the location or type of object at fault. SOM gives you complete control of the definition of the groups and their drill-down order.

You can create simple, reusable atomic groups first, and then specify them as child groups as you build up. Alternatively, you can specify your largest parent group first and create child groups as you go.

For example, your environment might contain EMC CIARiiON storage systems and VNX Filer. You can create parent groups for EMC devices and for all file storage. Because the hierarchy is specified when you create the parent and designate its children, each child group, such as EMC devices, can have multiple parents.

Hierarchies work well for the following situations:

- Types of nodes with similar monitoring needs
- Types of nodes to be quarantined together
- Groups of nodes by operator job responsibility
- When you use groups in map views and table views

Note: Keep in mind that as you use group definitions to specify monitoring configuration, hierarchy does not imply ordering for settings. The settings with the lowest ordering number apply to a node. By carefully incrementing ordering numbers, you can emulate inheritance concepts for settings.

Planning Node Groups

SOM provides a default collection of node groups to simplify your configuration tasks. You can use existing groups, modify them, or create your own. Over time HPE might add more default groups to simplify your configuration tasks.

Interaction with Device Profiles

When each device is discovered, SOM uses its system object ID to index into the list of available

Device Profiles. The Device Profile is used to derive additional attributes of the device, such as vendor, product family, and device category.

As you configure node groups, you can use these derived attributes to categorize devices to apply data collection settings. For example, you might want to collect data from all devices regardless of vendor throughout your environment at a certain interval. You can use the derived device category, Storage System, as the defining characteristic of your node group. All discovered devices whose system object ID maps to the category, Storage Systems, will receive the configured settings for the node group.

Considerations for Planning

Determine the criteria by which you want to group nodes. Following are some factors you can consider while planning node groups:

- Which are the critical devices that you want to collect data?
- Do you want to differentiate data collection intervals or data gathered by device type?
- Can you use the default node groups provided by SOM?

Recommendations for Planning Node Groups

Some key points to consider while planning node groups for your environment:

- Keep in mind that node groups add overheads to the system. Therefore, ensure that you have valid use cases based on your needs when creating node groups.
- Create node groups that cater to a definite purpose. Identify your topmost use cases before you begin planning your node groups. For example, you could create node groups for managing Windows hosts, Linux hosts or storage devices based on vendor, model or the device profile. You could then attach data collection or monitoring policies to these node groups.
- Use different node groups for different purposes. Not all node groups created for data collection makes sense for filtering views or restricting node access. So you will need to configure them independently based on the purpose.
- Find a balance by creating a rich set of groups for monitoring purpose and viewing purpose without overloading the system with a large number of superfluous node groups that will never be used.
- Do not use the Additional Nodes tab extensively to add nodes to a node group as it consumes excessive resources on the management server. As a rule of thumb, node group definitions should be filter-driven and this feature should be used as an exception.

Discovery

The devices that comprise your Storage Area Network (SAN) must be discovered so that they can be monitored and managed by SOM. To discover devices in your network, you must configure the addresses for

discovery and provide credentials, if required.

Notes on discovery before you begin planning:

- SOM does not perform any default discovery. You must configure discovery before any elements appear in the Inventory views.
- Discovery is handled on an individual address basis. The status of each address configured for discovery indicates whether the discovery is successful or not.
- The process of initial discovery takes some time depending on the number of addresses you have configured for discovery.
- You can create credentials and then associate them to multiple addresses.
- The Discovery Hint option enables you to select a value, based on which SOMinvokes only the selected provider for discovering the device instead of invoking all the providers thereby reducing discovery time.

Methods of Discovery

SOM provides the following methods of discovery.

Method	Notes
Automatic Discovery (*only initial discovery*)	Default method for initial discovery. Multiple elements can be discovered at once.
Manual Discovery	Only one element can be discovered.
Importing Addresses from a file	Discovery settings from a previous installation.

Automatic Discovery

This is the default and recommended method for initial discovery. This is best suited when you have a large bulk of addresses to be discovered. The discovery addresses that you add or import get into the queue for discovery after a pre-configured time.

Notes on automatic discovery

- Runs only run once during initial discovery
- Allows for multiply devices to be discovered at once, as well as scanning on a range of IP addresses.

Manual Discovery

This method is best suited when you have to add a single element or you have a small number of elements to be discovered. You must associate the device-specific credentials before you begin discovery. Though this method provides a tighter control over discovery, this is time-consuming if you have a large number of addresses to be discovered.

Importing Discovery Settings from a File

If you have discovery settings from a previous installation, you can import it into the management server rather than re-enter the information. The import discovery settings feature enables you to import the following information:

- IP addresses to be discovered
- Default user names and passwords, which are encrypted
- Agentless host inference rules

Notes on import:

- To prevent re-entering the information for each management server instance, you can import the same file for multiple management server instances.
- If you already have an existing configuration, and you import another configuration, the new configuration is merged with the previous one. Only the unique addresses are added and discovery will be queued only for these addresses.
- SOM also supports importing the configurations using a CSV file. You can enter the details of the discovery addresses, the discovery ranges and the host inference rules in a CSV file and import it using the `somdiscoveryconfigexportimport` command. See the *SOM CLI Reference Pages* for more information.
- If you receive an error message when you try to import the discovery settings, verify that you are using the right password. If you are using the correct password, there is a possibility that the file is corrupt.

When you import discovery settings file, it triggers automatic discovery of addresses. If you do not want to use automatic discovery, you can disable the option.

Host Discovery

SOM provides the following methods to discover and manage hosts and their associations to storage devices.

Discovery Method	Description
Discovery with a CIM Extension	Manage hosts by installing a CIM Extension on the host.
Agentless discovery	Manage hosts without installing a CIM Extension.
Inferred agentless discovery	Gather information from hosts based on host security groups, zones, and zone aliases without installing a CIM Extension to be installed.

Discovery with a CIM Extension

A SOM CIM Extension is a collection agent that runs on a storage host to gather information about that host. The SOM management server communicates with the CIM Extension while discovering and managing the

host. Install the CIM Extension on each host that you want to manage. The CIM Extension must be running for the management server to obtain information from the host.

If you change the password of a host after you discover it, you must change the password for the host in the discovery list, and then you must stop and restart the CIM Extension running on that host before you run a discovery.

Agentless Discovery

Agentless discovery provides management server the capability to discover hosts without installing the CIM Extension on the host. The management server supports the agentless discovery for hosts running on Microsoft Windows, Linux operating systems and Solaris systems.

The management server uses the following to discover a host:

- The Windows Management instrumentation (WMI) for discovering Windows host.
- Secure Shell (SSH) for discovering Linux hosts.

Agentless discovery works only if a CIM Extension is not running on the host to be discovered. If the management server finds a CIM Extension running on the host, by default it prefers discovery using a CIM Extension over the agentless discovery.

You can also rediscover hosts, which are already discovered using the CIM Extension in the management server, using the agentless discovery. However, all the history information associated with the host and applications on the host is deleted from the management server.

Data collected from the host depends on the discovery method used to gather information from the host. The following table summarizes the data collected for hosts based on the discovery method. Use the table as a guide to plan your approach to host discovery.

Inferred Agentless Discovery

SOM can display and gather information from hosts without CIM Extensions. You can infer agentless hosts by creating rules based on host security groups, zones or zone aliases configured on storage systems and fabrics in the SAN. After inferring hosts, you can discover the hosts by providing the credentials. If the discovery is successful, the hosts are reconciled and the inferred hosts become managed hosts.

Data collected from hosts varies based on the discovery method. You can plan host discovery based on the type of data you want to collect from the hosts.

Capabilities of Agentless Discovery

The management server gathers following information from a host discovered using the agentless discovery:

- Host associations to the applications, storage, and network devices.
- IP/DNS related information
- Gathers detailed configuration information for every host.

- Logical storage volume information, including mount points, physical devices, drive types, and file system details.
- Disk partition information, including disk partition names, mapped logical volumes, mapped physical drives, and total capacity.
- Disk drive information, including drive names, SCSI bus information, and mapped disk partitions.
- Multipathing and Volume Manager Configuration details.
- Information related to HBAs.

Limitations of Agentless Discovery

Although, agentless discovery enables the management server to discover and find extensive information related to the hosts, it has some limitations.

Note: All the mentioned limitations can be overcome by installing a CIM Extension on the host.

SOM will discover Windows host using agentless configuration on a host running CIM Extension if Discovery hint for agentless is provided during discovery.

Following are the limitations for an agentless host, based on the operating system it is running on:

Limitations for Windows hosts

- A user account with non-administrator privileges cannot discover a Windows host.
- Public folders and mailbox information is not available.
- Limited information related to disk partitions and disk drives is available, when the native volume manager volumes are used to obtain data. It is because the management server does not support the native volume manager software that is the Microsoft Virtual Disk Service Dynamic Provider.

Limitations for Linux hosts

- Following information is not available for a non-root user account:
  - Information related to Veritas DMP devices is not available.
  - Information related to serial number and manufacturer of the system is not available.
  - Information related to disk drives and disk partitions is not available.
- The following performance metrics are not available for a Linux host:
  - Disk Read
  - Disk Total
  - Disk Utilization

- Disk Write
- Processor utilization

- The number of target mappings obtained by the agentless discovery may be less than the number of target mappings returned by the CIM Extension. This difference is because some target mapping entries with a SCSI LUN value of zero are not shown.
- Following issues are observed for the Linux hosts containing HBAs discovered in the management server:
  - Following information is not available for HBAs:
    - Vendor name
    - Serial number
    - Hardware version
    - Information for Port Type on HBA Port Properties page.
  - When you try to rediscover the agentless hosts using the CIM Extension, the management server does not reconcile the HBA information obtained during the agentless discovery against the information obtained using CIM Extension. The old HBA data obtained using the agentless discovery is deleted and new information is collected for HBAs using the CIM Extension discovery. Thus, all the custom information related to HBAs is deleted when the host is rediscovered using the CIM Extension.
  - For a Linux host containing HBAs with dual port adapter, each port is displayed as an individual adapter on the HBA adapter page with each adapter mapped with its port on the HBA port page.
  - Bindings page is not updated when the following is performed:
    - Paths to the LUNs are disabled.
    - HBA port is disabled.
    - Subsequent data collection is run.

    This limitation can be overcome by rebooting the host. The Bindings page is automatically updated on rebooting the host.

Tenant and Initial Discovery Security Group Assignments

When SOM discovers elements in your storage network environment, Tenant and Security Group settings are established in the following manner:

When providing an address for discovery, specify a tenant for each discovery address. A node is automatically created for an IP address that is discovered successfully. When you define a tenant, then you must specify an Initial Discovery Security Group. A newly created node associated with a defined tenant is mapped to the security group (the Initial Discovery Security Group) that is associated with the selected tenant. Administrators can change either the node's tenant or security group assignment or both at any time.

Nodes assigned to the Default Security Group are visible from all views. To control access to a device, assign that device to a security group other than the Default Security Group.

Nodes within one tenant can each be assigned to different security groups, and nodes within one security group each be assigned to different tenants.

Consider setting up your security configuration so that all newly-discovered nodes belong to a security group that is mapped to User Group = SOM Administrators. Those nodes will be visible only to SOM administrators until an administrator intentionally moves the node into a security group that is also visible to the appropriate SOM operator or guest.

Tenant assignments are useful for identifying node groups within your network environment. Security group assignments enable administrators to restrict the visibility of nodes within the SOM console to specific user groups.

Host Clusters

The management server provides full support for managing clusters. Cluster support includes the following features:

- Clusters are recognized as managed elements.
- Cluster capacity utilization is accurately reported.
- The management server supports automatic discovery of several popular cluster servers.

Recommendations for Planning Discovery

Key points to consider when you plan discovery for your storage environment:

The maximum number of addresses for which you can start discovery from the user interface at a time is 1000. To configure addresses beyond this number, use the `somdiscoveryconfigexportimport.ovpl` command.

- To configure bulk discovery, set the following two properties in the `ovjboss.jvmargs` file.
  - da.bulkDiscoveryQueueSize default: 100
  - da.bulkDiscoveryIntervalInSeconds default: 20

  The file is located at `<Install_Dir>\HP\HP BTO Software\shared\nnm\conf\props\ovjboss.jvmargs`
- Plan sequence of discovery such that you discover switches first, storage systems followed by hosts. This helps reduce time to value in realizing connectivity information.
- Use the Queue Discovery option to automate the discovery process rather than manually discover each address.

- SOM relies on a healthy database and sufficient disk space to function properly. If you include the management server address for discovery and discover the management server, SOM will monitor its own health. You can review the product health using the Product tab on the System Information page (**Help** > **System Information**).
- Each discovered node (physical or virtual) counts toward the license limit. The capacity of your license might influence your approach to discovery.

Recommendations for Data Collection Policies

Key points to consider for data collection configuration:

- For effective data collection with minimal overload on the system, set the blackout period to less than or equal to half of the freshness interval. For example, if the freshness interval is 24 hours, the blackout period should not be more than 12 hours.
- It is good to ensure that data collection are not failing because of some very basic reasons such as provider problem, bad credentials, network issues, and such others. These failures add unnecessary overload to the system since there is at least one more data collection retry before the element is quarantined. After such elements are quarantined, visit the "Failure" pie in the collection dashboard to look for elements that report these errors. Take appropriate action to ensure that future data collections are successful and then manually un-quarantine the elements.
- When you assign priorities to policies, do not use numbers in a continuous sequence such as 0, 1, 2, 3, 4, 5, and so on. Ideally use multiples of a positive integer to set the priorities. For example, if you use multiples of 5 as the priority such as 5, 10, 15, 20, and so on. And suppose you want to modify the policy which has a priority of 10. You can change the priority to any number such as 12. This practice is helpful as you don’t have to change priorities of all policies that have priorities in immediate succession.

Enable Storage Tier Configuration

By default, storage tiers are not visible in the SOM console Configuration workspace. When storage tier configuration is enabled, the Storage Tiers folder is available in the Configuration workspace for all users with the Administrators role.

To enable storage tier configuration, follow these steps:

1. Back up the following file:
   - *Windows*: `%OvDataDir%\conf\som\custom.properties`
   - *Linux*: `/var/opt/OV/conf/som/custom.properties`
2. In a text editor, open the `/var/opt/OV/conf/som/custom.properties` file.
3. Set the `StorageTierEnabled` custom property to `Y`.
4. Restart the SOM services.

Recommendations for Monitoring Performance

Following are some recommendations to consider while configuring monitoring policies:

- Creating too many monitoring policies can add overheads to the system. You should create monitoring policies only for devices and the metrics on those devices that you want to monitor.
- The default interval set during creation of a policy is 15 minutes. It is recommended that you do not have intervals less than 15 minutes as this overloads the system. If you must use intervals less than 15 minutes, it is strongly recommended that you apply this to a very limited set of devices and change it to default interval as early as possible.
- When you assign priorities to policies, do not use numbers in a continuous sequence such as 0, 1, 2, 3, 4, 5, and so on. Ideally use multiples of a positive integer to set the priorities. For example, if you use multiples of 5 as the priority such as 5, 10, 15, 20, and so on. And suppose you want to modify the policy which has a priority of 10. You can change the priority to any number such as 12. This practice is helpful as you don’t have to change priorities of all policies that have priorities in immediate succession.
- Since metric collection is policy-driven, optimize your metric collection with a carefully planned approach:
  - Plan your node groups effectively by identifying high priority devices in your environment. Group collectors logically that is relevant to the node groups, for example do not associate host collectors to a storage system node group.
  - Set schedule intervals judiciously, as explained above.
  - Before configuring monitoring policies in your environment, ensure that one round of data collection is completed for the bulk of the environment. This can be verified from the collection status dashboard. As a rule of thumb, do not configure monitoring policies when a large number of data collections are in ‘Running’ state.

Managing Certificates

A certificate identifies the web server to the browser. This certificate can be self-signed or signed by a CA (Certificate Authority). The `nnm.keystore` file stores private keys and certificates with their corresponding public keys. The `nnm.truststore` file contains certificates from other parties that you expect to communicate with, or from Certificate Authorities that you trust to identify other parties. SOM includes a self-signed certificate in both of the `nnm.keystore` and `nnm.truststore` files.

This chapter contains instructions to replace an expired certificate with a new self-signed or CA-signed certificate.

An administrator can disable HTTP and other unencrypted access from the network to SOM. See the *SOM Hardening Guide*.

This chapter contains the following topics:

About SOM Certificates

This section describes useful terminology to help you work with certificates. Familiarize yourself with the terms mentioned in the following table.

Certificate Terminology

Concept	Description
Keystore and Truststore	**Truststore**: SOM truststore is the `nnm.truststore` file in which you store public keys from sources that you want SOM to trust. **Keystore**: SOM keystore is the `nnm.keystore` file in which you import SOM server's private key. The nnm.truststore and nnm.keystrore files are located at: • Windows: `%OvDataDir%\shared\nnm\certificates\` • Linux: `/var/opt/OV/shared/nnm/certificates/`
Default SOM certificates	SOM is installed with a self-signed certificate generated using default properties. You can replace the default certificate with another self-signed or CA-signed certificate.
Supported	SOM accepts certificates generated using RSA algorithm. DSA algorithm is not supported.

Certificate Terminology, continued

Concept	Description
encryption algorithms	
Self-Signed Certificate	A self-signed certificate is typically used for establishing secure communication between your server and a known group of clients. SOM installs with a self-signed certificate generated using default properties. **Note:** SOM instances configured to use a self-signed certificate will display a warning message when users try to access the SOM console in a web browser.
CA-Signed Certificate	Signed server certificate that you receive in response to the Certificate Signing Request will contain the SOM certificate that is CA signed and one or more CA certificates (if there is more than one CA certificate, this is also known as the certificate chain). **Note:** These certificates might be in a single file or in a two separate files.
Root CA Certificate	Identifies the certificate authority that is trusted to sign certificates for servers and users.
Intermediate CA Certificate	A certificate signed by either a root or intermediate CA that is itself an authority, rather than a server or user. **Note:** The list of certificates from the SOM server certificate to the root CA certificate, including any intermediate CA certificates, is known as the certificate chain.

Replacing an Existing Certificate with a new Self-Signed or CA-Signed Certificate

A self-signed certificate is created and installed during SOM installation. You would typically replace a certificate in any of the following scenarios:

- To use a new self-signed or CA-signed certificate instead of the default certificate.
- To renew an expired certificate.

To replace a certificate, do the following:

1. Generate a self-signed certificate. For details, see "Generating a Self-Signed Certificate" below.
2. If you organization requires the certificate to be signed by a CA, generate a CSR (Certificate Signing Request) file and obtain a CA signed certificate. For details, see "Generating and Installing a CA-Signed Certificate" on the next page
3. Open the following file and update the `com.hp.ov.nms.ssl.KEY_ALIAS` variable to the value you used for `<alias>` while generating a certificate.
   - *Windows*: `%OvDataDir%\conf\nnm\props\nms-local.properties`
   - *Linux*: `/var/opt/OV/conf/nnm/props/nms-local.properties`
4. Restart the SOM services.
   a. Run the `ovstop` command on the SOM management server.
   b. Run the `ovstart` command on the SOM management server.
5. Test HTTPS access to the SOM console using the following syntax:
   https://<fully_qualified_domain_name>:<port_number>/som/
   - If you have used a CA-signed certificate and if the web browser trusts the CA, the browser will trust the HTTPS connection to the SOM console.
   - If you have used a self-signed certificate, the web browser displays a warning message about the untrusted HTTPS connection to the SOM console.

Generating a Self-Signed Certificate

To generate a self-signed certificate, follow these steps:

1. Change to the directory on the SOM management server that contains the `nnm.keystore` and `nnm.truststore` files:
   - *Windows*: `%OvDataDir%\shared\nnm\certificates`
   - *Linux*: `/var/opt/OV/shared/nnm/certificates`
2. Save a backup copy of the `nnm.keystore` file.

Note:

- If you are replacing an existing SOM certificate, do not remove the existing certificate until you complete these steps. SOM must start up at least once with both the old and new certificate installed so that it can transfer encrypted information to the new certificate.
- Make sure the alias points to the new certificate as described in the next step to ensure SOM presents the new certificate on the SOM management server to the client servers.

3. Generate a private key from your system. Use the keytool command to generate this private key:
   a. Run the following command exactly as shown:
      - *Windows*: **%OvInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -genkeypair - validity 3650 -keyalg rsa -keystore nnm.keystore -storepass nnmkeypass - alias <*alias_name*>**
      - *Linux*: **/opt/OV/nonOV/jdk/hpsw/bin/keytool -genkeypair -validity 3650 -keyalg rsa -keystore nnm.keystore -storepass nnmkeypass -alias <*alias_name*>**

      Note: The alias, referred to as <*alias_name*> in this example, identifies this newly-created key. Although the alias can be any string, it is recommended to use the fully-qualified domain name (FQDN) followed by a suffix to help you easily identify the right version. For example, you can use alias name as `myserver.mydomain-<number>` or `myserver.mydomain-<date>`.

   b. Enter the requested information.

      Caution: When prompted for your first and last name, enter the FQDN of your system.

      A self-signed certificate is generated.

      For obtaining CA-signed certificates, you need to additionally generate and submit a CSR file to a CA. For more information, see "Generating and Installing a CA-Signed Certificate" below.

Generating and Installing a CA-Signed Certificate

To obtain and install a CA-signed certificate, follow these steps:

1. Generate a self-signed certificate. For details, see "Generating a Self-Signed Certificate" on the previous page.
2. Run the following command to create a CSR (Certificate Signing Request) file:
   - *Windows*:**%OvInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -keystore nnm.keystore -certreq -storepass nnmkeypass -alias <*alias_name*> -file CERTREQFILE**
   - *Linux*: **/opt/OV/nonOV/jdk/hpsw/bin/keytool -keystore nnm.keystore -certreq -storepass nnmkeypass -alias <*alias_name*> -file CERTREQFILE**

   Note:
   - In the command above, <*alias_name*> corresponds to the alias you had provided at the time of generating the certificate.
   - For more information about the `keytool` command, search for “Key and Certificate Management Tool” at **http://www.oracle.com/technetwork/java/index.html**.

3. Send the CSR to your CA signing authority which signs and returns the certificate files. For information about different types of CA certificates, see "Types of CA-Signed Certificates" on page 73.
4. Copy the files containing these certificates to a known location on the SOM management server. For this example, copy the files to the following location:
   - *Windows*: `%OvDataDir%\shared\nnm\certificates`
   - *Linux*: `/var/opt/OV/shared/nnm/certificates`
5. Change to the directory on the SOM management server that contains the `nnm.keystore` and `nnm.truststore` files:
   - *Windows*: `%OvDataDir%\shared\nnm\certificates`
   - *Linux*: `/var/opt/OV/shared/nnm/certificates`
6. Run the following command to import the certificate into the `nnm.keystore file:`
   - *Windows*: **`%OvInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -importcert -trustcacerts -keystore nnm.keystore -storepass nnmkeypass -alias <alias_name> -file <myserver.crt>`**
   - *Linux*: **`/opt/OV/nonOV/jdk/hpsw/bin/keytool -importcert -trustcacerts -keystore nnm.keystore -storepass nnmkeypass -alias <alias_name> -file <myserver.crt>`**

   Note:
   - In the above command,
     - `<myserver.crt>` corresponds to the full path of the location where you have stored the signed server certificate.
     - `<alias_name>` corresponds to the alias you had provided at the time of generating the certificate.
   - If you use the `-storepass` option and provide the password, the keystore program does not prompt you for the keystore password. If you do not use the `-storepass` option, enter **`nnmkeypass`** when prompted for the key store password.
7. When prompted to trust the certificate, enter: **y**

   The output from the command is of the form:

   ```
   Owner: CN=SOM_server.example.com
   Issuer: CN=SOM_server.example.com
   Serial number: 494440748e5
   Valid from: Tue Oct 28 10:16:21 MST 2015 until: Thu Oct 04 11:16:21 MDT 2115
   ```

```
Certificate fingerprints:

MD5:  29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02

SHA1: C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03

Trust this certificate? [no]:  y

Certificate was added to keystore
```

8. Run the following commands to import the certificate into the `nnm.truststore file:`
   - *Windows*: **%OvInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -import -alias <*alias_name*> -keystore nnm.truststore -file <*myca.crt*>**
   - *Linux*: **/opt/OV/nonOV/jdk/hpsw/bin/keytool -import -alias <*alias_name*> -keystore nnm.truststore -file <*myca.crt*>**

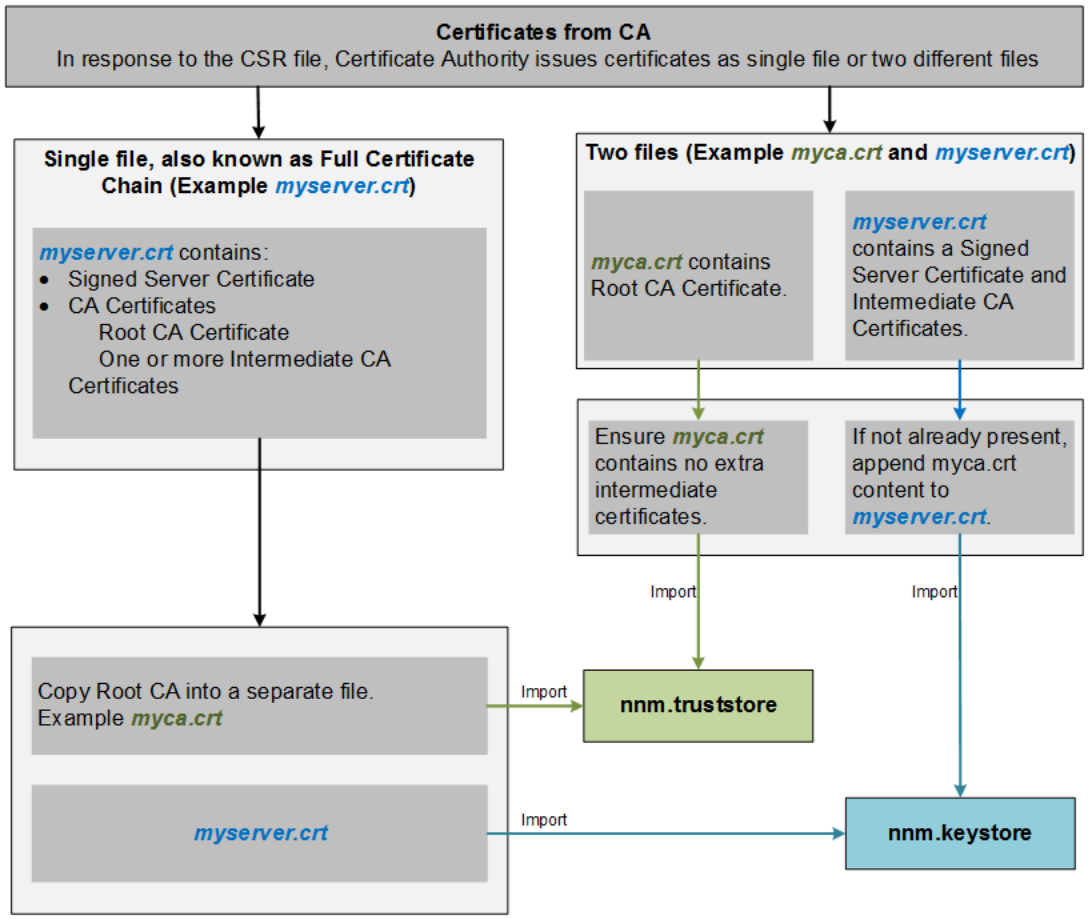
   Note:
   - In the above command,
     - <*myca.crt*> corresponds to the full path of the location where you have stored the CA certificates.
     - <*alias_name*> corresponds to the alias you had provided at the time of generating the certificate.
   - If you use the `-storepass` option and provide the password, the keystore program does not prompt you for the keystore password. If you do not use the `-storepass` option, enter **nnmkeypass** when prompted for the key store password.
9. When prompted for the truststore password, enter: **ovpass**
10. Examine the contents of the truststore:
    - *Windows*: **%OvInstallDir%\nonOV\jdk\hpsw\bin\keytool -list -keystore nnm.truststore**
    - *Linux*: **/opt/OV/nonOV/jdk/hpsw/bin/keytool -list -keystore nnm.truststore**
11. When prompted for the truststore password, enter: **ovpass**

    The truststore output is of the form:

```
Keystore type: jks

Keystore provider: SUN

Your keystore contains 1 entry

SOM_ldap, Nov 14, 2015, trustedCertEntry,

Certificate fingerprint (MD5): 29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
```

Tip: The truststore can include multiple certificates.

Types of CA-Signed Certificates



Note: If your CA returns the certificates in other forms, contact the CA provider for instructions about obtaining the certificate chain and the Root CA Certificate.

The Certificate Authority (CA) should provide you with one of the following:

- A signed server certificate file containing the **server certificate** (the SOM certificate that is CA signed) and one or more CA certificates. This section refers to the signed server certificate as `myserver.crt`.

  A CA Certificate can be either of the following:

  - Root CA Certificate - Identifies the authority that is trusted to sign certificates for servers and users.
  - Intermediate CA Certificate - A certificate signed by either a root or intermediate CA that is itself an

authority, rather than a server or user.

Note: The list of certificates from the SOM server certificate to the root CA certificate, including any intermediate CA certificates, is known as the **certificate chain**.

- A signed server certificate and a separate file containing one or more CA certificates. This section refers to the signed server certificate as `myserver.crt` and the CA certificates as `myca.crt`. The `myserver.crt` file should contain either a single server certificate or a certificate chain, but NOT the root CA certificate, which would be in the `myca.crt` file.

To configure SOM with the new certificate, you must import the certificate chain into the `nnm.keystore` and the root CA Certificate into the `nnm.truststore`. Use the `myserver.crt` file when importing the server certificate into the `nnm.keystore` file and the `myca.crt` file when importing the CA certificate into the `nnm.truststore` file.

Note: If your CA returns the certificates in other forms, contact the CA provider for instructions about obtaining the separate certificate chain and root CA Certificate.

When provided with one file that contains a full certificate chain, copy the root CA certificate from that file into the `myca.crt` file. Use the `myca.crt` file to import into the `nnm.truststore` so that SOM trusts the CA that issued the certificate.

When provided two files, add the `myca.crt` file content to the end of the `myserver.crt`, if the file does not include it, and also remove any extra intermediate certificates from the `myca.crt`, if it has any. This should result in one file, `myserver.crt`, containing the full certificate chain and one file, `myca.crt`, containing the root CA Certificate.

Note: When using a CA, only the root CA certificate is generally added to the `nnm.truststore`. Adding intermediate CA or server certificates to the `nnm.truststore` will cause those certificates to be explicitly trusted and not checked for additional information, such as revocation. Only add additional certificates to the `nnm.truststore` if your CA requires it.

The following examples show what the files received from a CA signing authority might look like:

Separate server and CA certificate files:

```
-----BEGIN CERTIFICATE-----
Sample/AVQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.....................................................................
.....................................................................
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
```

```
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
```

Combined server and CA certificates in one file:

```
-----BEGIN CERTIFICATE-----
Sample1/VQQKExNQU0EgQ29ycG9yYXRpb24gTHRkMRAwDgYDVQQLEwdOZXR3b3Js
eGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlw
.....
.....
TZImiZPyLGQBGRYDaW50MRIwEAYKCZImiZPyLGQBGRYCc2cxEzARBgNVBAMTCmNb
pSo6o/76yShtT7Vrlfz+mXjWyEHaIy/QLCpPebYhejHEg4dZgzWWT/lQt==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Sample2/Gh0dHA6Ly9jb3JwMWRjc2cyLnNnLmludC5wc2FnbG9iYWwuY29tL0Nlc
RaOCApwwggKYMB0GA1UdDgQWBBSqaWZzCRcpvJWOFPZ/Be9b+QSPyDAfBgNVHSMC
.....
.....
Wp5Lz1ZJAOu1VHbPVdQnXnlBkx7V65niLoaT90Eqd6laliVlJHj7GBriJ90uvVGu
BQagggEChoG9bGRhcDovLy9DTj1jb3JwMWRjc2cyL==
-----END CERTIFICATE-----
```

Configuring an SSL Connection to the Directory Service

By default, when directory service communications are enabled, SOM uses the LDAP protocol for retrieving data from a directory service. If your directory service requires an SSL connection, you must enable the SSL protocol to encrypt the data that flows between SOM and the directory service.

SSL requires a trust relationship between the directory service host and the SOM management server. To create this trust relationship, add a certificate to the SOM trust store. The certificate confirms the identity of the directory service host to the SOM management server.

To install a trust store certificate for SSL communications, follow these steps:

1. Obtain your company's trust store certificate from the directory server. The directory service administrator should be able to give you a copy of this text file.
2. Change to the directory that contains the SOM trust store:

- *Windows*: `%OvDataDir%\shared\nnm\certificates`
- *Linux*: `/var/opt/OV/shared/nnm/certificates`

Run all commands in this procedure from the `certificates` directory.

3. Import your company's trust store certificate into the SOM trust store:
   a. Run the following command:
      - *Windows*: **%OvInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -import -alias som_ldap -keystore nnm.truststore -file <*Directory_Server_Certificate.txt*>**
      - *Linux*: **/opt/OV/nonOV/jdk/hpsw/bin/keytool -import -alias som_ldap -keystore nnm.truststore -file <*Directory_Server_Certificate.txt*>**

      Where *<Directory_Server_Certificate.txt>* is your company's trust store certificate.
   b. When prompted for the keystore password, enter: **ovpass**
   c. When prompted to trust the certificate, enter: **y**

      The output from this command is of the form:

      ```
      Owner: CN=NNMi_server.example.com
      Issuer: CN=NNMi_server.example.com
      Serial number: 494440748e5
      Valid from: Tue Oct 28 10:16:21 MST 2008 until: Thu Oct 04 11:16:21 MDT 2108
      Certificate fingerprints:
      MD5:  29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
      SHA1: C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03:7E:C4:03
      Trust this certificate? [no]:  y
      Certificate was added to keystore
      ```

4. Examine the contents of the trust store:
   - *Windows*: **%OvInstallDir%\nonOV\jdk\hpsw\bin\keytool.exe -list -keystore nnm.truststore**
   - *Linux*: **/opt/OV/nonOV/jdk/hpsw/bin/keytool -list -keystore nnm.truststore**
5. When prompted for the keystore password, enter: **ovpass**

   The trust store output is of the form:

   ```
   Keystore type: jks
   Keystore provider: SUN
   Your keystore contains 1 entry
   SOM_ldap, Nov 14, 2015, trustedCertEntry,
   ```

```
Certificate fingerprint (MD5): 29:02:D7:D7:D7:D7:29:02:29:02:29:02:29:02:29:02
```

Tip: The trust store can include multiple certificates.

6. Restart the SOM services.
   a. Run the `ovstop` command on the SOM management server.
   b. Run the `ovstart` command on the SOM management server.

For more information about the `keytool` command, search for "Key and Certificate Management Tool" at **http://www.oracle.com/technetwork/java/index.html**.

Configuring SOM to Require Encryption for Remote Access

An administrator can disable HTTP and other unencrypted access from the network to SOM.

Note: Before configuring SOM to permit only encrypted remote access, ensure that all integrations support SSL. Configure them for SSL before configuring SOM to permit only encrypted remote access.

To disable HTTP and other unencrypted access from the network to SOM, edit the `server.properties` file as follows:

1. Edit the following file (you may need to create it if it does not exist):
   - *Windows*: `%OvDataDir%\nmsas\NNM\server.properties`
   - *Linux*: `/var/opt/OV/nmsas/NNM/server.properties`
2. Add the following lines to the `server.properties` file:

```
nmsas.server.net.bind.address = 127.0.0.1
nmsas.server.net.bind.address.ssl = 0.0.0.0
nmsas.server.net.hostname = localhost
nmsas.server.net.hostname.ssl = ${com.hp.ov.nms.fqdn}
```

3. Restart the SOM services.
   a. Run the `ovstop` command on the SOM management server.
   b. Run the `ovstart` command on the SOM management server.

With the modification just described, SOM will not "listen" to HTTP requests from a remote system; however, HTTP requests would still be supported for localhost access.

Enable Non-SSL Communications

By default, SOM supports HTTPS for communication.

Caution: It is strongly recommended 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
```

LDAP-Based Authentication

This chapter contains information about integrating SOM with a directory service for consolidating the storage of user names, passwords, and, optionally, SOM user group assignments. It contains the following topics:

SOM User Access Information and Configuration Options

Together, the following items define an SOM user:

- The **user name** uniquely identifies the SOM user. The user name provides access to SOM and receives incident assignments.

- The **password** is associated with the user name to control access to the SOM console or SOM command line.
- **SOM user group** membership controls the information available and the type of actions that a user can take in the SOM console. User group membership also controls the availability of SOM commands to the user.

SOM provides several options for where the SOM user access information is stored, as described in the following topics. Table 8 indicates the databases that store the SOM user access information for each configuration option.

Options for Storing User Information

Option	User Name	Password	User Group	User Group Membership
Mixed	Both	Directory Service	SOM	SOM
External	Directory Service	Directory Service	Both	Directory Service

Note: When adding new user accounts, or modifying existing accounts using mixed mode, you must select the **Directory Service Account** check box. SOM does not support a combination of mixed mode and external mode. Do not try to combine the two modes by selecting **Directory Service Account** for some users and not selecting it for others.

Mixed Mode: Some User Information in the SOM Database and Some User Information in the Directory Service

With mixed mode, SOM accesses a directory service for the user name and password, which are defined externally to SOM and are also available to other applications. The mapping of users to SOM user groups is maintained in the SOM console. The configuration and maintenance of SOM user access information is a joint effort as described here:

- The directory service administrator maintains the user names and password in the directory service.
- The SOM administrator enters the user names (as defined in the directory service), user group definitions, and the user group mappings in the SOM console.
- The SOM administrator configures the SOM `ldap.properties` file to describe the directory service database schema for user names to SOM. (In SOM User Sign-in Information Flow for Using Mixed Mode, the commented line indicates that SOM does not pull user group information from the directory service.)

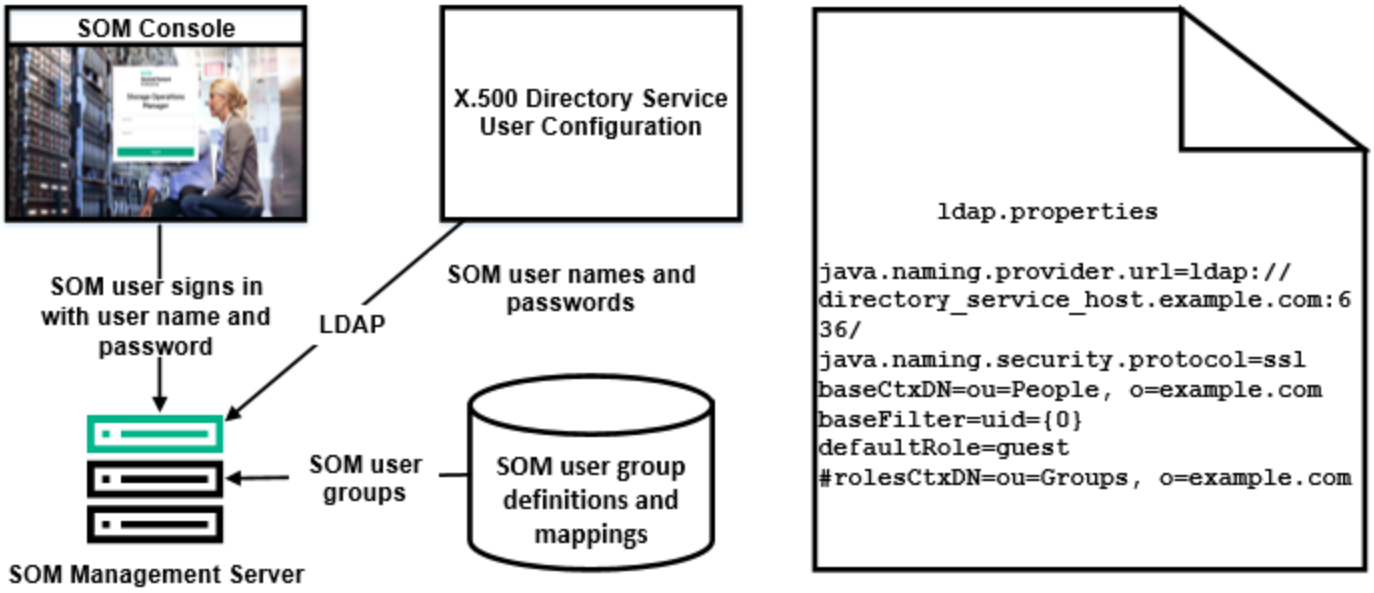
Because user names must be entered in two places, user name maintenance must be performed in both places.

SOM User Sign-in Information Flow for Using Mixed Mode shows the information flow for this option, which is appropriate in the following situations:

- The number of SOM users is small, and a directory service is available.
- The SOM administrator wants to control the user groups instead of requiring a directory service change for each user group change.
- The directory service group definitions are not easily expandable.

For information about integrating with a directory service for the user name and password, see the rest of this chapter and *SOM User Guide*.

SOM User Sign-in Information Flow for Using Mixed Mode



External Mode: All SOM User Information in the Directory Service

With this option, SOM accesses a directory service for all user access information, which is defined externally to SOM and is available to other applications. Membership in one or more directory service groups determines the SOM user groups for the user.

The configuration and maintenance of SOM user access information is a joint effort as described here:

- The directory service administrator maintains the user names, passwords, and group membership in the directory service.
- The SOM administrator maps the directory service groups to SOM user groups in the SOM console
- The SOM administrator configures the SOM `ldap.properties` file to describe the directory service database schema for user names and groups to SOM.

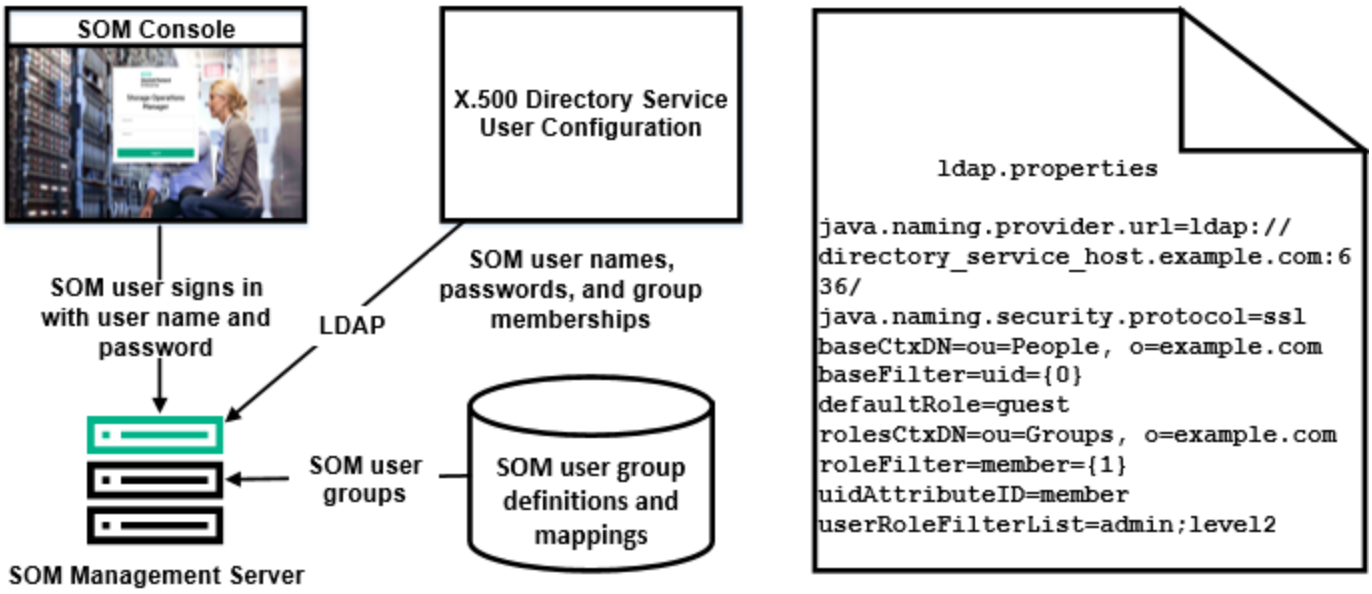
The following diagram shows the information flow for this option, which is appropriate for environments where the directory service can be modified to include user groups that align with the people who need access to SOM.

Because this option is an expansion of the mixed mode scenario, we recommend the following configuration process:

1. Configure and verify SOM user name and password retrieval from the directory service.
2. Configure SOM user group retrieval from the directory service.

For information about integrating with a directory service for all user information, see the rest of this chapter and the *SOM User Guide*.

SOM User Sign-in Information Flow for Using External Mode



Configuring SOM to Access a Directory Service

Directory service access is configured in the `ldap.properties` file. The `ldap.properties` file is located as follows:

- *Windows*: `%OvDataDir%\shared\nnm\conf\ldap.properties`
- *Linux*: `/var/opt/OV/shared/nnm/conf/ldap.properties`

For information about this file, see "ldap.properties Configuration File Reference" on page 94.

For information about the general structure of a directory service, see "Directory Service Queries" on page 86.

To configure user access from the directory service, follow the appropriate procedure for your directory service.

For configuration with the mixed mode, complete the following tasks:

- "Task 1: Back up the Current SOM User Information" below
- "Task 2: Configure User Access from the Directory Service" below
- "Task 4: Clean up to Prevent Unexpected Access to SOM" on page 85

For configuration with the external mode, complete the following tasks:

- "Task 1: Back up the Current SOM User Information" below
- "Task 2: Configure User Access from the Directory Service" below
- "Task 3: (External mode only) Map the Directory Service Groups to SOM User Groups" on page 84
- "Task 4: Clean up to Prevent Unexpected Access to SOM" on page 85

Task 1: Back up the Current SOM User Information

Back up the user information in the SOM database:

somsecurityinfoexport.ovpl [-h|-help] -c [account|security|securitymappings|all] -f <complete path to zip file>

Task 2: Configure User Access from the Directory Service

Follow the appropriate procedure for your directory service. This task includes the following sections:

- Simple Approach for Microsoft Active Directory
- Simple Approach for Other Directory Services

Steps for Microsoft Active Directory

1. Back up the `ldap.properties` file that was shipped with SOM, and then open the file in any text editor.
2. Overwrite the file contents with the following text:

   `java.naming.provider.url=ldap://<myldapserver>:389/`

   `bindDN=<mydomain>\\<myusername>`

   `bindCredential=<mypassword>`

   `baseCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,DC=<mysuffix>`

   `baseFilter=CN={0}`

   `defaultRole=guest`

   `#rolesCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,DC=<mysuffix>`

   `roleFilter=member={1}`

   `uidAttributeID=member`

   `userRoleFilterList=admin;level2;level1`
3. Specify the URL for accessing the directory service. In the following line:

   `java.naming.provider.url=ldap://<myldapserver>:389/`

Replace *<myldapserver>* with the fully-qualified hostname of the Active Directory server (for example: `myserver.example.com`).

> **Tip:** To specify multiple directory service URLs, separate each URL with a single space character ( ).

4. Specify credentials for a valid directory service user. In the following lines:

   ```
   bindDN=<mydomain>\\<myusername>
   bindCredential=<mypassword>
   ```

   Make the following substitutions:

   - Replace *<mydomain>* with the name of the Active Directory domain.
   - Replace *<myusername>* and *<mypassword>* with a user name and password for accessing the Active Directory server.
     - If you plan to add the password in plain text, specify a user name with read-only access to the directory service.
     - If you plan to specify an encrypted password, use the following command to encrypt the plain text password before adding it to the `ldap.properties` file:

       somldap.ovpl -encrypt <*mypassword*>

       > **Note:** This encrypted password only works for the SOM instance you create it for. Do not attempt to use it for a different SOM instance.

5. Specify the portion of the directory service domain that stores user records. In the following line:

   ```
   baseCtxDN=CN=Users,DC=<myhostname>,DC=<mycompanyname>,
     DC=<mysuffix>
   ```

   Replace *<myhostname>*, *<mycompanyname>*, and *<mysuffix>* with the components of the fully-qualified hostname of the Active Directory server (for example, for the hostname `myserver.example.com`, specify: `DC=myserver,DC=example,DC=com`).

   For more information, see "Example content structure for Active Directory" on page 87.

Steps for Other Directory Services

1. Back up the `ldap.properties` file that was shipped with SOM, and then open the file in any text editor.
2. Specify the URL for accessing the directory service. In the following line:

   ```
   #java.naming.provider.url=ldap://<myldapserver>:389/
   ```

   Do the following:

- Uncomment the line (by deleting the # character).
- Replace *<myldapserver>* with the fully-qualified hostname of the directory server (for example: `myserver.example.com`).

  Tip: To specify multiple directory service URLs, separate each URL with a single space character ( ).

3. Specify the portion of the directory service domain that stores user records. In the following line:

   `baseCtxDN=ou=People,o=myco.com`

   Replace `ou=People,o=myco.com` with the portion of the directory service domain that stores user records.

   For more information, see "Example content structure for other directory services" on page 89.
4. Specify the format of user names for signing in to SOM. In the following line:

   `baseFilter=uid={0}`

   Replace `uid` with the user name attribute from the directory service domain.

   For more information, see "Example content structure for other directory services" on page 89.

Task 3: (External mode only) Map the Directory Service Groups to SOM User Groups

Replicate the DN of the LDAP groups in SOM. Map the admin or level1 or level2 roles in SOM to the LDAP groups through the directory service name.

1. In the SOM console, map the predefined SOM user groups to their counterparts in the directory service:
   a. From the workspaces navigation panel, select the **Configuration**> **Security** > **User Groups**. The User Groups view is displayed.
   b. Double-click the admin row.
   c. In the Directory Service Name field, enter the full distinguished name (DN) of the Directory Service group for SOM administrators.
   d. Click **Save and Close**.
   e. Repeat step b through step d for each of the guest, level1, and level2 rows.

   Tip: These mappings provide SOM console access. Every user who will access the SOM console must be in a directory service group that is mapped to one of the predefined SOM user groups named in this step.
2. For other groups containing one or more SOM users in the directory service, create a new user group in the SOM console:

a. From the workspaces navigation panel, select the **Configuration**> **Security** > **User Groups**. The User Groups view is displayed.

b. Click **New**, and then enter the required information as mentioned in the table below:

Attribute	Description
Name	The name that uniquely identifies the user group. Short names are recommended, for example, `admin`.
Display Name	The name that should be displayed in the SOM console to identify this user group. For example, `Administrators`.
Directory Service Name	The full distinguished name of the directory service group, for example: ◦ *Windows*: `cn=Administrators,ou=people,dc=example,dc=com` ◦ *Linux*: `ou=people,o=example.com`
Description	Text that describes the purpose of this user group.

c. Click **Save and Close**.

d. Repeat step b and step c for each additional directory service group of SOM users.

Note: These mappings provide topology object access in the SOM console. Each directory service group can be mapped to multiple SOM user groups.

Task 4: Clean up to Prevent Unexpected Access to SOM

1. Optional. Change the value of, or comment out, the `defaultRole` parameter in the `ldap.properties` file.
2. To store user group membership in the SOM database, reset the user access information in the SOM database as follows:
   a. Remove any pre-existing user access information. (Delete all rows in the **User Accounts** view.)

      For instructions, see *Delete a User Account* in the SOM help.

   b. For each SOM user, create a new object in the **User Accounts** view for the user name.
      - For the **Name** field, enter the user name as defined in the directory service.
      - Select the **Directory Service Account** check box.

Note: SOM does not support a combination of mixed mode and external mode. Do not try to combine the two modes by selecting **Directory Service Account** for some users and not selecting it for others.

- Do not specify a password.

For more information, see *User Account Tasks* in the SOM help.

c. For each SOM user, map the user account to one or more SOM user groups.

For instructions, see *User Account Mapping Tasks* in the SOM help.

d. Update incident ownership so that each assigned incident is associated with a valid user name.

For instructions, see *Manage Incident Assignments* in the SOM help.

3. To rely on the user group membership in the directory service, reset the user access information in the SOM database as follows:

a. Remove any pre-existing user access information. (Delete all rows in the **User Accounts** view.)

For instructions, see *Delete a User Account* in the SOM help.

b. Update incident ownership so that each assigned incident is associated with a valid user name.

For instructions, see *Manage Incident Assignments* in the SOM help.

Directory Service Queries

SOM uses LDAP to communicate with a directory service. SOM sends a request, and the directory service returns stored information. SOM cannot alter the information that is stored in the directory service.

This section contains the following topics:

Directory Service Access

LDAP queries to a directory service use the following format:

`ldap://<directory_service_host>:<port>/<search_string>`

- `ldap` is the protocol indicator. Use this indicator for both standard connections and SSL connections to the directory service.
- *<directory_service_host>* is the fully-qualified name of the computer that hosts the directory service.

- *<port>* is the port that the directory service uses for LDAP communication. The default port for non-SSL connections is 389. The default port for SSL connections is 636.
- *<search_string>* contains the information request. For more information, see "Directory Service Content" below and RFC 1959, *An LDAP URL Format*, which is available at: **labs.apache.org/webarch/uri/rfc/rfc1959.txt**

You can enter an LDAP query as a URL in a web browser to verify that you have the correct access information and the correct structure for the search string.

Tip: If the directory service (for example, Active Directory) does not permit anonymous access, the directory service denies LDAP queries from a web browser. In this case, you can use a third-party LDAP browser (for example, the LDAP browser included in Apache Directory Studio) to validate your configuration parameters.

Directory Service Content

A directory service stores information such as user names, passwords, and group membership. To access the information in a directory service, you must know the distinguished name that references the storage location of the information. For sign-in applications, the distinguished name is a combination of variable information (such as a user name) and fixed information (such as the storage location of user names). The elements that make up a distinguished name depend on the structure and content of the directory service.

The following examples show possible definitions for a group of users called USERS-SOM-Admin. This group lists the directory service user IDs that have administrative access to SOM. The following information pertains to these examples:

- The Active Directory example is for the Windows operating system.
- The other directory services example is for Linux operating systems.
- The file shown in each example is a portion of a lightweight directory interchange format (LDIF) file. LDIF files provide for sharing directory service information.
- The figure shown in each example is a graphical representation of the directory service domain that provides an expanded view of the information in the LDIF file excerpt.

Example content structure for Active Directory

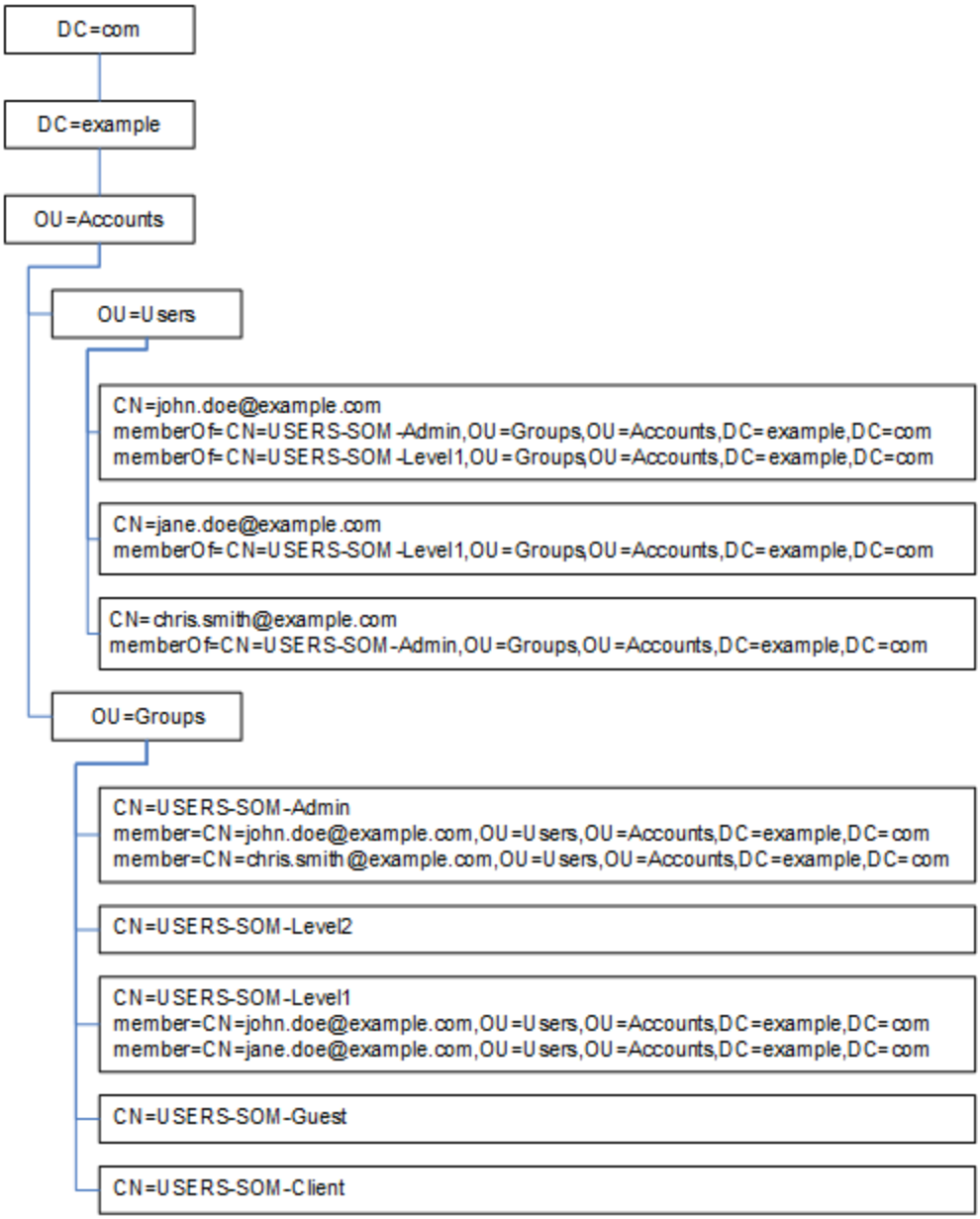
In this example, the following items are of interest:

- The distinguished name of the user John Doe is:
  `CN=john.doe@example.com,OU=Users,OU=Accounts,DC=example,DC=com`
- The distinguished name of the group USERS-SOM-Admin is:
  `CN=USERS-SOM-Admin,OU=Groups,OU=Accounts,DC=example,DC=com`
- The group attribute that stores the directory service user ID is:
  `member`

Example LDIF file excerpt:

```
groups |USERS-SOM-Admin
dn: CN=USERS-SOM-Admin,OU=Groups,OU=Accounts,DC=example,DC=com
cn: USERS-SOM-Admin
description: Group of users for SOM administration.
member: CN=john.doe@example.com,OU=Users,OU=Accounts,
 DC=example,DC=com
member: CN=chris.smith@example.com,OU=Users,OU=Accounts,
  DC=example,DC=com
```

The following diagram illustrates this directory service domain.



Example content structure for other directory services

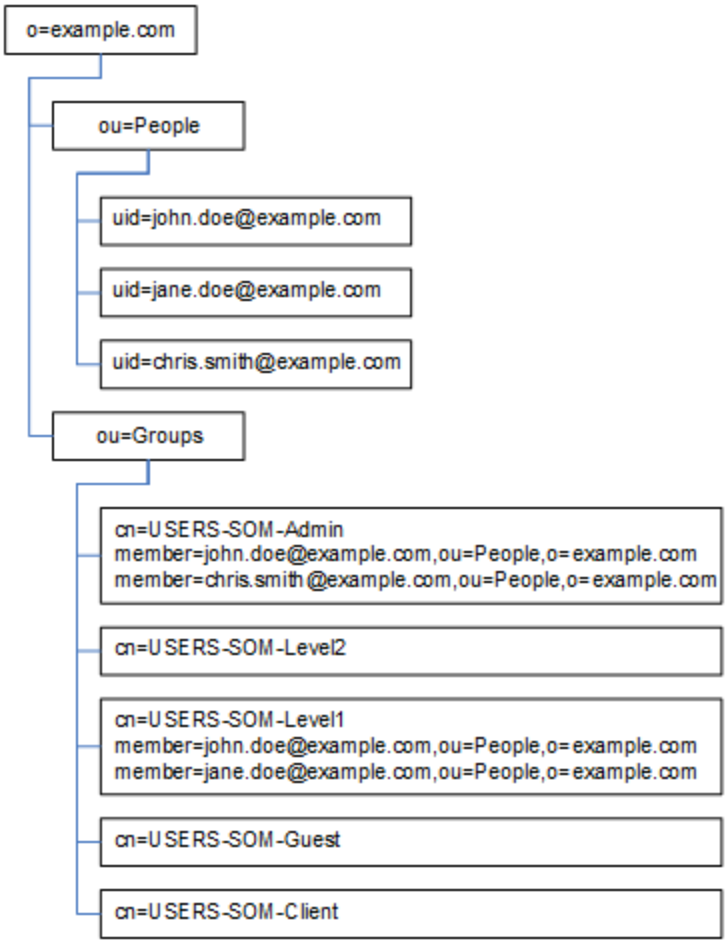
In this example, the following items are of interest:

- The distinguished name of the user John Doe is: `uid=john.doe@example.com,ou=People,o=example.com`
- The distinguished name of the group USERS-SOM-Admin is: `cn=USERS-SOM-Admin,ou=Groups,o=example.com`
- The group attribute that stores the directory service user ID is: `member`

Example LDIF file excerpt:

```
groups |USERS-SOM-Admin
dn: cn=USERS-SOM-Admin,ou=Groups,o=example.com
cn: USERS-SOM-Admin
description: Group of users for SOM administration.
member: uid=john.doe@example.com,ou=People,o=example.com
member: uid=chris.smith@example.com,ou=People,o=example.com
```

The following diagram illustrates this directory service domain.



Information Owned by the Directory Service Administrator

The following tables list the information to obtain from the directory service administrator before configuring SOM for LDAP access to a directory service.

Information for Retrieving User Names and Passwords from a Directory Service

Information	Active Directory Example	Other Directory Services Example
The fully-qualified name of the computer that hosts the directory service	`directory_service_host.example.com`	
The port that the directory service uses for LDAP communication	• 389 for non-SSL connections • 636 for SSL connections	
Does the directory service require an SSL connection?	If yes, obtain a copy of your company's trust store certificate and see "Configuring an SSL Connection to the Directory Service" on page 75.	
The distinguished name for one user name that is stored in the directory service (to demonstrate the directory service domain)	`CN=john.doe@example.com, OU=Users,OU=Accounts, DC=example,DC=com`	`uid=john.doe@example.com, ou=People,o=example.com`

Information for Retrieving Group Membership from a Directory Service

Information	Active Directory Example	Other Directory Services Example
The distinguished name for identifying the groups to which a user is assigned	The `memberOf` user attribute identifies the groups.	• `ou=Groups,o=example.com` • `cn=USERS-SOM-*, ou=Groups,o=example.com`
The method of identifying a user within a group	• `CN=john.doe@example.com, OU=Users,OU=Accounts, DC=example,DC=com` • `CN=john.doe@example.com`	• `cn=john.doe@example.com, ou=People,o=example.com` • `cn=john.doe@example.com`
The group attribute that stores the directory service user ID	`member`	`member`
The names of the groups in the directory service that apply to SOM access	• `CN=USERS-SOM-Admin, OU=Groups,OU=Accounts, DC=example,DC=com` • `CN=USERS-SOM-Level2,`	• `cn=USERS-SOM-Admin, ou=Groups,o=example.com` • `cn=USERS-SOM-Level2, ou=Groups,o=example.com`

Information for Retrieving Group Membership from a Directory Service, continued

Information	Active Directory Example	Other Directory Services Example
	OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-SOM-Level1, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-SOM-Client, OU=Groups,OU=Accounts, DC=example,DC=com • CN=USERS-SOM-Guest, OU=Groups,OU=Accounts, DC=example,DC=com	• cn=USERS-SOM-Level1, ou=Groups,o=example.com • cn=USERS-SOM-Client, ou=Groups,o=example.com • cn=USERS-SOM-Guest, ou=Groups,o=example.com

User Identification

The distinguished name for user identification is the fully-qualified method of locating one user in the directory service. SOM passes the user distinguished name in an LDAP request to the directory service.

In the `ldap.properties` file, the user distinguished name is the concatenation of the `baseFilter` value and the `baseCtxDN` value. If the password returned by the directory service matches the sign-in password the user entered into the SOM console, user sign in continues.

For external mode, the following information applies:

- For SOM console access, SOM examines the following information and grants the user the highest possible privileges:
  - The value of the `defaultRole` parameter in the `ldap.properties` file
  - This user's membership in the directory service groups that are mapped (with the **Directory Service Name** field) to the predefined SOM user groups in the SOM console
- For SOM topology object access, SOM grants access according to the security group mappings for the groups to which this user belongs in the directory service (as mapped to SOM user groups in the SOM console).

Active Directory user identification example

If a user signs in to SOM as `john.doe` when `baseFilter` is set to `CN={0}` and `baseCtxDN` is set to `OU=Users,OU=Accounts,DC=example,DC=com`, the string passed to the directory service is:

`CN=john.doe,OU=Users,OU=Accounts,DC=example,DC=com`

Other directory services user identification example

If a user signs in to SOM as `john.doe` when `baseFilter` is set to `uid={0}@example.com` and `baseCtxDN` is set to `ou=People,o=example.com`, the string passed to the directory service is:

`uid=john.doe@example.com,ou=People,o=example.com`

User Group Identification

SOM determines the user groups for an SOM user as follows:

1. SOM compares the values of the external names of all user groups configured in the SOM console with the names of the directory service groups.
2. For any user group match, SOM then determines whether the SOM user is a member of that group in the directory service.

In the SOM console, short text strings identify the unique names of the predefined SOM user groups that grant SOM console access. These text strings are also required by the `defaultRole` and `userRoleFilterList` parameters in the `ldap.properties` configuration file. The following table maps the unique names of these groups to their display names.

SOM User Group Name Mappings

SOM Role Name in the SOM Console	User Group Unique Name and Text String in SOM Configuration Files
Administrator	`admin`
Global Operators	`globalops`
Operator Level 2	`level2`
Operator Level 1	`level1`
Guest	`guest`
Web Service Client	`client`

Note: The SOM Global Operators user group (`globalops`) grants access to all topology objects only. A user must be assigned to one of the other user groups (`level2`, `level1`, or `guest`) to access the SOM console.

The administrator should not map the `globalops` user group to any security group because this user group is, by default, mapped to all security groups.

Directory Service Configuration for Storing SOM User Groups

If you plan to store SOM user groups in the directory service (external mode), the directory service must be configured with SOM user group information. Ideally, the directory service already contains appropriate user groups. If this is not the case, the directory service administrator can create new user groups specifically for SOM user group assignment.

Because directory service configuration and maintenance procedures depend on the specific directory service software and your company's policies, those procedures are not documented here.

Troubleshooting the Directory Service Integration

1. Verify the SOM LDAP configuration by running the following command:

   `somldap.ovpl -info`

   If the reported configuration is not as expected, verify the settings in the `ldap.properties` file.
2. Force SOM to re-read the `ldap.properties` file by running the following command:

   `somldap.ovpl -reload`
3. Test the configuration for one user by running the following command:

   `somldap.ovpl -diagnose <`*`SOM_user`*`>`

   Replace <*SOM_user*> with the sign-in name of an SOM user as defined in the directory service.

   Examine the command output and respond appropriately.
4. Verify that the directory service contains the expected records. Use a web browser or a third-party LDAP browser (for example, the LDAP browser included in Apache Directory Studio or Softerra LDAP browser) to examine the directory service information.

   Information about the format of a query to a directory service can be found in RFC 1959, *An LDAP URL Format*, which is available at:

   http://labs.apache.org/webarch/uri/rfc/rfc1959.txt
5. View the log file to verify that the sign-in request is correct, and to determine if any errors occurred:

   Windows: `%OvDataDir%\log\som\som.log`

   Linux: `/var/opt/OV/log/som/som.log`

   - A message similar to the following line indicates that the directory service requires HTTPS communication. In this case, enable SSL as described in "Configuring an SSL Connection to the Directory Service" on page 75.

     ```
     javax.naming.AuthenticationNotSupportedException: [LDAP: error code 13 -
     confidentiality required]
     ```

   - A message similar to the following line indicates that a timeout occurred while communicating with

the directory service. In this case, increase the value of `searchTimeLimit` in the `ldap.properties` file.

```
javax.naming.TimeLimitExceededException: [LDAP: error code 3 - Timelimit Exceeded]
```

ldap.properties Configuration File Reference

The `ldap.properties` file contains the settings for communicating with and building LDAP queries to the directory service. This file is located as follows:

- *Windows*: `%OvDataDir%\shared\nnm\conf\ldap.properties`
- *Linux*: `/var/opt/OV/shared/nnm/conf/ldap.properties`

In the `ldap.properties` file, the following conventions apply:

- To comment out a line, begin that line with a number sign character (#).
- The following rules apply to special characters:
  - To specify a backslash character (\), comma (,), semicolon (;), plus sign (+), less than sign (<), or greater than sign (>), escape the character with a backslash character. For example: \\ or \+
  - To include a space character ( ) as the *first* or *last* character in a string, escape the space character with a backslash character (\).
  - To include a number sign character (#) as the *first* character in a string, escape the number sign character with a backslash character (\).

  Characters not mentioned here do not need to be escaped or quoted.

Note: After editing the `ldap.properties` file, force SOM to re-read the LDAP configuration by running the following command:

```
somldap.ovpl -reload
```

The following table describes the parameters in the `ldap.properties` file.

Note: The initial `ldap.properties` file might not include all parameters that are listed in the following table. Add the parameters you need.

Parameters in the ldap.properties File

Parameter	Description
java.naming.provider.url	Specifies the URL for accessing the directory service. The format is the protocol (ldap), followed by the fully-qualified host name of the

Parameters in the ldap.properties File, continued

Parameter	Description

	directory server, optionally followed by the port number. For example:
	`java.naming.provider.url=ldap://ldap.example.com:389/`
	If the port number is omitted the following defaults apply:
	• For non-SSL connections, the default port is `389`.
	• For SSL connections, the default port is `636`.
	If you specify multiple directory service URLs, SOM uses the first directory service when possible. If that directory service is not accessible,SOM queries the next directory service in the list, and so forth. Separate each URL with a single space character. For example:
	`java.naming.provider.url=ldap://ldap1.example.com/ ldap://  ldap2.example.com/`
	Configuring this parameter enables LDAP communication between SOM and the directory service. To disable LDAP communication, comment out this parameter, and then save the file. SOM ignores the rest of the configuration in the `ldap.properties` file.

java.naming.security.protocol	Specifies the connection protocol specification. • If the directory service is configured to use LDAP over SSL, set this parameter to `ssl`. For example: `java.naming.security.protocol=ssl` • If the directory service does not require SSL, leave this parameter commented out. For more information, see "Configuring an SSL Connection to the Directory Service" on page 75.

bindDN	For a directory service (such as Active Directory) that does not permit anonymous access, specify the user name for accessing the directory service.
	For example:
	`bindDN=region1\\john.doe@example.com`
	• If you plan to add the password in plain text, specify a user name with read-only access to the directory service.
	For example:
	`bindCredential=PasswordForJohnDoe`
	• If you plan to specify an encrypted password, use the following command to encrypt the plain text password before adding it to the `ldap.properties` file:

Parameters in the ldap.properties File, continued

Parameter	Description
	`somldap.ovpl -encrypt <mypassword>` For example: `bindCredential={ENC}uaF22C+0CF9VozBVYj8OAw==` **Note:** This encrypted password only works for the SOM instance you create it for. Do not attempt to use it for a different SOM instance. For more information see the *somldap.ovpl* reference page.
bindCredential	When `bindDN` is set, specifies the password for the user name that `bindDN` identifies. For example: `bindCredential=PasswordForJohnDoe`
baseCtxDN	Specifies the portion of the directory service domain that stores user records. The format is a comma-separated list of directory service attribute names and values. For example: • `baseCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com` • `baseCtxDN=ou=People,o=example.com` For more information, see "User Identification" on page 91.

baseFilter	Specifies the format of user names for signing in to SOM.
	The format is the name of the directory service user name attribute and a string that relates the entered user sign-in name to the format of names in the directory service. The user name string contains the expression `{0}` (to denote the user name entered for sign in) and any other characters that are needed to match the directory service formatting of user names.
	• If the user name entered for SOM sign in is the same as the user name stored in the directory service, the value is the replacement expression. For example:
	  • `baseFilter=CN={0}`
	  • `baseFilter=uid={0}`
	• If the user name entered for SOM sign in is a subset of the user name stored in the directory service, include the additional characters in the value. For example:
	  • `baseFilter=CN={0}@example.com`

Parameters in the ldap.properties File, continued

Parameter	Description
	• `baseFilter=uid={0}@example.com` For more information, see "User Identification" on page 91.
defaultRole	Optional. Specifies a default role that applies to any directory service user who signs in to SOM through LDAP. If a user is directly configured for a predefined SOM user group, SOM grants the user the superset of privileges for the default role and the assigned user group. Valid values are as follows: `admin`, `level2`, `level1`, or `guest`. Note that although `admin` is a valid value, you should use caution and consider the implications of making `admin` a default role. These names are the unique names of the predefined SOM user group names. For example: `defaultRole=guest` If commented out or omitted, SOM does not use a default role.
rolesCtxDN	Specifies the portion of the directory service domain that stores group records. The format is a comma-separated list of directory service attribute names and values. For example: • `rolesCtxDN=CN=Users,DC=ldapserver,DC=example,DC=com` • `rolesCtxDN=ou=Groups,o=example.com` In other directory services (not Active Directory), for a faster search, you can identify one or more directory service groups that contain SOM user groups. If the group names form a pattern, you can specify a wildcard. For example, if the directory service includes groups named `USERS-SOM-administrators`, `USERS-SOM-level1Operators`, and so forth, you could use a search context similar to: `rolesCtxDN=cn=USERS-SOM-*,ou=Groups,o=example.com` Configuring this parameter enables directory service queries for SOM user group assignments through LDAP. To disable directory service queries for SOM user group assignments through LDAP, comment out this parameter, and then save the file. SOM ignores the remaining user group-related values in the `ldap.properties` file. For more information, see "User Group Identification" on page 92.

Parameters in the ldap.properties File, continued

Parameter	Description

roleFilter	Specifies the format of group member names in the directory service group definitions.
	
	The format is the name of the directory service group attribute for user ID and a string that relates the entered user sign-in name to the format of user IDs in the directory service. The user name string contains one of the following expressions and any other characters that are needed to match the directory service formatting of group member names.
	
	• The expression `{0}` denotes the user name entered for sign in (for example, `john.doe`).
	An example role filter that matches on the (short) user name entered for sign in is:
	`roleFilter=member={0}`
	• The expression `{1}` denotes the distinguished name of the authenticated user as returned by the directory service (for example,
	`CN=john.doe@example.com,OU=Users,OU=Accounts,`
	`DC=example,DC=com`
	or
	`uid=john.doe@example.com,ou=People,o=example.com).`
	An example role filter that matches on the (full) authenticated user name is:
	`roleFilter=member={1}`
	
	For more information, see "User Group Identification" on page 92.

uidAttributeID	Specifies the group attribute that stores the directory service user ID. For example: `uidAttributeID=member` For more information, see "User Group Identification" on page 92.
userRoleFilterList	Optional. Limits the SOM user groups whose associated users can be assigned incidents in the SOM console. The user groups in this list apply only to directory service user names authenticated through LDAP. This parameter provides functionality that is not available when SOM user groups are assigned in the SOM console and stored in the SOM database. The format is a semicolon-separated list of the unique names for one or more predefined SOM user group names.

Parameters in the ldap.properties File, continued

Parameter	Description
	`userRoleFilterList=admin;globalops;level2;level1`
searchTimeLimit	Optional. Specifies the timeout value in milliseconds. The default value is 10000 (10 seconds). If you are encountering timeouts during SOM user sign in, increase this value. For example: `searchTimeLimit=10000`

Examples

Example ldap.properties file for Active Directory

An example `ldap.properties` file follows for Active Directory:

```
java.naming.provider.url=ldap://MYldapserver.example.com:389/
bindDN=MYdomain\\MYusername
bindCredential=MYpassword
baseCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
baseFilter=CN={0}
defaultRole=guest
rolesCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
rolesCtxDN=CN=Users,DC=MYldapserver,DC=EXAMPLE,DC=com
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

Example ldap.properties file for other directory services

An example `ldap.properties` file follows for other directory services:

```
java.naming.provider.url=ldap://MYldapserver.example.com:389/
baseCtxDN=ou=People,o=EXAMPLE.com
baseFilter=uid={0}
defaultRole=guest
rolesCtxDN=ou=Groups,o=EXAMPLE.com
roleFilter=member={1}
uidAttributeID=member
userRoleFilterList=admin;level2;level1
```

Configuring SOM to Support Public Key Infrastructure User Authentication

SOM supports user authentication through Public Key Infrastructure (PKI) so that users must log on to SOM using an X.509 client certificate without using a password. The information in this chapter explains how to configure SOM (using PKI user authentication) to map certificates to SOM user accounts.

Note: PKI user authentication includes support for smart cards, such as Common Access Card (CAC) and Personal Identity Verification (PIV) cards.

After enabling SOM to use PKI user authentication, SOM users do not need to use an SOM-specific user name and password to log on to SOM.

Using this approach, SOM reads your PKI certificate to obtain your user name. To obtain SOM user roles, you need to define a user's roles within SOM or configure SOM to use Lightweight Directory Access Protocol (LDAP).

Note: PKI user authentication uses the HTTPS protocol.

This chapter contains the following topics:

User Authentication Strategies

SOM provides several options for where the SOM user access information is defined and stored.

The following table indicates the options available for PKI user authentication.

User Authentication Strategies

Option	Which Method for User Authentication?	User Account Definitions in SOM	User Group Definitions in SOM	Which Method for Group Membership
Mixed	X.509 Certificate	Yes	Yes	SOM User Account Mappings
External	X.509 Certificate	No	Yes	LDAP

In the Mixed option, SOM defines and stores the User Group assignments. For information about setting up all user information in SOM, see **Configuring User Accounts (User Account Form)** in the SOM help.

In the External option, SOM uses the Lightweight Directory Access Protocol (LDAP) User Group assignments. For more information, see "LDAP-Based Authentication" on page 78.

Configuring SOM for PKI User Authentication (X.509 Certificate Authentication)

Before configuring SOM for PKI user authentication, note that user account names must match the user names contained in the certificates. Set roles using one of the following methods:

- To use an LDAP directory service, see "LDAP-Based Authentication" on page 78.
- To use the SOM console to add a user account, select the **Directory Service Account** check box on the **User Account** form and leave the **Password** field blank. Then, use the user account name to match the previous mapping rule.

For SOM, enable and customize PKI user authentication in the following file:

- *Windows*: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`
- *Linux*: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`

To enable SOM to require PKI user authentication, also referred to as X.509 Certificate Authentication, follow these steps:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`

2. Search for the following text block:

```
<realm name="console">
  <mode>FORM</mode>
</realm>
```

3. Edit the located lines to read:

```
<realm name="console">
  <mode>X509</mode>
</realm>
```

4. Search for the following text block:

```
<principalMapping>
```

5. Configure SOM to extract (map) the principal by editing the items in the `<principalMapping>` section. You must know the format of your certificate to complete this step.

Note: SOM supports several options for extracting a principal and those options can be specified in any order and in any number.

- The attribute element extracts a field from the `SubjectDN`; for example, `EMAILADDRESS`.
  - If you are using LDAP, the extracted name must match the name the LDAP configuration expects. For more information, see Integrating SOM with a Directory Service through LDAP.
  - If you use internal accounts, the name must match the SOM user account name. If the account is used for PKI user authentication only, it should be created as a "Directory Service Account", without a password (using the SOM **User Account** form. Select the **Directory Service Account** check box and leave the **Password** field blank). If the account is used for both PKI user authentication and password logon, it should be created as a standard account with a password.
- The `regexp` element runs the regular expression against the whole `SubjectDN`.
- The `subjectAlternativeName` (SAN) element can be used with type `rfc822Name` (which is an email address).
- The `subjectAlternativeName` element with type `otherName` and an additional `oid` attribute. This option is commonly used for the Microsoft Universal Principal Name (UPN) field.

In addition to the examples provided in the `nms-auth-config.xml` file's `<principalMapping>` section, see the following examples:

Example 1: Edit the following lines to read as follows for using the EMAIL field:

```
<!-- The attribute element extracts a field from the SubjectDN;
for example, EMAILADDRESS, CN, or UID. -->
<attribute>EMAILADDRESS</attribute>
```

Example 2: Edit the following lines as an example of using a more complex regular expression to extract part of the field, as in extracting just part of the EMAILADDRESS field. To extract just the name part of the EMAILADDRESS field, use the following regular expression:

```
<!-- Extract the name part of the email field which appears first
in the subjectDN. If the subject is EMAILADDRESS=first.last@example.com,
CN=First Last, OU=MyGroup, O=My Company, the mapped username would be
"first.last"--> <regexp group="1">EMAILADDRESS=([^@]+).*</regexp>
```

Example 3: Edit the following lines as an example of using a more complex regular expression to match fields in the middle of the string:

```
<!--Extract the CN field which appears anywhere in the subjectDN.
Note the optional group before the CN which matches the
previous fields. If the subject is EMAILADDRESS=first.last@example.com,
CN=First Last, OU=MyGroup, O=My Company
```

In addition to the examples provided in the `nms-auth-config.xml` file's `<principalMapping>` section, see the following examples:

Example 1: Edit the following lines to read as follows for using the EMAIL field:

```
<!-- The attribute element extracts a field from the SubjectDN; for example,
EMAILADDRESS, CN, or UID. -->
<attribute>EMAILADDRESS</attribute>
```

Example 2: Edit the following lines as an example of using a more complex regular expression to extract part of the field, as in extracting just part of the EMAILADDRESS field. To extract just the name part of the EMAILADDRESS field, use the following regular expression:

```
<!-- Extract the name part of the email field which appears first in
the subjectDN. If the subject is EMAILADDRESS=first.last@example.com,
CN=First Last, OU=MyGroup, O=My Company, the mapped username would be
"first.last"-->
<regexp group="1">EMAILADDRESS=([^@]+).*</regexp>
```

Example 3: Edit the following lines as an example of using a more complex regular expression to match fields in the middle of the string:

```
<!--Extract the CN field which appears anywhere in the subjectDN.
Note the optional group before the CN which matches the previous fields.
If the subject is EMAILADDRESS=first.last@example.com, CN=First Last,
OU=MyGroup, O=My Company
Then the mapped username would be "First Last" -->
<regexp group="2">(.*, )?CN=([^,]+).*</regexp>
```

Example 4: Edit the following lines to read as follows to extract the email address from the Subject Alternative Name:

```
<!-- Extract the first match of type rfc822Name from the Subject
Alternative Name field of the certificate. -->
<subjectAlternativeName type="rfc822Name" />
```

Example 5: Edit the following lines to read as follows to extract a particular OID from the Subject Alternative Name:

```
<!-- Extract the first match of type otherName with the supplied
OID from the Subject Alternative Name field of the certificate. -->
<subjectAlternativeName type="otherName" oid="1.3.6.1.4.1.311.20.2.3" />
```

Note: The logging command to enable debug logging is as follows:

```
nnmsetlogginglevel.ovpl

com.hp.ov.nms.as.server.auth.x509.NmsCertMapper FINEST
```

6. Save your changes.
7. Edit the following file:

   Windows: `%OvInstallDir%\nmsas\server\nms\server.properties`

   Linux: `/opt/OV/nmsas/server/nms/server.properties`
8. In the `server.properties` file, add the following line:

   `nmsas.server.net.http.AUTH_REALM = com.hp.ov.nms.as.server.tomcat.NmsWebRealm`
9. Save the `server.properties` file.
10. Configure certificates.
    - If you have already installed your trusted CA certificates into the truststore, run the following script for the changes to the `nms-auth-config.xml` file to take immediate effect:

      `somsecurity.ovpl -reloadAuthConfig`

    - If you have not yet installed your certificates, follow these steps:

      i. Import your trusted CA certificate into the `nnm.truststore` file.

      For example, suppose the `example_ca.cer` file contains the certificate you must use. Run the following command to import the CA certificate into the SOM `nnm.truststore` file:

      Windows:

      ```
      %OvInstallDir%\nonOV\jdk\hpsw\jre\bin\keytool.exe -importcert -trustcacerts -
      keystore "%OvDataDir%\shared\nnm\certificates\nnm.truststore" -file "<full
      path of the example.cer file>" -storepass ovpass -alias myca
      ```

      Linux:

      ```
      /opt/OV/nonOV/jdk/hpsw/jre/bin/keytool -importcert -trustcacerts -keystore
      /var/opt/OV/shared/nnm/certificates/nnm.truststore -file <full path of the
      example.cer file> -storepass ovpass -alias myca
      ```

      ii. Restart the SOM services.

      A. Run the `ovstop` command on the SOM management server.

      B. Run the `ovstart` command on the SOM management server.

SOM is now configured to use PKI user authentication. You can no longer use passwords to log on SOM. Check that your LDAP and SOM user accounts are working correctly, and that the certificates and accounts are configured correctly for user access to SOM.

Logging on to SOM using a Client Certificate

To log on to SOM using a client certificate, follow these steps:

1. Ensure that your client certificate is accessible in your browser.
2. Point your browser to `https://<hostname>/som`.
3. SOM permits you access and assigns user roles based on your SOM or LDAP account configuration.

Revoking Access for a User Having a Client Certificate

To remove a user from accessing SOM, do one of the following:

- If you configured a user for access using an LDAP account, remove the user from all LDAP groups associated with SOM.
- If you configured a user for access using SOM user accounts, remove the user from the user group and remove their user account.

In either case, the user can no longer log on to the SOM console.

Special Considerations When PKI User Authentication in Global Network Management Environments

If you use SOM in a Global Network Management configuration, configure PKI user authentication for all of the SOM management servers included in the Global Network Management Configuration.

Certificate Validation (CRL and OCSP)

SOM supports two methods of checking for revoked certificates:

- Certificate Revocation List (CRL) - A CRL is a list of revoked certificates that is downloaded from the Certificate Authority (CA).
- Online Certificate Status Protocol (OCSP) - OCSP is a protocol for checking revocation of a single certificate interactively using an online service called an OCSP responder.

CRL and OCSP validation are two different ways to achieve the same result: denying access to any user whose certificate is revoked. In a web browser, OCSP is generally considered superior because a browser is usually dealing with many different Certificate Authorities (CAs), and having to download an entire CRL to check one web site is inefficient.

However, for a server that is often dealing with many clients, all with certificates from the same CA, CRL checking can be significantly more efficient because the CRL can be downloaded once per day instead of needing to check OCSP for every connection.

When both OCSP and CRL are enabled,SOM, by default, queries CRL first. CRL checking is performed first because the CRL usually has a much longer lifetime and, therefore, is more resilient to network outages. OCSP performs frequent requests so, if the network or the OCSP responder is down, users will be unable to log on. SOM attempts to obtain a valid CRL first to use in continuing operations in the case the network or OCSP responder goes down.

In addition, CRL comparison is much faster than OCSP; that is, matching a certificate against a list that exists on the disk is faster than querying a separate server over the network to validate each certificate. So if a certificate has been signed by a trusted entity, and is not expired, the CRL is queried to see if the certificate has been revoked. If it has been revoked, there is no need to check OCSP. But if the certificate is still valid after checking the CRL, OCSP will also be queried to ensure that the certificate has not been revoked recently (and an updated CRL listing the certificate is not yet available).

When both OCSP and CRL are enabled, SOM supports the following:

- SOM queries CRL first, followed by OCSP (this is the default behavior).
- If the CRL is not available, OCSP is used as a backup.
- If OCSP is not available, CRL is used as a backup.

General Configuration for Certificate Validation Protocols

You can configure how SOM checks for revoked certificates. For example, you can configure the order in which protocols are used, and whether all the protocols are used.

SOM uses the `nms-auth-config.xml` file to configure such settings.

Configuring Protocol Order

By default, SOM performs CRL checking, and then OCSP checking.

To configure the order in which the certificate validation protocols check for revoked certificates, do the following:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<revocation>` section of the file (find the `<revocation>` tag), search for the line that begins with the following text:

   `<ordering>`

3. Do one of the following:
   - To specify that CRL checking is to be used first, followed by OCSP, edit the line to read as follows:

     `<ordering>CRL OCSP</ordering>`

   - To specify that OCSP checking is to be used first, followed by CRL, edit the line to read as follows:

     `<ordering>OCSP CRL</ordering>`

4. Save the `nms-auth-config.xml` file.
5. Run the following command for the change to take effect:

   `somsecurity.ovpl -reloadAuthConfig`

Configuring Protocol Requests

You can configure SOM to do either of the following with regard to protocol requests:

- Check all certificate validation protocols for each certificate
- Check the protocol list in the preferred order and stop when a valid response is received

To configure protocol requests, do the following:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<revocation>` section of the file (find the `<revocation>` tag), search for the line that begins with the following text:

   `<mode>`
3. Do one of the following:
   - To have SOM check all protocols for each certificate, edit the line to read as follows:

     `<mode>CHECK_ALL</mode>`

   - To have SOM check the protocol list in the preferred order and stop when a valid response is received, edit the line to read as follows:

     `<mode>FIRST_SUCCESS</mode>`

4. Save the `nms-auth-config.xml` file.
5. Run the following command for the change to take effect:

   `somsecurity.ovpl -reloadAuthConfig`

Validating Certificates Using CRLs

SOM uses CRLs to properly deny access to clients using a certificate that is no longer trusted.

Note: During authentication, when a certificate's serial number is found in a CRL, SOM does not accept that certificate and authentication fails.

SOM checks CRLs by default when using X.509 authentication mode; however, you can specify a CRL by editing the `nms-auth-config.xml` file, as described in the following sections.

Note: SOM stores the CRL configuration in the following location:

- *Windows*: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`
- *Linux*: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`

There is also a default version of the configuration file, which can be used for reference purposes to view new available options. The default configuration file is stored in the following location:

- *Windows*: `%OvInstallDir%\newconfig\HPOvNnmAS\nmsas\conf\nms-auth-config.xml`
- *Linux*: `/opt/OV/newconfig/HPOvNnmAS/nmsas/conf/nms-auth-config.xml`

Enabling and Disabling CRL Checking

By default, SOM enables CRL checking.

To configure CRL checking, follow these steps:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<crl>` section of the file (find the `<crl>` tag), search for the line that begins with the following text:

   `<enabled>`
3. Do one of the following:
   - To enable CRL checking, change the line to read as follows:

     `<enabled>true</enabled>`
   - To disable CRL checking, change the line to read as follows:

     `<enabled>false</enabled>`
4. Save the `nms-auth-config.xml` file.
5. Run the following command for the change to take effect:

   `somsecurity.ovpl -reloadAuthConfig`

Changing the CRL Enforcement Mode

By default, SOM is set to enforce CRLs.

To change the product's enforcement of CRLs, follow these steps:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<crl>` section of the file (find the `<crl>` tag), search for the line that begins with the following text:

   `<mode>`
3. Change the line to read as one of the following:

   `<mode><value></mode>`

   where `<value>` is one of the following:

   - `ENFORCE`: Enforce CRLs where specified in the certificates
   - `ATTEMPT`: Check CRLs but allow access if the CRL is not available
   - `REQUIRE`: Require and enforce CRLs in certificates

   Note: In `REQUIRE` mode, authentication will fail if there is no CRL specified or available for a user's certificate.
4. Save the `nms-auth-config.xml` file.
5. Run the following command for the change to take effect:

   `somsecurity.ovpl -reloadAuthConfig`

Changing How Often a CRL Should be Refreshed

To configure how often SOM refreshes the CRL, follow these steps:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<crl>` section of the file (find the `<crl>` tag), search for the line that begins with the following text:

   `<refreshPeriod>`

3. Change the line to read as follows:

   `<refreshPeriod><value></refreshPeriod>`

   where `<value>` is the integer number of hours or days (the smallest value is 1h).

   For example, enter `24h` for 24 hours; enter `2d` for 2 days.
4. Save the `nms-auth-config.xml` file.
5. Run the following command for the change to take effect:

   `somsecurity.ovpl -reloadAuthConfig`

Changing the Maximum Idle Time for a CRL

You can configure how long SOM keeps a CRL after the CRL has been idle (has not been used or accessed).

To change the maximum idle time for a CRL, follow these steps:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<crl>` section of the file (find the `<crl>` tag), search for the line that begins with the following text:

   `<maxIdleTime>`
3. Change the line to read as follows:

   `<maxIdleTime><value></maxIdleTime>`

   where `<value>` is the integer number of hours or days (the smallest value is 1h).

   For example, enter `24h` for 24 hours; enter `2d` for 2 days.
4. Save the `nms-auth-config.xml` file.
5. Run the following command for the change to take effect:

   `somsecurity.ovpl -reloadAuthConfig`

CRL Expiration Warnings

When CRL checking is enabled, if a CRL expires, users might be locked out of the SOM console. To help avoid unwanted lockouts, SOM provides health warning messages to alert administrators that a CRL has either expired or will be expiring soon.

The *expired* CRL warning (Major severity) occurs when one or more CRLs have expired.

The *expiring* CRL warning (Minor severity) occurs when one or more CRLs has less than 1/6th of its valid period remaining. For example, if a CRL is valid for 24 hours, SOM displays a warning if the CRL expires in fewer than four hours.

Configure the refresh period such that CRLs are always kept fresh. A properly configured refresh period ensures that, if the CRL server is unavailable for a time, there is a sufficient valid period remaining for the downloaded CRLs. In this way, SOM can continue normal operation until the CRL server is available. In this example, a refresh period of eight hours might be appropriate.

Changing the Location for a CRL

By default, SOM downloads CRLs from the HTTP location embedded in the certificate. If this location is not accessible to the SOM management server, the administrator can obtain the required CRLs some other way and configure SOM to load those CRLs from the local file system.

Note: Only CRLs signed by the certificate issuer are considered when evaluating the certificate.

To configure SOM to load CRLs from the local file system, do the following:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<crl>` section of the file (find the `<crl>` tag), search for the following text block:

   ```
   <!--
   Optional specification for the CRL location...
   -->
   <!-- <location>file:///var/opt/OV/shared/nnm/certificates/myco.crl</location> -->
   ```
3. After the `-->` tag, add the following line, based on your operating system:

   Windows: `<location>file:///C:/CRLS/<crlname>.crl</location>`

   Linux: `<location>file:///var/opt/OV/shared/nnm/certificates/<crlname>.crl</location>`

   Replace `<crlname>.crl` with the name of the local CRL. Ensure that the path is correct.
4. Save the `nms-auth-config.xml` file.
5. Run the following command for the change to take effect:

   `somsecurity.ovpl -reloadAuthConfig`

Validating Certificates Using Online Certificate Status Protocol (OCSP)

SOM supports Online Certificate Status Protocol (OCSP) to check for revoked certificates interactively.

PKI user authentication uses OCSP to verify the revocation status of a certificate by querying an OCSP responder. An OCSP responder provides immediate and accurate revocation information on specific certificates as follows:

- An OCSP client submits a certificate status request to an OCSP responder.
- The OCSP client suspends acceptance of the certificate in question until the OCSP responder provides a digitally signed response.
- The OCSP responder indicates the status of the certificate by returning one of the following values:
  - `Good` (pass; user is granted access)
  - `Revoked` (fail; user is denied access)
  - `Unknown` (fail; user is denied access)

Because the OCSP responder is queried for every certificate, whereas the CRL is downloaded periodically (for example, once per day), OCSP responses might be more up-to-date than corresponding CRLs.

Note: SOM stores the OCSP configuration in the following location:

- *Windows*: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`
- *Linux*: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`

A default version of the configuration file can be used for reference purposes to view new available options. The default configuration file is stored in the following location:

- *Windows*: `%OvInstallDir%\newconfig\HPOvNnmAS\nmsas\conf\nms-auth-config.xml`
- *Linux*: `/opt/OV/newconfig/HPOvNnmAS/nmsas/conf/nms-auth-config.xml`

Enabling and Disabling OCSP Checking

To configure OCSP checking, follow these steps:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<ocsp>` section of the file (find the `<ocsp>` tag), search for the line that begins with the following text:

   `<enabled>`
3. Do one of the following:
   - To enable OCSP checking, change the line to read as follows:

     `<enabled>true</enabled>`
   - To disable OCSP checking, change the line to read as follows:

     `<enabled>false</enabled>`
4. Save the `nms-auth-config.xml` file.

5. Run the following command for the change to take effect:

   somsecurity.ovpl -reloadAuthConfig

Changing the OCSP Enforcement Mode

By default, SOM is set to enforce OCSP.

To change the product's enforcement of OCSP, follow these steps:

1. Edit the following file:

   Windows: %OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml

   Linux: /var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml
2. Within the <ocsp> section of the file (find the <ocsp> tag), search for the line that begins with the following text:

   <mode>
3. Change the line to read as one of the following:

   <mode><*value*></mode>

   where <*value*> is one of the following:

   - ENFORCE: Enforce OCSP where specified in the certificates
   - ATTEMPT: Check OCSP but allow access if OCSP is not available
   - REQUIRE: Require and enforce OCSP in certificates
4. Save the nms-auth-config.xml file.
5. Run the following command for the change to take effect:

   somsecurity.ovpl -reloadAuthConfig

Enabling Nonce

For added security (to avoid replay attacks), an OCSP requester can add a nonce to the certificate validation request. A nonce is a random number, attached to each request, that alters the encryption. When the nonce feature is enabled, the OCSP responder computes an appropriate response using the nonce value.

Note: Using a nonce puts more load on the OCSP responder because it cannot precalculate or cache responses. Some OCSP responders may not accept requests with a nonce.

Note: The nonce feature is disabled by default.

To enable the OCSP nonce feature, follow these steps:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<ocsp>` section of the file (find the `<ocsp>` tag), search for the line that begins with the following text:

   `<nonce>`
3. Do one of the following:
   - To enable the nonce feature, change the line to read as follows:

     `<nonce>true</nonce>`
   - To disable the nonce feature (and use a general request), change the line to read as follows:

     `<nonce>false</nonce>`
4. Save the `nms-auth-config.xml` file.
5. Run the following command for the change to take effect:

   `somsecurity.ovpl -reloadAuthConfig`

Specifying the URL of the OCSP Responder

Optionally, you can specify the URL of the OCSP responder as follows:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Within the `<ocsp>` section of the file (find the `<ocsp>` tag), search for the line that begins with the following text:

   `<responder>`
3. Edit the line to read as follows:

   `<responder><`*`URL`*`></responder>`

   where `<`*`URL`*`>` is the URL associated with the OCSP responder.
4. Save the `nms-auth-config.xml` file.
5. Run the following command for the change to take effect:

   `somsecurity.ovpl -reloadAuthConfig`

Note: The OCSP URL must use the HTTP protocol.

- If there is no OCSP URL specified in the `nms-auth-config.xml` file, SOM attempts to obtain an OCSP responder from the certificate itself.
- If there is no OCSP responder specified in the certificate, SOM uses the `<mode>` setting to determine what action to take:
  - If the mode is `ENFORCE` or `ATTEMPT`, SOM passes the OCSP validation step for this certificate.
  - If the mode is `REQUIRE`, SOM rejects the certificate.

Configuring SOM to Restrict Certificates Used for SOM Logon Access

If you are using SOM with PKI user authentication, you might want to restrict which certificates are considered valid for SOM logon access.

SOM supports the following types of restrictions:

- Restrictions on the certificate extended key usage, which can be used to restrict SOM access to hardware-based certificates or other specific certificates.
- Restrictions on the certificate issuer. These restrictions are intended to prevent a trusted certificate, which is loaded for purposes other than log on purposes, from being used to create log on certificates.

To configure SOM to restrict certificates used for log on access, do the following:

1. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
2. Locate the text block containing the following:

   `<certificateConstraints>`
3. Use the following examples as a guide to configure SOM to restrict certificates used for logons (replace values as appropriate):

   Example 1: To require client authentication, edit the following section:

   ```
   <!-- client authentication -->
   <extKeyUsage>1.3.6.1.5.5.7.3.2</extKeyUsage>
   ```

   Example 2: To require users to log on using a Microsoft smart card:

   ```
   <!-- Microsoft smart card logon -->
   <extKeyUsage>1.3.6.1.4.1.311.20.2.2</extKeyUsage>
   ```

   Example 3: To accept only certificates signed by a particular CA:

   ```
   <!-- Configures one or more trusted issuers. If this is configured, client
   certificates must be issued by one of these issuers to be used for client
   authentication -->
   <trustedIssuer>CN=MyIssuer, OU=MyOrgUnit, O=MyOrg, ST=CO, C=US</trustedIssuer>
   ```

Note: When multiple extKeyUsage entries are specified, the certificate must contain all of them (Boolean AND). When multiple trustIssuer entries are specified, only one must be the certificate trust issuer (Boolean OR).

4. Run the following command for the change to take effect:

   ```
   somsecurity.ovpl -reloadAuthConfig
   ```

Example: Configuring SOM to Require a Smart Card Logon

The following example illustrates how to configure SOM to use PKI user authentication to require a smart card logon.

Note: This example uses the Mixed user authentication strategy.

This example makes the following assumptions:

- The organization is using smart cards for logging on to SOM.
- The smart card contains a certificate with an email address in the Subject Alternative Name field.
- The organization uses CRLs to check revocation for all certificates.

To complete the example configuration, follow these steps:

1. In the SOM console, create a user called `myusername@example.com` with guest privileges.
   a. From the User Accounts view, create the `myusername@example.com` user.

      Tip: On the **User Account** form, be sure to select the **Directory Service Account** check box and leave the **Password** field blank. For more information, see the SOM help.

   b. From the User Account Mappings view, create a new user account mapping to assign the `myusername@example.com` user to the `SOM Guest Users` user group.
2. Edit the following file:

   Windows: `%OvDataDir%\nmsas\NNM\conf\nms-auth-config.xml`

   Linux: `/var/opt/OV/nmsas/NNM/conf/nms-auth-config.xml`
3. Search for the following text block:

```
<realm name="console">
  <mode>FORM</mode>
</realm>
```

4. To enable X.509 certificate authentication, edit the text to read as follows:

```
<realm name="console">
  <mode>X509</mode>
</realm>
```

5. Search for the following text block:

```
<principalMapping>
```

6. In the `<principalMapping>` block, include the following line to extract the first match of type `rfc822Name` from the Subject Alternative Name field of the certificate:

```
<subjectAlternativeName type="rfc822Name" />
```

7. Within the `<crl>` section of the file (find the `<crl>` tag), search for the line that begins with the following text:

```
<enabled>
```

8. To enable CRL checking, change the line to read as follows:

```
<enabled>true</enabled>
```

9. Within the `<crl>` section of the file, locate the text block containing the following text:

```
<mode>
```

10. To require and enforce CRLs, change the line to read as follows:

```
<mode>REQUIRE</mode>
```

Tip: In `REQUIRE` mode, authentication will fail if there is no CRL specified or available for a user's certificate. For information about other possible values, see "Changing the CRL Enforcement Mode" on page 109.

11. Locate the text block containing the following:

    ```
    <certificateConstraints>
    ```

12. To require client authentication, edit the following section:

    ```
    <!-- client authentication -->
    <extKeyUsage>1.3.6.1.5.5.7.3.2</extKeyUsage>
    ```

13. To require users to log on using a Microsoft smart card, add the following lines:

    ```
    <!-- Microsoft smart card logon -->
    <extKeyUsage>1.3.6.1.4.1.311.20.2.2</extKeyUsage>
    ```

14. Save your changes to the `nms-auth-config.xml` file.
15. Edit the following file:

    Windows: `%OvInstallDir%\nmsas\server\nms\server.properties`

    Linux: `/opt/OV/nmsas/server/nms/server.properties`

16. In the `server.properties` file, add the following line:

    ```
    nmsas.server.net.http.AUTH_REALM = com.hp.ov.nms.as.server.tomcat.NmsWebRealm
    ```

17. Save the `server.properties` file.
18. Import your trusted CA certificate into the `nnm.truststore` file.

    For example, suppose the `example_ca.cer` file contains the certificate you must use. Run the following command to import the CA certificate into the SOM `nnm.truststore` file:

    Windows:
    ```
    %OvInstallDir%\nonOV\jdk\hpsw\jre\bin\keytool.exe -importcert -trustcacerts
    -keystore "%OvDataDir%\shared\nnm\certificates\nnm.truststore" -file "<full path of
    the example.cer file>" -storepass ovpass -alias myca
    ```

    Linux:
    ```
    /opt/OV/nonOV/jdk/hpsw/jre/bin/keytool -importcert -trustcacerts -keystore
    /var/opt/OV/shared/nnm/certificates/nnm.truststore -file <full path of the
    example.cer file> -storepass ovpass -alias myca
    ```

19. Ensure that the user account's name matches the user name contained in the certificate (myusername).
20. Restart the SOM services.
    a. Run the `ovstop` command on the SOM management server.
    b. Run the `ovstart` command on the SOM management server.

SOM is now configured to require a smart card logon.

The following text is similar to how the `nms-auth-config.xml` file might appear after making the configuration changes described in this example:

```
<methods>
```

```
    <X509>
       <principalMapping>
            <subjectAlternativeName type="rfc822Name" />
       </principalMapping>
       <certificateConstraints>
            <extKeyUsage>1.3.6.1.5.5.7.3.2</extKeyUsage>
            <extKeyUsage>1.3.6.1.4.1.311.20.2.2</extKeyUsage>
            <trustedIssuer>CN=MyIssuer, OU=MyOrgUnit, O=MyOrg, ST=CO, C=US</trustedIssuer>
       </certificateConstraints>
       <revocation>
            <ordering>CRL OCSP</ordering>
            <mode>CHECK_ALL</mode>
        </revocation>
        <crl>
            <enabled>true</enabled>
            <mode>REQUIRE</mode>
            <!-- refresh CRLs every 12 hours -->
            <refreshPeriod>12h</refreshPeriod>
            <!-- remove CRLs that have not been used for 36 hours -->
            <maxIdleTime>36h</maxIdleTime>
         </crl>
         <ocsp>
            <enabled>false</enabled>
            <mode>ENFORCE</mode>
            <nonce>false</nonce>
         </ocsp>
  </X509>
</methods>
<realms>
  <realm name="console">
    <mode>X509</mode>
   </realm>
</realms>
```

Configuring CLI Authentication for PKI User Authentication

Authorized users can use the SOM command line interface (CLI) to configure SOM settings without having to navigate the SOM console.

Public Key Infrastructure (PKI) user authentications depend on client-side operating system and web browser settings to perform user authentication. Therefore, CLI sessions cannot use PKI user authentication because the commands run outside the web browser environment. To enable CLI authentication as a non-root user, you can provide authorized users read access to the following file (root users already have read access to this file):

Windows: `%OvDataDir%\nmsas\NNM\conf\nms-users.properties`

Linux: `/var/opt/OV/nmsas/NNM/conf/nms-users.properties`

This file contains the encrypted password for the SOM “system” user. Any user who can read this file can invoke CLI commands as the “system” user.

Note: Windows users who log on as a member of the Administrators group already have read access to the `nms-users.properties` file, so no further configuration is necessary for Windows users who belong to the Administrators group. For more information about configuring security, see the SOM help .

Read access to the `nms-users.properties` file can be achieved using the normal Linux `chmod` command. However, it is recommended to configure operating system-based Access Control Lists (ACLs) to provide fine-grained access control to this file. For more information, see "Setting ACLs to Enable Non-Root Users to Run CLI Commands" below.

Setting ACLs to Enable Non-Root Users to Run CLI Commands

ACL commands differ widely among operating systems and file system types on the same operating system. In addition, you might need to configure the operating system to enable ACLs; for example, adding a `,acl` entry to `/etc/fstab` on Linux.

This section provides an example using Linux (RHEL and SuSE) ACL commands with ext3 and ext4 file systems. If you are using a different file system type or operating system, see your operating system ACL documentation for more information.

This example gives the operating system user `user1` read permission for the `nms-users.properties` file.

Note: When setting ACL permissions, specify the complete set of permissions for the given file. The provided permissions overwrite the previous permissions.

Grant permission

1. Query the current ACLs using the following command:

   ```
   chacl –l nms-users.properties
   ```

   The output will look something like the following:

   ```
   nms-users.properties [u::rw-,u:user2:r--,u:user3:r--,g::r--,m::r--,o::---]
   ```

2. Append the new permission (`,u:user1:r--`) to the list output in the square brackets ([ ]), and run the following command:

   ```
   chacl <results from within square brackets in the ACL list>,u:user1:r-- nms-users.properties
   ```

Note: ACLs provide user-level control, group-level control, or both. You could also create a Linux group; for example, nnmiadm, and then provide read access to the `nms-users.properties` file to the group. Then, by adding or removing Linux users to or from that group, you are also granting or removing access to the `nms-users.properties` file, thereby granting or removing authentication as “system” user to CLI commands.

Caution: Use caution when setting ACLs because incorrect settings that prevent permissions for the `nmsproc` user or `nmsgrp` group can cause SOM to stop functioning.

List ACLs

Run the following command:

```
chacl -l nms-users.properties
```

Remove permission

1. Query the current ACLs using the following command:

   ```
   chacl –l nms-users.properties
   ```

2. Identify and delete the user that you want to delete (user1): `,u:user1:r--`
3. Paste the rest of the ACL listing into the chacl command:

   ```
   chacl <list results minus user1> nms-users.properties
   ```

Note: Each of the directories in the `nms-users.properties` file path must be accessible. Normally the permission for these folders is very restrictive, preventing access. This path includes the following directories:

- `/var/opt/OV/nmsas`
- `/var/opt/OV/nmsas/NNM`
- `/var/opt/OV/nmsas/NNM/conf`
- `/var/opt/OV/nmsas/NNM/conf/props`

You can use ACLs also on these folders, or regular Linux `chmod` to grant “search” access (in other words, the execute bit, or 0711 mode) to “other”.

Troubleshooting PKI User Authentication Issues

During PKI user authentication, a user might encounter an error. See the following table for a listing of errors and possible causes.

PKI User Authentication Errors and Possible Causes

Error Message	Possible Cause
401 Not Authenticated	Use of HTTP rather than HTTPS. For more information, see "Configuring SOM to Require Encryption for Remote Access" on page 77.
	User does not have a certificate. For more information, see "Managing Certificates" on page 67.
	User certificate is not trusted by a CA in the `nnm.truststore`. For more information, see "Managing Certificates" on page 67.
	User certificate is expired or not yet valid. For more information, see "Managing Certificates" on page 67.
	User certificate has been revoked or revocation check failed. For more information, see "Managing Certificates" on page 67.
	User certificate failed a constraint check. For more information, see "Configuring SOM to Restrict Certificates Used for SOM Logon Access" on page 115.
403 Not Authorized	Mapped user name does not exist in SOM or the LDAP directory service. For more information, see "Configuring SOM for PKI User Authentication (X.509 Certificate Authentication)" on page 101.

PKI User Authentication Errors and Possible Causes, continued

Error Message	Possible Cause
	Certificate principal to user name mapping is incorrect. For more information, see "Configuring SOM for PKI User Authentication (X.509 Certificate Authentication)" on page 101.
	User is not in a user group that provides access to the SOM console. For more information, see **Configuring Security** in the SOM help.

Note: To troubleshoot, disable HTTP access and turn on logging to help identify issues.

Security

In SOM, security and multi-tenancy provide for restricting user access to information about the objects in the SOMdatabase. This restriction is useful for customizing the views of operators to their areas of responsibility. It also supports service providers with per-organization configuration of SOM.

By default, all console users can see information for all objects in the SOM database. If this default configuration is acceptable for your environment, you do not need to read this section.

This section focuses on the SOM security and tenant models and provides suggestions and examples of configuration. The following topics are covered:

The SOM Security Model

The SOM security model provides user access control to the objects in the SOM database. This model is appropriate for use by any network management organization that wants to limit SOM user access to specific objects. The SOM security model has the following benefits:

- Provides a way to limit a SOM console operator's view of the network. Operators can focus on specific device types or network areas.
- Provides for customizing operator access to the SOM topology. The level of operator access can be configured per node.
- Simplifies the configuration and maintenance of node groups that align with the security configuration.
- Can be used independently of the SOM tenant model.

Security Groups

In the Storage Operations Manager security model, user access to nodes is controlled indirectly though user groups and security groups. Each node in the topology is associated with only one security group. A security group can be associated with multiple user groups.

Each user account is mapped to the following user groups:

- One or more of the following default user groups:
  - Administrator
  - Global operator
  - Level 1 operator
  - Level 2 operator
  - Guest user

  This mapping is required for SOMconsole access and determines which actions are available within the SOMconsole. If a user account is mapped to more than one of these SOMuser groups, the user receives the superset of the permitted actions.

  > **Note:** The Global Operators user group grants access to topology objects only. A user must be assigned to one of the other user groups (Level 1, Level 2 or Guest) to access the console.
  >
  > The administrator should not map the Global Operators user group to any security group because this user group is, by default, mapped to all security groups.

- (*Optional*) Custom user groups that are mapped to security groups.
  These mappings provide access to objects in the Storage Operations Manager database. Each mapping includes an object access privilege level that applies to the nodes for a security group.

Default Security Group

In a new installation, the Default Security Group is the initial security group assignment for all nodes. By default, all users can see all objects in the Default Security Group. You can control the configuration of nodes to the Default Security Group and users' access to the objects in the Default Security Group.

Recommendations for Planning Security Groups

- Map each user account to only one default user group.
- Do not map the default user groups to security groups.
- Because any user account mapped to the administrators user group receives administrator-level access to all objects in the SOM database, do not map this user account to any other user groups.
- In general, related elements should be configured as part of the same security group. Some examples of

related elements include the following:

- If a virtual machine is part of a security group, then its virtual server also needs to be part of the same group.
- Arrays where the storage volumes are part of remote replication pairs need to be part of the same group.
- The array which provides backend storage needs to be part of the security group as the storage virtualizer
- Cluster members and the cluster should be part of the same group.
- When host is presented storage from an array, the host , array, and fabric elements in path need to be part of the same group.
- Virtual switches that are part of the physical switch should also be mapped to the same security group.

A Sample Approach to Plan Security Groups

Following are an outline of high-level steps for planning the configuration of security groups:

1. Analyze the managed network topology to determine the groups of nodes to which the users need access.
2. Remove the default associations between the default user groups and the default security group and the Unresolved Incidents security group.
   Doing this step ensures that users do not inadvertently obtain access to nodes they should not be managing. At this point, only administrators can access objects in the topology.
3. Configure a security group for each subset of nodes. Remember that a given node can belong to only one security group.
   a. Create the security groups.
   b. Assign the appropriate nodes to each security group.
4. Configure custom user groups.
   a. For each security group, configure a user group for each level of user access.
      - If you are if storing user group membership in the Storage Operations Manager database, no users are mapped to these user groups yet.
      - If you are storing user group membership in a directory service, set the Directory Service Name field for each user group to the distinguished name of that group in the directory service.
   b. Map each custom user group to the correct security group. Set the appropriate object access privilege for each mapping.
5. Configure user accounts.
   - If you are storing user group membership in the Storage Operations Manager database, do the following:

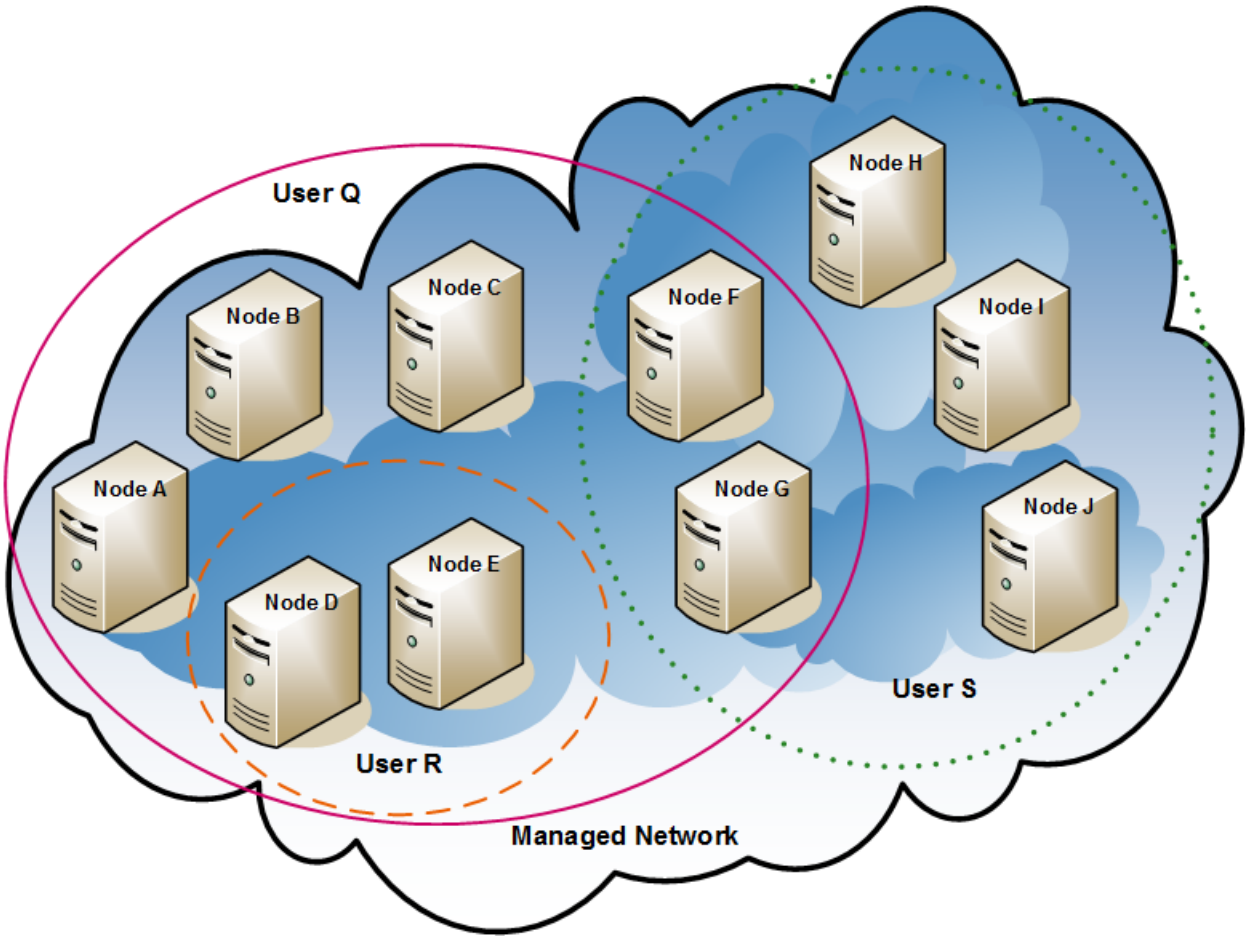
    - Create a user account object for each user who can access the console. (The process of configuring user accounts depends on whether you are using a directory service for Storage Operations Manager console logon.)
    - Map each user account to one of the default user groups (for access to the console).
    - Map each user account to one or more custom user groups (for access to topology objects).
  - If you are storing user group membership in a directory service, verify that each user belongs to one of the default user groups and one or more custom user groups.
6. Verify the configuration.
7. Maintain the configuration.
   - Watch for nodes added to the default security group, and move these nodes to the correct security groups.
   - Add new console users to the correct user groups.

Example Security Group Structure

The three ovals in the following diagram indicate the primary groupings for which users need to view the nodes in this example Storage Operations Manager topology. For complete user access control, each of the four unique subgroups corresponds to a unique security group. Each unique security group can be mapped to one or more user groups to represent the available levels of user access to the objects in that security group.

Example Security Group Mappings lists the mappings between the security groups and the possible custom user groups for this topology. (An actual implementation of this security model might not require all of these custom user groups.) Example User Account Mappings lists the mappings for several user accounts and the user groups for this topology.

Example Topology for User Access Requirements



Example Security Group Mappings

Security Group	Nodes of Security Group	User Group	Object Access Privilege
SG1	A, B, C	UG1 Administrator	Object Administrator
		UG1 Level 2	Object Operator Level 2
		UG1 Level 1	Object Operator Level 1
		UG1 Guest	Object Guest
SG2	D, E	UG2 Administrator	Object Administrator
		UG2 Level 2	Object Operator Level 2
		UG2 Level 1	Object Operator Level 1
		UG2 Guest	Object Guest

Example Security Group Mappings, continued

Security Group	Nodes of Security Group	User Group	Object Access Privilege
SG3	F, G	UG3 Administrator	Object Administrator
		UG3 Level 2	Object Operator Level 2
		UG3 Level 1	Object Operator Level 1
		UG3 Guest	Object Guest
SG4	H, I, J	UG4 Administrator	Object Administrator
		UG4 Level 2	Object Operator Level 2
		UG4 Level 1	Object Operator Level 1
		UG4 Guest	Object Guest

Example User Account Mappings

User Account	User Groups	Node Access	Notes
User Q	SOM Level 2 Operators	none	This user has operator level 2 access to the nodes in the pink oval (solid line).
	UG1 Level 2	A, B, C	
	UG2 Level 2	D, E	
	UG3 Level 2	F, G	
User R	SOM Level 1 Operators	none	This user has operator level 1 access to the nodes in the orange oval (dashed line).
	UG2 Level 1	D, E	
User S	SOM Level 2 Operators	none	This user has operator level 2 access to the nodes in the green oval (dotted line).
	UG3 Level 2	F, G	
	UG4 Level 2	H, I, J	

Example User Account Mappings, continued

User Account	User Groups	Node Access	Notes
User T	SOM Level 2 Operators	none	This user has access (with varying privilege levels) to all nodes in the example topology. This user has administrative access to nodes D and E but cannot see the menu items for tools that require administrative access. If this user has access to the management server, this user can run command-line tools that require administrative access against nodes D and E only.
	UG1 Guest	A, B, C	
	UG2 Administrator	D, E	
	UG3 Level 2	F, G	
	UG4 Level 1	H, I, J	

The SOM Tenant Model

The Storage Operations Manager tenant model provides strict segregation of topology discovery and data into tenants, also called organizations or customers. This model is appropriate for use by service providers, especially managed service providers and large enterprises.

The Storage Operations Manager tenant model has the following benefits:

- Marks the organization to which each node belongs.
- Meets regulatory requirements for separating operator access to customer data.
- Simplifies the configuration and maintenance of node groups that align with the tenant configuration.
- Simplifies configuration of security.

Tenants

The SOM tenant model adds the idea of an organization to the security configuration. Each node in the topology belongs to only one tenant. The tenant provides logical separation in the Storage Operations Manager database. Object access is managed through security groups.

For each node, the initial discovery tenant assignment occurs when the node is first discovered and added to the Storage Operations Manager database. Storage Operations Manager assigns all the discovered nodes to the default tenant. Therefore, if you use the security model without configuring any tenants, all nodes are assigned to the default tenant. By default, all users have access (through the default security group) to all objects associated with this tenant. An administrator can change the tenant for a node at any time after discovery.

Each tenant definition includes an initial discovery security group, the default security group. Storage Operations Manager assigns the node to the default security group along with the default tenant. An administrator can change the security group for a node at any time after discovery.

Note: When you change the tenant for a node, it does not automatically change the security group of the node.

Recommendations for Planning Tenants

Consider the following recommendations while planning tenant configuration:

- Configuring tenants during discovery reduces administration overheads of assigning discovered elements to respective tenants manually.
- For a small organization, a single security group per tenant is probably sufficient.
- You might want to subdivide a large organization into multiple security groups.
- To prevent users from accessing nodes across organizations, ensure that each security group includes nodes for only one tenant.

A Sample Approach to Plan Tenants

The following steps outline the high-level approach to planning and configuring multi-tenancy:

1. Analyze your customer requirements to determine how many tenants are required in the Storage Operations Manager environment.
   It is recommended that tenants be used only when managing multiple separate networks with a single management server.
2. Analyze the managed topology to determine which nodes belong to each tenant.
3. Analyze the topology of each tenant to determine the groups of nodes to which Storage Operations Manager users need access.
4. Remove the default associations between the default user groups and the default security group and the Unresolved Incidents security group.

   Doing this step assures that users do not inadvertently obtain access to nodes they should not be managing. At this point, only administrators can access objects in the topology.

5. Create the identified security groups and tenants.
   For each tenant, set the Initial Discovery Security Group to either the default security group or a tenant-specific security group with restricted access. This approach ensures that new nodes for the tenant are not generally visible until the administrator configures access.
6. Prepare for discovery by assigning tenants to seeds.

   Tip: After discovering a group of nodes, you can change the value of the Initial Discovery Security Group. Using this approach limits the manual re-assignment of nodes to security groups.

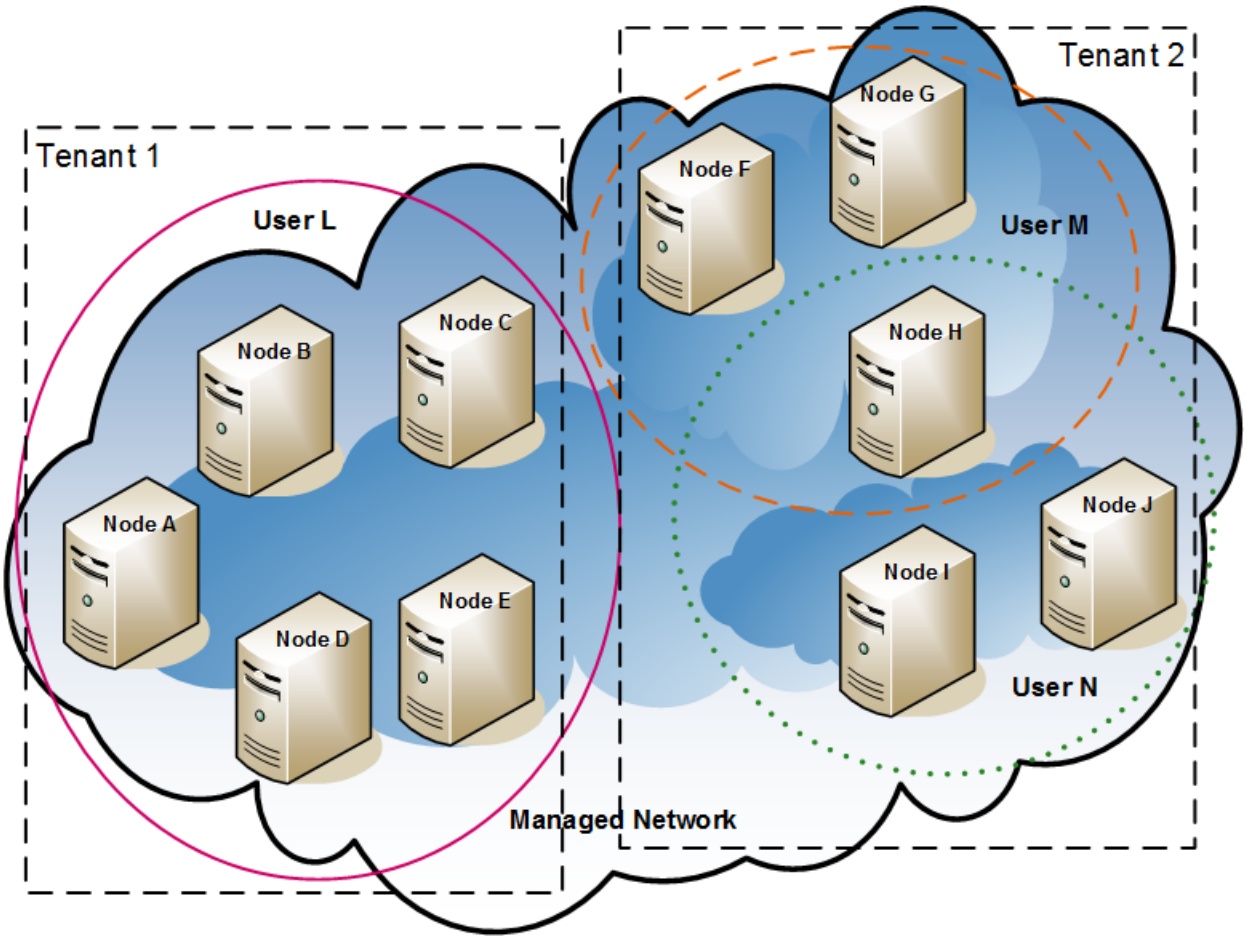
7. After discovery completes, do the following:
   a. Verify the tenant for each node and make changes as necessary.
   b. Verify the security group for each node and make changes as necessary.

Example Tenant Structure

The following diagram shows an example Storage Operations Manager topology containing two tenants, represented by the rectangles. The three ovals indicate the primary groupings for which users need to view the nodes. The topology for Tenant 1 is managed as a single group, so it needs only one security group. The topology for Tenant 2 is managed in overlapping sets, so it is separated into three security groups.

Example Security Group Mappings for Multiple Tenants lists the mappings between the security groups and the possible custom user groups for this topology. (An actual implementation of this security model might not require all of these custom user groups.) Example User Account Mappings for Multiple Tenants lists the mappings for several user accounts and the user groups for this topology.

Example Topology for Multiple Tenants



Example Security Group Mappings for Multiple Tenants

Security Group	Nodes of Security Group	User Group	Object Access Privilege
T1 SG	A, B, C, D, E	T1 Administrator	Object Administrator
		T1 Level 2	Object Operator Level 2
		T1 Level 1	Object Operator Level 1
		T1 Guest	Object Guest
T2 SGa	F, G	T2_a Administrator	Object Administrator
		T2_a Level 2	Object Operator Level 2
		T2_a Level 1	Object Operator Level 1
		T2_a Guest	Object Guest

Example Security Group Mappings for Multiple Tenants, continued

Security Group	Nodes of Security Group	User Group	Object Access Privilege
T2 SGb	H	T2_b Administrator	Object Administrator
		T2_b Level 2	Object Operator Level 2
		T2_b Level 1	Object Operator Level 1
		T2_b Guest	Object Guest
T2 SGc	I, J	T2_c Administrator	Object Administrator
		T2_c Level 2	Object Operator Level 2
		T2_c Level 1	Object Operator Level 1
		T2_c Guest	Object Guest

Example User Account Mappings for Multiple Tenants

User Account	User Groups	Node Access	Notes
User L	SOM Level 2 Operators	none	This user has operator level 2 access to the nodes in the pink oval (solid line), which groups all nodes in Tenant 1.
	T1 Level 2	A, B, C, D, E	
User M	SOM Level 1 Operators	none	This user has operator level 1 access to the nodes in the orange oval (dashed line), which groups a subset of the nodes in Tenant 2.
	T2_a Level 1	F, G	
	T2_b Level 1	H	
User N	SOM Level 2 Operators	none	This user has operator level 2 access to the nodes in the green oval (dotted line), which groups a subset of the nodes in Tenant 2.
	T2_b Level 2	H	
	T2_c Level 2	I, J	

Some Examples of Security Configuration

The following examples present possible security strategies. Use them as a guideline for configuring security. Select the example that best matches your security configuration requirements:

- "Example: Divide Node Access Between Two or More User Groups" below
- "Example: Allow a Subset of Users to Access a Subset of Nodes" on page 136

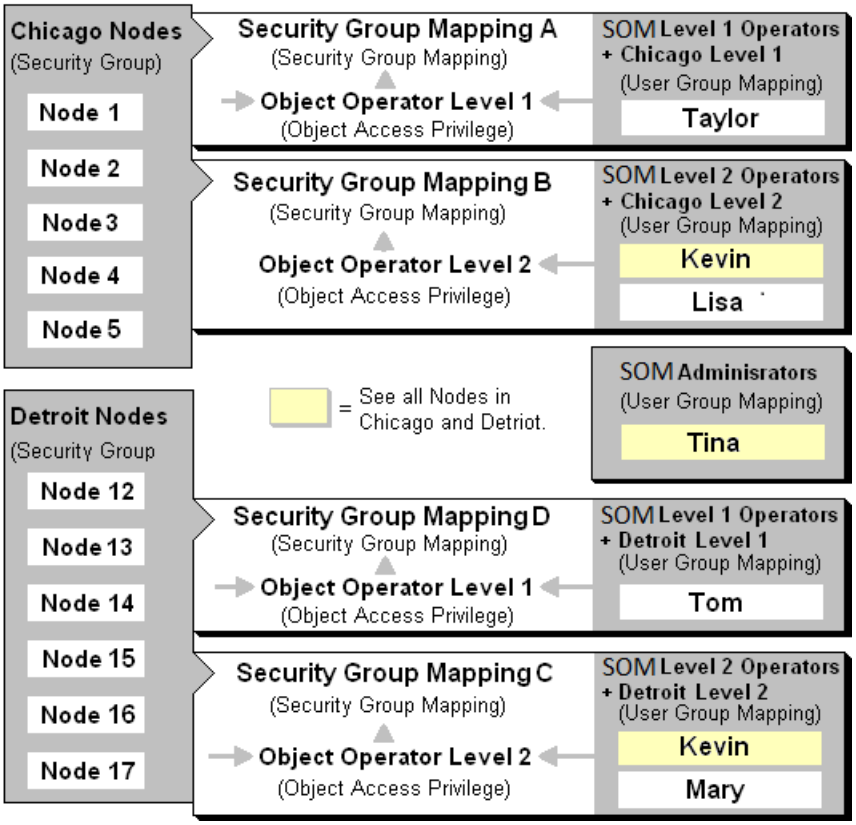
Example: Divide Node Access Between Two or More User Groups

This example configures security to divide the responsibility for network monitoring based on the following locations:

- Chicago
- Detroit

Each location includes a Level 1 Operator (with more limited access privileges than Level 2 Operators) and a Level 2 Operator. Tina, the Administrator, handles both locations. Kevin is a backup for both Chicago and Detroit and must access the nodes in both Chicago and Detroit.

The following diagram illustrates the security requirements:



The following table lists the SOM console (**SOM User Group**) and node access requirements (User Group, Object Access Privilege and Security Group) for each location.

Note: You can place all operators into the SOM Level 2 Operators if you want all operators to see all

menu options, but only have the ability to run them based on their Object Access Privilege.

Example Security Configuration

User Accounts	SOM User Groups	User Groups	Object Access Privileges	Security Groups
Tina	SOM Administrator	Not Applicable. The SOM Administrator can access all nodes.	Not Applicable. The SOM Administrator has Administrator privileges to all nodes.	Not Applicable. The SOM Administrator can access all nodes.
Kevin	SOM Level 2 Operators	Chicago Level 2 Detroit Level 2	Object Operator Level 2	Chicago Nodes, Detroit Nodes
Lisa	SOM Level 2 Operators	Chicago Level 2	Object Operator Level 2	Chicago Nodes
Taylor	SOM Level 1 Operators	Chicago Level 1	Object Operator Level 1	Chicago Nodes
Mary	SOM Level 2 Operators	Detroit Level 2	Object Operator Level 2	Detroit Nodes
Tom	SOM Level 1 Operators	Detroit Level 1	Object Operator Level 1	Detroit Nodes

To set up security for the Chicago and Detroit locations follow these procedures:

- Remove the Default Security Group Mapping to the default User Groups - Level 1 Operators, Level 2 Operators, and Guest user .

  Note: The default user groups are provided for those administrators who are not concerned with Security configuration. After you remove these Security Group Mappings, the user groups provide access only to the SOM console rather than to the SOM consoleand to all nodes.

- Create the User Accounts. See the Example Security Configuration table.
- Create the additional user groups required for the Chicago and Detroit Security Groups (Chicago Level 2, Chicago Level 1, Detroit Level 2, Deteroit Level 1). (See the Example Security Configuration table.)
- Map User Accounts to SOM User Groups. (See the Example Security Configuration table.)
- Create the Security Groups for Detroit and Chicago location.

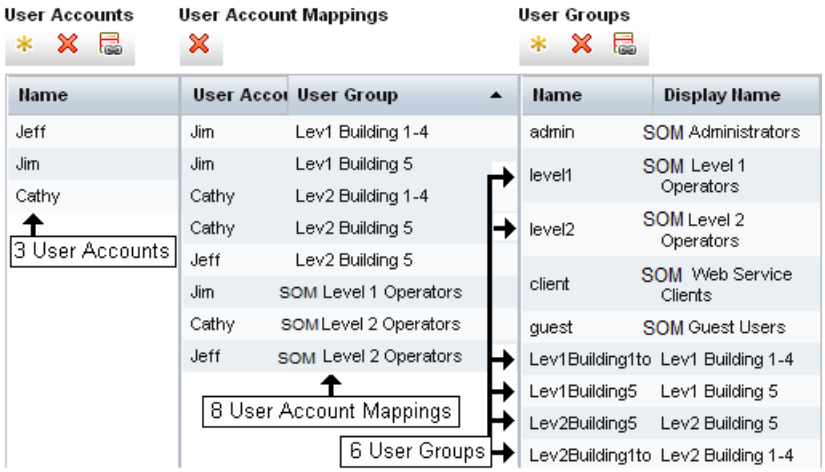
- Map each security group to the new User Groups. (See the Example Security Configuration table.)
  - **ChicagoLevel1** User Group to the **Chicago Nodes**
  - **DetroitLevel1** User Group to the **Detroit Nodes**
  - **DetroitLevel2** User Group to the **Detroit Nodes**
- Assign the nodes to the appropriate Security Group.
- View a summary of your configuration changes.
- Save you configuration changes.

Example: Allow a Subset of Users to Access a Subset of Nodes

This example configures security to allow a subset of users to access only those nodes in Building 5. The remaining users can access all nodes discovered by SOM.

This location includes a Level 1 Operator (with more limited access privileges than Level 2 Operators) and a Level 2 Operator. Jeff is a Level 2 Operator who can access only the nodes in Building 5.

Note: Be sure to create a user account that is mapped to the SOM Administrator User Group so that one person has access to the Configuration workspace and all the nodes in the network. See the topic "Restore the Administrator Role" in the Online Help for more information.



The following table lists the SOM console access requirements (SOM User Group) and node access requirements (User Group, Object Access Privilege and Security Group) for each User Account.

Note: You can place all operators into the SOM Level 2 Operators if you want all operators to see all menu options, but only have the ability to run them based on their Object Access Privilege.

Example Security Configuration

User Accounts	SOM User Groups	User Groups	Object Access Privileges	Security Groups
Jim	SOM Level 1 Operators	Lev1Buildings1-4 Lev1Building5	Object Operator Level 1	Default Security Group
Cathy	SOM Level 2 Operators	Lev2Buildings1-4 Lev2Building5	Object Operator Level 2	Default Security Group
Jeff	SOM Level 2 Operators	Lev2Building5	Object Operator Level 2	Building 5 Nodes

To set up security for this location follow these procedures:

- Remove the Default Security Group Mapping to the user groups - Level 1 Operators, Level 2 Operators, and Guest

  Note: The SOM User Groups are provided for those administrators who are not concerned with security configuration. After you remove these Security Group Mappings, the SOM User Groups provide access to the SOM console only rather than to the SOM console and to all nodes.

- Create the User Accounts. (See the Example Security Configuration table.)
- Create Additional User Groups. (See the Example Security Configuration table.)
- Map User Accounts to SOM User Groups. (See the Example Security Configuration table.)
  - Assign **Jim** to the **Lev1Building1-4** and **Lev1Building5** User Group
  - Assign **Cathy** to the **SOM Level 2 Operators**, **Lev2Building1-4**, and **Lev2Building5** User Groups
  - Assign **Jeff** to the **SOM Level 2 Operators** and **Lev2Building 5** User Groups.
- Create the Building 5 Security Group.
- Map each Security Group to the new User Groups. (See the Example Security Configuration table.)
  - **Lev1Building5** User Group to the **Building 5 Nodes**.
  - **Lev2Building1-4** User Group to the **Default Security Group**
  - **Lev2Building5** User Group to the **Building 5 Nodes**.
- Assign the nodes to the appropriate Security Group.
- View a summary of your configuration changes.

Export Configuration Data

You can move configuration data from one SOM management server to another. Moving configuring data helps reduce the effort to reconfigure data.

The following configuration data can be moved:

- Discovery Addresses
- Discovery Credentials
- Host Inference Rules / Agentless Rules
- Named generic hosts/WWN groupings
- IP Address range
- Hierarchical Groups
- Storage Tier Definitions

Movement of configuration data is possible using CLIs. See the *SOM CLI Reference Pages* for more information.

SOM Management Server Log Files

The SOM management server log files are available at the following location:

- *Windows*: `%OvDataDir%\log\som\`
- *Linux*: `/var/opt/OV/log/som`

Tip: By default, `%OvDataDir%` includes the `<drive>:\ProgramData` directory, which is a hidden Windows operating system directory. To view this directory in Windows Explorer, start typing the full path in one of the following locations:

- The Windows Explorer address bar
- The **Search** field on the Windows **Start** menu
- The Run dialog box (**Start > Run**)

Log File Rollover

The log file names use the *name*`.log` format. Any archived log file has a number appended to it in the form *name*`.log.`*%g*.

- *name* is the log file base name.
- *%g* relates to the archive number of the archived log file. The highest appended archive number represents the oldest file.

When an active log file exceeds the configured size limit, SOM archives that file by changing the file name to include the archive number and creates a new instance of that log file. For example, the `som.log` file becomes the `som.log.1` file and SOM begins logging to a new `som.log` file.

Log Levels

SOM logs messages at the following logging levels:

- SEVERE: Events that relate to abnormal SOM behavior.
- WARNING: Events that indicate potential problems and all messages included in the SEVERE logging level.
- INFO: Messages written to the SOM console (or its equivalent) and all messages included in the WARNING logging level.

Interesting Log Files

The most interesting SOM management server log files are listed here. When contacting Support, send copies of the following active and archive log files:

Log File	Descriptio
autopass.log	Licensing that uses Autopass
boot.log	SOM service startup details. Errors that occurred during startup modules, bundles, and so on that were loaded during service startup
CSVFailure.txt	Information about CSV export failures
DCFailure.txt	Data Collection devices along with times
dcMetrics.csv	The amount of time taken by various sub-processes during Data Collection
discoveryMetrics.csv	The amount of time taken by various sub-processes during Discovery
Health.log	Information about the SOM installation
nmsas.stderr nmsas.stdout	Information about JBoss running in the SOM server
som.log som.log.nnn	Information about various operations that occur in SOM. By default, max value of nnn is 100 and max size of each file is 10 MB
som-context.log	Discovery and Data Collection context log information that can also be seen from

Log File	Descriptio
som-context.log.n	the UI. By default, max value of n is 5 and max size of each file is 10 MB
som-install-config.log	Information about actions during post install pop ups
som-install-config.sh.log	Information about the post install system configuration. This file is seen only on Linux.
som-trace.log som-trace.log.nnn	Information about various operations that occur in SOM with additional details than what appears in the `som.log` file. By default, max value of nnn is 100 and size of each file is 10 MB.

SOM Reporting Server Log Files

The SOM reporting server log files are available at the following location:

`/opt/HP/BSM/PMDB/log`

Log File Rollover

The log file names use the *name*`.log` format. Any archived log file has a number appended to it in the form *name*`.log.`*%g*.

- *name* is the log file base name.
- *%g* relates to the archive number of the archived log file. The highest appended archive number represents the oldest file.

When an active log file exceeds the configured size limit, SOM archives that file by changing the file name to include the archive number and creates a new instance of that log file. For example, the `aggregate.log` file becomes the `aggregate.log.1` file and OBR begins logging to a new `aggregate.log` file.

For detailed information, you can configure OBR to log DEBUG or ALL message types in a log file. For more information about configuring log levels, see the *HPE OBR Troubleshooting Guide*.

Interesting Log Files

The most interesting SOM reporting server log files and the log messages they contain are listed here. When contacting Support, send copies of the following active and archive log files:

Log File	Description
AdministratorService.log	PMDB Platform Administrator service
aggregate.log	Loading of data from the rate tables to the hourly, daily, and forecast tables, and from the hourly tables to the daily tables

Log File	Description
aggrgen.log	Aggregate procedure generation
audit.log	The start time, end time, and duration of back-end processes. When a process begins, the file assigns a Process Identification (PID) that records the process end time.
backend.log	Information about the steps in the data processing job
BOEInstall_0.log BOE_FP_3_5_Install_0.log	SAP BusinessObjects installation log messages
BSMRApp.log	Application-wide log file with error messages from all the OBR modules except data processing.
BSMRCollectionService.log	PMDB Platform Collection Service
BSMRDBLoggerService.log	PMDB Platform DB Logger Service
bsmrfrontend.log	Administration Console UI web application
bsmrim.log	Internal monitoring of data processing job streams, Performance Management Database (PMDB) platform, and Content Packs
BSMRIMService.log	PMDB Platform IM Service
Catalina*.log	Apache Tomcat server
collectStep.log	Collect step that moves data from the `{PMDB_HOME}/collect` directory to the `{PMDB_HOME}/stage` directory
cppatch.log	Patch installation log file
customgroup.log	Import of custom groups defined in an XML file
downtimeutility.log	Configuring downtime and enriching the performance data with configured downtime information
dw_abclauncher.log	Job streams - process specific log files. For example, the `loader.log` file for the loader process
loader.log	Data loading from the stage area to the data store
localhost*.log	Server Access
metadata.log	Metadata repository persistence, access, and modification

Log File	Description
nodefilter.log	Node filters
Postgresql-<date and time>.log	PostgreSQL log file information. This log is available in the `<Postgres_install_directory>/data/pg_log` directory
postinstallconfig.log	Vertica database schema creation, and the OBR Management database schema creation on Postgresql
reload.log	Contrib utility that handles reload of failed data
reloadAppender	Contrib utility (`reload.exe`) that handles reload of failed data
runProc.log	Execution of database procedures and functions associated with each content pack
shiftmaint.log	Populating the shift fact tables based on shift configured in Administration Console
stage.log	Data staging, and purging of staging area
Stderr*.log	Standard error by the Tomcat server. This log is available in the `%PMDB_HOME%\adminServer\logs` directory
Stdout*.log	Standard output by the Tomcat server. This log is available in the `%PMDB_HOME%\adminServer\logs` directory
VerticaService.log	PMDB Platform Vertica Service
trend.log	OBR back-end processes. Each log message includes the start and end time of a logged process
Trendtimer_dbg.log TrendTimerService.log	OBR timer service

For more information about viewing the log levels of a log file, see the *HPE OBR Troubleshooting Guide*.

Chapter 6: Backup and Restore of the SOM Embedded Database

SOM provides the following commands to back up and restore the SOM embedded database. This functionality is useful for creating a snapshot of the data and restoring it.

Ensure that the `somdbmgr` service is running before you begin the backup and restore operations.

Commands and Description

Command

`sombackupembdb.ovpl [-?|-h|-help] [-force] [-noTimeStamp] - target <directory>`

Creates a complete backup of the SOM embedded database (excluding the file system data) while SOM is running.

Parameter	Description

`-?`
`-h`
`-help`
	Displays syntax and usage of the `sombackupembdb.ovpl` command.

`-force`	Starts SOM if it is not already running.
`-noTimeStamp`	Removes the time stamp from the back up name.
`-target <directory>`	(*Required*) Specifies the target directory where the data needs to be backed up.

`somrestoreembdb.ovpl [-?|-h|-help] [-force] -source <file>`

Restores a backup that was created by using the `sombackupembdb.ovpl` script.

Parameter	Description

`-?`
`-h`
`-help`
	Displays syntax and usage of the `somrestoreembdb.ovpl` command.

`-force`	Stops or starts SOM as required.
`-source <file>`	(*Required*) Specifies the source file name where the data that needs to be restored is saved.

`somresetembdb.ovpl`

Drops the SOM embedded database tables. Runs the ovstart command to recreate the tables.

When you reset the database, it is recommended that you delete the contents of the `repository` folder manually if you plan to use a different user for discovery the next time. The folder is located at the location:

- **Windows**: <*Install_Dir*>\HP\HP BTO Software\se\repository
- **Linux**: <*Install_Dir*>/var/opt/OV/se/repository/root/cimv2

Parameter	Description

`-?`
`-h`
`-help`
	Displays syntax and usage of the `somrestoreembdb.ovpl` command.

`-force`	Stops or starts SOM as required.
`-source <file>`	(*Required*) Specifies the source file name where the data that needs to be restored is saved.

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 Deployment 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!