Hewlett Packard
Enterprise

HPE Storage Operations Manager

Software Version: 10.20
Windows® and Linux® operating systems

HPE Operations Manager i Integration 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.

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: Introduction

HPE Operations Manager i (OMi) provides comprehensive event management, proactive performance monitoring and automated alerts, reports, and graphs to manage operating systems, middleware, and application infrastructure. OMi consolidates events from a wide range of sources into a single view.

The HPE Storage Operations Manager (SOM)—OMi integration provides event consolidation in the OMi active messages browser, so that OMi users can detect and investigate potential problems in the storage infrastructure.

The OMi systems management uses HPE Universal CMDB (UCMDB) to build a Runtime Service Module (RTSM) of the server infrastructure elements. It thereby captures the correlations between the application and server layers. RTSM allows you to define Configurations Items (CIs) that are stored in UCMDB. Each infrastructure element is represented by a CI in RTSM. A CI is a database representation and can be a line of business, business process, application, server hardware, or a service. CIs can be populated by any management system and are identified by business keys.

SOM manages the dependencies between the server and storage layers. The server layer is common to both the management systems. SOM populates the CIs in UCMDB just as OMi populates the same CIs in UCMDB. The UCMDB content packs populate and reconcile these CIs using business keys. Therefore, it gives OMi the end-to-end picture from the application to the storage dependency level in a data center.

RTSM allows you to build correlation rules to analyze the impact of events. Event attributes allow OMi to build workflows that highlight the criticality of events. Multiple related correlations help bring out the true value of integrating with OMi.

Prerequisites

To achieve the integration, both SOM and OMi, must be installed on separate servers, and can run on the same or different operating systems.

Ensure that these ports are open on the OMi server for the following protocols:

- **WMI** - 135
- **SSH** - 22

The Business Service Connector (BSMC) must be installed on the SOM management server after you install SOM. The BSMC comprises the Operations Agent (OA) and the BSM component. SOM uses the BSMC to filter and send events to the OMi active messages browser.

In addition, you must have a local copy of the following Content Pack from the SOM HPE Live Network web site (https://hpln.hpe.com/contentoffering/hp-som-1010-ucmdb-content-pack): **HP SOM 10.10 UCMDB Content Pack (for UCMDB 10.20 CP16), Version 10.10**.

This Content Pack contains the following files that are required to bring in the storage CIs into RTSM.

- HP_SOM_Integration.zip
- Storage_Basic.zip

For information about supported hardware platforms and operating systems, see the support matrices of the related products.

SOM–OMi Architecture

Data flows bidirectionally due to the the SOM—OMi integration. The SOM inventory data is periodically pulled by OMi while the SOM data about management events and traps is asynchronously sent to OMi.

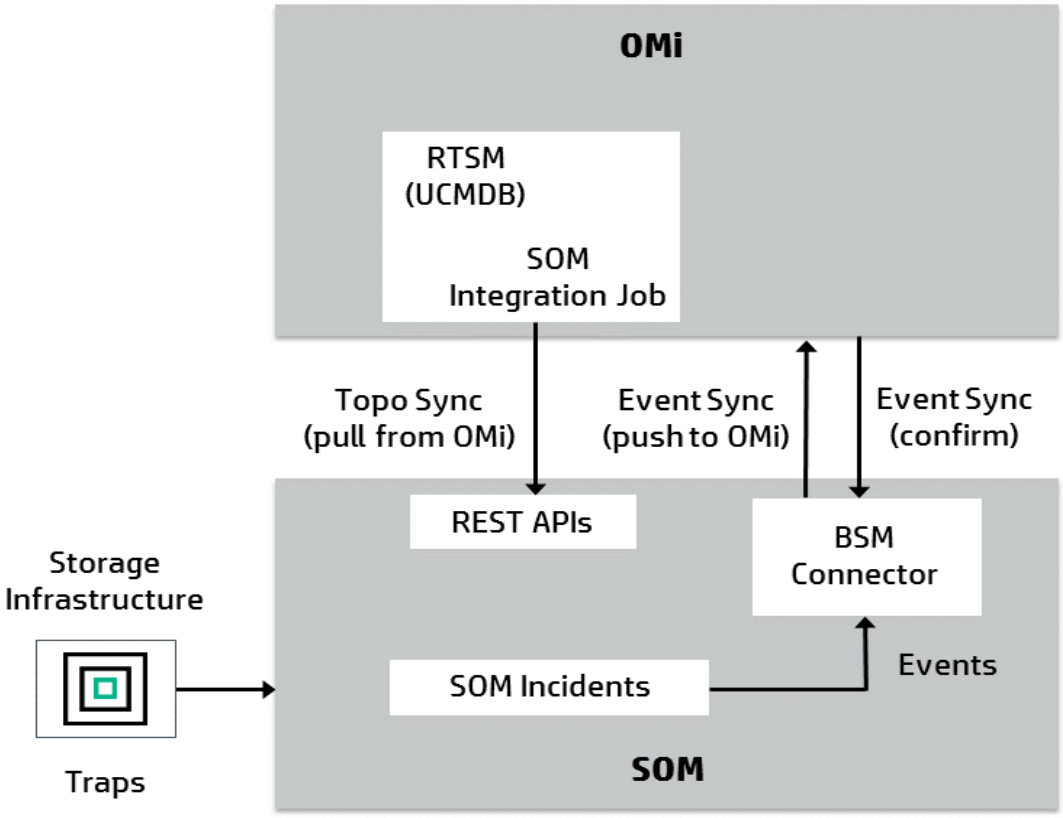
There are two aspects to the SOM—OMi integration: Topology Synchronization and Event Synchronization.

Topology Synchronization

OMi integrates with UCMDB to build a Real Time Service Map (RTSM) and maintains a Configuration Item (CI) in UCMDB for each storage infrastructure element managed by SOM. SOM collects data from the storage infrastructure elements using device or native APIs. This inventory data is periodically pulled by UCMDB using REST APIs via the HTTPS protocol. This data synchronization is referred to as Topology Synchronization (Topo Sync).

Event Synchronization

Devices send SNMP traps to SOM when generated by a device. SOM generates incidents for the third-party traps, and the SOM management events. These incidents are sent as SNMPv2c traps to the BSM Connector on the SOM management server. The BSM Connector filters the SOM traps and forwards them as events to the OMi event browser. This is referred to as Event Synchronization (Event Sync).


OMi
RTSM
(UCMDB)
SOM
Integration Job
Topo Sync
(pull from OMi)
Event Sync
(push to OMi)
Event Sync
(confirm)
REST APIs
BSM
Connector
Storage
Infrastructure
Events
SOM Incidents
SOM
Traps

Chapter 2: Configuring the SOM–OMi Integration

It is recommended that an experienced administrator completes all the procedures to achieve the SOM—OMi integration.

To configure the agent implementation of the SOM—OMi integration, complete the following:

- Install HPE Storage Operations Manager on the management server.

  For more information about the installation procedure see the *SOM Interactive Installation Guide*
- Install the Business Service Connector (BSMC) on the SOM management server.

  For more information about the installation procedure see the *BSM Connector 10.01 Installation and Upgrade Guide* (https://softwaresupport.hpe.com/km/KM01898688)

  Note: To install BSMC, the SOM user account must have an administrator role.

- "Configure Topology Synchronization" below
- "Configure Event Synchronization" on page 11

Configure Topology Synchronization

The inventory data collected by SOM is synchronized with OMi using the Data Flow Probe in UCMDB. SOM communicates with UCMDB using Rest APIs via the HTTPS protocol.

The SOM inventory data includes information about the storage infrastructure (storage systems, hosts, fibre channel switches, and fabrics) and infrastructure components (storage volumes, HBAs, controllers, switch ports, and so on).

To synchronize the topology information between SOM—OMi, complete the following:

1. Deploy the SOM packages.
   a. Obtain the following packages from the **HP SOM 10.10 UCMDB Content Pack (for UCMDB 10.20 CP16), Version 10.10** Content Pack on the SOM HPE Live Network web site (https://hpln.hpe.com/contentoffering/hp-som-1010-ucmdb-content-pack):
      - `HP_SOM_Integration.zip`
      - `Storage_Basic.zip`
   b. Log on to OMi as an administrator.
   c. Click **Administration** > **RTSM Administration** > **Administration** > **Package Manager**.

d. From the menu bar, click (**Deploy packages to server (from local disk)**). The **Deploy Packages to Server** dialog box appears.

e. Click **Add**.

f. Select the **HP_SOM_Integration.zip**, and the **Storage_Basic.zip** files together from your local folder, and then click **Open**.

g. Click **Deploy**.

2. Create an SOM user that belongs to the Web Service Clients user group.

a. On the SOM management server, click **Configuration** > **Security** > **User Accounts**, and then click **New**.

b. Specify the user account name and credentials, and click **Save and Close**.

c. To map the new user account to the Web Service Clients group, click **Configuration** > **Security** > **User Account Mappings**, and then double-click to **Open** the user account.

d. On the User Account Mapping form, from the **User Group** list, select the **Web Service Clients**.

e. Click **Save and Close**.

3. Install the Data Flow Probe Manager.

Ensure that the Data Flow Probe (DFP) Manager is installed either on the OMi server or on a separate server. Configure the probe to point to the OMi server. If the new data flow probe is on the OMi server, ensure that the UCMDB services are up. Else, start the following manually in the DFP Manager Services (Local):

- `UCMDB Probe`
- `UCMDB_Probe_DB`

4. Configure the required protocols with the DFP on the OMi server.

a. Click **Administration** > **RTSM Administration** > **Data Flow Management** > **Data Flow Probe Setup**.

b. In the **Domains and Probes** pane > **DefaultDomain(Default)**, expand **Data Flow Probes**, and click the probe you want to use.

c. In the **Ranges** pane, click (**New**). The **New Range** dialog box appears.

d. In the Range field, type the IP address range for the SOM management server.

> **Note:** You can add multiple ranges to support many SOM management servers.

e. Click **OK**.

f. From the **Domains and Probes** pane > **DefaultDomain(Default)**, expand **Credentials**, and configure the following selected protocols:

i. **WMI Protocol** for the SOM servers running on Windows.

ii. **SSH Protocol** for the SOM servers running on Linux.

g. In the selected protocol pane, click ✱ (**New**) to set the protocol parameters.

i. Click **Edit** to specify the network scope.

ii. In the Scope Definition dialog box, click the **Selected Range** option, and then click ✱ (**New**) to create a new range. Type the SOM server information, and then click **OK**.

iii. Enter the credentials of the Administrator/root user account to access the SOM management server.

iv. Click **OK** to save the protocol.

h. Select the **HTTP Protocol**, and then click ✱ (**New**) to set the protocol parameters.

- Follow the same setup procedure as WMI and SSH.
- Use the user account that belongs to the Web Service Clients group.
- Set the timeout to a minimum of 60,000 msec. (60 seconds)
- Set the Port number to 443.
- In the Host field, specify the IP of the SOM management server.
- Ignore the Realm field.
- Trust store information is optional.

5. Discover the data flow probe and the host connections.

a. Click **Administration** > **RTSM Administration** > **Data Flow Management** > **Discovery Control Panel**.

b. In the left pane, **Discovery Modules/Jobs** tab > **Discovery Modules**, expand **Network Infrastructure** > **Basic**.

c. Right-click **Range IPs by ICMP**, and then click **Activate** to discover the DFP.

d. Expand **Host Connection** in the file tree.

- For SOM servers running on Windows, right-click **Host Connection by WMI**, and then select **Activate**. This discovers the SOM management server through the DFP.
- For SOM servers running on Linux, right-click **Host Connection by Shell** and select **Activate** to discover the SOM management server through the DFP.

6. Create a new integration point.

a. Click **Administration** > **RTSM Administration** > **Data Flow Management** > **Integration Studio**.

b. Click ✱ (**New**) to create a new integration point.

c. Click the **Select Adapter** button. The **New Integration Point** dialog box appears.

d. Expand **HP Software Products**, and select **HP SOM Integration**.

e. From Integration Properties, set the following properties of the adapter:

i. Select **Is Integration Activated**.

ii. Set the credentials ID to the HTTPS protocol credential.

iii. Select the Data Flow Probe from the list.

iv. Near the **Trigger CI instance** field, click the cube, and choose a CI to be associated with the SOM management server.
The CI should be set to the IP of the SOM server.

7. Right-click the integration point, and select **Run All-Data Sync**.

Note: In UCMDB, if the combination of the IP address and name of a physical and virtual switch is the same, then the corresponding CIs are considered duplicates. Therefore, these CIs are merged into a single CI. To handle this issue, the IP address field is not populated for the virtual switches. However, the parent physical switch has the associated IP address.

Configure Event Synchronization

SOM generates incidents that are sent to OMi as events. These incidents result from SOM management events and the third-party SNMP traps received by SOM from discovered devices.

To synchronize SOM events with OMi, complete the following procedures:

- "Configure the SOM Management Server" below
- "Configure the OMi Server" on page 17

Configure the SOM Management Server

To enable the SOM management server to forward events to OMi, complete the following procedures:

1. Run the following command to verify that all the SOM services are in the RUNNING state :

   ```
   ovstatus -c
   ```

2. Identify an available port for SNMP communications between SOM and the BSM Connector.
   This port must be different from the SNMP port 162, that is used by SOM to receive third-party traps.

3. Configure BSMC with the custom port to receive SNMP traps.

   Type the following command on the SOM management server:

   Windows

   ```
   ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> -set SNMP_SESSION_MODE NNM_LIBS
   ```

   Linux

   ```
   ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> -set SNMP_SESSION_MODE NO_TRAPD
   ```

   where `<custom_port>` is the port number from step 2.

4. Generate a policy configuration file for SOM events.

   SOM events policy configurations determine how OMi treats and displays incoming traps from SOM. The SOM events policy configuration file includes a policy condition for each management event and SNMP trap configuration in the current SOM incident configuration.

   Tip: To configure SOM to automatically close incidents that are closed in OMi, see "Enable Event Acknowledgment" on page 17 and complete steps 1-3 before generating the SOM events policy configuration.

   Run the following command on the SOM management server to generate the policy file:

   Windows:

   ```
   %OvInstallDir%\bin\somopcexport.ovpl -u <SOM console username> -p <SOM console password> -template "SOM Management Events" -application "SOM" -omi_policy -omi_hi
   ```

   Linux:

   ```
   /opt/OV/bin/somopcexport.ovpl -u <SOM console username> -p <SOM console password> -template "SOM Management Events" -application "SOM" -omi_policy -omi_hi
   ```

   This command creates two files in the current directory—`<UUID>_data` and `<UUID>_header.xml`

5. From BSMC, create a certificate request for OMi by running the following command:

   Note: On OMi, ensure that you create a user account with the super admin role before you generate a certificate request.

   Windows:

   ```
   %OvDataDir%\installation\HPOprBSMC\bsmc-conf.bat –s <bsm server> -admin_user <bsmc_user> <bsmc_user_passwd>
   ```

   Linux:

   ```
   /var/opt/OV/installation/HPOprBSMC/bsmc-conf.sh –s <bsm server> -admin_user <bsmc_user> <bsmc_user_passwd>
   ```

   Where `<bsmc_user>` is the user account created on the OMi server with the super admin role. For example,

   ```
   %OvDataDir%\installation\HPOprBSMC\bsmc-conf.bat -s tcesx06vm9.fcusa.hp.com –admin_user bsmc_admin bsmc_admin
   ```

   Note: If your environment contains the SOM reporting Server (OBR) and the OMi server, you must configure the OMi server to be the primary certificate authority for SOM, the Operations agent, and the SOM reporting server.

For more information about configuring the OMi server as the primary certificate authority, see "Connect the SOM Management Server, the SOM Reporting Server, and the HPE OMi Server" on page 18

6. Verify that the certificate request has been accepted by OMi.
7. If OMi does not receive the certificate request ID , rerun the `bsmc-conf.bat` command with the `-f` option. Otherwise, skip this step.

   ```
   BSMC DataDir>\installation\HPOprBSMC\bsmc-conf.bat –s <bsm server> -f -admin_user <bsmc_user> <bsmc_user_passwd>
   ```
8. Verify that the certificate request has been accepted by OMi.
9. Verify that the DNS name of the OMi server is assigned to the CERTIFICATE_SERVER and MANAGER attributes by running the following command: `ovconfchg –edit`
10. Restart the BSMC trap service, by running the following command:

    ```
    ovc -restart opctrapi
    ```
11. Activate the SOM events policy configuration file on BSMC.
    a. Log on to the BSMC console, `https://<somServer>:30000/bsmconnector` with the credentials used during the BSMC installation.
    b. Click  (**Import**), and select the data and header files from the %OvInstallDir%\bin folder.
    c. Right-click the **SNMP Interceptor** (Policy Type), and activate the policy.
12. Configure the Integration Module Configuration workspace to enable SOM to forward incidents to OMi. To achieve this, follow these steps:
    a. From the left pane, click the **Integration Module Configuration** workspace, and select **HP OMi**. The **HP SOM–HP OMi Agent Destinations** form appears. It lists existing destinations, if any.
    b. Click **New**. The options required to create a new destination appear.
    c. Select the **Enabled** check box at the top of the form.
    d. Set the communication parameters in the form. For more information, see the "HP SOM—HP OMi Agent Destinations Form" below.
    e. Click **Submit**.

       A new window appears with a status message. If the message indicates a problem with the settings, click **Return**, and then adjust the values as suggested by the text of the error message.

    SOM begins forwarding incidents as soon as you enable the destination.

HP SOM–HP OMi Agent Destinations Form

The HP SOM—HP OMi Agent Destinations form contains the parameters required to configure data transfer between SOM and the BSMC Operations agent. This form is available from the Integration Module Configuration workspace.

Note: Only SOM users with the Administrator role can access this form.

The SOM—OMi Agent Destinations form collects information for the following areas:

- "Agent Communication" below
- "Integration Content" below
- "Status Information" on page 16

The parameters in the SOM—OMi Agent Destinations form are described in the following tables:

Agent Communication

Field	Description
Host	The fully-qualified domain name (preferred) or the IP address of the SOM management server. The Operations agent receives SNMP traps from SOM on this server. The integration supports the following methods for identifying the Operations agent host: • **SOM FQDN** SOM manages the connection to the Operations agent on the SOM management server and the Host field becomes read-only. This is the default and recommended configuration.
Port	The UDP port where the Operations agent receives SNMP traps. Type the port number specific to the Operations agent. This value is the port number that you identify in step 2 of "Configure the SOM Management Server" on page 11. To determine the port, run the `ovconfget eaagt` command on the SOM management server. The trap port is the value of the `SNMP_TRAP_PORT` variable.
Community String	A read-only community string for the Operations agent to receive traps. Use the default value, **public**.

Integration Content

Field	Description
Incidents	Incidents that are forwarded • **Management** SOM forwards SOM-generated management incidents to the Operations agent. • **3rd Party SNMP Trap** SOM forwards SNMP traps received from managed devices to the Operations agent.

Field	Description
Lifecycle State Changes	Specifications for changes in the incident states • **Enhanced Closed** SOM sends an incident closed trap to the Operations agent for each incident that changes to the CLOSED lifecycle state. This is the default configuration. • **State Changed** SOM sends an incident lifecycle state changed trap to the Operations agent only for CLOSED incidents. • **Both** SOM sends an incident closed trap to the Operations agent for each incident that changes to the CLOSED lifecycle state. Additionally, the integration sends an incident lifecycle state changed trap to the Operations agent for each incident that changes to the IN PROGRESS, COMPLETED, or CLOSED lifecycle state. **Note:** In this case, each time an incident changes to the CLOSED lifecycle state, the integration sends two notification traps: an incident closed trap and an incident lifecycle state changed trap.
Correlations	Specifications for incident correlations • **None** SOM does not notify the Operations agent of incident correlations resulting from SOM causal analysis. This is the default configuration. • **Single** SOM sends a trap for each parent-child incident correlation relationship resulting from SOM causal analysis. • **Group** SOM sends one trap per correlation that lists all child incidents correlated to a parent incident.
Deletions	Specifications for incident deletions **Note:** This feature will be supported in a future release. • **Don’t Send** SOM does not notify the Operations agent when incidents are deleted in SOM. This is the default configuration. • **Send**

Field	Description
	SOM sends a deletion trap to the Operations agent for each incident that is deleted in SOM.
SOM Console Access	The protocol used for communication between SOM and the OMi message browser. Select the **HTTPS** option.
Incident Filters	A list of SNMP trap object identifiers (OIDs) used to filter the events sent to the Operations agent. Each filter entry can be a valid numeric OID (for example, .1.3.6.1.6.3.1.1.5.4.1.3.6.1.4.1.9) or OID prefix (for example, .1.3.6.1.6.3.1.1.5.*). • **None** SOM sends all events to the Operations agent. This is the default configuration. • **Include** SOM sends only the specific events that match the OIDs identified in the filter. • **Exclude** SOM sends all events except for the specific events that match the OIDs identified in the filter. Specify an incident filter: • To add a filter, type an SNMP trap OID, and then click **Add**. • To delete a filter, select an SNMP trap OID from the list, and then click **Remove**.

Status Information

Field	Description
Trap Destination IP Address	The Operations agent destination host name resolves to this IP address. This value is unique to this Operations agent destination.
Uptime (seconds)	The time in seconds since the BSM component was last started. The traps that SOM sends to the Operations agent include this value in the sysUptime field (1.3.6.1.2.1.1.3.0). To see the latest value, either refresh or close and re-open the form.
SOM URL	The URL of the SOM console. The traps that SOM sends to the Operations agent include this value in the NmsUrl varbind (1.3.6.1.4.1.11.2.17.19.2.2.2).

Enable Event Acknowledgment

You can configure SOM to automatically close an incident after the corresponding event is closed on the OMi server.

To close incidents in SOM based on the events that are closed in OMi, follow these steps:

1. Run the following command:

   `somconfigurebacksync.ovpl`

   When prompted, type the SOM console user name and password.

   Note: If the password of the SOM user is changed, you must rerun the `backsync` command.

2. Run the following command from the **`%OvInstallDir%`** folder:

   ```
   newconfig\HPNmsCommon\scripts\nnm-configure-perl.ovpl –source
   newconfig\HPNmsCommon\perl\a -target nonOV\perl\a
   ```

3. Run the following command to restart the ombacksync process:

   `ovc –restart ombacksync`

4. On the SOM management server, regenerate the policy configuration file for the new traps.
5. On BSMC, import the policy configuration file.
6. To activate the policy files, follow these steps:
   a. From the list of policies in BSMC, select the policies that must be activated.

      The activation state of at least one of the selected policies must be Deactive or Active (reactivate for new version). If one of the policies in the selection is already active, the policy is ignored and not reactivated.

   b. Click the tool bar. The activation state changes to Activated.

Note: If you open a closed event in OMi, the event is not opened in SOM.

Configure the OMi Server

Event synchronization with OMi is achieved through the BSM Connector that integrates with the OMi server.

Before you proceed, ensure that all the OMi services are running and the required licenses are successfully installed.

1. Create a super admin user.
   a. Log on to the OMi server's jmx console with the following URL:

      `http://<OMi server>:21212/jmx-console`

b. Navigate to one of the following:
   - UCMDB:service = Security Services

     Or
   - UCMDB:service=Authorization Services

c. Create a new super admin user account with the `createUser` link.

d. Set the role to **SuperAdmin** for the new user account using the `setRolesForUser` link.

2. Accept the certificate request from BSMC.

   a. To display the `<request ID>` of the certificate, run the following command: `ovcm -listpending`

   b. If the `<request ID>` is listed, run the following command to grant the certificate request: `ovcm -grant <request ID>`

      Where `<request ID>` is obtained from the first command.

   c. To verify the communication with the BSM Integration Adapter, run the following command: `bbcutil -ping <SOMserver>`

3. Add the BSMC details to the OMi server.

   a. On the SOM management server, close any running instances of the `ovconfchg -edit` command.

   b. Log on to the OMi console with the `http://<OMi server>/omi` URL.

   c. Click **Administration** > **Setup and Maintenance** > **Connected Servers**.

   d. From the Connected Servers pane, click **New** > **BSM Connector**. The **Create New Server Connection - BSM Connector** form appears.

   e. On the **General** page, do the following:
      i. Type the **Display Name** of the BSM Connector.
      ii. Type the **Name** of the BSM Connector.
      iii. *Optional*. Type a **Description** of the BSMC if the environment has multiple connectors.
      iv. Select the **Activate BSM Connector Server after creation** check box.

   f. On the **Server Properties** page, type the FQDN of the SOM management server, and click **Next**.

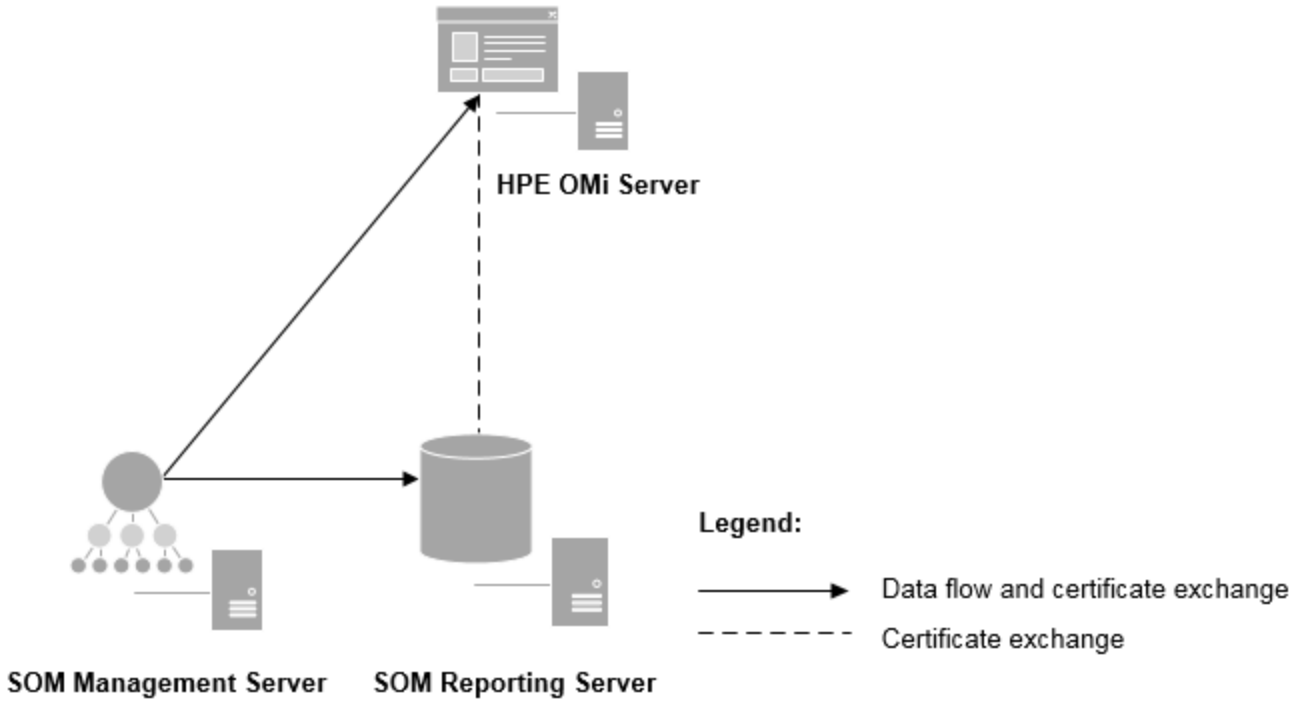
   g. On the **Policy Management** page, use the default settings, and click **Next**.

   h. On the **Event Drilldown** page, do the following:
      - Type the FQDN of the SOM management server.
      - Ensure that the **Port Number** is 443.
      - Click **Finish**.

      Implementing a BSMC integration automatically creates a BSMC connected server in OMi.

Connect the SOM Management Server, the SOM Reporting Server, and the HPE OMi Server

The content in this chapter applies to the following architecture with HPE OMi as the certificate authority:



HPE Operations Bridge Reporter (OBR) and HPE Operations Manager (HPE OMi) can each act as a certificate authority for SOM and the Operations agent. This section describes how to configure the OMi server to be the primary certificate authority for SOM, the Operations agent, and OBR (the SOM reporting server).

To connect an SOM management server with an SOM reporting server and an OMi server, complete all of the following tasks:

"Task 1: Connect the SOM Management Server to the HPE OMi Server" below

"Task 2: Connect the SOM Reporting Server to the HPE OMi Server" on the next page

"Task 3: Configure Data Transfer from the SOM Management Server to the SOM Reporting Server" on page 21

"Task 4: Configure the SOM Reporting Server to Populate the Analytics Dashboards" on page 21

Task 1: Connect the SOM Management Server to the HPE OMi Server

To configure the SOM management server to use the OMi server as its certificate authority, follow these steps:

1. On the SOM management server, install the Operations agent.

   The certificate request from the Operations agent does not automatically reach the OMi server.
2. On the SOM management server, delete any existing certificates configured on the SOM management server and request a new certificate by running the following command:

   somdatatransfercertconfig.ovpl -certserver *<OMi_server>*

Replace <*OMi_server*> with the IP address or fully qualified domain name of the OMi server.

3. On the OMi server, grant the certificate request.
4. Activate the Operations agent for the OMi server.
5. On the OMi server, add the SOM management server node, and then accept its certificate request.
6. To verify the communication from the OMi server to the SOM management server, send a test message from the Operations agent.

   For example:

   opcmsg s=critical o=test msg_g=OpC a=test msg_t="test"

Task 2: Connect the SOM Reporting Server to the HPE OMi Server

To configure the SOM reporting server to use the OMi server as its certificate authority, follow these steps:

1. On the SOM reporting server, install the Operations agent.

   The certificate request from the Operations agent does not automatically reach the OMi server.
2. On the SOM management server, copy the `somshrgrantcertrequest.ovpl` command from the following location to a known location:

   - *Windows*: `%OvInstallDir%\bin`
   - *Linux*: `/opt/OV/bin`

   on the SOM reporting server.
3. From the known location on the SOM reporting server, delete any existing certificates configured on the SOM reporting server and request a new certificate by running the following command:

   somshrgrantcertrequest.ovpl -certserver <*OMi_server*>

   Replace <*OMi_server*> with the IP address or fully qualified domain name of the OMi server.
4. On the OMi server, grant the certificate request.
5. Activate the Operations agent for the OMi server.
6. On the OMi server, add the SOM reporting server node, and then accept its certificate request.
7. To verify the communication from the OMi server to the SOM reporting server, send a test message from the Operations agent.

   For example:

   opcmsg s=critical o=test msg_g=OpC a=test msg_t="test"

Task 3: Configure Data Transfer from the SOM Management Server to the SOM Reporting Server

To configure data transfer from the SOM management server to the SOM reporting server, follow these steps:

1. On the SOM management server, start the OVC service by running the following command:
   - *Windows*: `%OvInstallDir%\bin\win64\ovc -start`
   - *Linux*: `/opt/OV/bin/ovc -start`
2. On the SOM management server, configure data transfer from the SOM management server to the SOM reporting server by running the following command:

   somdatatransfercertconfig.ovpl –remoteserver <*OBR_server*> -remotefolder /opt/HP/BSM/PMDB/extract

   Replace <*OBR_server*> with the IP address or fully qualified domain name of the local SOM reporting server.

   `/opt/HP/BSM/PMDB/extract` is the location on the SOM reporting server that will receive the SOM data. This location is not configurable.
3. On the SOM reporting server, configure the SOM reporting server to use the SOM management server as a data source by running the following command (copied to the SOM reporting server in Task 2):

   somshrgrantcertrequest.ovpl -datasource <*SOM_server*>

   Replace <*SOM_server*> with the IP address or fully qualified domain name of the SOM management server.

   Note: To send data from multiple SOM management servers to the reporting server, replace <*SOM_server*> with a whitespace separated list of SOM management servers. For example:
   `somshrgrantcertrequest.ovpl -datasource 10.226.151.10 10.226.153.10 10.226.153.25`

   The value of the `-datasource` parameter overwrites the current OBR configuration. Always specify *all* SOM management servers that connect to this reporting server when running this command.
4. Verify data transfer from the SOM management server to the SOM reporting server.
   a. On the SOM management server, send a test data file to all configured reporting servers by running the following command:

      somdatatransfercertconfig.ovpl –testtransfer

   b. On the SOM reporting server, change to the `/opt/HP/BSM/PMDB/extract` directory, and then verify that the `test_transfer_from_<SOM_server>.txt` file is present in the directory.

Task 4: Configure the SOM Reporting Server to Populate the Analytics Dashboards

SOM analytics dashboards display information obtained from the SOM Reporting Server database.

To support the data gathering from OBR for the analytics dashboards:

- Port 5433 must be open on the SOM reporting server.
- SOM must be connected to the SOM reporting server database that processes the capacity utilization data exported from the SOM management server.

To configure the SOM Reporting Server to pull data for the analytics dashboard, run the following command:

somdatatransfercertconfig.ovpl -shrdbconfig *<OBR_database_hostname> <OBR_database_port number> <OBR_database_username> <OBR_database_password>*

Replace *<OBR_database_hostname>* with the IP address or fully qualified domain name of the database server used by the SOM reporting server.

Replace *<OBR_database_port number>* with the port for connecting to the database used by the SOM reporting server. The default port number is 5433.

Replace *<OBR_database_username>* with the user name for accessing the database used by the SOMreporting server.

Replace *<OBR_database_password>* with the password for the specified user name as configured post installation of the SOM reporting server.

Chapter 3: Using the SOM–OMi Integration

The agent implementation of the SOM—OMi integration provides a one-way flow of SOM management events and SNMP traps to the BSM Connector. The SOM events policy configuration determines how OMi treats and shows the incoming traps. For example, you can change a policy condition to include the value of a trap custom message attribute (CMA) in the message text.

SOM sends only one copy of each management event or SNMP trap to the BSM Connector. You can see the forwarded SOM incidents in the OMi active messages browser. Information embedded in each message supports this cross-navigation:

- The `som.server.name` and the `som.server.port` CMAs in the message identify the SOM management server.
- The `som.incident.uuid` CMA identifies the incident in the SOM database.

The original source object appears in the Object column of the OMi active messages browser and in the `som.source.name` CMA.

> **Note:** When you select a Node CI or an event associated with a Node CI, a list of Tools appears. The current list of tools is not applicable to SOM.

Default Policy Conditions

The default integration behavior varies with the integration content, as described here:

- SOM management event incidents
  - When generated, the SOM events policy configuration file includes conditions for all SOM management event configurations.
  - The messages created from SOM management events appear in the OMi active messages browser.
  - These traps include the CI information.
  - The messages created from these traps might include health indicators.
- EventLifecycleStateClosed traps
  - The OA logs the messages created from these traps. Generally, they do not appear in the OMi active messages browser.
  - The SOM events policy configuration file causes the OA to acknowledge the message that corresponds to the closed SOM incident in the OMi active messages browser.

- LifecycleStateChangeEvent traps

  The SOM events policy configuration file does not include conditions for processing these traps. The OA does not forward these traps to the OMi active messages browser.

- EventDeleted traps

  The SOM events policy configuration file does not include conditions for processing these traps. The OA does not forward these traps to the OMi active messages browser.

- Correlation notification traps
  - The OA logs the messages created from these traps. They do not appear in the OMi active messages browser.
  - These traps have no impact on the OMi active messages browser.

Customizing Policy Conditions

To customize the default policy conditions, edit the conditions on the OMi management server, and then re-deploy the policy to the OA on the SOM management server. For more information, see the following:

- OMi for Windows: *SNMP Interceptor Policies* in the OMi help
- OMi for Linux: *OMi for UNIX and Linux Concepts Guide*

Chapter 4: Additional Tasks

This section includes the following topics that describe configuration and maintenance procedures that might be required post integration.

Update the SOM events policy configuration for New SOM Traps

If new SNMP trap configurations are added to SOM since the integration was configured, follow these steps:

1. On the SOM management server, use the `somopcexport.ovpl` command to create a new SOM events policy configuration file for the new traps.

   For the `-template` option, specify a name that is different from the existing SOM events policy configuration file.

   You can limit the file contents to a specific author or OID prefix value. For more information, see the `somopcexport.ovpl` reference page.
2. Copy and import the new SOM events policy configuration file from the SOM management server to the OMi management server.

Alternatively, you can re-create the SOM events policy configuration file for all SOM management events and SNMP traps. If you adopt this approach, importing the new policy file in OMi overwrites any existing policy customizations.

Change Configuration Parameters

To change the integration configuration parameters, follow these steps on the SOM management server:

1. From the left pane, click the **Integration Module Configuration** workspace, and select **HP OMi**. The **HP SOM–HP OMi Agent Destinations** page appears.
2. Select a destination, and then click **Edit**.
3. Modify the values as required.
4. Verify that the **Enabled** check box is selected at the beginning of the form.
5. Click **Submit**.

   A new window appears with a status message. If the message indicates a problem with the settings,

click **Return**, and then adjust the values as suggested by the text of the error message.

The changes are effective immediately.

Disable the SOM–OMi Integration

To stop forwarding SOM incidents to the OA, follow these steps:

Caution: SNMP traps are not queued when a destination is disabled.

1. From the left pane, click the **Integration Module Configuration** workspace, and select **HP OMi**. The **HP SOM–HP OMi Agent Destinations** page appears.
2. Select a destination, and then click **Edit**.
3. Clear the **Enabled** check box at the top of the form.
4. Click **Submit**.

   The changes are effective immediately.

Alternatively, click **Delete** to remove the configuration for the selected destination. Or, deactivate or delete the SOM events policy configuration as described in the OMi documentation.

Chapter 5: Troubleshooting the SOM–OMi Integration

This section provides information to resolve the following scenarios:

SOM incidents are not forwarded to OMi

1. Verify the OA configuration on the SOM management server.

   Windows

   ```
   %OVBIN%\ovconfget eaagt
   ```

   Linux

   ```
   $OVBIN/ovconfget eaagt
   ```

   The output of the command should include the following:

   Windows

   ```
   SNMP_SESSION_MODE=NNM_LIBS SNMP_TRAP_PORT=<custom_port>
   ```

   Linux

   ```
   SNMP_SESSION_MODE=NO_TRAPD SNMP_TRAP_PORT=<custom_port>
   ```

   The value of `<custom_port>` should not be 162 and should match the value of the port number on the **HP SOM–HP OMi Agent Destinations** page.

2. Evaluate the results of the OA configuration.

   - If the `SNMP_SESSION_MODE` parameter is not set correctly, run the following commands:

     i. `ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> -set SNMP_SESSION_MODE NNM_LIBS`

     ii. The `ovconfget` command to confirm that the result is as expected.

   - If the value of `<custom_port>` is 162 or does not match the value of the port number specified in the **HP SOM–HP OMi Agent Destinations** page, run the following commands:

     i. `ovconfchg -ns eaagt -set SNMP_TRAP_PORT <custom_port> -set SNMP_SESSION_MODE NNM_LIBS`

     ii. The `ovconfget` command to confirm that the result is as expected.

3. Verify that the OA is running on the SOM management server.

   Windows

   ```
   %OVBIN%\opcagt –status
   ```

Linux

```
$OVBIN/opcagt –status
```

The output of the command should include an opctrapi entry similar to the following:

```
opctrapi OVO SNMP Trap Interceptor AGENT, EA (4971) Running
```

If the output is not as expected, restart the agent with the following command:

```
ovc -restart opctrapi
```

4. Verify that the OA is listening to the expected SNMP trap port on the SOM management server.
   a. Run the following command:

      Windows

      ```
      netstat -an | findstr <custom_port>
      ```

      Linux

      ```
      netstat -an | grep <custom_port>
      ```

      Where the value of `<custom_port>` should match the value of the port number on the **HP SOM–HP OMi Agent Destinations** page.
   b. Verify that the output of the command includes the state as LISTENING or LISTEN.

      If the output is not as expected, restart the agent with the following command:

      ```
      ovc -restart opctrapi
      ```

   a. Verify that the SOM events policy configuration file is deployed on the BSMC installed on the SOM management server.

      Run the following command:

      Windows

      ```
      %OVBIN%\ovpolicy –list
      ```

      Linux

      ```
      $OVBIN/ovpolicy –list
      ```

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

      ```
      Type          Name                                          Status   Version
      ------------------------------------------------------
      trapi         "SOM Management Events"                       enabled  1.0
      ```

5. Check the OA log file for errors.

   The log file is available in the following location:

   Windows

   ```
   %OvDataDir%\log\System.txt
   ```

   Linux

   ```
   /var/opt/OV/log/System.txt
   ```

6. Verify that BSMC is receiving traps.
   a. Enable tracing in BSMC to determine whether the traps arrive at the BSM connector.

      From the **Options** tab of the SNMP policy, enable the log for incoming traps. The log file is available in the following location:

      Windows

      `%OvDataDir%\log\OpC\opcmsglg`

      Linux

      `/var/opt/OV/log/OpC/opcmsglg`
   b. Verify that BSMC can send events to the OMi event browser.
      i. From the **Options** tab of the SNMP policy, select **forward unmatched events to active browser** to create an open message interface policy.
      ii. Click **Save and activate**.
      iii. Run the `opcmsg` command to send events to the OMi event browser.
7. Verify that SOM is forwarding management events to the BSM Connector.
   a. Verify that the integration is running correctly.
      i. Open the **HP SOM–HP OMi Agent Destinations** page (**Integration Module Configuration** > **HP OMi**).
      ii. Select a destination, and then click **Edit**.
      iii. Verify that the **Enabled** option is selected.
   b. Generate a new event in SOM.
      i. Run data collection for an element.
      ii. After 30 seconds, check if OMi receives a "Data Collection Successful" event.
         - If OMi does not receive the trap, configure a new agent destination to connect with a different OMi server, and then repeat this test.
         - If the repeated test succeeds, the problem is with the first OMi server. Consult the OMi documentation for troubleshooting information.

Events are not acknowledged

1. Check if the `ombacksync` service is running. If not, restart the service with the following command:

   `ovc –restart ombacksync`
2. Restart the OMi services if required.
3. Check the `system.txt` log file for error logs if any.

CIs are not resolved

1. Verify that RTSM is configured correctly and that the integration is successful.
2. Check the frequency of the integration. A newly added element in SOM might not show up immediately in RTSM if the time difference is high as topo sync is based on a pull mechanism.

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 HPE Operations Manager i Integration 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!