Hewlett Packard
Enterprise

HPE SiteScope

Software Version: 11.33

Integration with Application Performance Management (APM) and Operations Manager i (OMi)

Document Release Date: December 2016
Software Release Date: December 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

© Copyright 2005 - 2016 Hewlett Packard Enterprise Development LP

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

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

iPod is a trademark of Apple Computer, Inc.

Java is a registered trademark of Oracle and/or its affiliates.

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

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

Support

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

This website 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 website 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 HPE Passport user and sign in. Many also require a support contract. To register for an HPE 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

HPE Software Integrations and Solutions

Visit the Integrations and Solutions Catalog at **https://softwaresupport.hpe.com/km/KM01702731** to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

Contents

Chapter 1: Overview

This guide describes benefits, integration prerequisites, details, features, and troubleshooting for the integration of SiteScope with Application Performance Management (APM) and Operations Manager i (OMi).

As part of APM simplification and footprint reduction implemented in the APM 9.30 release, embedded OMi is removed from APM. The following changes are the result of the APM-OMi separation:

- Event management module is no longer available in APM. This means that SiteScope cannot send events to APM.

- APM and OMi have two separate Run-time Service Models (RTSMs). SiteScope cannot connect simultaneously to both the RTSMs to report topology.

The following scenarios depict the integrations that are supported between SiteScope, APM and OMi and are detailed in the topics in this guide.

Chapter 2: SiteScope Integration with HPE Operations Manager i (OMi)

In this integration scenario SiteScope sends topology and events to OMi. The features available with this integration scenario are:

- Event management for SiteScope alerts and events
- Event-driven Service Health
- Topology-Based Event Correlation (TBEC)
- Performance Dashboard (PD)
- Monitoring Automation (MA)

This section contains details of the benefits, prerequisites, best practices, and troubleshooting for integrating SiteScope with OMi. This section covers the following topics:

Integration Benefits

- Events: Ability to configure and generate events directly from SiteScope, reuse existing alerts as events, and manage and use SiteScope events in OMi. For details, see Integrating SiteScope with HP Operations Manager Products. You can check the HP Software Integrations site for the latest version of this guide.

- Runtime Service Model (RTSM): SiteScope can discover and report topology on monitored systems to OMi's RTSM. You can then manage and work with these discovered configuration items (CIs) in views that provide a subset of the components in which your business functions. For details, see Integrate SiteScope Data with APM's Configuration Items.

- Service Health: Health indicators assigned to SiteScope monitor data provide a detailed view of the health of a configuration item (CI) when SiteScope reports events. For details on how to configure indicators in monitors, see the SiteScope Help.

- Reports: Ability to create and view reports of SiteScope monitor metrics in OMi. For details on Performance Dashboard in Operations Management, see the OMi User Guide.

- Downtime: Centralized management enables configuring downtime for your IT infrastructure from one place in OMi. For details, see CI Downtime.

- Monitoring Automation (MA): Automates the configuration of monitoring for infrastructure and composite applications.

Integration Prerequisites

The following are required to enable the integration.

SiteScope Integration	Prerequisites	Reports
Operations Manager i (OMi)	HP Operations Agent must be installed on the SiteScope server.	• Metrics • Events
APM		Topology

Integration Options and Details

The metrics and event data collected by SiteScope monitors is used in OMi. Choose the integration option according to the type of data to be collected, and the monitoring environment that exists in your organization.

Application	What to use	SiteScope Integration to use	References
Service Health	Events (metrics status change) (required)	HP Operations Manager	The section on sending events in Integrating SiteScope with HP Operations Manager Products. Note: You can check the HPE Software Integrations site for the latest version of this guide.
	Topology (required)	APM	How to Configure Topology Reporting Note: To report topology, make sure the Report monitor and related CI topology check box is selected in APM Integration Data and Topology Settings for each monitor instance.
Event Management	Events (required) Status change: • Use if you want to manage raw (low-level) events. • These events affect HIs and KPIs. Alerts: • Use if you want to manage alerts as events. • By default, these events do not affect HIs and KPIs.	HP Operations Manager	The section on sending events in Integrating SiteScope with HP Operations Manager Products.

Application	What to use	SiteScope Integration to use	References
	Topology (recommended) Recommended for: • Drill downs from events to views and related CIs. • Topology-Based Event Correlation (TBEC) rules.	APM	How to Configure Topology Reporting Note: To report topology, make sure the Report monitor and related CI topology check box is selected in APM Integration Data and Topology Settings for each monitor instance.
Performance Graphing	Metrics (required)	HP Operations Manager	The section on reporting metrics in Integrating SiteScope with HP Operations Manager Products.
	Topology (required)	APM	How to Configure Topology Reporting Note: To report topology, make sure the Report monitor and related CI topology check box is selected in APM Integration Data and Topology Settings for each monitor instance.

Recommendations

The following are recommendations for integrating SiteScope with OMi or Operations Manager (HPOM):

- It is recommended to integrate SiteScope directly with OMi rather than with HPOM.
- If your deployment prevents you from integrating directly with OMi, or you want to get event preprocessing in HPOM before forwarding SiteScope events to OMi, you should integrate SiteScope with HPOM.

Note: Even if you are integrating SiteScope with HPOM, it is recommended to integrate SiteScope directly with OMi and to configure SiteScope to report topology to OMi. Reporting topology provides topology based event correlation rules and drill down from events to views and related CIs.

Upgrade SiteScope-BSM 9.2x Integration to SiteScope-OMi 10.x Integration

Prerequisites:
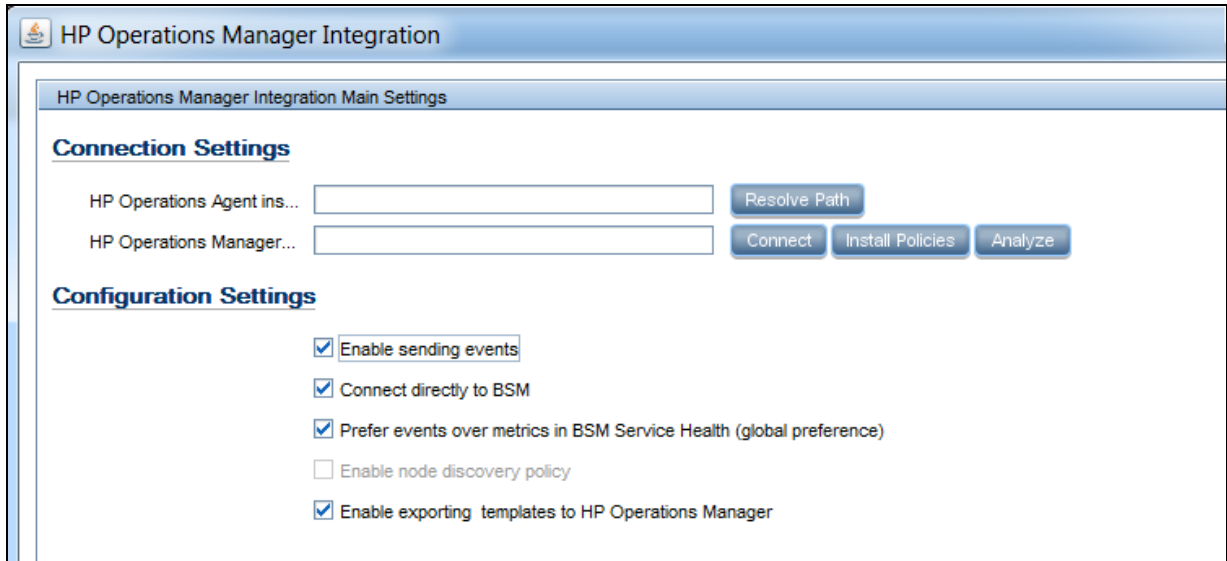
- Installation of OMi version 10.x on a new server.
- SiteScope installation with SiteScope-BSM 9.2x and SiteScope-OM integrations.

Steps to Upgrade the Integration

1. Log on to SiteScope with your credentials.

2. Go to **Preferences** > **Integration Preferences**.

3. Click the edit icon ✎ . In the Integration Preference Type page, select the existing BSM Integration and click **Edit Integration**.

4. Click the **BSM Preferences Available Operations** tab and click **Reset**.

5. Click **OK**. The BSM integration is deleted.

6. On the OMi server, go to the Connected Servers tab and add the SiteScope server details.

   > Note: On the SiteScope server, verify if the new BSM integration is updated with the OMi host details.

7. Click the edit icon ✎ . In the Integration Preferences page, select the current OMi integration and delete it. Create a new OMi integration pointing to the new OMi server. See Appendix A for more information. OR
   Redirect the current integration to the new OMi installation. See Appendix B for more information.

8. In the new/updated integration select the following check boxes under HP Operations Manager Integration Main Settings page:

   - Enable sending events

   - Connect directly to BSM

   - Prefer events over metrics in BSM Service Health (global preference)

> **Note**: The other check boxes and configurations are not relevant to this scenario.

9. Perform this step for all the existing monitors in SiteScope.

   a. From the monitors context, go to **Monitor** > **Properties** > **HP Integration Settings**

   b. Select the option **Disable reporting metrics to BSM** from the drop-down box under the **BSM Integration Data and Topology Settings** tab.

   c. Click the **HP Operations Manager Integration Settings** tab and select the **Send events** check box.

   d. Click the **BSM Service Health Preferences** and set the **BSM Service Health affected by:** to events.

   e. Click **Save**.

> Note: In case you need to adjust a large number of monitors, you can perform Step 9 using Global Search and Replace (GSAR). Also, if you have created these monitors from templates, you can adjust the templates and publish changes to the monitors. For more information on GSAR and publishing templates, see the Using SiteScope Guide.

Troubleshooting

For troubleshooting information specific to this scenario, refer to the following.

- For topology reporting issues, see "Topology Issues" on page 28.

- For Operations Manager Event Integration issues, see "Operations Manager Event Integration Issues" on page 31.

- For CI downtime issues, see "CI Downtime Issues" on page 39.

Chapter 3: SiteScope Integration with Application Performance Management (APM)

In this integration scenario SiteScope sends topology and metrics to APM. The features available with this integration are:

• Metrics driven Service Health and Application Health

• Service Level Management

• System Availability Management (SAM) reports

• System Availability Management administration (including HI mapping)

This section includes:

Integration Benefits

- Runtime Service Model (RTSM): SiteScope can discover and report topology on monitored systems to APM's RTSM. You can then manage and work with these discovered configuration items (CIs) in views that provide a subset of the components in which your business functions. For details, see Integrate SiteScope Data with APM's Configuration Items.

- Service Health and Service Level Management: Health indicators assigned to SiteScope monitor data provide a detailed view of the health of a configuration item (CI) when SiteScope reports metrics.
  - For details on managing indicators in the centralized Indicator Assignments repository in SAM Administration, see Indicator Assignment Settings in the APM Application Administration Guide in the APM Help.

  - For details on mapping metrics to indicators in SiteScope, see Assigning SiteScope Metrics to Indicators.

- System Availability Management administration: Enables viewing and managing multiple SiteScope instances from within System Availability Management administration. For details, see SAM Administration Overview in the APM Application Administration Guide in the APM Help.

- Reports: Ability to create and view reports of SiteScope monitor metrics in System Availability Management. For details on System Availability Management reports, see System Availability Management Reports in the APM User Guide in the APM Help.

- Service Health Analyzer (SHA): SHA analyzes metrics, calculates the dynamic baseline to detect if each metric behaves normally or not, and automatically correlates related metrics to a single meaningful event.

- Downtime: Centralized management enables configuring downtime for your IT infrastructure from one place in APM. For details, see CI Downtime.

Integration Prerequisites

The following are required to enable the integration.

SiteScope Integration	Prerequisites	Reports
APM	System Availability Management license. For details, see SAM Administration Overview in the APM Application Administration Guide in the APM Help. **Note**: If you are using the SiteScope points-based license, you must upgrade to the SAM points license. If you are using the SiteScope OSi-based license, the Premium and Ultimate edition include the SAM license.	• Metrics • Topology

Integration Options and Details

The metrics collected by SiteScope monitors are used in APM applications. Choose the integration option according to the type of data to be collected, and the monitoring environment that exists in your organization.

Application	What to Use	SiteScope Integration to Use	References
Service Health	Metrics (required) • Displays metrics values in Service Health tooltips. • You can create customized calculation rules. For details, see Business Rule Repository Overview in the APM Application Administration Guide in the APM Help.	APM	How to Configure SiteScope to Communicate with APM in the Using SiteScope Guide
	Topology (required)	APM	How to Configure Topology Reporting Note: To report topology, make sure the Report monitor and related CI topology check box is selected in APM Integration Data and Topology Settings for each monitor instance.
Service Level Management	Metrics (required)	APM	How to Configure SiteScope to Communicate with APM in the Using SiteScope Guide
	Topology (required)	APM	How to Configure Topology Reporting in the Using SiteScope Guide Note: To report topology, make sure the Report monitor and related CI topology check box is selected in APM Integration Data and Topology Settings for each monitor instance.
System Availability Management Reports	Metrics (required)	APM	How to Configure SiteScope to Communicate with APM in the Using SiteScope Guide

Upgrade SiteScope-BSM 9.2x Integration to SiteScope-APM 9.30 Integration

Prerequisites

- Installation of APM version 9.30 on a new server.

- SiteScope installation with SiteScope-BSM 9.2x integration.

- For SiteScope integration with BSM 9.26, you must deploy the BSM_926_package.zip package available with SiteScope 11.33. See the 11.33 Release Notes for location of the package and the Read Me file instructions. Restart SiteScope after you have deployed the package.

- After you upgrade to APM 9.30, you must deploy the APM_930_package.zip available with SiteScope 11.33. See the 11.33 Release Notes for location of the package and the Read Me file instructions. Restart SiteScope after you have deployed the package.

Steps to Upgrade the Integration

1. Log on to SiteScope with your credentials.

2. Perform this step for all the existing monitors in SiteScope.

    a. From the monitors context, select a monitor and click **Properties** > **HP Integration Settings**

    b. Click the **HP Operations Manager Integration Settings** tab and clear the **Send events** check box.

    c. Click the **BSM Service Health Preferences** tab and set the **BSM Service Health affected by:** to **Metrics**.

    d. Click **Save**.

    > Note: In case you need to adjust a large number of monitors, you can perform Step 2 using Global Search and Replace (GSAR). Also, if you have created these monitors from templates, you can adjust the templates and publish changes to the monitors. For more information on GSAR and publishing templates, see the Using SiteScope Guide.

3. Go to **Preferences** > **Integration Preferences**.

4. Select the existing OMi Integration and click the delete icon ❌. The OMi integration is deleted.

5. Select the BSM Integration and redirect the integration to the system where APM 9.30 is installed. Enter the IP address and credentials of the system where APM 9.30 is installed and re-synchronize the configuration.

SiteScope Post-upgrade Procedure

After performing a staging upgrade, you need to configure SiteScope to communicate with the new APM Gateway Servers.

Integrate SiteScope and APM 9.30

To integrate SiteScope and APM 9.30, after upgrading to APM 9.30, perform the following procedure.

On the APM 9.30 server:

1. Access the UCMDB JMX server (https://<full APM data processing server name>:21212/jmxconsole/ HtmlAdaptor?action=inspectMBean&name=UCMDB:service=Packaging Services).

2. From the Operations index, click undeployPackages.

3. In the packageNames Value field, type sitescope.zip.

4. Click **Invoke**.

5. From the Operations index, click deployPackages.

6. In the packageNames Value field, type sitescope.zip.

7. Click **Invoke.**

   On the SiteScope server:

8. Stop SiteScope.

9. Copy the jar files and SiSAPM930PostUpgradeUtil files from …/BSM/9.30/content/HPE_APM_9.30_
   SiS_Upgrade and save them in <SiteScope root dir>/bin.

10. For SiteScope installed on Windows, run the SiSAPM930PostUpgradeUtil.bat file.

    For SiteScope installed on Linux, run the SiSAPM930PostUpgradeUtil.sh file.

Change the Gateway Server to which SiteScope sends data

After performing a APM staging upgrade, you need to configure SiteScope to communicate with the new APM
Gateway Servers. To do so, perform one of the following:

- In SiteScope's BSM Integration Preferences, enter the new Gateway Server name or IP address in the
  Business Service Management machine name/IP address box. For user interface details, see BSM
  Integration Preferences Dialog Box in the Using SiteScope Guide in the SiteScope Help.

- In SAM Administration, update the SiteScope settings with the new Gateway Server name in Distributed
  Settings. For user interface details, see New/Edit SiteScope Page in the APM Application Administration
  Guide in the APM Help.

> **Note**: This can only be used for changing the Gateway Server for a SiteScope that is already registered
> with a given APM installation. It cannot be used to add a new SiteScope, or to connect a SiteScope to a
> different APM system.

Troubleshooting

For troubleshooting information specific to this scenario, refer to the following.

- For topology reporting issues, see "Topology Issues" on page 28.
- For APM Metrics integration issues, see "APM Metrics Integration Issues" on page 37.
- For CI downtime issues, see "CI Downtime Issues" on page 39.

Chapter 4: SiteScope Integration with APM and OMi

In this type of integration, SiteScope sends topology and metrics to APM. APM syncs topology and CI and HI statuses with OMi.
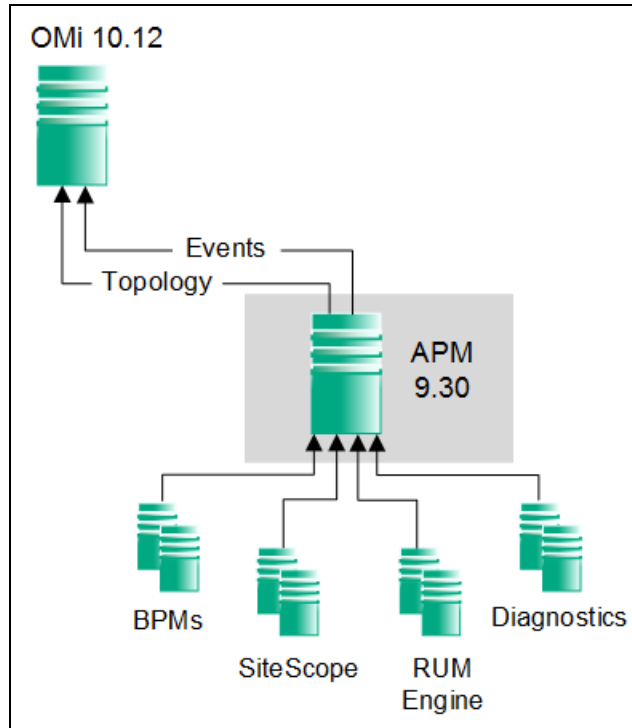
For more information on SiteScope integration with APM, see "SiteScope Integration with Application Performance Management (APM)" on page 15.

For more information on SiteScope integration with OMi, see the OMi Integrations Guide.

The main features of this integration include:

- Metrics-driven Service Health (in APM)
- Event-driven Service Health (in OMi) through topology sync (except for SiteScope groups and monitors) and HI status sync
- Service Level Management (in APM)
- System Availability Management (SAM) reports (in APM)
- System Availability Management administration (including HI mapping) (in APM)

Upgrade the Integration

To upgrade the integration for APM 9.30, follow the upgrade steps in the topic "Upgrade SiteScope-BSM 9.2x Integration to SiteScope-APM 9.30 Integration" on page 19.

Chapter 5: SiteScope Integration with APM and OMi with Event-Alert Configuration

In this type of integration, SiteScope is configured to send topology and metrics to APM and events to OMi. This scenario enables working with alerts in the event console of OMi.
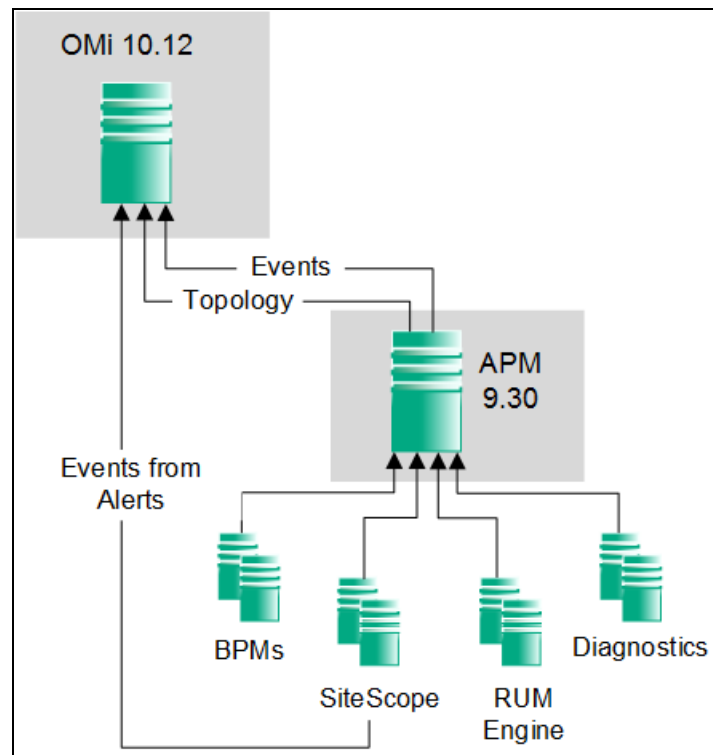
Note: This integration does NOT support metrics status change events.
Some possible workarounds for this limitation include:

- Connecting some of your SiteScope instances directly to OMi.(See chapter 2)
- If your SiteScope instances are configured to report events and metrics to BSM 9.2x, consider splitting each of them into two instances: one connected to an APM system and reporting metrics (see chapter 3) and another to OMi, reporting events (see chapter 2). For more information on how to export SiteScope configuration, see the SiteScope Deployment Guide.
- Using APM CI status alerts to send events to OMi.

This scenario is equivalent to the SiteScope integration with APM and OMi in terms of integration options and details. However, it has additional benefits because of the direct channel of sending alert events to OMi.

For more information, see APM and OMi integration.

Upgrade from BSM 9.2x to APM 9.30
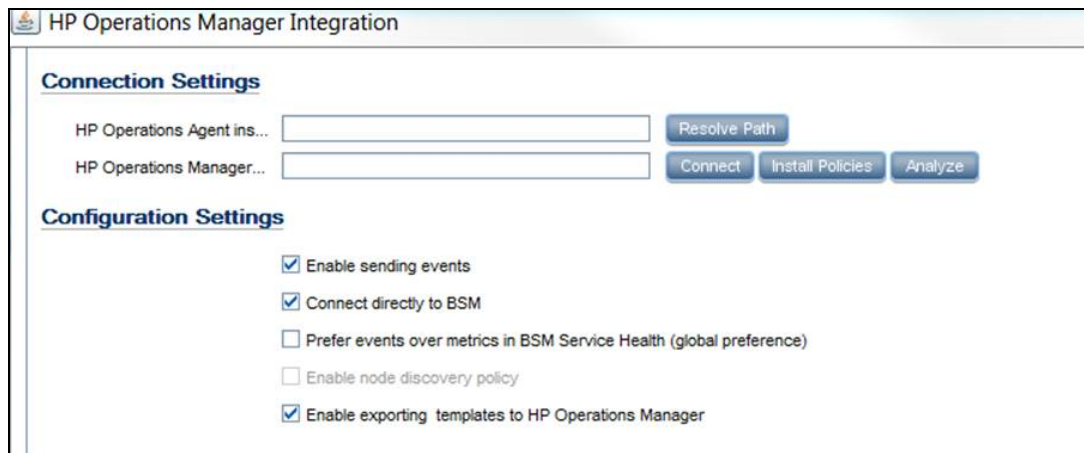
Prerequisites

- Installation of APM version 9.30 on a new server.

- Installation of OMi 10.12 on a new server.

- SiteScope installation with SiteScope-BSM 9.2x integration.

Steps to Upgrade the Integration

1. Log on to SiteScope.

2. Select **Preferences** > **Integration Preferences**. The list of integrations that are configured are displayed on the right.

3. Select the BSM integration and redirect the Business Service Management machine and credentials to point to the new APM 9.30 machine. For user interface details, see BSM Integration Preferences Dialog Box in the Using SiteScope Guide in the SiteScope Help.

4. Delete the current OMi integration and create a new one (HP Operations Manager Integration), pointing to the new OMi server or redirect the current one to the new OMi machine. For details on creating, deleting or redirecting the integration, see Appendix A and B.

5. In this new/updated integration make sure that the you have the following check boxes enabled/disabled as follows:

   - Enable sending events - Enabled

   - Connect directly to BSM - Enabled

   - Prefer events over metrics - Disabled

   Note: The other check boxes and configurations are not relevant to this scenario.

In the HP Operations manager metrics integration tab, the check box Enable metrics reporting for new monitors must be enabled.

Note: On Windows, the events are not reported to OMi due to certificate exchange issue between OMi and OA. See the "Unable to do event integration from OMi 10.12 with SiteScope 11.33 on Windows environment" on page 35 for troubleshooting.

6. Go to **Monitor** > **Properties** > **HP Integration Settings**, ensure the following settings for all the monitors:

   - Under HP Operations Manager Integration Settings, Send events check box must be disabled.

   - Under BSM Service Health Preferences, set BSM Service Health affected by as Metrics.

   Note: In case you need to adjust a large number of monitors, you can perform Step 6 using Global Search and Replace (GSAR). Also, if you have created these monitors from templates, you can adjust the templates and publish changes to the monitors. For more information on GSAR and publishing templates, see the Using SiteScope Guide.

7. When creating a new Alert make sure the alert is configured to send events to OMi.

8. Save the settings to complete the upgrade.

Chapter 6: Troubleshooting SiteScope Integration Issues

This topic describes troubleshooting when using and configuring the integration of SiteScope with APM and HPOM applications.

This section includes:

- "Topology Issues" on the next page
- "Operations Manager Event Integration Issues" on page 31
- "APM Metrics Integration Issues" on page 37
- "CI Downtime Issues" on page 39

Topology Issues

This section describes troubleshooting and limitations when SiteScope is integrated with APM/OMi and enabled to report monitor and related CI topology to APM/OMi.

This section includes:

- "Opening Logs in SiteScope in Debug Mode" below
- "Opening Logs in APM/OMi in Debug Mode" below
- "No Topology Reported" on the next page
- "RTSM Troubleshooting" on the next page
- "Where to Configure the Port to Which Data Flow Reports" on page 30
- "Error "Failed Running script :filesystem_topology.py" in bac_integration.log " on page 30

Opening Logs in SiteScope in Debug Mode

The following log files in SiteScope contain information relating to the APM/OMi integration.

- **SiteScope\logs\bac_integration\bac_integration.log**
- **SiteScope\logs\bac_integration\discovery.log**
- **SiteScope\logs\bac_integration\probeGW-taskResults.log**
- **SiteScope\logs\bac_integration\topology_queue_consumer.log**

Open the relevant log files in debug mode using the instructions listed below.

To open logs in SiteScope in debug mode:

1. In the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder, open the **bac_integration.properties** file and change the debug level to the appenders listed in **attachment1.txt** (attached to this PDF). To view the attachment, select **View > Navigation Panels > Attachments**, and select **attachment1.txt**.

2. Add the appenders listed in **attachment2.txt** (attached to this PDF) to the **probeGW-taskResults.log** file. To view the attachment, select **View > Navigation Panels > Attachments**, and select **attachment2.txt**.

3. Add the appender listed in **attachment3.txt** (attached to this PDF) to the **log topology_queue_consumer.log** file. To view the attachment, select **View > Navigation Panels > Attachments**, and select **attachment3.txt**.

Opening Logs in APM/OMi in Debug Mode

The following log files in APM/OMi contain information relating to the integration with SiteScope. Open the relevant log files in debug mode using the instructions listed below.

- **<APM/OMi root directory>\log\odb\odb\mam.autodiscovery.log**
- **<APM/OMi root directory>\log\odb\odb\cmdb.reconciliation.log**
- **<APM/OMi root directory>\log\odb\odb\cmdb.reconciliation.datain.ignored.log**
- **<APM/OMi root directory>\log\odb\odb\discoveryServlet.log**

To open logs in APM/OMi (on the Data Processing server machine in a distributed environment) in debug mode:

Change RTSM debug level in APM/OMi:

- **<APM/OMi root directory>\odb\conf\log\reconciliation.properties**
- **<APM/OMi root directory>\odb\conf\log\mam.properties**
- **<APM/OMi root directory>\odb\conf\log\mam.web.properties**

No Topology Reported

1. Open all SiteScope and APM/OMi logs in debug mode. For details, see "Opening Logs in SiteScope in Debug Mode" on the previous page and "Opening Logs in APM/OMi in Debug Mode" on the previous page.

2. Check if there are **\bin** files stuck in the **<SiteScope root directory>\cache\topologyresultsData\merged** directory.

3. Check for errors in the logs in the following order:

   - **bac_integration.log**. Topology is not sent due to general errors or syntax problems in the scripts.

   - **discovery.log**. Shows the complete picture of the topology reported from SiteScope to APM/OMi using Data Flow Management.

   - **topology_queue_consumer.log**. Shows the topology SiteScope is trying to send to the Data Flow probe. (It does not mean that this is the topology that the probe client sends to the server). This log reflects what SiteScope script intended to report to Data Flow Management.

   - **probeGW-taskResults.log**. Shows the topology Data Flow Management sends to the RTSM server.

   - **mam.autodiscovery.log**. Shows the steps Data Flow Management probe is doing on the topology reporting from SiteScope to Data Flow Management (bulk creation) and the interaction with the RTSM server.

   - **cmdb.reconciliation.log**. If the issues are on the RTSM server-side, it is most likely a reconciliation issue.

   - **cmdb.reconciliation.datain.ignored.log**. Shows topology that is ignored by the RTSM server and not reported.

   - **discoveryServlet.log**. Shows data from the connection opened by SiteScope and the reply sent to SiteScope. Check for exceptions in this log when there are issues with topology not being sent to APM/OMi. This log exists also on BAC 8.0.

4. It is recommended to open logs that are in XML format using an XML editor.

RTSM Troubleshooting

To get the properties of a CI reported to a Data Flow database with JMX:

1. Open http://<APM/OMi_machine>:21212/jmx-console/ in a Web browser.
2. Click **UCMDB:service= Model Services**.
3. Invoke method: retrieveObjectProperties.

Where to Configure the Port to Which Data Flow Reports

The server settings are initialized in APM in **Admin > System Availability Management > Topology Settings** from the **Topology receiver port** or **Topology receiver SSL port** boxes.

Error "Failed Running script :filesystem_topology.py" in bac_integration.log

This is caused by the download mechanism which fails to rename the **filesystem_topology.py.11** file to **filesystem_topology.py** after it is downloaded from APM/OMi to SiteScope.

To fix this issue, reload the scripts from APM/OMi:

1. Stop the SiteScope service.

2. Delete the contents of the **<SiteScope root directory>\discovery\hsqldb** folder.

3. Start the SiteScope service. This should reload the scripts from APM/OMi and rename them.

Operations Manager Event Integration Issues

This section describes troubleshooting when using the Operations Manager integration to send SiteScope events directly to the OMi server.

This section includes:

- "Integration Setup Problems" below
- "Unable to send events" on page 33
- "Certificate Requests Do Not Reach the Operations Management Server" on page 35

> **Tip:** When referring to the integration log file, you can open it from the SiteScope user interface (**Server Statistics > Log files > HPSiteScopeOperationsManagerIntegration.log**).

Integration Setup Problems

Symptom:

Any problem that occurs while trying to configure the Operations Manager Integration (between connecting the agent to the HPOM/OMi server and sending a test message).

Troubleshooting:

1. In SiteScope, open the HP Operations Manager Integration dialog box panel (**Preferences > Integration Preferences > HP Operations Manager Integration**).

2. In the HP Operations Manager Integration Main Settings pane, check the **HP Operations agent installation path**.

    a. Click the **Resolve Path** button.

    b. Make sure the agent is installed on the path you see in this field.

        ○ If the agent is installed on a different path, update the path accordingly.

        ○ If you do not see the path is resolved (probably the agent is not installed properly), try restarting the server machine. If it does not help, remove the Operations Agent and then install it again (it is also recommended to restart the server).

    c. Make sure your HPOM management server or OMi Gateway host name is typed correctly in the host field.

3. Click the **Analyze** button.

    a. If the command outputs are empty, there is a problem with the agent installation. Remove the Operations Agent and then install it again (it is also recommended to restart the server).

    b. Check that the `bbcutil` command output returns **status=eServiceOK**. If it does not, there is a connectivity problem to your HPOM management server.

    c. Check the `opcagt -status` command output. You should see a few processes running (some can be in Aborted state—this is fine at this stage). If they are not running, manually start the agent by running command line: `opcagt -start`, or restart your server machine.

4. Make sure your HPOM management server is up and running.

5. If you are working with OMi, check your Gateway and Data Processing Server:

a. Run command line `ovc -status` to check the server. Make sure all processes are running (in particular, the "Certificate Broker"). If they do not start, run command line `ovc -start`

b. Check the connection from SiteScope to the Gateway Server by running the command: `ping https://<OMi Gateway Server>/com.hp.ov.opc.msgr`. If this fails, restart the WDE process on the Gateway Server.

6. If you are working with a distributed OMi environment, follow the procedures for initiating trust between your Gateway and Data Processing Server, and forwarding the certificate request from the Gateway to the Data Processing Server.

   For details, see the section on sending events to OMi or HPOM in Integrating SiteScope with HP Operations Manager Products in the SiteScope Help. You can check the HPE Software Integrations site for the latest version of this guide.

7. Click the **Connect** button, and make sure the command output returns: `opcactivate Info: Successfully activated OVO agent.`

   If it does not work, contact your HPOM administrator for assistance.

   > **Note:** If there is a large time difference (more than 24 hours) between the certificate server and the HP Operations agent, you might encounter the following error when running agent commands such as `ovc – status`, `ovc –start`, or `opcagt -status`:
   >
   > `(ctrl-21) Communication error when executing 'Status' method.`
   > `(sec.core-113) SSL certificate verification error (The presented peer certificate is not yet valid.)`
   >
   > This problem occurs because certificates are only valid in the specified time period, and usually solves itself (after a day) when the certificate becomes valid. The time is specified in Coordinated Universal Time (UTC), independent from time zones, and certificates are issued to be valid from 24 hours in the past.

8. Accept the certificate request.

   - When connecting to an OMi server, follow the step for accepting the agent connection request in Integrating SiteScope with HP Operations Manager Products in the SiteScope Help. You can check the HPE Software Integrations site for the latest version of this guide.

   - When connecting to an HPOM management server, consult your HPOM administrator. If you do not see the certificate request, contact your HPOM administrator.

9. Click the **Analyze** button.

   a. Make sure the `ovcert -check` is ok, and it ends with "Check Succeeded".

   b. Make sure `ovcert -list` lists some certificates.

   c. If there are problems with the command outputs:

      ○ Contact your HPOM administrator, or

      ○ Start the integration process troubleshooting from the connect phase, or even reinstall the agent.

10. Click the **Install Policies** button.

    a. If you get an error here or this process is stuck with "please wait" and:

       ○ You recently reinstalled the agent and did not restart yet, restart your server.

       ○ Otherwise, there is a problem with the agent (and the additional policy activation tool package) installation. Reinstall on a clean image.

  b. Click the **Analyze** button, or check the output of the Install Policies for the list of policies. Make sure you see the following list with all enabled:

    ○ HP_SiteScope_to_Operations_Manager_Integration_by_Log_File

    ○ HP_SiteScope_to_Operations_Manager_Integration

    ○ SiteScope_Hosts_Discovery

11. In the **Test Message** box, type a message and click **Send test message**.

  a. Check your HPOM Event Console or Operations Management Event Browser.

  b. If you do not see the message in the Event Console/Browser:

    ○ Run command line: `opcmsg a=a o=o msg_t=xxx`

    ○ If the command is not available, something went wrong with the process so far (either the certificate or the policies does not work). Try to install the policies again, and if the same problem occurs contact HPE Software Support.

    ○ If the command is executed but you still do not see the message in the Event Console, contact your HPOM administrator for support.

Unable to send events

Symptom 1:

Sending a test event from the HP Operations Manager Integration dialog box does not reach the HPOM Event Console/Operations Management Event Browser.

Troubleshooting:

1. In the HP Operations Manager Integration dialog box, enter a test message in the **Test message** box, and click **Send test message**. If the test message is not displayed in the Event Console, follow all the steps in "Integration Setup Problems" on page 31, and then try again.

2. Click the **Analyze** button, and make sure all commands are successful (in particular, see the list of policies installed). For details, see "Operations Manager Event Integration Issues" on page 31.

3. Click the **Send Test Event** button.

4. In the **<SiteScope root directory>\logs** directory, check the events log file, **HPSiteScopeOperationsManagerIntegration.log**. Verify the event entry in the log file. If you do not see it, contact HPE Software Support.

5. If you still do not see the event in the HPOM Event Console/Operations Management Event Browser, check you are viewing the correct node in HPOM, or are not filtering out anything in the Operations Management Event Browser. If you still do not see the event, contact HPE Software Support.

6. Open the **<SiteScope root directory>\tools\OMIntegration\Policies\F516CEC3-3AD4-4627-9CFD-BB155B894349_data** file, and check that the path specified for **HPSiteScopeOperationsManagerIntegration.log** is correct (it might use an environment variable). If you make any changes here, you must install the policies again.

7. Check if the agent received the event and sent it to HPOM/Operations Management:

 Make sure that the agent knows the location of the log file.

 On Windows: Check if %SITESCOPE_HOME% variable is defined. If it is not defined:

 a. Define %SITESCOPE_HOME%.

 b. Remove the policy:

```
ovpolicy -remove -polname HP_SiteScope_to_Operations_Manager_Integration_by_Log_
File
```

   c. Reinstall the policies from the SiteScope user interface.

   On UNIX: Check if the log file policy contains the location of the log:

   a. Open the policy:

   "`opt/HP/SiteScope/tools/OMIntegration/Policies/F516CEC3-3AD4-4627-9CFD-BB155B894349_data`"

   b. Check `LOGPATH` is set to "`opt/HP/SiteScope logs/HPSiteScopeOperationsManagerIntegration.log`"

    If it is not, change the path and reinstall the policy (see the Windows steps above).

8. If you still do not see the event in the HPOM Event Console/Operations Management Event Browser, check:

   - You are viewing the correct node (in HPOM).

   - You are not filtering out anything (in the Operations Management Event Browser).

   Otherwise contact support.

Symptom 2:

The metric status change or alert event is not displayed in the HPOM Event Console/Operations Management Event Browser.

Troubleshooting:

1. Check if the test event is displayed in the Event Console/Browser. If it is not displayed, follow the guidelines for Symptom 1 in "Unable to send events" on the previous page.

2. Check that event integration is enabled in the monitor or alert configuration settings. Change the monitor metric status, or trigger an alert. In the **<SiteScope root directory>\logs** directory, check the events log file, **HPSiteScopeOperationsManagerIntegration.log**.

3. If you do not see the event entry in the log file, check you enabled event integration correctly in the monitor or alert you are running. For details, see Integrating SiteScope with HP Operations Manager Products in the SiteScope Help or check the HPE Software Integrations site for the latest version of this guide.

   If it is still not in the log file, contact HPE Software Support.

4. If you see the event entry in the log file, but not in the Event Console/Browser:

   a. Check that no filter is set in the Event Browser.

   b. If it is a newly-created monitor, and you are filtering the related CI in Operations Management, it is possible that the CI topology is not reported yet. Try again in a few minutes.

   c. In HPOM legacy, make sure the event target node exists on your console.

   d. Contact HPE Software Support.

Symptom 3:

You see the metric or alert event in the Operations Management Event Browser, but it has no related CI or HI, or Indicator state or severity.

Troubleshooting:

1. Check the event attribute values in the **HPSiteScopeOperationsManagerIntegration.log** file located in the **<SiteScope root directory>\logs** directory. Look for the HI (ETI) and CI hint. They should look like

this: `CPULoad:High:80` and `SiteScope:3:123456` respectively.

   a. To know the attribute order in this tab separated values line, you can send a test event before this event and compare the lines. The test event writes the name of each attribute in its order.

   b. If the CI Hint or HI hint are unknown, empty, or look different than the example, there is a problem with the SiteScope configuration.

      ○ Check that the SiteScope is registered to OMi.

      ○ Check that the monitor thresholds have indicator states assigned to them, or that your alert has some ETI and ETI state set.

      ○ Check the preference setting for reporting SiteScope data in the monitor configuration is set to **Events** (in **HP Integration Settings > BSM Service Health Preferences**).

2. If everything looks fine in the log file in SiteScope, open the event in the Operations Management Event Browser.

   a. In the **General** tab, check the **related CI** attribute. If you do not see the related CI, select the **Resolver** tab and check the **Status** field.

      ○ Check if there is information about the CI resolution failure.

      ○ Check that the monitor topology is available in the OMi server (you can check this in the System Hardware or System Monitors views).

> **Note:** If this is a newly-created monitor, it will take few minutes for the topology to arrive and the event to be assigned with a related CI.

   b. In the **General** tab, if you see the **related CI** but **Event Type Indicator** is empty:

      ○ Select the **Resolver** tab and check the ETI Hint attribute value sent by SiteScope. If it is empty or unknown, check your SiteScope configuration.

      ○ If the value exists but does not show up in **Event Type Indicator** in the General tab, there was a problem when applying the indicator to the CI. Check Service Health or Operations Management for support.

Certificate Requests Do Not Reach the Operations Management Server

Troubleshooting: Run the following command on the Operations Manager server:

`"ovconfchg -ns sec.cm.server -set IsIPV6Enabled FALSE"`

Unable to do event integration from OMi 10.12 with SiteScope 11.33 on Windows environment

Description: During the SiteScope integration with OMi, the certificate exchange between OA and OMi is not successful. Therefore, SiteScope events are not reported to OMi.

Troubleshooting:

Perform the following steps to exchange certificates manually:

1. On the SiteScope server, go to the command prompt and type the command "ovcoreid to generate certificates.

2. On the OMi server, run the following command:
ovcm –issue –file node.cert -name <*SiteScope_server_FQDN* > -pass passwd -coreid <*ovcoreid*>

where *ovcoreid* is the result of Step 1

Example

ovcm –issue –file node.cert -name btpvm1003.hpeswlab.net -pass passwd -coreid cab78312-fc1a-758e-0e5d-8c563f158fc5

3. Copy node.cert created in step 2 to the SiteScope server.

4. Run the following command on the SiteScope server:
   `ovcert –importcert -file <the path of node.cert> -pass passwd`

5. On the SiteScope server, run the command `overt -list` to confirm that certificates are listed.

6. Install the policies and check if events are being sent.

APM Metrics Integration Issues

This section describes troubleshooting when working with the APM metrics integration if CI statuses are not displayed in Service Health.

This section includes the following troubleshooting steps:

- "Check HI/KPI assignment" below
- "Check that SiteScope data is not ignored by APM" below
- "Check CI resolution" on the next page
- "If there are no HIs on the relevant CI (in case the problem is with the monitored CI and not the monitor/measurement)" on the next page
- "If there are no KPIs on the relevant CI (in case the problem is with the monitored CI and not the monitor/measurement)" on the next page
- "If there are no HIs/KPIs and everything seemed to work in the previous two steps" on the next page

1. **Check HI/KPI assignment**

   If CI statuses are not displayed in Service Health, check if HIs and KPIs are assigned to the relevant CI:

   a. In APM, select **Admin > Service Health > CI indicators**, expand the **Monitors** folder, and select one of the following views: System Monitors, System Hardware Monitoring, or System Software Monitoring.

   b. In the view you have selected, check if there are HIs and KPIs assigned to the relevant CI, as follows:

      ○ System Monitors view: SiteScope Monitor or SiteScope Measurement CI

      ○ System Hardware Monitoring view: Node or Computer CI

      ○ System Software Monitoring view: Running Software CI

2. **Check that SiteScope data is not ignored by APM**

   If HIs and KPIs are assigned to the relevant CI, check if SiteScope sends data and that the data is not ignored by APM.

   a. Run the relevant monitor in SiteScope.

   b. On the APM machine, open the **wdeIgnoredSamples.log** located in **<APM root directory>\log\wde** folder. If this log includes samples of the monitor you have just run, or you see many ignored samples, this means SiteScope is sending the wrong data.

   c. If you do not see the relevant SiteScope sample, look for it in the **wdePublishedSamples.log** and check that `Eti_id` and `ci_hint` are not null.

   d. If you cannot find the SiteScope sample in the wde logs in APM, check in SiteScope if the sample was generated. Open the **bac_integration.properties** file located in **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** and add the text found in **attachment4.txt** (attached to this PDF) to the end of the file. To view the attachment, select **View > Navigation Panels > Attachments**, and select **attachment4.txt**.

   e. Run the monitor, and check the **samples.log file** in the **<SiteScope root directory>\logs\bac_ integration** directory.

3. **Check CI resolution**

   If HIs and KPIs are assigned to the relevant CI, and samples are not ignored by the wde logs in APM, check CI resolution (in case the problem is with the monitored CI and not the monitor or measurement).

   a. Run the relevant monitor in SiteScope.

   b. On the APM machine, open the **cir_enrichment.log** file located in the **<APM root directory>\log\wde** folder, and check if there are `badHint` or `CI not found` messages.

   > **Note:** To change the log file to debug mode, open the **cir_enrichment_service.properties** file located in the **<APM root directory>\conf\core\Tools\log4j\wde** folder and change `loglevel` to `loglevel=DEBUG`.

4. **If there are no HIs on the relevant CI (in case the problem is with the monitored CI and not the monitor/measurement)**

   If the relevant CI does not have any HIs, in SiteScope, check the indicator mappings in the monitor user interface (**HP Integration Settings > Indicator Settings**).

   - If the mapping seems correct, go to the correct SiteScope Monitor CI or SiteScope Measurement CI in RTSM in APM, and check that you can see the HI ID in the **health_indicator_list** attribute.

   - If you can see it, check that you can see the monitored CI connected to this SiteScope Monitor or Measurement CI with a **monitored_by** link.

5. **If there are no KPIs on the relevant CI (in case the problem is with the monitored CI and not the monitor/measurement)**

   If the relevant CI does not have any KPIs, check if KPI assignments are defined for the CI types.

   a. In APM, select **Admin > Service Health > Assignments > KPI Assignments**.

   b. In the CI Types tree, drill down to the relevant CI (for example, **Infrastructure Element > Node > Computer**), and check if the CIT has a KPI assignment defined. KPI assignments appear in the right pane.

6. **If there are no HIs/KPIs and everything seemed to work in the previous two steps**

   Try to resynchronize the HI and KPI assignments on the problematic CIs, based on their CI types.

   a. In APM, select **Admin > Service Health > Assignments > Health Indicator Assignments.**

   b. Select the problematic CI type (for example, `computer`), and select the HI assignment you want to run.

   c. Click the **Synchronize CI Type** button.

   d. When this is done, perform the same action on the KPI assignment using the **KPI Assignments** tab.

CI Downtime Issues

This section describes troubleshooting CI downtime issues when SiteScope is integrated with APM/OMi.

This section includes:

- "Troubleshooting CI Downtime (APM/OMi-side)" below
- "Troubleshooting CI Downtime" below

Troubleshooting CI Downtime (APM/OMi-side)

If the SiteScope monitor does not enter downtime (it is still running, or is sending alerts while it should not be according to the downtime configuration), perform the following checks on SiteScope and APM/OMi:

1. Check SiteScope reported topology to APM/OMi. In APM/OMi, select **Admin > RTSM Administration** and check the node and monitor CIs.

2. Logs:

   - Open **<APM/OMi root directory>\conf\core\Tools\log4j\PlainJava\topaz.properties** and change the debug level to the following appender:

     ```
     log4j.category.com.mercury.topaz.sitescopetmc=DEBUG, aims.appender
     ```

   - Open the **aims.ejb.log** file located in **<APM/OMi root directory>\log\EJBContainer** and search for "downtime" string. Check whether your downtime was created, which CIs were affected by it, and when a downtime request was made from SiteScope.

Troubleshooting CI Downtime

If the SiteScope monitor is still running after configuring downtime on a specific node using the stop monitoring option, perform the following checks on SiteScope:

1. In **Preferences > Infrastructure Preferences > General Settings**, check the **Enable downtime mechanism** setting is enabled.

2. Check the following logs:

   - **<SiteScope root directory>\logs\audit.log**

   - **<SiteScope root directory>\logs\downtime.log**

   To open these logs in debug mode:

   a. In the **<SiteScope root directory>\conf\core\Tools\log4j\PlainJava** folder, open the **log4j.properties** file.

   b. Change the debug level to the appenders listed in **attachment5.txt** (attached to this PDF). To view the attachment, select **View > Navigation Panels > Attachments**, and select **attachment5.txt**.

Appendix A: Delete an Existing Operations Manager Integration and Create a New Operations Manager Integration

This topic covers the detailed steps required to delete the existing OMi integration and create a new one.

1. Log on to SiteScope.
2. Click **Preferences** > **Integration Preferences** and select the OMi integration.
3. Click to delete the integration.
4. Clean the agent manually using any one of the following options:

   - Uninstall and reinstall HPE Operations Agent.

   - Clear the OMi server details in the Operations Agent config files.

Uninstall and reinstall the HP Operations Agent

1. Uninstall HP Operations Agent.

   (Windows) In the Control Panel, select Add or Remove Programs or Programs and Features, and uninstall HP Operations Agent

   (Linux) Run the following commands (Linux)

   ```
   cd /opt/OV/bin/OpC/install
   ./oainstall.sh -r -a
   ```

2. Reinstall HP Operations Agent 11.14.

   (Windows) Browse to the folder where the agents bits are located and run the command:

   ```
   cscript oainstall.vbs -i —a
   ```

   (Linux) Browse to the folder where the agents bits are located and run the command:

   ```
   ./oainstall.sh -i —a
   ```

Clear the OMi server configuration from Operations Agent manually

1. Remove the certificates with the following command:

   ```
   ovcert -list
   ```

2. For all IDs in the output, run the command:

   ```
   ovcert -remove 'id'
   ```

3. Remove the old OMi server details using the following command:

   ```
   ovconfchg -ns -clear -all
   ```

4. Restart agent

```
ovc -kill
ovc -start
```

Create a new OMi integration in SiteScope

Verify that the Operations Agent is installed successfully before you create a new integration.

1. Complete the HP Operations Agent installation using the SiteScope Configuration Tool.

   a. Run the SiteScope Configuration Tool on the SiteScope server:

      ○ On Windows: Select Start > All Programs > HP SiteScope > Configuration Tool.

      ○ On Linux (graphic mode): Run <SiteScope install Directory>/bin/config_tool.sh;

      ○ In console mode, run <SiteScope install Directory>/bin/config_tool.sh -i console.

   b. In the Configure HP Operations Agent installed separately option (HP Operations Agent option in console mode), select Configure HP Operations Agent to complete the configuration of the HP Operations agent.

   c. Restart SiteScope.

      After configuring the HP Operations Agent, check the installation status in the following log files.

      ○ Log file name: HPSiteScope_config_tool.log

      ○ Log file location: win- %temp% on Windows platforms and /temp or /var/temp on UNIX/Linux platforms

      Tip: Search for results of "installOATask"

2. Configure the Operations Agent connection settings on the SiteScope server.

   Under Integration Preferences, configure the HP Operations Agent connection settings to the HPOM(i) management server.

   a. Select Preferences > Integration Preferences and click . The Integration Preferences Type dialog box is displayed.

   b. Select the HP Operations Manager Integration from the list of integrations. The HP Operations Manager dialog box is displayed.

   c. Under the HP Operations Manager Integration Main Settings panel, enter the following under Connection Settings:

      ○ **HP Operations Agent installation path**. Enter the path to the HP Operations Agent installation on the SiteScope server.

      > **Note**:
      > On Windows platforms, the installation path is automatically resolved from the HP Operations Agent `InstallDir` key in the registry and appears in this field. The default path is `C:\Program Files\HP\HP BTO Software\`. If the key is not found, the field is left empty, and you must manually enter the installation path.
      >
      > On UNIX platforms, SiteScope checks to see if the HP Operations Agent is installed in the default `/opt/OV` path. If it is not there, the field is left empty, and you must manually enter the agent installation path. If you manually entered a different path, click the **Resolve Path** button to restore the default installation path found by SiteScope.

      ○ **HP Operations Manager server**. Enter the name or IP address of the HPOM/OMi server to which you want to connect.

   d. Click **Connect** to connect the agent to the HPOM management or OMi server. This sends a connection request from the agent to the specified server.

e. Accept the certificate request from HPOM/OMi.

f. Click the **Install Policies** button to install policies from SiteScope.

g. Click Analyze to verify if everything is working fine.

h. Check connection status and send test message from the SiteScope server.

Appendix B: Redirect the Operations Manager Integration

This topic covers the detailed steps to redirect the Operations Manager integration to a different server.

Steps

1. On the SiteScope server where the HP Operations Agent is installed, run the following command to create a new core ID:

   ```
   ovcoreid -create -force
   ```

2. To remove the certificates, run the command:

   ```
   ovcert -list
   ```

   For all IDs in the output, run the command:

   ```
   ovcert -remove 'id'
   ```

3. Set the new server host name and core ID with the following commands:

   ```
   ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <new OM(i) server>

   ovconfchg -ns sec.core.auth -set MANAGER <new OM(i) server>

   ovconfchg -ns sec.core.auth -set MANAGER_ID <new OM(i) server ovcoreid>

   ovconfchg -ns eaagt.lic.mgrs -set general_licmgr <new OM(i) server>

   ovconfchg -ns sec.cm.certificates -set CERT_INSTALLED FALSE
   ```

4. Run the following commands to restart the HP Operations Agent:

   ```
   ovc -kill

   ovc -start
   ```

5. Create a new certificate with the following command:

   ```
   ovcert -certreq
   ```

6. Grant a certificate request on the HPOM or OMi Gateway Server (in case of distributed OMi, grant certificate request on the Data Processing Server).

7. On SiteScope, open the Operations Manager Integration dialog box and in the HP Operations Manager Integration Main Settings panel,

   change the name or IP address of the HPOM/OMi server in the HP Operations Manager /OMi server box.

> **Note**: After reconnecting to the HPOM server, it can take some time until events are sent to HPOM. Restarting the HPOM server, the HP Operations agent, or both, might fix it.

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 Integration with Application Performance Management (APM) and Operations Manager i (OMi) (SiteScope 11.33)

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 sitescope-doc-feedback@hpe.com.

We appreciate your feedback!