Hewlett Packard
Enterprise

HPE SiteScope

Software Version: 11.32

Integration with HP Operations Manager Products

Document Release Date: March 2016
Software Release Date: March 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® 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.hp.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.

This document was last updated: Wednesday, March 30, 2016

Support

Visit the HPE Software Support web site at: **https://softwaresupport.hp.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 HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to **https://softwaresupport.hp.com** and click **Register**.

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

HPE Software Integrations, Solutions and Best Practices

Visit the Integrations and Solutions Catalog at https://hpenterprise.sharepoint.com/teams/aztec/Portal/index.html to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

Visit the Cross Portfolio Best Practices Library at **https://hpln.hpe.com/group/best-practices-hpsw** to access a wide variety of best practice documents and materials.

Contents

Part 1: Integrating with Operations Manager Products

Chapter 1: Configuring SiteScope to Communicate with HPOM and Operations Management Overview

SiteScope, which is an agentless solution for IT infrastructure performance and availability monitoring, can work together with Operations Manager (HPOM) and Operations Management in BSM 9.x, to provide a powerful combination of agentless and agent-based infrastructure management.

Note: SiteScope can also be integrated with Operations Manager i 10 (OMi 10) which is a separate product from BSM and HPOM. For details on performing this integration, see the Operations Manager i - HP SiteScope Integration section of the OMi Integrations Guide 10.00.

- **Events**. SiteScope communicates events to these applications using the HP Operations agent, which must be installed on the SiteScope server. Events in SiteScope are based on SiteScope monitor metric status changes and alerts being triggered. SiteScope sends events by writing them to a log file which is monitored by the HP Operations agent. The agent reads the data and converts it to events, which it forwards to the HPOM management server, or to BSM for use in Operations Management, Service Health, and Service Level Management. For details on sending events, see "Configuring SiteScope to Send Events to HPOM or Operations Management Overview" on page 14.
- **Metrics Integration.** SiteScope makes its metrics data available for use in HP Performance Manager (the reporting component of HPOM) and Performance Graphing in BSM's Operations Management.
  - For **Performance Graphing**, you can use either of the following data sources for reporting data to BSM:
    - Profile database in BSM, as part of the BSM integration (this is the recommended data source).
    - HP Operations agent installed on the SiteScope server, as part of the Operations Manager metric integration.

      Note: While reporting metrics data to the HP Operations agent is supported for Performance Graphing in this release, HP plan to stop supporting it in the future, and recommend that you use the BSM profile database method instead. Reporting metrics to the HP Operations agent as part of the Operations Manager metric integration is still supported for making metrics available in Performance Manager.
  - For **Performance Manager**, you must use the HP Operations agent installed on the SiteScope server, as part of the Operations Manager metric integration.

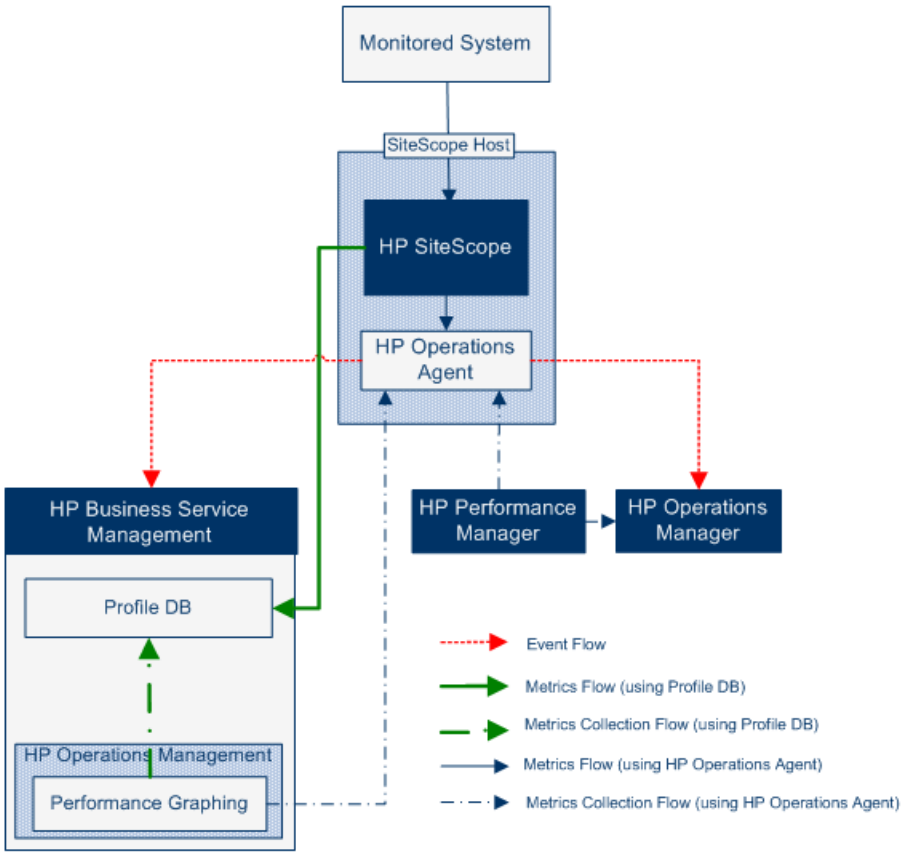
  For details on reporting metrics, see "Configuring SiteScope to Report Metrics for Use in HPOM or Operations Management" on page 67.

Note:

- This integration replaces the need to install the HP SiteScope Adaptor on the HPOM server that was required for the earlier integration solution when using the basic alert script mechanism.
- Metrics integration using the HP Operations agent (where metrics data is used in Performance Graphing in BSM's Operations Management) should not be confused with the BSM integration where SiteScope monitor metrics are used by the various BSM applications to calculate CI status (for example, in Service Health, Service Level Management, and System Availability Management). For details on BSM metrics integration, see the Connecting to a BSM Server section of the Using SiteScope Guide in the SiteScope Help.

Tip: For best practices and troubleshooting for reporting data to BSM and HPOM products, see the Integration with BSM and HPOM Best Practices Guide available from the SiteScope Help.

Event and Metrics Flow Diagram



HP Operations Agent Topology

HP Operations agent CIs are created when SiteScope is connected to HPOM, and HPOM is connected to BSM.

When SiteScope is connected directly to BSM, SiteScope creates the agent CI through its usual topology flow. When SiteScope sends its main topology (profile CI) and there is either an event or metrics integration with Operations Manager active, it also sends the agent topology.

Note:

- The agent CI is deleted only when both event and metrics integrations are removed.
- The agent CI is not deleted when SiteScope is disconnected from BSM, because SiteScope cannot detect if the connection is through HPOM or BSM (the agent CI eventually disappears due to the aging process).

Chapter 2: Centralized Template Management from HPOM

This integration enables you to centrally manage and deploy templates from multiple SiteScope instances from within HPOM (this is not relevant when SiteScope is integrated with Operations Management).

Benefits

This integration provides the following benefits:

- Centralized management of templates across multiple SiteScope instances—you no longer have to worry about templates getting out of sync or to manually sync templates.
- Version control for templates (including roll-back functionality).
- Automatic and robust deployment of templates based on group policy assignment (desired state handling).
- Scheduled roll out of template deployment.
- Reduced firewall configuration, leveraging existing Operations agent-HPOM management server connectivity.
- Unified management of SiteScope and the Operations Agent through a single administrative console.

Note: This integration is currently not supported for HPOM for Windows.

Available Actions

When managing SiteScope templates with HPOM, you can perform the following actions:

- Export all templates from SiteScope and import them to HPOM as policies, which you can later on assign and deploy. Use the **Export to OM** option in the Template shortcut menu in SiteScope to export SiteScope templates to HPOM when SiteScope and HPOM are installed on the same machine.
- Create or modify a template on SiteScope and then move this template to HPOM (only when SiteScope and HPOM are installed on the same system). This means that you can either create a new template or modify an existing template to contain the text or the variables that you choose.
- Deploy a SiteScope template or import template container from HPOM.
- Delete SiteScope templates.

Note: When deploying a template to SiteScope from HPOM, all mandatory SiteScope variables must have a value set in the OM Policy. If not, the deployment fails.

For details on managing SiteScope templates with HPOM, see the Deploying SiteScope Configuration with HPOM Guide, available from the Home page of the SiteScope Help, or from the HPE Software Support site.

System Requirements

Template integration with HPOM is available provided your system conforms to the following requirements:

- SiteScope is installed and connected to a supported version of HPOM. For the HPOM versions supported in this release, see the HP Operations Manager Integration Support Matrix in the SiteScope Deployment Guide (available from the HPE Software Support site), or check the HPE Integrations site.
- Before installing SiteScope, you should create a predefined SiteScope configuration with a defined username and password for the SiteScope Administrator. For details, see the Deploying SiteScope Configuration with HPOM Guide, available from the SiteScope Help or from the HP Software Support site.
- The Operations agent is installed on the SiteScope server. You can install Operations Agent 11.14 from the root directory of the SiteScope release media. For details, see the Installing SiteScope section of the HPE SiteScope Deployment Guide (available from the HPE Software Support site).
- Operations Manager integration is configured in SiteScope and the **Enable exporting templates to HP Operations Manager** check box is selected in HP Operations Manager Integration Main Settings. For details, see "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19.

Chapter 3: SiteScope Failover and Operations Manager Integration

The SiteScope Failover (automated mirroring) solution provides support for Operations Manager event and metrics integration.

Event Integration

To enable SiteScope Failover support for OM event integration, perform the steps in "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19, both for the primary SiteScope and for the SiteScope Failover.

Event flow and host discovery flow work without any additional steps. For the Monitor Discovery integration, follow the steps in "How to Enable the SiteScope Monitor Discovery Policy" on page 36 for the primary SiteScope only.

Notes and Limitations

- Since there is only one SiteScope service tree (and it is affected by events), it is not possible to know if it is affected by what was reported from the primary or failover SiteScope.
- When the primary is down, events triggered from monitors that are monitoring the SiteScope server (in this case, the SiteScope server is the failover) do not affect the service tree.
- Groups and monitors added when the primary is down are not displayed in the service tree.
- The Drill Down to SiteScope tool works only when the primary SiteScope is running.
- If there are different agent configurations on the primary and SiteScope Failover (for example, an agent is installed on a different path), the agent command on the failover server will not run from the Event Integration preferences user interface and you need to enter the agent path manually beforehand.

Metrics Integration

SiteScope Failover provides support for OM metrics integration.

Note: When using the Operations Agent as the data source for reporting metrics to Operations Management, SiteScope Failover reports metrics to the Operations Agent and not to the primary's agent.

Part 2: Sending Events to HPOM or Operations Management

Chapter 4: Configuring SiteScope to Send Events to HPOM or Operations Management Overview

You can enable SiteScope to send events directly to the HPOM management server and to BSM (for use in Operations Management, Service Health, and Service Level Management). Events in SiteScope are based on SiteScope monitor metric status changes and alerts being triggered.

To enable SiteScope to send events, the HP Operations agent must be installed on the SiteScope server. You can install the Operations Agent from the SiteScope installer package, or download it from the HPE Software Support web site.

After the agent is installed, it must be configured in SiteScope Integration Preferences. This involves entering the installation path of the agent and the host name or IP address of the HPOM management or BSM Gateway Server, and connecting the agent to HPOM or BSM. The agent then sends a connection request to HPOM or BSM which must grant the certificate request (the HPOM management server can be configured to accept this client automatically).

After the certificate request has been granted on the HPOM or BSM server, a preconfigured log file policy should be installed and signed on the agent installation on the SiteScope server. This enables SiteScope to sign the preconfigured Operations Manager policies locally and automatically. This policy comes with SiteScope, and is deployed from the Operations Manager Integration dialog box in SiteScope's Integration Preferences.

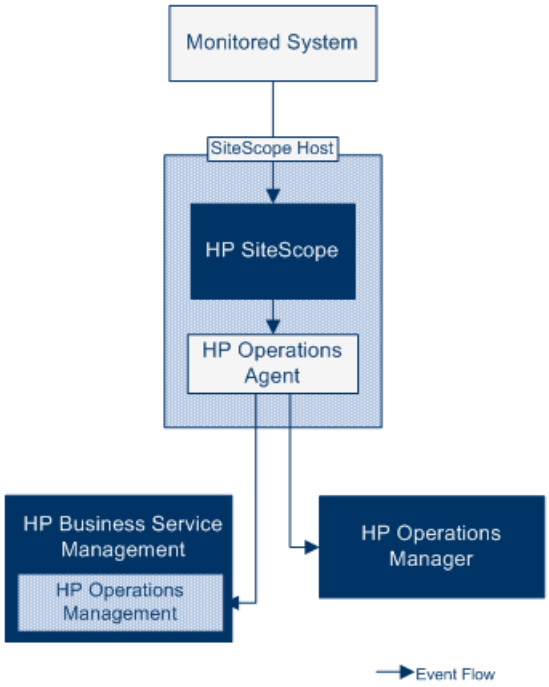
When an event is triggered, SiteScope writes the event data to the **HPSiteScopeOperationsManagerIntegration.log** file which is located in the **<SiteScope root directory>\logs** directory. Each event is written as a separate line in the log. The log file policy instructs the agent to read this file and create event messages that are sent to HPOM or BSM.

The format of the event attributes is determined using the event mapping template. The template maps SiteScope runtime data to the event attribute values that are sent to the HPOM management or BSM Gateway Server when an event is triggered. For details on event mappings, see the section on Common Event Mappings in the Using SiteScope Guide in the SiteScope Help.

After the data is converted to an event, the agent sends the event to the HPOM management/BSM Gateway Server. Events appear in:

- HPOM's Event Console.
- BSM's Operations Management Event Browser if you have an Event Management Foundation license, and in Service Health for events that affect CIs. If Operations Management is not part of your BSM installation, you can still view events that affect CI status using a health indicator in Service Health.

The following diagram illustrates event data flow:



Note: The HP Operations agent can be configured either to report events to an HPOM management or a BSM Gateway Server—not to both.

For details on configuring SiteScope to send events, see "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19.

Event Generation

You can configure events to be generated and sent to the HPOM management server or to Operations Management in BSM following a change in a monitor's metric status or when a SiteScope alert is triggered.

- **Status Change**. Every metric/counter status change is an event (for example, if the CPU utilization status changes from `Good` to `Error`). You can choose whether events are triggered for metrics status changes in the monitor's properties. By default, SiteScope sends an event for each metric status change for the monitor instance.

  You can change the default settings for sending events and the event attribute values used when an event is triggered. The event attribute values are filled according to the event configuration mappings using the monitor's properties. For details on event mappings, see the event mapping section in the Using SiteScope Guide in the SiteScope Help.

  In addition to sending the monitor properties, SiteScope also sends health indicators or event type indicators ("indicators") for the monitor instance. Events are categorized according to indicators. The BSM event manager uses indicators to categorize events according to the type of occurrence in the managed IT environment (for example, CPU Load). Indicators that provide CI state information are then used to calculate the CI.

  Note: Status change is applicable only to metrics that are configured in the monitor's Thresholds Settings.

- **Alert**. Every alert is an event. Since alerts are triggered per monitor, an event triggered by an alert can use the monitor's properties, but not the indicators associated with a specific metric. Therefore, when configuring an event alert, you can manually select the indicator that is reported when an event is triggered by an alert. As a result, the indicator is more generic, and you should select indicators that do not affect health indicators in BSM.

  You can choose whether an alert sends events to HPOM or BSM in the alert definition in the Operations Manager Integration Settings panel.

  Note:

  - When a SiteScope alert is triggered, it is possible that two events are generated if both the alert and monitor are configured to send events. When configuring alerts to send events, you should not also enable the monitors to send events. Conversely, if you want an alert for each metric status change (together with health or event type indicators for the monitor instance), we do not recommend also using alert events.
  - SiteScope also includes threshold information in alerts that are sent to HPOM. In earlier versions of SiteScope and BSM, it was not possible to include the thresholds created for monitors in alerts.
  - In Operations Management, it is recommended to use alert events for notification purposes only.

Discovery Scripts and Drilling Down User to View HPOM Events

When SiteScope is integrated with HPOM, the **Node discovery** and **Monitor discovery** policies are activated for nodes and monitors on the HPOM management server.

Both discovery policies rely on the **Integration Viewer** user in SiteScope. This is the user provided by SiteScope for drilling down from HPOM events. This user has been granted view permissions, and permissions to refresh groups and monitors. For details on users and user permissions, see the User Management Preferences section of the Using SiteScope Guide in the SiteScope Help.

Note:

- If the Integration Viewer user is deleted from User Management Preferences, this user type is automatically created when SiteScope is restarted.
- If the Integration Viewer user properties are changed, you must restart SiteScope to update the user properties file, or you can manually update the user properties in the **<SiteScope root directory>\conf\sitescope_connection.properties** file.

  When changing Integration Viewer user properties manually, the user login name and password should be encrypted using the SiteScope Encryption Tool as follow:

  a. Run the following batch file:
     - **For Windows:** `<SiteScope root directory>/tools/AutoDeployment/encrypt_password.bat`
     - **For UNIX:** `<SiteScope root directory>/tools/AutoDeployment/encrypt_password.sh<SiteScope`

  b. Open a command prompt window.
     - In Windows, drag and drop the file into your command prompt window.
     - In UNIX, you must run the .sh file from its directory.

  c. Enter space and the password value (for example `Mypassword`). Click `Enter`.

  d. Use the returned string as a value for the encrypted variable in the XML file. You much change the value of the attribute **encrypted** to **yes** and the **value** of the variable attribute to the returned string.

     For example, the following value was generated by the encryption tool: `<deploy:variables encrypted="yes" name="password" value="(sisp)d5JLOSWaVfE="/>`

For details on deploying the discovery policies on the HPOM management server, refer to the HPOM documentation.

For troubleshooting discovery policy issues, see "Node Discovery and Monitor Discovery Troubleshooting" on page 64.

Node Discovery Policy

When SiteScope is connected with HPOM, a node is automatically created and registered in HPOM for each node monitored by SiteScope. This enables SiteScope to report all the nodes that it monitors to HPOM. Only hosts for monitors which report events are sent to HPOM through the discovery policy.

Tip: When you are not connected to HPOM (if connected to Operations Management), it is recommended to disable the node discovery by running the command: `ovpolicy -disable -polname SiteScope_Hosts_Discovery`

Note:

- SiteScope does not report nodes or services to HPOM for monitors that are disabled, or are not configured to send events.
- By default, SiteScope reports all the nodes that it monitors to HPOM every 5 minutes. You can modify this frequency by adding the **_timeOutRunDiscoveryPolicyMinutes=** property to the **<SiteScope root directory>\groups\master.config** file, and a value, in minutes, representing the reporting frequency. For example, `_timeOutRunDiscoveryPolicyMinutes=10` means that the discovery policy is run every 10 minutes.
- When SiteScope uses an SSL connection, you need to update the node discovery policies batch file with the trust store password and keystore password and run the policy again. For details, see the "Update Discovery Policies when SiteScope uses SSL" on page 38.

Monitor Discovery Policy

This is an optional policy that must be activated manually on HPOM using the files in the **<SiteScope root directory>\tools\OMIntegration\SiteScopeMonitorDiscoveryPolicy** directory. After the policy has been activated, SiteScope runs the SiteScope-OM monitor discovery script when it is connected with HPOM.

This policy enables the HPOM Service Navigator to view the SiteScope monitor tree in the HPOM service maps. When new monitors, groups, or both, are added or changes are made in the SiteScope monitor tree, the services tree is updated in HPOM to reflect these changes. In addition, when events arrive to HPOM, they affect the SiteScope services tree and color all related nodes affected by them.

For details on how to enable the monitor discovery policy, see "How to Enable the SiteScope Monitor Discovery Policy" on page 36.

For details on enabling the tool to drill down to SiteScope from HPOM, see "How to Enable the Drill Down to SiteScope Tool on HPOM for Windows" on page 32 and "How to Enable the Drill Down to SiteScope Tool on HPOM for UNIX/Linux/Solaris" on page 34.

Chapter 5: How to Enable SiteScope to Send Events to HPOM or Operations Management

This task describes how to enable SiteScope to be used to send events to the HPOM management server or BSM Gateway Server.

1. **Prerequisites**

- Your system must conform to the following requirements:
  - SiteScope version 11.00 or later is installed.
  - For Operations Management, BSM 9.00 or later is installed.

    Note: SiteScope can also be integrated with Operations Manager i 10 (OMi 10) which is a separate product from BSM and HPOM. For details on performing this integration, see the Operations Manager i - SiteScope Integration section of the OMi Integrations Guide 10.00.

  - For HPOM, Operations Manager for UNIX 9.0x or later, or Operations Manager for Windows 8.1x or later is installed.

    Note: The node discovery, monitor discovery, and template integration are not supported for all versions of HPOM. For details of the integrations that are supported and of any patch requirements, refer to the Operations Manager (HPOM) Integration Support Matrix in the HP SiteScope Deployment Guide (available from the HPE Software Support site).

- Only a SiteScope administrator user, or a user granted **Edit integration preferences** and **Add, edit or delete common event mappings** permissions can configure the integration and event mappings. For details on user permissions, see the User Management Preferences section of the Using SiteScope Guide in the SiteScope Help.

- (If SiteScope is installed on a Red Hat ES Linux 6.0 64-bit environment) You must install the following dependencies before installing the Operations Agent:
  - Install **compat-libstdc++-33-3.2.3-69.el6.i686.rpm** on the Red Hat Enterprise Linux 6 x64 node.

    Note: To install SiteScope with the Operations Agent on RHEL x64 in graphics mode, you must run the installer with the machine default 64-bit JRE.

    ./<PRODUCT_NAME>_<VERSION>_setup.bin LAX_VM /usr/bin/java $@

    For example, if /usr/bin/java points to the 64-bit JRE or JDK:

    ./HPSiteScope_11.30_setup.bin LAX_VM /usr/bin/java $@

- Install **compat-libstdc++-33-3.2.3-69.el6.ppc64.rpm** on the Red Hat Enterprise Linux 6 PPC node.

You can install the dependencies, using the yum package manager provided in Red Hat Enterprise Linux, by running the command:

- `yum install compat-libstdc++-33-3.2.3-69.el6.i686`

  or

- `yum install compat-libstdc++-33-3.2.3-69.el6.ppc64`

2. **Install the Operations Agent on the SiteScope server**

Install Operations Agent 11.14 from the SiteScope installer package, or download it from the HPE Software Support web site (in the Search box, type "Operations Agent", select the relevant version, under Document Type, select **Patches**, and locate the installation file).

Note: If an older version of the agent is already installed, or the agent is already integrated with OMi/OMu/OMw, you should:

a. Upgrade the agent according to the instructions in the HPE Operations Agent 11.14 Installation Guide.

b. Configure the agent using the SiteScope Configuration Tool as described in step 3 below.

On Windows:

a. Log on to the node with the administrator privileges.

b. Go to the directory where you extracted the contents of the ISO file.

c. Run the following command to install the agent:

```
cscript oainstall.vbs -i –a
```

On UNIX/Linux:

a. Log on to the node with the root privileges.

b. Go to the directory where you extracted the contents of the ISO file.

c. Run the following command to start the installation:

```
./oainstall.sh -i -a
```

d. When the installation is complete, the agent starts its operation on the node and all the necessary components start running.

For more detailed installation instructions, see the HPE Operations Agent 11.14 Installation Guide, available from the HPE Software Support site.

Note:

- Only Operations Agent version 11.14 is certified with SiteScope 11.30 or later.
- Use the `-includeupdates` installation option to install Operations Agent 11.14 with pre-packed hotfixes. For details, refer to the Operations Agent 11.14 Installation Guide.
- To enable the Operations Manager event integration, the Operations Agent on the SiteScope machine must run under the same user as in SiteScope, namely a non-root user. For details, see Configure an Agent to run Under an Alternative User on UNIX in the Operations Manager for UNIX - HTTPS Agent Concepts and Configuration Guide.

3. Complete the Operations Agent installation using the SiteScope Configuration Tool

Note: This step must be performed before integrating the Operations Agent to HPOM.

The Configuration Tool installs two components:

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`.
   - On Linux (console mode): Run `/opt/HP/SiteScope/bin/config_tool.sh -i console`.

   For more details on using the SiteScope Configuration Tool, see the HPE SiteScope Deployment Guide (available from the HPE Software Support site).

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 installation of the Operations Agent.

c. Restart SiteScope (if required).

d. (If the agent is installed on a Red Hat ES Linux 6.0 environment) After installing the Operations Agent, check the installation status in the log files.
   - SiteScope log. This just shows whether the installation passed successfully or not.

     Log file name: **HPSiteScope_config_tool.log**

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

     (search for results of "installOATask")
   - Operations Agent log files.

     Log file name: **oainstall.log**, **oapatch.log**

Log file location:

- **%ovdatadir%\log** on Windows platforms
- **/var/opt/OV/log/** on UNIX/Linux platforms

4. **(For Operations Management only) Configure the connection request to be passed to the Data Processing Server if BSM is installed on a distributed environment, or if BSM Gateway Servers are behind a load balancer**

   If BSM uses a separate Gateway and Data Processing Server, perform the following to enable the request received on the Gateway Server to be passed to the Data Processing Server:

   a. In BSM, select **Admin > Platform > Infrastructure Settings**:
      - Select **Applications**.
      - Select **Operations Management**.
      - In the **Certificate Server Settings**, locate the **Certificate Server Host**. Make sure that the value matches the host name or IP address of the active BSM Data Processing Server that acts as the certificate server host. If it does not match, change it accordingly.

        Note: If the BSM Data Processing Server fails and automatic failover has been configured, you must change the **Certificate Server Host** setting to the name of the backup Data Processing Server to handle new certificate requests. However, if you do not expect any new certificate requests during the Data Processing Server failover timeframe, you can keep the setting unchanged as it does not affect any event integrations configured previously.

   b. Configure the Gateway Server:
      - Change the active directory to the **\bin** directory by typing `cd <HPBSM root directory>\bin`.
      - Run **setup-secure-communication.bat** and enter the DNS name of the Data Processing Server.

   c. Configure the Data Processing Server:
      - Change the active directory to the **\bin** directory by typing `cd <HPBSM root directory>\bin`.
      - Run **setup-secure-communication.bat** and type `g` to grant the request (make sure that you grant this request and not some other request).

   d. If you are using a BSM failover environment with load balancer, make sure to keep the certificate server of each Data Processing Server synchronized.
      - Repeat steps b and c for every Gateway Server. It does not matter to which Data Processing Server you send the certificate request because the Data Processing Servers already trust each other. As a result, all Gateway Servers trust both Data Processing Servers and can communicate with them regardless of which one is active at any given moment.

- If you install a new certificate on the running Data Processing Server, you also have to install the certificate on the secondary Data Processing Server which is used as failover. To install the new certificate, run the following commands:

```
ovcert -importtrusted -file <newCertificateFilePath>
ovcert -importtrusted -file <newCertificateFilePath> -ovrg server
```

- Configure the load balancer to forward all HTTPS traffic that arrives on port 383 to the Gateway Servers. This enables the certificate requests and event forwarding to work.

5. **Configure the agent connection settings on the SiteScope server**

In SiteScope Integration Preferences, configure the Operations agent connection settings to the HPOM management server or BSM server.

a. Select **Preferences** > **Integration Preferences**. In the Integration Preferences page:

- Click the **New Integration** button and select **HP Operations Manager Integration**, or
- Select an existing integration and click the **Edit Integration** button.

b. In the Operations Manager Integration dialog box, expand the **HP Operations Manager Integration Main Settings** panel, and enter the following in the **Connection Settings** area:

- **HP Operations Agent installation path**. Path to the HP Operations agent installation on the SiteScope machine.
  - On Windows platforms, the installation path is automatically resolved from the 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 agent installation path.
  - On UNIX platforms: SiteScope checks to see if the 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/BSM server**. Enter the name or IP address of the HPOM/BSM server to which you want to connect. If you are connecting to a BSM-distributed environment, enter the BSM Gateway Server name or IP address. If your BSM Gateway Servers are behind a load balancer:
  - For BSM data/topology integration: Enter the name or IP address of the load balancer that is configured for users.
  - For OM event integration (Operations Management in BSM): Enter the name or IP address of the load balancer that is configured for data collectors.

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

6. **Accept the agent connection request on the HPOM management server or BSM Gateway/Web Processing server**

- **For HPOM:**

  In HPOM, you need to configure the SiteScope node, map the certificate request to this node, and accept the certificate request.

  i. In HPOM, add SiteScope as a managed node.

  - For HPOM for Windows, you can use the **ovownodeutil** command-line tool to add a node, or you can use the user interface. For details, see the "Configure nodes" section in the HPOM for Windows documentation.
  - For HPOM for UNIX/Linux, you can use the **opcnode** command-line tool to add a node.

    Example - Using the opcnode command line tool:

    ```
    # opcnode -add_node node_name=<SiteScope_node_name> \net_type=<network_
    type> mach_type=<machine_type> \group_name=<group_name> node_
    type=<node_type>
    ```

    For detailed information, see the HPOM for UNIX and Linux documentation:

    - "Adding a Managed Node to the HPOM Database" in the Administrator's Reference Guide.
    - "Install HPOM Software on HTTPS Nodes" and "Working with Certificates" in the HTTPS Agent Concepts and Configuration Guide.

  ii. List the pending certificate request IDs with the following command. If you want that detailed information on every pending request is listed, use the -l option:

    ```
    ovcm -listpending [-l]
    ```

    Note the request ID for the SiteScope node.

    For more information, see the ovcm manual page.

  iii. Grant the certificate request to the SiteScope node, with the following command:

    ```
    ovcm -grant <SiteScope_node_request_id>
    ```

- **For BSM:**
  - If you are integrating with BSM 9.20 or later, go to **Admin > Operations Manager > Certificate Request**, and follow the instructions to locate and grant your certificate request.
  - If you are integrating with versions of BSM earlier than 9.20:

    For BSM running on a Gateway Server only, perform the following on the BSM Gateway Server. If BSM runs on a distributed environment, perform the following on the Data Processing Server.

i. (Optional) To make sure that the OV Certificate Server process is running, run the command line `run ovc -status`. If it is not running, run the command `ovc -start` or contact your BSM administrator.

ii. Change the active directory to the **\bin** directory by typing `cd <BSM root directory>\bin`.

iii. Run **setup-secure-communication.bat** and type `g` to grant the request (make sure that you grant this request and not some other request).

iv. Make sure that the request ID you are going to accept is associated with the agent's core ID. To retrieve the agent's core ID, in SiteScope, click the **Analyze** button in HP Operations Manager Integration, or run the agent's `ovcoreid` command on the SiteScope server.

7. **Install the log policies on the SiteScope server**

After the certificate request has been granted on the HPOM/BSM server, click **Install Policies** in the **HP Operations Manager Integrations Main Settings** panel of the HP Operations Manager Integration dialog box. This installs and signs the preconfigured log file policy file on the Operations Agent.

Note:

- If an agent is connected to an HPOM or BSM server and you want to connect it to a different server, you must uninstall and reinstall the agent or redirect the agent to another server. For task details, see "How to Reconnect the Operations Agent to a Different HPOM or BSM Server" on page 30.
- Customizing the default integration polices is not supported. Any changes made to the default integration policies results in SiteScope events being written to the event log only and not arriving to the HPOM Event Console/Operations Management Event Browser.

8. **Check connection status and send test message from the SiteScope server - optional**

If there are connectivity problems, you can perform problem analysis and check the status of the agent and the certificate request.

a. In the HP Operations Manager Integration dialog box, expand the **HP Operations Manager Integrations Main Settings** panel, and click **Analyze**.

Use the information supplied in the analysis results to perform problem analysis and for troubleshooting. For example, you can verify connectivity between the agent and server by checking the `bbcutil` connection protocol.

b. To check that the agent is connected to the HPOM management or BSM server, expand the **HP Operations Manager Integrations Advanced Settings** panel, type a message in the **Test message** text box, and click **Send Test Message**.

c. If the test is successful, the text message is displayed in the HPOM console or in the Operations

Management Event Browser in BSM. This message is generated by a basic **opcmsg** policy command.

9. **(For HPOM only) Extend the integration with HPOM using monitor discovery - optional**

   To enable the HPOM Service Navigator to view SiteScope groups and monitors in the HPOM service maps, you must manually enable the Monitor discovery policy on HPOM using the files in the **<SiteScope root directory>\tools\OMIntegration\SiteScopeMonitorDiscoveryPolicy** directory.

   For details on how to enable the policy, see "How to Enable the SiteScope Monitor Discovery Policy" on page 36.

   Note: To enable SiteScope Failover support for the Operations Manager event integration, follow the steps for configuring the monitor discovery policy in "SiteScope Failover and Operations Manager Integration" on page 12.

   Tip: You can also use the Drill Down to SiteScope tool to enable opening the SiteScope user interface from the monitor or group service that was discovered by the monitor discovery policy and added to the HPOM Service Navigator.

   - For details on enabling the tool on HPOM for Windows, see "How to Enable the Drill Down to SiteScope Tool on HPOM for Windows" on page 32.
   - For details on enabling the tool on HPOM for UNIX/Linux/Solaris, see "How to Enable the Drill Down to SiteScope Tool on HPOM for UNIX/Linux/Solaris" on page 34.

10. **Enable SiteScope to send events to HPOM or Operations Management**

    a. In the HP Operations Manager Integration dialog box, expand the **HP Operations Manager Integrations Main Settings** panel, and in the **Configuration Settings** area select **Enable sending events**.

    b. Configure the following settings as required:

    - **Connect directly to BSM**. When the agent is connected to Operations Management, select to automatically deactivate the node discovery policy if it was installed and enabled on the SiteScope server. When this option is selected:
      - The **Enable node discovery policy** option is not available, and the node discovery policy is disabled if it was installed and enabled on the SiteScope server.
      - The **Prefer events over metrics in BSM Service Health (global preference)** option is automatically selected.
    - **Prefer events over metrics in BSM Service Health (global preference)**. Determines the global default preference for influencing BSM's Service Health when both SiteScope events and metrics are reported to Service Health (since indicators for SiteScope events and metrics both affect CIs). This is relevant only when both BSM and Operations Manager integrations are active,

and are connected to the same BSM server (the BSM server is used instead of the HPOM server).

If selected, the **Events** option is set as the default preference for every new monitor created in **HP Integration Settings > BSM Service Health Preferences > BSM Service Health affected by**. If not selected, **Metrics** is the default preference for reporting data to BSM. By default, this is selected.

> **Note:** This setting does not override the preference already set for individual monitor instances in the monitor **Properties** tab **> HP Integration Settings > BSM Service Health Preferences > BSM Service Health affected by** box.

For more information on choosing the preference to use, see the section on integrating SiteScope with BSM in the Integration with BSM and HPOM Best Practices Guide in the SiteScope Help.

- **Enable node discovery policy**. SiteScope enables the node discovery policy (if installed) on the SiteScope server. This option is automatically selected when the **Connect directly to BSM** option is cleared. For details on Node discovery, see "Discovery Scripts and Drilling Down User to View HPOM Events" on page 17.
- **Enable exporting templates to HP Operations Manager**. Enables exporting all templates from SiteScope and importing them to HPOM as policies (only when SiteScope and HPOM are installed on the same system), which you can later on assign and deploy from HPOM. For details on the template integration with HPOM, see "Centralized Template Management from HPOM" on page 10.

11. **Enable default event severity mappings to be used - optional**

Severity mappings correlate the severity level in HPOM or BSM to the monitor threshold status in SiteScope. You can use the default severity mappings or customize the mapping between the Error, Warning, Good, and Unavailable status threshold for each monitor instance in SiteScope and the HPOM/BSM server in the **HP Operations Manager Integrations Advanced Settings** panel.

If **Use default severity** is selected, the default mappings are sent when:

- Events are created by a triggered alert.
- SiteScope is not connected to BSM.
- The indicator state and severity value is missing. For example, when using monitors that do not have a defined topology.

> **Note:**
>
> - This option is not available when SiteScope is connected to BSM (and the default global severity mappings cannot be sent).
> - By default, the `Warning` state is mapped to `Minor` (not `Warning`).

Note: You can override the severity mapping at the monitor level by modifying the **Severity** attribute in Common Event Mappings. For details, see "Configure event mappings for monitors and alerts - optional" below.

12. **Enable/Disable sending events for monitor instances and alerts**

By default, each newly-created monitor instance is configured to send an event for each metric status change, and each new alert is configured to send an event when triggered. Monitors and alerts that are upgraded from earlier versions of SiteScope are not configured to send events.

- To disable sending events when there is a change of a metric status (Good/Warning/Error/Unavailable) for a monitor instance, in the monitor properties for the selected monitor instance, expand **HP Integration Settings > HP Operations Manager Integration Settings**, and clear the **Send events** check box. Status change is only applicable on metrics that are configured in the monitor's Threshold Setting.
- To disable sending events for an alert, in the New/Edit Alert dialog box, expand the **HP Operations Manager Integration Settings** panel, and clear the **Send events** check box.

Note: The **Send events** option is selected by default when event integration is enabled in the HP Operations Manager Integration Main Settings panel (otherwise this option is not available).

13. **Configure event mappings for monitors and alerts - optional**

Monitor instances and alerts are assigned a common event mapping that is used when an event is triggered. This is the mapping between SiteScope runtime data and the values of the attributes of the event that will be sent.

You can use the default event mapping associated with the monitor or alert, select a different event mapping (if any exist), or create a new event mapping in **Preferences > Common Event Mappings**. Alternatively, for alerts, you can use the event mapping template associated with the monitor that triggered the alert.

You can select the event mapping template:

- When configuring a monitor instance from the monitor **Properties** tab **> Event Mapping Settings**.
- When configuring alerts from the **Alerts** tab > **New/Edit Alert** > **HP Operations Manager Integration Settings > Event mapping**.

For details on configuring Common Event Mappings, see "How to Configure Common Event Mappings for HPOM or BSM" on page 40.

14. **Results**

After a monitor metric status change or an alert is triggered in SiteScope, the event is written to the integration log file in the format selected for the monitor instance or alert in Common Event Mappings.

The agent monitors the log file and creates an event, which it sends to HPOM or BSM. Events are displayed in the Event Console in HPOM, or in BSM in the Operations Management Event Browser (if you have an Event Management Foundation license). If Operations Management is not part of your BSM installation, you can view events that affect CI status using a health indicator in Service Health.

For notes and limitations on event integrations, see "Notes and Limitations" on page 58.

For troubleshooting event integration issues, see "Troubleshooting Event Integration Issues" on page 58.

Chapter 6: How to Reconnect the Operations Agent to a Different HPOM or BSM Server

You can reconnect the Operations Agent to a different HPOM management or BSM server by either:

- Uninstalling and reinstalling the Operations Agent.
- Redirecting the Operations Agent to a different server.

> **Note:** This task is part of a higher-level task. For details, see "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19.

To uninstall and reinstall the HP Operations agent:

1. In SiteScope, select **Preferences > Integration Preferences**, and delete the Operations Manager integration.
2. In the Control Panel, select **Add or Remove Programs** or **Programs and Features**, and uninstall **HP Operations Agent**.
3. Install Operations Agent 11.14 which is available from the root directory of the SiteScope release media. For details, see "How to Enable SiteScope to Send Events to HPOM or OMi" on page 1.
4. Configure the Operations Agent using the SiteScope Configuration Tool. For details, see the Configuration Tool section of the SiteScope Deployment Guide (available from the HPE Software Support site).
5. In SiteScope, configure the Operations Manager integration with the new HPOM/BSM server to which you want to connect. For details, see "Configure the agent connection settings on the SiteScope server" on page 23.

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

To redirect the Operations Agent to a different server:

> **Note:** If you are cloning a machine with an Operations Agent which usually includes a host name and IP address change, start from step 1 below; otherwise start from step 4.

1. To remove the certificates, run:

   ```
   ovcert -list
   ```

   For all IDs in the output, run the command:

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

2. Adapt the xpl configuration variable OPC_NODENAME by running the command:

   ```
   ovconfchg -ns eaagt -set OPC_NODENAME 'hostname'
   ```

3. Set the new server host name and core ID by running the commands:

   ```
   ovconfchg -ns sec.cm.client -set CERTIFICATE_SERVER <new OM server>
   ovconfchg -ns sec.core.auth -set MANAGER <new OM server>
   ovconfchg -ns sec.core.auth -set MANAGER_ID <new OM server ovcoreid>
   ```

   Tip: To get the ovcoreid for MANAGER_ID in a distributed installation, run the command:

   ```
   ovcert -list -ovrg server
   ```

   ```
   ovconfchg -ns eaagt.lic.mgrs -set general_licmgr <new OM server>
   ovconfchg -ns sec.cm.certificates -set CERT_INSTALLED FALSE
   ```

   ovcoreid -show

4. Restart the Operations Agent by running the commands:

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

5. Create a new certificate request by running the command:

   ```
   ovcert -certreq
   ```

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

7. In SiteScope, open the Operations Manager Integration dialog box and perform the following in the **HP Operations Manager Integration Main Settings** panel:

   - Change the name or IP address of the HPOM/BSM server in the **HP Operations Manager / BSM server** box. For details, see "Configure the agent connection settings on the SiteScope server" on page 23.
   - Install the log policies by clicking the **Install Policies** button.

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

Chapter 7: How to Enable the Drill Down to SiteScope Tool on HPOM for Windows

This task describes how to enable the Drill Down to SiteScope tool on the HPOM for Windows management server. This tool enables you to open the SiteScope user interface from the monitor or group service that was discovered by the monitor discovery policy and added to the HPOM Service Navigator.

Note: This task is part of a higher-level task. For details, see "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19.

1. **Prerequisites**

   The Monitor Discovery policy must be enabled and deployed on the SiteScope Server node on HPOM.

   For task details, see "How to Enable the SiteScope Monitor Discovery Policy" on page 36.

2. **Install the Drill Down to SiteScope tool on the HPOM for Windows server**

   a. Log on to the HPOM for Windows server machine as an Administrator.

   b. Copy the **drillDownToSiteScope.vbs** file from the **<SiteScope root>\tools\OMIntegration\DrillDownTool\ForOMW** folder to **\\<HPOM server>\SPI-Share\SiteScope**.

   c. Upload the Drill Down to SiteScope tool to the HPOM server:

      - Copy the **tls_drillDownToSIS.mof** file from the **<SiteScope root>\tools\OMIntegration\DrillDownTool\ForOMW** folder to any folder on the HPOM server machine (`<tls path>`).
      - Open a command line and run the command:

        ```
        >> ovpmutil cfg tls upl <tls path>\tls_drillDownToSIS.mof
        ```

   d. The Drill Down to SiteScope tool is available on the HPOM server under **Tools > SiteScope Tools**.

3. **Associate the tool with the SiteScope Service**

   a. In the HPOM for Windows console, open the Service Type Configuration Editor, select **Application Services > SiteScope**, and click **Properties**.

   b. In the SiteScope Properties dialog box, click the **Tools** tab, select **SiteScope Tools**, and then click **OK.**

4. **Launch the tool (from the SiteScope service)**

   a. In the HPOM for Windows console, right-click the SiteScope service that you want to view (SiteScope monitor, group, or server service), and select **All Tasks > Launch Tool**.

   b. Select the **Drill Down to SiteScope** tool, and click **Launch**.

   c. The SiteScope user interface opens displaying the selected monitor, group, or the default Dashboard

view (if SiteScope Server service was selected).

5. **Launch the tool (from the Tools repository)**
   a. In the HPOM for Windows console, expand **Tools > SiteScope Tools**. In the right pane, right-click the **Drill Down to SiteScope** tool and select **All Tasks > Launch Tool**.
   b. In the Edit Parameters dialog box, select the monitor, group, or SiteScope Server service that you want to view, and click **Launch**.
   c. The SiteScope user interface opens displaying the selected monitor, group, or default Dashboard view (if SiteScope Server service was selected).

Chapter 8: How to Enable the Drill Down to SiteScope Tool on HPOM for UNIX/Linux/Solaris

This task describes how to enable the Drill Down to SiteScope tools on the HPOM for UNIX/Linux/Solaris management server. This tool enables you to open the SiteScope user interface from events or from the monitor or group service that was discovered by the monitor discovery policy and added to the HPOM Service Navigator.

Note: This task is part of a higher-level task. For details, see "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19.

1. **Prerequisites**

   The Monitor Discovery policy must be enabled and deployed on the SiteScope Server node on HPOM.

   For task details, see "How to Enable the SiteScope Monitor Discovery Policy" on page 36.

2. **Install the Drill Down to SiteScope tools on the HPOM for UNIX/Linux/Solaris server**

   a. Log on to the HPOM for UNIX/Linux/Solaris server machine as an Administrator.

   b. Open a command shell and create a new directory by typing:

   ```
   # mkdir -p /opt/OV/newconfig/SiteScope
   ```

   c. Change to the SiteScope directory by typing:

   ```
   cd /opt/OV/newconfig/SiteScope
   ```

   d. Copy the **DrillDownToSIS.tar** file from the **<SiteScope root>\tools\OMIntegration\DrillDownTool\ForOMX** folder to **/opt/OV/newconfig/SiteScope** on the HPOM server machine.

   e. Extract the .tar file to the current directory by typing:

   ```
   # cd /opt/OV/newconfig/SiteScope
   # tar -xvf DrillDownToSIS.tar
   ```

   f. Upload the Drill Down to SiteScope tools to the HPOM server by typing:

   ```
   # cd /opt/OV/bin/OpC/
   # opccfgupld -replace -subentity /opt/OV/newconfig/SiteScope/ DrillDownToSIS
   ```

   g. The Drill Down to SiteScope tools are available on the HPOM Administrator user interface under **Browse > All Tool Groups**.

   h. Assign **Drill Down to SiteScope tools** to the **opc_adm** user.

- Click **Action > Assign to User/Profile...**
- Select **All Users > opc_adm** and click **OK**.

i. Update the HPOM user interface by selecting **File > Reload Configuration**.

j. The Drill Down to SiteScope tools are available on the HPOM server under **Tools > Drill Down to SiteScope tools**.

3. **Launch the tool (from the SiteScope service)**

a. In the HPOM Administrator user interface, right-click the SiteScope service (server, group, or monitor), select **Start > Tools > Drill Down to SiteScope tools > Drill Down to SiteScope service**, and select the tool according to the service type selected.

b. The SiteScope user interface opens displaying the selected monitor, group, or default SiteScope Dashboard view.

4. **Launch the tool (from an event)**

a. In the HPOM Administrator user interface, right-click an event and select **Start > Drill Down to SiteScope tools > Drill Down to SiteScope event**.

b. The SiteScope user interface opens displaying the selected monitor that send the event.

Chapter 9: How to Enable the SiteScope Monitor Discovery Policy

This task describes how to enhance the SiteScope integration with HPOM by enabling HPOM Service Navigator to view SiteScope groups and monitors in HPOM service maps.

Note:

- This task is part of a higher-level task. For details, see "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19.
- HPOM 9.0 for Windows 64-bit consoles support the services tree view with patch OMW_00132 or later.

1. **Copy policy files to the instrumentation folder**

   On the SiteScope server:

   - For Windows: Copy the **discoverSiteScope.bat** file from the **<SiteScope root directory>\integrations\om\bin** folder to the **%OvDataDir%\bin\instrumentation** folder.
   - For Linux, UNIX, Solaris: Copy all files from **/opt/HP/SiteScope/integrations/om/bin/*** to the **/var/opt/OV/bin/instrumentation** folder.

     Note: All relevant policy files can be found in the **<SiteScope root directory>\tools\OMIntegration\SiteScopeMonitorDiscoveryPolicy\SiS_Discovery_policy_3.0** folder.

2. **Upload the policy to the HPOM server (for HPOM for Windows servers)**

   Prerequisites:

   - HPOM for Windows 8.16 (or an equivalent patched 8.10 server) or 9.10, and sufficient user rights (typically, Administrator).
   - All uploads are performed using the HPOM for Windows command line tool **ovpmutil** which is normally in the environment path.

   To upload the policy to the HPOM server:

   a. Open a command prompt, and navigate to the folder where the SiteScope Discovery 3.0 server components are located. For example, C:\temp\SiS_Discovery_3.0:

   ```
   cd C:\temp\SiS_Discovery_3.0\ForServer
   ```

   b. Upload the Service Model using **ovpmutil**:

   ```
   ovpmutil cfg svt upl .\DiscoverSiteScope.mof
   ```

The Service Model is displayed in the HPOM Service Type Configuration Editor (under **Application Services > SiteScope**).

c. Upload the SiteScope monitor discovery policy using **ovpmutil** and the provided index file:

```
ovpmutil cfg pol upl .\PolicyConfig_77BFF2F6-38BD-45B3-BEA9-E237C55F7877.xml
```

The policy is now available in the HPOM server policy repository under **Policy management > Policy groups**.

3. Upload the policy to the HPOM server (for HPOM for Linux, UNIX, Solaris 9.x servers)

a. Upload the HPOM Service Model to the HPOM management server. Open a command shell and type:

```
/opt/OV/bin/OpC/utils/mof_cfgupld.sh /opt/HP/SiteScope/tools/\
SiS_Discovery_policy_3.0/ForServer/DiscoverSiteScope.mof
OMIntegration/SiteScopeMonitorDiscoveryPolicy/\
```

(The .mof file is located in the **<SiteScope>/tools/OMIntegration/SiteScopeMonitorDiscoveryPolicy/SiS_Discovery_policy_3.0/ForServer** folder.)

b. Upload the policies by typing in a command shell:

```
/opt/OV/bin/OpC/utils/opcpolicy -upload dir=/opt/HP/SiteScope/\
tools/OMIntegration/SiteScopeMonitorDiscoveryPolicy/\
SiS_Discovery_policy_3.0/ForServer
```

c. Assign the policies to the node, and deploy to the SiteScope node by typing in a command shell:

```
# /opt/OV/bin/OpC/utils/opcnode -assign_pol node_name=<NODENAME> net_
    type=NETWORK_IP pol_name= "SiteScope Discovery" pol_type=svcdisc
```

4. Set the Schedule Interval

You can set the schedule interval for running the SiteScope monitor discovery policy on the HPOM agent in the HPOM for Windows console.

a. Select **Policy management > Policy groups > SiteScope Discovery**. In the right pane, right-click **SiteScope Discovery** and select **All Tasks > Edit**.

b. In the Service Auto-Discovery policy editor, select the **Schedule** tab and specify an interval for running the SiteScope monitor discovery policy on the HPOM agent in the HPOM for Windows console.

By default, the SiteScope monitor discovery policy runs every 5 minutes. You can change this frequency

5. Deploy the policy

Prerequisites:

- The Operations Agent is running and connected (for details, see "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19).

- The SiteScope server to be integrated is set up as an HPOM managed node, and a certificate has been granted. For details, see "Accept the agent connection request on the HPOM management server or BSM Gateway/Web Processing server" on page 24.
- The SiteScope monitor discovery policy has been uploaded to the **SiteScope Discovery** policy group (for details, see "Upload the policy to the HPOM server (for HPOM for Windows servers)" on page 36 or "Upload the policy to the HPOM server (for HPOM for Linux, UNIX, Solaris 9.x servers)" on the previous page).

To deploy the policy for HPOM for Linux, UNIX, Solaris 9.x servers:

Open a command shell and type: `# opcragt -dist <NODENAME>`

To deploy the policy for HPOM for Windows servers:

a. Right-click the **SiteScope Discovery** policy and select **All Tasks > Deploy on**.

b. In the Deploy Policies on dialog box, select the SiteScope Server OM node from the available managed nodes, and click **OK**. The deployment status is displayed in **Deployment jobs** in the OM Console.

c. To view the policy inventory of the node, right-click the SiteScope Server OM node under **Nodes**, and select **View > Policy Inventory**.

d. The policy inventory is displayed in the right pane, showing all policies deployed to the node.

6. Update Discovery Policies when SiteScope uses SSL

When discovery policies are activated and SiteScope uses an SSL connection, you need to update the policies batch file with the trust store password and keystore password and run the policy again.

a. Open **<SiteScope root directory>\integrations\om\bin\run_api_call_om.bat** in a text editor and replace the line:

```
%JAVA_LOCATION%\java.exe -Xmx512M -classpath %CLASS_PATH% %*
```

With this one (enter the values of `clientTrustStore_path`, `clientKeystore_path`, `trustStorePass`, and `keyStorePass`):

```
%JAVA_LOCATION%\java.exe -Xmx512M
-Djavax.net.ssl.keyStore=%clientKeystore_path%/clientKeystore
-Djavax.net.ssl.keyStorePassword=$keyStorePass
-Djavax.net.ssl.trustStore=%clientTrustStore_path%/clientTrustStore
-Djavax.net.ssl.trustStorePassword=$trustStorePass
-classpath %CLASS_PATH% %*
```

b. Run the policy again.

7. Manually run the Monitor Discovery policy - optional

For testing or debugging purposes, it is useful to run the discovery manually. This can be done using the **ovagtrep** command line tool on the SiteScope server HPOM agent node where the policy is running.

To do so, run the following commands:

a. To force execution of the policy, run the command:

```
ovagtrep -run "SiteScope Discovery"
```

b. To force submittal to server, run the command:

```
ovagtrep -publish
```

c. For troubleshooting, use the **System.txt** file in the **%OvDataDir%\log** folder.

8. **Drill down to the SiteScope user interface from HPOM - optional**

You can also use the Drill Down to SiteScope tool to enable opening the SiteScope user interface from the monitor or group service that was discovered by the monitor discovery policy and added to the HPOM Service Navigator.

For details on enabling the tool for HPOM for Windows, see "How to Enable the Drill Down to SiteScope Tool on HPOM for Windows" on page 32.

For details on enabling the tool for HPOM for UNIX/Linux/Solaris, see "How to Enable the Drill Down to SiteScope Tool on HPOM for UNIX/Linux/Solaris" on page 34.

9. **Troubleshooting**

- You can check the following files:
  - **System.txt** file in the **<SiteScope Server>\%OvDataDir%\log** folder (for Linux: **<SiteScope Server>/var/opt/OV/log**).
  - **agtrep.xml** file in **<SiteScope Server>\%OvDataDir%\datafiles** folder (for Linux: **<SiteScope Server>/var/opt/OV/datafile**) to see the discovered instances the agent knows about.
  - **<HPOM Server>\%OvShareDir%\server\log\OvSvcDiscServer.log** to see what the HPOM server receives.
- See "Node Discovery and Monitor Discovery Troubleshooting" on page 64.

Chapter 10: How to Configure Common Event Mappings for HPOM or BSM

This task describes how to use Common Event Mappings to configure event mappings for monitors and alerts. This is the mapping between SiteScope runtime data and the values of event attributes that will be sent.

1. **Prerequisites**
   - To create or make changes to event mappings, you must be a SiteScope administrator user, or a user granted **Add, edit or delete common event mappings** permissions. For details on user permissions, see the section on user management preferences in the Using SiteScope Guide in the SiteScope Help.
   - To select an event mapping when configuring an alert or a monitor instance:
     - The Operations Agent must be installed and connected to an HPOM or BSM server. For details, see How to Enable SiteScope to Send Events to HPOM or Operations Management.
     - Event integration must be enabled in the Operations Manager Integration dialog box (In **Preferences > Integration Preferences > HP Operations Manager Integration**. For details, see "Enable SiteScope to send events to HPOM or Operations Management" on page 26.
2. **Configure the alerts or monitor instances**

   You configure the alerts or monitor instances that, where triggered, create the relevant events in the event system.

   For task details, see the alerts or monitors section in the Using SiteScope Guide in the SiteScope Help.
3. **Configure the event mappings for an alert or monitor instance**

   You configure an event mapping to map an alert or monitor instance to the corresponding event attributes. You can create several mappings for each type of alert or monitor.
   - You configure alerts from the **Alerts** tab > **New/Edit Alert > HP Operations Manager Integration Settings > Event mapping**.
   - You configure a monitor instance from monitor **Properties** tab > **Event Mapping Settings**.

   For each alert or monitor instance, you can use the default event mapping associated with the monitor or alert, select a different event mapping (if any exist), or create a new event mapping in Common Event Mappings. Alternatively, for alerts, you can use the event mapping template associated with the monitor that triggered the alert.

   To create or edit a mapping:

a. In the New/Edit Event Mappings dialog box, click the **New Event Mapping**  button, or select an existing event and click the **Edit Event Mapping**  button.

b. In the Main Settings panel, enter a name to identify the common event and a description.

c. In the **Common Event Model Settings - General** tab, you can use the default settings, or edit them as necessary. For details, see "Common Event Model Settings - General Tab" on page 52.

d. Use the **Common Event Model Settings - Custom Attributes** tab to add attributes which provide additional information about the event that is not provided in any of the other common event attributes. A custom attribute consists of a key and a value (both are strings). The value can be any string and is used by the common event mapping as any other value. For details, see "Common Event Model Settings - Custom Attributes Tab" on page 56.

4. ## Results

You can view the events corresponding to the triggered alerts or changes in a monitor's metric status in the Event Console in HPOM, or in Operations Management in BSM (if you have an Event Management Foundation license).

If Operations Management is not part of your BSM installation, you can view events that affect CI status using a health indicator in Service Health.

For troubleshooting relating to the HP Operations agent installation, event integration setup, sending events, and with node and monitor discovery, see "Troubleshooting Event Integration Issues" on page 58.

Chapter 11: Properties Available in Alerts, Templates, and Events

The following properties can be found or used in SiteScope alerts, alert and email templates, and common event mappings for sending events to management consoles.

This section includes:

Alerts, Alert Template, and Event Properties

The following is a list of the common properties found in SiteScope alerts, alert templates, and attributes used in common event mappings (for monitor and alert events).

Note:

- Attributes in event mappings have an additional left ("<") and right (">") angle bracket which is not shown in the table below.
- ✔ indicates whether properties can be used in alerts and/or common event mappings (associated with a monitor or an alert).
- Where properties are included in specific alert templates, the relevant templates are listed in the **Included in Alert Template** column.

Available Properties	Description	Included in Alert Templates	Alerts	Events	
				Monitor	Alert
<alertHelpURL>	URL of the SiteScope help including the alert topic.	NoDetails Traceroute WithDiagnostic	✔	✔	✔
<alert::name>	The name of the alert.		✔		
<alert::id>	The alert ID.		✔		
<alert::description>	Text description for the alert definition.		✔		
<alert::disable Description>	Description of the purpose of the disable operation.		✔		
<alert::actionID>	The ID for the alert action.		✔		
<alert::actionName>	The name of the alert action.		✔		

Available Properties	Description	Included in Alert Templates	Alerts	Events	
				Monitor	Alert
<all>	All of the properties of the monitor.		✔	✔	✔
<allThresholds>	Returns all the thresholds in the monitor in the email alert.		✔	✔	✔
<analyticsResults>	Shows a summary of analytics results, which includes: • Name of analyzed monitor and name of analytics object. • All correlation results or top 500 best fitting ones per analyzed (source) monitor metric. • For an alert triggered by a static threshold: metrics that are in the status for which the alert was triggered. • For an alert triggered by Analytics: metrics of the monitor which are out of the baseline sleeve.	AnalyticsMail			
<bacMonitorID>	The monitor's BSM ID.		✔		
<bacSessionID>	The BSM profileID.		✔		
<category>	The monitor category.	Typical	✔	✔	✔
<changedToErrorOnly>	Shows only the metrics that have changed to error status.		✔	✔	✔
<changedToWarningOnly>	Shows only the metrics that have changed to warning status.		✔	✔	✔
<changedToGoodOnly>	Shows only the metrics that have changed to good status.		✔	✔	✔
<classifier> (or _<classifier>)	Returns the first threshold in the monitor in the email alert.		✔	✔	✔
<currentTime>	The time that the alert is run.		✔	✔	✔
<customerId>	Customer ID for SAAS environment		✔	✔	✔
<_description>	Displays the description entered in the **Report description** field of the monitor's General Settings that makes it easier to understand what the monitor does. This description is displayed on each bar chart and graph in Management Reports.		✔	✔	✔
<diagnosticText>	Calculates a string from other properties that the monitor is able to return. The translation can be different for different types of monitors because every monitor can choose a different value combination for this property.	Default User NoDetails WithDiagnostic	✔	✔	✔
<diagnosticTrace Route>	This tag is filled only for warning and error conditions when the Traceroute Email template is used with the URL Content monitor.	Traceroute WithDiagnostic	✔	✔	✔
<errorCounterOnly>	List of the monitor counters in error status (returns counter name only).		✔	✔	✔

Available Properties	Description	Included in Alert Templates	Alerts	Events	
				Monitor	Alert
<errorOnly>	List of the monitor counters in error status (returns counter name and counter value).	Typical	✔	✔	✔
<firstgroupdescription>	Partial group description. Only the first description from several different ones.		✔	✔	✔
<fullgroupdescription>	Full group's description.		✔	✔	✔
<FullGroupId>	Full path from the SiteScope root directory to the group, exclude\SiteScope.		✔	✔	✔
<fullMonitorName>	Full path from the SiteScope root directory to the monitor. For example, \SiteScope\MyGroup\MyCPUMonitor.		✔	✔	✔
<goodCounterOnly>	List of the monitor counters in good status (returns counter name only).	Typical	✔	✔	✔
<goodOnly>	List of the monitor counters that are in good status.	Typical	✔	✔	✔
<group>	Name of the group in which the monitor is located.	AllErrors AnalyticsMail Default Default User lr-Default_mail_ template NoDetails NTEventlogt PagerMail ShortMail Traceroute Typical WithDiagnostic XMLMail	✔	✔	✔
<groupdescription>	Full group's description and group's parent description.		✔	✔	✔
<groupID>	ID of the group.	Default Typical WithDiagnostic XMLMail	✔	✔	✔
<group.propertyname>	Property of the group in which the monitor is located. Group properties that can be used in the tags include: `_externalId`, `_dependsCondition`, `_name`, and `_topazId`.		✔	✔	✔
<group.parent. propertyname>	Property of the parent group of the group in which the monitor is located. Group properties that can be used in the tags include: `_externalId`, `_dependsCondition`, `_name`, and `_topazId`.		✔		
<_httpPort>	Port number used to access SiteScope (as in Email Report Properties)	NTEventlog	✔	✔	✔

Available Properties	Description	Included in Alert Templates	Alerts	Events	
				Monitor	Alert
<id>	Current monitor's ID number. It identifies the monitor within the group	XMLMail	✔	✔	✔
<mainParameters>	List of the main monitor properties that are set as parameter.	Default Default User NTEventlog WithDiagnostic	✔	✔	✔
<mainStateProperties>	List of main monitor properties that are set as state properties. These are the result statistics that are shown on the Reports.	Default Default User NTEventlog WithDiagnostic	✔	✔	✔
<matchedLine>	Use for Multi Log monitor when the "For each log entry matched" option is selected in **Run alerts**. When this property is used, the monitor status displays the whole line instead of just the matched content and the file where it was found.		✔		
<monitorClass>	The monitor's class name.			✔	✔
<monitorDrilldownUrl>	Creates a hyperlink in the event to the monitor URL.		✔	✔	✔
<monitorDrilldown Url Secured>	Creates a hyperlink in the event to the monitor URL without login information in the link itself.		✔	✔	✔
<_monitorDescription>	Displays the description of the monitor entered in the **Monitor description** field of the monitor's General Settings.		✔	✔	✔
<monitorName>	Name of the monitor. (same as "<name>")		✔	✔	✔
<<monitorServiceId>>	Enables customizing the service name that is sent from SiteScope events to HPOM by entering the value of the monitor service ID. This is useful for relating the SiteScope monitor with the HPOM Service Name.		✔	✔	✔
<monitorType>	The type of monitor, such as CPU.		✔	✔	✔
<monitorTypeDisplay Name>	The Monitor's class Topaz name		✔	✔	✔
<monitorUUID>	Monitor's UUID		✔	✔	✔
<mountName>	Returns mount names. This is applicable when monitoring remote UNIX servers while using the Dynamic Disk Space monitor.		✔	✔	✔
<multiViewUrl>	Creates a hyperlink to the SiteScope Multi-View URL.		✔	✔	✔

Available Properties	Description	Included in Alert Templates	Alerts	Events	
				Monitor	Alert
<name>	Name of the monitor. (same as "<monitorName>")	AnalyticsMail Default Default User lr-Default_mail_ template NoDetails NTEventlog PagerMail ShortestMail ShortMail ShortSubject Traceroute Typical WithDiagnostic XMLMail	✔	✔	✔
<newSiteScopeURL>	URL of the SiteScope server.	Default Typical	✔	✔	✔
<processtext>	Process Stats, only relevant if the object has a machine.		✔	✔	✔
<remoteMachineName>	Displays the name of the configured remote server used by the monitor.		✔	✔	✔
<sample>	Sample #	AllErrors AnalyticsMail Default Default User NoDetails NTEventlog PagerMail ShortMail Traceroute Typical Typical.mail WithDiagnostic XMLMail	✔	✔	✔
<sitescopeurl>	URL of the SiteScope server with extra account information.		✔	✔	✔
<siteScopeBaseUrl>	URL of the SiteScope server in a different format.		✔	✔	✔
<siteScopeHost>	URL of the SiteScope host name.		✔	✔	✔
<secondaryParameters>	Lists the main state properties and other internal properties.		✔	✔	✔

Available Properties	Description	Included in Alert Templates	Alerts	Events	
				Monitor	Alert
<secondaryState Properties>	Lists the main state properties and other internal properties.		✔	✔	✔
<sitescopeURL>	The URL to the main page of SiteScope for admin access.	AllErrors Default User NoDetails Traceroute WithDiagnostic	✔	✔	✔
<sitescopeuserurl>	The URL to the main page of SiteScope for user access.		✔	✔	✔
<state>	Status string reported by the monitor. (same as stateString)	AllErrors AnalyticsMail Default Default User lr-Default_mail_ template NoDetails PagerMail ShortestMail ShortMail ShortSubject Traceroute Typical WithDiagnostic XMLMail	✔	✔	✔
<tag>	Tags of the monitor (if exists).	AnalyticsMail Default Default User lr-Default_mail_ template NoDetails NTEventlog PagerMail ShortestMail ShortMail ShortSubject Traceroute Typical WithDiagnostic XMLMail	✔	✔	✔

Available Properties	Description	Included in Alert Templates	Alerts	Events	
				Monitor	Alert
<tag:[tagName]>	Displays the value or values of the Search/Filter tag with the [tagName] assigned to the monitor that triggered the alert. **Example:** You have a tag named `AppServer` with value `Apache` assigned to a monitor, and you include **<tag:AppServer>** in the alert template configured for that monitor. If an alert is triggered, the new property is replaced with `Apache` in the alert text.		✔	✔	✔
<targetHost>	Name of the target host.		✔	✔	✔
<targetIP>	IP of the target host.		✔	✔	✔
<targetIPAsHEX>	IP of the target host in HEX fomat.		✔	✔	✔
<targetIPVersion>	Retrieves monitor host IP version (IPV6 or IPV4).		✔	✔	✔
<templateDeployPath>	Displays the path of the template group from which the monitor was deployed.		✔	✔	✔
<time>	Time that the monitor completed the last run.	AllErrors AnalyticsMail Default Default User lr-Default_mail_ template NoDetails NTEventlog Traceroute Typical WithDiagnostic XMLMail	✔	✔	✔
<time-date>	The date portion of the time that the monitor completed.		✔	✔	✔
<time-time>	The time portion of the time that the monitor completed.		✔	✔	✔
<warningCounterOnly>	List of the monitor counters in warning status (returns counter name only).		✔	✔	✔
<warningOnly>	List of the monitor counters in warning status (returns counter name and counter value).	Typical	✔	✔	✔
<unifiedConsoleUrl>	Opens the Ops View in the Unified Console, which displays Multi-View and the Event Console.			✔	✔
<_webserverAddress>	IP address for the SiteScope Server (as in Email Report Properties)	NTEventlog	✔	✔	✔

Common Event Template Properties

The following metric specific properties are resolved from the monitor's counter data and should be used in the Common Event Template for monitor events only.

These properties are relevant for monitor events because they are triggered by a specific metric change. They are not relevant for alert events because they are triggered by a status change, which is a single state that can be resolved from several metric changes.

Available Properties	Description
<metric>	The name of the counter that triggered the alert.
<metricValue>	The ETI value associated with the threshold that has been crossed.
<newStatus>	Current status of the metric.
<oldStatus>	Previous status of the metric.
<etiValue>	The ETI value associated with the threshold that has been crossed.
<etiType>	The ETI type associated with the counter that crossed the threshold that created the event.
<thresholdCrossed>	The display name of the threshold setting that was crossed.
<thresholdCrossedFull>	The full string representation of the threshold setting that was crossed. It also contains the ETI value and the status associated with this threshold, which uniquely identifies the threshold.
<severity>	Severity of the occurrence that the event relates to.
<ciHint>	Information about the CI that is related to the event. This attribute is for providing one or several hints that enables the event processing to find the correct "related CI".

Available Properties	Description
<subCiHint>	Information used to identify a subcomponent of a CI. This CI subcomponent is used to calculate an aggregated status within BSM's Service Health for selected CIs. If an HI is populated by events from multiple components, you can specify a component name in this field in order to ensure the correct calculation of the HI state. **Example:** If you have a Computer CI with two CPUs, cpu #1 and cpu #2, events from both CPUs will be sent to the same CPU Load HI. By default, the events will overide each other and create an incorrect HI state. To prevent this, you can populate ComponentCi with values "cpu #1" and "cpu #2" which will cause the HI state to be calculated as an aggregated state between the two events.
<alertName>	The name of the alert.

Microsoft Windows Event Log Monitor Properties

The following properties can only be used in the Microsoft Windows Event Log monitor. They can be used in SiteScope alerts, alert templates, and common event mappings (monitors and alerts).

Available Properties	Included in Templates
<eventCategory>	NTEventlog
<eventID>	NTEventlog
<eventMachine>	NTEventlog
<eventSource>	NTEventlog
<eventType>	NTEventlog

Email Report Properties

The following properties are applicable to the email templates stored in the **<SiteScope>\templates.history** directory:

Available Properties	Description
_httpPort	Port number used to access SiteScope
_webserverAddress	IP address for the SiteScope Server
basicAlertSummary	Basic information on what alerts have been triggered

Available Properties	Description
detailAlert Summary	More detailed information on alerts
reportIndexURL	URL to the index page for the management report
reportPeriod	Time period for this report
reportURL	URL to the HTML version of the management report
summary	Summary and measurement information
textReportURL	URL to the comma-delimited file generated by SiteScope
userReportIndexURL	URL to the index page for a user-accessible report
userTextReportURL	URL to the comma-delimited file generated by a user-accessible report
userXMLReportURL	URL to the XML file generated by a user-accessible report
xmlReportURL	URL to the XML file generated by the management report

Chapter 12: Common Event Mappings User Interface

The New/Edit Event Mappings dialog box enables you to create new common event mappings or edit existing mappings. These are mappings between SiteScope runtime data and the attribute values that are used for sending events. Common event mappings are used when configuring the Operations Manager event integration and the Generic Event integration.

This section includes:

Common Event Model Settings - General Tab

User interface elements are described below:

UI Element	Description
General	
Title	Descriptive text describing the occurrence represented by the event. This should include information about what threshold has been crossed (or other trigger conditions), and the current values. **Default value:** • For metric status change: Metric '<<metric>>' changed status from '<<oldStatus>>' to '<<newStatus>>' • For alerts: Alert '<<alertName>>' was fired on monitor '<<fullMonitorName>>' status change **Tip:** Since the text is typically shown within a single line in the event browser, it is recommended to put the most relevant information at the beginning.
Description	Additional information describing the event. **Default value:** • For metric status change: Metric '<<metric>>' crossed '<<thresholdCrossed>>' with value '<<metricValue>>' • For alerts: Monitor '<<fullMonitorName>>' changed status from '<<oldStatus>>' to '<<newStatus>>'

UI Element	Description
Severity	Severity of the occurrence related to the event. The severity level can be Unknown, Normal, Warning, Minor, Major, or Critical. **Default value:** <<severity>>. The <<severity>> attribute is replaced by the severity in the **Indicator State and Severity** field in the Threshold Settings for the selected monitor metric.
Category	Value used for organizing or grouping events by monitor type. **Default value:** <<monitorType>> **Examples:** Database, Application, J2EE
Subcategory	Value used for organizing or grouping events that have the same category. **Default value:** • For metric status change: <<metric>> • For alerts: <<fullMonitorName>> **Example:** Oracle
Log only	If **True** is selected, enables submitting an event that goes directly into the history event browser as a closed event. Such an event goes through the complete event processing, but has its **Life Cycle State** set to close from the beginning. Typical examples are events that result in resetting an indicator to a normal or good state, or an event signaling that a previous problem no longer exists (where the problem was reported in another event). If **True for normal severity** is selected, all messages forwarded from SiteScope to HPOM are sent to the **Acknowledged** message browser (instead of the **Active** message browser) if their severity is normal. This prevents the **Active** message browser becoming unnecessarily cluttered with normal severity messages. **Default value:** False
Event Type Indicator	Link between the event and the indicator so that information about the indicator can be updated as a result of submitting the event. **Default value:** • For metric status change: <<etiType>>:<<etiValue>>:<<metricValue>> • For alerts: <<etiType>>:<<etiValue>> **Example of metric status change:** CPU Load:High:90 **Note:** This field is mandatory for updating the indicator. It is recommended not to change the template value of this attribute.

UI Element	Description
Correlation	
Key	A unique string representing the type of event that occurred. Two events can have the same key if both events represent the same situation in the managed environment. Duplicate events are discarded after the number of duplicate events is increased in the "Number of Duplicates" count. **Default value:** • For metric status change: <<siteScopeHost>>:<<monitorUUID>>:<<metric>>:<<etiValue>>: <<severity>> • For alerts: <<siteScopeHost>>:<<monitorUUID>>:<<alertName>>:<<etiValue>> **Example of metric status change:** labmachine1:OMEventIntegration:CPU Utilization on SiteScope Server: utilization:Good
Submit close key condition	Enables the close key pattern to be evaluated by the event subsystem. If selected, enter the pattern in the **Close key pattern** box below. **Default value:** Selected
Close key pattern	(This box is available only if **Submit close key condition** is selected.) Enables the event that is sent to automatically close all the events whose key attribute matches this expression. It is recommended that this field contain the same value as in the Key field. **Note:** SiteScope event integration policy always adds "<*>" to the end of your close key pattern. The "<" and ">" signs cannot be used here since that they cannot be interpreted by the log file policy. **Default value:** • For metric status change: <<siteScopeHost>>:<<fullgroupid>>:<<monitorName>>:<<metric>> • For alerts: <<siteScopeHost>>:<<monitorUUID>>:<<alertName>> **Example:** labmachine1:OMEventIntegration:CPU Utilization on SiteScope Server:utilization<*>
Advanced Parameters	

UI Element	Description
CI hint	Information about the CI that is related to the event. This attribute is used for providing hints to enable the event processing to find the correct related CI (RTSM ID of the related CI). **Default value:** <<ciHint>>. The value in this field varies, depending on whether SiteScope is connected to BSM or HPOM. This field is not editable.
Host hint	The target host being monitored by the monitor that triggered the event. The value is translated to the legacy node attribute in HPOM. If the node does not exist in HPOM, the event will be lost. **Default value:** <<targetHost>> **Examples:** • IPv4: 15.15.12.13, • DNS: host1.hp.com
Generating source hint	Information about the monitoring application and the corresponding probe/agent that is responsible for creating the event. **Default value:** SiteScope@@<<siteScopeHost>> **Example:** SiteScope@@host1.hp.com
Attributes	
<Attributes list>	Displays the list of available attribute variables. You can add an attribute by dragging it from the **Attributes** list to the selected text box, or select the cell in which to copy the selected attribute, and click Ctrl+I. For a description of the available attribute variables, see "Properties Available in Alerts, Templates, and Events" on page 42.

Common Event Model Settings - Custom Attributes Tab

User interface elements are described below

UI Element	Description
	Enables creating a new custom attribute for the event. Each event can have any number of custom attributes. • **New Key.** Adds a new line to the table, enabling you to add a name and value for the attribute. • **Known Key.** Opens a submenu with the known keys as options. You can select the relevant key. A new row opens in the Name/Value table, with the name of the selected key in the Name column. You can then enter the value of the key in the corresponding Value column.
	**Delete Custom Attribute.** Deletes the selected custom attribute from the table.
Name and Value	Each event can have any number of custom attributes. Custom attributes can be used to provide additional information with the event that is not provided in any of the other common event attributes or that is contained in any of the other attributes. Each custom attribute is a **Name-Value** pair, where you enter the name of the attribute in the **Name** field and the value of the attribute in the **Value** field. This feature may be used when you manage the environment of multiple customers using one instance of the product. The multiple customers might be handled by a custom attribute object. **Example:** Name = "cma1" ; Value = "XYZ Company" **Note:** Make sure that the name of the attribute you are defining is unique and does not already exist in the attributes list.
Attributes	

UI Element	Description
<Attributes list>	Displays the list of available attribute variables. You can add an attribute by dragging it from the **Attributes** list to the selected box, or select the cell in which to copy the selected attribute, and click Ctrl+I. For a description of the available attribute variables, see "Properties Available in Alerts, Templates, and Events" on page 42. **HP CDA Event Mapping template** This is an out-of-the-box template that is specially configured for CDA (Continuous Delivery Automation). CDA is a policy-based platform that provides infrastructure provisioning in hybrid cloud environments. CDA integrates with SiteScope to deploy SiteScope monitors and receive events from them. Monitoring status based on the events received is available in the CDA user interface. For more details on CDA, refer to the CDA documentation. The following attributes are included in the Custom Attributes tab for the HP CDA Event Mapping template which is included by default in Common Event Mappings: • **<<TemplateDeployPath>>**. Displays the full path to the template group from which the monitor was deployed. • **<<monitorServiceId>>**. See Service ID below. • **<<monitorDrilldownURL>>**. Creates a hyperlink in the event to the monitor URL. • **<<newStatus>>**. Current status of the metric.
Service ID	Enables customizing the service name that is sent from SiteScope events to HPOM by entering the value of the monitor service ID. This is useful for relating the SiteScope monitor with the HPOM Service Name. **Default value:** <<monitorServiceId>>

Chapter 13: Troubleshooting Event Integration Issues

This section contains notes and limitations, and provides troubleshooting when using the Operations Manager integration to send events directly to the HPOM management server or to Operations Management in BSM.

This section includes:

Notes and Limitations

- Upgrades for SiteScope-HPOM event integrations earlier than SiteScope 11.00 are not supported.
- While SiteScope 10.x versions support HPOM event integration, events generated in SiteScope versions earlier than 11.00 do not affect Service Health and Service Level Management in BSM 9.0x.
- If SiteScope is installed on the same machine as HPOM, when uninstalling SiteScope you should also uninstall the Operations Agent.
- Sending events to HPOM using the Operations Agent is available only when connected to BSM 9.00 or later. Although the earlier HPOM integration solution of installing the HP SiteScope Adaptor on the HPOM management server is supported in earlier versions of SiteScope, it is not supported with SiteScope11.00 or later and should be uninstalled. You should therefore upgrade to the implementation using the Operations Agent.
- If you are having problems activating node discovery or deploying the monitor discovery policy, verify that the SiteScope node system properties are discovered correctly, and fix them if necessary. In the Node Properties dialog box, select the **System** tab and make sure the settings matches you SiteScope node system settings.
- If you are using Operations Manager for Windows 9, patch OMW_00097/98 or later (32-bit/64-bit) is required to support the Node discovery feature without overriding SiteScope node properties.
- If you currently use HPOM with SiteScope and you plan to upgrade HPOM to BSM, you must connect SiteScope directly to BSM to perform the upgrade. This also enables SiteScope to report the topology to BSM. For details on connecting SiteScope to BSM, see section on working with BSM in the Using SiteScope Guide in the SiteScope Help..
- When SiteScope sends an event in which a monitor metric value does not match any of the thresholds, the

indicator severity **Normal** is sent to the HPOM management/BSM Gateway Server.

- When SiteScope is connected to BSM, after a monitor is created on a new host, the event is sent to Operations Management without the value of the related CI (the event is triggered before topology is reported to BSM). To avoid waiting for the next event to be sent, select the **Manually send first event** check box in the monitor's **HP Integration Settings** > **HP Operations Manager Integration Settings**. This action can be performed globally using Global Search and Replace.
- If there are no ETIs from SiteScope in the Operations Management Event Browser, make sure when configuring event integration that the **BSM Service Health affected by** setting in **HP Integration Settings > BSM Service Health Preferences** is set to **Events**. If **Metrics** is selected, status change events reported by SiteScope do not have any influence on CIs in Service Health or Operations Management.
- Events are not closed (relevant to HPOM and BSM) and the indicator status is not cleared (relevant to BSM) if SiteScope stops monitoring in the following instances:
  - The related SiteScope monitor skipped or was disabled/suspended (permanently or by the scheduler)
  - The related SiteScope monitor was deleted
  - SiteScope stops reporting to BSM (for example, if it is disconnected)
- To exclude indicators of disabled monitors from Service Health, Service Level Management, or both, it is recommended to use Downtime Management in BSM 9.0x or later. For details, see the section on downtime management in the BSM Platform Administration Guide in the BSM Help.

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/BSM 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, uninstall the Operations Agent and then install it again (it is also recommended to restart the server).

c. Make sure your HPOM management server or BSM 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. Uninstall 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 BSM, 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://<BSM 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 BSM environment (in BSM 9.00 or later), 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 "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19.
7. Click the **Connect** button, and make sure the command output returns: `opcactivate Info: Successfully activated OVO agent.`

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

   Note: If there is a large time difference (more than 24 hours) between the certificate server and the 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 a BSM server, follow the step for accepting the agent connection request in "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19.
   - 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 HP 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.

Problems Sending 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 59, 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 "Integration Setup Problems" on page 59.
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 HP 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 HP 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 "Problems Sending 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 "How to Enable SiteScope to Send Events to HPOM or Operations Management" on page 19). If it is still not in the log file, contact HP 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 HP 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 BSM.
   - 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 BSM (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.

Node Discovery and Monitor Discovery Troubleshooting

Node Discovery:

- If you are using Operations Manager for Windows 8.1x, patch OMW_00071 is required to support the Node discovery feature in SiteScope-HPOM event integration.
- If you are using Operations Manager for Windows 9, patch OMW_00097/98 or later (32-bit/64-bit) is required to support the Node discovery feature without overriding SiteScope node properties.
- If you are using Operations Manager for Solaris/HP-UX/Linux 9.10, patch 9.10.200 is required to support the Node discovery feature in SiteScope-HPOM event integration.

Troubleshooting problems with Node discovery:

1. Click the **Analyze** button in the HP Operations Manager Integration dialog box. Make sure you see the **SiteScope_Hosts_Discovery policy** installed and enabled.

2. Check that your event configuration is set. Send a test event and make sure you see it in the HPOM Event Console on the SiteScope node.

   New nodes are reported within 5 minutes from the time they started to being monitored by SiteScope monitors.

   The discovery policy runs SiteScope scripts that generate XML consumed by the policy. Each run is logged in the following log: **%OvDataDir%\log\System.txt** (for Linux **<SiteScope Server>/var/opt/OV/log**).

3. You can invoke the process manually, by running the following commands:

```
ovagtrep -run "SiteScope_Hosts_Discovery"ovagtrep -publish
```

Monitor Discovery:

To enable HPOM Service Navigator to view SiteScope groups and monitors in HPOM service maps, follow the configuration instructions in "How to Enable the SiteScope Monitor Discovery Policy" on page 36.

Certificate Requests Do Not Reach the Operations Management Server

Problem: Event integration between SiteScope and BSM could not be created because certificate requests are not reaching the Operations Management server.

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

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

Part 3: Reporting Metrics to HPOM and Operations Management

Chapter 14: Configuring SiteScope to Report Metrics for Use in HPOM or Operations Management

SiteScope makes its metrics data available for use in Performance Manager (the reporting component of HPOM) and Performance Graphing in BSM's Operations Management.

- For **Performance Graphing** in Operations Management, you can use either of the following data sources for reporting data to BSM:
  - Profile database in BSM, as part of the BSM integration (this is the recommended data source).
  - Operations Agent installed on the SiteScope server, as part of the Operations Manager metric integration.

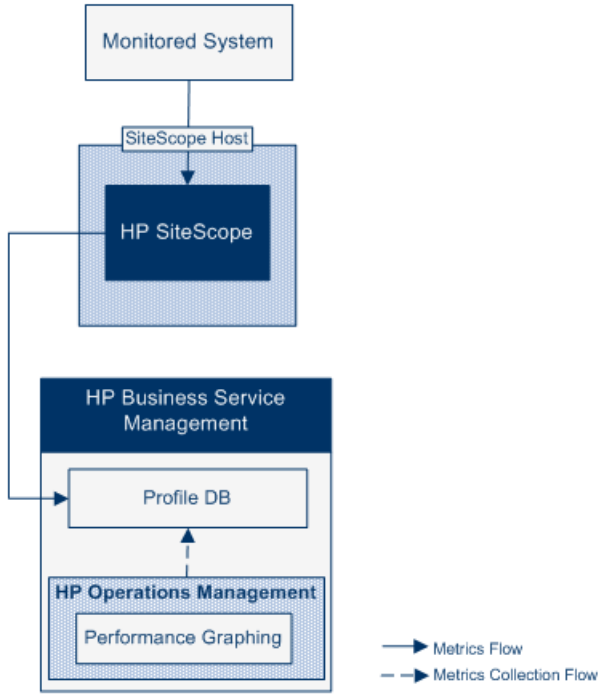
    Note: While reporting metrics data to the Operations Agent is supported for Performance Graphing in this release, HPE plans to stop supporting it in the future, and recommend that you use the BSM profile database method instead.
- For **Performance Manager** in HPOM, you must use the Operations Agent installed on the SiteScope server, as part of the Operations Manager metric integration.

For details on reporting data to BSM using the profile database, see "Reporting Data to the Profile Database in BSM" on the next page.

For details on reporting data to the Operations Agent, see "Reporting Data to theOperations Agent" on page 69.

Reporting Data to the Profile Database in BSM

By default, SiteScope reports metrics data to the profile database in BSM. When a user in Performance Graphing in Operations Management draws or designs a graph, Performance Graphing collects the data from the profile database for the CI monitored by SiteScope, and draws the graph.



The advantages of using a profile database for reporting data to Performance Graphing, include:

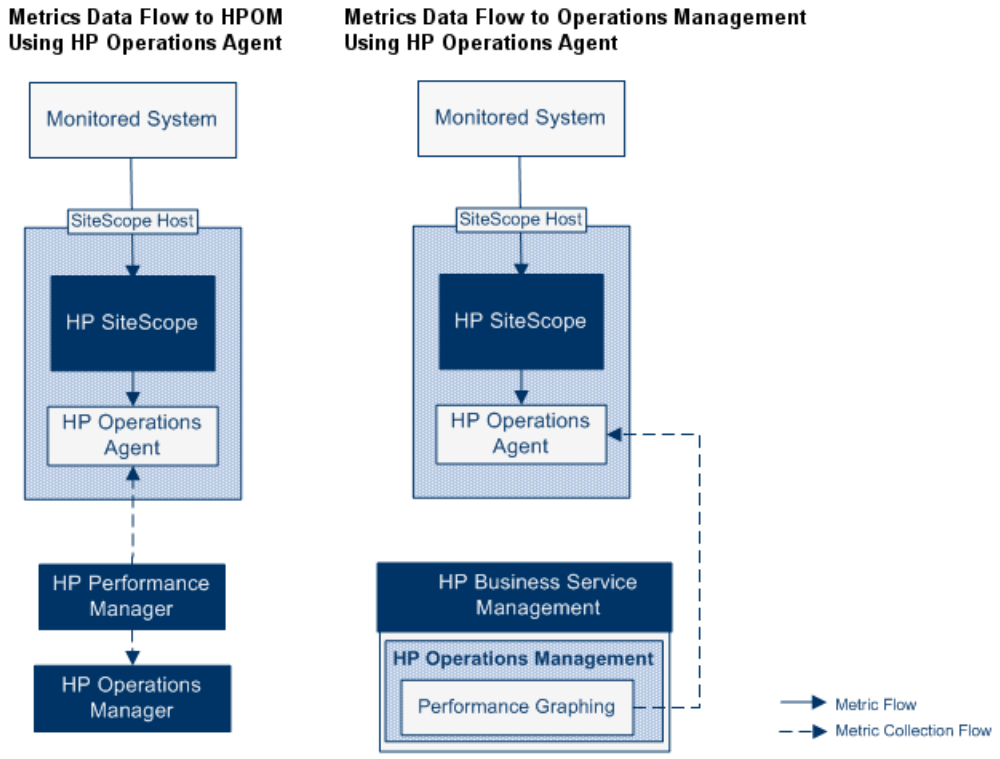
- No additional configuration is required.
- Better performance and scalability than the Operations Agent.
- Easier to troubleshoot than the Operations Agent.

For details on configuring metrics integration using a profile database, see "How to Enable SiteScope to Report Metrics to Profile DB in BSM" on page 71.

Reporting Data to theOperations Agent

SiteScope reports metrics data to the Operations Agent store installed on the SiteScope server. This data can then be made available to Performance Manager (the reporting component of HPOM) and to Performance Graphing (in Operations Management).

Note: While reporting metrics data to the Operations Agent is supported for Performance Graphing in this release, HPE plans to stop supporting it in the future, and recommend that you use the BSM profile database method instead. For details, see "Reporting Data to the Profile Database in BSM" on the previous page. Reporting metrics to the Operations Agent as part of the Operations Manager metric integration is still supported for making metrics available in Performance Manager.



When a user in Performance Manager draws or designs a graph, Performance Manager collects metrics data from the agent data store for the selected node in Performance Manager that is monitored by SiteScope, and draws the graph. Agentless graphing is supported in Performance Manager 9.0 or later. For details on Performance Manager, refer to the Performance Manager documentation. Metrics data collected from SiteScope can also be used in Performance Graphing.

Sizing is important for planning the maximum number of monitors, metrics, and monitors types that can be stored within the SiteScope-HPOM metrics integration. For sizing recommendations, see "Sizing Recommendations for SiteScope-Operations Manager Metrics Integration" on page 82.

Metrics name alignment, the process of aligning metrics names in SiteScope with those used in HPOM or BSM, has been performed for some of the most commonly used monitors. For details, see "SiteScope-Operations Agent Metrics Alignment" on page 78. Performance Manager can graph any metrics (whether aligned or not), and metrics alignment for all possible metrics is not required for viewing the data in Performance Manager.

For details on configuring metrics integration, see "How to Enable SiteScope to Report Metrics to the Operations Agent" on page 74.

Note:

- Metrics integration using the Operations Agent should not be confused with the integration of SiteScope monitor metrics used by the various BSM applications when calculating status for CIs (for example, in Service Health, Service Level Management, and System Availability Management). For details on BSM metrics integration, see the Connecting to a BSM Server section of the Using SiteScope Guide in the SiteScope Help.
- Metrics integration with Performance Manager can be activated regardless of the connection status between the Operations Agent and the HPOM or BSM server, since metrics are collected by the agent.
- The Operations Manager metrics integration is supported by SiteScopes running on Windows and UNIX platforms for HPOM and Operations Management.

Tip: For best practices and troubleshooting for reporting metrics data to BSM and HPOM products using the Operations Agent, see the Integration with BSM and HPOM Best Practices Guide available from the SiteScope Help.

Chapter 15: How to Enable SiteScope to Report Metrics to Profile DB in BSM

This task describes how to enable SiteScope to report metrics data to profile database in BSM.

1. **Prerequisites**
   - Your system must conform to the following requirements:
     - SiteScope version 11.00 or later is installed.
     - For Operations Management, BSM 9.22 or later is installed.
2. **Configure SiteScope to Communicate with BSM**

   SiteScope must be connected to a BSM server, and reporting monitor metrics to BSM should be enabled in HP Integration Settings.

   For details on configuring SiteScope to communicate with BSM, see the section on connecting SiteScope to a BSM server in *Using SiteScope* in the SiteScope Help.

   For details on enabling BSM logging options and topology reporting settings for monitor instances, see the section on HP Integration Settings in *Using SiteScope* in the SiteScope Help.
3. **Select Profile DB as the Data Source in BSM Infrastructure Settings**

   By default, SiteScope reports metrics data to the profile database to make it available to Performance Graphing in BSM's Operations Management.

   To modify the data source setting in BSM in **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:
   - Select **Applications**.
   - Select **Performance Graphing**.
   - In the Performance Graphing table, locate **SiteScope Datasource Name**, and make sure that **Profile DB** is selected.
4. **Results**

   When SiteScope reports metrics to BSM, the data is stored in the profile database.

   When a user in Performance Graphing in Operations Management draws or designs a graph, the metrics data is collected from the profile database.

   A user can select the following in the Performance Perspective page:
   - **Data Sources.** Displays the profile name of the SiteScope CI that should be used by performance grapher.

- **Metric Classes.** Displays the monitor types on the SiteScope CI.
- **Instances.** Displays monitor instances on the SiteScope CI. Instances are in the format: `<SIS profile name>-<full monitor pathname>`.
- **Metrics.** Displays monitor metrics for the selected metric classes (monitor type).

Chapter 16: How to Change Data Source from Profile DB to Operations Agent

This task describes how to change the data source from Profile DB to the Operations Agent to make the data available in HPOM (Performance Manager) and Operations Management (Performance Graphing).

Note: While the Operations Agent is supported for reporting data to Performance Graphing in this release, HPE plans to stop supporting it for reporting metrics data to Performance Graphing in the future, and recommend that you use the profile database method instead. Reporting metrics to the Operations Agent as part of the Operations Manager metric integration is still supported for making metrics available in Performance Manager.

1. **Select HP Operations Agent as the Data Source in BSM Infrastructure Settings**

   Modify the data source setting in BSM in **Admin > Platform > Setup and Maintenance > Infrastructure Settings**:

   - Select **Applications**.
   - Select **Performance Graphing**.
   - In the Performance Graphing table, locate **SiteScope Datasource Name**, and select **Embedded HP Operations Agent**.

2. **Enable SiteScope to report metrics data to the HP Operations agent to make it available in HPOM and Operations Management**

   Perform the steps described in "How to Enable SiteScope to Report Metrics to the Operations Agent" on page 74.

Chapter 17: How to Enable SiteScope to Report Metrics to the Operations Agent

This task describes how to enable SiteScope to report metrics data to the Operations Agent to make it available in HPOM (Performance Manager) and Operations Management (Performance Graphing).

Note: While reporting metrics data to the Operations Agent is supported for Performance Graphing in this release, HPE plans to stop supporting it in the future, and recommend that you use the BSM profile database method instead. For details, see "Reporting Data to the Profile Database in BSM" on page 68. Reporting metrics to the Operations Agent as part of the Operations Manager metric integration is still supported for making metrics available in Performance Manager.

1. **Prerequisites**

- Your system must conform to the following requirements:
  - SiteScope version 11.00 or later is installed.
  - For Operations Management, BSM 9.00 or later is installed.
  - For HPOM, Performance Manager 9.0 or later is installed.

    Note: The node discovery, monitor discovery, and template integration are not supported for all versions of HPOM. For details of the integrations that are supported and of any patch requirements, refer to the Operations Manager (HPOM) Integration Support Matrix in the HP SiteScope Deployment Guide (available from the HPE Software Support site.

- Only a SiteScope administrator user, or a user granted **Edit integration preferences** permissions. can configure the integration. For details on user permissions, see the section on user management preferences in the Using SiteScope Guide in the SiteScope Help.

- The Performance Manager administrator must configure Performance Manager to connect to the SiteScope node where the SiteScope instance is logging data. For details, refer to the Performance Manager documentation.

- (If SiteScope is installed on a Red Hat ES Linux 6.0 64-bit environment) You must install the following dependencies before installing the Operations Agent:
  - Install **compat-libstdc++-33-3.2.3-69.el6.i686.rpm** on the Red Hat Enterprise Linux 6 x64 node.

    Note: To install SiteScope with the Operations Agent on RHEL x64 in graphics mode, you must run the installer with the machine default 64-bit JRE.

    ./<PRODUCT_NAME>_<VERSION>_setup.bin LAX_VM /usr/bin/java $@

For example, if /usr/bin/java points to the 64-bit JRE or JDK:

./HPSiteScope_11.30_setup.bin LAX_VM /usr/bin/java $@

- Install **compat-libstdc++-33-3.2.3-69.el6.ppc64.rpm** on the Red Hat Enterprise Linux 6 PPC node.

You can install the dependencies, using the yum package manager provided in Red Hat Enterprise Linux, by running the command:

- `yum install compat-libstdc++-33-3.2.3-69.el6.i686`

  or

- `yum install compat-libstdc++-33-3.2.3-69.el6.ppc64`

2. **Install the HP Operations agent on the SiteScope server**

The agent enables SiteScope to act as data storage for metrics data collected by SiteScope.

Install HP Operations Agent 11.14 from the SiteScope installer package, or download it from the HPE Software Support web site (in the Search box, type "Operations Agent", select the relevant version, under Document Type, select **Patches**, and locate the installation file).

Note: If an older version of the agent is already installed, or the agent is already integrated with OMi/OMu/OMw, you should:

a. Upgrade the agent according to the instructions in the HPE Operations Agent 11.14 Installation Guide.

b. Configure the agent using the SiteScope Configuration Tool as described in step 3 below.

On Windows:

a. Log on to the node with the administrator privileges.

b. Go to the directory where you extracted the contents of the ISO file.

c. Run the following command to install the agent:

```
cscript oainstall.vbs -i –a
```

On UNIX/Linux:

a. Log on to the node with the root privileges.

b. Go to the directory where you extracted the contents of the ISO file.

c. Run the following command to start the installation:

./oainstall.sh -i -a

d. When the installation is complete, the agent starts its operation on the node and all the necessary components start running.

For more detailed installation instructions, see the Operations Agent 11.14 Installation Guide, available from the HPE Software Support site.

Note:

- Only Operations Agent version 11.14 is certified with SiteScope 11.3x.
- Use the `-includeupdates` installation option to install Operations Agent 11.14 with pre-packed hotfixes. For details, refer to the Operations Agent 11.14 Installation Guide.
- To enable the Operations Manager metrics integration, the Operations agent on the SiteScope machine must run under the same user as in SiteScope, namely a non-root user. For details, see Configure an Agent to run Under an Alternative User on UNIX in the Operations Manager for UNIX - HTTPS Agent Concepts and Configuration Guide.

3. **Complete the HP Operations Agent installation using the SiteScope Configuration Tool**

Note: This step must be performed before integrating the Operations Agent to HPOM.

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`.
   - On Linux (console mode): Run `/opt/HP/SiteScope/bin/config_tool.sh -i console`.

   For more details on using the SiteScope Configuration Tool, see the HPE SiteScope Deployment Guide (available from the HPE Software Support site).

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 installation of the Operations Agent.

c. Restart SiteScope (if required).

d. (If the agent is installed on a Red Hat ES Linux 6.0 environment) After installing the Operations Agent, check the installation status in the log files.
   - SiteScope log. This just shows whether the installation passed successfully or not.

     Log file name: **HPSiteScope_config_tool.log**

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

     (search for results of "installOATask")
   - Operations Agent log files.

     Log file name: **oainstall.log**, **oapatch.log**

     Log file location:

- **%ovdatadir%\log** on Windows platforms
- **/var/opt/OV/log/** on UNIX/Linux platforms

4. **Enable SiteScope to send metrics**

   In SiteScope, navigate to **Preferences > Integration Preferences**, and create a new or edit an existing **HP Operations Manager integration**. In the HP Operations Manager Integration dialog box, expand the **HP Operations Manager Metrics Integration** panel and select **Enable HP Operations Manager metrics integration**.

   Note: Metrics integration with Operations Manager can be activated regardless of the connection status between the Operations Agent and the HPOM/BSM server, since metrics are collected by the agent.

5. **Enable monitor instances to send metrics**

   For each monitor instance that you want to report metrics data to the agent data storage, expand **HP Integration Settings** in the monitor properties, and select **Report metrics to HP Operations agent** in the **HP Operations Manager Integration Settings** section.

   Tip: You can automatically enable metrics reporting for particular monitor types without having to select **Report metrics to HP Operations agent** for each monitor instance. To do so, select **Integration Preferences > HP Operations Manager Integration**, expand the **HP Operations Manager Metrics Integration** panel, and:

   - Select **Enable metrics reporting for new monitors** to enable SiteScope to report metrics to the HP Operations agent for all newly-created monitors.
   - Click the **Enable metrics reporting for specific monitors** button to enable reporting metrics for Memory, CPU, Disk Space, and Windows Resources monitors only.

6. **Results**

   Each monitor metric is logged as an instance by the agent on the SiteScope host node, with the time and host as the instance identifier. The metrics data is collected from the agent data storage by HPOM and BSM for use in the reporting products.

   Metrics error data is written to the **oa_metric_integration.log** file which is found in the **<SiteScope root directory>\logs** directory.

   For notes and limitations on metrics integrations, see "Notes and Limitations" on page 84.

   For troubleshooting metrics integration issues, see "Troubleshooting Metrics Integration Issues" on page 84.

Chapter 18: SiteScope-Operations Agent Metrics Alignment

Metrics name alignment is the process of aligning metrics names in SiteScope with those used by Operations Manager Performance Agent (PA). Performance Manager can graph any metrics (whether aligned or not), and metrics alignment for all possible metrics is not required for viewing the data in Performance Manager.

For more information on metrics provided by Performance Agent, refer to the Performance Agent Metric Help Viewer in the Performance Agent 5.0 documentation (https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM864772). To enter the HP Software Self-solve Knowledge Base, you must log on with your HPE Passport ID.

Metrics name alignment has been performed for the commonly used metrics listed below.

PA Metrics Name (Display Name)	**SiteScope Metrics Name**
BYCPU_CPU_TOTAL_UTIL (Total CPU%)	**Windows:** • CPU Monitor \utilization (cpu #1, cpu #2, etc) • Microsoft Windows Resources Monitor \Processor\{instance}%\ Processor Time **Linux:** UNIX Resources Monitor \Processor\{instance}\System **HP-UX:** N/A **Solaris:** N/A **AIX:** UNIX Resources Monitor \Processor\{instance}\%sys
BYNETIF_IN_BYTE_RATE (In KB Rate)	**Windows:** Microsoft Windows Resources Monitor \Network Interface\{instance}\Bytes Received\sec **Linux:** N/A **HP-UX:** N/A **Solaris:** N/A **AIX:** N/A

PA Metrics Name (Display Name)	SiteScope Metrics Name
BYNETIF_OUT_BYTE_RATE (Out KB Rate)	**Windows:** Microsoft Windows Resources Monitor \Network Interface\{instance}\Bytes Sent\sec **Linux:** N/A **HP-UX:** N/A **Solaris:** N/A **AIX:** N/A
BYDSK_PHYS_READ_BYTE_RATE (Phys Read KB Rate)	**Windows:** Microsoft Windows Resources Monitor \Physical Disk\{instance}\% Disk Read Bytes\sec **Linux:** N/A **HP-UX:** N/A **Solaris:** N/A **AIX:** N/A
BYDSK_PHYS_WRITE_BYTE_RATE (Phys Write KB Rate)	**Windows:** Microsoft Windows Resources Monitor \Physical Disk\{instance}\% Disk Write Bytes\sec **Linux:** N/A **HP-UX:** N/A **Solaris:** N/A **AIX:** N/A
BYDSK_REQUEST_QUEUE (Req Queue)	**Windows:** Microsoft Windows Resources Monitor \Physical Disk\{instance}\Avg. Disk Queue Length **Linux:** N/A **HP-UX:** N/A **Solaris:** N/A **AIX:** N/A

PA Metrics Name (Display Name)	SiteScope Metrics Name
BYDSK_UTIL (Disk %)	**Windows:** Microsoft Windows Resources Monitor \Physical Disk\ {instance}\% Disk Time **Linux:** N/A **HP-UX:** UNIX Resources Monitor \Block device activity\<device>\%busy **Solaris:** UNIX Resources Monitor \Block device activity\<device>\%busy **AIX:** UNIX Resources Monitor\Block device activity\<device>\%busy
FS_SPACE_UTIL (Space%)	**Windows:** Disk Space Monitor \percent full **Linux:** Disk Space Monitor \percent full **HP-UX:** Disk Space Monitor \percent full **Solaris:** Disk Space Monitor \percent full **AIX:** Disk Space Monitor \percent full
GBL_CPU_TOTAL_UTIL (CPU %)	**Windows:** • CPU Monitor \utilization (avgas) • Microsoft Windows Resources Monitor \Processor_Total\% Processor Time **Linux:** UNIX Resources Monitor \Processor\Total\System **HP-UX:** N/A **Solaris:** N/A **AIX:** UNIX Resources Monitor\Processor\Total\%sys
GBL_MEM_PAGEOUT_RATE (Pg Out Rate)	**Windows:** Microsoft Windows Resources Monitor \Memory\Pages Output/sec **Linux:** N/A **HP-UX:** N/A **Solaris:** UNIX Resources Monitor \Page-out memory and memory freeing activities\ppgout/s **AIX:** N/A

PA Metrics Name (Display Name)	SiteScope Metrics Name
GBL_MEM_UTIL (Memory %)	**Windows:** Memory Monitor \percent used **Linux:** N/A **HP-UX:** N/A **Solaris:** N/A **AIX:** N/A
GBL_SWAP_SPACE_UTIL (Swap %)	**Windows:** Microsoft Windows Resources Monitor \Memory\% Committed Bytes In Use **Linux:** N/A **HP-UX:** N/A **Solaris:** N/A **AIX:** N/A

Chapter 19: Sizing Recommendations for SiteScope-Operations Manager Metrics Integration

While the default SiteScope configuration enables running thousands of monitors, sizing is important for planning the maximum number of monitors, metrics, and monitors types that can be stored within the SiteScope-HPOM metrics integration.

The sizing should not exceed:

- Maximum insertion rate of 1000 metrics per minute.
- Total retention storage of 1 GB.
- Total retention period of 5 weeks.

Definitions

The following are definitions of the terms used in the validation calculations below:

- **Monitors**. The number of monitors that report metrics to HPOM Performance Manager.
- **Metrics**. The average number of metrics of the above mentioned monitors that report to HPOM Performance Manager.
- **Frequency**. The average frequency at which the above mentioned monitors feed data into the integration.

Validation

When choosing the specific SiteScope monitors and metrics to store within the SiteScope-HPOM metrics integration, you should validate that the insertion and retention rates do not exceed the recommendations. You can do that using the formulae below:

- **Supported Insertion Rate Validation**:

  `(Monitors * Metrics) / Frequency <= 1000 metrics/minute`
- **Supported Retention Period Validation**:

  `(1000 MB) / ((Monitors * Metrics / Frequency) * 0.07 MB) = configured retention period in days`

  (which should be less than the maximum retention period of 5 weeks)

where `0.07 MB` is the storage size for each metric/minute per day.

Example

If you have 2500 monitors that report data using the HPOM metrics integration, and every monitor has 4 metrics, the frequency of these monitors is every 10 minutes, and the average metric storage size per day is 0.07 MB, you will be able to store your historical data for 14 days.

Validation calculations:

- **Insertion Rate Validation**:

  (2500 monitors * 4 metrics) / 10 minutes = 1000 <= 1000 metrics/minute

- **Retention Period Validation**:

  1000 MB / (((2500 * 4 Metrics) / 10 minutes) * 0.07 MB) = 14.28 days (<= 5 weeks)

Chapter 20: Troubleshooting Metrics Integration Issues

This section includes:

Notes and Limitations

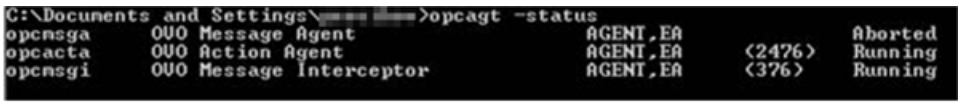
- The agent data store supports only alphanumeric and the underscore (_) character in SiteScope metric names. All other characters are converted to supported characters (the metric display name (heading) remains in the SiteScope style).
- Web Script monitor data cannot be reported …to Operations Management or HPOM.
- After upgrading from Performance Manager to Performance Graphing and connecting SiteScope to BSM, historical report data cannot be upgraded since it does not have CI-based reporting capability (it can still be viewed in the old Performance Manager way).
- To enable reporting numerical values with postfixes (such as 25% or 400MB) to the agent data store, add the list of postfixes, separated by commas, to the **_omMetricIntergationAllowedNumberPostfixs** property in the **<SiteScope root directory>\groups\master.config** file. For example, to include %, MB, KB, and GB, add **=%,mb,kb,gb**. Note that all postfixes should be in lower case.
- In an Operations Management Manager of Managers configuration (where multiple HPOM servers are connected to Operations Management, and multiple SiteScopes are connected to the HPOM servers, and indirectly to Operations Management), data sent from SiteScope is not supported by Performance Graphing, since SiteScope does not send topology to Operations Management. For details on Operations Management deployment configurations, see the section on Connected Servers in the BSM Application Administration Guide.
- To prevent overloading the agent data store, follow the sizing recommendations as described in "Sizing Recommendations for SiteScope-Operations Manager Metrics Integration" on page 82.

Troubleshooting the HP Operations Agent Configuration

Check the HP Operations Agent Configuration

1. Check the status of the HP Operations agent installed on the SiteScope server by running the following command: `opcagt -status`

   The expected output is:

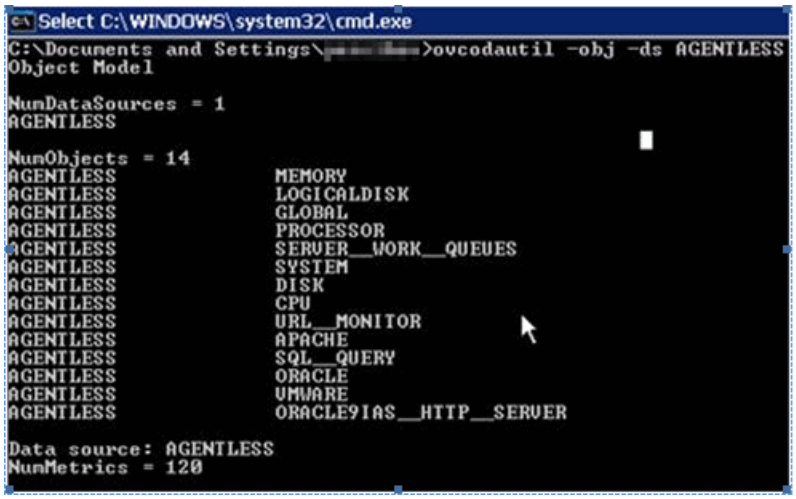
   If `opcacta` or `opcmsgi` are not running, try to restart the agent by running:

   ```
   opcagt -stop
   opcagt -start
   ```

2. Select **Preferences > Integration Preferences**, and select an existing or create a new **HP Operations Manager Integration**. Verify that the **Enable sending events** check box is selected.
3. Under the Properties tab for the monitor, expand the HP Integration Settings panel, and verify that the **Report metrics to HP Operations agent** check box is selected.
4. Run the monitor, and wait for about a minute.
5. Run the following command to check if the agent data store contains the data:

   ```
   set CODAMAGIC=0X05201993
   ovcodautil -obj -ds AGENTLESS
   ```

   You should receive object names from AGENTLESS data source (similar to the following):

6. To dump the summarized last record for AGENTLESS data source, run the following command:

   ```
   ovcodautil -dumpds AGENTLESS
   ```

Check the Relevant SiteScope Logs

Check the following logs that are available from the **<SiteScope root directory>\logs** directory:

- **error.log**
- **RunMonitor.log**
- **om_metric_integration.log**
- **data_integration.log**

Health Monitors Errors

In the SiteScope monitor tree, expand **Health** and click **Log Event Checker**.

- If the **Failed to report data to HP OM Agent** counter is in error, SiteScope failed to connect or report data to the HP Operations agent using Java API. For more information, see the **oa_metric_integration.log** file in the **<SiteScope root directory>\logs** directory.
- If the **Generic Data Integration queue exceeded allowed size** counter is in error, the queue of metrics waiting to be sent is oversized and some metrics were dropped to maintain SiteScope stability. For more information, **data_integration.log** file in the **<SiteScope root directory>\logs** directory.

HP Performance Manager Configuration

1. On the Performance Manager server, open the **OVPMconfig.ini** file in the **%ovdatadir%\shared\server\conf\perf** directory.
2. Update the SiteScope server details as follows:
   - [SITESCOPE]
   - SERVER = servername
   - NODEGROUP = Agentless
3. Restart the HP Openview Tomcat(B) service.

CI Resolution does not work ("BadHint error" in the cir_enrichment.log)

1. Go to **Admin > Platform > Infrastructure Setting**.
2. In the **Application** dropdown, select **End User/System Availability Management**.
3. In the **SiteScope CI Resolver Settings**, check for **TQL Queries** value.

   The default value is `CIs Monitored by SiteScope` (in BSM versions earlier than 9.20).
4. Go to **Admin > RTSM Administration** and check for **CIs Monitored by SiteScope** query results. If you do not get the requested CI in the query results, CI resolution will not find it as well.

Possible problem: CI has missing attributes or the SiteScope monitor CI is not connected to any monitored CI.

System runs out of ports when reporting data to the HP Operations agent

Problem: The system runs out of ports when reporting metrics data to the HP Operations Agent in a loaded environment.

- In SiteScope Health, an error is displayed in the Log Event Checker monitor for the .*Failed to report data to HP OM Agent.* counter.
- In the **oa_metric_integration.log**, the following error is displayed: "ERROR - Failed to report data to /Hewlett-Packard/OpenView/Coda/ IO error while gettingSingle Object;Address already in use: connect".

Possible solution: Increase the upper range of ephemeral ports and reduce the client TCP/IP socket connection timeout value in Windows. For details, see http://msdn.microsoft.com/en-us/library/aa560610%28v=bts.20%29.aspx.

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 HP Operations Manager Products (SiteScope 11.32)

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!