Hewlett Packard
Enterprise

HPE Network Node Manager i Software

Software Version: NNMi 10.20

HPE Network Node Manager i Software–HPE SiteScope Integration Guide

Document Release Date: July 2016
Software Release Date: July 2016

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Apple is a trademark of Apple Computer, Inc., registered in the U.S. and other countries.

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

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

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

Internet Explorer, Lync, Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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

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

sFlow is a registered trademark of InMon Corp.

UNIX® is a registered trademark of The Open Group.

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

This product includes software developed by the Visigoth Software Society (http://www.visigoths.org/).

Documentation Updates

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

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

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

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

Support

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

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

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

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

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

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

Contents

HPE SiteScope

You can use HPE SiteScope as a data collector for HPE Network Node Manager i Software (HPE NNMi), which is an event console used for network monitoring. HPE SiteScope monitors the application side of the systems that HPE NNMi is monitoring, and uses SNMP Traps to forward event data from HPE SiteScope to HPE NNMi. HPE SiteScope can also report metrics data to HPE NNMi.

For information about purchasing HPE SiteScope, contact your HPE sales representative.

This chapter describes the following integrations:

- "HPE NNMi–HPE SiteScope Events Integration"
- "HPE NNMi–HPE SiteScope System Metrics Integration"

For information about the NNM iSPI for IP Telephony–HPE SiteScope integration, see *Configuring Integration with SiteScope* the NNM iSPI for IP Telephony help.

HPE NNMi-HPE SiteScope Events Integration

This section contains the following topics:

- "About the HPE NNMi–HPE SiteScope Events Integration"
- "Enabling the HPE NNMi–HPE SiteScope Events Integration"
- "Using the HPE NNMi–HPE SiteScope Events Integration"
- "SNMP Trap Formats used to Identify the SiteScope Object"
- "Changing the HPE NNMi–HPE SiteScope Events Integration" on page 10
- "Disabling the HPE NNMi–HPE SiteScope Events Integration"
- "Troubleshooting the HPE NNMi–HPE SiteScope Events Integration"

About the HPE NNMi-HPE SiteScope Events Integration

With the HPE NNMi–HPE SiteScope Events integration, SiteScope servers send SNMP traps to the NNMi management server when the configured SiteScope monitor alert conditions are met. HPE NNMi converts the monitor alert traps into NNMi incidents. From these incidents, an NNMi console user can launch HPE SiteScope in the context of that monitor. For the list of SNMP trap formats used to identify the SiteScope object sending the message to the NNMi management server, see "Table 1 SNMP Trap Format for SiteScope Objects Sent to NNMi".

Value

By providing SiteScope incident configuration in HPE NNMi, the HPE NNMi–HPE SiteScope Events integration simplifies the process of interpreting SNMP traps regarding status of devices and applications that SiteScope monitors.

These traps are generated only for alerts configured in HPE SiteScope. The integration makes these traps visible in the NNMi console as incidents. HPE NNMi automatically closes these alert incidents if HPE SiteScope indicates that the alert condition no longer exists (becomes normal).

Integrated Products

The information in this section applies to the following products:

- HPE SiteScope

  > **TIP:** For the list of supported versions, see the NNMi System and Device Support Matrix located at **https://softwaresupport.hpe.com/**.

- NNMi 10.20

HPE NNMi and HPE SiteScope can be installed on the same computer or on different computers.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Supported SiteScope Monitors

The HPE NNMi–HPE SiteScope Event integration receives SNMP traps sent from the SiteScope server for any SiteScope monitor type, as configured in HPE SiteScope. The SiteScope alert configuration must include the NNMi management server as the trap target.

The SiteScope trap configuration determines whether the SiteScope server or the managed host is set as the source object. If the source object is not managed in HPE NNMi, the **Discard Unresolved SNMP Traps** check box setting on the **Incident Configuration** form determines how HPE NNMi handles that trap. For more information, see *Handle Unresolved Incoming Traps* in the NNMi help.

Documentation

This section describes how to configure and use the integration.

For more details about the procedures performed in SiteScope, see the *HPE SiteScope Using SiteScope* guide, which is included on the HPE SiteScope product media.

Enabling the HPE NNMi-HPE SiteScope Events Integration

To enable the HPE NNMi–HPE SiteScope Events integration, configure one or more SiteScope monitors to send SNMP traps to HPE NNMi. The high-levels steps are as follows:

> **TIP:** The NNMi incident types are enabled by default.

1. In the SiteScope user interface, create an SNMP preference to send the SiteScope event trap to the NNMi management server. In SiteScope, select **Preferences** > **SNMP Preferences**; use the **SNMP Preferences** page to configure both send and receive SNMP trap preferences. Create a preference for the server to which you want to report the SNMP trap using the following settings:
   a. **SNMP trap ID**. Select **Enterprise-Specific SNMP trap ID**, and enter **1**.
   b. **SNMP object ID**. Select **Preconfigured SNMP object IDs** and choose **HP SiteScope Event** from the list; deselect **Add System OID as a prefix to SNMP Trap**.

   c. Make sure **Add System OID as a prefix to SNMP Trap** *is NOT checked*. The **Add System OID as a prefix to SNMP Trap** checkbox *should not be checked*.

   Complete the other SNMP trap fields as required. For user interface details, see the *SNMP preferences* section in the *SiteScope Help.*

2. In the SiteScope user interface, create an alert that sets the SNMP trap preference as the alert action target. In this alert, create an alert action for each possible monitor status. See "Figure 1 Configuring an SNMP Trap Alert Action for Each Monitor Status" when completing these steps.

   a. In the SiteScope monitor tree, right-click the **SiteScope** root and select **New** > **Alert**.

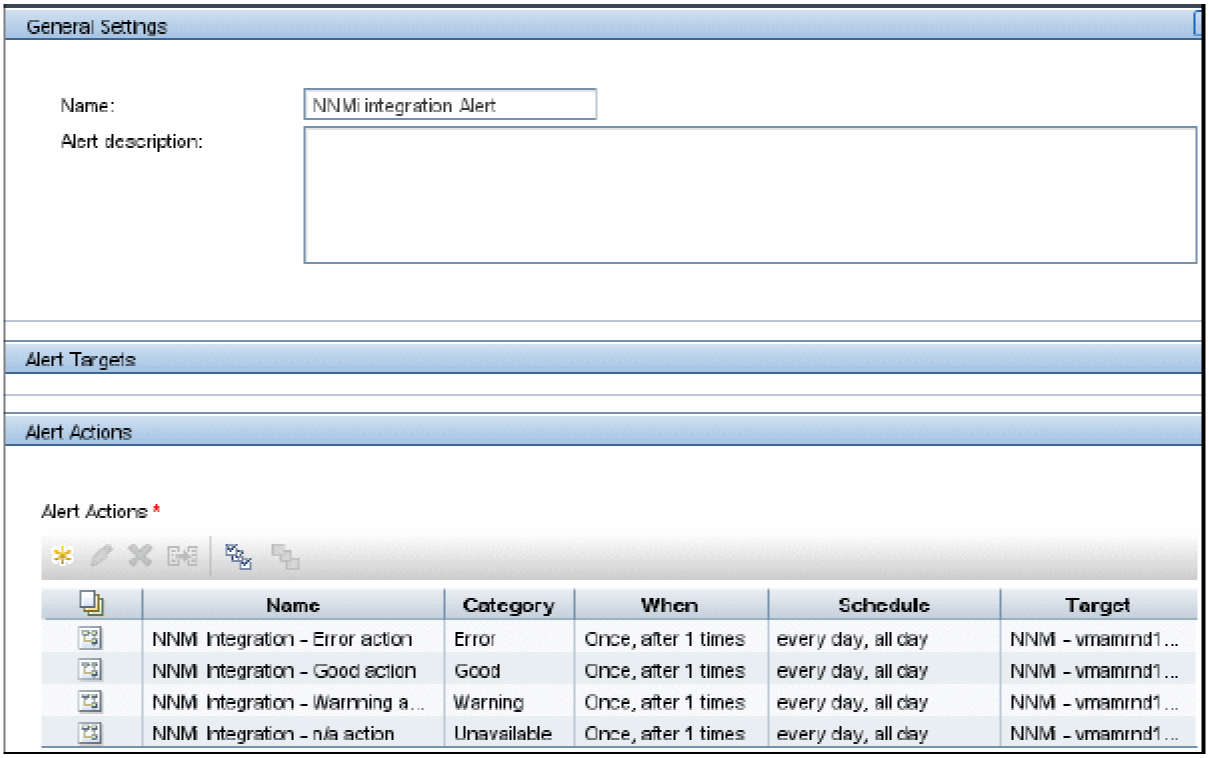
   b. In the Alert Targets panel, select the groups, monitors, or both, to trigger this alert.

   c. In the Alert Actions panel, click **New Alert Action** and select **SNMP Trap** action type.

   d. In the **Alert Action: SNMP Trap** dialog box, configure an SNMP Trap alert action for each monitor status.

      - In the Action Type Settings panel, select **SiteScopeEvent.xml** from the **Template** list. This template contains the format and content of messages sent by SNMP to NNMi when a SNMP trap is triggered. You can copy and customize this template which is located in the <*SiteScope root directory*>`\templates.snmp` file.
      - In the Status Trigger panel, select an SNMP trap status.
      - Repeat "In the Alert Actions panel, click New Alert Action and select SNMP Trap action type." for each monitor status in the Status Trigger panel (Error, Warning, Good, and Unavailable).

Figure 1 Configuring an SNMP Trap Alert Action for Each Monitor Status



General Settings

Name: NNMi integration Alert

Alert description:

Alert Targets

Alert Actions

Alert Actions *

	Name	Category	When	Schedule	Target
	NNM Integration - Error action	Error	Once, after 1 times	every day, all day	NNM - vmamrnd1...
	NNM Integration - Good action	Good	Once, after 1 times	every day, all day	NNM - vmamrnd1...
	NNM Integration - Warrning a...	Warning	Once, after 1 times	every day, all day	NNM - vmamrnd1...
	NNM Integration - n/a action	Unavailable	Once, after 1 times	every day, all day	NNM - vmamrnd1...

3. When an alert is triggered in SiteScope as a result of a monitor status change, the alert reports an SNMP trap to the NNMi management server. NNMi reads the SNMP trap, translates the attributes, and displays the SiteScope event data in NNMi's **Incident Browsing** workspace.

Using the HPE NNMi-HPE SiteScope Events Integration

HPE NNMi defines two incident types for the SiteScope monitor alert traps:

- SiteScopeAlertEvent1 converts SNMPv1-format traps to NNMi incidents.
- SiteScopeAlertEvent2 converts SNMPv2c-format traps to NNMi incidents.

The configuration of these incident types is identical. The SiteScope SNMP trap preference determines whether HPE SiteScope sends SNMPv1- or SNMPv2c-format traps to HPE NNMi.

Within the incident configuration, incident severity is set as follows:

- The default incident status is CRITICAL, which maps to SiteScope event severity of ERROR, NOTAVAILABLE, or NODATA.
- Incident enrichment sets the incident status to WARNING when the SiteScope event severity is WARNING.
- Incident enrichment sets the incident status to NORMAL when the SiteScope event severity is GOOD.

Each SiteScopeAlertEvent trap contains a URL for launching SiteScope in the context of that monitor. This URL is available in the .1.3.6.1.4.1.11.15.1.2.1.4 custom incident attribute (CIA) on the **Custom Attributes** tab of the **Incident** form. The URL passes encrypted credentials for logging on to SiteScope as the Integration Viewer user.

For each SiteScopeAlertEvent incident, HPE NNMi performs pairwise handling on the SiteScopeAlertEvent traps by comparing data included in the traps' payloads. Each trap contains an event key varbind (OID .1.3.6.1.4.1.11.15.1.3.1.7). If a trap also contains an event close key pattern varbind (OID .1.3.6.1.4.1.11.15.1.3.1.8), HPE NNMi compares the value of the event close key pattern varbind with that of the event key varbind in existing incidents. HPE NNMi closes the matching existing incidents and correlates them under the incoming trap. HPE NNMi adds the cia.reasonClosed CIA and a correlation note to each of the closed incidents. Additionally, HPE NNMi automatically closes each SiteScopeAlertEvent incident of NORMAL status.

The SiteScope SNMP traps appear in the System and Applications family.

For more information about the contents of the SiteScopeAlertEvent trap, the HP-SITESCOPE-MIB, which is delivered with HPE NNMi.

SNMP Trap Formats used to Identify the SiteScope Object

"Table 1 SNMP Trap Format for SiteScope Objects Sent to NNMi" shows a list of SNMP trap formats used to identify the SiteScope object sending the message to the NNMi management server. This enables an NNMi console user to launch SiteScope in the context of that monitor.

The SNMP trap formats are stored in the `SiteScopeEvent.xml` file, which is located in the `<SiteScope root directory>\templates.snmp` folder.

Table 1 SNMP Trap Format for SiteScope Objects Sent to NNMi

Field Name	Object ID (OID)	Description	Values
Enterprise OID	.1.3.6.1.4.1.11.15.1	SiteScope root Object ID	.1.3.6.1.4.1.11.15.1
Trap	.1.3.6.1.4.1.11.15.1.	SNMP Trap Object ID	(OID)

Table 1 SNMP Trap Format for SiteScope Objects Sent to NNMi, continued

Field Name	Object ID (OID)	Description	Values
OID	0		For V1: [1.3.6.1.4.1.11.15.1.4.0.1] For V2: [1.3.6.1.4.1.11.15.1.4.1]
SiteScope Host	.1.3.6.1.4.1.11.15.1.1.2	IP address or host name of the SiteScope server	(IpAddress) [16.55.244.182] or (OctetString) [sisserver.mydomain]
Provider (Collector)	.1.3.6.1.4.1.11.15.1.1.3	SiteScope application name	(OctetString) SiteScope
Monitor Name	.1.3.6.1.4.1.11.15.1.2.1.1	SiteScope monitor name	(OctetString) [Memory monitor on myhost.mydomain]
Monitor Type	.1.3.6.1.4.1.11.15.1.2.1.2	SiteScope monitor type	(OctetString) [Memory Monitor]
Monitor ID	.1.3.6.1.4.1.11.15.1.2.1.3	Monitor unique ID	(OctetString) [067e6162-3b6f-4ae2-a171-2470b63dff00]
Monitor Drill-Down URL Secured	.1.3.6.1.4.1.11.15.1.2.1.4	URL that opens SiteScope in context of the alerted monitor, without silent log on information. This permits configuration by integration instance level. To get drill down URL with user credentials, change the reference value from monitorDrilldownUrlSecured to monitorDrilldownUrl.	(OctetString) http://sisserver:8080/SiteScope/servlet/Main?activeid=__SiteScopeRoot__&activerighttop= dashboard&view=new&dashboard_view= Details&dashboard_model=true&dashb
Monitor Target Host	.1.3.6.1.4.1.11.15.1.2.1.5	Monitor target host	(IpAddress) [16.55.244.182] or (OctetString) [myhost.mydomain]
Monitor	.1.3.6.1.4.1.11.15.1.	Monitor target IP	(IpAddress)

Table 1 SNMP Trap Format for SiteScope Objects Sent to NNMi, continued

Field Name	Object ID (OID)	Description	Values
Target IP	2.1.6	address	[16.55.244.182]
Monitor Full Name	.1.3.6.1.4.1.11.15.1.2.1.7	SiteScope monitor name including full path from the root	(OctetString) [Memory monitor on myhost.mydomain]
Title	.1.3.6.1.4.1.11.15.1.3.1.1	SiteScope Event Title	(OctetString) [Alert 'Memory Alert' was triggered on monitor 'Memory monitor on myhost.mydomain' due to a status change]
Event Source	.1.3.6.1.4.1.11.15.1.3.1.2	Source of the event (alert or metric)	(OctetString)
Severity	.1.3.6.1.4.1.11.15.1.3.1.3	SiteScope event severity	(Integer) [0,1,2,3] For [unavailable, good, warning, error]
Event Time	.1.3.6.1.4.1.11.15.1.3.1.4	Original event time in milliseconds	(TimeTicks) 1287316779
Value	.1.3.6.1.4.1.11.15.1.3.1.5	(Not for alerts flow)	(OctetString) [running] or [25] or [n/a] - for alerts
Event Description	.1.3.6.1.4.1.11.15.1.3.1.6	Description of fired event	(OctetString)
Event Key	.1.3.6.1.4.1.11.15.1.3.1.7	Key of the event	(OctetString) [sisserver:067e6162-3b6f-4ae2-a171-2470b63dff00:Memory
Event Close Key Pattern	.1.3.6.1.4.1.11.15.1.3.1.8	Key to identify paring events	[sisserver:067e6162-3b6f-4ae2-a171-2470b63dff00]

Changing the HPE NNMi-HPE SiteScope Events Integration

To change the HPE NNMi–HPE SiteScope Events integration, do any of the following:

- In the NNMi console, edit the incident configurations for the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 SNMP traps.
- In the SiteScope user interface, change the monitor alert configurations.

Disabling the HPE NNMi-HPE SiteScope Events Integration

To disable the HPE NNMi–HPE SiteScope Events integration, do one or both of the following:

- In the NNMi console, clear the **Enabled** check box on the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 **SNMP Trap Configuration** forms.
- In the SiteScope user interface, do one of the following:
  - Remove monitors and groups from the alert action target.
  - Disable or delete the SNMP trap alert associated with the SiteScope monitors.

Troubleshooting the HPE NNMi-HPE SiteScope Events Integration

This section contains the following topics:

- "NNMi Incident Views Do Not Display SiteScopeAlertEvent Incidents"
- "HPE SiteScope Does Not Open Correctly from the URL in a SiteScope Incident"

NNMi Incident Views Do Not Display SiteScopeAlertEvent Incidents

If the NNMi incident views do not contain all of the expected SiteScopeAlertEvent incidents, follow these steps:

1. In the NNMi console, check the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 incident configurations:
   - Verify that the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 incident types are enabled.
   - If interface or node settings are configured, verify that they are not blocking expected SiteScope traps.
2. In the NNMi console, check the filter for the incident view.

   Compare the current filter with the SiteScopeAlertEvent1 and SiteScopeAlertEvent2 incident configurations. Verify that the filter does not block these incident types.
3. If the **Discard Unresolved SNMP Traps** check box on the **Incident Configuration** form is selected, verify that the nodes associated with SiteScope monitors are in the NNMi topology.

   The SiteScope trap configuration determines whether the SiteScope server or the managed host is set as the source object.

   <<When trap receipt troubleshooting content is added to the Incidents chapter in the Dref, point to it.>>
4. In the SiteScope user interface, verify the configuration of the SNMP trap preference for the HPE SiteScope event trap.
5. In the SiteScope user interface, verify that each expected monitor alert sets the SNMP trap preference as the alert action target.
6. In the SiteScope user interface, send a test trap to HPE NNMi.

HPE SiteScope Does Not Open Correctly from the URL in a SiteScope Incident

If HPE SiteScope does not correctly launch from the URL in the .1.3.6.1.4.1.11.15.1.2.1.4 CIA on the **Custom Attributes** tab of the **Incident** form, follow these steps:

1. Verify access to the SiteScope user interface:
   a. In a new browser window, open the SiteScope user interface directly.

      If the SiteScope user interface does not work correctly, verify that the browser configuration matches the requirements described in the *HPE SiteScope Release Notes*.

   b. Copy the URL from the .1.3.6.1.4.1.11.15.1.2.1.4 CIA to the browser address field. Delete the logon credentials. In the SiteScope logon window, enter your SiteScope logon information.
2. Verify the SiteScope Integration Viewer user credentials in the URL. Copy the URL from the .1.3.6.1.4.1.11.15.1.2.1.4 CIA to the browser address field. (Keep the logon credentials.)

   If this test fails, ask the SiteScope administrator about the status of the Integration Viewer user. If the password for the Integration Viewer user has changed recently, the URLs to SiteScope that existed before the password change do not work.

HPE NNMi-HPE SiteScope System Metrics Integration

This section contains the following topics:

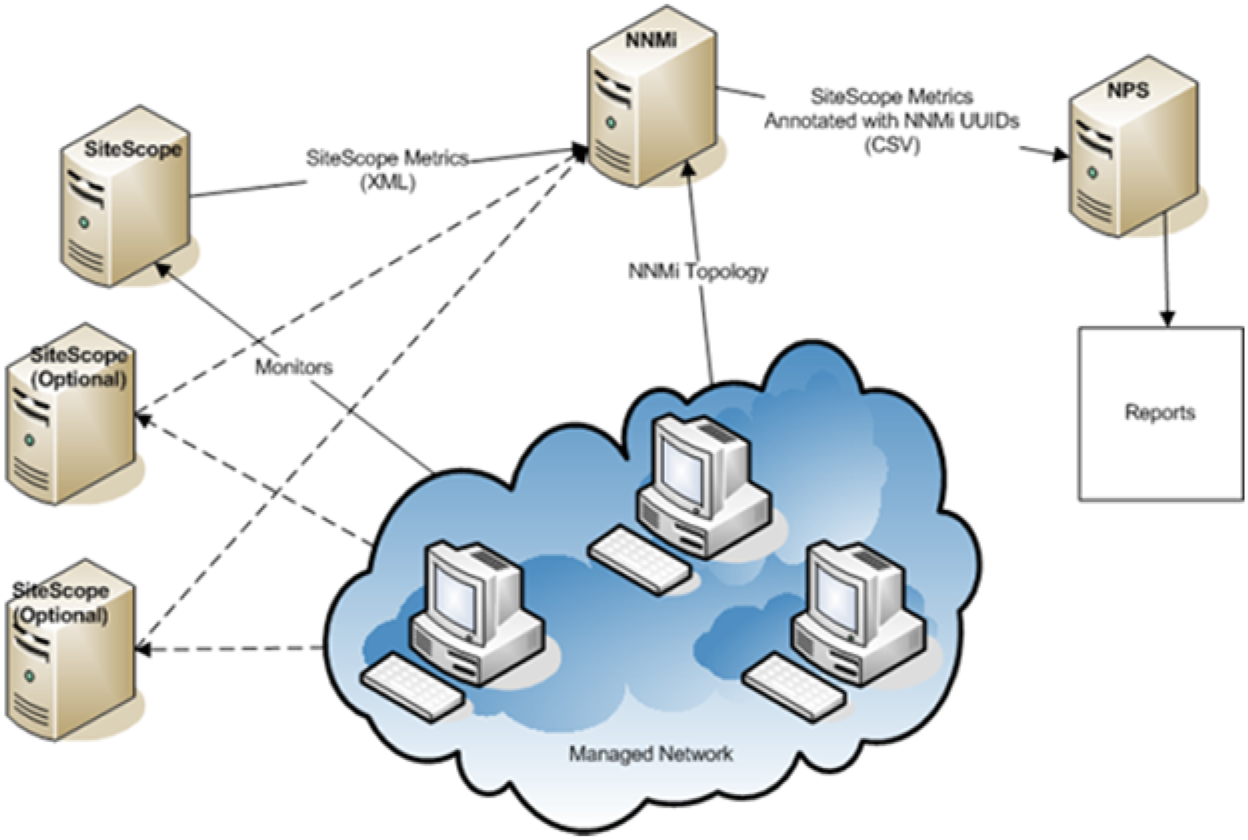
About the HPE NNMi-HPE SiteScope System Metrics Integration

The HPE NNMi–HPE SiteScope System Metrics integration populates the HPE NNM iSPI Performance for Metrics Network Performance Server (NPS) with system metrics data collected by SiteScope monitors. The integration handles data as follows:

1. HPE SiteScope collects monitor data into XML files and passes the collected data to HPE NNMi at the reporting interval of the SiteScope data integration preference.
2. HPE NNMi augments the SiteScope data with NNMi node UUIDs.
3. HPE NNMi places the augmented data in the configured location for NPS retrieval.
4. The NPS consumes the augmented data at the NPS accumulation interval.

"Figure 2 HPE NNMi–HPE SiteScope System Metrics Integration Data Flow" shows the data flow for the HPE NNMi–HPE SiteScope System Metrics integration.

Figure 2 HPE NNMi–HPE SiteScope System Metrics Integration Data Flow



Value

The HPE NNMi–HPE SiteScope System Metrics integration enables reporting of SiteScope-collected metrics in the NPS.

Integrated Products

The information in this section applies to the following products:

- HPE SiteScope

> **TIP:** For the list of supported versions, see the NNMi System and Device Support Matrix.

- NNMi 10.20
- HPE NNM iSPI Performance for Metrics version 10.10

> **NOTE:** This integration requires an HPE NNM iSPI Performance for Metrics license.

HPE NNMi, the HPE NNM iSPI Performance for Metrics, and HPE SiteScope can be installed on the same computer or on different computers.

For the most recent information about supported hardware platforms and operating systems, see the support matrices for all products.

Supported SiteScope Monitors

The HPE NNMi–HPE SiteScope System Metrics integration understands data from the following types of SiteScope monitors:

- CPU Utilization Monitor
- Dynamic Disk Space Monitor
- Disk Space Monitor
- Memory Monitor
- The Process monitored object of the Microsoft Windows Resources Monitor
- The Process monitored object of the Linux Resources Monitor

The nodes being monitored must be managed in HPE NNMi. The integration discards data for nodes that are not in the NNMi topology and for unmanaged nodes.

Documentation

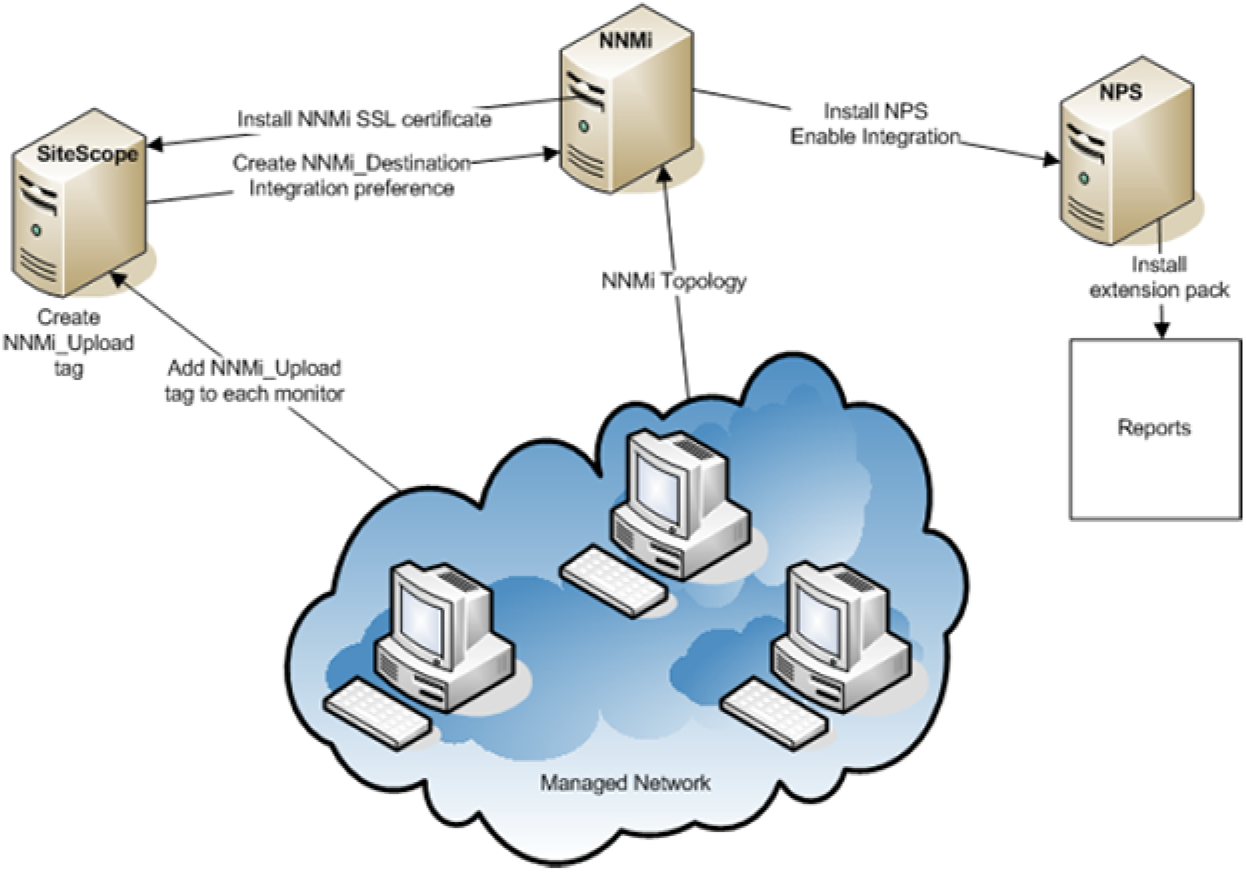
This section describes how to configure HPE NNMi to communicate with HPE SiteScope and the NPS reports available for the SiteScope-collected data.

The *HPE SiteScope Using SiteScope guide*, which is included on the SiteScope product media, describes how to configure SiteScope monitors.

Enabling the HPE NNMi-HPE SiteScope System Metrics Integration

"Figure 3 HPE NNMi–HPE SiteScope System Metrics Integration Configuration Points" shows the configuration points for the HPE NNMi–HPE SiteScope System Metrics integration.

Figure 3 HPE NNMi–HPE SiteScope System Metrics Integration Configuration Points


NNMi
SiteScope
NPS
Install NNMi SSL certificate
Create NNMi_Destination Integration preference
Install NPS Enable Integration
NNMi Topology
Install extension pack
Reports
Create NNMi_Upload tag
Add NNMi_Upload tag to each monitor
Managed Network

To enable the HPE NNMi–HPE SiteScope System Metrics integration, follow these steps:

1. In the NNMi console, enable integration and configure the NPS with the SiteScope system metrics integration pack:
   a. *Optional*. Create an NNMi user with the Web Service Client role that the integration uses to connect to the NNMi console.

      Alternatively, you can use an existing user with the Web Service Client role for the integration.

   b. Open the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form (**Integration Module Configuration > HPE SiteScope System Metrics**).
   c. Select the **Enable Integration** check box.
   d. Enter the information for connecting to the NNMi management server. For information about these fields, see "Enabling the HPE NNMi–HPE SiteScope System Metrics Integration".
   e. Click **Submit** at the bottom of the form.

      The window displays a status message. If the message indicates a problem with the NNMi credentials, click **Return**, and then adjust the values as suggested by the text of the error message.

   f. From the results window, copy the data integration URL to a temporary location. You will use this value while configuring HPE SiteScope.
2. In the SiteScope user interface, configure the SiteScope server for SSL communications with HPE NNMi:
   a. From the **Preferences** workspace, open the **Certificate Management** page, and then click **Import Certificates** ✱.

   b. Under **Source Selection**, provide information to identify the NNMi management serverr to HPE SiteScope:

      - Verify that **Host** is selected, and then enter the fully-qualified domain name of the NNMi management server.
      - If necessary, change the port number to match the HTTPS port on the NNMi management server.

        For more information, see "Enabling the HPE NNMi–HPE SiteScope System Metrics Integration".

   c. Click **Load**.

      The NNMi certificate information appears under **Loaded Certificates**. Note the certificate alias.

   d. Select the NNMi certificate, and then click **Import**.

      The NNMi certificate is listed on the **Certificate Management** page.

3. In the SiteScope user interface, create a search/filter tag that you will use to identify the NNMi target.

   a. From the **Preferences** workspace, open the **Search/Filter Tag** page, and then click **New Tag** ✳.

   b. Enter a tag name (for example, NNMi_upload) and at least one value.

4. In the SiteScope user interface, configure the connection between HPE SiteScope and HPE NNMi:

   a. From the **Preferences** workspace, open the **Integration Preferences** page, and then click **New Integration** ✳, and then click **Data Integration**.

   b. Under **General Settings**, enter a name (for example, NNMi_receiver) and optional description.

   c. Under **Data Integration Preferences Settings**, include the following settings:

      - In the **Receiver URL** field, paste the URL you saved at the end of "In the NNMi console, enable integration and configure the NPS with the SiteScope system metrics integration pack:" of this procedure (for example: `https://nnmi_server.example.com:443/sitescope-adapter/sitescopereceiver`).
      - Select the **GZIP compression** check box.
      - Clear the **Include additional data** and **Error on redirect** check boxes. (These are the default settings.)
      - Select the **Authentication when requested** check box. (This is the default setting.)
      - Clear the **Disable integration** check box. (This is the default setting.)

      For all other settings, the default configuration is acceptable.

   d. Under **Web Server Security Settings**, enter the user name and password for the NNMi user that you specified on the integration configuration form in "In the NNMi console, enable integration and configure the NPS with the SiteScope system metrics integration pack:".

   e. Under **Reporting Tags**, select the search/filter tag that you created in "In the SiteScope user interface, create a search/filter tag that you will use to identify the NNMi target." (for example, NNMi_upload).

5. In the SiteScope user interface, configure the monitors that contribute to the SiteScope reports in the NPS:

   a. As needed, create new monitors or identify existing monitors of the supported types:

      - CPU Utilization Monitor
      - Disk Space Monitor
      - Memory Monitor

- The Process monitored object of the Microsoft Windows Resources Monitor
- The Process monitored object of the Linux Resources Monitor

b. Add the search/filter tag that you created in "In the SiteScope user interface, create a search/filter tag that you will use to identify the NNMi target." (for example, NNMi_upload) to the monitors that should pass data to HPE NNMi.

The integration can only process data for managed nodes in the NNMi topology. So, only apply the tag to monitors on nodes in the NNMi topology.

c. Recommended. Collect the monitors that pass data to HPE NNMi in one monitor group.

Using the HPE NNMi-HPE SiteScope System Metrics Integration

The HPE NNMi–HPE SiteScope System Metrics integration provides the following SiteScope monitor reports in the NPS:

- Calendar
- Chart Detail
- Heat Chart
- Managed Inventory
- Most Changed
- Peak Period
- Threshold Sleeve
- Top N
- Top N Chart

To access the SiteScope system metric reports, follow these steps:

1. In the NNMi console, click **Actions > Reporting – Report Menu**.
2. In the **Reports** workspace of the NPS, open the **SiteScope System Metrics > SiteScope > System_Metrics** folder.

The following tips apply to the SiteScope system metric reports:

- For some reports, such as Top N, a report that focuses on one type of SiteScope monitor is easier to interpret than a report on multiple monitor types. In the topology filter, select a single value for the ComponentType attribute.
- If the Node Name attribute is not set, the report includes data for all monitors of the selected type. To limit the report data to one or more specific nodes, set the Node Name attribute accordingly. If the ComponentType attribute is set, the Node Name selection list shows only those nodes that have the selected monitor type.
- For reports on Windows Resource Monitors, it might be helpful to filter out the `_Total on` and `Idle on` data. To do so, in the topology filter, set the ComponentName attribute to not equal `_Total on` and `Idle on`.

"Table 2 Available Report Grouping Options" lists the grouping options added by the integration.

Table 2 Available Report Grouping Options

Option Name	Description
Windows Process – Creating Process	An integer value that identifies the process ID (PID) of the parent process that created the measured process.
Windows Process – ID Process	An integer value that identifies the process ID (PID) of the measured process.
Linux Process – PID	An integer value that identifies the process ID (PID) of the measured process.
Linux Process – User	An integer value that identifies the Linux user ID (uid) of the measured process.
Qualified Component Name	A string value that identifies the metric name and the node the metric is collected for. The qualified component name is in the form *<metric_name>* `on` *<node_long_name>* (for example: `disk percent full on device.example.com`). Qualified Component Name is the recommended grouping selection.

"Table 3 Available SiteScope System Metrics" lists the metrics added by integration. For each metric, you can select to report the actual values. For many metrics, you can also report threshold information. For information about interpreting the reported values, see the documentation for each operating system.

Table 3 Available SiteScope System Metrics

Monitor Type	Available Metrics
CPU Utilization[1]	• CPU Utilization
Disk Space	• Disk MB Free • Disk Percent Full
Memory[2]	• Memory Pages/Sec • Virtual Memory Used Percent • Virtual Memory MB Free • Swap Memory Used Percent • Swap Memory MB Free • Physical Memory Used Percent • Physical Memory MB Free
Microsoft Windows Resources	• Windows Process – Percent Privileged Time • Windows Process – Percent Processor Time • Windows Process – Percent User Time • Windows Process – Creating Process ID • Windows Process – Elapsed Time • Windows Process – Handle Count

Table 3 Available SiteScope System Metrics, continued

Monitor Type	Available Metrics
	• Windows Process – ID Process • Windows Process – IO Data Bytes/sec • Windows Process – IO Data Operations/sec • Windows Process – IO Data Other Bytes/sec • Windows Process – IO Other Operations/sec • Windows Process – IO Read Bytes/sec • Windows Process – IO Read Operations/sec • Windows Process – IO Write Bytes/sec • Windows Process – IO Write Operations/sec • Windows Process – Page Faults • Windows Process – Page File Bytes • Windows Process – Page File Bytes Peak • Windows Process – Pool Nonpaged Bytes • Windows Process – Pool Paged Bytes • Windows Process – Priority Base • Windows Process – Private Bytes • Windows Process – Thread Count • Windows Process – Virtual Bytes • Windows Process – Virtual Bytes Peak • Windows Process – Working Set • Windows Process – Private Working Set • Windows Process – Working Set Peak
Linux Resources[3]	• Linux Process – CPU Percent • Linux Process – Memsize • Linux Process – Number_Running • Linux Process – PID • Linux Process – User
1 HPE SiteScope summarizes CPU utilization data collected on the Linux and AIX operating systems as a single average value for the system, not per specific CPU. Because the integration does not send average values to NPS, CPU utilization data is not available for the Linux and AIX operating systems. 2 HPE SiteScope does not collect all of these metrics for all operating systems. 3 For the Linux Resources monitor on the Linux operating system, HPE SiteScope collects CPU percent, number running, and process ID only. Memory size and user data are not available for Linux nodes.	

Changing the HPE NNMi-HPE SiteScope System Metrics Integration

You can change the HPE NNMi–HPE SiteScope System Metrics integration in the following ways:

- "Change the Connection from HPE NNMi to the NPS"
- "Change the Connection from HPE SiteScope to HPE NNMi"

Change the Connection from HPE NNMi to the NPS

To change the information for connecting to the NPS, follow these steps:

1. In the NNMi console, open the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form (**Integration Module Configuration > HPE SiteScope System Metrics**).
2. Modify the values as appropriate. For information about the fields on this form, see "Change the Connection from HPE NNMi to the NPS".
3. Verify that the **Enable Integration** check box at the top of the form is selected, and then click **Submit** at the bottom of the form.

   The changes take effect immediately. The effect is to update the data integration URL displayed on the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form If this URL changes, update the SiteScope data integration preference as described in "Change the Connection from HPE NNMi to the NPS".

Change the Connection from HPE SiteScope to HPE NNMi

To change the information for the SiteScope data receiver, follow these steps:

1. In the SiteScope interface, open the data integration that defines the connection between HPE SiteScope and HPE NNMi (from **Preferences > Integration Preferences**).
2. Modify the values as appropriate. For information about the fields on this form, see the SiteScope help.
3. Verify that the **Disable Integration** check box is cleared, and then click **OK** at the bottom of the form.

   The changes take effect immediately.

Disabling the HPE NNMi-HPE SiteScope System Metrics Integration

To completely disable the HPE NNMi–HPE SiteScope System Metrics integration, complete both of the following procedures:

- "Disable the Connection from HPE NNMi to the NPS"
- "Disable the Connection from HPE SiteScope to HPE NNMi"

Disable the Connection from HPE NNMi to the NPS

To stop HPE NNMi from processing the SiteScope monitor data, follow these steps:

1. In the NNMi console, open the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form (**Integration Module Configuration > HPE SiteScope System Metrics**).
2. Clear the **Enable Integration** check box at the top of the form, and then click **Submit** at the bottom of the form.

   The changes take effect immediately.

Disable the Connection from HPE SiteScope to HPE NNMi

To stop HPE SiteScope from sending monitor data to the NNMi management server, follow these steps:

1. In the SiteScope interface, open the data integration that defines the connection between HPE SiteScope and HPE NNMi (from **Preferences > Integration Preferences**).
2. Select the **Disable Integration** check box, and then click **OK** at the bottom of the form.

   The changes take effect immediately.

Troubleshooting the HPE NNMi-HPE SiteScope System Metrics Integration

Messages related to the processing of SiteScope data, including XML parsing errors and monitor data for nodes not in the NNMi topology, are logged to the `nnm.0.0.log` (and older) files on the NNMi management server. If you encounter problems on the NNMi management server, check these log files for SEVERE and WARNING messages for the classes beginning with the string `com.hp.ov.nnm.sitescope.im` or `com.hp.ov.nms.im.sitescope`. For more information, see *NNMi Logging* in the *NNMi Deployment Reference*.

The SiteScope log file collects messages about problems with the data integration. Look in the SiteScope log file for data transmission errors, which most likely result from one or more of the following configuration problems:

- Certificate errors; the NNMi certificate is not properly loaded into HPE SiteScope.
- User name and password authentication errors; the values for **NNMi User**, **NNMi Password**, or both are incorrect on the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form in the NNMi console.
- Integration module enablement errors; the **Enable Integration** check box is cleared on the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form in the NNMi console.

For more information on the SiteScope log file, see the SiteScope documentation.

This section contains the following topics:

- "Verify the Integration Data Flow"
- "Verify the HPE NNMi Side of the Integration Configuration"
- "No Report Data for Nodes in a NAT'd Environment Behind a Firewall"

Verify the Integration Data Flow

XML files from SiteScope

The system metrics integration places the SiteScope data samples as `*.gz` files in the following directory on the NNMi management server:

- *Windows*: `%NnmDataDir%\shared\perfspi\datafiles\metric\working\sitescope`
- *Linux*: `$NnmDataDir/shared/perfspi/datafiles/metric/working/sitescope`

By default, the system metrics integration places a new file in this directory every minute, and HPE NNMi consumes these files every five minutes.

> **TIP:** The reporting interval of the SiteScope data integration preference determines the frequency HPE SiteScope sends data samples to the system metrics integration. The NNMi consumption rate is not customer configurable.

If the `sitescope` directory remains empty for more than two minutes, HPE SiteScope is not delivering the files. In this case, do the following:

1. In the SiteScope user interface, verify that the data integration preference is enabled and configured is as described in "Verify the Integration Data Flow".

   Also verify the value of the **Reporting Interval** field.
2. In the SiteScope user interface, verify that at least one monitor configuration includes the search/filter tag associated with the data integration preference.

If files accumulate in the `sitescope` directory, HPE NNMi is not consuming the files. In this case, in the NNMi console, verify that the HPE NNMi–HPE SiteScope System Metrics integration is configured correctly. For detailed information, see "Verify the Integration Data Flow".

CSV files from NNMi

HPE NNMi places `SiteScopeMetrics_*.csv.gz` files for NPS consumption in the following directory on the NNMi management server:

- *Windows*: `%NnmDataDir%\shared\perfspi\datafiles\metric\final`
- *Linux*: `$NnmDataDir/shared/perfspi/datafiles/metric/final`

HPE NNMi places a new file in this directory approximately every five minutes, and the NPS consumes these files approximately every five minutes.

> **TIP:** The NNMi placement rate is not customer configurable. The NPS accumulation rate determines the frequency that NPS consumes the files in this directory. The HPE NNM iSPI Performance for Metrics sets the NPS accumulation rate, which is not customer configurable.

If the `final` directory remains empty for more than ten minutes, HPE NNMi is not delivering the files. In this case, in the NNMi console, verify that the HPE NNMi–HPE SiteScope System Metrics integration is configured correctly. For detailed information, see "Verify the Integration Data Flow".

If files accumulate in the `final` directory, the NPS is not consuming the files. In this case, see the NPS troubleshooting documentation.

Reports

If the SiteScope reports are not available in the NPS user interface within two hours after files pass through the `final` directory, the integration is not correctly configured. In this case, restart HPE SiteScope, the NNMi ovjboss process, and the NPS:

1. Restart HPE SiteScope:
   - *Windows*:
     - Open the **Services** control panel (**Start > Control Panel > Administrative Tools > Services**).
     - In the list of services, right-click **SiteScope**, and then click **Start**.
   - *Linux or Solaris*:
     - Open a terminal window on the server where SiteScope is installed.
     - Run the start command shell script using the following syntax:

       `<installpath>/SiteScope/start`
2. Restart HPE NNMi by running the following commands:
   a. **`ovstop`**
   b. **`ovstart`**
3. Restart the NPS.

Verify the HPE NNMi Side of the Integration Configuration

1. In the NNMi console, open the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form (**Integration Module Configuration > HPE SiteScope System Metrics**).

   For information about the fields on this form, see "Change the Connection from HPE NNMi to the NPS".
2. To check the status of the integration, in the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form, click **Submit** at the bottom of the form (without making any configuration changes).

   The window displays a status message.
3. Verify that the connection to NNMi is configured correctly:

   > **NOTE:** If you used the information described in this step to connect to the NNMi console in "In the NNMi console, open the HPE NNMi–HPE SiteScope System Metrics Integration Configuration form (Integration Module Configuration > HPE SiteScope System Metrics)." of this procedure, you do not need to reconnect to the NNMi console. Continue with "Update the HPE NNMi–HPE SiteScope System Metrics Integration Configuration form with the values that you used for successful connections in "Verify that the connection to NNMi is configured correctly:" of this procedure.".

   a. In a web browser, enter the following URL:

      ***<protocol>*://*<NNMiserver>*:*<port>*/nnm/**

      Where the variables are related to values on the **HPE NNMi–HPE SiteScopeSystem Metrics Integration Configuration** form as follows:
      - If the **NNMi SSL Enabled** check box is selected, `<protocol>` is `https`.
      - If the **NNMi SSL Enabled** check box is cleared, `<protocol>` is `http`.
      - `<NNMiserver>` is the value of **NNMi Host**.
      - `<port>` is the value of **NNMi Port**.

   b. When prompted, enter the credentials for an NNMi user with the Administrator role.

You should see the NNMi console. If the NNMi console does not appear, contact the NNMi administrator to verify the information that you are using to connect to HPE NNMi. Continue to troubleshoot the connection to HPE NNMi until the NNMi console appears.

> **NOTE:** You cannot log on to the NNMi console as a user with the Web Service Client role.

c. Contact the NNMi administrator to verify the values of **NNMi User** and **NNMi Password** for the NNMi integration user with the Web Service Client role.

Passwords are hidden in the NNMi console. If you are not sure what password to specify for an NNMi user name, ask the NNMi administrator to reset the password.

4. Update the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form with the values that you used for successful connections in "Verify that the connection to NNMi is configured correctly:" of this procedure.

   For more information, see "Change the Connection from HPE NNMi to the NPS".
5. Click **Submit** at the bottom of the form.
6. If the status message still indicates a problem, do the following:
   a. Clear the web browser cache.
   b. Clear all saved form or password data from the web browser.
   c. Close the web browser window completely, and then re-open it.
   d. Repeat "Update the HPE NNMi–HPE SiteScope System Metrics Integration Configuration form with the values that you used for successful connections in "Verify that the connection to NNMi is configured correctly:" of this procedure." and "Click Submit at the bottom of the form." of this procedure.
7. Test the configuration by watching the transfer of SiteScope monitor data as described in "Verify the Integration Data Flow".

No Report Data for Nodes in a NAT’d Environment Behind a Firewall

In a network address translation (NAT) environment, if the SiteScope server is deployed behind a firewall and reports data for nodes with duplicate IP addresses outside the firewall, HPE NNMi cannot determine the node being monitored. In this case the integration does not provide the SiteScope data for these nodes to the NPS, so the NPS reports do not include this information.

HPE NNMi-HPE SiteScope System Metrics Integration Configuration Form Reference

The **HPE NNMi–HPE SiteScope System Metric Integration Configuration** form contains the parameters for configuring communications between HPE NNMi and HPE SiteScope. This form is available from the **Integration Module Configuration** workspace.

> **NOTE:** Only NNMi users with the Administrator role can access the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form.

The **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form collects information for the identifying the NNMi management server.

To apply changes to the integration configuration, update the values on the **HPE NNMi–HPE SiteScope System Metrics Integration Configuration** form, and then click **Submit**.

"Table 4 NNMi Management Server Information" lists the parameters for connecting to the NNMi management server. This is the same information that you use to open the NNMi console. You can determine many of these values by examining the URL that invokes an NNMi console session. Coordinate with the NNMi administrator to determine the appropriate values for this section of the configuration form.

Table 4 NNMi Management Server Information

Field	Description
NNMi SSL Enabled	The connection protocol specification. • If the NNMi console is configured to use HTTPS, select the **NNMi SSL Enabled** check box. • If the NNMi console is configured to use HTTP, clear the **NNMi SSL Enabled** check box.
NNMi Host	The fully-qualified domain name of the NNMi management server. This field is pre-filled with host name that was used to access the NNMi console. Verify that this value is the name that is returned by the **`nnmofficialfqdn.ovpl -t`** command run on the NNMi management server.
NNMi Port	The port for connecting to the NNMi console. This field is pre-filled with the port that the jboss application server uses for communicating with the NNMi console, as specified in the following file: • *Windows*: `%NnmDataDir%\conf\nnm\props\nms-local.properties` • *Linux*: `$NnmDataDir/conf/nnm/props/nms-local.properties` You cannot change the NNMi port value using the NNMi console. For non-SSL connections, use the value of `nmsas.server.port.web.http`, which is `80` or `8004` by default (depending on the presence of another web server when HPE NNMi was installed). For SSL connections, use the value of `nmsas.server.port.web.https`, which is 443 by default.
NNMi User	The user name for connecting to the NNMi console. This user must have the Web Service Client role.
NNMi Password	The password for the specified NNMi user.

Requirement for New HPENNMi 10.20 Installations

In a new installation of NNMi 10.20, NNMi-SiteScope integration requires you to perform additional configuration tasks if you want to use the HTTPS mode.

To configure NNMi to support the NNMi-SiteScope integration in the HTTPS mode:

Note: This procedure enables NNMi to use less secure cryptographic protocols that are not FIPS 140-2-

certified. This is a global change and may reduce the security of the product.

1. Log on to the NNMi management server.
2. Configure NNMi to allow protocols and algorithms that are not FIPS-certified:
   a. On the NNMi management server, go to the following directory:
      - *On Windows:*`%nnminstalldir%\newconfig\HPNmsServStgs\Windows`
      - *On Linux:*`/opt/OV/newconfig/HPNmsServStgs/Linux`
   b. Copy the `java.security` file, and then place the copied file in the following directory:
      - *On Windows:*`%nnmdatadir%\conf\nnm`
      - *On Linux:*`/var/opt/OV/conf/nnm`
3. Restart the NNMi processes by running the following commands:
   - *On Windows:*
     i. **%nnminstalldir%\bin\ovstop -c**
     ii. **%nnminstalldir%\bin\ovstart -c**
   - *On Linux:*
     i. **/opt/OV/bin/ovstop -c**
     ii. **/opt/OV/bin/ovstart -c**

Send Documentation Feedback

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

Feedback on HPE Network Node Manager i Software—HPE SiteScope Integration Guide (Network Node Manager i Software NNMi 10.20)

Just add your feedback to the email and click send.

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

We appreciate your feedback!