HP Network Node Manager iSPI Performance for Quality Assurance

Software Version: 10.10
Windows ® and Linux operating systems

Deployment Reference

Document Release Date: November 2015
Software Release Date: November 2015

Legal Notices

Warranty

The only warranties for HP 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. HP 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 HP 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.

Oracle Technology — Notice of Restricted Rights

Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

For the full Oracle license text, see the license-agreements directory on the NNM iSPI Performance for QA product DVD.

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

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

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

Acknowledgements

This product includes software developed by the Apache Software Foundation.

(http://www.apache.org)

This product includes software developed by the Indiana University Extreme! Lab.

(http://www.extreme.indiana.edu)

This product includes software developed by The Legion Of The Bouncy Castle.

(http://www.bouncycastle.org)

This product contains software developed by Trantor Standard Systems Inc.

(http://www.trantor.ca)

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**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:
https://hpp12.passport.hp.com/hppcf/createuser.do

Or click the **the Register** link at the top of the HP Software Support page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **https://softwaresupport.hp.com**

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

HP Software online 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 HP 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://hpp12.passport.hp.com/hppcf/createuser.do

To find more information about access levels, go to:

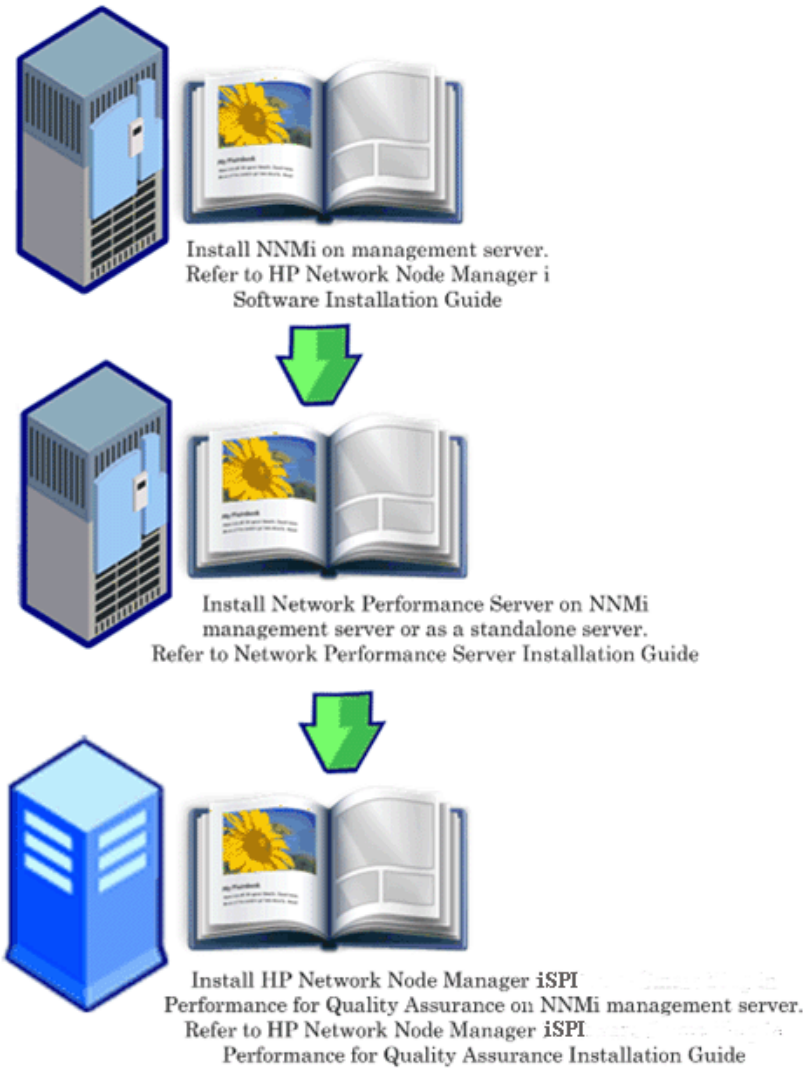
https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1: About This Guide

Typical sequence to deploy the HP Network Node Manager iSPI Performance for Quality Assurance Software (referred to as NNM iSPI Performance for QA, in the rest of the document) is represented in the following illustration:



This guide contains a collection of information and best practices for deploying the NNM iSPI Performance for QA. This guide is targeted to:

- HP Network Node Manager i Software (NNMi) and Network Performance Server (NPS) system administrator
- Network engineer
- HP support
- Engineer with experience in deploying and managing networks in large installations

Chapter 2: Preparation

Before installing the NNM iSPI Performance for QA, read the documents described in the following list:

- HP Network Node Manager i Software Ultimate Edition Support Matrix
- HP Network Node Manager i Software Ultimate Edition Release Notes

For current versions of all documents, go to:

http://h20230.www2.hp.com/selfsolve/manuals

Chapter 3: Deploying NNM iSPI Performance for QA

You must install the NNM iSPI Performance for QA on the NNMi management server. You can install the Network Performance Server (NPS) on the same NNMi management server where the NNM iSPI Performance for QA is installed, or you can install NPS on a different NNMi management server. NPS is shipped as one of the components in the NNM iSPI Performance for QA DVD media. The NNM iSPI Performance for QA integrates with NPS to display the Quality Assurance reports.

You can integrate the NNM iSPI Performance for QA with the following NNM iSPIs that enable you to extend the capability of NNMi to monitor the overall health of the network:

- HP Network Node Manager iSPI for MPLS Software (NNM iSPI for MPLS)
- HP Network Node Manager iSPI for IP Telephony Software (NNM iSPI for IP Telephony)

The integration of the NNM iSPIs with the NNM iSPI Performance for QA enhances the capabilities of these NNM iSPIs in the following ways:

- Enables you to view the quality of performance for the network elements managed by the NNM iSPIs
- Generates quality assurance reports for the health and performance of the network elements managed by the NNM iSPIs

Before Deployment

Before you deploy the NNM iSPI Performance for QA, you must plan the installation based on your deployment requirements. You must identify the ideal deployment scenario among the supported configurations and ensure that all the prerequisites are met before you begin the installation process.

The following factors impact the deployment of the NNM iSPI Performance for QA:

- Type of database configured with NNMi (embedded PostgreSQL or Oracle)
- Size of the network that you want to monitor
- Number of QA probes that you want to configure, monitor, and generate reports in the Network Performance Server (NPS)

See the documents listed in "Preparation" on page 9 to identify your deployment requirements.

Co-Existence with Network Performance Server

You can deploy NNMi 10.00, the NNM iSPIs, and Network Performance Server on the same NNMi management server. Alternatively, you can deploy NPS on a separate server.

Note: The NNMi management server where you have installed the NNM iSPI Performance for QA and the NPS must have time synchronization

Scenario 1: Network Performance Server installed on the NNMi Management Server

This deployment scenario is recommended for development environments. In this scenario:

- NNMi database (embedded PostgreSQL or Oracle) stores information on discovered network nodes, network topology, incidents, and network health information from the NNM iSPI Performance for QA
- NNMi shares the collected information with Network Performance Server for generating reports.

Scenario 2: Network Performance Server installed on a Separate Server

This deployment scenario is recommended for production environments. In this scenario:

- NNMi database (embedded PostgreSQL or Oracle) stores information on discovered network nodes, network topology, incidents, and network health information from the NNM iSPI Performance for QA

  The NNM iSPI Performance for QA shares metrics information in the following directory:

  On Windows: `%NnmDataDir%\shared\perfSpi\datafiles`

  On Linux: `$NnmDataDir/shared/perfSpi/datafiles`

- NNMi and the NNM iSPI Performance for QA shares the collected information with NPS through a shared data storage. This data is used by NPS to generate the reports.

Deploying the NNM iSPI Performance for QA with the NNM iSPI for MPLS

The integration of the NNM iSPI for MPLS with the NNM iSPI Performance for QA enables you to perform the following:

- View the specific QA probes configured for each VRF
- Generate reports based on the performance of the selected VRF
- Monitor the quality of the connectivity between multiple sites in the context of the selected VRF.
- View the Quality Assurance reports that includes network performance metrics collected by the NNM iSPI Performance for QA for MPLS specific probes.

To deploy the NNM iSPI Performance for QA with the NNM iSPI for MPLS, both the software must be installed on the same NNMi management server.

Note: For every 5000 QA probes that are specific to MPLS, you need to increase the `Xmx` value by 500 MB for qajboss

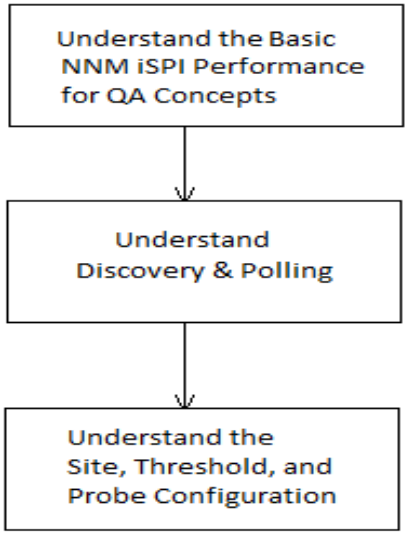
Deploying the NNM iSPI Performance for QA with the NNM iSPI for IP Telephony

The integration of the NNM iSPI for IP Telephony with the NNM iSPI Performance for QA enables you to do the following:

- Launch the Quality Assurance reports to monitor the health and performance of the voice path of Cisco IP Telephony network
- Perform a trend analysis for any persistent performance problems in the Cisco IP Telephony network. For example, if voice calls passing through two IP routers are facing persistent voice quality problems, you can use metrics like Round Trip Time (RTT), Jitter, or Mean Opinion Score (MOS) for the network path between these IP routers to identify the cause of the problem. The integration of the NNM iSPI Performance for QA with the NNM iSPI for IP Telephony enables you to generate reports in NPS for the QA probes such as IPSLA tests that are configured on the routers where the voice call is routed.
- View the Quality Assurance reports that includes network performance metrics collected by collected by the NNM iSPI Performance for QA for IP Telephony specific probes.

To deploy the NNM iSPI Performance for QA with the NNM iSPI for IP Telephony, both the software must be installed on the same NNMi management server.

Chapter 4: Basic Concepts



Understand the Basic NNM iSPI Performance for QA Concepts

The NNM iSPI Performance for QA enables you to monitor all QA probes that run on the network. QA probes are tests that are configured on the network devices managed by NNMi. You can categorize QA probes based on the vendor-specific technologies as below:

- Cisco IP SLA
- JUNIPER RPM
- Other vendors supporting the DISMAN Ping using RFC 4560

You must configure QA probes on the network devices managed by NNMi for the NNM iSPI Performance for QA to discover the QA probe. See the section "Probe Configuration" on page 26 to configure probe.

Monitored Services

The NNM iSPI Performance for QA recognizes the following services:

- UDP Echo
- ICMP Echo
- UDP (Cisco, iRA)
- TCP Connect
- VoIP (Cisco)
- Oracle (iRA)
- HTTP (Cisco, Juniper)
- HTTPS (iRA)
- DNS (Cisco)
- DHCP (Cisco)
- PATH Echo (Cisco)

Supported MIBs

The NNM iSPI Performance for QA loads the network performance information in NNMi using the following MIBs:

- CISCO-RTTMON-MIB
- DISMAN-PING-MIB
- JNX-RPM-MIB

NNM iSPI Performance for QA Metrics

The NNM iSPI Performance for QA measures the network performance using the following metrics:

- RTT (msecs and µsecs)
- RTT can either be measured in milliseconds or in micro seconds based on the precision configured for the QA probe.
- Positive Jitter (source to destination, destination to source, two way)
- Negative Jitter (source to destination, destination to source, two way)
- Percentage Packet Loss (source to destination, destination to source, two way)
- Mean Opinion Score (MOS)

Understand Discovery and Polling

Discovery

- The NNM iSPI Performance for QA discovers the QA probes configured on the nodes managed by NNMi.
- The NNM iSPI Performance for QA discovers the shadow routers configured for your Multiprotocol Label Switching (MPLS) network. You can integrate the NNM iSPI Performance for QA with the NNM iSPI for MPLS to yield more benefits from this feature.

  Note: If you want NNM iSPI Performance for QA to discover QA probes that run on shadow routers, it is mandatory to seed the shadow routers in the NNMi topology.

- The NNM iSPI Performance for QA discovers the following during each NNMi configuration poll:
  - Discovers the newly added or updated QA probes
  - Updates the destination IP address to hostname and updates the interfaces for the newly added managed nodes

- Resolves the target IP address of a QA probe with the IP address specified for a hostname. If the target IP address is not available in NNMi, the NNM iSPI Performance for QA resolves the target address by launching DNS query during discovery.

  You can disable DNS lookup to ensure that you resolve the target address of the QA probes accurately. To disable DNS lookup follow these steps:

  a. Open the file from the following directory:

     For Windows: `%NnmDataDir%\shared\qa\conf\nms-qa.jvm.properties`

     For Linux: `$NnmDataDir/nmsas/qa/conf/nms-qa.jvm.properties`

  b. Set the startup value for the property `com.hp.ov.nms.spi.qa.disco.dns` to **FALSE**.

- You can view the QA probe names resolved during discovery to generate the Quality Assurance reports in the NPS.
- Each on-demand or scheduled NNMi configuration poll re-discovers the QA probes configured on the polled nodes, and these polled nodes are the source nodes for each of these QA probes.

Discovery Filter Configuration

The NNM iSPI Performance for QA enables you to exclude the QA probes you do not require based on the QA probe owners, IP addresses, and service types. If the NNMi nodes hosting the QA probes are discovered after you configure the QA probe discovery filters, the QA probes that meet the discovery filter criteria are not discovered. Also, the poller stops polling the existing QA probes that meet the discovery filter criteria. Consequently in both these cases, the QA probes that meet the discovery filter criteria does not appear in the QA Probes view. You can set three types of discovery filters in a Global Network Management environment, which are listed below:

- Discovery filter option is selected to exclude the QA probes discovered on the network
- Regional Data Forwarding filter option is selected to exclude the QA probes forwarded to the global manager
- Global Receiver filter option is selected to exclude the QA probes received by the global manager

You can add, edit, delete, export, or import a discovery filter.

Polling

- The NNM iSPI Performance for QA polls the QA probe results every time the QA probes runs. The frequency of the QA Probes discovered in the NNM iSPI Performance for QA is equal to the frequency configured for the QA probe on the device.
- The NNM iSPI Performance for QA polls the following MIB objects:
  - **rttMonLatestOper**

    The NNM iSPI Performance for QA polls the rttMonLatestOper MIB object if the QA probes are configured with a polling frequency greater than 1 minute or 60 seconds. In this case, the SNMP polling frequency is equal to the QA probe polling frequency.
  - **rttMonStats**

    The NNM iSPI Performance for QA polls the rttMonStats MIB value if the QA probes are configured with a polling frequency lesser than 1 minute or 60 seconds. In this case, the SNMP polling frequency is always set to 2 minutes or 120 seconds.
- The NNM iSPI Performance for QA poller measures the collected metrics against the configured thresholds and calculates the threshold violation state. You can view the threshold violation state using the QA Probes form. In the Analysis pane, you can view the summary, Threshold State, Baseline State, and Latest Polled Values panels. The Latest Polled Values panel displays the last five polled values for the relevant metrics, which may be RTT, two-way jitter, two-way packet loss, and MOS metric. You can also view the last polled time.
- The NNM iSPI Performance for QA supports sub-minute polling.

  By default, the SNMP polling interval for the discovered QA probes is equal to the frequency of the IP SLA operations. If the operation frequency is less than 60 seconds for a QA probe, NNM iSPI Performance for QA applies sub-minute polling for that QA probe.

  In the case of sub-minute polling, the QA probe status refreshes every 2 minutes. The QA probe status gets updated based on the average polling value obtained for the last 2 minutes.

- Cisco IOS IP SLA allows to configure a history distribution of statistics to report a statistics distribution of the response time. However, NNM iSPI Performance for QA does not support this feature. You must redefine the IP SLA QA probes on the source router as having no history, or history distribution-of-statistics-kept 1 to generate correct Quality Assurance reports on.
- The state poller may encounter errors while polling. These errors are sent to the Network Performance Server to generate reports. The following are the possible errors encountered while polling:
  - **Unresponsive Target**

    This error occurs when the node does not respond to the SNMP request, which results in SNMP time out.
  - **Target Error**

    This error occurs when one of the target QA probes of a node is not found. For example, while you reconfigure the probes, one of the QA probes may not be found.
  - **Reboot**

    This error occurs when the node restarts in between the polling cycle or the system uptime is reset.
  - **Invalid Data**

    This error occurs due to failure of authentication or returns invalid values while polling for data.

  In addition, these polling errors are logged into the `qa_spi*.log.*` log file. This log file contains details such as node name that was polled, error state, and the set of UUID of the QA probes.

Inventory Views

Using the QA Probes view, you can analyze the QA probe status and the threshold states based on these metrics.

Using the Critical Probes view, you can segregate and view only the QA probes whose status is critical.

Using the Threshold Exceptions Probes view, you can view the probes that have violated the configured threshold for any one or more of the metrics of the NNM iSPI Performance for QA.

Using the Baseline Exceptions Probes view, you can view the QA probes with the baseline state as Abnormal Range, Unavailable, No Policy, or Not Polled for any one or more of the metrics of the NNM iSPI Performance for QA.

Multi-tenancy

The NNM iSPI Performance for QA supports multi-tenant architecture configured in NNMi. Multi-tenancy is useful to customize the views and restricts visibility to parts of the network based on the user's areas of responsibility. In NNMi, a tenant is the top-level organization to which a node belongs. Tenants enable you to partition your network across multiple customers. This feature restricts the access to certain objects such as QA Probes, and Sites in the NNM iSPI Performance for QA based on the tenant configuration, security group configuration, and user group configuration in NNMi.

See the topic *Configuring Security* in the *NNMi Online Help* for more information on Tenants and Security Groups.

Impact of Restricting Object Access

- QA Probe Inventory View: All QA probes cannot be viewed by all users either in a table view or a form view. For example, if a user has access to a set of nodes, the user can view only the QA probes configured on those nodes as source nodes.
- View a Site: A user can view a source site and destination site only if at least one of the QA probes associated with the source site can be accessed by the user.
- Site Map: A user can view the site map only if any one of the QA probes of the site can be accessed by the user.
- Real Time Line Graph: A user can view the Real Time Line graph only if the source node or the QA probe can be accessed by the user.
- Incidents: A user can view only those incidents where the source node or QA probe can be accessed by the user.

- Reports: Multi-tenancy is also applicable for the Network Performance Server and restricts a user to view only selective QA probes and reports. For example, while generating Top N report, a user can view the report for the probes that can be accessed by the user.

An administrator can create, update, and delete all configurations whereas other users can only view the configuration details, and no multi-tenancy is required as the configuration is allowed based on the user group.

See the topic *NNMi Security and Multi-Tenancy* in the *HP Network Node Manager i Software Deployment Reference* guide for more information.

Understand the Site, Threshold, and Probe Configurations

Site Configuration

- A site is a collection of QA probes configured on the network elements managed by NNMi. A network element can be a node, an interface, a Virtual Routing and Forwarding instance (VRF) in a Virtual Private Network (VPN), and so on. The NNM iSPI Performance for QA enables you to create sites when you need to categorize these network elements into groups. For example, a site can be created based on the geographic proximity of the network elements, the similar node groups, or similar node IDs.
- Sites can be created based on NNMi Node Groups, IP Address ranges, Probe Name patterns, or VRFs.
- Sites are identified by their names. A site name must be unique. Site names are case-sensitive.
- The NNM iSPI Performance for QA enables you to export the new or updated site configurations in an XML file and import them whenever required. You can specify the location to store the XML file.

You can export the existing site configuration using the following command line utility:

For Linux:

```
$NnmInstallDir/bin/nmsqasiteconfigutil.ovpl -u <username> -p
<password> –export <filename>;
```

For Windows:

```
%NnmInstallDir%\bin\nmsqasiteconfigutil.ovpl -u <username> -p
<password> –export <filename>
```

where *<username>* and *<password>* are optional parameters.

See the topic "Exporting a Site" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help* for more information.

- NNM iSPI Performance for QA associates each QA probe with a specific site. A QA probe can be associated with only one source site.
- The QA probe associations for each site are recomputed during each configuration poll.
- HP Network Node Manager iSPI Performance for Quality Assurance Software associates the QA probes with the respective sites during the configuration poll. However, if there are changes in the site configuration, the probes can be associated to the site by clicking on **Recompute Probes Associations** in the Site Configuration form. The QA probe associations for a newly added or updated site are recomputed during the configuration poll.

  NNM iSPI Performance for QA reflects deletion of sites immediately and recomputes the QA probes associations for the deleted sites.

  See the topic *Re-Computing Probes Associated to a Site* in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help* for more information.
- The sites configured and exported in the NNM iSPI Performance for QA 9.2x version can be accessed in NNM iSPI Performance for QA 10.10 as well.
- NNM iSPI Performance for QA enables you to configure sites for a global manager or regional manager

- Local Sites: The sites configured in the local NNMi management server are referred to as Local Sites. The local sites are owned by the Manager on which it is configured.
- Remote Sites: The sites exported from the regional manager to the global manager are known as Remote Sites.

Threshold Configuration

- A threshold can be defined on all the metrics available for the QA probes associated with an existing site.
- While defining thresholds for sites, you must define a source site for the threshold, and you can define the destination site, if required.
- A threshold can be defined for the metrics of selective QA probes, which may or may not be associated to a site. This overrides the threshold values defined for the probes associated to a site.
- NNM iSPI Performance for QA calculates the threshold states for the metrics while polling the QA probe information.
- NNM iSPI Performance for QA enables you to generate incidents if a threshold is violated. You can monitor the network performance and generate an incident based on the count based threshold configuration or time based threshold configuration
- You can view the threshold state and incidents generated for each discovered QA probe using the QA Probes form or the Incident Inventory View of NNMi.

Note: For configuring thresholds for probes, it is recommended to use the QA group–based threshold configuration than the site-based threshold configuration. For more information about configuring thresholds for QA groups, see the *Adding QA Group Threshold Configuration* section in the NNM iSPI Performance for QA Help for Administrators.

Count Based Threshold Configuration

You can generate an incident based on the count or the consecutive number of times a metric violates the threshold value.

Time Based Threshold Configuration

Time based threshold configuration is useful when you intend to alert the user when the threshold breached state persists for more than a specific time period. This is derived by specifying X as the duration of time in minutes when the metric is in a threshold breached state within Y number of minutes (X-of-Y) specified in the sliding window.

Threshold States

The valid threshold states are listed below:

- High
- Nominal
- Low
- Not Polled
- Unavailable
- Threshold Not Set
- None

For more information, see the topic *Accessing the QA Probe Inventory View* of the *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help*.

Baseline Setting Configuration

Apart from the time based and count based threshold configuration, you can also do a baseline monitoring. Baseline monitoring is dynamic and updates the baseline state by comparing the extent of deviation from the average real-time data of the metric with the previous average values in a similar situation.

You can do a baseline deviation setting configuration for the selected site, service, and metric. An incident is generated and the baseline state transitions to Abnormal Range only if it meets all the criteria listed below:

- Exceeds the count or the number of standard deviation that is above the average value for the metric, or exceeds the count or the number of standard deviation that is below the average value for the metric. This count is specified in the Upper

Baseline Limit Deviations or Lower Baseline Limit Deviations for the selected metric in the baseline deviation settings configuration.

- Exceeds the duration for which the upper or lower baseline deviation persists in the specified sliding window duration

Baseline States

Baseline Monitoring sets a new state referred to as Baseline state for the QA probes. The valid baseline states for the QA probes are listed below:

- Normal Range
- Abnormal Range
- Unavailable
- Unset
- Not polled

QA Probes

QA probes can be categorized as Local QA probes and Remote QA Probes. Local QA probes are QA probes owned by the local NNMi management server. Remote QA Probes are primarily discovered and polled at the regional manager in a Global Network Management environment.

QA Probe Status

The valid QA probe statuses are listed below:

- No Status
- Normal
- Disabled
- Unknown
- Warning

- Major
- Critical

For more information, click on the *QA Probe Status* link in the topic *Accessing the QA Probe Inventory View* of the *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help*.

Probe Configuration

You can configure the QA probes (tests on network such as Cisco IPSLA tests) on the device managed by NNMi using the Probe Configuration form or the `nmsqaprobeconfig.ovpl` command line utility in NNM iSPI Performance for QA 10.10 version. Alternatively, you can configure probes on the devices by referring to the vendor-specific configuration guides.

The Probe configuration form enables you to do the following:

- Create a probe definition. You can specify the service, duration, and payload details of the probe, and so on.
- Create a template for probe definition that can be reused whenever required
- Deploy the probe, or save the probe details to a file and deploy at a later point of time
- View the Real Time Line graph for the metrics of QA probes that are deployed successfully
- Reconfigure the probes if the deployment for the configured probes fail
- View the probe list and template list
- View the pre-configured probes for a selected source and destination node

Basic Steps to Configure Probes

The steps to configure probes are as follows:

1. You can launch the Probe Configuration form from the Nodes Inventory, Network Overview, Interfaces Inventory, or IP Addresses inventory view.

2. Select the node, and click on **Actions → Quality Assurance → Probe Configuration**

   Note: Asterisk "*" symbol in the Probe Configuration form indicates the field is mandatory

3. Enter the source node details in the **Source Node Details** section:

   a. Select the source hostname for which you want to configure probes

   b. Optionally, enter the IP Address and the Write Community String of the source node

4. Enter the destination node details in the **Destination Node Details** section:

   a. Select the destination hostname. Leave this field blank if the destination node is not managed.

   b. Type the IP address.

5. To configure a probe, click on the **Probe Definition** tab and follow the steps below:

   a. In the **Protocol Details** section, enter the probe name and select the Service.

   b. After you select the service, you must enter the port number in the **Port Number** field of the **Source Node Details** and **Destination Node Details** section for all the services other than ICMP echo.

   c. Optionally, enter the VRF and ToS.

   d. In the **Duration Details** section, enter the frequency. For example enter the duration as 5 minutes. All the other fields in this section are optional.

   e. The fields in the **Payload Details** section appear based on the service selected. All the fields are optional, but **Codec Type** is mandatory for VoIP service.

   Note: You can either deploy the probe or add the probes to the list and deploy all the configured probes later. Also, you can save the probe configuration details to a file and deploy at a later point of time

6. To deploy a single probe, click on **Deploy**

7. To deploy probes in bulk, click **Add** and the probes gets added to the Probe List below. Click **Select All** in the Probe List, and click on **Deploy**
8. To save the probe configuration to a file, click on **Save**, and enter the absolute path of the file
9. To view whether the probes are deployed successfully, click **Deploy Status** tab

Note: You can also select a template from the drop-down list to use an existing probe definition.

For more information on configuring probes, see the topic *Configure Probes* in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help*.

Example

Consider a scenario where you need to configure and deploy probes of `UDP` service with a frequency of 5 minutes for a node. You can understand the basic probe configuration for such a scenario by following these steps:

1. Click on **Actions → Quality Assurance → Probe Configuration**
2. Select the hostname as `ciscope6524.test.example.com` in the **Source Node Details** section
3. Select the hostname as `ciscope2851.test.example.com` in the **Destination Node Details** section
4. Click on the **Probe Definition** tab to configure a probe
5. Enter the following in the **Protocol Details** section:
   a. Enter the probe name as `udptest` and select the `UDP` service from the Service drop-down list
   b. Enter the port number within the range `0-65535` in the Port Number field of the **Source Node Details** section and the **Destination Node Details** section
6. In the **Duration Details** section, enter the following:
   - Enter the frequency at which the specific QA probe test must be repeated as 5 minutes in the **Frequency** field

7. Click **Deploy** to deploy the probes on the node
8. Click **Deploy Status** tab to view the deployment status

Probe Maintenance

The probes that are discovered can be enabled, disabled, or deleted using the Probe Maintenance form.

To launch the Probe Maintenance form:

Select the probes in the QA Probe Inventory View, and then select **Actions** → **Quality Assurance** → **Probe Maintenance** in the NNMi console.

You can view the enable status, disable status, and deletion status as well.

Chapter 5: Configuring Access with Public Key Infrastructure Authentication

You can configure NNMi to map the Public Key Infrastructure (PKI) certificates to NNMi user accounts. As a result, you can log on to the NNMi console without having to type in the NNMi user name and password on the Login page. However, you will be prompted to provide NNMi user name and password again when you try to launch the NNM iSPI Performance for QA Configuration form, unless you perform additional steps to reconcile the mapping with the iSPI.

Note: When NNMi is configured to use the PKI authentication, it is mandatory for the iSPI to use the PKI authentication. Also, do not configure only the iSPI to use the PKI authentication when NNMi continues to use the credentials-based authentication.

Configuring the iSPI to use the PKI authentication involves the following tasks:

1. "Configuring NNMi" on the next page
2. "Configuring a Certificate Validation Method" on the next page
3. "Enabling SSL" on the next page
4. "Enabling and Disabling SSLv3 Ciphers" on page 32
5. "Configuring the NNM iSPI Performance for QA" on page 33

Note: When the NNM iSPI Performance for QA is configured in a High Availability (HA) environment, make sure that `nms-auth-config.xml` from the `%NnmDataDir%\nmsas\qa\conf\` or `/var/opt/OV/nmsas/qa/conf/` directory is replicated on to each cluster member, to use the PKI authentication.

Configuring NNMi

To configure NNMi to use the PKI authentication, follow the steps in the *Configuring NNMi to Support Public Key Infrastructure Authentication* section in the *HP Network Node Manager Deployment Reference*.

After configuring NNMi to use the PKI authentication, if you do not perform Task 4, you will be prompted to provide NNMi user name and password when you try to launch the NNM iSPI Performance for QA Configuration form.

Configuring a Certificate Validation Method

When NNMi is configured to use the PKI authentication, unauthorized access using invalid certificates must be prevented. You must perform additional steps to configure NNMi to use a certificate validation method—Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP).

Follow the steps in the *Certificate Validation (CRL and OCSP)* section in the *HP Network Node Manager Deployment Reference*.

Enabling SSL

To enable NNMi-NNM iSPI Performance for QA communication, SSL should be enabled in the NNM iSPI Performance for QA.

Modify the following parameters in the `extended.properties` file from the `%nnmdatadir%\shared\qa\conf` or `/var/opt/OV/shared/qa/conf` to enable SSL:

```
com.hp.ov.nms.spi.qa.spi.isSecure=true

com.hp.ov.nms.spi.qa.Nnm.isSecure=true
```

For the SSL configuration changes to take effect, restart the NNM iSPI Performance for QA processes by running the following commands:.

- `ovstop -c qajboss`
- `ovstart -c qajboss`

Enabling and Disabling SSLv3 Ciphers

To configure NNM iSPI Performance for QA to enable SSLv3 ciphers:

1. Open the following file:

   For Windows: `%NnmDataDir%\nmsas\qa\server.properties`

   For Linux: `$NnmDataDir/nmsas/qa/server.properties`

2. Uncomment the following line:

   ```
   #com.hp.ov.nms.ssl.PROTOCOLS =
   SSLv2Hello,SSLv3,TLSv1,TLSv1.1,TLSv1.2
   ```

   For example:

   ```
   com.hp.ov.nms.ssl.PROTOCOLS =
   SSLv2Hello,SSLv3,TLSv1,TLSv1.1,TLSv1.2
   ```

   Note: You can remove any protocols contained in this line.

3. Save the file.

To disable the SSLv3 ciphers after they have been enabled:

1. Open the following file:

   For Windows: `%NnmDataDir%\nmsas\qa\server.properties`

   For Linux: `$NnmDataDir/nmsas/qa/server.properties`

2. Reinsert the comment in the following line:
   `com.hp.ov.nms.ssl.PROTOCOLS =`
   `SSLv2Hello,SSLv3,TLSv1,TLSv1.1,TLSv1.2`

   For example:

```
#com.hp.ov.nms.ssl.PROTOCOLS =
SSLv2Hello,SSLv3,TLSv1,TLSv1.1,TLSv1.2
```

Note: You can remove any protocols contained in this line.

3. Save the file.

Configuring the NNM iSPI Performance for QA

Configuring NNM iSPI Performance for QA to use the PKI authentication essentially requires updating the `nms-auth-config.xml` file in the NNM iSPI Performance for QA's configuration data directory (`%NnmDataDir%\nmsas\qa\conf` on Windows; `/var/opt/OV/nmsas/qa/conf` on Linux) to reflect the changes done in the `nms-auth-config.xml` file on the NNMi management server.

To configure the NNM iSPI Performance for QA to use the PKI authentication, follow these steps:

1. Make sure that Task 1, Task 2, and Task 3 are complete.
2. Log on to the NNMi management server.
3. Navigate to the following directory:

   On Windows

   `%nnmdatadir%\nmsas\qa\conf`

   On Linux

   `/var/opt/OV/nmsas/qa/conf`
4. Open the `nms-auth-config.xml` file using a text editor.
5. Modify the `nms-auth-config.xml` file to match the changes done on the `nms-auth-config.xml` file in the NNMi management server (`%nnmdatadir%\nmsas\NNM\conf\` or `/var/opt/OV/nmsas/NNM/conf/`).

For more information on the required changes, see the "*Configuring NNMi for PKI (X.509 Certificate Authentication)*" section in the *HP Network Node Manager Deployment Reference*.

6. Save and close the file.
7. Run the following command:

   On Windows:

   ```
   %NnmInstallDir%\qa\bin\nmsqaauthconfigreload.ovpl
   ```

   On Linux:

   ```
   /opt/OV/qa/bin/nmsqaauthconfigreload.ovpl
   ```

Note: Do not enable the Single Sign-On feature when NNMi and the NNM iSPI Performance for QA are configured to use the Public Key Infrastructure (PKI) authentication.

For more information on Single Sign-On feature, see "*Enabling Single Sign-On*" topic in the *NNM iSPI Performance for QA Online Help*.

Chapter 6: Best Practices

Some of the best practices for deploying NNM iSPI Performance for QA are listed below:

- Refer to the *HP Network Node Manager i Software Ultimate Edition Support Matrix* available at http://h20230.www2.hp.com/selfsolve/manuals for the hardware sizing guidelines.
- Install NNM iSPI Performance for QA on the NNMi management server.
- Install NNM iSPI Performance for QA and NNM iSPI for MPLS on the same NNMi management server to integrate NNM iSPI Performance for QA with NNM iSPI for MPLS.
- Install NNM iSPI Performance for QA and NNM iSPI for IP Telephony on the same NNMi management server to integrate NNM iSPI Performance for QA with NNM iSPI for IP Telephony.
- Install NNMi on the management server before installing the NNM iSPIs for NNMi.
- Install the Network Performance Server before installing the NNM iSPI Performance for QA.
- Create the Web Service Client user for NNM iSPI Performance for QA in NNMi.
- Use the NNMi database (embedded PostgreSQL or Oracle) for NNM iSPI Performance for QA.
- Do not modify the value for the NNMi Java Naming and Directory Interface (JNDI) port in the Parameters for QA iSPI to NNMi and NNMi to QA iSPI Communication dialog box, while installing the NNM iSPI Performance for QA.
- Use secure mode of transmission. Select **isSecure** for secured communication in the Parameters for QA iSPI to NNMi and NNMi to QA iSPI Communication dialog box.
- You cannot modify the default HTTP and HTTPS ports in NNM iSPI Performance for QA.
- Look at the following file to find the ports you need to open up, if you have firewalls activated:

For Windows: `%NnmDataDir%\shared\qa\conf\nms-qa.ports.properties`

For Linux: `$NnmDataDir/shared/qa/conf/nms-qa.ports.properties`

- Start the QA process using the following command before you start using NNM iSPI Performance for QA:

  ```
  ovstart -c qajboss
  ```

- Before you start discovery and polling, configure discovery filters if required.
- After discovery, perform the following tasks as required:
  - If you have shadow routers configured, seed the shadow routers and set the SNMP community strings for the shadow routers. Do not set up the community strings for the physical routers.
  - Configure probes.
  - Configure sites.
  - Configure thresholds for sites, QA probes, or QA groups.
  - Export the site, QA group, and threshold configurations. You can edit the exported XML file manually.
  - Import the site, QA group, and threshold configurations.

NNM iSPI Performance for QA Administration

- NNM iSPI Performance for QA enables you to view the QA probes configured locally. You can also forward incidents from regional managers to global managers and consolidate the QA probes on the global manager.
- Use the following commands to backup and restore configuration information and polled data:
  - Backup: `nnmbackup.ovpl`
  - Restore: `nnmrestore.ovpl`

For information on these commands, see *NNMi Documentation Library > Reference Pages* in the NNMi console.

Chapter 7: Installing and Upgrading the NNM iSPI Performance for QA in an HA Cluster

You can install NNMi and NNM iSPI Performance for QA in a High Availability (HA) environment to achieve redundancy in your monitoring setup. The prerequisites to configure the NNM iSPI Performance for QA in an HA environment is similar to NNMi. For information, see the *NNMi 10.10 Deployment Reference*.

Configuring the NNM iSPI Performance for QA

You can configure the NNM iSPI Performance for QA for the following scenarios:

- Install NNMi and the NNM iSPI Performance for QA in your environment before configuring NNMi to run under HA. See "Configuring an HA Cluster on a Set of Systems with NNMi and iSPI Installed" below.
- Install and configure the NNM iSPI Performance for QA in an existing NNMi HA cluster environment. See "Installing the NNM iSPI Performance for QA in an Existing NNMi HA Cluster Environment" on page 45.

Configuring an HA Cluster on a Set of Systems with NNMi and iSPI Installed

If you have NNMi and the NNM iSPI Performance for QA installed on at least two systems, you can create an HA cluster and configure NNMi and the iSPI to run under HA.

You can configure NNMi and NNM iSPI Performance for QA on the primary node and secondary node in an HA environment. For more information on how to install NNMi in an HA environment, see *NNMi Deployment Reference*.

Configuring the NNM iSPI Performance for QA on the Primary Node

To configure the NNM iSPI Performance for QA on the primary node, follow these steps:

1. Install NNMi (with the necessary patch), NNM iSPI Performance for QA, and the latest patch for the NNM iSPI Performance for QA on the primary system (in the given sequence). For more information, see the *NNMi Interactive Installation Guide* and the *NNM iSPI Performance for QA Installation Guide*.

2. Configure the HA software on the systems and configure NNMi to run under HA. See the *NNMi Deployment Reference* for information on configuring NNMi to run under HA. Do not start the resource group while configuring NNMi to run under the HA (do not run the `nnmhastartrg.ovpl` command). If the resource group is already started, stop it with the following command:

   On Windows:

   `%NnmInstallDir%\misc\nnm\ha\nnmhastoprg.ovpl NNM <resource_group>`

   On Linux:

   `/opt/OV/bin/misc/nnm/ha/nnmhastoprg.ovpl NNM <resource_group>`

3. Configure the NNM iSPI Performance for QA on the primary (active) node:

   a. Run the following command to find the virtual hostname:

      `nnmofficialfqdn.ovpl`

   b. Modify the following files from the `/var/opt/OV/shared/qa/conf` or `%NnmdataDir%\shared\qa\conf` to replace the host name with the virtual FQDN for the following parameters:

File Name	Variable Name
`nms-qa.jvm.properties`	`-Dcom.hp.ov.nms.ssl.KEY_ALIAS`
`nms-qa.jvm.properties`	`-Djava.rmi.server.hostname`

File Name	Variable Name
nnm.extended.properties	com.hp.ov.nms.spi.qa.Nnm.hostname
nnm.extended.properties	com.hp.ov.nms.spi.qa.spi.hostname

c. Modify the server.properties file from the %nnmdatadir%\nmsas\qa or /var/opt/OV/nmsas/qa directory to reflect the virtual FQDN of the NNMi management server for the java.rmi.server.hostname and nmsas.server.net.hostname.private parameters.

d. Modify the login-config.xml file from the %nnminstalldir%\qa\server\conf or /opt/OV/qa/server/conf directory to reflect the virtual FQDN of the NNMi management server:

   - Open the login-config.xml file with a text editor.
   - Look for the element <module-option name="nnmAuthUrl">.
   - Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
   - Save the file.

e. Modify the server.properties file from the %nnminstalldir%\qa\server\ or /opt/OV/qa/server/ directory to reflect the virtual FQDN of the NNMi management server for the following parameters:
   - java.rmi.server.hostname
   - nmsas.server.net.hostname.private
   - java.rmi.server.hostname
   - nmsas.server.net.hostname.private
   - jboss.host.name
   - jboss.node.name
   - jboss.qualified.host.name

- nmsas.server.net.hostname
- nmsas.server.net.hostname.http

f. If any of the files listed below are modified, replicate them on each cluster member:

For Windows:

```
%NnmInstallDir%\qa\server\conf\logging.properties

%NnmInstallDir%\qa\server\deploy\jboss-logging.xml

%NnmDataDir%\nmsas\qa\conf\nms-auth-config.xml

%NnmDataDir%\shared\qa\conf\PingPair.conf

%NnmDataDir%\shared\qa\conf\discovery.exclude

%NnmDataDir%\shared\qa\conf\discovery.include
```

For Linux:

```
/var/opt/OV/qa/server/conf/logging.properties

/var/opt/OV/qa/server/deploy/jboss-logging.xml

/var/opt/OV/nmsas/qa/conf/nms-auth-config.xml

/var/opt/OV/shared/qa/conf/PingPair.conf

/var/opt/OV/shared/qa/conf/discovery.exclude

/var/opt/OV/shared/qa/conf/discovery.include
```

g. Run the following command to start the NNMi HA resource group:

For Windows:

```
%NnmInstallDir%\misc\nnm\ha\nnmhastartrg.ovpl NNM
<resource_group>
```

For Linux:

```
/opt/OV/misc/nnm/ha/nnmhastartrg.ovpl NNM <resource_group>
```

For more information, see *NNMi Deployment Reference* guide.

The NNM iSPI Performance for QA and NNMi must start after this step. If NNMi or the NNM iSPI Performance for QA does not start, see *Troubleshooting the HA Configuration* from *NNMi Deployment Reference*.

h. Run the following command to configure the NNM iSPI Performance for QA to run under the HA cluster:

For Windows:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon
QASPIHA
```

For Linux:

```
/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon QASPIHA
```

Configuring the NNM iSPI Performance for QA on the Secondary Node

To configure the NNM iSPI Performance for QA on the secondary node, follow these steps:

1. Install NNMi (with the necessary patch), the NNM iSPI Performance for QA, and the latest patch for the NNM iSPI Performance for QA on the secondary system (in the given sequence). For more information, see the *NNMi Interactive Installation Guide* and the *NNM iSPI Performance for QA Installation Guide*.
2. Configure the NNM iSPI Performance for QA on the secondary (passive) node:
   a. Run the following command to find the virtual hostname:

   ```
   nnmofficialfqdn.ovpl
   ```

   b. Modify the following files from the `/var/opt/OV/shared/qa/conf` or `%NnmdataDir%\shared\qa\conf`to replace the host name with the virtual FQDN for the following parameters:

File Name	Variable Name
`nms-qa.jvm.properties`	`-Dcom.hp.ov.nms.ssl.KEY_ALIAS`

File Name	Variable Name
nms-qa.jvm.properties	-Djava.rmi.server.hostname
nnm.extended.properties	com.hp.ov.nms.spi.qa.Nnm.hostname
nnm.extended.properties	com.hp.ov.nms.spi.qa.spi.hostname

c. Modify the `server.properties` file from the `%nnmdatadir%\nmsas\qa` or `/var/opt/OV/nmsas/qa` directory to reflect the virtual FQDN of the NNMi management server for the `java.rmi.server.hostname` and `nmsas.server.net.hostname.private` parameters.

d. Modify the `login-config.xml` file from the `%nnminstalldir%\qa\server\conf` or `/opt/OV/qa/server/conf` directory to reflect the virtual FQDN of the NNMi management server:

   - Open the `login-config.xml` file with a text editor.
   - Look for the element `< module-option name="nnmAuthUrl">`.
   - Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
   - Save the file.

e. Modify the `server.properties` file from the `%nnminstalldir%\qa\server\` or `/opt/OV/qa/server/` directory to reflect the virtual FQDN of the NNMi management server for the following parameters:

   - `java.rmi.server.hostname`
   - `nmsas.server.net.hostname.private`
   - `java.rmi.server.hostname`
   - `nmsas.server.net.hostname.private`
   - `jboss.host.name`
   - `jboss.node.name`

- jboss.qualified.host.name
- nmsas.server.net.hostname
- nmsas.server.net.hostname.http

f. If any of the files listed below are modified, replicate them on each cluster member:

For Windows:

```
%NnmInstallDir%\qa\server\conf\logging.properties

%NnmInstallDir%\qa\server\deploy\jboss-logging.xml

%NnmDataDir%\nmsas\qa\conf\nms-auth-config.xml

%NnmDataDir%\shared\qa\conf\PingPair.conf

%NnmDataDir%\shared\qa\conf\discovery.exclude

%NnmDataDir%\shared\qa\conf\discovery.include
```

For Linux:

```
/var/opt/OV/qa/server/conf/logging.properties

/var/opt/OV/qa/server/deploy/jboss-logging.xml

/var/opt/OV/nmsas/qa/conf/nms-auth-config.xml

/var/opt/OV/shared/qa/conf/PingPair.conf

/var/opt/OV/shared/qa/conf/discovery.exclude

/var/opt/OV/shared/qa/conf/discovery.include
```

g. Run the following commands to configure the NNM iSPI Performance for QA on the secondary node to run under the HA cluster:

For Windows:

```
%NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon
QASPIHA
```

For Linux:

```
/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon QASPIHA
```

h. Repeat the procedure if you have additional secondary nodes in the HA cluster.

i. Optionally, test the configuration by failing over to a passive node and failing back to the original node.

Installing the NNM iSPI Performance for QA in an Existing NNMi HA Cluster Environment

You can configure the NNM iSPI Performance for QA in an NNMi HA cluster environment. For more information on how to install NNMi in an HA environment, see the *NNMi Deployment Reference.*

1. Make sure that NNMi is running on the active node.
2. Log on to the active node.
3. Put the NNMi resource group to the HA maintenance mode by placing the `maintenance` file under the following directory:

   On Windows

   `%nnmdatadir%\hacluster\<resource_group_name>`

   On Linux

   `$NnmDataDir/hacluster/<resource_group_name>`
4. Run `ovstatus -c` to make sure that `ovjboss` is running.
5. Install the latest NNMi patch, the NNM iSPI Performance for QA and the latest patch for the NNM iSPI Performance for QA (in the given sequence), but do *not* start the iSPI.
6. Remove the `maintenance` file that you added in step 3.
7. Initiate a failover to a passive node in the cluster where you want to install the NNM iSPI Performance for QA. Make sure that NNMi fails over successfully.
8. On this system, follow these steps:

a. Put the NNMi resource group to the HA maintenance mode by placing the `maintenance` file under the following directory:

   `%nnmdatadir%\hacluster\<resource_group_name>`

   `$NnmDataDir/hacluster/<resource_group_name>`

b. Run `ovstatus -c` to make sure that `ovjboss` is running.

c. Install the latest NNMi patch, the NNM iSPI Performance for QA, and the latest patch for the NNM iSPI Performance for QA (in the given sequence). However, do *not* start the iSPI.

d. Modify the following files from the `/var/opt/OV/shared/qa/conf` or `%NnmdataDir%\shared\qa\conf` to replace the host name with the virtual FQDN for the following parameters :

File Name	Variable Name
`nms-qa.jvm.properties`	`-Dcom.hp.ov.nms.ssl.KEY_ALIAS`
`nms-qa.jvm.properties`	`-Djava.rmi.server.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.qa.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.qa.spi.hostname`

e. Modify the `login-config.xml` file from the `%nnminstalldir%\qa\server\conf` or `/opt/OV/qa/server/conf` directory to reflect the virtual FQDN of the NNMi management server:

   - Open the `login-config.xml` file with a text editor.
   - Look for the element `<module-option name="nnmAuthUrl">`.
   - Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
   - Save the file.

f. If any of the files listed below are modified, replicate them on each cluster

member:

For Windows:

```
%NnmInstallDir%\qa\server\conf\logging.properties

%NnmInstallDir%\qa\server\deploy\jboss-logging.xml

%NnmDataDir%\nmsas\qa\conf\nms-auth-config.xml

%NnmDataDir%\shared\qa\conf\PingPair.conf

%NnmDataDir%\shared\qa\conf\discovery.exclude

%NnmDataDir%\shared\qa\conf\discovery.include
```

For Linux:

```
/var/opt/OV/qa/server/conf/logging.properties

/var/opt/OV/qa/server/deploy/jboss-logging.xml

/var/opt/OV/nmsas/qa/conf/nms-auth-config.xml

/var/opt/OV/shared/qa/conf/PingPair.conf

/var/opt/OV/shared/qa/conf/discovery.exclude

/var/opt/OV/shared/qa/conf/discovery.include
```

g. Remove the `maintenance` file that you added in step a.

9. If you have multiple nodes in the cluster, fail over to another passive node, and then repeat step a through step h.
10. Fail over to the server that was active when you started this procedure.
11. Run the following command on the active server first, and then on all passive servers:

    For Windows:

    ```
    %NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon
    QASPIHA
    ```

For Linux:

```
/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon QASPIHA
```

Note: Running the `nnmhaconfigure.ovpl`command updates the virtual host names in the server.property files. However, it is recommended to check the values after configuring the High-Availability cluster, and in case they are not updated, they must be manually updated. To manually update, go to the server.properties file from the `%nnmdatadir%\nmsas\qa` or `/var/opt/OV/nmsas/qa` directory and update the virtual FQDN of the NNMi management server for the `java.rmi.server.hostname` and `nmsas.server.net.hostname.private` parameters.

12. Verify that the NNM iSPI Performance for QA is successfully registered by running the following command:

    On Windows:

    ```
    %nnminstalldir%\misc\nnm\ha\nnmhaclusterinfo.ovpl –config NNM
    –get NNM_ADD_ON_PRODUCTS
    ```

    On Linux:

    ```
    /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl –config NNM –get
    NNM_ADD_ON_PRODUCTS
    ```

Upgrading the NNM iSPI Performance for QA in an HA Cluster

To upgrade the NNM iSPI Performance for QA to the version 10.10 in an HA cluster, follow these steps:

1. On the active node in the cluster, follow these steps:

    a. Put the NNMi resource group to the HA maintenance mode by placing the `maintenance` file under the following directory:

    On Windows

`%nnmdatadir%\hacluster\<resource_group_name>`

On Linux

`/var/opt/OV/hacluster/<resource_group_name>`

b. Upgrade NNMi to the version 10.10(with the necessary patch). See the *NNMi Deployment Reference* for more information.

c. Run `ovstatus -c` to make sure that `ovjboss` is running.

d. Upgrade the NNM iSPI Performance for QA to the version 10.10, and then install the latest patch for the NNM iSPI Performance for QA. However, do *not* start any iSPI processes.

e. Make sure that the following files from the `/var/opt/OV/shared/qa/conf` or `%NnmdataDir%\shared\qa\conf` contain the virtual FQDN for the following parameters :

File Name	Variable Name
`nms-qa.jvm.properties`	`-Dcom.hp.ov.nms.ssl.KEY_ALIAS`
`nms-qa.jvm.properties`	`-Djava.rmi.server.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.qa.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.qa.spi.hostname`

f. Make sure that the `server.properties` file from the `%nnmdatadir%\nmsas\qa` or `/var/opt/OV/nmsas/qa` directory contains the virtual FQDN of the NNMi management server for the `java.rmi.server.hostname` and `nmsas.server.net.hostname.private` parameters.

g. Modify the `login-config.xml` file from the `%nnminstalldir%\qa\server\conf` or `/opt/OV/qa/server/conf` directory to reflect the virtual FQDN of the NNMi management server:

- Open the `login-config.xml` file with a text editor.
- Look for the element `<module-option name="nnmAuthUrl">`.
- Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
- Save the file.

h. Run the following command:

```
ovstart -c qajboss
```

2. On the passive node in the cluster, follow these steps:

a. Put the NNMi resource group to the HA maintenance mode by placing the `maintenance` file under the following directory:

On Windows

`%nnmdatadir%\hacluster\<resource_group_name>`

On Linux

`/var/opt/OV/hacluster/<resource_group_name>`

b. Upgrade NNMi to the version 10.10 (with the necessary patch). See the *NNMi Deployment Reference* for more information.

c. Upgrade the NNM iSPI Performance for QA to the version 10.10, and then install the latest patch for the NNM iSPI Performance for QA. However, do *not* start any processes.

d. Make sure that the following files from the `/var/opt/OV/shared/qa/conf` or `%NnmdataDir%\shared\qa\conf` contain the virtual FQDN for the following parameters :

File Name	Variable Name
`nms-qa.jvm.properties`	`-Dcom.hp.ov.nms.ssl.KEY_ALIAS`
`nms-qa.jvm.properties`	`-Djava.rmi.server.hostname`

File Name	Variable Name
nnm.extended.properties	com.hp.ov.nms.spi.qa.Nnm.hostname
nnm.extended.properties	com.hp.ov.nms.spi.qa.spi.hostname

e. Make sure that the `server.properties` file from the `%nnmdatadir%\nmsas\qa` or `/var/opt/OV/nmsas/qa` directory contains the virtual FQDN of the NNMi management server for the `java.rmi.server.hostname` and `nmsas.server.net.hostname.private` parameters.

f. Modify the `login-config.xml` file from the `%nnminstalldir%\qa\server\conf` or `/opt/OV/qa/server/conf` directory to reflect the virtual FQDN of the NNMi management server:

- Open the `login-config.xml` file with a text editor.
- Look for the element `<module-option name="nnmAuthUrl">`.
- Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.
- Save the file.

3. Repeat step 2 on each passive node.
4. Remove the `maintenance` file from all passive nodes in the cluster.
5. Remove the `maintenance` file from the active node.

Tuning the Time Out Parameters

Depending on the type of cluster software used, you must tune the time out parameters for an HA deployment.

The important time out parameters to be tuned for Veritas Cluster Software are listed below:

- OfflineTimeout
- OnlineTimeout
- MonitorTimeout

The important time out parameters to be tuned for Windows Cluster Manager software are listed below:

- PendingTimeout
- Deadlock Timeout parameters

You must modify or tune these parameters specifically when you have installed two or more NNM iSPI products on the same NNMi management server.

Patching the NNM iSPI Performance for QA Under HA

If you have already configured NNMi and the NNM iSPI Performance for QA to work in an HA cluster, you must follow this section to apply necessary patches (for both NNMi and the NNM iSPI Performance for QA).

To apply patches for NNMi and the NNM iSPI Performance for QA, follow these steps:

1. Determine which node in the HA cluster is active:
   - Windows:

     ```
     %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -group
     <resource_group> -activeNode
     ```

   - Linux:

     ```
     $NnmInstallDir/misc/nnm/ha/nnmhaclusterinfo.ovpl -group
     <resource_group> -activeNode
     ```

2. On the active node, put the NNMi HA resource group into maintenance mode by creating the following file:

- Windows:

  ```
  %NnmDataDir%\hacluster\<resource_group>\maintenance
  ```

- Linux:

  ```
  $NnmDataDir/hacluster/<resource_group>/maintenance
  ```

  Include the `NORESTART` keyword.

3. On all passive nodes, put the NNMi HA resource group into maintenance mode by creating the following file:

   - Windows:

     ```
     %NnmDataDir%\hacluster\<resource_group>\maintenance
     ```

   - Linux:

     ```
     $NnmDataDir/hacluster/<resource_group>/maintenance
     ```

     Include the `NORESTART` keyword.

4. On the active node, follow these steps:

   a. Stop NNMi:

      ```
      ovstop -c
      ```

   b. Back up the shared disk by performing a disk copy.

   c. *Optional*. Use the `nnmbackup.ovpl` command, or another database command, to back up all NNMi data. For example:

      ```
      nnmbackup.ovpl -type offline -scope all -target nnmi_
      backups
      ```

      For more information about this command, see "NNMi Backup and Restore Tools" section in the *NNMi Deployment Reference*.

   d. Apply the appropriate NNMi and NNM iSPI patches to the system.

   e. Start NNMi:

      ```
      ovstart -c
      ```

f. Verify that NNMi started correctly:

```
ovstatus -c
```

All NNMi services should show the state `RUNNING`.

5. On each passive node, apply the appropriate patches to the system.
6. On all passive nodes, take the NNMi HA resource group out of maintenance mode by deleting the maintenance file from the nodes.
7. On the active node, take the NNMi HA resource group out of maintenance mode by deleting the maintenance file from that node.

Unconfiguring the NNM iSPI Performance for QA from an HA Cluster

To remove the NNM iSPI Performance for QA from an HA cluster environment, first remove the NNM iSPI Performance for QA from the secondary node and then from the primary node.

To remove the NNM iSPI Performance for QA from an HA cluster environment, follow these steps:

1. Run the following command to remove the NNM iSPI Performance for QA:

   For Windows:

   ```
   %NnmInstallDir%\misc\nnm\ha\nnmhaunconfigure.ovpl NNM -addon
   QASPIHA
   ```

   For Linux:

   ```
   $NnmInstallDir/misc/nnm/ha/nnmhaunconfigure.ovpl NNM -addon
   QASPIHA
   ```

2. Remove NNMi from the HA cluster environment. For information, see *NNMi Deployment Reference*.

Running NNM iSPI Performance for QA Outside HA

To run the NNM iSPI Performance for QA outside HA cluster environment:

1. Follow the steps in *Running NNMi Outside HA with the Existing Database* section given in *NNMi Deployment Reference*. However, do not start the processes.
2. Make sure NNMi is not running. If NNMi is running, stop it by running the following command:

   ```
   ovstop -c
   ```

   Note: If required, you can take a backup of all the old QA log files located at `%NnmDataDir%\log\QA` or `/var/opt/OV/log/QA`.
3. Run the following command to find the host name:

   ```
   nnmofficialfqdn.ovpl
   ```
4. Replace the virtual FQDN with the host name in all the files that were modified to replace the host name with the virtual FQDN during configuring NNM iSPI Performance for QA for HA cluster environment.
5. Create a folder named QA at `%NnmDataDir%\log\` or `/var/opt/OV/log`.
6. Run the following command to start NNMi:

   ```
   ovstart -c
   ```

Chapter 8: Deploying the NNM iSPI Performance for QA in Application Failover Environment

Configuration tasks to configure application failover for the NNM iSPI Performance for QA are similar to the configuration tasks to configure NNMi for application failover. Refer to the *NNMi Deployment Reference* guide for information on these configuration tasks.

Note: The web service client user name and password must be same on both the primary and standby servers.

Deploying the NNM iSPI Performance for QA for Application Failover Using an Oracle Database

Scenario 1: The NNM iSPI Performance for QA is Installed with NNMi and Application Failover is configured on NNMi

In this scenario, you can make the following assumptions:

- NNMi is installed in the Primary server mode in System1.
- NNMi is installed in the Secondary server mode in System2.
- Oracle is installed with Primary and Secondary server enabled for the application failover environment.

Follow these steps to deploy NNM iSPI Performance for QA in an application failover environment:

1. Start NNMi on System1 as Primary server and install the NNM iSPI Performance for QA on System1.
2. Install the NNM iSPI Performance for QA with Oracle Database by following the procedure explained in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Installation* guide.
3. Merge the keystores on either System1 or System2 and copy them to the other system. For information on how to merge the keystores and copy them to another system, see the contents in the *NNMi Deployment Reference*.
4. Stop NNMi on System1.
5. Stop NNMi on System2.
6. Install the NNM iSPI Performance for QA on System2.

   To install the NNM iSPI Performance for QA on the Secondary server (System2) provide the same database instance used on the Primary server (System1).

Configure the NNM iSPI Performance for QA for application failover between System1 and System2. The steps to configure the NNM iSPI Performance for QA for application failover are similar to the steps to configure NNMi for application failover. For information on how to configure the NNM iSPI Performance for QA for application failover, see the contents in the *NNMi Deployment Reference*.

Scenario 2: The NNM iSPI Performance for QA is Installed after NNMi is Configured for Application Failover

1. Remove configuration for application failover from the NNMi Primary and Secondary servers.
2. Restore the old keystore and truststore specific to the Primary server and the Secondary server.
3. Install the NNM iSPI Performance for QA on both Primary and Secondary servers.

4. Follow instructions documented in the NNMi Deployment Reference Guide to configure NNMi in an application failover mode. After this, the NNM iSPI Performance for QA automatically gets configured in the application failover mode.

Deploying the NNM iSPI Performance for QA for Application Failover Using the Embedded PostgreSQL Database

Scenario 1: The NNM iSPI Performance for QA is Installed with NNMi and Application Failover is Configured on NNMi

In this scenario, you can make the following assumptions:

The NNM iSPI Performance for QA and NNMi are installed on stand-alone systems.

If NNMi is configured for application failover, the NNM iSPI Performance for QA automatically gets configured for application failover.

Scenario 2: The NNM iSPI Performance for QA is Installed after NNMi is Configured for Application Failover

1. Remove the NNMi application failover from the Primary and Secondary servers.
2. Restore the old keystore and truststore specific to the Primary server and the Secondary server. See the contents of the *NNMi Deployment Reference* guide for instructions.
3. Install the NNM iSPI Performance for QA on both Primary and Secondary servers.

4. Follow instructions documented in the NNMi Deployment Reference Guide to configure NNMi in an application failover mode. After this, the NNM iSPI Performance for QA automatically gets configured in the application failover mode.

Patching the NNM iSPI Performance for QA in an Application Failover Environment

If you have already configured the NNMi and NNM iSPI Performance for QA 10.10 to work in an application failover environment, you must follow this section to apply necessary patches (for both NNMi and NNM iSPI Performance for QA).

Both NNMi management servers must be running the same NNMi version and patch level. To add patches to the active and standby NNMi management servers, use the below procedure:

Applying Patches for Application Failover (Shut Down Both Active and Standby)

You can use this procedure when you are not concerned with an interruption in network monitoring.

This procedure results in both NNMi management servers being non-active for some period of time during the patch process. To apply patches to the NNMi management servers configured for application failover, follow these steps:

1. As a precaution, back up your NNMi data on both the active and standby NNMi management servers before proceeding. For information, see NNMi Backup and Restore Tools in the NNMi Deployment Reference.

2. As a precaution, on the active NNMi management server, do the following steps:

   a. Run the `nnmcluster` command.

   b. Embedded database only: After NNMi prompts you, type **`dbsync`**, then press **Enter**. Review the displayed information to make sure it includes the following messages:

      `ACTIVE_DB_BACKUP`: This means that the active NNMi management server is performing a new backup.

ACTIVE_NNM_RUNNING: This means that the active NNMi management server completed the backup referred to by the previous message.

STANDBY_READY: This shows the previous status of the standby NNMi management server.

STANDBY_RECV_DBZIP: This means that the standby NNMi management server is receiving a new backup from the active NNMi management server.

STANDBY_READY: This means that the standby NNMi management server is ready to perform if the active NNMi management server fails.

3. Run the `nnmcluster -halt` command on both the active and standby NNMi management server. This shuts down all nnmcluster processes on both the active and standby NNMi management servers.
4. To verify there are no nnmcluster nodes running on either server, complete the following steps on both the active and standby NNMi management servers:
   a. Run the `nnmcluster` command.
   b. Verify that there are no nnmcluster nodes present except the one marked (SELF).
   c. Run `exit` or `quit` to stop the interactive nnmcluster process you started.
5. On the active NNMi management server, comment out the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
   a. Edit the following file:

      On Windows:

      `%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`

      On Linux:

      `/var/opt/OV/shared/nnm/conf/props/nms-cluster.properties`

   b. Comment out the `com.hp.ov.nms.cluster.name` parameter.
   c. Save your changes.

6. Apply the NNMi and the NNM iSPI Performance for QA patch to the active NNMi management server using the instructions provided with the patch.
7. On the active NNMi management server, uncomment the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
   a. Edit the following file:

      On Windows:

      `%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`

      On Linux:

      `/var/opt/OV/shared/nnm/conf/props/nms-cluster.properties`

   b. Uncomment the `com.hp.ov.nms.cluster.name` parameter.
   c. Save your changes.
8. Run the `nnmcluster –daemon` command on the active NNMi management server.
9. Run the `nnmcluster -dbsync` command to create a new backup.
10. On the standby NNMi management server, comment out the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
11. Apply the NNMi and the NNM iSPI Performance for QA patch to the standby NNMi management server.
12. On the standby NNMi management server, uncomment the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
13. Run the `nnmcluster -daemon` command on the standby NNMi management server.

Disabling Application Failover for the NNM iSPI Performance for QA

To disable the application failover for the NNM iSPI Performance for QA, follow these steps:

1. Disable application failover for the NNM iSPI Performance for QA by following the steps discussed in the “Disabling NNMi for Application Failover” section in the *NNMi Deployment Reference*.
2. Restore the keystore and the truststore for the systems that you backed up before configuring them for application failover.

Chapter 9: Deploying NNM iSPI Performance for QA in a Global Network Management Environment

The Global Network Management (GNM) feature in NNM iSPI Performance for QA is useful in large scale enterprise networks where you need to monitor the overall network performance. Consider a scenario where the HP Network Node Manager iSPI Performance for Quality Assurance Software is deployed on multiple NNMi management servers in several geographic locations or sites. The QA probes are discovered and monitored in each NNMi management server. However, you may be interested to monitor the QA probes of two or more NNMi management servers in a single QA Probe inventory view. In such instances, you can designate a specific NNMi management server as *global manager* which enables you to monitor the QA probes discovered in other NNMi management servers referred to as *regional managers*. The GNM feature enables you to get a holistic view of all the regional managers in an enterprise network.

The NNM iSPI Performance for QA extends the capabilities of NNMi global manager, and provides a centralized view to monitor multiple regional managers in a distributed network environment. The NNM iSPI Performance for QA enables you to configure the regional manager connections using the Quality Assurance Global Network Management Configuration form. After you establish the connection, you can view and monitor the QA probes discovered across the regional managers from the QA Probe view of the global manager.

For more information on how to configure the NNM iSPI Performance for QA regional managers, see the topic "NNM iSPI Performance for QA Global Network Management Configuration" in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help*.

Connecting Global Manager to Regional Managers

You can add regional manager connections to the global manager. A regional manager connection must be established in NNMi before configuring the connection in NNM iSPI Performance for QA. Make sure that all NNMi management servers in your network environment that participate in global network management (global managers and regional managers) have their internal time clocks synchronized in universal time. The global manager and regional managers configured in NNMi must be the same in NNM iSPI Performance for QA. For example, a regional manager in NNMi cannot be a global manager in NNM iSPI Performance for QA. Also, you must make sure that the regional manager connection name specified in NNM iSPI Performance for QA is the same as the connection name specified in NNMi. For more information, to add a regional manager connection, see the "Adding a Regional Manager Connection" topic in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help*.

While you add the regional manager connection, you must also decide the connection sequence for monitoring the common QA probes across regional managers. The global manager considers the common QA probes of the regional manager that is first connected and ignores the common QA probes of the regional managers configured later.

Disconnecting Communication between the Global Manager and Regional Managers

Typically, you shut down the global manager when you do not intend to use the global manager permanently or stop the usage of global manager for a long period. In such instances, you must check if the global manager has any active subscriptions to the regional managers. You must disconnect the associated regional managers before you shut down the global manager. For more information, to delete a Regional Manager Connection, see the "Deleting an Existing Regional Manager" topic in the *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help*.

Deployment Scenarios

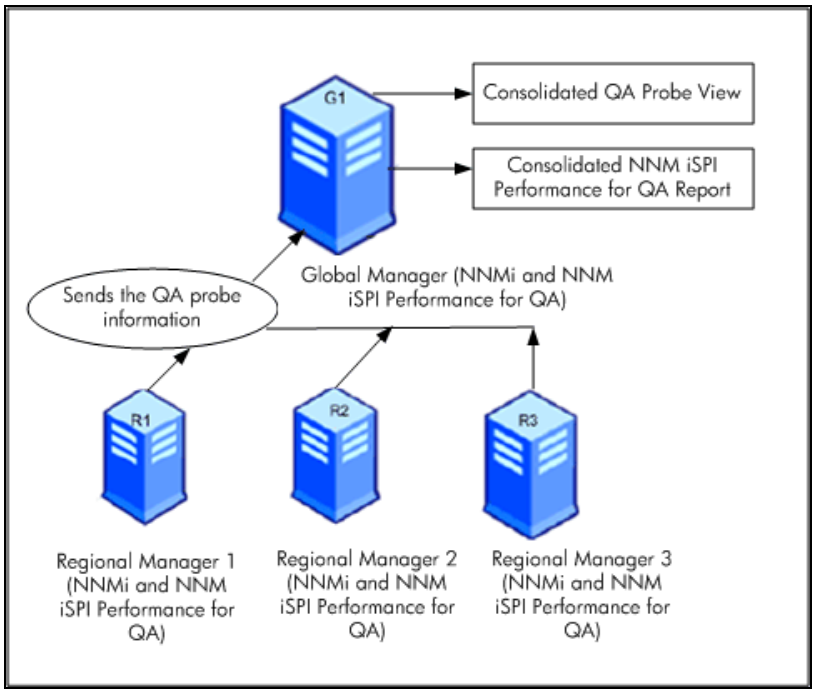
You can deploy NNMi and NNM iSPI Performance for QA in a GNM environment for the following possible scenarios:

- Deploy NNMi and NNM iSPI Performance for QA on the global manager and regional manager
- Deploy only NNMi on the global manager, and deploy NNMi and NNM iSPI Performance for QA on the regional manager
- Deploy NNMi and NNM iSPI Performance for QA on the global manager and deploy only NNMi on the regional manager
- Deploy global manager or regional manager in an Application Failover environment

For more information on the deployment in a Global Network Management environment, see the topic "*Global Network Management*" in the *HP Network Node Manager i Software Deployment Reference*.

Deploying NNMi and NNM iSPI Performance for QA on the Global Manager and Regional Manager

You can install and configure NNMi and the NNM iSPI Performance for QA on the global manager and regional managers. For information on the configuration steps, see *NNMi Online Help* and *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help*. The following figure represents a deployment scenario, where NNMi and NNM iSPI Performance for QA are configured on the global manager (G1) and regional managers (R1, R2, and R3). In this deployment scenario, all the regional managers (R1, R2, and R3) send the QA probe information to the global manager (G1). You can view the following information from G1:

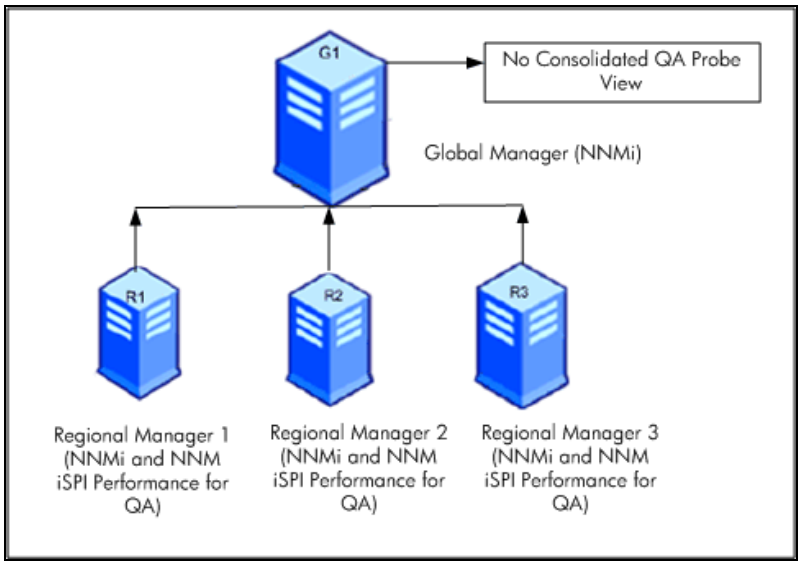


Consolidated NNM iSPI Performance for QA topology: All the regional managers (R1, R2, and R3) send the QA probe information to the global manager (G1).

Consolidated NNM iSPI Performance for QA Report: You can view the consolidated NNM iSPI Performance for QA reports.

Deploying only NNMi on the Global Manager and NNMi, NNM iSPI Performance for QA on the Regional Manager

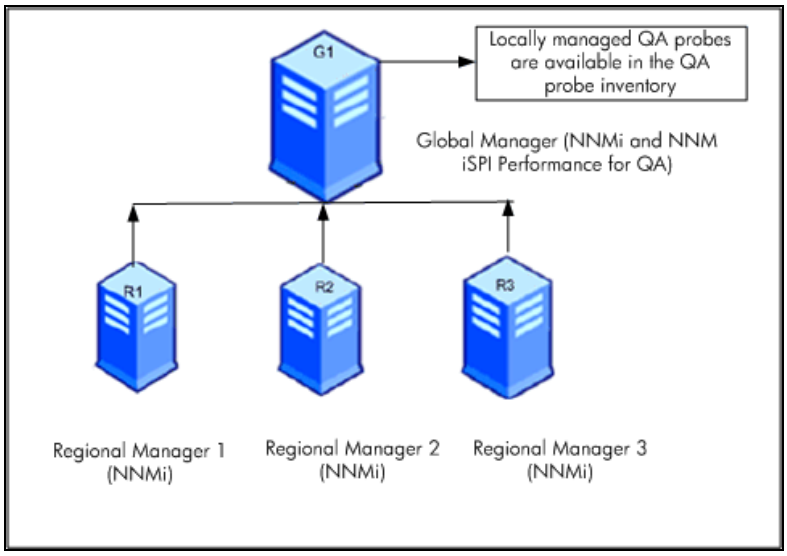
You can install and configure NNMi on the global manager and NNMi, NNM iSPI Performance for QA on the regional managers. For information on the configuration steps, see the *HP Network Node Manager i Software Online Help* and *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help*. The following figure represents a deployment scenario where NNMi is configured on the global manager (G1), and NNMi, NNM iSPI Performance for QA are configured on the regional managers (R1, R2, and R3):



In this deployment scenario, all the regional managers (R1, R2, and R3) discover the QA probes configured in the network managed by the regional managers (R1, R2 and R3). The NNM iSPI Performance for QA is not available on G1, so there is no communication established between G1 and regional managers. Thus, the NNM iSPI Performance for QA nodes from the regional managers are not available in the G1 inventory. In addition, no aggregated NNM iSPI Performance for QA reports are available in the global manager inventory.

Deploying NNMi and NNM iSPI Performance for QA on the Global Manager and NNMi on the Regional Manager

You can install and configure NNMi and the NNM iSPI Performance for QA on the global manager and only NNMi on the regional managers. For information on the configuration steps, see in the *NNMi Online Help* and *HP Network Node Manager iSPI Performance for Quality Assurance Software Online Help*. The following figure represents a deployment scenario, where NNMi and NNM iSPI Performance for QA are configured on the global manager (G1) and NNMi on the regional managers (R1, R2, and R3):



In this deployment scenario, only the locally managed QA probes are available in the QA probe inventory.

Deploying the Global Manager or Regional Manager in an Application Failover Environment

When the NNM iSPI Performance for QA regional manager is in the Application failover environment, use the `ORDERING` parameter to decide the priority to establish the connection. For example, during Application Failover, the regional manager connection with the `ORDERING` parameter value as 1 is given higher priority to establish connection than a regional manager with the `ORDERING` parameter as 2, and so on.

To deploy NNM iSPI Performance for QA in an application failover environment, follow these steps:

1. Configure the Regional Manager connection using *Quality Assurance Global Network Management Configuration* form
2. Add the two regional manager connections and provide the two hostnames.
3. Use the `ORDERING` parameter to give different values to the two Regional Managers.

Whenever there is an application fail-over on the regional manager, the global manager always use the lowest ordering value to establish the next connection.

You can configure the regional manager in the application failover environment by using the steps documented in the "Deploying the NNM iSPI Performance for QA for Application Failover Using an Oracle Database" on page 56 and "Deploying the NNM iSPI Performance for QA for Application Failover Using the Embedded PostgreSQL Database" on page 58.

Discovery in a GNM Environment

Discovery in a GNM environment triggers based on the sequence that you follow to discover probes. The two possible scenarios of deployment are listed below:

Scenario 1

Create regional manager connections to the global manager, and then seed the nodes at the regional managers. In this case, the probes that are discovered at the regional managers are automatically propagated to the global manager.

Scenario 2

You can discover the probes at the NNMi management server, and then connect the NNMi management server as the regional manager to the global manager. The probes of regional manager will be available at the global manager only after one discovery cycle. However, if you intend to manage QA probes of regional manager immediately at the global manager, you must run the following command at the regional manager:

```
nnmnoderediscover.ovpl -u <username> -p <password> -all
```

Alternatively, you can run the following command at the regional manager:

```
nmsqadisco.ovpl -u <username> -p <password> -node <nodename>
```

You can run the commands from the following directory:

For Linux:

```
$NnmInstallDir/bin
```

For Windows:

```
%NnmInstallDir%\bin
```

Site Configuration in a GNM Environment

In a GNM environment, you can configure sites on a global manager or a regional manager. Based on this configuration, sites can be categorized as follows:

- Local Sites: Sites configured in the local NNMi management server are referred to as Local Sites. The local sites are owned by the manager on which it is configured.
- Remote Sites: The sites exported from the regional manager to the global manager are known as Remote Sites.

Whenever you create, edit, or delete a site in the regional manager, the changes are propagated to the global manager. You can export local sites, but you cannot export or delete remote sites.

QA Probes Association

QA probes can be associated with either a local site or a remote site. Probes can be categorized as follows:

- Local QA Probes: Local QA probes are QA probes owned by the local manager.
- Remote QA Probes: Remote QA probes are primarily discovered and polled at the regional manager

If a QA probe associated with the remote site matches the local site, the QA probes of the local site overrides the remote site QA probes. In such instances, NNM iSPI Performance for QA overrides the site configuration and not the thresholds configured for the site. However, if there is no local site that matches the remote site, the QA probes are associated with the remote site.

Example:

Consider a network managed in a GNM environment with branch offices 1 and 2 monitored by regional managers R1 and R2 with the global manager as G1. Consider a set of sites configured in R1 and R2, which are exported to G1. The probes obtained from R1 and R2 are consolidated in G1.

If the sites matching the remote probes are configured in G1, the QA probes of G1 override the remote site QA probes. If there is no match, the remote QA probes are available in G1.

Threshold Configuration in a GNM Environment

In a GNM environment, the global manager receives the threshold states from the regional managers. You cannot configure thresholds for remote sites. The thresholds configured for the sites of the global managers are not applicable for the sites of regional managers.

Discovery Filter Configuration in a GNM Environment

You can set three types of discovery filters in a GNM environment, which are as follows:

- Discovery filter is selected to exclude the QA probes discovered on the network
- Regional Data Forwarding filter is configured in the regional manager and excludes the QA probes forwarded to the global manager
- Global Receiver filter is configured in the global manager and excludes the QA probes received by the global manager

If you add a Regional Data Forwarding filter and a Global Receiver filter, both the discovery filters will be applied on the QA probes in the global manager.

Multi-tenancy and Reporting in a GNM Environment

Multi-tenancy in a GNM environment is based on the user group, security group, and tenant configuration in NNMi.

The user group configuration for the users in a regional manager and the global manager are independent. The users for a regional manager are determined based on the user group configuration in NNMi for the regional manager. Likewise, the users for a global manager are determined based on the user group configuration in NNMi for the global manager.

If a user has access to a set of probes in a regional manager, the user can access only those probes. Also, a user can view the reports in the regional manager only if the user has access to the set of probes.

Likewise, in a global manager if a user has access to a set of probes, the user can access only those probes. Also, a user can view the reports in the global manager only if the user has access to the set of probes.

Chapter 10: Maintaining the NNM iSPI Performance for QA

Updating the Security Mode (HTTP to HTTPS)

After installing NNMi and the NNM iSPI Performance for QA, if you want to modify the security mode from HTTPS to HTTP or from HTTP to HTTPS without reinstalling NNMi and the NNM iSPI Performance for QA, follow these steps:

1. On the management server, open the `nnm.extended.properties` file from the `%NnmDataDir%\shared\qa\conf` directory with a text editor.

   On the management server, open the `nnm.extended.properties` file from the `$NnmDataDir/shared/qa/conf` directory with a text editor.

2. Update the values to true or false from the following:

   `com.hp.ov.nms.spi.qa.Nnm.isSecure=false`: To modify the mode of communication used by the NNM iSPI Performance for QA to communicate with NNMi.

   `com.hp.ov.nms.spi.qa.spi.isSecure=false`: To modify the mode of communicatikon used by NNMi to communicate with the NNM iSPI Performance for QA.

   The value TRUE represents HTTPS mode of communication and the value FALSE represents HTTP mode of communication.

   > **Note:** Always select the same mode of transmission for NNMi and the NNM iSPI Performance for QA.

3. Restart the NNM iSPI Performance for QA with the following commands:

   ```
   ovstop -c qajboss

   ovstart -c qajboss
   ```

Configuring the NNM iSPI Performance for QA to Use the Modified NNMi Ports

After installing the NNM iSPI Performance for QA, you can modify the following configuration parameters: NNMi HTTP port and HTTPS port

You can configure the NNM iSPI Performance for QA to use the modified NNMi ports by following the steps listed:

1. Open the `nms-local.properties` file available in the following directory:

   ```
   %NnmDataDir%\conf\nnm\props\nms-local.properties
   $NnmDataDir/conf/nnm/props/nms-local.properties
   ```

2. Obtain the values of the following properties: `nmsas.server.port.web.http` and `nmsas.server.port.web.https`

3. Open the `nnm.extended.properties` file from the `%NnmDataDir%\shared\qa\conf` directory with a text editor.

   Open the `nnm.extended.properties` file from the `$NnmDataDir/shared/qa/conf` directory with a text editor.

4. If you changed the NNMi HTTP port, replace the value for `com.hp.ov.nms.spi.qa.Nnm.port` property with the value of `nmsas.server.port.web.http` obtained in step 2.

5. If you changed the NNMi HTTPS port, replace the value for `com.hp.ov.nms.spi.qa.Nnm.secureport` property with the value of `nmsas.server.port.web.https` obtained in step 2.

6. Restart the NNM iSPI Performance for QA with the following commands:

   ```
   ovstop -c qajboss

   ovstart -c qajboss
   ```

Configuring the NNM iSPI Performance for QA to Use the Modified NNMi Web Services Client User Name, Password

If you have changed the password for the NNMi Web Services client user specified during the installation of the NNM iSPI Performance for QA, perform the following steps:

1. Log on to the NNMi Management Server as an administrator user.
   Log on to the NNMi Management Server as a root user.

2. Run the following commands:

- To encrypt new password, run the following command:

  ```
  nmsqaencryptpassword.ovpl -e qa<new password>
  ```

- To copy `nms-users.properties` from NNM jboss to SPI jboss, run the following command:

  ```
  nmsqaencryptpassword.ovpl -c qa
  ```

3. Restart the NNM iSPI Performance for QA with the following commands:

   ```
   ovstop -c qajboss

   ovstart -c qajboss
   ```

If you want to configure the NNM iSPI Performance for QA to use an NNMi Web Service Client user name that is different from the user name specified during the installation of the NNM iSPI Performance for QA, do as follows:

1. Open the `nnm.extended.properties` file available in the following directory:

   ```
   %NnmDataDir%\shared\qa\conf\

   $NnmDataDir/shared/qa/conf/
   ```

2. Edit the value of the following property:

   ```
   com.hp.ov.nms.spi.qa.Nnm.username
   ```

3. Run the following commands:

   To encrypt password for the new user run the following command

   ```
   nmsqaencryptpassword.ovpl -e qa<password for the new user>
   ```

   To copy `nms-users.properties` from NNM jboss to SPI jboss, run the following command:

   ```
   nmsqaencryptpassword.ovpl -c qa
   ```

4. Restart the NNM iSPI Performance for QA with the following commands:

   ```
   ovstop -c qajboss

   ovstart -c qajboss
   ```

Modifying the NNM iSPI Performance for QA Ports

The NNM iSPI Performance for QA uses a set of ports for its operation. These ports are configured at the time of installation by the installer and the installer offers you the option to choose non-default values for the HTTP and HTTPS ports. The `server.properties` file provides a list of those ports. The file is available under the following directory:

`%NnmDataDir%\nmsas\qa`

`/var/opt/OV/nmsas/qa`

After installation, you can configure the NNM iSPI Performance for QA to use different ports (different from what was configured at the time of installation).

If you want to configure the NNM iSPI Performance for QA to use non-default ports, follow these steps:

1. Log on to the NNMi Management Server as an administrator user.
   Log on to the NNMi Management Server as a root user.
2. Open the `server.properties` file with a text editor.
3. To resolve the port conflict created by another application on the system:
   a. Identify the port number in the file.
   b. Replace the port number with a new port number; make sure that the new port is not used by any other applications on the system.
4. To use a new HTTPS port, replace the value of the `nmsas.server.port.web.https` property with the new HTTPS port.
5. To use a new HTTP port, replace the value of the `nmsas.server.port.web.http` property with the new HTTP port.
6. To use a new JNDI port, replace the value of the `nmsas.server.port.naming.port` property with the new JNDI port.
7. To use a new port for the embedded database, replace the value of the `com.hp.ov.nms.postgres.port` property with the new port.

   Note: Before you change this value, make sure that NNMi is configured to use the new port for the embedded database. For information on modifying the embedded database port for NNMi, see the *NNMi Deployment Reference*.
8. Restart the NNM iSPI Performance for QA processes:

```
ovstop -c qajboss

ovstart -c qajboss
```

Appendix A: Troubleshooting

Troubleshooting the Error Encountered while Loading Data from the NNMi Management Server

Problem Statement

While working with the NNM iSPI Performance for QA views, the following error message appears:

```
A problem occurred while loading the data from the NNMi
management server for this component. Additional error
information: Service Unavailable.
```

Resolution

If NNM iSPI Performance for QA and NNMi are using a remote Oracle database, this error occurs when you restart the Oracle server. Follow these steps to resolve this error:

1. Stop the QA process using the following command:

   ```
   ovstop -c qajboss
   ```

2. Start the QA process using the following command:

   ```
   ovstart -c qajboss
   ```

Updating the NNM iSPI Performance for QA Configuration when the FQDN for the NNMi Management Server Changes

Problem Statement

Any change in the host name on the NNMi server after deploying the NNM iSPI Performance for QA stops the NNM iSPI Performance for QA from working.

Resolution

To update the new FQDN in the NNM iSPI Performance for QA, follow these steps:

1. Run the **nnmofficialfqdn.ovpl** command to find the FQDN of the new NNMi server.
2. Edit the following two parameters in the `nms-qa.jvm.properties` file to reflect the new FQDN:
   - Dcom.hp.ov.nms.ssl.KEY_ALIAS
   - Djava.rmi.server.hostname

   On Windows : `%NnmdataDir%\shared\qa\conf\nms-qa.jvm.properties`

   On Unix : `/var/opt/OV/shared/qa/conf/nms-qa.jvm.properties`
3. Edit the following two parameters in the `nnm.extended.properties` file to reflect the new FQDN:
   - com.hp.ov.nms.spi.qa.Nnm.hostname
   - com.hp.ov.nms.spi.qa.spi.hostname

   On Windows : `%NnmdataDir%\shared\qa\conf\nnm.extended.properties`

   On Unix : `/var/opt/OV/shared/qa/conf/nnm.extended.properties`
4. Edit the following two parameters in the `server.properties` file to reflect the new FQDN:

- java.rmi.server.hostname
- nmsas.server.net.hostname.private

On Windows : `%nnmdatadir%\nmsas\qa\server.properties`

On Unix : `/var/opt/OV/nmsas/qa/server.properties`

5. Edit the `login-config.xml` file for the 'module-option' element, to reflect the virtual FQDN of the NNMi management server:

   On Windows : `%nnminstalldir%\qa\server\conf\login-config.xml`

   On Unix : `/opt/OV/qa/server/conf/login-config.xml`

   a. Open the login-config.xml file with a text editor.

   b. Look for the element <module-option name="nnmAuthUrl">.

   c. Modify the string contained within the element to reflect the virtual FQDN of the NNMi management server.

   d. Save the file.

Send Documentation Feedback

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

Feedback on Deployment Reference (Network Node Manager iSPI Performance for Quality Assurance 10.10)

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 docfeedback@hp.com.

We appreciate your feedback!