HP Network Node Manager iSPI for IP Telephony Software

For the Windows® and Linux operating systems

Software Version: 10.00

Deployment Reference

Document Release Date: July 2014

Software Release Date: July 2014

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.
(missing or bad snippet)

Copyright Notice

Trademark Notices

(missing or bad snippet)(missing or bad snippet)

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

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login 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.
(missing or bad snippet)

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

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:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

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**

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Chapter 1: Introducing the NNM iSPI for IP Telephony

The HP Network Node Manager i Smart Plug-in for IP Telephony (NNM iSPI for IP Telephony) Software helps you to extend the capability of the HP Network Node Manager i (NNMi) Software to monitor the overall health of the network.

The factors that impact the deployment of the NNM iSPI for IP Telephony include the type of database that is configured with the NNMi, and the size of the network to be monitored. Make sure to install the latest NNMi patches before installing the NNM iSPI for IP Telephony.

Plan the deployment of the NNM iSPI for IP Telephony based on the NNMi deployment in the environment. While planning the deployment, consider the following to achieve an optimum size and performance of the system:

- The number of managed IP telephony nodes
- The number of managed non-IP telephony nodes
- Deployment of the NNM iSPI for IP Telephony in a High Availability (HA) environment
- Deployment of the NNM iSPI for IP Telephony in an Application Failover environment
- Deployment of the NNM iSPI for IP Telephony in a Global Network Management (GNM) environment
- Deployment of the NNM iSPI for IP Telephony along with other iSPIs (such as the NNM iSPI for IP Multicast)

Preparing for the Deployment

Before you start deploying the NNM iSPI for IP Telephony, do the following:

- Plan the installation based on your deployment requirements
- Identify the supported configurations
- Make sure that the installation process complies with all the prerequisites

For information about the installation and configuration of the NNM iSPI for IP Telephony in an HA and Application failover environment, see the *Configuring NNMi in a High Availability Cluster* and the *Configuring NNMi for Application Failover* chapters of the *HP Network Node Manager i Software Deployment Reference*.

Additionally, the following guides will help you in preparing for the deployment:

- *HP Network Node Manager i Software Deployment Reference*
- *HP Network Node Manager i Software Release Notes*
- *HP Network Node Manager i Software Support Matrix*
- *HP Network Node Manager iSPI for IP Telephony Software Installation Guide*
- *HP Network Node Manager iSPI for IP Telephony Software Release Notes*
- *HP Network Node Manager iSPI for IP Telephony Software Support Matrix*

Note: Make sure that you read the latest versions of these guides. You can download the latest versions from http://h20230.www2.hp.com/selfsolve/manuals.

Chapter 2: Deploying the NNM iSPI for IP Telephony

You can deploy the NNM iSPI for IP Telephony only after you install the NNMi on a system. For information about installing and configuring the NNMi on a system, see the *HP NNM i Software Interactive Installation Guide 10.00*.

Note: Install the NNMi and the NNM iSPI for IP Telephony on the same server.

You can deploy the NNM iSPI for IP Telephony for the following scenarios:

- Install the NNMi and the NNM iSPI for IP Telephony together.
- Install the NNM iSPI for IP Telephony on a system where NNMi is already installed.
- Install the NNMi, NNM iSPI for IP Telephony, and the NNM iSPI Performance for Metrics on the same system.
- Install the NNMi and the NNM iSPI for IP Telephonyon one system, and the NNM iSPI Performance for Metrics on a different system. You can choose this scenario for the best performance results.

For information about installing the NNM iSPI for IP Telephony, see the *HP Network Node Manager iSPI for IP Telephony SoftwareInstallation Guide 10.00*.

Deploying the NNMi and the NNM iSPI for IP Telephony Together

To deploy the NNM iSPI for IP Telephony after installing the NNMi, on a management server, follow these steps:

1. Start the NNMi installation process.

   Note: When you install the NNM iSPI for IP Telephony, use the same database type (Embedded or Oracle) that you used for the NNMi installation.

2. Install the NNM iSPI for IP Telephony. Follow the *HP Network Node Manager iSPI for IP Telephony Software Installation Guide 10.00* to perform the steps during the pre-installation, installation, and the post installation phases.

> **Note:**
> Make sure that you have tuned the `Xmx` values in the `ovjboss.jvmargs` and the `ipt.jvm.properties` file of the NNMi and the NNM iSPI for IP Telephony respectively. In the `ipt.jvm.properties` file, you can update only the `Xms` (Initial Java Heap Size) and the `Xmx` (Maximum Java Heap Size) values.
>
> To update the `Xmx` values, see the steps listed in *Tuning the jboss Memory* section of the *HP Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix 10.00* document.

3. Modify the values in `nms-ds.xml` and `postgresql.conf` as mentioned in Tuning Embedded Database for Scalability and Performance of NNMi and iSPI for IP Telephony section of Sizing and Configurations for Scalability and Performance of the NNM iSPI for IP Telephony.
4. Restart the NNMi and the NNM iSPI for IP Telephony processes.
5. Configure the auto-discovery rules for IP phones. For more information, see the Setting NNMi Auto-Discovery Rules to Discover IP Phones.
6. Seed the IP telephony devices from the NNMi console. Seeding enables NNMi to start the discovery process. The NNM iSPI for IP Telephony nodes are discovered along with the NNMi nodes. For more information about seeding nodes for the NNM iSPI for IP Telephony, see the *HP Network Node Manager iSPI for IP Telephony Software Installation Guide*.
7. After sometime—when the NNM iSPI for IP Telephony nodes are discovered—log on to the NNMi console, and then verify the availability of the IP Telephony workspace and IP Telephony views.

Deploying the NNM iSPI for IP Telephony on an NNMi-installed Management Server

To deploy the NNM iSPI for IP Telephony on a management server where the NNMi is already installed, follow these steps:

1. Install the NNM iSPI for IP Telephony on the management server where the NNMi is running, and the nodes are discovered. For information about the steps during the pre-installation, installation, and the post installation phases, follow the steps listed in the *HP Network Node Manager iSPI for IP Telephony Software Installation Guide 10.00*.

   > **Note**: When you install the NNM iSPI for IP Telephony, use the same database type (Embedded or Oracle) that you used for the NNMi installation.

2. Modify the values in `nms-ds.xml` and `postgresql.conf` as mentioned in Sizing and

Configurations for Scalability and Performance of the iSPI for IP Telephony.

Note: Follow the instruction given in Step 3 only if you are using an Embedded database. For the Oracle database, go to Step 4.

3. Based on the database that you are using, do one of the following:
   - *If you are using an Embedded Database.* Restart the NNMi and the NNM iSPI for IP Telephony processes.
   - *If you are using an Oracle Database.* Configure the auto-discovery rules for IP phones. For more information about configuring the auto-discovery rules, see Setting NNMi Auto-Discovery Rules to Discover IP Phones.
4. Start the NNM iSPI for IP Telephony discovery process (to discover the IP Telephony nodes from the discovered NNMi nodes) by performing one of the following tasks:
   - Run the configuration poll on each node (except on nodes that host the IP phones) from the NNMi Inventory workspace. For more information about the Configuration Poll command, see the *HP Network Node Manager i Software Online Help: Help for Operators*.
   - Wait for the next NNMi discovery cycle to rediscover the nodes and to start the discovery of the NNM iSPI for IP Telephony nodes.

Installing the NNM iSPI for IP Telephony in an HA Cluster

You can install the NNMi and the NNM iSPI for IP Telephony in a High Availability (HA) environment to achieve redundancy in your monitoring setup. The prerequisites to configure the NNM iSPI for IP Telephony in an HA environment is similar to that of NNMi. For more information, see the *HP HP Network Node Manager i Software Deployment Reference 10.00*.

Configuring the NNM iSPI for IP Telephony

You can configure the NNM iSPI for IP Telephony for the following scenarios:

- Install the NNMi and the NNM iSPI for IP Telephony in your environment before configuring the NNMi to run under an HA cluster.
- Install and configure the NNM iSPI for IP Telephony in an existing NNMi HA cluster environment.

Configuring an HA Cluster on Systems that have the NNMi and the NNM iSPI for IP Telephony Installed

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

the HA.cluster. In an HA environment you can configure the NNMi and the NNM iSPI for IP Telephonyon the primary and the secondary nodes. For more information about installing the NNMi in an HA environment, see the *HP Network Node Manager i Software Deployment Reference 10.00*.

To configure the NNM iSPI for IP Telephony on the primary (active) node, follow these steps:

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

   `nnmofficialfqdn.ovpl`

2. Modify the following files from the `%NnmdataDir%\shared\ipt\conf` or the `/opt/OV/shared/ipt/conf` to replace the hostname with the virtual Fully Qualified Domain Name (FQDN) for the following parameters:

File Name	Variable Name
`nms-ipt.jvm.properties`	`-Dnmsas.server.security.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.spi.hostname`

3. Modify the `login-config.xml` file from the `%Nnminstalldir%\ipt\server\conf` or the `/opt/OV/ipt/server/conf` directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).

4. 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 about starting the NNMi HA resource group, see the *HP Network Node Manager i Software Deployment Reference 10.00*.

   If the NNMi does not start, see the *Troubleshooting the HA Configuration* section of the *HP Network Node Manager i Software Deployment Reference 10.00*.

5. Run the following command to configure the NNM iSPI for IP Telephony to run under the HA cluster:

   For Windows:

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

For Linux:

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

To configure the NNM iSPI for IP Telephony on the secondary (passive) node, follow these steps:

1. Install the NNMi with the NNM iSPI for IP Telephony on the secondary node. Make sure that the secondary node has a separate FQDN during the installation. For more information, see the *HP Network Node Manager i SoftwareInstallation Guide* and the *NNM iSPI for IP Telephony Installation Guide*.

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

   ```
   nnmofficialfqdn.ovpl
   ```

3. Modify the following files from the `%NnmdataDir%\shared\ipt\conf` or the `/opt/OV/shared/ipt/conf` to replace the hostname with the virtual Fully Qualified Domain Name (FQDN) for the following parameters:

File Name	Variable Name
`nms-ipt.jvm.properties`	`-Dnmsas.server.security.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.spi.hostname`

4. Modify the `login-config.xml` file from the `%Nnminstalldir%\ipt\server\conf`or the `/opt/OV/ipt/server/conf` directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).

5. Run the following command to configure the NNM iSPI for IP Telephony on the secondary node to run under the HA cluster:

   For Windows:

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

   For Linux:

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

Installing the NNM iSPI for IP Telephony in an Existing NNMi HA Cluster Environment

To configure the NNM iSPI for IP Telephony on the primary and secondary nodes in an existing NNMi HA cluster environment, follow these steps:

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

   For Windows:

   `%Nnmdatadir%\hacluster\`*<resource_group_name>*

   For Linux:

   `/opt/OV/hacluster/`*<resource_group_name>*
3. Run `ovstatus -c` to make sure that `ovjboss` is running.
4. Install the NNM iSPI for IP Telephony on the primary (active) node in the cluster. However, do not start the iSPI.
5. Modify the following files from the `%NnmdataDir%\shared\ipt\conf` or the `/opt/OV/shared/ipt/conf` to replace the hostname with the virtual Fully Qualified Domain Name (FQDN) for the following parameters:

File Name	Variable Name
`nms-ipt.jvm.properties`	`-Dnmsas.server.security.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.spi.hostname`

6. Modify the `login-config.xml` file from the `%Nnminstalldir%\ipt\server\conf` or the `/opt/OV/ipt/server/conf` directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).
7. Remove the `maintenance` file that you added in Step 2.
8. Initiate a failover to a secondary (passive) node in the cluster where you want to install the NNM iSPI for IP Telephony. Make sure that the NNMi fails over and runs on the secondary server successfully.
9. On the secondary server, follow these steps:
   a. Put the NNMi resource group to the HA maintenance mode by placing the `maintenance` file under the following directory:

      For Windows:

      `%Nnmdatadir%\hacluster\`*<resource_group_name>*

      For Linux:

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

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

c. Install the NNM iSPI for IP Telephony on the server. However, do not start the iSPI.

d. Modify the following files from the `%NnmdataDir%\shared\ipt\conf` or the `/opt/OV/shared/ipt/conf` to replace the hostname with the virtual Fully Qualified Domain Name (FQDN) for the following parameters:

File Name	Variable Name
`nms-ipt.jvm.properties`	`-Dnmsas.server.security.keystore.alias`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.Nnm.hostname`
`nnm.extended.properties`	`com.hp.ov.nms.spi.ipt.spi.hostname`

e. Modify the `login-config.xml` file from the `%Nnminstalldir%\ipt\server\conf` or the `/opt/OV/ipt/server/conf` directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).

f. Remove the `maintenance` file that you added in Step 9 a.

Note: If you have multiple nodes in the cluster, fail over to another passive server, and then repeat the steps from 9 a through 9 f.

10. Fail over to the server that was active when you started this procedure.

11. Run the following command, first on the active server, and then on all the passive servers:

For Windows:

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

For Linux:

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

12. Run the following command to verify the successful registration of the NNM iSPI for IP Telephony:

For Windows:

```
%Nnminstalldir%\misc\nnm\ha\nnmhaclusterinfo.ovpl –config NNM –get NNM_ADD_
ON_PRODUCTS
```

For Linux:

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

Licensing

You require the following licenses to run the NNM iSPI for IP Telephony in an HA cluster:

- The production license tied to the IP address of one of the physical cluster nodes
- The non-production license tied to the virtual IP address of the NNMi HA resource group

After obtaining these licenses for the NNM iSPI for IP Telephony, follow the procedure in the *Licensing NNMi in an HA Cluster* section of the *HP Network Node Manager i Software Deployment Reference 10.00*.

Patching the NNM iSPI for IP Telephony Under High Availability

If you have already configured the NNMi and the NNM iSPI for IP Telephony 10.00 to work in an HA cluster, you must follow this section to apply the necessary patches (for both the NNMi and the NNM iSPI for IP Telephony).

To apply patches for NNMi and NNM iSPI for IP Telephony, follow these steps:

1. Determine the active node in the HA cluster by running the following command:

   On Windows:

   ```
   %NnmInstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl\

   -group <resource_group> -activeNode
   ```

   On Linux:

   ```
   /opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl\

   -group <resource_group> -activeNode
   ```

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

   On Windows:

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

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

   On Linux:

```
/var/opt/OV/hacluster/<resource_group>/maintenance

/var/opt/OV/hacluster/<resource_group>/maint_NNM
```

Include the `NORESTART` keyword in both the files.

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

   On Windows:

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

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

   On Linux:

   ```
   /var/opt/OV/hacluster/<resource_group>/maintenance

   /var/opt/OV/hacluster/<resource_group>/maint_NNM
   ```

   Include the `NORESTART` keyword in both the files.

4. On the active node, follow these steps:

   a. Stop NNMi by running the following command:

      ```
      ovstop -c
      ```

   b. Take a back up of the shared disk by performing a disk copy.

   c. *Optional*. Use the `nnmbackup.ovpl` command or another database command to take a back up of all the NNMi data. For example, `nnmbackup.ovpl -type offline -scope all -target nnmi_backups`. For more information about this command, see the *NNMi Backup and Restore Tools* section in the *HP Network Node Manager i Software Deployment Reference (Software Version 10.00)*.

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

   e. Start NNMi by running the following command:

      ```
      ovstart -c
      ```

   f. Run the following command to check if the NNMi has started correctly:

      ```
      ovstatus -c
      ```

      All NNMi services must display the status as `RUNNING`.

5. On each passive node, apply the appropriate patches to the system.

6. On each passive node, delete the maintenance file from the node to take the NNMi HA resource group out of the maintenance mode.

7. On the active node, delete the maintenance file from the node to take the NNMi HA resource group out of the maintenance mode.

Deploying the NNM iSPI for IP Telephony in an Application Failover Environment

This section provides instructions to deploy the NNM iSPI for IP Telephony in different scenarios in an application failover environment.

Application Failover with Oracle Configured as the Database

You can deploy the NNM iSPI for IP Telephony in an application failover environment, with an Oracle database, in the following scenarios:

- Install the NNM iSPI for IP Telephony with NNMi, and then configure the application failover over a LAN or a WAN
- Install the NNM iSPI for IP Telephony after configuring NNMi in an application failover environment

Note: Install Oracle as the database by following the steps listed in the *Network Node Manager iSPI for IP Telephony Software Telephony Installation Guide 10.00*.

Installing the NNM iSPI for IP Telephony with NNMi, and then configuring the application failover over a LAN or a WAN

For this scenario, follow these steps:

1. Install the NNMi in the primary server mode on server 1 and in the secondary server mode on server 2.

   Note: With Oracle as the database, NNMi provides you the options to install NNMi in the primary and secondary server modes for deployment in an application failover or a high availability environment.

2. On server 1, start the NNMi.

3. On server 1, install the NNM iSPI for IP Telephony.

4. After the installation of the NNM iSPI for IP Telephony on server 1, install the NNM iSPI for IP Telephony non-production license.
5. Merge the keystores on one server and copy them to both the primary and the secondary servers. For more information, see the *Network Node Manager i Software Deployment Reference 10.00*.
6. On server 1, stop the NNMi.
7. On server 2, start the NNMi.
8. On server 2, install the NNM iSPI for IP Telephony.
9. On server 2, configure the NNM iSPI for IP Telephony with the same database instance, user name, and password as configured on server 1.
10. After the installation of the NNM iSPI for IP Telephony on server 2, install the NNM iSPI for IP Telephony non-production license.
11. Configure the application failover on server 1 and server 2. For information about the instructions to configure the application failover, see the *Configuring NNMi for Application Failover* topic of the *HP Network Node Manager i Software Deployment Reference 10.00*.

Installing the NNM iSPI for IP Telephony after configuring NNMi in an application failover environment

For this scenario, follow these steps:

1. Remove the NNMi application failover configuration.
2. Restore the old keystore and truststore specific to server 1 and server 2. For more information, see the *Network Node Manager i Software Deployment Reference 10.00*.
3. Follow the steps listed in the previous scenario to install the NNM iSPI for IP Telephony and configure application failover between the server 1 and the server 2.

> **Note:** Do not perform the steps related to installing the NNMi.

Installing the NNM iSPI for IP Telephony in an Application Failover Environment with the Embedded Database

You can deploy the NNM iSPI for IP Telephony in an application failover environment, with an embedded database, in the following scenarios:

- Install the NNM iSPI for IP Telephony with NNMi, and then configure the application failover mode
- Install the NNM iSPI for IP Telephony after configuring NNMi in an application failover mode

Installing the NNM iSPI for IP Telephony with NNMi, and then configuring the application failover mode

For this scenario, follow these steps:

1. Install the NNMi and the NNM iSPI for IP Telephony both on the primary and secondary servers.
2. After the installation of the NNM iSPI for IP Telephony, install the NNM iSPI for IP Telephony non production licenses on both the servers.
3. Configure the NNMi in application failover mode by following the instructions listed in the *Network Node Manager i Software Deployment Reference 10.00*. After this, the NNM iSPI for IP Telephony gets automatically configured in the application failover mode.

Installing the NNM iSPI for IP Telephony after configuring NNMi in an application failover mode

For this scenario, follow these steps:

1. Remove the NNMi application failover configuration.
2. Restore the old keystore and truststore specific to the configured primary server and the secondary server. For more information, see the *Network Node Manager i Software Deployment Reference 10.00*.
3. Install the NNM iSPI for IP Telephony on both the primary and the secondary servers.
4. After the installation of the NNM iSPI for IP Telephony, install the NNM iSPI for IP Telephony non production licenses on both the servers.
5. Configure the NNMi in application failover mode by following the instructions listed in the *Network Node Manager i Software Deployment Reference 10.00*. After this, the NNM iSPI for IP Telephony automatically gets configured in the application failover mode.

Guidelines for Discovery

For the discovery of the Cisco SRST routers by the NNM iSPI for IP Telephony, follow these guidelines:

- Make sure that the Cisco SRST routers are already discovered by NNMi.
- Run the Configuration Poll action on Cisco Unified Communication Manager systems that belong to the cluster that hosts the Cisco SRST routers.

The Cisco SRST routers get discovered after the next polling cycle is complete.

Deploying the NNM iSPI for IP Telephony in a Global Network Management Environment

You can deploy the NNM iSPI for IP Telephony in a Global Network Management (GNM) environment. The NNM iSPI for IP Telephony supports the following scenarios in a GNM environment:

- NNMi and the NNM iSPI for IP Telephony on Global Manager and Regional Managers
- NNMi and the NNM iSPI for IP Telephony on the Global Manager and NNMi on the Regional Manager
- Deploying the Regional Manager in an Application failover Environment

For information about the GNM, see the *Network Node Manager i Software Deployment Reference 10.00*.

Consider the following points when you deploy the NNM iSPI for IP Telephony in a GNM environment:

- You can enable automatic discovery for a large group of nodes that host IP phones, up to 50,000, on the regional manager along with the seeding of the related neighboring switches and routers.
- You can create automatic discovery rules to discover the nodes (that host IP phones) across the regional managers and classify the nodes based on the clusters (for Cisco) and Communication Manager (for Avaya). You can then seed all the Cisco Call Managers and all the Avaya Communication Managers with the global manager. You can also seed all the nodes that host the Cisco Gatekeepers, Cisco Gateways, Cisco Unity devices, Cisco Call Manager Express, Cisco SRST, Avaya Communications Manager, Avaya LSP, and Avaya Media Gateways on the global manager.
- The NNM iSPI for IP Telephony can be run on the global manager only if the scalability limit for a single instance of the NNM iSPI for IP Telephony along with NNMi is within the supported limits. You must also make sure that the latency is minimal in the network path between NNMi and the managed nodes that host IP telephony entities across the WAN (possibly for geographic dispersed regions). For more information about the scalability limit, see Performance and Scalability Metrics for NNM iSPI for IP Telephony.
- If the scalability limit is not high enough to exceed the limits supported with this version of the NNM iSPI for IP Telephony and if the latency is not a constraint, it is recommended to run the NNM iSPI for IP Telephony only on the global manager. You can make this decision when testing the latency aspect for SNMP across the WAN for nodes that host IP telephony entities.
- All the configuration changes done on the NNM iSPI for IP Telephony running on a regional manager are synchronized with the global manager during the subsequent polling cycle of the global manager.

NNMi and the NNM iSPI for IP Telephony on Global Manager and Regional Managers

In this scenario, all the regional managers send the IP Telephony information to the global manager. You can view the following information on the global manager:

- Consolidated IP telephony topology
- Consolidated IP telephony reports

NNMi and the NNM iSPI for IP Telephony on the Global Manager and NNMi on the Regional Manager

In this deployment scenario you can only see the locally managed IP telephony nodes by the global manager in the IP telephony inventory from the global manager.

Deploying the Regional Manager in an Application failover Environment

When you deploy the NNM iSPI for IP Telephony regional manager in the application failover environment, use the `ORDER` parameter to decide the priority to establish the connection with the regional manager from the global manager.

To use the regional manager in an application failover environment, follow these steps:

1. Configure the regional manager connection using the NNM iSPI for IP Telephony configuration workspace. For more information, see the *Adding a Regional Manager Configuration* topic in the *Network Node Manager iSPI for IP Telephony Online Help 10.00*.
2. Add two regional manager connections and provide the host names.
3. Use the `ORDER` parameter to give different values to the two regional managers.

Whenever an application failover occurs on the regional manager, the global manager establishes the next connection with the lowest order value. To configure the regional manager in the application failover environment, follow the steps documented in the Deploying the NNM iSPI for IP Telephony in an Application Failover Environment topic.

Sizing and Configurations for Scalability and Performance of the NNM iSPI for IP Telephony

For information related to the sizing of the NNM iSPI for IP Telephony, see the *HP Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix 10.00*.

To achieve optimal performance and scalability of NNMi and the NNM iSPI for IP Telephony, do the following:

- Tune the embedded database
- Tune the NNMi Polling Configurations

Tuning the Embedded Database for the Scalability and Performance of the NNMi and the NNM iSPI for IP Telephony

While installing the NNM iSPI for IP Telephony using an embedded database, you can achieve optimal performance and sacalability if you modify certain files. To accomplish this, follow these steps:

1. Stop all the processes.
2. Take a backup of the files to be modified.
3. Modify the value of `<max-pool-size>60</max-pool-size>` to `<max-pool-size>120</max-pool-size>` in the `nms-ds.xml` of the `<INST_DIR>/nonOV/jboss/nms/server/nms/deploy/nms-ds.xml` directory.
4. Modify the value of `max_connections=100` to `max_connections=200` in the `<DATA_DIR>/shared/nnm/databases/Postgres/postgresql.conf` directory.
5. Restart both the NNMi and NNM iSPI for IP Telephony processes.

Tuning the NNMi Polling Configurations for the Scalability and Performance of the NNMi and the NNM iSPI for IP Telephony

You can increase the performance of NNMi with the NNM iSPI for IP Telephony by disabling the polling of IP phones. To disable the polling of IP phones, follow these steps:

1. From the **Workspaces** navigation pane, select **Configuration**, and then click **Monitoring** > **Monitoring Configuration**. The **Monitoring Configuration** page opens.
2. On the page, click the **Node Settings** tab.
3. Select the **Ordering** column that is specified as 400, and then click the **Open** icon to view the details.

   Note: The **Ordering** column specified as 400 corresponds to the non-SNMP devices.

4. On the page, from the Fault Monitoring section, deselect the following check boxes:
   - **Enable ICMP Fault Polling**
   - **Enable SNMP Fault Polling**
   - **Enable Component Health Fault Polling**
5. Click **Save and Close** to save the configuration.

Setting NNMi Auto-Discovery Rules to Discover the IP Phones

To discover the IP phones as non-SNMP devices, you must set the auto-discovery rules in NNMi. To set the rules follow these steps:

1. From the **Workspaces** navigation pane, select **Configuration**, and then click **Discovery** > **Discovery Configuration**. The **Discovery Configuration** page opens.
2. On the page, click the **Auto-Discovery Rules** tab.

   Note: On the left pane of the page, in the **Node Resolution** section, select the following:

   - **First Choice**: IP Address
   - **Second Choice**: Short sysName
   - **Third Choice**: Short DNS Name

3. Click the **New** icon. The **Auto-Discovery Rule** page opens.
4. On the page, in the Basics section, specify the required details. For more information, see the *HP Network Node Manager i Software Online Help 10.00*.

   Note: Make sure you select the **Discover Non-SNMP Devices** check box and deselct the **Enable Ping Sweep** check box.

5. From the IP Address Ranges for this Rule section of the IP Ranges tab, click the **New** icon to add the range of IP addresses of call managers that manage IP phones in your IP telephony environment.
6. Click **Save and Close** to save the configuration.

If NNMi discovers and stores the details of the Cisco and Avaya IP phones, you can enable the custom attributes for these IP phones. After you enable the custom attributes for the Cisco and Avaya IP phones, you can see the phone icons for all the discovered Cisco and Avaya IP phones in the NNMi topology maps.

To enable the custom attributes for Cisco IP phones, follow these steps:

1. From the **Workspaces** navigation pane of the NNM iSPI for IP Telephony console, select **Configuration**, and then click **iSPI for IP Telephony Configuration...** > **Cisco Configuration**. The NNM iSPI for IP Telephony Cisco configuration console opens.
2. Click **IP Phone Configuration**. The NNM iSPI for IP Telephony Cisco IP Phone Configuration form opens.
3. In the **Discovery Configuration** section, select the **Enable Phone Custom Attribute Setting** check box.
4. Click **Apply Changes**.

To enable the custom attributes for Cisco IP phones, follow these steps:

1. From the **Workspaces** navigation pane of the NNM iSPI for IP Telephony console, click **Configuration** > **iSPI for IP Telephony Configuration** > **Avaya Configuration**. The HP NNM iSPI for IP Telephony Avaya Configuration Console opens.

2. Click **IP Phone Configuration**. The NNM iSPI for IP Telephony Avaya IP Phone Configuration form opens.

3. In the **Discovery Configuration** section, select the **Enable Phone Custom Attribute Setting** check box.

4. Click **Apply Changes**.

Chapter 3: Deploying in a Multiple Tenant Model

The multiple tenant model, supported by NNMi, helps you to logically group nodes in the NNMi database and assign security and user level permissions to these node groups. This helps in restricting the information about these nodes from being viewed by operators who are not designated to monitor these nodes. By default, all the operators have access to view all the nodes in the NNMi console. By assigning security and user level permissions to these node groups, you gain the following benefits:

- Restrict access to nodes in the NNMi database for operators who are not assigned for monitoring those nodes
- Customize operator views based on the nodes that the operator must monitor
- Simplify configuration of nodes and node groups
- Display the topology inventory based on the node access permissions for the operator
- Display the maps and path views relevant to the nodes that the operator is designated to monitor
- Perform actions using the NNMi console only on the nodes that are accessible to the operator
- Display incidents based on the nodes that the operator monitors

For more information about the multiple tenant model supported by NNMi, see the *HP Network Node Manager i Software Deployment Reference 10.00*.

Multiple Tenant Model for Cisco IP Telephony

To implement the multiple tenant model for an enterprise where the Cisco IP telephony infrastructure is monitored using the NNMi and the NNM iSPI for IP Telephony, make sure that you follow the guidelines discussed in this section.

Cisco Unified Communications Managers

Make sure that you seed all the nodes hosting the Cisco Unified Communications Manager (CUCM) in a cluster with the same tenant–security group combination. Failure to follow this guideline might result in the inconsistent implementation of the security and user level permissions for nodes.

IP Phones

The IP phones configured with the CUCM in a cluster derive the security groups that are configured for the CUCM. This indicates that an operator who has access to the CUCM in the cluster can also access the IP phones that are configured with it.

Hosting Nodes for Gateways, Gatekeepers, Unity Devices, and SRST Router

You can seed the nodes that host the gateways, gatekeepers, unity devices, and SRST routers using any security group–tenant combination. It is recommended to use the same tenant–security

group combination configured for the CUCM in the cluster with which these devices are associated. Note that the NNM iSPI for IP Telephony considers a gateway as a call routing device associated with a cluster. For an H323 gateway shared with multiple clusters, all the CUCMs participating in the clusters and all the gateways associated to the clusters must belong to the same tenant–security group combination. For the SRST router deployed for failover, you must make sure that you configure the same tenant–security group combination configured for the CUCM that is designated as the primary call controller.

Intercluster IP Trunks

The intercluster IP trunks derive the security group–tenant combination from the CUCM associated with the IP trunk. Note that the NNM iSPI for IP Telephony considers the intercluster IP trunk as a call routing resource associated with a CUCM in the cluster.

Reporting

The metrics in the following extension packs for reporting derive the security group–tenant combination configured for the CUCM cluster that handles the call. This makes sure that the row level security in NPS is implemented along with multitenancy:

- Call Details
- Gateway Calls
- IP Trunk Calls
- Call Types and Termination Reasons

The Cisco VM Systems extension pack for reporting derives the security group–tenant combination from the Cisco Unity device or the Unity connection for which the metrics are applicable.

Multiple Tenant Model for Avaya IP Telephony

To implement the multiple tenant model for an enterprise where the Avaya IP telephony infrastructure is monitored using the NNMi and the NNM iSPI for IP Telephony, make sure that you follow the guidelines discussed in this section.

Communication Managers

Make sure that both the nodes hosting the primary Communication Managers in a duplex redundant pair are seeded with the same security group–tenant combination. Failure to follow this guideline might result in the inconsistent implementation of the security and user level permissions for nodes.

IP Phones

The IP phones configured on any Communication Manager in a duplex redundant pair of primary communication manager or a standalone primary communication manager derive the security group–tenant combination from the nodes hosting any communication manager in the redundant pair or the node hosting the primary standalone communication manager. This indicates that an operator who has access to the communication manager in the redundant pair also has access to the IP phones configured with the communication manager.

Primary Communication Manager Servers, Local Survivable Processors, and H.248 Media Gateways

You can seed standalone primary communication manager servers, Local Survivable Processors (LSP) and H.248 media gateways using any security group–tenant combination. It is recommended that you seed the nodes hosting the H.248 media gateways with the same security group–tenant combination configured for the node hosting the primary communication manager (in the pair or in the standalone mode) that uses the H.248 media gateway for call routing.

For nodes hosting LSPs, it is recommended that you seed the nodes with the same security group–tenant combination configured for the node hosting the primary communication manager (in the pair or in the standalone mode) that acts as the primary call controller for the branch where the LSP is deployed for failover.

Port Network Media Gateways

The port network media gateways such as the G650 and the associated components supported by the NNM iSPI for IP Telephony such as CLAN, IPSI, media processor, and so on derive the security group–tenant combination from the node hosting the primary communication manager (in the pair or in the standalone mode) to which the Port Network media gateway is associated.

Reporting

The metrics in the following extension packs derive the security group–tenant combination from the primary communication manager that handles the call. This makes sure that the row level security in NPS is implemented along with multitenancy:

- Call Details
- Gateway Calls
- Trunk Calls
- Call Types and Termination Reasons

The metrics in the following extension packs for reporting derive the security group–tenant combination from the primary communications manager that uses the trunk groups, route patterns, network regions, or port networks for which the metrics are applicable:

- Trunk Activity
- Trunk Group and Route Pattern Usage
- Processor Occupancy Summary
- Port Network Load Statistics
- Network Region DSP/CODEC Usage Summary

The metrics for the RTP Session Metrics extension pack derives the security group–tenant combination from the primary communications manager configured for the RTP endpoint.

Multiple Tenant Model for Microsoft IP Telephony

To implement the multiple tenant model for an enterprise where the Microsoft IP telephony infrastructure is monitored using the NNMi and the NNM iSPI for IP Telephony, make sure that you follow the guidelines discussed in this section.

As an administrator, you must configure at least one front end pool for a central site, using the Add Front End Pool Configuration page provided by the iSPI for IP Telephony. The iSPI for IP telephony uses this configuration information to retrieve information related to the topology, policies, CDR and QoE collection, and users from the central site. The iSPI for IP Telephony discovers the topology of the central site and all the associated branch sites through the seeded front end pool. The iSPI for IP Telephony also maps the tenant name (provided while configuring the front end pool), the tenant UUID, and the UUID of the default security group of the tenant with the front end pool.

During discovery, the iSPI for IP Telephony seeds the servers and gateways with NNMi and maps these entities with the tenant details associated with the front end pool. The iSPI for IP Telephony uses the tenant mapping for any entities discovered through the front end pool.

As voice policies, voice routes, dial plans, and normalization rule configuration settings can be associated to multiple frontend pools in an organization, the iSPI for IP Telephony groups these entities based on the tenants associated with the front end pools associated with these entities.

After NNMi completes the discovery of the servers and gateways, the iSPI for IP Telephony retrieves the security group information for the discovered entities and maps the security group information against the discovered entities. See the following points before deploying the iSPI for IP Telephony to monitor the Microsoft IP Telephony entities:

- You can access a Gateway or server if you are assigned to the same security group assigned to the corresponding NNMi node.
- You can access a site if you have access to at least one server in the site.
- You can access a SIP trunk configuration if you have access to the site that includes the SIP trunk.
- You can access all the Lync users of an organization if you are assigned to the default security group of the tenant with which the frontend pool was seeded.
- You can access all the policies of an organization if you are assigned to the default security group of the Tenant with which the frontend pool was seeded.
- You can access an end user group if you have access to at least one user in the end user group.
- A non-administrative user does not have access to the NNMi sites configured in the iSPI for IP Telephony.

Chapter 4: Overlapping IP Addresses

If your network supports Network Address Translation (NAT) protocol or Port Address Translation (PAT) protocol, you must follow the instructions provided in the Managing Overlapping IP Addresses in NAT Environments section in the NNMi Deployment Reference.

In addition to the common instructions mentioned in the *HP Network Node Manager i Software Deployment Reference 10.00*, you must follow a few guidelines to monitor the IP telephony infrastructure.

Overlapping Address Domain Support for Cisco IP Telephony

If you manage a Cisco IP telephony infrastructure in your enterprise, make sure that you follow these guidelines:

- All Cisco IP Telephony entities, such asCisco Unified Communications Manager clusters, Cisco Unified Communication Manager Subscriber groups, Cisco Unified Communication Managers, gateways, Survivable Remote Site Telephony (SRST) routers, intercluster trunks, Unified Communication Manager Expresses, IP phones, gatekeepers, unity devices, and so on, that belong to an overlapping address domain must be associated with a single tenant.
- TheNNM iSPI for IP Telephony discovers the Cisco IP phones using the internal (private) IP addresses of the IP phones. Therefore, you must map the external IP address and the internal IP address of all Cisco IP phones using Overlapping Address Mapping form of NNMi. If you do not complete this mapping, the NNM iSPI for IP Telephony may not be able to draw the voice paths and control paths correctly. For more information, see NNMi Online Help, Overlapping IP Address Mapping.
- When you configure the NNM iSPI for IP Telephony to access data with AXL and SSH, you must provide the external IP address (public address) of the Cisco Unified Communications Manager.

Overlapping Address Domain Support for Avaya IP Telephony

If you manage an Avaya IP telephony infrastructure in your enterprise, make sure that you follow these guidelines:

- All Avaya IP Telephony entities, such as call controllers, IP phones, media gateways, and so on, that belong to an overlapping address domain must be associated with a single tenant.
- You must also map the external IP address and the internal IP address of all Avaya Media Processors and Avaya IP Server Interfaces (IPSIs) using the Overlapping IP Address Mapping

form of NNMi. If you do not complete the mapping for these entities, theNNM iSPI for IP Telephony may not generate incidents related to these entities.

- The NNM iSPI for IP Telephony discovers the Avaya Control Local Area Networks (CLANs) and Avaya IP phones firstly using their internal (private) IP addresses. The NNM iSPI for IP Telephony seeds them to NNMi database later. You must map the external IP address and the internal IP address of all Avaya CLANs and Avaya IP phones using Overlapping Address Mapping form of NNMi. If you do not complete this mapping, the NNM iSPI for IP Telephony may not be able to draw the voice paths and control paths correctly. The CLAN and IP phones association polling also may not take place. For more information, the *Overlapping IP Address Mapping* topic of the *NNMi Online Help*.
- When you configure CDR Access, RTCP reception, and SSH access, you must provide the external IP address (public address) of the Avaya Communication Manager.

Overlapping Address Domain Support for Microsoft IP Telephony

If you manage a Microsoft IP telephony infrastructure in your enterprise, you must make sure that all the Microsoft servers and gateways that belong to an overlapping address domain are associated with a single tenant.

Chapter 5: Administration Tasks

This chapter provides you information on the administration tasks that you can perform after you have installed the NNM iSPI for IP Telephony.

Enabling Single Sign On

For an overview on single sign-on, see the *Using Single Sign-on with NNMi* section in the *HP Network Node Manager i Software Deployment Reference 10.00*. You can grant Single Sign-on (SSO) access to users who do not have the system privileges to access the NNMi console. SSO is not enabled during installation or when you upgrade from the previous versions.

Note: You can enable SSO to allow the non-system users to access the NNMi console, the configuration screens, and the integrated application screens by signing in once to the NNMi console.

To enable the single sign-on for the NNM iSPI for IP Telephony, follow these steps:

1. In the following file, change the value of `com.hp.nms.ui.sso.isEnabled` from `false` to `true`:

   For Windows:

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

   For Linux:

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

2. Run the `nnmsso.ovpl -reload` script.
3. Run the `iptssoreload.ovpl` script.

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

Configuring Access with Public Key Infrastructure Authentication

Configuring NNMi to map the Public Key Infrastructure (PKI) certificates to the NNMi user accounts enables you to log on to the NNMi console without having to type in the user name and password on the Login page. However, when you try to launch the NNM iSPI for IP Telephony forms, you will be prompted to provide the NNMi user name and password. You must perform some additional steps to reconcile the mapping with the NNM iSPI for IP Telephony and configure access with the PKI authentication.

Note: When the NNMi is configured to use the PKI authentication, the NNM iSPI for IP Telephony must also use the same. Similarly, you must not configure the NNM iSPI for IP Telephony to use the PKI authentication when the NNMi uses the credentials-based authentication.

Prerequisites

Before configuring the NNM iSPI for IP Telephony to use the PKI authentication, make sure you follow these tasks:

- Task 1 - Configure NNMi to use the PKI Authentication
- Task 2 - Configure a Certificate Validation Method
- Task 3 - Enable SSL

Task 1 - Configuring NNMi to use the PKI Authentication

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 i SoftwareDeployment Reference*.

Task 2 - Configuring a Certificate Validation Method

To prevent unauthorized access using invalid certificates of NNMi configured with PKI authentication, you must configure NNMi to use one of the following certification methods:

- Certificate Revocation List (CRL)
- Online Certificate Status Protocol (OCSP)

For more information about the steps to be followed to configure a certificate validation method, see the *Certificate Validation (CRL and OCSP)* section in the *HP Network Node Manager i Software Deployment Reference*.

Task 3 - Enabling SSL

After configuring NNMi to use the PKI authentication, you must enable SSL on the NNM iSPI for IP Telephony. Enabling SSL ensures communication between the NNMi management server and the NNM iSPI for IP Telephony.

To enable SSL on the NNM iSPI for IP Telephony, follow these steps:

1. Log on to the NNM iSPI for IP Telephony server.
2. Navigate to the following directory:

   On Windows:

   ```
   %nnmdatadir%\shared\ipt\conf
   ```

   On Linux:

```
/var/opt/OV/shared/ipt/conf
```

3. Open the `nnm.extended.properties` file with a text editor.
4. In the properties file, set the value of the following properties to `true`:
   - `com.hp.ov.nms.spi.ipt.spi.isSecure`
   - `com.hp.ov.nms.spi.ipt.Nnm.isSecure`
5. Save the changes and close the file.
6. Restart the `iptjboss` process by running the following commands:
   a. `ovstop -c iptjboss`
   b. `ovstart -c iptjboss`

   This ensures the enabling of SSL on the NNM iSPI for IP Telephony.

Configuring theNNM iSPI for IP Telephony

While configuring NNMi to use PKI authentication, you must update the `nms-auth-config.xml` file that is available in the configuration data dictionary of NNMi (`%nnmdatadir%\nmsas\NNM\conf` or the `/var/opt/OV/nmsas/NNM/conf`). You must modify the `nms-auth-config.xml` file in the NNM iSPI for IP Telephony configuration data directory based on the updated `nms-auth-config.xml` file to enable the iSPI to use the PKI authentication.

To configure the NNM iSPI for IP Telephony to use the PKI authentication, follow these steps:

1. Log on to the NNMi management server.
2. Navigate to the following directory:

   On Windows:

   ```
   %nnmdatadir%\nmsas\ipt\conf
   ```

   On Linux:

   ```
   /var/opt/OV/nmsas/ipt/conf
   ```
3. Open the `nms-auth-config.xml` file using a text editor.
4. Modify the `nms-auth-config.xml` file on the NNM iSPI for IP Telephony to enable the PKI authentication. For information on the required changes, see the *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager i Software Deployment Reference 10.00*.

Note: Make sure that the modifications that you make to the NNM iSPI for IP Telephony `nms-auth-config.xml` file matches to the changes done to the `nms-auth-config.xml` file on the NNMi management server.

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

   On Windows:

   `%nnminstalldir%\bin\nmsiptauthconfigreload.ovpl`

   On Linux:

   `/opt/OV/bin/nmsiptauthconfigreload.ovpl`

Running the `nmsiptconfigimport.ovpl` Command

The `nmsiptconfigimport.ovpl` command requires you to provide the NNMi administrator user credentials as command-line arguments. However, when the NNM iSPI for IP Telephony is configured to use the PKI authentication, you can run the command without providing the user credentials — that is, you can run the command without the `-u` and the `-p` options. Make sure that the user account with which you logged on to the NNMi management server to run the command has **Read** access to the following file:

For Windows:

`%nnmdatadir%\nmsas\ipt\conf\props\nms-users.properties`

For Linux:

`/var/opt/OV/nmsas/ipt/conf/props/nms-users.properties`

Adding IP Telephony Nodes after Installing the NNM iSPI for IP Telephony

After installing the NNM iSPI for IP Telephony, you can add more IP Telephony nodes (such as CUCM, Voice Gateways, and Gatekeepers) to your deployment environment. To add nodes, follow these steps:

1. Use the NNM iSPI for IP Telephony configuration workspace to specify the required settings for the newly added entities. For more information, see the *Help for Administrators* section of the *HP NNM iSPI for IP Telephony Software Online Help*.
2. Seed the nodes that host the IP Telephony entities using the Discovery Configuration form in the NNMi configuration workspace. For more information about seeding nodes, see the *HP Network Node Manager i Software Online Help*.

3. Wait for the next discovery cycle by NNMi to trigger the discovery of the newly added IP Telephony entities. Alternatively, you can select the nodes from the NNMi node inventory and perform a configuration poll for the nodes. For more information about discovery cycles and performing configuration polls, see the *HP Network Node Manager i Software Online Help*.

Guidelines for Configuring Data Access

This section lists the guidelinesfor configuring data access using the corresponding NNM iSPI for IP Telephony Data Access Configuration form for the following IP Telephony environments:

- Cisco
- Avaya
- Acme

Configuring Data Access for Avaya

To configure data access for Avaya IP telephony, make sure that you configure all the primary communication managers (CM) and Local Survivable Processors (LSP) as valid sources of the CDR data. For a duplex pair of primary communication managers, you must configure the CDR data access for both the primary communication managers in the pair.

In the NNM iSPI for IP Telephony Avaya Data Access Configuration form, provide the following details for each CM in your deployment environment:

- The format of the CDRs used by the communication manager.
  You can retrieve the information about the format of CDRs from the appropriate SAT screen on the native configuration manager of the selected CM. For more information, see the documentation on the Avaya Communication Manager or contact the administrator of such communication manager servers.
- The time-zone of the CM.
- The date format for the month and the day in the date fields of CDRs from the CM.
  The format can be either in the MMDD or the DDMM format. You can obtain this information for a specific CM from the appropriate SAT screen on the native configuration manager of the selected CM. For more information, see the documentation on the Avaya Communication Manager or contact the administrator of such communication manager servers.
- Note whether the circuit ID fields for the trunk group members appear in the CDRs; also note if the circuit ID is modified while the CDRs are populated by the CM, and if the circuit ID fields must be interpreted in a way to re-construct the appropriate circuit ID. You can retrieve this configuration flag from the appropriate SAT screen on the native configuration manager of the communication manager. For more information, see the documentation on the Avaya Communication Manager or contact the administrator of such communication manager servers.
- The mode used by a specific CM for collecting CDRs.

You must determine the mode used by a specific communication manager before proceeding with the remaining configuration tasks for CDR data access. TheNNM iSPI for IP Telephony supports collection of CDR using one of the following methods:

- File-based survivable CDR collection
- Accessing CDRs pushed through a TCP/IP link using the Reliable Session Protocol

- The valid SFTP user name and password to access the CDR directory on the CM that contains the CDR files, if the verification is true for both the following cases:
  - The survivable CDR feature is enabled for the CM
  - The CM is configured to periodically write files containing CDR information at the designated location on the CM.

  Make sure that you work with the administrator for the CM to create the appropriate SFTP user and to turn on the CDR access at the Communication Manager. You can retrieve the information about the survivability of CDRs from the appropriate SAT screen (system-parameters cdr) on the native configuration manager of the CM. For more information, see the documentation on the Avaya Communication Manager or contact the administrator of such communication manager servers.

- Format Specification File Path: If you had specified customized CDR format, then specify the absolute path of the customized CDR format specification file on the iSPI for IP Telephony server. You must prepare this file for each communication manager server before configuring the iSPI for IP Telephony for accessing CDR data from each communication manager server.

- If you have not configured survivable CDRs for the communication manager and if the CDRs are pushed through a TCP/IP link using the Reliable Session Protocol, then, you must do additional configuration using the SAT screen on the native configuration manager of the communication manager. Using this configuration, you must create a valid Avaya node name linked to the IP Address of the iSPI for IP Telephony server where you want the CDRs to be pushed by the communication manager. You must also do the IP-services configuration to specify the previously configured node name as the CDR link peer and specify the TCP/IP port number on the iSPI for IP Telephony server where you want the CDRs to be sent. Note down the other Reliable Session Protocol (RSP) settings such as the Packet Response Timer and the Inactivity Timer as they are configured in the IP-services SAT screen. You must specify the same values in the Avaya CDR Data Access configuration page for the iSPI for IP Telephony. Note that you must set the Reliable flag to true in the IP-services SAT screen as the iSPI for IP Telephony only works with the communication manager acting as an RSP peer while sending the CDR data through a TCP/IP link. Depending on whether the communication manager is configured to send CDRs directly to the iSPI for IP Telephony or through a CLAN device, specify the CLAN IP address in the Avaya CDR Data Access configuration page of iSPI for IP Telephony. You can retrieve the information about the survivability of CDRs from the appropriate SAT screen on the native configuration manager of the communication manager. For more information, see the Avaya Communication Manager documentation or contact the administrator of such communication manager servers.

- If the communication manager uses customized CDR format, then you must create the format specification file, save it on the disk of your iSPI for IP Telephony server, and specify the absolute path to the format specification file while configuring Avaya CDR data access using the iSPI for IP Telephony. It is recommended that the format specification file is saved in specific folders on the iSPI for IP Telephony server. This makes sure of implementing consistency in the Avaya CDR processing-based features in the iSPI for IP Telephony deployed in an Applicable Failover or HA environment. The designated folder where the iSPI for IP Telephony saves the format specification file is as follows: $NnmDataDir/shared/ipt/avayacdr/conf. You must also make sure that you create a format specification file for each communication manager which has a different customized CDR format. You must specify the absolute path to the file when configuring CDR data access for individual communication managers using the iSPI for IP Telephony. In case multiple communication managers have the same customized CDR format, then, you can specify the absolute path to the same customized format specification file while configuring CDR data access for each of these communication managers.

The NNM iSPI for IP Telephony supports the following standard CDR formats for Avaya IP Telephony:

- 59 characters
- Printer
- TELESEER
- ISDN-Printer
- ISDN-TELESEER

For customized CDR format, configure the `NnmDataDir/shared/ipt/conf/CustomizedCDRFormat.properties` as required. While you modify the file, refer to the instructions in the file. Make sure that you do not include blank space characters before or after the changes you make.

Configuring Avaya RTCP Reception

To monitor the voice quality at the Avaya RTP endpoints during a call, and to generate reports on the voice quality, the NNM iSPI for IP Telephony relies on the reception and processing of RTCP packets from Avaya RTP endpoints such as the IP phones, the media processors, and the H.248 gateways. To enable the NNM iSPI for IP Telephony to process the RTCP packets from the Avaya RTP endpoints, you must configure the reception of RTCP packets using the **NNM iSPI for IP Telephony Avaya Data Access Configuration** form. You can perform this configuration by logging on to the NNMi console as an administrator.

The points to consider while configuring Avaya RTCP reception are as follows:

- Make sure that you perform the required configuration tasks on the Avaya Communication Managers using the support SAT screens in the native configuration UI.

  - Specify the IP address and the port number of the RTCP server to be used as the destination for a copy of the RTCP packets sent by the Avaya RTP session participants to other session participants.
  - Configure the endpoints of the primary communication managers appropriately to send the RTCP packets to the iSPI for IP Telephony.

- Make sure that all the endpoints included in the network region on the communication manager use the same default RTCP server settings (the same IP address and UDP port number combination that maps to a valid IP address and UDP port number on the iSPI for IP Telephony server).
- Specify the correct IP address and the UDP port number combination in the Data Access Configuration form for the NNM iSPI for IP Telephony. You must specify the same values that you had specified in the native configuration wizard for the communication manager for receiving and processing the RTCP packets at the NNM iSPI for IP Telephony server.
- If you have seeded the node hosting a primary communication manager using an iSPI for IP Telephony instance, then you must do the required configuration first on the communication manager and then on the NNM iSPI for IP Telephony. This makes sure that the copies of RTCP packets sent from the endpoints of the communication manager are received by the NNM iSPI for IP Telephony instance used to seed the node hosting the primary communication manager.

Configuring Data Access for Acme Session Director

Configuration Parameters for CDR Data Access

The NNM iSPI for IP Telephony uses the timestamps from the CDR records. If the time-stamp of the Session Director is different from that of the NNM iSPI for IP Telephony Server, the time-stamp of the call data differs from that of the NNM iSPI for IP Telephony Server.

To configure CDR access, you must provide the following details:

- **Acme SD IP Address**: The management IP Address of the Acme Session Director

Note: If Acme Session Directors are deployed in an HA 1:1 redundancy mode, consider the following:

- For a Push Receiver mode—where the CDR files are pushed by the Acme Session Director to the NNM iSPI for IP Telephony Server— you need to configure the Management IP Address of only one of the Session Directors from the redundant pair.
- For an FTP mode—used where the CDR files are pulled from Acme Session Director the NNM iSPI for IP Telephony Server—you must configure the Management IP Addresses of both the Session Directors.

- **Format Specification File**: The default Format Specification Path (`/var/opt/OV/shared/ipt/conf/acme/AcmeCDRStopRecordFormat.properties`) is pre-populated . You can customize this file if the CDR **STOP** Record format from your Acme Session Director is different from the one that is defined in the default `AcmeCDRStopRecordFormat.properties` file.
- **CDR Files Download Path**: The CDR Files Download Path is pre-populated, suffixed by the management IP Address provided in the Acme SD IP Address field. You can modify the path, however, make sure that it is created in the `/var/opt/OV/shared/ipt/acmecdr` directory if the NNMi is installed on a Linux server. However, if the NNMi is installed on a Windows server, you need to specify only the newly-created directory (`\acmecdr`)

  Note: For a Push Receiver mode the path must be configured in the Session Director under the `account-config -> push-receiver -> Remote Path`, on both the Active and Standby Servers.

- **Is IPT SPI Server configured as a push receiver?**: Select **True** if the Push Receiver mode is used, and **False** if the FTP Mode is used.

  Note: If the FTP server is used, you must configure the following parameters aditionally:

  - CDR File Remote Path: Indicates the path on the Acme Session Director, from where CDR files can be downloaded using the FTP by the NNM iSPI for IP Telephony Server.
  - CDR Polling Interval: Indicates the interval (in minutes) at which the NNM iSPI for IP Telephony performs an FTP connect to the Acme Session Director to collect the CDR files. Specify an interval between 2 – 60 minutes.
  - User Name: Indicates the FTP user name to be used by the NNM iSPI for IP Telephony to connect to the Session Director.
  - Password: Indicates the password for the created user name.

Configuration Parameters for HDR Data Access

The HDR download subdirectory for Acme Session Director must exist in the `/var/opt/OV/shared/ipt/acmehdr` directory.

Opening Firewall Ports

To monitor the different types of IP telephony infrastructure, you must enable communication through firewalls by opening a few firewall ports. This section provides you information on the firewall ports to be opened for the following IP telephony infrastructure:

- Cisco IP Telephony
- Avaya IP Telephony

- Microsoft IP Telephony

Cisco IP Telephony

The following table lists the ports that must be opened in the NNMi management server to monitor the Cisco IP telephony:

Port Number	Protocol	Comments
162	SNMP over UDP	This port is used for receiving SNMP traps from the devices.
21	FTP over TCP	This port is used for CDR push using FTP from Cisco Unified Communications Manager clusters; specifically from the publisher Cisco Unified Communications Manager in the cluster.

The following table lists the ports that must be opened in the relevant Cisco IP telephony entities:

Port Number	Protocol	Comments
161	SNMP over UDP	This port is used for sending SNMP queries to the Cisco devices to collect data from them. Open this port in the relevant IP telephony devices such as Cisco Unified Communications Managers, Cisco Unified Communications Manager Expresses, voice gateways, gatekeepers, SRST routers, unity connections, unity devices, and so on.
8443	SOAP/HTTPS over TCP	This port is required by the NNM iSPI for IP Telephony to collect essential configuration and CDR data by communicating with the `CDRonDemand` Web services serviceability interface and AXL Web services serviceability interface on Cisco Unified Communications Manager cluster.
22	SSH over TCP	This port is required by NNM iSPI for IP Telephony to execute UCOS CLI commands programmatically on the Cisco Unified Communications Manager nodes. Open this port in all the Cisco Unified Communications Managers in the CUCM cluster.
80	HTTP over TCP	This port is required for the programmatic collection of Quality of Experience (QoE) measures for active RTP sessions and audio calls in which the Cisco IP phones take part. Open this port in all Cisco IP phones controlled by various the CUCM clusters. You can decide not to open this port in the phones for which you want the real time monitoring of QoE measures, such as MOS, jitter, latency, and delay.

Avaya IP Telephony

The following table lists the ports that must be opened in the NNMi management server to monitor the Avaya IP telephony:

Port Number	Protocol	Comments
162	SNMP over UDP	This port is used for receiving SNMP traps from the Avaya Communication Managers.
Configurable	RTCP over UDP	Configure a port for RTCP packets reception in the NNMi management server for each Avaya Communication Manager. The ports must be distinct for each Avaya Communication Manager. You cannot use the same port for two or more Avaya Communication Managers. The Avaya RTP endpoints (such as IP Phones, media gateways, and media processors) controlled by an Avaya Communication Manager send the RTCP packets to the port configured for that particular Avaya Communication Manager. If the primary Avaya Communication Manager is deployed in duplex redundant pair, you need to open this port in only one of the two physical Avaya Communication Managers.
Configurable	Avaya RSP over TCP	Configure a port for Avaya Reliable Session Protocol (RSP) in the NNMi management server for each Avaya Communication Manager. You must not use the same port for more than one Avaya Communication Manager. Each Avaya Communication Manager streams the CDRs to the port configured for this purpose. An Avaya Communication Manager may stream CDRs to this port directly or through its Processor Ethernet IP node or CLAN IP node. If the primary Avaya Communication Manager is deployed in duplex redundant pair, you need to open this port in only one of the two physical Avaya Communication Managers.

The following table lists the ports that must be opened in the relevant Avaya IP telephony:

Port Number	Protocol	Comments
161	SNMP over UDP	This port is used for sending SNMP queries to the Avaya devices to collect data from them. Open this port in the relevant IP telephony devices such as Avaya Communication Managers, Local Survivable Processors (LSPs), H248 media gateways, CLANs, and so on.

Port Number	Protocol	Comments
5022	SSH over TCP	This port is required by NNM iSPI for IP Telephony to execute Avaya SAT commands programmatically on the Avaya Communications Manager servers. Open this port in both physical Avaya Communication Managers in redundant pairs.
22	SSH over TCP	This port is required for the programmatic execution of SFTP/SSH to collect the CDR files from Avaya Communication Managers. Open this port in both the physical Avaya Communication Managers of the redundant pair. Open this port only if the Avaya Communication Manager streams its CDR data using RSP. If the Avaya Communication Manager provides the CDR data through survivable file based CDR interface, you may not have to open this port.

Microsoft IP Telephony

The following table lists the ports that must be opened in the NNMi management server to monitor the Microsoft IP telephony:

Port Number	Protocol	Comments
162	SNMP over UDP	This port is used for receiving SNMP traps from the devices.

The following table lists the ports that must be opened in the relevant Microsoft IP telephony:

Port Number	Protocol	Comments
161	SNMP over UDP	This port is used for sending SNMP queries to the Sangoma gateways and NET gateways to collect data from them. Open this port in the Sangoma gateways and NET gateways.
1433	TCP	This port is used for CDR/QOE data collection from the monitoring server database. The default port is 1433, but you can configure any other port also for this purpose. Open this port on each server in the monitoring server pool.
1434	UDP	This port is used for CDR/QOE data collection from the monitoring server database. Open this port on each server in the monitoring server pool.

Port Number	Protocol	Comments
5985/5986 (HTTP/HTTPS)	TCP	These ports are used for initiating remote powershell commands on Lync Frontend server. Open these ports on each server in the Lync Frontend server pool.

Configuring the Reporting Data Retention Period

After integrating the NNM iSPI for IP Telephony with the iSPI Performance for Metrics/Network Performance Server(NPS) for reporting, you can configure the reporting data retention period. This value can be configured while installing the NPS. You can modify the data retention period using the configuration utility provided by the NPS. For more information, see the *HP Network Mode Manager i SPI for Metrics Software Installation Guide 10.00*.

Setting up Shared Directory for the NPS

When installed on a dedicated server, the NPS creates a shared directory on the NNMi management server to gather the data collected by the NNMi. You must make sure that the shared directory is present before using the NNM iSPI for IP Telephony and the iSPI Performance for Metrics/NPS to view the reports. For more information about creating a shared directory, see the *HP Network Mode Manager i SPI for Metrics Software Installation Guide 10.00*.

Configuring Data Access for Cisco

To configure data access for Cisco IP telephony, you must provide the configuration parameter details for the AVVID XML Layer (AXL) and the Call Details Record (CDR) data access.

Configuration Parameters for AXL Data Access

Specify the following parameters to configure the AXL API exposed data:

- **Cluster ID**: Specifies the cluster identifier. You can retrieve this information from the administration web page of the CUCM.
- **CM IP Address**: Specifies the IP address of the CUCM server node in the cluster. The NNM iSPI for IP Telephony uses this IP address to obtain the AXL data for this cluster. It is recommended that you provide the IP address of the publisher CUCM node in your cluster.
- **AXL User Name**: Specifies the AXL user name to be used for invoking the AXL Web Services.
- **AXL Password**: Specifies the password associated with the AXL user name.

Configuration Parameters for CDR Data Access

- Make sure that the system time for the NNM iSPI for IP Telephony server must be equal to or slower than the system time of the CDR repository server if both the servers belong to the same time zone. If the servers are in different time zones, the NNM iSPI for IP Telephony uses the system time of the server for CDR retrieval. This might cause the time stamp of the call data to be different when compared to the actual time of the call.

  Before configuring CDR access, make sure that the `CDRonDemand` Web Service is running on the Call Manager repository server.

  Specify the following parameters to configure the CDR access:

  - **Cluster ID**: Specifies the cluster identifier. You can retrieve this information from the administration web page of the CUCM.
  - **Server IP**: Specifies the IP address of the CUCM CDR repository server in the cluster where the `CDRonDemand` Web Service is running.
  - **SOAP User Name**: Specifies the SOAP user name to access the `CDRonDemand` Web Service in the cluster.
  - **SOAP Password**: Specifies the password associated with the SOAP user name.
  - **Port**: Specifies the port number used by the `CDRonDemand` Web Service on the server that hosts the Web Service.

    Note: Do not include blank space characters before or after the values.

- Configure an SFTP/FTP user name and password on the NNM iSPI for IP Telephony server that the `CDRonDemand` Web Service uses to send CDR files to the NNM iSPI for IP Telephony server. If you are running the NNM iSPI for IP Telephony on a Microsoft Windows operating system, you must configure an SFTP/FTP client and make sure that the `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection` folder is shared for SFTP/FTP user access.

  Note: If the NNM iSPI for IP Telephony is installed on a Microsoft Windows operating system, you must make sure that the home directory for the user, specified in SFTP/FTP user name, is configured as `%NnmDataDir%\shared\ipt\IPTCiscoCDRCollection` and the user has write access to the home directory.

CDR Data Access Configuration Guidelines for Clusters

The NNM iSPI for IP Telephony enables you to access the CDR data from all the CUCM clusters. The NNM iSPI for IP Telephony collects the data in one of the following modes:

- `CDRonDemand` Web Service
- Billing Server

CDRonDemand Web Service Mode

In this mode the NNM iSPI for IP Telephony acts as a web service client for the CDRonDemand Web Service hosted on a server node inside the cluster. For collection of data in this mode, you must do the required configuration on the CUCM server in a cluster that hosts the CDR repository node role for the cluster. The configuration includes specifying the following details:

- The IP address or the fully qualified domain name of the CUCM server node on the cluster that hosts the CDR-on-Demand Web Service
- The SOAP/Web-Services user name
- The SOAP/Web-Services password
- The time interval at which the NNM iSPI for IP Telephony server must look for newly–created CDR files - It is recommended that you specify a time interval of two minutes to five minutes for a scalable processing of the CDR information across a period of time. It is also recommended that you configure the CDR repository server node in the cluster to publish the CDR files after short time intervals, instead of publishing the accumulated CDR information after a time interval of two minutes to five minutes.

Additionally, make sure of the following:

- The home directory of the SFTP/FTP server on the NNM iSPI for IP Telephony must be a valid sub directory under the NnmDataDir/shared/ipt/IPTCiscoCDRCollection directory.
- The CDR repository–hosting node in the cluster has adequate ability to perform SFTP/FTP transfers and upload files at the specified folder location on the NNM iSPI for IP Telephony server.

Billing Server Mode

In this mode the NNM iSPI for IP Telephony exports the CDR data from the repository server to the NNMi management server. For collection of data in this mode, you must do the required configuration on the CUCM server in a cluster that hosts the CDR repository node role for the cluster. The configuration includes specifying the following details:

- The fully qualified domain name of the NNM iSPI for IP Telephony server as the designated billing server
- The SFTP/FTP user name
- The SFTP/FTP password
- The complete directory path of the newly-created directory, if NNMi is installed on a Linux server (/var/opt/OV/shared/ipt/IPTCiscoCDRCollection/); however, if the NNMi is installed on a Windows server only the name of the newly-created directory (\IPTCiscoCDRCollection)
- The time interval at which the NNM iSPI for IP Telephony server must scan the billing server directory for the newly–arriving CDR files - It is recommended that you specify a time interval of two minutes to five minutes for a scalable processing of the CDR information across a period of

time. It is also recommended that you configure the CDR repository server node in the cluster to publish the CDR files after short time intervals, instead of publishing the accumulated CDR information after a time interval of two minutes to five minutes.

Additionally, make sure of the following:

- The directory in the NNM iSPI for IP Telephony server file-system, where the CDR files must be uploaded by the CDR repository node in the cluster, is a subdirectory of the `NnmDataDir/shared/ipt/IPTCiscoCDRCollection` directory.
- The home directory of the SFTP/FTP user on the NNM iSPI for IP Telephony must be a valid sub directory under the `NnmDataDir/shared/ipt/IPTCiscoCDRCollection` directory.
- The CDR repository—hosting node in the cluster has adequate ability to perform SFTP/FTP transfers and upload files at the specified folder location on the NNM iSPI for IP Telephony server.

Chapter 6: Troubleshooting

Acme CDR File Processing Fails due to CDR-field Mismatch

Problem

The NNM iSPI for IP Telephony fails to process the Acme CDRs due to CDR-field mismatch.

Solution

The `cdr-output-inclusive` parameter (disabled by default), in the account configuration file of the Session Director, must be enabled to ensure that the empty fields in the local CDR files are filled with zeros (0s). Else, the NNM iSPI for IP Telephony cannot process the Acme CDRs due to the CDR-field mismatch between the fields defined in the default `AcmeStopCDRRecordFormat.properties` file and the fields in the CDR files of the Session Director. If the `cdr-output-inclusive` parameter cannot be enabled for some reason, make sure that you edit the `AcmeStopCDRRecordFormat.properties` file manually—to include only the non-empty CDR fields from the CDR file of the Session Director in your environment.

Secure Shell (SSH) Authentication Issue

For any authentication issue during an SSH connection, make sure that, on the client machine, a proper entry of the server exists in the **known_hosts** file (for example, `~/.ssh/known_hosts`). To achieve this, you must login to the remote server manually (using SSH) and make an entry into the **known_hosts** file.

Monitoring Parameters for a UCM Cluster show 'No Value' in the Analysis Pane

Problem

One or more monitoring parameters for a UCM Cluster may show `No Value` in the Analysis Pane.

Cause

This ocurs when one of the UCMs does not respond or not collect data for the particular monitoring parameter.

Solution

To resolve this problem, follow these steps:

1. Log on to the NNMi console.
2. Click **Cisco IP Telephony**, and then click **UCM Clusters**.

3. Double-click the UCM Cluster that you want to verify. The **UCM Cluster Details** form opens.
4. Click **UCMs** tab in the right pane. The UCMs view opens on the right pane.
5. From the list check for the UCM that is not responding to data collection request for the monitoring parameter that is showing `No Value`.
6. Check and resolve if there are any SNMP or SSH access issues for the particular UCM.

SNMP Trap Loading Fails for Avaya and Nortel Devices

Problem

The NNMi fails to load the NNM iSPI for IP Telephony–specific SNMP traps if you have `Avaya G3 Alarms` and `Nortel COMMON MIB` SNMP traps loaded before you install the NNM iSPI for IP Telephony.

Cause

NNMi fails to load the NNM iSPI for IP Telephony–specific SNMP traps because the traps with the same **SNMP Object ID** are loaded in the NNMi database. This results in the `duplicate key - unique constraint violation` exception.

Symptom

Symptom can be one of the following:

- The NNM iSPI for IP Telephony workspace is not available.
- The `%NnmDataDir%\log\nnm\nnm-trace.log` file contains trace messages similar to the following message:

  ```
  ERROR: duplicate key value violates unique constraint "nms_snmp_trap_config_
  oid_key"
  ```

Solution

If you have any `Avaya G3 Alarm` SNMP traps loaded before installing the NNM iSPI for IP Telephony, you must delete them. To delete the SNMP traps, follow these steps:

1. Log on to the NNMi console.
2. From the **Workspace** pane, click **Configuration** and expand **Incidents**.
3. Click **SNMP Trap Configurations**. The SNMP Trap Configurations view opens in the right pane.
4. Select the SNMP traps with the following `SNMP Trap Object ID (OID)`:

- .1.3.6.1.4.1.6889.1.8.1.0.2
- .1.3.6.1.4.1.6889.1.8.1.0.3
- .1.3.6.1.4.1.6889.1.8.1.0.4
- .1.3.6.1.4.1.6889.1.8.1.0.5
- .1.3.6.1.4.1.6889.1.8.1.0.6
- .1.3.6.1.4.1.6889.1.8.1.0.12
- .1.3.6.1.4.1.6889.1.8.1.0.14
- .1.3.6.1.4.1.6889.1.8.1.0.15

5. Click **Delete**.
6. Restart the ovjboss process by running the following commands:
   - **ovstop -c ovjboss**
   - **ovstart -c ovjboss**

If you have any Nortel COMMON MIB SNMP traps loaded before installing theNNM iSPI for IP Telephony, follow these steps:

1. Log on to the NNMi console.
2. From the **Workspace** pane, click **Configuration** and expand **Incidents**.
3. Click **SNMP Trap Configurations**. The SNMP Trap Configurations view opens in the right pane.
4. Select the SNMP traps with the following SNMP Trap Object ID (OID):
   - .1.3.6.1.4.1.562.3.10.10.1.0.1
   - .1.3.6.1.4.1.562.3.10.10.1.0.2>
   - .1.3.6.1.4.1.562.3.10.10.1.0.3
   - .1.3.6.1.4.1.562.3.10.10.1.0.4
   - .1.3.6.1.4.1.562.3.10.10.1.0.5
   - .1.3.6.1.4.1.562.3.10.10.1.0.6
   - .1.3.6.1.4.1.562.3.10.10.1.0.7
5. Click **Delete**.

6. Restart the `ovjboss` process by running the following commands:
   - **`ovstop -c ovjboss`**
   - **`ovstart -c ovjboss`**

Discovery of the Avaya Communications Manager Server Fails

To resolve this issue, perform the following tasks:

Create Communication Configuration Regions for Avaya Communication Manager

- When you specify the communication configuration for Avaya Communication Manager servers, it is recommended that SNMP queries do not use `SNMP GetBulk` while communicating with these nodes. To enforce this restriction and consistent behavior of SNMP agents on the Avaya Communications Manager server nodes, use the Communication Configuration form in the NNMi Configuration workspace and specify Regions that include this exclusive specification of communication configurations only for the required set of Avaya Communications Manager Server nodes.

  Note: You must complete this configuration task for all the Avaya Communications Manager server nodes, including each of the following:

  - Physical server in duplex redundant pairs of Primary Servers
  - Stand-alone Primary Server that is not deployed in duplex redundant pairs
  - Local Survivable Processor (LSP) server node in your environment

- For better consistency in request response sessions, it is also recommended that you set up the regions in such a way that NNMi and the NNM iSPI for IP Telephony use a time-out value of 59 seconds and retry count value of 1 for all the SNMP communications with these nodes. For more information on specifying Regions, see the *HP Network Node Manager i Software Online Help for Administrators 10.00.*

Configure IP Address for SNMP Access on Avaya Communication Manager

- Make sure that the Avaya Communication Manager receives SNMP requests only from the NNMi management server. Therefore, you must configure the IP address of the NNMi management server alone for the SNMP access in the System Management Interface (SMI) window of the Avaya Communication Manager. For more information, see the Avaya Communication Manager documentation.

Configure SNMP Communities on Avaya Communication Manager

- Enable the SNMP Version 1 and the SNMP Version 2c in the Avaya Communication Manager. You must also configure the same Community Name (read-only) for SNMP Version 1 and SNMP Version 2c.

Configure the Discovery Cycle for Avaya

Before you configure the discovery cycle for Avaya, install the following Avaya service packs (patches) on the Avaya Communication Managers:

- Service pack 6 (Patch 18576) or later versions of the service packs if you are using version 5.x of the Avaya Communication Manager.
- Service pack 2 (Patch 18567) or later versions of the service packs if you are using version 6.x of the Avaya Communication Manager.

To configure the discovery cycle for Avaya, follow these steps:

1. On the **NNM iSPI for IP Telephony Avaya Discovery Configuration** form, clear the **Use NNMi node discovery interval** check box.
2. Type the **Discovery Interval** in hours. The default and the recommended interval is 2160 hours (90 days).
3. Select the **Pause state pollers during discovery** check box.

For more information, see the **Configuring Discovery Settings for Avaya Primary Servers** topic of the *Network Node Manager iSPI for IP Telephony Software Online Help 10.00*.

SNMP Request to Nortel Devices Times Out

To resolve this issue and for the consistent behavior of SNMP agents on the Nortel nodes, use the **Communication Configuration** form in the NNMi Configuration workspace and specify the regions only for the Nortel nodes.

For better consistency in request response sessions, do as follows:

- Set up the regions in such a way that the NNMi and NNM iSPI for IP Telephony use a time-out value of 59 seconds and the retry count value of 2.
- Use SNMPv1 for all the communications with these nodes.

For more information on specifying Regions, see the *HP Network Node Manager i Software Online Help for Administrators 10.00.*

Chapter 7: Performance and Scalability Metrics for the NNM iSPI for IP Telephony

You can use the following performance and scalability metric values to plan the single instance deployment of the NNM iSPI for IP Telephony in your enterprise:

Entity	Count	Additional Information
IP phone extensions and associated IP telephony functions/devices	Up to 50,000	You can include devices from different vendors. Note that the device count stays below 50,000. It is assumed that the count of the remaining NNMi objects (routers, switches, nodes, and so on) is less than 3500. In a Global Network Management (GNM) environment, the iSPI for IP Telephony supports up to 2,50,000 IP phone extensions and associated IP telephony functions/devices.
Host Channel Adapter (HCA) /Horizontal Cross Connect (HCC) sustained with 100,000 Busy Hour Call Attempts (BHCA)/ Busy Hour Call Completion (BHCC) for CDR collection, analysis and reporting on Call Duration, Call Counts, Call Quality Metrics Jitter, Packet Loss, Delay and MOS.	Up to 53,000	Call Quality Metrics reporting is available only for Cisco in the 9.01 version of the iSPI for IP Telephony. The reporting data is retained for a period of 70 days. In a Global Network Management (GNM) environment, the iSPI for IP Telephony supports up to 5,30,000 HCA/HCC sustained with 100,000 BHCA/BHCC for CDR collection, analysis and reporting.
User sessions	Up to 40	Support for up to 40 simultaneous user sessions.

Entity Discovered	Discovery Time	Additional Information
Discovery of IP telephony entities and the corresponding configuration properties required for subsequent monitoring and diagnostics	24 hours	After the discovery is complete, the iSPI for IP Telephony completes the initialization of the states and the current values of hourly performance and usage metrics from the network within 30 minutes.
Detect state changes for IP telephony entities after discovery and initialization	Within 10 minutes	For the IP phone entities, you can configure the iSPI for IP Telephony to detect changes in registration states within five minutes.

Entity Discovered	Discovery Time	Additional Information
Alerts for breach of set thresholds for Cisco IP Telephony Call Quality metrics (Jitter, Packet Loss, Delay and MOS)	Within five minutes	The alert is generated within five minutes of call completion.
Alerts for breach of set thresholds for Avaya IP Telephony hourly performance and usage measures such as Call Processor Occupancy Summaries, Port Network Load Summaries, DSP/CODEC Usage Summaries, Route Pattern/Trunk Group Usage Summaries, and so on	Within 30 minutes	The alert is generated within 30 minutes of threshold violation.

Note: For more information, see the *HP Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix 10.00*. For more information about sizing your NNMi and iSPI Performance for Metrics/Network Performance servers adequately to support the highest sustained demands on scalability and performance, contact the HP Support or see the *HP Network Node Manager i Software System and Device Support Matrix 10.00* and the *HP Network Node Manager iSPI Performance for Metrics Software Support Matrix 10.00*.

We appreciate your 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 for IP Telephony Software 10.00)

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.