Hewlett Packard
Enterprise

HPE Network Node Manager iSPI for IP Telephony Software

Software Version: 10.20
for the Windows® and Linux® operating systems

Deployment Reference

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

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

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

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

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

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

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

sFlow is a registered trademark of InMon Corp.

UNIX® is a registered trademark of The Open Group.

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

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

Contents

Introducing the NNM iSPI for IP Telephony

The HPE Network Node Manager i Smart Plug-in for IP Telephony (NNM iSPI for IP Telephony) Software helps you to extend the capability of the HPE 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 *HPE Network Node Manager i Software Deployment Reference*.

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

- *HPE Network Node Manager i Software Deployment Reference*
- *HPE Network Node Manager i Software Release Notes*
- *HPE Network Node Manager i Software Support Matrix*
- *HPE Network Node Manager iSPI for IP Telephony Software Installation Guide*
- *HPE Network Node Manager iSPI for IP Telephony Software Release Notes*
- *HPE 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 **https://softwaresupport.hpe.com**.

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 *HPE NNM i Software Interactive Installation Guide 10.20*.

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 *HPE Network Node Manager iSPI for IP Telephony SoftwareInstallation Guide 10.20*.

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 *HPE Network Node Manager iSPI for IP Telephony Software Installation Guide 10.20* 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 *HPE Network Node Manager iSPI for IP Telephony Software System and Device Support Matrix 10.20* 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.

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 *HPE 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 *HPE Network Node Manager iSPI for IP Telephony Software Installation Guide 10.20*.

   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 *HPE 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 *HPE HPE Network Node Manager i Software Deployment Reference 10.20*.

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 *HPE Network Node Manager i Software Deployment Reference 10.20*.

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 `/opt/OV/shared/ipt/conf`*`%NnmdataDir%`*`\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/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:

   `%NnmInstallDir%``\misc\nnm\ha\nnmhastartrg.ovpl NNM<`*`resource_group`*`>/opt/OV/misc/nnm/ha/nnmhastartrg.ovpl NNM <`*`resource_group`*`>`

   For more information about starting the NNMi HA resource group, see the *HPE Network Node Manager i Software Deployment Reference 10.20*.

If the NNMi does not start, see the *Troubleshooting the HA Configuration* section of the *HPE Network Node Manager i Software Deployment Reference 10.20*.

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

   %NnmInstallDir%\misc\nnm\ha\nnmhaconfigure.ovpl NNM -addon IPT/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 *HPE 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 /opt/OV/shared/ipt/conf*%NnmdataDir%*\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/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:

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

   %Nnmdatadir%\hacluster\<*resource_group_name*>/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 /opt/OV/shared/ipt/conf*%NnmdataDir%*\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/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:

      %Nnmdatadir%\hacluster\<*resource_group_name*>/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 /opt/OV/shared/ipt/conf*%NnmdataDir%*\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/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:

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

%Nnminstalldir%\misc\nnm\ha\nnmhaclusterinfo.ovpl –config NNM –get NNM_ADD_ON_PRODUCTS/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 *HPE Network Node Manager i Software Deployment Reference 10.20*.

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 *HPE Network Node Manager i Software Deployment Reference*.

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 security group–tenant 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 the SRST router deployed for failover, you must make sure that you configure the same security group–tenant 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 B Channel Activity 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.

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 *HPE Network Node Manager i Software Deployment Reference 10.20*, 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.

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 *HPE Network Node Manager i Software Deployment Reference 10.20*. 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 *%NnmDataDir%*`\shared\nnm\conf\props\nms-ui.properties/opt/OV/shared/nnm/conf/props/nms-ui.properties` file, change the value of `com.hp.nms.ui.sso.isEnabled` from `false` to `true`.
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 *HPE 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 *HPE 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:
   %nnmdatadir%`\shared\ipt\conf/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/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:

   %nnmdatadir%\nmsas\ipt\conf/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 *HPE Network Node Manager i Software Deployment Reference 10.20*.

   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:

   %nnminstalldir%\bin\nmsiptauthconfigreload.ovpl/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:

- *%nnmdatadir%*\nmsas\ipt\conf\props\nms-users.properties/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 *HPENNM 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 *HPE 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 *HPE Network Node Manager i Software Online Help*.

Requirement for New NNMi 10.20 Installations

New installations of NNMi support only TLS v1.2 protocol by default. However, to be able to discover and monitor Cisco IP telephony data, NNMi is required to use the TLSv1 cryptographic protocol.

To configure NNMi to support the TLSv1 cryptographic protocol for device communication:

Note: This procedure enables NNMi to use less secure cryptographic protocols that are not FIPS 140-2-certified. This is a global change and may reduce the security of the product.

1. Log on to the NNMi management server.
2. Open the following file with a text editor:
   - *Windows:* `%NnmDataDir%\nmsas\nms\server.properties`
   - *Linux:* `/var/opt/OV/nmsas/nms/server.properties`
3. Update the `com.hp.ov.nms.ssl.PROTOCOLS` property to include the value `TLSv1`.
   If the property does not exist, add the following line:
   `com.hp.ov.nms.ssl.PROTOCOLS=TLSv1.2,TLSv1.1,TLSv1`
4. Configure NNMi to allow protocols and algorithms that are not FIPS-certified:
   a. On the NNMi management server, go to the following directory:
      - *On Windows:* `%nnminstalldir%\newconfig\HPNmsServStgs\Windows`
      - *On Linux:* `/opt/OV/newconfig/HPNmsServStgs/Linux`
   b. Copy the `java.security` file, and then place the copied file in the following directory:
      - *On Windows:* `%nnmdatadir%\conf\nnm`
      - *On Linux:* `/var/opt/OV/conf/nnm`
5. Restart the NNMi processes by running the following commands:
   - *On Windows:*
     i. **%nnminstalldir%\bin\ovstop -c**
     ii. **%nnminstalldir%\bin\ovstart -c**
   - *On Linux:*
     i. **/opt/OV/bin/ovstop -c**
     ii. **/opt/OV/bin/ovstart -c**

Recommendations for Configuring Data Access

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

- Cisco
- Avaya

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 AXL Data Access

You must 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 iSPI for IP Telephony uses the same time zone. If the servers are in different time zones, the iSPI for IP Telephony uses the system time of the iSPI for IP Telephony 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, you must also 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 you type.

You must also configure an SFTP/FTP user name and password on the NNM iSPI for IP Telephony server which 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\log\ipt\tmp` folder is shared for SSFTP/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%\log\ipt\tmp` and the user has write access to the home directory.

Data Access Recommendations for Clusters

Make sure that you configure the NNM iSPI for IP Telephony to access the CDR data from all the clusters.

You must note down the following details for each CUCM Cluster in the environment and provide this information in the Data Access Configuration form for the NNM iSPI for IP Telephony:

- The NNM iSPI for IP Telephony supports collection of CDR data using the following mechanisms supported by Cisco:
  - Mechanism that requires the iSPI for IP Telephony to act as a billing server.
  - Mechanism that requires NNM iSPI for IP Telephony to act as a web services client for the `CDR-on-Demand` Web Service hosted on a server node inside the cluster.

    You must determine the mode used by a specific cluster before proceeding with CDR data access configuration.
    - For the billing server—based collection 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 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: Usually, on the NNM iSPI for IP Telephony server, this directory is located at a relative path to the `$NnmDataDir/log/ipt/tmp` directory. The home directory of the SFTP/FTP server on the NNM iSPI for IP Telephony must be a valid sub directory under the `$NnmDataDir/log/ipt/tmp` directory. Make sure that 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. While configuring CDR access for a cluster in the NNM iSPI for IP Telephony Cisco Data Access Configuration page, you must specify the name of the relative path to the directory of NNM iSPI for IP Telephony where the CDR files are uploaded by the CDR repository node in the cluster.
- The `CDR-on-Demand` Web Service—based collection requires you to specify the following details:
  - The SOAP/Web-Services user name and password
  - 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 home directory of the SFTP/FTP server on the NNM iSPI for IP Telephony must be a valid sub directory under the `$NnmDataDir/log/ipt/tmp` directory. Make sure that 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.
- Specify the time interval at which the NNM iSPI for IP Telephony server must scan the billing server directory for newly arriving CDR or CMR files. If you are using the `CDR-on-Demand` Web Service method, specify the time interval at which the NNM iSPI for IP Telephony server must look for newly created CDR or CMR files. It is recommended that you specify a time interval of two minutes to five minutes for scalable

processing of the CDR or CMR 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 or CMR files after short time intervals, instead of publishing the accumulated CDR or CMR information after a time interval of two minutes to five minutes.

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 Avaya Data Access Configuration form of the NNM iSPI for IP Telephony, 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 in the *HPENNM iSPI for IP Telephony Online Help* 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 in the *HPENNM iSPI for IP Telephony Online Help* or contact the administrator of such communication manager servers.
- Note whether the circuit ID fields for the trunk group members appear in the CDRs.
  You must 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 in the *HPENNM iSPI for IP Telephony Online Help* 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 in the *HPE NNM iSPI for IP Telephony Online Help* or contact the administrator of such communication manager servers.

Send Documentation Feedback

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

Feedback on Deployment Reference (Network Node Manager iSPI for IP Telephony Software 10.20)

Just add your feedback to the email and click send.

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

We appreciate your feedback!