

HP Network Node Manager iSPI for IP Multicast

Software Version: 10.10
for the Windows® and Linux® operating systems

Deployment Reference

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



Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notice

© Copyright 2008-2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

AMD is a trademark of Advanced Micro Devices, Inc.

Google™ is a registered trademark of Google Inc.

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

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

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

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

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

sFlow is a registered trademark of InMon Corp.

UNIX® is a registered trademark of The Open Group.

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

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

Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://softwaresupport.hp.com>

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

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

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

Support

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

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

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

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

<https://hpp12.passport.hp.com/hppcf/createuser.do>

To find more information about access levels, go to:

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is

<http://h20230.www2.hp.com/sc/solutions/index.jsp>

Contents

Chapter 1: Introducing the NNM iSPI for IP Multicast	6
Preparing for Deployment	6
Environment Variables Used in the NNM iSPI for IP Multicast Documents	7
Chapter 2: Deploying the NNM iSPI for IP Multicast	8
Deploy the NNM iSPI for IP Multicast and NNMi Together	8
Deploy the NNM iSPI for IP Multicast in an NNMi Environment	9
Using Single Sign-On with NNMi	9
Configuring Access with Public Key Infrastructure Authentication	10
Configuring NNMi	11
Configuring a Certificate Validation Method	11
Enabling Secure Sockets Layer (SSL) on the NNM iSPI for IP Multicast	11
Configuring the NNM iSPI for IP Multicast	12
Deploy the NNM iSPI for IP Multicast with the NNM iSPI Performance for Metrics/NPS	12
Installing the NNM iSPI for IP Multicast in an HA Cluster	15
Installing the NNM iSPI for IP Multicast	15
Configuring an HA Cluster on a Set of Systems with NNMi and iSPI	15
Installing the NNM iSPI for IP Multicast in an Existing NNMi HA Cluster Environment	18
Patching the NNM iSPI for IP Multicast in an HA Cluster	20
Remove the NNM iSPI for IP Multicast from a High Availability Cluster Environment	22
Deploy the NNM iSPI for IP Multicast in an Application Failover Environment	23
Deploying the NNM iSPI for IP Multicast in an Application Failover Environment with Oracle Database	23
Deploying the NNM iSPI for IP Multicast in an Application Failover Environment with Embedded Database	24
Patching the NNM iSPI for IP Multicast in an Application Failover Environment	25
Applying Patches for Application Failover (Shut Down Both Active and Standby)	25
Deploy the NNM iSPI for IP Multicast with the NNM iSPI for MPLS	27
Deploy the NNM iSPI for IP Multicast in Global Network Management Environment	28
Deploying NNMi and NNM iSPI for IP Multicast on the Global Manager and Regional Manager Management Server	28
Deploying NNMi on the Global Manager and NNMi and NNM iSPI for IP Multicast on the Regional Manager Management Server	29
Deploying NNMi and the NNM iSPI for IP Multicast on the Global Manager and NNMi on the Regional Manager Management Server	30
Deploying the Regional Manager in the Application Failover Environment	31

Send Documentation Feedback32

Chapter 1: Introducing the NNM iSPI for IP Multicast

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

You can plan the deployment of the NNM iSPI for IP Multicast based on how NNMi is deployed in the environment. While planning the deployment, consider the following areas to achieve an optimum performance of the system:

- Number of IP Multicast nodes, PIM interfaces, and IP Multicast flows.
- Deployment of the NNM iSPI for IP Multicast in a High Availability (HA) environment
- Deployment of the NNM iSPI for IP Multicast in an Application Failover environment
- Deployment of the NNM iSPI for IP Multicast with other iSPIs (NNM iSPI for MPLS and NNM iSPI Performance for Metrics/NPS)
- Deployment of the NNM iSPI for IP Multicast in a Global Network Management (GNM) environment.

Preparing for Deployment

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

Factors that impact the deployment of the NNM iSPI for IP Multicast include the type of database configured with NNMi and the size of the network that you want to monitor. In addition, ensure to install the latest NNMi patches before installing the NNM iSPI for IP Multicast.

Read the following NNMi documents before you start installing and configuring the NNM iSPI for IP Multicast:

- *HP Network Node Manager i Software Deployment Guide, 10.10*
- *HP Network Node Manager i Ultimate Edition Release Notes, 10.10*
- *HP Network Node Manager i Ultimate Edition Support Matrix, 10.10*
- *HP Network Node Manager Smart Plug-in for IP Multicast Installation Guide, 10.10*

For current versions of all documents listed here, go to:

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

Environment Variables Used in the NNM iSPI for IP Multicast Documents

The NNM iSPI for IP Multicast documents use the following NNMi environment variables to refer to file and directory locations. The default values are listed here. Actual values depend upon the selections made during NNMi installation.

The NNMi installation process creates the following system environment variables:

- On Windows:
 - *%NnmInstallDir%*: <drive>\Program Files\HP\HP BTO Software
 - *%NnmDataDir%*: <drive>\ProgramData\HP\HP BTO Software
- On Linux:
 - *\$NnmInstallDir*: /opt/OV
 - *\$NnmDataDir*: /var/opt/OV

Chapter 2: Deploying the NNM iSPI for IP Multicast

The NNM iSPI for IP Multicast and NNMi must be installed on the same management server. To install and configure NNMi on a management server, see the *NNMi Installation Guide and Deployment Reference Guide*.

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

- Installing NNMi and NNM iSPI for IP Multicast together on a single server. NNMi and NNM iSPI for IP Multicast are both configured together.
- Installing the NNM iSPI for IP Multicast in a system where NNMi is already installed and configured.
- Installing the NNM iSPI for IP Multicast in a Global Network Management environment.
- Installing NNMi, iSPI Performance for Metrics/ Network Performance Server (NPS), and NNM iSPI for IP Multicast on the same management server.
- Installing NNMi and NNM iSPI for IP Multicast on a management server and the NNM iSPI Performance for Metrics/ NPS in a dedicated server.

Deploy the NNM iSPI for IP Multicast and NNMi Together

To deploy NNMi and the NNM iSPI for IP Multicast on a management server, follow these steps:

1. Complete the NNMi installation process.
2. Create a New User with the Web Service Client Role from the NNMi console.

For more information about creating users, see *NNMi Help, Configure User Accounts (User Account Form)*.

Note: Make sure to use the same database type (Postgres Embedded database or Oracle) as NNMi when you are installing the NNM iSPI for IP Multicast

3. Install the NNM iSPI for IP Multicast, 10.10. For more information, see the NNM iSPI for IP Multicast *Installation Guide*.
4. Start the IP Multicast processes by using the command: `ovstart -c mcastjboss`.
5. After installing the NNM iSPI for IP Multicast and starting the IP Multicast processes, log on to the NNMi console, and then verify the availability of the IP Multicast workspace and IP Multicast views.

6. Seed the IP Multicast nodes from the NNMi console. The discovery process starts after you seed the nodes and multicast capability of nodes are discovered along with the other capabilities of the nodes. For more information, see *NNMi Online Help*.
7. Wait for sometime till the NNM iSPI for IP Multicast nodes are discovered. Navigate to the NNMi console to verify the availability of the IP Multicast workspace, IP Multicast views, and IP Multicast configuration workspace.

Deploy the NNM iSPI for IP Multicast in an NNMi Environment

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

1. Install the NNM iSPI for IP Multicast on a management server where NNMi is already installed, running, and nodes are discovered.

Note: Make sure to use the same database type (Postgres Embedded or Oracle) as NNMi when you are installing the NNM iSPI for IP Multicast.
2. Start the IP Multicast process by using the command: `ovstart -c mcastjboss`.
3. You can start the discovery process to discover the IP Multicast nodes from the discovered NNMi nodes in any *one* of the following ways:
 - Select all the IP Multicast nodes from NNMi inventory workspace and start the configuration poll. For more information, see *Help for NNMi*.
 - Wait for the next NNMi discovery cycle to rediscover the nodes and also start the discovery of the NNM iSPI for IP Multicast nodes.
 - Run the command `nmsmulticastdisco.ovpl` to discover all multicast nodes.
4. After installing the NNM iSPI for IP Multicast, log on to the NNMi console, and then verify the availability of the IP Multicast workspace, IP Multicast views, and IP Multicast configuration workspace.

Using Single Sign-On with NNMi

You can configure HP Network Node Manager i Software (NNMi) single sign-on (SSO) to facilitate access to the NNM iSPI for IP Multicast Configuration workspace from the NNMi console without needing to log on again. SSO is not enabled during installation or when you upgrade from the previous versions.

To enable SSO:

For Windows:

1. Edit the `%NnmDataDir%\shared\nnm\conf\props\nms-ui.properties` file. Change `com.hp.nms.ui.sso.isEnabled= "false"` to `com.hp.nms.ui.sso.isEnabled = "true"`.
2. Run the `nnmsso.ovpl -reload` script.
3. Run the `nnsmulticastssoreload.ovpl` script.

For Linux:

1. Edit the `$NnmDataDir/shared/nnm/conf/props/nms-ui.properties` file. Change `com.hp.nms.ui.sso.isEnabled= "false"` to `com.hp.nms.ui.sso.isEnabled = "true"`.
2. Run the `nnmsso.ovpl -reload` script.
3. Run the `nnsmulticastssoreload.ovpl` script.

Note: Do not enable Single Sign-On feature when NNMi and the NNM iSPI for IP Multicast is configured to use Public Key Infrastructure (PKI) authentication

For more information about SSO, see *NNMi Deployment Reference, Using Single Sign-On*.

Configuring Access with Public Key Infrastructure Authentication

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

When the NNMi is configured to use the PKI authentication, it is mandatory for the iSPI to use the PKI authentication.

Note: You can continue to authenticate users with the NNMi user credentials for the NNM iSPI for IP Multicast Configuration form. However, do not configure only the iSPI to use the PKI authentication when NNMi continues to use the credentials-based authentication.

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

1. ["Configuring NNMi" on the next page](#)
2. ["Configuring a Certificate Validation Method" on the next page](#)
3. ["Enabling Secure Sockets Layer \(SSL\) on the NNM iSPI for IP Multicast" on the next page](#)
4. ["Configuring the NNM iSPI for IP Multicast" on page 12](#)

Note: To configure PKI authentication on the NNM iSPI for IP Multicast in an HA cluster, you must perform all the required changes on both, primary and secondary node.

Configuring NNMi

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

Configuring a Certificate Validation Method

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

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

Enabling Secure Sockets Layer (SSL) on the NNM iSPI for IP Multicast

When NNMi is configured to use the PKI authentication, you must enable SSL on the NNM iSPI for IP Multicast to ensure communication between the NNMi management server and the NNM iSPI for IP Multicast.

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

1. Log on to the NNM iSPI for IP Multicast.
2. Navigate to the following directory:
On Windows
`%nnmdatadir%\shared\multicast\conf`
On Linux
`var/opt/OV/shared/multicast/conf`
3. Open the **nnm.extended.properties** file with a text editor.
4. Set the value of following properties to true:
`com.hp.ov.nms.spi.multicast.spi.isSecure`
`com.hp.ov.nms.spi.multicast.Nnm.isSecure`
5. Save and close the file.
6. Restart the ovjboss process by running the following commands:
`ovstop -c multicastjboss`
`ovstart -c multicastjboss`

Configuring the NNM iSPI for IP Multicast

Configuring the NNM iSPI for IP Multicast to enable the PKI authentication you must modify the `nms-auth-config.xml` file in the iSPI configuration data directory (`%nnmdatadir%\nmsas\multicast\conf` on Windows; `/var/opt/OV/nmsas/multicast/conf` on Linux) based on the updated `nms-auth-config.xml` file.

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

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

On Windows

`%nnmdatadir%\nmsas\multicast\conf`

On Linux

`/var/opt/OV/nmsas/multicast/conf`

Open the `nms-auth-config.xml` file using a text editor.

Modify the `nms-auth-config.xml` file to enable the PKI authentication. For more information, see *Configuring NNMi for PKI (X.509 Certificate Authentication)* section in the *HP Network Node Manager Deployment Reference*

Note: Make sure that you modify the iSPI `nms-auth-config.xml` file to match the changes done to the `nms-auth-config.xml` file on the NNMi management server.

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

On Windows

`%NnmInstallDir%\multicast\bin\nmsmulticastauthconfigreload.ovpl`

On Linux

`/opt/OV/multicast/bin/nmsmulticastauthconfigreload.ovpl`

The NNM iSPI for IP Multicast now starts using the PKI authentication.

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

The `-u <user>` and `-p <password>` parameters are optional for Command Line Interface (CLI) in the NNM iSPI for IP Multicast.

Deploy the NNM iSPI for IP Multicast with the NNM iSPI Performance for Metrics/NPS

You must install NNMi 10.10, the NNM iSPI for IP Multicast 10.10, NNM iSPI Performance for Metrics/Network Performance Server 10.10 to view the IP Multicast reports. You can deploy these

products in the following scenarios:

- Installing NNMi, iSPI for IP Multicast, and the NNM iSPI Performance for Metrics/NPS on the same server.
- Installing the NNM iSPI for IP Multicast and NNMi on a management server and the NNM iSPI Performance for Metrics/NPS on a dedicated server.

To deploy all the products on the same management server, follow these steps:

1. Install NNMi, 10.10.
2. Install the NNM iSPI Performance for Metrics/NPS 10.10. For information about the steps to install, see *HP NNMi iSPI Performance for Metrics/NPS Installation Guide*.
3. Install the NNM iSPI for IP Multicast, 10.10.

Note: Always install the NNM iSPI Performance for Metrics/NPS and then install the NNM iSPI for IP Multicast. If you have installed NNMi and NNM iSPI for IP Multicast before installing NPS and NNM iSPI Performance for Metrics, remove the *<Extension Pack>.processed* copy from the following location.

- Linux:
`<$NnmDataDir>/shared/perfSpi/datafiles/extension/final folder.`
- Windows:
`<%NnmDataDir%>\shared\perfSpi\datafiles\extension\final folder`

Replace the *<extension pack>* in the *<Extension Pack>.processed* copy with the following:

- IP_Multicast_Flow
- IP_Multicast_Interface

After removing the file, the extension packs are installed automatically.

To deploy NNMi and NNM iSPI for IP Multicast on the same management server and the NNM iSPI Performance for Metrics/NPS on a dedicated server, follow these steps:

1. Install NNMi, 10.10 and NNM iSPI for IP Multicast, 10.10 on the same management server.
2. Install the NNM iSPI Performance for Metrics/ NPS 10.10 on a dedicated server.
3. Complete the necessary configurations for NNMi, iSPI for IP Multicast and iSPI Performance for Metrics/NPS.

Note: Always install the NNM iSPI Performance for Metrics/NPS and then install the NNM iSPI for IP Multicast. If you have installed NNMi and NNM iSPI for IP Multicast before installing NPS and iSPI Performance for Metrics, remove the *<Extension Pack>.processed* copy from the following location:

- On Linux:
`<$NnmDataDir>/shared/perfSpi/datafiles/extension/ final folder.`
- On Windows:
`<%NnmDataDir%>\shared\perfSpi\datafiles\extension\final folder.`

Replace the *<extension pack>* in the *<Extension Pack>.processed* copy with the following extension pack:

- IP_Multicast_Flow
- IP_Multicast_Interface

After removing the file, the extension packs are installed automatically.

After you complete the installations, the NNM iSPI for IP Multicast introduces the following extension packs on the Metrics console:

Extension Pack Name	Purpose
IP_Multicast_Interface	Shows report for IP multicast traffic passing through the multicast nodes and Protocol-Independent Multicast (PIM) interfaces on the network.
IP_Multicast_Flow	Shows report for the IP multicast traffic for the selected flows.

The extension packs use data collected by the NNM iSPI for IP Multicast. Make sure that the NNM iSPI Performance for Metrics/ NPS is up and running. To view the IP Multicast reports from the NNMi console, click **Actions -> HP NNM iSPI Performance -> Reporting - Report Menu**. The iSPI Performance for Metrics console appears with the IP Multicast metrics and you can generate the IP Multicast reports.

After you uninstall the NNM iSPI for IP Multicast, the extension packs introduced by the NNM iSPI for IP Multicast are not removed. If the NNM iSPI Performance for Metrics is running, the extension packs introduced by the NNM iSPI for IP Multicast, still appear. You must remove the extension packs manually before you start installing the NNM iSPI for IP Multicast again. For more information, see *Troubleshooting the NNM iSPI for IP Multicast* section from the NNM iSPI for IP Multicast *Installation Guide*.

Installing the NNM iSPI for IP Multicast in an HA Cluster

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

Installing the NNM iSPI for IP Multicast

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

- Install NNMi and the NNM iSPI for IP Multicast in your environment before configuring NNMi to run under HA. See ["Configuring an HA Cluster on a Set of Systems with NNMi and iSPI" below](#).
- Install and configure the NNM iSPI for IP Multicast in an existing NNMi HA cluster environment. See ["Installing the NNM iSPI for IP Multicast in an Existing NNMi HA Cluster Environment" on page 18](#).

Note: To configure PKI authentication on the NNM iSPI for IP Multicast in an HA cluster, you must perform all the required changes on both, primary and secondary node. For information on required changes, see ["Configuring Access with Public Key Infrastructure Authentication" on page 10](#)

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

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

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

To configure the NNM iSPI for IP Multicast on the primary node, follow these steps:

1. Install NNMi and NNM iSPI for IP Multicast on each system. See the *NNMi Installation Guide* and the *NNM iSPI for IP Multicast Installation* guide for more information.
2. Configure the HA software on the systems and configure NNMi to run under HA. See the *NNMi Deployment Reference* for information on configuring NNMi to run under HA. Do not start the resource group while configuring NNMi to run under the HA (do not run the `nnmhastartrg.ovpl` command).

3. Configure the NNM iSPI for IP Multicast on the primary (active) node:

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

```
nnmofficialfqdn.ovpl
```

- b. Modify the following files from the \$NnmdataDir/shared/multicast/conf or %NnmdataDir%\shared\multicast\conf to replace the host name with the virtual FQDN for the following parameters:

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

- c. Modify the server.properties file from the %nnminstallDir%\multicast\server\ or /opt/OV/multicast/server/ directory to reflect the Virtual FQDN of the NNMi management server for the com.hp.ov.nms.fqdn parameter.
- d. Modify the login-config.xml file from the %nnminstallDir%\multicast\server\conf or /opt/OV/multicast/server/conf directory to reflect the virtual FQDN of the NNMi management server (for the module-option element).
- e. Modify the relevant files in the following directory with the up-to-date information on both the primary and secondary cluster nodes:

For Linux:

```
/var/opt/OV/shared/multicast/conf
```

For Windows:

```
%NnmDataDir%\shared\multicast\conf
```

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

For Windows:

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

For Linux

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

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

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

- g. Run the following command to configure the NNM iSPI for IP Multicast to run under the HA cluster:

For Windows:

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

For Linux:

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

4. Configure the NNM iSPI for IP Multicast on the secondary (passive) node:
 - a. Install NNMi with NNM iSPI for IP Multicast on the secondary node. Make sure the secondary node has a separate Fully Qualified Domain Names (FQDN) during the installation. See the *NNMi Installation Guide* and the *HP Network Node Manager iSPI for IP Multicast Software Installation Guide* for more information.
 - b. Run the following command to find the virtual hostname:

```
nnmofficialfqdn.ovpl
```
 - c. Modify the following files in the `$NnmdataDir/shared/multicast/conf` or `%NnmdataDir%\shared\multicast\conf` to replace the host name with the virtual FQDN for the following parameters:

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

- d. Modify the `server.properties` file from the `%nnminstalldir%\multicast\server\` or `/opt/OV/multicast/server/` directory to reflect the Virtual FQDN of the NNMi management server for the `com.hp.ov.nms.fqdn` parameter.
 - e. Modify the `login-config.xml` file from the `%nnminstalldir%\multicast\server\conf` or `/opt/OV/multicast/server/conf` directory to reflect the virtual FQDN of the NNMi management server (for the `module-option` element).
 - f. Modify the relevant files in the following directory with the up-to-date information on both the primary and secondary cluster nodes:
 For UNIX:

```
/var/opt/OV/shared/multicast/conf
```

 For Windows:

```
%NnmDataDir%\shared\multicast\conf
```
 - g. Run the following commands to configure the NNM iSPI for IP Multicast on the secondary node to run under the HA cluster:
 For Windows:

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

 For UNIX:

```
/opt/OV/misc/nnm/ha/nnmhaconfigure.ovpl NNM -addon MULTICAST
```
5. Repeat "[Configure the NNM iSPI for IP Multicast on the secondary \(passive\) node:](#)" above on all passive nodes if you have additional passive nodes in the HA cluster.
6. Verify that the NNM iSPI for IP Multicast is successfully registered by running the following command:

- *On Windows:*

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

- *On UNIX/Linux:*

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

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

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

1. Make sure that 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\
```

```
$NnmDataDir/hacluster/<resource_group_name>
```

3. Run `ovstatus -c` to make sure that `ovjboss` is running.
4. Install the NNM iSPI for IP Multicast on the primary (active) node in the cluster, but do *not* start the iSPI.

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

```
nnmofficialfqdn.ovpl
```

6. Make sure that the following files from the `$NnmdataDir/shared/multicast/conf` or `%NnmdataDir%\shared\multicast\conf` contain the virtual FQDN for the following parameters:

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

- a. Modify the `server.properties` file from the `%nnminstalldir%\multicast\server\` or `/opt/OV/multicast/server/` directory to reflect the Virtual FQDN of the NNMi management server for the `com.hp.ov.nms.fqdn` parameter.
- b. Make sure that the `login-config.xml` file from the `%nnminstalldir%\multicast\server\conf` or `/opt/OV/multicast/server/conf` directory contains the virtual FQDN of the NNMi management server (for the `module-option` element).

- c. Modify the relevant files in the following directory with the up-to-date information on both the primary and secondary cluster nodes:

For Linux

/var/opt/OV/shared/multicast/conf

For Windows:

%NnmDataDir%\shared\multicast\conf

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 Multicast. Make sure that NNMi fails over and runs on the secondary server successfully.
9. On this system, follow these steps:
 - a. Put the NNMi resource group to the HA maintenance mode by placing the maintenance file under the following directory:

%nnmdatadir%\hacluster\\$NnmDataDir/hacluster/<resource_group_name>
 - b. Run **ovstatus -c** to make sure that ovjboss is running.
 - c. Install the NNM iSPI for IP Multicast on this server., but do *not* start the iSPI.
 - d. Make sure that the following files from the /var/opt/OV/shared/multicast/conf or %NnmDataDir%\shared\multicast\conf contain the virtual FQDN for the following parameters :

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

- e. Modify the server.properties file from the %nnminstallldir%\multicast\server\ or /opt/OV/multicast/server/ directory to reflect the Virtual FQDN of the NNMi management server for the com.hp.ov.nms.fqdn parameter.
- f. Make sure that the login-config.xml file from the %nnminstallldir%\multicast\server\conf or /opt/OV/multicast/server/conf directory contains the virtual FQDN of the NNMi management server (for the module-option element).
- g. Modify the relevant files in the following directory with the up-to-date information on both the primary and secondary cluster nodes:

For Linux:

/var/opt/OV/shared/multicast/conf

For Windows:

```
%NnmDataDir%\shared\multicast\conf
```

- h. Remove the maintenance file that you added in [step a](#).
10. If you have multiple nodes in the cluster, fail over to another passive server, and then repeat [step a](#) through [step h](#).
11. Fail over to the server that was active when you started this procedure. Make sure that NNMi and NNM iSPI for IP Multicast are running.
12. Run the following command on the active server first, and then on all passive servers:

- *For Windows:*

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

- *For Linux:*

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

13. Verify that the NNM iSPI for IP Multicast is successfully registered by running the following command:

- *On Windows:*

```
%nnminstallDir%\misc\nnm\ha\nnmhaclusterinfo.ovpl -config NNM -get NNM_ADD_ON_PRODUCTS
```

- *On Linux:*

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

Patching the NNM iSPI for IP Multicast in an HA Cluster

If you have already configured NNMi and the NNM iSPI for IP Multicast 10.10 to work in an HA cluster, you must follow this section to apply necessary patches (for both NNMi and the NNM iSPI for IP Multicast).

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

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

- *Windows:*

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

- *Linux:*

```
/opt/OV/misc/nnm/ha/nnmhaclusterinfo.ovpl \-group <resource_group> -activeNode
```

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

- *Windows:*

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

- *Linux:*

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

Include the **NORESTART** keyword in both these files.

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

- *Windows:*

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

- *Linux:*

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

Include the **NORESTART** keyword in both these files.

4. On the active node, follow these steps:

- a. Stop NNMi:

```
ovstop -c
```

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

- c. Optional. Use the `nnmbackup.ovpl` command or another database command to backup all NNMi data. For example:

```
nnmbackup.ovpl -type offline -scope all -target nnmi_backups
```

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

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

- e. Start NNMi:

```
ovstart -c
```

- f. Verify that NNMi started correctly:

```
ovstatus -c
```

All NNMi services should show the state **RUNNING**.

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

Remove the NNM iSPI for IP Multicast from a High Availability Cluster Environment

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

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

1. Remove the NNM iSPI for IP Multicast by running the following command:

- Windows:

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

- For Linux:

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

Note: Run this command on the passive node first, and then on the active node as well.

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

Deploy the NNM iSPI for IP Multicast in an Application Failover Environment

You can deploy the NNM iSPI for IP Multicast in an application failover environment by selecting the database from the following scenarios:

Deploying the NNM iSPI for IP Multicast in an Application Failover Environment with Oracle Database

Scenario 1: In this deployment scenario, consider that you want to install the NNM iSPI for IP Multicast with NNMi and then configure application failover on NNMi.

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

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

2. Start NNMi on server 1.
3. Install the NNM iSPI for IP Multicast on server 1 with Oracle database by following the steps listed in the *HP NNM iSPI for IP Multicast Installation Guide*.
4. Merge the keystores on one server and copy the keystores to both the primary and the secondary servers. For information, see the *NNMi Deployment Reference Guide* for instructions.
5. After the installation of the NNM iSPI for IP Multicast, install the NNM iSPI for IP Multicast non production license on server 1.
6. Stop NNMi on server 1.
7. Start NNMi on server 2.
8. Install the NNM iSPI for IP Multicast in the secondary server mode on the server 2 with the same database instance, user name, and password as configured on the server 1. For more information, see *HP NNM iSPI for IP Multicast Installation Guide*.
9. Install the non production license available for the NNM iSPI for IP Multicast on server 2.
10. Configure the NNM iSPI for IP Multicast for an application failover between server 1 and server 2. The steps to configure the NNM iSPI for IP Multicast for application failover are similar to the steps to configure NNMi for application failover. For information about how to configure the iSPI for application failover, see *NNMi Deployment Reference Guide*.

Scenario 2: In this scenario, consider that you want to install the NNM iSPI for IP Multicast after configuring NNMi in an application failover environment:

1. Remove configuration for application failover from the NNMi primary and secondary servers.
2. Restore the old keystore and truststore specific to the primary server and the secondary server.
3. Install the NNM iSPI for IP Multicast on both primary and secondary servers following the steps discussed in Scenario 1.
4. Install the non production licenses available for the NNM iSPI for IP Multicast installed on a server 1 and a server 2.
5. Configure the NNM iSPI for IP Multicast for an application failover. For information about how to configure the iSPI for application failover, see *NNMi Deployment Reference Guide*.

Deploying the NNM iSPI for IP Multicast in an Application Failover Environment with Embedded Database

Scenario 1: In this scenario, consider that you want to install the NNM iSPI for IP Multicast and NNMi in an application failover mode:

1. Install NNMi and NNM iSPI for IP Multicast on the primary server and the secondary server.
2. Install the NNM iSPI for IP Multicast non production licenses on both the servers.
3. Follow instructions given in the *NNMi Deployment Reference Guide* to configure NNMi in application failover mode. After this, the NNM iSPI for IP Multicast automatically gets configured in the application failover mode.

Scenario 2: In this scenario, consider that you want to install the NNM iSPI for IP Multicast after configuring NNMi in an application failover mode:

1. Remove the NNMi application failover configuration from the primary and secondary server.
2. Restore the old keystore and truststore specific to the primary server and the secondary server. For information, see the *NNMi Deployment Reference Guide*.
3. Install the NNM iSPI for IP Multicast on both the primary and the secondary servers.
4. Install the NNM iSPI for IP Multicast non production license on both the servers.
5. Configure the NNM iSPI for IP Multicast for application failover.
6. Configure NNMi in the application failover mode. For more information about the steps to configure NNMi, see *NNMi Deployment Reference Guide*.

Patching the NNM iSPI for IP Multicast in an Application Failover Environment

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

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

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

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

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

1. As a precaution, back up your NNMi data on both the active and standby NNMi management servers before proceeding. For information, see NNMi Backup and Restore Tools in the NNMi Deployment Reference.
2. As a precaution, on the active NNMi management server, do the following steps:
 - a. Run the `nnmcluster` command.
 - b. Embedded database only: After NNMi prompts you, type `dbsync`, then press Enter. Review the displayed information to make sure it includes the following messages:

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

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

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

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

`STANDBY_READY`: This means that the standby NNMi management server is ready to perform if the active NNMi management server fails.
3. Run the `nnmcluster -halt` command on the active NNMi management server. This shuts down all `nnmcluster` processes on both the active and standby NNMi management servers.
4. To verify there are no `nnmcluster` nodes running on either server, complete the following steps on both the active and standby NNMi management servers.
 - a. Run the `nnmcluster` command.
 - b. Verify that there are no `nnmcluster` nodes present except the one marked (SELF).
 - c. Run `exit` or `quit` to stop the interactive `nnmcluster` process you started.

5. On the active NNMi management server, comment out the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
 - a. Edit the following file:
On Windows:
`%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
On Linux:
`opt/OV/shared/nnm/conf/props/nms-cluster.properties`
 - b. Comment out the `com.hp.ov.nms.cluster.name` parameter.
 - c. Save your changes.
6. Apply the NNMi and the NNM iSPI for IP Multicast patch to the active NNMi management server using the instructions provided with the patch.
7. On the active NNMi management server, uncomment the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
 - a. Edit the following file:
On Windows:
`%NnmDataDir%\shared\nnm\conf\props\nms-cluster.properties`
On Linux
`opt/OV/shared/nnm/conf/props/nms-cluster.properties`
 - b. Uncomment the `com.hp.ov.nms.cluster.name` parameter.
 - c. Save your changes.
8. Run the `nnmcluster -daemon` command on the active NNMi management server.
9. Run the `nnmcluster -dbsync` command to create a new backup.
10. On the standby NNMi management server, comment out the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
11. Apply the NNMi and the NNM iSPI for IP Multicast patch to the standby NNMi management server.
12. On the standby NNMi management server, uncomment the `com.hp.ov.nms.cluster.name` parameter in the `nms-cluster.properties` file.
13. Run the `nnmcluster -daemon` command on the standby NNMi management server.

Deploy the NNM iSPI for IP Multicast with the NNM iSPI for MPLS

The NNM iSPI for IP Multicast helps you to monitor the multicast services in the network. If the multicast services are used over an MPLS cloud, the integration of the NNM iSPI for IP Multicast and MPLS provides the collaborative monitoring of MVPN topology.

The NNM iSPI for MPLS helps you to monitor the Provider Edge (PE) routers discovered in an MVPN topology. The PE routers are configured with the multicast-enabled VRF (MVRP) capabilities and use the multicast services to transmit data.

Navigate from the NNM iSPI for MPLS to the NNM iSPI for IP Multicast to view the tree of multicast traffic in the core network (cloud between the PE routers). The multicast tree shows the default and data Multicast Distribution Tree (MDTs). For more information, see *the NNM iSPI for MPLS Online Help, Overview of the Multicast VPN (MVPN) and IP Multicast View*.

To deploy the NNM iSPI for IP Multicast with the NNM iSPI for MPLS, follow the steps:

1. Install NNMi 10.10.
2. Install the NNM iSPI for IP Multicast, 10.10.
3. Install the NNM iSPI for MPLS, 10.10.

There is no order to deploy the iSPIs (iSPI for MPLS or iSPI for IP Multicast) on a management server.

Deploy the NNM iSPI for IP Multicast in Global Network Management Environment

You can deploy the NNM iSPI for IP Multicast in a Global Network Management (GNM) environment. The NNM iSPI for IP Multicast uses the capabilities of NNMi Global Manager (NNMi GM) and provides a centralized view to monitor the multiple sites. The NNM iSPI for IP Multicast allows you to configure the regional manager connections by using the *IP Multicast Configuration* workspace. After the connection is established, view and monitor the IP Multicast nodes from the NNM iSPI for IP Multicast inventory (GM). For more information about how to configure the NNM iSPI for IP Multicast regional managers, see the NNM iSPI for IP Multicast *Online Help*.

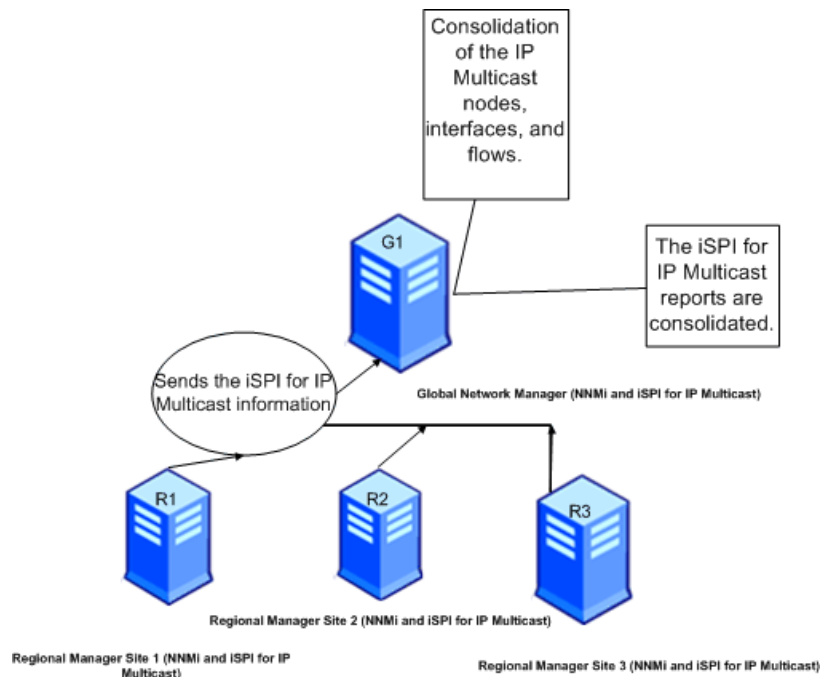
You can deploy NNMi and NNM iSPI for IP Multicast in a GNM environment for the following scenarios:

- Both NNMi and NNM iSPI for IP Multicast are configured on the global manager server and regional manager servers.
- NNMi is configured on the global manager server and NNMi and NNM iSPI for IP Multicast are configured on the regional manager servers.
- Both NNMi and NNM iSPI for IP Multicast are configured on the global manager server and only NNMi is configured on the regional manager server.

Deploying NNMi and NNM iSPI for IP Multicast on the Global Manager and Regional Manager Management Server

You can install and configure NNMi and the NNM iSPI for IP Multicast on the global manager and regional managers. For information about the configuration steps, see *NNMi and NNM iSPI for IP Multicast Online Help*.

The following figure represents a deployment scenario, where NNMi and NNM iSPI for IP Multicast is configured on the global manager (G1) and regional managers (R1, R2, and R3):



In this deployment scenario, all the regional managers (R1, R2, and R3) send the IP Multicast information to the global manager (G1). You can view the following information from G1:

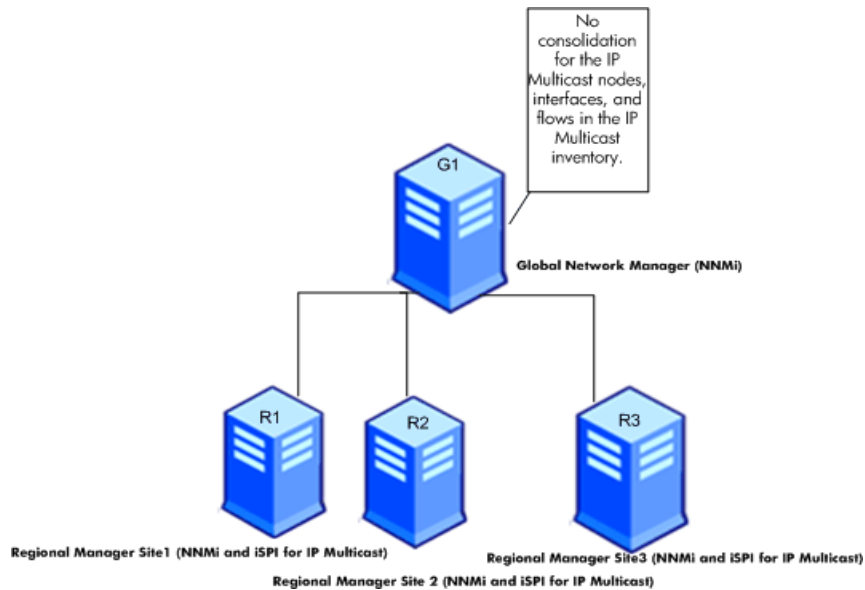
- Consolidated IP Multicast topology. The status of the IP Multicast nodes, interfaces, and PIM neighbors is calculated again in the global manager environment.
- Consolidated IP Multicast reports.

Note: You must install NNM iSPI Performance for Metrics/Network Performance Server to view the IP Multicast reports.

Deploying NNMi on the Global Manager and NNMi and NNM iSPI for IP Multicast on the Regional Manager Management Server

You can install and configure NNMi on the global manager and NNMi and NNM iSPI for IP Multicast on the regional managers. For information about the configuration steps, see the *NNMi and NNM iSPI for IP Multicast Online Help*.

The following figure represents a deployment scenario, where NNMi is configured on the global manager (G1). NNMi and the NNM iSPI for IP Multicast are configured on the regional managers (R1, R2, and R3):

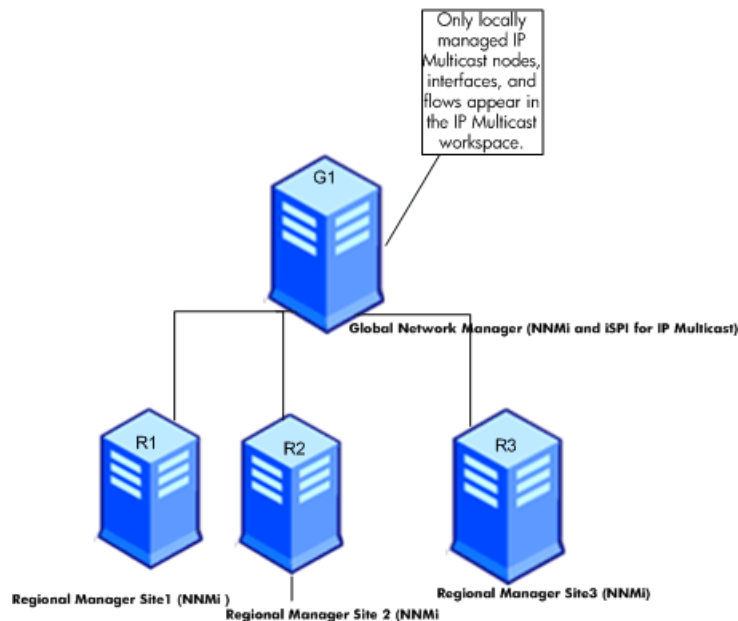


In this deployment scenario, all the regional managers (R1, R2, and R3) discover the IP Multicast nodes, interfaces, and flows. The NNM iSPI for IP Multicast is not available on G1 so there is no communication established between G1 and regional managers for the NNM iSPI for IP Multicast. Thus, the Multicast nodes, interfaces, and flows from the regional managers are not available in the G1 inventory. In addition, no aggregated IP Multicast reports are available in the IP Multicast (GNM) inventory.

Deploying NNMi and the NNM iSPI for IP Multicast on the Global Manager and NNMi on the Regional Manager Management Server

You can install and configure NNMi and the NNM iSPI for IP Multicast on the global manager and only NNMi on the regional managers. For information about the configuration steps, see in the *NNMi and NNM iSPI for IP Multicast Online Help*.

The following figure represents a deployment scenario, where NNMi and NNM iSPI for IP Multicast are configured on the global manager (G1) and NNMi on the regional managers (R1, R2, and R3):



In this deployment scenario, only the locally managed IP Multicast nodes, interfaces, and flows are available in the IP Multicast inventory (G1).

Deploying the Regional Manager in the Application Failover Environment

When the NNM iSPI for IP Multicast regional manager is in the Application failover environment, use the ORDER parameter to decide the priority to establish the connection.

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

1. Configure the regional manager connection using IP Multicast configuration workspace.
2. Add the two regional manager connections and provide the two hostnames.
3. Use the ORDER parameter to give different values to the two regional managers.

Whenever there is an application fail-over available on the regional manager, the GNM establishes the next connection with the lowest order value.

You can configure the regional manager in the application failover environment by using the steps documented in the following:

- ["Deploying the NNM iSPI for IP Multicast in an Application Failover Environment with Oracle Database" on page 23](#)
- ["Deploying the NNM iSPI for IP Multicast in an Application Failover Environment with Embedded Database" on page 24.](#)

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 Multicast 10.10)

Just add your feedback to the email and click send.

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

We appreciate your feedback!