HP Network Node Manager i Software

For the Windows®, HP-UX, Linux, and Solaris operating systems

Software Version: NNMi 9.23

HP Network Node Manager i Software—HP Intelligent Management Center Integration Guide

Document Release Date: May 2013
Software Release Date: May 2013Legal 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

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

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

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

UNIX® is a registered trademark of The Open Group.

Oracle Technology — Notice of Restricted Rights

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

For the full Oracle license text, see the license-agreements directory on the NNMi product DVD.

Acknowledgements

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

This product includes software developed by the Indiana University Extreme! Lab. (http://www.extreme.indiana.edu)

Available Product Documentation

In addition to this guide, the following documentation is available for NNMi:

- *HP Network Node Manager i Software Documentation List*—Available on the HP manuals web site. Use this file to track additions to and revisions within the NNMi documentation set for this version of NNMi. Click a link to access a document on the HP manuals web site.
- *NNMi Installation Guide*—This is an interactive document, and is available on the NNMI 9.20 product media.
  See the nnmi_interactive_installation_en_README.txt file, located on the product media, for more information.
- *HP Network Node Manager i Software Upgrade Reference*—Available on the HP manuals web site.
- *HP Network Node Manager i Software Release Notes*—Available on the product media and the NNMi management server.
- *HP Network Node Manager i Software System and Device Support Matrix*—Available on the product media and the NNMi management server.
- *HP Network Node Manager iSPI Network Engineering Toolset Planning and Installation Guide*—Available on the NNM iSPI NET diagnostics server product media.

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

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

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

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

Or click the **New users - please register** link on the HP Passport sign-in 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:

www.hp.com/go/hpsoftwaresupport

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches and associated patch documentation
- 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 user ID, go to:

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

To find more information about access levels, go to:

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

Contents

HP NNMi - HP IMC Integration 3
Value 4
Integrated Products 4
Documentation 5
Installing, Enabling and Configuring the HP NNMi - HP IMC Integration 5
Steps to Install and Enable the HP NNMi - HP IMC Integration 5
Discovering Information from IMC 13
Using the HP NNMi - HP IMC Integration 13
Opening an IMC console from a Node in NNMi 13
Using the Analysis Pane to View Device Information 15
Disabling the HP NNMi - HP IMC Integration 18
Maintaining the HP NNMi - HP IMC Integration 19
Loading Trap Definitions: I need to load a large quantity of HP IMC trap definitions and am encountering *Configuration Import Errors* 19
Discovery Configuration Change: Make configuration changes so NNMi automatically updates customAttributes for devices found in IMC. 19

HP Intelligent Management Center

HP Network Node Manager i Software (HP NNMi) enables you to quickly detect, isolate, and troubleshoot abnormal network behavior. Using HP NNMi, you can also record what has been done to date to troubleshoot or resolve a problem.

You can combine HP NNMi with other powerful HP tools by implementing Automated Network Management (ANM). ANM is a solution that integrates network fault detection, performance monitoring, configuration management and compliance, as well as diagnostic and automation tools. ANM enables the ITILv3 best practices in the network domain—namely event, incident, and problem management; change configuration; and release and deploy management. For more information, see the *HP Automated Network Management Concept Guide*.

When HP Networking devices are installed in your network, you can combine either ANM or HP NNMi with HP Intelligent Management Center (HP IMC) using the HP NNMi - HP IMC integration. The result is a better solution for managing your enterprise network. HP IMC adds change, configuration, and compliance features along with add-on modules for other device management needs.

For information about purchasing ANM (includes HP NNMi), HP NNMi, and HP IMC, contact your HP sales representative.

This document contains the following topics:

- HP NNMi - HP IMC Integration
- Installing, Enabling and Configuring the HP NNMi - HP IMC Integration
- Discovering Information from IMC
- Using the HP NNMi - HP IMC Integration
- Disabling the HP NNMi - HP IMC Integration
- Maintaining the HP NNMi - HP IMC Integration

HP NNMi - HP IMC Integration

You can deploy NNMi in either of two ways to enjoy the benefits of the HP NNMi - HP IMC integration:

- Use NNMi and the HP NNMi - HP IMC integration to leverage the features of HP NNMi and HP IMC together.
- Use NNMi and the HP NNMi - HP IMC integration along with Automated Network Management (ANM).
  ANM is a solution that integrates network fault detection, performance monitoring, configuration management and compliance, as well as diagnostic and automation tools. If you choose to implement the HP NNMi - HP IMC integration along with ANM, the result is complete network management using HP Software network management products. Wherever possible, these products automate network management tasks, thereby minimizing the time network engineers must spend on network maintenance.

Use the same set of instructions, shown in Installing, Enabling and Configuring the HP NNMi - HP IMC Integration, to implement either of these two approaches. Either approach combines the features of both HP NNMi and HP IMC. Together, HP NNMi and HP IMC provide better tools to manage networks with heterogeneous elements that require highly scalable and fully integrated network management tools.

Using the HP NNMi - HP IMC integration or using the HP NNMi - HP IMC integration with ANM provides the following functionality:

- Displays HP IMC fault events in HP NNMi.
- You can launch the HP IMC console from within HP NNMi to obtain H3C device details.
- Synchronizes the NNMi topology with the IMC inventory by using the IMC inventory as seeds for HP NNMi.
- Displays analysis panes so you can view device information.

Value

The HP NNMi–HP Intelligent Management Center integration provides the following benefits:

- You see a consolidated and correlated list of network events and notifications, resulting in better root-cause analysis and reduced meant time to repair (MTTR).
- You see a comprehensive inventory, augmented by HP IMC's rich model of H3C devices.
- You use one tool to monitor and manage your heterogenous network.
- You see a synchronized and consistent view of the network that enables self documentation and automation and reduces the total cost of ownership of your network.

Integrated Products

The information in this chapter applies to the following products:

- HP Intelligent Management Center

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

- NNMi 9.23

Documentation

This document describes how to configure and use the integration.

Obtain and read the following manuals to prepare for installing and configuring the HP NNMi - HP IMC integration:

- *HP Intelligent Management Center Installation Guide*
- *HP Intelligent Management Center Getting Started Guide*
- *HP Intelligent Management Center Base Platform Administrator Guide*

Installing, Enabling and Configuring the HP NNMi - HP IMC Integration

After you complete Task 1 through Task 4, HP IMC and HP NNMi begin sharing device information.

Steps to Install and Enable the HP NNMi - HP IMC Integration

Task 1: Installing NNMi 9.23 (Patch 3)

Task 2: Loading the MIBs Supported by HP IMC (Optional)

Task 3: Loading the Trap Definitions

Task 4: Enabling and Configuring the HP NNMi - HP IMC Integration

Task 1: Installing NNMi 9.23 (Patch 3)

To obtain and install NNMi 9.23 (Patch 3), do the following:

1. Point your browser to http://support.openview.hp.com/selfsolve/patches.
2. Search for NNMi 9.23 (Patch 3) for your operating system, then download the patch.
3. Install the patch according to the NNMi 9.23 (Patch 3) installation instructions.

Task 2: Loading the MIBs Supported by HP IMC (Optional)

Although not mandatory, manually loading the MIBs supported by HP IMC extends NNMi's monitoring capabilities. For example, having this additional information enables you to create custom collections using NNMi. See *Managing MIBs* in the *NNMi Help* for more information.

During the NNMi 9.23 (Patch 3) installation, the MIBs supported by HP IMC are *installed* on the NNMi management server. Complete the following steps to manually load these installed MIBs into NNMi using the `nnmloadmib.ovpl` script:

1. All of the NNMi processes must be running before you attempt to load any additional MIBs.
2. Look in the following directories and locate the additional MIBs that you want to load to support the HP NNMi - HP IMC integration

   Windows:

— `%NNM_SNMP_MIBS%\Vendor\H3C`

— `%NNM_SNMP_MIBS%\IMC`

UNIX:

— `$NNM_SNMP_MIBS/Vendor/H3C`

— `$NNM_SNMP_MIBS/IMC`

3 To load the additional MIBs for devices supported by HP IMC that exist in your network, see the directories shown in step 1. Run the following commands to load any of the MIBs for devices supported by HP IMC. Make sure to verify that the displayed results include the MIBs you load:

Windows:

```
nnmloadmib.ovpl -load %NNM_SNMP_MIBS%\Vendor\H3C\<mib name> -u
<username> -p <password>
```

```
nnmloadmib.ovpl -load %NNM_SNMP_MIBS%\IMC\<mib name> -u
<username> -p <password>
```

UNIX:

```
nnmloadmib.ovpl -load $NNM_SNMP_MIBS/Vendor/H3C/<mib name> -u
<username> -p <password>
```

```
nnmloadmib.ovpl -load $NNM_SNMP_MIBS/IMC/<mib name> -u
<username> -p <password>
```

Check for prerequisite MIBs before using the **`nnmloadmib.ovpl`** script to load these MIBs. The commands shown in this step will not load the MIBs if the prerequisite MIBs are not loaded.

Instead of using the **`nnmloadmib.ovpl`** script to load these MIBs, use the **Tools** > **Load/Unload MIB** menu in the NNMi console, as it lists any prerequisite MIBs.

4 Verify that the MIBs loaded correctly, by doing one of the following:

— Enter the following command:

```
nnmloadmib.ovpl -list -u <username> -p <password>
```

— From the NNMi console, navigate to **Configuration** > **MIBs** > **Loaded MIBs**.

Verify the presence of the MIBs you loaded from step 3.

Task 3: Loading the Trap Definitions

For HP NNMi to retain (not drop) HP IMC traps, you must manually load the HP IMC trap definitions that are important for your network. If you do not load any HP IMC trap definitions, HP NNMi drops the HP IMC traps forwarded to HP NNMi by HP IMC.

For most network environments, you will not want to load all of the HP IMC trap definitions into HP NNMi. It is important that you determine the traps that are important for your network, then load only those traps into HP NNMi.

To load the trap definitions for HP IMC-managed devices, do the following:

a Change to the following directory:

— *Windows*: `%NnmInstallDir%\newconfig\HPOvNmsEvent`

— *UNIX*: `$NnmInstallDir/newconfig/HPOvNmsEvent`

b For HP NNMi to retain (not drop) HP IMC traps, you must manually load the HP IMC trap definitions that are important for your network. If you do not load any HP IMC trap definitions, HP NNMi drops the HP IMC traps forwarded to HP NNMi by HP IMC.

HP NNMi provides the `nnm-imc-incidentConfig.xml` file that contains thousands of the HP IMC trap definitions. In most network environments, you do not want to load all of these trap definitions into HP NNMi. To stop from loading unnecessary trap definitions, create a subset of the `nnm-imc-incidentConfig.xml` file, removing any of the trap definitions you do not need.

To help determine which incidents to retain from the `nnm-imc-incidentConfig.xml` file, you might do the following:

a Access your HP IMC product.

b Browse the alarms that you are receiving, and determine which IMC alarms you want to forward to HP NNMi.

c Look for and save the incident definitions that contain the OIDs for those alarms in a file, such as `myincidents.xml`,

d Use the `myincidents.xml` file in the `nnmconfigimport.ovpl` command as shown below.

In rare circumstances, you might need to load a large number of trap definitions and could experience **Configuration Import Errors**. See Loading Trap Definitions: I need to load a large quantity of HP IMC trap definitions and am encountering Configuration Import Errors. on page 19 for more information.

Depending on whether you decide to use the `nnm-imc-incidentConfig.xml` file or the `myincidents.xml` file, use one of the following commands to load the HP IMC trap definitions:

– **`nnmconfigimport.ovpl -f myincidents.xml -u <username> -p <password>`**

– **`nnmconfigimport.ovpl -f nnm-imc-incidentConfig.xml -u <username> -p <password>`**

Task 4: Enabling and Configuring the HP NNMi - HP IMC Integration

After completing the steps in this section NNMi gathers data from the IMC servers you configured for the integration. During this discovery process, NNMi adds seeds for devices found in the set of IMC servers and links the devices to their IMC source.

NNMi discovers the devices contained in the IMC inventory and obtains information from IMC about these devices if they meet the following criteria:

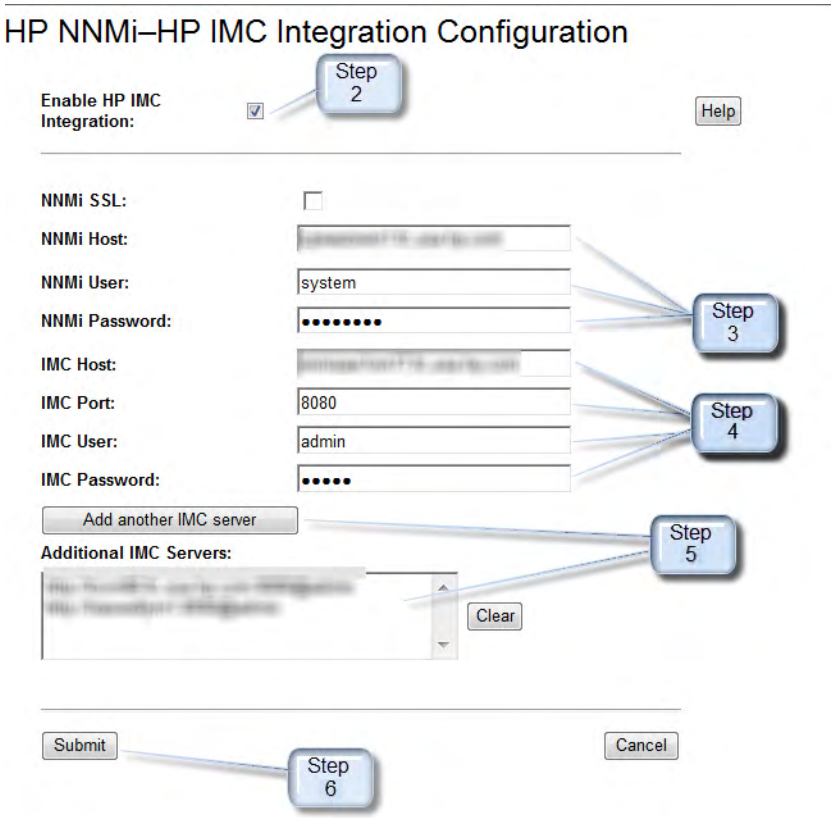
- NNMi has not already discovered the device.
- The device is not already entered as a seed device in NNMi.

See Discovering Information from IMC on page 13 for more information.

To enable the HP NNMi - HP IMC integration, do the following:

1 From the NNMi console, click **Integration Module Configuration** > **IMC**. HP NNMi shows the **HP NNMi - HP IMC Integration Configuration** screen show in Figure 1. See Figure 1 while configuring the HP NNMi - HP IMC integration.

Figure 1 Enabling the HP NNMi - HP IMC Integration.



2 Select **Enable IMC Integration**.

3 Select **IMC SSL** if you configured IMC to accept SSL connections.

You must also complete the steps shown in Configuring SSL Access for the HP NNMi - HP IMC Integration on page 9 to manually import the HP IMC certificate into the HP NNMi `truststore` file.

4 Add the following HP NNMi integration information:

- `NNMi host`: This field contains the fully qualified domain name of the NNMi management server.
- `NNMi User`: Enter an NNMi username that is mapped to an NNMi Administrators user group. This can also be an NNMi username mapped to an NNMi Web Service Clients user group.
- `NNMi Password`: Enter the NNMi username password.

5 Add the following HP IMC integration information:

- `IMC host`: This field contains the fully qualified domain name of the IMC server.
- `IMC Port`: This field contains the port number used for accessing the IMC server.
- `IMC User`: Enter the IMC username.
- `IMC Password`: Enter the IMC username password.

6 Optional: You can configure the HP NNMi - HP IMC integration module for multiple IMC servers. These IMC servers function as element managers for a set of devices. These devices would then be seeded into NNMi so that NNMi is aware of the full set of devices. To add another IM server, click **Add another IMC server**.

You do not need to configure the same username and password on each IMC host. HP NNMi supports using a separate IMC host username and password for each IMC host.

7 Click **Submit** to finish enabling the HP NNMi - HP IMC integration. After you click **Submit**, HP IMC and HP NNMi begin sharing device information.

NNMi periodically reads the set of management IP addresses from each configured IMC server. For each device that NNMi has not already discovered, and that does not already have a NNMi seed entry, NNM adds the new device or devices to its inventory. NNMi also saves the device ID as a custom attribute on the NNMi node.

If a node is removed from HP IMC or HP NNMi, you must manually remove the node from the other application. There is no automatic discovery synchronization for removing a node from HP IMC or HP NNMi.

Task 5: Configuring SSL Access for the HP NNMi - HP IMC Integration

After completing this task, single sign-on works between the NNMi console and the IMC console. Completing this task permits you to open the IMC console from the NNMi console to view the device details residing in IMC,

If you selected **IMC SSL** in step 3 on page 9, complete the following steps to configure an SSL connection between HP NNMi and HP IMC.

The instructions in this section include how to import the IMC trust certificate into the NNMi trust store. Before you import the IMC trust certificate into the NNMi trust store, you must replace the IMC keystore with one that you create (as shown in step a through step b), so that the hostname verification succeeds when HP NNMi connects to HP IMC.

SSL authentication relies on certificate path validation. For example, if VeriSign guarantees HP NNMi, and HP NNMi guarantees HP IMC, then the certificate path will be HP IMC <- HP NNMi <- VeriSign and authentication works correctly. These instructions assume that most systems trust VeriSign, and that you only need to import the HP NNMi and HP IMC certificates.

Important: If the HP IMC <- HP NNMi <- VeriSign chain is broken due to the HP NNMi certificate not being imported into HP IMC, or the HP IMC certificate not being imported into HP NNMi, the SSL authentication will not work properly.

a Generate a replacement IMC `keystore` file using the following command.

Replace *<IMC_FQDN>* with the fully qualified domain name of the IMC server.

Windows:
```
<IMC_Installation_Directory>\deploy\jdk\jre\bin\keytool.exe
-genkey -v -alias iMC -validity 3650 -keyalg RSA -dname
"CN=<IMC_FQDN>, OU=your_workgroup, O=Unknown, L=Unknown,
S=Unknown, C=Unknown" -keypass iMCV300R002 -storepass
iMCV300R002 -keystore keystore
```

UNIX:
```
<IMC_Installation_Directory>/deploy/jdk/jre/bin/keytool
-genkey -v -alias iMC -validity 3650 -keyalg RSA -dname
"CN=<IMC_FQDN>, OU=your_workgroup, O=Unknown, L=Unknown,
S=Unknown, C=Unknown" -keypass iMCV300R002 -storepass
iMCV300R002 -keystore keystore
```

b Replace the `keystore` file in the *<IMC_Installation_Directory>*`\client\security\` directory with the `keystore` file you generated in step a.

c Export the IMC certificates from the `keystore` file using the following command:

Windows:
```
<IMC_Installation_Directory>\deploy\jdk\jre\bin\keytool.exe
-export -alias imc -file C:\temp\IMC.cer -keystore
<IMC_Installation_Directory>\client\security\keystore
-storepass iMCV300R002
```

UNIX:
```
<IMC_Installation_Directory>/deploy/jdk/jre/bin/keytool
-export -alias imc -file /tmp/IMC.cer -keystore
<IMC_Installation_Directory>/client/security/keystore
-storepass iMCV300R002
```

d Verify that you see the `Certificate stored in file <directory>:\IMC.cer` message.

e Copy the certificate from the `IMC.cer` file you created in step c to the NNMi management server.

f Open a command window on the NNMi management server.

g To import the IMC certificate into the NNMi `nnm.truststore` file, run the following command:

Windows:
"%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe" -import -alias sentinel -file <*directory*>\IMC.cer -keystore "%NnmDataDir%\shared\nnm\certificates\nnm.truststore" -storepass ovpass

UNIX:
$NnmInstallDir/nonOV/jdk/nnm/bin/keytool -import -alias sentinel -file <*directory*>/IMC.cer -keystore $NnmDataDir/shared/nnm/certificates/nnm.truststore -storepass ovpass

Make sure you answer **yes** when asked whether to `Trust this certificate?`. The following program listing is an example of what happens after you run this command:

```
Owner: CN=iMC Development Team, OU=R&D Beijing, O="Hangzhou H3C
Technologies Co,. Ltd.", L=Shang-Di Information Industry Base,
ST=Beijing, C=CN
Issuer: CN=iMC Development Team, OU=R&D Beijing, O="Hangzhou H3C
Technologies Co,. Ltd.", L=Shang-Di Information Industry Base,
ST=Beijing, C=CN
Serial number: 4609e6be
Valid from: Tue Mar 27 21:53:34 MDT 2007 until: Sun Mar 27
21:53:34 MDT 2022
Certificate fingerprints:
         MD5:  A6:3D:D9:F2:15:13:09:4A:22:00:D9:C1:35:CD:53:02
         SHA1:
3D:40:80:73:C8:32:FA:23:F5:24:02:2D:6B:D9:12:C2:DA:94:66:85
         Signature algorithm name: MD5withRSA
         Version: 1
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

h Obtain the NNMi certificate alias name using the following command. Write down the alias value obtained during this step, as you will need that value for the `<alias>` variable used during the next step.

Windows:

"%NnmInstallDir%\nonOV\jdk\nnm\bin\keytool.exe" -v -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.keystore" -storepass nnmkeypass

Unix:

<NnmInstallDir>/nonOV/jdk/nnm/bin/keytool -v -list -keystore <NnmDataDir>/OV/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass

i Export the NNMi certificate to a file using the following command.

Windows:

"%NnmInstallDir%\nonOV\nnm\bin\keytool.exe" -export -alias <alias> -file <directory>\nnm.cer -keystore %NNMDataDir%\shared\nnm\certificates\nnm.keystore -storepass nnmkeypass

Unix:

<NnmInstallDir>/nonOV/jdk/nnm/bin/keytool -export -alias <alias> -file <Directory>/nnm.cer -keystore <NnmDataDir>/shared/nnm/certificates/nnm.keystore -storepass nnmkeypass

j Copy the NNMi certificate file to a directory on the IMC server.

For multiple IMC servers, complete step j through step l for each IMC server you plan to use in the HP NNMi - HP IMC integration.

k Import the NNMi certificate to the IMC `truststore` file using the following command.

Windows:

<*IMC_Installation_Directory*>\deploy\jdk\jre\bin\keytool.exe -import -alias <alias> -file <Directory>\nnm.cer -keystore <*IMC_Installation_Directory*>\iMC\client\security\truststore -storepass iMCV300R002

Unix:

<*IMC_Installation_Directory*>/deploy/jdk/jre/bin/keytool -import -alias <alias> -file <Directory>/nnm.cer -keystore <*IMC_Installation_Directory*>/iMC/client/security/truststore -storepass iMCV300R002

Make sure you answer **yes** when asked whether to `Trust this certificate?`. The following program listing is an example of what happens after you run this command:

```
Owner: CN=<fully qualified system name>
Issuer: CN=<fully qualified system name>
Serial number: 50789c62
Valid from: Fri Oct 12 16:40:34 MDT 2012 until: Sun Sep 18
16:40:34 MDT 2112
Certificate fingerprints:
         MD5:  CA:10:C4:8E:88:D5:21:04:DC:F2:95:74:47:65:B5:82
         SHA1:
0B:8D:1D:3F:F0:AA:87:87:D9:E9:1C:CD:DA:4F:C1:62:BF:62:E1:03
         Signature algorithm name: SHA1withRSA
         Version: 3
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

l Restart the IMC server using the HP Intelligent Deployment Monitoring Agent.

m Run the following command sequence on the NNMi management server:

– **ovstop**

– **ovstart**

n *Optional*: Run the following commands on both the NNMi management server and the IMC server. Compare the outputs to make sure the keystore certificates reside on both servers' truststore files:

NNMi management server (Windows):
keytool.exe -v -list -keystore %NnmDataDir%\shared\nnm\certificates\nnm.truststore -storepass ovpass

NNMi management server (UNIX):

```
keytool -v -list -keystore $NnmDataDir/shared/nnm/
certificates/nnm.truststore -storepass ovpass
```

IMC server (Windows):

```
<IMC_Installation_Directory>\deploy\jdk\jre\bin\keytool.exe
-v -list -keystore <IMC_Installation_Directory>/iMC/client/
security/truststore -storepass iMCV300R002
```

IMC server (UNIX):

```
<IMC_Installation_Directory>/deploy/jdk/jre/bin/keytool -v
-list -keystore <IMC_Installation_Directory>/iMC/client/
security/truststore -storepass iMCV300R002
```

Discovering Information from IMC

During discovery, NNMi gathers data from the IMC servers you configured for the integration. During this discovery process, NNMi adds seeds for all the devices found in the set of IMC servers and links the devices to their IMC source. NNMi also saves the device ID as a custom attribute on the NNMi node.

During discovery, if there are devices that have been discovered by multiple IMC servers, NNMi links the first IMC server reporting these devices as the IMC source. If multiple IMC servers discover a device, then NNMi only discovers the device from the first IMC server reporting the device to NNMi.

Devices contained in the IMC inventory share information with NNMi if they meet the following criteria:

- NNMi has not already discovered the device.
- The device is not already listed as a seed address in NNMi.

If NNMi has already discovered nodes that also reside in the IMC database, NNMi does not automatically update `customAttributes` for these devices. To make configuration changes so NNMi automatically updates customAttributes for devices found in IMC, see Discovery Configuration Change: Make configuration changes so NNMi automatically updates customAttributes for devices found in IMC. on page 19.

Using the HP NNMi - HP IMC Integration

Opening an IMC console from a Node in NNMi

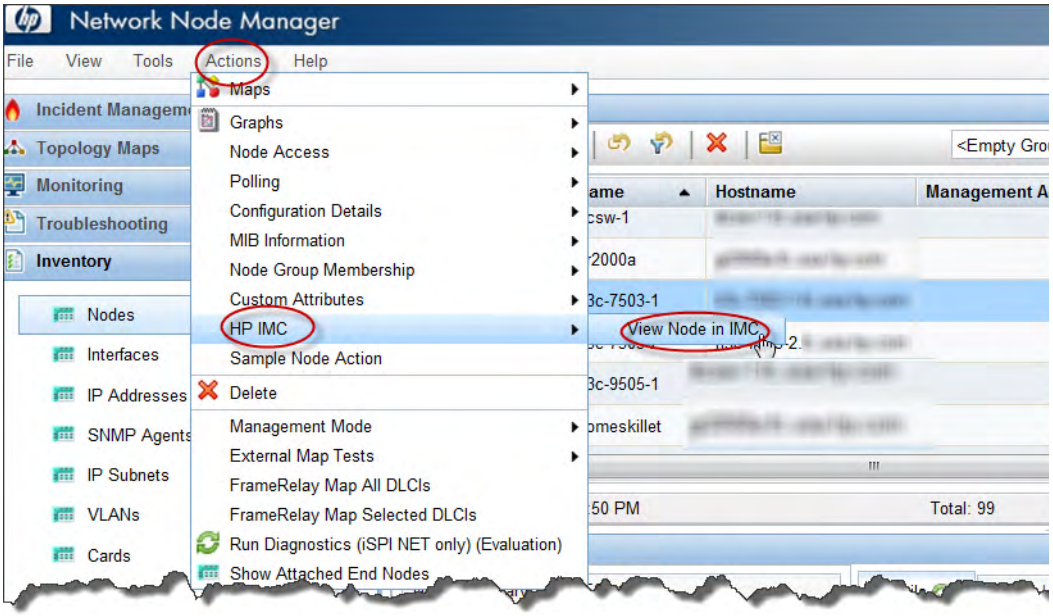
If you select any node in HP NNMi that was seeded from an IMC server, you can use the **HP IMC->View node in IMC** menu from the NNMi console to open the IMC console. From the IMC console, you can log on to view information about the selected node. If you configured SSL access for the HP NNMi - HP IMC Integration, the **HP IMC->View node in IMC** menu in the NNMi console takes you directly to the device view in the corresponding IMC console.

The **HP IMC->View node in IMC** menu item is enabled only if the selected node is *SNMP enabled*.

To open an IMC console view from the NNMi console (of any node that was seeded from an IMC server), complete these steps:

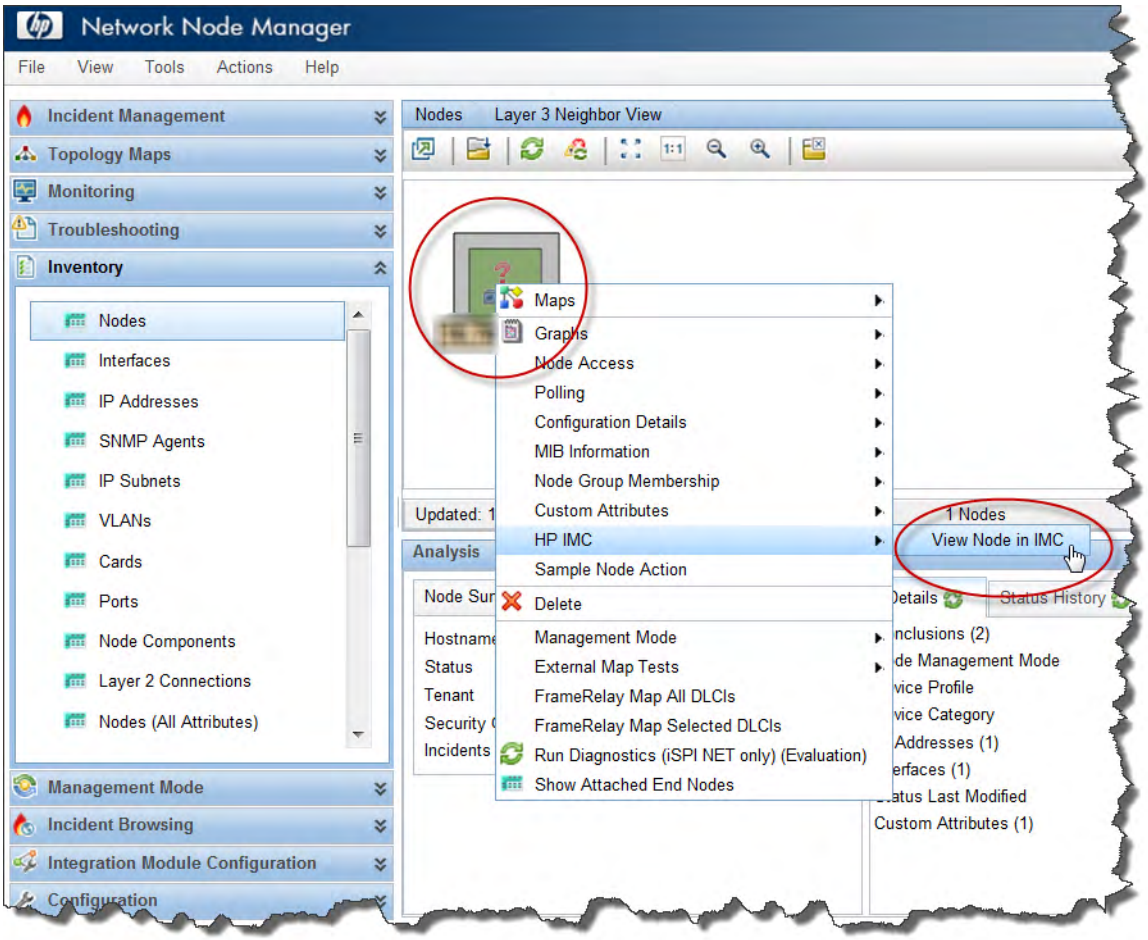
1 Use the **Action** > **HP IMC** > **View Node in IMC** menu to open a view of the node in the IMC console as shown in Figure 2.

Figure 2 Open a View from HP NNMi to HP IMC.



2 You can also use nodes located in Topology Maps in the NNMi console to access the IMC console: for example, select a node from a Layer 3 Neighbor view; then right-click the node and use the **HP IMC** > **View Node in IMC** to open a view of the node in the IMC console as shown in Figure 3.

Figure 3 Open a View from an NNMi to HP IMC



Using the Analysis Pane to View Device Information

When using the HP NNMi - HP IMC integration, the NNMi console includes two additional analysis panels. These panels show device information when a selected node originates from an IMC server. These two panels are labeled **Asset Details** and **Hardware/Firmware**. Select **Asset Details** to view a table of HP IMC-monitored device components as shown in Figure 4 on page 16. Select **Hardware/Firmware** to view additional hardware and firmware details discovered by HP IMC as shown in Figure 5 on page 17.

The menu option is disabled for non-IMC nodes OR for non-SNMP nodes (even if they came from IMC).

Figure 4 Asset Details from HP IMC

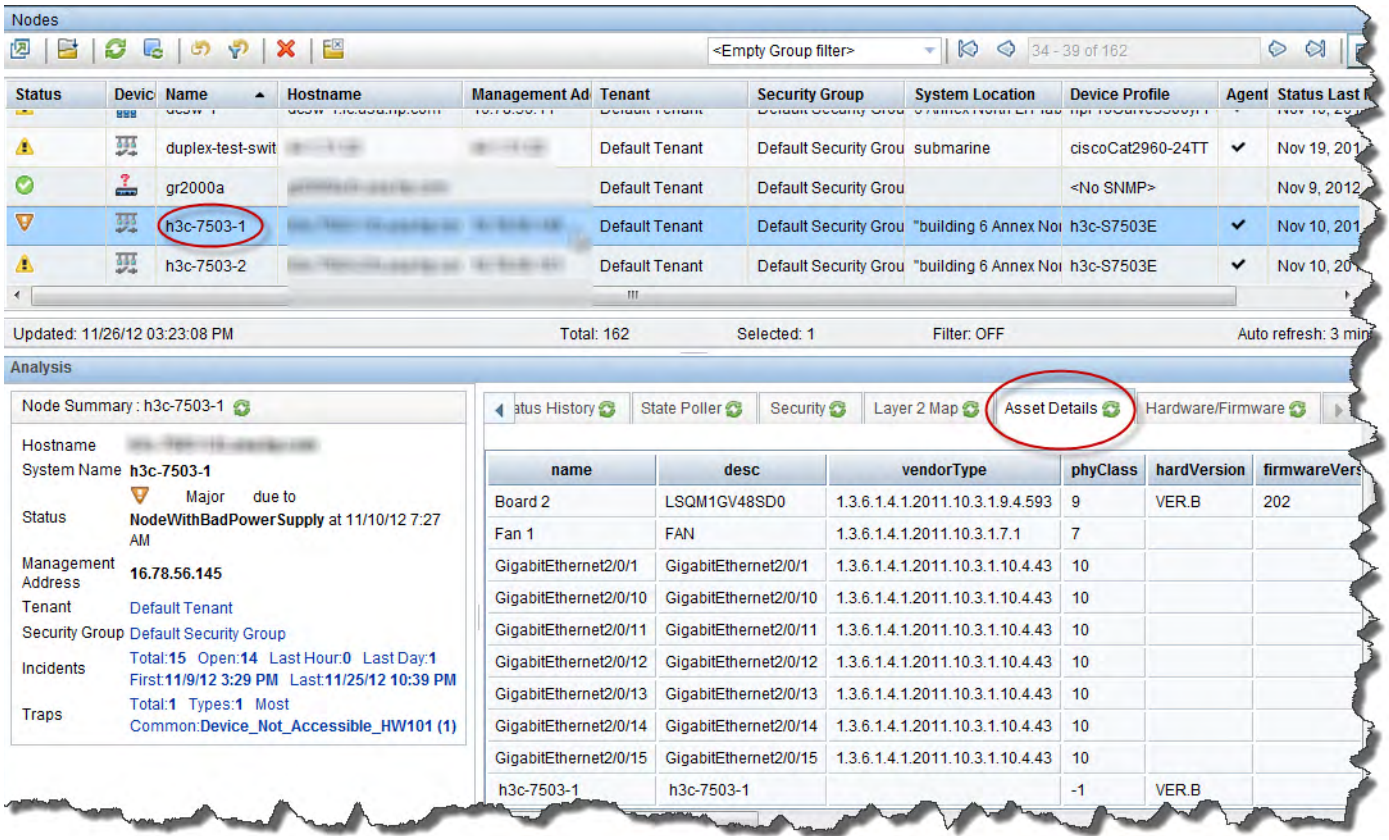
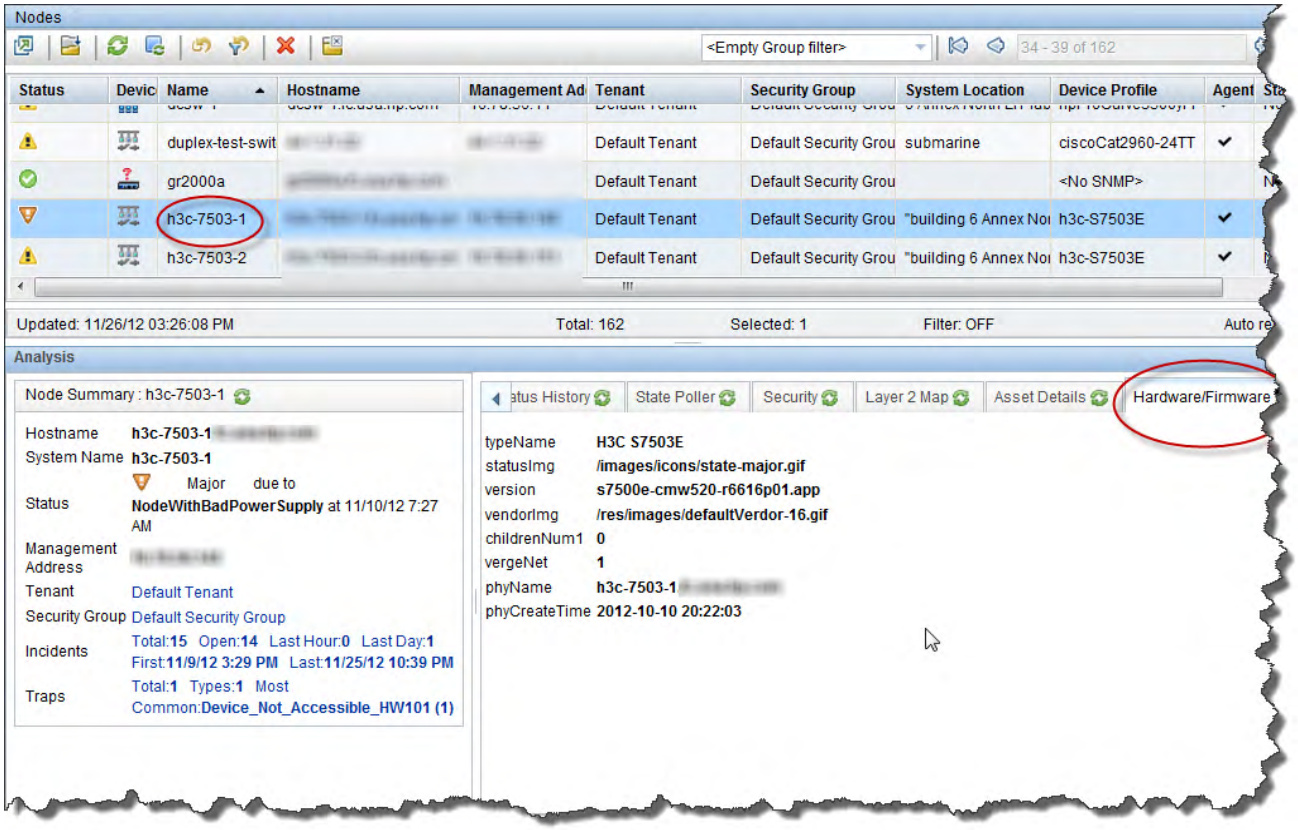


Figure 5 Hardware/Firmware from HP IMC

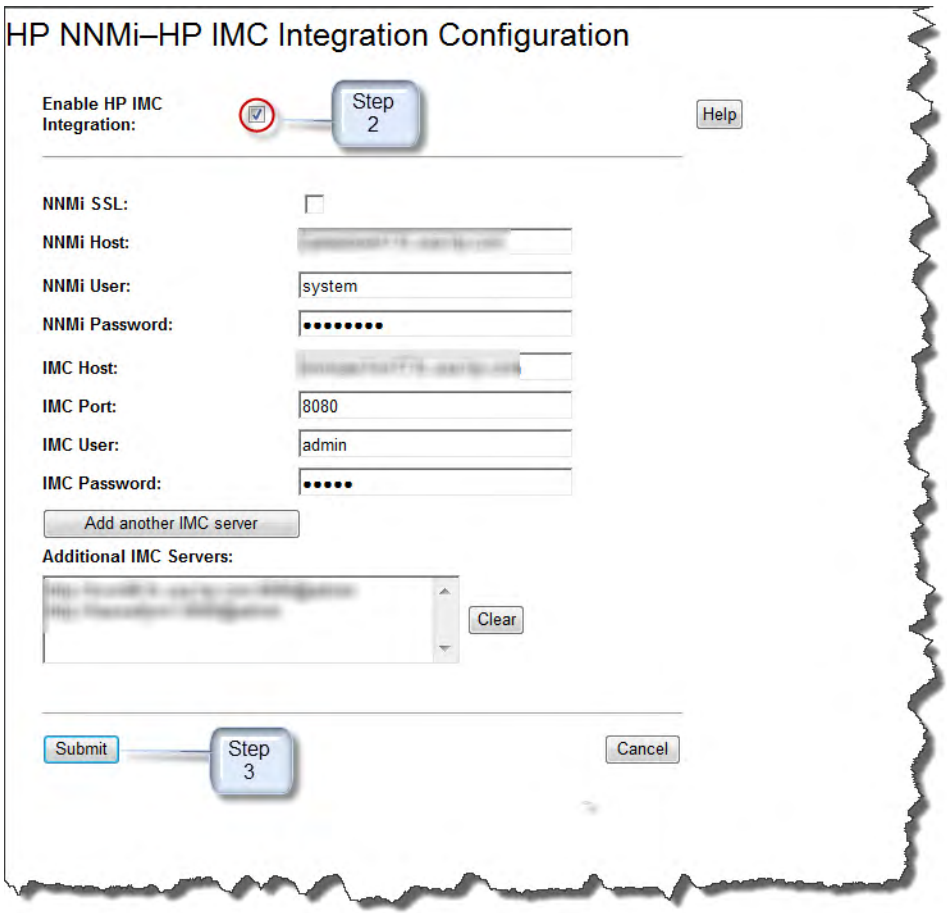


Disabling the HP NNMi - HP IMC Integration

To disable the HP NNMi - HP IMC integration, do the following:

1 From the NNMi console, click **Integration Module Configuration** > **IMC**. HP NNMi shows the **HP NNMi - HP IMC Integration Configuration** screen show in Figure 6. See Figure 6 while configuring the HP NNMi - HP IMC integration.

Figure 6 Disabling the HP NNMi - HP IMC Integration



2 Deselect **Enable IMC Integration**.

3 Click **Submit** to finish disabling the HP NNMi - HP IMC integration.

If you disable the HP NNMi - HP IMC integration, then enable the integration at a later time, the discovery process starts again (re-synchronizes) to ensure that NNMi has the latest device information from the IMC servers.

After you disable the HP NNMi - HP IMC integration, log out of the NNMi console, then log back in, you will no longer see the IMC-related menu items in the NNMi console. There are no other user actions required after completing these steps.

Maintaining the HP NNMi - HP IMC Integration

Loading Trap Definitions: I need to load a large quantity of HP IMC trap definitions and am encountering *Configuration Import Errors*.

Solution: Although HP discourages loading all of the IMC incident definitions discussed in Loading the Trap Definitions on page 6, there might be rare situations that require you to load many of the IMC incident definitions. If you must load a large number of trap definitions, split the **`nnm-imc-incidentConfig.xml`** file into two or more separate files, each containing a subset of the trap definitions, then load each file separately.

Discovery Configuration Change: Make configuration changes so NNMi automatically updates customAttributes for devices found in IMC.

Required Configuration Changes: NNMi will not automatically update customAttributes for devices found in IMC if these devices already reside in the NNMi database. To configure the HP NNMi - HP IMC integration to automatically update customAttributes for devices found in IMC, do the following:

1. Remove the seeds for the devices from NNMi. To do this use the **Configuration** > **Discovery** > **Seeds** menu.
2. Delete the node from NNMi:
   a. Use the **Inventory** > **Nodes** menu.
   b. Select the nodes you want to delete.
   c. Use the **Action** > **Delete** menu to delete the nodes.
3. NNMi now receives information about the deleted devices, including `customAttributes`, from IMC.
4. NNMi rediscovers the device using information forwarded by IMC.

   NNMi might not initiate a discovery for 24 hours, so the nodes might not be seeded in NNMi for some time, unless you disable, then enable the configuration.

If you delete any nodes that NNMi assigned to tenants other than the **Default Tenant**, then NNMi will rediscover those nodes and assign them to the Default Tenant. This Default Tenant assignment could disrupt an NNMi tenant model configuration. See *NNMi Security and Multi-Tenancy* in the *NNMi Deployment Reference*.

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click *here*.

If no email client is available, copy the information below to a new message in a web mail client, and then send this message to **ovdoc-nsm@hp.com**.

Product name and version: NNMi 9.23

Document title: *HP NNMi—HP Intelligent Management Center Integration Guide*

Feedback:


Java™
COMPATIBLE