HP Network Node Manager i Software

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

Software Version: NNMi 9.21

HP Network Node Manager i Software—HP ArcSight Logger Integration Guide

Document Release Date: August 2012
Software Release Date: August 2012

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

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:

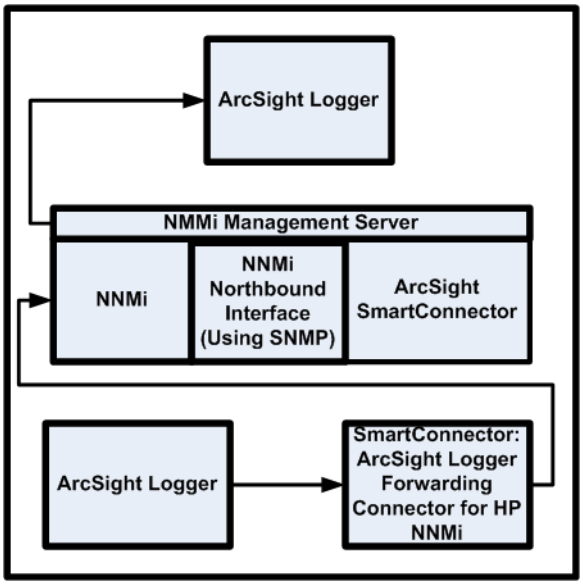
http://h20229.www2.hp.com/passport-registration.html

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.

Contents

HP ArcSight Logger



HP ArcSight Logger is a universal log management solution that unifies searching, reporting, alerting and analysis across any type of enterprise log data – making it unique in its ability to collect, analyze and store massive amounts of data generated by modern networks.

For information about purchasing HP ArcSight Logger, point your browser to http://www.arcsight.com/products.

.This document describes the available integrations:

- HP NNMi–HP ArcSight Logger Integration
- Enabling the HP NNMi-HP ArcSight Logger Integration
- Modifying the HP NNMi - HP ArcSight Logger Integration
- Using the HP NNMi - HP ArcSight Logger Integration
- Disabling the HP NNMi–HP ArcSight Logger Integration

HP NNMi–HP ArcSight Logger Integration

About the HP NNMi–HP ArcSight Logger

By using the instructions included in this chapter to configure HP ArcSight Logger to forward `ArcSightEvents` to HP NNMi, a network operations staff can view Syslog incidents in the NNMi console.

Value

The HP NNMi–HP ArcSight Logger integration adds Syslog information to HP NNMi, so that HP NNMi users can view these Syslog messages and investigate potential problems.

Integrated Products

The information in this chapter applies to the following products:

- HP ArcSight Logger
- SmartConnector: ArcSight HP Network Node Manager i SNMP
- SmartConnector: ArcSight Logger Forwarding Connector for HP NNMi

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

- NNMi 9.21

For the most recent information about supported hardware platforms and operating systems, see the support matrices for both products.

Customizing the HP ArcSight Logger Filters

There are Syslog messages that pass the HP ArcSight Logger filter and forward to HP NNMi. Without configuring the HP ArcSight Logger filter, HP ArcSight Logger forwards large quantities of `ArcSightEvents to` HP NNMi. This can adversely affect HP NNMi performance. *It is very important that you configure this filter promptly to limit the quantity of* `ArcSightEvents` *flowing from HP ArcSight Logger to HP NNMi.* From the NNMi console, you can navigate to the Logger Filters configuration page. From there you can add, then maintain a Logger Filter to adjust the messages HP ArcSight Logger forwards to NNMi.

It is a good practice to supply non-administrator (search only) credentials to open HP ArcSight Logger from HP NNMi. If you enter administrator credentials, HP ArcSight Logger permits HP NNMi users access to HP ArcSight Logger with these administrator privileges, permitting you to make filter configuration changes. If you do not need to make HP ArcSight Logger configuration changes, enter non-administrator credentials.

Documentation

Obtain and read the following manuals to prepare for installing and configuring the HP NNMi - HP ArcSight Logger integration.

- *SmartConnector Configuration Guide for HP Network Node Manager i SNMP* (NNMi Northbound Interface)
  The SmartConnector for HP Network Node Manager i SNMP forwards NNMi incidents and other information to Logger.
- *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi*
  The HP ArcSight Logger Forwarding Connector for HP NNMi forwards Syslog messages in the form of `ArcSightEvents` to NNMi.
- *Logger Administrator's Guide*
  For this integration, HP ArcSight Logger forwards SNMP traps in the form of `ArcSightEvents` to HP NNMi.

In addition to the *Logger Administrator's Guide*, HP ArcSight Logger's integrated online help contains much of the same information as the *Logger Administrator's Guide.*

To obtain copies of HP ArcSight manuals, such as the *SmartConnector Configuration Guides* and the *Logger Administrator's Guide*, point your browser to the following location:
https://protect724.arcsight.com
You must be an HP ArcSight customer (be able to provide user credentials) to access HP ArcSight product documentation.

To view the supported system requirements for HP ArcSight Logger, including the supported operating systems and browsers, point your browser to http://www.arcsight.com/products/products-logger. You can also view the supported system requirements for HP ArcSight Logger in the *Logger Administrator's Guide.*

Enabling the HP NNMi-HP ArcSight Logger Integration

You might have creatively used existing HP NNMi features, such as the HP NNMi northbound interface, to configure a custom integration between HP ArcSight Logger and HP NNMi. If you plan to install NNMi 9.21, you must disable this custom HP NNMi - HP ArcSight Logger integration. After you disable this custom integration, complete the tasks in this section to enable the more robust HP NNMi - HP ArcSight Logger integration delivered in NNMi 9.21.

Prerequisites

Before Enabling the HP NNMi - HP ArcSight Logger integration, do the following:

- Install NNMi 9.21. To assist you with this task, point your browser to http://support.openview.hp.com/selfsolve/manuals and download an interactive version of the *Network Node Manager i Installation Guide*.
- Install the SmartConnector for HP Network Node Manager i SNMP using instructions from the *SmartConnector Configuration Guide for HP Network Node Manager i SNMP* manual.

- Install the HP ArcSight Logger Forwarding Connector for HP NNMi using instructions from the *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi* manual.

Steps to Enable the HP NNMi HP ArcSight Logger Integration

Complete the following tasks to enable the HP NNMi HP ArcSight Logger integration:

Task 1: Install NNMi 9.21

Task 2: Understanding the HP ArcSight MIBs

After you complete Task 1 through Task 5, HP ArcSight Logger begins forwarding filtered `ArcSightEvents` to HP NNMi. HP NNMi resolves interfaces and nodes to the source objects included in these `ArcSightEvents`. During the NNMi 9.21 installation, the **`hp-arcsight.mib`** MIB is installed and loaded on the NNMi management server. Use HP NNMi's **Node Action** > **MIB Information** feature to better understand the OIDs that are present in the `ArcSightEvent`.

Task 3: Configuring the HP ArcSight Logger Forwarding Connector for HP NNMi

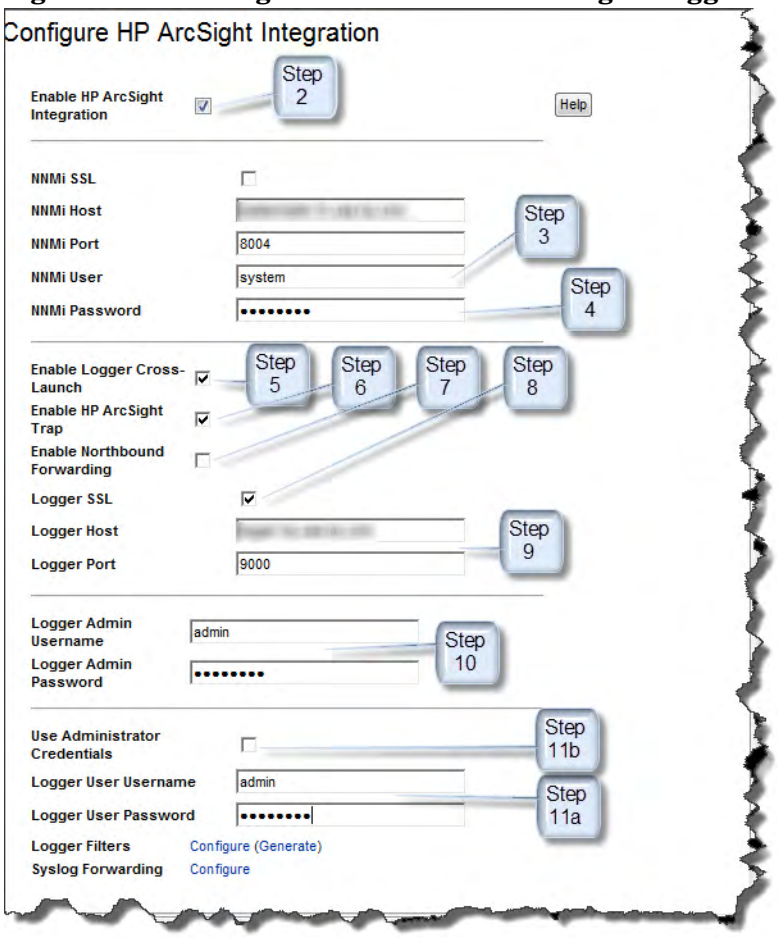
Configure the HP ArcSight Logger Forwarding Connector for HP NNMi using instructions from the *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi* manual.

Task 4: Configuring the HP NNMi–HP ArcSight Logger Integration

By enabling the HP NNMi - HP ArcSight Logger integration and the `ArcSightEvent`, along with configuring HP ArcSight Logger to forward SNMP traps in the form of `ArcSightEvents`, HP NNMi can evaluate each `ArcSightEvent` content and show it as an SNMP trap or a Syslog message. To enable the HP NNMi - HP ArcSight Logger integration complete the following steps:

1 From the NNMi console, click **Integration Module Configuration** > **HP ArcSight**. HP NNMi shows the **Configure ArcSight Integration** screen show in Figure 1. Refer to Figure 1 while configuring the HP NNMi - HP ArcSight Logger integration.

Figure 1 Enabling the HP NNMi-HP ArcSight Logger Integration



2 Select **Enable ArcSight Integration**.

3 Add or observe the following HP NNMi integration information:

- `NNMi host`: This field contains the fully qualified domain name of the NNMi management server.
- `NNMi port`: This field contains the HTTP port number used for accessing NNMi. For more information see the *NNMi Deployment Reference*.
- `NNMi User`: Enter an NNMi username that is mapped to an NNMi administrator user group.

4 `NNMi Password`: Enter the username password.

5 Select **Enable Logger Cross-Launch**.

6 Select **Enable ArcSight Trap**.

You can also do the following to enable the ArcSight Trap:

a From the NNMi console, click **Configuration** > **Incidents** > **SNMP Trap Configurations**.

b Click **ArcSightEvent** > **Open**.

c Select **Enabled**.

d Click **Save and Close**.

7 If you want to forward HP NNMi incidents to HP ArcSight Logger, select **Enable Northbound Forwarding**.

8 Not all HP ArcSight Logger applications are configured to use SSL. If the HP ArcSight Logger application included in this HP NNMi - HP ArcSight Logger integration is configured to use SSL, select **Logger SSL**.

See the *HP ArcSight Logger v5.1 Administrators Guide* about configuring Logger for SSL.

9 Add the following HP ArcSight Logger integration information:

- `Logger Host` (the fully qualified domain name of the Logger Host)
- `Logger Port`

10 Add the following HP ArcSight Logger administrator credentials:

- `Logger Admin Username`
- `Logger Admin Password`

11 Complete step a. You can complete step b, however step a is the recommended method.

a Add the following user credentials for read-only cross-launches. Configure these credentials only if you want to use a read-only user within HP ArcSight Logger:

- `Logger User Username`
- `Logger User Password`

b Select **Use Administrator Credentials**. This applies the administrator credentials to the Logger User Username and Logger User Password fields. Although this might be useful in some applications, selecting this option does give the HP NNMi level 1 operator full administrator privileges in HP ArcSight Logger. For security purposes, step a is the recommended method.

12 Click **Submit** to save these changes.

13 For the cross-launch menu changes to become visible in the NNMi console, do the following:

a Sign out of HP NNMi.

b Sign in to HP NNMi.

After you complete Task 4, HP ArcSight Logger forwards unfiltered `ArcSightEvents to` HP NNMi. HP NNMi evaluates the `ArcSightEvent` content and shows it as an SNMP trap or a Syslog message.

Next, *promptly* complete Task 5 to identify and configure only those Syslog messages that you want HP ArcSight Logger to forward to HP NNMi.

Task 5: Configuring the HP ArcSight Logger Filter

In Task 5 you configure the HP ArcSight Logger filter to specify the Syslog messages to forward to HP NNMi.

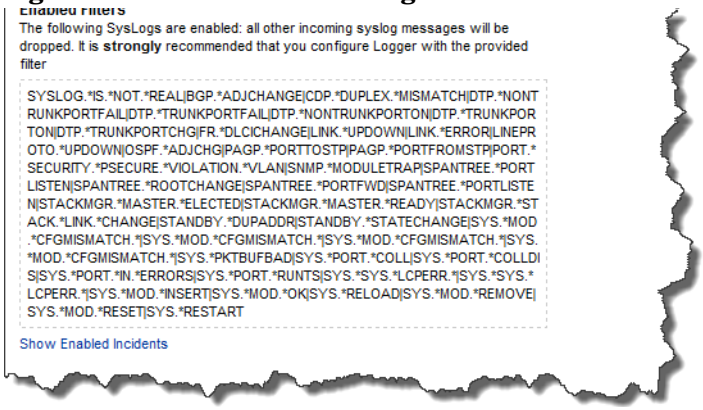
To avoid receiving an unmanageable number of traps, be sure to complete Task 5 immediately after you complete Task 4.

Complete step 1 through step 6 any time you click **Configuration** > **Syslog Message Configurations** and make modifications, such as enabling or disabling Syslog messages.

To access HP ArcSight Logger's configuration and add new filter content, do the following

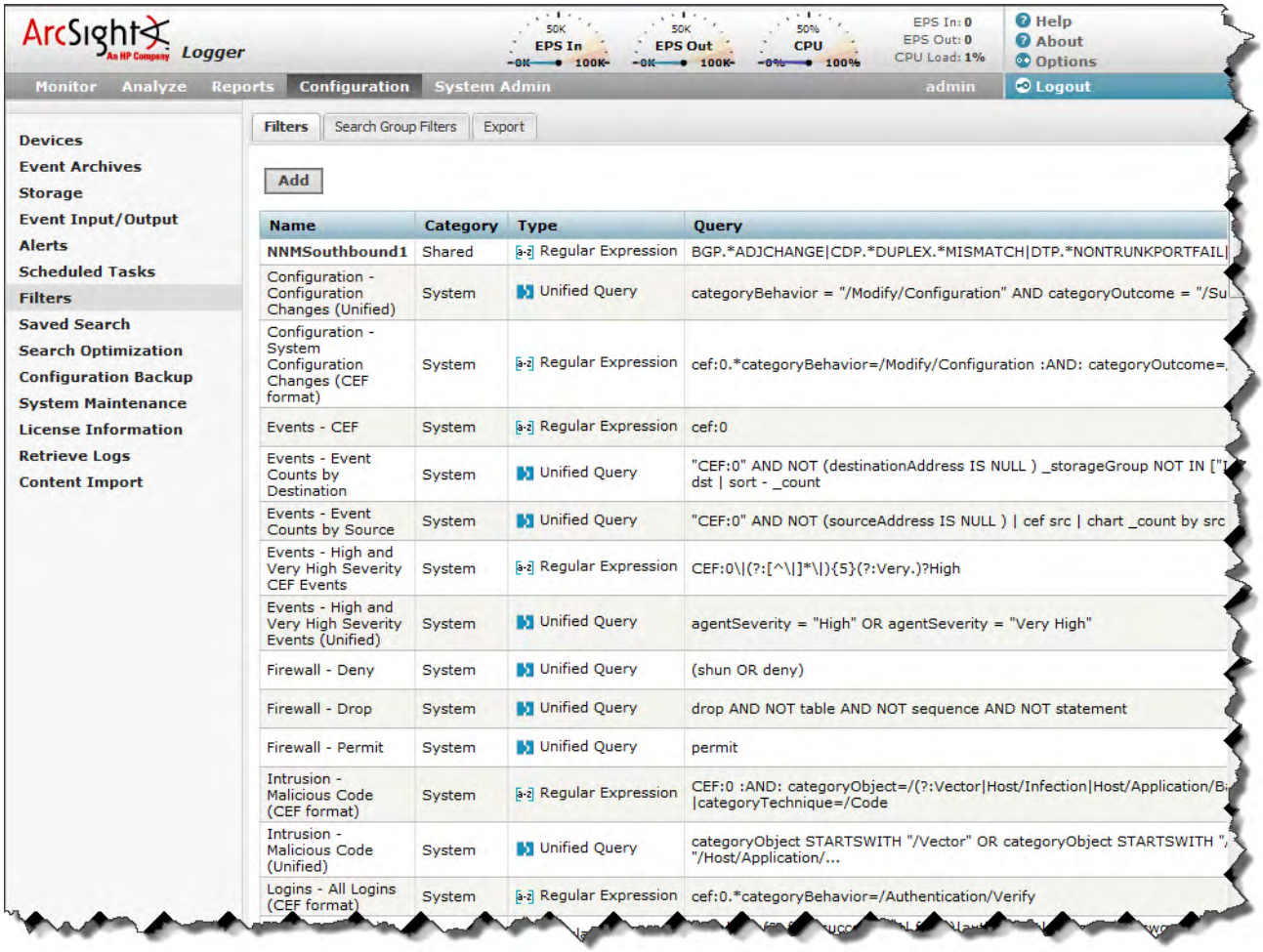
1. From the NNMi console, click **Integration Module Configuration** > **HP ArcSight**.
2. Click **Logger Filters->(Generate)**. HP NNMi translates the `Enabled` Syslog messages shown in **Configuration** > **Syslog Message Configurations** into a format that you can use in a HP ArcSight Logger filter, then shows these translations on the `Enabled Filters` page.

Figure 2 Enabled Filters Page



3. Select the filter contents located on the `Enabled Filters` page. You will copy and paste this content into a filter within HP ArcSight Logger in a later step. Close the window.
4. Click **Logger Filters->Configure**. This launches a view into the HP ArcSight Logger **Configuration** page shown in Figure 3 on page 14.

Figure 3 The HP ArcSight Logger Configuration Page



5 Click **Filters**, then wait for the list of filters to load.

6 Complete one of the following actions to configure a filter that determines the Syslog messages to forward to HP NNMi.

If this is the first time you are creating a filter to determine the Syslog messages to forward to HP NNMi, do the following:

a Click **Add**.

b After HP ArcSight Logger shows the Add Filter form, add a name for the filter, select the **Regex Query** filter type, then select **Next**.

c Copy the contents from step 3 into the `Query` field.

d Save your work.

If you are modifying an existing filter that determines the Syslog messages to forward to HP NNMi, do the following:

a Edit the existing filter that HP ArcSight Logger uses to determine the Syslog messages to forward to HP NNMi.

b Clear out the existing filter contents.

c Copy the contents from step 3 into the `Query` field.

d Save your work.

HP ArcSight Logger now forwards only those Syslog messages you want forwarded to HP NNMi.

Task 6: Configuring the SmartConnector for HP Network Node Manager i SNMP (Connector for Northbound Interface, Optional Task)

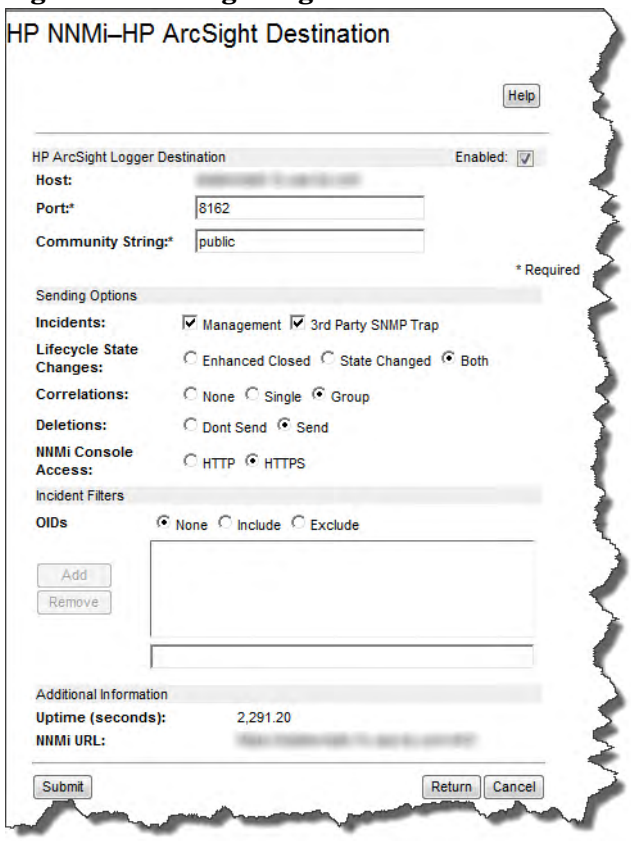
Configure the SmartConnector for HP Network Node Manager i SNMP using instructions from the *SmartConnector Configuration Guide for HP Network Node Manager i SNMP* manual.

Task 7: Configuring HP NNMi to Forward SNMPv1, v2, and v3 Trap Incidents to HP ArcSight Logger (Northbound Interface, Optional Task)

1 From the NNMi console, click **Integration Module Configuration** > **HP ArcSight**.

2 Click **Syslog Forwarding** > **Configure** this launches a view to the **NNMi - Logger Destination** page. Refer to Figure 4 while completing the steps for this task.

Figure 4 Configuring the HP NNMi - HP ArcSight Logger Destination



3 Select **ArcSight Logger Destination** > **Enabled**.

4 Add `8162` as the value of the port field. HP NNMi forwards to a connector that is installed on theNNMi management server. The port is automatically set to the default for the connector.

5 Enter the `Community String` for the `Logger` host.
If you do not specify a community string, the integration module attempts to use the empty community string.

6 Make sections for the `Sending Options`. Without changes to those values, HP NNMi forwards everything.

7 Click **Submit**.

8 HP NNMi tests for any configuration errors. Fix any errors, then repeat step 7 until the submit is successful.

HP NNMi now forwards SNMPv1, v2, and v3 trap incidents to HP ArcSight Logger.

Modifying the HP NNMi - HP ArcSight Logger Integration

This section discusses how to modify and improve the HP NNMi- HP ArcSight Logger integration after enabling it.

Managing the Number of Incoming Syslog Messages

The HP NNMi–HP ArcSight Logger Integration supports Syslog messages from all vendors supported by HP ArcSight Logger.

You might find that HP NNMi does not have a Syslog Message Incident configuration for a supported vendor. Use the following steps as a guideline for creating Syslog configurations for an undefined Syslog message:

1 Obtain the list of undefined Syslog Messages to define:

- If the HP NNMi installation has a low trap arrival rate, run the nnmtrapdump.ovpl script to show all of the traps stored in HP NNMi for a specified time frame. The following example shows all of the traps by HP NNMi in the last 10 minutes:

  `nnmtrapdump.ovpl -last 10`

  Adjust your use of the ***`nnmtrapdump.ovpl`*** script options to meet your needs. For more information about the available options, see the *nnmtrapdump.ovpl* reference page, or the UNIX manpage.

- If the HP NNMi installation has a high trap arrival rate, import the following file into an Excel spreadsheet:

  Windows: `%NNM_DATA%\log\nnm\trap.csv.<compression>`
  UNIX: `$NNM_DATA/log/nnm/trap.csv.<compression>`

  See the *NNMi Deployment Reference* for more information about the `trap.csv.<compression>` file.

If you do not see the specific Syslog message to define, you might need to reconfigure the Syslog messages to forward to HP NNMi. See Configuring the HP ArcSight Logger Filter on page 13.

If you configure the HP ArcSight Logger filter and still do not see the specific Syslog message to define, submit a support call for HP ArcSight Support at http://www.hp.com/go/hpsoftwaresupport.

2 Using the list you obtained from step 1, find the first Syslog message in the list to define in HP NNMi.
For example, suppose you are looking for a message for a *Cisco* device that contains some specific text, such as LINK-3-UPDOWN on interface FastEthernet0/3.

3 Search the list for the specific message name.

For example, after searching the list of Syslog messages, you find the following Cisco Syslog message:

```
.1.3.6.1.4.1.11937.1.16       Apr 6 01:08:30 10.10.10.10 49349: 16w3d:
%LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to up
```

In this example, `LINK-3-UPDOWN` is the message name.

Each message name is vendor-specific. Cisco messages often place the message name immediately after the percent (%) sign.

4 Next, find the OID that is associated with the message name. Look for the value associated with OID .1.3.6.1.4.1.11937.1.42.1.3.1.

In this example, look for a log entry containing the `LINK-3-UPDOWN` name. You find an entry that resembles the following:

```
state=HAS_VALUE type=OCTET STRING oid=.1.3.6.1.4.1.11937.1.42.1.1.1
value=mnemonic
```

```
state=HAS_VALUE type=OCTET STRING oid=.1.3.6.1.4.1.11937.1.42.1.3.1
value=LINK-3-UPDOWN
```

Note the OID value text string. This is the value that HP NNMi uses to look up the respective syslog message incident configuration. HP NNMi replaces any character not permitted in the name field with _ (underscore). In this example, use the text string value assigned to OID .1.3.6.1.4.1.11937.1.42.1.3.1 as the name of the syslog message when you define it instep 7. In this example, the value is set to `LINK-3-UPDOWN`.

5 From the NNMi console, click **Syslog Message Configurations** in the **Configuration** workspace.

6 Click **New** to open a form. You will use this form to create a new Syslog configuration for the undefined syslog message.

7 Add the OID text string value obtained in step 4 as the name of the undefined Syslog message you plan to define.

In this example the value of OID `.1.3.6.1.4.1.11937.1.42.1.3.1` is `LINK-3-UPDOWN`.

Alpha-numeric, spaces, and the following special characters are permitted: _ (underscore), : (colon), - (dash), and / (slash).

If the mnemonic value includes non-supported characters, replace each character with an underscore character (_) or space.

8 Configure the remaining fields for this new Syslog configuration.

9 Click the **Save and Close** icon.

10 Using the list you obtained from step 1, repeat step 1 through step 9 for the remaining Syslog messages to define in NNMi.

To keep HP NNMi performing at a high level, HP NNMi drops incoming SNMP traps (including Syslog messages) after storing a specific number of SNMP traps in its database.

You can use the auto-trim oldest SNMP trap incidents feature to adjust this number. See the *NNMi Deployment Reference* for more information.

Using the HP NNMi - HP ArcSight Logger Integration

The information in this section discusses how to use the HP NNMi - HP ArcSight Logger integration after enabling it and modifying it to meet your needs.

Opening HP ArcSight Logger from the NNMi Console

When launching from the NNMi console to HP ArcSight Logger, the browser might prompt you to trust the HP ArcSight Logger before initiating the cross-launch.

Often when an application attempts to redirect to an untrusted site, it prompts you to trust the site before completing the redirect.

Viewing ArcSightEvent SNMP Traps and ArcSightEvent SNMP Trap Configurations

To view `ArcSightEvent` SNMP traps, click **SNMP Traps** in the **Incident Browsing** workspace. To view `ArcSightEvent` Syslog messages, click **Syslog Messages** in the **Incident Browsing** workspace.

After enabling the HP NNMi - HP ArcSight Logger integration, the `ArcSightEvents` that HP ArcSight Logger forwards to HP NNMi are structured the same as SNMP traps. To view the ArcSightEvent SNMP trap configuration, do the following:

1 From the NNMi console, navigate to **Configuration** > **Incidents** > **SNMP Trap Configurations.**

2 Open the **ArcSightEvent** trap definition.

To view the `ArcSightEvents` that HP ArcSight Logger forwards to NNMi 9.20, and that are actual Syslog messages, do the following:

1 From the NNMi console, navigate to **Configuration** > **Incidents** > **Syslog Message Configurations.**

2 HP NNMi shows the current list of `Syslog Message Configurations`.

Changes to the NNMi Console's Actions Menu

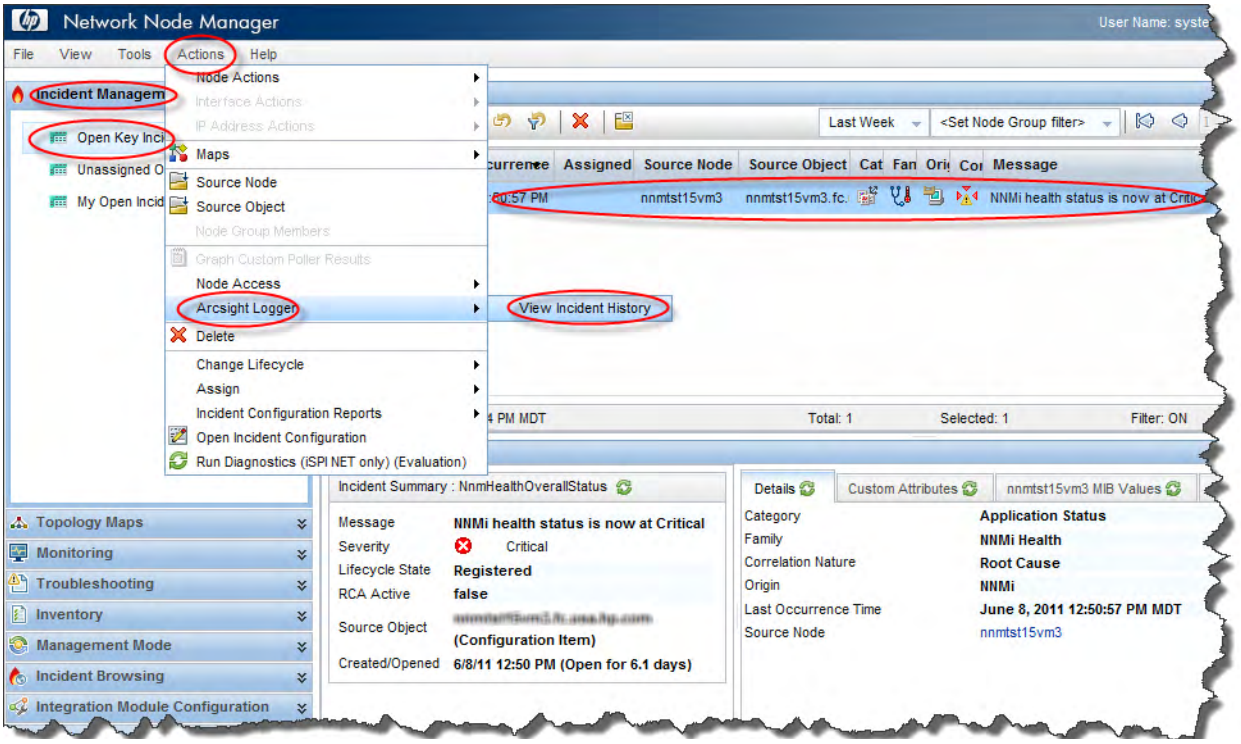
After enabling the HP NNMi - HP ArcSight Logger integration, the NNMi console provides the following new functionality in the NNMi management server.

Incident Management Workspace

In the **Incident Management** workspace, click **Open Key Incidents**.

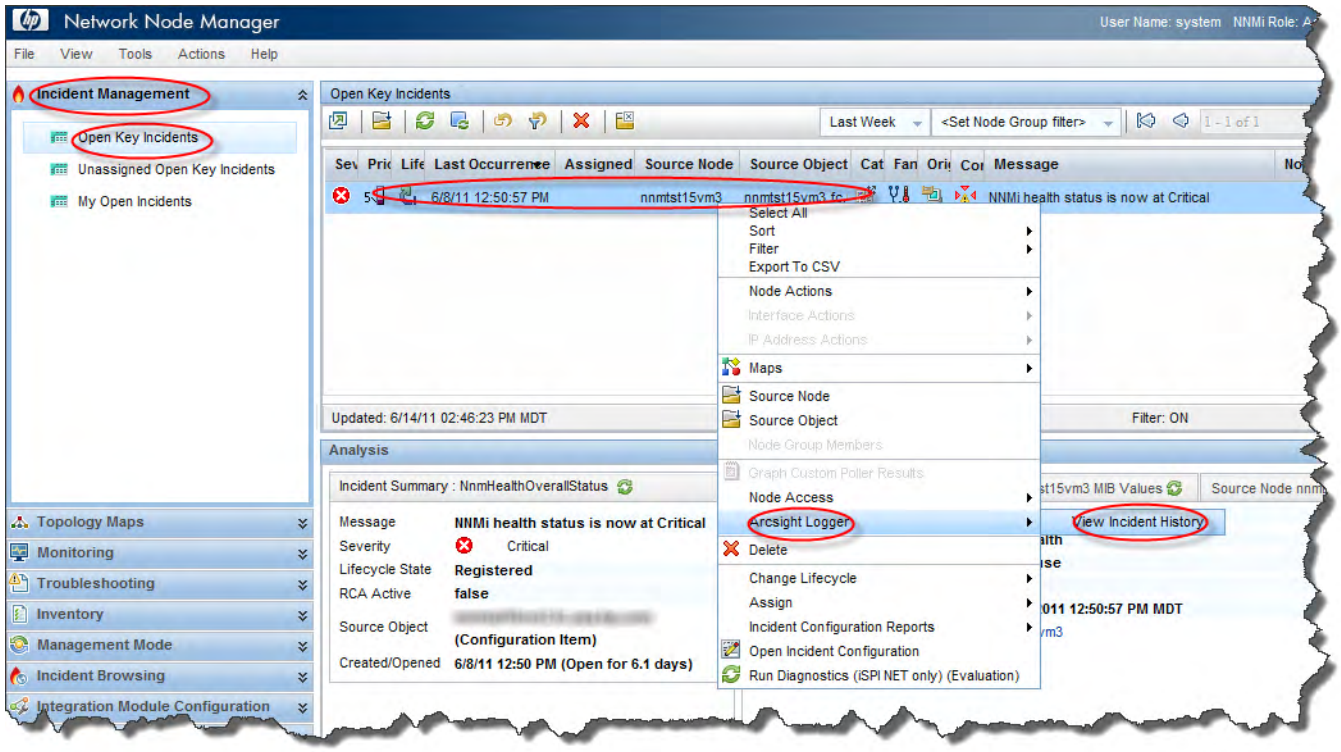
Use the NNMi console to open the HP ArcSight Logger application from an incident. To do this, select an incident while using the **Incident Management** workspace; then use the NNMi console **Actions** menu to open the HP ArcSight Logger application as shown in Figure 5.

Figure 5 Opening HP ArcSight Logger from an HP NNMi Incident in the Incident Management Workspace



You can also right-click an incident; then use the menu to open the HP ArcSight Logger application as shown in Figure 6.

Figure 6 Opening HP ArcSight Logger by Right-Clicking on an Incident in the Incident Management Workspace

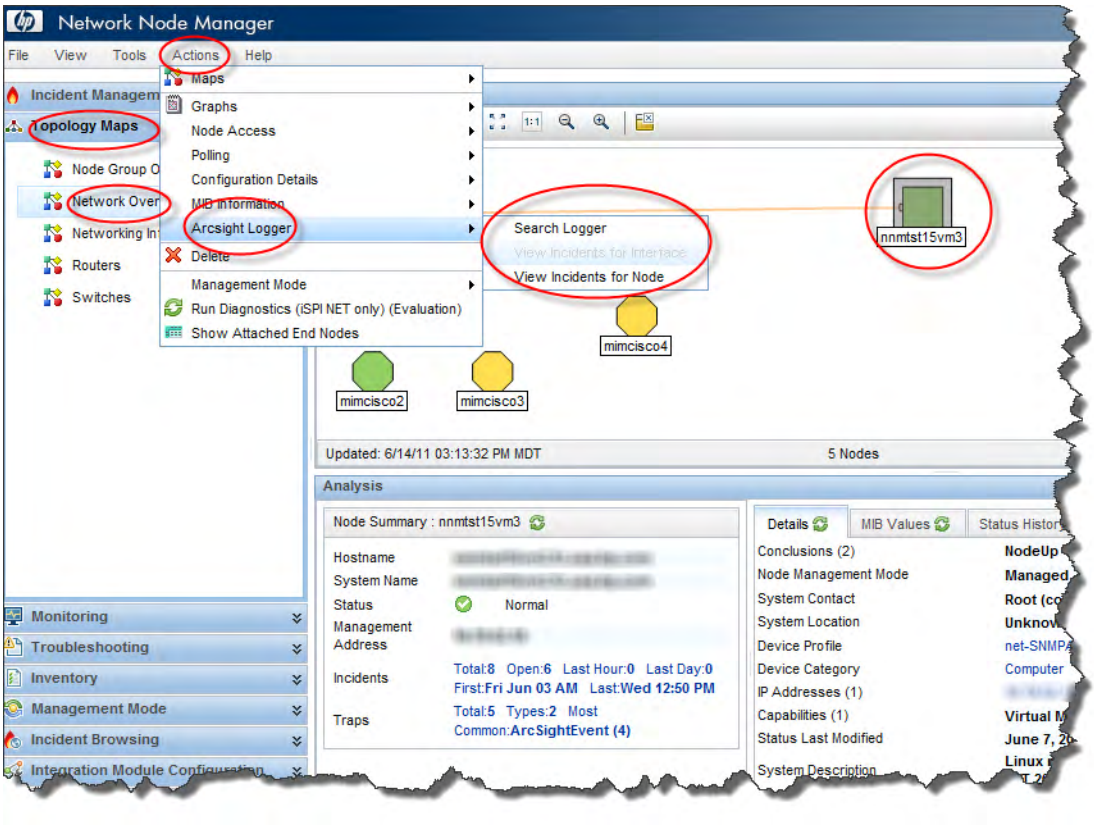


Topology Maps Workspace

In the **Topology Maps** workspace, click **Network Overview**.

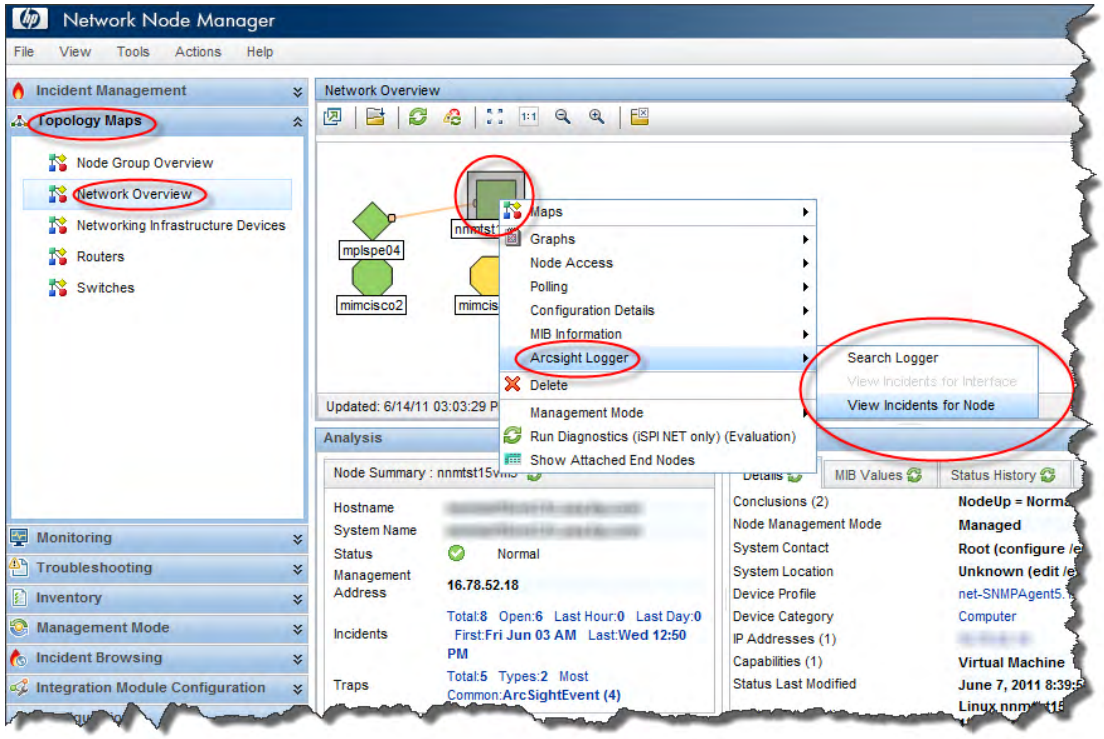
Use the NNMi console to open the HP ArcSight Logger application from a node. To do this, select a node while using the **Topology Maps** workspace; then use the NNMi console **Actions** menu to open the HP ArcSight Logger application as shown in Figure 7.

Figure 7 Opening HP ArcSight Logger from a Node in the Topology Maps Workspace



You can also right-click a node; then use the menu to open the HP ArcSight Logger application as shown in Figure 8.

Figure 8 Opening HP ArcSight Logger by Right-Clicking on a Node in the Topology Maps Workspace

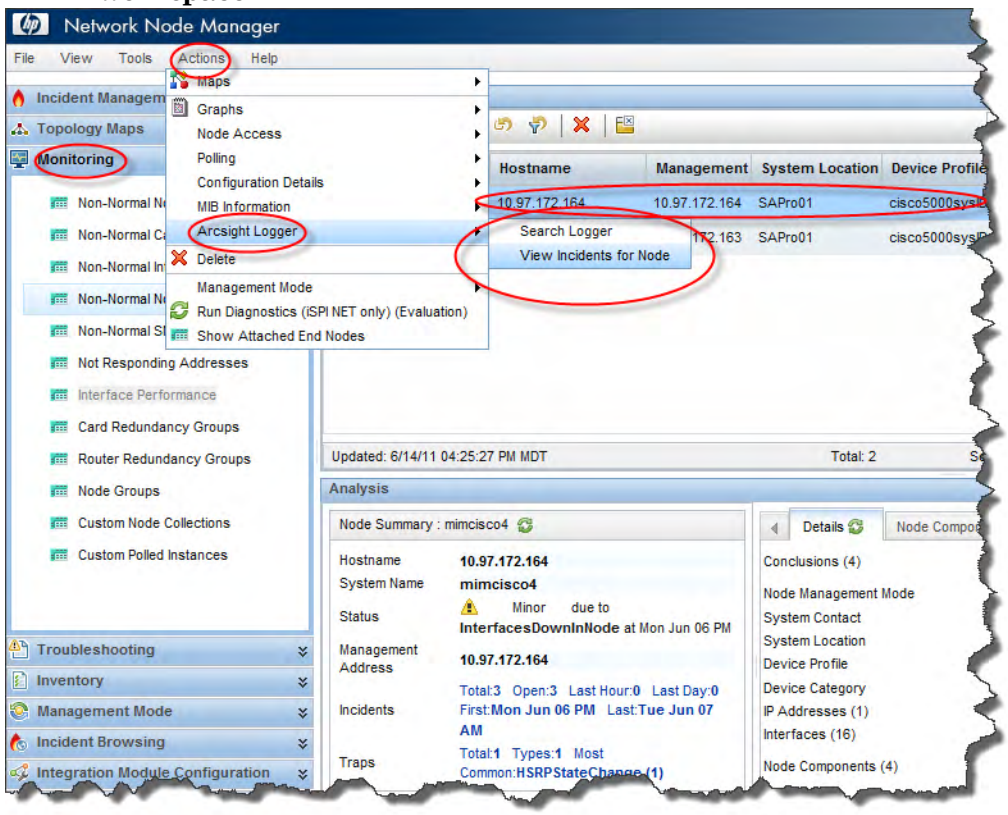


Monitoring Workspace

In the **Monitoring** workspace, click **Non-Normal Nodes**.

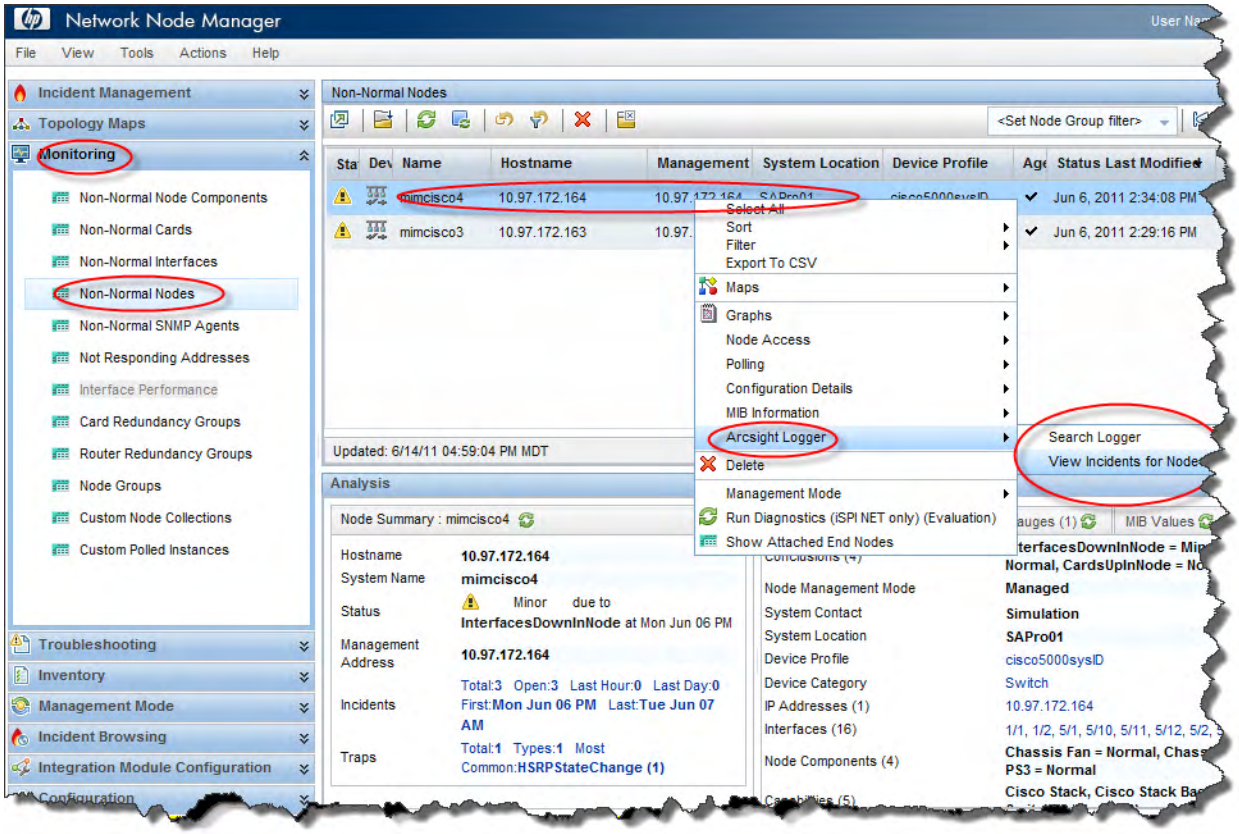
Use the NNMi console to open the HP ArcSight Logger application from a node or interface. To do this, select a node or interface while using the **Monitoring** workspace; then use the NNMi console **Actions** menu to open the HP ArcSight Logger application as shown in Figure 9.

Figure 9 Opening HP ArcSight Logger from a Node in the Monitoring Workspace



You can also right-click a node in the **Monitoring** workspace; then use the menu to open the HP ArcSight Logger application as shown in Figure 10.

Figure 10 Opening HP ArcSight Logger by Right-Clicking on a Node in the Monitoring Workspace

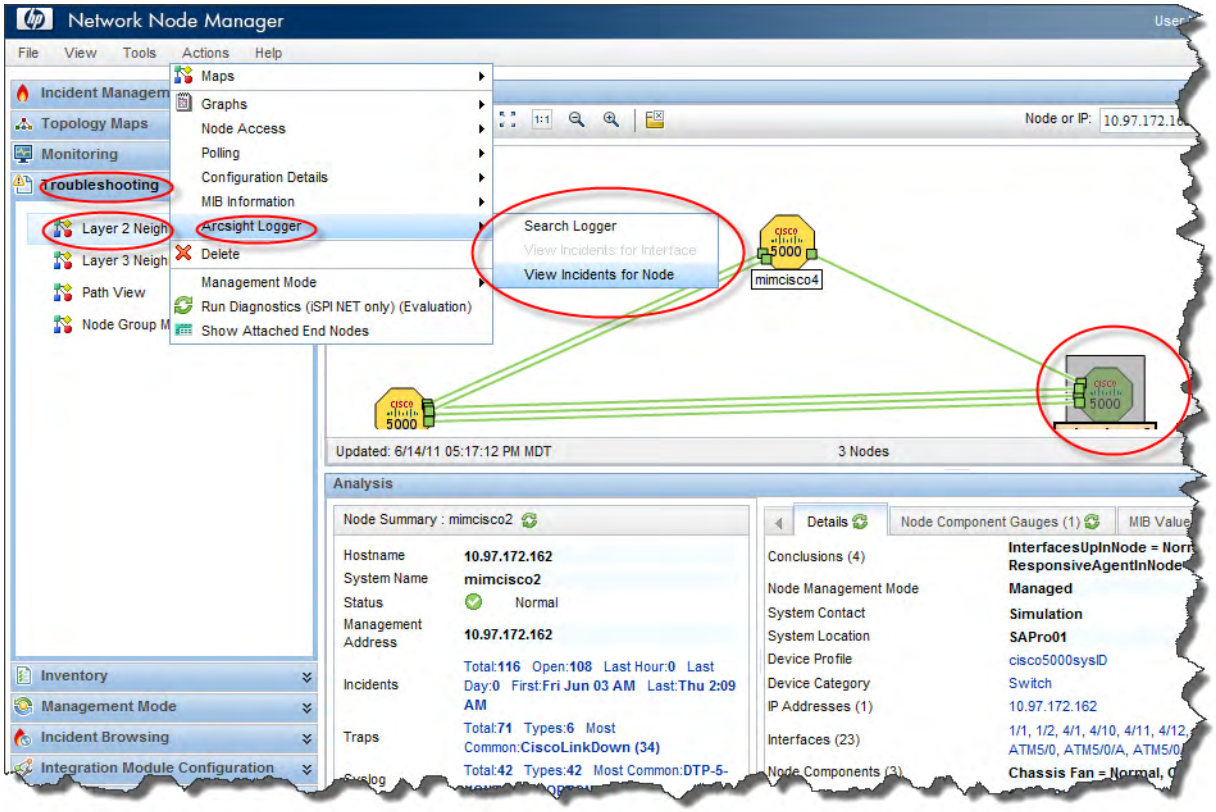


Troubleshooting Workspace

In the **Troubleshooting** workspace, open a **Layer 2 Neighbor View.**

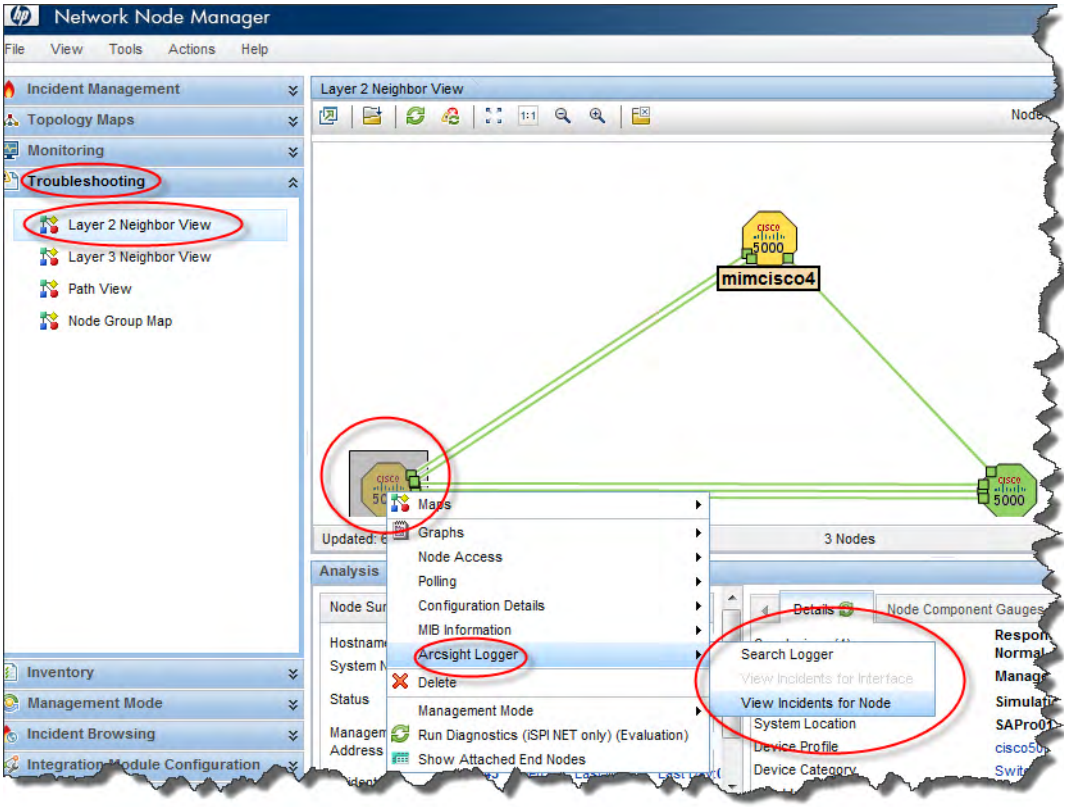
Use the NNMi console to open the HP ArcSight Logger application from a node. To do this, select a node while using the **Troubleshooting** workspace; then use the NNMi console **Actions** menu to open the HP ArcSight Logger application as shown inFigure 11.

Figure 11 Opening HP ArcSight Logger from a Node in the Troubleshooting Workspace



You can also right-click a node in the **Troubleshooting** workspace; then use the menu to open the HP ArcSight Logger application from a node as shown in Figure 12.

Figure 12 Opening HP ArcSight Logger by Right-Clicking on a Node in the Troubleshooting Workspace

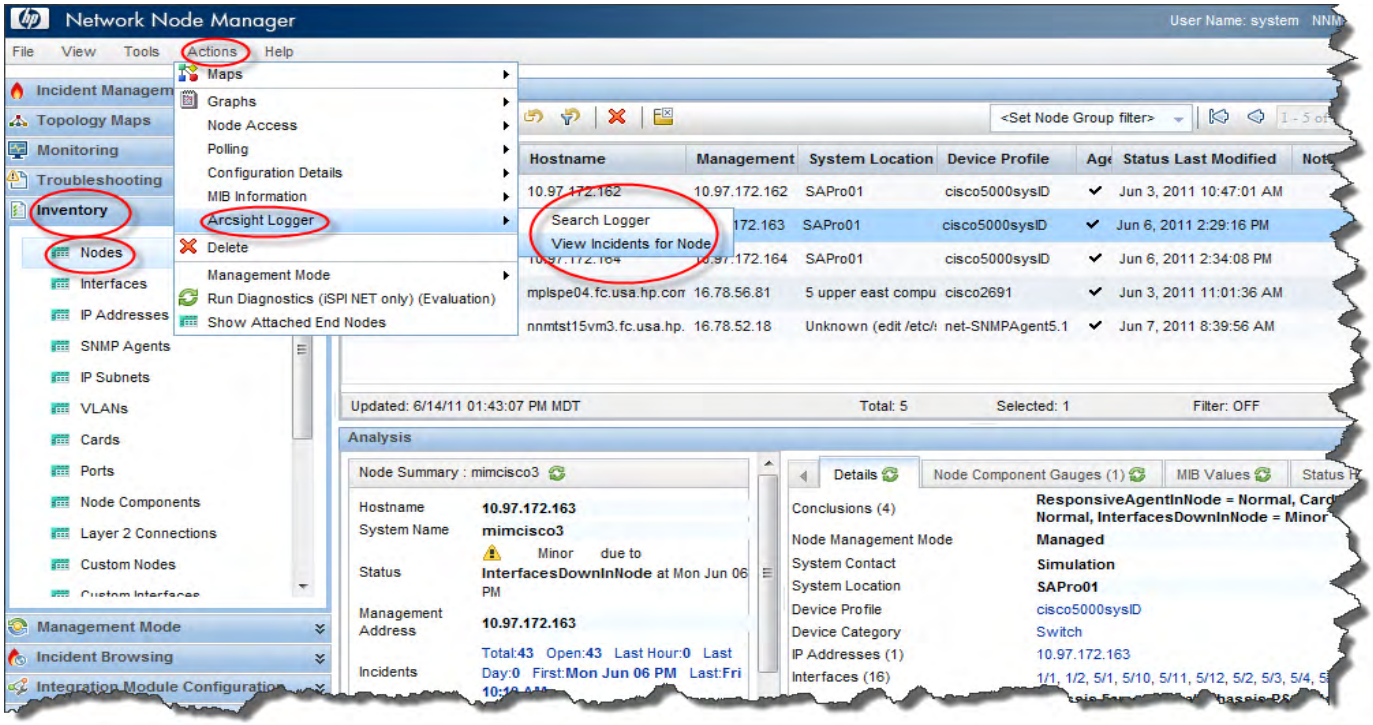


Inventory Workspace

In the **Inventory** workspace, click **Nodes**.

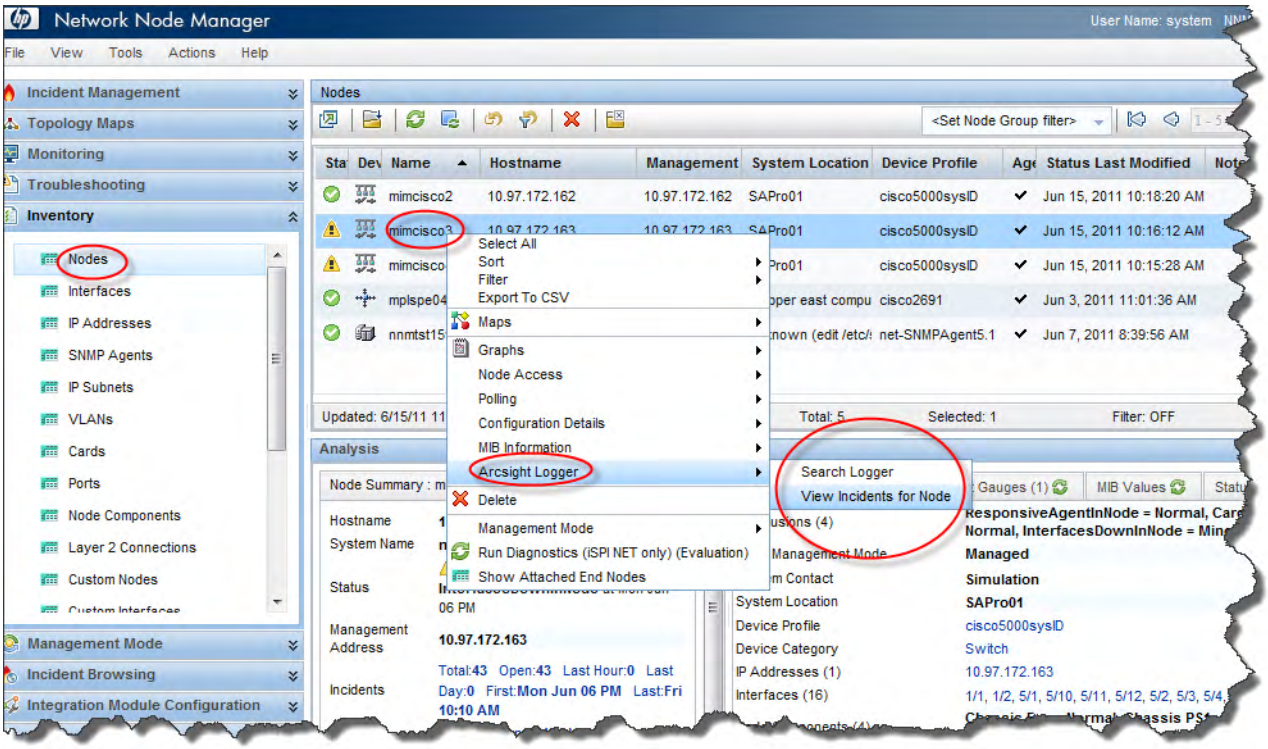
Use the NNMi console to open the HP ArcSight Logger application from a node or interface. To do this, select a node or interface while using the **Inventory** workspace; then use the NNMi console menus to open the HP ArcSight Logger application as shown in Figure 13**.**

Figure 13 Opening HP ArcSight Logger from a Node or Interface in the Inventory Workspace



You can also right-click a node in the **Inventory** workspace; then use the menu to open the HP ArcSight Logger application from a node as shown in Figure 14.

Figure 14 Opening HP ArcSight Logger by Right-Clicking on a Node or Interface in the Inventory Workspace

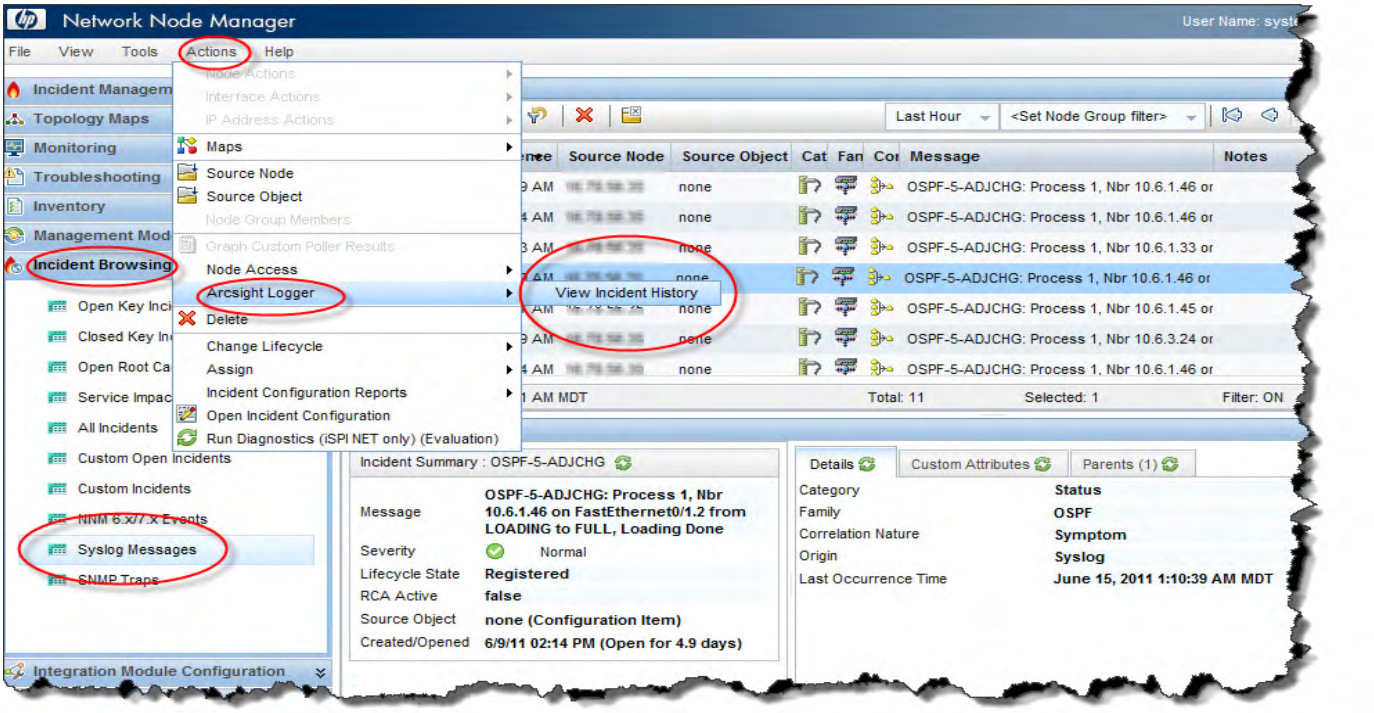


Incident Browsing Workspace

In the **Incident Browsing** workspace, click **Syslog Messages** to view the `ArcSightEvents` HP ArcSight Logger forwarded to `HP NNMi`.

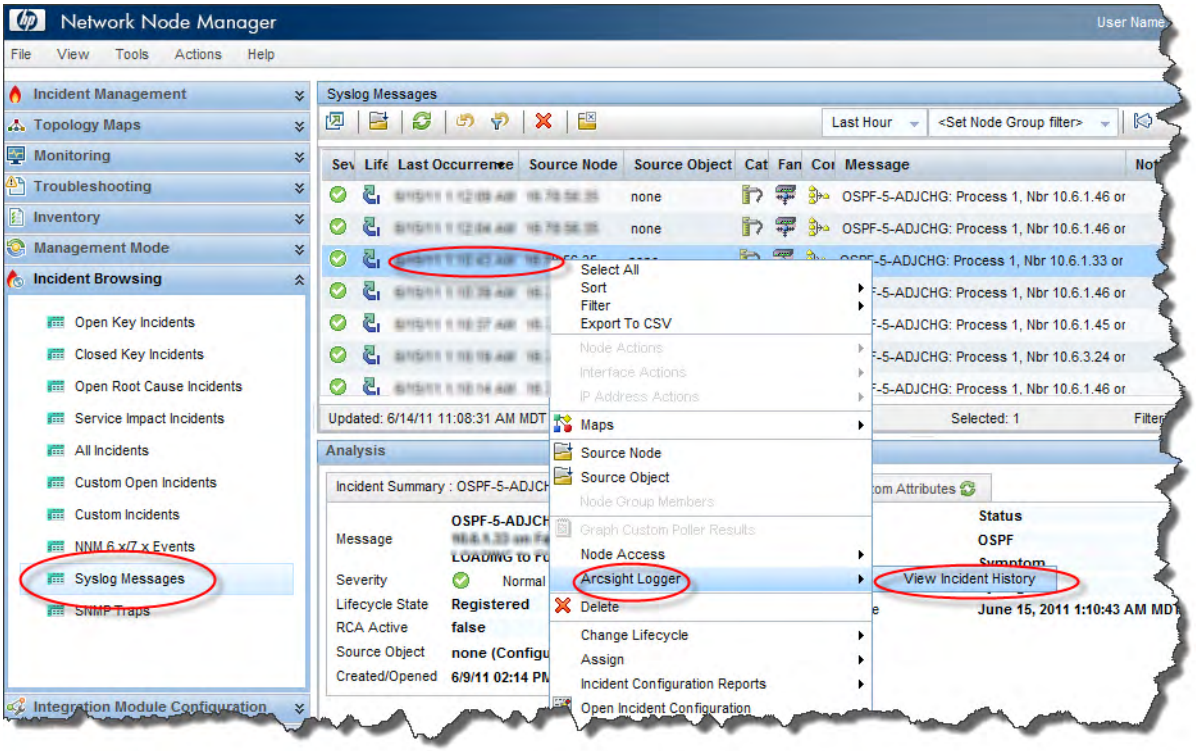
You can use the NNMi console to open the HP ArcSight Logger application from an HP NNMi incident. To do this, select an incident while using the **Incident Browsing** workspace and use the NNMi console menus to view the incident history as shown in Figure 15.

Figure 15 View Incident History Using Actions Menu



You can also right-click an incident and use the **ArcSight Logger** > **View Incident History** to open the HP ArcSight Logger application from an HP NNMi incident.

Figure 16 Fight-Click a Syslog Message, then View Incident History



Disabling the HP NNMi–HP ArcSight Logger Integration

To disable the integration, do the following:

1. From the NNMi console, click **Integration Module Configuration** > **HP ArcSight**.
2. Remove the **Enable ArcSight Integration** selection.
3. Click **Submit**.

Problems and Solutions

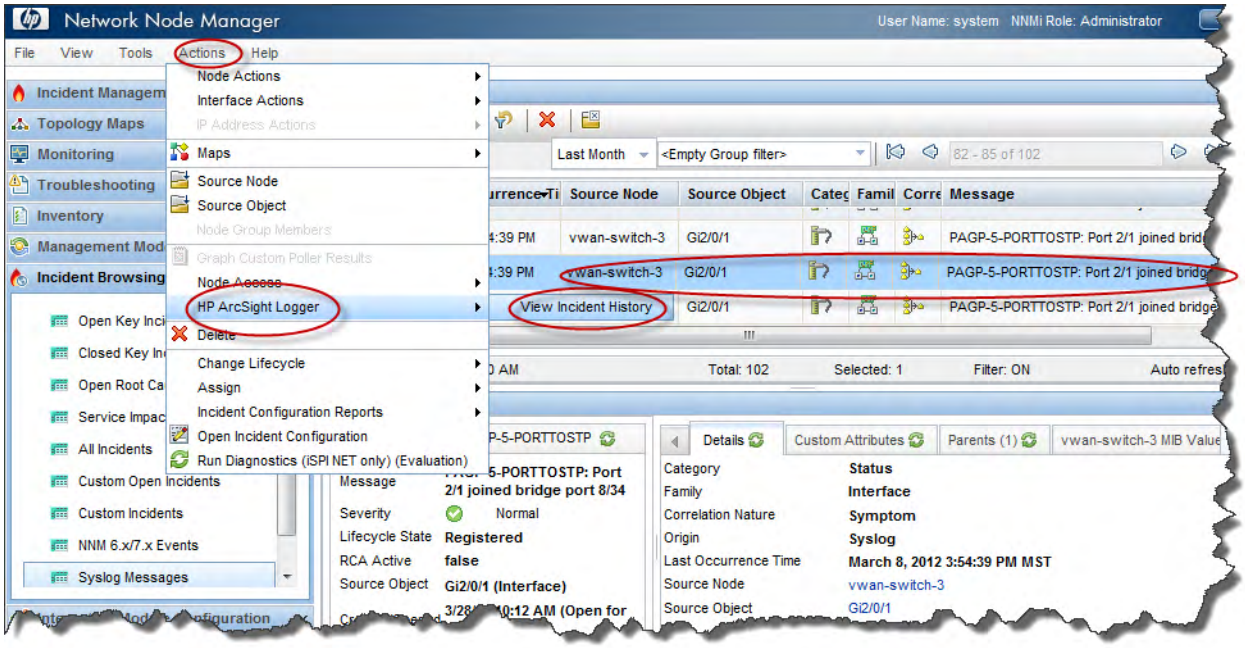
Problem: If you open the HP ArcSight Logger application from the NNMi console by selecting an incident that contains port data, HP NNMi cannot find the incident in HP ArcSight Logger.

Solution: This happens because HP NNMi resolves the source object to an interface, and not to the port, while HP ArcSight Logger does not have interface data associated with the syslog message in its database. To remedy this, do one the following:

- Open HP ArcSight Logger from the NNMi console by selecting an interface (do not open HP ArcSight Logger by selecting an incident associated with an interface). After HP ArcSight Logger opens, modify the query in HP ArcSight Logger to include the port name that is associated with the interface.
- Select a syslog message and use a HP ArcSight Logger query to view the information. The following steps show an example of this approach:

  a Open HP ArcSight Logger from the NNMi console by selecting the interface; then clicking **View Incident History**.

Figure 17 Open View Incident History by Selecting an Interface



  b After HP ArcSight Logger opens, modify the query in HP ArcSight Logger to include the port name for the incident that is associated with the interface.

  c Run the modified HP ArcSight Logger query to find the incident in HP ArcSight Logger.

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 9.21

Document title: ***HP Network Node Manager i Software - HP ArcSight Logger Integration Guide***

Feedback:


Java™
COMPATIBLE