Hewlett Packard
Enterprise

HPE Network Node Manager i Software

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

HPE Network Node Manager i Software–HPE ArcSight Logger Integration Guide

Document Release Date: May 2017
Software Release Date: May 2016

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

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.

Copyright Notice

© Copyright 2008–2017 Hewlett Packard Enterprise Development LP

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.

Acknowledgements

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.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HP Passport account. If you do not have one, click the **Create an account** button on the HP Passport Sign in page.

Support

Visit the HPE Software Support web site at: **https://softwaresupport.hpe.com**

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

HPE Software 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:

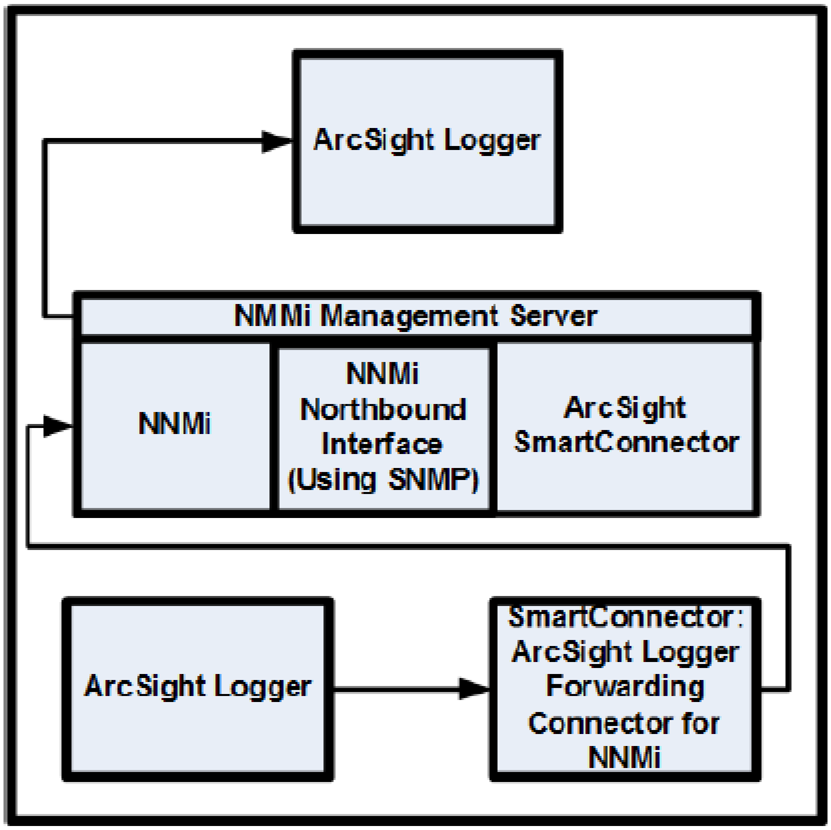
- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research 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://softwaresupport.hpe.com** and click **Register**.

To find more information about access levels, go to:
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

Contents

Integrate NNMi with HPE ArcSight Logger


ArcSight Logger
NMMi Management Server
NNMi
NNMi Northbound Interface (Using SNMP)
ArcSight SmartConnector
ArcSight Logger
SmartConnector: ArcSight Logger Forwarding Connector for NNMi

HPE 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 HPE ArcSight Logger, point your browser to http://www.arcsight.com/products.

About the NNMi-HPE ArcSight Logger

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

Value

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

Integrated Products

The information in this chapter applies to the following products:

- HPE ArcSight Logger
- SmartConnector: ArcSight NNMi SNMP
- SmartConnector: ArcSight Logger Forwarding Connector for NNMi

  TIP: For the list of supported Logger versions, see the NNMi Support Matrix.

- NNMi 10.20

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

Customizing the HPE ArcSight Logger Filters

There are Syslog messages that pass the HPE ArcSight Logger filter and forward to NNMi. Without configuring the HPE ArcSight Logger filter, HPE ArcSight Logger forwards large quantities of `ArcSightEvents` to NNMi. This can adversely affect NNMi performance. *It is very important that you configure this filter promptly to limit the quantity of `ArcSightEvents` flowing from HPE ArcSight Logger to 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 HPE ArcSight Logger forwards to NNMi.

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

Documentation

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

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

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

To obtain copies of HPE 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 HPE ArcSight customer (be able to provide user credentials) to access HPE ArcSight product documentation.

To view the supported system requirements for HPE 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 HPE ArcSight Logger in the *Logger Administrator's Guide.*

Enabling the NNMi-HPE ArcSight Logger Integration

You might have creatively used existing NNMi features, such as the NNMi northbound interface, to configure a custom integration between HPE ArcSight Logger and NNMi. If you plan to install NNMi 10.20, you must disable this custom NNMi - HPE ArcSight Logger integration. After you disable this custom integration, complete the tasks in this section to enable the more robust NNMi - HPE ArcSight Logger integration delivered in NNMi 10.20.

Prerequisites

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

- Install NNMi 10.20.
- Install the SmartConnector for NNMi SNMP using instructions from the *SmartConnector Configuration Guide for NNMi Network Node Manager i SNMP* manual.
- Install the HPE ArcSight Logger Forwarding Connector for NNMi using instructions from the *SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for NNMi* manual.

Steps to Enable the NNMi-HPE ArcSight Logger Integration

Complete the following tasks to enable the NNMi- HPE ArcSight Logger integration:

"Task 1: Install and configure NNMi 10.20"

"Task 2: Understanding the HPE ArcSight MIBs"

"Task 3: Configuring the HPE ArcSight Logger Forwarding Connector for NNMi"

"Task 4: Configuring the NNMi–HPE ArcSight Logger Integration"

"Task 5: Configuring the HPE ArcSight Logger Filter"

"Task 6: Configuring the SmartConnector for NNMi SNMP (Connector for Northbound Interface, Optional Task)"

"Task 7: Configuring NNMi to Forward SNMPv1, v2c, and v3 Trap Incidents to HPE ArcSight Logger (Northbound Interface, Optional Task)"

Task 1: Install and configure NNMi 10.20

Install and configure NNMi.

After that, import the HPE ArcSight Logger certificate to NNMi.

Perform this task of importing certificate only when NNMi is configured to use the HTTPS protocol and uses the PKCS#12 certificate repository.

1. Check that NNMi uses the PKCS#12 certificate repository.

   To check the type of certificate repository:

   a. Log on to the NNMi console.
   b. Click **Help > System Information**, and then go to the Server tab.
   c. Check the value of the `javax.net.ssl.keyStore` property.

      If the property points to the `nnm-key.p12` file, your environment has a PKCS#12 repository.

      If the property points to the `nnm.keystore` file, your environment has a JKS repository.

   Alternatively, do the following:

   a. On the NNMi management server, as root or administer, run the following command:
      - *On Windows:* **%nnminstalldir%\bin\nnmprops -l**
      - *On Linux:* **/opt/OV/bin/nnmprops -l**
   b. From the command output, note the value of the `javax.net.ssl.trustStoreType` property.

      The value of this property indicates the type of certificate repository.
2. On the HPE ArcSight Logger server, export the HPE ArcSight certificate to a file, and then transfer the file to a local directory on the NNMi management server.
3. Log on to the NNMi management server as root or administrator.
4. Import the certificate to NNMi's truststore by running the following command:
   - *On Windows:* **%nnminstalldir%\bin\nnmkeytool.ovpl -importcert -keystore %nnmdatadir%\shared\nnm\certificates\nnm-trust.p12 -storetype PKCS12 -storepass ovpass -file** <*Cert_Path*>

   - *On Linux:* **/opt/OV/bin/nnmkeytool.ovpl -importcert -keystore /var/opt/OV/shared/nnm/certificates/nnm-trust.p12 -storetype PKCS12 -storepass ovpass -file** <*Cert_Path*>

   In this instance, <*Cert_Path*> is the directory on the NNMi management server where you have
5. Restart NNMi:
   a. **ovstop -c**
   b. **ovstart -c**

Task 2: Understanding the HPE ArcSight MIBs

After you complete "Task 1: Install and configure NNMi 10.20" through "Task 5: Configuring the HPE ArcSight Logger Filter", HPE ArcSight Logger begins forwarding filtered `ArcSightEvents` to NNMi. NNMi resolves interfaces and nodes to the source objects included in these `ArcSightEvents`. During the NNMi 10.20 installation, the **`hp-arcsight.mib`** MIB is installed and loaded on the NNMi management server. Use NNMi's **Node Action** > **MIB Information** feature to better understand the OIDs that are present in the `ArcSightEvent.`

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

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

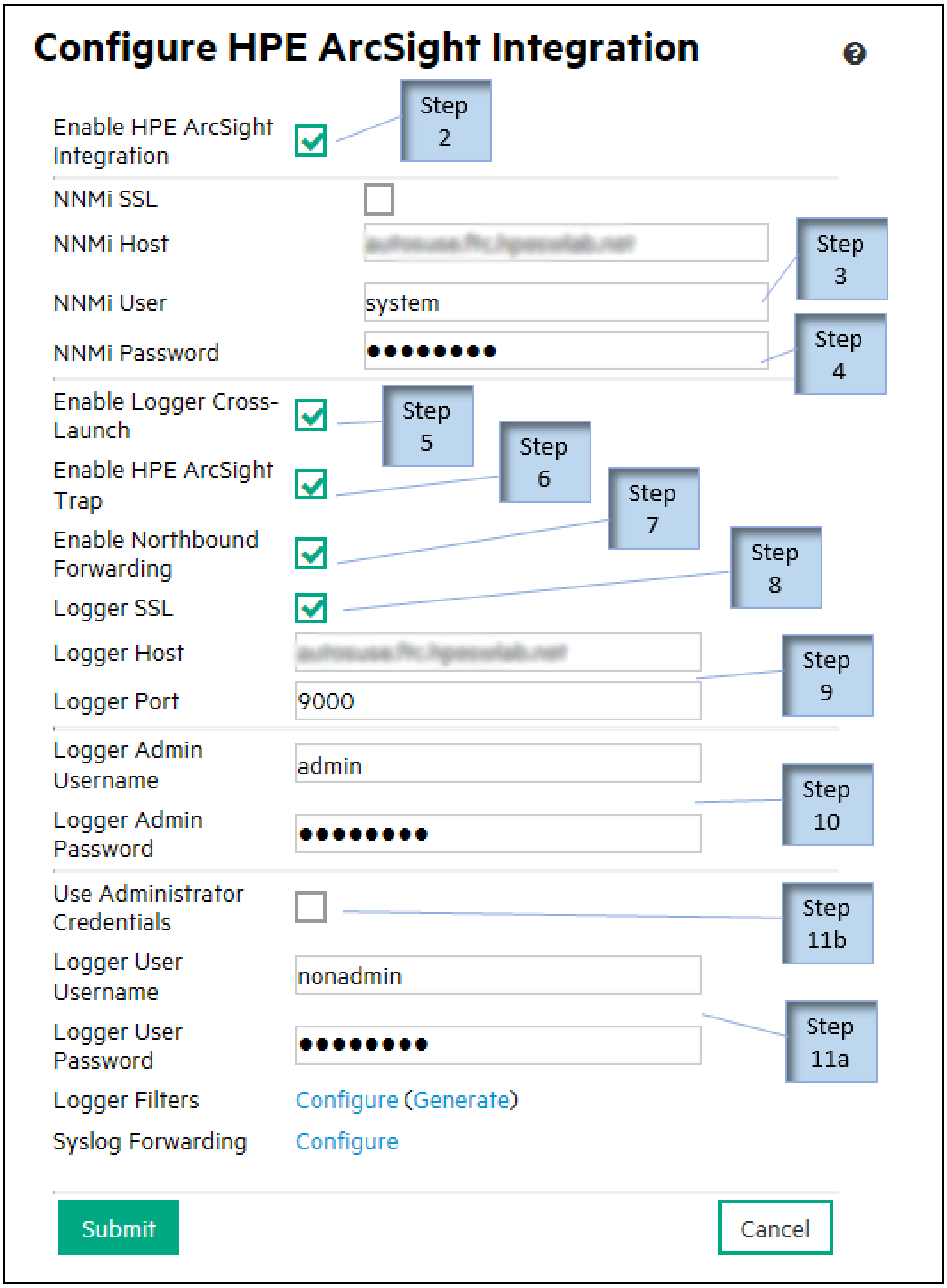
Task 4: Configuring the NNMi–HPE ArcSight Logger Integration

By enabling the NNMi - HPE ArcSight Logger integration and the `ArcSightEvent`, along with configuring HPE ArcSight Logger to forward SNMP traps in the form of `ArcSightEvents`, NNMi can evaluate each

`ArcSightEvent` content and show it as an SNMP trap or a Syslog message. To enable the NNMi - HPE ArcSight Logger integration complete the following steps:

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

Figure 1 Enabling the NNMi-HPE ArcSight Logger Integration



Configure HPE ArcSight Integration

Enable HPE ArcSight Integration ☑

NNMi SSL □

NNMi Host [redacted]

NNMi User system

NNMi Password ●●●●●●●●

Enable Logger Cross-Launch ☑

Enable HPE ArcSight Trap ☑

Enable Northbound Forwarding ☑

Logger SSL ☑

Logger Host [redacted]

Logger Port 9000

Logger Admin Username admin

Logger Admin Password ●●●●●●●●

Use Administrator Credentials □

Logger User Username nonadmin

Logger User Password ●●●●●●●●

Logger Filters Configure (Generate)

Syslog Forwarding Configure

2. Select **Enable HPE ArcSight Integration**.
3. If NNMi is configured to use SSL, select **NNMi SSL**.
4. Add or observe the following 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 or HTTPS 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.

5. `NNMi Password`: Enter the username password.
6. Select **Enable Logger Cross-Launch**.
7. Select **Enable HPE 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**.
8. If you want to forward NNMi incidents to HPE ArcSight Logger, select **Enable Northbound Forwarding**.
9. Not all HPE ArcSight Logger applications are configured to use SSL. If the HPE ArcSight Logger application included in this NNMi - HPE ArcSight Logger integration is configured to use SSL, select **Logger SSL**.

   NOTE: See the *HPE ArcSight Logger v5.1 Administrators Guide* about configuring Logger for SSL.
10. Add the following HPE ArcSight Logger integration information:
    - `Logger Host` (the fully qualified domain name of the Logger Host)
    - `Logger Port`
11. Add the following HPE ArcSight Logger administrator credentials:
    - `Logger Admin Username`
    - `Logger Admin Password`
12. 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 HPE 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 NNMi level 1 operator full administrator privileges in HPE ArcSight Logger. For security purposes, step a is the recommended method.
13. Click **Submit** to save these changes.
14. For the cross-launch menu changes to become visible in the NNMi console, do the following:

    a. Sign out of NNMi.

    b. Sign in to NNMi.

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

Next, *promptly* complete "Task 5: Configuring the HPE ArcSight Logger Filter" to identify and configure only those Syslog messages that you want HPE ArcSight Logger to forward to NNMi.

Task 5: Configuring the HPE ArcSight Logger Filter

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

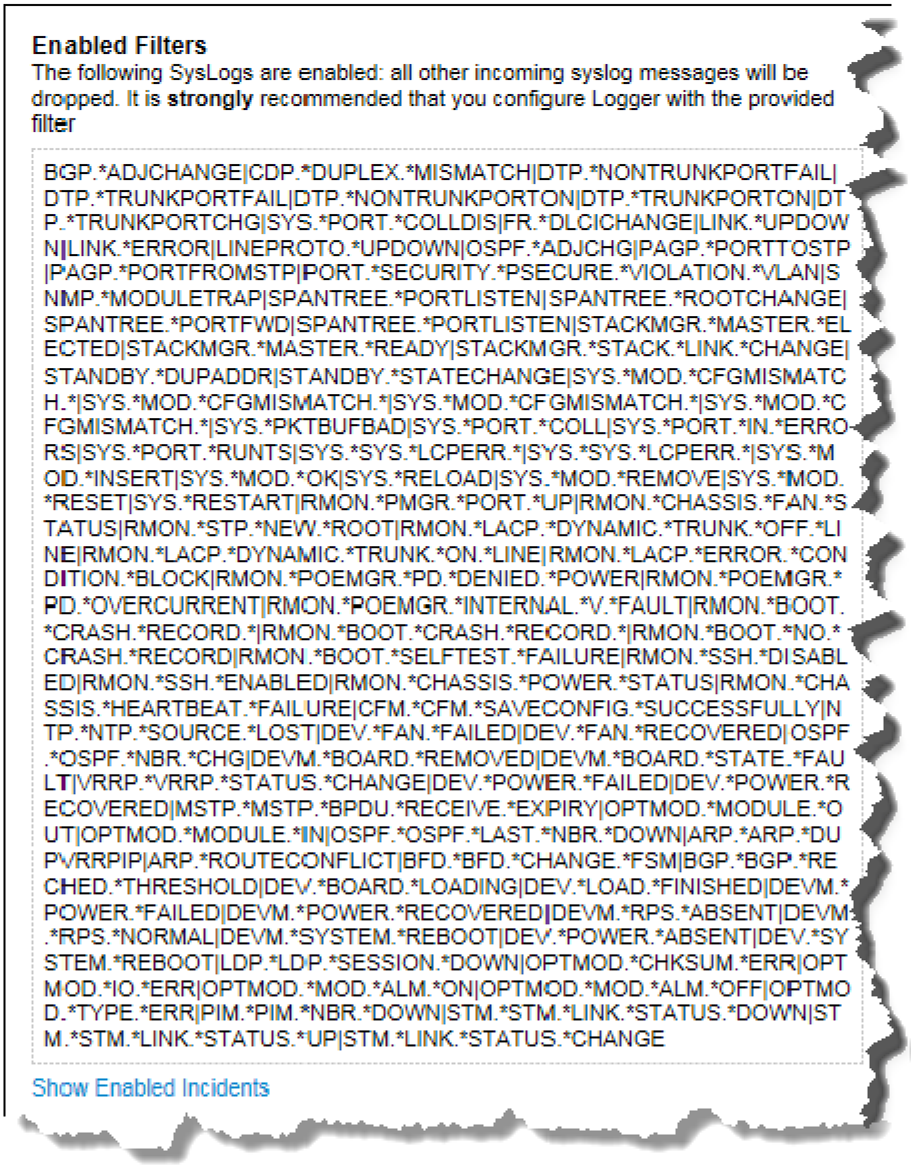
> **NOTE:** To avoid receiving an unmanageable number of traps, be sure to complete Task 5 immediately after you complete Task 4.

> **NOTE:** 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 HPE ArcSight Logger's configuration and add new filter content, do the following:

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

Figure 2 Enabled Filters Page



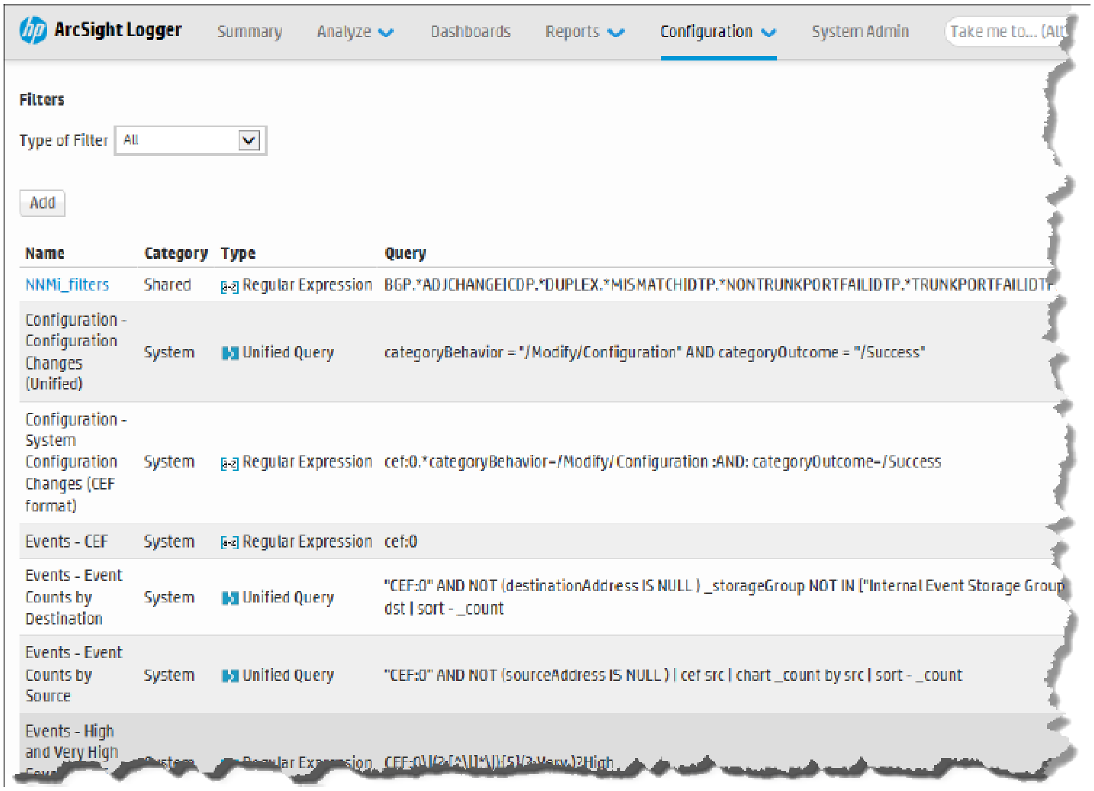
Enabled Filters

The following SysLogs are enabled: all other incoming syslog messages will be dropped. It is **strongly** recommended that you configure Logger with the provided filter

```
BGP.*ADJCHANGE|CDP.*DUPLEX.*MISMATCH|DTP.*NONTRUNKPORTFAIL|
DTP.*TRUNKPORTFAIL|DTP.*NONTRUNKPORTON|DTP.*TRUNKPORTON|DT
P.*TRUNKPORTCHG|SYS.*PORT.*COLLDIS|FR.*DLCICHANGE|LINK.*UPDOW
N|LINK.*ERROR|LINEPROTO.*UPDOWN|OSPF.*ADJCHG|PAGP.*PORTTOSTP
|PAGP.*PORTFROMSTP|PORT.*SECURITY.*PSECURE.*VIOLATION.*VLAN|S
NMP.*MODULETRAP|SPANTREE.*PORTLISTEN|SPANTREE.*ROOTCHANGE|
SPANTREE.*PORTFWD|SPANTREE.*PORTLISTEN|STACKMGR.*MASTER.*EL
ECTED|STACKMGR.*MASTER.*READY|STACKMGR.*STACK.*LINK.*CHANGE|
STANDBY.*DUPADDR|STANDBY.*STATECHANGE|SYS.*MOD.*CFGMISMATC
H.*|SYS.*MOD.*CFGMISMATCH.*|SYS.*MOD.*CFGMISMATCH.*|SYS.*MOD.*C
FGMISMATCH.*|SYS.*PKTBUFBAD|SYS.*PORT.*COLL|SYS.*PORT.*IN.*ERRO
RS|SYS.*PORT.*RUNTS|SYS.*SYS.*LCPERR.*|SYS.*SYS.*LCPERR.*|SYS.*M
OD.*INSERT|SYS.*MOD.*OK|SYS.*RELOAD|SYS.*MOD.*REMOVE|SYS.*MOD.
*RESET|SYS.*RESTART|RMON.*PMGR.*PORT.*UP|RMON.*CHASSIS.*FAN.*S
TATUS|RMON.*STP.*NEW.*ROOT|RMON.*LACP.*DYNAMIC.*TRUNK.*OFF.*LI
NE|RMON.*LACP.*DYNAMIC.*TRUNK.*ON.*LINE|RMON.*LACP.*ERROR.*CON
DITION.*BLOCK|RMON.*POEMGR.*PD.*DENIED.*POWER|RMON.*POEMGR.*
PD.*OVERCURRENT|RMON.*POEMGR.*INTERNAL.*V.*FAULT|RMON.*BOOT.
*CRASH.*RECORD.*|RMON.*BOOT.*CRASH.*RECORD.*|RMON.*BOOT.*NO.*
CRASH.*RECORD|RMON.*BOOT.*SELFTEST.*FAILURE|RMON.*SSH.*DISABL
ED|RMON.*SSH.*ENABLED|RMON.*CHASSIS.*POWER.*STATUS|RMON.*CHA
SSIS.*HEARTBEAT.*FAILURE|CFM.*CFM.*SAVECONFIG.*SUCCESSFULLY|N
TP.*NTP.*SOURCE.*LOST|DEV.*FAN.*FAILED|DEV.*FAN.*RECOVERED|OSPF
.*OSPF.*NBR.*CHG|DEVM.*BOARD.*REMOVED|DEVM.*BOARD.*STATE.*FAU
LT|VRRP.*VRRP.*STATUS.*CHANGE|DEV.*POWER.*FAILED|DEV.*POWER.*R
ECOVERED|MSTP.*MSTP.*BPDU.*RECEIVE.*EXPIRY|OPTMOD.*MODULE.*O
UT|OPTMOD.*MODULE.*IN|OSPF.*OSPF.*LAST.*NBR.*DOWN|ARP.*ARP.*DU
PVRRPIP|ARP.*ROUTECONFLICT|BFD.*BFD.*CHANGE.*FSM|BGP.*BGP.*RE
CHED.*THRESHOLD|DEV.*BOARD.*LOADING|DEV.*LOAD.*FINISHED|DEVM.*
POWER.*FAILED|DEVM.*POWER.*RECOVERED|DEVM.*RPS.*ABSENT|DEVM
.*RPS.*NORMAL|DEVM.*SYSTEM.*REBOOT|DEV.*POWER.*ABSENT|DEV.*SY
STEM.*REBOOT|LDP.*LDP.*SESSION.*DOWN|OPTMOD.*CHKSUM.*ERR|OPT
MOD.*IO.*ERR|OPTMOD.*MOD.*ALM.*ON|OPTMOD.*MOD.*ALM.*OFF|OPTMO
D.*TYPE.*ERR|PIM.*PIM.*NBR.*DOWN|STM.*STM.*LINK.*STATUS.*DOWN|ST
M.*STM.*LINK.*STATUS.*UP|STM.*LINK.*STATUS.*CHANGE
```

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

Figure 3 The HPE ArcSight Logger Configuration Page



Name	Category	Type	Query
NNMi_filters	Shared	Regular Expression	BGP.*ADJCHANGE|CDP.*DUPLEX.*MISMATCH|DTP.*NONTRUNKPORTFAIL|DTP.*TRUNKPORTFAIL|DTP
Configuration - Configuration Changes (Unified)	System	Unified Query	categoryBehavior = "/Modify/Configuration" AND categoryOutcome = "/Success"
Configuration - System Configuration Changes (CEF format)	System	Regular Expression	cef:0.*categoryBehavior=/Modify/ Configuration :AND: categoryOutcome=/Success
Events - CEF	System	Regular Expression	cef:0
Events - Event Counts by Destination	System	Unified Query	"CEF:0" AND NOT (destinationAddress IS NULL) _storageGroup NOT IN ["Internal Event Storage Group dst | sort - _count
Events - Event Counts by Source	System	Unified Query	"CEF:0" AND NOT (sourceAddress IS NULL) | cef src | chart _count by src | sort - _count
Events - High and Very High Even	System	Regular Expression	CEF:0|(?:[^|]*|){5}(?:Very)?High

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 NNMi.

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

   a. Click **Add**.

   b. After HPE 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 NNMi, do the following:

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

   b. Clear out the existing filter contents.

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

   d. Save your work.

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

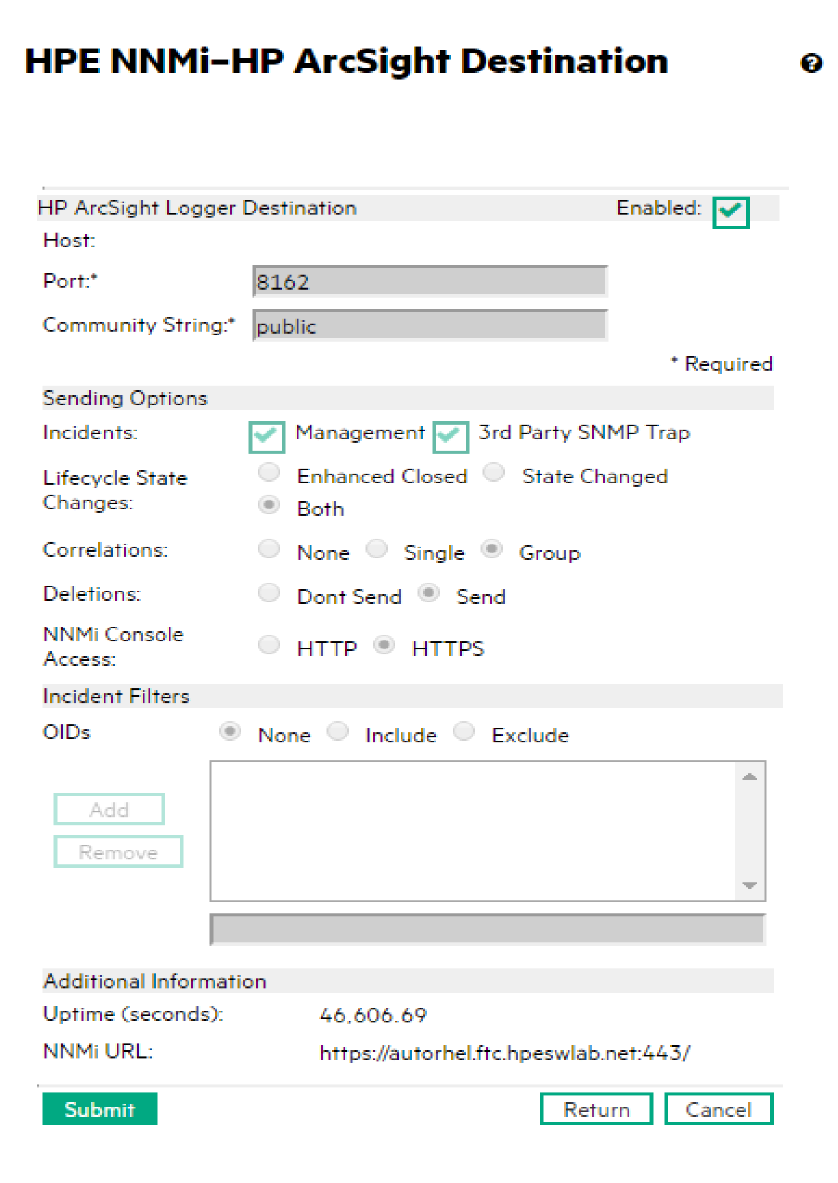
Task 6: Configuring the SmartConnector for NNMi SNMP (Connector for Northbound Interface, Optional Task)

Configure the SmartConnector for NNMi SNMP using instructions from the *SmartConnector Configuration Guide for NNMi SNMP* manual.

Task 7: Configuring NNMi to Forward SNMPv1, v2c, and v3 Trap Incidents to HPE ArcSight Logger (Northbound Interface, Optional Task)

1. From the NNMi console, click **Integration Module Configuration** > **HPE 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 NNMi - HPE ArcSight Logger Destination



HPE NNMi–HP ArcSight Destination

HP ArcSight Logger Destination Enabled: ☑

Host:

Port:* 8162

Community String:* public

* Required

Sending Options

Incidents: ☑ Management ☑ 3rd Party SNMP Trap

Lifecycle State Changes: ○ Enhanced Closed ○ State Changed ● Both

Correlations: ○ None ○ Single ● Group

Deletions: ○ Dont Send ● Send

NNMi Console Access: ○ HTTP ● HTTPS

Incident Filters

OIDs ● None ○ Include ○ Exclude

Additional Information

Uptime (seconds): 46,606.69

NNMi URL: https://autorhel.ftc.hpeswlab.net:443/

3. Select **ArcSight Logger Destination** > **Enabled**.
4. Add 8162 as the value of the port field. NNMi forwards to a connector that is installed on the NNMi 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, NNMi forwards everything.
7. Click **Submit**.
8. NNMi tests for any configuration errors. Fix any errors, then repeat step 7 until the submit is successful.

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

Modifying the NNMi - HPE ArcSight Logger Integration

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

Managing the Number of Incoming Syslog Messages

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

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

     `nnmtrapdump.ovpl -last 10`

     > **NOTE:** 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 Linux manpage.

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

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

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

   > **NOTE:** If you do not see the specific Syslog message to define, you might need to reconfigure the Syslog messages to forward to NNMi. See "Task 5: Configuring the HPE ArcSight Logger Filter".
   >
   > If you configure the HPE ArcSight Logger filter and still do not see the specific Syslog message to define, submit a support call for HPE ArcSight Support at https://softwaresupport.hpe.com/.

2. Using the list you obtained from step 1, find the first Syslog message in the list to define in 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.

   > **NOTE:** 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 NNMi uses to look up the respective syslog message incident configuration. 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 in step 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.`

   > **NOTE:** 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.

> **TIP:** To keep NNMi performing at a high level, 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 NNMi - HPE ArcSight Logger Integration

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

Opening HPE ArcSight Logger from the NNMi Console

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

> **NOTE:** 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 NNMi - HPE ArcSight Logger integration, the `ArcSightEvents` that HPE ArcSight Logger forwards to 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 HPE ArcSight Logger forwards to NNMi 10.20, and that are actual Syslog messages, do the following:

1. From the NNMi console, navigate to **Configuration** > **Incidents** > **Syslog Message Configurations.**
2. NNMi shows the current list of `Syslog Message Configurations`.

Changes to the NNMi Console's Actions Menu

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

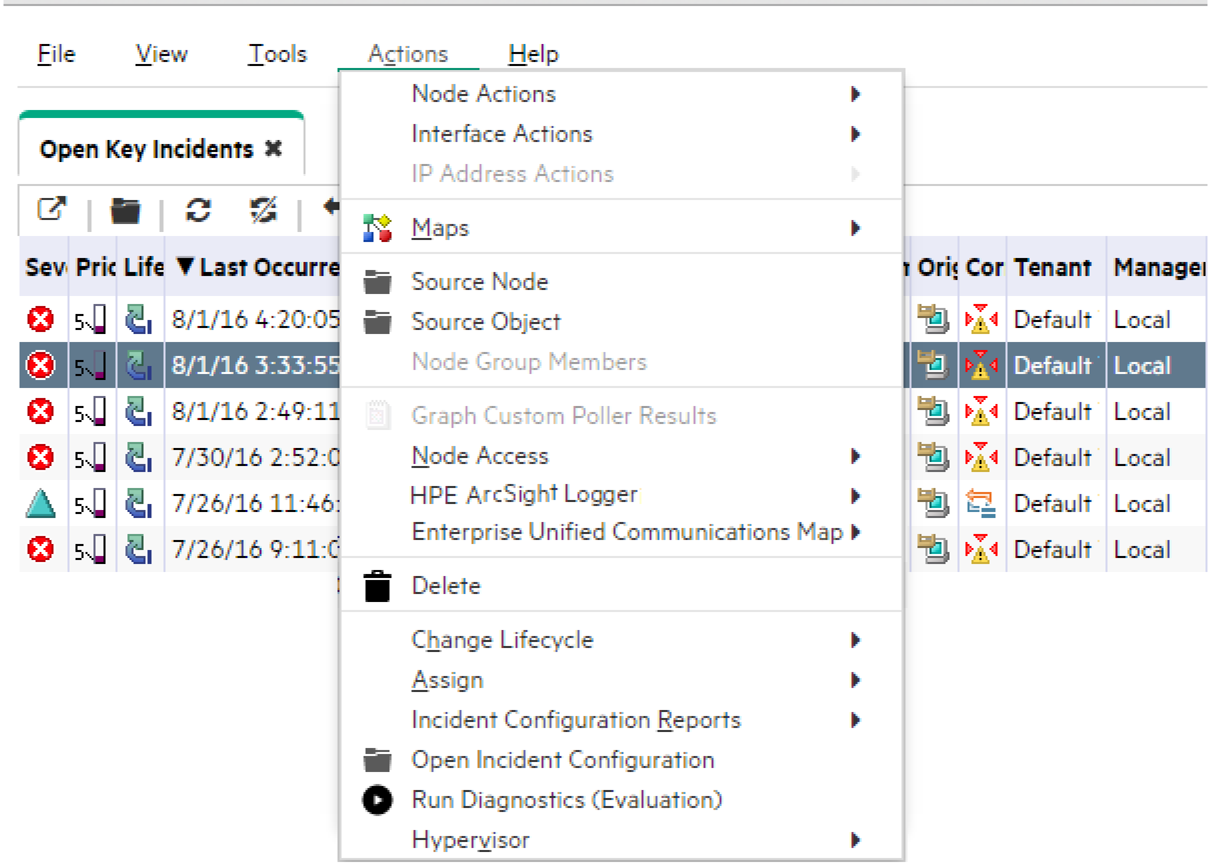
Incident Management Workspace

In the **Incident Management** workspace, use the NNMi console to open the HPE ArcSight Logger application from an incident.

In an incident view, select an incident. Then, on the NNMi console **Actions** menu, click **HPE ArcSight Logger > View Incident History**, as shown in Figure 5.

Alternatively, right-click an incident, and then click **HPE ArcSight Logger > View Incident History**.

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



Sev	Pric	Life	▼ Last Occurre	Orig	Cor	Tenant	Manager
✖	5		8/1/16 4:20:05			Default	Local
✖	5		8/1/16 3:33:55			Default	Local
✖	5		8/1/16 2:49:11			Default	Local
✖	5		7/30/16 2:52:0			Default	Local
▲	5		7/26/16 11:46:			Default	Local
✖	5		7/26/16 9:11:0			Default	Local

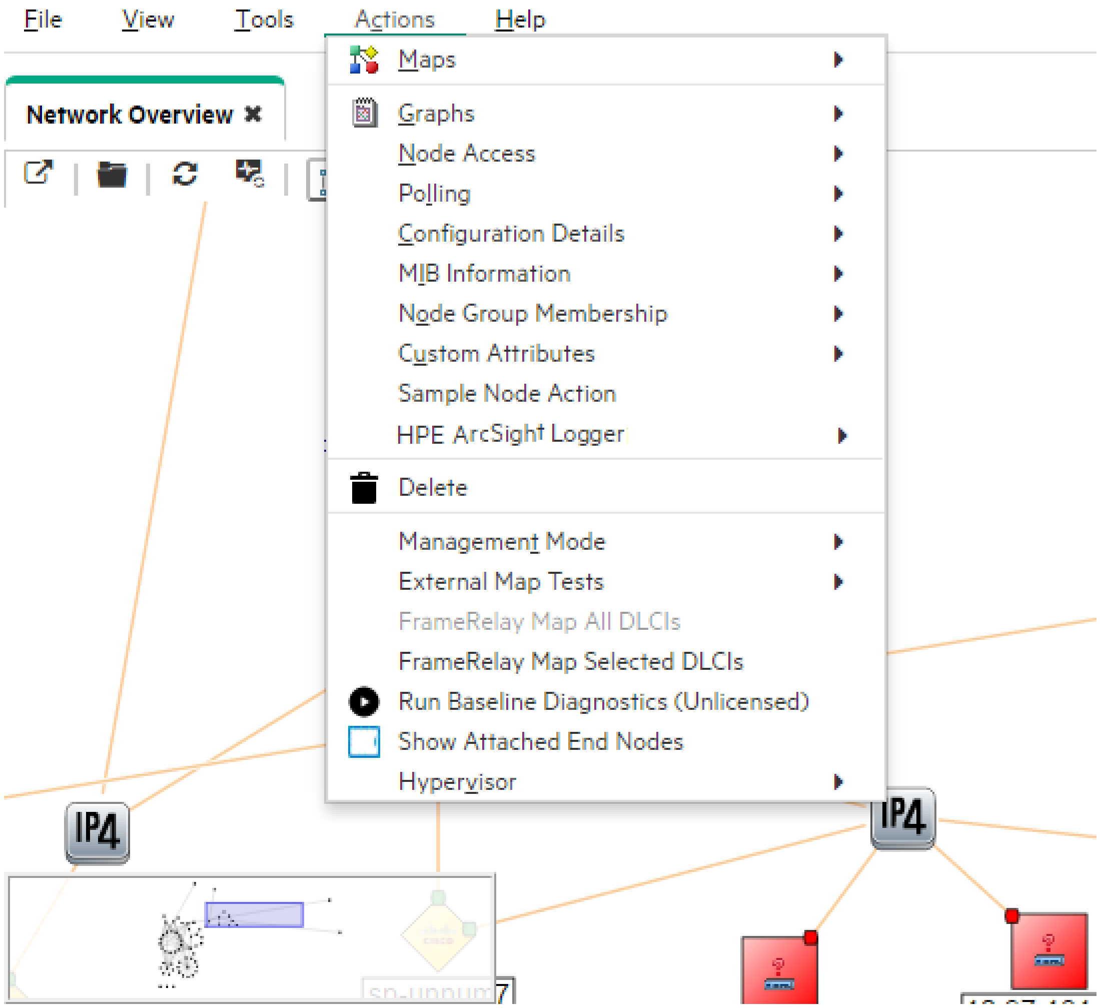
Topology Maps Workspace

In the **Topology Maps** workspace, use the NNMi console to open the HPE ArcSight Logger application from a node.

In a map view, select a node or interface. Then, on the NNMi console **Actions** menu, click **HPE ArcSight Logger**, and then click one of the available options, as shown in Figure 6.

Alternatively, right-click a node or interface, click **HPE ArcSight Logger**, and then click one of the available options.

Figure 6 Opening HPE ArcSight Logger from a Node in the Topology Maps Workspace



Monitoring Workspace

In the **Monitoring** workspace, use the NNMi console to open the HPE ArcSight Logger application from a node or interface. In a monitoring view, select a node or interface. Then, on the NNMi console **Actions** menu, click **HPE ArcSight Logger**, and then click one of the available options.

Alternatively, right-click a node or incident, click **HPE ArcSight Logger**, and then click one of the available options.

Troubleshooting Workspace

In the **Troubleshooting** workspace, use the NNMi console to open the HPE ArcSight Logger application from a node or interface. In a troubleshooting view, select a node or interface. Then, on the NNMi console **Actions** menu, click **HPE ArcSight Logger**, and then click one of the available options.

Alternatively, right-click a node or interface, click **HPE ArcSight Logger**, and then click one of the available options.

Inventory Workspace

In the **Inventory** workspace, use the NNMi console to open the HPE ArcSight Logger application from a node or interface.

In an inventory view, select a node or interface. Then, on the NNMi console **Actions** menu, click **HPE ArcSight Logger**, and then click one of the available options.

Alternatively, right-click a node or interface, click **HPE ArcSight Logger**, and then click one of the available options.

Incident Browsing Workspace

In the **Incident Browsing** workspace, use the NNMi console to open the HPE ArcSight Logger application from an incident.

In an incident view, select an incident. Then, on the NNMi console **Actions** menu, click **HPE ArcSight Logger > View Incident History**.

Alternatively, right-click an incident, and then click **HPE ArcSight Logger > View Incident History**.

Disabling the NNMi-HPE ArcSight Logger Integration

To disable the integration, do the following:

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

Problems and Solutions

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

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

- Open HPE ArcSight Logger from the NNMi console by selecting an interface (do not open HPE ArcSight Logger by selecting an incident associated with an interface). After HPE ArcSight Logger opens, modify the query in HPE ArcSight Logger to include the port name that is associated with the interface.
- Select a syslog message and use a HPE ArcSight Logger query to view the information. The following steps show an example of this approach:
  a. Open HPE ArcSight Logger from the NNMi console by selecting the interface; then clicking **View Incident History**.
  b. After HPE ArcSight Logger opens, modify the query in HPE ArcSight Logger to include the port name for the incident that is associated with the interface.
  c. Run the modified HPE ArcSight Logger query to find the incident in HPE ArcSight Logger.

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 HPE Network Node Manager i Software—HPE ArcSight Logger Integration Guide (Network Node Manager i Software 10.20)

Just add your feedback to the email and click send.

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

We appreciate your feedback!

Glossary

A

AES

Advanced Encryption Standard

Anycast Rendezvous Point IP Address

Rendezvous Point addresses are loopback addresses used for routers in multi-cast network configurations.

Autonomous System

An Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes that present a common, clearly defined Border Gateway Protocol (BPG) routing policy to the Internet by having an officially registered Autonomous System Number (ASN).

B

BGP

Border Gateway Protocol

C

Causal Engine

The NNMi Causal Engine analyzes the health of your network and provides the ongoing health status reading for each device. The Causal Engine also extensively evaluates problems and determines the root cause for you, whenever possible, sending incidents to notify you of problems. Any incident generated from a Causal Engine management event has an Origin of NNMi in your incident views.

CBC

Cipher Block Chaining

CE

Customer Edge router. The router in your network that sends data to an Internet Service Provider's router (the Provider Edge) on the path to the data's final desination.

CRC

Cyclic Redundancy Check

Custom Node Collection

A Custom Node Collection identifies a topology node that has at least one associated Custom Poller Policy. Because a topology node can be associated with more than one Policy, the same topology node might appear in multiple Custom Node Collections.

Custom Polled Instance

A Custom Polled Instance represents the results of a MIB variable when it is evaluated against a node. The first time a MIB variable is validated with discovery information, the results appear in the Monitoring workspace's Custom Polled Instances view. The Custom Polled Instance is updated whenever a change in State occurs and includes the most recent polled value that caused the State to change. These results are then used to determine the Status of the associated Custom Node Collection.

Custom User Groups

Custom User Groups are the User Groups that you create. These User Groups are additional to the NNMi User Groups, which are those User Groups that NNMi provides.

D

DES

Data Encryption Standard

E

EIGRP

Enhanced Interior Gateway Routing Protocol

EVPN

Ethernet Virtual Private Network.

G

global unicast address

(2000:: to 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff) A publically routable IPv6 unicast address, used for communication between nodes anywhere on the internet. The first part of the address is a global routing prefix in the 2000::/3 address space for your organization (assigned by the Internet Service Providers). The complete host address can either be manually configured or automatically assigned using IPv6 auto-configuration and neighbor discovery.

H

HMAC

Hash-based Message Authentication Code

hops

A hop is a node representing any network device, such as a workstation, gateway, or switch, which is connected by a link with no intermediate nodes.

HSRP

Hot Standby Router Protocol

hypervisor

The virtual machine manager in charge of delegating various aspects from a pool of resources to become virtual devices. The delegations might be static or dynamic, depending on the manufacture's implementation. The type of virtual machines being generated depends on the manufacturer's implementation.

I

IPv6 link-local address

A non-routable IPv6 unicast address only used for communication with other nodes on the same link (LAN or VLAN). Link local addresses cannot be used for communication that must be forwarded through a router. IPv6 auto-configuration automatically assigns a unique link local address in the fe80::/10 address space to each IPv6-enabled interface on a system.

ISIS

Intermediate System to Intermediate System Protocol

J

Jython

Jython is a programming language (successor of JPython) uses Java class, instead of Python modules.

K

Key Incident

Incidents with both: (1) Severity = other than Normal. (2) Correlation Nature = equal to Root Cause, Service Impact, Stream Correlation, Rate Stream Correlation, Info, or None.

L

Layer 2

Refers to the Data Link layer of the multilayered communication model, Open Systems Interconnection (OSI). The Data Link layer moves data across the physical links in the network. The switches and switch-routers are devices that redirect data messages at the layer 2 level, using the destination Media Access Control (MAC) address to determine where to direct the message.

Layer 3

Refers to the Network layer of the multilayered communication model, Open Systems Interconnection (OSI). The Network layer is concerned with knowing the address of the neighboring nodes in the network, selecting routes and quality of service, and recognizing and forwarding incoming messages to local host domains. The router and switch-router are the devices that redirect data messages at the Layer 3 level. Everything in a subnet is connected at the Layer 3 (IP) level.

Link Aggregation

Protocols used on Switches to configure multiple Interfaces (Aggregation Member Interfaces) to function as if they were one (an Aggregator Interface). When two Aggregator Interfaces establish a connection, that connection is an Aggregator Layer 2 Connection. The Aggregator Layer 2 Connection appears on Layer 2 Neighbor View maps as a thick line with an Interface icon at each end (representing the Aggregator Interface).

loopback address

The address associated with the loopback interface. The loopback interface is a virtual interface on a device that provides a route for internal communication. Many vendors provide a specially configured loopback for management purposes. Exact details of how loopbacks are configured varies by vendor and model. See each device's documentation for details. NNMi identifies these loopback addresses by using ifType Number 24, softwareloopback from the IANA ifType-MIB.

M

MAC address

The Media Access Control address (hardware address or physical address) that the factory burns into a network adapter or device with built-in networking capability. A MAC address has six pairs of hexadecimal digits, separated by colons or dashes. For example 02:1F:33:16:BC:55

MAC addresses

The Media Access Control address (hardware address or physical address) that the factory burns into a network adapter or device with built-in networking capability. A MAC address has six pairs of hexadecimal digits, separated by colons or dashes. For example 02:1F:33:16:BC:55

MD5

Message-Digest algorithm 5

MIB file

Management Information Base files are the basic building block of SNMP communication protocol. SNMP Agents are configured to respond to requests defined by a group of supported MIB files.

MPLS

Multiprotocol Label Switching

multicast address

Used to identify a group of hosts joined into a group. IPv4 multicast addresses are in the range 224.0.0.0 to 239.255.255.255 and IPv6 multicast addresses have the prefix ff00::/8.

multiconnection

A multiconnection is a thick line on a map view between two Node icons, two Node Group icons, or between a Node icon and a Node Group icon (with no Interface icon or IP Address icon at either end of the line). This thick line represents a set of multiple connections that have been combined to preserve space and simplify the map. Your NNMi administrator specifies the number of connections that must exist before NNMi condenses them into a multiconnection line (User Interface Configuration's Multiconnection Threshold attribute). Double-click the thick line to convert it into the original set of connections with Interface icons or IP Address icons at either end of the lines.

N

NAT

Network Address Translation. NNMi supports the following protocols: Static Network Address Translation, Dynamic Network Address Translation, Dynamic Port Address Translation.

NIC

Network Interface Controller

NNMi Role

Determined by your membership in one of four special NNMi User Groups (NNMi Administrators, NNMi Level 2 Operators, NNMi Level 1 Operators, or NNMi Guest Users). This membership determines what you can see and do within the NNMi console.

NNMi User Group

NNMi User Groups are those User Groups provided by NNMi. Users cannot access the NNMi console until their User Account is mapped to at least one of the following NNMi User Groups: NNMi Administrators, NNMi Level 2 Operators, NNMi Level 1 Operators (with more limited access privileges than Level 2 Operators), and NNMi Guest Users

Node

A physical or virtual collection of network interfaces that NNMi can pragmatically associate together.

O

OSPF

Open Shortest Path First Protocol

P

PE

Provider Edge router. The Internet Service Provider's router that receives your data on the path to your data's final desination. The Customer Edge (CE) router in your network connects to this PE.

private IP addresses

These are IPv4 addresses that can be reused in home and office local area networks (LANs). Following the standards set by RFC 1918 and RFC 4193 (10.*.*.*, 169.254.*.*, 172.16-31.*.*, and 192.168.*.*)

R

RAMS

HPE Router Analytics Management System

routing prefixes

A network protocol technique used to shorten or filter the amount of required routing information in each packet by declaring a prefix for an entire group of packets. This prefix also indicated the number of bits in the address.

S

SHA

Secure Hash Algorithm

SNMP

Simple Network Management Protocol

SNMP Agent

Simple Network Management Protocol (SNMP) is an Internet-standard protocol used to manage devices on IP networks. The SNMP Agent uses this protocol to report information to authorized management programs.

SOAP

Simple Object Access Protocol

Split Link Aggregation

Link Aggregation with more than two endpoints. Some vendors refer to this as Multi-Chassis Link Aggregation, SLAG, MLAG, or MC-LAG.

U

unique local address

(fd00:: to fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff) A privately routable IPv6 unicast address used only for communication between nodes within your organization. The unique local addresses cannot be routed to the public internet. The address consists of a routing prefix in the fd00:/8 address spaces, assigned locally by your organization. And the full host address might be manually configured or automatically assigned using IPv6 auto-configuration and neighbor discovery.

Unmanaged

Indicates the Management Mode is "Not Managed" or "Out of Service".

USM

User-based Security Model

UUID

Universally Unique Object Identifier, which is unique across all databases.

V

virtual machine

A device that utilizes components from multiple physical devices. Depending on the manufacture's implementation, the virtual machine may be static or dynamic.

VMware

VMware ESX and VMware ESXi software uses SOAP protocol to implement bare-metal hypervisors.

VRRP

Virtual Router Redundancy Protocol

W

WAN Cloud

Layer 3 connectivity between your network and any MPLS networks.

Web Agent

The Web Agent represents a management service running on a device and contains the settings NNMi uses to communicate with the device.