Installing and Configuring Network Performance Insight

IBM
Note
Before using this information and the product it supports, read the information in “Notices” on page 219.

This edition applies to version 1.3.0.0 of IBM® Network Performance Insight® and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2015, 2019.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Contents

Introduction ......................................................................................................................... v
   Intended audience .............................................................................................................. v
   Network Performance Insight architecture ....................................................................... v
   IBM Community ................................................................................................................ viii
   Network Performance Insight technical training ............................................................. ix
   Support information ........................................................................................................... ix
   Conventions used in this publication ................................................................................ ix
   Typeface conventions ....................................................................................................... ix

Chapter 1. System requirements ....................................................................................... 1
   Hardware requirements ....................................................................................................... 1
   Software requirements ........................................................................................................ 3
   Port requirements for a typical installation ......................................................................... 4

Chapter 2. Installing and configuring ............................................................................. 9
   Required microservices in different installation scenarios .................................................. 9
   Scenario 1 - NetFlow data and performance data from Network Performance Insight .......... 11
      Installing ......................................................................................................................... 11
      Configuring ..................................................................................................................... 53
   Scenario 2 - NetFlow data and Performance data from Cacti ............................................ 71
      Installing ......................................................................................................................... 71
      Configuring ..................................................................................................................... 112
   Scenario 3 - NetFlow only data ......................................................................................... 131
      Installing ......................................................................................................................... 131
      Configuring ..................................................................................................................... 165
   Scenario 4 - Add on Performance data to NetFlow only data ........................................... 181
      Installing ......................................................................................................................... 181
      Configuring ..................................................................................................................... 191
   Installing and un安装ing Interim Fix1 ............................................................................... 194
      Applying the Interim Fix1 ............................................................................................... 195
      Uninstalling the Exporter Service .................................................................................. 196
   Installing and un安装ing Interim Fix2 ............................................................................... 196
      Applying the Interim Fix2 ............................................................................................... 196
      Postinstallation tasks ...................................................................................................... 198
   Installing and un安装ing Interim Fix3 ............................................................................... 199
      Applying the Interim Fix3 ............................................................................................... 200
      Updating the Technology Packs .................................................................................... 201
      Rolling back the Interim Fix3 ......................................................................................... 202
   Installing and un安装ing Interim Fix4 ............................................................................... 204
      Applying the Interim Fix4 ............................................................................................... 204
      Rolling back the Interim Fix4 ......................................................................................... 206

Chapter 3. Additional configuration settings ................................................................... 209
   Additional configuration settings for some Network Performance Insight services .......... 209
      Configuring the setting to handle the web request size in Device Dashboard ................... 209
      Moving the Timeseries Service wozk directory to a non-default location ....................... 209
      Enabling additional Flow raw fields collection ................................................................ 210
      Configuring the number of interfaces ............................................................................ 211
      Blacklisting exporter from Remote Flow Collector ......................................................... 212
      Configuring logging ....................................................................................................... 212
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring retention period for timeseries data</td>
<td>213</td>
</tr>
<tr>
<td>Configuring and tuning the IP SLA probes</td>
<td>214</td>
</tr>
<tr>
<td>Reusing an entity after deletion from Cacti</td>
<td>214</td>
</tr>
<tr>
<td>Disabling collection for some metrics in Network Performance Insight</td>
<td>215</td>
</tr>
<tr>
<td>Configuring Ambari for non-root access</td>
<td>216</td>
</tr>
<tr>
<td>Optional: Configuring Ambari server for non-root access</td>
<td>216</td>
</tr>
<tr>
<td>Configuring Network Performance Insight node hosts for non-root access</td>
<td>217</td>
</tr>
</tbody>
</table>

**Notices**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trademarks</td>
<td>220</td>
</tr>
<tr>
<td>Terms and conditions for product documentation</td>
<td>221</td>
</tr>
</tbody>
</table>
Introduction

Use this information to install and configure IBM Network Performance Insight 1.3.

You need to configure the system before you can start using it.

Important: Before you install Network Performance Insight, read the Release Summary that might have late-breaking information specific to your installation.

Network Performance Insight, v1.3 integrates with the following components of IBM Netcool Operations Insight 1.5:

- IBM Tivoli® Network Manager IP Edition for entity metric data collection and discovery
- IBM Tivoli Netcool®/OMNIbus component of IBM Netcool Operations Insight for fault management of network traffic.

Intended audience

The audience who are network administrators or network users who are responsible for installing and using the Network Performance Insight product on an enterprise network.

To install Network Performance Insight successfully, you must have a thorough understanding of the following subjects:

- Network Performance Insight 1.3 system
- Basic principles of network protocols and network management
- NetFlow and Cisco IP SLA concepts
- Linux administration
- Jazz® for Service Management
- IBM Tivoli Network Manager IP Edition
- IBM Tivoli Netcool/OMNIbus

Network Performance Insight architecture

IBM Network Performance Insight is a network performance monitoring system. It offers both real-time and historical trends in network performance and interactive view on the network data that helps in reduced network downtime and optimized network performance.

Network Performance Insight provides IBM Netcool Operations Insight with comprehensive IP network device performance monitoring and session traffic analysis.

The following diagram shows how data is flowing through the various components in Network Performance Insight:
Network Performance Insight services
Network Performance Insight services are running on microservice architecture that has the software application as a suite of independently deployable, small, modular services in which each service runs a unique process and communicates through a well-defined, lightweight mechanism. Currently, Network Performance Insight 1.3 consists of the following microservices:

Foundation services
- DNS
- Event
- Manager
- Storage
- UI

Entity Metric services
- Cacti Collector
- Exporter
- Formula Service
- Entity Analytics
- SNMP Collector
- Threshold
- Tivoli Network Manager Collector
Flow Metric services

- Flow Analytics
- Flow Collector
- SNMP Discovery

For more information about these services, see their respective sections in *IBM Network Performance Insight: Product Overview*.

Network Performance Insight additional components

Some of the additional components that are introduced in Network Performance Insight V1.3 for enhanced functions are described here:

Technology Packs

A set of ready-to-use Technology Packs is provided to perform second-level discovery and polling of resources to collect entity metric data. These Technology Packs can help to collect standard SNMP metrics, and Performance Metric OOTB Device Support metrics.

For more information, see *Installing the Technology Packs* section in *Installing and Configuring IBM Network Performance Insight*.

Network Performance Insight Dashboards

These interactive dashboards are the built-in JSON-based dashboards suite that can display aggregated network data from Network Performance Insight database with the help of REST API calls. It supports a combination of data from multiple data sources.

This feature provides a wide variety of dashboards for Network Operators, Network Engineers, and Network Capacity Planners. These dashboards help in pinpointing the troubled resources and general resource performance. A number of web-based configuration options are available to control the data that is displayed on the dashboards.

For more information, see *Network Performance Insight Dashboards* section in *IBM Network Performance Insight: Product Overview*.

Note: Networks for Operations Insight is a solution extension of Netcool Operations Insight that includes the following components and products:

- Tivoli Network Manager
- Tivoli Netcool Configuration Manager
- Network Performance Insight
- Network Health Dashboard
- Device Dashboard
- Topology Search

Hortonworks Data Platform components

Hortonworks Data Platform (HDP®) can be used to help process and analyze the volume, variety, and velocity of data that continually enters your organization every day. Network Performance Insight is installed as a service extension to the installed HDP® stack.

The features of HDP® that are used in Network Performance Insight:

- HDP®
- Default support for rolling upgrades for Hadoop services
- Support for long-running applications within YARN for enhanced reliability
- Spark in-memory distributed compute engine for dramatic performance increase
- Apache Ambari operational framework. Apache Ambari is an open framework for provisioning, managing, and monitoring Apache Hadoop clusters. Ambari provides an intuitive and easy-to-use
Hadoop management web UI backed by its collection of tools and APIs that simplify the operation of Hadoop clusters.

• Essentially includes the following open source technologies for working with Network Performance Insight:
  – Apache Hadoop
  – Apache Kafka
  – Apache Ambari
  – Apache Spark
  – Apache ZooKeeper

  **Note:** Because Zookeeper requires a majority, it is best to use an odd number of machines. For example, with four machines ZooKeeper can handle the failure of a single machine; if two machines fail, the remaining two machines do not constitute a majority. However, with five machines ZooKeeper can handle the failure of two machines.

**Integrated products**

Products that are integrated with Network Performance Insight 1.3:

**Jazz for Service Management**
Dashboard Application Services Hub provides visualization and dashboard services in Jazz for Service Management. It has a single console for administering IBM products and related applications. Visualization for Network Performance Insight is federated into Dashboard Application Services Hub.

**IBM Tivoli Network Manager IP Edition**
Tivoli Network Manager provides first-level device discovery and polling of some standard SNMP metrics.

**Tivoli Netcool/OMNIbus component of IBM Netcool Operations Insight**
Netcool Operations Insight is powered by the fault management capabilities of IBM Tivoli Netcool/OMNIbus. In Network Performance Insight, V1.3, Tivoli Netcool/OMNIbus is an important part of the solution for monitoring the network threshold violations.

**Related information**
IBM Network Performance Insight on IBM Knowledge Center
Apache Hadoop YARN
IBM Netcool Operations Insight
IBM Tivoli Network Manager IP Edition

**IBM Community**

Connect, learn, and share with professionals and product support technical experts who provide their perspectives and expertise.

Access the IBM Network Performance Insight community. Use IBM Community in the following ways:

• Become involved with transparent development, an ongoing, open engagement between other users and IBM developers of Tivoli products. You can access early designs, sprint demonstrations, product roadmaps, and prerelease code.
• Connect one-on-one with the experts to collaborate and network about Tivoli and the Network and Service Assurance community.
• Read blogs to benefit from the expertise and experience of others.
• Use wikis and forums to collaborate with the broader user community.
Network Performance Insight technical training

For Tivoli technical training information, see the following Network Performance Insight Training website at https://tnpmsupport.persistentsys.com/updated_trainings.

Support information

If you have a problem with your IBM Software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

**Online**

**IBM Support Assistant**
The IBM Support Assistant is a free local software serviceability workbench that helps you resolve questions and problems with IBM Software products. The Support Assistant provides quick access to support-related information and serviceability tools for problem determination. To install the Support Assistant software, go to https://www.ibm.com/software/support/isa.

**Troubleshooting Guide**
For more information about resolving problems, see the problem determination information for this product.

Conventions used in this publication

Several conventions are used in this publication for special terms, actions, commands, and paths that are dependent on your operating system.

**Typeface conventions**

This publication uses the following typeface conventions:

**Bold**
- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as Tip:, and Operating system considerations:)
- Keywords and parameters in text

**Italic**
- Citations (examples: titles of publications, diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a point-to-point line)
- Emphasis of words and letters (words as words example: "Use the word that to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter L.")
- New terms in text (except in a definition list): a view is a frame in a workspace that contains data.
- Variables and values you must provide: ... where myname represents....

**Monospace**
- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
IBM Network Performance Insight 1.3: Installing and Configuring Network Performance Insight
Chapter 1. System requirements

Complete set of requirements for IBM Network Performance Insight 1.3.
Lists the configurations and the supported platforms and components of Network Performance Insight.
For requirements of other integrated products, see the related product documentation for them.

Related information
IBM Netcool Operations Insight: Supported products and components

Hardware requirements

Hardware specifications vary according to the size of your network and server topology that you want to use.

Network Performance Insight has the following minimum requirements that are based on the specific default functions on Linux environment in a stand-alone mode of deployment:

<table>
<thead>
<tr>
<th>Features</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow records collected</td>
<td>20,000 flows per second that are shared between Flow Collector and Remote Flow Collector.</td>
</tr>
</tbody>
</table>
| Records with QoS metrics collected            | • Number of queues = 32  
                                            | • Number of records = 1.92 million                                      |
| Records with ART metrics collected            | 24,000,000                                                            |
| Supported number of Interfaces                | 2000 per Flow Collector Service that is running on each Network Performance Insight node in your cluster for inbound and outbound traffic. |
| Supported IP SLA probes                       | 1800                                                                 |
| Note: If you want to support more IP SLA probes, see “Configuring and tuning the IP SLA probes” on page 214. |
| SNMP metrics collected and stored by Network Performance Insight | 5,000,000 records per hour                                             |
| Note: Includes the following types of metrics: | You can also set up Network Performance Insight to collect SNMP metrics alone and can be targeted to collect 100 million records per hour. For more information about this deployment, see IBM Network Performance Insight V1.3.0 Sizing Guidelines on developerWorks®. |
| • IP SLA                                      |                                                                       |
| • Performance Metric OOTB Device Support metrics |                                                                     |
| SNMP metrics collected by Tivoli Network Manager and stored by Network Performance Insight. | 20,000,000 records per hour                                              |
| SNMP metrics collected by Cacti                | 22,000,000 records per hour for SNMP data, IP SLA data, and Performance Metric OOTB Support data. |

© Copyright IBM Corp. 2015, 2019
Table 1: Factors that determine the Hardware requirements of Network Performance Insight. (continued)

<table>
<thead>
<tr>
<th>Features</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data retention time</td>
<td>• Flow metrics RAW data = 5 Days</td>
</tr>
<tr>
<td></td>
<td>• Flow metrics 1 min aggregated data = 1 Month</td>
</tr>
<tr>
<td></td>
<td>• Flow metrics 30 min aggregated data = 12 Months</td>
</tr>
<tr>
<td></td>
<td>• Flow metrics daily aggregated data = 12 Months</td>
</tr>
<tr>
<td></td>
<td>• DNS data = 3 Months</td>
</tr>
<tr>
<td></td>
<td>• Events data = 6 Weeks</td>
</tr>
<tr>
<td></td>
<td>• Logs = 10 Days</td>
</tr>
<tr>
<td></td>
<td>• Entity metric Threshold state data = 90 days</td>
</tr>
<tr>
<td></td>
<td>• Timeseries data = 365 Days</td>
</tr>
</tbody>
</table>

Note: You can collect 100,000 Flow records per second (FPS) with five Flow Collectors on separate Network Performance Insight nodes where each Flow Collector can handle 20,000 FPS from 2,000 Flow interfaces.

Table 2: Hardware specifications for a cluster with separate Ambari server

<table>
<thead>
<tr>
<th>System</th>
<th>CPU</th>
<th>Memory</th>
<th>Hard disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ambari Server</td>
<td>4 Core CPU</td>
<td>8 GB RAM</td>
<td>100 GB</td>
</tr>
<tr>
<td>Network Performance Insight node</td>
<td>32 Core CPU (16 Physical Cores, 2 threads per CPU)</td>
<td>64 GB RAM</td>
<td>18 TB</td>
</tr>
</tbody>
</table>

Note: CPU is based on Intel Xeon E5-2640 2.00 GHz model.

Table 3: Hardware specifications for a cluster without separate Ambari server

<table>
<thead>
<tr>
<th>System</th>
<th>CPU</th>
<th>Memory</th>
<th>Hard disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ambari Server and Network Performance Insight node A</td>
<td>32 Core CPU (16 Physical Cores, 2 threads per CPU)</td>
<td>64 GB RAM</td>
<td>18 TB</td>
</tr>
<tr>
<td>Network Performance Insight node B</td>
<td>32 Core CPU (16 Physical Cores, 2 threads per CPU)</td>
<td>64 GB RAM</td>
<td>18 TB</td>
</tr>
</tbody>
</table>

Table 4: Hardware specifications for single node cluster

<table>
<thead>
<tr>
<th>System</th>
<th>CPU</th>
<th>Memory</th>
<th>Hard disk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ambari Server and Network Performance Insight node</td>
<td>32 Core CPU (16 Physical Cores, 2 threads per CPU)</td>
<td>64 GB RAM</td>
<td>18 TB</td>
</tr>
</tbody>
</table>

2 IBM Network Performance Insight 1.3: Installing and Configuring Network Performance Insight
**Desktop Resolution**

1366 x 768

**Note:** For best rendering of your dashboards, view them in maximized window mode.

**Sizing guidelines**

For more information about Network Performance Insight 1.3 hardware sizing guidelines, see IBM Network Performance Insight Sizing Guidelines on the IBM Developer community.

**Related information**

Hardware requirements for Tivoli Network Manager 4.2
ITNM 4.2 Calculator for system sizing and polled data storage
Tivoli Netcool/OMNIbus 8.1.0 - Sizing your deployment

**Software requirements**

The supported operating systems, modules, and third-party applications for Network Performance Insight.

Software requirements for Network Performance Insight.

<table>
<thead>
<tr>
<th>Table 5: Supported Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>redhat Linux</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Note:** Enable JavaScript and cookies.

<table>
<thead>
<tr>
<th>Table 6: Supported web browsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browsers</td>
</tr>
<tr>
<td>---------------</td>
</tr>
<tr>
<td>Internet Explorer</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Mozilla Firefox ESR</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Google Chrome</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 7: Prerequisite software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
</tr>
<tr>
<td>-------------------------------</td>
</tr>
<tr>
<td>Hortonworks Data Platform</td>
</tr>
<tr>
<td>Ambari</td>
</tr>
<tr>
<td>Jazz for Service Management</td>
</tr>
<tr>
<td>IBM Tivoli Netcool/OMNIbus</td>
</tr>
<tr>
<td>IBM Tivoli Netcool/OMNIbus Web GUI</td>
</tr>
</tbody>
</table>
Table 7: Prerequisite software (continued)

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Tivoli Network Manager IP Edition</td>
<td>4.2.0.5</td>
</tr>
<tr>
<td><strong>Note:</strong> Required only if you are integrating with Tivoli Network Manager.</td>
<td></td>
</tr>
<tr>
<td>Device Dashboard</td>
<td>1.1.0.2</td>
</tr>
<tr>
<td><strong>Note:</strong> Required only if you are integrating with Tivoli Network Manager.</td>
<td></td>
</tr>
<tr>
<td>Network Health Dashboard</td>
<td>4.2.0.5</td>
</tr>
<tr>
<td><strong>Note:</strong> Required only if you are integrating with Tivoli Network Manager.</td>
<td></td>
</tr>
<tr>
<td>Cacti</td>
<td>V0.8.8 to V1.1.36 for RHEL only</td>
</tr>
<tr>
<td><strong>Note:</strong> Required only if you are integrating with Cacti.</td>
<td></td>
</tr>
</tbody>
</table>

Table 8: Bundled software

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Front End Toolkit</td>
<td>1.5.x</td>
</tr>
<tr>
<td>Open JDK x86_64</td>
<td>1.8.0</td>
</tr>
<tr>
<td>Kairos DB</td>
<td>1.2.0</td>
</tr>
<tr>
<td>Apache Cassandra</td>
<td>3.11.2</td>
</tr>
</tbody>
</table>

Table 9: Supported hypervisors

<table>
<thead>
<tr>
<th>Hypervisors</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux with KVM</td>
<td>RHEL 7.x</td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>5.0</td>
</tr>
<tr>
<td></td>
<td>5.1</td>
</tr>
</tbody>
</table>

Related information

Release details

Supported versions of Web Browsers and mobile OS in DASH

Port requirements for a typical installation

Before you install Network Performance Insight and Hortonworks Data Platform (HDP®) software, open the ports in this table to avoid any conflicts that might exist in your system.
Table 10: Default port numbers for HDP® and Network Performance Insight services.

<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Protocol</th>
<th>Port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ambari Metrics</td>
<td>ams</td>
<td>tcp</td>
<td>6188</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>60200</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6188</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>37266</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>41824</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>45884</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>61181</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>61310</td>
</tr>
<tr>
<td>HDFS</td>
<td>hdfs</td>
<td>tcp</td>
<td>8010</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8020</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50010</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50070</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50075</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>50090</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>58042</td>
</tr>
<tr>
<td>KAFKA</td>
<td>kafka</td>
<td>tcp</td>
<td>6667</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8083</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>39122</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>56969</td>
</tr>
<tr>
<td>Cacti Collector</td>
<td>netcool</td>
<td>tcp</td>
<td>2568</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>28910</td>
</tr>
<tr>
<td>Flow Collector</td>
<td>netcool</td>
<td>tcp</td>
<td>2554</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>14081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>14443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>14910</td>
</tr>
<tr>
<td>Flow Analytics</td>
<td>netcool</td>
<td>tcp</td>
<td>2555</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>15081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>15443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>15910</td>
</tr>
</tbody>
</table>

Note: make sure to open the port numbers for MySQL and SFTP that are specified in Configuring Cacti servers section in Installing and Configuring IBM Network Performance Insight.
<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Protocol</th>
<th>Port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>netcool</td>
<td>tcp</td>
<td>2556</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>16081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>16443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>16910</td>
</tr>
<tr>
<td>Event</td>
<td>netcool</td>
<td>tcp</td>
<td>2557</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>17081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>17443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>17910</td>
</tr>
<tr>
<td>Tivoli® Network Manager</td>
<td>netcool</td>
<td>tcp</td>
<td>2558</td>
</tr>
<tr>
<td>Collector</td>
<td></td>
<td></td>
<td>18081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>18443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>18910</td>
</tr>
<tr>
<td>Timeseries</td>
<td>netcool</td>
<td>tcp</td>
<td>2571</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>31910</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>31081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>31443</td>
</tr>
<tr>
<td>Kairos DB</td>
<td>netcool</td>
<td>tcp</td>
<td>4242</td>
</tr>
<tr>
<td>Kairos DB UI</td>
<td>N/A</td>
<td>tcp</td>
<td>9090</td>
</tr>
<tr>
<td>Cassandra</td>
<td>N/A</td>
<td>tcp</td>
<td>7000</td>
</tr>
<tr>
<td>Cassandra CQL</td>
<td>N/A</td>
<td>tcp</td>
<td>9042</td>
</tr>
<tr>
<td>Manager</td>
<td>netcool</td>
<td>tcp</td>
<td>2560</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>20910</td>
</tr>
<tr>
<td>Threshold</td>
<td>netcool</td>
<td>tcp</td>
<td>2562</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>22081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>22443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>22910</td>
</tr>
<tr>
<td>SNMP Discovery</td>
<td>netcool</td>
<td>tcp</td>
<td>2567</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>27910</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>27081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>27443</td>
</tr>
<tr>
<td>Service</td>
<td>User</td>
<td>Protocol</td>
<td>Port number</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Storage</td>
<td>netcool</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2553</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13910</td>
</tr>
<tr>
<td>UI Service</td>
<td>netcool</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2552</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9010</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9443</td>
</tr>
<tr>
<td>SNMP Collector</td>
<td>netcool</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2563</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>23081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>23443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>23910</td>
</tr>
<tr>
<td>Formula Service</td>
<td>netcool</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2565</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>25081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>25443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>25910</td>
</tr>
<tr>
<td>Remote Flow Collector</td>
<td>netcool</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9092</td>
</tr>
<tr>
<td>Kafka Schema Registry</td>
<td>kafka</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8093</td>
</tr>
<tr>
<td>Ambari Server</td>
<td>root</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8670</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8080</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8440</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8441</td>
</tr>
<tr>
<td>YUM Repository</td>
<td>root</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9091</td>
</tr>
<tr>
<td>YARN</td>
<td>yarn</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7337</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8025</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8030</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8040</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8141</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8042</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8050</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8088</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8188</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10200</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13562</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>45454</td>
</tr>
</tbody>
</table>
Table 10: Default port numbers for HDP® and Network Performance Insight services. (continued)

<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
<th>Protocol</th>
<th>Port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>YARN For Spark Executors</td>
<td>yarn</td>
<td>tcp</td>
<td>46100 - 46600</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>47100 - 47600</td>
</tr>
<tr>
<td>Mapreduce</td>
<td>mapred</td>
<td>tcp</td>
<td>10020</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10033</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>19888</td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>zookeeper</td>
<td>tcp</td>
<td>2182</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2888</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3888</td>
</tr>
<tr>
<td>Flow Exporter</td>
<td></td>
<td>udp</td>
<td>4379</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sctp</td>
<td>4381</td>
</tr>
<tr>
<td>IP SLA Agent and SNMP Agent</td>
<td></td>
<td>udp</td>
<td>161</td>
</tr>
</tbody>
</table>

**Note:** This is different from the UDP port 4379 that must be opened on Flow exporter. This UDP port must be opened on the server where IP SLA agent is available.
Chapter 2. Installing and configuring

Use this information to install and configure IBM Network Performance Insight, Version 1.3.

Installation scenarios:

<table>
<thead>
<tr>
<th>Goal</th>
<th>Installation scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>To collect NetFlow data from Network Performance Insight and Performance data from both Tivoli Network Manager and Network Performance Insight. Discovery for Performance Metric OOTB Device Support resources is handled by Network Performance Insight.</td>
<td>Scenario 1</td>
</tr>
<tr>
<td>NetFlow data from Network Performance Insight. Performance data is discovered and collected by integrating with Cacti.</td>
<td>Scenario 2</td>
</tr>
<tr>
<td>NetFlow data alone from Network Performance Insight.</td>
<td>Scenario 3</td>
</tr>
<tr>
<td>NetFlow data alone from Network Performance Insight. Later, extend Network Performance Insight to collect performance data. Discovery for Performance Metric OOTB Device Support resources is handled by Network Performance Insight.</td>
<td>Scenario 4</td>
</tr>
</tbody>
</table>

- Installation of Network Performance Insight includes these tasks.
- Install prerequisite software.
- Install Network Performance Insight RPM packages.
- Install Hortonworks Data Platform packages.
- Deploy the Ambari agent hosts in your cluster from Ambari web UI.
- Set up Network Performance Insight services on the cluster hosts from Ambari web UI.
- Set up integrations with Dashboard Application Services Hub and Tivoli Network Manager.
- Install Technology Packs.

After the installation is complete according to your installation scenario, configure the system from System Configurations on Dashboard Application Services Hub portal.

Required microservices in different installation scenarios

Microservices that are required in different installation scenarios.
<table>
<thead>
<tr>
<th>Microservice</th>
<th>Scenario 1</th>
<th>Scenario 2</th>
<th>Scenario 3</th>
<th>Scenario 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Foundation Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Event</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td><strong>Exporter</strong></td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td><strong>Note:</strong> This microservice is required only if you are integrating with Predictive Insights.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manager</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Storage</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Timeseries</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>UI</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td><strong>Entity Metric Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cacti Collector</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Formula</td>
<td>YES</td>
<td>Yes</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td><strong>Initially, it is not required. Enable this service to collect performance data.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP Collector</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Threshold</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td><strong>Initially, it is not required. Enable this service after integration with Tivoli Network Manager.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tivoli Network Manager Collector</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td><strong>Initially, it is not required. Enable this service after integration with Tivoli Network Manager.</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Flow Metric Services</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow Analytics</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Flow Collector</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>
Table 12: Microservices applicable for different installation scenarios. (continued)

<table>
<thead>
<tr>
<th>Microservice</th>
<th>Scenario 1</th>
<th>Scenario 2</th>
<th>Scenario 3</th>
<th>Scenario 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Flow Collector</td>
<td>OPTIONAL</td>
<td>OPTIONAL</td>
<td>OPTIONAL</td>
<td>OPTIONAL</td>
</tr>
<tr>
<td>SNMP Discovery</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
</tbody>
</table>

You can disable this service to collect performance data. Only discovery data is collected from Tivoli Network Manager.

Note: For more information about the different installation scenarios, see the Getting Started section.

For more information about these microservices, see Network Performance Insight architecture section in IBM Network Performance Insight: Product Overview.

Scenario 1 - NetFlow data and performance data from Network Performance Insight

In this scenario, Network Performance Insight can be used to extend its functionality to complement Tivoli Network Manager to discover, collect, the performance data. The data can then be stored and rendered on Network Performance Insight Dashboards.

Network discovery for devices is done by Tivoli Network Manager and discovery for resources from within the devices is done by Network Performance Insight.

Network polling for all Performance Metric OOTB Device Support metrics is done by Network Performance Insight itself and the data is stored in the timeseries database.

Some SNMP metrics can continue to be polled by Tivoli Network Manager as usual. Some additional metrics are polled by Network Performance Insight.

Related information
Roadmap for installing and configuring - Scenario1

Installing
The installation information contains the installation prerequisites, instructions for preparing to install, installing, and uninstalling the software based on your scenario.

About this task
Follow the general installation roadmap to complete required and optional steps, according to your needs.

Planning for Network Performance Insight installation
Before you install the product, read the hardware and software requirements.

For more information, see Suggested node and services layout from IBM Network Performance Insight: Product Overview.

Related concepts
“System requirements” on page 1
Complete set of requirements for IBM Network Performance Insight 1.3.

**Downloading and extracting the Network Performance Insight software**

How to get the product distribution?

**Procedure**

1. Download the electronic installation images from the IBM Passport Advantage website to a location of your choice on Ambari server.
   
   For example, /opt/IBM/Installers/NPI that is referred to as `<DIST_DIR>`.

2. Extract the media by using the following commands:

   ```
   tar -zxvf NPI-1.3.0.0.tgz
   tar -zxvf CNVI6ML.tar
   cd CNVI6ML
   tar -zxvf NPI-1.3.0.0.tgz
   ```

   Or, use the following command:

   ```
   gunzip -c NPI-1.3.0.0.tgz | tar -xvf -
   ```

   You can see the following files and folders in the `<DIST_DIR>`:

   - NPI-1.3.0.0/
     - bin
       - agent_setup_nonRoot.sh
       - install.sh
       - installRemoteFlowCollector.sh
       - npi_prereq_check.sh
       - prereq_check.sh
       - setup_cluster_ssh.sh
       - upgrade
         
         This folder contains a lot of script files that are required to upgrade from 1.2.3 to 1.3. It also contains the libraries and script to migrate the SNMP device credentials from the previous environment to the new one.

   - basecamp-installer-tools-1.3.0.0-<build_signature>.noarch.rpm
   - basecamp-repo-1.3.0.0-<build_signature>.noarch.rpm
   - npi-ambari-1.3.0.0-<build_signature>.noarch.rpm
   - npi-repo-1.3.0.0-<build_signature>.noarch.rpm

**Downloading the Hortonworks Data Platform (HDP®)**

Download the HDP® components.

**About this task**

Download the following packages to a single location of your choice on Ambari server. For example, /opt/IBM/Installers/NPI that is referred to as `<DIST_DIR>`.

- HDP-2.6.4.0-centos7-rpm.tar.gz
- HDP-UTILS-1.1.0.22-centos7.tar.gz
- HDP-GPL-2.6.4.0-centos7-rpm.tar.gz
- ambari-2.6.1.0-centos7.tar.gz

**Note:** You do not need to extract these packages.
Procedure
Download the following repositories:

- HDP
- HDP-UTILS
- HDP-GPL
- Ambari

Gathering required information
Collect the following information before you start your installations.

- The fully qualified domain name (FQDN) for each host in your system, and the components that you want to set up on different hosts. The Ambari installation wizard does not support IP addresses. Use hostname -f to check for the FQDN.
  
  An example for FQDN: myserver.ibm.com
- Plan for the base directories for the following components:
  - NameNode data
  - DataNodes data
  - MapReduce data
  - ZooKeeper data
  - Various log, pid, and database files according to your installation type
- Users and groups for Network Performance Insight
  - root
  - netcool
    The netcool user is created during Network Performance Insight installation and all Network Performance Insight services are run as netcool user.
  - smadmin
- Users and groups for HDP®:
  
<table>
<thead>
<tr>
<th>Service</th>
<th>Group</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>hadoop</td>
<td>hdfs</td>
</tr>
<tr>
<td>MapReduce</td>
<td>hadoop</td>
<td>mapred</td>
</tr>
<tr>
<td>YARN</td>
<td>hadoop</td>
<td>yarn</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>hadoop</td>
<td>ams</td>
</tr>
<tr>
<td>Kafka</td>
<td>hadoop</td>
<td>kafka</td>
</tr>
<tr>
<td>Spark</td>
<td>hadoop</td>
<td>spark</td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>hadoop</td>
<td>zookeeper</td>
</tr>
</tbody>
</table>

  Note: Click Admin > Service Accounts to see the user information from your Ambari server.
- Download the Device Dashboard.
  
  Note: The Device Dashboard must be installed after the installation of Network Performance Insight.
- Download the Network Health Dashboard.
  
  See Default users section in Administering IBM Network Performance Insight.
Installing the prerequisite software
Install the prerequisite products before you install Network Performance Insight.

About this task
Install the required products in your IBM Netcool Operations Insight solution according to your entitlement.

You require the following components from IBM Netcool Operations Insight solution to work with Network Performance Insight:

- Tivoli Network Manager core component
- Tivoli Network Manager GUI component
- Device Dashboard
- Network Health Dashboard
- Tivoli Netcool/OMNIbus core component
- Tivoli Netcool/OMNIbus Web GUI component
- Jazz for Service Management
- Tivoli Common Reporting

This component is required only if you have Cognos-based reports from your other product integrations. It is not required to work with Network Performance Insight.

Note: If your Dashboard Application Services Hub that has Tivoli Common Reporting and Network Performance Insight integration fails, see Troubleshooting Dashboard Application Services Hub and Network Performance Insight integration section in Troubleshooting IBM Network Performance Insight

Procedure
1. Install the Operations Management components of Netcool Operations Insight according to your Netcool Operations Insight entitlement.
   For more information, see Quick reference to installing in Netcool Operations Insight documentation on IBM Knowledge Center.
2. Install the Network Management components of Netcool Operations Insight according to your Netcool Operations Insight entitlement.
   For more information, see Quick reference to installing in Netcool Operations Insight documentation on IBM Knowledge Center.

What to do next
Continue with installation of Network Performance Insight.

Activating SLA agent
Activate the SLA agent if you want to discover the SNMP data from IP SLA enabled devices on your Tivoli Network Manager system. You can specify the SLA agent for a full discovery or for a partial discovery.

About this task
SLA agent allows discovery of Service Level Agreement supporting data. Currently, Network Performance Insight retrieves IP SLA data from Cisco, Huawei, and Juniper devices.

Procedure
1. Log in to the Jazz for Service Management portal where Tivoli Network Manager is installed.
2. Click the Discovery icon and select Network Discovery Configuration.
3. From the Domain list, select the required domain.
   For example, NCOMS
**Note:** The Reset button in the **Partial Discovery Agents** window sets the partial agents to match the settings that are defined in the Full Discovery Agents window.

4. Click one of the following tabs, based on your requirements:

**Full Discovery Agents**
- Select agents from this tab to run a full discovery.

**Partial Discovery Agents**
- Select agents from this tab to run a partial discovery.

5. The **Agents** list is displayed, showing all available discovery agents for the selected discovery option.

6. Select the **SLA** check box.

7. Click the save ( ) icon.

**Related information**

**Configuring network discovery**

**Preparing your environment**
Before you run the installation, you must prepare your target environments. Make sure you have installed Jazz for Service Management.

**Setting SSH passwordless login**
You must set up passwordless SSH connections for the Ambari server host to remotely connect to all other Network Performance Insight node hosts that are in the cluster, and also the Dashboard Application Services Hub server without entering the password.

**Procedure**

1. Log in to the system where you want to install Ambari server host as *root* user.
2. On the Ambari server host, run the following command:

   ```
   <DIST_DIR>/NPI-1.3.0.0/bin/setup_cluster_ssh.sh
   ```

   Enter the required details on the prompts.

   **Note:** Always, give fully qualified domain name (FQDN) for the Network Performance Insight node hosts.

   ```
   INFO: Hostname <myserver.ibm.com>
   INFO: USER root
   INFO: User home directory /root
   INFO: Generating public keys pair ...
   Continue to setup remote hosts[Y/n]?y
   Enter remote hostname (FQN): <myserver2.ibm.com>
   INFO: Creating .ssh directory on <myserver2.ibm.com> ...
   root@<myserver2.ibm.com>'s password:
   INFO: Uploading public key to remote host ...
   root@<myserver2.ibm.com> 's password:
   INFO: Upgrading remote host's folder permission ...
   INFO: Verifying ssh passwordless setup ...
   Verified SSH connection
   SSH Passwordless setup to <myserver2.ibm.com> is completed successfully.
   Continue to setup next remote hosts[Y/n]?y
   ```

   If you are configuring the integration of Network Performance Insight with non-root installation of supported Netcool Operations Insight products, run following commands:

   ```
   cd /root/.ssh
   ssh-copy-id -i id_rsa.pub <non-root-user>@<myserver.ibm.com>
   ssh <non-root-user>@<myserver.ibm.com>
   ```
3. Repeat the connection attempt from the Ambari server host to each Network Performance Insight node host to make sure that the Ambari server can connect to each Network Performance Insight node.

Setting Kernel parameters
Setting the ulimit and kernel parameters in Network Performance Insight nodes.

About this task
Run the following steps to set the ulimit and kernel parameters.

Note: You can see the error messages in Ambari start operation stderr and Network Performance Insight log file if the ulimit or the kernel settings are not set correctly during Storage or Flow Collector services start-ups.

Procedure
1. Log in to Network Performance Insight system as root user to change the Linux kernel parameters.
2. Edit the /etc/sysctl.conf file to add or modify the kernel parameters.

```
net.core.rmem_default = 33554432
net.core.rmem_max = 33554432
net.core.netdev_max_backlog = 10000
```

Change the /etc/sysctl.conf to ensure that the values are set on a system start.
   a) Run `sysctl -p` as root user to refresh with the new configuration in the current environment.
3. From the Network Performance Insight node, edit the /etc/security/limits.conf file to add or modify the number of open files to at least 65536 as follows:

```
* - nofile 65536
* - nproc 65536
```
4. Log out and log in the session again as root user for the changes to take effect.
5. Repeat the steps 1 - 4 on all the servers where Network Performance Insight services are installed.

Preparing to run the prerequisite scanner
In addition to Network Performance Insight-specific tasks, complete these common tasks before you start an installation. Network Performance Insight installation script calls the prerequisite scanner that checks if your environment meets these requirements during installation.

Before you begin
Make sure that you have the following operating system packages and their related repos are installed and enabled:

- `libtirpc-devel`
- `redhat-1sb`

Note: These packages are required for Hortonworks Data Platform.

About this task
Use the root user account to perform the following steps.

Procedure
Follow the steps that are specified in Preparing the environment in HDP® documentation.

Related information
HDP Documentation
Configuring Security-Enhanced Linux (SELinux) to support SCTP protocol

By default, the Linux kernel security module (SELinux) runs in enforcing mode. When your RHEL system runs in SELinux enforcing mode, it might deny the SCTP ports.

About this task

This information provides details about how to configure SELinux to enable SCTP support.

Procedure

1. Set SELinux to permissive as root user on all Network Performance Insight node hosts in your cluster as follows:
   ```bash
   setenforce 0
   ```

2. Proceed to install Network Performance Insight system and set up the clusters.

3. Make sure that the Network Performance Insight system is up and running for sometime.
   It might take a while to notice the AVC denied messages in the log file after the Network Performance Insight system is up and running.

4. Check SELinux audit log with this command:
   ```bash
   tail -f /var/log/audit/audit.log
   ```
   You might notice the AVC denied message as follows:
   ```
   type=AVC msg=audit(1508149696.075:38284): avc: denied { getattr } for pid=1412
   comm="npi-akka.actor." laddr=::ffff:10.55.236.146 lport=4381 faddr=::ffff:10.212.6.20
   fport=33859 scontext=system_u:system_r:unconfined_service_t:s0 tcontext=system_u:
   object_r:unlabeled_t:s0 tclass=rawip_socket
   ```

5. Create local policy to enable the access as follows:
   ```bash
   mkdir <workdir>
   cd <workdir>
   grep npi-akka.actor. /var/log/audit/audit.log | audit2allow -M npi
   semodule -i npi.pp
   ```
   The local policy helps in suppressing the AVC denied error message.

6. Optional: You can change the SELinux mode to enforcing as root user as follows:
   ```bash
   setenforce 1
   ```

Related tasks

“Installing Network Performance Insight” on page 17
Install HDP® and Network Performance Insight on a single host or multi-host environments.

Installing Network Performance Insight

Install HDP® and Network Performance Insight on a single host or multi-host environments.

Before you begin

- Ensure that Jazz for Service Management is installed.
- Ensure that the necessary user permissions are in place for all the installation directories.
- Ensure that all the hosts in your cluster are in the same timezone.
- Ensure that you configured your devices to send all the required Flow fields for collection.

For more information, see the following topics:
- Default normalized flow record fields in Network Performance Insight in IBM Network Performance Insight: Product Overview
- Configuring Flexible NetFlow and AVC in IBM Network Performance Insight: References
**About this task**

All the services are distributed under the following default directories:

- /opt/IBM/npi
- /opt/IBM/basecamp

**Procedure**

1. Remove the existing yum cache that might be saved in your system by using the following command as root user:

   ```bash
   rm -rf /var/cache/yum
   ```

2. Start the installation by using the following command as root user on Ambari server:

   ```bash
   cd <DIST_DIR>/NPI_1.3.0.0/bin
   ./install.sh <DIST_DIR>
   ```

   Where `<DIST_DIR>` is the directory where the Network Performance Insight and HDP® software is located. For example, opt/IBM/Installers/NPI.

3. Enter y or n in the prompt based on the prerequisite checker errors.

**Results**

These tasks are completed after the command is run:

- Prerequisite checker script (`prereq_check.sh`) is called to ensure that your environment is set up correctly. Check the `prereq_check_<timestamp>.log` for any errors.
- `/var/www/html/repos` directory is created if it does not exist.
- HDP® files are extracted.
- Network Performance Insight services are set up in `/var/www/html/repos/npi` folder.
- These dependent packages are installed:
  - apr
  - apr-util
  - mailcap
  - postgresql
  - postgresql-libs
  - postgresql-server
- Apache Hypertext Transfer Protocol Server (`httpd`) server is installed.
- `httpd` port is updated to 9091.
- Ambari server is installed and started.
- Ambari server is configured to auto restart Network Performance Insight services and components.
- Related repo files are updated in `/etc/yum.repos.d/` to point to local yum repositories.

You require only the following repositories in `/etc/yum.repos.d/` directory. The rest of the files can be removed to ensure that the cluster setup is not interrupted:

- `ambari.repo`
- `ambari-hdp-1.repo`
- `hdp.repo`
- `hdp-utils.repo`
- `hdp-gpl.repo`
- `npi.repo`
Network Performance Insight service stack is updated to repoinfo.xml file to point to local RPM repositories.

**Note:** If you encounter any prerequisite checker warnings during installation, see “Preparing to run the prerequisite scanner” on page 16.

**What to do next**
You can see the installation output in the following log files that are located in <DIST_DIR>/NPI_1.3.0.0:
- install_<timestamp>.log
- prereq_check_<timestamp>.log

**Setting up Network Performance Insight cluster**
Use the Ambari installation wizard in your browser to complete your installation, configuration, and deployment of Network Performance Insight components and Hadoop components.

**Before you begin**
- Ensure that you have the SSH Private key for root user on Ambari server host.
- Ensure that you have configured the SSH Passwordless login entry to all target hosts.

**Procedure**
1. Open a browser and access the Ambari server dashboard.
   - Use the following default URL: http://<myserver.ibm.com>:8080
   - The default user name is admin, and the default password is admin.
2. Click **Launch Install Wizard** on the Ambari Welcome page.
   - The CLUSTER INSTALL WIZARD opens.
3. Enter a name for the cluster you want to create on the Get Started page and click Next.
   - **Note:** The name cannot contain blank spaces or special characters.
   - For example, npi.
4. On the Select Stack page, select HDP-2.6.NPI stack and select the Use Public Repository option option.
5. Click Next.
6. Complete the following steps on the Install Options page:
   a) List all the nodes that are used in the HDP® cluster on Target Hosts pane.
      - Specify one node per line, as in the following example:

      ```
      node1.abc.com
      node2.abc.com
      node3.abc.com
      ```
      - **Note:** The host name must be the fully qualified domain name (FQDN).
   b) Select **Provide your SSH Private Key to automatically register hosts** on Host Registration Information pane.
      - If the root user installed the Ambari server, the private key file is /<root>/ .ssh/id_rsa.
      - Where <root> is the root user home directory.
      - You have two options to get the private key file:
        1) Browse to the location of the .ssh/id_rsa
        Or
2) Copy the contents of the .ssh/id_rsa file and paste the contents in the SSH key field. Make sure to copy all the content from:

```
-----BEGIN RSA PRIVATE KEY-----
To
-----END RSA PRIVATE KEY-----
```

c) Click Register and Confirm.

7. Ensure that the correct hosts are registered successfully on the Confirm Hosts page.

If you want to change the hosts that are selected, remove the hosts one-by-one by following these steps:

a. Click the check box next to the server to be removed.

b. Click Remove in the Action column.

Note:

- If warnings are found during the check process, click Click here to see the warnings to see the warnings. The Host Checks page identifies any issues with the hosts. For example, a host might have Firewall issues.
- Ignore the process issues that are not related to Network Performance Insight.

c. After you resolve the issues, click Rerun Checks on the Host Checks page. After you have confirmed the hosts, click Next.

8. Select the following services on the Choose Services page:

<table>
<thead>
<tr>
<th>Service</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>2.7.3</td>
<td>Apache Hadoop Distributed File System (HDFS)</td>
</tr>
<tr>
<td>YARN + MapReduce2</td>
<td>2.7.3</td>
<td>Apache Hadoop NextGen MapReduce (YARN)</td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>3.4.6</td>
<td>Centralized service that provides reliable distributed coordination.</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>0.1.0</td>
<td>A system for metric collection that provides storage and retrieval capability for metrics that are collected from the cluster.</td>
</tr>
<tr>
<td>Kafka</td>
<td>0.10.1</td>
<td>A high-throughput messaging system.</td>
</tr>
<tr>
<td>NPI</td>
<td>1.3.0.0</td>
<td>Network Performance Insight cluster service</td>
</tr>
<tr>
<td>NPI Spark Client Scala 2.11</td>
<td>2.0.1</td>
<td>Apache Spark is an engine for large-scale data processing. The Apache Spark client library is compiled on Scala 2.11 and is specific to Network Performance Insight 1.3.</td>
</tr>
</tbody>
</table>

9. Click Next.

10. Assign the master services to hosts in your cluster on the Assign Masters page and click Next.

You can accept the current default assignments. To assign a new host to run services, click the list next to the master node in the left column and select a new host.

11. Click Next.

12. Assign the slave and client components to hosts in your cluster on the Assign Slaves and Clients page.

Click all to assign all the services on your hosts. Or, you can select one or more components next to a selected host.

Important: If you do not need a microservice based on your installation scenario, do not select the check box against the service on a host. For example, do not select Timeseries Exporter Service.
can select this service if you have applied 1.3.0.0-TIV-NPI-IF0001 to integrate with IBM Operations Analytics - Predictive Insights.

13. Click Next.

14. Update the configuration settings for the following services and components on Customize Services pane.

You can see a set of tabs from where you can manage configuration settings for Hadoop and Network Performance Insight components.

Note: Default values are completed automatically when available and they are the recommended values.

- Set up HDFS
- Set up YARN
- Set up Zookeeper
- “Setting up Ambari Metrics” on page 23
- Set up Kafka
- Set up communication with Tivoli Network Manager
- Set up Network Performance Insight
- “Setting up the OMNIbus Standard Input probe” on page 28

15. Click Next after you have reviewed your settings, and completed the configuration of the services.

16. Verify that your settings are correct and click Deploy on the Review page.

17. See the progress of the installation on Install, Start, and Test page.

The progress bar at the top of the page gives the overall status and the main section of the page gives the status for each host. When you click the task, log for a specific task can be displayed.

18. Click Next after the services are installed successfully.

19. Review the completed tasks on the Summary page and click Complete.

Results
It might take a while for Ambari to start all the services. To see the status of all the services in a host, click the Hosts tab in the Ambari server host, and then select a host. You can see the services that are started from the Summary page.

Related concepts
“Required microservices in different installation scenarios” on page 9

Microservices that are required in different installation scenarios.

Setting up HDFS Service
Set properties for the NameNode, SNameNode, DataNodes, and some general and advanced properties. Click the name of the group to expand and collapse the display.

Procedure
Click HDFS > Settings.

Accept all the default values for the following required settings:

Note: These values are prepopulated based on your choices on previous pages.

- NameNode and DataNode directories as /<data1>/hadoop/hdfs/namenode and /<data1>/hadoop/hdfs/data.

  Ensure that the /<data1> directory has sufficient or the recommended disk space.

  Note: Do not set up these directories in /tmp directory.

- NameNode Java heap size: 1 GB
- NameNode server threads: 200
• Minimum replicated blocks: 100%
• DataNode failed disk tolerance: 0
• DataNode maximum Java heap size: 1 GB
• DataNode max data transfer threads: 4098

**Related concepts**
“Hardware requirements” on page 1
Hardware specifications vary according to the size of your network and server topology that you want to use.

“Gathering required information” on page 13
Collect the following information before you start your installations.

**Setting up YARN Service**
YARN decouples resource management and scheduling capabilities from the data processing component. The YARN framework uses a ResourceManager service, a NodeManagers service, and an Application master service.

**Procedure**
1. Click **YARN > Settings**.
2. Configure the required settings as follows:
   • Ensure that the node memory is 15000 MB or more.
   • Ensure that minimum container memory per container is 1024 MB.
   • Ensure that maximum container memory per container is 15000 MB.
   • Set the number of virtual cores to minimum 32.

**Related information**
YARN

**Setting up Zookeeper**
Modify the default settings for Zookeeper from Ambari web UI.

**About this task**
Zookeeper requires a majority. It is best to use an odd number of nodes in your cluster. For example, with four Network Performance Insight nodes, ZooKeeper can handle the failure of a single machine; if two systems fail, the remaining two Network Performance Insight nodes do not constitute a majority. However, with five Network Performance Insight nodes, ZooKeeper can handle the failure of two Network Performance Insight nodes.

If a Network Performance Insight node is removed or added to your cluster, the conf/application.conf file in the UI Service is automatically updated to reflect the correct number of host names with the ZooKeeper Service in the following lines:

• main.zk-url=<host name1>,<host name2>,<host name3>
• messaging.kafka.zk-connect=<host name1>,<host name2>,<host name3>

**Procedure**
1. Click **Zookeeper > Zookeeper Server**.
2. Update the value of **ZooKeeper directory** field as per your environment.
   By default, Ambari might decide on a default directory with sufficient space. For example, /<data1>/hadoop/zookeeper.
   **Note:** Do not set the **ZooKeeper directory** in /tmp directory.
Setting up Kafka
Modify the Kafka Broker log settings from Ambari web UI.

Procedure
1. Click Kafka > Kafka Broker.
2. Update the values for the following fields as per your environment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kafka Broker host</td>
<td>Hosts where the Kafka broker is running.</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>zookeeper.connect</td>
<td>Comma-separated list of connection strings where the ZooKeeper is running in this format: host1:port1,host2:port2</td>
<td>&lt;myserver.ibm.com&gt;:2182</td>
</tr>
<tr>
<td>log.dirs</td>
<td>A comma-separated list of one or more directories in which Kafka data is stored.</td>
<td>/&lt;data&gt;/kafka-logs</td>
</tr>
<tr>
<td>log.roll.hours</td>
<td>A setting that forces Kafka to roll a new log segment even if logs.segment.bytes size is not reached.</td>
<td>168</td>
</tr>
<tr>
<td>log.retention.hours</td>
<td>The number of hours the logs are stored after which they are deleted.</td>
<td>168</td>
</tr>
<tr>
<td>Listeners</td>
<td></td>
<td>PLAINTEXT://localhost:6667</td>
</tr>
</tbody>
</table>

Setting up Ambari Metrics
Modify the default settings for Ambari Metrics from Ambari web UI.

Procedure
1. Click Ambari Metrics > Configs > General.
2. Provide values for the following fields:
   • Grafana Admin Username
   • Grafana Admin Password

   Note: You can retain the default values for the rest of the fields.
Setting up Network Performance Insight services
Set up all the Network Performance Insight services from web-based Ambari user interface. The configuration setting from Ambari UI are written to application.conf files that are located in the conf directory of each microservice.

Procedure
1. Click Services > NPI > NPI Settings.
2. Change the default values in the following fields:
   Make sure that you are in the Configs tab if you are changing these values after the installation is complete.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeseries.datasource</td>
<td>The timeseries data source. Currently, timeseries data is stored on Kairos DB that is integrated with Apache Cassandra.</td>
<td>kairosdb</td>
</tr>
<tr>
<td>timeseries.data.retention</td>
<td>It is the data retention period for timeseries data in days. For more information about this setting, see Configuring retention period for timeseries data section in Installing and Configuring IBM Network Performance Insight.</td>
<td>1 Year</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage.jdbc-service</td>
<td>Used to build the path to storage location with http port for JDBC service.</td>
<td>&lt;myserver.ibm.com&gt;:13081</td>
</tr>
<tr>
<td></td>
<td>Note: This setting is required only if the Storage Service is not installed on all Network Performance Insight node hosts.</td>
<td></td>
</tr>
<tr>
<td>kafka.zk-connect</td>
<td>ZooKeeper URL with Kafka znode. The string {{zookeeper.connect}} is populated with settings in zookeeper.connect.</td>
<td>{{zookeeper.connect}}</td>
</tr>
<tr>
<td></td>
<td>Note: This setting need not be changed.</td>
<td></td>
</tr>
<tr>
<td>kafka.broker-list</td>
<td>List of Kafka brokers. The string {{kafka.broker-list}} is populated with cluster's Kafka hosts and ports.</td>
<td>{{kafka.broker-list}}</td>
</tr>
<tr>
<td></td>
<td>Note: This setting need not be changed.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 16: NPI Manager settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>manager.ambari.user</td>
<td>Ambari user name</td>
<td>admin</td>
</tr>
<tr>
<td>manager.ambari.password</td>
<td>Ambari password</td>
<td>admin</td>
</tr>
</tbody>
</table>

To set or edit the networking time outs for resiliency in DNS resolution:

### Table 17: NPI DNS Service settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns.server.address</td>
<td>DNS Server address. If this value is not specified, it is resolved from the system's /etc/resolv.conf file.</td>
<td></td>
</tr>
<tr>
<td>dns.server.port</td>
<td>DNS Server port</td>
<td>53</td>
</tr>
<tr>
<td>dns.network.initiation.timeout</td>
<td>The maximum amount of time that the DNS Server waits in Disconnected state before it attempts to connect to the DNS Server again.</td>
<td>30 Seconds</td>
</tr>
<tr>
<td>dns.network.connection.timeout</td>
<td>The maximum amount of time that the DNS Server waits in Connecting state for the networking layer to respond that the connection is established.</td>
<td>10 Seconds</td>
</tr>
<tr>
<td>dns.network.acknowledgement.timeout</td>
<td>The maximum amount of time that the DNS Server waits in Waiting state for the networking layer to respond to with an acknowledgment that the outbound packet is written to the operating system or networking buffers.</td>
<td>5 Seconds</td>
</tr>
</tbody>
</table>
Table 17: NPI DNS Service settings. (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns.network.disconnect.timeout</td>
<td>The maximum amount of time that the DNS Server waits in Disconnecting state before it resets and moves to Disconnected state to close the connection.</td>
<td>5 Seconds</td>
</tr>
</tbody>
</table>

Table 18: NPI Web Services settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>https.port</td>
<td>The https port on which Network Performance Insight application console can be accessed.</td>
<td>9443</td>
</tr>
</tbody>
</table>

Setting up the UI Service to render data from Timeseries Service
Use these steps to configure the UI service to retrieve the data from Timeseries Service instead of the Storage Service to render on the Network Performance Insight Dashboards.

About this task
For more information about the Timeseries Service functionality, see Timeseries Service in IBM Network Performance Insight: Product Overview.

Procedure
1. Log in to Ambari server dashboard.
   Use the following default URL:
   http://<myserver.ibm.com>:8080
   The default user name is admin, and the default password is admin.
2. Click Services > NPI > Configs > Advanced.
3. Expand the Advanced npi-env pane and add the following lines in content text area:

   
   ```
   ui.timeseries.rest.url="http://<myserver.ibm.com>:31081"
   ```

   Where, <myserver.ibm.com> is the server where Timeseries Service is available.
4. Click Save to save the configuration.
5. Restart the UI Service as follows:
   a) Click Services > NPI.
   b) Click Service Actions > Restart Uls.

Setting up Flow Collector Service
Use these steps to set up the Flow Collector Service.

Procedure
1. Click Services > NPI > NPI Settings.
2. Change the default values in the following fields:
Make sure that you are in the **Configs** tab if you are changing these values after the installation is complete.

| Table 19: **NPI Components > NPI Flow Collector** settings. |
|--------------------------|--------------------------|--------------------------|
| **Option**               | **Description**          | **Default value**        |
| collector.flow.udp.ports | The UDP ports that the Flow collector listens to for Flow packets. | 4379                     |
|                          | **Note:** Make sure that the flow enabled devices are sending the data to the Flow collector from the same port, 4379. |                         |
| collector.flow.sctp.ports| The SCTP ports that the Flow collector listens to for Flow packets. | 4381                     |
|                          | **Note:** Make sure that the flow enabled devices are sending the data to the Flow collector from the same port, 4381. |                         |
| collector.flow.exporter.blacklist | Comma-separated list of IP addresses in square brackets. The flow data from these exporters in the list is blocked from further processing. | ipAddress1, ipAddress2 |
| collector.flow.art.dscp.whitelist | Comma-separated list of IP DSCP, which are integer values in the range 0 - 255 to enable ART. This setting is to enable the traffic classes that must be monitored. You can further control the applications with the specified traffic classes for ART enablement. See Configuring NBAR section in Installing and Configuring IBM Network Performance Insight. |                         |
|                          | **Note:** To use this option, ensure that ipDiffServCodePoint Flow field is enabled in your ART data template. |                         |
| collector.flow.max-interfaces | The maximum number of interfaces that the collectors collect from Network Performance Insight agent node. | 1000                     |

**Setting up communication with Tivoli Network Manager**

These settings are required for communicating with Tivoli Network Manager

**Procedure**

1. Click **NPI > NOI Core Settings**.
2. Change the default values in the following fields:
Make sure that you are in the **Configs** tab if you are changing these values after the installation is complete.

**Note:**
- Use `db2jcc-4.19.49.jar` JDBC driver that is available in the `/opt/IBM/basecamp/basecamp-connect/libs` folder to connect to IBM DB2 database for Tivoli Network Manager. For more information about compatible drivers, see DB2 JDBC Driver Versions and Downloads.
- Use `ojdbc6-11gR2.jar` JDBC driver that is available in the `/opt/IBM/basecamp/basecamp-connect/libs` folder to connect to Oracle database.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>itnm.platform</td>
<td>The database platform for Tivoli Network Manager. You can select Oracle or DB2 from the list.</td>
<td>DB2 or ORACLE</td>
</tr>
<tr>
<td>itnm.host</td>
<td>Name of the host where Tivoli Network Manager database is installed.</td>
<td><code>&lt;myserver.ibm.com&gt;</code></td>
</tr>
<tr>
<td>itnm.port</td>
<td>The network port to connect to Tivoli Network Manager</td>
<td>50000 1521</td>
</tr>
<tr>
<td>itnm.username</td>
<td>An authorized database user name</td>
<td><code>db2inst1</code></td>
</tr>
<tr>
<td>itnm.password</td>
<td>Password for the authorized database user</td>
<td><code>ncim</code></td>
</tr>
<tr>
<td>itnm.database</td>
<td>Database name</td>
<td><code>NCIM</code></td>
</tr>
<tr>
<td>itnm.probe.import.interval</td>
<td>Time interval for SNMP Collector to check the Tivoli Network Manager system for probe discovery changes.</td>
<td>60</td>
</tr>
<tr>
<td>itnm.kafka.connect.rest.url</td>
<td>Kafka connect REST URL. Specify the hostname where Kafka Connect is installed.</td>
<td><code>http://&lt;myserver.ibm.com&gt;:8083/connectors</code></td>
</tr>
</tbody>
</table>

**What to do next**

Enable integration between Network Performance Insight® and Tivoli Network Manager. For more information, see [Enabling the integration with Network Performance Insight](#).

**Setting up the OMNIbus Standard Input probe**
The Standard Input probe is bundled with Network Performance Insight and is installed along with it.

**About this task**
Most of the configuration settings are done when you install Network Performance Insight. Follow these steps to work with OMNIbus Standard Input probe:
Procedure

1. Configure the host name resolution to resolve omnihost to the actual host name where Tivoli Netcool/OMNIbus is installed. Add an alias entry in the /etc/hosts file on all systems where Network Performance Insight services are installed as follows:

   `<IP_Address> <fully_qualified_host_name> <alias> omnihost`

   For example:

   `192.0.2.0 <myserver.ibm.com> myserver omnihost`

   **Note:** This step must be performed on all Network Performance Insight node hosts where the Event Service is installed.

2. Ensure that you have the following 32-bit RHEL operating system libraries:
   - zlib
   - ncurses
   - bzip2
   - libstdc++

3. Follow the steps in Configuring non-default ObjectServer name section in Installing and Configuring IBM Network Performance Insight if you have a non-default Object Server name.

4. **Note:** Change or add these settings only when recommended by IBM Professional Services.

   Optional: Modify these settings for Tivoli Netcool/OMNIbus Standard Input (STDIN) probe to send events to OMNIbus. Follow these steps:

   a) Click **Services > NPI > Configs > Advanced.**

   b) Expand **Advanced npi-env** section and enter the following lines in the **content** text area:

   ```
   event.netcool.home = "<netcool_installation_directory>"
   event.netcool.omnibus.home = "<omnibus_installation_directory>"
   event.netcool.omnibus.temp = "<temp_directory_for_log_files>"
   event.netcool.omnibus.stdin.args = "<additional_probe_command_line_args>"
   event.netcool.omnibus.stdin.props = "<omnibus_stdin_probe_properties_file_location>"
   event.netcool.omnibus.stdin.rules = "<omnibus-stdin-probe-rules-file_location>"
   ```

   Where

   **Table 21: Configurations for OMNIbus STDIN probe.**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>event.netcool.home</td>
<td>Root installation directory for your Netcool products</td>
<td><code>$NCHOME</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>$NCHOME</code> defaults to <code>/opt/IBM/tivoli/netcool</code>.</td>
</tr>
<tr>
<td>event.netcool.omnibus.home</td>
<td>Root OMNIbus Installation directory</td>
<td><code>$NCHOME/omnibus</code></td>
</tr>
<tr>
<td>event.netcool.omnibus.temp</td>
<td>Temp directory where the log files are located.</td>
<td><code>&lt;NPI_HOME&gt;/npi-event/stdin-probe/omnibus/probes/omnibus/var</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, <code>&lt;NPI_HOME&gt;</code> is <code>opt/IBM/npi</code>.</td>
</tr>
</tbody>
</table>
Table 21: Configurations for OMNIbus STDIN probe. (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>event.netcool.omnibus.stdin.argvs</td>
<td>You can configure the STDIN probe to log at different levels (for example, DEBUG). For more information, see Configuring logging in Troubleshooting IBM Network Performance Insight Anything that is specified in this setting is passed directly on the command line to the STDIN probe at startup.</td>
<td>-messagelevel INFO -messagelevel DEBUG -raw</td>
</tr>
<tr>
<td>event.netcool.omnibus.stdin.props</td>
<td>STDIN probe properties file location</td>
<td>&lt;NPI_HOME&gt;/npi-event/stdin-probe/omnibus/probes/omnibus/stdin.props</td>
</tr>
<tr>
<td>event.netcool.omnibus.stdin.rules</td>
<td>STDIN probe rules file location</td>
<td>&lt;NPI_HOME&gt;/npi-event/stdin-probe/omnibus/probes/omnibus/stdin.rules</td>
</tr>
</tbody>
</table>

See Configuring non-default ObjectServer name section in Installing and Configuring IBM Network Performance Insight.

Setting up integration with Jazz for Service Management

Use this information to set up the federation between Jazz for Service Management and Network Performance Insight to work correctly and to access the web-based visualizations.

Perform these tasks during fresh installation scenarios where you are doing the integration for the first time.

Editing the configuration files

Edit the custom.cfg configuration file according to your environment and use these files in all the required integration tasks for Jazz for Service Management and Network Performance Insight.

About this task

You must edit these files only once before you start the integration.

Procedure

Update the following fields in the file custom.cfg file that are specific to the Dashboard Application Services Hub instance that you want to use for integration:

By default, the custom.cfg file is located in /opt/IBM/basecamp/basecamp-installer-tools/dash-integration folder.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DASH_ENABLE_OPTION</td>
<td>If Dashboard Application Services Hub integration is to be included, specify TRUE. If Dashboard Application Services Hub integration is not required, specify FALSE.</td>
<td>TRUE</td>
</tr>
<tr>
<td>DASH_CONNECTION</td>
<td>Set the FQDN hostname of the Dashboard Application Services Hub server.</td>
<td>root@&lt;myserver.ibm.com&gt; Or &lt;non-root-user&gt;@&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>DASH_SSH_PORT</td>
<td>If non default port number is used, update the SSH port.</td>
<td>22</td>
</tr>
<tr>
<td>WEBSHERE_APP_SERVER_PATH</td>
<td>WebSphere Application Server installation path on Dashboard Application Services Hub server.</td>
<td>/opt/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td>JAZZSM_PATH</td>
<td>Dashboard Application Services Hub installation path.</td>
<td>/opt/IBM/JazzSM</td>
</tr>
<tr>
<td>DASH_USERNAME</td>
<td>Dashboard Application Services Hub administration user.</td>
<td>smadmin</td>
</tr>
<tr>
<td>DASH_PASSWORD</td>
<td>Dashboard Application Services Hub administration user password.</td>
<td>netcool</td>
</tr>
</tbody>
</table>
| KEYSSTORE_OPTION       | USE_DEFAULT_KEY or USE_EXIST_KEY  
**Note:** If you want to reuse your existing key, use the USE_EXIST_KEY.                                                                 | USE_DEFAULT_KEY                         |
<p>| EXIST_KEYSTORE_FILEPATH | Location of the keystore                                                                                                                                                | /tmp/keystore.security                  |
| EXIST_CA_FILEPATH      | CA certificate file location                                                                                                                                                    | /tmp/ca.crt                             |
| KEYSSTORE_PASSWORD     | Password for the keystore                                                                                                                                                    | changeit                                |
| KEY_PASSWORD           | Password for key                                                                                                                                                    | changeit                                |
| ALIAS                  | Alias name                                                                                                                                                                       | npi                                     |
| DOMAIN_NAME            | Domain name                                                                                                           | *.domain.name                           |
| ORG_NAME               | Organization name                                                                                                                                                              | DEMO                                    |
| LOCALITY               | Locality                                                                                                             | DEMO_LOCALITY                           |
| STATE                  | State                                                                                                                 | DEMO_STATE                              |
| COUNTRY                | Country                                                                                                              | &lt;MY&gt;                                   |
| WAS_PROFILE_NAME       | WebSphere Application Server profile for Jazz for Service Management on the target application server.                                                             | JazzSMProfile                           |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS_NODE</td>
<td>The default server node for the WebSphere Application Server profile.</td>
<td>JazzSMNode01</td>
</tr>
<tr>
<td>WAS_SERVER_NAME</td>
<td>Name of the application server that is specified when the application server profile is created.</td>
<td>server1</td>
</tr>
<tr>
<td>WAS_PROFILE_PATH</td>
<td>Location of the application server profile.</td>
<td>/opt/IBM/JazzSM/profile/</td>
</tr>
<tr>
<td>NPI_UI_HOST</td>
<td>Host where the UI service is installed.</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
</tbody>
</table>

**Generating the certificate and keystore files**

Generate the certificate authority (CA) certificates and other keystore files on Ambari server.

**Procedure**

Generate ca.crt key store file by using the following command as root user:

Run the following command in a single line:

```
 cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
 <DASH_INTEGRATION_PATH>/securityKeyTool.sh
 -default=<DASH_INTEGRATION_PATH>/default.cfg
 -custom=<DASH_INTEGRATION_PATH>/custom.cfg
```

Where `<DASH_INTEGRATION_PATH>` is `BASECAMP_INSTALLER_TOOLS_DIR/dash-integration`

For example:

```
 /opt/IBM/basecamp/basecamp-installer-tools/dash-integration/securityKeyTool.sh
 -default=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.cfg
 -custom=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/custom.cfg
```

**What to do next**

Check these log files in the `/tmp` directory for any errors:

- `ambari_npi_key_startup.log`
- `securityKeyTool.<timestamp>.log`
- `genSecurityKey.log`

**Related tasks**

“Installing Network Performance Insight” on page 17  
Install HDP® and Network Performance Insight on a single host or multi-host environments.

**Enabling integration with Jazz for Service Management**

Use this information to enable integration between Network Performance Insight and Dashboard Application Services Hub portal.

**Before you begin**

Make sure that Tivoli Netcool/OMNIbus Object Server is up and running.

**Procedure**

Run the integration script as root user as follows:
By default, the npiDashIntegration.sh script is located in /opt/IBM/basecamp/basecamp-installer-tools/dash-integration folder.

```bash
# <DASH_INTEGRATION_PATH>/npidashintegration.sh
-default=<DASH_INTEGRATION_PATH>/default.cfg
-custom=<DASH_INTEGRATION_PATH>/custom.cfg
```

Where <DASH_INTEGRATION_PATH> is BASECAMP_INSTALLER_TOOLS_DIR/dash-integration.

For example:

```bash
cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/npidashintegration.sh
-default=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.cfg
-custom=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/custom.cfg
```

After the completion of this command, the following tasks are done:

- The dash-integration directory is created at the same level as the WebSphere Application Server based on the value set in the WEBSPHERE_APP_SERVER_PATH field in custom.cfg file. By default, it is /opt/IBM/dash-integration
- The following files are transferred to the dash-integration directory:
  - enableDash.sh
  - signkey
  - eWasAddUsersAndGroups.py
  - priv_key.key
  - ca.crt (Not copied if KEYSTORE_OPTION value is USE_EXIST_KEY)
  - install.User.cfg (Not copied if KEYSTORE_OPTION value is USE_EXIST_KEY)
- The enableDash.sh script is run at the dash-integration directory.
- dashboarduser group that is required to access the Network Performance Insight Dashboards is created.

**What to do next**

Check these log files for any errors:

- `/tmp/npidashintegration.log`
  
  **Note:** This log file is available on the Ambari server from where the Dashboard Application Services Hub integration script is run.

- `/tmp/enableDash.log`
  
  **Note:** This log file is available on server where Dashboard Application Services Hub is running.

**Setting up communication with Jazz for Service Management on Ambari**

These settings are pre-populated on Ambari for communicating with Jazz for Service Management.

**Procedure**

1. Open a browser and access the Ambari server dashboard.
   
   Use the following default URL: `http://<myserver.ibm.com>:8080`
   
   The default user name is admin, and the default password is admin.
2. Click **Services > NPI.**
3. Make sure that you are in the **Configs** tab.
4. Click **NOI Core Settings > NOI Services** and change the values in the following fields:
### Table 22: NOI Core Settings > NOI Services Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>web.auth</td>
<td>Single sign-on mode. Select <strong>DASH</strong> for Jazz for Service Management managed LDAP user repository.</td>
<td>DASH</td>
</tr>
<tr>
<td>security.dash.username</td>
<td>Administrator user name for Jazz for Service Management for security service</td>
<td>smadmin</td>
</tr>
<tr>
<td>security.dash.password</td>
<td>Password for Jazz for Service Management administrator user name</td>
<td>&lt;DASH_password&gt;</td>
</tr>
<tr>
<td>https.keystore.file</td>
<td>Full path for the keystore file that stores the SSL certificate that is used by Network Performance Insight.</td>
<td>/opt/IBM/basecamp/basecamp-ui/conf/security/security.keystore</td>
</tr>
<tr>
<td>https.keystore.password</td>
<td>Password for the SSL keystore that is used by Network Performance Insight.</td>
<td>changeit</td>
</tr>
<tr>
<td>https.key.password</td>
<td>Password for the SSL key that is used by Network Performance Insight.</td>
<td>changeit</td>
</tr>
</tbody>
</table>

5. Click **NPI > Advanced > Advanced npi-auth** and change the default values in the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>security.dash.hostnames</td>
<td>Full DNS name for the Jazz for Service Management server</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>security.dash.port</td>
<td>HTTPS port on which the Jazz for Service Management communicates.</td>
<td>16311</td>
</tr>
</tbody>
</table>

6. Save the configuration.

7. Restart all the Network Performance Insight services as follows:
   a) Click **Services > NPI**.
   b) Select **Restart All** from the **Service Actions** list.

Verification on the systems where Network Performance Insight services are installed:

8. Verify whether the security.keystore file is created in the following location:

   `/opt/IBM/basecamp/basecamp-ui/conf/security`

9. Check that the cacerts file with `webSphereCACert` alias is available in `/opt/IBM/basecamp/basecamp-ui/conf/security` directory by running the following command on all Network Performance Insight nodes:

   ```
   cd /opt/IBM/basecamp/basecamp-jre/java-1.8.0-openjdk.x86_64/jre/bin
   keytool -keystore /opt/IBM/basecamp/basecamp-jre/java-1.8.0-openjdk.x86_64
   /jre/lib/security/cacerts -storepass changeit -list -alias WebSphereCACert
   ```

10. Get the fingerprint from the keystore file, run the following command:

    ```
    keytool -keystore /opt/IBM/basecamp/basecamp-ui/conf/security/
    ```
11. Make sure that the trustedCertEntry certificate fingerprint of the npi_ca is same as the trustedCertEntry certificate fingerprint of the WebSphereCACert that is generated in step 9.

**Configuring the SSL communication for integration**

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

**Before you begin**

Make sure that you have configured the passwordless login as described in Setting SSH passwordless login section in Installing and Configuring IBM Network Performance Insight.

**About this task**

Configure SSL communication on Jazz for Service Management portal after you install Network Performance Insight.

You must configure the SSL one time only. If you are reinstalling or upgrading Network Performance Insight, back up the security.keystore, priv_key.key, which is the private key, and ca.crt, which is the public key if you plan to reuse them.

**Configuring SSL settings on WebSphere Application Server**

Use this information to define Secure Sockets Layer (SSL) configuration properties.

**Procedure**

1. Log in to Dashboard Application Services Hub as administrator user.
2. Select Console Settings > General > WebSphere Administrative Console in the console navigation.
3. Click Launch WebSphere administrative console.
4. Click Security > SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings from the list of Secure Socket Layer (SSL) configurations.
5. Update the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Suggested value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default server certificate alias</td>
<td>If it is not defined earlier, this setting specifies the certificate alias that is used as the identity for this SSL configuration.</td>
<td>netcool</td>
</tr>
<tr>
<td>Default client certificate alias</td>
<td>Specifies the description for a client certificate alias.</td>
<td>netcool</td>
</tr>
</tbody>
</table>

For rest of the settings, you can keep the prepopulated default values.

6. Click OK and save the changes to master configuration.

   **Note:** Make sure to convert all your certificates to use SHA256withRSA in WebSphere Application Server.

7. Verify that the netcool personal certificate is available in SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.
8. Verify that the npi_ca signer certificate is available in SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates.
9. Restart the WebSphere Application Server.
10. Press y in the SSL Signer Prompt window if the signer certificate information is displayed.
Related information
Certificates must be converted to use SHA256withRSA in WebSphere Application Server
Restarting Jazz for Service Management application servers

Adding the signer certificate to your browser
The ca.crt file that is extracted from Jazz for Service Management must be imported to browser’s Trusted CA Certificate store.

About this task
This task must be done on all computers that access Network Performance Insight data for visualization. These steps differ on different browsers. Instructions are provided for Internet Explorer and Firefox.

Procedure
Perform these steps on Jazz for Service Management server.
• Go to the following location where Jazz for Service Management server is installed:
  For example:
  /opt/IBM/dash-integration
• Copy the ca.crt signer certificate that is generated earlier to your local machine.
  Follow these steps on the browser on your local machine that you use to access the visualization dashboards.
  • For Internet Explorer, follow these steps:
    a) Click Tools > Internet Options.
    b) Click Content > Certificates > Trusted Root Certification Authorities.
    c) Click Import.
    d) Browse to the location of the exported ca.crt file.
    e) Click Next.
    f) Select to place the certificates in Trusted Root Certification Authorities option and click Finish.
  • For Firefox, follow these steps:
    a) Click Tools > Options.
    b) Click Advanced > Certificates > View Certificates.
    c) Click Authorities > Import.
    d) Browse to the location of the exported ca.crt file and click Open.
    e) Select all the check boxes on the Downloading Certificate page and click OK.
    f) Click OK to close the window.
  • For Chrome, follow these steps:
    a) Click Settings > Advanced > Manage certificates.
    b) Click Import.
    c) Browse to the location of the exported ca.crt file and click Open.
    d) Select Place all certificates in the following store and click Browse.
    e) Select to place the certificate in Trusted Root Certification Authorities and click OK.
    f) Click Next and Finish.

Related tasks
“Enabling integration with Jazz for Service Management” on page 32
Use this information to enable integration between Network Performance Insight and Dashboard Application Services Hub portal.

**Installing the Technology Packs**

Use this information to install the Technology Pack content that is available within Network Performance Insight installation media. The ready-to-use Technology Pack content includes predefined vendor-specific discovery formulas, collection formulas, metrics, and MIB files that you can use for discovery and polling the devices.

**Before you begin**

Make sure that you have installed, set up your cluster, and configured your Network Performance Insight system successfully.

Make sure that you have Tivoli Network Manager V4.2.0.5 installed.

**About this task**

The following ready-to-use Technology Packs are available from the build after installation in `/opt/IBM/basecamp/basecamp-installer-tools/ootb-packs` directory:

- `network-health-1.0.0.jar`
- `network-health-cisco-1.0.0.jar`
- `network-health-generic-1.0.0.jar`
- `network-health-huawei-1.0.0.jar`
- `network-health-juniper-1.0.0.jar`
- `network-health-extension-1.0.0.jar`

These Technology Packs can be installed in Network Performance Insight system by using the `pack-install.sh` script in `/opt/IBM/basecamp/basecamp-installer-tools/pack-installer`.

**Note:**

- Install the packs in this order:
  - `network-health-1.0.0.jar`
  - `network-health-generic-1.0.0.jar`
  - Vendor-specific packs
- Do not install the `network-health-extension-1.0.0.jar` pack if you are polling the following metrics from Tivoli Network Manager to avoid double-polling of these metrics:
  - `cpuBusy`
  - `ifOutDiscards`
  - `ifInDiscards`
  - `snmpOutBandwidth`
  - `snmpInBandwidth`
  - `ifInErrors`
  - `ifOutErrors`

Each Technology Pack contains the following content:

- Discovery formulas
- Metrics
- Collection formulas
- Vendor-specific and standard MIB files
Procedure

Install the Technology Pack contents by using the following commands:

Run the command on Ambari server and the pack is installed on all Network Performance Insight hosts in your cluster.

```
cd /opt/IBM/basecamp/basecamp-installer-tools/pack-installer
./pack-install.sh install ../ootb-packs/<tech_pack>-1.0.0.jar
```

For example:

```
/opIBM/basecamp/basecamp-installer-tools/pack-installer/pack-install.sh
install ../ootb-packs/network-health-cisco-1.0.0.jar
```

At the prompt, provide the following information:

- **NPI Username**
  By default, it is npiadmin.

- **NPI Password**
  By default, it is netcool.

- Accept the default port number.

The Technology Pack is installed and the content within the pack is distributed to vendor-specific directories as follows:

**Discovery formulas**

```
/opt/IBM/npi/npi-itnm-collector/discovery/
```

The discovery directory has all the collection formulas and their related files.

**Formulas**

```
/opt/IBM/npi/npi-itnm-collector/discovery/content
```

Contains all the discovery formula files that are arranged in separate vendor-specific directories from the custom Technology Pack.

**MIB files**

```
/opt/IBM/npi/npi-itnm-collector/discovery/content/mibs
```

Contains all the MIB files that are arranged in separate directories from the custom Technology Pack.

**Metrics**

```
/opt/IBM/basecamp/basecamp-timeseries/content/metrics
```

The metrics directory has all the metric files.

**Collection formulas**

```
/opt/IBM/npi/npi-formula/content/
```

The content directory has all the collection formulas and their related files.

**Formulas**

```
/opt/IBM/npi/npi-formula/content/formulas
```

Contains all the collection formula files from the custom Technology Pack.

**MIB files**

```
/opt/IBM/npi/npi-formula/content/mibs
```

Contains all the MIB files that are arranged in separate directories from the custom Technology Pack.

**Bindings**

```
/opt/IBM/npi/npi-formula/content/bindings
```

38 IBM Network Performance Insight 1.3: Installing and Configuring Network Performance Insight
Contains all the MIB object class files that are created when the polling is run. Class files are generated by the Formula Service during network polling.

**What to do next**

Check the log files that are available in `/opt/IBM/basecamp/basecamp-installer-tools/pack-installer/logs`. When installation of the pack is successful, you might find the output as follows in the log file:

```
Checking dependencies for pack network-health-juniper-1.0.0.jar
Fetch NPI hosts from Ambari
Found NPI in the <myserver.ibm.com>
Pushing pack file to the <myserver.ibm.com>
Starting network-health-juniper-1.0.0.jar installation process to <myserver.ibm.com>
<myserver.ibm.com> completed
Script completed
```

**Viewing the installed Technology Pack details**

The Pack Details page gives all the information related to the Technology Packs that are installed in your information Network Performance Insight system. This information is retrieved from the CFG.PACK_DETAILS table.

**About this task**

This page gives you the following information related to the installed Technology Packs:

- Technology Pack name
- Technology Pack version
- Timestamp
- Tool version
- Content that includes all the discovery formulas, collection formulas, properties, and metrics within the Technology Pack.

**Procedure**

1. Click **Console Integrations** in the navigation bar, and select **Pack Details** under **System Configuration**.

   You can see the list of built-in Technology pack and other custom Technology Packs that you have installed.

2. Click the **Filter** icon and type an item name or ID in the **Filter by <keyword>** field.

3. Click the **Refresh** icon to refresh the list of items.

**Postinstallation tasks**

Perform these postinstallation tasks after the installation of Network Performance Insight is complete.

- Copy the `conf.key` file from Tivoli Network Manager to Network Performance Insight. This encryption key is used by Network Performance Insight system to get SNMP device credentials (community strings) from Tivoli Network Manager.

```
cd /opt/IBM/npi/npi-itnm-collector/
mkdir -p resources/itnm/security/keys
```

1. Create the following directories if they do not exist by using the following commands:

2. Copy the `conf.key` file from `$NCHOME/etc/security/keys` directory to `/opt/IBM/npi/npi-itnm-collector/resources/itnm/security/keys` directory.
Where NCHOME is the Tivoli Network Manager installation directory. For example, /opt/IBM/netcool/core.

3. Copy the conf.key on all servers where Tivoli Network Manager Collector is installed.

- If you have previously disabled firewall, enable the firewall on all nodes in your cluster. Use these commands:

```bash
systemctl start firewalld.service
systemctl enable firewalld
```

**Verifying the installation**

You can verify the Network Performance Insight 1.3 installation status.

**Before you begin**

Make sure that the flow exporter is configured and sending the flow data to the Collector subsystem.

For more information, see *Configuring Flow devices*.

**Procedure**

1. Verify the installation logs that are available at /tmp directory.

   To list all the log files, run the following command:

   ```bash
   ls -lrt /tmp/*.log
   ```

   You can see the following log files:

   ```
   /tmp/npi-ambari.<timestamp>.log
   /tmp/securityKeyTool.<timestamp>.log
   /tmp/npi-ambari.<timestamp>.log
   /tmp/securityKeyTool.<timestamp>.log
   /tmp/npi-ambari.<timestamp>.log
   /tmp/npi-ambari.<timestamp>.log
   /tmp/host_name_host_cleanup.log
   /tmp/npi-ambari.<timestamp>.log
   /tmp/securityKeyTool.<timestamp>.log
   /tmp/jccdiag.log
   /tmp/npi-ambari.<timestamp>.log
   /tmp/securityKeyTool.<timestamp>.log
   /tmp/cleanup.log
   /tmp/npi-ambari.<timestamp>.log
   /tmp/npi-ambari.<timestamp>.log
   /tmp/startupAmbariServer.log
   /tmp/genSecurityKey.log
   /tmp/securityKeyTool.<timestamp>.log
   /tmp/ambari_npi_key_startup.log
   /tmp/npiDashIntegration.log
   ```

   **Note:** Dashboard Application Services Hub integration script execution log file is located here:

   ```bash
   <DASH_Host>/tmp/enableDash.log
   ```

   For more information about log files, see *Log files in Network Performance Insight* in *Troubleshooting IBM Network Performance Insight*.

2. Run the following yum command to list all the installed packages in the current version:

```bash
# yum list installed | egrep "npi|basecamp"
```

Sample output:
Verifying the status of Standard Input probe

You can verify the status of Tivoli Netcool/OMNibus Standard Input probe that is packaged with Network Performance Insight 1.3.

Before you begin

Ensure that you have installed Network Performance Insight and verified the status as running.

Procedure

1. Check the status of the Event Service by using the following command:

   ```
   <NPI_Home>/basecamp/basecamp-manager/bin
   ./basecamp-manager-cmd status
   ```

2. Run the following command to check the status of Standard Input probe on the node that has the oldest to make sure that the probe is installed successfully:

   ```
   ps -ef | grep nco_p_stdin
   ```

   Check the process ID of the probe that is displayed.

   For more information, see Configuring the OMNibus Standard Input probe to work with Network Performance Insight in Installing and Configuring IBM Network Performance Insight.

Related tasks

“Verifying the installation” on page 40
You can verify the Network Performance Insight 1.3 installation status.

“Setting up the OMNibus Standard Input probe” on page 28
The Standard Input probe is bundled with Network Performance Insight and is installed along with it.

Installation directory structure

Use this information to understand the important directories that are created during installation.

These directories are created in /opt/IBM/ path:

```
basecamp directory contains the following sub directories:

**basecamp-connect**
Contains the Kafka connect script that is called from Ambari to start the service. It also contains the JDBC driver files that are needed to connect to IBM Db2®, Oracle, and for Kafka to connect to Tivoli Network Manager database.

**basecamp-exporter**
Contains the directories and files that are needed to integrate with IBM Operations Analytics - Predictive Insights.

**basecamp-installer-tools**
This directory is available on the Ambari server host only. It contains the following subdirectories:

- **ambari** contains the scripts that are needed for Ambari management.
- **dash-integration** contains scripts:
  - Scripts that are needed for Dashboard Application Services Hub and Network Performance Insight integration.
  - Installing and uninstalling the security services
  - Creating and deleting console integration
The dash-integration directory also has security-service subdirectory that contains the bundled security services software.
- **ootb_packs**
  Contains the ready-to-use Technology Packs that can be installed in Network Performance Insight system for discovery and polling for resources.
- **pack_installer**
  Contains the pack-install.sh script to install the Technology Pack and distribute the content to different Network Performance Insight services.
- **snmp**
  Contains the snmp-scoping.sh script to filter and restrict the devices and resources for network polling.
- **upgrade** contains scripts that are needed for upgrading to 1.3.
  - **credential-migration**
    Contains the snmp-credential-migration.sh script and JAR files for porting the existing Kafka and Flow device credentials to the new environment.

**basecamp-jre**
Contains the Open Java™ SDK that is bundled with Network Performance Insight.

**basecamp-manager**
Contains the directories and files that are needed for the Manager Service to function. It also contains the license files for Network Performance Insight.

**basecamp-schema-registry**
Schema Registry provides a serving layer for your metadata. It stores a versioned history of all schemas, provides multiple compatibility settings, and allows evolution of schemas according to the configured compatibility setting.

**basecamp-storage**
Contains the directories and files that are needed for Network Performance Insight Storage Service to function.

**basecamp-timeseries**
Contains the directories and files that are needed for Timeseries Service to function. It has the following important additional sub directories:
• 3rdParty
  Contains Apache Cassandra and Kairos DB for timeseries data.
• content/metrics
  Contains all the metrics to be collected. Each metric file is identified with an extension .metric. For example, Network-Inbound-Discards-Count.metric.

**basecamp-tools**
  Contains the encryption script, npm-encrypt.sh that can be used to encrypt passwords.

**basecamp-ui**
  Contains the directories and files that are needed for UI Service to function.
  It also contains the following files and directories that are needed for Network Performance Insight Dashboards:
• resources/dashboards
  Contains the following sub directories:
  – json
    Contains all the dashboard JSON files that are successfully parsed and loaded after the installation in good directory and those dashboards that failed to load are in the bad directory. The JSON files that are under process are placed in processing directory.
  – properties
    Contains all the dashboard properties files.
• resources/oed
  Contains the following files and subdirectory:
  – oed.war
    It is the Network Performance Insight Dashboards application engine WAR file.
  – sql
    Contains the SQL files that are related to the dashboards.
• work/oed
  This directory is a symbolic link to basecamp/work/basecamp-ui/oed. Contains the H2 database file as oed.mv.db.

**npi**
  npi directory contains the following sub directories:

  **npi-cacti-collector**
  Contains the directories and files that are needed for Cacti Collector Service to function.
  • resources
    Contains the following files:
    – PODS.zip
    – MIB2.zip
    – CiscoIPSLA.zip
    – cacti_reflector-1.0.0.tgz

  **npi-dns**
  Contains the directories and files that are needed for DNS Service to function.

  **npi-event**
  Contains the directories and files that are needed for Event Service to function. 64-bit STDIN probe is available in this directory and can be supported on Linux, AIX®, and Solaris platforms.
**npi-flow-analytics**
Contains the directories and files that are needed for Analytics Aggregation Service to function.

**npi-flow-collector**
Contains the directories and files that are needed for Flow Collector Service to function.

**npi-formula**
Contains the directories and files that are needed for Formula Service to calculate formulas on the IP SLA metrics based on the data that is collected by the SNMP Collector Service. It also has the collection formulas and their related MIB files for polling the network for Performance Metric OOTB Device Support metrics. It has the following additional directories:

- **content**
  - **bindings**
    Contains the class files for the MIB OBJECT_TYPES that are used in the collection formulas.
  - **formulas**
    Contains all the collection formulas that are used for metric polling.
  - **mibs**
    Contains all the MIB files that are required for your formulas.

**npi-itnm-collector**
Contains the directories and files that are needed for Tivoli Network Manager - Collector Service to function.

- **discovery**
  Contains all the required folders and files for performing the second-level discovery by Network Performance Insight. Typically, devices are discovered by Tivoli Network Manager and all the resource types from those devices are discovered by Network Performance Insight. In Rapid SNMP device onboarding scenario, you can write your own discovery formulas and use them to do SNMP device discovery independent of Tivoli Network Manager.
  - **content**
    Contains the discovery formula files and MIB files that are extracted from technology pack content. The discovery files are arranged according to the vendor. The vendor-specific directories are manually created for organizing the discovery files. All the MIB files that are required for discovery formulas are placed in the /content/mibs directory.
  - **device**
    Contains the sysobjectid.discovery file that is required for discovering the new devices.

**npi-snmp-collector**
Contains the directories and files that are needed for SNMP Collector Service that provides metric polling data from IP SLA enabled SNMP devices to Network Performance Insight.

**npi-snmp-discovery**
Contains the directories and files that are needed for accessing the devices with SNMP credentials to obtain and store the data for enriching the interfaces.

**npi-threshold**
Contains the directories and files that are needed for Threshold Service to function.

Typically, all the microservices have the directory stack as follows:
The logs directory contains a separate log file for each microservice.

**Installing the Device Dashboard**
To use the Device Dashboard on the Dashboard Application Services Hub console, console integration must be configured. When you install the Device Dashboard, this task is automated.

**About this task**
When you install the Device Dashboard that is available for Netcool Operations Insight entitled customers, the following tasks are performed automatically:

- Installs the Security Services if it is not available.

  **Note:** If the Security Services are not installed, you might encounter an Authentication Service client error with the following message ID: CTGES0039E

- Console integrations are configured.

**Procedure**
Install and configure the Device Dashboard.

**Results**
If the connection is successful, the console content is available in the navigation bar of the Dashboard Application Services Hub through the icon.

Log in with npiadmin and netcool credentials and click **Console Settings > Console Integrations** in the navigation bar to see the Network Performance Insight integration.

For troubleshooting console integration, see **Missing console integration icon in Troubleshooting IBM Network Performance Insight**.

**Installing and setting up Remote Flow Collector**
You can optionally install the Flow Collector Service on a remote host as a cluster singleton to keep the collector closer to your data center.

**Before you begin**
Make sure that the server where you are installing the Remote Flow Collector Service has connection to RPM repository in Ambari server host.

**Procedure**
1. Copy the `<DIST_DIR>/NPI_1.3.0.0/bin/installRemoteFlowCollector.sh` file from Ambari server to the host where you want to install Remote Flow Collector.
2. Run the `installRemoteFlowCollector.sh` script as root user as follows:

```
./installRemoteFlowCollector.sh <yum-repo-server> <yum-repo-port>
```
Where:
- `<yum-repo-server>` is the server where the Ambari server is installed.
- `<yum-repo-port>` is the HTTPD port 9091 that is used by Ambari server for components installation in the cluster.

The following components are installed:
- Remote Flow Collector Service
- JRE
- Kafka
- Zookeeper

Zookeeper server and Kafka are set up in the `/usr/iop/current` folder.

3. Set up the connection between the Flow Collector and Remote Flow Collector through Ambari by using the following steps:
   a) Open a browser and access the Ambari server dashboard.
      Use the following default URL:
      http://<myserver.ibm.com>:8080
      
      **Note:** You can use the fully qualified domain name (FQDN) or the IP address of the server.
      The default user name is admin, and the default password is admin.
   b) Click **Services > NPI > Configs > Advanced**.
   c) Expand the **Advanced npi-env** pane and add the following lines in **npi-env template** text area and provide the list of servers where Kafka services are available where Remote Flow Collectors are installed:

```
collector.flow.remote.kafkaBroker = ["<kafka1>:9092", "<kafka2>:9092"]
```

Where:
- `kafka1` and `kafka2` are the host names of the servers that have the Kafka Service running along with remote Flow Collector Service. For example, `<myserver.ibm.com>`.

   **Note:** The ratio between remote and local collectors must be 1:1.
   d) Start the Network Performance Insight services.

4. Optional: To change the port number of the ZooKeeper Service to resolve the port number conflict, perform the following steps:
   a) Update the following properties in `/opt/IBM/npi/npi-remote-flow-collector/conf/application.conf` file:

```
main.zk-url = "localhost:<new_port_number>"
messaging.kafka.zk-connect = "localhost:<new_port_number>"
```

   b) Update the following properties in `/etc/kafka/conf/server.properties` file:

```
zookeeper.connect=localhost:<new_port_number>
```

5. Start the following services:
- Zookeeper
- Kafka
- Remote Flow Collector

6. Optional: To change the port numbers for UDP or SCTP protocols, update the following properties in `/opt/IBM/npi/npi-remote-flow-collector/conf/application.conf`.

```
collector.flow.udp.ports = <new_port_number>
collector.flow.sctp.ports = <new_port_number>
```
7. Start the following services in sequence by using the following command:
   a. Start Zookeeper Service
      
```
      sudo /usr/hdp/current/zookeeper-server/bin/zkServer.sh start
      ```
   b. Start Kafka Service
      
```
      sudo /usr/hdp/current/kafka-broker/bin/kafka start
      ```
   c. Start Remote Flow Collector
      
```
      sudo systemctl start npi-remote-flow-collector
      ```

Results

The Remote Flow Collector is available with the following default configurations in /opt/IBM/npi/npi-remote-flow-collector/conf/application.conf file:

```
collector.flow.udp.ports = [4379]
collector.flow.sctp.ports = [4381]
main.zk-url = "localhost:2181"
messaging.kafka.broker-list = "localhost:9092"
messaging.kafka.zk-connect = "localhost:2181"
```

Note: To restart the Remote Flow Collector Service, see Controlling remote Flow Collector Service in Administering IBM Network Performance Insight.

Check the log files for the collector in npi-remote-flow-collector/logs directory.
Check the log files for Zookeeper and Kafka in the following locations:

- /var/log/zookeeper
- /var/log/kafka

Installing and setting up Remote SNMP Collector

You can optionally install the SNMP Collector on a separate node to enhance the collection of SNMP metrics. You can set up Network Performance Insight to collect SNMP metrics alone and can be targeted to collect 100 million records per hour.

Before you begin

Compress the following microservices from any of the Network Performance Insight nodes in your cluster:

- /opt/IBM/npi/npi-snmp-collector
- /opt/IBM/npi/npi-formula
- /opt/IBM/basecamp/basecamp-jre

Use the following commands to create the compressed files for these microservices:

```
cd /opt/IBM/npi
    tar -cvf <npi.tar> npi-snmp-collector npi-formula

cd /opt/IBM/basecamp
    tar -cvf <basecamp.tar> basecamp-jre
```

Procedure

1. On a separate server where you want to install the SNMP Collector as cluster singleton, copy the following archived files:

- <npi.tar>
- <basecamp.tar>
2. Extract the archived files by using the following commands:

```
tar -xvf <npi.tar>
tar -xvf <basecamp.tar>
```

3. Edit the application.conf files in both npi-snmp-collector microservice as follows:

```
cd /opt/IBM/npi/npi-snmp-collector/conf
vi application.conf
```

Update the following lines with the host name of any Network Performance Insight node in your cluster:

**Note:** You can use the fully qualified domain name (FQDN) or the IP address of the server.

```
ams.collector.endpoint.hostname = "<npi_node_server>"
ams.collector.host = "<npi_node_server>"
ams.collector.port = 6188
main.zk-url = "<npi_node_server>:6188"
messaging.kafka.broker-list = "<npi_node_server>:6667"
messaging.kafka.zk-connect = "<npi_node_server>:2182"
storage.jdbc-service = "<npi_node_server>:13081"
storage.schema-registry.urls = "http://<npi_node_server>:8093"
timeseries-service.hosts = [ "<npi_node_server>" ]
timeseries-service.port = 31081
```

Set SNMP scoping as follows:

```
snmp.consumer-group.suffix = "<local_server>"
```

Where `<local_server>` is the IP address of the fully qualified domain name (FQDN) of the server where SNMP Collector is installed.

4. Edit the application.conf files in both npi-formula microservice as follows:

```
cd /opt/IBM/npi/npi-formula/conf
vi application.conf
```

Update the following lines with the host name of any Network Performance Insight node in your cluster:

**Note:** You can use the fully qualified domain name (FQDN) or the IP address of the server.

```
ams.collector.endpoint.hostname = "<npi_node_server>"
ams.collector.host = "<npi_node_server>"
ams.collector.port = 6188
main.zk-url = "<npi_node_server>:2182"
messaging.kafka.broker-list = "<npi_node_server>:6667"
messaging.kafka.zk-connect = "<npi_node_server>:2182"
storage.jdbc-service = "<npi_node_server>:13081"
storage.schema-registry.urls = "http://<npi_node_server>:8093"
timeseries-service.hosts = [ "<npi_node_server>" ]
timeseries-service.port = 31081
```

Set SNMP scoping as follows:

```
formula.entity-scope = "True"
```

Where `<local_server>` is the IP address of the fully qualified domain name (FQDN) of the server where SNMP Collector is installed.
Where `<local_server>` is the IP address of the fully qualified domain name (FQDN) of the server where SNMP Collector is installed.

5. Start the microservices with the following commands:

```bash
nohup bin/npi-snmp-collector &
nohup bin/npi-formula &
```

Uninstalling Network Performance Insight
Uninstall Network Performance Insight and the related software from the system.

**Before you begin**
Before you uninstall, back up the following contents:

- Manually, back up the `/opt/IBM/basecamp/basecamp-installer-tools` folder in the Ambari Server host to save the previous configuration.
- Make sure to back up the following files from `/opt/IBM/basecamp/basecamp-installer-tools/dash-integration` directory if you plan to reuse them:
  - `security.keystore`
  - `priv_key.key` - private key
  - `ca.crt` - public key

**About this task**
Uninstall the following components that you installed:

- Hortonworks Data Platform, including YARN, HDFS, and Zookeeper services.
- Ambari agents that contain Network Operations Insight instances.
- Ambari server

To uninstall all these components, follow these steps:

**Related information**
- Removing Tivoli Netcool/OMNIbus
- Uninstalling Network Manager
- Uninstalling Jazz for Service Management and related software

**Listing working directories**
Network Performance Insight related components working directories can reside in the recommended locations or in the customized locations.

**About this task**
List down the working directories before you run the uninstallation scripts to make sure that they are removed.

**Note:** Manually, remove these working directories after the uninstallation scripts are run.

**Procedure**
1. Log in to Ambari server host as follows:
   ```bash
   http://<ambari_server_host>:8080
   ```
2. Click **Services** and select the specific service and click the **Configs** tab.
3. Note down the following directories for the services and components:

<table>
<thead>
<tr>
<th>Services</th>
<th>Ambari Component directory</th>
<th>Example installation path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kafka</td>
<td>Kafka &gt; Configs &gt; Kafka Broker &gt; logdirs</td>
<td>&lt;data&gt;/kafka-logs</td>
</tr>
</tbody>
</table>
### Services

<table>
<thead>
<tr>
<th>Services</th>
<th>Ambari Component directory</th>
<th>Example installation path</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>HDFS &gt; Configs &gt; Settings &gt; NameNode</td>
<td>&lt;data&gt;/hadoop/hdfs/namenode</td>
</tr>
<tr>
<td></td>
<td>HDFS &gt; Configs &gt; Settings &gt; DataNode</td>
<td>&lt;data&gt;/hadoop/hdfs/datanode</td>
</tr>
<tr>
<td></td>
<td>HDFS &gt; Configs &gt; Advanced &gt; Secondary NameNode &gt; SecondaryNameNode</td>
<td>&lt;data&gt;/hadoop/hdfs/namesecondary</td>
</tr>
<tr>
<td></td>
<td>Checkpoint directories</td>
<td></td>
</tr>
<tr>
<td>YARN</td>
<td>YARN &gt; Configs &gt; Advanced &gt; Application Timeline Server &gt; yarn.timeline-service.leveldb-timeline-store.path</td>
<td>&lt;data&gt;/var/log/hadoop-yarn/timeline</td>
</tr>
<tr>
<td>YARN</td>
<td>YARN &gt; Configs &gt; Advanced &gt; Advanced yarn-site &gt; yarn.timeline-service.leveldb-state-store.path</td>
<td>&lt;data&gt;/hadoop/yarn/timeline</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>Ambari Metrics &gt; Configs &gt; Advanced ams-hbase-site &gt; hbase.rootdir</td>
<td>&lt;data&gt;/var/lib/ambari-metrics-collector/hbase</td>
</tr>
<tr>
<td></td>
<td>Ambari Metrics &gt; Configs &gt; Advanced ams-hbase-site &gt; hbase.tmp.dir</td>
<td>/var/lib/ambari-metrics-collector/hbase-tmp</td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>ZooKeeper &gt; Configs &gt; ZooKeeper Server &gt; ZooKeeper directory</td>
<td>&lt;data&gt;/hadoop/zookeeper</td>
</tr>
</tbody>
</table>

**Note:** <data> is the full directory path where you have set up all the services.

#### Uninstalling Network Performance Insight node

Run the host_cleanup.sh script to uninstall the Ambari Server hosts and Network Performance Insight node hosts.

**Before you begin**

- Stop all the services for each host from Ambari.
- Back up your data.

**Procedure**

1. Copy the host_cleanup.sh script from `/opt/IBM/basecamp/basecamp-installer-tools/ambari/host_cleanup.sh` to the Network Performance Insight Nodes that you want to uninstall. For example, `/tmp/host_cleanup.sh`.
2. Run the script as root user as follows:

```bash
cd /tmp
./host_cleanup.sh
```

The host_cleanup.sh script performs the following functions:

- Checks the user who is running the script is root or not
- Checks for the HostCleanup.ini file
• Stops the Ambari Server and the Network Performance Insight node, if they are still running.
• Stops the Linux processes that are started by a list of service users. The users are defined in the HostCleanup.ini file. You can also specify a list of Linux processes to be stopped.
• Removes the PRM packages that are listed in the HostCleanup.ini file.
• Removes the Network Performance Insight packages and working folders.
• Removes the service users that are listed in the HostCleanup.ini file.
• Deletes directories, symbolic links, and files that are listed in the HostCleanup.ini file.
• Deletes repositories that are defined in the HostCleanup.ini file.

Related information
Cleaning up nodes before reinstalling software

Uninstalling Ambari server host
Use the cleanup scripts to remove the Ambari server host, which is the master node.

Procedure
1. Move the uninstallation scripts from /opt/IBM/basecamp/basecamp-installer-tools/ambari to /tmp directory.
2. Run the cleanup scripts as root user on the Ambari server in the following order:
   ```shell
   /tmp/host_cleanup.sh
   /tmp/cleanup.sh
   ```
   Note: Ignore the error messages from cleanup.sh as most of the uninstallation is done by the host_cleanup.sh script.
   Ambari Server and all the Network Performance Insight microservices are removed.
3. Remove all the working directories that are listed previously.
   For more information, see “Listing working directories” on page 49.

Removing Dashboard Application Services Hub integration
Use this information to remove the directories and settings that are related to Dashboard Application Services Hub integration.

Procedure
1. Log in to Dashboard Application Services Hub as administrator user.
2. In the navigation pane, click Console Settings > Websphere Administrative Console and click Launch Websphere administrative console.
3. Click Security > SSL certificate and key management.
4. Under Related items on the right, click SSL configurations > NodeDefaultSSLSettings.
5. Change the Default server certificate alias and Default client certificate alias to Default.
6. Click OK and save the changes to master configuration.
7. Click Key stores and certificates > NodeDefaultKeyStore > Personal certificates and remove the netcool certificate.
8. Save the changes to master configuration.
9. Click Key stores and certificates > NodeDefaultTrustStore > Signer certificates and remove the npi-ca certificate.
10. Save the changes to master configuration.
11. Restart WebSphere Application Server.
12. Remove the /opt/IBM/dash-integration directory.
**Uninstalling Remote Flow Collector**

Use these steps to uninstall all the Remote Flow Collectors.

**Before you begin**

Stop the Remote Flow Collector Service. For more information, see *Stopping the Remote Flow Collector associated services* in *Administering IBM Network Performance Insight*.

**Procedure**

Run these manual commands on the servers where you set up the Remote Flow Collectors to erase the packages:

```bash
yum erase -y npi-remote-flow-collector
dm erase -y zookeeper_2_6_4_0_91
dm erase -y hdp-select
dm erase -y ranger_2_6_4_0_91-kafka-plugin
dm erase -y basecamp-jre
```

**What to do next**

After the uninstallation is complete, perform the following steps:

- Remove the `.repo` files from `/etc/yum.repos.d` directory if they exist:
  - `npi.repo`
  - `hdp.repo`

- Remove the following folders:
  - `/data/kafka-logs`
  - `/var/log/zookeeper`
  - `/var/lib/zookeeper`

**Troubleshooting installation**

Problems that might occur during an installation and how to resolve them.

**About this task**

For all troubleshooting issues in installation of Network Performance Insight, see *Troubleshooting installation and uninstallation* section in *Troubleshooting Network Performance Insight*.

For all troubleshooting issues in deploying Ambari clusters, see *Troubleshooting Ambari server* section in *Troubleshooting Network Performance Insight*.

For all troubleshooting issues in integration of Network Performance Insight, see *Troubleshooting integration with Tivoli Netcool/OMNibus* section in *Troubleshooting Network Performance Insight*.
You can configure IBM Network Performance Insight, Version 1.3 and its integration services through user interface console and command line interface. You can also administer and manage application security and single sign-on from Dashboard Application Services Hub portal.

About this task
Most of the configurations are performed through web-based UI on Ambari server. For Network Performance Insight to be fully functional and accessible on Jazz for Service Management, you must perform the following configurations:

- Configure Network Performance Insight system.
- Configure the required Ambari services and Network Performance Insight services from Ambari web interface.
- Configure integration with Tivoli Netcool/OMNIbus.
- Configure integration with Tivoli Network Manager.

Configuring Network Performance Insight system environment
Use this information to configure your Network Performance Insight system that is integrated with Dashboard Application Services Hub from the graphical user interface.

You must do some general system configuration and tuning for optimizing the system performance. During implementation, you must configure the application options to meet your requirements.

You can view the current settings, modify the settings, add new, or delete an existing configuration item. These configuration settings are stored in the database and can be retrieved from the CFG schema tables. Each configuration setting is associated with a separate widget on Dashboard Application Services Hub UI.

The Network Performance Insight dashboards are pre-configured with working sets of default configurations that are created right after installation. A broad range of functions in Network Performance Insight can be administratively configured.

You can configure the following items from system configuration:

- NBAR
- Autonomous System
- Domain names
- Entity Thresholds
- Flow Aggregations
- Flow IP Grouping
- Interfaces
- Polling Configuration
- Resource Type
- Retention profiles
- Sites
- Thresholds
- Type of Service

For information about troubleshooting system configurations, see Troubleshooting IBM Network Performance Insight.
**Logging in to the Dashboard Application Services Hub portal**

Depending upon your organization’s deployment, you can access the reporting interface through Dashboard Application Services Hub.

**Procedure**

- Access the reporting interface from Dashboard Application Services Hub as follows:
  
  a) Open a web browser and enter the following URL for the Jazz™ for Service Management UI and reporting server:
     
     `https://host.domain:port/DASH_context_root`
     
     For example: `https://<myserver.ibm.com>:16311/ibm/console`
     
     Where:
     
     - `host.domain` is the fully qualified host name or IP address of the Jazz for Service Management UI and reporting server.
     - `port` is the secure HTTP port number that was specified during installation. The default value is 16311.
     - `/DASH_context_root` is the context root for the console that was specified during installation. The default value is `/ibm/console`.
  
  b) Enter the user ID and password in the Dashboard Application Services Hub login page. Click Log in.
     
     For example, npiadmin/netcool
     
     The Dashboard Application Services Hub Welcome page opens.

  c) Click Console Integration icon on the navigation bar and select the dashboard of your choice under System Configuration.

**Configuring Autonomous System**

To assign a routing domain for your network, configure the Autonomous System that uses Border Gateway Protocol (BGP). BGP shares routing information with other autonomous systems with the help of a globally unique 16-digit identification number that is known as the AS number (ASN). AS numbers are assigned by the Internet Assigned Numbers Authority (IANA).

**About this task**

The Autonomous Systems information that is configured and stored is displayed in the Top Autonomous System Conversations view in Traffic Details dashboard.

**Procedure**

1. Click Console Integrations in the navigation bar, and select Autonomous System under System Configuration.
   
   Add an Autonomous System.
   
2. Click New icon and enter the Autonomous System information as follows:
   
   **Id**
   
   Mandatory field that represents a unique ASN.
**Note:** Autonomous System numbers one to 64511 are available by IANA/ARIN (IANA/American Registry for Internet Numbers) for global use. The 64512 - 65535 series is reserved for private and reserved purposes.

**Name**
Name of the Autonomous System.

**Note:** Autonomous System numbers, one to 64511 have predefined names for global use. The 64512 - 65535 series is reserved for private and reserved purposes.

**Country**
Country to which the specific network routing domain belongs to.

**Is public**
Whether network domain is a private use ASN or with in the public AS range.

Edit an Autonomous System.

3. Select a row from the table and click the **Edit** icon to change the information for the Autonomous System.

Delete an Autonomous System.

4. Select an entry from the table and click the **Delete** icon to delete an entry that is not needed. Common tasks that are applicable for most of the configuration settings.

5. Click the **Filter** icon and type an item name or ID in the **Filter by <keyword>** field.

6. Click the **Refresh** icon to refresh the list of items.

7. Select a number in the lower-right corner to change the number of items to be displayed in the table.

8. Go to a specific page by using the arrows in the bottom of the page.

9. Navigate to a specific page from the page numbers at the bottom of the page.

**Related information**
List of Autonomous Numbers

**Configuring domain names**
Domain name is an identification of a unique computer system on the internet that is universally agreed by web servers and online administrations and offers all related destination information. To access an organization’s web-based facilities, website users must identify the exact domain name. A complete domain name consists of one or more subdomain names and one top-level domain name that is separated by dots (.). For example, `<myserver.ibm.com>` is a complete domain name.

**About this task**
Configuring domain names helps in handling the frequently used, well-known domain names of your organization.

You can add a set of pre-defined domain names in Network Performance Insight system, such as `youtube.com`, `facebook.com`, `yahoo.com`, and so on.

With these pre-defined configurations, the DNS performs forward resolution to get a list of IP addresses for the domain names. When a flow record is received, DNS service in Network Performance Insight tries to match the source IP and destination IP with the resolved IP address and maps it to the domain name. The traffic detail page then displays as the configured domain name instead of a string of IP.

Without these pre-defined configurations, the aggregation takes the IP address and performs DNS reserve resolution, which might not populate a friendly domain name.

You can configure domain names to be resolved for IP address mapping.
Note: Database tables store specific types of data and can be categorized into the configuration, event, aggregation, and flow data in database tables. The database table for configuration displays the data for domain names.

**Procedure**

1. Log in to Jazz for Service Management server.

2. Click **Console Integrations** in the navigation bar, and select **Domain Names** under **System Configuration**.
   
   Add a domain name.

3. Click **New** icon and enter the domain name to create a new domain name to be resolved.
   
   Delete a domain name.

4. Select an entry from the table and click **icon to delete an entry that is not needed.**
   
   This option helps you to delete an entry that has a typographical error.
   
   a) Delete any entry that is no longer needed.
   
   b) Delete a wrong entry and create a new entry.

   **Note:** The domain names that start or end with "." or "-" are not accepted.

5. Click **OK** to save the settings.

**What to do next**

You can repeat the same process to configure commonly used domain names as needed.

**Configuring Entity thresholds**

A threshold is a value that is compared against a metric to determine whether the metric violates a specific constraint. Entity thresholds provide a mechanism for identifying anomalies in performance metrics that is polled from Network Performance Insight and Cacti.

**About this task**

Events can be created when a performance metric exceeds a certain user-defined value. For example, when the response time for a monitored service is too high, or when bandwidth utilization exceeds a certain amount.

The threshold violations and their values are user-defined and not dynamically generated. You can configure entity thresholds for each of the performance metrics that are collected and stored in Network Performance Insight database.

**Important:** Entity Threshold configuration is required in the following installation scenarios:

- For the metrics collected by Network Performance Insight in “**Scenario 1 - NetFlow data and performance data from Network Performance Insight**” on page 11.

  **Note:** To configure thresholds for standard SNMP metrics that is collected by Tivoli Network Manager, see Defining anomaly thresholds.

- For all the performance metrics collected by “**Scenario 2 - NetFlow data and Performance data from Cacti**” on page 71.

**Procedure**

1. Click **Console Integrations** in the navigation bar and select **Entity Thresholds** under **System Configuration**.
You can see the Entity Thresholds table.
2. Select the threshold that you want to edit.

3. Click the **Edit** icon.
   
   The **Edit Entity Threshold** window displays the configuration details.

4. Modify the settings for the threshold as needed.
   
   a) Select the limit type from the **Limit Type** list to **Over**, **Under**, or **Band**.
      
      **Over**
      
      Detect violations when the metric value exceeds the set threshold value.
      
      **Under**
      
      Detect violations when the metric value falls short of the set threshold value.
      
      **Band**
      
      Detect violations the metric value goes outside a range (or band) between two set threshold values.
   
   b) Enter a value in the **Upper Limit** field for the metric to trigger a threshold violation.
   
   c) Enter a value in the **Lower Limit** field for the metric to trigger a threshold violation.
   
   d) Enter the number of events for triggering the threshold in the **Consecutive Occurrences** field.
   
   e) Select the **Enabled** check box to enable a threshold on the interface.
   
   f) Click **Ok** to save the modification.

   **Note:** When the threshold limit is violated, it displays the severity as **Critical**.

   For more information, see **Threshold violation** in *IBM Network Performance Insight: Product Overview*

5. You can perform the following tasks in the **Actions** column:
   
   a) Click **Edit** to edit or configure the selected threshold.
   
   b) Click **Enable** or **Disable** to enable or disable a metric to detect its threshold violation states.

**Results**

Any metric that is violating the configured threshold value is reported in the Event Viewer.

**What to do next**

You must repeat the same process to enable and configure thresholds for every metric as needed.

**Related tasks**

“**Configuring Flow thresholds**” on page 67

Thresholds provide a mechanism for identifying anomalies in flow and metric data that is polled from Tivoli Network Manager. Threshold is a metric value that is compared against a value to determine whether an interface violated a specific constraint. The threshold violations and their values are user-defined and not dynamically generated. These threshold values are defined per interface in each direction.

**Configuring Flow aggregations**

User configurable Flow aggregations increase the performance of NPI system by optimizing the CPU utilization and reduce the I/O demands on database. It helps in Top Talker optimizations. Top N Talkers support feature helps you analyze large amount of data that Flexible NetFlow captures from the network traffic. You can filter, aggregate, and sort the data for display. When you are sorting and displaying the data in the NetFlow cache, you can limit the display output to a specific number of entries with the highest values (Top N Talkers) for traffic volume, packet counters, and so on.
**About this task**

By default, some of the aggregations are enabled and the others are user configurable. Some of these aggregations require other related configurations to be enabled. The following table provides information about all the available user configurable aggregations:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Type of aggregation</th>
<th>Enabled by default</th>
<th>Required additional configuration setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Top Applications</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Applications with Source ToS</td>
<td>No</td>
<td>See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td>Conversations</td>
<td>Top Conversations</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Conversations with Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Conversations with ToS</td>
<td>No</td>
<td>See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td>Destinations</td>
<td>Top Destinations</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Destinations with Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>Type of aggregation</td>
<td>Enabled by default</td>
<td>Required additional configuration setting</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------</td>
<td>--------------------</td>
<td>--------------------------------------------</td>
</tr>
</tbody>
</table>
| Top IP Group Conversations with Source ToS | No                  | • See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.  
• See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight. |
| Top Destination IP Groups with Source ToS | No                  | • See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.  
• See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight. |
<table>
<thead>
<tr>
<th>Resource</th>
<th>Type of aggregation</th>
<th>Enabled by default</th>
<th>Required additional configuration setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Source IP Groups</td>
<td>No</td>
<td></td>
<td>See Configuring Autonomous System section in Installing and Configuring IBM Network Performance Insight</td>
</tr>
<tr>
<td>with Protocol</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top Source IP Groups</td>
<td>No</td>
<td></td>
<td>• See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td>with Source ToS</td>
<td></td>
<td></td>
<td>• See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td>Top Destination IP Groups</td>
<td>No</td>
<td></td>
<td>See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td>Quality of Service</td>
<td>No</td>
<td></td>
<td>QoS fields must be configured on your devices. See Configuring Flexible NetFlow and AVC section in Configuring Flow devices.</td>
</tr>
<tr>
<td>Top QoS Hierarchies</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>with Queue ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocols</td>
<td>Top Protocols</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Protocols with Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Protocols with Conversation</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Protocols with Destination IP</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>Type of aggregation</td>
<td>Enabled by default</td>
<td>Required additional configuration setting</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Top Protocols with Source IP</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sources</td>
<td>Top Sources</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Sources with Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Type of Service</td>
<td>Top Source ToS</td>
<td>No</td>
<td>See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
</tbody>
</table>

**Procedure**

Enable or disable an aggregation or modify the aggregation fields from the list.

1. Click **Console Integrations** in the navigation, and select **Flow Aggregation** under **System Configuration**.

2. Select a row from the table and click the **Edit** button or select **Edit** in the **Actions** column as follows:

   **Aggregation**
   - Name of the aggregation as it appears in the table.

   **Aggregation Fields**
   - Aggregation grouping keys or fields in the aggregation.

   **Visible in Traffic Details**
   - By default, when an aggregation type is disabled, the Top Talker view that is associated with the specific aggregation is not visible from the Traffic Details dashboard. Select the check box to display the Top Talker view with the historical data even if the aggregation is disabled.

     **Note**: This control affects only the Traffic Details dashboard views but does not affect the Flow dashboard views.

   **Enabled**
   - Select the check box to enable the aggregation.

3. Optional: Click **Enable** or **Disable** to enable or disable an aggregation in the **Actions** column.

**Results**

When an aggregation type is disabled, the historical data remains in the database with no further updates to the CFG schema tables and Flow Metric schema tables.

**Configuring Flow interfaces**

Flow records provide unidirectional measurements of traffic that is entering (ingress) or leaving (egress) a network interface. Network Performance Insight models this process by associating an Ingress Interface and Egress Interface with each network interface. Each flow record is associated with the appropriate flow interface.

**About this task**

Network Performance Insight automatically creates flow interfaces when flow records are processed. When new interfaces are created, they are enabled unless the total number of interfaces exceeds the...
limit. Network Performance Insight processes the data that is associated with a flow interface only if it is enabled.

**Procedure**

1. Log in to Jazz for Service Management server.

2. Click **Console Integrations** in the navigation, and select **Interfaces** under **System Configuration**.

3. Select a row from the table and click the **Edit** button to enable or disable the selected interface.

4. Click **OK** to save the configuration.

5. Optional: Enter the following interface details to manually update the interface details for enrichment:
   - **Interface Name**
   - **Interface Description**
   - **Speed**

   **Note:** These details override the information that is obtained from devices by configuring the SNMP credentials in Configuring Flow Devices section in *Installing and Configuring IBM Network Performance Insight*.

6. Optional: Click **Enable** or **Disable** to enable or disable an Interface for flow data collection in the **Actions** column.

**What to do next**

You must repeat the same process to enable or disable all interfaces as needed.

**Note:** Currently, you cannot select multiple interfaces to configure to enable or disable for traffic data collection at a time.

**Configuring Flow IP Grouping**

Create logical grouping of IP addresses and address ranges. This grouping helps in monitoring the individual NetFlow bandwidth usage, usage-based billing, and accounting.

**About this task**

- To configure multiple IP ranges into a single IP address group, create multiple row entries with same IP address group.
- Make sure that the IP range does not overlap with existing ones. Otherwise, you might see *Overlapping Ip address grouping range* message.

**Procedure**

1. Click **Console Integrations** in the navigation bar, and select **Flow IP Grouping** under **System Configuration**.

Add an IP address group.

2. Click **New** icon and enter the IP address grouping information as follows:

   **IP Address Group**
   Logical name to the group. Create your IP Grouping by location. For example, branch offices or departments for easier monitoring.

   **Start Address Range**
   Start IP address for the range.
**End Address Range**
End IP address for the range.

**Enabled**
A flag to enable or disable the specified IP address group.

3. Click **Ok** to save the settings.

Edit an IP address group.

4. Select a row from the table and click the **Edit ( )** button to change the information for the IP Address Group.

5. Click **Ok** to save the settings.

Delete an IP address group.

6. Select an entry from the table and click **( )** icon to delete an entry that is not needed.

**Configuring NBAR**
Configure your devices to send NBAR and NBAR2 data to gain better visibility on the applications in your NetFlow traffic. This information helps you identify the bandwidth usage of the applications in your network and also prioritize and control the application traffic. You can define the business relevance of the applications and apply the correct QoS policies to improve the performance and user experience of business-critical applications.

**About this task**
NBAR and NBAR2 configured devices send Flow packets that contain the following metrics:

- Engine ID
- Selector ID
- Name
- Description
- Category Name
- Subcategory Name
- Group Name
- P2P Technology
- Tunnel Technology
- Encrypted Technology
- Business Relevance

**Procedure**

1. Click **Console Integrations ( )** in the navigation bar, and select **NBAR** under **System Configuration**.
Edit the NBAR and NBAR2 settings.

2. Click **Edit ( )** icon to enable or disable the ART metric collection:
   
   Select the **Enable ART** check box to enable the collection of Application Response Time (ART) metrics for TCP traffic.
   
   The following fields are not editable:

   **Engine ID**
   A unique identifier for the engine that determined the Selector ID. The Engine ID is the first 8 bits that provide information about the engine that classifies the flow.
Selector ID
The remaining 24 bits that provide information about the application.

Note: Engine ID and Selector ID constitute the Application ID.

Name
Name of the application that is derived from the Application ID.

Description
Application description that can be derived from the Application option template.

3. Click Ok to save the settings.
4. Optional: Click Enable or Disable to enable or disable an ART in the Actions column.

Related information
Cisco Application Visibility and Control Field Definition Guide for Third-Party Customers

Configuring the metric polling interval
Network polling depends on the polling formulas and metrics that are derived from the Technology Pack content, polling interval that can be configured on the Polling Configuration page, and polling scope.

About this task
Polling interval defines the frequency of polling and it can affect the polling performance. List of resource types and their resources are populated on this page from Inventory schema tables based on the available Technology Pack content.

Procedure

1. Click Console Integrations ( ) in the navigation bar and select Polling Configuration under System Configuration.
   You can see the following tabs:
   • Resource Config
     Contains a list of all the resource types in the installed Technology Packs content and their polling intervals.
   • Entity Config
     Contains a list of all the resources in the installed Technology Packs content and their polling intervals. You can also add more resources and set the polling interval.

2. Click the Resource Config tab.

3. Select a resource type from the table and click the Edit button ( ).
4. Specify the required polling interval for the resource type and click Ok.
   The default polling interval is 300 seconds.

Important:
• The polling interval for the resource type Probe cannot be configured from this page. Set the polling interval for probe on the device itself.
• If you set polling interval to zero for a resource type, then polling from the resources for that resource type is stopped.

5. Click Entity Config tab.

6. Select a resource and click the Edit button ( ).
7. Or, click Edit in the Actions column.
8. Specify the required polling interval for the resource and click Ok.
Resource interval setting from the Entity Config page takes precedence over the resource type setting on the Resource Config page.

9. Click Clear in the Actions column to clear the polling interval setting on the selected resource.

**Configuring resource types**

Configure the resource types for discovery.

**About this task**

All the existing resource types from the installed Technology Pack content are populated on this page. You can also add new resource type names.

**Procedure**

1. Click **Console Integrations** ( ) in the navigation bar and select **Resource Type** under **System Configuration**.

   You can see a table containing all the Resource types that are available in the technology pack content in your environment.

   Add new resource type and its details.

2. Click **New** ( ) icon and enter the following details:

   **Name**
   Name of the resource type to be discovered.

3. Click **Ok**.

Delete an existing entry.

4. Select an entry from the table and click the Delete button ( ) icon to delete an entry that is not needed.

**Configuring data retention profiles**

Describes how to configure the retention profiles for different type of data that is collected by Network Performance Insight.

**About this task**

Retention profiles control how long the raw and aggregated data, and log files are retained by the system. Setting the retention profiles help in maintaining the amount of data to be stored in the database and free the additional disk space. You can change the default values to modify the retention periods. For timeseries data alone, set the retention period from Ambari.

**Note:** Entity Metric schema tables retention profile settings are not available in a fresh installation, since the data is now moved to timeseries database. But you notice the retention profile settings for Entity Metric schema tables in an upgraded system.

For more information, see **Retention period** section in Network Performance Insight overview IBM.

To configure retention profiles:

**Procedure**

1. Log in to Jazz for Service Management server.

2. Click **Console Integrations** ( ) in the navigation bar and select **Retention Profiles** under **System Configuration**.

   You can see Retention Profiles table.
3. Select a row from the table and click the **Edit** button to configure a retention profile period for an Interface. Enter the following details:

**Name**
- The **Name** field is already selected.

**Period**
- Type the period for which you want to retain the data.

**Unit**
- Select the unit; **Days**, **Weeks**, or **Months**.

**Note:** Retention period must be configured with tradeoff between storage size and number of days to keep the data. The graphs will not show any data after the time period that you selected for a particular interface.

For more information, see *Data storage* section in *Network Performance Insight overview IBM*.

4. Click **OK** to save the settings.

**What to do next**
Repeat the same process to configure retention profiles as needed. For timeseries data alone, set the retention period from Ambari.

For more information, see *Configuring retention period for timeseries data* section on *Installing and Configuring IBM Network Performance Insight*.

*Configuring site grouping*
You can categorize your enterprise network based on different geographical areas by specifying the IP address ranges for each site. Each site can be configured for specific business and non-business days and hours.

**About this task**
This grouping helps in monitoring the individual site bandwidth usage, usage-based billing, and accounting. You can also get visibility on the network bandwidth usage during business and non-business days and hours.

**Procedure**

1. Click **Console Integrations** in the navigation bar, and select **Sites** under **System Configuration**. Add a site group.

2. Click **New** icon and enter a site information as follows:

   **Site Name**
   - Logical name to the site. Create your site by location. For example, branch office locations for easier monitoring.

   **IP Address Ranges**
   - Start and end IP address for the range that is specific to the site. You can give the ranges separated by a hyphen or as comma-separated list.

   **<Day>**
   - All days from Sunday to Saturday are listed. Select the days based on the typical business days for your site.

   **Business Start Time**
   - Specify the typical business start time in `hh:mm` format.
Business End Time
Specify the typical business end time in hh:mm format.

Time Zone
Select the time zone to which the site belongs to from the list.

Edit a site group.

3. Select a row from the table and click the Edit button to change the information for the site.
4. Click Ok to save the settings.
Delete a site group.

5. Select an entry from the table and click the Delete button icon to delete an entry that is not needed.

Configuring Flow thresholds
Thresholds provide a mechanism for identifying anomalies in flow and metric data that is polled from Tivoli Network Manager. Threshold is a metric value that is compared against a value to determine whether an interface violated a specific constraint. The threshold violations and their values are user-defined and not dynamically generated. These threshold values are defined per interface in each direction.

About this task
You can configure the threshold value per interface for anomalies detection.

Procedure
1. Log in to Jazz for Service Management server.
2. Click Console Integrations in the navigation bar and select Thresholds under System Configuration.
   You can see Flow Thresholds table.
3. Select a row from the table and click the Edit button to configure a Threshold for that Interface. Enter the following details:
   a) Select the Enabled check box to enable a Threshold on the Interface.
   b) Select the limit type from the Limit Type list to Over, Under, or Band and their units.
      Over
      Detect violations when the interface exceeds the set Threshold value.
      Under
      Detect violations when the interface falls short of the set Threshold value.
      Band
      Detect violations the interface goes outside a range (or band) between two set Threshold values.
   c) Enter a value in the Upper Limit field for the interface to trigger a Threshold violation.
   d) Enter a value in the Lower Limit field for the interface to trigger a Threshold violation.
   e) Enter the number of events for triggering the Threshold.
   Note: When the Threshold limit is violated, it displays the severity as Critical.
   For more information, see Threshold violation in IBM Network Performance Insight: Product Overview
4. Perform the following tasks in the Actions column:
   a) Click Edit to edit or configure the selected Threshold. Repeat step 3
b) Click **Enable** or **Disable** to enable or disable an interface to detect its Threshold violation states.

5. Click **OK** to save the settings.

**Results**

Any interface that is violating the set Threshold value is reported in the Event Viewer.

**What to do next**

You must repeat the same process to enable and configure thresholds for every Interface as needed.

**Note:** Currently, you cannot select multiple interfaces to configure the Thresholds values at a time.

To configure thresholds for metric data, see [Defining anomaly thresholds](#).

**Configuring Type of Service**

Typically, this feature determines the packet delivery prioritization for low-delay, high-throughput, highly reliable service, or normal service for NetFlow traffic. On all Flow packets, Type of Service byte is represented as Differentiated Service Code Point (DSCP) and Explicit Congestion Notification.

**Procedure**

1. Click **Console Integrations** in the navigation bar, and select **Type of Services** under **System Configuration**.

   Edit the Type of Services mappings.

2. Click **Edit** icon and modify the Type of Services metrics as follows:

   **ToS ID**
   
   This field is not editable. This field implements the Type of Service on the NetFlow packet to tradeoff on delay, throughput, reliability, and cost.

   **ToS Name**
   
   You can specify any name to your Type of Service class. Typically, the classes and their IDs are as follows:

<table>
<thead>
<tr>
<th>DSCP Code</th>
<th>DSCP ID (Decimal format)</th>
<th>IP Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Effort</td>
<td>0</td>
<td>0 - Routine or Best Effort</td>
</tr>
<tr>
<td>CS1, AF11-13</td>
<td>8,10,12,14</td>
<td>1 - Priority</td>
</tr>
<tr>
<td>CS2, AF21-23</td>
<td>16,18,20,22</td>
<td>2 - Immediate</td>
</tr>
<tr>
<td>CS3, AF31-33</td>
<td>24,26,28,30</td>
<td>3 - Flash - used for voice signaling</td>
</tr>
<tr>
<td>CS4, AF41-43</td>
<td>32,34,36,38</td>
<td>4 - Flash Override</td>
</tr>
<tr>
<td>CS5, EF</td>
<td>40, 46</td>
<td>5 - Critical - used for voice RTP</td>
</tr>
<tr>
<td>CS6</td>
<td>48</td>
<td>6 - Internetwork Control</td>
</tr>
<tr>
<td>CS7</td>
<td>56</td>
<td>7 - Network Control</td>
</tr>
</tbody>
</table>

   Where:
   
   - CS - Class Selector
   - AFXy - Assured Forwarding (x=class, y=drop precedence)
   - EF - Expedited Forwarding
Note: Traffic classification is an automated process that categorizes network traffic according to various parameters into a number of traffic classes.

Note: The ToS names must be unique.

3. Click Ok to save the settings.

Related information
DSCP and Precedence Values

Configuring integration with Tivoli Netcool/OMNIbus
Use this information to integrate Network Performance Insight with the Tivoli Netcool/OMNIbus Web GUI application. The Tivoli Netcool/OMNIbus Web GUI customizable dashboards display real-time performance information and event data.

About this task
An event contains the Event ID, host name, and port information. When an event is selected, some of the data for the event is sent to Network Performance Insight and used to determine the best report to present. Network Performance Insight then builds a block of HTML content that redirects the browser to a Network Performance Insight display.

Right-click an event in Event Viewer or Active Event List of Web GUI to display the tools that are added from the alerts menu. You select an option from this menu to display a detailed Network Performance Insight report for the time period of the threshold violation or an AEL report.

Configuring launch-in-context integration with Network Performance Insight
Launch-in-context integrations are supported between the Web GUI and other Netcool Operations Insight widgets. A launch-out integration describes the launching of another product from a Web GUI widget. A launch-in integration describes the launching of the Web GUI from another product.

About this task
Launch-in-context is the concept of moving seamless from one Tivoli product UI to another Tivoli product UI (either in a different console or in the same console or portal interface) with single sign-on and with the target UI in position at the proper point for users to continue with their task.

Related information
Configuring launch-in-context integrations with Tivoli products

Creating a launch-in-context tool
You can create tools that are run from right-click menus in event lists or when users click a widget. Different tool formats are supported.

Procedure
1. Log in to Jazz for Service Management server as an administrator user, such as npiadmin.
2. Select Administration > Event Management Tools > Tool Configuration from the left pane.
3. Click Create Tool and enter the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>npiFlowTvLiC</td>
</tr>
<tr>
<td>Type</td>
<td>script</td>
</tr>
<tr>
<td>Script Commands</td>
<td>Copy and paste the contents of the file npiFlowTvLiC.js that is available in opt/IBM/basecamp/basecamp-ui/resources/ael.</td>
</tr>
</tbody>
</table>

4. Select the data source name OMNIBUS.
5. Clear the Execute for each selected row check box.
6. Click Save.
A confirmation message is displayed. Click **OK** to close the message.

### Related information

**Tools overview**

**Configuring launch-in-context menu**

In event lists, users access default and custom tools through menus. You can add tool entries to the menus, create new submenus, and modify or delete menu items.

### About this task

The two supplied menus are the **Alerts** menu and the **Tools** menu. The **Alerts** menu can also be opened from the right-click menu when you select an event.

### Procedure

1. Log in to Jazz for Service Management server as **npiadmin** user.
2. Select **Administration > Event Management Tools > Menu Configuration** from the left pane.
3. Select the **alerts** menu in the window, and then click the **Modify** button.

    The **Menus Editor** is displayed.

4. Select the **npiFlowTvLiC** tool in the **Available items** on the left, click the arrow to move it to the **Current items** section.
5. Select **npiFlowTvLiC** from the **Current items** section and click **Rename**.
6. In the **Label** text box, enter a meaningful name for the new button.
   For example, Flow Dashboard. If needed, enter a value in the **Mnemonic** text box, if needed.
7. Click **Save**.
8. Use the button selections on the right to move the menu option up or down.

    Separators might also be added by selecting `<Separator>` in the **Available Items** area of the window.
    The separator might be moved up and down.
9. Click **Save**.

    The following message is displayed:
    **Menu has been successfully modified.**
10. Click **OK** to close the message.

### Results

When you right-click any event in **Event Viewer** or in **Active Event List**, you can see the **npiFlowTvLiC** tool that is renamed to Flow Dashboard as a selectable option in the menu. Select the tool to see the Traffic Details report associated with the interface that violated the threshold and generated the event.

### Configuring non-default ObjectServer name

By default, the Tivoli Netcool/OMNibus Object Server name is NCOMS. If you configured a non-default name for the ObjectServer, use this information to configure to work with the non-default ObjectServer name.

### Procedure

1. Edit the **npi-flow-stdin.props** file that is located in `/opt/IBM/npi/npi-event/stdin-probe/omnibus/probes/linux2x86` to change the following value:

```plaintext
# Add your settings here
```

---

70 IBM Network Performance Insight 1.3: Installing and Configuring Network Performance Insight
2. Save the file.
3. Edit the interfaces.linux2x86 file that is located in /opt/IBM/npi/npi-event/stdin-probe/etc to comment the NCOMS and add the non-default ObjectServer name as follows:

```
# NCOMS => omnihost 4100
# NCOMS
<non-default ObjectServer name>
master tcp sun-ether omnihost 4100
query tcp sun-ether omnihost 4100
```

4. Save the file.
5. Restart the Event Service from Ambari.

- See Controlling the services from Ambari administration interface in Administering IBM Network Performance Insight.
- See Setting up the OMNIbus Standard Input probe section in Installing and Configuring IBM Network Performance Insight.

### Scenario 2 - NetFlow data and Performance data from Cacti

In this scenario, Network Performance Insight can be used to collect, aggregate, and render the NetFlow data. It can be integrated with Cacti to discover, poll, and render the performance data.

**Related information**
- Roadmap for installing and configuring - Scenario2

### Installing

The installation information contains the installation prerequisites, instructions for preparing to install, installing, and uninstalling the software based on your scenario.

**About this task**

Follow the general installation roadmap to complete required and optional steps, according to your needs.

**Planning for Network Performance Insight installation**

Before you install the product, read the hardware and software requirements.

For more information, see Suggested node and services layout from .

**Related concepts**

- “System requirements” on page 1
  Complete set of requirements for IBM Network Performance Insight 1.3.

**Downloading and extracting the software**

How to get the product distribution?

**Procedure**

1. Download the electronic installation images from the IBM Passport Advantage website to a location of your choice on Ambari server.

   For example, /opt/IBM/Installers/NPI that is referred to as <DIST_DIR>.

2. Extract the media by using the following commands:

```
tar -zxvf NPI-1.3.0.0.tgz
```

```
Or, use the following command:

```
gunzip -c NPI-1.3.0.0.tgz | tar -xvf -
```

You can see the following files and folders in the `<DIST_DIR>`:

- NPI-1.3.0.0/
  - bin
    - agent_setup_nonRoot.sh
    - install.sh
    - installRemoteFlowCollector.sh
    - npi_prereq_check.sh
    - prereq_check.sh
    - setup_cluster_ssh.sh
  - upgrade
    This folder contains a lot of script files that are required to upgrade from to . It also contains the libraries and script to migrate the SNMP device credentials from the previous environment to the new one.
    - basecamp-installer-tools-1.3.0.0-<build_signature>.noarch.rpm
    - basecamp-repo-1.3.0.0-<build_signature>.noarch.rpm
    - npi-ambari-1.3.0.0-<build_signature>.noarch.rpm
    - npi-repo-1.3.0.0-<build_signature>.noarch.rpm

**Downloading the ()**

Download the components.

**About this task**

Download the following packages to a single location of your choice on Ambari server. For example, `/opt/IBM/Installers/NPI` that is referred to as `<DIST_DIR>`.

- HDP-2.6.4.0-centos7-rpm.tar.gz
- HDP-UTILS-1.1.0.22-centos7.tar.gz
- HDP-GPL-2.6.4.0-centos7-rpm.tar.gz
- ambari-2.6.1.0-centos7.tar.gz

**Note:** You do not need to extract these packages.

**Procedure**

Download the following repositories:

- HDP
- HDP-UTILS
- HDP-GPL
- Ambari
Gathering required information
Collect the following information before you start your installations.

- The fully qualified domain name (FQDN) for each host in your system, and the components that you want to set up on different hosts. The Ambari installation wizard does not support IP addresses. Use `hostname -f` to check for the FQDN.

  An example for FQDN: `myserver.ibm.com`

- Plan for the base directories for the following components:
  - NameNode data
  - DataNodes data
  - MapReduce data
  - ZooKeeper data
  - Various log, pid, and database files according to your installation type

- Users and groups for
  - `root`
  - `netcool`

    The `netcool` user is created during installation and all services are run as `netcool` user.
  - `smadmin`

- Users and groups for:

<table>
<thead>
<tr>
<th>Service</th>
<th>Group</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>hadoop</td>
<td>hdfs</td>
</tr>
<tr>
<td>MapReduce</td>
<td>hadoop</td>
<td>mapred</td>
</tr>
<tr>
<td>YARN</td>
<td>hadoop</td>
<td>yarn</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>hadoop</td>
<td>ams</td>
</tr>
<tr>
<td>Kafka</td>
<td>hadoop</td>
<td>kafka</td>
</tr>
<tr>
<td>Spark</td>
<td>hadoop</td>
<td>spark</td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>hadoop</td>
<td>zookeeper</td>
</tr>
</tbody>
</table>

  Note: Click Admin > Service Accounts to see the user information from your Ambari server.

- Download the .

  Note: The must be installed after the installation of .

- Download the .

  See Default users section in .

Installing the prerequisite software
Install the prerequisite products before you install Network Performance Insight.

About this task
Install the required products in your IBM Netcool Operations Insight solution according to your entitlement.

You require the following components from IBM Netcool Operations Insight solution to work with Network Performance Insight:

- Tivoli Netcool/OMNIbus core component
- Tivoli Netcool/OMNIbus Web GUI component
• Cacti
• Jazz for Service Management
• Tivoli Common Reporting

This component is required only if you have Cognos-based reports from your other product integrations. It is not required to work with Network Performance Insight.

Note: If your Dashboard Application Services Hub that has Tivoli Common Reporting and Network Performance Insight integration fails, see Troubleshooting Dashboard Application Services Hub and Network Performance Insight integration section in Troubleshooting IBM Network Performance Insight

Procedure
1. Perform steps 1 - 14 from Quick reference to installing according to your Netcool Operations Insight entitlement.
2. Install and configure Cacti and the related software.

What to do next
Continue with installation of Network Performance Insight.

Installing and configuring Cacti and related software
Cacti application is an open source web-based network monitoring and system monitoring graphing solution for enterprises. Cacti enables a user to poll services at regular intervals to create graphs on resulting data by using the RRDtool. Typically, it is used to graph time-series data of metrics such as network bandwidth utilization, CPU load, running processes, disk space.

About this task
Note: Cacti is supported on RHEL platform only in Network Performance Insight.

Follow these steps to install and configure Cacti and the related software.

Important: If you have an existing Cacti environment, you can install the Reflector plug-in in it. See “Installing the Reflector plug-in” on page 75.

Note: Cacti must collect the performance metrics that are based on the data templates that are provided in Network Performance Insight software bundle. For more information, see:
• “Importing performance data templates” on page 76.
• Supported performance metrics from Cacti section in IBM Network Performance Insight: References.

Required packages for Cacti
Cacti requires some additional packages to be installed on your Linux operating system.

Required RHEL packages for Cacti:
• Apache
  A web server to display network graphs created by PHP and RRDTool.
• MySQL or MariaDB
  A database server to store cacti information.
• PHP
  A script module to create graphs by using RRDTool.
• PHP-SNMP
  A PHP extension for SNMP to access data.
• NET-SNMP
  An SNMP (Simple Network Management Protocol) is used to manage network.
• RRDTool
A database tool to manage and retrieve time series data like CPU load, Network Bandwidth.

**Installing Cacti**
Step-by-step installation of Cacti. Supported Cacti versions are V0.8.8 and V1.1.36.

**Procedure**
Install Cacti.
Follow the instructions from here:
https://www.cacti.net/downloads/docs/html/install_unix.html

**What to do next**
To verify the installation, open the following link:
http://<Host_IP_Address>/cacti/

**Related information**
Cacti The ULTIMATE Management Solution
Tutorial: How to install Cacti 1.1.26 on CentOS7

**Installing the Reflector plug-in**
You can mirror your poller’s output to a log file with the help of the Reflector plug-in.

**About this task**
The Reflector plug-in is bundled with Network Performance Insight distribution. After Network Performance Insight is installed, you can find the Reflector plug-in from /opt/IBM/npi/npi-cacti-collector/resources.

**Procedure**
1. Copy the cacti_reflector-1.0.0.tgz file from Network Performance Insight server to the server where your Cacti is available at <CACTI_HOME>/plugins/ directory.
2. Extract the cacti_reflector-1.0.0.tgz file to <CACTI_HOME>/plugins/ with the following command:
   ```bash
   tar -zxvf cacti_reflector-1.0.0.tgz
   ```
   Where, the default <CACTI_HOME> is /var/www/cacti/ and the non-default path is /usr/share/cacti/.
3. Ensure that correct permissions and correct owner are set to <CACTI_HOME>/plugins/reflector folder.
4. Install the Reflector plug-in through Plugin Management page in Cacti.
   a) Log in to the Cacti web interface as follows:
   ```bash
   http://<cacti_server_IP>/cacti
   ```
   b) Click Console > Configuration > Plugin Management.
   c) Click the Install Plugin icon on the Reflector plug-in that is listed in the Plugin Management page.
   d) Review and save the Reflector plug-in settings.
   e) Enable the Reflector plug-in through Plugin Management page.

**Configuring the Reflector plug-in**
After the Reflector plug-in is installed, the plug-in must be configured. The same configuration settings must be applied to each Cacti instance on the Cacti Servers page from System Configuration.

**Procedure**
1. From your Cacti web interface, click Settings in the Configuration tab.
2. Click the **Reflector** tab.

3. Enter the following details:

   - **Reflector output format**
     The output format in the log file. It is **logfile (kv pairs)**.

   - **Reflector output path**
     The path location to output the log files. For example, `<CACTI_HOME>/log/`.

   - **Reflector log prefix**
     The file prefix that contains the poller output data. For example, enter `reflector_poller`.

   - **File retention max file time**
     Set the maximum file retention time in seconds. By default, it is 1800 seconds.

   - **Enable Reflector Debug**
     Select the check box. The debug logs are available in `cacti.log` file and the Reflector plug-in log files are available in `reflector_poller.<timestamp>.log.gz`. The `reflector_poller.<timestamp>.log.gz` file contains the metrics and their values.

     For more information about configuring Cacti servers, see *Installing and Configuring IBM Network Performance Insight*.

---

**Importing performance data templates**

Network Performance Insight contains specific templates for monitoring the devices and to collect the Cisco IP SLA, Performance Metric OOTB Device Support, and SNMP metrics from MIB-II. Typically, a set of templates is provided as XML files that hold all the required definitions for data templates and graph templates.

**About this task**

You can find three .zip files that contain the data templates in the following directory in your installation directory: `/opt/IBM/npi/npi-cacti-collector/resources`:

- CiscoIPSLA.zip
- MIB2.zip
- PODS.zip

**Procedure**

1. Extract the three .zip files to your `<DIST_DIR>`.

   You can find the following directories:

   - CiscoIPSLA
   - MIB2
   - PODS
     - CiscoDevice
     - HuaweiDevice
     - JuniperChassis
     - JuniperErx

   **Note:** Each folder contains the following subdirectories inside it:

     - dict
     - query

2. Create a directory by name NPI in `<CACTI_HOME>/resource/snmp_queries/NPI`path.
3. Copy all the three extracted folders from step 1 to `<CACTI_HOME>/resource/snmp_queries/NPI`. For example:
   - CiscoIPSLA
   - MIB2
   - P0DS
4. Log in to the Cacti web interface as follows:
   ```
   http://<cacti_server_IP>/cacti
   ```
5. Click **Console > Import Templates**.
6. Make sure that you select the **Select your RRA settings below (Recommended)**.
7. Click **Browse** and locate the query XML files from the query directory in each template directory one by one.
   ```
   Note: You can either select from `<DIST_DIR>/CiscoIPSLA/query/cacti_data_query_npi-_cisco_ipsla_stats.xml` or from `<CACTI_HOME>/resource/snmp_queries/NPI/CiscoIPSLA/query/cacti_data_query_npi-_cisco_ipsla_stats.xml`
   ```
8. Click **Import**.
   ```
   Note: You must import the XML files according to your requirement one by one.
   ```

**Configuring devices to collect performance data**

Use this information to understand how to add and configure the devices in your network in Cacti to collect the performance data for Network Performance Insight system.

**About this task**

Skip steps 1 - 2 if you have set up your devices on Cacti already.

**Procedure**

1. Log in to the Cacti web interface as follows:
   ```
   http://<cacti_server_IP_Address>/cacti
   ```
2. Add all the devices in your network in Cacti. See Creating a Device.
3. Click **Console > Management > Devices** and click a device name that you want to configure.
4. Click **Add Data Query** list in Associated Data Queries pane and select the Network Performance Insight metrics that are prefixed with NPI.
5. Click **Add**.
   ```
   For example, NPI - Cisco Device Chassis.
   ```
6. Click **Add Data Query** list in Associated Data Queries pane and select the built-in **SNMP - Interface Statistics** Data Query and click **Add**.
   ```
   The following SNMP metrics are collected:
   - ifOutDiscards
   - ifInDiscards
   - IfInOctets for snmpInBandwidth
   - IfOutOctets for snmpOutBandwidth
   - ifInErrors
   - ifOutErrors
   ```
   ```
   Note: You can see the SNMP - Interface Statistics template XML file in the following location:
   `<CACTI_HOME>/resource/snmp_queries/interface.xml`
   ```
7. Repeat step 4 for each performance metric that you want to monitor for this device one by one.
8. Click **Save**.
9. Click **New Graphs**. Or, if you are at the device edit page, click **Create Graphs for this Host**.
10. Create the graphs for each device. See **Creating the Graphs**.

**Preparing your environment**
Before you run the installation, you must prepare your target environments. Make sure you have installed .

**Setting SSH passwordless login**
You must set up passwordless SSH connections for the Ambari server host to remotely connect to all other hosts that are in the cluster, and also the server without entering the password.

**Procedure**
1. Log in to the system where you want to install Ambari server host as **root** user.
2. On the Ambari server host, run the following command:

   ```bash
   <DIST_DIR>/NPI-1.3.0.0/bin/setup_cluster_ssh.sh
   ```

   Enter the required details on the prompts.
   **Note:** Always, give fully qualified domain name (FQDN) for the hosts.

   ```
   INFO: Hostname <myserver.ibm.com>
   INFO: USER root
   INFO: User home directory /root
   INFO: Generating public keys pair ...
   Continue to setup remote hosts[Y/n]?y
   Enter remote hostname (FQN): <myserver2.ibm.com>
   INFO: Creating .ssh directory on <myserver2.ibm.com> ...
   root@<myserver2.ibm.com>'s password:
   INFO: Uploading public key to remote host ... root@<myserver2.ibm.com>'s password:
   INFO: Updating remote host's folder permission ...
   INFO: Verifying ssh passwordless setup ...
   Verified SSH connection
   SSH Passwordless setup to <myserver2.ibm.com> is completed successfully.
   Continue to setup next remote hosts[Y/n]?y
   ```

   If you are configuring the integration of with non-root installation of supported products, run following commands:

   ```bash
   cd /root/.ssh
   ssh-copy-id -i id_rsa.pub <non-root-user>@<myserver.ibm.com>
   ssh <non-root-user>@<myserver.ibm.com>
   ```

   3. Repeat the connection attempt from the Ambari server host to each host to make sure that the Ambari server can connect to each.

**Setting Kernel parameters**
Setting the ulimit and kernel parameters in nodes.

**About this task**
Run the following steps to set the ulimit and kernel parameters.

**Note:** You can see the error messages in Ambari start operation stderr and log file if the ulimit or the kernel settings are not set correctly during Storage or Flow Collector services start-ups.

**Procedure**
1. Log in to system as **root** user to change the Linux kernel parameters.
2. Edit the `/etc/sysctl.conf` file to add or modify the kernel parameters.

   ```
   net.core.rmem_default = 33554432
   net.core.rmem_max = 33554432
   net.core.netdev_max_backlog = 10000
   ```

   Change the `/etc/sysctl.conf` to ensure that the values are set on a system start.
   a) Run `sysctl -p` as root user to refresh with the new configuration in the current environment.

3. From the node, edit the `/etc/security/limits.conf` file to add or modify the number of open files to at least 65536 as follows:

   ```
   * - nofile 65536
   * - nproc 65536
   ```

4. Log out and log in the session again as root user for the changes to take effect.

5. Repeat the steps 1 - 4 on all the servers where services are installed.

**Configuring Security-Enhanced Linux (SELinux) to support SCTP protocol**

By default, the Linux kernel security module (SELinux) runs in enforcing mode. When your RHEL system runs in SELinux enforcing mode, it might deny the SCTP ports.

**About this task**

This information provides details about how to configure SELinux to enable SCTP support.

**Procedure**

1. Set SELinux to permissive as root user on all hosts in your cluster as follows:

   ```
   setenforce 0
   ```

2. Proceed to install system and set up the clusters.

3. Make sure that the system is up and running for sometime.

   It might take a while to notice the AVC denied messages in the log file after the system is up and running.

4. Check SELinux audit log with this command:

   ```
   tail -f /var/log/audit/audit.log
   ```

   You might notice the AVC denied message as follows:

   ```
   type=AVC msg=audit(1508149696.075:38284): avc: denied { getattr } for pid=1412
   comm="npi-akka.actor." laddr=::ffff:10.55.236.146 lport=4381 faddr=::ffff:10.212.6.20
   fport=33859 scontext=system_u:system_r:unconfined_service_t:s0 tcontext=system_u:
   object_r:unlabeled_t:s0 tclass=rawip_socket
   ```

5. Create local policy to enable the access as follows:

   ```
   mkdir <workdir>
   cd <workdir>
   grep npi-akka.actor. /var/log/audit/audit.log | audit2allow -M npi
   semodule -i npi.pp
   ```

   The local policy helps in suppressing the AVC denied error message.

6. Optional: You can change the SELinux mode to enforcing as root user as follows:

   ```
   setenforce 1
   ```

**Related tasks**

“Installing Network Performance Insight” on page 17
Install HDP® and Network Performance Insight on a single host or multi-host environments.

**Preparing to run the prerequisite scanner**
In addition to specific tasks, complete these common tasks before you start an installation. Installation script calls the prerequisite scanner that checks if your environment meets these requirements during installation.

**Before you begin**
Make sure that you have the following operating system packages and their related repos are installed and enabled:

- libtirpc-devel
- redhat-1sb

**Note:** These packages are required for

**About this task**
Use the root user account to perform the following steps.

**Procedure**
Follow the steps that are specified in Preparing the environment in documentation.

**Related information**
HDP Documentation

**Installing**
Install and on a single host or multi-host environments.

**Before you begin**
- Ensure that is installed.
- Ensure that the necessary user permissions are in place for all the installation directories.
- Ensure that all the hosts in your cluster are in the same timezone.
- Ensure that you configured your devices to send all the required Flow fields for collection.

For more information, see the following topics:
- Default normalized flow record fields in
- Configuring Flexible NetFlow and AVC in

**About this task**
All the services are distributed under the following default directories:

- /opt/IBM/npi
- /opt/IBM/basecamp

**Procedure**
1. Remove the existing yum cache that might be saved in your system by using the following command as root user:

   ```
   rm -rf /var/cache/yum
   ```

2. Start the installation by using the following command as root user on Ambari server:

   ```
   cd <DIST_DIR>/NPI_1.3.0.0/bin
   ./install.sh <DIST_DIR>
   ```
Where <DIST_DIR> is the directory where the software is located. For example, opt/IBM/Installers/NPI.

3. Enter y or n in the prompt based on the prerequisite checker errors.

**Results**

These tasks are completed after the command is run:

- Prerequisite checker script (prereq_check.sh) is called to ensure that your environment is set up correctly. Check the prereq_check_<timestamp>.log for any errors.
- /var/www/html/repos directory is created if it does not exist.
- files are extracted.
- services are set up in /var/www/html/repos/npi folder.
- These dependent packages are installed:
  - apr
  - apr-util
  - mailcap
  - postgresql
  - postgresql-libs
  - postgresql-server
- Apache Hypertext Transfer Protocol Server (httpd) server is installed.
- httpd port is updated to 9091.
- Ambari server is installed and started.
- Ambari server is configured to auto restart services and components.
- Related repo files are updated in /etc/yum.repos.d/ to point to local yum repositories.

You require only the following repositories in /etc/yum.repos.d/ directory. The rest of the files can be removed to ensure that the cluster setup is not interrupted:

- ambari.repo
- ambari-hdp-1.repo
- hdp.repo
- hdp-utils.repo
- hdp-gpl.repo
- npi.repo
- service stack is updated to repoinfo.xml file to point to local RPM repositories.

**Note:** If you encounter any prerequisite checker warnings during installation, see “Preparing to run the prerequisite scanner” on page 16.

**What to do next**

You can see the installation output in the following log files that are located in <DIST_DIR>/NPI_1.3.0.0:

- install_<timestamp>.log
- prereq_check_<timestamp>.log

Installing and configuring 81
Setting up Network Performance Insight cluster
Use the Ambari installation wizard in your browser to complete your installation, configuration, and deployment of Network Performance Insight components and Hadoop components.

Before you begin
• Ensure that you have the SSH Private key for root user on Ambari server host.
• Ensure that you have configured the SSH Passwordless login entry to all target hosts.

Procedure
1. Open a browser and access the Ambari server dashboard.
   Use the following default URL:
   http://<myserver.ibm.com>:8080
   The default user name is admin, and the default password is admin.
2. Click Launch Install Wizard on the Ambari Welcome page.
   The CLUSTER INSTALL WIZARD opens.
3. Enter a name for the cluster you want to create on the Get Started page and click Next.
   Note: The name cannot contain blank spaces or special characters.
   For example, npi.
4. On the Select Stack page, select HDP-2.6.NPI stack and select the Use Public Repository option.
5. Click Next.
6. Complete the following steps on the Install Options page:
   a) List all the nodes that are used in the HDP® cluster on Target Hosts pane.
      Specify one node per line, as in the following example:

      node1.abc.com
      node2.abc.com
      node3.abc.com

      Note: The host name must be the fully qualified domain name (FQDN).
   b) Select Provide your SSH Private Key to automatically register hosts on Host Registration Information pane.
      If the root user installed the Ambari server, the private key file is /<root>/ .ssh/id_rsa.
      Where <root> is the root user home directory.
      You have two options to get the private key file:
      1) Browse to the location of the .ssh/id_rsa
      Or
      2) Copy the contents of the .ssh/id_rsa file and paste the contents in the SSH key field.
      Make sure to copy all the content from:

      -----BEGIN RSA PRIVATE KEY-----

      To

      -----END RSA PRIVATE KEY-----

   c) Click Register and Confirm.
7. Ensure that the correct hosts are registered successfully on the Confirm Hosts page.
If you want to change the hosts that are selected, remove the hosts one-by-one by following these steps:

a. Click the check box next to the server to be removed.

b. Click Remove in the Action column.

Note:

- If warnings are found during the check process, click Click here to see the warnings to see the warnings. The Host Checks page identifies any issues with the hosts. For example, a host might have Firewall issues.
- Ignore the process issues that are not related to Network Performance Insight.

c. After you resolve the issues, click Rerun Checks on the Host Checks page. After you have confirmed the hosts, click Next.

8. Select the following services on the Choose Services page:

<table>
<thead>
<tr>
<th>Service</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>2.7.3</td>
<td>Apache Hadoop Distributed File System (HDFS)</td>
</tr>
<tr>
<td>YARN + MapReduce2</td>
<td>2.7.3</td>
<td>Apache Hadoop NextGen MapReduce (YARN)</td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>3.4.6</td>
<td>Centralized service that provides reliable distributed coordination.</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>0.1.0</td>
<td>A system for metric collection that provides storage and retrieval capability for metrics that are collected from the cluster.</td>
</tr>
<tr>
<td>Kafka</td>
<td>0.10.1</td>
<td>A high-throughput messaging system.</td>
</tr>
<tr>
<td>NPI</td>
<td>1.3.0.0</td>
<td>Network Performance Insight cluster service</td>
</tr>
<tr>
<td>NPI Spark Client Scala 2.11</td>
<td>2.0.1</td>
<td>Apache Spark is an engine for large-scale data processing. The Apache Spark client library is compiled on Scala 2.11 and is specific to Network Performance Insight 1.3.</td>
</tr>
</tbody>
</table>

9. Click Next.

10. Assign the master services to hosts in your cluster on the Assign Masters page and click Next.

You can accept the current default assignments. To assign a new host to run services, click the list next to the master node in the left column and select a new host.

11. Click Next.

12. Assign the slave and client components to hosts in your cluster on the Assign Slaves and Clients page.

Click all to assign all the services on your hosts. Or, you can select one or more components next to a selected host.

Note: If you do not need a microservice based on your installation scenario, do not select the check box against the service on a host.

13. Click Next.

14. Update the configuration settings for the following services and components on Customize Services pane.

You can see a set of tabs from where you can manage configuration settings for Hadoop and Network Performance Insight components.

Note: Default values are completed automatically when available and they are the recommended values.

- Set up HDFS
- Set up YARN
• Set up Zookeeper
• “Setting up Ambari Metrics” on page 23
• Set up Kafka
• Set up Network Performance Insight
• “Setting up the OMNIbus Standard Input probe” on page 28

15. Click Next after you have reviewed your settings, and click Deploy on the Review page.
16. Verify that your settings are correct and click Deploy on the Review page.
17. See the progress of the installation on Install, Start, and Test page.
   The progress bar at the top of the page gives the overall status and the main section of the page gives the status for each host. When you click the task, log for a specific task can be displayed.
18. Click Next after the services are installed successfully.
19. Review the completed tasks on the Summary page and click Complete.

Results
It might take a while for Ambari to start all the services. To see the status of all the services in a host, click the Hosts tab in the Ambari server host, and then select a host. You can see the services that are started from the Summary page.

Related concepts
“Required microservices in different installation scenarios” on page 9
Microservices that are required in different installation scenarios.

Setting up HDFS Service
Set properties for the NameNode, SNameNode, DataNodes, and some general and advanced properties. Click the name of the group to expand and collapse the display.

Procedure
Click HDFS > Settings.
Accept all the default values for the following required settings:

Note: These values are prepopulated based on your choices on previous pages.

• NameNode and DataNode directories as /<data1>/hadoop/hdfs/namenode and /<data1>/hadoop/hdfs/data.
  Ensure that the /<data1> directory has sufficient or the recommended disk space.

Note: Do not set up these directories in /tmp directory.
• NameNode Java heap size: 1 GB
• NameNode server threads: 200
• Minimum replicated blocks: 100%
• DataNode failed disk tolerance: 0
• DataNode maximum Java heap size: 1 GB
• DataNode max data transfer threads: 4098

Related concepts
“Hardware requirements” on page 1
Hardware specifications vary according to the size of your network and server topology that you want to use.

“Gathering required information” on page 13
Collect the following information before you start your installations.

**Setting up YARN Service**
YARN decouples resource management and scheduling capabilities from the data processing component. The YARN framework uses a ResourceManager service, a NodeManagers service, and an Application master service.

**Procedure**
1. Click **YARN > Settings**.
2. Configure the required settings as follows:
   - Ensure that the node memory is 15000 MB or more.
   - Ensure that minimum container memory per container is 1024 MB.
   - Ensure that maximum container memory per container is 15000 MB.
   - Set the number of virtual cores to minimum 32.

**Related information**
YARN

**Setting up Zookeeper**
Modify the default settings for Zookeeper from Ambari web UI.

**About this task**
Zookeeper requires a majority. It is best to use an odd number of nodes in your cluster. For example, with four Network Performance Insight nodes, ZooKeeper can handle the failure of a single machine; if two systems fail, the remaining two Network Performance Insight nodes do not constitute a majority. However, with five Network Performance Insight nodes, ZooKeeper can handle the failure of two Network Performance Insight nodes.

*Interim Fix* If a Network Performance Insight node is removed or added to your cluster, the conf/application.conf file in the UI Service is automatically updated to reflect the correct number of host names with the ZooKeeper Service in the following lines:

- main.zk-url=<host name1>,<host name2>,<host name3>
- messaging.kafka.zk-connect=<host name1>,<host name2>,<host name3>

**Procedure**
1. Click **Zookeeper > Zookeeper Server**.
2. Update the value of **ZooKeeper directory** field as per your environment.
   
   By default, Ambari might decide on a default directory with sufficient space. For example, /<data1>/hadoop/zookeeper.
   
   **Note**: Do not set the **ZooKeeper directory** in /tmp directory.

**Setting up Ambari Metrics**
Modify the default settings for Ambari Metrics from Ambari web UI.

**Procedure**
1. Click **Ambari Metrics > Configs > General**.
2. Provide values for the following fields:
   - **Grafana Admin Username**
   - **Grafana Admin Password**
   
   **Note**: You can retain the default values for the rest of the fields.
Setting up Kafka
Modify the Kafka Broker log settings from Ambari web UI.

Procedure
1. Click Kafka > Kafka Broker.
2. Update the values for the following fields as per your environment:

<table>
<thead>
<tr>
<th>Table 24: Kafka Broker settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
</tr>
<tr>
<td>Kafka Broker host</td>
</tr>
<tr>
<td>zookeeper.connect</td>
</tr>
<tr>
<td>log.dirs</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>log.roll.hours</td>
</tr>
<tr>
<td>log.retention.hours</td>
</tr>
<tr>
<td>Listeners</td>
</tr>
</tbody>
</table>

Setting up Network Performance Insight services
Set up all the Network Performance Insight services from web-based Ambari user interface. The configuration setting from Ambari UI are written to application.conf files that are located in the conf directory of each microservice.

Procedure
1. Click Services > NPI > NPI Settings.
2. Change the default values in the following fields:
   - Make sure that you are in the Configs tab if you are changing these values after the installation is complete.
### Table 25: NPI Timeseries Service settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeseries.datasource</td>
<td>The timeseries data source. Currently, timeseries data is stored on Kairos DB that is integrated with Apache Cassandra.</td>
<td>kairosdb</td>
</tr>
<tr>
<td>timeseries.data.retention</td>
<td>It is the data retention period for timeseries data in days. For more information about this setting, see Configuring retention period for timeseries data section in Installing and Configuring IBM Network Performance Insight.</td>
<td>1 Year</td>
</tr>
</tbody>
</table>

### Table 26: NPI Common settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage.jdbc-service</td>
<td>Used to build the path to storage location with http port for JDBC service.</td>
<td><code>&lt;myserver.ibm.com&gt;</code>:13081</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This setting is required only if the Storage Service is not installed on all Network Performance Insight node hosts.</td>
<td></td>
</tr>
<tr>
<td>kafka.zk-connect</td>
<td>ZooKeeper URL with Kafka znode. The string <code>{{zookeeper.connect}}</code> is populated with settings in <code>zookeeper.connect</code>.</td>
<td><code>{{zookeeper.connect}}</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This setting need not be changed.</td>
<td></td>
</tr>
<tr>
<td>kafka.broker-list</td>
<td>List of Kafka brokers. The string <code>{{kafka.broker-list}}</code> is populated with cluster's Kafka hosts and ports.</td>
<td><code>{{kafka.broker-list}}</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This setting need not be changed.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 27: NPI Manager settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>manager.ambari.user</td>
<td>Ambari user name</td>
<td>admin</td>
</tr>
<tr>
<td>manager.ambari.password</td>
<td>Ambari password</td>
<td>admin</td>
</tr>
</tbody>
</table>

To set or edit the networking time outs for resiliency in DNS resolution:
Table 28: **NPI DNS Service** settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns.server.address</td>
<td>DNS Server address. If this value is not specified, it is resolved from the system's <code>/etc/resolv.conf</code> file.</td>
<td></td>
</tr>
<tr>
<td>dns.server.port</td>
<td>DNS Server port</td>
<td>53</td>
</tr>
<tr>
<td>dns.network.initiation.timeout</td>
<td>The maximum amount of time that the DNS Server waits in <code>Disconnected</code> state before it attempts to connect to the DNS Server again.</td>
<td>30 Seconds</td>
</tr>
<tr>
<td>dns.network.connection.timeout</td>
<td>The maximum amount of time that the DNS Server waits in <code>Connecting</code> state for the networking layer to respond that the connection is established.</td>
<td>10 Seconds</td>
</tr>
<tr>
<td>dns.network.acknowledgement.timeout</td>
<td>The maximum amount of time that the DNS Server waits in <code>Waiting</code> state for the networking layer to respond to with an acknowledgment that the outbound packet is written to the operating system or networking buffers.</td>
<td>5 Seconds</td>
</tr>
<tr>
<td>dns.network.disconnect.timeout</td>
<td>The maximum amount of time that the DNS Server waits in <code>Disconnecting</code> state before it resets and moves to <code>Disconnected</code> state to close the connection.</td>
<td>5 Seconds</td>
</tr>
</tbody>
</table>
Table 29: **NPI Web Services** settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>https.port</td>
<td>The https port on which Network Performance Insight application console can be accessed.</td>
<td>9443</td>
</tr>
</tbody>
</table>

Setting up the UI Service to render data from Timeseries Service

Use these steps to configure the UI service to retrieve the data from Timeseries Service instead of the Storage Service to render on the Network Performance Insight Dashboards.

**About this task**

For more information about the Timeseries Service functionality, see Timeseries Service in *IBM Network Performance Insight: Product Overview*.

**Procedure**

1. Log in to Ambari server dashboard.
   
   Use the following default URL:
   
   `http://<myserver.ibm.com>:8080`
   
   The default user name is admin, and the default password is admin.
2. Click **Services > NPI > Configs > Advanced**.
3. Expand the **Advanced npi-env** pane and add the following lines in content text area:

   ```
   ui.timeseries.rest.url="http://<myserver.ibm.com>:31081"
   ```

   Where, `<myserver.ibm.com>` is the server where Timeseries Service is available.
4. Click **Save** to save the configuration.
5. Restart the UI Service as follows:
   
   a) Click **Services > NPI**.
   
   b) Click **Service Actions > Restart UIs**.

Setting up Flow Collector Service

Use these steps to set up the Flow Collector Service.

**Procedure**

1. Click **Services > NPI > NPI Settings**.
2. Change the default values in the following fields:

   Make sure that you are in the **Configs** tab if you are changing these values after the installation is complete.

Table 30: **NPI Components > NPI Flow Collector** settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>collector.flow.udp.ports</td>
<td>The UDP ports that the Flow collector listens to for Flow packets.</td>
<td>4379</td>
</tr>
</tbody>
</table>

**Note:** Make sure that the flow enabled devices are sending the data to the Flow collector from the same port, 4379.
Table 30: NPI Components > NPI Flow Collector settings. (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>collector.flow.sctp.ports</td>
<td>The SCTP ports that the Flow collector listens to for Flow packets.</td>
<td>4381</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure that the flow enabled devices are sending the data to the Flow collector from the same port, 4381.</td>
<td></td>
</tr>
<tr>
<td>collector.flow.exporter.blacklist</td>
<td>Comma-separated list of IP addresses in square brackets. The flow data from these exporters in the list is blocked from further processing.</td>
<td>ipAddress1, ipAddress2</td>
</tr>
<tr>
<td>collector.flow.art.dscp.whitelist</td>
<td>Comma-separated list of IP DSCP, which are integer values in the range 0 - 255 to enable ART. This setting is to enable the traffic classes that must be monitored. You can further control the applications with the specified traffic classes for ART enablement. See Configuring NBAR section in Installing and Configuring IBM Network Performance Insight.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To use this option, ensure that ipDiffServCodePoint Flow field is enabled in your ART data template.</td>
<td></td>
</tr>
<tr>
<td>collector.flow.max-interfaces</td>
<td>The maximum number of interfaces that the collectors collect from Network Performance Insight agent node.</td>
<td>1000</td>
</tr>
</tbody>
</table>

Setting up the OMNIbus Standard Input probe
The Standard Input probe is bundled with Network Performance Insight and is installed along with it.

About this task
Most of the configuration settings are done when you install Network Performance Insight. Follow these steps to work with OMNIbus Standard Input probe:

Procedure
1. Configure the host name resolution to resolve omnihost to the actual host name where Tivoli Netcool/OMNIbus is installed. Add an alias entry in the /etc/hosts file on all systems where Network Performance Insight services are installed as follows:

   `<IP_Address> <fully_qualified_host_name> <alias> omnihost`

   For example:

   `192.0.2.0 <myserver.ibm.com> myserver omnihost`
**Note:** This step must be performed on all Network Performance Insight node hosts where the Event Service is installed.

2. Ensure that you have the following 32-bit RHEL operating system libraries:
   - zlib
   - ncurses
   - bzip2
   - libstdc++

3. Follow the steps in Configuring non-default ObjectServer name section in Installing and Configuring IBM Network Performance Insight if you have a non-default Object Server name.

4. **Note:** Change or add these settings only when recommended by IBM Professional Services.

Optional: Modify these settings for Tivoli Netcool/OMNIbus Standard Input (STDIN) probe to send events to OMNIbus. Follow these steps:

a) Click **Services > NPI >Configs > Advanced.**

b) Expand **Advanced npi-env** section and enter the following lines in the **content** text area:

   ```
   event.netcool.home = "<netcool_installation_directory>"
   event.netcool.omnibus.home = "<omnibus_installation_directory>"
   event.netcool.omnibus.temp = "<temp_directory_for_log_files>"
   event.netcool.omnibus.stdin.args = "<additional_probe_command_line_args>"
   event.netcool.omnibus.stdin.props = "<omnibus_stdin_probe_properties_file_location>"
   event.netcool.omnibus.stdin.rules = "<omnibus-stdin-probe-rules-file_location>"
   ```

Where

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>event.netcool.home</td>
<td>Root installation directory for your Netcool products</td>
<td>$NCHOME $NCHOME defaults to /opt/IBM/tivoli/netcool.</td>
</tr>
<tr>
<td>event.netcool.omnibus.home</td>
<td>Root OMNIbus Installation directory</td>
<td>$NCHOME/omnibus</td>
</tr>
<tr>
<td>event.netcool.omnibus.temp</td>
<td>Temp directory where the log files are located.</td>
<td>$NPI_HOME/npi-event/stdin-probe/omnibus/probes/omnibus/var</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, $NPI_HOME is opt/IBM/npi.</td>
</tr>
<tr>
<td>event.netcool.omnibus.stdin.args</td>
<td>You can configure the STDIN probe to log at different levels (for example, DEBUG). For more information, see Configuring logging in Troubleshooting IBM Network Performance Insight Anything that is specified in this setting is passed directly on the command line to the STDIN probe at startup.</td>
<td>-messagelevel INFO - messagelog /var/tmp/stdinprobe.DEBUG.log Or -messagelevel DEBUG -raw</td>
</tr>
</tbody>
</table>
Table 31: Configurations for OMNIbus STDIN probe. (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>event.netcool.omnibus.stdin.props</td>
<td>STDIN probe properties file location</td>
<td>&lt;NPI_HOME&gt;/npi-event/stdin-probe/omnibus/probes/omnibus/stdin.props</td>
</tr>
<tr>
<td>event.netcool.omnibus.stdin.rules</td>
<td>STDIN probe rules file location</td>
<td>&lt;NPI_HOME&gt;/npi-event/stdin-probe/omnibus/probes/omnibus/stdin.rules</td>
</tr>
</tbody>
</table>

See Configuring non-default ObjectServer name section in Installing and Configuring IBM Network Performance Insight.

Setting up integration with
Use this information to set up the federation between and to work correctly and to access the web-based visualizations.

Perform these tasks during fresh installation scenarios where you are doing the integration for the first time.

Editing the configuration files
Edit the custom.cfg configuration file according to your environment and use these files in all the required integration tasks for and .

About this task
You must edit these files only once before you start the integration.

Procedure
Update the following fields in the file custom.cfg file that are specific to the instance that you want to use for integration:

By default, the custom.cfg file is located in /opt/IBM/basecamp/basecamp-installer-tools/dash-integration folder.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DASH_ENABLE_OPTION</td>
<td>If integration is to be included, specify TRUE. If integration is not required, specify FALSE.</td>
<td>TRUE</td>
</tr>
<tr>
<td>DASH_CONNECTION</td>
<td>Set the FQDN hostname of the server.</td>
<td>root@&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or &lt;non-root-user&gt;@&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>DASH_SSH_PORT</td>
<td>If non default port number is used, update the SSH port.</td>
<td>22</td>
</tr>
<tr>
<td>WEBSHERE_APP_SERVER_PATH</td>
<td>WebSphere Application Server installation path on server.</td>
<td>/opt/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td>JAZZSM_PATH</td>
<td>installation path.</td>
<td>/opt/IBM/JazzSM</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>DASH_USERNAME</td>
<td>administration user.</td>
<td>smadmin</td>
</tr>
<tr>
<td>DASH_PASSWORD</td>
<td>administration user password.</td>
<td>netcool</td>
</tr>
<tr>
<td>KEYSTORE_OPTION</td>
<td>USE_DEFAULT_KEY or USE_EXIST_KEY</td>
<td>USE_DEFAULT_KEY</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you want to reuse your existing key, use the USE_EXIST_KEY.</td>
<td></td>
</tr>
<tr>
<td>EXIST_KEYSTORE_FILEPATH</td>
<td>Location of the keystore</td>
<td>/tmp/keystore.security</td>
</tr>
<tr>
<td>EXIST_CA_FILEPATH</td>
<td>CA certificate file location</td>
<td>/tmp/ca.crt</td>
</tr>
<tr>
<td>KEYSTORE_PASSWORD</td>
<td>Password for the keystore</td>
<td>changeit</td>
</tr>
<tr>
<td>KEY_PASSWORD</td>
<td>Password for key</td>
<td>changeit</td>
</tr>
<tr>
<td>ALIAS</td>
<td>Alias name</td>
<td>npi</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Domain name</td>
<td>*.domain.name</td>
</tr>
<tr>
<td>ORG_NAME</td>
<td>Organization name</td>
<td>DEMO</td>
</tr>
<tr>
<td>LOCALITY</td>
<td>Locality</td>
<td>DEMO_LOCALITY</td>
</tr>
<tr>
<td>STATE</td>
<td>State</td>
<td>DEMO_STATE</td>
</tr>
<tr>
<td>COUNTRY</td>
<td>Country</td>
<td>&lt;MY&gt;</td>
</tr>
<tr>
<td>WAS_PROFILE_NAME</td>
<td>WebSphere Application Server profile for on the target application server.</td>
<td>JazzSMProfile</td>
</tr>
<tr>
<td>WAS_NODE</td>
<td>The default server node for the WebSphere Application Server profile.</td>
<td>JazzSMNode01</td>
</tr>
<tr>
<td>WAS_SERVER_NAME</td>
<td>Name of the application server that is specified when the application server profile is created.</td>
<td>server1</td>
</tr>
<tr>
<td>WAS_PROFILE_PATH</td>
<td>Location of the application server profile.</td>
<td>/opt/IBM/JazzSM/profile/</td>
</tr>
<tr>
<td>NPI_UI_HOST</td>
<td>Host where the UI service is installed.</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
</tbody>
</table>

**Installing the security services**

If your environment does not have, you cannot install the to obtain the security services. In such a scenario, install the security services that are bundled with to access the web-based visualizations from Console Integration on.

**About this task**

Security Services is bundled in /opt/IBM/basecamp/basecamp-installer-tools/dash-integration/security-service.
Procedure
Run the `installSecurityService.sh` script that is available in `/opt/IBM/basecamp/basecamp-installer-tools/dash-integration` as follows:

```
cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
sudo `pwd`/installSecurityService.sh -default=`pwd`/default.cfg -custom=`pwd`/custom.cfg
```

The following tasks are performed after this script is run:

- Detects whether the security services are already available or not and proceeds to install only if it is not available.
- JazzSM_Home/security folder is created.
- Copies the `com.ibm.tivoli.ac.ess.authnsvc_1.1.2.201501192348.zip` file from `/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/security-service` to JazzSM_Home/security.
- Extracts the `com.ibm.tivoli.ac.ess.authnsvc_1.1.2.201501192348.zip` file.

Creating console integration
Use this information to create the console integration.

About this task
In the earlier releases of , console integration is performed automatically with the installation of that comes with . Starting from V, console integration can be performed with the `createConsoleIntegration.sh` script that is available in the following directory: `/opt/IBM/basecamp/basecamp-installer-tools/dash-integration`

Procedure
Run the `createConsoleIntegration.sh` script as follows:

```
sudo `pwd`/createConsoleIntegration.sh -default=`pwd`/default.cfg -custom=`pwd`/custom.cfg
```

Results
If the script runs successfully, the console content is available in the navigation bar of the Dashboard Application Services Hub through the icon.

Log in with npiadmin and netcool credentials and click `Console Settings > Console Integrations` in the navigation bar to see the integration.

For troubleshooting console integration, see `Missing console integration icon` in .

Generating the certificate and keystore files
Generate the certificate authority (CA) certificates and other keystore files on Ambari server.

Procedure
Generate `ca.crt` key store file by using the following command as root user:

Run the following command in a single line:

```
cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
< DASH_INTEGRATION_PATH >/securityKeyTool.sh
-default=< DASH_INTEGRATION_PATH >/default.cfg
-custom=< DASH_INTEGRATION_PATH >/custom.cfg
```

Where `<DASH_INTEGRATION_PATH>` is `BASECAMP_INSTALLER_TOOLS_DIR/dash-integration`
For example:

```
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/securityKeyTool.sh
 -default=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.cfg
 -custom=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/custom.cfg
```

What to do next
Check these log files in the /tmp directory for any errors:

- ambari_npi_key_startup.log
- securityKeyTool.<timestamp>.log
- genSecurityKey.log

Related tasks
“Installing Network Performance Insight” on page 17
Install HDP® and Network Performance Insight on a single host or multi-host environments.

Enabling integration with
Use this information to enable integration between and portal.

Before you begin
Make sure that Object Server is up and running.

Procedure
Run the integration script as root user as follows:

By default, the npiDashIntegration.sh script is located in /opt/IBM/basecamp/basecamp-installer-tools/dash-integration folder.

```
# <DASH_INTEGRATION_PATH>/npiDashIntegration.sh
 -default=<DASH_INTEGRATION_PATH>/default.cfg
 -custom=<DASH_INTEGRATION_PATH>/custom.cfg
```

Where <DASH_INTEGRATION_PATH> is BASECAMP_INSTALLER_TOOLS_DIR/dash-integration.

For example:

```
cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/npiDashIntegration.sh
 -default=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.cfg
 -custom=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/custom.cfg
```

After the completion of this command, the following tasks are done:

- The dash-integration directory is created at the same level as the WebSphere Application Server based on the value set in the WEBSPHERE_APP_SERVER_PATH field in custom.cfg file. By default, it is /opt/IBM/dash-integration
- The following files are transferred to the dash-integration directory:
  - enableDash.sh
  - signkey
  - eWasAddUsersAndGroups.py
  - priv_key.key
  - ca.crt (Not copied if KEYSTORE_OPTION value is USE_EXIST_KEY)
  - install.User.cfg (Not copied if KEYSTORE_OPTION value is USE_EXIST_KEY)
- The enableDash.sh script is run at the dash-integration directory.
- dashboarduser group that is required to access the is created.
What to do next

Check these log files for any errors:

- /tmp/npiDashIntegration.log
  
  **Note:** This log file is available on the Ambari server from where the integration script is run.

- /tmp/enableDash.log
  
  **Note:** This log file is available on server where is running.

Setting up communication with on Ambari

These settings are pre-populated on Ambari for communicating with Jazz for Service Management.

Procedure

1. Open a browser and access the Ambari server dashboard.
   
   Use the following default URL: http://<myserver.ibm.com>:8080
   
   The default user name is admin, and the default password is admin.

2. Click **Services > NPI**.

3. Make sure that you are in the **Configs** tab.

4. Click **NOI Core Settings > NOI Services** and change the values in the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>web.auth</td>
<td>Single sign-on mode. Select <strong>DASH</strong> for Jazz for Service Management managed LDAP user repository.</td>
<td>DASH</td>
</tr>
<tr>
<td>security.dash.username</td>
<td>Administrator user name for Jazz for Service Management for security service</td>
<td>smadmin</td>
</tr>
<tr>
<td>security.dash.password</td>
<td>Password for Jazz for Service Management administrator user name</td>
<td>&lt;DASH_password&gt;</td>
</tr>
<tr>
<td>https.keystore.file</td>
<td>Full path for the keystore file that stores the SSL certificate that is used by Network Performance Insight.</td>
<td>/opt/IBM/basecamp/basecamp-ui/conf/security/security.keystore</td>
</tr>
<tr>
<td>https.keystore.password</td>
<td>Password for the SSL keystore that is used by Network Performance Insight.</td>
<td>changeit</td>
</tr>
<tr>
<td>https.key.password</td>
<td>Password for the SSL key that is used by Network Performance Insight.</td>
<td>changeit</td>
</tr>
</tbody>
</table>

5. Click **NPI > Advanced > Advanced npi-auth** and change the default values in the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>security.dash.hostnames</td>
<td>Full DNS name for the Jazz for Service Management server</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
</tbody>
</table>
Table 33: **Advanced > Advanced npi-auth Settings (continued)**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>security.dash.port</td>
<td>HTTPS port on which the Jazz for Service Management communicates.</td>
<td>16311</td>
</tr>
</tbody>
</table>

6. Save the configuration.
7. Restart all the services as follows:
   a) Click **Services > NPI**.
   b) Select **Restart All** from the **Service Actions** list.

Verification on the systems where services are installed:
8. Verify whether the `security.keystore` file is created in the following location:

   /opt/IBM/basecamp/basecamp-ui/conf/security

9. Check that the cacerts file with webSphereCACert alias is available in `/opt/IBM/basecamp/basecamp-ui/conf/security` directory by running the following command on all s:

   ```
   cd /opt/IBM/basecamp/basecamp-jre/java-1.8.0-openjdk.x86_64/jre/bin
   keytool -keystore /opt/IBM/basecamp/basecamp-jre/java-1.8.0-openjdk.x86_64/jre/lib/security/cacerts -storepass changeit -list -alias WebSphereCACert
   ```

10. Get the fingerprint from the keystore file, run the following command:

    ```
    keytool -keystore /opt/IBM/basecamp/basecamp-ui/conf/security/security.keystore -storepass changeit -list
    ```

11. Make sure that the trustedCertEntry certificate fingerprint of the npi_ca is same as the trustedCertEntry certificate fingerprint of the WebSphereCACert that is generated in step 9.

**Configuring the SSL communication for integration**
The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

**Before you begin**
Make sure that you have configured the passwordless login as described in **Setting SSH passwordless login** section in **Installing and Configuring IBM Network Performance Insight**

**About this task**
Configure SSL communication on Jazz for Service Management portal after you install Network Performance Insight.

You must configure the SSL one time only. If you are reinstalling or upgrading Network Performance Insight, back up the `security.keystore`, `priv_key.key`, which is the private key, and `ca.crt`, which is the public key if you plan to reuse them.

**Configuring SSL settings on WebSphere Application Server**
Use this information to define Secure Sockets Layer (SSL) configuration properties.

**Procedure**
1. Log in to Dashboard Application Services Hub as administrator user.
2. Select **Console Settings > General > WebSphere Administrative Console** in the console navigation.
3. Click **Launch WebSphere administrative console**.

Installing and configuring 97
4. Click Security > SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings from the list of Secure Socket Layer (SSL) configurations.

5. Update the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Suggested value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default server certificate alias</td>
<td>If it is not defined earlier, this setting specifies the certificate alias that is used as the identity for this SSL configuration.</td>
<td>netcool</td>
</tr>
<tr>
<td>Default client certificate alias</td>
<td>Specifies the description for a client certificate alias.</td>
<td>netcool</td>
</tr>
</tbody>
</table>

For rest of the settings, you can keep the prepopulated default values.

6. Click OK and save the changes to master configuration.

   **Note:** Make sure to convert all your certificates to use SHA256withRSA in WebSphere Application Server.

7. Verify that the netcool personal certificate is available in SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates.

8. Verify that the npi_ca signer certificate is available in SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates.

9. Restart the WebSphere Application Server.

10. Press y in the SSL Signer Prompt window if the signer certificate information is displayed.

**Related information**

Certificates must be converted to use SHA256withRSA in WebSphere Application Server

Restarting Jazz for Service Management application servers

*Adding the signer certificate to your browser*

The ca.crt file that is extracted from Jazz for Service Management must be imported to browser’s Trusted CA Certificate store.

*About this task*

This task must be done on all computers that access Network Performance Insight data for visualization. These steps differ on different browsers. Instructions are provided for Internet Explorer and Firefox.

**Procedure**

Perform these steps on Jazz for Service Management server.

- Go to the following location where Jazz for Service Management server is installed:
  
  /opt/IBM/dash-integration

- Copy the ca.crt signer certificate that is generated earlier to your local machine.

  Follow these steps on the browser on your local machine that you use to access the visualization dashboards.

- For Internet Explorer, follow these steps:
  
  a) Click Tools > Internet Options.
  b) Click Content > Certificates > Trusted Root Certification Authorities.
  c) Click Import.
  d) Browse to the location of the exported ca.crt file.
  e) Click Next.
  f) Select to place the certificates in Trusted Root Certification Authorities option and click Finish.
• For Firefox, follow these steps:
  a) Click **Tools > Options**.
  b) Click **Advanced > Certificates > View Certificates**.
  c) Click **Authorities > Import**.
  d) Browse to the location of the exported ca.crt file and click **Open**.
  e) Select all the check boxes on the **Downloading Certificate** page and click **OK**.
  f) Click **OK** to close the window.

• For Chrome, follow these steps:
  a) Click **Settings > Advanced > Manage certificates**.
  b) Click **Import**.
  c) Browse to the location of the exported ca.crt file and click **Open**.
  d) Select **Place all certificates in the following store** and click **Browse**.
  e) Select to place the certificate in **Trusted Root Certification Authorities** and click **OK**.
  f) Click **Next** and **Finish**.

**Related tasks**

"Enabling integration with Jazz for Service Management" on page 32
Use this information to enable integration between Network Performance Insight and Dashboard
Application Services Hub portal.

**Installing and setting up Remote Flow Collector**
You can optionally install the Flow Collector Service on a remote host as a cluster singleton to keep
the collector closer to your data center.

**Before you begin**
Make sure that the server where you are installing the Remote Flow Collector Service has connection to
RPM repository in Ambari server host.

**Procedure**

1. Copy the `<DIST_DIR>/NPI_1.3.0.0/bin/installRemoteFlowCollector.sh` file from Ambari
   server to the host where you want to install Remote Flow Collector.
2. Run the `installRemoteFlowCollector.sh` script as root user as follows:

   ```
   ./installRemoteFlowCollector.sh <yum-repo-server> <yum-repo-port>
   ```

   Where:
   - `<yum-repo-server>` is the server where the Ambari server is installed.
   - `<yum-repo-port>` is the HTTPD port 9091 that is used by Ambari server for components installation
     in the cluster.

   The following components are installed:
   - Remote Flow Collector Service
   - JRE
   - Kafka
   - Zookeeper

   Zookeeper server and Kafka are set up in the `/usr/iop/current` folder.
3. Set up the connection between the Flow Collector and Remote Flow Collector through Ambari by using
   the following steps:
   a) Open a browser and access the Ambari server dashboard.

Installing and configuring 99
Use the following default URL:
http://<myserver.ibm.com>:8080

**Note:** You can use the fully qualified domain name (FQDN) or the IP address of the server.
The default user name is admin, and the default password is admin.

b) Click **Services > NPI > Configs > Advanced.**
c) Expand the **Advanced npi-env** pane and add the following lines in **npi-env template** text area and provide the list of servers where Kafka services are available where Remote Flow Collectors are installed:

```plaintext
collector.flow.remote.kafkaBroker = ["<kafka1>:9092", "<kafka2>:9092"]
```

Where:

- *kafka1* and *kafka2* are the host names of the servers that have the Kafka Service running along with remote Flow Collector Service. For example, `<myserver.ibm.com>`.

**Note:** The ratio between remote and local collectors must be 1:1.

d) Start the services.

4. Optional: To change the port number of the ZooKeeper Service to resolve the port number conflict, perform the following steps:
   a) Update the following properties in `/opt/IBM/npi/npi-remote-flow-collector/conf/application.conf` file:
      ```plaintext
      main.zk-url = "localhost:<new_port_number>"
messaging.kafka.zk-connect = "localhost:<new_port_number>"
      ```
   b) Update the following properties in `/etc/kafka/conf/server.properties` file:
      ```plaintext
      zookeeper.connect=localhost:<new_port_number>
      ```

5. Start the following services:
   - Zookeeper
   - Kafka
   - Remote Flow Collector

6. Optional: To change the port numbers for UDP or SCTP protocols, update the following properties in `/opt/IBM/npi/npi-remote-flow-collector/conf/application.conf`:

```plaintext
collector.flow.udp.ports = <new_port_number>
collector.flow.sctp.ports = <new_port_number>
```

7. Start the following services in sequence by using the following command:
   a. Start Zookeeper Service
      ```bash
      sudo /usr/hdp/current/zookeeper-server/bin/zkServer.sh start
      ```
   b. Start Kafka Service
      ```bash
      sudo /usr/hdp/current/kafka-broker/bin/kafka start
      ```
   c. Start Remote Flow Collector
      ```bash
      sudo systemctl start npi-remote-flow-collector
      ```
Results

The Remote Flow Collector is available with the following default configurations in `/opt/IBM/npi/npi-remote-flow-collector/conf/application.conf` file:

```plaintext
collector.flow.udp.ports = [4379]
collector.flow.sctp.ports = [4381]
main.zk-url = "localhost:2181"
messaging.kafka.broker-list = "localhost:9092"
messaging.kafka.zk-connect = "localhost:2181"
```

**Note:** To restart the Remote Flow Collector Service, see *Controlling remote Flow Collector Service* in .

Check the log files for the collector in `npi-remote-flow-collector/logs` directory.

Check the log files for Zookeeper and Kafka in the following locations:

- `/var/log/zookeeper`
- `/var/log/kafka`

**Installing and setting up Remote SNMP Collector**

You can optionally install the SNMP Collector on a separate node to enhance the collection of SNMP metrics. You can set up to collect SNMP metrics alone and can be targeted to collect 100 million records per hour.

**Before you begin**

Compress the following microservices from any of the nodes in your cluster:

- `/opt/IBM/npi/npi-snmp-collector`
- `/opt/IBM/npi/npi-formula`
- `/opt/IBM/basecamp/basecamp-jre`

Use the following commands to create the compressed files for these microservices:

```plaintext
cd /opt/IBM/npi
rm -rfv npi.tar
chmod 777 npi-snmp-collector npi-formula
rm -rfv basecamp.tar
chmod 777 basecamp-jre

tar -cvf npi.tar npi-snmp-collector npi-formula

tar -cvf basecamp.tar basecamp-jre
```

**Procedure**

1. On a separate server where you want to install the SNMP Collector as cluster singleton, copy the following archived files:
   
   - `<npi.tar>`
   - `<basecamp.tar>`

2. Extract the archived files by using the following commands:

   ```plaintext
tar -xvf <npi.tar>
tar -xvf <basecamp.tar>
```

3. Edit the `application.conf` files in both `npi-snmp-collector` microservice as follows:

   ```plaintext
cd /opt/IBM/npi/npi-snmp-collector/conf
vi application.conf
```

Update the following lines with the host name of any node in your cluster:

**Note:** You can use the fully qualified domain name (FQDN) or the IP address of the server.

```plaintext
ams.collector.endpoint.hostname = "<npi_node_server>"
```
Set SNMP scoping as follows:

```yaml
snmp.consumer-group.suffix = "<local_server>"
snmp.npi.topic.data = "npi.snmp.poll.data-<local_server>"
snmp.npi.topic.definitions = "npi.snmp.poll.definitions-<local_server>"
```

Where `<local_server>` is the IP address of the fully qualified domain name (FQDN) of the server where SNMP Collector is installed.

4. Edit the `application.conf` files in both `npi-formula` microservice as follows:

```bash
cd /opt/IBM/npi/npi-formula/conf
vi application.conf
```

Update the following lines with the host name of any node in your cluster:

**Note:** You can use the fully qualified domain name (FQDN) or the IP address of the server.

```yaml
ams.collector.endpoint.hostname = "<npi_node_server>"
ams.collector.host = "<npi_node_server>"
ams.collector.port = 6188
main.zk-url = "<npi_node_server>:2182"
messaging.kafka.broker-list = "<npi_node_server>:6667"
messaging.kafka.zk-connect = "<npi_node_server>:2182"
storage.jdbc-service = "<npi_node_server>:13081"
storage.schema-registry.urls = "http://<npi_node_server>:8093"
storage.uri = "hdfs://<npi_node_server>:8020/npi/"
timeseries-service.hosts = [ "<npi_node_server>" ]
timeseries-service.port = 31081
```

Set SNMP scoping as follows:

```yaml
formula.entity-scope = "True"
snmp.consumer-group.suffix = "<local_server>"
snmp.npi.topic.data = "npi.snmp.poll.data-<local_server>"
snmp.npi.topic.definitions = "npi.snmp.poll.definitions-<local_server>"
```

Where `<local_server>` is the IP address of the fully qualified domain name (FQDN) of the server where SNMP Collector is installed.

5. Start the microservices with the following commands:

```bash
nohup bin/npi-snmp-collector &
nohup bin/npi-formula &
```

**Postinstallation tasks**
Perform these postinstallation tasks after the installation of Network Performance Insight is complete.

- If you have previously disabled firewall, enable the firewall on all nodes in your cluster. Use these commands:

```bash
systemctl start firewalld.service
systemctl enable firewalld
```

- Download and copy the MySQL database driver file by using the following steps:
Download the mysql-connector-java-5.1.16.jar file from the following link:
https://mvnrepository.com/artifact/mysql/mysql-connector-java/5.1.16

Copy the driver JAR file to /opt/IBM/npi/npi-cacti-collector/lib directory, and then start the Cacti Collector.

**Verifying the installation**

You can verify the Network Performance Insight 1.3 installation status.

**Before you begin**

Make sure that the flow exporter is configured and sending the flow data to the Collector subsystem.

For more information, see *Configuring Flow devices*.

**Procedure**

1. Verify the installation logs that are available at /tmp directory.

   To list all the log files, run the following command:

   ```bash
   ls -lrt /tmp/*.log
   ```

   You can see the following log files:

   ```
   install_2018039121342.log
   test_install_main.log
   apr_install.log
   apr_util_install.log
   httpd_install.log
   iop_http_repos.log
   iop_utils_http_repos.log
   ambari_http_repos.log
   npi_http_repos.log
   setupRepoServer.log
   ambari_repo_baseurl.log
   postgresql_libs_install.log
   postgresql_core_install.log
   postgresql_server_install.log
   ambari_server_install.log
   ambari_server_setup.log
   ambari_server_start.log
   setupAmbari.log
   ambari_npi_startup.log
   setupNpiServiceStack.log
   dashkey.log
   npiDashIntegration.log
   setupGenKeyTool.log
   ambari_npi_key_startup.log
   ```

   **Note:** Dashboard Application Services Hub integration script execution log file is located here:

   ```bash
   <DASH_Host>/tmp/enableDash.log
   ```

   For more information about log files, see *Log files in Network Performance Insight* in *Troubleshooting IBM Network Performance Insight*.

2. Run the following yum command to list all the installed packages in the current version:

   ```bash
   # yum list installed | egrep "npi|basecamp"
   ```

   Sample output:
# yum list installed | egrep "npi|basecamp"

```
apr.x86_64                              1.5.2-<build_signature>  @npi
apr-util.x86_64                          1.5.2-<build_signature>  @npi
basecamp-connect.noarch                  1.2.3.0-<build_signature>  @npi
basecamp-entity-analytics.noarch         1.2.3.0-<build_signature>  @npi
basecamp-httpd.noarch                   1.2.3.0-<build_signature>  @npi
basecamp-installer-tools.noarch         1.2.3.0-<build_signature>  @npi-1.2.3.0
basecamp-jre.x86_64                      1.2.3.0-<build_signature>  @npi
basecamp-manager.noarch                 1.2.3.0-<build_signature>  @npi
basecamp-repo.noarch                    1.2.3.0-<build_signature>  @npi-1.2.3.0
basecamp-schema-registry.noarch         1.2.3.0-<build_signature>  @npi
basecamp-spark.noarch                   1.2.3.0-<build_signature>  @npi
basecamp-storage.noarch                 1.2.3.0-<build_signature>  @npi
basecamp-tools.noarch                   1.2.3.0-<build_signature>  @npi
basecamp-ui.noarch                      1.2.3.0-<build_signature>  @npi
httpd.x86_64                            2.4.18-<build_signature>  @npi
mailcap.noarch                          2.1.31-<build_signature>  @npi
npi-ambari.noarch                       1.2.3.0-<build_signature>  @npi-1.2.3.0
npi-cacti-collector.noarch              1.2.3.0-<build_signature>  @npi-1.2.3.0
npi-dns.noarch                          1.2.3.0-<build_signature>  @npi
npi-event.i386                           1.2.3.0-<build_signature>  @npi
npi-flow-analytics.noarch                1.2.3.0-<build_signature>  @npi
npi-flow-collector.noarch                1.2.3.0-<build_signature>  @npi
npi-formula.noarch                       1.2.3.0-<build_signature>  @npi
npi-itnm-collector.noarch                1.2.3.0-<build_signature>  @npi
npi-repo.noarch                          1.2.3.0-<build_signature>  @npi-1.2.3.0
npi-snmp-collector.noarch                1.2.3.0-<build_signature>  @npi
npi-snmp-discovery.noarch                1.2.3.0-<build_signature>  @npi-1.2.3.0
npi-threshold.noarch                     1.2.3.0-<build_signature>  @npi
postgresql.x86_64                        9.2.14-1.<build_signature>  @npi
postgresql-libs.x86_64                   9.2.14-1.<build_signature>  @npi
postgresql-server.x86_64                 9.2.14-1.<build_signature>  @npi
```

## Verifying the status of Standard Input probe
You can verify the status of Standard Input probe that is packaged with .

### Before you begin
Ensure that you have installed and verified the status as running.

### Procedure

1. Check the status of the Event Service by using the following command:

   ```bash
   <NPI_Home>/basecamp/basecamp-manager/bin ./basecamp-manager-cmd status
   ```

2. Run the following command to check the status of Standard Input probe on the node that has the oldest to make sure that the probe is installed successfully:

   ```bash
   ps -ef | grep nco_p_stdin
   ```

   Check the process ID of the probe that is displayed.

   For more information, see Configuring the OMNIbus Standard Input probe to work with Network Performance Insight in .

### Related tasks

“Verifying the installation” on page 40
You can verify the Network Performance Insight 1.3 installation status.

“Setting up the OMNIbus Standard Input probe” on page 28
The Standard Input probe is bundled with Network Performance Insight and is installed along with it.

### Installation directory structure
Use this information to understand the important directories that are created during installation.

These directories are created in /opt/IBM/ path:
**basecamp**

The `basecamp` directory contains the following subdirectories:

**basecamp-connect**
Contains the Kafka connect script that is called from Ambari to start the service. It also contains the JDBC driver files that are needed to connect to IBM Db2, Oracle, and for Kafka to connect to database.

**basecamp-exporter**
Contains the directories and files that are needed to integrate with .

**basecamp-installer-tools**
This directory is available on the Ambari server host only. It contains the following subdirectories:

- `ambari` contains the scripts that are needed for Ambari management.
- `dash-integration` contains scripts:
  - Scripts that are needed for and integration.
  - Installing and uninstalling the security services
  - Creating and deleting console integration

The `dash-integration` directory also has `security-service` subdirectory that contains the bundled security services software.

- `ootb_packs`
  Contains the ready-to-use Technology Packs that can be installed in system for discovery and polling for resources.

- `pack_installer`
  Contains the `pack-install.sh` script to install the Technology Pack and distribute the content to different services.

- `snmp`
  Contains the `snmp-scoping.sh` script to filter and restrict the devices and resources for network polling.

- `upgrade`
  Contains scripts that are needed for upgrading to :
  
  - `credential-migration`
    Contains the `snmp-credential-migration.sh` script and JAR files for porting the existing Kafka and Flow device credentials to the new environment.

**basecamp-jre**
Contains the Open Java SDK that is bundled with .

**basecamp-manager**
Contains the directories and files that are needed for the Manager Service to function. It also contains the license files for .

**basecamp-schema-registry**
Schema Registry provides a serving layer for your metadata. It stores a versioned history of all schemas, provides multiple compatibility settings, and allows evolution of schemas according to the configured compatibility setting.

**basecamp-storage**
Contains the directories and files that are needed for Storage Service to function.

**basecamp-timeseries**
Contains the directories and files that are needed for Timeseries Service to function. It has the following important additional sub directories:

- `3rdParty`
  Contains Apache Cassandra and Kairos DB for timeseries data.
• **content/metrics**
  Contains all the metrics to be collected. Each metric file is identified with an extension `.metric`. For example, `Network-Inbound-Discards-Count.metric`.

**basecamp-tools**
Contains the encryption script, `npm-encrypt.sh` that can be used to encrypt passwords.

**basecamp-ui**
Contains the directories and files that are needed for UI Service to function.

It also contains the following files and directories that are needed for:

• **resources/dashboards**
  Contains the following sub directories:
  - `json`
    Contains all the dashboard JSON files that are successfully parsed and loaded after the installation in `good` directory and those dashboards that failed to load are in the `bad` directory. The JSON files that are under process are placed in `processing` directory.
  - `properties`
    Contains all the dashboard properties files.

• **resources/oed**
  Contains the following files and subdirectory:
  - `oed.war`
    It is the application engine WAR file.
  - `sql`
    Contains the SQL files that are related to the dashboards.

• **work/oed**
  This directory is a symbolic link to `basecamp/work/basecamp-ui/oed`. Contains the H2 database file as `oed.mv.db`.

**npi**

*npi* directory contains the following sub directories:

**npi-cacti-collector**
Contains the directories and files that are needed for Cacti Collector Service to function.

• **resources**
  Contains the following files:
  - `PODS.zip`
  - `MIB2.zip`
  - `CiscoIPSLA.zip`
  - `cacti_reflector-1.0.0.tgz`

**npi-dns**
Contains the directories and files that are needed for DNS Service to function.

**npi-event**
Contains the directories and files that are needed for Event Service to function. 64-bit STDIN probe is available in this directory and can be supported on Linux, AIX, and Solaris platforms.

**npi-flow-analytics**
Contains the directories and files that are needed for Analytics Aggregation Service to function.

**npi-flow-collector**
Contains the directories and files that are needed for Flow Collector Service to function.
**npi-formula**
Contains the directories and files that are needed for Formula Service to calculate formulas on the IP SLA metrics based on the data that is collected by the SNMP Collector Service. It also has the collection formulas and their related MIB files for polling the network for metrics. It has the following additional directories:

- **content**
  - bindings
    Contains the class files for the MIB OBJECT_TYPES that are used in the collection formulas.
  - formulas
    Contains all the collection formulas that are used for metric polling.
  - mibs
    Contains all the MIB files that are required for your formulas.

**npi-itnm-collector**
Contains the directories and files that are needed for Tivoli Network Manager - Collector Service to function.

- **discovery**
  Contains all the required folders and files for performing the second-level discovery by . Typically, devices are discovered by and all the resource types from those devices are discovered by . In scenario, you can write your own discovery formulas and use them to do SNMP device discovery independent of .

- **content**
  Contains the discovery formula files and MIB files that are extracted from technology pack content. The discovery files are arranged according to the vendor. The vendor-specific directories are manually created for organizing the discovery files. All the MIB files that are required for discovery formulas are placed in the /content/mibs directory.

- **device**
  Contains the sysobjectid.discovery file that is required for discovering the new devices.

**npi-snmp-collector**
Contains the directories and files that are needed for SNMP Collector Service that provides metric polling data from IP SLA enabled SNMP devices to .

**npi-snmp-discovery**
Contains the directories and files that are needed for accessing the devices with SNMP credentials to obtain and store the data for enriching the interfaces.

**npi-threshold**
Contains the directories and files that are needed for Threshold Service to function.

Typically, all the microservices have the directory stack as follows:

```
<NPI_Service>
  ... bin
  ... conf
  ... lib
  ... logs
  ... var
  ... work

The logs directory contains a separate log file for each microservice.
```

Installing and configuring 107
Uninstalling
Uninstall and the related software from the system.

Before you begin
Before you uninstall, back up the following contents:

- Manually, back up the `/opt/IBM/basecamp/basecamp-installer-tools` folder in the Ambari Server host to save the previous configuration.
- Make sure to back up the following files from `/opt/IBM/basecamp/basecamp-installer-tools/dash-integration` directory if you plan to reuse them:
  - `security.keystore`
  - `priv_key.key` - private key
  - `ca.crt` - public key

About this task
Uninstall the following components that you installed:

- , including YARN, HDFS, and Zookeeper services.
- Ambari agents that contain Network Operations Insight instances.
- Ambari server

To uninstall all these components, follow these steps:

Procedure
1. Log in to Ambari server host as follows:
   `http://<ambari_server_host>:8080`
2. Click **Services** and select the specific service and click the **Configs** tab.
3. Note down the following directories for the services and components:

<table>
<thead>
<tr>
<th>Services</th>
<th>Ambari Component directory</th>
<th>Example installation path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kafka</td>
<td>Kafka &gt; Configs &gt; Kafka Broker &gt; log.dirs</td>
<td><code>&lt;data&gt;/kafka-logs</code></td>
</tr>
</tbody>
</table>
## Services

<table>
<thead>
<tr>
<th>Services</th>
<th>Ambari Component directory</th>
<th>Example installation path</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HDFS</strong></td>
<td>HDFS &gt; Configs &gt; Settings &gt; NameNode</td>
<td>&lt;data&gt;/hadoop/hdfs/namenode</td>
</tr>
<tr>
<td></td>
<td>HDFS &gt; Configs &gt; Settings &gt; DataNode</td>
<td>&lt;data&gt;/hadoop/hdfs/datanode</td>
</tr>
<tr>
<td></td>
<td>HDFS &gt; Configs &gt; Advanced &gt; Secondary NameNode &gt; SecondaryNameNode Checkpoint directories</td>
<td>&lt;data&gt;/hadoop/hdfs/namesecondary</td>
</tr>
<tr>
<td><strong>YARN</strong></td>
<td>YARN &gt; Configs &gt; Advanced &gt; Application Timeline Server &gt; yarn.timeline-service.leveldb-timeline-store.path</td>
<td>&lt;data&gt;/var/log/hadoop-yarn/timeline</td>
</tr>
<tr>
<td><strong>YARN</strong></td>
<td>YARN &gt; Configs &gt; Advanced &gt; Advanced yarn-site &gt; yarn.timeline-service.leveldb-state-store.path</td>
<td>&lt;data&gt;/hadoop/yarn/timeline</td>
</tr>
<tr>
<td><strong>Ambari Metrics</strong></td>
<td>Ambari Metrics &gt; Configs &gt; Advanced ams-hbase-site &gt; hbase.rootdir</td>
<td>&lt;data&gt;/var/lib/ambari-metrics-collector/hbase</td>
</tr>
<tr>
<td><strong>ZooKeeper</strong></td>
<td>ZooKeeper &gt; Configs &gt; ZooKeeper Server &gt; ZooKeeper directory</td>
<td>&lt;data&gt;/hadoop/zookeeper</td>
</tr>
</tbody>
</table>

### Note:
<code>data</code> is the full directory path where you have set up all the services.

### Uninstalling Network Performance Insight node

Run the `host_cleanup.sh` script to uninstall the Ambari Server hosts and Network Performance Insight node hosts.

### Before you begin
- Stop all the services for each host from Ambari.
- Back up your data.

### Procedure

1. Copy the `host_cleanup.sh` script from `/opt/IBM/basecamp/basecamp-installer-tools/ambari/host_cleanup.sh` to the Network Performance Insight Nodes that you want to uninstall.
   
   For example, `/tmp/host_cleanup.sh`.

2. Run the script as `root` user as follows:

   ```bash
   cd /tmp
   ./host_cleanup.sh
   ```

   The `host_cleanup.sh` script performs the following functions:
   - Checks the user who is running the script is `root` or not
   - Checks for the `HostCleanup.ini` file
• Stops the Ambari Server and the Network Performance Insight node, if they are still running.
• Stops the Linux processes that are started by a list of service users. The users are defined in the HostCleanup.ini file. You can also specify a list of Linux processes to be stopped.
• Removes the PRM packages that are listed in the HostCleanup.ini file.
• Removes the Network Performance Insight packages and working folders.
• Removes the service users that are listed in the HostCleanup.ini file.
• Deletes directories, symbolic links, and files that are listed in the HostCleanup.ini file.
• Deletes repositories that are defined in the HostCleanup.ini file.

Related information
Cleaning up nodes before reinstalling software

Uninstalling Ambari server host
Use the cleanup scripts to remove the Ambari server host, which is the master node.

Procedure
1. Move the uninstallation scripts from /opt/IBM/basecamp/basecamp-installer-tools/ambari to /tmp directory.
2. Run the cleanup scripts as root user on the Ambari server in the following order:
   ```
   /tmp/host_cleanup.sh
   /tmp/cleanup.sh
   ```
   Note: Ignore the error messages from cleanup.sh as most of the uninstallation is done by the host_cleanup.sh script.

   Ambari Server and all the Network Performance Insight microservices are removed.
3. Remove all the working directories that are listed previously.
   For more information, see “Listing working directories” on page 49.

Removing Dashboard Application Services Hub integration
Use this information to remove the directories and settings that are related to Dashboard Application Services Hub integration.

Procedure
1. Log in to Dashboard Application Services Hub as administrator user.
2. In the navigation pane, click Console Settings > Websphere Administrative Console and click Launch Websphere administrative console.
3. Click Security > SSL certificate and key management.
4. Under Related items on the right, click SSL configurations > NodeDefaultSSLSessions.
5. Change the Default server certificate alias and Default client certificate alias to Default.
6. Click OK and save the changes to master configuration.
7. Click Key stores and certificates > NodeDefaultKeyStore > Personal certificates and remove the netcool certificate.
8. Save the changes to master configuration.
9. Click Key stores and certificates > NodeDefaultTrustStore > Signer certificates and remove the npi-ca certificate.
10. Save the changes to master configuration.
11. Restart WebSphere Application Server.
12. Remove the /opt/IBM/dash-integration directory.
Uninstalling Remote Flow Collector
Use these steps to uninstall all the Remote Flow Collectors.

Before you begin
Stop the Remote Flow Collector Service. For more information, see Stopping the Remote Flow Collector
associated services in Administering IBM Network Performance Insight.

Procedure
Run these manual commands on the servers where you set up the Remote Flow Collectors to erase the
packages:

```
yum erase -y npi-remote-flow-collector
yum erase -y zookeeper_2.6.4.0.91
yum erase -y hdp-select
yum erase -y ranger_2.6.4.0.91-kafka-plugin
yum erase -y basecamp-jre
```

What to do next
After the uninstallation is complete, perform the following steps:

- Remove the .repo files from /etc/yum.repos.d directory if they exist:
  - npi.repo
  - hdp.repo
- Remove the following folders:
  - /data/kafka-logs
  - /var/log/zookeeper
  - /var/lib/zookeeper

Troubleshooting installation
Problems that might occur during an installation and how to resolve them.

About this task
For all troubleshooting issues in installation of, see Troubleshooting installation and uninstallation section in Troubleshooting Network Performance Insight.

For all troubleshooting issues in deploying Ambari clusters, see Troubleshooting Ambari server section in Troubleshooting Network Performance Insight.

For all troubleshooting issues in integration of, see Troubleshooting integration with section in Troubleshooting Network Performance Insight.
Configuring
You can configure IBM Network Performance Insight, Version 1.3 and its integration services through user interface console and command line interface. You can also administer and manage application security and single sign-on from Dashboard Application Services Hub portal.

About this task
Most of the configurations are performed through web-based UI on Ambari server. For Network Performance Insight to be fully functional and accessible on Jazz for Service Management, you must perform the following configurations:

• Configure Network Performance Insight system.
• Configure the required Ambari services and Network Performance Insight services from Ambari web interface.
• Configure integration with Tivoli Netcool/OMNIbus.
• Configure integration with Cacti.

Configuring Network Performance Insight system environment
Use this information to configure your Network Performance Insight system that is integrated with Dashboard Application Services Hub from the graphical user interface.

You must do some general system configuration and tuning for optimizing the system performance. During implementation, you must configure the application options to meet your requirements.

You can view the current settings, modify the settings, add new, or delete an existing configuration item. These configuration settings are stored in the database and can be retrieved from the CFG schema tables. Each configuration setting is associated with a separate widget on Dashboard Application Services Hub UI.

The Network Performance Insight dashboards are pre-configured with working sets of default configurations that are created right after installation. A broad range of functions in Network Performance Insight can be administratively configured.

You can configure the following items from system configuration:

• Autonomous System
• Cacti servers
• Domain names
• Entity thresholds
• Flow aggregations
• Flow devices
• Interfaces
• IP Grouping
• NBAR
• Retention profiles
• Site grouping
• Thresholds
• Type of Services

Note: These configuration settings are specific for performance metrics only.

For more information about troubleshooting system configurations, see Troubleshooting IBM Network Performance Insight.
Logging in to the portal
Depending upon your organization’s deployment, you can access the reporting interface through Dashboard Application Services Hub.

Procedure
• Access the reporting interface from Dashboard Application Services Hub as follows:
  a) Open a web browser and enter the following URL for the Jazz™ for Service Management UI and reporting server:
     https://host.domain:port/DASH_context_root
     For example: https://<myserver.ibm.com>:16311/ibm/console
     Where:
     – host.domain is the fully qualified host name or IP address of the Jazz for Service Management UI and reporting server.
     When single sign-on (SSO) is enabled, ensure that you use the fully qualified host name in the URL of the Jazz for Service Management reporting and UI server. SSO requires that the browser pass LTPA cookies to the Jazz for Service Management application server, and these cookies contain the fully qualified host name.
     – port is the secure HTTP port number that was specified during installation. The default value is 16311.
     – /DASH_context_root is the context root for the console that was specified during installation. The default value is /ibm/console.
   b) Enter the user ID and password in the Dashboard Application Services Hub login page. Click Log in. For example, npiadmin/netcool
      The Dashboard Application Services Hub Welcome page opens.
   c) Click Console Integration icon (��) on the navigation bar and select the dashboard of your choice under System Configuration.

Configuring Autonomous System
To assign a routing domain for your network, configure the Autonomous System that uses Border Gateway Protocol (BGP). BGP shares routing information with other autonomous systems with the help of a globally unique 16-digit identification number that is known as the AS number (ASN). AS numbers are assigned by the Internet Assigned Numbers Authority (IANA).

About this task
The Autonomous Systems information that is configured and stored is displayed in the Top Autonomous System Conversations view in Traffic Details dashboard.

Procedure
1. Click Console Integrations (藏) in the navigation bar, and select Autonomous System under System Configuration. Add an Autonomous System.
2. Click New (藏) icon and enter the Autonomous System information as follows:
   Id
   Mandatory field that represents a unique ASN.
**Note:** Autonomous System numbers one to 64511 are available by IANA/ARIN (IANA/American Registry for Internet Numbers) for global use. The 64512 - 65535 series is reserved for private and reserved purposes.

**Name**
Name of the Autonomous System.

**Note:** Autonomous System numbers, one to 64511 have predefined names for global use. The 64512 - 65535 series is reserved for private and reserved purposes.

**Country**
Country to which the specific network routing domain belongs to.

**Is public**
Whether network domain is a private use ASN or with in the public AS range.

Edit an Autonomous System.

3. Select a row from the table and click the Edit (edit) icon to change the information for the Autonomous System.

Delete an Autonomous System.

4. Select an entry from the table and click the Delete (delete) icon to delete an entry that is not needed.

Common tasks that are applicable for most of the configuration settings.

5. Click the Filter (filter) icon and type an item name or ID in the Filter by <keyword> field.

6. Click the Refresh (refresh) icon to refresh the list of items.

7. Select a number in the lower-right corner to change the number of items to be displayed in the table.

8. Go to a specific page by using the arrows in the bottom of the page.

9. Navigate to a specific page from the page numbers at the bottom of the page.

**Related information**
List of Autonomous Numbers

**Configuring Cacti servers**
You can set up multiple Cacti instances in your network to integrate with Network Performance Insight on the Cacti Servers page.

**About this task**
You can configure the Cacti server details to enable performance metric polling. Cacti polls the data at predetermined intervals and the stored data is available for visualization.

To support multiple Cacti instances in your network environment, partitioning method is introduced. One million entities can be configured in each Cacti Server instance that includes 100,000 devices and 900,000 subentities such as interface, physical card (CPU, Fan), and probe and so on.

**Procedure**

1. Click Console Integrations (console) in the navigation bar and select Cacti Servers under System Configuration.

   The Cacti Servers page displays the Cacti servers configuration in a table.

2. To configure a Cacti server, click the New (new) icon.

   The Add/Edit Cacti Servers window displays the configuration fields.

3. Specify the server settings for the Cacti server as needed.
<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>The fully qualified server name or the IP address.</td>
</tr>
<tr>
<td>SFTP Port</td>
<td>The SFTP port number. By default, 22.</td>
</tr>
<tr>
<td>SFTP User</td>
<td>The SFTP user name.</td>
</tr>
<tr>
<td>SFTP Password</td>
<td>The SFTP password.</td>
</tr>
<tr>
<td>Reflector Output Path</td>
<td>The path location to output the poller logs.</td>
</tr>
<tr>
<td></td>
<td>Reflector is a Cacti plug-in that is designed to mirror SNMP polling data to a log file before the files are written into RRD files.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The output path must be same as the path that is specified in “Configuring the Reflector plug-in” on page 75.</td>
</tr>
<tr>
<td></td>
<td>After the Cacti plug-in is enabled, you can retrieve the polling logs from the specified Reflector output path. For example: reflector_poller_output.log.&lt;timestamp&gt;.log.gz</td>
</tr>
<tr>
<td>Reflector Log Prefix Path</td>
<td>The prefix of the log output directory path.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The log prefix must be same as the prefix that is specified in “Configuring the Reflector plug-in” on page 75.</td>
</tr>
<tr>
<td>JDBC Connection URL</td>
<td>The database JDBC connection URL string to connect to the database. For example: jdbc:mysql://&lt;IP_Address&gt;:3306/cacti</td>
</tr>
<tr>
<td>JDBC User</td>
<td>The database user name.</td>
</tr>
<tr>
<td>JDBC Password</td>
<td>The database password.</td>
</tr>
<tr>
<td>Enabled</td>
<td>To enable the Cacti server to poll the performance metrics.</td>
</tr>
</tbody>
</table>

a. Click **Ok** to save the modification.

4. To edit an existing Cacti server configuration, select a server from the table.

5. Click the **Edit** icon.

   The **Add/Edit Cacti Servers** window displays the configuration details.

6. Modify the settings for the Cacti server as needed. See Step 3.

7. You can perform the following tasks in the **Actions** column:

   a) Click **Edit** to edit the Cacti server configurations. See Step 3.

   b) Click **Enable** or **Disable** to enable or disable the Cacti server.

   **Important:** If you’re migrating any Cacti instance to a different server, make sure to disable the old instance on the **Cacti Servers** configuration page.

**Results**

Cacti server details that are configured are stored in the Servers table in Cacti schema.
Note: After a Cacti server is enabled on the configuration page, it takes a while for the Cacti Collector Service to start the data collection. Approximately, it might take about 2 - 3 mins before you start seeing data in the log files.

What to do next
You must repeat the same process to enable or configure every Cacti server as needed.

Related tasks
“Configuring the Reflector plug-in” on page 75
After the Reflector plug-in is installed, the plug-in must be configured. The same configuration settings must be applied to each Cacti instance on the Cacti Servers page from System Configuration.

Configuring domain names
Domain name is an identification of a unique computer system on the internet that is universally agreed by web servers and online administrations and offers all related destination information. To access an organization’s web-based facilities, website users must identify the exact domain name. A complete domain name consists of one or more subdomain names and one top-level domain name that is separated by dots (.). For example, <myserver.ibm.com> is a complete domain name.

About this task
Configuring domain names helps in handling the frequently used, well-known domain names of your organization.

You can add a set of pre-defined domain names in system, such as youtube.com, facebook.com, yahoo.com, and so on.

With these pre-defined configurations, the DNS performs forward resolution to get a list of IP addresses for the domain names. When a flow record is received, DNS service in Network Performance Insight tries to match the source IP and destination IP with the resolved IP address and maps it to the domain name. The traffic detail page then displays as the configured domain name instead of a string of IP.

Without these pre-defined configurations, the aggregation takes the IP address and performs DNS reserve resolution, which might not populate a friendly domain name.

You can configure domain names to be resolved for IP address mapping.

Note: Database tables store specific types of data and can be categorized into the configuration, event, aggregation, and flow data in database tables. The database table for configuration displays the data for domain names.

Procedure
1. Log in to Jazz for Service Management server.

2. Click Console Integrations ( ) in the navigation bar, and select Domain Names under System Configuration.

Add a domain name.

3. Click New ( ) icon and enter the domain name to create a new domain name to be resolved. Delete a domain name.

4. Select an entry from the table and click icon to delete an entry that is not needed.
   This option helps you to delete an entry that has a typographical error.
   a) Delete any entry that is no longer needed.
   b) Delete a wrong entry and create a new entry.

Note: The domain names that start or end with "." or "-" are not accepted.
5. Click **OK** to save the settings.

**What to do next**
You can repeat the same process to configure commonly used domain names as needed.

**Configuring Entity thresholds**
A threshold is a value that is compared against a metric to determine whether the metric violates a specific constraint. Entity thresholds provide a mechanism for identifying anomalies in performance metrics that is polled from and.

**About this task**
Events can be created when a performance metric exceeds a certain user-defined value. For example, when the response time for a monitored service is too high, or when bandwidth utilization exceeds a certain amount.

The threshold violations and their values are user-defined and not dynamically generated. You can configure entity thresholds for each of the performance metrics that are collected and stored in database.

**Important:** Entity Threshold configuration is required in the following installation scenarios:

- For the metrics collected by in “Scenario 1 - NetFlow data and performance data from Network Performance Insight” on page 11.
  
  **Note:** To configure thresholds for standard SNMP metrics that is collected by , see Defining anomaly thresholds.

- For all the performance metrics collected by “Scenario 2 - NetFlow data and Performance data from Cacti” on page 71.

**Procedure**

1. Click **Console Integrations** in the navigation bar and select **Entity Thresholds** under System Configuration.
   
   You can see the Entity Thresholds table.

2. Select the threshold that you want to edit.

3. Click the **Edit** icon.
   
   The **Edit Entity Threshold** window displays the configuration details.

4. Modify the settings for the threshold as needed.
   a) Select the limit type from the **Limit Type** list to **Over**, **Under**, or **Band**.
      
      **Over**
      
      Detect violations when the metric value exceeds the set threshold value.

      **Under**
      
      Detect violations when the metric value falls short of the set threshold value.

      **Band**
      
      Detect violations the metric value goes outside a range (or band) between two set threshold values.

   b) Enter a value in the **Upper Limit** field for the metric to trigger a threshold violation.

   c) Enter a value in the **Lower Limit** field for the metric to trigger a threshold violation.

   d) Enter the number of events for triggering the threshold in the **Consecutive Occurrences** field.

   e) Select the **Enabled** check box to enable a threshold on the interface.

   f) Click **Ok** to save the modification.

**Note:** When the threshold limit is violated, it displays the severity as **Critical**.
For more information, see *Threshold violation* in 5. You can perform the following tasks in the **Actions** column:

a) Click **Edit** to edit or configure the selected threshold.

b) Click **Enable** or **Disable** to enable or disable a metric to detect its threshold violation states.

**Results**

Any metric that is violating the configured threshold value is reported in the Event Viewer.

**What to do next**

You must repeat the same process to enable and configure thresholds for every metric as needed.

**Related tasks**

“Configuring Flow thresholds” on page 67

Thresholds provide a mechanism for identifying anomalies in flow and metric data that is polled from Tivoli Network Manager. Threshold is a metric value that is compared against a value to determine whether an interface violated a specific constraint. The threshold violations and their values are user-defined and not dynamically generated. These threshold values are defined per interface in each direction.

**Configuring Flow aggregations**

User configurable Flow aggregations increase the performance of NPI system by optimizing the CPU utilization and reduce the I/O demands on database. It helps in Top Talker optimizations. Top N Talkers support feature helps you analyze large amount of data that Flexible NetFlow captures from the network traffic. You can filter, aggregate, and sort the data for display. When you are sorting and displaying the data in the NetFlow cache, you can limit the display output to a specific number of entries with the highest values (Top N Talkers) for traffic volume, packet counters, and so on.

**About this task**

By default, some of the aggregations are enabled and the others are user configurable. Some of these aggregations require other related configurations to be enabled. The following table provides information about all the available user configurable aggregations:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Type of aggregation</th>
<th>Enabled by default</th>
<th>Required additional configuration setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Top Applications</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Applications with Source ToS</td>
<td>No</td>
<td>See Configuring Type of Service section in .</td>
</tr>
<tr>
<td>Autonomous systems</td>
<td>Top Autonomous System Conversations</td>
<td>No</td>
<td>See Configuring Autonomous System section in</td>
</tr>
<tr>
<td></td>
<td>Top Destination Autonomous System</td>
<td>No</td>
<td>See Configuring Autonomous System section in</td>
</tr>
<tr>
<td></td>
<td>Top Source Autonomous System</td>
<td>No</td>
<td>See Configuring Autonomous System section in</td>
</tr>
<tr>
<td>Conversations</td>
<td>Top Conversations</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Conversations with Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Resource</td>
<td>Type of aggregation</td>
<td>Enabled by default</td>
<td>Required additional configuration setting</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Destinations</td>
<td>Top Destinations</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Destinations with Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Address Grouping</td>
<td>Top IP Group Conversations with Application</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td></td>
<td>Top IP Group Conversations with Protocol</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td></td>
<td>Top IP Group Conversations with Source ToS</td>
<td>No</td>
<td>• See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• See Configuring Type of Service section in.</td>
</tr>
<tr>
<td></td>
<td>Top Destination IP Groups with Application</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td></td>
<td>Top Destination IP Groups with Protocol</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td></td>
<td>Top Destination IP Groups with Source ToS</td>
<td>No</td>
<td>• See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• See Configuring Type of Service section in.</td>
</tr>
<tr>
<td></td>
<td>Top Source IP Groups with Application</td>
<td>No</td>
<td>See Configuring Autonomous System section in.</td>
</tr>
<tr>
<td></td>
<td>Top Source IP Groups with Protocol</td>
<td>No</td>
<td>See Configuring Autonomous System section in.</td>
</tr>
<tr>
<td></td>
<td>Top Source IP Groups with Source ToS</td>
<td>No</td>
<td>• See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• See Configuring Type of Service section in.</td>
</tr>
<tr>
<td></td>
<td>Top Source IP Groups</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td></td>
<td>Top IP Group Conversations</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td></td>
<td>Top Destination IP Groups</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
</tr>
<tr>
<td>Resource</td>
<td>Type of aggregation</td>
<td>Enabled by default</td>
<td>Required additional configuration setting</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Quality of Service</td>
<td>Top QoS Hierarchies with Queue ID</td>
<td>No</td>
<td>QoS fields must be configured on your devices. See <a href="#">Configuring Flexible NetFlow and AVC</a> section in Configuring Flow devices.</td>
</tr>
<tr>
<td>Protocols</td>
<td>Top Protocols</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Protocols with Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Protocols with Conversation</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Protocols with Destination IP</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Protocols with Source IP</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sources</td>
<td>Top Sources</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Sources with Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Type of Service</td>
<td>Top Source ToS</td>
<td>No</td>
<td>See <a href="#">Configuring Type of Service</a> section in .</td>
</tr>
</tbody>
</table>

**Procedure**

Enable or disable an aggregation or modify the aggregation fields from the list.

1. Click [Console Integrations](#) in the navigation, and select **Flow Aggregation** under **System Configuration**.

2. Select a row from the table and click the [Edit](#) button or select **Edit** in the **Actions** column as follows:
   - **Aggregation**: Name of the aggregation as it appears in the table.
   - **Aggregation Fields**: Aggregation grouping keys or fields in the aggregation.
   - **Visible in Traffic Details**: By default, when an aggregation type is disabled, the Top Talker view that is associated with the specific aggregation is not visible from the Traffic Details dashboard. Select the check box to display the Top Talker view with the historical data even if the aggregation is disabled.
     - **Note**: This control affects only the Traffic Details dashboard views but does not affect the Flow dashboard views.
   - **Enabled**: Select the check box to enable the aggregation.

3. Optional: Click **Enable** or **Disable** to enable or disable an aggregation in the **Actions** column.
Results
When an aggregation type is disabled, the historical data remains in the database with no further updates to the CFG schema tables and Flow Metric schema tables.

Configuring Flow Devices
You can configure the SNMP credentials for all NetFlow enabled devices in your network to send the data to from System Configuration on navigation. All devices must be configured to export SNMP data to . This information is stored in the database and required for interface enrichment.

About this task
You must specify SNMP community strings for to discover the devices for SNMP data. To configure the general parameters for the SNMP requests, follow these steps:

Procedure

1. Click Console Integrations  in the navigation bar, and select Flow Devices under System Configuration.
2. Select an Exporter IP of a device from the table and click Info in the Actions column to see the existing information for the exporter.
3. Select an Exporter IP of a device from the table and click the Edit button or select Edit in the Actions column.
4. Enter the following details:
   Read Community String
   SNMP community string is like the user ID or password and is required for SNMP V1 and V2 versions only. SNMP V3 version uses user name and password credentials with encryption key. Specify the name of the SNMP read community. By default, the SNMP community string for SNMP V1 and V2 versions is set to public. You can change all the community strings to customized values in this field.

   SNMP Version
   Specify the SNMP version that is associated with this SNMP configuration. Make sure to select the version that is supported on the device. SNMP versions are as follows:
   - V1
     Basic version of SNMP. This version is supported by most devices and easy to set up. It has limited security.
   - V2
     Supports 64-bit counters to monitor the bandwidth usage of networks high volumes of data. It has limited security.
   - V3
     Supports authentication and encryption of the credentials for multiple users. Highly secure version.
5. If the SNMP version for the device is V3, specify the following information:
   Level
   Specify the required level of authentication and privacy. The following levels are available:
   - noAuthNoPriv
     Select this option for SNMP communities that have no authentication or private key. In this case, you do not need to specify any passwords. Then, specify the Context Name and Security Name.
   - authNoPriv
Select this option for SNMP communities that have an authentication key but no private key. Then, specify values in the **Auth Type**, **Context Name**, **Security Name**, and **Auth Password** fields.

- **authPriv**
  Select this option for SNMP communities that have both an authentication and a private key. Then, specify values in the **Auth Type**, **Priv Type**, **Priv Password**, **Context Name**, **Security Name**, **Auth Password**, and **Priv Password** fields.

**Auth Type**
This field is applicable if the level is **authNoPriv** and **authPriv** to specify the type of encryption for the authentication password. The following types of encryption are available:

- SHA1
- MD5

**Priv Type**
This field is applicable if the level is **authPriv** to specify the type of encryption for the privacy password. The following types of encryption are available:

- 3-DES
- AES 128
- AES 192
- AES 256

**SNMP Port**
Specify the required port. By default, the port number is 161.

**Context Name**
An SNMP context defines a collection of management information that is accessible to an SNMP entity. Each context in a management domain has a unique identifier. The **Context Name** field is optional and depends on the user.

**Security Name**
Security Name is used when access control is set up.

**Auth Password**
Authentication password. It must be same as the device authentication password.

**Priv Password**
Privacy password. It must be same as the device privacy password.

6. Click **Enrich** from the **Actions** column.

After the interface is enriched with additional information, such as interface speed, interface name, and interface description from the device and the **Enrichment State** field value is changed to **COMPLETE**. This information for the specific interface is updated in the **Interfaces** configuration page and also updated in the database.

Optionally, you can do the manual enrichment by entering the interface details from **Interfaces** page from System Configuration. For more information, see “Configuring Flow interfaces” on page 61. The manual enrichment overrides the enrichment from Flow Devices configuration.

Optionally, you can do the manual enrichment by entering the interface details from **Interfaces** page from System Configuration. For more information, see Configuring Flow interfaces section from . The manual enrichment overrides the enrichment from Flow Devices configuration.

**Configuring Flow interfaces**
Flow records provide unidirectional measurements of traffic that is entering (ingress) or leaving (egress) a network interface. Network Performance Insight models this process by associating an Ingress Interface
and Egress Interface with each network interface. Each flow record is associated with the appropriate flow interface.

**About this task**

automatically creates flow interfaces when flow records are processed. When new interfaces are created, they are enabled unless the total number of interfaces exceeds the limit. processes the data that is associated with a flow interface only if it is enabled.

**Procedure**

1. Log in to Jazz for Service Management server.

2. Click **Console Integrations** ( ) in the navigation, and select **Interfaces** under **System Configuration**.

3. Select a row from the table and click the **Edit** ( ) button to enable or disable the selected interface.

4. Click **OK** to save the configuration.

5. Optional: Enter the following interface details to manually update the interface details for enrichment:
   - Interface Name
   - Interface Description
   - Speed

   **Note:** These details override the information that is obtained from devices by configuring the SNMP credentials in the **Configuring Flow Devices** section in .

6. Optional: Click **Enable** or **Disable** to enable or disable an Interface for flow data collection in the **Actions** column.

**What to do next**

You must repeat the same process to enable or disable all interfaces as needed.

**Note:** Currently, you cannot select multiple interfaces to configure to enable or disable for traffic data collection at a time.

---

**Configuring Flow IP Grouping**

Create logical grouping of IP addresses and address ranges. This grouping helps in monitoring the individual NetFlow bandwidth usage, usage-based billing, and accounting.

**About this task**

- To configure multiple IP ranges into a single IP address group, create multiple row entries with same IP address group.
- Make sure that the IP range does not overlap with existing ones. Otherwise, you might see **Overlapping IP address grouping range** message.

**Procedure**

1. Click **Console Integrations** ( ) in the navigation bar, and select **Flow IP Grouping** under **System Configuration**.

   Add an IP address group.

2. Click **New** ( ) icon and enter the IP address grouping information as follows:
IP Address Group
Logical name to the group. Create your IP Grouping by location. For example, branch offices or departments for easier monitoring.

Start Address Range
Start IP address for the range.

End Address Range
End IP address for the range.

Enabled
A flag to enable or disable the specified IP address group.

3. Click Ok to save the settings.

Edit an IP address group.

4. Select a row from the table and click the Edit button to change the information for the IP Address Group.

5. Click Ok to save the settings.

Delete an IP address group.

6. Select an entry from the table and click icon to delete an entry that is not needed.

Configuring NBAR
Configure your devices to send NBAR and NBAR2 data to gain better visibility on the applications in your NetFlow traffic. This information helps you identify the bandwidth usage of the applications in your network and also prioritize and control the application traffic. You can define the business relevance of the applications and apply the correct QoS policies to improve the performance and user experience of business-critical applications.

About this task
NBAR and NBAR2 configured devices send Flow packets that contain the following metrics:

- Engine ID
- Selector ID
- Name
- Description
- Category Name
- Subcategory Name
- Group Name
- P2P Technology
- Tunnel Technology
- Encrypted Technology
- Business Relevance

Procedure

1. Click Console Integrations in the navigation bar, and select NBAR under System Configuration.

Edit the NBAR and NBAR2 settings.

2. Click Edit icon to enable or disable the ART metric collection:

   Select the Enable ART check box to enable the collection of Application Response Time (ART) metrics for TCP traffic.
The following fields are not editable:

**Engine ID**
A unique identifier for the engine that determined the Selector ID. The Engine ID is the first 8 bits that provide information about the engine that classifies the flow.

**Selector ID**
The remaining 24 bits that provide information about the application.

*Note:* Engine ID and Selector ID constitute the Application ID.

**Name**
Name of the application that is derived from the Application ID.

**Description**
Application description that can be derived from the Application option template.

3. Click **Ok** to save the settings.
4. Optional: Click **Enable** or **Disable** to enable or disable an ART in the **Actions** column.

**Related information**
Cisco Application Visibility and Control Field Definition Guide for Third-Party Customers

### Configuring data retention profiles

Describes how to configure the retention profiles for different type of data that is collected by.

**About this task**
Retention profiles control how long the raw and aggregated data, and log files are retained by the system. Setting the retention profiles help in maintaining the amount of data to be stored in the database and free the additional disk space. You can change the default values to modify the retention periods. For timeseries data alone, set the retention period from Ambari.

*Note:* Entity Metric schema tables retention profile settings are not available in a fresh installation, since the data is now moved to timeseries database. But you notice the retention profile settings for Entity Metric schema tables in an upgraded system.

For more information, see *Retention period* section in *Network Performance Insight overview IBM*.

To configure retention profiles:

**Procedure**
1. Log in to server.

2. Click **Console Integrations ( )** in the navigation bar and select **Retention Profiles** under **System Configuration**.
   You can see Retention Profiles table.

3. Select a row from the table and click the **Edit ( )** button to configure a retention profile period for an Interface. Enter the following details:

   **Name**
   The **Name** field is already selected.

   **Period**
   Type the period for which you want to retain the data.

   **Unit**
   Select the unit; **Days**, **Weeks**, or **Months**.

   *Note:* Retention period must be configured with tradeoff between storage size and number of days to keep the data. The graphs will not show any data after the time period that you selected for a particular interface.
For more information, see Data storage section in Network Performance Insight overview IBM.
4. Click OK to save the settings.

**What to do next**
Repeat the same process to configure retention profiles as needed. For timeseries data alone, set the retention period from Ambari.

For more information, see Configuring retention period for timeseries data section on .

**Configuring site grouping**
You can categorize your enterprise network based on different geographical areas by specifying the IP address ranges for each site. Each site can be configured for specific business and non-business days and hours.

**About this task**
This grouping helps in monitoring the individual site bandwidth usage, usage-based billing, and accounting. You can also get visibility on the network bandwidth usage during business and non-business days and hours.

**Procedure**

1. Click **Console Integrations** in the navigation bar, and select **Sites** under **System Configuration**.
   Add a site group.

2. Click **New** icon and enter a site information as follows:
   - **Site Name**
     Logical name to the site. Create your site by location. For example, branch office locations for easier monitoring.
   - **IP Address Ranges**
     Start and end IP address for the range that is specific to the site. You can give the ranges separated by a hyphen or as comma-separated list.
   - **<Day>**
     All days from Sunday to Saturday are listed. Select the days based on the typical business days for your site.
   - **Business Start Time**
     Specify the typical business start time in hh:mm format.
   - **Business End Time**
     Specify the typical business end time in hh:mm format.
   - **Time Zone**
     Select the time zone to which the site belongs to from the list.

   Edit a site group.

3. Select a row from the table and click the **Edit** button to change the information for the site.

4. Click **Ok** to save the settings.

Delete a site group.

5. Select an entry from the table and click the Delete button icon to delete an entry that is not needed.
Configuring Flow thresholds
Thresholds provide a mechanism for identifying anomalies in flow and metric data that is polled from . Threshold is a metric value that is compared against a value to determine whether an interface violated a specific constraint. The threshold violations and their values are user-defined and not dynamically generated. These threshold values are defined per interface in each direction.

About this task
You can configure the threshold value per interface for anomalies detection.

Procedure
1. Log in to server.
2. Click Console Integrations ( ) in the navigation bar and select Thresholds under System Configuration. You can see Flow Thresholds table.
3. Select a row from the table and click the Edit ( ) button to configure a Threshold for that Interface. Enter the following details:
   a) Select the Enabled check box to enable a Threshold on the Interface.
   b) Select the limit type from the Limit Type list to Over, Under, or Band and their units.
      - Over: Detect violations when the interface exceeds the set Threshold value.
      - Under: Detect violations when the interface falls short of the set Threshold value.
      - Band: Detect violations the interface goes outside a range (or band) between two set Threshold values.
   c) Enter a value in the Upper Limit field for the interface to trigger a Threshold violation.
   d) Enter a value in the Lower Limit field for the interface to trigger a Threshold violation.
   e) Enter the number of events for triggering the Threshold.
      Note: When the Threshold limit is violated, it displays the severity as Critical.
      For more information, see Threshold violation in
4. Perform the following tasks in the Actions column:
   a) Click Edit to edit or configure the selected Threshold. Repeat step 3
   b) Click Enable or Disable to enable or disable an interface to detect its Threshold violation states.
5. Click OK to save the settings.

Results
Any interface that is violating the set Threshold value is reported in the Event Viewer.

What to do next
You must repeat the same process to enable and configure thresholds for every Interface as needed.

Note: Currently, you cannot select multiple interfaces to configure the Thresholds values at a time.
To configure thresholds for metric data, see Defining anomaly thresholds.
**Configuring Type of Service**

Typically, this feature determines the packet delivery prioritization for low-delay, high-throughput, highly reliable service, or normal service for NetFlow traffic. On all Flow packets, Type of Service byte is represented as Differentiated Service Code Point (DSCP) and Explicit Congestion Notification.

**Procedure**

1. Click **Console Integrations** in the navigation bar, and select **Type of Services** under **System Configuration**.
   Edit the Type of Services mappings.

2. Click **Edit** icon and modify the Type of Services metrics as follows:
   - **ToS ID**
     This field is not editable. This field implements the Type of Service on the NetFlow packet to tradeoff on delay, throughput, reliability, and cost.
   - **ToS Name**
     You can specify any name to your Type of Service class. Typically, the classes and their IDs are as follows:

     | DSCP Code   | DSCP ID (Decimal format) | IP Precedence                           |
     |-------------|--------------------------|-----------------------------------------|
     | Best Effort | 0                        | 0 - Routine or Best Effort              |
     | CS1, AF11-13| 8,10,12,14               | 1 - Priority                            |
     | CS2, AF21-23| 16,18,20,22              | 2 - Immediate                           |
     | CS3, AF31-33| 24,26,28,30              | 3 - Flash - used for voice signaling    |
     | CS4, AF41-43| 32,34,36,38              | 4 - Flash Override                      |
     | CS5, EF     | 40, 46                   | 5 - Critical - used for voice RTP       |
     | CS6         | 48                       | 6 - Internetwork Control                |
     | CS7         | 56                       | 7 - Network Control                     |

   Where:
   - CS - Class Selector
   - AFxy - Assured Forwarding (x=class, y=drop precedence)
   - EF - Expedited Forwarding

   **Note**: Traffic classification is an automated process that categorizes network traffic according to various parameters into a number of traffic classes.

   **Note**: The ToS names must be unique.

3. Click **Ok** to save the settings.

**Related information**

DSCP and Precedence Values
Configuring the default entity scope for data visualization on Ambari
To display the performance data that is collected from Cacti in Network Performance Insight Dashboards, the default scope must be set to cacti from Ambari web interface.

Procedure
1. Log in to Ambari server dashboard.
   Use the following default URL:http://<myserver.ibm.com>:8080
   The default user name is admin, and the default password is admin.
2. Click Services > NPI > Configs > Advanced.
3. Expand the Advanced npi-env pane and add the following lines in npi-env template text area to set the grace period:
   ```
   ui.default-entity-scope = cacti
   ```
   **Note:** This setting is required only if your Network Performance Insight is integrated with Cacti for performance metrics.
4. Click Save to save the configuration.
   This setting is written to /etc/npi/npi-cacti-collector/application.conf file.
5. Restart the Network Performance Insight UI Service from Ambari for all hosts in your cluster as follows:
   a) Click Services > NPI.
   b) Click Service Actions > Restart UIs.

Configuring integration with Tivoli Netcool/OMNIbus
Use this information to integrate with the Tivoli Netcool/OMNIbus Web GUI application. The Tivoli Netcool/OMNIbus Web GUI customizable dashboards display real-time performance information and event data.

About this task
An event contains the Event ID, host name, and port information. When an event is selected, some of the data for the event is sent to and used to determine the best report to present. Then builds a block of HTML content that redirects the browser to a display.

Right-click an event in Event Viewer or Active Event List of Web GUI to display the tools that are added from the alerts menu. You select an option from this menu to display a detailed report for the time period of the threshold violation or an AEL report.

Configuring launch-in-context integration with Network Performance Insight
Launch-in-context integrations are supported between the Web GUI and other widgets. A launch-out integration describes the launching of another product from a Web GUI widget. A launch-in integration describes the launching of the Web GUI from another product.

About this task
Launch-in-context is the concept of moving seamless from one Tivoli product UI to another Tivoli product UI (either in a different console or in the same console or portal interface) with single sign-on and with the target UI in position at the proper point for users to continue with their task.

Related information
Configuring launch-in-context integrations with Tivoli products
Creating a launch-in-context tool
You can create tools that are run from right-click menus in event lists or when users click a widget. Different tool formats are supported.

**Procedure**

1. Log in to server as an administrator user, such as npiadmin.
2. Select Administration > Event Management Tools > Tool Configuration from the left pane.
3. Click Create Tool and enter the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>npiFlowTvLiC</td>
</tr>
<tr>
<td>Type</td>
<td>script</td>
</tr>
<tr>
<td>Script Commands</td>
<td>Copy and paste the contents of the file npiFlowTvLiC.js that is available in opt/IBM/basecamp/basecamp-ui/resources/ael.</td>
</tr>
</tbody>
</table>

4. Select the data source name OMNIBUS.
5. Clear the Execute for each selected row check box.
6. Click Save.

A confirmation message is displayed. Click OK to close the message.

**Related information**

Tools overview

**Configuring launch-in-context menu**

In event lists, users access default and custom tools through menus. You can add tool entries to the menus, create new submenus, and modify or delete menu items.

**About this task**

The two supplied menus are the Alerts menu and the Tools menu. The Alerts menu can also be opened from the right-click menu when you select an event.

**Procedure**

1. Log in to server as npiadmin user.
2. Select Administration > Event Management Tools > Menu Configuration from the left pane.
3. Select the alerts menu in the window, and then click the Modify button.

   The Menus Editor is displayed.
4. Select the npiFlowTvLiC tool in the Available items on the left, click the arrow to move it to the Current items section.
5. Select npiFlowTvLiC from the Current items section and click Rename.
6. In the Label text box, enter a meaningful name for the new button.
   For example, Flow Dashboard. If needed, enter a value in the Mnemonic text box, if needed.
7. Click Save.
8. Use the button selections on the right to move the menu option up or down.

   Separators might also be added by selecting <Separator> in the Available Items area of the window.
   The separator might be moved up and down.
9. Click Save.

   The following message is displayed:
   Menu has been successfully modified.
10. Click OK to close the message.
Results
When you right-click any event in Event Viewer or in Active Event List, you can see the npiflowTvLiC tool that is renamed to Flow Dashboard as a selectable option in the menu. Select the tool to see the Traffic Details report associated with the interface that violated the threshold and generated the event.

Configuring non-default ObjectServer name
By default, the Object Server name is NCOMS. If you configured a non-default name for the ObjectServer, use this information to configure to work with the non-default ObjectServer name.

Procedure
1. Edit the npi-flow-stdin.props file that is located in /opt/IBM/npi/npi-event/stdin-probe/omnibus/probes/linux2x86 to change the following value:

   ```
   # Add your settings here
   Manager : 'NPI'
   Server  : '<non-default ObjectServer name>'
   ```

2. Save the file.

3. Edit the interfaces.linux2x86 file that is located in /opt/IBM/npi/npi-event/stdin-probe/etc to comment the NCOMS and add the non-default ObjectServer name as follows:

   ```
   # NCOMS => omnihost 4100
   # NCOMS
   <non-default ObjectServer name>
   master tcp sun-ether omnihost 4100
   query tcp sun-ether omnihost 4100
   ```

4. Save the file.

5. Restart the Event Service from Ambari.
   - See Controlling the services from Ambari administration interface in .
   - See Setting up the OMNIbus Standard Input probe section in .

Scenario 3 - NetFlow only data
In this scenario, Network Performance Insight can be used to collect, aggregate, and render the NetFlow data alone. In this scenario, performance data is not monitored.

Installing
The installation information contains the installation prerequisites, instructions for preparing to install, installing, and uninstalling the software based on your scenario.

About this task
Follow the general installation roadmap to complete required and optional steps, according to your needs.

Planning for Network Performance Insight installation
Before you install the product, read the hardware and software requirements.

For more information, see Suggested node and services layout from .

Related concepts
“System requirements” on page 1
Complete set of requirements for IBM Network Performance Insight 1.3.

**Downloading and extracting the software**

How to get the product distribution?

**Procedure**

1. Download the electronic installation images from the IBM Passport Advantage website to a location of your choice on Ambari server.

   For example, `/opt/IBM/Installers/NPI` that is referred to as `<DIST_DIR>`.

2. Extract the media by using the following commands:

   ```
   tar -zxvf NPI-1.3.0.0.tgz
   tar -zxvf CNVI6ML.tar
   cd CNVI6ML
   tar -zxvf NPI-1.3.0.0.tgz
   ```

   Or, use the following command:

   ```
   gunzip -c NPI-1.3.0.0.tgz | tar -xvf -
   ```

   You can see the following files and folders in the `<DIST_DIR>`:

   • NPI-1.3.0.0/
     - bin
       - agent_setup_nonRoot.sh
       - install.sh
       - installRemoteFlowCollector.sh
       - npi_prereq_check.sh
       - prereq_check.sh
       - setup_cluster_ssh.sh
       - upgrade
         This folder contains a lot of script files that are required to upgrade from to . It also contains the libraries and script to migrate the SNMP device credentials from the previous environment to the new one.
     - basecamp-installer-tools-1.3.0.0-<build_signature>.noarch.rpm
     - basecamp-repo-1.3.0.0-<build_signature>.noarch.rpm
     - npi-ambari-1.3.0.0-<build_signature>.noarch.rpm
     - npi-repo-1.3.0.0-<build_signature>.noarch.rpm

**Downloading the ()**

Download the components.

**About this task**

Download the following packages to a single location of your choice on Ambari server. For example, `/opt/IBM/Installers/NPI` that is referred to as `<DIST_DIR>`.

• HDP-2.6.4.0-centos7-rpm.tar.gz
• HDP-UTILS-1.1.0.22-centos7.tar.gz
• HDP-GPL-2.6.4.0-centos7-rpm.tar.gz
• ambari-2.6.1.0-centos7.tar.gz

**Note:** You do not need to extract these packages.
Procedure
Download the following repositories:

- HDP
- HDP-UTILS
- HDP-GPL
- Ambari

Gathering required information
Collect the following information before you start your installations.

- The fully qualified domain name (FQDN) for each host in your system, and the components that you want to set up on different hosts. The Ambari installation wizard does not support IP addresses. Use hostname -f to check for the FQDN.
  
  An example for FQDN: myserver.ibm.com
- Plan for the base directories for the following components:
  - NameNode data
  - DataNodes data
  - MapReduce data
  - ZooKeeper data
  - Various log, pid, and database files according to your installation type
- Users and groups for
  - root
  - netcool
    The netcool user is created during installation and all services are run as netcool user.
  - smadmin
- Users and groups for:

<table>
<thead>
<tr>
<th>Service</th>
<th>Group</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>hadoop</td>
<td>hdfs</td>
</tr>
<tr>
<td>MapReduce</td>
<td>hadoop</td>
<td>mapred</td>
</tr>
<tr>
<td>YARN</td>
<td>hadoop</td>
<td>yarn</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>hadoop</td>
<td>ams</td>
</tr>
<tr>
<td>Kafka</td>
<td>hadoop</td>
<td>kafka</td>
</tr>
<tr>
<td>Spark</td>
<td>hadoop</td>
<td>spark</td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>hadoop</td>
<td>zookeeper</td>
</tr>
</tbody>
</table>

Note: Click Admin > Service Accounts to see the user information from your Ambari server.

- Download the .

  Note: The must be installed after the installation of .

- Download the .

  See Default users section in .
Installing the prerequisite software
Install the prerequisite products before you install Network Performance Insight.

About this task
Install the required products in your IBM Netcool Operations Insight solution according to your entitlement.

You require the following components from IBM Netcool Operations Insight solution to work with Network Performance Insight for NetFlow only data:

• Tivoli Netcool/OMNIbus core component
• Tivoli Netcool/OMNIbus Web GUI component
• Jazz for Service Management
• Tivoli Common Reporting

This component is required only if you have Cognos-based reports from your other product integrations. It is not required to work with Network Performance Insight.

Note: If your Dashboard Application Services Hub that has Tivoli Common Reporting and Network Performance Insight integration fails, see Troubleshooting Dashboard Application Services Hub and Network Performance Insight integration section in Troubleshooting IBM Network Performance Insight

Procedure
Perform steps 1 - 14 from Quick reference to installing according to your Netcool Operations Insight entitlement.

What to do next
Continue with installation of Network Performance Insight.

Preparing your environment
Before you run the installation, you must prepare your target environments. Make sure you have installed .

Setting SSH passwordless login
You must set up passwordless SSH connections for the Ambari server host to remotely connect to all other hosts that are in the cluster, and also the server without entering the password.

Procedure
1. Log in to the system where you want to install Ambari server host as root user.
2. On the Ambari server host, run the following command:

   `<DIST_DIR>/NPI-1.3.0.0/bin/setup_cluster_ssh.sh`

   Enter the required details on the prompts.

   Note: Always, give fully qualified domain name (FQDN) for the hosts.
INFO: Hostname <myserver.ibm.com>
INFO: USER root
INFO: User home directory /root
INFO: Generating public keys pair ...
Continue to setup remote hosts?[Y/n]?y

Enter remote hostname (FQN): <myserver2.ibm.com>
INFO: Creating .ssh directory on <myserver2.ibm.com> ...
root@<myserver2.ibm.com>’s password:
INFO: Uploading public key to remote host ...
root@<myserver2.ibm.com>’s password:
INFO: Updating remote host's folder permission ...
INFO: Verifying ssh passwordless setup ...
Verified SSH connection
SSH Passwordless setup to <myserver2.ibm.com> is completed successfully.
Continue to setup next remote hosts?[Y/n]?y

If you are configuring the integration of with non-root installation of supported products, run following commands:

```
cd /root/.ssh
ssh-copy-id -i id_rsa.pub <non-root-user>@<myserver.ibm.com>
ssh <non-root-user>@<myserver.ibm.com>
```

3. Repeat the connection attempt from the Ambari server host to each host to make sure that the Ambari server can connect to each.

**Setting Kernel parameters**

Setting the ulimit and kernel parameters in nodes.

**About this task**

Run the following steps to set the ulimit and kernel parameters.

**Note:** You can see the error messages in Ambari start operation stderr and log file if the ulimit or the kernel settings are not set correctly during Storage or Flow Collector services start-ups.

**Procedure**

1. Log in to system as root user to change the Linux kernel parameters.
2. Edit the `/etc/sysctl.conf` file to add or modify the kernel parameters.

```
net.core.rmem_default = 33554432
net.core.rmem_max = 33554432
net.core.netdev_max_backlog = 10000
```

Change the `/etc/sysctl.conf` to ensure that the values are set on a system start.

a) Run `sysct1 -p` as root user to refresh with the new configuration in the current environment.

3. From the node, edit the `/etc/security/limits.conf` file to add or modify the number of open files to at least 65536 as follows:

```
* - nofile 65536
* - nproc 65536
```

4. Log out and log in the session again as root user for the changes to take effect.
5. Repeat the steps 1 - 4 on all the servers where services are installed.
Configuring Security-Enhanced Linux (SELinux) to support SCTP protocol

By default, the Linux kernel security module (SELinux) runs in enforcing mode. When your RHEL system runs in SELinux enforcing mode, it might deny the SCTP ports.

About this task

This information provides details about how to configure SELinux to enable SCTP support.

Procedure

1. Set SELinux to permissive as root user on all hosts in your cluster as follows:

   ```bash
   setenforce 0
   ```

2. Proceed to install system and set up the clusters.
3. Make sure that the system is up and running for sometime.

   It might take a while to notice the AVC denied messages in the log file after the system is up and running.

4. Check SELinux audit log with this command:

   ```bash
   tail -f /var/log/audit/audit.log
   ```

   You might notice the AVC denied message as follows:

   ```plaintext
   type=AVC msg=audit(1508149696.075:38284): avc: denied {getattr} for pid=1412
   comm="npi-akka.actor." laddr::ffff:10.55.236.146 lport=4381 faddr::ffff:10.212.6.20
   fport=33859 scontext=system_u:system_r:unconfined_service_t:s0 tcontext=system_u:
   object_r:unlabeled_t:s0 tclass=rawip_socket
   ```

5. Create local policy to enable the access as follows:

   ```bash
   mkdir <workdir>
   cd <workdir>
   grep npi-akka.actor. /var/log/audit/audit.log | audit2allow -M npi
   semodule -i npi.pp
   ```

   The local policy helps in suppressing the AVC denied error message.

6. Optional: You can change the SELinux mode to enforcing as root user as follows:

   ```bash
   setenforce 1
   ```

Related tasks

“Installing Network Performance Insight” on page 17
Install HDP® and Network Performance Insight on a single host or multi-host environments.

Preparing to run the prerequisite scanner

In addition to specific tasks, complete these common tasks before you start an installation. installation script calls the prerequisite scanner that checks if your environment meets these requirements during installation.

Before you begin

Make sure that you have the following operating system packages and their related repos are installed and enabled:

- `libtirpc-devel`
- `redhat-lsb`

**Note:** These packages are required for .

About this task

Use the root user account to perform the following steps.
Procedure
Follow the steps that are specified in Preparing the environment in documentation.

Related information
HDP Documentation

Installing
Install and on a single host or multi-host environments.

Before you begin
• Ensure that is installed.
• Ensure that the necessary user permissions are in place for all the installation directories.
• Ensure that all the hosts in your cluster are in the same timezone.
• Ensure that you configured your devices to send all the required Flow fields for collection.
   For more information, see the following topics:
   – Default normalized flow record fields in
   – Configuring Flexible NetFlow and AVC in

About this task
All the services are distributed under the following default directories:
• /opt/IBM/npi
• /opt/IBM/basecamp

Procedure
1. Remove the existing yum cache that might be saved in your system by using the following command as root user:

   rm -rf /var/cache/yum

2. Start the installation by using the following command as root user on Ambari server:

   cd <DIST_DIR>/NPI_1.3.0.0/bin
   ./install.sh <DIST_DIR>

   Where <DIST_DIR> is the directory where the and software is located. For example, opt/IBM/Installers/NPI.

3. Enter y or n in the prompt based on the prerequisite checker errors.

Results
These tasks are completed after the command is run:
• Prerequisite checker script (prereq_check.sh) is called to ensure that your environment is set up correctly. Check the prereq_check_<timestamp>.log for any errors.
• /var/www/html/repos directory is created if it does not exist.
• files are extracted.
• services are set up in /var/www/html/repos/npi folder.
• These dependent packages are installed:
   – apr
   – apr-util
   – mailcap
   – postgresql
• Apache Hypertext Transfer Protocol Server (httpd) server is installed.
  • httpd port is updated to 9091.
  • Ambari server is installed and started.
  • Ambari server is configured to auto restart services and components.
  • Related repo files are updated in /etc/yum.repos.d/ to point to local yum repositories.
    You require only the following repositories in /etc/yum.repos.d/ directory. The rest of the files can be removed to ensure that the cluster setup is not interrupted:
    - ambari.repo
    - ambari-hdp-1.repo
    - hdp.repo
    - hdp-utils.repo
    - hdp-gpl.repo
    - npi.repo
  • service stack is updated to repoinfo.xml file to point to local RPM repositories.

Note: If you encounter any prerequisite checker warnings during installation, see “Preparing to run the prerequisite scanner” on page 16.

What to do next
You can see the installation output in the following log files that are located in <DIST_DIR>/NPI_1.3.0.0:
• install_<timestamp>.log
• prereq_check_<timestamp>.log

Setting up Network Performance Insight cluster
Use the Ambari installation wizard in your browser to complete your installation, configuration, and deployment of Network Performance Insight components and Hadoop components.

Before you begin
• Ensure that you have the SSH Private key for root user on Ambari server host.
• Ensure that you have configured the SSH Passwordless login entry to all target hosts.

Procedure
1. Open a browser and access the Ambari server dashboard.
   Use the following default URL:
   http://<myserver.ibm.com>:8080
   The default user name is admin, and the default password is admin.
2. Click Launch Install Wizard on the Ambari Welcome page.
   The CLUSTER INSTALL WIZARD opens.
3. Enter a name for the cluster you want to create on the Get Started page and click Next.
   Note: The name cannot contain blank spaces or special characters.
   For example, npi.
4. On the Select Stack page, select HDP-2.6.NPI stack and select the Use Public Repository option option.
5. Click Next.
6. Complete the following steps on the **Install Options** page:
   a) List all the nodes that are used in the HDP ® cluster on **Target Hosts** pane.
      Specify one node per line, as in the following example:

      ```
      node1.abc.com
      node2.abc.com
      node3.abc.com
      ```

      **Note:** The host name must be the fully qualified domain name (FQDN).

   b) Select **Provide your SSH Private Key to automatically register hosts** on **Host Registration Information** pane.

      If the root user installed the Ambari server, the private key file is `/<root>/.ssh/id_rsa`. Where `<root>` is the root user home directory.

      You have two options to get the private key file:

      1) Browse to the location of the `.ssh/id_rsa`

      Or

      2) Copy the contents of the `.ssh/id_rsa` file and paste the contents in the SSH key field.

      Make sure to copy all the content from:

      ```
      -----BEGIN RSA PRIVATE KEY-----
      To
      -----END RSA PRIVATE KEY-----
      ```

   c) Click **Register and Confirm**.

   7. Ensure that the correct hosts are registered successfully on the **Confirm Hosts** page.

   If you want to change the hosts that are selected, remove the hosts one-by-one by following these steps:

   a. Click the check box next to the server to be removed.

   b. Click **Remove** in the **Action** column.

   **Note:**

   • If warnings are found during the check process, click **Click here to see the warnings** to see the warnings. The **Host Checks** page identifies any issues with the hosts. For example, a host might have Firewall issues.

   • Ignore the process issues that are not related to Network Performance Insight.

   c. After you resolve the issues, click **Rerun Checks** on the **Host Checks** page. After you have confirmed the hosts, click **Next**.

   8. Select the following services on the **Choose Services** page:

<table>
<thead>
<tr>
<th>Service</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HDFS</td>
<td>2.7.3</td>
<td>Apache Hadoop Distributed File System (HDFS)</td>
</tr>
<tr>
<td>YARN + MapReduce2</td>
<td>2.7.3</td>
<td>Apache Hadoop NextGen MapReduce (YARN)</td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>3.4.6</td>
<td>Centralized service that provides reliable distributed coordination.</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>0.1.0</td>
<td>A system for metric collection that provides storage and retrieval capability for metrics that are collected from the cluster.</td>
</tr>
<tr>
<td>Service</td>
<td>Version</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Kafka</td>
<td>0.10.1</td>
<td>A high-throughput messaging system.</td>
</tr>
<tr>
<td>NPI</td>
<td>1.3.0.0</td>
<td>Network Performance Insight cluster service</td>
</tr>
<tr>
<td>NPI Spark Client Scala 2.11</td>
<td>2.0.1</td>
<td>Apache Spark is an engine for large-scale data processing. The Apache Spark client library is compiled on Scala 2.11 and is specific to Network Performance Insight 1.3.</td>
</tr>
</tbody>
</table>

9. Click **Next**.

10. Assign the master services to hosts in your cluster on the Assign Masters page and click **Next**.

   You can accept the current default assignments. To assign a new host to run services, click the list next to the master node in the left column and select a new host.

11. Click **Next**.

12. Assign the slave and client components to hosts in your cluster on the Assign Slaves and Clients page.

   Click all to assign **all** the services on your hosts. Or, you can select one or more components next to a selected host.

   **Note:** If you do not need a microservice based on your installation scenario, do not select the check box against the service on a host.

13. Click **Next**.

14. Update the configuration settings for the following services and components on Customize Services pane.

   You can see a set of tabs from where you can manage configuration settings for Hadoop and Network Performance Insight components.

   **Note:** Default values are completed automatically when available and they are the recommended values.

   • Set up HDFS
   • Set up YARN
   • Set up Zookeeper
   • “Setting up Ambari Metrics” on page 23
   • Set up Kafka
   • Set up Network Performance Insight
   • “Setting up the OMNibus Standard Input probe” on page 28

15. Click **Next** after you have reviewed your settings, and completed the configuration of the services.

16. Verify that your settings are correct and click **Deploy** on the Review page.

17. See the progress of the installation on Install, Start, and Test page.

   The progress bar at the top of the page gives the overall status and the main section of the page gives the status for each host. When you click the task, log for a specific task can be displayed.

18. Click **Next** after the services are installed successfully.

19. Review the completed tasks on the Summary page and click **Complete**.

**Results**

It might take a while for Ambari to start all the services. To see the status of all the services in a host, click the Hosts tab in the Ambari server host, and then select a host. You can see the services that are started from the Summary page.

**Related concepts**

“Required microservices in different installation scenarios” on page 9
Microservices that are required in different installation scenarios.

**Setting up HDFS Service**
Set properties for the NameNode, SNameNode, DataNodes, and some general and advanced properties. Click the name of the group to expand and collapse the display.

**Procedure**
Click **HDFS > Settings**.
Accept all the default values for the following required settings:

**Note:** These values are prepopulated based on your choices on previous pages.

- NameNode and DataNode directories as `/<data1>/hadoop/hdfs/namenode` and `/<data1>/hadoop/hdfs/data`.
  
  Ensure that the `/<data1>` directory has sufficient or the recommended disk space.

  **Note:** Do not set up these directories in `/tmp` directory.

- NameNode Java heap size: 1 GB
- NameNode server threads: 200
- Minimum replicated blocks: 100%
- DataNode failed disk tolerance: 0
- DataNode maximum Java heap size: 1 GB
- DataNode max data transfer threads: 4098

**Related concepts**
“Hardware requirements” on page 1
Hardware specifications vary according to the size of your network and server topology that you want to use.

“Gathering required information” on page 13
Collect the following information before you start your installations.

**Setting up YARN Service**
YARN decouples resource management and scheduling capabilities from the data processing component. The YARN framework uses a ResourceManager service, a NodeManagers service, and an Application master service.

**Procedure**
1. Click **YARN > Settings**.
2. Configure the required settings as follows:
   
   - Ensure that the node memory is 15000 MB or more.
   - Ensure that minimum container memory per container is 1024 MB.
   - Ensure that maximum container memory per container is 15000 MB.
   - Set the number of virtual cores to minimum 32.

**Related information**
YARN

**Setting up Zookeeper**
Modify the default settings for Zookeeper from Ambari web UI.

**About this task**
Zookeeper requires a majority. It is best to use an odd number of nodes in your cluster. For example, with four Network Performance Insight nodes, ZooKeeper can handle the failure of a single machine; if two
systems fail, the remaining two Network Performance Insight nodes do not constitute a majority. However, with five Network Performance Insight nodes, ZooKeeper can handle the failure of two Network Performance Insight nodes.

If a Network Performance Insight node is removed or added to your cluster, the conf/application.conf file in the UI Service is automatically updated to reflect the correct number of host names with the ZooKeeper Service in the following lines:

- main.zk-url=<host name1>,<host name2>,<host name3>
- messaging.kafka.zk-connect=<host name1>,<host name2>,<host name3>

**Procedure**

1. Click Zookeeper > Zookeeper Server.
2. Update the value of **ZooKeeper directory** field as per your environment.

   By default, Ambari might decide on a default directory with sufficient space. For example, /<data1>/hadoop/zookeeper.

   **Note:** Do not set the **ZooKeeper directory** in /tmp directory.

**Setting up Ambari Metrics**

Modify the default settings for Ambari Metrics from Ambari web UI.

**Procedure**

1. Click **Ambari Metrics > Configs > General**.
2. Provide values for the following fields:
   - **Grafana Admin Username**
   - **Grafana Admin Password**

   **Note:** You can retain the default values for the rest of the fields.

**Setting up Kafka**

Modify the Kafka Broker log settings from Ambari web UI.

**Procedure**

1. Click **Kafka > Kafka Broker**.
2. Update the values for the following fields as per your environment:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kafka Broker host</td>
<td>Hosts where the Kafka broker is running.</td>
<td><code>&lt;myserver.ibm.com&gt;</code></td>
</tr>
<tr>
<td>zookeeper.connect</td>
<td>Comma-separated list of connection strings where the ZooKeeper is running in this format: host1:port1,host2:port2</td>
<td><code>&lt;myserver.ibm.com&gt;:2182</code></td>
</tr>
</tbody>
</table>
Table 34: Kafka Broker settings. (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>log.dirs</td>
<td>A comma-separated list of one or more directories in which Kafka data is stored.</td>
<td>/&lt;data&gt;/kafka-logs&lt;br&gt;Note: Ensure that the /&lt;data&gt; directory has sufficient or the recommended disk space. Do not set up Kafka logs in /tmp directory.</td>
</tr>
<tr>
<td>log.roll.hours</td>
<td>A setting that forces Kafka to roll a new log segment even if logs.segment.bytes size is not reached.</td>
<td>168&lt;br&gt;Accept the default value.</td>
</tr>
<tr>
<td>log.retention.hours</td>
<td>The number of hours the logs are stored after which they are deleted.</td>
<td>168&lt;br&gt;Accept the default value.</td>
</tr>
<tr>
<td>Listeners</td>
<td>PLAINTEXT://localhost:6667</td>
<td></td>
</tr>
</tbody>
</table>

Setting up Network Performance Insight services
Set up all the Network Performance Insight services from web-based Ambari user interface. The configuration setting from Ambari UI are written to application.conf files that are located in the conf directory of each microservice.

Procedure
1. Click Services > NPI > NPI Settings.
2. Change the default values in the following fields:
   Make sure that you are in the Configs tab if you are changing these values after the installation is complete.

Table 35: NPI Timeseries Service settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeseries.datasource</td>
<td>The timeseries data source. Currently, timeseries data is stored on Kairos DB that is integrated with Apache Cassandra.</td>
<td>kairosdb</td>
</tr>
<tr>
<td>timeseries.data.retention</td>
<td>It is the data retention period for timeseries data in days. For more information about this setting, see Configuring retention period for timeseries data section in Installing and Configuring IBM Network Performance Insight.</td>
<td>1 Year</td>
</tr>
</tbody>
</table>
### Table 36: NPI Common settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage.jdbc-service</td>
<td>Used to build the path to storage location with http port for JDBC service.</td>
<td>&lt;myserver.ibm.com&gt;:13081</td>
</tr>
<tr>
<td></td>
<td>Note: This setting is required only if the Storage Service is not installed on all Network Performance Insight node hosts.</td>
<td></td>
</tr>
<tr>
<td>kafka.zk-connect</td>
<td>ZooKeeper URL with Kafka znode. The string {{zookeeper.connect}} is populated with settings in zookeeper.connect.</td>
<td>{{zookeeper.connect}}</td>
</tr>
<tr>
<td></td>
<td>Note: This setting need not be changed.</td>
<td></td>
</tr>
<tr>
<td>kafka.broker-list</td>
<td>List of Kafka brokers. The string {{kafka.broker-list}} is populated with cluster's Kafka hosts and ports.</td>
<td>{{kafka.broker-list}}</td>
</tr>
<tr>
<td></td>
<td>Note: This setting need not be changed.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 37: NPI Manager settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>manager.ambari.user</td>
<td>Ambari user name</td>
<td>admin</td>
</tr>
<tr>
<td>manager.ambari.password</td>
<td>Ambari password</td>
<td>admin</td>
</tr>
</tbody>
</table>

To set or edit the networking time outs for resiliency in DNS resolution:

### Table 38: NPI DNS Service settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns.server.address</td>
<td>DNS Server address. If this value is not specified, it is resolved from the system's /etc/resolv.conf file.</td>
<td></td>
</tr>
<tr>
<td>dns.server.port</td>
<td>DNS Server port</td>
<td>53</td>
</tr>
<tr>
<td>dns.network.initiation.timeout</td>
<td>The maximum amount of time that the DNS Server waits in Disconnected state before it attempts to connect to the DNS Server again.</td>
<td>30 Seconds</td>
</tr>
</tbody>
</table>
Table 38: NPI DNS Service settings. (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns.network.connection.timeout</td>
<td>The maximum amount of time that the DNS Server waits in Connecting state for the networking layer to respond that the connection is established.</td>
<td>10 Seconds</td>
</tr>
<tr>
<td>dns.network.acknowledgement.timeout</td>
<td>The maximum amount of time that the DNS Server waits in Waiting state for the networking layer to respond to with an acknowledgment that the outbound packet is written to the operating system or networking buffers.</td>
<td>5 Seconds</td>
</tr>
<tr>
<td>dns.network.disconnect.timeout</td>
<td>The maximum amount of time that the DNS Server waits in Disconnecting state before it resets and moves to Disconnected state to close the connection.</td>
<td>5 Seconds</td>
</tr>
</tbody>
</table>

Table 39: NPI Web Services settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>https.port</td>
<td>The https port on which Network Performance Insight application console can be accessed.</td>
<td>9443</td>
</tr>
</tbody>
</table>

Setting up the UI Service to render data from Timeseries Service

Use these steps to configure the UI service to retrieve the data from Timeseries Service instead of the Storage Service to render on the Network Performance Insight Dashboards.

About this task

For more information about the Timeseries Service functionality, see Timeseries Service in IBM Network Performance Insight: Product Overview.

Procedure

1. Log in to Ambari server dashboard.

   Use the following default URL:
http://<myserver.ibm.com>:8080

The default user name is admin, and the default password is admin.

2. Click Services > NPI > Configs > Advanced.
3. Expand the Advanced npi-env pane and add the following lines in content text area:
   
   ```java
   ui.timeseries.rest.url="http://<myserver.ibm.com>:31081"
   ```

   Where, <myserver.ibm.com> is the server where Timeseries Service is available.

4. Click Save to save the configuration.
5. Restart the UI Service as follows:
   a) Click Services > NPI.
   b) Click Service Actions > Restart UIs.

Setting up Flow Collector Service
Use these steps to set up the Flow Collector Service.

Procedure
1. Click Services > NPI > NPI Settings.
2. Change the default values in the following fields:

Make sure that you are in the Configs tab if you are changing these values after the installation is complete.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>collector.flow.udp.ports</td>
<td>The UDP ports that the Flow collector listens to for Flow packets.</td>
<td>4379</td>
</tr>
<tr>
<td>collector.flow.sctp.ports</td>
<td>The SCTP ports that the Flow collector listens to for Flow packets.</td>
<td>4381</td>
</tr>
<tr>
<td>collector.flow.exporter.blacklist</td>
<td>Comma-separated list of IP addresses in square brackets. The flow data from these exporters in the list is blocked from further processing.</td>
<td>ipAddress1, ipAddress2</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Default value</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>collector.flow.art.dscp.whitelist</td>
<td>Comma-separated list of IP DSCP, which are integer values in the range 0 - 255 to enable ART. This setting is to enable the traffic classes that must be monitored. You can further control the applications with the specified traffic classes for ART enablement. See Configuring NBAR section in Installing and Configuring IBM Network Performance Insight.</td>
<td>Note: To use this option, ensure that ipDiffServCodePoint Flow field is enabled in your ART data template.</td>
</tr>
<tr>
<td>collector.flow.max-interfaces</td>
<td>The maximum number of interfaces that the collectors collect from Network Performance Insight agent node.</td>
<td>1000</td>
</tr>
</tbody>
</table>

**Setting up the OMNIbus Standard Input probe**

The Standard Input probe is bundled with Network Performance Insight and is installed along with it.

**About this task**

Most of the configuration settings are done when you install Network Performance Insight. Follow these steps to work with OMNIbus Standard Input probe:

**Procedure**

1. Configure the host name resolution to resolve omnihost to the actual host name where Tivoli Netcool/OMNIbus is installed. Add an alias entry in the /etc/hosts file on all systems where Network Performance Insight services are installed as follows:

   `<IP_Address> <fully_qualified_host_name> <alias> omnihost`

   For example:

   `192.0.2.0 <myserver.ibm.com> myserver omnihost`

   **Note:** This step must be performed on all Network Performance Insight node hosts where the Event Service is installed.

2. Ensure that you have the following 32-bit RHEL operating system libraries:

   - zlib
   - ncurses
   - bzip2
   - libstdc++

3. Follow the steps in Configuring non-default ObjectServer name section in Installing and Configuring IBM Network Performance Insight if you have a non-default Object Server name.

4. **Note:** Change or add these settings only when recommended by IBM Professional Services.
Optional: Modify these settings for Tivoli Netcool/OMNIbus Standard Input (STDIN) probe to send events to OMNIbus. Follow these steps:

a) Click **Services > NPI > Configs > Advanced**.

b) Expand **Advanced npi-env** section and enter the following lines in the **content** text area:

```plaintext
event.netcool.home = "<netcool_installation_directory>"
event.netcool.omnibus.home = "<omnibus_installation_directory>"
event.netcool.omnibus.temp = "<temp_directory_for_log_files>"
event.netcool.omnibus.stdin.args = "<additional_probe_command_line_args>"
event.netcool.omnibus.stdin.props = "<omnibus_stdin_probe_properties_file_location>"
event.netcool.omnibus.stdin.rules = "<omnibus-stdin-probe-rules-file_location>"
```

Where

**Table 41: Configurations for OMNIbus STDIN probe.**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>event.netcool.home</td>
<td>Root installation directory for your Netcool products</td>
<td>$NCHOME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$NCHOME defaults to /opt/IBM/tivoli/netcool.</td>
</tr>
<tr>
<td>event.netcool.omnibus.home</td>
<td>Root OMNIbus Installation directory</td>
<td>$NCHOME/omnibus</td>
</tr>
<tr>
<td>event.netcool.omnibus.temp</td>
<td>Temp directory where the log files are located.</td>
<td>&lt;NPI_HOME&gt;/npi-event/stdin-probe/omnibus/probes/omnibus/var</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, &lt;NPI_HOME&gt; is opt/IBM/npi.</td>
</tr>
<tr>
<td>event.netcool.omnibus.stdin.args</td>
<td>You can configure the STDIN probe to log at different levels (for example, DEBUG). For more information, see Configuring logging in Troubleshooting IBM Network Performance Insight. Anything that is specified in this setting is passed directly on the command line to the STDIN probe at startup.</td>
<td>-messagelevel INFO - messagelog /var/tmp/ stdin.probe.DEBUG.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or -messagelevel DEBUG -raw</td>
</tr>
<tr>
<td>event.netcool.omnibus.stdin.props</td>
<td>STDIN probe properties file location</td>
<td>&lt;NPI_HOME&gt;/npi-event/stdin-probe/omnibus/probes/omnibus/stdin.props</td>
</tr>
<tr>
<td>event.netcool.omnibus.stdin.rules</td>
<td>STDIN probe rules file location</td>
<td>&lt;NPI_HOME&gt;/npi-event/stdin-probe/omnibus/probes/omnibus/stdin.rules</td>
</tr>
</tbody>
</table>

See Configuring non-default ObjectServer name section in Installing and Configuring IBM Network Performance Insight.
Setting up integration with
Use this information to set up the federation between and to work correctly and to access the web-based visualizations.

Perform these tasks during fresh installation scenarios where you are doing the integration for the first time.

Editing the configuration files
Edit the custom.cfg configuration file according to your environment and use these files in all the required integration tasks for and .

About this task
You must edit these files only once before you start the integration.

Procedure
Update the following fields in the file custom.cfg file that are specific to the instance that you want to use for integration:

By default, the custom.cfg file is located in /opt/IBM/basecamp/basecamp-installer-tools/dash-integration folder.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DASH_ENABLE_OPTION</td>
<td>If integration is to be included, specify TRUE. If integration is not required, specify FALSE.</td>
<td>TRUE</td>
</tr>
<tr>
<td>DASH_CONNECTION</td>
<td>Set the FQDN hostname of the server.</td>
<td>root@&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;non-root-user&gt;@&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>DASH_SSH_PORT</td>
<td>If non default port number is used, update the SSH port.</td>
<td>22</td>
</tr>
<tr>
<td>WEBSHERE_APP_SERVER_PATH</td>
<td>WebSphere Application Server installation path on server.</td>
<td>/opt/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td>JAZZSM_PATH</td>
<td>installation path.</td>
<td>/opt/IBM/JazzSM</td>
</tr>
<tr>
<td>DASH_USERNAME</td>
<td>administration user.</td>
<td>smadmin</td>
</tr>
<tr>
<td>DASH_PASSWORD</td>
<td>administration user password.</td>
<td>netcool</td>
</tr>
<tr>
<td>KEYSTORE OPTION</td>
<td>USE_DEFAULT_KEY or USE_EXIST_KEY</td>
<td>USE_DEFAULT_KEY</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you want to reuse your existing key, use the USE_EXIST_KEY.</td>
<td></td>
</tr>
<tr>
<td>EXIST_KEYSTORE_FILEPATH</td>
<td>Location of the keystore</td>
<td>/tmp/keystore.security</td>
</tr>
<tr>
<td>EXIST_CA_FILEPATH</td>
<td>CA certificate file location</td>
<td>/tmp/ca.crt</td>
</tr>
<tr>
<td>KEYSSTORE_PASSWORD</td>
<td>Password for the keystore</td>
<td>changeit</td>
</tr>
<tr>
<td>KEYS_PASSWORD</td>
<td>Password for key</td>
<td>changeit</td>
</tr>
<tr>
<td>ALIAS</td>
<td>Alias name</td>
<td>npi</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>DOMAIN_NAME</td>
<td>Domain name</td>
<td>*.domain.name</td>
</tr>
<tr>
<td>ORG_NAME</td>
<td>Organization name</td>
<td>DEMO</td>
</tr>
<tr>
<td>LOCALITY</td>
<td>Locality</td>
<td>DEMO_LOCALITY</td>
</tr>
<tr>
<td>STATE</td>
<td>State</td>
<td>DEMO_STATE</td>
</tr>
<tr>
<td>COUNTRY</td>
<td>Country</td>
<td>&lt;MY&gt;</td>
</tr>
<tr>
<td>WAS_PROFILE_NAME</td>
<td>WebSphere Application Server profile for on the target application server.</td>
<td>JazzSMProfile</td>
</tr>
<tr>
<td>WAS_NODE</td>
<td>The default server node for the WebSphere Application Server profile.</td>
<td>JazzSMNode01</td>
</tr>
<tr>
<td>WAS_SERVER_NAME</td>
<td>Name of the application server that is specified when the application server profile is created.</td>
<td>server1</td>
</tr>
<tr>
<td>WAS_PROFILE_PATH</td>
<td>Location of the application server profile.</td>
<td>/opt/IBM/JazzSM/profile/</td>
</tr>
<tr>
<td>NPI_UI_HOST</td>
<td>Host where the UI service is installed.</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
</tbody>
</table>

*Installing the security services*

If your environment does not have . , you cannot install the to obtain the security services. In such a scenario, install the security services that are bundled with to access the web-based visualizations from Console Integration on .

**About this task**

Security Services is bundled in /opt/IBM/basecamp/basecamp-installer-tools/dash-integration/security-service.

**Procedure**

Run the `installSecurityService.sh` script that is available in /opt/IBM/basecamp/basecamp-installer-tools/dash-integration as follows:

```bash
cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
sudo `pwd`/installSecurityService.sh -default=`pwd`/default.cfg -custom=`pwd`/custom.cfg
```

The following tasks are performed after this script is run:

- Detects whether the security services are already available or not and proceeds to install only if it is not available.
- JazzSM_Home/security folder is created.
- Copies the `com.ibm.tivoli.ac.ess.authnsvc_1.1.2.201501192348.zip` file from /opt/IBM/basecamp/basecamp-installer-tools/dash-integration/security-service to JazzSM_Home/security.
- Extracts the `com.ibm.tivoli.ac.ess.authnsvc_1.1.2.201501192348.zip` file.
Creating console integration
Use this information to create the console integration.

About this task
In the earlier releases of , console integration is performed automatically with the installation of that comes with . Starting from V, console integration can be performed with the createConsoleIntegration.sh script that is available in the following directory:
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration

Procedure
Run the createConsoleIntegration.sh script as follows:

```
sudo `pwd`/createConsoleIntegration.sh -default=`pwd`/default.cfg -custom=`pwd`/custom.cfg
```

Results
If the script runs successfully, the console content is available in the navigation bar of the Dashboard Application Services Hub through the icon.

Log in with npiadmin and netcool credentials and click Console Settings > Console Integrations in the navigation bar to see the integration.

For troubleshooting console integration, see Missing console integration icon in.

Generating the certificate and keystore files
Generate the certificate authority (CA) certificates and other keystore files on Ambari server.

Procedure
Generate ca.crt key store file by using the following command as root user:

Run the following command in a single line:

```
cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
<DASH_INTEGRATION_PATH>/securityKeyTool.sh
-default=<DASH_INTEGRATION_PATH>/default.cfg
-custom=<DASH_INTEGRATION_PATH>/custom.cfg
```

Where <DASH_INTEGRATION_PATH> is BASECAMP_INSTALLER_TOOLS_DIR/dash-integration

For example:

```
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/securityKeyTool.sh
-default=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.cfg
-custom=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/custom.cfg
```

What to do next
Check these log files in the /tmp directory for any errors:

- ambari_npi_key_startup.log
- securityKeyTool.<timestamp>.log
- genSecurityKey.log

Related tasks
“Installing Network Performance Insight” on page 17
Install HDP® and Network Performance Insight on a single host or multi-host environments.

**Enabling integration with**
Use this information to enable integration between and portal.

**Before you begin**
Make sure that Object Server is up and running.

**Procedure**
Run the integration script as root user as follows:

By default, the `npiDashIntegration.sh` script is located in `/opt/IBM/basecamp/basecamp-installer-tools/dash-integration` folder.

```
# <DASH_INTEGRATION_PATH>/npiDashIntegration.sh
-DASH_INTEGRATION_PATH=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration
-DASH_INTEGRATION_PATH=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.cfg
-DASH_INTEGRATION_PATH=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/custom.cfg
```

Where `<DASH_INTEGRATION_PATH>` is BASECAMP_INSTALLER_TOOLS_DIR/dash-integration.

For example:

```
< Dash_INTEGRATION_PATH>/npiDashIntegration.sh
-DASH_INTEGRATION_PATH=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration
-DASH_INTEGRATION_PATH=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.cfg
-DASH_INTEGRATION_PATH=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/custom.cfg
```

After the completion of this command, the following tasks are done:

- The `dash-integration` directory is created at the same level as the WebSphere Application Server based on the value set in the `WEBSPHERE_APP_SERVER_PATH` field in `custom.cfg` file. By default, it is `/opt/IBM/dash-integration`
- The following files are transferred to the `dash-integration` directory:
  - `enableDash.sh`
  - `signkey`
  - `eWasAddUsersAndGroups.py`
  - `priv_key.key`
  - `ca.crt` (Not copied if KEYSTORE_OPTION value is USE_EXIST_KEY)
  - `install.User.cfg` (Not copied if KEYSTORE_OPTION value is USE_EXIST_KEY)
- The `enableDash.sh` script is run at the `dash-integration` directory.
- `dashboarduser` group that is required to access the is created.

**What to do next**
Check these log files for any errors:
- `/tmp/npiDashIntegration.log`
  - **Note:** This log file is available on the Ambari server from where the integration script is run.
- `/tmp/enableDash.log`
  - **Note:** This log file is available on server where is running.
Setting up communication with on Ambari
These settings are pre-populated on Ambari for communicating with Jazz for Service Management.

Procedure

1. Open a browser and access the Ambari server dashboard. Use the following default URL:
   http://<myserver.ibm.com>:8080
   The default user name is admin, and the default password is admin.

2. Click Services > NPI.
3. Make sure that you are in the Configs tab.
4. Click NOI Core Settings > NOI Services and change the values in the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>web.auth</td>
<td>Single sign-on mode. Select DASH for Jazz for Service Management managed LDAP user repository.</td>
<td>DASH</td>
</tr>
<tr>
<td>security.dash.username</td>
<td>Administrator user name for Jazz for Service Management for security service</td>
<td>smadmin</td>
</tr>
<tr>
<td>security.dash.password</td>
<td>Password for Jazz for Service Management administrator user name</td>
<td>&lt;DASH_password&gt;</td>
</tr>
<tr>
<td>https.keystore.file</td>
<td>Full path for the keystore file that stores the SSL certificate that is used by Network Performance Insight.</td>
<td>/opt/IBM/basecamp/basecamp-ui/conf/security/security.keystore</td>
</tr>
<tr>
<td>https.keystore.password</td>
<td>Password for the SSL keystore that is used by Network Performance Insight.</td>
<td>changeit</td>
</tr>
<tr>
<td>https.key.password</td>
<td>Password for the SSL key that is used by Network Performance Insight.</td>
<td>changeit</td>
</tr>
</tbody>
</table>

5. Click NPI > Advanced > Advanced npi-auth and change the default values in the following fields:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>security.dash.hostnames</td>
<td>Full DNS name for the Jazz for Service Management server</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>security.dash.port</td>
<td>HTTPS port on which the Jazz for Service Management communicates.</td>
<td>16311</td>
</tr>
</tbody>
</table>

6. Save the configuration.
7. Restart all the services as follows:
   a) Click Services > NPI.
   b) Select Restart All from the Service Actions list.

Verification on the systems where services are installed:
8. Verify whether the security.keystore file is created in the following location:
   /opt/IBM/basecamp/basecamp-ui/conf/security

9. Check that the cacerts file with webSphereCACert alias is available in /opt/IBM/basecamp/basecamp-ui/conf/security directory by running the following command on all s:

   cd /opt/IBM/basecamp/basecamp-jre/java-1.8.0-openjdk.x86_64/jre/bin
   keytool -keystore /opt/IBM/basecamp/basecamp-jre/java-1.8.0-openjdk.x86_64/jre/lib/security/cacerts -storepass changeit -list -alias WebSphereCACert

10. Get the fingerprint from the keystore file, run the following command:

    keytool -keystore /opt/IBM/basecamp/basecamp-ui/conf/security/security.keystore -storepass changeit -list

11. Make sure that the trustedCertEntry certificate fingerprint of the npi_ca is same as the trustedCertEntry certificate fingerprint of the WebSphereCACert that is generated in step 9.

**Configuring the SSL communication for integration**

The Secure Sockets Layer (SSL) protocol provides secure communications between remote server processes or endpoints. SSL security can be used for establishing communications inbound to and outbound from an endpoint. To establish secure communications, a certificate and an SSL configuration must be specified for the endpoint.

**Before you begin**

Make sure that you have configured the passwordless login as described in Setting SSH passwordless login section in Installing and Configuring IBM Network Performance Insight

**About this task**

Configure SSL communication on Jazz for Service Management portal after you install Network Performance Insight.

You must configure the SSL one time only. If you are reinstalling or upgrading Network Performance Insight, back up the security.keystore, priv_key.key, which is the private key, and ca.crt, which is the public key if you plan to reuse them.

**Configuring SSL settings on WebSphere Application Server**

Use this information to define Secure Sockets Layer (SSL) configuration properties.

**Procedure**

1. Log in to Dashboard Application Services Hub as administrator user.
2. Select Console Settings > General > WebSphere Administrative Console in the console navigation.
3. Click Launch WebSphere administrative console.
4. Click Security > SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings from the list of Secure Socket Layer (SSL) configurations.
5. Update the following information:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Suggested value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default server certificate alias</td>
<td>If it is not defined earlier, this setting specifies the certificate alias that is used as the identity for this SSL configuration.</td>
<td>netcool</td>
</tr>
<tr>
<td>Default client certificate alias</td>
<td>Specifies the description for a client certificate alias.</td>
<td>netcool</td>
</tr>
</tbody>
</table>

For rest of the settings, you can keep the prepopulated default values.
6. Click OK and save the changes to master configuration.

   **Note:** Make sure to convert all your certificates to use SHA256withRSA in WebSphere Application Server.

7. Verify that the netcool personal certificate is available in **SSL certificate and key management > Key stores and certificates > NodeDefaultKeyStore > Personal certificates**.

8. Verify that the npi_ca signer certificate is available in **SSL certificate and key management > Key stores and certificates > NodeDefaultTrustStore > Signer certificates**.

9. Restart the WebSphere Application Server.

10. Press y in the **SSL Signer Prompt** window if the signer certificate information is displayed.

**Related information**

Certificates must be converted to use SHA256withRSA in WebSphere Application Server

**Restarting Jazz for Service Management application servers**

**Adding the signer certificate to your browser**

The ca.crt file that is extracted from Jazz for Service Management must be imported to browser’s Trusted CA Certificate store.

**About this task**

This task must be done on all computers that access Network Performance Insight data for visualization. These steps differ on different browsers. Instructions are provided for Internet Explorer and Firefox.

**Procedure**

Perform these steps on Jazz for Service Management server.

- Go to the following location where Jazz for Service Management server is installed:
  For example:
  ```
  /opt/IBM/dash-integration
  ```
- Copy the ca.crt signer certificate that is generated earlier to your local machine.
  Follow these steps on the browser on your local machine that you use to access the visualization dashboards.
- For Internet Explorer, follow these steps:
  a) Click **Tools > Internet Options**.
  b) Click **Content > Certificates > Trusted Root Certification Authorities**.
  c) Click **Import**.
  d) Browse to the location of the exported ca.crt file.
  e) Click **Next**.
  f) Select to place the certificates in **Trusted Root Certification Authorities** option and click **Finish**.
- For Firefox, follow these steps:
  a) Click **Tools > Options**.
  b) Click **Advanced > Certificates > View Certificates**.
  c) Click **Authorities > Import**.
  d) Browse to the location of the exported ca.crt file and click **Open**.
  e) Select all the check boxes on the **Downloading Certificate** page and click **OK**.
  f) Click **OK** to close the window.
- For Chrome, follow these steps:
  a) Click **Settings > Advanced > Manage certificates**.
  b) Click **Import**.
  c) Browse to the location of the exported ca.crt file and click **Open**.
d) Select **Place all certificates in the following store** and click **Browse**.

e) Select to place the certificate in **Trusted Root Certification Authorities** and click **OK**.

f) Click **Next** and **Finish**.

### Related tasks

“Enabling integration with Jazz for Service Management” on page 32

Use this information to enable integration between Network Performance Insight and Dashboard Application Services Hub portal.

### Postinstallation tasks

Perform these postinstallation tasks after the installation of Network Performance Insight is complete.

- If you have previously disabled firewall, enable the firewall on all nodes in your cluster. Use these commands:

  ```
  systemctl start firewalld.service  
  systemctl enable firewalld
  ```

### Verifying the installation

You can verify the Network Performance Insight 1.3 installation status.

### Before you begin

Make sure that the flow exporter is configured and sending the flow data to the Flow Collector Service.

For more information, see *Configuring Flow devices*.

### Procedure

1. Verify the installation logs that are available at `/tmp` directory.

   To list all the log files, run the following command:

   ```
   ls -lrt /tmp/*.log
   ```

   You can see the following log files:

   ```
   install_2018039121342.log  
   test_install_main.log  
   apr_install.log  
   apr_util_install.log  
   httpd_install.log  
   iop_http_repos.log  
   iop_util_http_repos.log  
   ambari_http_repos.log  
   npi_http_repos.log  
   setuprepoServer.log  
   ambari_repo_baseurl.log  
   postgresql_libs_install.log  
   postgresql_core_install.log  
   postgresql_server_install.log  
   ambari_server_install.log  
   ambari_server_setup.log  
   ambari_server_start.log  
   setupAmbrai.log  
   ambari_npi_startup.log  
   setupNpiServiceStack.log  
   dashkey.log  
   npiDashIntegration.log  
   setupGenKeyTool.log  
   ambari_npi_key_startup.log
   ```

   **Note:** Dashboard Application Services Hub integration script execution log file is located here:

   ```
   <DASH_Host>/tmp/enableDash.log
   ```

   For more information about log files, see *Log files in Network Performance Insight* in *Troubleshooting IBM Network Performance Insight*.
2. Run the following `yum` command to list all the installed packages in the current version:

```bash
# yum list installed | egrep "npi|basecamp"
```

Sample output:

```
# yum list installed | egrep "npi|basecamp"
apr.x86_64                              1.5.2-<build_signature> @npi
apr-util.x86_64                         1.5.2-<build_signature> @npi
basecamp-connect.noarch                 1.2.3.0-<build_signature> @npi
basecamp-entity-analytics.noarch        1.2.3.0-<build_signature> @npi
basecamp-httpd.noarch                  1.2.3.0-<build_signature> @npi
basecamp-installer-tools.noarch        1.2.3.0-<build_signature> @npi-1.2.3.0 @npi
basecamp-jre.x86_64                     1.2.3.0-<build_signature> @npi
basecamp-manager.noarch                 1.2.3.0-<build_signature> @npi-1.2.3.0 @npi
basecamp-repo.noarch                    1.2.3.0-<build_signature> @npi-1.2.3.0 @npi
basecamp-schema-registry.noarch         1.2.3.0-<build_signature> @npi
basecamp-spark.noarch                   1.2.3.0-<build_signature> @npi
basecamp-storage.noarch                 1.2.3.0-<build_signature> @npi
basecamp-tools.noarch                   1.2.3.0-<build_signature> @npi
basecamp-ui.noarch                      1.2.3.0-<build_signature> @npi
httpd.x86_64                            2.4.18-<build_signature> @npi
mailcap.noarch                          2.1.31-<build_signature> @npi
npi-ambari.noarch                       1.2.3.0-<build_signature> @npi-1.2.3.0
npi-cacti-collector.noarch              1.2.3.0-<build_signature> @npi-1.2.3.0
npi-cacti.collector.noarch              1.2.3.0-<build_signature> @npi
npi-dns.noarch                          1.2.3.0-<build_signature> @npi
npi-event.i386                           1.2.3.0-<build_signature> @npi
npi-flow-analytics.noarch                1.2.3.0-<build_signature> @npi
npi-flow-collector.noarch                1.2.3.0-<build_signature> @npi
npi-formula.noarch                       1.2.3.0-<build_signature> @npi
npi-itqm-collector.noarch                1.2.3.0-<build_signature> @npi
npi-repo.noarch                          1.2.3.0-<build_signature> @npi
npi-smnp-collector.noarch                1.2.3.0-<build_signature> @npi-1.2.3.0 @npi
npi-smnp-discovery.noarch                1.2.3.0-<build_signature> @npi
npi-threshold.noarch                     1.2.3.0-<build_signature> @npi
postgresql.x86_64                       9.2.14-1.<build_signature> @npi
postgresql-libs.x86_64                   9.2.14-1.<build_signature> @npi
postgresql-server.x86_64                9.2.14-1.<build_signature> @npi
```

**Verifying the status of Standard Input probe**

You can verify the status of Standard Input probe that is packaged with .

**Before you begin**

Ensure that you have installed and verified the status as running.

**Procedure**

1. Check the status of the Event Service by using the following command:

   ```
   <NPI_Home>/basecamp/basecamp-manager/bin
   ./basecamp-manager-cmd status
   ```

2. Run the following command to check the status of Standard Input probe on the node that has the oldest to make sure that the probe is installed successfully:

   ```
   ps -ef | grep nco_p_stdin
   ```

   Check the process ID of the probe that is displayed.

   For more information, see Configuring the OMNIbus Standard Input probe to work with Network Performance Insight in .

**Related tasks**

“Verifying the installation” on page 40
You can verify the Network Performance Insight 1.3 installation status.

"Setting up the OMNIbus Standard Input probe" on page 28
The Standard Input probe is bundled with Network Performance Insight and is installed along with it.

**Installation directory structure**
Use this information to understand the important directories that are created during installation.

These directories are created in `/opt/IBM/` path:

**basecamp**
- basecamp directory contains the following sub directories:
  - **basecamp-connect**
    Contains the Kafka connect script that is called from Ambari to start the service. It also contains the JDBC driver files that are needed to connect to IBM Db2, Oracle, and for Kafka to connect to database.
  - **basecamp-exporter**
    Contains the directories and files that are needed to integrate with .
  - **basecamp-installer-tools**
    This directory is available on the Ambari server host only. It contains the following subdirectories:
    - ambari contains the scripts that are needed for Ambari management.
    - dash-integration contains scripts:
      - Scripts that are needed for and integration.
      - Installing and uninstalling the security services
      - Creating and deleting console integration
    The dash-integration directory also has security-service subdirectory that contains the bundled security services software.
    - ootb_packs
      Contains the ready-to-use Technology Packs that can be installed in system for discovery and polling for resources.
    - pack_installer
      Contains the pack-install.sh script to install the Technology Pack and distribute the content to different services.
    - snmp
      Contains the snmp-scoping.sh script to filter and restrict the devices and resources for network polling.
    - upgrade contains scripts that are needed for upgrading to .
      - credential-migration
        Contains the snmp-credential-migration.sh script and JAR files for porting the existing Kafka and Flow device credentials to the new environment.
  - **basecamp-jre**
    Contains the Open Java SDK that is bundled with .
  - **basecamp-manager**
    Contains the directories and files that are needed for the Manager Service to function. It also contains the license files for .
  - **basecamp-schema-registry**
    Schema Registry provides a serving layer for your metadata. It stores a versioned history of all schemas, provides multiple compatibility settings, and allows evolution of schemas according to the configured compatibility setting.
**basecamp-storage**
Contains the directories and files that are needed for Storage Service to function.

**basecamp-timeseries**
Contains the directories and files that are needed for Timeseries Service to function. It has the following important additional sub directories:

- 3rdParty
  Contains Apache Cassandra and Kairos DB for timeseries data.
- content/metrics
  Contains all the metrics to be collected. Each metric file is identified with an extension .metric. For example, Network-Inbound-Discards-Count.metric.

**basecamp-tools**
Contains the encryption script, npm-encrypt.sh that can be used to encrypt passwords.

**basecamp-ui**
Contains the directories and files that are needed for UI Service to function.
It also contains the following files and directories that are needed for:

- resources/dashboards
  Contains the following sub directories:
  - json
    Contains all the dashboard JSON files that are successfully parsed and loaded after the installation in good directory and those dashboards that failed to load are in the bad directory. The JSON files that are under process are placed in processing directory.
  - properties
    Contains all the dashboard properties files.
- resources/oed
  Contains the following files and subdirectory:
  - oed.war
    It is the application engine WAR file.
  - sql
    Contains the SQL files that are related to the dashboards.
- work/oed
  This directory is a symbolic link to basecamp/work/basecamp-ui/oed. Contains the H2 database file as oed.mv.db.

**npi**

npi directory contains the following sub directories:

**npi-cacti-collector**
Contains the directories and files that are needed for Cacti Collector Service to function.

- resources
  Contains the following files:
  - PODS.zip
  - MIB2.zip
  - CiscoIPSLA.zip
  - cacti_reflector-1.0.0.tgz
npi-dns
Contains the directories and files that are needed for DNS Service to function.

npi-event
Contains the directories and files that are needed for Event Service to function. 64-bit STDIN probe is available in this directory and can be supported on Linux, AIX, and Solaris platforms.

npi-flow-analytics
Contains the directories and files that are needed for Analytics Aggregation Service to function.

npi-flow-collector
Contains the directories and files that are needed for Flow Collector Service to function.

npi-formula
Contains the directories and files that are needed for Formula Service to calculate formulas on the IP SLA metrics based on the data that is collected by the SNMP Collector Service. It also has the collection formulas and their related MIB files for polling the network for metrics. It has the following additional directories:

• content
  – bindings
    Contains the class files for the MIB OBJECT_TYPES that are used in the collection formulas.
  – formulas
    Contains all the collection formulas that are used for metric polling.
  – mibs
    Contains all the MIB files that are required for your formulas.

npi-itnm-collector
Contains the directories and files that are needed for Tivoli Network Manager - Collector Service to function.

• discovery
  Contains all the required folders and files for performing the second-level discovery by . Typically, devices are discovered by and all the resource types from those devices are discovered by . In scenario, you can write your own discovery formulas and use them to do SNMP device discovery independent of .

  – content
    Contains the discovery formula files and MIB files that are extracted from technology pack content. The discovery files are arranged according to the vendor. The vendor-specific directories are manually created for organizing the discovery files. All the MIB files that are required for discovery formulas are placed in the /content/mibs directory.
  – device
    Contains the sysobjectid.discovery file that is required for discovering the new devices.

npi-snmp-collector
Contains the directories and files that are needed for SNMP Collector Service that provides metric polling data from IP SLA enabled SNMP devices to .

npi-snmp-discovery
Contains the directories and files that are needed for accessing the devices with SNMP credentials to obtain and store the data for enriching the interfaces.

npi-threshold
Contains the directories and files that are needed for Threshold Service to function.

Typically, all the microservices have the directory stack as follows:
The logs directory contains a separate log file for each microservice.

**Uninstalling**

Uninstall and the related software from the system.

**Before you begin**

Before you uninstall, back up the following contents:

- Manually, back up the `/opt/IBM/basecamp/basecamp-installer-tools` folder in the Ambari Server host to save the previous configuration.
- Make sure to back up the following files from `/opt/IBM/basecamp/basecamp-installer-tools/dash-integration` directory if you plan to reuse them:
  - `security.keystore`
  - `priv_key.key` - private key
  - `ca.crt` - public key

**About this task**

Uninstall the following components that you installed:

- , including YARN, HDFS, and Zookeeper services.
- Ambari agents that contain Network Operations Insight instances.
- Ambari server

To uninstall all these components, follow these steps:

**Related information**

- Removing Tivoli Netcool/OMNibus
- Uninstalling Network Manager
- Uninstalling Jazz for Service Management and related software

**Listing working directories**

Network Performance Insight related components working directories can reside in the recommended locations or in the customized locations.

**About this task**

List down the working directories before you run the uninstallation scripts to make sure that they are removed.

**Note:** Manually, remove these working directories after the uninstallation scripts are run.

**Procedure**

1. Log in to Ambari server host as follows:
   
   ```http://<ambari_server_host>:8080```

2. Click **Services** and select the specific service and click the **Configs** tab.

3. Note down the following directories for the services and components:
<table>
<thead>
<tr>
<th>Services</th>
<th>Ambari Component directory</th>
<th>Example installation path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kafka</td>
<td>Kafka &gt; Configs &gt; Kafka Broker &gt; log.dirs</td>
<td>&lt;data&gt;/kafka-logs</td>
</tr>
<tr>
<td>HDFS</td>
<td>HDFS &gt; Configs &gt; Settings &gt; NameNode</td>
<td>&lt;data&gt;/hadoop/hdfs/namenode</td>
</tr>
<tr>
<td></td>
<td>HDFS &gt; Configs &gt; Settings &gt; DataNode</td>
<td>&lt;data&gt;/hadoop/hdfs/datanode</td>
</tr>
<tr>
<td></td>
<td>HDFS &gt; Configs &gt; Advanced &gt; Secondary NameNode &gt; SecondaryNameNode</td>
<td>&lt;data&gt;/hadoop/hdfs/namesecondary</td>
</tr>
<tr>
<td></td>
<td>Checkpoint directories</td>
<td></td>
</tr>
<tr>
<td>YARN</td>
<td>YARN &gt; Configs &gt; Advanced &gt; Application Timeline Server &gt; yarn.timeline-service.leveldb-timeline-store.path</td>
<td>&lt;data&gt;/var/log/hadoop-yarn/timeline</td>
</tr>
<tr>
<td></td>
<td>YARN &gt; Configs &gt; Advanced &gt; Advanced yarn-site &gt; yarn.timeline-service.leveldb-state-store.path</td>
<td>&lt;data&gt;/hadoop/yarn/timeline</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>Ambari Metrics &gt; Configs &gt; Advanced ams-hbase-site &gt; hbase.rootdir</td>
<td>&lt;data&gt;/var/lib/ambari-metrics-collector/hbase/var/var/lib/ambari-metrics-collector/hbase-tmp</td>
</tr>
<tr>
<td>ZooKeeper</td>
<td>ZooKeeper &gt; Configs &gt; ZooKeeper Server &gt; ZooKeeper directory</td>
<td>&lt;data&gt;/hadoop/zookeeper</td>
</tr>
</tbody>
</table>

**Note:** `<data>` is the full directory path where you have set up all the services.

**Uninstalling Network Performance Insight node**

Run the `host_cleanup.sh` script to uninstall the Ambari Server hosts and Network Performance Insight node hosts.

**Before you begin**

- Stop all the services for each host from Ambari.
- Back up your data.

**Procedure**

1. Copy the `host_cleanup.sh` script from `/opt/IBM/basecamp/basecamp-installer-tools/ambari/host_cleanup.sh` to the Network Performance Insight Nodes that you want to uninstall.

   For example, `/tmp/host_cleanup.sh`.

2. Run the script as `root` user as follows:

   ```
   cd /tmp
   ./host_cleanup.sh
   ```

The `host_cleanup.sh` script performs the following functions:
• Checks the user who is running the script is root or not
• Checks for the HostCleanup.ini file
• Stops the Ambari Server and the Network Performance Insight node, if they are still running.
• Stops the Linux processes that are started by a list of service users. The users are defined in the HostCleanup.ini file. You can also specify a list of Linux processes to be stopped.
• Removes the PRM packages that are listed in the HostCleanup.ini file.
• Removes the Network Performance Insight packages and working folders.
• Removes the service users that are listed in the HostCleanup.ini file.
• Deletes directories, symbolic links, and files that are listed in the HostCleanup.ini file.
• Deletes repositories that are defined in the HostCleanup.ini file.

Related information
Cleaning up nodes before reinstalling software

Uninstalling Ambari server host
Use the cleanup scripts to remove the Ambari server host, which is the master node.

Procedure
1. Move the uninstallation scripts from /opt/IBM/basecamp/basecamp-installer-tools/ambari to /tmp directory.
2. Run the cleanup scripts as root user on the Ambari server in the following order:

   /tmp/host_cleanup.sh
   /tmp/cleanup.sh

   **Note:** Ignore the error messages from cleanup.sh as most of the uninstallation is done by the host_cleanup.sh script.
   Ambari Server and all the Network Performance Insight microservices are removed.
3. Remove all the working directories that are listed previously.

   For more information, see “Listing working directories” on page 49.

Removing Dashboard Application Services Hub integration
Use this information to remove the directories and settings that are related to Dashboard Application Services Hub integration.

Procedure
1. Log in to Dashboard Application Services Hub as administrator user.
2. In the navigation pane, click **Console Settings > Websphere Administrative Console** and click **Launch Websphere administrative console**.
3. Click **Security > SSL certificate and key management**.
4. Under **Related items** on the right, click **SSL configurations > NodeDefaultSSLSessions**.
5. Change the **Default server certificate alias** and **Default client certificate alias** to **Default**.
6. Click **OK** and save the changes to master configuration.
7. Click **Key stores and certificates > NodeDefaultKeyStore > Personal certificates** and remove the netcool certificate.
8. Save the changes to master configuration.
9. Click **Key stores and certificates > NodeDefaultTrustStore > Signer certificates** and remove the npi-ca certificate.
10. Save the changes to master configuration.
11. Restart WebSphere Application Server.
12. Remove the /opt/IBM/dash-integration directory.

**Related tasks**

“Generating the certificate and keystore files” on page 32
Generate the certificate authority (CA) certificates and other keystore files on Ambari server.

“Enabling integration with Jazz for Service Management” on page 32
Use this information to enable integration between Network Performance Insight and Dashboard Application Services Hub portal.

**Related information**

Restarting Jazz for Service Management application servers

**Uninstalling Remote Flow Collector**

Use these steps to uninstall all the Remote Flow Collectors.

**Before you begin**

Stop the Remote Flow Collector Service. For more information, see *Stopping the Remote Flow Collector associated services* in *Administering IBM Network Performance Insight*.

**Procedure**

Run these manual commands on the servers where you set up the Remote Flow Collectors to erase the packages:

```
yum erase -y npi-remote-flow-collector
yum erase -y zookeeper_2_6_4_0_91
yum erase -y hdp-select
yum erase -y ranger_2_6_4_0_91-kafka-plugin
yum erase -y basecamp-jre
```

**What to do next**

After the uninstallation is complete, perform the following steps:

- Remove the .repo files from /etc/yum.repos.d directory if they exist:
  - npi.repo
  - hdp.repo
- Remove the following folders:
  - /data/kafka-logs
  - /var/log/zookeeper
  - /var/lib/zookeeper

**Troubleshooting installation**

Problems that might occur during an installation and how to resolve them.

**About this task**

For all troubleshooting issues in installation of, see *Troubleshooting installation and uninstallation* section in *Troubleshooting Network Performance Insight*.

For all troubleshooting issues in deploying Ambari clusters, see *Troubleshooting Ambari server* section in *Troubleshooting Network Performance Insight*.

For all troubleshooting issues in integration of, see *Troubleshooting integration with* section in *Troubleshooting Network Performance Insight*. 
Configuring
You can configure IBM Network Performance Insight, Version 1.3 and its integration services through user interface console and command line interface. You can also administer and manage application security and single sign-on from Dashboard Application Services Hub portal.

About this task
Most of the configurations are performed through web-based UI on Ambari server. For Network Performance Insight to be fully functional and accessible on Jazz for Service Management, you must perform the following configurations:

• Configure Network Performance Insight system.
• Configure the required Ambari services and Network Performance Insight services from Ambari web interface.
• Configure integration with Tivoli Netcool/OMNIbus.

Configuring Network Performance Insight system environment
Use this information to configure your Network Performance Insight system that is integrated with Dashboard Application Services Hub from the graphical user interface.

You must do some general system configuration and tuning for optimizing the system performance. During implementation, you must configure the application options to meet your requirements.

You can view the current settings, modify the settings, add new, or delete an existing configuration item. These configuration settings are stored in the database and can be retrieved from the CFG schema tables. Each configuration setting is associated with a separate widget on Dashboard Application Services Hub UI.

The Network Performance Insight dashboards are pre-configured with working sets of default configurations that are created right after installation. A broad range of functions in Network Performance Insight can be administratively configured.

You can configure the following items from system configuration:

• Autonomous System
• Domain names
• Flow Aggregations
• Flow Devices
• Interfaces
• IP Grouping
• NBAR
• Retention profiles
• Thresholds
• Type of Services

Note: These configuration settings are specific for Flow data only. Only the following Dashboards are applicable for the scenario where NetFlow data alone is collected, stored and aggregated:

• NetFlow Dashboards
• On Demand Filtering - Flow Dashboard

For more information about troubleshooting system configurations, see Troubleshooting IBM Network Performance Insight.
Logging in to the portal
Depending upon your organization’s deployment, you can access the reporting interface through Dashboard Application Services Hub.

Procedure
• Access the reporting interface from Dashboard Application Services Hub as follows:
  a) Open a web browser and enter the following URL for the Jazz™ for Service Management UI and reporting server:
     https://host.domain:port/DASH_context_root
     For example: https://<myserver.ibm.com>:16311/ibm/console
     Where:
     - host.domain is the fully qualified host name or IP address of the Jazz for Service Management UI and reporting server.
       When single sign-on (SSO) is enabled, ensure that you use the fully qualified host name in the URL of the Jazz for Service Management reporting and UI server. SSO requires that the browser pass LTPA cookies to the Jazz for Service Management application server, and these cookies contain the fully qualified host name.
     - port is the secure HTTP port number that was specified during installation. The default value is 16311.
     - /DASH_context_root is the context root for the console that was specified during installation. The default value is /ibm(console).
  b) Enter the user ID and password in the Dashboard Application Services Hub login page. Click Log in.
     For example, npiadmin/netcool
     The Dashboard Application Services Hub Welcome page opens.
  c) Click Console Integration icon ( ) on the navigation bar and select the dashboard of your choice under System Configuration.

Configuring Autonomous System
To assign a routing domain for your network, configure the Autonomous System that uses Border Gateway Protocol (BGP). BGP shares routing information with other autonomous systems with the help of a globally unique 16-digit identification number that is known as the AS number (ASN). AS numbers are assigned by the Internet Assigned Numbers Authority (IANA).

About this task
The Autonomous Systems information that is configured and stored is displayed in the Top Autonomous System Conversations view in Traffic Details dashboard.

Procedure
  1. Click Console Integrations ( ) in the navigation bar, and select Autonomous System under System Configuration.
     Add an Autonomous System.
  2. Click New ( ) icon and enter the Autonomous System information as follows:
     Id
     Mandatory field that represents a unique ASN.
**Note:** Autonomous System numbers one to 64511 are available by IANA/ARIN (IANA/American Registry for Internet Numbers) for global use. The 64512 - 65535 series is reserved for private and reserved purposes.

**Name**
Name of the Autonomous System.

**Note:** Autonomous System numbers, one to 64511 have predefined names for global use. The 64512 - 65535 series is reserved for private and reserved purposes.

**Country**
Country to which the specific network routing domain belongs to.

**Is public**
Whether network domain is a private use ASN or with in the public AS range.

Edit an Autonomous System.

3. Select a row from the table and click the **Edit** icon to change the information for the Autonomous System.

Delete an Autonomous System.

4. Select an entry from the table and click the **Delete** icon to delete an entry that is not needed.

Common tasks that are applicable for most of the configuration settings.

5. Click the **Filter** icon and type an item name or ID in the **Filter by <keyword>** field.

6. Click the **Refresh** icon to refresh the list of items.

7. Select a number in the lower-right corner to change the number of items to be displayed in the table.

8. Go to a specific page by using the arrows in the bottom of the page.

9. Navigate to a specific page from the page numbers at the bottom of the page.

**Related information**
List of Autonomous Numbers

**Configuring domain names**
Domain name is an identification of a unique computer system on the internet that is universally agreed by web servers and online administrations and offers all related destination information. To access an organization’s web-based facilities, website users must identify the exact domain name. A complete domain name consists of one or more subdomain names and one top-level domain name that is separated by dots (.). For example, `<myserver.ibm.com>` is a complete domain name.

**About this task**
Configuring Domain Names helps in handling the frequently used, well-known domain names of your organization.

You can add a set of pre-defined domain names in system, such as `youtube.com`, `facebook.com`, `yahoo.com`, and so on.

With these pre-defined configurations, the DNS performs forward resolution to get a list of IP addresses for the domain names. When a flow record is received, DNS service in Network Performance Insight tries to match the source IP and destination IP with the resolved IP address and maps it to the domain name. The traffic detail page then displays as the configured domain name instead of a string of IP.

Without these pre-defined configurations, the aggregation takes the IP address and performs DNS reserve resolution, which might not populate a friendly domain name.

You can configure domain names to be resolved for IP address mapping.
**Note:** Database tables store specific types of data and can be categorized into the configuration, event, aggregation, and flow data in database tables. The database table for configuration displays the data for Domain Names.

**Procedure**

1. Log in to Jazz for Service Management server.

2. Click **Console Integrations** in the navigation bar, and select **Domain Names** under **System Configuration**.

   Add a domain name.

3. Click **New** icon and enter the domain name to create a new domain name to be resolved.

4. Select an entry from the table and click **X** icon to delete an entry that is not needed.
   
   This option helps you to delete an entry that has a typographical error.

   a) Delete any entry that is no longer needed.
   
   b) Delete a wrong entry and create a new entry.

   **Note:** Domain names that start or end with "." or ":" are not accepted.

5. Click **OK** to save the settings.

**What to do next**

You can repeat the same process to configure commonly used Domain Names as needed.

**Configuring Flow aggregations**

User configurable Flow aggregations increase the performance of NPI system by optimizing the CPU utilization and reduce the I/O demands on database. It helps in Top Talker optimizations. Top N Talkers support feature helps you analyze large amount of data that Flexible NetFlow captures from the network traffic. You can filter, aggregate, and sort the data for display. When you are sorting and displaying the data in the NetFlow cache, you can limit the display output to a specific number of entries with the highest values (Top N Talkers) for traffic volume, packet counters, and so on.

**About this task**

By default, some of the aggregations are enabled and the others are user configurable. Some of these aggregations require other related configurations to be enabled. The following table provides information about all the available user configurable aggregations:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Type of aggregation</th>
<th>Enabled by default</th>
<th>Required additional configuration setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Top Applications</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Applications with Source ToS</td>
<td>No</td>
<td>See Configuring Type of Service section in</td>
</tr>
<tr>
<td>Autonomous systems</td>
<td>Top Autonomous System Conversations</td>
<td>No</td>
<td>See Configuring Autonomous System section in</td>
</tr>
<tr>
<td></td>
<td>Top Destination Autonomous System</td>
<td>No</td>
<td>See Configuring Autonomous System section in</td>
</tr>
<tr>
<td>Resource</td>
<td>Type of aggregation</td>
<td>Enabled by default</td>
<td>Required additional configuration setting</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Top Source Autonomous System</td>
<td></td>
<td>No</td>
<td>See Configuring Autonomous System section in</td>
</tr>
<tr>
<td>Conversations</td>
<td>Top Conversations</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Conversations with Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Conversations with ToS</td>
<td>No</td>
<td>See Configuring Type of Service section in .</td>
</tr>
<tr>
<td>Destinations</td>
<td>Top Destinations</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Destinations with Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>IP Address Grouping</td>
<td>Top IP Group Conversations with Application</td>
<td>No</td>
<td>See Configuring IP Grouping section in .</td>
</tr>
<tr>
<td></td>
<td>Top IP Group Conversations with Protocol</td>
<td>No</td>
<td>See Configuring IP Grouping section in .</td>
</tr>
</tbody>
</table>
|                        | Top IP Group Conversations with Source ToS | No                 | • See Configuring IP Grouping section in .  
|                        |                                            |                    | • See Configuring Type of Service section in .  |
|                        | Top Destination IP Groups with Application  | No                 | See Configuring IP Grouping section in .  |
|                        | Top Destination IP Groups with Protocol     | No                 | See Configuring IP Grouping section in .  |
|                        | Top Destination IP Groups with Source ToS   | No                 | • See Configuring IP Grouping section in .  
|                        |                                            |                    | • See Configuring Type of Service section in .  |
|                        | Top Source IP Groups with Application       | No                 | See Configuring Autonomous System section in |
|                        | Top Source IP Groups with Protocol          | No                 | See Configuring Autonomous System section in |
|                        | Top Source IP Groups with Source ToS        | No                 | • See Configuring IP Grouping section in .  
<p>|                        |                                            |                    | • See Configuring Type of Service section in .  |</p>
<table>
<thead>
<tr>
<th>Resource</th>
<th>Type of aggregation</th>
<th>Enabled by default</th>
<th>Required additional configuration setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Source IP Groups</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
<td></td>
</tr>
<tr>
<td>Top IP Group Conversations</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
<td></td>
</tr>
<tr>
<td>Top Destination IP Groups</td>
<td>No</td>
<td>See Configuring IP Grouping section in.</td>
<td></td>
</tr>
<tr>
<td>Quality of Service</td>
<td>Top QoS Hierarchies with Queue ID</td>
<td>No</td>
<td>QoS fields must be configured on your devices. See Configuring Flexible NetFlow and AVC section in Configuring Flow devices.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocols</th>
<th>Top Protocols</th>
<th>Yes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Protocols with Application</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Top Protocols with Conversation</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Top Protocols with Destination IP</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Top Protocols with Source IP</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sources</td>
<td>Top Sources</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Top Sources with Application</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

| Type of Service           | Top Source ToS                       | No                  | See Configuring Type of Service section in.                                    |

**Procedure**

Enable or disable an aggregation or modify the aggregation fields from the list.

1. Click **Console Integrations** in the navigation, and select **Flow Aggregation** under **System Configuration**.

2. Select a row from the table and click the **Edit** button or select **Edit** in the **Actions** column as follows:

   **Aggregation**
   Name of the aggregation as it appears in the table.

   **Aggregation Fields**
   Aggregation grouping keys or fields in the aggregation.
Visible in Traffic Details
By default, when an aggregation type is disabled, the Top Talker view that is associated with the
specific aggregation is not visible from the Traffic Details dashboard. Select the check box to
display the Top Talker view with the historical data even if the aggregation is disabled.

Note: This control affects only the Traffic Details dashboard views but does not affect the Flow
dashboard views.

Enabled
Select the check box to enable the aggregation.

3. Optional: Click Enable or Disable to enable or disable an aggregation in the Actions column.

Results
When an aggregation type is disabled, the historical data remains in the database with no further updates
to the CFG schema tables and Flow Metric schema tables.

Configuring Flow Devices
You can configure the SNMP credentials for all NetFlow enabled devices in your network to send the data
to from System Configuration on navigation. All devices must be configured to export SNMP data to. This
information is stored in the database and required for interface enrichment.

About this task
You must specify SNMP community strings for to discover the devices for SNMP data. To configure the
general parameters for the SNMP requests, follow these steps:

Procedure

1. Click Console Integrations ( ) in the navigation bar, and select Flow Devices under System
Configuration.
2. Select an Exporter IP of a device from the table and click Info in the Actions column to see the existing
information for the exporter.
3. Select an Exporter IP of a device from the table and click the Edit ( ) button or select Edit in the
Actions column.
4. Enter the following details:

Read Community String
SNMP community string is like the user ID or password and is required for SNMP V1 and V2
versions only. SNMP V3 version uses user name and password credentials with encryption key.
Specify the name of the SNMP read community. By default, the SNMP community string for SNMP
V1 and V2 versions is set to public. You can change all the community strings to customized values
in this field.

SNMP Version
Specify the SNMP version that is associated with this SNMP configuration. Make sure to select the
version that is supported on the device. SNMP versions are as follows:

• V1
  Basic version of SNMP. This version is supported by most devices and easy to set up. It has
  limited security.
• V2
  Supports 64-bit counters to monitor the bandwidth usage of networks high volumes of data. It
  has limited security.
• V3
Supports authentication and encryption of the credentials for multiple users. Highly secure version.

5. If the SNMP version for the device is V3, specify the following information:

   **Level**
   Specify the required level of authentication and privacy. The following levels are available:
   - **noAuthNoPriv**
     Select this option for SNMP communities that have no authentication or private key. In this case, you do not need to specify any passwords. Then, specify the **Context Name** and **Security Name**.
   - **authNoPriv**
     Select this option for SNMP communities that have an authentication key but no private key. Then, specify values in the **Auth Type**, **Context Name**, **Security Name**, and **Auth Password** fields.
   - **authPriv**
     Select this option for SNMP communities that have both an authentication and a private key. Then, specify values in the **Auth Type**, **Priv Type**, **Priv Password**, **Context Name**, **Security Name**, **Auth Password**, and **Priv Password** fields.

   **Auth Type**
   This field is applicable if the level is **authNoPriv** and **authPriv** to specify the type of encryption for the authentication password. The following types of encryption are available:
   - SHA1
   - MD5

   **Priv Type**
   This field is applicable if the level is **authPriv** to specify the type of encryption for the privacy password. The following types of encryption are available:
   - 3-DES
   - AES 128
   - AES 192
   - AES 256

   **SNMP Port**
   Specify the required port. By default, the port number is 161.

   **Context Name**
   An SNMP context defines a collection of management information that is accessible to an SNMP entity. Each context in a management domain has a unique identifier. The **Context Name** field is optional and depends on the user.

   **Security Name**
   Security Name is used when access control is set up.

   **Auth Password**
   Authentication password. It must be same as the device authentication password.

   **Priv Password**
   Privacy password. It must be same as the device privacy password.

6. Click **Enrich** from the **Actions** column.

After the interface is enriched with additional information, such as interface speed, interface name, and interface description from the device and the **Enrichment State** field value is changed to **COMPLETE**. This information for the specific interface is updated in the **Interfaces** configuration page and also updated in the database.
Optionally, you can do the manual enrichment by entering the interface details from *Interfaces* page from System Configuration. For more information, see “Configuring Flow interfaces” on page 61. The manual enrichment overrides the enrichment from Flow Devices configuration.

Optionally, you can do the manual enrichment by entering the interface details from *Interfaces* page from System Configuration. For more information, see *Configuring Flow interfaces* section from . The manual enrichment overrides the enrichment from Flow Devices configuration.

*Configuring Flow interfaces*

Flow records provide unidirectional measurements of traffic that is entering (ingress) or leaving (egress) a network interface. Network Performance Insight models this process by associating an Ingress Interface and Egress Interface with each network interface. Each flow record is associated with the appropriate flow interface.

**About this task**

automatically creates flow interfaces when flow records are processed. When new interfaces are created, they are enabled unless the total number of interfaces exceeds the limit. processes the data that is associated with a flow interface only if it is enabled.

**Procedure**

1. Log in to Jazz for Service Management server.

2. Click *Console Integrations* in the navigation, and select *Interfaces* under *System Configuration*.

3. Select a row from the table and click the *Edit* button to enable or disable the selected interface.

4. Click *OK* to save the configuration.

5. Optional: Enter the following interface details to manually update the interface details for enrichment:
   - *Interface Name*
   - *Interface Description*
   - *Speed*

   **Note:** These details override the information that is obtained from devices by configuring the SNMP credentials in *Configuring Flow Devices* section in .

6. Optional: Click *Enable* or *Disable* to enable or disable an Interface for flow data collection in the *Actions* column.

**What to do next**

You must repeat the same process to enable or disable all interfaces as needed.

**Note:** Currently, you cannot select multiple interfaces to configure to enable or disable for traffic data collection at a time.

*Configuring Flow IP Grouping*

Create logical grouping of IP addresses and address ranges. This grouping helps in monitoring the individual NetFlow bandwidth usage, usage-based billing, and accounting.

**About this task**

- To configure multiple IP ranges into a single IP address group, create multiple row entries with same IP address group.
- Make sure that the IP range does not overlap with existing ones. Otherwise, you might see Overlapping Ip address grouping range message.
Procedure

1. Click **Console Integrations** in the navigation bar, and select **Flow IP Grouping** under **System Configuration**.
   Add an IP address group.

2. Click **New** icon and enter the IP address grouping information as follows:
   - **IP Address Group**
     Logical name to the group. Create your IP Grouping by location. For example, branch offices or departments for easier monitoring.
   - **Start Address Range**
     Start IP address for the range.
   - **End Address Range**
     End IP address for the range.
   - **Enabled**
     A flag to enable or disable the specified IP address group.

3. Click **Ok** to save the settings.

4. Select a row from the table and click the **Edit** button to change the information for the IP Address Group.

5. Click **Ok** to save the settings.

6. Select an entry from the table and click **icon to delete an entry that is not needed.**

**Configuring NBAR**
Configure your devices to send NBAR and NBAR2 data to gain better visibility on the applications in your NetFlow traffic. This information helps you identify the bandwidth usage of the applications in your network and also prioritize and control the application traffic. You can define the business relevance of the applications and apply the correct QoS policies to improve the performance and user experience of business-critical applications.

**About this task**
NBAR and NBAR2 configured devices send Flow packets that contain the following metrics:
- Engine ID
- Selector ID
- Name
- Description
- Category Name
- Subcategory Name
- Group Name
- P2P Technology
- Tunnel Technology
- Encrypted Technology
- Business Relevance
**Procedure**

1. Click **Console Integrations** in the navigation bar, and select **NBAR** under **System Configuration**.

   Edit the NBAR and NBAR2 settings.

2. Click **Edit** icon to enable or disable the ART metric collection:

   Select the **Enable ART** check box to enable the collection of Application Response Time (ART) metrics for TCP traffic.

   The following fields are not editable:

   **Engine ID**
   - A unique identifier for the engine that determined the Selector ID. The Engine ID is the first 8 bits that provide information about the engine that classifies the flow.

   **Selector ID**
   - The remaining 24 bits that provide information about the application.

   **Note:** Engine ID and Selector ID constitute the Application ID.

   **Name**
   - Name of the application that is derived from the Application ID.

   **Description**
   - Application description that can be derived from the Application option template.

3. Click **Ok** to save the settings.

4. Optional: Click **Enable** or **Disable** to enable or disable an ART in the **Actions** column.

**Related information**
Cisco Application Visibility and Control Field Definition Guide for Third-Party Customers

**Configuring data retention profiles**
Describes how to configure the retention profiles for different type of data that is collected by.

**About this task**
Retention profiles control how long the raw and aggregated data, and log files are retained by the system. Setting the retention profiles help in maintaining the amount of data to be stored in the database and free the additional disk space. You can change the default values to modify the retention periods. For timeseries data alone, set the retention period from Ambari.

**Note:** Entity Metric schema tables retention profile settings are not available in a fresh installation, since the data is now moved to timeseries database. But you notice the retention profile settings for Entity Metric schema tables in an upgraded system.

For more information, see **Retention period** section in Network Performance Insight overview IBM.

To configure retention profiles:

**Procedure**

1. Log in to server.

2. Click **Console Integrations** in the navigation bar and select **Retention Profiles** under **System Configuration**.

   You can see Retention Profiles table.

3. Select a row from the table and click the **Edit** button to configure a retention profile period for an Interface. Enter the following details:
Name

The Name field is already selected.

Period

Type the period for which you want to retain the data.

Unit

Select the unit; Days, Weeks, or Months.

Note: Retention period must be configured with tradeoff between storage size and number of days to keep the data. The graphs will not show any data after the time period that you selected for a particular interface.

For more information, see Data storage section in Network Performance Insight overview IBM.

4. Click OK to save the settings.

What to do next

Repeat the same process to configure retention profiles as needed. For timeseries data alone, set the retention period from Ambari.

For more information, see Configuring retention period for timeseries data section on .

Configuring site grouping

You can categorize your enterprise network based on different geographical areas by specifying the IP address ranges for each site. Each site can be configured for specific business and non-business days and hours.

About this task

This grouping helps in monitoring the individual site bandwidth usage, usage-based billing, and accounting. You can also get visibility on the network bandwidth usage during business and non-business days and hours.

Procedure

1. Click Console Integrations ( ) in the navigation bar, and select Sites under System Configuration.

Add a site group.

2. Click New ( ) icon and enter a site information as follows:

Site Name

Logical name to the site. Create your site by location. For example, branch office locations for easier monitoring.

IP Address Ranges

Start and end IP address for the range that is specific to the site. You can give the ranges separated by a hyphen or as comma-separated list.

Day

All days from Sunday to Saturday are listed. Select the days based on the typical business days for your site.

Business Start Time

Specify the typical business start time in hh:mm format.

Business End Time

Specify the typical business end time in hh:mm format.

Time Zone

Select the time zone to which the site belongs to from the list.

Edit a site group.
3. Select a row from the table and click the Edit (✔️) button to change the information for the site.
4. Click Ok to save the settings.

Delete a site group.

5. Select an entry from the table and click the Delete button (❌) icon to delete an entry that is not needed.

**Configuring Flow thresholds**
Thresholds provide a mechanism for identifying anomalies in flow and metric data that is polled from. Threshold is a metric value that is compared against a value to determine whether an interface violated a specific constraint. The threshold violations and their values are user-defined and not dynamically generated. These threshold values are defined per interface in each direction.

**About this task**
You can configure the threshold value per interface for anomalies detection.

**Procedure**

1. Log in to server.

2. Click **Console Integrations** (🔍) in the navigation bar and select **Thresholds** under **System Configuration**.
   You can see Flow Thresholds table.

3. Select a row from the table and click the Edit (✔️) button to configure a Threshold for that Interface. Enter the following details:
   a) Select the **Enabled** check box to enable a Threshold on the Interface.
   b) Select the limit type from the **Limit Type** list to **Over**, **Under**, or **Band** and their units.
      - **Over**
        Detect violations when the interface exceeds the set Threshold value.
      - **Under**
        Detect violations when the interface falls short of the set Threshold value.
      - **Band**
        Detect violations the interface goes outside a range (or band) between two set Threshold values.
   c) Enter a value in the **Upper Limit** field for the interface to trigger a Threshold violation.
   d) Enter a value in the **Lower Limit** field for the interface to trigger a Threshold violation.
   e) Enter the number of events for triggering the Threshold.
      **Note:** When the Threshold limit is violated, it displays the severity as **Critical**.
      For more information, see **Threshold violation** in

4. Perform the following tasks in the **Actions** column:
   a) Click **Edit** to edit or configure the selected Threshold. Repeat step 3
   b) Click **Enable** or **Disable** to enable or disable an interface to detect its Threshold violation states.

5. Click **OK** to save the settings.

**Results**
Any interface that is violating the set Threshold value is reported in the Event Viewer.
**What to do next**
You must repeat the same process to enable and configure thresholds for every Interface as needed.

**Note:** Currently, you cannot select multiple interfaces to configure the Thresholds values at a time.
To configure thresholds for metric data, see Defining anomaly thresholds.

**Configuring Type of Service**
Typically, this feature determines the packet delivery prioritization for low-delay, high-throughput, highly reliable service, or normal service for NetFlow traffic. On all Flow packets, Type of Service byte is represented as Differentiated Service Code Point (DSCP) and Explicit Congestion Notification.

**Procedure**

1. Click **Console Integrations** (WebSocket) in the navigation bar, and select **Type of Services** under **System Configuration**. Edit the Type of Services mappings.

2. Click **Edit** icon and modify the Type of Services metrics as follows:

   **ToS ID**
   This field is not editable. This field implements the Type of Service on the NetFlow packet to tradeoff on delay, throughput, reliability, and cost.

   **ToS Name**
   You can specify any name to your Type of Service class. Typically, the classes and their IDs are as follows:

<table>
<thead>
<tr>
<th>DSCP Code</th>
<th>DSCP ID (Decimal format)</th>
<th>IP Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best Effort</td>
<td>0</td>
<td>0 - Routine or Best Effort</td>
</tr>
<tr>
<td>CS1, AF11-13</td>
<td>8,10,12,14</td>
<td>1 - Priority</td>
</tr>
<tr>
<td>CS2, AF21-23</td>
<td>16,18,20,22</td>
<td>2 - Immediate</td>
</tr>
<tr>
<td>CS3, AF31-33</td>
<td>24,26,28,30</td>
<td>3 - Flash - used for voice signaling</td>
</tr>
<tr>
<td>CS4, AF41-43</td>
<td>32,34,36,38</td>
<td>4 - Flash Override</td>
</tr>
<tr>
<td>CS5, EF</td>
<td>40, 46</td>
<td>5 - Critical - used for voice RTP</td>
</tr>
<tr>
<td>CS6</td>
<td>48</td>
<td>6 - Internetwork Control</td>
</tr>
<tr>
<td>CS7</td>
<td>56</td>
<td>7 - Network Control</td>
</tr>
</tbody>
</table>

   Where:
   - CS - Class Selector
   - AFxy - Assured Forwarding (x=class, y=drop precedence)
   - EF - Expedited Forwarding

   **Note:** Traffic classification is an automated process that categorizes network traffic according to various parameters into a number of traffic classes.

   **Note:** The ToS names must be unique.

3. Click **Ok** to save the settings.

**Related information**
DSCP and Precedence Values
Configuring integration with Tivoli Netcool/OMNIbus
Use this information to integrate with the Tivoli Netcool/OMNIbus Web GUI application. The Tivoli Netcool/OMNIbus Web GUI customizable dashboards display real-time performance information and event data.

About this task
An event contains the Event ID, host name, and port information. When an event is selected, some of the data for the event is sent to and used to determine the best report to present. Then builds a block of HTML content that redirects the browser to a display.

Right-click an event in Event Viewer or Active Event List of Web GUI to display the tools that are added from the alerts menu. You select an option from this menu to display a detailed report for the time period of the threshold violation or an AEL report.

Configuring launch-in-context integration with Network Performance Insight
Launch-in-context integrations are supported between the Web GUI and other widgets. A launch-out integration describes the launching of another product from a Web GUI widget. A launch-in integration describes the launching of the Web GUI from another product.

About this task
Launch-in-context is the concept of moving seamless from one Tivoli product UI to another Tivoli product UI (either in a different console or in the same console or portal interface) with single sign-on and with the target UI in position at the proper point for users to continue with their task.

Related information
Configuring launch-in-context integrations with Tivoli products

Creating a launch-in-context tool
You can create tools that are run from right-click menus in event lists or when users click a widget. Different tool formats are supported.

Procedure
1. Log in to server as an administrator user, such as npiadmin.
2. Select Administration > Event Management Tools > Tool Configuration from the left pane.
3. Click Create Tool and enter the following details:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>npiFlowTvLiC</td>
</tr>
<tr>
<td>Type</td>
<td>script</td>
</tr>
<tr>
<td>Script Commands</td>
<td>Copy and paste the contents of the file npiFlowTvLiC.js that is available in opt/IBM/basecamp/basecamp-ui/resources/ael.</td>
</tr>
</tbody>
</table>
4. Select the data source name OMNIBUS.
5. Clear the Execute for each selected row check box.
6. Click Save.
   A confirmation message is displayed. Click OK to close the message.

Related information
Tools overview
Configuring launch-in-context menu
In event lists, users access default and custom tools through menus. You can add tool entries to the menus, create new submenus, and modify or delete menu items.

About this task
The two supplied menus are the Alerts menu and the Tools menu. The Alerts menu can also be opened from the right-click menu when you select an event.

Procedure
1. Log in to server as npiadmin user.
2. Select Administration > Event Management Tools > Menu Configuration from the left pane.
3. Select the alerts menu in the window, and then click the Modify button.
4. Select the npiFlowTvLiC tool in the Available items on the left, click the arrow to move it to the Current items section.
5. Select npiFlowTvLiC from the Current items section and click Rename.
6. In the Label text box, enter a meaningful name for the new button.
   For example, Flow Dashboard. If needed, enter a value in the Mnemonic text box, if needed.
7. Click Save.
8. Use the button selections on the right to move the menu option up or down.
   Separators might also be added by selecting <Separator> in the Available Items area of the window. The separator might be moved up and down.
9. Click Save.
10. The following message is displayed:
    Menu has been successfully modified.
Results
When you right-click any event in Event Viewer or in Active Event List, you can see the npiFlowTvLiC tool that is renamed to Flow Dashboard as a selectable option in the menu. Select the tool to see the Traffic Details report associated with the interface that violated the threshold and generated the event.

Configuring non-default ObjectServer name
By default, the Object Server name is NCOMS. If you configured a non-default name for the ObjectServer, use this information to configure to work with the non-default ObjectServer name.

Procedure
1. Edit the npi-flow-stdin.props file that is located in /opt/IBM/npi/npi-event/stdin-probe/omnibus/probes/linux2x86 to change the following value:

```plaintext
#######################################################################
# Add your settings here
#
Manager                       : 'NPI'
Server                        : '<non-default ObjectServer name>'
```
2. Save the file.
3. Edit the interfaces.linux2x86 file that is located in /opt/IBM/npi/npi-event/stdin-probe/etc to comment the NCOMS and add the non-default ObjectServer name as follows:

```bash
# NCOMS => omnihost 4100
# NCOMS
<non-default ObjectServer name>
master tcp sun-ether omnihost 4100
query tcp sun-ether omnihost 4100
```

4. Save the file.
5. Restart the Event Service from Ambari.
   - See Controlling the services from Ambari administration interface in .
   - See Setting up the OMNIbus Standard Input probe section in .

**Scenario 4 - Add on Performance data to NetFlow only data**

In this scenario, Network Performance Insight can be used to collect, aggregate, and render the NetFlow data alone. Later, if you choose to obtain the performance data.

Extended functions from Network Performance Insight itself to collect, store and render the performance data. Integration with Tivoli Network Manager is required only for discovery data.

**Installing**

The installation information contains the installation prerequisites, instructions for preparing to install, installing, and uninstalling the software based on your scenario.

**About this task**

Follow the general installation roadmap to complete required and optional steps, according to your needs.

**Integrating with Tivoli Network Manager**

Use this information to integrate your NetFlow only environment with Tivoli Network Manager.

**Preparing to integrate with Tivoli Network Manager**

If you decide to monitor Performance data that is collected from Tivoli Network Manager, then you must perform these tasks to prepare for the integration.

**Before you begin**

Before you begin your integration with Tivoli Network Manager, follow these steps:

**Enabling the required services**

You must enable the microservices that are required to integrate with IBM Tivoli Network Manager IP Edition. You might have disabled these services after the installation is complete.

**About this task**

You must enable the following services that are disabled:

- Tivoli Network Manager Collector
- Formula Service

**Procedure**

1. Open a browser and access the Ambari server dashboard.
   - Use the following default URL: http://<myserver.ibm.com>:8080
   - The default user name is admin, and the default password is admin.
2. Click the Hosts tab and select an Network Performance Insight node host.
All the services are displayed in the **Summary** page.

3. Select **Start** from the **Stopped** list.

   The service is started.

4. Click **Turn off Maintenance Mode** for that service from **Started** list.

   This service can be started when you start all the services next time.

**What to do next**

You can disable the SNMP Discovery Service since it is no longer required after the integration with Tivoli Network Manager.

**Deleting console integration**

Use this information to delete the console integration.

**About this task**

If you have performed console integration directly by using the `createConsoleIntegration.sh` script, then delete the console integration during the uninstallation process. The `createConsoleIntegration.sh` is available in the following directory:

```
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration
```

**Procedure**

Run the `deleteConsoleIntegration.sh` script as follows:

```
sudo `pwd`/deleteConsoleIntegration.sh -default=`pwd`/default.cfg -custom=`pwd`/custom.cfg
```

The **Console Integration** icon disappears from navigation.

**Installing the prerequisite software**

To monitor Performance data from Tivoli Network Manager, install the required software.

**About this task**

You must perform the following tasks:

- Install Tivoli Network Manager core and GUI
- Install the Device Dashboard.
- Activate the SLA agents on Tivoli Network Manager for IP SLA data collection.

**Installing and configuring Tivoli Network Manager**

Since you have installed and configured the base products and components of Netcool Operations Insight that include Tivoli Netcool/OMNIbus, you can proceed to install Network Performance Insight for Performance data.

**Procedure**

1. Perform step 16 to step 20 according to your entitlement from Quick reference to installing section to install Network Manager core and GUI components.

2. Apply the latest supported fix pack.

**Related information**

- Installing Network Manager IP Edition and Netcool Configuration Manager
Activating SLA agent
Activate the SLA agent if you want to discover the SNMP data from IP SLA enabled devices on your system. You can specify the SLA agent for a full discovery or for a partial discovery.

About this task
SLA agent allows discovery of Service Level Agreement supporting data. Currently, retrieves IP SLA data from Cisco, Huawei, and Juniper devices.

Procedure
1. Log in to the portal where is installed.
2. Click the Discovery icon and select Network Discovery Configuration.
3. From the Domain list, select the required domain.
   For example, NCOMS
   **Note:** The Reset button in the Partial Discovery Agents window sets the partial agents to match the settings that are defined in the Full Discovery Agents window.
4. Click one of the following tabs, based on your requirements:
   - **Full Discovery Agents**
     Select agents from this tab to run a full discovery.
   - **Partial Discovery Agents**
     Select agents from this tab to run a partial discovery.
5. The Agents list is displayed, showing all available discovery agents for the selected discovery option.
6. Select the SLA check box.
7. Click the save (✓) icon.

Related information
Configuring network discovery

Installing the
To use the on the Dashboard Application Services Hub console, console integration must be configured. When you install the, this task is automated.

About this task
When you install the that is available for entitled customers, the following tasks are performed automatically:
- Installs the Security Services if it is not available.
  **Note:** If the Security Services are not installed, you might encounter an Authentication Service client error with the following message ID: CTGES0039E
- Console integrations are configured.

Procedure
Install and configure the Device Dashboard.

Results
If the connection is successful, the console content is available in the navigation bar of the Dashboard Application Services Hub through the icon.
Log in with npiadmin and netcool credentials and click **Console Settings > Console Integrations** in the navigation bar to see the integration.

For troubleshooting console integration, see *Missing console integration icon*.

**Setting up communication with**

These settings are required for communicating with

**Procedure**

1. Click **NPI > NOI Core Settings**.
2. Change the default values in the following fields:

   Make sure that you are in the **Configs** tab if you are changing these values after the installation is complete.

   **Note:**
   - Use db2jcc-4.19.49.jar JDBC driver that is available in the /opt/IBM/basecamp/basecamp-connect/libs folder to connect to IBM DB2 database for Tivoli Network Manager. For more information about compatible drivers, see DB2 JDBC Driver Versions and Downloads.
   - Use ojdbc6-11gR2.jar JDBC driver that is available in the /opt/IBM/basecamp/basecamp-connect/libs folder to connect to Oracle database.

   **Table 44: NOI Core Settings > NOI Components > NOI SNMP Collector settings.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>itnm.platform</td>
<td>The database platform for . You can select Oracle or DB2 from the list.</td>
<td>DB2 or ORACLE</td>
</tr>
<tr>
<td>itnm.host</td>
<td>Name of the host where database is installed.</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>itnm.port</td>
<td>The network port to connect to</td>
<td>50000, 1521</td>
</tr>
<tr>
<td>itnm.username</td>
<td>An authorized database user name</td>
<td>db2inst1, ncim</td>
</tr>
<tr>
<td>itnm.password</td>
<td>Password for the authorized database user</td>
<td>db2inst1, ncim</td>
</tr>
<tr>
<td>itnm.database</td>
<td>Database name</td>
<td>NCIM</td>
</tr>
<tr>
<td>itnm.probe.import.interval</td>
<td>Time interval for SNMP Collector to check the system for probe discovery changes.</td>
<td>60</td>
</tr>
<tr>
<td>itnm.kafka.connect.rest.url</td>
<td>Kafka connect REST URL. Specify the hostname where Kafka Connect is installed.</td>
<td>http://&lt;myserver.ibm.com&gt;:8083/connectors</td>
</tr>
</tbody>
</table>

**What to do next**

Enable integration between and . For more information, see *Enabling the integration with Network Performance Insight*. 

184 IBM Network Performance Insight 1.3: Installing and Configuring Network Performance Insight
**Copying the encryption key for SNMP device credentials**

During installation of Network Manager, a 128-bit encryption key is generated and is stored in the following location: `$NCHOME/etc/security/keys/conf.key`.

**About this task**

Copy the `conf.key` file from Tivoli Network Manager to Network Performance Insight. This encryption key is used by Network Performance Insight system to get SNMP device credentials (community strings) from Tivoli Network Manager.

**Procedure**

1. Create the following directories if they do not exist by using the following commands:
   ```
   cd /opt/IBM/npi/npi-itnm-collector/
   mkdir -p resources/itnm/security/keys
   ```

2. Copy the `conf.key` file from `$NCHOME/etc/security/keys` directory to `/opt/IBM/npi/npi-itnm-collector/resources/itnm/security/keys` directory.
   
   Where `$NCHOME` is the Tivoli Network Manager installation directory. For example, `/opt/IBM/netcool/core`.

3. Copy the `conf.key` file on all servers where Tivoli Network Manager Collector is installed.

**Related information**

**Administering system passwords**

**Installing the Technology Packs**

Use this information to install the Technology Pack content that is available within Network Performance Insight installation media. The ready-to-use Technology Pack content includes predefined vendor-specific discovery formulas, collection formulas, metrics, and MIB files that you can use for discovery and polling the devices.

**Before you begin**

Make sure that you have installed, set up your cluster, and configured your Network Performance Insight system successfully.

Make sure that you have Tivoli Network Manager V4.2.0.5 installed.

**About this task**

The following ready-to-use Technology Packs are available from the build after installation in `/opt/IBM/basecamp/basecamp-installer-tools/ootb-packs` directory:

- `network-health-1.0.0.jar`
- `network-health-cisco-1.0.0.jar`
- `network-health-generic-1.0.0.jar`
- `network-health-huawei-1.0.0.jar`
- `network-health-juniper-1.0.0.jar`
- `network-health-extension-1.0.0.jar`

These Technology Packs can be installed in Network Performance Insight system by using the `pack-install.sh` script in `/opt/IBM/basecamp/basecamp-installer-tools/pack-installer`

**Note:**

- Install the packs in this order:
  - `network-health-1.0.0.jar`
  - `network-health-generic-1.0.0.jar`
- Vendor-specific packs
- Do not install the network-health-extension-1.0.0.jar pack if you are polling the following metrics from Tivoli Network Manager to avoid double-polling of these metrics:
  - cpuBusy
  - ifOutDiscards
  - ifInDiscards
  - snmpOutBandwidth
  - snmpInBandwidth
  - ifInErrors
  - ifOutErrors

Each Technology Pack contains the following content:
- Discovery formulas
- Metrics
- Collection formulas
- Vendor-specific and standard MIB files

Procedure
Install the Technology Pack contents by using the following commands:
Run the command on Ambari server and the pack is installed on all Network Performance Insight hosts in your cluster.

```bash
 cd /opt/IBM/basecamp/basecamp-installer-tools/pack-installer
 ./pack-install.sh install ../ootb-packs/<tech_pack>-1.0.0.jar
```

For example:

```bash
 /opt/IBM/basecamp/basecamp-installer-tools/pack-installer/pack-install.sh
 install ../ootb-packs/network-health-cisco-1.0.0.jar
```

At the prompt, provide the following information:
- **NPI Username**
  By default, it is npiadmin.
- **NPI Password**
  By default, it is netcool.
- Accept the default port number.

The Technology Pack is installed and the content within the pack is distributed to vendor-specific directories as follows:

**Discovery formulas**
```
/opt/IBM/npi/npi-itnm-collector/discovery/
```

The discovery directory has all the collection formulas and their related files.

**Formulas**
```
/opt/IBM/npi/npi-itnm-collector/discovery/content
```

Contains all the discovery formula files that are arranged in separate vendor-specific directories from the custom Technology Pack.

**MIB files**
```
/opt/IBM/npi/npi-itnm-collector/discovery/content/mibs
```
Contains all the MIB files that are arranged in separate directories from the custom Technology Pack.

**Metrics**

/opt/IBM/basecamp/basecamp-timeseries/content/metrics

The metrics directory has all the metric files.

**Collection formulas**

/opt/IBM/npi/npi-formula/content/

The content directory has all the collection formulas and their related files.

**Formulas**

/opt/IBM/npi/npi-formula/content/formulas

Contains all the collection formula files from the custom Technology Pack.

**MIB files**

/opt/IBM/npi/npi-formula/content/mibs

Contains all the MIB files that are arranged in separate directories from the custom Technology Pack.

**Bindings**

/opt/IBM/npi/npi-formula/content/bindings

Contains all the MIB object class files that are created when the polling is run. Class files are generated by the Formula Service during network polling.

**What to do next**

Check the log files that are available in /opt/IBM/basecamp/basecamp-installer-tools/pack-installer/logs. When installation of the pack is successful, you might find the output as follows in the log file:

```
Checking dependencies for pack network-health-juniper-1.0.0.jar
Fetch NPI from Ambari
Found NPI in the <myserver.ibm.com>
Pushing pack file to the <myserver.ibm.com>
Starting network-health-juniper-1.0.0.jar installation process to <myserver.ibm.com>
<myserver.ibm.com> completed
Script completed
```

**Viewing the installed Technology Pack details**

The Pack Details page gives all the information related to the Technology Packs that are installed in your information Network Performance Insight system. This information is retrieved from the CFG.PACK_DETAILS table.

**About this task**

This page gives you the following information related to the installed Technology Packs:

- Technology Pack name
- Technology Pack version
- Timestamp
- Tool version
- Content that includes all the discovery formulas, collection formulas, properties, and metrics within the Technology Pack.
Procedure

1. Click **Console Integrations** in the navigation bar, and select **Pack Details** under **System Configuration**.
   
   You can see the list of built-in Technology pack and other custom Technology Packs that you have installed.

2. Click the **Filter** icon and type an item name or ID in the **Filter by <keyword>** field.

3. Click the **Refresh** icon to refresh the list of items.

**Installing and setting up Remote Flow Collector**

You can optionally install the Flow Collector Service on a remote host as a cluster singleton to keep the collector closer to your data center.

**Before you begin**

Make sure that the server where you are installing the Remote Flow Collector Service has connection to RPM repository in Ambari server host.

**Procedure**

1. Copy the `<DIST_DIR>/NPI_1.3.0.0/bin/installRemoteFlowCollector.sh` file from Ambari server to the host where you want to install Remote Flow Collector.

2. Run the `installRemoteFlowCollector.sh` script as root user as follows:

   ```
   ./installRemoteFlowCollector.sh <yum-repo-server> <yum-repo-port>
   ```

   Where:
   
   - `<yum-repo-server>` is the server where the Ambari server is installed.
   - `<yum-repo-port>` is the HTTPD port 9091 that is used by Ambari server for components installation in the cluster.

   The following components are installed:
   
   - Remote Flow Collector Service
   - JRE
   - Kafka
   - Zookeeper

   Zookeeper server and Kafka are set up in the `/usr/iop/current` folder.

3. Set up the connection between the Flow Collector and Remote Flow Collector through Ambari by using the following steps:

   a) Open a browser and access the Ambari server dashboard.

   Use the following default URL:

   ```
   http://<myserver.ibm.com>:8080
   ```

   **Note:** You can use the fully qualified domain name (FQDN) or the IP address of the server.

   The default user name is admin, and the default password is admin.

   b) Click **Services > NPI > Configs > Advanced**.

   c) Expand the **Advanced npi-env** pane and add the following lines in **npi-env template** text area and provide the list of servers where Kafka services are available where Remote Flow Collectors are installed:

   ```
   collector.flow.remote.kafkaBroker = ["<kafka1>:9092", "<kafka2>:9092"]
   ```
Where:

- `kafka1` and `kafka2` are the host names of the servers that have the Kafka Service running along with remote Flow Collector Service. For example, `<myserver.ibm.com>`.

**Note:** The ratio between remote and local collectors must be 1:1.

d) Start the services.

4. Optional: To change the port number of the ZooKeeper Service to resolve the port number conflict, perform the following steps:
   a) Update the following properties in `/opt/IBM/npi/npi-remote-flow-collector/conf/application.conf` file:

   ```
   main.zk-url = "localhost:<new_port_number>"
   messaging.kafka.zk-connect = "localhost:<new_port_number>"
   ```

   b) Update the following properties in `/etc/kafka/conf/server.properties` file:

   ```
   zookeeper.connect=localhost:<new_port_number>
   ```

5. Start the following services:

   - Zookeeper
   - Kafka
   - Remote Flow Collector

6. Optional: To change the port numbers for UDP or SCTP protocols, update the following properties in `/opt/IBM/npi/npi-remote-flow-collector/conf/application.conf`.

   ```
   collector.flow.udp.ports = <new_port_number>
   collector.flow.sctp.ports = <new_port_number>
   ```

7. Start the following services in sequence by using the following command:
   a. Start Zookeeper Service

   ```
   sudo /usr/hdp/current/zookeeper-server/bin/zkServer.sh start
   ```

   b. Start Kafka Service

   ```
   sudo /usr/hdp/current/kafka-broker/bin/kafka start
   ```

   c. Start Remote Flow Collector

   ```
   sudo systemctl start npi-remote-flow-collector
   ```

**Results**

The Remote Flow Collector is available with the following default configurations in `/opt/IBM/npi/npi-remote-flow-collector/conf/application.conf` file:

```
collector.flow.udp.ports = [4379]
collector.flow.sctp.ports = [4381]
main.zk-url = "localhost:2181"
messaging.kafka.broker-list = "localhost:9092"
messaging.kafka.zk-connect = "localhost:2181"
```

**Note:** To restart the Remote Flow Collector Service, see *Controlling remote Flow Collector Service* in .

Check the log files for the collector in `npi-remote-flow-collector/logs` directory.

Check the log files for Zookeeper and Kafka in the following locations:

- `/var/log/zookeeper`
- `/var/log/kafka`
Installing and setting up Remote SNMP Collector
You can optionally install the SNMP Collector on a separate node to enhance the collection of SNMP metrics. You can set up to collect SNMP metrics alone and can be targeted to collect 100 million records per hour.

Before you begin
Compress the following microservices from any of the nodes in your cluster:

- `/opt/IBM/npi/npi-snmp-collector`
- `/opt/IBM/npi/npi-formula`
- `/opt/IBM/basecamp/basecamp-jre`

Use the following commands to create the compressed files for these microservices:

```
cd /opt/IBM/npi
  tar -cvf <npi.tar> npi-snmp-collector npi-formula

cd /opt/IBM/basecamp
  tar -cvf <basecamp.tar> basecamp-jre
```

Procedure

1. On a separate server where you want to install the SNMP Collector as cluster singleton, copy the following archived files:
   - `<npi.tar>`
   - `<basecamp.tar>`

2. Extract the archived files by using the following commands:

```
tar -xvf <npi.tar>
tar -xvf <basecamp.tar>
```

3. Edit the `application.conf` files in both `npi-snmp-collector` microservice as follows:

   ```
cd /opt/IBM/npi/npi-snmp-collector/conf
vi application.conf
```

Update the following lines with the host name of any node in your cluster:

**Note:** You can use the fully qualified domain name (FQDN) or the IP address of the server.

```
ams.collector.endpoint.hostname = "<npi_node_server>",
ams.collector.host = "<npi_node_server>",
ams.collector.port = 6188,
main.zk-url = "<npi_node_server>".
messaging.kafka.broker-list = "<npi_node_server>:9092",
messaging.kafka.zk-connect = "<npi_node_server>:2182",
storage.jdbc-service = "<npi_node_server>:13081",
storage.schema-registry.urls = "http://<npi_node_server>:8093",
storage.uri = "hdfs://<npi_node_server>:8020/npi/",
timeseries-service.hosts = ["<npi_node_server>"]
timeseries-service.port = 31081
```

Set SNMP scoping as follows:

```
snmp.consumer-group.suffix = "<local_server>"
snmp.npi.topic.data = "npi.snmp.poll.data-<local_server>"
snmp.npi.topic.definitions = "npi.snmp.poll.definitions-<local_server>"
```

Where `<local_server>` is the IP address of the fully qualified domain name (FQDN) of the server where SNMP Collector is installed.
4. Edit the application.conf files in both npi-formula microservice as follows:

```
cd /opt/IBM/npi/npi-formula/conf
vi application.conf
```

Update the following lines with the host name of any node in your cluster:

**Note:** You can use the fully qualified domain name (FQDN) or the IP address of the server.

```
ams.collector.endpoint.hostname = "<npi_node_server>"
ams.collector.host = "<npi_node_server>"
ams.collector.port = 6188
main.zk-url = "<npi_node_server>:2182"
messaging.kafka.broker-list = "<npi_node_server>:6667"
messaging.kafka.zk-connect = "<npi_node_server>:2182"
storage.jdbc-service = "<npi_node_server>:13081"
storage.schema-registry.urls = "http://<npi_node_server>:8093"
storage.uri = "hdfs://<npi_node_server>:8020/npi/"
timeseries-service.hosts = [ "<npi_node_server>" ]
timeseries-service.port = 31081
```

Set SNMP scoping as follows:

```
formula.entity-scope = "True"
ssnp.consumer-group.suffix = "<local_server>"
ssnp.npi.topic.data = "npi.snmp.poll.data-<local_server>"
ssnp.npi.topic.definitions = "npi.snmp.poll.definitions-<local_server>"
```

Where `<local_server>` is the IP address of the fully qualified domain name (FQDN) of the server where SNMP Collector is installed.

5. Start the microservices with the following commands:

```
nohup bin/npi-snmp-collector &
nohup bin/npi-formula &
```

## Configuring

You can configure IBM Network Performance Insight, Version 1.3 and its integration services through user interface console and command line interface. You can also administer and manage application security and single sign-on from Dashboard Application Services Hub portal.

## About this task

Most of the configurations are performed through web-based UI on Ambari server. For Network Performance Insight to be fully functional and accessible on Jazz for Service Management, you must perform the following configurations:

- Configure Network Performance Insight system.
- Configure the required Ambari services and Network Performance Insight services from Ambari web interface.
- Configure integration with Tivoli Netcool/OMNIbus.
- Configure integration with Tivoli Network Manager.
Configuring Entity thresholds
A threshold is a value that is compared against a metric to determine whether the metric violates a specific constraint. Entity thresholds provide a mechanism for identifying anomalies in performance metrics that is polled from Network Performance Insight and Cacti.

About this task
Events can be created when a performance metric exceeds a certain user-defined value. For example, when the response time for a monitored service is too high, or when bandwidth utilization exceeds a certain amount.

The threshold violations and their values are user-defined and not dynamically generated. You can configure entity thresholds for each of the performance metrics that are collected and stored in Network Performance Insight database.

Important: Entity Threshold configuration is required in the following installation scenarios:

- For the metrics collected by Network Performance Insight in “Scenario 1 - NetFlow data and performance data from Network Performance Insight” on page 11.
  
  Note: To configure thresholds for standard SNMP metrics that is collected by Tivoli Network Manager, see Defining anomaly thresholds.

- For all the performance metrics collected by “Scenario 2 - NetFlow data and Performance data from Cacti” on page 71.

Procedure

1. Click Console Integrations in the navigation bar and select Entity Thresholds under System Configuration.
   
   You can see the Entity Thresholds table.
2. Select the threshold that you want to edit.
3. Click the Edit icon.

   The Edit Entity Threshold window displays the configuration details.

4. Modify the settings for the threshold as needed.
   
   a) Select the limit type from the Limit Type list to Over, Under, or Band.

   Over
   
   Detect violations when the metric value exceeds the set threshold value.

   Under
   
   Detect violations when the metric value falls short of the set threshold value.

   Band
   
   Detect violations the metric value goes outside a range (or band) between two set threshold values.

   b) Enter a value in the Upper Limit field for the metric to trigger a threshold violation.

   c) Enter a value in the Lower Limit field for the metric to trigger a threshold violation.

   d) Enter the number of events for triggering the threshold in the Consecutive Occurrences field.

   e) Select the Enabled check box to enable a threshold on the interface.

   f) Click Ok to save the modification.

   Note: When the threshold limit is violated, it displays the severity as Critical.

   For more information, see Threshold violation in IBM Network Performance Insight: Product Overview

5. You can perform the following tasks in the Actions column:
   
   a) Click Edit to edit or configure the selected threshold.
b) Click **Enable** or **Disable** to enable or disable a metric to detect its threshold violation states.

**Results**

Any metric that is violating the configured threshold value is reported in the Event Viewer.

**What to do next**

You must repeat the same process to enable and configure thresholds for every metric as needed.

**Related tasks**

“Configuring Flow thresholds” on page 67

Thresholds provide a mechanism for identifying anomalies in flow and metric data that is polled from Tivoli Network Manager. Threshold is a metric value that is compared against a value to determine whether an interface violated a specific constraint. The threshold violations and their values are user-defined and not dynamically generated. These threshold values are defined per interface in each direction.

**Configuring the metric polling interval**

Network polling depends on the polling formulas and metrics that are derived from the Technology Pack content, polling interval that can be configured on the **Polling Configuration** page, and polling scope.

**About this task**

Polling interval defines the frequency of polling and it can affect the polling performance. List of resource types and their resources are populated on this page from Inventory schema tables based on the available Technology Pack content.

**Procedure**

1. Click **Console Integrations** in the navigation bar and select **Polling Configuration** under **System Configuration**.

   You can see the following tabs:

   • **Resource Config**
     Contains a list of all the resource types in the installed Technology Packs content and their polling intervals.

   • **Entity Config**
     Contains a list of all the resources in the installed Technology Packs content and their polling intervals. You can also add more resources and set the polling interval.

2. Click the **Resource Config** tab.

3. Select a resource type from the table and click the **Edit** button.

4. Specify the required polling interval for the resource type and click **Ok**.

   The default polling interval is 300 seconds.

**Important:**

• The polling interval for the resource type **Probe** cannot be configured from this page. Set the polling interval for probe on the device itself.

• If you set polling interval to zero for a resource type, then polling from the resources for that resource type is stopped.

5. Click **Entity Config** tab.

6. Select a resource and click the **Edit** button.

7. Or, click **Edit** in the **Actions** column.
8. Specify the required polling interval for the resource and click Ok.

   Resource interval setting from the Entity Config page takes precedence over the resource type setting on the Resource Config page.
9. Click Clear in the Actions column to clear the polling interval setting on the selected resource.

### Configuring resource types
Configure the resource types for discovery.

### About this task
All the existing resource types from the installed Technology Pack content are populated on this page. You can also add new resource type names.

### Procedure

1. Click Console Integrations in the navigation bar and select Resource Type under System Configuration.
   
   You can see a table containing all the Resource types that are available in the technology pack content in your environment.

   **Add new resource type and its details.**

2. Click New icon and enter the following details:
   - **Name**: Name of the resource type to be discovered.
3. Click Ok.

   **Delete an existing entry.**

4. Select an entry from the table and click the Delete button icon to delete an entry that is not needed.

---

**Installing and uninstalling Interim Fix1**

You can apply the Interim Fix1 to Network Performance Insight and uninstall to the previous version if required.

### About this task
Interim Fix1 is applicable to 1.3 only and includes the following fixes or enhancements:

- To support the integration with IBM Operations Analytics - Predictive Insights.
- To support Kafka version 0.11.0.2 or 0.11.0.3 that is required for integration with Predictive Insights.

  **Note:** The Kafka version that is supported by Network Performance Insight is 0.10.1.

- To improve the performance of Timeseries Exporter Service to handle large timeseries data efficiently.

The following microservices are updated to handle these fixes:

- Timeseries Exporter

For more information about the Timeseries Exporter Service, see *IBM Network Performance Insight: Product Overview.*
**Applying the Interim Fix1**

Keep your Network Performance Insight environment that is running at the latest fix level to ensure problem-free operation and also to get enhancements and new functionality.

**Before you begin**

If you have already installed the Exporter Service, follow these steps to:

- Stop the Exporter Service on all nodes in your cluster with the following steps:
  1. Open a browser and access the Ambari server dashboard.
     - Use the following default URL:
       `http://<myserver.ibm.com>:8080`
       - The default user name is `admin`, and the default password is `admin`.
  2. Click **Services > NPI** on each host in your cluster.
  3. Click **Timeseries Exporters** from the **Summary** tab.
  4. Click each host in your cluster and stop the Timeseries Exporter Service.

- Ensure that Network Performance Insight V1.3 is up and running and is working correctly.

**Procedure**

1. Obtain the interim fix `1.3.0.0-TIV-NPI-IF0001.tgz` from IBM Fix Central and save it to a location of your choice.
   - For example, `/opt/IBM/Installers/NPI` that is referred to as `<DIST_DIR>`.
2. Extract the `1.3.0.0-TIV-NPI-IF0001.tgz` file by using the following command:
   ```bash
tar -zxvf 1.3.0.0-TIV-NPI-IF0001.tgz
   ```
   You can see the following directory structure:
   - basecamp-exporter/
     - README
     - basecamp-exporter-1.3.0.1-<build_signature>.noarch.rpm
     - bin
       - install.sh
       - npiConf.py
       - timeseries.py
       - metainfo.xml
3. Run the `install.sh` script on the Ambari server host by using the following command:
   ```bash
   # bin/install.sh
   ```

**What to do next**

- (Optional) If the Exporter Service is not installed with your Network Performance Insight 1.3, add the service on all hosts in your cluster with the following steps:
  1. Open a browser and access the Ambari server dashboard.
     - Use the following default URL:
       `http://<myserver.ibm.com>:8080`
       - The default user name is `admin`, and the default password is `admin`.
  2. Click Hosts and select a host in your cluster.
3. Click **Add** and select **Timeseries Exporters** Service from the list from the **Summary** tab.

- Configure the Exporter Service. For more information, see *Integrating with IBM Operations Analytics - Predictive Insights*.

### Uninstalling the Exporter Service

Follow these steps to uninstall the Exporter Service.

**Procedure**

1. Stop the Exporter Service from Ambari.
2. Run the following command on all the hosts in your cluster:

   ```
   yum erase -y basecamp-exporter.noarch
   ```

   The Exporter Service is deleted from your installation environment.

**Related tasks**

“Installing and uninstalling Interim Fix1” on page 194

You can apply the Interim Fix1 to Network Performance Insight and uninstall to the previous version if required.

### Installing and uninstalling Interim Fix2

Use this information to apply the Interim Fix2 to your existing Network Performance Insight 1.3 environment.

**About this task**

Interim Fix2 is applicable to 1.3 only and includes the following fixes or enhancements:

- Fix the failures in cluster deployment during the installation of Network Performance Insight.
  
  **Note:** This fix is applicable only in fresh installation scenario.

- Fix the failure in obtaining data by the UI Services. Whenever the Storage Service is restarted, the UI Service is found to be stopped automatically.

- Increase the efficiency of the Storage Service that might fail after 20 -22 hours.

- Enhance the functionality of the Timeseries Service.

### Applying the Interim Fix2

Keep your Network Performance Insight environment that is running at the latest fix level to ensure problem-free operation and also to get enhancements and new functionality.

**Procedure**

1. Obtain the interim fix `1.3.0.0-TIV-NPI-IF0002.tgz` from IBM Fix Central and save it to a location of your choice.

   For example, `/opt/IBM/Installers/NPI` that is referred to as `<DIST_DIR>`.

2. As `root` user, extract the `1.3.0.0-TIV-NPI-IF0002.tgz` file on the Ambari server host by using the following command:

   ```
   tar -zxvf 1.3.0.0-TIV-NPI-IF0002.tgz
   ```

   You can see the following file structure:
3. Run the `main.sh` script as follows:

**Important:** If your Network Performance Insight 1.3 is up and running correctly, skip step 3 through 4.

```bash
cd <DIST_DIR>/1.3.0.0-TIV-NPI-IF0002
./main.sh -npi_ga=<DIST_DIR>
```

Where, `<DIST_DIR>` is the location where Network Performance Insight V 1.3.0.0 media is extracted. For example, `<DIST_DIR>`, which can be `/INSTALLERS/NPI`.

The following tasks are performed after the script is run:

- All the script files and libraries are copied to the `<DIST_DIR>` directory.

4. Run the `install.sh` script on the Ambari server host by using the following command:

```bash
cd <DIST_DIR>/NPI_1.3.0.0/bin
./install.sh <DIST_DIR>
```

a) Provide the number of hosts in your cluster when prompted.

```bash
Enter the number of hosts that will be a part of cluster including ambari host
2
```

b) Provide the hostname of all the Network Performance Insight hosts in your cluster when prompted.
Enter the hostname that will be part of cluster myserver1.ibm.com
INFO: Checking prerequisites on myserver1.ibm.com
Executing prerequisite checker...
The log file after running the prerequisite checker can be found in
the following location: /tmp/prereq_check_201901031209_myserver1.ibm.com.log.
WARNING: Disk space available is below recommended 80GB: 76G
WARNING: Total memory is below recommended 24GB: 7
WARNING: Network Time Protocol (NTP) is not installed.
This is required to synchronize the clocks of all servers in the cluster
Please check the WARNINGS before proceeding.
The log file is at myserver1.ibm.com:/tmp
Do you want to continue(y/n)

y

Enter the hostname that will be part of cluster myserver2.ibm.com
INFO: Checking prerequisites on myserver2.ibm.com
Executing prerequisite checker...
The log file after running the prerequisite checker can be
found in the following location:
WARNING: Total memory is below recommended 24GB: 15
WARNING: Network Time Protocol (NTP) is not installed.
This is required to synchronize the clocks of all servers in the cluster
Please check the WARNINGS before proceeding.
The log file is at myserver2.ibm.com:/tmp
Do you want to continue(y/n)

y

The following tasks are performed after the script is run:

• The prereq_check.sh script is run on all the Network Performance Insight hosts in your cluster.
• If the prerequisites are met, the script installs the 1.3.0.0 software.

For more information on install and configure, see Chapter 2, “Installing and configuring,” on page 9
Network Performance Insight 1.3.

5. Run the following command after the installation and cluster deployment are successful:

   cd <DIST_DIR>/1.3.0.0-TIV-NPI-IF0002
   # ./tss_ds.sh

   The following tasks are performed after the script is run:

• Overwrites timeseriesDatasource script that is available in /opt/IBM/basecamp/basecamp-
timeseries/bin.
• Overwrites NetworkTrafficOverview.json file that is available in /opt/IBM/basecamp/
basicamp-ui/resources/dashboards/json.

Related tasks
“Preparing to run the prerequisite scanner” on page 16
In addition to Network Performance Insight-specific tasks, complete these common tasks before you
start an installation. Network Performance Insight installation script calls the prerequisite scanner that
checks if your environment meets these requirements during installation.

Postinstallation tasks

Procedure
1. Restart the Timeseries Service on each host in your cluster.
   a) Open a browser and access the Ambari server dashboard.
Use the following default URL:
http://<myserver.ibm.com>:8080

The default user name is admin, and the default password is admin.

b) Click Services > NPI on each host in your cluster.
c) Click Timeseries (s) from the Summary tab.
d) Click each host in your cluster and click Restart Timeseries.

2. Restart the UI Service on each host in your cluster.

a) Open a browser and access the Ambari server dashboard.
   Use the following default URL:
   http://<myserver.ibm.com>:8080
   The default user name is admin, and the default password is admin.
b) Click Services > NPI on each host in your cluster.
c) Click UI (s) from the Summary tab.
d) Click each host in your cluster and click Restart UI.

3. Turn on Auto Start for the Timeseries Service.

a) Open a browser and access the Ambari server dashboard.
   Use the following default URL:
   http://<myserver.ibm.com>:8080
   The default user name is admin, and the default password is admin.
b) Click Admin > Service Auto Start.
   The Service Auto Start Configuration page loads.
c) Click NPI from the Service pane.
d) Change the status of the Timeseries component from Disabled to Enabled by clicking on the Timeseries status bar.
   The Timeseries status is changed to Enabled.
e) Click Save to save the configuration.

---

**Installing and uninstalling Interim Fix3**

You can apply the Interim Fix3 to Network Performance Insight and rollback to the previous version if required.

**About this task**

Interim Fix3 is applicable to 1.3 only and includes fixes or enhancements:

- Graceful shutdown of Kairos DB.
- Some vendor-specific discovery formulas are updated to display the data correctly.
- Network Performance Overview by Deviation dashboard is updated to display the data correctly.
- Data is displayed on all Network Performance Insight Dashboards even if the DNS server is not configured for hostname to IP address resolution.
- The Flow History dashboard is updated to display the data correctly.
- Some of the existing collection formulas are updated and some new functions are added in the Technology Packs.
- Some metrics names are changed to be in sync with the formulas in the Technology Packs.
- All performance metrics are visible in the Event Viewer when an event is triggered on them.
• If the device name has some special characters like ",", the Traffic Details dashboard can now be launched from the Event Viewer.
• The Sites configuration page is fixed for filtering the data correctly.
• The metrics REST API is updated not to return device level metrics when parent is excluded.
• In the Interfaces tab in the Device Dashboard, metrics for the selected interface alone are displayed.
• Network Performance Overview and Network Traffic Overview dashboards are updated to display the data correctly based on your site grouping settings on the Sites configuration page.
• Corrected the issue with rediscovery of device performance metrics that overwrite the polling interval configuration.
• The Timeseries Service starts automatically on all Network Performance Insight nodes in your cluster after upgrade from V1.2.3 to V1.3.
• All Network Performance Insight Dashboards display data correctly on all supported locales.
• The Traffic Details dashboard displays data correctly on all supported locales.
• The Edit button is removed from the Resource Type configuration page.
• Discovery is now able to determine the devices with SNMP v3 credentials.
• Fixed the NetFlow parsing issue with samplerId field.

### Applying the Interim Fix3

Keep your Network Performance Insight environment that is running at the latest fix level to ensure problem-free operation and also to get enhancements and new functionality.

#### Before you begin

Stop all the Network Performance Insight services from Ambari by using the following steps:

1. Open a browser and access the Ambari server dashboard.
   
   Use the following default URL:
   
   http://<myserver.ibm.com>:8080
   
   The default user name is admin, and the default password is admin.

2. Stop all the Network Performance Insight services by using the following step:

   Click Services > NPI > Service Actions > Stop.

#### Procedure

1. Obtain the interim fix 1.3.0.0-TIV-NPI-IF0003.tgz from IBM Fix Central and save it to a location of your choice.
   
   For example, /opt/IBM/Installers/NPI that is referred to as <DIST_DIR>.

2. As root user, extract the 1.3.0.0-TIV-NPI-IF0003.tgz file on the Ambari Server host by using the following command:

   ```
   tar -zxvf 1.3.0.0-TIV-NPI-IF0003.tgz
   ```

   You can see the following file structure:

   • 1.3.0.0-TIV-NPI-IF0003/
     
     – README
     – npiConf.py
     – npi-conf.xml
     – basecamp-storage-1.3.0.0-<build_signature>.noarch.rpm
     – basecamp-timeseries-1.3.0.0-<build_signature>.noarch.rpm
Updating the Technology Packs

Interim Fix3 includes updated collection formulas for MIB-II that are provided in the Technology Pack JAR files.

Before you begin
If you have any customized MIB-II formulas in your environment, manually back up the formulas and put them in the following location:

/opt/IBM/basecamp/basecamp-installer-tools/PACKS/BACKUP
About this task

The following updated Technology Packs are provided with Interim Fix3:

- network-health-1.1.0.jar
- network-health-extension-1.2.0.jar
- network-health-generic-1.1.0.jar

Procedure

1. Run the following command to update the existing Technology Packs with the new ones on Ambari server:

   cd <DIST_DIR>/1.3.0.0-TIV-NPI-IF0003/bin
   ./packs_update.sh

   - The following currently installed Technology Packs are replaced with the new ones on Ambari server node and all Network Performance Insight nodes in your cluster:
     - network-health-1.0.0.jar
     - network-health-extension-1.0.0.jar
     - network-health-generic-1.0.0.jar

   - On Ambari server node, the backup copies of the existing Technology Packs are created and placed in /opt/IBM/basecamp/basecamp-installer-tools/ootb-packs directory. The new versions of the Technology Packs are also placed in the same directory.

   - On the Network Performance Insight node, the backup copies of the existing Technology Packs are created and placed in /opt/IBM/basecamp/basecamp-installer-tools/PACKS/BACKUP directory. The new versions of the Technology Packs are also placed in the same directory.

2. Optional: If you customized the existing formulas or added new formulas and metrics, follow these steps:
   a) Manually, back up the updated content.
   b) Copy the content in their respective new versions of the Technology Packs.
   c) Build the Technology Pack.

   For more information, see Packaging the Technology Pack bundle section in IBM Network Performance Insight: Network Operations.

3. Restart all the Network Performance Insight services from Ambari by using the following steps:
   a) Open a browser and access the Ambari server dashboard.

      The default user name is admin, and the default password is admin.

      Use the following default URL:
      http://<myserver.ibm.com>:8080

   b) Click Services > NPI > Service Actions > Start.

Rolling back the Interim Fix3

Follow these steps to revert to the previous version Network Performance Insight after you apply the Interim Fix3.

Before you begin
Manually, back up all your currently existing Technology Packs.

About this task
After the interim fix is applied, the following services are rolled back to previous versions:
• Storage
• Timeseries
• UI
• Event
• Flow Analytics
• Flow Collector
• Formula
• Tivoli Network Manager Collector
• Threshold

Procedure

1. Stop all the Network Performance Insight services from Ambari by using the following steps:
   a) Open a browser and access the Ambari server dashboard.
      The default user name is admin, and the default password is admin.
      Use the following default URL:
      http://<myserver.ibm.com>:8080
   b) Click Services > NPI > Service Actions > Stop.
2. Run the rollback command on the Ambari server host as follows:
   ```
   cd <DIST_DIR>/1.3.0.0-TIV-NPI-IF0003/bin
   ./fix_rollback.sh
   ```
   The updated microservices are rolled back to V1.3.
3. Restart the Storage Service and UI Service from Ambari by using the following steps:
   a) Open a browser and access the Ambari server dashboard.
      The default user name is admin, and the default password is admin.
      Use the following default URL:
      http://<myserver.ibm.com>:8080
   b) Click Services > NPI > Service Actions > Restart Storages.
   c) Click Services > NPI > Service Actions > Restart UIs.
4. Roll back the Technology Packs to their previous versions by using the following command:
   ```
   cd <DIST_DIR>/1.3.0.0-TIV-NPI-IF0003/bin
   ./packs_rollback.sh
   ```
   All the currently existing Technology Packs are removed.
5. Restart all the Network Performance Insight services from Ambari by using the following steps:
   a) Open a browser and access the Ambari server dashboard.
      The default user name is admin, and the default password is admin.
      Use the following default URL:
      http://<myserver.ibm.com>:8080
   b) Click Services > NPI > Service Actions > Start.
Installing and uninstalling Interim Fix4

You can apply the Interim Fix4 to Network Performance Insight and rollback to the previous version if required.

About this task

Interim Fix4 is applicable to 1.3 only. It includes the following fixes or enhancements:

• Future time stamp is no longer visible in FLOW_METRIC.AGG_STATUS table.
• Cassandra can be started automatically if the Timeseries Service is restarted.
• Timeseries Service work directory and its contents can be moved to a non-default location to free up space.
• Script to create users to access the Network Performance Insight Dashboards from command line.
  For more information about this script, see Creating users to access the Network Performance Insight Dashboards from command line section, in Administering IBM Network Performance Insight
• LDAP authentication is supported to access the dashboards and system configuration UI pages that are available on Jazz for Service Management.
  For more information about the LDAP authentication setup, see Setting up LDAP authentication section in Administering IBM Network Performance Insight
• A new setting http.max-request-size to configure the web request size to Device Dashboard is available.
  For more information about this setting, see “Configuring the setting to handle the web request size in Device Dashboard” on page 209.
• Synchronize the time between the Remote Flow Collector server to its mapped Flow Collector server to get the data in NetFlow dashboards with current time.
  See “Installing and setting up Remote Flow Collector” on page 45.
• If the ZooKeeper Service is added or removed from a node in your initial deployment, the information on the available host names is updated correctly in conf/application.conf file in the UI Service.
• The data display in Network Performance Insight Dashboards with one day aggregated data is faster.
• Tivoli Network Manager Collector Service can discover the devices that do not have an IP address associated with them on Tivoli Network Manager.

Deprecated features after the Interim Fix4 is applied:

• You cannot use the collector.flow.raw-write-all-fields=true to enable additional Flow raw fields collection. For more information about this feature, see “Enabling additional Flow raw fields collection” on page 210.

Applying the Interim Fix4

Keep your Network Performance Insight environment that is running at the latest fix level to ensure problem-free operation and also to get enhancements and new functionality.

Before you begin

Important: You must install Interim Fix3 in your environment before you apply the Interim Fix4.

Stop all the Network Performance Insight services from Ambari by using the following steps:

1. Open a browser and access the Ambari server dashboard.

Use the following default URL:
http://<myserver.ibm.com>:8080

The default user name is admin, and the default password is admin.

2. Stop all the Network Performance Insight services by using the following step:

   Click Services > NPI > Service Actions > Stop.

Procedure

1. Obtain the interim fix 1.3.0.0-TIV-NPI-IF0004.tgz from IBM Fix Central and save it to a location of your choice.

   For example, /opt/IBM/Installers/NPI that is referred to as <DIST_DIR>.

2. As root user, extract the 1.3.0.0-TIV-NPI-IF0004.tgz file on the Ambari Server host by using the following command:

   ```
   tar -zxvf 1.3.0.0-TIV-NPI-IF0004.tgz
   ```

   You can see the following file structure:

   - 1.3.0.0-TIV-NPI-IF0004/
     - bin
       - auto.conf
       - curl_get_all_hosts.sh
       - curl_get_cluster_name.sh
       - curl_get_comp_by_host.sh
       - fix_rollback.sh
       - fix_update.sh
       - functions.sh
       - rollback_service.sh
       - update_service.sh
     - basecamp-timeseries-1.3.0.0-<build_signature>.noarch.rpm
     - basecamp-ui-1.3.0.0-<build_signature>.noarch.rpm
     - npi-flow-analytics-1.3.0.0-<build_signature>.noarch.rpm
     - npi-flow-collector-1.3.0.0-<build_signature>.noarch.rpm
     - npi-remote-flow-collector-1.3.0.0-<build_signature>.noarch.rpm
     - npi-itnm-collector-1.3.0.0-<build_signature>.noarch.rpm
     - kafka.py
     - npiConf.py
     - README

3. Run the fix_update.sh script on the Ambari Server host by using the following command:

   ```
   cd <DIST_DIR>/1.3.0.0-TIV-NPI-IF0004/bin
   ./fix_update.sh
   ```

   Where, <DIST_DIR> is the location where Network Performance Insight V 1.3.0.0 media is extracted. For example, <DIST_DIR>, which can be /opt/IBM/Installers/NPI.

4. Remove the following Kafka topics with the following commands:

   Run in any Network Performance Insight node where Kafka Broker is installed.

   ```
   /usr/hdp/2.6.4.0-91/kafka/bin/kafka-topics.sh --zookeeper <zookeeper_node_fqdn>:2182 --delete --topic npi.flow-collector-mgr
   ```
5. Restart all the services by using the following steps:

   Click Services > NPI > Service Actions > Start.

Optional: Updating the Remote Flow Collector
Use this information if you have Remote Flow Collectors in your deployment.

Procedure
1. Copy the npi-remote-flow-collector-1.3.0.0-<build_signature>.noarch.rpm file to the remote server.
   Make sure that the server where you are installing the Remote Flow Collector Service has connection to RPM repository in Ambari server host.
2. Stop the Remote Flow Collector Service with the following command:
   ```
   sudo systemctl stop npi-remote-flow-collector
   ```
3. Uninstall the Remote Flow Collector with the following command:
   ```
   yum erase npi-remote-flow-collector.noarch
   ```
4. Install the Remote Flow Collector that you copied in step 1 with the following command:
   ```
   yum install npi-remote-flow-collector-1.3.0.0-<build_signature>.noarch.rpm
   ```
5. Start the Remote Flow Collector Service with the following command:
   ```
   sudo systemctl start npi-remote-flow-collector
   ```
6. Repeat these steps on all servers where Remote Flow Collector is installed in your deployment.

Rolling back the Interim Fix4

Follow these steps to revert to the previous version Network Performance Insight after you apply the Interim Fix4.

About this task
After the interim fix is applied, the following services are rolled back to previous versions:

- Timeseries
- UI
- Flow Analytics
- Flow Collector
- Tivoli Network Manager Collector

Procedure
1. Stop all the Network Performance Insight services from Ambari by using the following steps:
   a) Open a browser and access the Ambari server dashboard.
      The default user name is admin, and the default password is admin.
      Use the following default URL:
      http://<myserver.ibm.com>:8080
   b) Click Services > NPI > Service Actions > Stop.
2. Run the rollback command on the Ambari server host as follows:

```bash
cd <DIST_DIR>/1.3.0.0-TIV-NPI-IF0004/bin
./fix_rollback.sh
```

The updated microservices are rolled back to V1.3.

3. Remove the following Kafka topics with the following commands:

Run in any Network Performance Insight node where Kafka Broker is installed.

```bash
/usr/hdp/2.6.4.0-91/kafka/bin/kafka-topics.sh --zookeeper <zookeeper_node_fqdn>:2182 --delete --topic npi.flow-collector-mgr
/usr/hdp/2.6.4.0-91/kafka/bin/kafka-topics.sh --zookeeper <zookeeper_node_fqdn>:2182 --delete --topic snapshot.npi.flow-collector-mgr
```

4. Restart all the Network Performance Insight services from Ambari by using the following steps:

   a) Open a browser and access the Ambari server dashboard.
   
      The default user name is admin, and the default password is admin.
   
      Use the following default URL:
      http://<myserver.ibm.com>:8080
   
   b) Click Services > NPI > Service Actions > Start.

**Optional: Uninstalling Remote Flow Collector**

Follow these steps if you want to uninstall the Remote Flow Collector that is installed from Interim Fix4 and install the Remote Flow Collector from the earlier release.

**About this task**

**Procedure**

1. Stop the Remote Flow Collector Service with the following command:

   ```bash
   sudo systemctl stop npi-remote-flow-collector
   ```

2. Remove the topic with the following command from the Remote Flow Collector node:

   ```bash
   /usr/hdp/2.6.4.0-91/kafka/bin/kafka-topics.sh --zookeeper <zookeeper_node_fqdn>:2181 --delete --topic udp.flow.packet
   ```

3. Uninstall the Remote Flow Collector from Interim Fix4 with the following command:

   ```bash
   yum erase npi-remote-flow-collector.noarch
   ```

4. Install the Remote Flow Collector from V1.3 GA distribution by using the following command:

   ```bash
   yum install npi-remote-flow-collector-1.3.0.0-<build_signature>.noarch.rpm
   ```

5. Start the Remote Flow Collector Service with the following command:

   ```bash
   sudo systemctl start npi-remote-flow-collector
   ```

6. Repeat these steps on all servers where Remote Flow Collector is installed in your deployment.
Chapter 3. Additional configuration settings

Use this information to perform some additional configuration settings in your Network Performance Insight environment. Use these settings as applicable for your specific installation scenario.

Additional configuration settings for some Network Performance Insight services

These tasks are optional and help to configure additional settings for some Network Performance Insight services to improve your system functionality.

**Configuring the setting to handle the web request size in Device Dashboard**

Setting to increase the web requests to Device Dashboard. This setting is required if the number of interfaces is too high and the Device Dashboard might fail to load.

**Procedure**

1. Open a browser and access the Ambari server dashboard.
   
   Use the following default URL:
   
   http://<myserver.ibm.com>:8080
   
   The default user name is admin, and the default password is admin.

2. Click Services > NPI > Configs > Advanced.

3. Expand the Advanced npi-env pane and add the following lines in content text area to increase the max request size for web requests:

   http.max-request-size=32768

   Or

   https.max-request-size=32768

4. Click Save to save the configuration.

5. Restart the Timeseries Service by using the following commands:

   a) Click Services > NPI.

   b) Click Service Actions > Restart Timeseriess.

**Moving the Timeseries Service work directory to a non-default location**

The Timeseries Service might grow too large as it starts collecting and storing more data and you might find it useful to move the /opt/ibm/basecamp/basecamp-timeseries/work directory from its default location to create more space for the database.

**About this task**

By default, all microservices have the directory stack as follows:
Follow these steps to move the /opt/ibm/basecamp/basecamp-timeseries/work directory to a non-default location:

**Procedure**

1. Create the directory to which you want to move the /opt/ibm/basecamp/basecamp-timeseries directory as follows:
   ```
   mkdir /opt/basecamp-timeseries
   ```

2. Change the owner of the directory to netcool user and group as follows:
   ```
   chown netcool:netcool /opt/basecamp-timeseries
   ```

3. Open a browser and access the Ambari server dashboard. Use the following default URL:
   ```
   http://<myserver.ibm.com>:8080
   ```
   The default user name is admin, and the default password is admin.

4. Click **Services > NPI > Configs > Advanced**.

5. Expand the **Advanced npi-env** pane and add the following lines in **content** text area to move the work directory of the Timeseries Service to a different location:
   ```
   timeseries.work.dir="/opt/basecamp-timeseries"
   ```

6. Click **Save** to save the configuration.

7. Optional: Move the following folders to the new /opt/basecamp-timeseries/work directory:
   ```
   • /opt/IBM/basecamp/basecamp-timeseries/work/cassandra
   • /opt/IBM/basecamp/basecamp-timeseries/work/kairos_cache
   • /opt/IBM/basecamp/basecamp-timeseries/work/queue
   ```

8. Restart the Timeseries Service by using the following commands:
   a) Click **Services > NPI**.
   b) Click **Service Actions > Restart Timeseries**.

**Enabling additional Flow raw fields collection**

User-configurable Flow raw fields helps in optimizing the disk space. Due to high volume of Flow data that is collected and stored in database, this option helps in saving the disk space and CPU utilization during aggregation.

**About this task**

In a typical installation of Network Performance Insight, it stores specific predefined set of Flow fields in the database. If you want to store all the Flow fields from the Flow-enabled devices, follow these tasks:
**Important:** All the other non-default Flow fields are stored in Hadoop file system and can be read by using an Apache Parquet Reader.

For more information, see *Default normalized flow record fields in Network Performance Insight* section in *IBM Network Performance Insight: Product Overview."

**Note:** You cannot use this setting is deprecated with Network Performance Insight V1.3.0, Interim Fix4.

**Procedure**

1. Log in to Ambari server dashboard.
   
   Use the following default URL: http://<myserver.ibm.com>:8080
   
   The default user name is admin, and the default password is admin.

2. Click **Services > NPI > Configs > Advanced**.

3. Expand the **Advanced npi-env** pane and add the following lines in **content** text area to enable the storage of all the available Flow RAW fields:

   ```
   collector.flow.raw-write-all-fields =true
   ```

4. Click **Save** to save the configuration.

5. Restart the Flow Collector Service as follows:
   
   a) Click **Services > NPI**.
   
   b) Click **Service Actions > Restart Flow Collectors**.

**Configuring the number of interfaces**

IBM Network Performance Insight does not support automatic load-balancing.

You need to manually configure the exporter in your network to support load-balancing.

Typically, Network Performance Insight supports 1000 interfaces per collector. It is recommended that in a multiple-node environment, you configure the exporters to collect not more than 1000 interfaces per collector for processing.

To configure the number interfaces, follow these steps:

- Configure your exporter to send not more than 1000 interfaces per collector for processing.

  See *System requirements* in *Installing and Configuring IBM Network Performance Insight*.

- Configure the `collector.flow.max-interfaces` setting according to your total number of interfaces that are handled by your network exporters.

Consider the following example, which shows few exporters that are configured to collectors with the following number of interfaces:

- Exporter 1 with 500 interfaces that is configured to Collector 1
- Exporter 2 with 500 interfaces that is configured to Collector 2
- Exporter 3 with 1000 interfaces that is configured to Collector 3

Set the `collector.flow.max-interfaces` according to your exporters configuration. For this example, set the `collector.flow.max-interfaces` to 2000.

**Note:** In this example, it does not take the traffic load into consideration.

For more information about this setting, see *Configuring the Flow Collector Service* in *Installing and Configuring IBM Network Performance Insight."

**CAUTION:** Configuring more than 1000 interfaces for a collector might cause performance issues.
If your exporter is configured to have more than 1000 interfaces in your Network Performance Insight cluster, contact IBM Professional Services for assistance.

**Blacklisting exporter from Remote Flow Collector**

Use this information on how to blacklist exporters from a Remote Flow Collector on Network Performance Insight.

**About this task**

**Procedure**

1. Log in to the Remote Flow Collector server as root user.
2. Open the application.conf file in edit mode, by using the following command:

   ```
   vi /opt/IBM/npi/npi-remote-flow-collector/conf/application.conf
   ```

3. Add the following line to blacklist an exporter from the Remote Flow Collector:

   ```
   collector.flow.exporter.blacklist=["ipAddress1"]
   ```

   For example:

   ```
   collector.flow.exporter.blacklist=["10.55.239.250"]
   ```

4. Stop the following services in sequence by using the following command:
   a. Stop Remote Flow Collector
      ```
      sudo systemctl stop npi-remote-flow-collector
      ```
   b. Stop Kafka Service
      ```
      sudo /usr/hdp/current/kafka-broker/bin/kafka stop
      ```
   c. Stop Zookeeper Service
      ```
      sudo /usr/hdp/current/zookeeper-server/bin/zkServer.sh stop
      ```

5. Start the following services in sequence by using the following command:
   a. Start Zookeeper Service
      ```
      sudo /usr/hdp/current/zookeeper-server/bin/zkServer.sh start
      ```
   b. Start Kafka Service
      ```
      sudo /usr/hdp/current/kafka-broker/bin/kafka start
      ```
   c. Start Remote Flow Collector
      ```
      sudo systemctl start npi-remote-flow-collector
      ```

**Configuring logging**

The default logging level can be set from Ambari server web user interface.

**Procedure**

1. Open a browser and access the Ambari server dashboard.

   Use the following default URL:
   ```
   http://<myserver.ibm.com>:8080
   ```
   The default user name is admin, and the default password is admin.

2. Click **Services > NPI > Configs > Advanced.**
3. Expand the **Advanced npi-env** pane and add the following lines in **content** text area to configure the log level for the error messages that are logged in various log files:

```java
logging.level = {DEBUG | INFO | WARN | ERROR | ALL | OFF}
```

If you do not set any values, the default logging level is INFO. After you restart the Network Performance Insight server, the logging level that you have entered becomes the default logging level. If you set the logging level as OFF, the logging is disabled.

<table>
<thead>
<tr>
<th>Logging level</th>
<th>DEBUG</th>
<th>INFO</th>
<th>WARN</th>
<th>ERROR</th>
<th>ALL</th>
<th>OFF</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEBUG</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>INFO</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>WARN</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>ERROR</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>OFF</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

4. To specify the retention period for the historical log files, add the following lines in **npi-env template** text area:

```java
logging.history = nn
```

Where `nn` is an integer value.

*Note:* The default value is 10. A new log file is created everyday and the log file that is created on the previous day is renamed to `npi-<mm_dd_yyyy>.log`. This setting determines how many days these log files are maintained in the `<npi_service>/logs` directory.

5. Restart the Network Performance Insight services.

For more information about restarting Network Performance Insight services, see *Controlling the Ambari server and Network Performance Insight node services* in *Administering IBM Network Performance Insight*.

### Configuring retention period for timeseries data

Timeseries data that is stored in Kairos DB is not pre-aggregated. Retention period for timeseries data is set from Ambari.

**About this task**

Typically, you can set the retention period for timeseries data during cluster set up. If you must change the retention period, follow these steps:

*Note:* For all other types of data, you can set the retention periods from **System Configuration** on Dashboard Application Services Hub.

For more information, see *Configuring data retention profiles* in *Installing and Configuring IBM Network Performance Insight*.

**Procedure**

1. Open a browser and access the Ambari server dashboard.

   Use the following default URL:
   ```
   http://<myserver.ibm.com>:8080
   ```

   The default user name is `admin`, and the default password is `admin`.

2. Click **Services > NPI > Configs > NPI Settings.**
3. Specify a value in the `timeseries.data.retention` field. It is the data retention period in days.

4. Restart the Timeseries Service from Ambari.
   - a) Click **Service Actions > Restart Timeseries**.
   - You can see the setting in `/opt/IBM/basecamp/basecamp-timeseries/conf/application.conf` file as:

   ```
   timeseries.data.retention = 2
   ```

5. Verify that the value is updated in `/opt/IBM/basecamp/basecamp-timeseries/3rdParty/kairosdb-1.2.0/conf/kairosdb.properties` in the following parameter:

   ```
   kairosdb.datastore.cassandra.datapoint_ttl=172800
   ```

   172800 is value of two days in seconds.

## Configuring and tuning the IP SLA probes

Network Performance Insight 1.3 is optimized to support 2000 configured probes. If you want to support more number of probes, you can increase the buffer size with these settings from Ambari web UI.

### Procedure

1. Open a browser and access the Ambari server dashboard.
   - Use the following default URL: `http://<myserver.ibm.com>:8080`
   - The default user name is `admin`, and the default password is `admin`.

2. Click **Services > NPI > Configs > Advanced**.

3. Expand the **Advanced npi-env** pane and add the following lines in `content` text area to configure the additional probes.

   ```
   formula.poll-definition-buffer-size = <number_of_probes> * 40
   formula.timeseries-raw-buffer-size= <number_of_probes> * 20
   snmp.poll.data.buffer.size = <number_of_probes> * 20
   ```

   Where `<number_of_probes>` is the total number of probes you want to support in your network.

   For example, if you must support 4000 probes, the settings are as follows:

   **Note:** Ensure that you are aware of the number of probes that you must support additionally in your network.

   ```
   formula.poll-definition-buffer-size = 160000
   formula.timeseries-raw-buffer-size= 80000
   snmp.poll.data.buffer.size = 80000
   ```

   The default value for these settings is 100000. You must use these settings only if you require more than the default value.

4. Restart the Formula Service on all the hosts in your cluster if you change the `formula.poll-definition-buffer-size` and `formula.timeseries-raw-buffer-size` parameters.

   If you change the `snmp.poll.data.buffer.size` parameter, then restart the SNMP Collector Service on all hosts in your cluster.

## Reusing an entity after deletion from Cacti

This configuration setting is applicable only if you have Cacti integration.

### About this task

When you delete or add an entity in Cacti, you might notice that the `inventory.entities` table in Network Performance Insight database is not updated correctly. For example, if you delete or disable an
entity in Cacti, the inventory.entities table shows the state as D for that device or entity. If you add or enable that entity back, the state remains as D. The device is allotted a new ID and the old ID also remains in the table.

You can set the removedEntityGracePeriod parameter that keeps the deleted entity for a week. If the entity is enabled or added again, it is assigned the same ID.

**Procedure**

1. Log in to Ambari server dashboard.
   - Use the following default URL: `http://<myserver.ibm.com>:8080`
   - The default user name is `admin`, and the default password is `admin`.
2. Click **Services > NPI > Configs > Advanced**.
3. Expand the **Advanced npi-env** pane and add the following lines in **content** text area to set the grace period:
   
   ```
   collector.cacti.removed-entity-graceperiod = Time in milliseconds
   ```

   By default, the deleted entity is retained for 7 days in the database.

   This setting allows a grace period for the entity that is in deleted stated and the original ID is assigned to it if it is enabled again on Cacti.
4. Click **Save** to save the configuration.

   This setting is written to `/etc/npi/npi-cacti-collector/application.conf` file.
5. Restart the Network Performance Insight UI Service from Ambari for all hosts in your cluster as follows:
   a) Click **Services > NPI**.
   b) Click **Service Actions > Restart Cacti Collectors**.

**Disabling collection for some metrics in Network Performance Insight**

Starting from V1.3, the Performance Metric OOTB Device Support metrics are polled by Network Performance Insight from the preinstalled Technology Pack content. The other SNMP metrics are polled by Tivoli Network Manager.

**About this task**

Configure the **formula.disabled-metrics** setting on Ambari web interface to control the polling from Network Performance Insight for the metrics that are not needed according to your requirements.

**Procedure**

1. Log in to Ambari server dashboard.
   - Use the following default URL:
     `http://<myserver.ibm.com>:8080`
   - The default user name is `admin`, and the default password is `admin`.
2. Click **Services > NPI > Configs > Advanced**.
3. Expand the **Advanced npi-env** pane and add the following lines in **content** text area to list the metric names that must be disabled from polling by Network Performance Insight:
   
   ```
   formula.disabled-metrics=["<metric_name1>", "<metric_name2>", <metric_name3>]
   ```

   For example:

   ```
   "Network.Inbound.Discards.Count.1"
   ```
Related information
Polling the network in Tivoli Network Manager

Configuring Ambari for non-root access

Many secure environments require restricted access and limit the services that run as the root user. If you need to restrict root access, you must configure the Ambari Server and all the Network Performance Insight nodes to operate without direct root access.

Optional: Configuring Ambari server for non-root access

Perform these steps on the Ambari server host.

Procedure

1. Log in to the Ambari server host as root user.
2. Create a user name by using the following command:

   For example, ambari

   \texttt{useradd ambari}

3. Stop the Ambari server by using the following command:

   \texttt{service ambari-server stop}

4. Run the \texttt{ambari-server setup} command to see the following output and prompts:

   \texttt{ambari-server setup}
   \texttt{Using python /usr/bin/python2}
   \texttt{Setup ambari-server}
   \texttt{Checking SELinux...}
   \texttt{SELinux status is 'disabled'}
   \texttt{Ambari-server daemon is configured to run under user 'root'. Change this setting [y/n] (n)? y}
   \texttt{Enter user account for ambari-server daemon (root):ambari}
   \texttt{Adjusting ambari-server permissions and ownership...}
   \texttt{Checking firewall status... Redirecting to /bin/systemctl status iptables.service}
   \texttt{Checking JDK...}
   \texttt{Do you want to change the current JDK [y/n] (n)?}
   \texttt{Completing setup...}
   \texttt{Configuring database...}
   \texttt{Enter advanced database configuration [y/n] (n)?}
   \texttt{Configuring database...}
   \texttt{Default properties detected. Using built-in database.}
   \texttt{Configuring ambari database...}
   \texttt{Checking PostgreSQL...}
   \texttt{Configuring local database...}
   \texttt{Connecting to local database...done.}
   \texttt{Configuring PostgreSQL...}
   \texttt{Backup for pg_hba found, reconfiguration not required}
   \texttt{Extracting system views...}
   \texttt{......}
   \texttt{Adjusting ambari-server permissions and ownership...}
   \texttt{Ambari Server 'setup' completed successfully.}

5. Start the Ambari server with the following command:

   \texttt{service ambari-server start}
Configuring Network Performance Insight node hosts for non-root access

Perform these steps on all Network Performance Insight node hosts in your cluster.

**Before you begin**

Copy the script `/opt/IBM/basecamp/basecamp-installer-tools/ambari/agent_setup_nonRoot.sh` from Ambari server host to each Ambari agent node in your cluster to a temporary location. For example, `/tmp/agent_setup_nonRoot.sh`.

**Procedure**

1. Log in to an Network Performance Insight node as **root** user.
2. Stop the Network Performance Insight node by using the following command:
   ```
   service ambari-agent stop
   ```
3. Run the `agent_setup_nonRoot.sh` script as follows:
   ```
   /tmp/agent_setup_nonRoot.sh
   ```
   The script performs the following functions:
   - Creates the `ambari` user.
   - Updates the `/etc/sudoers` file to add new sudo permissions for the Ambari non-root user, that is `ambari`.
   - Updates the `/etc/ambari-agent/conf/ambari-agent.ini` to run as user `ambari`.
4. Start the Network Performance Insight node by using the following command:
   ```
   service ambari-agent start
   ```
5. Repeat these steps on all Network Performance Insight node hosts.
Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS"
WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A
PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in
certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically
made to the information herein; these changes will be incorporated in new editions of the publication.
IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this
publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in
any manner serve as an endorsement of those websites. The materials at those websites are not part of
the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without
incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the
exchange of information between independently created programs and other programs (including this
one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

© Copyright IBM Corp. 2015, 2019
Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM’s suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.
Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED,