Note

Before using this information and the product it supports, read the information in “Notices” on page 263.

This edition applies to version 1.2.3.0 of IBM Network Performance Insight and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2015, 2018.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
## Contents

### Introduction .................................................. vii
- Intended audience ........................................ vii
- Network Performance Insight architecture .......... vii
- developerWorks community ............................... xi
- Network Performance Insight technical training ...... xi
- Support information ........................................ xi
- Conventions used in this publication .................. xi
  - Typeface conventions ................................. vi

### 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 Tivoli Network Manager ................. 10
    - Installing ........................................... 10
      - Planning for Network Performance Insight installation ........................................ 10
      - Downloading and extracting the Network Performance Insight software ..................... 10
      - Downloading the IBM Open Platform with Apache Spark and Apache Hadoop .......... 11
      - Gathering required information ................................................................. 12
      - Installing the prerequisite software ....................................................... 13
      - Activating SLA agent ........................................ 14
      - Preparing your environment ........................................ 14
      - Setting SSH passwordless login .................................................. 14
      - Setting Kernel parameters ............................................................... 15
      - Configuring Security-Enhanced Linux (SELinux) to support SCTP protocol .............. 16
      - Preparing to run the prerequisite scanner ........................................... 17
      - Installing Network Performance Insight ........................................... 17
      - Setting up Network Performance Insight cluster ..................................... 19
        - Setting up HDFS Service ........................................ 21
        - Setting up YARN Service ........................................ 22
        - Setting up Zookeeper ........................................ 22
        - Setting up Kafka ........................................... 22
        - Setting up communication with Tivoli Network Manager ................................ 23
        - Setting up Network Performance Insight services ......................... 24
        - Setting up the OMNibus Standard Input probe .................................. 27
        - Disabling the services not required for an installation scenario ..................... 29
        - Setting up integration with Jazz for Service Management ....................... 29
        - Editing the configuration files ........................................ 29
        - Generating the certificate and key-store files ................................... 31
      - Enabling integration with Jazz for Service Management ................................ 31
      - Setting up communication with Jazz for Service Management on Ambari ............ 32
      - Configuring the SSL communication for integration ..................................... 34
      - Installing the Device Dashboard ........................................ 36
      - Installing and setting up Remote Flow Collector ..................................... 37
      - Installing the Performance Metric OOTB Device Support component .................. 39
        - Installing the Performance Metric OOTB Device Support pack .................. 39
        - Running the network discovery for vendor-specific device performance metrics .... 42
        - Setting up a cronjob to update the tables ........................................... 43
        - Enabling the Performance Metric OOTB Device Support poll definitions .......... 44
      - Postinstallation tasks .................................... 45
        - Verifying the installation ............................................... 45
        - Verifying the status of Standard Input probe ..................................... 46
        - Installation directory structure ..................................................... 47
      - Uninstalling Network Performance Insight ........................................ 50
        - Listing working directories ......................................................... 50
        - Uninstalling Ambari agent nodes .................................................. 51
        - Uninstalling Ambari server host ................................................. 52
        - Removing Dashboard Application Services Hub integration ......................... 52
        - Uninstalling Remote Flow Collector ............................................. 53
        - Uninstalling Performance Metric OOTB Device Support component .................. 53
        - Troubleshooting installation .......................................................... 55
      - Configuring .............................................. 55
        - Configuring Network Performance Insight system environment ................... 55
        - Logging in to the Dashboard Application Services Hub portal ....................... 56
        - Configuring Autonomous System ................................................... 57
        - Configuring domain names ......................................................... 58
        - Configuring Flow aggregations ...................................................... 59
        - Configuring Flow interfaces ......................................................... 63
        - Configuring IP Grouping .............................................................. 64
        - Configuring NBAR .................................................. 64
        - Configuring retention profiles ...................................................... 66
        - Configuring Flow thresholds ......................................................... 66
        - Configuring Type of Service ....................................................... 68
      - Configuring integration with Tivoli Netcool/OMNibus .................................. 69
        - Configuring launch-in-context integration with Network Performance Insight .... 69
      - Scenario 2 - NetFlow data and Performance data from Cacti ............................. 71
        - Installing .............................................. 71
        - Planning for Network Performance Insight installation .......................... 72

© Copyright IBM Corp. 2015, 2018
Configuring Network Performance Insight

Uninstalling Network Performance Insight

Installing and setting up Remote Flow Collector

Editing the configuration files

Generating the certificate and keystores

Enabling integration with Jazz for Service Management

Setting up communication with Jazz for Service Management on Ambari

Installing the OMNibus Standard Input probe

Disabling the services not required for an installation scenario

Setting up integration with Jazz for Service Management

Setting up communication with Jazz for Service Management on Ambari

Configuring the SSL communication for integration

Installing and setting up Remote Flow Collector

Verifying the installation

Verifying the status of Standard Input probe

Installation directory structure

Uninstalling Network Performance Insight

Listing working directories

Uninstalling Ambari agent nodes

Uninstalling Ambari server host

Removing Dashboard Application Services

Hub integration

Uninstalling Remote Flow Collector

Uninstalling the security services

Deleting console integration

Troubleshooting installation

Configuring

Configuring Network Performance Insight system environment

Logging in to the Dashboard Application Services Hub portal

Configuring Autonomous System

Configuring Cacti servers

Configuring domain names

Configuring Entity thresholds

Configuring Flow aggregations

Configuring Flow Devices

Configuring Flow interfaces

Configuring IP Grouping

Configuring NBAR

Configuring retention profiles

Configuring Flow thresholds

Configuring Type of Service

Configuring the default entity scope for data visualization on Ambari

Configuring integration with Tivoli Netcool/OMNibus

Configuring launch-in-context integration with Network Performance Insight

Scenario 3 - NetFlow only data

Installing

Planning for Network Performance Insight installation

Downloading and extracting the Network Performance Insight software

Downloading the IBM Open Platform with Apache Spark and Apache Hadoop

Gathering required information

Preparing to run the prerequisite scanner

Installing Network Performance Insight

Setting up Network Performance Insight cluster

Setting up HDFS Service

Setting up YARN Service

Setting up Zookeeper

Setting up Kafka

Setting up Network Performance Insight services

Setting up the OMNibus Standard Input probe

Disabling the services not required for an installation scenario

Setting up integration with Jazz for Service Management

Editing the configuration files

Installing the security services

Creating console integration

Generating the certificate and keystores

Enabling integration with Jazz for Service Management

Setting up communication with Jazz for Service Management on Ambari

Installing the prerequisite software

Preparing your environment

Setting SSH passwordless login

Setting Kernel parameters

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

Preparing to run the prerequisite scanner

Installing Network Performance Insight

Setting up Network Performance Insight cluster

Setting up HDFS Service

Setting up YARN Service

Setting up Zookeeper

Setting up Kafka

Setting up Network Performance Insight services

Setting up the OMNibus Standard Input probe

Disabling the services not required for an installation scenario

Setting up integration with Jazz for Service Management

Editing the configuration files

Installing the security services

Creating console integration

Generating the certificate and keystores

Enabling integration with Jazz for Service Management

Setting up communication with Jazz for Service Management on Ambari

Configuring the SSL communication for integration

Postinstallation tasks
Verifying the installation ........................................ 160
Verifying the status of Standard Input probe .............. 162
Installation directory structure .................................. 163
Uninstalling Network Performance Insight .................. 165
Listing working directories ...................................... 166
Uninstalling Ambari agent nodes ............................... 167
Uninstalling Ambari server host ............................... 167
Removing Dashboard Application Services Hub integration . 168
Uninstalling Remote Flow Collector ............................ 169
Uninstalling the security services ............................. 169
Deleting console integration ...................................... 169
Troubleshooting installation ................................... 170
Configuring .................................................. 170
Configuring Network Performance Insight system environment .................................................. 170
Logging in to the Dashboard Application Services Hub portal .................................................. 171
Configuring Autonomous System .............................. 172
Configuring domain names ...................................... 173
Configuring Flow aggregations .................................. 174
Configuring Flow Devices ...................................... 178
Configuring Flow interfaces .................................... 180
Configuring IP Grouping ....................................... 181
Configuring NBAR ........................................... 182
Configuring retention profiles .................................. 183
Configuring Flow thresholds .................................... 184
Configuring Type of Service .................................... 185
Configuring integration with Tivoli Netcool/OMNiBuss .... 186
Configuring launch-in-context integration with Network Performance Insight .......................... 186
Scenario 4 - Add on Performance data from Tivoli Network Manager to NetFlow only data ........ 189
Installing .................................................. 189
Planning for Network Performance Insight installation ........................................................................... 189
Downloading and extracting the Network Performance Insight software ........................................... 189
Downloading the IBM Open Platform with Apache Spark and Apache Hadoop .......................... 190
Gathering required information ................................ 191
Installing the prerequisite software .............................................. 192
Preparing your environment ..................................... 192
Setting SSH passwordless login ................................ 192
Setting Kernel parameters ...................................... 193
Configuring Security-Enhanced Linux (SELinux) to support SCTP protocol ............................................ 194
Preparing to run the prerequisite scanner ................. 194
Installing Network Performance Insight .................. 195
Setting up Network Performance Insight cluster ........ 197
Setting up HDFS Service ..................................... 199
Setting up YARN Service .................................... 200
Setting up Zookeeper .......................................... 200
Setting up Kafka ............................................ 200
Setting up Network Performance Insight services ........ 201
Setting up the OMNiBuss Standard Input probe ......... 204
Disabling the services not required for an installation scenario .................................................. 206
Setting up integration with Jazz for Service Management .................................................. 206
Editing the configuration files .................................. 206
Installing the security services ................................ 208
Creating console integration .................................... 208
Generating the certificate and keystores .................... 209
Enabling integration with Jazz for Service Management .................................................. 209
Setting up communication with Jazz for Service Management on Ambari .......................... 210
Configuring the SSL communication for integration .................................................. 212
Postinstallation tasks ........................................... 214
Verifying the installation ....................................... 214
Verifying the status of Standard Input probe ...................... 216
Installation directory structure .................................. 216
Integrating with Tivoli Network Manager ................................. 219
Preparing to integrate with Tivoli Network Manager .................................................. 219
Installing the Performance Metric OOTB Device Support component ........................................ 222
Activating SLA agent ......................................... 228
Setting up communication with Tivoli Network Manager .................................................. 228
Copying the encryption key for SNMP device credentials .................................................. 230
Uninstalling Network Performance Insight .................. 230
Listing working directories ...................................... 231
Uninstalling Ambari agent nodes ............................... 232
Uninstalling Ambari server host ............................... 232
Removing Dashboard Application Services Hub integration .................................................. 233
Uninstalling Remote Flow Collector ............................ 233
Uninstalling the security services ............................. 234
Deleting console integration ...................................... 234
Uninstalling Performance Metric OOTB Device Support component ........................................ 235
Troubleshooting installation ................................... 236
Configuring .................................................. 236
Configuring Network Performance Insight system environment .................................................. 237
Logging in to the Dashboard Application Services Hub portal .................................................. 237
Configuring Autonomous System .................................. 238
Configuring domain names ...................................... 239
Configuring Flow aggregations .................................. 240
Configuring Flow Devices ...................................... 244
Configuring Flow interfaces .................................... 246
Configuring IP Grouping ....................................... 247
Configuring NBAR ........................................... 248
Configuring retention profiles .................................. 249
Configuring Flow thresholds .................................... 250
Configuring Type of Service .................................... 251
Configuring integration with Tivoli Netcool/OMNiBuss .... 252
Configuring launch-in-context integration with Network Performance Insight .................. 252
### Chapter 3. Additional configuration settings

Additional configuration settings for some Network Performance Insight services

- Enabling additional Flow raw fields collection ........................................... 257
- Configuring the number of interfaces ......................................................... 258
- Blacklisting exporter from Remote Flow Collector ......................................... 258
- Configuring logging ...................................................................................... 259
- Configuring and tuning the IP SLA probes ................................................... 260
- Reusing an entity after deletion from Cacti .................................................. 261
- Configuring Ambari for non-root access ....................................................... 261
- Configuring Ambari server for non-root access ............................................ 261
- Configuring Ambari agent hosts for non-root access .................................... 262

### Notices

- Trademarks ..................................................................................................... 265
- Terms and conditions for product documentation .......................................... 266
Introduction

Use this information to install and configure IBM® Network Performance Insight® 1.2.3.

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, v1.2.3 integrates with the following components of IBM Netcool Operations Insight 1.4.1.2:
- 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 1.2.3 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 1.2.3 consists of the following microservices:

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

**Entity Metric services**
- Cacti Collector
- Formula Service
- Entity Analytics
- SNMP Collector
- SNMP Discovery
- Tivoli Network Manager Collector
- Threshold

**Flow Metric services**
- Flow Analytics
- Flow Collector
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 V1.2.3 for enhanced functions are described here:

**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

**IBM Open Platform with Apache Spark and Apache Hadoop components**

IBM Open Platform with Apache Spark and Apache Hadoop (IOP) 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 IBM Open Platform with Apache Spark and Apache Hadoop stack.

The features of IOP that are used in Network Performance Insight:

- IBM Open Platform with Apache Spark and Apache Hadoop
- 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:
  - HDFS
Integrated products

Products that are integrated with Network Performance Insight 1.2.3:

**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 network discovery, device polling, including storage of polled SNMP data for reporting and analysis, and topology visualization. In addition, Network Manager can display network events, perform root-cause analysis of network events, and enrich network events with topology and other network data.

**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 V1.2.3, 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](https://www.ibm.com)
- [IBM BigInsights 4.2 documentation](https://www.ibm.com)
- [HDFS Architecture](https://www.ibm.com)
- [Apache Hadoop YARN](https://www.ibm.com)
- [Apache Kafka](https://www.ibm.com)
- [Apache Zookeeper](https://www.ibm.com)
- [IBM Networks for Operations Insight](https://www.ibm.com)
developerWorks community

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

Access the IBM Network Performance Insight community. Use developerWorks 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
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

**Bold monospace**

- Command names, and names of macros and utilities that you can type as commands
- Environment variable names in text
- Keywords
- Parameter names in text: API structure parameters, command parameters and arguments, and configuration parameters
- Process names
- Registry variable names in text
- Script names
Chapter 1. System requirements

Complete set of requirements for IBM Network Performance Insight 1.2.3.

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>30000 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                | 1000 per Flow Collector Service that is running on each Ambari node in your cluster. |
| Network Performance Insight records collected | 20,000,000 records per hour for Tivoli Network Manager               |
|                                               | 22,000,000 records per hour for SNMP data, IP SLA data, and Performance Metric OOTB Support data. |
| 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 260. |
| IP SLA metrics collected                      | 1,800,000 IP SLA metrics per hour for a poll definition of 1 minute   |

Note: If you want to support more IP SLA probes, see “Configuring and tuning the IP SLA probes” on page 260.
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 metrics RAW data = 10 Days</td>
</tr>
<tr>
<td></td>
<td>• Entity metrics 30 minutes aggregated = 30 Days</td>
</tr>
<tr>
<td></td>
<td>• Entity metrics 6 hours aggregated = 30 Days</td>
</tr>
<tr>
<td></td>
<td>• Entity metrics daily aggregated data = 30 Days</td>
</tr>
<tr>
<td></td>
<td>• Entity metric Threshold state data = 90 days</td>
</tr>
</tbody>
</table>

Table 2. Hardware specifications

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

Note: CPU is based on Intel Xeon E5-2640 2.2 GHz model.

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 1.2.3 hardware sizing guidelines, see IBM Network Performance Insight 1.2.2 Sizing Guidelines on the dW 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
- Jazz for Service Management Detailed System Requirements
Software requirements

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

Software requirements for Network Performance Insight.

Table 3. Supported Operating System

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 7.2 64-bit</td>
<td></td>
</tr>
<tr>
<td>RHEL 7.4 64-bit</td>
<td></td>
</tr>
</tbody>
</table>

Note: Enable JavaScript and cookies.

Table 4. Supported web browsers

<table>
<thead>
<tr>
<th>Web browsers</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>11</td>
</tr>
<tr>
<td>Mozilla Firefox ESR</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>52</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Latest version with in 90 days of release</td>
</tr>
</tbody>
</table>

Table 5. Prerequisite software

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jazz for Service Management</td>
<td>1.1.3.0 with Cumulative Patch 4</td>
</tr>
<tr>
<td>IBM Tivoli Netcool/OMNIbus</td>
<td>8.1.0.15</td>
</tr>
<tr>
<td>IBM Tivoli Netcool/OMNIbus Web GUI</td>
<td>8.1.0.12</td>
</tr>
<tr>
<td>IBM Tivoli Network Manager IP Edition</td>
<td>4.2.0.4</td>
</tr>
<tr>
<td></td>
<td>Note: Required only if you are integrating with Tivoli Network Manager.</td>
</tr>
<tr>
<td>Device Dashboard</td>
<td>1.1.0.2</td>
</tr>
<tr>
<td></td>
<td>Note: Required only if you are integrating with Tivoli Network Manager.</td>
</tr>
<tr>
<td>Network Health Dashboard</td>
<td>4.2.0.4</td>
</tr>
<tr>
<td></td>
<td>Note: Required only if you are integrating with Tivoli Network Manager.</td>
</tr>
<tr>
<td>Cacti</td>
<td>V0.8.8 to V1.1.36 for RHEL only</td>
</tr>
<tr>
<td></td>
<td>Note: Required only if you are integrating with Cacti.</td>
</tr>
</tbody>
</table>

Table 6. 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>IBM SDK, Java™ Technology Edition 64-bit</td>
<td>8.0.2.10 (Version 8, Service Refresh 2 Fix Pack 10)</td>
</tr>
</tbody>
</table>
Table 7. 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:
- [System requirements for BigInsights](#)
- [Version 1.4.1.2](#)
- [Supported versions of Web Browsers and mobile OS in DASH](#)

Port requirements for a typical installation

Before you install Network Performance Insight and IBM Open Platform with Apache Spark and Apache Hadoop (IOP) software, open the ports in this table to avoid any conflicts that might exist in your system.

Table 8. Default port numbers for IOP 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>Ambari Metrics</td>
<td>ams</td>
<td>tcp</td>
<td>60200</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>ams</td>
<td>tcp</td>
<td>37266</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>ams</td>
<td>tcp</td>
<td>41824</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>ams</td>
<td>tcp</td>
<td>45884</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>ams</td>
<td>tcp</td>
<td>61181</td>
</tr>
<tr>
<td>Ambari Metrics</td>
<td>ams</td>
<td>tcp</td>
<td>61310</td>
</tr>
<tr>
<td>HDFS</td>
<td>hdfs</td>
<td>tcp</td>
<td>8010</td>
</tr>
<tr>
<td>HDFS</td>
<td>hdfs</td>
<td>tcp</td>
<td>8020</td>
</tr>
<tr>
<td>HDFS</td>
<td>hdfs</td>
<td>tcp</td>
<td>50010</td>
</tr>
<tr>
<td>HDFS</td>
<td>hdfs</td>
<td>tcp</td>
<td>50070</td>
</tr>
<tr>
<td>HDFS</td>
<td>hdfs</td>
<td>tcp</td>
<td>50075</td>
</tr>
<tr>
<td>HDFS</td>
<td>hdfs</td>
<td>tcp</td>
<td>50090</td>
</tr>
<tr>
<td>HDFS</td>
<td>hdfs</td>
<td>tcp</td>
<td>58042</td>
</tr>
<tr>
<td>KAFKA</td>
<td>kafka</td>
<td>tcp</td>
<td>6667</td>
</tr>
<tr>
<td>KAFKA</td>
<td>kafka</td>
<td>tcp</td>
<td>8083</td>
</tr>
<tr>
<td>KAFKA</td>
<td>kafka</td>
<td>tcp</td>
<td>39122</td>
</tr>
<tr>
<td>KAFKA</td>
<td>kafka</td>
<td>tcp</td>
<td>56969</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>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></td>
<td></td>
<td></td>
<td><strong>Note:</strong> 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.</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>
<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 Collector</td>
<td>netcool</td>
<td>tcp</td>
<td>2558</td>
</tr>
<tr>
<td></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>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>Entity Analytics</td>
<td>netcool</td>
<td>tcp</td>
<td>2561</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>21081</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>21443</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>21910</td>
</tr>
</tbody>
</table>
Table 8. Default port numbers for IOP 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>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>Storage</td>
<td>netcool</td>
<td>tcp</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>2552</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8081</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>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>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>9092</td>
</tr>
<tr>
<td>Kafka Schema Registry</td>
<td>kafka</td>
<td>tcp</td>
<td>8093</td>
</tr>
<tr>
<td>Ambari Server</td>
<td>root</td>
<td>tcp</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>9091</td>
</tr>
</tbody>
</table>
Table 8. Default port numbers for IOP 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</td>
<td>yarn</td>
<td>tcp</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>
<tr>
<td>YARN</td>
<td>yarn</td>
<td>tcp</td>
<td>46100 - 46600</td>
</tr>
<tr>
<td>For Spark Executors</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.

**Related information:**

[IBM BigInsights - Get ready to install](#)
Chapter 2. Installing and configuring

Installation of IBM Network Performance Insight, Version 1.2.3 includes these tasks.

- Installation of Network Performance Insight RPM packages
- Installation IBM Open Platform with Apache Spark and Apache Hadoop packages
- Deploying the Ambari agent hosts in your cluster from Ambari Web UI
- Setting up Network Performance Insight services on the cluster hosts from Ambari Web UI
- Setting up integrations with Dashboard Application Services Hub and Tivoli Network Manager

Required microservices in different installation scenarios

Microservices that are required in different installation scenarios.

*Table 9. Microservices applicable for 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 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>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>Entity Analytics</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Formula</td>
<td>YES</td>
<td>YES</td>
<td>NO</td>
<td>YES</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>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Tivoli Network Manager Collector</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
<td>Initially, it is not required. Enable this service after integration with Tivoli Network Manager.</td>
</tr>
<tr>
<td>Cacti Collector</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
<td>NO</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>
<tr>
<td>Remote Flow Collector</td>
<td>OPTIONAL</td>
<td>OPTIONAL</td>
<td>OPTIONAL</td>
<td>OPTIONAL</td>
</tr>
</tbody>
</table>

© Copyright IBM Corp. 2015, 2018
Table 9. 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>SNMP Discovery</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>

You can disable this service after integration with Tivoli Network Manager.

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 Tivoli Network Manager

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

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:

Chapter 1, “System requirements,” on page 1
Complete set of requirements for IBM Network Performance Insight 1.2.3.

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 NETCOOL_OPERATIONS_INSIGHT_PERFOR.tgz
   tar -zxvf CNS1IML.tar
   cd CNS1IML
   tar -zxvf NPI-1.2.3.0.tgz
   ```
Or, use the following command:

```
gunzip -c NETCOOL_OPERATIONS_INSIGHT_PERFOR.tgz | tar -xvf -
```

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

- NPI-1.2.3.0/
  - pods_1.2.3.zip
    Contains the files and folders that are required for Performance Metric OOTB Device Support component.
  - bin
    - agent_setup_nonRoot.sh
    - install.sh
    - installRemoteFlowCollector.sh
    - npi_prereq_check.sh
    - prereq_check.sh
    - setup_cluster_ssh.sh
  - upgrade
    - auto.conf
    - auto_rollback_ambari_server.sh
    - curl_get_all_hosts.sh
    - curl_get_cluster_name.sh
    - curl_get_comp_by_host.sh
    - curl_get_service_state.sh
    - curl_stop_service.sh
    - generate_upgrade_by_host.sh
    - h2.tgz
    - npi_backup_remote_comp.sh
    - npi_prep.sh
    - npi_rollback.sh
    - npi_upgrade.sh
    - README
    - rollback_by_host.sh
    - upgradeAmbariDashHostConfig.sh
- basecamp-installer-tools-1.2.3.0-<build_signature>.noarch.rpm
- basecamp-repo-1.2.3.0-<build_signature>.noarch.rpm
- npi-ambari-1.2.3.0-<build_signature>.noarch.rpm
- npi-repo-1.2.3.0-<build_signature>.noarch.rpm

**Related tasks:**

- “Installing the Performance Metric OOTB Device Support pack” on page 39

Use this information to install Performance Metric OOTB Device Support pack.

**Downloading the IBM Open Platform with Apache Spark and Apache Hadoop:**

Download the IBM Open Platform with Apache Spark and Apache Hadoop 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>.

- ambari-2.2.0.e17.x86_64.tar.gz
- iop-4.2.0.0.e17.x86_64.tar.gz
- iop-utils-1.2.0.0.e17.x86_64.tar.gz

Note: You do not need to extract these packages.

Procedure

Download the following packages:

- [Ambari](#)
- [IOP](#)
- [IOP-UTILS](#)

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 IBM Open Platform with Apache Spark and Apache Hadoop

<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>Service</td>
<td>Group</td>
<td>User</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>----------</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
- 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**

Perform steps 1 - 20 from Quick reference to installing according to your Netcool Operations Insight entitlement.

**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-related data from Cisco devices that support the Response Time Monitor MIB (CISCO-RTTMON-MIB), such as information on the configured probes.

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 check boxes next to SLA and CiscoIPSLA check box is also checked.
7. Click the save ( ) icon.

Related information:

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 Ambari agent 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-1.2.3.0/bin/setup_cluster_ssh.sh`
Enter the required details on the prompts.

**Note:** Always, give fully qualified domain name (FQDN) for the Ambari agent 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 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 Ambari agent host to make sure that the Ambari server can connect to each Ambari agent.

**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 hard and soft limit to at least 20000 for the number of open files as follows:
   netcool hard nofile 20000
   netcool soft nofile 20000

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.

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 Ambari agent hosts in your cluster as follows:
   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:
   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 IBM Open Platform with Apache Spark and Apache Hadoop and Network Performance Insight on a single host or multi-host environments.
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.

About this task

Use the root user account to perform the following steps.

Procedure

Follow the steps that are specified in [Preparing your environment](#) in IBM BigInsights documentation.

Related information:

- Get ready to install
- Directories created when installing IBM Open Platform with Apache Spark and Apache Hadoop

Installing Network Performance Insight

Install IBM Open Platform with Apache Spark and Apache Hadoop 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_1.2.3.0/bin
   ./install.sh <DIST_DIR>
   ```
Where <DIST_DIR> is the directory where the Network Performance Insight and IBM Open Platform with Apache Spark and Apache Hadoop 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.
- IBM Open Platform with Apache Spark and Apache Hadoop 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
  - IOP.repo
  - IOP-UTILS.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 17.

**What to do next**

You can see the installation output in the following log files that are located in <DIST_DIR>/NPI_1.2.3.0:
- 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.
4. On the Select Stack page, select BigInsights 4.2 NPI stack and click Next.
5. Complete the following steps on the Install Options page:
   a. List all of the nodes that are used in the IBM Open Platform with Apache Spark and Apache Hadoop cluster in 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.
6. 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**.

7. 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>2.7.2</td>
<td>Apache Hadoop Distributed File System (HDFS)</td>
</tr>
<tr>
<td>YARN + MapReduce2</td>
<td>2.7.2</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>0.9.0.1</td>
<td>A high-throughput messaging system.</td>
</tr>
<tr>
<td>NPI</td>
<td>1.2.3.0</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 1.2.3.</td>
</tr>
</tbody>
</table>

8. Click **Next**.

9. 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.

10. Click **Next**.

11. 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.

12. Click **Next**.

13. 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 HD FS**
- **Set up YARN**
- **Set up Zookeeper**
• Set up Kafka
• Set up communication with Tivoli Network Manager
• Set up Network Performance Insight
• “Setting up the OMNIbus Standard Input probe” on page 27

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

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

16. 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.

17. Click Next after the services are installed successfully.

18. 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.

What to do next

• “Disabling the services not required for an installation scenario” on page 29

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: 800
• 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 12
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:

Setting up Zookeeper:

Modify the default settings for Zookeeper from Ambari web UI.

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 10. Kafka Broker settings**

<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><code>&lt;data&gt;/kafka-logs</code> Note: Ensure that the <code>&lt;data&gt;</code> directory has sufficient or the recommended disk space. Do not set up Kafka logs in <code>/tmp</code> directory.</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 Accept the default value.</td>
</tr>
</tbody>
</table>
Table 10. Kafka Broker settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<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></td>
<td>Accept the default value.</td>
<td></td>
</tr>
<tr>
<td>zookeeper.connect</td>
<td>Comma-separated list of connection strings in this format where the ZooKeeper is running: host1:port1,host2:port2</td>
<td>&lt;myserver.ibm.com&gt;:2182</td>
</tr>
<tr>
<td>Kafka Broker host</td>
<td>Hosts where the Kafka broker is running.</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
</tbody>
</table>

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:

- ![IBM DB2](image) 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](#).

- ![Oracle](image) Use ojdbc6-11gR2.jar JDBC driver that is available in the /opt/IBM/basecamp/basecamp-connect/libs folder to connect to Oracle database.

Table 11. 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>itmm.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>itmm.host</td>
<td>Name of the host where Tivoli Network Manager database is installed.</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>itmm.port</td>
<td>The network port to connect to Tivoli Network Manager</td>
<td><img src="image" alt="IBM DB2" /> 50000</td>
</tr>
<tr>
<td>itmm.username</td>
<td>An authorized database user name</td>
<td><img src="image" alt="IBM DB2" /> db2inst1</td>
</tr>
</tbody>
</table>

Chapter 2. Installing and configuring
Table 11. NOI Core Settings > NOI Components > NOI SNMP Collector settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>itnm.password</td>
<td>Password for the authorized database user</td>
<td>db2inst1</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 Tivoli Network Manager system</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 Network Performance Insight and Tivoli Network Manager. For more information, see [Enabling the integration with Network Performance Insight](#).

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 12. 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 only if the Storage Service is not installed on all Ambari agent 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 13. 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 14. 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 14. 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 15. NPI Web Services settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>http.port</td>
<td>The http port on which Network Performance Insight application console can be accessed.</td>
<td>8081</td>
</tr>
<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 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 16. 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>
<tr>
<td>Note: Make sure that the flow enabled devices are sending the data to the Flow collector from the same port, 4379.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 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. |
Table 16. 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.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.</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 Ambari agent 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. Optional:

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

   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 **npi-env template** 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 17. 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 -messagelevel DEBUG -raw /var/tmp/stdin.probe.DEBUG.log 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>
</tbody>
</table>
Table 17. 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.rules</td>
<td>STDIN probe rules file location</td>
<td><code>&lt;NPI_HOME&gt;/npi-event/stdin-probe/omnibus/probes/omnibus/stdin.rules</code></td>
</tr>
</tbody>
</table>

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

Disabling the services not required for an installation scenario:

You do not require all the Network Performance Insight microservices for your selected scenario. You can disable the services that are not applicable after the installation is complete.

About this task

After you set up the clusters, all microservices are started and the microservice that are not applicable for your installation scenario must be disabled. For more information about the microservices that must be disabled, see “Required microservices in different installation scenarios” on page 9.

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 Ambari agent host.
   All the services are displayed in the Summary page.
3. Select Stopped from the Started list.
   The service is stopped.
4. Click Turn On Maintenance Mode for that service from Stopped list.
   This service is not restarted when you start all the services next time.

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 and default.cfg configuration files 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 and default.cfg files that are specific to the Dashboard Application Services Hub instance that you want to use for integration:

By default, the custom.cfg and default.cfg files are 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>
</table>
| DASH_ENABLE_OPTION         | If Dashboard Application Services Hub integration is to be included, specify TRUE.  
                             | If Dashboard Application Services Hub integration is not required, specify FALSE. | TRUE                                                         |
| DASH_CONNECTION            | Set the FQDN hostname of the Dashboard Application Services Hub server.        | root@<myserver.ibm.com>Or <non-root-user>@<myserver.ibm.com>  |
| DASH_SSH_PORT              | If non default port number is used, update the SSH port.                      | 22                                                           |
| WEBSHERE_APP_SERVER_PATH   | WebSphere Application Server installation path on Dashboard Application Services Hub server. | /opt/IBM/WebSphere/AppServer                                 |
| JAZZSM_PATH                | Dashboard Application Services Hub installation path.                         | /opt/IBM/JazzSM                                              |
| DASH_USERNAME              | Dashboard Application Services Hub administration user.                       | smadmin                                                      |
| DASH_PASSWORD              | Dashboard Application Services Hub administration user password.             | netcool                                                       |
| KEystore_OPTION            | USE_DEFAULT_KEY or USE_EXIST_KEY                                              | USE_DEFAULT_KEY                                              |
| EXIST_KEYSTORE_FILEPATH    | Location of the keystore                                                      | /tmp/keystore.security                                       |
| EXIST_CA_FILENAME          | CA certificate file location                                                  | /tmp/ca.crt                                                  |
| KEYSTORE_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                                                            | DEVO                                                         |
| LOCALITY                   | Locality                                                                      | DEMO_LOCALITY                                                |
| STATE                      | State                                                                          | DEMO_STATE                                                   |
| COUNTRY                    | Country                                                                        | <MY>                                                         |
**Option** | **Description** | **Example**
---|---|---
WAS_PROFILE_NAME | WebSphere Application Server profile for Jazz for Service Management on the target application server. | JazzSMProfile
WAS_NODE | The default server node for the WebSphere Application Server profile. | JazzSMNode01
WAS_SERVER_NAME | Name of the application server that is specified when the application server profile is created. | server1
WAS_PROFILE_PATH | Location of the application server profile. | /opt/IBM/JazzSM/profile/
NPI_UI_HOST | Host where the UI service is installed. | <myserver.ibm.com>

**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:

```
# 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:

```
```

**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 IBM Open Platform with Apache Spark and Apache Hadoop 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.

```
# <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
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/install.User.cfg
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.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 18. 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 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 19. Advanced > Advanced npi-auth Settings**

<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:
9. Check that the ca.crt file with webSphereCACert alias is available in /opt/IBM/basecamp/basecamp-jre/conf/security directory by running the following command on all Ambari agents:

   keytool -keystore /opt/IBM/basecamp/basecamp-jre/ibm-java-x86_64-80/jre/lib/security/cacerts -storepass changeit -list -alias WebSphereCACert

10. Get the finger print 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 finger print of the npi_ca is same as the trustedCertEntry certificate finger print 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:
### Option | Description | Suggested value
--- | --- | ---
**Default server certificate alias** | If it is not defined earlier, this setting specifies the certificate alias that is used as the identity for this SSL configuration. | netcool

**Default client certificate alias** | Specifies the description for a client certificate alias. | netcool

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:
  1. Click **Tools > Internet Options**.
  2. Click **Content > Certificates > Trusted Root Certification Authorities**.
3. Click Import.
4. Browse to the location of the exported ca.crt file.
5. Click Next.
6. Select to place the certificates in **Trusted Root Certification Authorities** option and click **Finish**.

* For Firefox, follow these steps:
  1. Click **Tools > Options**.
  2. Click **Advanced > Certificates > View Certificates**.
  3. Click **Authorities > Import**.
  4. Browse to the location of the exported ca.crt file and click **Open**.
  5. Select all the check boxes on the Downloading Certificate page and click **OK**.
  6. Click **OK** to close the window.

* For Chrome, follow these steps:
  1. Click **Settings > Advanced > Manage certificates**.
  2. Click **Import**.
  3. Browse to the location of the exported ca.crt file and click **Open**.
  4. Select **Place all certificates in the following store** and click **Browse**.
  5. Select to place the certificate in **Trusted Root Certification Authorities** and click **OK**.
  6. Click **Next** and **Finish**.

**Related tasks:**

“Enabling integration with Jazz for Service Management” on page 31

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

**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:

• Security Services are installed.

  **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_1.2.3.0/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:
   ```bash
   ./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. Restart 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. Restart 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. Restart the following services:

   - Zookeeper
   - Kafka
   - 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/logs/zookeeper
   - /var/logs/kafka
Installing the Performance Metric OOTB Device Support component

Install the Performance Metric OOTB Device Support component that produces and stores the vendor-specific device performance metrics in the database.

Before you begin

- Make sure that you have Tivoli Network Manager V4.2.0.4 installed. Download the required fixes from IBM Fix Central. You require both 4.2.0-TIV-NOIHD-<platform>-FP0004 and 4.2.0-TIV-ITNMIP-<platform>-FP0004 files.

About this task

The Performance Metric OOTB Device Support component contains two archive files.

- The Performance Metric OOTB Device Support pack that produces the vendor-specific device performance metrics.
- The Performance Metric OOTB Device Support cronjob package that contains database-specific cronjobs that can be scheduled every 5 minutes to check and update any missing entry in the Tivoli Network Manager tables.

For more information, see Performance Metric OOTB Device Support section in IBM Network Performance Insight: Product Overview.

Procedure

Extract the pods_1.2.3.zip file in the <DIST_DIR> directory by using the following command:

```
unzip pods_1.2.3.zip
```

The following files are available in the generated pods_1.2.3-<build_number> directory:

- pods_pack_1.2.3-<build_number>.tar.gz
- pods_upsertent_1.2.3-<build_number>.tar.gz

Installing the Performance Metric OOTB Device Support pack:

Use this information to install Performance Metric OOTB Device Support pack.

Before you begin

- The following MIB files are required for this solution. Most of them are available in a typical Tivoli Network Manager system and the missing MIB files are bundled in Performance Metric OOTB Device Support package:
<table>
<thead>
<tr>
<th>MIBs required for the solution</th>
<th>Bundled MIBs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco</strong></td>
<td><strong>Cisco</strong></td>
</tr>
<tr>
<td>• CISCO-ENTITY-FRU-CONTROL-MIB.mib</td>
<td>• CISCO-ENHANCED-MEMPOOL.mib</td>
</tr>
<tr>
<td>• CISCO-ENTITY-SENSOR-MIB.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-ENVMON.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-MEMORY-POOL-MIB.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-PROCESS-MIB.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-SMI.mib</td>
<td></td>
</tr>
<tr>
<td>• ENTITY.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-ENHANCED-MEMPOOL.mib</td>
<td></td>
</tr>
<tr>
<td>• OLD-CISCO-SYS.mib</td>
<td></td>
</tr>
<tr>
<td>• OLD-CISCO-INTERFACES-MIB.mib</td>
<td></td>
</tr>
<tr>
<td><strong>Juniper</strong></td>
<td><strong>Juniper ERX</strong></td>
</tr>
<tr>
<td>• juniMibs.mib</td>
<td>• juniSystem.mib</td>
</tr>
<tr>
<td>• juniSm.mib</td>
<td></td>
</tr>
<tr>
<td>• juniTc.mib</td>
<td></td>
</tr>
<tr>
<td>• mib-jnx-chassis.mib</td>
<td></td>
</tr>
<tr>
<td>• juniSystem.mib</td>
<td></td>
</tr>
<tr>
<td><strong>Huawei</strong></td>
<td><strong>Huawei</strong></td>
</tr>
<tr>
<td>• huawei-entity-extent-mib.mib</td>
<td>• huawei-entity-extent-mib.mib</td>
</tr>
<tr>
<td>• huawei-mib.mib</td>
<td>• huawei-mib.mib</td>
</tr>
</tbody>
</table>

Agent that discovers the containment information:
• ENTITY-MIB.mib
  The Entity agent queries the MIB for each entity and retrieves containment information for that entity. Before you enable this agent, you must configure SNMP access and the SNMP Helper. For more information, see Discovering containment information.

• Ensure that Korn Shell (ksh) is present in the /bin/ksh path. If ksh is not available, then create a softlink by using the following command:
  ```bash
  ln -s /bin/ksh /usr/bin/ksh
  ```

**Procedure**
1. Log in to the server where Tivoli Network Manager server is installed as root user.
2. Copy the pods_pack_1.2.3-<build_number>.tar.gz file from the <DIST_DIR> to the following directory:
   ```bash
   $NCHOME/precision/scripts
   ```
   By default, $NCHOME is /opt/IBM/netcool/core.
3. Extract the pods_pack_1.2.3-<build_number>.tar.gz file.
   ```bash
   gunzip -c pods_pack_1.2.3-<build_number>.tar.gz | tar -xvf -
   ```

**Note:** Make sure that the /pods directory has correct Tivoli Network Manager owner. If it is not, change to the correct owner and group by using the following command:
```bash
chown -R <itnm_owner>:<group> pods
```
For example:

```
chown -R netcool:netcool pods
```

The following directories and files are available in the `/pods` directory:

- 1.2.3
  - agents
  - defs
    - mibs
      Contains the vendor-specific MIB files that are missing from Tivoli Network Manager system.
    - polldef
      Contains the vendor-specific XML files and scripts.
    - sql
      - Installation and uninstallation scripts
  - tools

4. Set the Tivoli Network Manager environment to pick up your changes as follows:

```
cd $NCHOME
source env.sh
```

5. Create the `.db_connect` for fresh installation as follows:

```
It is a one time task. Two sample files for Oracle and Db2 setup are provided in the following location:
$NCHOME/precision/scripts/pods:
- `.db_connect.db2.sample`
- `.db_connect.ora.sample`
```

The sample settings are as follows:

**ORACLE**

```
export pods_db_host=<DB_Host_IP_Address>
export pods_db_name=ncim
export pods_db_port=1521
export pods_db_user=ncim
export pods_db_pwd=ncim
```

**IBM**

```
export pods_db_host=<DB_Host_IP_Address>
export pods_db_name=ncim
export pods_db_port=50000
export pods_db_user=db2inst1
export pods_db_pwd=db2inst1
```

6. Run the following command based on your Tivoli Network Manager supported database:

**ORACLE**

```
cd $NCHOME/precision/scripts/pods/1.2.3
./inst.sh ora <domain_name> pods_1.2.3.dict default | tee /tmp/<pods>/inst_<domain_name>_pods_1.2.3.log
```

**IBM**

```
cd $NCHOME/precision/scripts/pods/1.2.3
./inst.sh db2 <domain_name> pods_1.2.3.dict default | tee /tmp/<pods>/inst_<domain_name>_pods_1.2.3.log
```
Where:

- `<domain_name>` is the ObjectServer name. By default, it is NCOMS.

**Note:** Ensure that `/tmp/<pods>` directory is existing in your environment. This command installs the agents, imports the bundled MIB files, and XML files. It also compiles the MIB files and imports all the poll definitions.

If the existing MIB files are compiled previously, you might see the following message:

`. /inst_mib_db2 starting...
Skipped existing MIB CISCO-ENHANCED-MEMPOOL.mib
Skipped existing MIB huawei-entity-extent-mib.mib
Skipped existing MIB huawei-mib.mib
Skipped existing MIB jundiSystem.mib
WARNING: All mibs already exist. Do nothing

Use the force option to ensure that all the existing and new MIB files are compiled successfully by using the following command:

`. /inst.sh ora <domain_name> inst_pods_1.2.3.dict force | tee /tmp/inst_<domain_name>_pods_1.2.3.log

**What to do next**

- Update kafka.properties file by using the following steps:
  1. Stop Tivoli Network Manager Storm Spout by using this command:
     `itm_stop storm`
  2. Edit the `${NCHOME}/precision/storm/conf/kafka.properties` file to add the following line:
     `kafka.table.monitoredinstance=monitoredinstance_vw`
  3. Start Tivoli Network Manager Storm Spout by using this command:
     `itm_start storm`

- (Optional) If you do not see the descriptions for the newly installed agents that belong to Performance Metric OOTB Device Support application from Network Discovery Configuration > Full Discovery Agents, restart the Tivoli Network Manager system.

**Running the network discovery for vendor-specific device performance metrics:**

**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. Select the required domain from the Domain list.
   For example, NCOMS.
4. Click the Full Discovery Agents tab and select the following agents based on the vendor devices and required metrics for your environment:
   - PODS_Cisco_Envmon
   - PODS_Cisco_Entity_Sensor
   - PODS_Cisco_Memory_Pool
   - PODS_Cisco_Processor
   - PODS_Cisco_ Enhanced_Mempool
   - PODS_Juniper_Chassis
   - PODS_Juniper_System
   - PODS_Huawei_Entity
• **Entity**

The Entity agent is supplied by Tivoli Network Manager. It queries the MIB for each entity and retrieves containment information for that entity. Before you enable this agent, you must configure SNMP access and the SNMP Helper. For more information about this agent, see Discovering containment information.

5. Click the save ( ) icon.

6. Start the discovery:
   a. **Scope the discovery.**
   b. Click the **Discovery** icon and select **Network Discovery Status**.
   c. Select the domain in which you want to run a discovery from the **Domain** menu.
   d. Click **Start Discovery** ( ).

Log files are generated for each metric that is discovered in /tmp directory and the file format is as follows:

PODS_<agent_name>_<timestamp>_<ID>.log. For example, PODS_Cisco_Processor_20171103_091045.log.

**Related tasks:**

“Activating SLA agent” on page 14

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.

**Related information:**

Discovering the network

**Setting up a cronjob to update the tables:**

A one time task to schedule a cronjob to check every 5 minutes and update the Tivoli Network Manager tables with Entity ID.

**Procedure**

1. Log in to the server where Tivoli Network Manager server is installed as root user.

2. Copy the pods_upsertent_1.2.3-<build_number>.tar.gz file to the following location:

   $NCHOME/precision/scripts

3. Extract the pods_upsertent_1.2.3-<build_number>.tar.gz file.

   gunzip -c pods_upsertent_1.2.3-<build_number>.tar.gz | tar -xvf -

   The following directories are available in the /pods directory:

   • upsertEnt
   • tools

   This directory contains scripts to set up the cronjob for specific database support.
   – db2
   – ora

4. Set up the cronjob by adding the following line to crontab:
crontab -e
*/5 * * * * (cd $NCHOME/precision/scripts/pods/upsertEnt/ora;
./run_upsertEnt.sh)

crontab -e
*/5 * * * * (cd <$NCHOME>/precision/scripts/pods/upsertEnt/db2;
./run_upsertEnt.sh)

Where:
$NCHOME is Tivoli Network Manager installation directory. By default, it is,
/opt/IBM/netcool/core.

What to do next

You can observe the following log files for any issues in /tmp directory:

- upsertEnt.wk.log
  This log file is overwritten with latest data every 5 minutes.
- upsertEnt.all.log
  If an update for an Entity ID is available in the ncpolldata.monitoredinstance
table, the information is appended in this file.

Enabling the Performance Metric OOTB Device Support poll definitions:

To activate the Performance Metric OOTB Device Support polls, you must activate
them in Tivoli Network Manager system.

Before you begin

Make sure that you have updated the kafka.properties file as specified in
"Installing the Performance Metric OOTB Device Support pack" on page 39.

Procedure

1. Log in to the Jazz for Service Management portal where Tivoli Network
   Manager is installed.
2. Click the Administration icon and select Network > Network Polling.
3. Select the check box next to the following policies:
   - Cisco Device
   - Huawei Device
   - Juniper Device
   - RFC MIB II
   Since these default poll policies contain many metrics, it is a good practice to
   create new poll policies for the specific metrics that you want to poll.
4. Click Enable Selected Policies.
5. Click OK.

Related information:

- Creating polls
- Enabling and disabling polls
**Postinstallation tasks**

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

- To make sure that all the services start automatically when the Ambari server host is restarted, run the following command as root user on the Ambari server host:

  ```
  unlink /etc/rc.d/init.d/ambari-server
  cp -a /usr/sbin/ambari-server /etc/rc.d/init.d/ambari-server && systemctl daemon-reload
  ```

  **Note:** If you do not run this script, some services that are available on the Ambari server host might not start. Ignore the No such file or directory error that you might encounter.

- 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.
  
  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` 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:

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

**Verifying the installation:**

You can verify the Network Performance Insight 1.2.3 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:

   ```
   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_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:
<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:

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

Sample output:

```
# yum list installed | egrep 'npi|basecamp'
apr.x86_64 1.5.2-<build_signature> 0mpi
apr-util.x86_64 1.5.2-<build_signature> 0mpi
basecamp-connect.noarch 1.2.3.0-<build_signature> 0mpi
basecamp-entity-analytics.noarch 1.2.3.0-<build_signature> 0mpi
basecamp-httpd.noarch 1.2.3.0-<build_signature> 0mpi
basecamp-installer-tools.noarch 1.2.3.0-<build_signature> 0mpi
basecamp-jre.x86_64 1.2.3.0-<build_signature> 0mpi
basecamp-manager.noarch 1.2.3.0-<build_signature> 0mpi
basecamp-repo.noarch 1.2.3.0-<build_signature> 0mpi-1.2.3.0
basecamp-schema-registry.noarch 1.2.3.0-<build_signature> 0mpi
basecamp-spark.noarch 1.2.3.0-<build_signature> 0mpi
basecamp-storage.noarch 1.2.3.0-<build_signature> 0mpi
basecamp-tools.noarch 1.2.3.0-<build_signature> 0mpi
basecamp-ui.noarch 1.2.3.0-<build_signature> 0mpi
httpd.x86_64 2.4.18-<build_signature> 0mpi
mailcap.noarch 2.1.31-<build_signature> 0mpi
npi-cacti-collector.noarch 1.2.3.0-<build_signature> 0mpi-1.2.3.0
npi-event.i386 1.2.3.0-<build_signature> 0mpi
npi-flow-analytics.noarch 1.2.3.0-<build_signature> 0mpi
npi-flow-collector.noarch 1.2.3.0-<build_signature> 0mpi
npi-formula.noarch 1.2.3.0-<build_signature> 0mpi
npi-ftp-collector.noarch 1.2.3.0-<build_signature> 0mpi
npi-snmp-collector.noarch 1.2.3.0-<build_signature> 0mpi
npi-snmp-discovery.noarch 1.2.3.0-<build_signature> 0mpi
npi-threshold.noarch 1.2.3.0-<build_signature> 0mpi
postgresql.x86_64 9.2.14-1.<build_signature> 0mpi
postgresql-libs.x86_64 9.2.14-1.<build_signature> 0mpi
postgresql-server.x86_64 9.2.14-1.<build_signature> 0mpi
```

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 1.2.3.
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 45
You can verify the Network Performance Insight 1.2.3 installation status.

“Setting up the OMNIbus Standard Input probe” on page 27
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 default directories that are created during installation.

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

**basecamp**

   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 Tivoli Network Manager database.

   **basecamp-entity-analytics**
   
   Contains the directories and files that are needed for Entity Analytics Service to function.

   **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:
     - Script 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.

- `upgrade` contains scripts that are needed for upgrading to 1.2.3.

**basecamp-jre**
Contains the IBM Java 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-tools**
Contains the encryption script that Ambari uses for encrypting the 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:

```
/basecamp-ui/resources/dashboards
```
Contains the following subdirectories:

- `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.

- `properties`
  Contains all the dashboard properties files.

```
/basecamp-ui/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.

```
/basecamp-ui/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 subdirectories:

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

**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 that calculates formulas on the IP SLA metrics based on the data that is collected by the SNMP Collector Service.

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

**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:

```<NPI_Service>
  .  bin
     .  conf
     .  lib
     .  logs
     .  var
     .  work
```

The `logs` directory contains a separate log file for each microservice.
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:
• IBM Open Platform with Apache Hadoop components, 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:
- Remove 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. Manually, remove these working directories after the uninstallation scripts are run.

About this task

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

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

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

**Uninstalling Ambari agent nodes:**

Run the host_cleanup.sh script to uninstall the Ambari server hosts and Ambari agent 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 Ambari agent 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 Ambari agent, 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 /opt/IBM/basecamp directory.
4. Remove /opt/IBM/npi directory if you have installed the Network Performance Insight microservices.
5. Remove all the working directories that are listed previously.
   For more information, see “Listing working directories” on page 50.

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.

**Related tasks:**

"Generating the certificate and keystore files” on page 31
Generate the certificate authority (CA) certificates and other keystore files on Ambari server.

"Enabling integration with Jazz for Service Management” on page 31
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.

**Procedure**

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

- `yum erase npi-remote-flow-collector`
- `yum erase zookeeper_4_2_0_0.noarch`
- `yum erase iop-select.noarch`
- `yum erase npi-jre`

**What to do next**

After the uninstallation is complete, manually, remove the following .repo files from /etc/yum.repos.d directory if they exist:

- `npi.repo`
- `npi.repo.*`
- `iop*.repo`
- `ambari.repo`

### Uninstalling Performance Metric OOTB Device Support component:

Follow these steps to uninstall the Performance Metric OOTB Device Support component.

**Before you begin**

Disable the poll policies by using the following steps:

- Log in to the Dashboard Application Services Hub server that has Tivoli Network Manager server is installed as Dashboard Application Services Hub administrator user.
- Click the **Administration** icon and select **Network > Network Polling**.
• Select the policies to disable and click **Disable Selected Policies**.

**Procedure**

1. Clean up all the data from upsertEnt cron script as follows:

   ![Oracle]

   a. Log in to the server where Tivoli Network Manager server is installed as root user.
   b. Set the Tivoli Network Manager environment to display your changes after uninstallation as follows:
      ```
cd $NCHOME
source env.sh
```
   c. Run the following commands to delete the data from the cron script:
      ```
cd $NCHOME/precision/scripts/pods/upsertEnt/ora
./cleanupEnt.sh
```
   d. Remove the following line in crontab based on your database:
      ```
crontab -e*/5 * * * * (cd $NCHOME/precision/scripts/pods/upsertEnt/ora;
./run_upsertEnt.sh)
```

   ![IBM DB2]

   a. Log in to the server where Tivoli Network Manager server is installed as root user.
   b. Run the following commands to delete the data from the cron script:
      ```
cd $NCHOME/precision/scripts/pods/upsertEnt/db2
./cleanupEnt.sh
```
   c. Remove the following line in crontab:
      ```
*/5 * * * * (cd $NCHOME>/precision/scripts/pods/upsertEnt/db2;
./run_upsertEnt.sh)
```

   Where:
   $NCHOME is Tivoli Network Manager installation directory. By default, it is, /opt/IBM/netcool/core.

2. Uninstall the agents as follows:

   ![Oracle]

   a. Log in to the server where Tivoli Network Manager server is installed as root user.
   b. Set the Tivoli Network Manager environment to display your changes after uninstallation as follows:
      ```
cd $NCHOME
source env.sh
```
   c. Run the following command to uninstall the agents:
      ```
cd $NCHOME/precision/scripts/pods/1.2.3
./uninst.sh <db_type> <domain> entity_dict
```

   For example:

   ![Oracle]

   ```
./uninst.sh ora NCOMS pods_1.2.3.dict
```

   ![IBM DB2]

   ```
./uninst.sh db2 NCOMS pods_1.2.3.dict
```

   **Note:** The MIB files aren’t removed with these commands.

3. Rerun the discovery to clean up.

4. Remove the poll definitions as follows:
a. Log in to the Dashboard Application Services Hub server that has Tivoli Network Manager server is installed as Dashboard Application Services Hub administrator user.

b. Click the Administration icon and select Network > Network Polling.

c. Select the policies to delete and click Delete selected item(s).

d. Delete all the Performance Metric OOTB Device Support metrics.

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.

Configuring
You can configure IBM Network Performance Insight, Version 1.2.3 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:
- Autonomous System
- Domain names
- Flow Aggregations
- Interfaces
- IP Grouping
- NBAR
- Retention profiles
- Thresholds
- Type of Services

Note: These configuration settings are specific for Flow data only.

For more 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:

1. 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.

2. 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.
3. 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** ( ) button to change the information for the Autonomous System.

Delete an Autonomous System.

4. Select an entry from the table and click **X** icon to delete an entry that is not needed.

Common tasks that are applicable for most of the configuration settings.

5. Click **Search** icon and type an item name or ID in the **Filter by <keyword>** field.
6. Click 🔄 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. Click the up arrow 20 | 50 | 100 ↑ in the lower-right corner and enter a page number that you want to navigate to.

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:** 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 Installing and Configuring IBM Network Performance Insight.</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>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></td>
<td>Top IP Group Conversations with Source ToS</td>
<td>No</td>
<td>• See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</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 Destination IP Groups with Source ToS</td>
<td>No</td>
<td></td>
<td>• See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td>Top Source IP Groups with Source ToS</td>
<td>No</td>
<td></td>
<td>• See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td>Top Source IP Groups</td>
<td>No</td>
<td></td>
<td>• See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
</tbody>
</table>

Chapter 2. Installing and configuring 61
<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>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 See Configuring Flexible NetFlow and AVC 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 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 inConfiguring 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 IP Grouping:**

Create logical grouping of IP addresses and address ranges. This grouping helps in monitoring the individual 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 **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 **X** 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 retention profiles:

Describes how to configure the retention profiles for different type of data.

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 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.

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**.
      - **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>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</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 NCMS. 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:

```
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 NCMS and add the non-default ObjectServer name as follows:

```
# NCMS => omnihost 4100
# NCMS
<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.

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:

Chapter 1, “System requirements,” on page 1
Complete set of requirements for IBM Network Performance Insight 1.2.3.

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 -zxf NETCOOL_OPERATIONS_INSIGHT_PERFOR.tgz
tar -zxf CNSIIML.tar
cd CNSIIML
tar -zxf NPI-1.2.3.0.tgz
   ```

   Or, use the following command:

   ```
   gunzip -c NETCOOL_OPERATIONS_INSIGHT_PERFOR.tgz | tar -xvf -
   ```

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

   - NPI-1.2.3.0/
     - pods_1.2.3.zip
       Contains the files and folders that are required for Performance Metric OOTB Device Support component.
     - bin
       - agent_setup_nonRoot.sh
       - install.sh
       - installRemoteFlowCollector.sh
       - npi_prereq_check.sh
       - prereq_check.sh
       - setup_cluster_ssh.sh
       - upgrade
         - auto.conf
         - auto_rollback_ambari_server.sh
         - curl_get_all_hosts.sh
         - curl_get_cluster_name.sh
         - curl_get_comp_by_host.sh
         - curl_get_service_state.sh
         - curl_stop_service.sh
         - generate Upgrade_by_host.sh
         - h2.tgz
         - npi_backup_remote_comp.sh
         - npi_prep.sh
- npi_rollback.sh
- npi_upgrade.sh
- README
- rollback_by_host.sh
- upgradeAmbariDashHostConfig.sh

- basecamp-installer-tools-1.2.3.0-<build_signature>.noarch.rpm
- basecamp-repo-1.2.3.0-<build_signature>.noarch.rpm
- npi-ambari-1.2.3.0-<build_signature>.noarch.rpm
- npi-repo-1.2.3.0-<build_signature>.noarch.rpm

Related tasks:
“Installing the Performance Metric OOTB Device Support pack” on page 39
Use this information to install Performance Metric OOTB Device Support pack.

Downloading the IBM Open Platform with Apache Spark and Apache Hadoop:

Download the IBM Open Platform with Apache Spark and Apache Hadoop 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>.

- ambari-2.2.0.el7.x86_64.tar.gz
- iop-4.2.0.0.el7.x86_64.tar.gz
- iop-utils-1.2.0.0.el7.x86_64.tar.gz

Note: You do not need to extract these packages.

Procedure

Download the following packages:

- Ambari
- IOP
- IOP-UTILS

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 IBM Open Platform with Apache Spark and Apache Hadoop

<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.

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 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 76.

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 77.
- 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:
   ```
   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:
      ```
      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
   - PODS

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 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 Ambari agent 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:
   ```sh
   <DIST_DIR>/NPI-1.2.3.0/bin/setup_cluster_ssh.sh
   ```
   Enter the required details on the prompts.

   **Note:** Always, give fully qualified domain name (FQDN) for the Ambari agent hosts.
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 Ambari agent host to make sure that the Ambari server can connect to each Ambari agent.

### 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 hard and soft limit to at least 20000 for the number of open files as follows:

   ```
   netcool hard nofile 20000
   netcool soft nofile 20000
   ```

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.

**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 Ambari agent 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:
   ```bash
   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 IBM Open Platform with Apache Spark and Apache Hadoop and Network Performance Insight on a single host or multi-host environments.

**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.
About this task

Use the root user account to perform the following steps.

Procedure

Follow the steps that are specified in [Preparing your environment](#) in IBM BigInsights documentation.

**Related information:**
- [Get ready to install](#)
- [Directories created when installing IBM Open Platform with Apache Spark and Apache Hadoop](#)

**Installing Network Performance Insight**

Install IBM Open Platform with Apache Spark and Apache Hadoop 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:
   
   ```
   rm -rf /var/cache/yum
   ```

2. Start the installation by using the following command as root user on Ambari server:
   
   ```
   cd <DIST_DIR>/NPI_1.2.3.0/bin
   ./install.sh <DIST_DIR>
   ```

   Where `<DIST_DIR>` is the directory where the Network Performance Insight and IBM Open Platform with Apache Spark and Apache Hadoop 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.

• IBM Open Platform with Apache Spark and Apache Hadoop 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
  – IOP.repo
  – IOP-UTILS.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 17.

What to do next

You can see the installation output in the following log files that are located in <DIST_DIR>/NPI_1.2.3.0:

• 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.
4. On the Select Stack page, select BigInsights 4.2 NPI stack and click Next.
5. Complete the following steps on the Install Options page:
   a. List all of the nodes that are used in the IBM Open Platform with Apache Spark and Apache Hadoop cluster in 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.
6. 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**.

7. 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>2.7.2</td>
<td>Apache Hadoop Distributed File System (HDFS)</td>
</tr>
<tr>
<td>YARN + MapReduce2</td>
<td>2.7.2</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>0.9.0.1</td>
<td>A high-throughput messaging system.</td>
</tr>
<tr>
<td>NPI</td>
<td>1.2.3.0</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 1.2.3.</td>
</tr>
</tbody>
</table>

8. Click **Next**.

9. 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.

10. Click **Next**.

11. 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.

12. Click **Next**.

13. 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**
- **Set up Kafka**
• **Set up Network Performance Insight**
• **“Setting up the OMNIbus Standard Input probe” on page 27**

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

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

16. 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.

17. Click **Next** after the services are installed successfully.

18. 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.

**What to do next**

• **“Disabling the services not required for an installation scenario” on page 29**

**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: 800
• 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 12**

   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:

Setting up Zookeeper:

Modify the default settings for Zookeeper from Ambari web UI.

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 20. Kafka Broker settings

<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</td>
</tr>
<tr>
<td></td>
<td>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>
<td></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></td>
<td>Accept the default value.</td>
<td></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></td>
<td>Accept the default value.</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 21. 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>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>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>
</tbody>
</table>

### Table 22. 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 23. 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>
<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 24. NPI Web Services settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>http.port</td>
<td>The http port on which Network Performance Insight application console can be accessed.</td>
<td>8081</td>
</tr>
<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 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 25. 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>
<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, 4379.</td>
<td></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></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>
</tbody>
</table>

Installing and Configuring Network Performance Insight
### Table 25. 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.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 Ambari agent hosts where the Event Service is installed.

2. Ensure that you have the following 32-bit RHEL operating system libraries:

   - zlib
   - ncurses
   - bzip
   - 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. Optional:

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

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 **npi-env template** 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>"
```

---

**Table 26. 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).</td>
<td>-messagelevel INFO -messageLog /var/tmp/stdin.probe.DEBUG.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-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.
Disabling the services not required for an installation scenario:

You do not require all the Network Performance Insight microservices for your selected scenario. You can disable the services that are not applicable after the installation is complete.

About this task

After you set up the clusters, all microservices are started and the microservice that are not applicable for your installation scenario must be disabled. For more information about the microservices that must be disabled, see “Required microservices in different installation scenarios” on page 9.

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 Ambari agent host. All the services are displayed in the Summary page.
3. Select Stopped from the Started list.
   The service is stopped.
4. Click Turn On Maintenance Mode for that service from Stopped list.
   This service is not restarted when you start all the services next time.

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 and default.cfg configuration files 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 and default.cfg files that are specific to the Dashboard Application Services Hub instance that you want to use for integration:

By default, the custom.cfg and default.cfg files are 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>WEBSPHERE_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>
<tr>
<td>KEYSTORE_OPTION</td>
<td>USE_DEFAULT_KEY or USE_EXIST_KEY Note: If you want to reuse your existing key, use the USE_EXIST_KEY.</td>
<td>USE_DEFAULT_KEY</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>npl</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 Jazz for Service Management 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>Option</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------</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 Tivoli Network Manager, you cannot install the Device Dashboard to obtain the security services. In such a scenario, install the security services that are bundled with Network Performance Insight to access the web-based visualizations from Console Integration on Jazz for Service Management.

**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 Network Performance Insight, console integration is performed automatically with the installation of Device Dashboard that comes with Tivoli Network Manager. Starting from V1.2.3, 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 Network Performance Insight integration.

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

**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:
```
```

**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 IBM Open Platform with Apache Spark and Apache Hadoop 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
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/install.User.cfg
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.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 `USEEXIST_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>
<thead>
<tr>
<th>Table 27. NOI Core Settings &gt; NOI Services Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
</tr>
<tr>
<td>web.auth</td>
</tr>
<tr>
<td>security.dash.username</td>
</tr>
<tr>
<td>security.dash.password</td>
</tr>
<tr>
<td>https.keystore.file</td>
</tr>
<tr>
<td>https.keystore.password</td>
</tr>
<tr>
<td>https.key.password</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Table 28. Advanced &gt; Advanced npi-auth Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
</tr>
<tr>
<td>security.dash.hostnames</td>
</tr>
<tr>
<td>security.dash.port</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:
9. Check that the ca.crt file with webSphereCACert alias is available in the /opt/IBM/basecamp/basecamp-jre/conf/security directory by running the following command on all Ambari agents:
   keytool -keystore /opt/IBM/basecamp/basecamp-jre/ibm-java-x86_64-80/jre/lib/security/cacerts -storepass changeit -list -alias WebSphereCACert

10. Get the finger print 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 finger print of the npi_ca is same as the trustedCertEntry certificate finger print 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:
  1. Click Tools > Internet Options.
  2. Click Content > Certificates > Trusted Root Certification Authorities.
3. Click **Import**.
4. Browse to the location of the exported ca.crt file.
5. Click **Next**.
6. Select to place the certificates in **Trusted Root Certification Authorities** option and click **Finish**.

- For Firefox, follow these steps:
  1. Click **Tools > Options**.
  2. Click **Advanced > Certificates > View Certificates**.
  3. Click **Authorities > Import**.
  4. Browse to the location of the exported ca.crt file and click **Open**.
  5. Select all the check boxes on the Downloading Certificate page and click **OK**.
  6. Click **OK** to close the window.

- For Chrome, follow these steps:
  1. Click **Settings > Advanced > Manage certificates**.
  2. Click **Import**.
  3. Browse to the location of the exported ca.crt file and click **Open**.
  4. Select **Place all certificates in the following store** and click **Browse**.
  5. Select to place the certificate in **Trusted Root Certification Authorities** and click **OK**.
  6. Click **Next** and **Finish**.

**Related tasks:**

"Enabling integration with Jazz for Service Management” on page 31
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_1.2.3.0/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:
   
   ```bash
   ./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. Restart 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. Restart 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. Restart the following services:

   • Zookeeper
   • Kafka
   • 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/logs/zookeeper
- /var/logs/kafka

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

- To make sure that all the services start automatically when the Ambari server host is restarted, run the following command as root user on the Ambari server host:
  
  ```
  unlink /etc/rc.d/init.d/ambari-server
  cp -a /usr/sbin/ambari-server /etc/rc.d/init.d/ambari-server &
  systemctl daemon-reload
  ```

  **Note:** If you do not run this script, some services that are available on the Ambari server host might not start. Ignore the No such file or directory error that you might encounter.

- 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
  ```

- 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](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 1.2.3 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:
   ```
   ls -lrt /tmp/*.log
   ```

   You can see the following log files:
### Note:
Dashboard Application Services Hub integration script execution log file is located here:

```bash
<Environment>/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:**

<table>
<thead>
<tr>
<th>Package Name</th>
<th>Version</th>
<th>Dependency</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>apr.x86_64</td>
<td>1.5.2-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>apr-util.x86_64</td>
<td>1.5.2-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-connect.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-entity-analytics.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-httpd.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-installer-tools.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-jre.x86_64</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-manager.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-repo.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-schema-registry.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-spark.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-storage.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-tools.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>basecamp-ui.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>httpd.x86_64</td>
<td>2.4.38-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mailcap.noarch</td>
<td>2.1.31-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-ambari.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-cacti-collector.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-dns.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-event.1386</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-flow-analytics.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-flow-collector.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-formula.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-itnm-collector.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-repo.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-snmp-collector.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-snmp-discovery.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>mpi-threshold.noarch</td>
<td>1.2.3.0-&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>postgresql.x86_64</td>
<td>9.2.14-1.&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>postgresql11ibs.x86_64</td>
<td>9.2.14-1.&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
<tr>
<td>postgresql-server.x86_64</td>
<td>9.2.14-1.&lt;build_signature&gt;</td>
<td>0mpi</td>
<td></td>
</tr>
</tbody>
</table>
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 1.2.3.

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 45
  You can verify the Network Performance Insight 1.2.3 installation status.

- "Setting up the OMNIbus Standard Input probe" on page 27
  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 default directories that are created during installation.

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

**basecamp**

- 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 Tivoli Network Manager database.

  **basecamp-entity-analytics**
  
  Contains the directories and files that are needed for Entity Analytics Service to function.

  **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:
- Script 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.

- upgrade contains scripts that are needed for upgrading to 1.2.3.

basecamp-jre
Contains the IBM Java 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-tools
Contains the encryption script that Ambari uses for encrypting the 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:

/basecamp-ui/resources/dashboards
Contains the following subdirectories:

- 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.

- properties
  Contains all the dashboard properties files.

/basecamp-ui/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.
/basecamp-ui/work/oed
This directory is a symbolic link to basecamp/work/basecamp-ui/oed. Contains the H2 database file as oed.mv.db.

npi
directory contains the following subdirectories:
npi-cacti-collector
Contains the directories and files that are needed for Cacti Collector Service to function.
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 that calculates formulas on the IP SLA metrics based on the data that is collected by the SNMP Collector Service.
npi-itnm-collector
Contains the directories and files that are needed for Tivoli Network Manager - Collector Service to function.
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:
<NPI_Service>
  ...
  bin
  conf
  lib
  logs
  var
  work
...

The logs directory contains a separate log file for each microservice.

**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:

- IBM Open Platform with Apache Hadoop components, 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. Manually, remove these working directories after the uninstallation scripts are run.

**About this task**

List down the working directories before you run the uninstallation scripts to make sure that they are removed.
### Procedure

1. Log in to Ambari server host as follows:
   
   \[ \text{http://<ambari_server_host>:8080} \]

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 Checkpoint directories</td>
<td>&lt;data&gt;/hadoop/hdfs/ namesecondary</td>
</tr>
<tr>
<td>YARN</td>
<td>YARN &gt;Configs &gt; Advanced &gt; Application Timeline Service &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>file:///&lt;data&gt;/var/lib/ambari-metrics-collector/hbase</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 Ambari agent nodes:

Run the `host_cleanup.sh` script to uninstall the Ambari server hosts and Ambari agent 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 Ambari agent 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 Ambari agent, 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 `/opt/IBM/basecamp` directory.
4. Remove `/opt/IBM/npi` directory if you have installed the Network Performance Insight microservices.
5. Remove all the working directories that are listed previously.
   For more information, see “Listing working directories” on page 50.

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.

**Related tasks:**
- "Generating the certificate and keystore files” on page 31
  Generate the certificate authority (CA) certificates and other keystore files on Ambari server.
- "Enabling integration with Jazz for Service Management” on page 31
  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.

**Procedure**

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

```
yum erase npi-remote-flow-collector
yum erase zookeeper_4_2_0_0.noarch
yum erase iop-select.noarch
yum erase npi-jre
```

**What to do next**

After the uninstallation is complete, manually, remove the following .repo files from */etc/yum.repos.d* directory if they exist:

- npi.repo
- npi.repo.*
- iop*.repo
- ambari.repo

**Uninstalling the security services:**

Use this information to uninstall the security services.
Before you begin

During the uninstallation of the Ambari Server, the /opt/IBM/basecamp directory is removed. Copy the uninstallSecurityService.sh from the backup folder. For more information, see “Uninstalling Network Performance Insight” on page 50.

About this task

Make sure that the security services are installed.

Procedure

1. Run the uninstallSecurityService.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`/uninstallSecurityService.sh -default=`pwd`/default.cfg -custom=`pwd`/custom.cfg
   ```
2. Manually, remove the JazzSM_Home/security folder.

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 Dashboard Application Services Hub navigation.

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.
Configuring

You can configure IBM Network Performance Insight, Version 1.2.3 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
- 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 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:

1. 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`.

2. 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.

3. 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 within the public AS range.

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

4. Select an entry from the table and click **X** icon to delete an entry that is not needed.

5. Click **Filter by <keyword>** field.

6. Click **Refresh** 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. Click the up arrow in the lower-right corner and enter a page number that you want to navigate to.

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 ( ) 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 ( ) 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>Reflector Log Prefix Path</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. Note: The output path must be same as the path that is specified in “Configuring the Reflector plug-in” on page 77. 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>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 77

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 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 **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 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 metric that is polled from 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 for Cacti metrics only.
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 66

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>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 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>
</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. |
<table>
<thead>
<tr>
<th>Resource</th>
<th>Type of aggregation</th>
<th>Enabled by default</th>
<th>Required additional configuration setting</th>
</tr>
</thead>
</table>
| 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. |
| Top Source IP Groups with Application | No | See Configuring Autonomous System section in Installing and Configuring IBM Network Performance Insight |
| Top Source IP Groups with Protocol | No | See Configuring Autonomous System section in Installing and Configuring IBM Network Performance Insight |
| Top Source 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. |
<p>| Top Destination IP Groups | No | See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight. |</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>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>
<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 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 Devices:**

You can configure the SNMP credentials for all NetFlow enabled devices in your network to send the data to Network Performance Insight from System Configuration on Dashboard Application Services Hub navigation. All devices must be configured to export SNMP data to Network Performance Insight. This information is stored in the database and required for interface enrichment.

**About this task**

You must specify SNMP community strings for Network Performance Insight 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 the Entity ID of a device from the table and click the **Edit** button or select **Edit** in the **Actions** column.

3. 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.
4. 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**, **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

**Priv Password**
Privacy password

5. 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 63. 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

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 IP Grouping:

Create logical grouping of IP addresses and address ranges. This grouping helps in monitoring the individual 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 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 of 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 retention profiles:

Describes how to configure the retention profiles for different type of data.
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 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.

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**.
      
      **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 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 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:

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:

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:

   ```
   #######################################################################
   #
   # 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.
Scenario 3 - NetFlow only data

In this scenario, Network Performance Insight can be used to collect, aggregate, and render the NetFlow data alone.

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:

Chapter 1, “System requirements,” on page 1

Complete set of requirements for IBM Network Performance Insight 1.2.3.

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:
   
   ```bash
   tar -zxvf NETCOOL_OPERATIONS_INSIGHT_PERFOR.tgz
   tar -zxvf CNS1IML.tar
   cd CNS1IML
   tar -zxvf NPI-1.2.3.0.tgz
   ```

   Or, use the following command:
   
   ```bash
   gunzip -c NETCOOL_OPERATIONS_INSIGHT_PERFOR.tgz | tar -xvf -
   ```

   You can see the following files and folders in the <DIST_DIR>:
   
   - NPI-1.2.3.0/
     - pods_1.2.3.zip
       Contains the files and folders that are required for Performance Metric OOTB Device Support component.
     - bin
       - agent_setup_nonRoot.sh
- install.sh
- installRemoteFlowCollector.sh
- npi_prereq_check.sh
- prereq_check.sh
- setup_cluster_ssh.sh
- upgrade
  - auto.conf
  - auto_rollback_ambari_server.sh
  - curl_get_all_hosts.sh
  - curl_get_cluster_name.sh
  - curl_get_comp_by_host.sh
  - curl_get_service_state.sh
  - curl_stop_service.sh
  - generate_upgrade_by_host.sh
  - h2.tgz
  - npi_backup_remote_comp.sh
  - npi_prep.sh
  - npi_rollback.sh
  - npi_upgrade.sh
  - README
  - rollback_by_host.sh
  - upgradeAmbariDashHostConfig.sh
  - basecamp-installer-tools-1.2.3.0-<build_signature>.noarch.rpm
  - basecamp-repo-1.2.3.0-<build_signature>.noarch.rpm
  - npi-ambari-1.2.3.0-<build_signature>.noarch.rpm
  - npi-repo-1.2.3.0-<build_signature>.noarch.rpm

Related tasks:

"Installing the Performance Metric OOTB Device Support pack" on page 39
Use this information to install Performance Metric OOTB Device Support pack.

Downloading the IBM Open Platform with Apache Spark and Apache Hadoop:

Download the IBM Open Platform with Apache Spark and Apache Hadoop 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>.
- ambari-2.2.0.el7.x86_64.tar.gz
- iop-4.2.0.0.el7.x86_64.tar.gz
- iop-utils-1.2.0.0.el7.x86_64.tar.gz

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

Download the following packages:

- [Ambari](https://www.ambari.org)
- [IOP](https://github.com/IBM/IOP)
- [IOP-UTILS](https://github.com/IBM/IOP-UTILS)

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 IBM Open Platform with Apache Spark and Apache Hadoop

<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.

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 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 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 Ambari agent 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-1.2.3.0/bin/setup_cluster_ssh.sh`
   Enter the required details on the prompts.

**Note:** Always, give fully qualified domain name (FQDN) for the Ambari agent 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 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 Ambari agent host to make sure that the Ambari server can connect to each Ambari agent.

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 hard and soft limit to at least 20000 for the number of open files as follows:

   netcool hard nofile 20000
   netcool soft nofile 20000
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.

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 Ambari agent hosts in your
cluster as follows:
   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:
   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=sysconfined_service_t:s0 tcontext=sysunconfined_t:s0
   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 IBM Open Platform with Apache Spark and Apache Hadoop and Network
Performance Insight on a single host or multi-host environments.

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.
About this task

Use the root user account to perform the following steps.

Procedure

Follow the steps that are specified in [Preparing your environment](#) in IBM BigInsights documentation.

Related information:
- Get ready to install
- Directories created when installing IBM Open Platform with Apache Spark and Apache Hadoop

Installing Network Performance Insight

Install IBM Open Platform with Apache Spark and Apache Hadoop 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_1.2.3.0/bin
   ./install.sh <DIST_DIR>
   ```

   Where `<DIST_DIR>` is the directory where the Network Performance Insight and IBM Open Platform with Apache Spark and Apache Hadoop 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.
- IBM Open Platform with Apache Spark and Apache Hadoop 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
  - IOP.repo
  - IOP-UTILS.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 17.

What to do next

You can see the installation output in the following log files that are located in <DIST_DIR>/NPI_1.2.3.0:

- 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 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.
4. On the Select Stack page, select BigInsights 4.2 NPI stack and click Next.
5. Complete the following steps on the Install Options page:
   a. List all of the nodes that are used in the IBM Open Platform with Apache Spark and Apache Hadoop cluster in 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.
6. 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 confirmed the hosts, click Next.

7. 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>2.7.2</td>
<td>Apache Hadoop Distributed File System (HDFS)</td>
</tr>
<tr>
<td>YARN + MapReduce2</td>
<td>2.7.2</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>0.9.0.1</td>
<td>A high-throughput messaging system.</td>
</tr>
<tr>
<td>NPI</td>
<td>1.2.3.0</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 1.2.3.</td>
</tr>
</tbody>
</table>

8. Click Next.

9. 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.

10. Click Next.

11. 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.

12. Click Next.

13. 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
   - Set up Kafka
   - Set up Network Performance Insight
   - "Setting up the OMNIbus Standard Input probe" on page 27
14. Click Next after you reviewed your settings, and completed the configuration of the services.

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

16. 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.

17. Click Next after the services are installed successfully.

18. 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.

What to do next

- “Disabling the services not required for an installation scenario” on page 29

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: 800
- 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 12

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:

Setting up Zookeeper:

Modify the default settings for Zookeeper from Ambari web UI.

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>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></td>
<td><strong>Note:</strong> Ensure that the /&lt;data&gt; directory has sufficient or the recommended disk space. Do not set up Kafka logs in /tmp directory.</td>
<td></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></td>
<td>Accept the default value.</td>
<td></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></td>
<td>Accept the default value.</td>
<td></td>
</tr>
</tbody>
</table>
Table 29. Kafka Broker settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>zookeeper.connect</td>
<td>Comma-separated list of connection strings in this format where the ZooKeeper is running: host1:port1,host2:port2</td>
<td>&lt;myserver.ibm.com&gt;:2182</td>
</tr>
<tr>
<td>Kafka Broker host</td>
<td>Hosts where the Kafka broker is running.</td>
<td>&lt;myserver.ibm.com&gt;</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 30. 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 Note: This setting is only if the Storage Service is not installed on all Ambari agent hosts.</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}} Note: This setting need not be changed.</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}} Note: This setting need not be changed.</td>
</tr>
</tbody>
</table>

Table 31. 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 32. 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>
<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 33. NPI Web Services settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>http.port</td>
<td>The http port on which Network Performance Insight application console can be accessed.</td>
<td>8081</td>
</tr>
<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 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 34. 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>
<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, 4379.</td>
<td></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></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>
</tbody>
</table>


### Table 34. 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.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 Ambari agent 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. Optional:

   **Note:** Change or add these settings only when recommended by IBM Professional Services.
   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 **npi-env template** 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 35. 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).</td>
<td>-messagelevel INFO -messaginglog /var/tmp/stdin.probe.DEBUG.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-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.
Disabling the services not required for an installation scenario:

You do not require all the Network Performance Insight microservices for your selected scenario. You can disable the services that are not applicable after the installation is complete.

About this task

After you set up the clusters, all microservices are started and the microservice that are not applicable for your installation scenario must be disabled. For more information about the microservices that must be disabled, see “Required microservices in different installation scenarios” on page 9.

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 Ambari agent host.
   All the services are displayed in the Summary page.
3. Select Stopped from the Started list.
   The service is stopped.
4. Click Turn On Maintenance Mode for that service from Stopped list.
   This service is not restarted when you start all the services next time.

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 and default.cfg configuration files 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 and default.cfg files that are specific to the Dashboard Application Services Hub instance that you want to use for integration:
By default, the custom.cfg and default.cfg files are 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>WEBSPHERE_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>
<tr>
<td>KEYSTORE_OPTION</td>
<td>USE_DEFAULT_KEY or USE_EXIST_KEY Note: If you want to reuse your existing key, use the USE_EXIST_KEY.</td>
<td>USE_DEFAULT_KEY</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 Jazz for Service Management 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>Option</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------</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 Tivoli Network Manager, you cannot install the Device Dashboard to obtain the security services. In such a scenario, install the security services that are bundled with Network Performance Insight to access the web-based visualizations from Console Integration on Jazz for Service Management.

**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.authsvc_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.authsvc_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 Network Performance Insight, console integration is performed automatically with the installation of Device Dashboard that comes with Tivoli Network Manager. Starting from V1.2.3, 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 Network Performance Insight integration.

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

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:
```
```

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 IBM Open Platform with Apache Spark and Apache Hadoop 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:
```
cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/npiDashIntegration.sh
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/install.User.cfg
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.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 36. 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 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 37. Advanced > Advanced npi-auth Settings

<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:
9. Check that the ca.crt file with webSphereCACert alias is available in /opt/IBM/basecamp/basecamp-jre/conf/security directory by running the following command on all Ambari agents:
   
   ```
   keytool -keystore /opt/IBM/basecamp/basecamp-jre/ibm-java-x86_64-80/jre/lib/security/cacerts -storepass changeit -list -alias WebSphereCACert
   ```

10. Get the finger print 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 finger print of the npi_ca is same as the trustedCertEntry certificate finger print 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:
  1. Click **Tools > Internet Options**.
  2. Click **Content > Certificates > Trusted Root Certification Authorities**.
3. Click Import.
4. Browse to the location of the exported ca.crt file.
5. Click Next.
6. Select to place the certificates in Trusted Root Certification Authorities option and click Finish.

- For Firefox, follow these steps:
  1. Click Tools > Options.
  2. Click Advanced > Certificates > View Certificates.
  3. Click Authorities > Import.
  4. Browse to the location of the exported ca.crt file and click Open.
  5. Select all the check boxes on the Downloading Certificate page and click OK.
  6. Click OK to close the window.

- For Chrome, follow these steps:
  1. Click Settings > Advanced > Manage certificates.
  2. Click Import.
  3. Browse to the location of the exported ca.crt file and click Open.
  4. Select Place all certificates in the following store and click Browse.
  5. Select to place the certificate in Trusted Root Certification Authorities and click OK.
  6. Click Next and Finish.

Related tasks:

“Enabling integration with Jazz for Service Management” on page 31
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.

- To make sure that all the services start automatically when the Ambari server host is restarted, run the following command as root user on the Ambari server host:

```
unlink /etc/rc.d/init.d/ambari-server
cp -a /usr/sbin/ambari-server /etc/rc.d/init.d/ambari-server && systemctl daemon-reload
```

**Note:** If you do not run this script, some services that are available on the Ambari server host might not start. Ignore the No such file or directory error that you might encounter.

- 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 1.2.3 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_utils_http_repos.log
   ambari_http_repos.log
   npi_http_repos.log
   setupReposServer.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:

   ```
   <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:

   ```
   # 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 1.2.3.

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 45
You can verify the Network Performance Insight 1.2.3 installation status.

"Setting up the OMNIbus Standard Input probe” on page 27
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 default directories that are created during installation.

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

**basecamp**

- 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 Tivoli Network Manager database.
  - **basecamp-entity-analytics**
    - Contains the directories and files that are needed for Entity Analytics Service to function.
  - **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:
        - Script 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.
      - `upgrade` contains scripts that are needed for upgrading to 1.2.3.
  - **basecamp-jre**
    - Contains the IBM Java 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-tools**
    - Contains the encryption script that Ambari uses for encrypting the 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:

/basecamp-ui/resources/dashboards
Contains the following subdirectories:
- 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.
- properties
  Contains all the dashboard properties files.

/basecamp-ui/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.

/basecamp-ui/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 subdirectories:

npi-cacti-collector
Contains the directories and files that are needed for Cacti Collector Service to function.

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 that calculates formulas on the IP SLA metrics based on the data that is collected by the SNMP Collector Service.
npi-itnm-collector
Contains the directories and files that are needed for Tivoli Network Manager - Collector Service to function.

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:

```
<NPI_Service>
  .  bin
  .  conf
  .  lib
  .  logs
  .  var
  .  work
```

The `logs` directory contains a separate log file for each microservice.

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:

- IBM Open Platform with Apache Hadoop components, 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. Manually, remove these working directories after the uninstallation scripts are run.

**About this task**

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

**Procedure**

1. Log in to Ambari server host as follows:
   ```plaintext
   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>
<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 Checkpoint directories</td>
<td>&lt;data&gt;/hadoop/hdfs/namessecondary</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>file:///&lt;data&gt;/var/lib/ambari-metrics-collector/hbase</td>
</tr>
<tr>
<td>Services</td>
<td>Ambari Component directory</td>
<td>Example installation path</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------</td>
<td>---------------------------</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 Ambari agent nodes:**

Run the host_cleanup.sh script to uninstall the Ambari server hosts and Ambari agent 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 Ambari agent 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 Ambari agent, 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 `/opt/IBM/basecamp` directory.
4. Remove `/opt/IBM/npi` directory if you have installed the Network Performance Insight microservices.
5. Remove all the working directories that are listed previously.
   For more information, see "Listing working directories" on page 50.

**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.

**Related tasks:**
- "Generating the certificate and keystore files" on page 31
  Generate the certificate authority (CA) certificates and other keystore files on Ambari server.
- "Enabling integration with Jazz for Service Management" on page 31
  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.

Procedure

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

```bash
yum erase npi-remote-flow-collector
yum erase zookeeper_4_2_0_0.noarch
yum erase iop-select.noarch
yum erase npi-jre
```

What to do next

After the uninstallation is complete, manually, remove the following .repo files from /etc/yum.repos.d directory if they exist:

- npi.repo
- npi.repo.*
- iop*.repo
- ambari.repo

Uninstalling the security services:

Use this information to uninstall the security services.

Before you begin

During the uninstallation of the Ambari Server, the /opt/IBM/basecamp directory is removed. Copy the uninstallSecurityService.sh from the backup folder. For more information, see “Uninstalling Network Performance Insight” on page 50.

About this task

Make sure that the security services are installed.

Procedure

1. Run the uninstallSecurityService.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"/uninstallSecurityService.sh -default="pwd"/default.cfg -custom="pwd"/custom.cfg
```

2. Manually, remove the JazzSM_Home/security folder.

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 ( mạch ) disappears from Dashboard Application Services Hub navigation.

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.

Configuring

You can configure IBM Network Performance Insight, Version 1.2.3 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 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:

1. 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.
2. 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.

3. 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.

3. Select a row from the table and click the Edit ( ) button to change the information for the Autonomous System.
   Delete an Autonomous System.
4. Select an entry from the table and click \( \times \) icon to delete an entry that is not needed.
Common tasks that are applicable for most of the configuration settings.

5. Click \( \rightarrow \) icon and type an item name or ID in the Filter by <keyword> field.

6. Click \( \leftrightarrow \) 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. Click the up arrow \( \uparrow \) in the lower-right corner and enter a page number that you want to navigate to.

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, \(<\text{myserver.ibm.com}>\) 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.

Chapter 2. Installing and configuring   173
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 **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>See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td></td>
<td>Top Applications with Source ToS</td>
<td>No</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>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>
<tr>
<td>Top IP Group Conversations with Source ToS</td>
<td>No</td>
<td>• See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.&lt;br&gt;• See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</td>
<td></td>
</tr>
<tr>
<td>Top Destination IP Groups with Source ToS</td>
<td>No</td>
<td>• See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.&lt;br&gt;• See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</td>
<td></td>
</tr>
<tr>
<td>Top Source IP Groups with Application</td>
<td>No</td>
<td>See Configuring Autonomous System section in Installing and Configuring IBM Network Performance Insight</td>
<td></td>
</tr>
<tr>
<td>Top Source IP Groups with Protocol</td>
<td>No</td>
<td>See Configuring Autonomous System section in Installing and Configuring IBM Network Performance Insight</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 Source 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.  |
| Top Destination IP Groups      | No                                           |                    | See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.        |
| Quality of Service             | Top QoS Hierarchies with Queue ID            | No                 | QoS fields must be configured on your devices. See                                                    |
|                                |                                              |                    | See Configuring Flexible NetFlow and AVC section in Configuring Flow devices.                       |
| Protocols                      | Top Protocols                                | Yes                |                                                                                                         |
|                                | Top Protocols with Application               | Yes                |                                                                                                         |
|                                | Top Protocols with Conversation              | Yes                |                                                                                                         |
|                                | Top Protocols with Destination IP            | Yes                |                                                                                                         |
|                                | Top Protocols with Source IP                 | Yes                |                                                                                                         |
| Sources                        | Top Sources                                  | Yes                |                                                                                                         |
|                                | Top Sources with Application                 | Yes                |                                                                                                         |
### Procedure

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

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

2. Select a row from the table and click the **Edit** (Edit Icon) 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 Network Performance Insight from System Configuration on Dashboard Application Services Hub navigation. All devices must be configured to export SNMP data to Network Performance Insight. This information is stored in the database and required for interface enrichment.

### Table

<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>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>

---

178  Installing and Configuring Network Performance Insight
About this task

You must specify SNMP community strings for Network Performance Insight 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 the Entity ID of a device from the table and click the Edit ( ) button or select Edit in the Actions column.

3. 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.

4. 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

Priv Password
Privacy password

5. 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 63. 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

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 IP Grouping:

Create logical grouping of IP addresses and address ranges. This grouping helps in monitoring the individual 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 **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 **X** 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 retention profiles:

Describes how to configure the retention profiles for different type of data.

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 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.

**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.
      - **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:

   #######################################################################
   #
   # 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 Administering IBM Network Performance Insight.
• See Setting up the OMNibus Standard Input probe section in Installing and Configuring IBM Network Performance Insight.

Scenario 4 - Add on Performance data from Tivoli Network Manager 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 Tivoli Network Manager, it can be integrated with Tivoli Network Manager to discover, poll, and render the performance data also.

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:

Chapter 1, “System requirements,” on page 1
Complete set of requirements for IBM Network Performance Insight 1.2.3.

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 NETCOOL_OPERATIONS_INSIGHT_PERFOR.tgz
   tar -zxvf CNS1IML.tar
   cd CNS1IML
   tar -zxvf NPI-1.2.3.0.tgz
   ```
   Or, use the following command:
   ```
   gunzip -c NETCOOL_OPERATIONS_INSIGHT_PERFOR.tgz | tar -xvf -
   ```
   You can see the following files and folders in the <DIST_DIR>:
   • NPI-1.2.3.0/
     - pods_1.2.3.zip
     Contains the files and folders that are required for Performance Metric OOTB Device Support component.
- bin
  - agent_setup_nonRoot.sh
  - install.sh
  - installRemoteFlowCollector.sh
  - npi_prereq_check.sh
  - prereq_check.sh
  - setup_cluster_ssh.sh
- upgrade
  - auto.conf
  - auto_rollback_ambari_server.sh
  - curl_get_all_hosts.sh
  - curl_get_cluster_name.sh
  - curl_get_comp_by_host.sh
  - curl_get_service_state.sh
  - curl_stop_service.sh
  - generate_upgrade_by_host.sh
  - h2.tgz
  - npi_backup_remote_comp.sh
  - npi_prep.sh
  - npi_rollback.sh
  - npi_upgrade.sh
  - README
  - rollback_by_host.sh
  - upgradeAmbariDashHostConfig.sh
- basecamp-installer-tools-1.2.3.0-<build_signature>.noarch.rpm
- basecamp-repo-1.2.3.0-<build_signature>.noarch.rpm
- npi-ambari-1.2.3.0-<build_signature>.noarch.rpm
- npi-repo-1.2.3.0-<build_signature>.noarch.rpm

Related tasks:

"Installing the Performance Metric OOTB Device Support pack" on page 39
Use this information to install Performance Metric OOTB Device Support pack.

**Downloading the IBM Open Platform with Apache Spark and Apache Hadoop:**

Download the IBM Open Platform with Apache Spark and Apache Hadoop 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>`.

- ambari-2.2.0.0.e17.x86_64.tar.gz
- iop-4.2.0.0.e17.x86_64.tar.gz
- iop-utils-1.2.0.0.e17.x86_64.tar.gz

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

Download the following packages:

- Ambari
- IOP
- IOP-UTILS

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 IBM Open Platform with Apache Spark and Apache Hadoop

<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.

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 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 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 Ambari agent 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-1.2.3.0/bin/setup_cluster_ssh.sh`
   Enter the required details on the prompts.

   Note: Always, give fully qualified domain name (FQDN) for the Ambari agent hosts.
If you are configuring the integration of Network Performance Insight with non-root installation of supported Netcool Operations Insight products, run the 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 Ambari agent host to make sure that the Ambari server can connect to each Ambari agent.

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 hard and soft limit to at least 20000 for the number of open files as follows:

   netcool hard nofile 20000
   netcool soft nofile 20000

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.

**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 Ambari agent 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:
   
   ```bash
   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=sysm_u:system_r:unconfined_service_t:s0 tcontext=sysm_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 IBM Open Platform with Apache Spark and Apache Hadoop and Network Performance Insight on a single host or multi-host environments.

**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.
About this task

Use the root user account to perform the following steps.

Procedure

Follow the steps that are specified in Preparing your environment in IBM BigInsights documentation.

Related information:

- Get ready to install
- Directories created when installing IBM Open Platform with Apache Spark and Apache Hadoop

Installing Network Performance Insight

Install IBM Open Platform with Apache Spark and Apache Hadoop 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:
   
   ```
   rm -rf /var/cache/yum
   ```

2. Start the installation by using the following command as root user on Ambari server:
   
   ```
   cd <DIST_DIR>/NPI_1.2.3.0/bin
   ./install.sh <DIST_DIR>
   ```

   Where `<DIST_DIR>` is the directory where the Network Performance Insight and IBM Open Platform with Apache Spark and Apache Hadoop 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.
- IBM Open Platform with Apache Spark and Apache Hadoop 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
  - IOP.repo
  - IOP-UTILS.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 17.

What to do next

You can see the installation output in the following log files that are located in <DIST_DIR>/NPI_1.2.3.0:

- 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.
4. On the Select Stack page, select BigInsights 4.2 NPI stack and click Next.
5. Complete the following steps on the Install Options page:
   a. List all of the nodes that are used in the IBM Open Platform with Apache Spark and Apache Hadoop cluster in 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.
6. 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**.

7. 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>2.7.2</td>
<td>Apache Hadoop Distributed File System (HDFS)</td>
</tr>
<tr>
<td>YARN + MapReduce2</td>
<td>2.7.2</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>0.9.0.1</td>
<td>A high-throughput messaging system.</td>
</tr>
<tr>
<td>NPI</td>
<td>1.2.3.0</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 1.2.3.</td>
</tr>
</tbody>
</table>

8. Click **Next**.

9. 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.

10. Click **Next**.

11. 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.

12. Click **Next**.

13. 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**
    - **Set up Kafka**
14. Click Next after you have reviewed your settings, and completed the configuration of the services.

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

16. 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.

17. Click Next after the services are installed successfully.

18. 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.

What to do next

• “Disabling the services not required for an installation scenario” on page 29

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: 800
• 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 12

   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:

Setting up Zookeeper:

Modify the default settings for Zookeeper from Ambari web UI.

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>Table 38. Kafka Broker settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option</td>
</tr>
<tr>
<td>log.dirs</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>log.retention.hours</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>log.roll.hours</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Table 38. Kafka Broker settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>zookeeper.connect</td>
<td>Comma-separated list of connection strings in this format where the ZooKeeper is running: host1:port1,host2:port2</td>
<td>&lt;myserver.ibm.com&gt;:2182</td>
</tr>
<tr>
<td>Kafka Broker host</td>
<td>Hosts where the Kafka broker is running.</td>
<td>&lt;myserver.ibm.com&gt;</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 39. 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>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>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>
</tbody>
</table>

Table 40. 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>
<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>
<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 42. NPI Web Services settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>http.port</td>
<td>The http port on which Network Performance Insight application console can be accessed.</td>
<td>8081</td>
</tr>
<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 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 43. 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>
<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, 4379.</td>
<td></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></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>
</tbody>
</table>
Table 43. NPI Components > NPI Flow Collector settings (continued).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
<th>Note:</th>
</tr>
</thead>
<tbody>
<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>
<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>
<td></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 Ambari agent 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. Optional:

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

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 **npi-env template** 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 44. 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).</td>
<td>-messagelevel INFO -messagelog /var/tmp/stdin.probe.DEBUG.log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-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.
Disabling the services not required for an installation scenario:

You do not require all the Network Performance Insight microservices for your selected scenario. You can disable the services that are not applicable after the installation is complete.

**About this task**

After you set up the clusters, all microservices are started and the microservice that are not applicable for your installation scenario must be disabled. For more information about the microservices that must be disabled, see "Required microservices in different installation scenarios" on page 9.

**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 Ambari agent host.
   
   All the services are displayed in the Summary page.

3. Select **Stopped** from the **Started** list.
   
   The service is stopped.

4. Click **Turn On Maintenance Mode** for that service from **Stopped** list.
   
   This service is not restarted when you start all the services next time.

**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` and `default.cfg` configuration files 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` and `default.cfg` files that are specific to the Dashboard Application Services Hub instance that you want to use for integration:

By default, the `custom.cfg` and `default.cfg` files are 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>
</table>
| DASH_ENABLE_OPTION         | If Dashboard Application Services Hub integration is to be included, specify TRUE.  
                            | If Dashboard Application Services Hub integration is not required, specify FALSE. | TRUE                            |
| DASH_CONNECTION            | Set the FQDN hostname of the Dashboard Application Services Hub server.     | root@<myserver.ibm.com>Or         |
|                            |                                                                            | <non-root-user>@<myserver.ibm.com>|
| DASH_SSH_PORT              | If non default port number is used, update the SSH port.                    | 22                               |
| WEBSHERE_APP_SERVER_PATH   | WebSphere Application Server installation path on Dashboard Application Services Hub server. | /opt/IBM/WebSphere/AppServer     |
| JAZZSM_PATH                | Dashboard Application Services Hub installation path.                       | /opt/IBM/JazzSM                  |
| DASH_USERNAME              | Dashboard Application Services Hub administration user.                     | smadmin                          |
| DASH_PASSWORD              | Dashboard Application Services Hub administration user password.            | netcool                          |
| KEYSTORE_OPTION            | USE_DEFAULT_KEY or USEEXIST_KEY                                             | USE_DEFAULT_KEY                  |
|                            | **Note:** If you want to reuse your existing key, use the USE_EXIST_KEY.     |                                  |
| EXIST_KEYSTORE_FILEPATH    | Location of the keystore                                                     | /tmp/keystore.security           |
| EXIST_CA_FILEPATH          | CA certificate file location                                                 | /tmp/ca.crt                      |
| KEYSTORE_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                                                                     | <MY>                             |
| WAS_PROFILE_NAME           | WebSphere Application Server profile for Jazz for Service Management on the target application server. | JazzSMProfile                    |
| WAS_NODE                   | The default server node for the WebSphere Application Server profile.       | JazzSMNode01                     |
### Installing the security services:

If your environment does not have Tivoli Network Manager, you cannot install the Device Dashboard to obtain the security services. In such a scenario, install the security services that are bundled with Network Performance Insight to access the web-based visualizations from Console Integration on Jazz for Service Management.

**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 Network Performance Insight, console integration is performed automatically with the installation of Device Dashboard that comes with Tivoli Network Manager. Starting from V1.2.3, 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 Network Performance Insight integration.

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

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 IBM Open Platform with Apache Spark and Apache Hadoop 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.

```
# <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
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/install.User.cfg
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.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 45. 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 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 46. Advanced > Advanced npi-auth Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>security.dash.names</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:
9. Check that the ca.crt file with webSphereCACert alias is available in /opt/IBM/basecamp/basecamp-jre/conf/security directory by running the following command on all Ambari agents:
   
   keytool -keystore /opt/IBM/basecamp/basecamp-jre/ibm-java-x86_64-80/jre/lib/security/cacerts -storepass changeit -list -alias WebSphereCACert

10. Get the finger print 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 finger print of the npi_ca is same as the trustedCertEntry certificate finger print 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</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>alias</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Default client certificate</td>
<td>Specifies the description for a client certificate alias.</td>
<td>netcool</td>
</tr>
<tr>
<td>alias</td>
<td></td>
<td></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:
  1. Click Tools > Internet Options.
  2. Click Content > Certificates > Trusted Root Certification Authorities.
3. Click Import.
4. Browse to the location of the exported ca.crt file.
5. Click Next.
6. Select to place the certificates in Trusted Root Certification Authorities option and click Finish.

- For Firefox, follow these steps:
  1. Click Tools > Options.
  2. Click Advanced > Certificates > View Certificates.
  3. Click Authorities > Import.
  4. Browse to the location of the exported ca.crt file and click Open.
  5. Select all the check boxes on the Downloading Certificate page and click OK.
  6. Click OK to close the window.

- For Chrome, follow these steps:
  1. Click Settings > Advanced > Manage certificates.
  2. Click Import.
  3. Browse to the location of the exported ca.crt file and click Open.
  4. Select Place all certificates in the following store and click Browse.
  5. Select to place the certificate in Trusted Root Certification Authorities and click OK.
  6. Click Next and Finish.

Related tasks:
“Enabling integration with Jazz for Service Management” on page 31
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.

- To make sure that all the services start automatically when the Ambari server host is restarted, run the following command as root user on the Ambari server host:

  unlink /etc/rc.d/init.d/ambari-server
  cp -a /usr/sbin/ambari-server /etc/rc.d/init.d/ambari-server && systemctl daemon-reload

  Note: If you do not run this script, some services that are available on the Ambari server host might not start. Ignore the No such file or directory error that you might encounter.

- 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 1.2.3 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:
   
   ```
   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
   - setupReposServer.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:

   ```
   <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:

   ```
   # 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 1.2.3.

### 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:
   ```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 Installing and Configuring IBM Network Performance Insight.

### Related tasks:

- "Verifying the installation" on page 45
- "Setting up the OMNibus Standard Input probe" on page 27

You can verify the Network Performance Insight 1.2.3 installation status. 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 default directories that are created during installation.

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

**basecamp**

- 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 Tivoli Network Manager database.
  - **basecamp-entity-analytics**
    - Contains the directories and files that are needed for Entity Analytics Service to function.
  - **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:
        - Script that are needed for Dashboard Application Services Hub and Network Performance Insight integration.
        - Installing and un Installing the security services
        - Creating and deleting console integration
      - The `dash-integration` directory also has `security-service` subdirectory that contains the bundled security services software.
      - `upgrade` contains scripts that are needed for upgrading to 1.2.3.
  - **basecamp-jre**
    - Contains the IBM Java 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-tools**
    - Contains the encryption script that Ambari uses for encrypting the 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:

/basecamp-ui/resources/dashboards
Contains the following subdirectories:
- 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.
- properties
  Contains all the dashboard properties files.

/basecamp-ui/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.

/basecamp-ui/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 subdirectories:

npi-cacti-collector
Contains the directories and files that are needed for Cacti Collector Service to function.

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 that calculates formulas on the IP SLA metrics based on the data that is collected by the SNMP Collector Service.
**npi-itnm-collector**
Contains the directories and files that are needed for Tivoli Network Manager - Collector Service to function.

**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:

```
<NPI_Service>
  .  bin
  .  conf
  .  lib
  .  logs
  .  var
  .  work
```

The `logs` directory contains a separate log file for each microservice.

**Integrating with Tivoli Network Manager**
Use this information if you want 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 Ambari agent 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.

Uninstalling the security services:
Use this information to uninstall the security services.

Before you begin
During the uninstallation of the Ambari Server, the /opt/IBM/basecamp directory is removed. Copy the uninstallSecurityService.sh from the backup folder. For more information, see “Uninstalling Network Performance Insight” on page 50.

About this task
Make sure that the security services are installed.

Procedure
1. Run the uninstallSecurityService.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`/uninstallSecurityService.sh -default=`pwd`/default.cfg -custom=`pwd`/custom.cfg
2. Manually, remove the JazzSM_HOME/security folder.

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 Dashboard Application Services Hub 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.
- Install and configure the Performance Metric OOTB Device Support component that is bundled with Performance Metric OOTB Device Support
- 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

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:
- Security Services are installed.

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 the Performance Metric OOTB Device Support component:

Install the Performance Metric OOTB Device Support component that produces and stores the vendor-specific device performance metrics in the database.

Before you begin

- Make sure that you have Tivoli Network Manager V4.2.0.4 installed.
  - Download the required fixes from IBM Fix Central. You require both 4.2.0-TIV-N01HD-<platform>-FP0004 and 4.2.0-TIV-ITNMIP-<platform>-FP0004 files.

About this task

The Performance Metric OOTB Device Support component contains two archive files.

- The Performance Metric OOTB Device Support pack that produces the vendor-specific device performance metrics.
- The Performance Metric OOTB Device Support cronjob package that contains database-specific cronjobs that can be scheduled every 5 minutes to check and update any missing entry in the Tivoli Network Manager tables.

For more information, see Performance Metric OOTB Device Support section in IBM Network Performance Insight: Product Overview.

Procedure

Extract the pods_1.2.3.zip file in the <DIST_DIR> directory by using the following command:

```
unzip pods_1.2.3.zip
```

The following files are available in the generated pods_1.2.3-<build_number> directory:

- `pods_pack_1.2.3-<build_number>.tar.gz`
- `pods_upsertent_1.2.3-<build_number>.tar.gz`
Installing the Performance Metric OOTB Device Support pack:

Use this information to install Performance Metric OOTB Device Support pack.

**Before you begin**

- The following MIB files are required for this solution. Most of them are available in a typical Tivoli Network Manager system and the missing MIB files are bundled in Performance Metric OOTB Device Support package:

<table>
<thead>
<tr>
<th>MIBs required for the solution</th>
<th>Bundled MIBs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>Cisco</td>
</tr>
<tr>
<td>• CISCO-ENTITY-FRU-CONTROL-MIB.mib</td>
<td>• CISCO-ENHANCED-MEMPOOL.mib</td>
</tr>
<tr>
<td>• CISCO-ENTITY-SENSOR-MIB.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-ENVMON.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-MEMORY-POOL-MIB.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-PROCESS-MIB.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-SMI.mib</td>
<td></td>
</tr>
<tr>
<td>• ENTITY.mib</td>
<td></td>
</tr>
<tr>
<td>• CISCO-ENHANCED-MEMPOOL.mib</td>
<td></td>
</tr>
<tr>
<td>• OLD-CISCO-SYS.mib</td>
<td></td>
</tr>
<tr>
<td>• OLD-CISCO-INTERFACES-MIB.mib</td>
<td></td>
</tr>
<tr>
<td>Juniper</td>
<td>Juniper ERX</td>
</tr>
<tr>
<td>• juniMibs.mib</td>
<td>• juniSystem.mib</td>
</tr>
<tr>
<td>• juniSmi.mib</td>
<td></td>
</tr>
<tr>
<td>• juniTc.mib</td>
<td></td>
</tr>
<tr>
<td>• mib-jnx-chassis.mib</td>
<td></td>
</tr>
<tr>
<td>• juniSystem.mib</td>
<td></td>
</tr>
<tr>
<td>Huawei</td>
<td>Huawei</td>
</tr>
<tr>
<td>• huawei-entity-extent-mib.mib</td>
<td>• huawei-entity-extent-mib.mib</td>
</tr>
<tr>
<td>• huawei-mib.mib</td>
<td>• huawei-mib.mib</td>
</tr>
</tbody>
</table>

**Agent that discovers the containment information:**

- ENTITY-MIB.mib

  The Entity agent queries the MIB for each entity and retrieves containment information for that entity. Before you enable this agent, you must configure SNMP access and the SNMP Helper. For more information, see Discovering containment information.

- Ensure that Korn Shell (ksh) is present in the /bin/ksh path. If ksh is not available, then create a softlink by using the following command:

  ```bash
  ln -s /bin/ksh /usr/bin/ksh
  ```

**Procedure**

1. Log in to the server where Tivoli Network Manager server is installed as root user.
2. Copy the pods_pack_1.2.3-<build_number>.tar.gz file from the <DIST_DIR> to the following directory:

   ```bash
   $NCHOME/precision/scripts
   ```
By default, $NCHOME is /opt/IBM/netcool/core.

3. Extract the pods_pack_1.2.3-<build_number>.tar.gz file.

   gunzip -c pods_pack_1.2.3-<build_number>.tar.gz | tar -xvf -

   Note: Make sure that the /pods directory has correct Tivoli Network Manager owner. If it is not, change to the correct owner and group by using the following command:

   chown -R <itm_owner>:<group> pods

   For example:

   chown -R netcool:netcool pods

   The following directories and files are available: in the /pods directory:

   • 1.2.3
     - agents
     - defs
       This folder contains the following folders:
         - mibs
           Contains the vendor-specific MIB files that are missing from Tivoli Network Manager system.
         - polldef
           Contains the vendor-specific XML files and scripts.
     - sql
       - Installation and uninstallation scripts
   • tools

4. Set the Tivoli Network Manager environment to pick up your changes as follows:

   cd $NCHOME
   source env.sh

5. Create the .db_connect for fresh installation as follows:

   It is a one time task. Two sample files for Oracle and Db2 setup are provided in the following location:

   $NCHOME/precision/scripts/pods:

   • .db_connect.db2.sample
   • .db_connect.ora.sample

   The sample settings are as follows:

   ORACLE

   export pods_db_host=<DB_Host_IP_Address>
   export pods_db_name=ncim
   export pods_db_port=1521
   export pods_db_user=ncim
   export pods_db_pwd=ncim

   IBM

   export pods_db_host=<DB_Host_IP_Address>
   export pods_db_name=ncim
   export pods_db_port=50000
   export pods_db_user=db2inst1
   export pods_db_pwd=db2inst1

6. Run the following command based on your Tivoli Network Manager supported database:
cd $NCHOME/precision/scripts/pods/1.2.3
./inst.sh ora <domain_name> pods_1.2.3.dict default | tee /tmp/<pods>/inst_<domain_name>_pods_1.2.3.log

Where:
- `<domain_name>` is the ObjectServer name. By default, it is NCOMS.

**Note:** Ensure that `/tmp/<pods>` directory is existing in your environment. This command installs the agents, imports the bundled MIB files, and XML files. It also compiles the MIB files and imports all the poll definitions.

If the existing MIB files are compiled previously, you might see the following message:

```
./inst_mib_db2 starting...
Skipped existing MIB CISCO-ENHANCED-MEMPOOL.mib
Skipped existing MIB huawei-entity-extent-mib.mib
Skipped existing MIB huawei-mib.mib
Skipped existing MIB juniSystem.mib
WARNING: All mibs already exist. Do nothing
```

Use the force option to ensure that all the existing and new MIB files are compiled successfully by using the following command:

```
./inst.sh ora <domain_name> inst_pods_1.2.3.dict force | tee /tmp/inst_<domain_name>_pods_1.2.3.log
```

**What to do next**

- Update `kafka.properties` file by using the following steps:
  1. Stop Tivoli Network Manager Storm Spout by using this command:
     ```
     itnm_stop storm
     ```
  2. Edit the `$NCHOME/precision/storm/conf/kafka.properties` file to add the following line:
     ```
     kafka.table.monitoredinstance=monitoredinstance_vw
     ```
  3. Start Tivoli Network Manager Storm Spout by using this command:
     ```
     itnm_start storm
     ```
  4. (Optional) If you do not see the descriptions for the newly installed agents that belong to Performance Metric OOTB Device Support application from Network Discovery Configuration > Full Discovery Agents, restart the Tivoli Network Manager system.

**Running the network discovery for vendor-specific device performance metrics:**

**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. Select the required domain from the Domain list.
   For example, NCOMS.
4. Click the **Full Discovery Agents** tab and select the following agents based on the vendor devices and required metrics for your environment:
   - PODS_Cisco_Envmon
   - PODS_Cisco_Entity_Sensor
   - PODS_Cisco_Memory_Pool
   - PODS_Cisco_Processor
   - PODS_Cisco_Enhanced_Mempool
   - PODS_Juniper_Chassis
   - PODS_Juniper_System
   - PODS_Huawei_Entity

   **Entity**
   The Entity agent is supplied by Tivoli Network Manager. It queries the MIB for each entity and retrieves containment information for that entity. Before you enable this agent, you must configure SNMP access and the SNMP Helper. For more information about this agent, see [Discovering containment information](#).

5. Click the save (usahaan) icon.

6. Start the discovery:
   a. **Scope the discovery**
   b. Click the **Discovery** icon and select **Network Discovery Status**.
   c. Select the domain in which you want to run a discovery from the **Domain** menu.
   d. Click **Start Discovery**.

   Log files are generated for each metric that is discovered in /tmp directory and the file format is as follows:
   
   PODS_<agent_name>_<timestamp>_<ID>.log. For example, PODS_Cisco_Processor_20171103_091045.log.

---

**Related tasks:**

- "Activating SLA agent" on page 14

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.

**Related information:**

- [Discovering the network](#)

**Setting up a cronjob to update the tables:**

A one time task to schedule a cronjob to check every 5 minutes and update the Tivoli Network Manager tables with Entity ID.

**Procedure**

1. Log in to the server where Tivoli Network Manager server is installed as root user.
2. Copy the pods_upsertent_1.2.3-<build_number>.tar.gz file to the following location:
   
   $NCHOME/precision/scripts

3. Extract the pods_upsertent_1.2.3-<build_number>.tar.gz file.
gunzip -c pods_upsertent_1.2.3-<build_number>.tar.gz | tar -xvf -
The following directories are available in the /pods directory:

- upsertEnt
- tools

This directory contains scripts to set up the cronjob for specific database support.

- db2
- ora

4. Set up the cronjob by adding the following line to crontab:

```
*/5 * * * * (cd $NCHOME/precision/scripts/pods/upsertEnt/ora; ./run_upsertEnt.sh)
```

```
*/5 * * * * (cd <$NCHOME>/precision/scripts/pods/upsertEnt/db2; ./run_upsertEnt.sh)
```

Where:

$NCHOME is Tivoli Network Manager installation directory. By default, it is, /opt/IBM/netcool/core.

What to do next

You can observe the following log files for any issues in /tmp directory:

- upsertEnt.wk.log
  This log file is overwritten with latest data every 5 minutes.
- upsertEnt.all.log
  If an update for an Entity ID is available in the ncpolldata.monitoredinstance table, the information is appended in this file.

**Enabling the Performance Metric OOTB Device Support poll definitions:**

To activate the Performance Metric OOTB Device Support polls, you must activate them in Tivoli Network Manager system.

Before you begin

Make sure that you have updated the kafka.properties file as specified in "Installing the Performance Metric OOTB Device Support pack" on page 39.

**Procedure**

1. Log in to the Jazz for Service Management portal where Tivoli Network Manager is installed.
2. Click the Administration icon and select Network > Network Polling.
3. Select the check box next to the following policies:
   - Cisco Device
   - Huawei Device
   - Juniper Device
   - RFC MIB II
Since these default poll policies contain many metrics, it is a good practice to create new poll policies for the specific metrics that you want to poll.

4. Click **Enable Selected Policies**.
5. Click **OK**.

Related information:
- Creating polls
- Enabling and disabling polls

**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-related data from Cisco devices that support the Response Time Monitor MIB (CISCO-RITMON-MIB), such as information on the configured probes.

**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 check boxes next to **SLA** and **CiscoIPSLA** check box is also checked.
7. Click the save ( ) icon.

Related information:
- Configuring network discovery

**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 47. 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 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>IBM DB2 50000 ORACLE 1521</td>
</tr>
<tr>
<td>itnm.username</td>
<td>An authorized database user name</td>
<td>IBM DB2 <code>db2inst1</code> ORACLE <code>ncim</code></td>
</tr>
<tr>
<td>itnm.password</td>
<td>Password for the authorized database user</td>
<td>IBM DB2 <code>db2inst1</code> ORACLE <code>ncim</code></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 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](#).
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

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:

- IBM Open Platform with Apache Hadoop components, 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. Manually, remove these working directories after the uninstallation scripts are run.

About this task

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

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</td>
<td>&lt;data&gt;/hadoop/hdfs/namesecondary</td>
</tr>
<tr>
<td></td>
<td>SecondaryNameNode Checkpoint directories</td>
<td></td>
</tr>
<tr>
<td></td>
<td>YARN &gt; Configs &gt; Advanced &gt; Application Timeline Server</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-timeline-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>file:///&lt;data&gt;/var/lib/ambari-metrics-collector/hbase</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 Ambari agent nodes:

Run the host_cleanup.sh script to uninstall the Ambari server hosts and Ambari agent 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 Ambari agent 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 Ambari agent, 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 /opt/IBM/basecamp directory.
4. Remove /opt/IBM/npi directory if you have installed the Network Performance Insight microservices.
5. Remove all the working directories that are listed previously.
   For more information, see “Listing working directories” on page 50.

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.

Related tasks:
- “Generating the certificate and keystore files” on page 31
  Generate the certificate authority (CA) certificates and other keystore files on Ambari server.
- “Enabling integration with Jazz for Service Management” on page 31
  Use this information to enable integration between Network Performance Insight and Dashboard Application Services Hub portal.

Uninstalling Remote Flow Collector:

Use these steps to uninstall all the Remote Flow Collectors.

Procedure

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

```bash
yum erase npi-remote-flow-collector
yum erase zookeeper_4_2_0_0.noarch
yum erase iop-select.noarch
yum erase npi-jre
```
What to do next

After the uninstallation is complete, manually, remove the following .repo files from /etc/yum.repos.d directory if they exist:
• npi.repo
• npi.repo.*
• iop*.repo
• ambari.repo

Uninstalling the security services:

Use this information to uninstall the security services.

Before you begin

During the uninstallation of the Ambari Server, the /opt/IBM/basecamp directory is removed. Copy the uninstallSecurityService.sh from the backup folder. For more information, see “Uninstalling Network Performance Insight” on page 50.

About this task

Make sure that the security services are installed.

Procedure
1. Run the uninstallSecurityService.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`/uninstallSecurityService.sh -default=`pwd`/default.cfg -custom=`pwd`/custom.cfg
2. Manually, remove the JazzSM_Home/security folder.

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 Dashboard Application Services Hub navigation.
Uninstalling Performance Metric OOTB Device Support component:

Follow these steps to uninstall the Performance Metric OOTB Device Support component.

Before you begin

Disable the poll policies by using the following steps:

- Log in to the Dashboard Application Services Hub server that has Tivoli Network Manager server is installed as Dashboard Application Services Hub administrator user.
- Click the **Administration** icon and select **Network > Network Polling**.
- Select the policies to disable and click **Disable Selected Policies**.

Procedure

1. **Clean up all the data from upsertEnt cron script as follows:**

   ```
   a. Log in to the server where Tivoli Network Manager server is installed as root user.
   b. Set the Tivoli Network Manager environment to display your changes after uninstallation as follows:
      
   cd $NCHOME
   source env.sh

   c. Run the following commands to delete the data from the cron script:
      
   cd $NCHOME/precision/scripts/pods/upsertEnt/ora
   ./cleanupEnt.sh

   d. Remove the following line in crontab based on your database:
      
   crontab -e*/5 * * * *(cd $NCHOME/precision/scripts/pods/upsertEnt/ora;
   ./run_upsertEnt.sh)
   ```

   - **Oracle**

   ```
   a. Log in to the server where Tivoli Network Manager server is installed as root user.
   b. Run the following commands to delete the data from the cron script:
      
   cd $NCHOME/precision/scripts/pods/upsertEnt/ora
   ./cleanupEnt.sh

   c. Remove the following line in crontab:
      
   */5 * * * *(cd <$NCHOME>/precision/scripts/pods/upsertEnt/ora;
   ./run_upsertEnt.sh)
   ```

   Where:

   $NCHOME is Tivoli Network Manager installation directory. By default, it is, 
   /opt/IBM/netcool/core.

2. **Uninstall the agents as follows:**

   ```
   a. Log in to the server where Tivoli Network Manager server is installed as root user.
   b. Set the Tivoli Network Manager environment to display your changes after uninstallation as follows:
      
   cd $NCHOME
   source env.sh

   c. Run the following command to uninstall the agents:
      ```
For example:

```
./uninst.sh ora NCOMS pods_1.2.3.dict
```

```
./uninst.sh db2 NCOMS pods_1.2.3.dict
```

**Note:** The MIB files aren’t removed with these commands.

3. Rerun the discovery to clean up.
4. Remove the poll definitions as follows:
   a. Log in to the Dashboard Application Services Hub server that has Tivoli Network Manager server is installed as Dashboard Application Services Hub administrator user.
   b. Click the **Administration** icon and select **Network > Network Polling**.
   c. Select the policies to delete and click **Delete selected item (s)**.
   d. Delete all the Performance Metric OOTB Device Support metrics.

**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**.

**Configuring**

You can configure IBM Network Performance Insight, Version 1.2.3 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

If you have integrated with Tivoli Network Manager later, you can see all the dashboards that display the performance metrics.

For more 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:
1. 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.

2. 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.

3. 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 ( ) button to change the information for the Autonomous System.

Delete an Autonomous System.

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

Common tasks that are applicable for most of the configuration settings.

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

6. Click 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. Click the up arrow in the lower-right corner and enter a page number that you want to navigate to.

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 **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>See Configuring Type of Service section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td></td>
<td>Top Applications with Source ToS</td>
<td>No</td>
<td></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>IP Address Grouping</td>
<td>Top IP Group Conversations with</td>
<td>No</td>
<td>See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td></td>
<td>Application</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top IP Group Conversations with</td>
<td>No</td>
<td>See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td></td>
<td>Protocol</td>
<td></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></td>
<td>No</td>
<td>• See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.</td>
</tr>
<tr>
<td></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 Source IP Groups with Source ToS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Top Destination IP Groups</td>
<td></td>
<td>No</td>
<td>See Configuring IP Grouping section in Installing and Configuring IBM Network Performance Insight.</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>

| Protocols                | Top Protocols                        | Yes                |                                                                                                           |
|                         | Top Protocols with Application       | Yes                |                                                                                                           |
|                         | Top Protocols with Conversation      | Yes                |                                                                                                           |
|                         | Top Protocols with Destination IP    | Yes                |                                                                                                           |
|                         | Top Protocols with Source IP         | Yes                |                                                                                                           |
| Sources                 | Top Sources                           | Yes                |                                                                                                           |
|                         | Top Sources with Application         | Yes                |                                                                                                           |
### Resource Parameters

<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>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 Devices:

You can configure the SNMP credentials for all NetFlow enabled devices in your network to send the data to Network Performance Insight from System Configuration on Dashboard Application Services Hub navigation. All devices must be configured to export SNMP data to Network Performance Insight. This information is stored in the database and required for interface enrichment.
About this task

You must specify SNMP community strings for Network Performance Insight 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 the Entity ID of a device from the table and click the Edit ( ) button or select Edit in the Actions column.

3. 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 username 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.

4. 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, 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

Priv Password
Privacy password

5. 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 63. 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

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 IP Grouping:

Create logical grouping of IP addresses and address ranges. This grouping helps in monitoring the individual 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 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 retention profiles:**

Describes how to configure the retention profiles for different type of data.

**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 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.

**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.
      
      **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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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:

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:

```
#######################################################################
# 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 Administering IBM Network Performance Insight.
• See Setting up the OMNIbus Standard Input probe section in Installing and Configuring IBM Network Performance Insight.
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.

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.

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 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, following these steps:

1. 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.
2. 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:
```bash
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
      ```bash
      sudo systemctl stop npi-remote-flow-collector
      ```
m b. Stop Kafka Service
      ```bash
      sudo /usr/iop/current/kafka-broker/bin/kafka stop
      ```
   c. Stop Zookeeper Service
      ```bash
      sudo /usr/iop/current/zookeeper-server/bin/zkServer.sh stop
      ```

5. Start the following services in sequence by using the following command:
   a. Start Zookeeper Service
      ```bash
      sudo /usr/iop/current/zookeeper-server/bin/zkServer.sh start
      ```
   b. Start Kafka Service
      ```bash
      sudo /usr/iop/current/kafka-broker/bin/kafka start
      ```
   c. Start Remote Flow Collector
      ```bash
      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 `npi-env template` text area to configure the log level for the error messages that are logged in various log files:

   ```bash
   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 48. Log level rules for different options**

<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:

   ```bash
   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 Ambari agent services in Administering IBM Network Performance Insight.

Configuring and tuning the IP SLA probes

Network Performance Insight 1.2.3 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 npi-env template 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:

   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 0 for that device or entity. If you add or enable that entity back, the state remains as 0. 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 npi-env template 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.

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 of the Ambari Agents to operate without direct root access.

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`
   `useradd ambari`
3. Stop the Ambari server by using the following command:
   `service ambari-server stop`
4. Run the ambari-server setup command to see the following output and prompts:

```
ambari-server setup
Using python /usr/bin/python2
Setup ambari-server
Checking SELinux...
SELinux status is 'disabled'
Ambari-server daemon is configured to run under user 'root'.
Change this setting [y/n] (n)? y
Enter user account for ambari-server daemon (root):ambari
Adjusting ambari-server permissions and ownership...
Checking firewall status...
Redirecting to /bin/systemctl status iptables.service
Checking JDK...
Do you want to change the current JDK [y/n] (n)?
Completing setup...
Configuring database...
Enter advanced database configuration [y/n] (n)?
Configuring database...
Default properties detected. Using built-in database.
Configuring ambari database...
Checking PostgreSQL...
Configuring local database...
Connecting to local database...done.
Configuring PostgreSQL...
Backup for pg_hba found, reconfiguration not required
Extracting system views...
......
Adjusting ambari-server permissions and ownership...
Ambari Server 'setup' completed successfully.
```

5. Start the Ambari server with the following command:

```
service ambari-server start
```

**Configuring Ambari agent hosts for non-root access**

Perform these steps on all Ambari agent 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 Ambari agent node as root user.
2. Stop the Ambari agent 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 Ambari agent by using the following command:

```
service ambari-agent start
```
5. Repeat these steps on all Ambari agent 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

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](http://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.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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 GUARANEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.