IBM Network Performance Insight 1.2.0
Document Revision R2E1

Configuring Network Performance Insight

IBM
Note

Before using this information and the product it supports, read the information in "Notices" on page 39.

This edition applies to version 1.2.0.0 of IBM Network Performance Insight and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2015, 2016.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
# Contents

**Configuring Network Performance Insight** .......................... v
Intended audience .................................................. v
Organization ....................................................... v
Network Performance Insight architecture ................... vi
Service Management Connect .................................. viii
Network Performance Insight technical training .......... vii
Support information ................................................ viii
Conventions used in this publication ............................ viii
  Typeface conventions ........................................... ix

**Chapter 1. Introduction** ........................................... 1

**Chapter 2. Configuring Ambari for non-root access** ............ 3
Configuring Ambari server for non-root access ............... 3
Configuring Ambari agent hosts for non-root access .......... 4

**Chapter 3. Configuring Network Performance Insight services** ..... 5
Configuring Network Performance Insight services ........ 5
Configuring the Flow Collector Service ...................... 7
  Configuring the number of interfaces ...................... 8

**Chapter 4. Configuring Network Performance Insight system** ..... 9
Configuring flow interfaces ...................................... 9
Configuring flow thresholds .................................... 10
Configuring domain names ....................................... 11
Configuring retention profiles .................................. 13

**Chapter 5. Configuring Jazz for Service Management portal** .... 15
Configuring Jazz for Service Management after the installation of Network Performance Insight .... 15
Configuring communication with Jazz for Service Management .................................................. 16
Logging in to the Dashboard Application Services Hub portal .................................................. 17
  Common directory locations for Jazz for Service Management .................................................. 18
Configuring the SSL communication for integration .......... 21
  Configuring SSL settings ........................................ 21
  Adding the signer certificate to your browser ................ 22
Configuring console integration on Jazz for Service Management .................................................. 23

**Chapter 6. Configuring integration with Tivoli Network Manager** . 25
Deployment considerations ........................................ 25
Configuring communication with Tivoli Network Manager .... 26
Configuring Apache Storm Spout in Network Manager .......... 27

**Chapter 7. Configuring integration with Tivoli Netcool/OMNibus** .... 29
Configuring launch-in-context integration with Network Performance Insight .......................... 29
  Creating a launch-in-context tool ............................. 29
  Configuring launch-in-context menu ......................... 30
  Configuring the OMNibus Standard Input probe .......... 31

**Appendix A. Starting Jazz for Service Management application servers** .... 35

**Appendix B. Stopping Jazz for Service Management application servers** ........ 37

**Notices** ......................................................... 39
Trademarks ........................................................ 41
Terms and conditions for product documentation ................ 42

---

© Copyright IBM Corp. 2015, 2016
Configuring Network Performance Insight

You can configure IBM® Network Performance Insight, Version 1.2.0 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.

Related information:

- Configuring network discovery on Tivoli Network Manager

Intended audience

The audience who are network administrator or operations specialist responsible for configuring the Network Performance Insight product suite on an enterprise network.

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

- Network Performance Insight 1.2.0 system
- Basic principles of network protocols and network management
- Flow concepts
- RHEL Administration
- Jazz for Service Management

Organization

Read this summary to help you find the information that you need.

- Chapter 1, “Introduction,” on page 1
- Chapter 2, “Configuring Ambari for non-root access,” on page 3
- Chapter 3, “Configuring Network Performance Insight services,” on page 5
- Chapter 4, “Configuring Network Performance Insight system,” on page 9
- Chapter 5, “Configuring Jazz for Service Management portal,” on page 15
- Chapter 6, “Configuring integration with Tivoli Network Manager,” on page 25
- Chapter 7, “Configuring integration with Tivoli Netcool/OMNIbus,” on page 29

Network Performance Insight architecture

IBM Network Performance Insight is a network performance monitoring system.

Network Performance Insight provides comprehensive, flexible, and scalable traffic data management with visualization and reporting to support complex, multi-vendor, multi-technology networks. It offers a range of dashboard views with robust security features that are designed to meet the needs of executive management and converging network and IT operations teams.

Network Performance Insight offers near real-time and interactive view on the traffic 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:

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

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 installing 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 increases
- 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
  – Kafka
  – Ambari
  – Spark
  – ZooKeeper

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

**Integrated products**

The products that are needed to work with Network Performance Insight, V1.2.0 are as follows:

**Jazz™ for Service Management 1.1.3.0**
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.

Products that are integrated with Network Performance Insight 1.2.0:

**IBM Tivoli® Network Manager IP Edition 4.2.0.1**
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 1.4.0.3**
Netcool Operations Insight is powered by the fault management capabilities of IBM Tivoli Netcool/OMNIbus. In Network Performance Insight v1.2.0, Tivoli Netcool/OMNIbus 8.1.0.8 is an important part of the solution for monitoring the network threshold violations.

**Network Performance Insight services**

Network Performance Insight components 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.

For more information about these services, see IBM Network Performance Insight: Product Overview.

**Related information:**

- [IBM Network Performance Insight on IBM Knowledge Center](#)
- [IBM BigInsights 4.2 documentation](#)
- [HDFS Architecture](#)
Service Management Connect

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


Use Service Management Connect 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.

Related information:


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](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 [http://www.ibm.com/software/support/isa](http://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, multicolon 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. Introduction

Requires simple configuration settings. Network Performance Insight collects data from the monitored flow-enabled devices. The processed and aggregated data can be viewed from the Network Health Dashboard after integration with IBM Tivoli Network Manager IP Edition. This version has minimal system requirements for the large data that it can manage.

Important: Before you configure Network Performance Insight, read the Release Summary.

Network Performance Insight, v1.2.0 integrates with IBM Tivoli Network Manager IP Edition and IBM Tivoli Netcool/OMNibus components of IBM Netcool Operations Insight 1.4.0.3.

For Network Performance Insight to be fully functional and for traffic data to be available on Jazz for Service Management, you must perform the following configurations:

- Configure Network Performance Insight configuration file.
  Create and edit the Network Performance Insight configuration file npi.conf.
- Configure the Jazz for Service Management portal where Network Performance Insight is federated for visualization of traffic data and events from Network Health Dashboard.
  Configure Dashboard Application Services Hub to access the federated Network Performance Insight user interfaces that are available through Network Health Dashboard.
- Configure your network discovery by using the following tools available in Tivoli Network Manager GUI:
  - Discovery Configuration Wizard to perform initial discoveries.
  - Discovery Configuration GUI to perform subsequent discoveries.
- Configure the launch-in-context Traffic Details dashboards from Active Event List or Event Viewer on Dashboard Application Services Hub.

Related information:

- [Configuring network discovery on Tivoli Network Manager](#)
Chapter 2. 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:

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

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/NPI/installer-tools/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.
Chapter 3. Configuring Network Performance Insight services

Configure all the Network Performance Insight services from web-based Ambari user interface. You do not need to create or edit the npi.conf file. The configuration setting from Ambari UI are written to npi.conf files that are located in the conf directory of each microservice.

Configuring Network Performance Insight services

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 > NPI Settings.
3. Make sure that you are in the Configs tab and change the default values in the following fields:

   Table 1. 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 2. 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 4. 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 Manager application console can be accessed.</td>
<td>8081</td>
</tr>
<tr>
<td>https.port</td>
<td>The https port on which Network Performance Manager application console can be accessed.</td>
<td>9443</td>
</tr>
</tbody>
</table>

Configuring the Flow Collector 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 Services > NPI > NPI Settings.
3. Make sure that you are in the Configs tab and change the default values in the following fields:

Table 5. 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. Currently, only UDP is supported.</td>
<td>4379</td>
</tr>
<tr>
<td>collector.flow.exporter.blacklist</td>
<td>Comma-separated list of IP addresses in square brackets. The flow data from these exporters in the list is blocked from further processing.</td>
<td>ipAddress1, ipAddress2</td>
</tr>
<tr>
<td>collector.flow.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>

Related concepts:

"Configuring the number of interfaces" on page 8
IBM Network Performance Insight does not support automatic load-balancing.
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:

- Configure your exporter to send not more than 1000 interfaces per collector for processing.
  See System requirements in Installing IBM Network Performance Insight.
- Configure the collector.flow.max-interfaces setting according to your total number of interfaces that are handled by your network exporters.

Consider the following example, which shows few exporters that are configured to collectors with the following number of interfaces:

- Exporter 1 with 500 interfaces that is configured to Collector 1
- Exporter 2 with 500 interfaces that is configured to Collector 2
- Exporter 3 with 1000 interfaces that is configured to Collector 3

Set the collector.flow.max-interfaces according to your exporters configuration. For this example, set the collector.flow.max-interfaces to 2000.

Note: In this example, it does not take the traffic load into consideration.

For more information about this setting, see Configuring the Flow Collector Service in 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.
Chapter 4. Configuring Network Performance Insight system

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

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

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

The Network Performance Insight dashboard is pre-configured with working sets of default configurations that can create 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:
- Interfaces
- Thresholds
- Domain names
- Retention profiles

Note: These configuration settings are specific for Flow data.

Configuring flow interfaces

Flow records provide unidirectional measurements of traffic that is entering (ingress) or leaving (egress) a MIB-II interface. Network Performance Insight models this process by associating an Ingress Interface and Egress Interface with each MIB-II 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 to refresh the list of interfaces.

5. Click and type an Interface in the Filter by Interface field. You can view the details of the particular interface.

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

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 $^{20\mid50\mid100}$ in the lower-right corner and enter a page number that you want to navigate to.

**What to do next**

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

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

## Configuring flow 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. These Thresholds are static Thresholds because the Threshold violations and their values are user-defined.

**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. Click and type an Interface in the **Filter by Domain Name** field. You can view the details of that particular entity.

5. 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.

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

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.

**Results**

Any interface that is violating the set Threshold value is reported in the Active Event List and 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 Configuring basic threshold poll definitions.

---

**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**.

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

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

   **Note:** Domain names that start or end with “.” or “-” are not accepted.

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

6. Click **refresh** icon to refresh the list of domains.

7. Click **add** icon and type a Domain Name in the **Filter by Domain Name** field.

   You can view the details of the particular domain.

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

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

10. Click the up arrow **20 | 50 | 100** in the lower-right corner and enter a page number that you want to navigate to.

**What to do next**

You can repeat the same process to configure commonly used Domain Names as needed.
Configuring retention profiles

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

**About this task**

Retention profiles control how long raw and aggregated data and log files are retained by the system. 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 in Days, Weeks, or Months

   **Note:** Retention period must be configured with trade-off 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 Refresh ( ) to refresh the list of domains.

5. Click OK to save the settings.

6. Select a number to change the number of items in the table. In the lower-right corner, the numbers that are displayed are the number of items to be displayed on each page.

7. Enter a page number that you want to navigate in the Go to Page and click Go.

**What to do next**

Repeat the same process to configure retention profiles as needed.
Chapter 5. Configuring Jazz for Service Management portal

Jazz for Service Management must be set up for Network Performance Insight federation to work correctly and you can access the web-based visualizations.

Perform the following tasks:

Configuring Jazz for Service Management after the installation of Network Performance Insight

If you choose to install Jazz for Service Management server after you install Network Performance Insight.

About this task

In the scenario where you do not select the Automate DASH SSL Configuration check box during the installation of Network Performance Insight, follow these steps to configure the communications with Jazz for Service Management:

Procedure

1. Update the following fields in the configuration file install.User.cfg file that is located in /opt/IBM/npi/installer-tools:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>DASH_ENABLE_OPTION</td>
<td>If Dashboard Application Services Hub integration is to be automated, specify TRUE. If Dashboard Application Services Hub integration is not required, specify FALSE.</td>
<td>TRUE</td>
</tr>
<tr>
<td>DASH_CONNECTION</td>
<td>The Dashboard Application Services Hub server user. Ambari Server refers to this user to run SSH to the Dashboard Application Services Hub server.</td>
<td>root@&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td>WEBSHHERE_APP_SERVER_PATH</td>
<td>WebSphere Application Server installation path on Jazz for Service Management server.</td>
<td>/opt/IBM/WebSphere/AppServer</td>
</tr>
<tr>
<td>JAZZSM_PATH</td>
<td>Jazz for Service Management installation path.</td>
<td>/opt/IBM/JazzSM</td>
</tr>
<tr>
<td>DASH_USERNAME</td>
<td>Jazz for Service Management administration user.</td>
<td>smadmin</td>
</tr>
<tr>
<td>DASH_PASSWORD</td>
<td>Jazz for Service Management administration user password.</td>
<td>netcool</td>
</tr>
</tbody>
</table>
2. Run `/opt/IBM/npi/installer-tools/npiDashIntegration.sh` script by using the following command:

```
  cd /opt/IBM/npi/installer-tools
  /npiDashIntegration.sh install_user.cfg default.cfg
```

This command performs the following tasks:

- Configures Single Sign-On.
- Creates users and groups.
- Optionally, configures the SSL key.

---

### Configuring communication with Jazz for Service Management

These settings are set automatically on Ambari for communicating with Jazz for Service Management.

#### Procedure

Click NPI > NPI Core Settings and change the default values in the following fields:

**Table 6. 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.hostname</td>
<td>Full DNS name for the Jazz for Service Management server. This entry must be added before you start the Dashboard Application Services Hub for the first time.</td>
<td><code>&lt;myserver.ibm.com&gt;</code></td>
</tr>
<tr>
<td>security.dash.port</td>
<td>HTTPS port on which the Jazz for Service Management communicates</td>
<td>16311</td>
</tr>
<tr>
<td>security.ldap.hostname</td>
<td>Enterprise LDAP host name</td>
<td></td>
</tr>
<tr>
<td>security.ldap.port</td>
<td>Enterprise LDAP server port number</td>
<td>10389</td>
</tr>
</tbody>
</table>

**Table 7. 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.hostname</td>
<td>Administrator user name for Jazz for Service Management for security service.</td>
<td><code>&lt;myserver.ibm.com&gt;</code></td>
</tr>
<tr>
<td>security.dash.port</td>
<td>Password for Jazz for Service Management administrator user name.</td>
<td></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></td>
</tr>
</tbody>
</table>
Table 7. NOI Core Settings > NOI Services settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>https.keystore.password</td>
<td>Password for the SSL keystore that is used by Network Performance Insight.</td>
<td></td>
</tr>
<tr>
<td>https.key.password</td>
<td>Password for the SSL key that is used by Network Performance Insight.</td>
<td></td>
</tr>
</tbody>
</table>

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 LTTP 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.
     The Dashboard Application Services Hub Welcome page opens.
  3. Note: Console Integration icon is available only after you complete the task Configuring Network Performance Insight console integration on Jazz for Service Management that is available in Configuring Network Performance Insight.

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

- Click Incident ( ) on the navigation bar and select Network Health Dashboard under Network Availability.
Common directory locations for Jazz for Service Management

Jazz for Service Management topics use path name variables for paths to common directories, for example, home directories.

Jazz for Service Management home directory

The JazzSM_HOME variable describes the location where Jazz for Service Management is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: /opt/IBM/JazzSM
- Non-root user installations: <user_home_directory>/IBM/JazzSM

Jazz for Service Management profile directory

The JazzSM_WAS_Profile variable describes the location of the application server profile that is used for Jazz for Service Management. This location is in the /profile subdirectory of the Jazz for Service Management home directory.

- Root user installations: /opt/IBM/JazzSM/profile
- Non-root user installations: <user_home_directory>/IBM/JazzSM/profile

Jazz for Service Management profile name

The JazzSM_Profile_Name variable refers to the name assigned to the WebSphere® Application Server profile for Jazz for Service Management. The default name is JazzSMProfile.

Installation images home directory

The Install_Img_Home variable describes the common root directory that contains the extracted contents of the installation images depending on the installation scenario.

Full installation

IBM DB2®, IBM WebSphere Application Server.

Attention: You must extract the contents of the installation media for this software to the same common root directory, otherwise the full installation displays error messages for missing software.

Custom installation

IBM WebSphere Application Server, if you do not want to use an existing installation.

Note: It is not necessary to extract the contents of the installation media for this software to the same common root directory, but it is preferable to maintain all extracted installation media in a central location.

Jazz for Service Management installation images home directory

The JazzSM_Image_Home variable describes the common root directory in which the Jazz for Service Management is extracted. It contains the launchpad, IBM
Installation Manager, IBM Prerequisite Scanner, the Installation Manager repository with the software packages for the integration services except Tivoli Common Reporting.

**Tip:** Ensure that the path to the JazzSM_Image_Home directory does not contain any spaces or special characters, otherwise the launchpad does not start.

**IBM DB2 home**

The `DB2_HOME` variable describes the location where IBM DB2 is installed. This location is specified during installation. If not specified, the following default locations are used:

- Root user installations: `/opt/ibm/db2`
- Non-root user installations: `$HOME/sql1ib`

$HOME represents the non-root user’s home directory.

**WebSphere Application Server home directory**

The `WAS_HOME` variable describes the location where WebSphere Application Server is installed. This location is specified during installation. If not specified, the following default locations are used:

- Root user installations: `/opt/IBM/WebSphere/AppServer`
- Non-root user installations: `<user_home_directory>IBM/WebSphere/AppServer`

**Administration Services home directory**

The `ADMIN_HOME` variable describes the location where Administration Services is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: `/opt/IBM/JazzSM/admin`
- Non-root user installations: `/home/nonrootuser_name/IBM/JazzSM/admin`

**Administration Services UI home directory**

The `ADMINUI_HOME` variable describes the location where Administration Services UI is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: `/opt/IBM/JazzSM/adminui`
- Non-root user installations: `/home/nonrootuser_name/IBM/JazzSM/adminui`

**Registry Services home directory**

The `REGISTRY_HOME` variable describes the location where Registry Services is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: `/opt/IBM/JazzSM/registry`
- Non-root user installations: `/home/nonrootuser_name/IBM/JazzSM/registry`
Security Services home directory

The SECURITY_HOME variable describes the location where Security Services is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: /opt/IBM/JazzSM/security
- Non-root user installations: /home/nonrootuser_name/IBM/JazzSM/security

Dashboard Application Services Hub home directory

The DASH_HOME variable describes the location where Dashboard Application Services Hub is installed. This location can be specified during installation. If not specified, the following default locations are used:

- Root user installations: /opt/IBM/JazzSM/ui
- Non-root user installations: <user_home_directory>IBM/JazzSM/ui

Dashboard Application Services Hub profile directory

The DASH_Profile variable describes the location of the application server profile that is used for Dashboard Application Services Hub. This location is in the/profiles subdirectory of the Jazz for Service Management home directory.

- Root user installations: /opt/IBM/JazzSM/profile
- Non-root user installations: <user_home_directory>IBM/JazzSM/profile

Full installation log directory

The Simple_install_log_dir directory into which general and offering specific logs are created during full installation:

- On UNIX systems: $HOME/jazzsm_launchpad/logs/

IBM Prerequisite Scanner installation directory

The ips_root directory that contains the contents of the extracted Prerequisite Scanner platform package. If not specified, the default locations are used:

- On UNIX systems: Install_Imgs_Home/PrereqScanner/UNIX_Linux

Related information:

Common directory locations
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

Configure the passwordless login as described in Setting SSH passwordless login section in Installing 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

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

Procedure

1. Log in to Jazz for Service Management server as admin user. See “Logging in to the Dashboard Application Services Hub portal” on page 17.
2. In the navigation pane, click Console Settings > Websphere Administrative Console and click Launch Websphere administrative console.
3. In the WebSphere Application Server administrative console navigation pane, click Security > SSL certificate and key management.
4. Click 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>Specifies the certificate alias that is used as the identity for this SSL configuration, if it is not defined earlier.</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.
7. Restart the WebSphere Application Server.
   The signer certificate information is displayed.
8. Press y in the SSL Signer Prompt window
What to do next

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

Related information:

Certificates must be converted to use SHA256withRSA in WebSphere Application Server

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.

1. Go to the following location where Jazz for Service Management server is installed:
   
   /opt/IBM/NPI/installer-tools

2. Copy the ca.crt signer certificate that was generated earlier to your local machine.

Follow these steps on the browser on your local machine that you use to access the visualization dashboards.

3. For Internet Explorer, follow these steps:
   
   a. Click Tools > Internet Options.
   b. Click Content > Certificates > Trusted Root Certification Authorities.
   c. Click Import.
   d. Browse to the location of the exported ca.crt file.
   e. Click Next.
   f. Select to place the certificates in Trusted Root Certification Authorities option and click Finish.

4. For Firefox, follow these steps:
   
   a. Click Tools > Options.
   b. Click Advanced > Certificates > View Certificates.
   c. Click Authorities > Import.
   d. Browse to the location of the exported ca.crt file and click Open.
   e. Select all the check boxes on the Downloading Certificate page and click OK.
   f. Click OK to close the window.
Configuring console integration on Jazz for Service Management

To display external content from a stand-alone console in the Dashboard Application Services Hub console, you can configure a new console integration.

Before you begin

For the integration, these components of Jazz for Service Management are required:
- IBM Dashboard Application Services Hub
- Security Services

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

About this task

When you install the Device Dashboard that is available for Netcool Operations Insight entitled customers, the following tasks are performed automatically:
- Install Security Services
- Configure the Console Integrations.

Results

If the connection is successful, the console content is available in the navigation bar of the Dashboard Application Services Hub console through the icon. Click Console Settings > Console Integrations in the navigation bar to see the Network Performance Insight integration.

Note: You can check the status of the connection from here.

Related information:

Stand-alone console content integration
Chapter 6. Configuring integration with Tivoli Network Manager

Use this information to integrate Network Performance Insight with Tivoli Network Manager component of Netcool Operations Insight.

Deployment considerations

Network Performance Insight is supported as a stand-alone single-server installation. But its integrated components exist in a distributed installation setup.

Install the following Network Manager components:

Network Manager core components
This component consists of the core Network Manager processes: network discovery, polling, root cause analysis, and event enrichment.

NCIM database
This database stores topology data.

Tivoli Netcool/OMNibus
This component consists of the Tivoli Netcool/OMNibus event management software that includes the Object Server and Tivoli Netcool/OMNibus Web GUI.

Network Manager GUI components
This component includes the Dashboard Application Services Hub GUI framework, Web GUI components, Jazz for Service Management, and Java.

Other components
IBM Networks for Operations Insight. Networks for Operations Insight adds network management capabilities to the Netcool Operations Insight solution. The Networks for Operations Insight capability is provided through setting up the following products in Netcool Operations Insight:

• Network Manager
  A main feature that is provided by Networks for Operations Insight is the Network Health Dashboard. Network Health Dashboard is only available if you have Network Manager as part of Netcool Operations Insight.

• Netcool Configuration Manager

Note: Network Performance Insight 1.2.0 does not integrate with this component.

Related information:

IBM Networks for Operations Insight
Configuring communication with Tivoli Network Manager

These settings are required for communicating with Tivoli Network Manager

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 NPI > NPI Core Settings.
3. Make sure that you are in the Configs tab and change the default values in the following fields:

   Note:
   - Use db2jcc-4.19.49.jar JDBC driver that is available in the
     /opt/IBM/NPI/npi-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/NPI/npi-connect/libs folder to connect to Oracle database.

   Table 8. NOI Core Settings > NOI Components settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>itnm.platform</td>
<td>The database platform for Tivoli</td>
<td>DB2 or ORACLE</td>
</tr>
<tr>
<td></td>
<td>Network Manager. You can select</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oracle or DB2 from the list.</td>
<td></td>
</tr>
<tr>
<td>itnm.host</td>
<td>Name of the host where Tivoli</td>
<td>&lt;myserver.ibm.com&gt;</td>
</tr>
<tr>
<td></td>
<td>Network Manager database is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installed.</td>
<td></td>
</tr>
<tr>
<td>itnm.port</td>
<td>The network port to connect to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tivoli Network Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>itnm.username</td>
<td>An authorized database user name</td>
<td></td>
</tr>
<tr>
<td>itnm.password</td>
<td>Password for the authorized</td>
<td></td>
</tr>
<tr>
<td></td>
<td>database user</td>
<td></td>
</tr>
<tr>
<td>itnm.database</td>
<td>Database name</td>
<td></td>
</tr>
<tr>
<td>itnm.schema</td>
<td>The schema name</td>
<td></td>
</tr>
<tr>
<td>itnm.poller</td>
<td>The name of the Tivoli Network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manager poller</td>
<td></td>
</tr>
<tr>
<td>itnm.kafka.connect.url</td>
<td>Kafka connect REST URL</td>
<td></td>
</tr>
<tr>
<td>itnm.kafka.connect.realm</td>
<td>Kafka connect REST realm</td>
<td></td>
</tr>
<tr>
<td>itnm.kafka.connect.username</td>
<td>User name for Kafka</td>
<td></td>
</tr>
<tr>
<td>itnm.kafka.connect.password</td>
<td>connector</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

26 Configuring Network Performance Insight
Configuring Apache Storm Spout in Network Manager

Use this information to configure Storm Spout in Tivoli Network Manager to work with Network Performance Insight.

Before you begin

Ensure that the Ambari host that has Kafka Broker installed is up and running.

Procedure

1. Copy the $NCHOME/precision/storm/default/kafka.properties file to the following location:
   $NCHOME/precision/storm/conf
   
   Note: By default, $NCHOME is /opt/IBM/netcool/core.

2. Edit the new $NCHOME/precision/storm/conf/kafka.properties file to add the following mandatory fields:
   kafka.producer.bootstrap.servers=$KAFKA Server:$PORT
   kafka.consumer.bootstrap.servers=$KAFKA Server:$PORT

   Where:
   • $KAFKA Server is the host name where Kafka Broker is installed on Network Performance Insight cluster.
   • $PORT is the port number of the Kafka Broker, which is 6667.

3. Optional: Add the kafka.enabled property to the following files to disable the integration between Tivoli Network Manager and Network Performance Insight:
   • $NCHOME/precision/storm/conf/NMStormTopology.properties
   • $NCHOME/precision/storm/conf/kafka.properties
   
   Note: By default, Kafka is enabled.
   Add the following field to disable the integration:
   kafka.enabled=false

4. Restart Storm.

Related information:

- Configuring integration with Netcool Performance Insight
- Kafka producer configurations
- Kafka consumer configurations
Chapter 7. 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 <code>&lt;NPI_home&gt;/npi-ui/resources/ael</code>. Where, <code>&lt;&lt;NPI_home&gt;&gt;</code> is Network Performance Insight installation directory.</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 left 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 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 as follows:

   `<IP_Address> <fully_qualified_host_name> <alias>`

   For example,

   `192.0.2.0 <myserver.ibm.com> omnihost`

2. Ensure that you have the following 32-bit Linux operating system libraries:
   - `lib32z1`
   - `lib32ncurses5`
   - `lib32bz2-1.0`
   - `libstdc++6`
   - `lib32stdc++6`

3. 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. Open a browser and access the Ambari server dashboard.
      - Use the following default URL:
        `http://<myserver.ibm.com>:8080`
      - The default user name is `admin`, and the default password is `admin`.
   b. Click Services > NPI > Configs > Advanced.
   c. 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>
<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>$NCHOME defaults to /opt/IBM/tivoli/netcool.</td>
</tr>
<tr>
<td>event.netcool.omnibus.home</td>
<td>Root OMNIbus Installation directory</td>
<td>$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>

**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:

   `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.
Appendix A. Starting Jazz for Service Management application servers

You can start any Jazz for Service Management virtualization and reporting servers by using the IBM WebSphere `startServer` command. You might need to restart the application server after you complete a configuration task for an integration service, or after you stop the application server for maintenance.

**About this task**

The same procedure applies to any Jazz for Service Management application server.

**Procedure**

1. On the relevant Jazz for Service Management server, open a command window.
2. Change to the JazzSM_WAS_Profile/bin directory.
   The default location for `<JazzSM_WAS_Profile>` is /opt/IBM/JazzSM/profile.
3. Run the following command:

   ```
   AIX
   ./startServer.sh server_name
   ```

   Where

   `server_name`
   Enter the name of the application server that was specified when the application server profile was created.

   For example, `server1`.

**Related information:**

- [Common directory locations](#)
Appendix B. Stopping Jazz for Service Management application servers

You can stop any Jazz for Service Management application server by using the IBM WebSphere stopServer command. You might need to restart the application server after you complete a configuration task for an integration service, or stop the application server for maintenance. To start the server again, use the startServer command.

Procedure
1. On the relevant Jazz for Service Management server, open a command window.
2. Change to the WAS_HOME/bin directory. The default location for <JazzSM_WAS_Profile> is /opt/IBM/JazzSM/profile.
3. Run the following command:

   ./stopServer.sh <server_name> -username <WAS_admin_user_name> -password <WAS_admin_password>

   Where

   server_name
   Enter the name of the application server that was specified when the application server profile was created. For example, server1.

   WAS_admin_user_name
   The default user name is smadmin.

   WAS_admin_password
   Password that is specified at the time of installation.

Example

stopServer.sh server1 -username smadmin -password jazzsmpwd

Related information:

Common directory locations
**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.
Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY,
NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.