Getting started with Network Performance Insight
Note
Before you use this information and the product it supports, read the information in "Notices" on page 29.

This edition applies to version _1_, release _1_, modification _1_ 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

**Using Network Performance Insight**
- Intended audience: v
- Organization: v
- Network Performance Insight overview: v
- Service Management Connect: vii
- Network Performance Insight technical training: vii
- Support information: vii
- Conventions used in this publication: viii
  - Typeface conventions: viii

**Chapter 1. Getting started**
- Logging in to the Dashboard Application Services Hub portal: 1

**Chapter 2. Network Performance Insight system configuration**
- Configuring flow interfaces: 3
- Configuring thresholds: 4
- Configuring domain names: 5
- Configuring retention profiles: 7

**Chapter 3. Introduction to visualization dashboards**
- Features of Network Performance Insight visualization dashboards: 9
- Available Dashboards: 10

**Chapter 4. Traffic Details dashboard**
- Discovering networks: 11
- Configuring the network discoveries: 11
- Setting up network for visualizations: 12
- Network Health Dashboard: 13
- Getting started with Network Health Dashboard: 13
- Structure Browser: 14
- Traffic Details from Network Health dashboard: 14
  - Adding Network Performance Insight widget in Network Health dashboard: 15
  - Monitoring Traffic Details from Network Health dashboard: 16
  - Monitoring Traffic Details dashboard: 17
  - Traffic Details dashboard views: 19
  - Monitoring events from Web GUI on Dashboard Application Services Hub: 24
  - Event severity levels: 25

**Chapter 5. Troubleshooting visualizations**

** Notices**
- Trademarks: 31
- Terms and conditions for product documentation: 32

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

This information helps you to understand the visualizations that are available in Network Performance Insight and also configure some of the settings to your needs.

Intended audience

The audience who are network administrators or operations specialist responsible for installing 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 1.1.1 system
- Basic principles of network protocols and network management
- NetFlow concepts
- Administration of RHEL
- IBM® Netcool® Operations Insight
- IBM Tivoli® Network Manager
- Jazz™ for Service Management

Organization

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

- Chapter 1, “Getting started,” on page 1
- Chapter 2, “Network Performance Insight system configuration,” on page 3
- Chapter 3, “Introduction to visualization dashboards,” on page 9
- Chapter 4, “Traffic Details dashboard,” on page 11
- Chapter 5, “Troubleshooting visualizations,” on page 27

Network Performance Insight overview

IBM Network Performance Insight is a flow-based network traffic 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 repair times and optimized network performance.

Network Performance Insight provides IBM Netcool Operations Insight with network performance monitoring capabilities to address modern network management challenges around application-oriented, software-defined-networks in the enterprise data centers and intranet.
The following diagram shows how data is flowing through the various components in Network Performance Insight:

![Diagram of data flow through Network Performance Insight components]

The flow records that are sent by the configured flow exporters are collected by Collector, and sent to Inventory or Analytics component based on the information that they contain.

Analytics component performs flow data aggregation. These results are then stored in Network Performance Insight database.

Additionally, you can enable or disable the processing of flow records on each flow interface on Dashboard Application Services Hub portal. The dashboards provide up-to-date actionable information to provide an insight into network problems and streamline root cause analysis.

The data from the Storage component can be queried to display the results on Network Health Dashboard or OMNibus Web GUI from Active Event List or Event Viewer.

You must integrate Network Performance Insight with IBM Tivoli Network Manager and Tivoli Netcool/OMNibus components of IBM Netcool Operations Insight to take advantage of its network topology views and fault management capabilities.

Network Performance Insight includes the following documents:
- Release summary
- Quick Start Guide
- Installing Network Performance Insight
- Configuring Network Performance Insight
- Integrating with Netcool Operations Insight
• Getting Started with Network Performance Insight
• Troubleshooting Network Performance Insight
• References
• Technical notes

Related information:

IBM Network Performance Insight on IBM Knowledge Center

Service Management Connect

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


• 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:

IBM Network Performance Insight community on developerWorks

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, 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. Getting started

This information provides instructions and general information on how to use IBM Network Performance Insight software to view and configure the performance analysis reports for a network.

Network Performance Insight is a Dashboard Application Services Hub - based network monitoring tool that gives you a complete traffic data analysis of NetFlow, NetStream, CFlow, J-Flow, and IPFIX flows.

In today’s telecom networks, the rate at which data is generated is increasing at an alarming rate, which is driven by an increasingly information-based economy. The volume of data to be consumed and analyzed is increased significantly, underlining the importance of effective visualizations, for an easier analysis and resolution of network issues.

The traffic visualization dashboards are rendered from Network Health Dashboard after you integrate with IBM Tivoli Network Manager.

You can use the Network Performance Insight that is federated on Dashboard Application Services Hub system for the following tasks:

• Configure the system settings.
• View the interactive traffic data visualization dashboards for monitoring the flow data from Network Health Dashboard, when the Network Performance Insight system is integrated with Tivoli Network Manager.
• Monitor the thresholds on Active Event List and Event Viewer, when the Network Performance Insight system is integrated with IBM Tivoli Netcool/OMNibus Web GUI on Dashboard Application Services Hub.

For more information about Monitoring the thresholds on Active Event List and Event Viewer, see Integrating with Tivoli Netcool/OMNibus.

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.
   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 (寒) on the navigation bar and select the dashboard of your choice under System Configuration.

   • Click Incident (ğa) on the navigation bar and select Network Health Dashboard under Network Availability.
Chapter 2. Network Performance Insight system configuration

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

A set of administrative tasks to configure Network Performance Insight. 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: Each tab contains various graphical utilities. By using these utilities, you can do the administrative tasks.

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.

To configure the flow interfaces:

Procedure

1. Log in to Jazz for Service Management server.

2. Click Console Integrations in the navigation, and select Flow 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. Perform the following tasks in the **Actions** column:
   a. Click **Enable** or **Disable** to enable or disable an Interface.
   b. Click **Traffic Details** to view the Traffic Details for an Interface.

7. 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 interfaces to be displayed on each page.

8. Click the arrow to go to a particular page.

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

**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 thresholds

Thresholds provide a mechanism for identifying anomalies in flow data. In this release, thresholds are applied to the total traffic on a flow interface. Threshold is a metric value that is compared against a value to determine whether an interface violated a specific constraint.

**About this task**

These thresholds are considered static thresholds because you set the value for them by using the configuration dialog box. You also define how you want the threshold to act.

**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 an Interface. Enter the following details:
   a. Select the **Enabled** check box to enable a Threshold on the Interface.
   b. Select the **Limit Type** list to **Over, Under, or Band**.
      - **Over** Detect violations when they exceed threshold values.
Under **Detect violations when they fall short of threshold values.**

**Band** Detect violations when they go outside a range (or band) between two threshold values.

c. Enter the **Upper Limit** for the traffic flow for triggering the Threshold.

d. Enter the **Lower Limit** for the traffic flow for triggering the Threshold.
e. Enter the number of events for triggering the Threshold.

**Note:** When the threshold violation limit is crossed, it displays the severity as **Critical**.
For more information, see **Threshold levels in Network Performance Insight 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 the Threshold for an entity.
   c. Click **Traffic Details** to view the Traffic Details for an entity.

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

7. Select a number to change the number of items in the table. Click the arrow to go to a particular page.
   In the lower-right corner, the numbers that are displayed are the number of interfaces to be displayed on each page.

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

**Results**

Any interface that is violating the new 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.

## 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**

You can configure and resolve the domain names by using this procedure.
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.

For more information, see Data storage section in Network Performance Insight overview IBM.
To configure or resolve:

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 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 icon to refresh the list of domains.

7. Click 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 to change the number of items in the table from the lower-right corner. The numbers that are displayed are the number of items to be displayed on each page.

9. Click the arrow to go to a particular page.

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

What to do next

You can repeat the same process to enable and configure 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 3. Introduction to visualization dashboards

A dashboard is a user interface that helps you visualize data. These dashboards are interactive and display metrics and data. They can pull real-time data from all the sources.

Dashboards are a means of displaying various types of data from different sources onto a single page, which can be useful for tracking status, progress, and activity at a glance.

IBM Network Performance Insight visualization allows built-in and interactive dashboards that cover the entire traffic data representation.

Features of Network Performance Insight visualization dashboards

Visualization dashboards that are available in IBM Network Performance Insight help network administrators to configure and monitor routers and switches for any anomalies in network traffic. The main focus is to contain congestion and abuse.

Network Performance Insight visualization provides rich and adaptive features to display real time or near real-time dashboards, for quick analysis of data. The visualization features and capabilities are as follows:

Near real-time flow monitoring
- Analyze the network traffic patterns and resolve network performance issues with the help of interactive dashboards.
- Detects which applications are hogging maximum bandwidth.
- Simplified reports on detailed traffic data over a specified time period.

Ready to use traffic details dashboard
- Ten network topology level dashboards for top 10 talkers.
- Fifteen top ten views that show the interface level details.

Bandwidth consumption by applications
- Detects top applications usage of bandwidth.
- Monitors their ports.

Thresholding and alerting
- Traceable alerts are sent instantly when an interface crosses the pre-configured threshold value.
- Helps to drill-down to the interface that exceeds its threshold value.

Historical data
Configurable flow data from a specific date or time to view activity and problems in the captured data.

Filtering flow data
- Ability to filter across records
- Ability to filter flows by the following traffic data views:
  - Top Sources
  - Top Sources with Application
  - Top Applications
- Top Applications with Source
- Top Applications with Conversation
- Top Applications with Destination
- Top Protocols
- Top Protocols with Source
- Top Protocols with Application
- Top Protocols with Conversation
- Top Protocols with Destination
- Top Conversations
- Top Conversations with Application
- Top Destinations
- Top Destinations with Application

**Built in DNS name resolution**
Performs DNS forward and reverse resolutions.

---

**Available Dashboards**

A dashboard is an arrangement of one or more widgets in the work area and contain the widgets that are needed to complete tasks.

A dashboard provides a simplified view of data in widgets. A widget is a graphical representation of information, which is designed to provide a quick overview of statistics, or other important information. The variety of widgets available to add to dashboards is dependent upon Dashboard Type.

Following is the main dashboard that is available in Network Performance Insight 1.1.1:

**Traffic Details**
Displays the traffic details at interface and network level.

For more information about the Traffic Details dashboard, see “Monitoring Traffic Details dashboard” on page 17.
Chapter 4. Traffic Details dashboard

You can view the traffic details of a particular interface in your network.

Start the Traffic Details dashboard from one of the following ways:

- Click Incident (play button) in the navigation bar and select Network Health Dashboard under Network Availability.
  - The traffic details for an interface are populated in the Network View page, from a selected network view.

- Click Incident (play button) in the navigation bar and select Active Event List (AEL) or Event Viewer under Events.
  - Right-click any event from the Event Viewer or the AEL and select NPI Flow, to view the traffic details for the event.

Note: The NPI Flow option is the launch-in-context tool created for Network Performance Insight. For more information, see Configuring launch-in-context integration with Network Performance Insight in Network Performance Insight integrations.

- Click Console Integrations (play button) in the navigation bar and select Interfaces or Thresholds under System Configuration.
  - Click Traffic Details to view the traffic details for an Interface.

Discovering networks

Using Network Manager, you can discover your network and schedule regular discoveries to ensure that your network topology stays up to date.

After Network Manager is installed, configure and verify your network discovery to produce the most complete and accurate network topology possible for the devices and technologies in your network. An accurate network topology facilitates efficient root-cause analysis of network problems.

You can configure how your network is discovered, including which kinds of devices you want to discover, and where the boundaries of the discovery must be.

Configuring the network discoveries

Network Manager provides tools for discovering your network that uses a phased approach.

About this task

You can edit the topology after discovery is complete by using the topology management features in the Network Hop View. Use these tools to configure your network discoveries:

- Use the Discovery Configuration Wizard to perform initial discoveries.
The wizard provides a guided discovery and makes configuration choices for you based on the answers that you provide as you work through the wizard.

- Use the Discovery Configuration GUI to perform subsequent discoveries.

  Using the GUI you can configure detailed discovery settings, including scope, seeds, community strings, agent selection, and many other configuration settings.

**Note:** If you are an experienced user of Network Manager, you can also configure a discovery by using the discovery configuration files and the command line.

**Procedure**

1. **Plan for the discovery**
   
   Before you configure and run a discovery, you must check several system settings, parameters, and requirements.

2. **Configure standard discoveries**
   
   You can configure discovery by using the Discovery Configuration Wizard, by using the Discovery Configuration GUI, or by using the command line.

3. **Configure specialized discoveries**
   
   You can configure the system to perform more complex discoveries, such as MPLS and NAT discovery.

**Related information:**

- Getting started with discovery
- Discovering the network

---

**Setting up network for visualizations**

To set up network visualization, follow these administration tasks.

**About this task**

You can set up Network Views for your operators, and configure users, roles, and groups. Run some of these tasks before you work with your Network Health Dashboard.

**Procedure**

1. **Administer the GUI framework**
   
   Use the functions of the Dashboard Application Services Hub within Jazz for Service Management to administer pages, folders, views, widgets, and console preference profiles.

2. **Administer network views**
   
   Network Views widget shows logical groupings of devices that you might need to monitor within your network. Create new views or change existing views to help network operators visualize devices.

3. **Administer network view bookmarks**
   
   Network view bookmarks group just those network views that you or your team need to monitor. Create new bookmarks or change existing bookmarks to help network operators visualize just those devices that they need to monitor.

4. **Configure tools and menus**
You can create and edit menus, configure user access to menu items, define the context in which menus are available, and create tools that can be run from the menus.

5. **Editing network topology**
   Edit the discovered network topology to manually add and remove devices and connections.

---

**Network Health Dashboard**

IBM Networks for Operations Insight is an optional feature that can be added to a deployment of the base IBM Netcool Operations Insight solution to provide service assurance in dynamic network infrastructures. The capabilities of Networks for Operations Insight include network discovery, visualization, event correlation and root-cause analysis, and configuration and Compliance Management that provide service assurance in dynamic network infrastructures.

The Networks for Operations Insight capability is provided through setting up the following products in Netcool Operations Insight:
- IBM Tivoli Network Manager
- IBM Tivoli Netcool Configuration Manager

**Note:** Currently, Network Performance Insight does not integrate with Netcool Configuration Manager and works independent of Netcool Configuration Manager.

Network Health Dashboard is one of the main features that is provided by the Networks for Operations Insight solution. The Network Health Dashboard is only available if you have Network Manager as part of Netcool Operations Insight.

The Network Health Dashboard monitors a selected network view, and displays device and interface availability within that network view. It also reports on performance by presenting graphs, tables, and traces of KPI data for monitored devices and interfaces.

Traffic Details dashboard can also be started for the interfaces that are available in the Structured Browser.

The dashboard includes the event viewer, for more detailed event information. You can start the Traffic Details dashboard to display the NetFlow traffic details for the interface that violated the set threshold value.

Related information:

- [IBM Networks for Operations Insight](#)

**Getting started with Network Health Dashboard**

Perform these tasks for efficient usage Network Health Dashboard.

**Procedure**

1. **Administer the Network Health Dashboard**
   You can configure and maintain the Network Health Dashboard for users.

2. **Develop custom dashboards**
You can create pages and place the various widgets that are provided with Network Manager, Tivoli Netcool/OMNibus Web GUI, Network Performance Insight, and other integrated products that are deployed in your Dashboard Application Services Hub environment.

3. **Monitor the network by using the Network Health Dashboard**
   
   You can use the Network Health Dashboard to determine any network issues, and how to navigate from the dashboard to other parts of the product for more detailed information.

### Structure Browser

Structure Browser is one of the Network Manager widgets that are available to add to a page. Use the Structure Browser to view the internal structure of the device and investigate the health of the device components. You can then isolate a fault within a network device.

The Structure Browser has two modes; tree and table. You can change the Structure Browser from tree mode to table mode by editing the portlet preferences. You can specify the default mode for the Structure Browser by using the configuration files. You can use the Structure Browser from the following views:

- **Network Hop View**
  Network visualization GUI. Use the Network Hop View to search the network for a specific device and display a specified network device. You can also use the Network Hop View as a starting point for network troubleshooting. Formerly known as the Hop View.

- **Network Views**
  Network visualization GUI that shows hierarchically organized views of a discovered network. Use the Network Views to view the results of a discovery and to troubleshoot network problems.

- **Event list**
  You can view the events list in Event Viewer and Active Event List.

**Related information:**

- [List of Network Manager widgets](#)
- [About the Structure Browser](#)

### Traffic Details from Network Health dashboard

Network Health Dashboard displays the traffic details of a particular network.

The Traffic Details widget data is populated from NCIM view that is part of Network Performance Insight database structure, where it joins multiple tables into a single virtual table.

NCIM view represents the subset of data discovered from the Tivoli Network Manager and Network Performance Insight Flow tables.

The discovered data by Tivoli Network Manager is mapped with Flow records by using the following fields:

**Table 1. Mappings table**

<table>
<thead>
<tr>
<th>Flow table</th>
<th>NCIM view</th>
</tr>
</thead>
<tbody>
<tr>
<td>exporter ip</td>
<td>device ip address</td>
</tr>
</tbody>
</table>
Table 1. Mappings table (continued)

<table>
<thead>
<tr>
<th>Flow table</th>
<th>NCIM view</th>
</tr>
</thead>
<tbody>
<tr>
<td>if index</td>
<td>interface index</td>
</tr>
</tbody>
</table>

The following SNMP fields in the Traffic Details widget are populated from the NCIM view:

**Note:** If the discovered interfaces are not mapped with Network Performance Insight flow data, you can’t see the SNMP fields in the table on Traffic Details dashboard.

Table 2. SNMP fields in Traffic Details dashboard

<table>
<thead>
<tr>
<th>Traffic Details fields</th>
<th>Description</th>
<th>Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>The device name.</td>
<td>The exporter ip from Flow table is mapped to the device name in the NCIM view. This mapping results to the device name populated in the traffic details widget.</td>
</tr>
<tr>
<td>Index</td>
<td>A unique identifying number associated with the physical or logical interface.</td>
<td>The if index from Flow table is mapped to the interface index from in the NCIM view. This mapping results to the index value populated in the traffic details widget.</td>
</tr>
<tr>
<td>Description</td>
<td>The interface name.</td>
<td>The interfaces that are discovered by Tivoli Network Manager are mapped with the collected Network Performance Insight flow data as interface name. This mapping results to the description of the device populated in the traffic details widget.</td>
</tr>
<tr>
<td>Speed</td>
<td>The value of the traffic flow through network interfaces, which measures the speed of the data transferred.</td>
<td>The speed from Flow table is mapped to the interface speed from NCIM view. This mapping results to the speed value populated in the traffic details widget.</td>
</tr>
</tbody>
</table>

Related concepts:

“Traffic Details dashboard views” on page 19

Views give you details about Traffic Details reports at network and interface level.

Adding Network Performance Insight widget in Network Health dashboard

Dashboards or pages, are an arrangement of one or more widgets in the work area and contain the widgets that are needed to complete tasks. Users whose roles have Editor or Manager access to a dashboard can edit a dashboard’s layout and content. You can add multiple widgets in a screen. When you are adding widgets, you can also rearrange the widgets as needed.
About this task

By default, the Network Health Dashboard page displays the Network View, Structure Browser, and Event Viewer widgets.

To view the traffic details from Network Health Dashboard for the first time, you need to add the Network Performance Insight widget.

Procedure

1. Log in to Jazz for Service Management server.

2. Click the Incident icon ( ) and select Network Health Dashboard under Network Availability.

3. In the Network Health Dashboard, select a network view.
   A second tab, called Network View, opens.

4. In the tab bar, click Page Actions icon ( ) and select Edit Page.
   The dashboard is changed to show the widget palette and a series of buttons in the tab bar. The menu that is associated with the Edit options icon for each widget is updated so that you can edit its layout and content.

5. Click the NPI folder from the widget palette.
   The NPI folder name is based on the launch-in-context tool created for Network Performance Insight. For more information, see Configuring launch-in-context integration with Network Performance Insight in Integrating Network Performance Insight.

6. Click and drag the Traffic Details widget from the palette.
   To assist you in positioning the widget, use the background layout grid. You can change the size of the layout grid and have widgets snap to the layout guide lines through the Layout button in the tab bar.

7. Click Save and Exit to exit the dashboard from the edit mode, after you complete editing.

Related tasks:

“Monitoring Traffic Details from Network Health dashboard”

The Traffic Details widget displays the details of an interface from a selected network device.

Related information:

Editing dashboard content and layout

Monitoring Traffic Details from Network Health dashboard

The Traffic Details widget displays the details of an interface from a selected network device.

About this task

Browse from Network Health dashboard to view the specific traffic details of an interface in the Traffic Details page.

By default, the Traffic Details page displays the details for Top Ingress interfaces at Ingress level, Top Egress interfaces at Egress level. Whereas, Top Interfaces and all Top Networks display the traffic details as Both.
Procedure

1. Log in to Jazz for Service Management server.

2. Click the Incident icon and select Network Health Dashboard under Network Availability.
   The dashboard page populates the configured network devices.

3. Select a view from the Network Views bookmark that you configured from the Network Health Dashboard.
   The other widgets update to show information based on the network view that you selected.
   The Network View dashboard opens in another tab. This dashboard contains Network Views GUI, the Event Viewer, the Structure Browser, and the Traffic Details, and it displays the selected network view.

4. Double-click a network from the Network View.
   For example, double-click All Routers.

5. Click an entity or device from the Network View.
   The selected entity details are displayed on the Structure Browser.

6. Click the Show Interfaces icon from the Structure Browser.
   List of interfaces for the entity is displayed.

7. Click an interface.
   The traffic details data with the interface details is displayed on the Traffic Details.

8. Select an entity from View list.
   For information on monitoring traffic details, see “Monitoring Traffic Details dashboard.”

9. Optional: Click the Maximize icon from the upper right of the Traffic Details widget.
   The traffic details dashboard is displayed in full screen mode.

Related tasks:
“Getting started with Network Health Dashboard” on page 13
Perform these tasks for efficient usage Network Health Dashboard.

Monitoring Traffic Details dashboard

The Traffic Details dashboard displays the details at an interface level or at a network level.

About this task

By default, the Traffic Details page displays the details for Top Ingress interfaces at Ingress level, Top Egress interfaces at Egress level. Whereas, Top Interfaces and all Top Networks display the traffic details as Both.

Procedure

1. Select Traffic Details for Ingress, Egress, or Both from the list.
2. Select any dashboard view from the View list.
For more information about dashboard views, see “Traffic Details dashboard views” on page 19.

3. Click 🕒 to select a start date from the **Start** field.

4. Click 🕒 to select start time.

5. Click 🕒 to select an end date from the **End** field.

6. Click 🕒 to select end time.

7. Click **Update** to update the details for selected date and time.
   Two red lines are displayed in the graph that notify the Upper Threshold and Lower Threshold limits are crossed. When you hover over the area charts, a tooltip is flashed giving you the details for that particular source.
   For more information about aggregated data for a specific duration, see Data storage section in Network Performance Insight overview. The graphical presentation of data is updated for the selected date and time.

8. Click 🔄 to refresh the page.

9. Select one or more interfaces from the legend on the right.
   It displays the top 10 interface details.

10. Optional: Clear a particular interface from the check-box.
    The details for that interface are hidden.

11. Optional: Check the **Remaining** check box.
    It displays the details for the remaining traffic on the interfaces.

**Note:** If the upper limit and lower limit of a threshold is crossed, two extra check boxes for Upper Threshold and Lower Threshold are seen in the legend.

The table at the bottom displays top 10 interface details. The table displays the following details for an interface:

**Rank**   Display the number in ascending order.

**Grouping**
Displays the interface for which you are viewing the data. For example, if you select Top Protocols from the View list, the grouping that is displayed is for Protocol.

The columns change depending on the view selected. The main grouping keys for the Traffic Details dashboard can be defined as:

<table>
<thead>
<tr>
<th>Grouping Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>It is a standard that is defined on how a network conversation is established. It delivers the packets from the source host to the destination host.</td>
</tr>
<tr>
<td>Source</td>
<td>Each data series in the donut chart represents the source that is sending the traffic.</td>
</tr>
<tr>
<td>Application</td>
<td>Applications are mapped based on port, protocol, and IP address or network.</td>
</tr>
<tr>
<td>Destination</td>
<td>Destination can be a host computer to which the network flow comes from a source computer.</td>
</tr>
</tbody>
</table>

**Octets**   Displays the amount of data that is used in KB and Bytes.
Percentage
Percentage of traffic on the grouping that occupies the traffic.

Note: If the top 10 interface table is not shown, reduce the zoom percentage of your current browser.

Traffic Details dashboard views
Views give you details about Traffic Details reports at network and interface level.

The dashboard View list displays the following views:

**Top Sources**
Displays the details about top Sources for a particular entity. The report shows the top-most sources for ingress, egress and both. The table at the bottom displays the following details.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Source</td>
<td>Identity of the source.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data used in KB, Bytes, and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

**Top Sources with Application**
Displays the traffic details for top Sources and top Application. The reports show the conversation between top most source and applications for ingress, egress, and both.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Source</td>
<td>Identity of the source.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data that is utilized in KB, Bytes, and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

**Top Applications**
Displays the traffic details for top Applications. The reports show the top-most Applications for ingress, egress and both.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data that is utilized in KB, Bytes, and so on.</td>
</tr>
</tbody>
</table>
Table 6. APPLICATION_NAME (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

Top Applications with Source

Displays the details about top Applications with top Sources for a particular entity. The report shows the conversation between top most applications and sources for ingress, egress and both. The table at the bottom displays the following details.

Table 7. APPLICATION_NAME + SOURCE_IP

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Source</td>
<td>Identity of the source.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data that is utilized in KB, Bytes, and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

Top Applications with Destination

Displays the traffic details for top Applications with top Destinations for a particular entity. The reports show the conversation between top most Applications and Destinations for ingress, egress and both.

Table 8. APPLICATION_NAME + DESTINATION_IP

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Destination</td>
<td>Identity of the destination.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data that is utilized in KB, Bytes, and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

Top Applications with Conversation

Displays the traffic details for top Applications with top Destinations. The reports show the conversation between top most Applications, Sources, and Destinations for ingress, egress and both.

Table 9. APPLICATION_NAME + SOURCE_IP + DESTINATION_IP

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Source</td>
<td>Identity of the source.</td>
</tr>
<tr>
<td>Destination</td>
<td>Identity of the destination.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data that is utilized in KB, Bytes, and so on.</td>
</tr>
</tbody>
</table>
Table 9. APPLICATION_NAME + SOURCE_IP + DESTINATION_IP (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

**Top Protocols**
Displays the traffic details for top Protocols. The reports show top most Protocols for ingress, egress and both.

Table 10. PROTOCOL_ID

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Identity of the protocol.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data that is utilized in KB, Bytes, and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

**Top Protocols with Source**
Displays the traffic details for top Protocols with top Sources. The reports show the conversation between top most Protocols with Sources for ingress, egress and both.

Table 11. PROTOCOL_ID + SOURCE_IP

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Identity of the protocol.</td>
</tr>
<tr>
<td>Source</td>
<td>Identity of the source.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data that is utilized in KB, Bytes and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping which occupies the traffic.</td>
</tr>
</tbody>
</table>

**Top Protocols with Application**
Displays the traffic details for top Protocols with top Applications. The reports show the conversation between top most Protocols with Applications for ingress, egress and both.

Table 12. PROTOCOL_ID + APPLICATION_NAME

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Identity of the protocol.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data utilized in KB, Bytes and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping which occupies the traffic.</td>
</tr>
</tbody>
</table>

**Top Protocols with Conversation**
Displays the traffic details for top Protocols with top conversations. The
reports show the conversation between top most applications, sources, and destinations for ingress, egress and both.

**Table 13. PROTOCOL_ID + SOURCE_IP + DESTINATION_IP**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Identity of the protocol</td>
</tr>
<tr>
<td>Source</td>
<td>Identity of the source</td>
</tr>
<tr>
<td>Destination</td>
<td>Identity of the destination</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data utilized in KB, Bytes and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping which occupies the traffic.</td>
</tr>
</tbody>
</table>

**Top Protocols with Destination**

Displays the traffic details for top Protocols with top Destinations. The reports show the conversation between top most Protocols and top most Destinations for ingress, egress and both.

**Table 14. PROTOCOL_ID + DESTINATION_IP**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Identity of the protocol</td>
</tr>
<tr>
<td>Destination</td>
<td>Identity of the destination</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data utilized in KB, Bytes and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping which occupies the traffic.</td>
</tr>
</tbody>
</table>

**Top Conversations**

Displays the traffic details for top Conversations for a particular entity. The reports show the top most conversations for ingress, egress and both.

**Table 15. SOURCE_IP + DESTINATION_IP**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Source</td>
<td>Identity of the source</td>
</tr>
<tr>
<td>Destination</td>
<td>Identity of the destination</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data used in KB, Bytes, and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

**Top Conversations with Application**

Displays the traffic details for top Conversations and top Application. The reports show the conversation between top most source, destination, and applications for ingress, egress and both.
Table 16. SOURCE_IP + DESTINATION_IP + APPLICATION_NAME

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Source</td>
<td>Identity of the source.</td>
</tr>
<tr>
<td>Destination</td>
<td>Identity of the destination.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data used in KB, Bytes, and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

Top Destinations
Displays the traffic details for top Destinations for a particular entity. The reports show the top-most Destinations for ingress, egress and both.

Table 17. DESTINATION_IP

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Destination</td>
<td>Identity of the destination.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data that is utilized in KB, Bytes, and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>

Top Destinations with Application
Displays the traffic details for top Destinations with top Application. The reports show the conversation between top most Destinations and Applications for ingress, egress, and both.

Table 18. DESTINATION_IP + APPLICATION_NAME

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rank</td>
<td>Displays the number in ascending order.</td>
</tr>
<tr>
<td>Application</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Destination</td>
<td>Identity of the destination.</td>
</tr>
<tr>
<td>Octets</td>
<td>Displays the amount of data that is utilized in KB, Bytes, and so on.</td>
</tr>
<tr>
<td>Percentage</td>
<td>Percentage of traffic on the grouping that occupies the traffic.</td>
</tr>
</tbody>
</table>
Monitoring events from Web GUI on Dashboard Application Services Hub

You can monitor and manage Tivoli Netcool/OMNibus by using the Web GUI that is started on the reporting interface of Jazz for Service Management.

**About this task**

You can access the events from:

- **Managing events in the Event Viewer**
  
  Use the JavaScript Event Viewer to monitor and manage events. You can access Event Viewers in any page in Dashboard Application Services Hub that hosts an Event Viewer widget.

- **Monitoring events in Active Event Lists**
  
  The Active Event List (AEL) is an interactive Java applet for displaying alert data from the ObjectServer. Communication between the ObjectServer and the AEL is bidirectional. The AEL presents alert information from the alerts.status table in the ObjectServer to operators. Operators can perform actions against alerts such as changing the results from the alert properties in the alerts.status table from the AEL.

**Procedure**

1. Log in to Jazz for Service Management server.
   
   See “Logging in to the Dashboard Application Services Hub portal” on page 1

2. In the navigation bar, click **Incident** > Events > **Active Event List (AEL)**.

3. Right-click any event from the Active Event List (AEL) page and select **Flow Dashboard**.

   The Traffic Details report associated with the selected event is displayed in another window.

4. Optional: In the navigation bar, click **Incident** > Events > **Event Viewer**.

5. Right-click any event from the **Event Viewer** page and select **Flow Dashboard**.

   The Traffic Details report associated with the selected event is displayed in another window.

**Related information:**

- Monitoring events in the Web GUI
Event severity levels

A severity level is associated with each generated alert to help you to prioritize and manage alerts in the Event list. Severity levels are color-coded for easy identification.

There are six default severity levels, as shown in the following table.

<table>
<thead>
<tr>
<th>Level</th>
<th>Threshold type</th>
<th>Color</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Clear</td>
<td>Green</td>
</tr>
<tr>
<td>1</td>
<td>Intermediate</td>
<td>Gray</td>
</tr>
<tr>
<td>2</td>
<td>Warning</td>
<td>Blue</td>
</tr>
<tr>
<td>3</td>
<td>Minor</td>
<td>Yellow</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Orange</td>
</tr>
<tr>
<td>5</td>
<td>Critical</td>
<td>Red</td>
</tr>
</tbody>
</table>

You can customize the event data and how the event data is displayed.

Related information:

[Customizing event displays in the Web GUI]
Chapter 5. Troubleshooting visualizations

Problems that might occur during network visualizations and how to resolve them.

About this task

For all troubleshooting issues in Network Performance Insight dashboards, see Troubleshooting Network Performance Insight.
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.
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.
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 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.