

IBM Netcool Operations Insight
Version 1 Release 4.0.5

Integration Guide



Note

Before using this information and the product it supports, read the information in “Notices” on page 303.

This edition applies to version 1, release 4 of IBM Netcool Operations Insight (product number 5725-Q09) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2014, 2017.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this publication v

Accessing terminology online. v

Tivoli technical training. v

Typeface conventions v

Solution overview 1

Supported products and components 3

Deployment considerations 8

Deployment considerations for Netcool/OMNIBus
and the connection to Operations Analytics - Log
Analysis 8

Deployment considerations for the Networks for
Operations Insight feature 15

Ports used by products and components. 15

Data flows. 16

Data flows for the base Netcool Operations
Insight solution 17

Networks for Operations Insight data flow 19

Which documentation do I need? 24

Installing Netcool Operations Insight 27

Quick reference to installing. 27

Performing a fresh installation 32

Checking prerequisites. 34

Obtaining IBM Installation Manager 36

Installing Installation Manager (GUI or console
example) 38

Installing Netcool/OMNIBus and
Netcool/Impact 40

Installing DB2 and configuring the REPORTER
schema 41

Installing IBM Operations Analytics - Log
Analysis 42

Configuring the Gateway for JDBC and Gateway
for Message Bus 43

Installing Dashboard Application Services Hub
and the UI components 44

Installing the Networks for Operations Insight
feature 46

Installing the Insight Packs 79

Installing Network Performance Insight and
configuring integration with Netcool Operations
Insight 82

Installing and configuring the Device Dashboard

Configuring Single Sign-On 84

Getting started with Netcool Operations Insight 85

Upgrading to the latest Netcool Operations Insight. 87

Quick reference to upgrading 87

Upgrading Netcool Operations Insight 89

Event search 93

Configuring event search. 94

Configuring single sign-on for the event search

capability 97

Customizing event management tools 98

Adding custom apps to the Table View toolbar 101

Searching for events 102

Event search workflow for operators 105

Troubleshooting event search 106

Event Analytics 111

Event Analytics overview 111

Installing and uninstalling Event Analytics 112

Prerequisites. 112

Installing Event Analytics 113

Uninstalling Event Analytics 129

Configure Analytics portlet. 131

Setting the Impact data provider and other
portlet preferences. 133

Viewing current analytics configurations 134

Creating a new or modifying an existing
analytics configuration 136

Manually running an unscheduled analytics
configuration 138

Stopping an analytics configuration 139

Deleting an analytics configuration 139

Changing the expiry time for related events
groups 140

Changing the choice of fields for the Event
Identity 141

View Seasonal Events portlet 142

Viewing a list of seasonal event configurations
and events 143

Reviewing a seasonal event. 143

Sorting columns in the View Seasonal Events
portlet. 144

Exporting all seasonal events for a specific
configuration to Microsoft Excel 145

Exporting selected seasonal events for a specific
configuration to Microsoft Excel 145

Seasonal Event Rules. 146

Creating a seasonal event rule. 146

Seasonal event rule states 150

Modifying the default seasonal event rule
expiry time 151

Viewing performance statistics for seasonal
event rules 152

Modifying an existing seasonal event rule. 153

Viewing seasonal event rules grouped by state 153

Modifying a seasonal event rule state 154

Applying rule actions to a list of events 155

Setting the column value for an event 156

Updating the NOI_DefaultValues properties file
to suppress and unsuppress events 157

Seasonal Event Graphs 158

Viewing seasonal event graphs for a seasonal
event 159

Viewing historical events from seasonality graphs.	159
Exporting seasonal event graphs for a specified seasonal event to Microsoft Excel.	160
Editing confidence thresholds of Seasonal Event Graphs	161
Historical events	162
Viewing historical events for a seasonal event	163
Exporting historical event data	163
Exporting historical event data for a specified seasonal event to Microsoft Excel.	164
Related events	165
Work with related events	166
Extra details about related events.	174
Correlation rules and related events.	179
Creating patterns	184
Starting the Events Pattern portlet	185
Creating an event pattern	186
Applying a regular expression to the pattern criteria	188
Editing a pattern criteria regular expression	189
Viewing related event details in the Events Pattern portlet	190
Editing an existing pattern	190
Deleting an existing pattern	191
Exporting pattern generalization test results to Microsoft Excel.	191
Configuring the type properties used for event pattern creation in Netcool/Impact	192
Reference.	199
Netcool/Impact installation components	199
Configuring the Event Analytics ObjectServer	199
Configuring Oracle database connection within Impact	200
Configuring DB2 database connection within Impact	202
Configuring MS SQL database connection within Impact	204
Netcool/Impact remote connection	206
Generated properties file	206
Adding a cluster to the Netcool/Impact environment.	212
Extra failover capabilities	213
Viewing historical events in the Event Viewer	214
Understanding the timeline chart.	215
Troubleshooting Event Analytics	215
Event relationships display in the Event Viewer, only if the parent and child events match the filter	224

IBM Networks for Operations Insight	227
Network Health Dashboard	227
Administering the Network Health Dashboard	227
Developing custom dashboards	233
Monitoring the network using the Network Health Dashboard.	241
Device Dashboard.	252
Troubleshooting network issues using the Device Dashboard.	252
Configuring the Performance Insights widget	258
Configuring thresholds	259
Monitoring traffic flow	263
Traffic Details dashboard	263
Traffic Details from Network Health Dashboard	270
Monitoring network performance from Event Viewer	273

Topology search	275
Supported products and components	276
Configuring topology search	276
Configuring single sign-on for the topology search capability	279
Searching the topology	280

Configuring integration to IBM Connections	283
IBM Connections Overview	283
Parameters for the IBMConnections function	284
IBMConnections Project and artifacts.	286
Automatic topic management	287
Automatic topic management with event management tools.	288
Enabling historical events	288

Release notes	289
--------------------------------	------------

Creating your own PDF of a subset of topics using My Collections	301
---	------------

Notices	303
Trademarks	304

About this publication

This guide contains information about how to integrate the components of the IBM Netcool Operations Insight solution.

The guide is set up by scenario and not meant to be read in its entirety, read only the scenario that you are interested in. For more information, see “Which documentation do I need?” on page 24.

Accessing terminology online

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

<http://www.ibm.com/software/globalization/terminology>.

Tivoli technical training

For Tivoli® technical training information, refer to the following IBM® Tivoli Education Web site at <http://www.ibm.com/software/tivoli/education>.

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 that 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

Solution overview

IBM Netcool Operations Insight leverages real-time alarm and alert analytics, combined with broader historic data analytics. Netcool Operations Insight is powered by the fault management capabilities of IBM Tivoli Netcool/OMNIBus and IBM's leading big data technologies within IBM Operations Analytics - Log Analysis, providing powerful event search and historical analysis in a single solution.

Netcool Operations Insight consists of a base solution for managing and analyzing application monitoring environments and also an optional extension called Networks for Operations Insight, which widens the scope to include network discovery, visualization, event correlation, topology-based root-cause analysis, and configuration and compliance management. The Networks for Operations Insight capability is provided through the Network Manager and Netcool Configuration Manager products.

In addition, you can also set up IBM Network Performance Insight as part of your Netcool Operations Insight solution to monitor network traffic performance, and you can integrate with further solutions such as IBM Alert Notification and IBM Runbook Automation.

Netcool Operations Insight integrates infrastructure and operations management into a single coherent structure across business applications, virtualized servers, network devices and protocols, internet protocols, and security and storage devices.

Netcool Operations Insight includes the following capabilities.

Event search

Event search applies the search and analysis capabilities of Operations Analytics - Log Analysis to events that are monitored and managed by Tivoli Netcool/OMNIBus. Events are transferred from the ObjectServer through the Gateway for Message Bus to Operations Analytics - Log Analysis, where they are ingested into a datasource and indexed for searching. After the events are indexed, you can search every occurrence of real-time and historical events. The Tivoli Netcool/OMNIBus Insight Pack is installed into Operations Analytics - Log Analysis and provides custom apps that search the events based on various criteria. The custom apps can generate dashboards that present event information to show how your monitoring environment is performing over time. Keyword searches and dynamic drilldown functions allow you to go deeper into the event data for detailed information. The apps can be run from the Operations Analytics - Log Analysis. Tooling can be installed into the Web GUI that launches the apps from the right-click menus of the Event Viewer and the Active Event List. An “event reduction wizard” is also supplied that includes information and apps that can help you analyze and reduce volumes of events and minimize the “noise” in your monitored environment.

For more information, see “Event search” on page 93.

Event Analytics

Event Analytics performs statistical analysis of Tivoli Netcool/OMNIBus historical event data.

- It can identify seasonal patterns, such as when, and how frequently events occur. Seasonality analyses are output in reports and graphs so that you can find seasonal patterns. For example, an event that periodically occurs at an unscheduled specific time is highlighted. You can use the information from the seasonality reports to create network, device, or suppression rules to reduce the number of events.
- It can determine which events have a statistical tendency to occur together and output the results on a scheduled basis as event groups. You can deploy valid event groups as Netcool/Impact correlation rules. The rules act on the event data and show a single parent event from the event group, with all other events in the group as children. This reduces the number of events that are presented to operators.

Event Analytics is installed as two separate packages. One is installed into Netcool/Impact and the other is installed into the Netcool/OMNIBus Web GUI. Both are required for Event Analytics to work.

For more information, see “Event Analytics” on page 111.

Networks for Operations Insight

Networks for Operations Insight is an optional feature that can be added to a deployment of the base 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. It contributes to overall operational insight into application and network performance management. The Networks for Operations Insight capability is provided through the Network Manager and Netcool Configuration Manager products.

For more information, see “IBM Networks for Operations Insight” on page 227.

Topology search

The topology search capability is an extension of the Networks for Operations Insight feature. It applies the search and analysis capabilities of Operations Analytics - Log Analysis to give insight into network performance. Events that have been enriched with network data are analyzed by the Network Manager Insight Pack and are used to calculate the lowest-cost routes between two endpoints on the network topology over time. The events that occurred along the routes over the specified time period are identified and shown by severity. The topology search requires the Networks for Operations Insight feature to be installed and configured.

For more information, see “Topology search” on page 275.

IBM Connections integration

Netcool/Impact enables social collaboration through IBM Connections by automatically providing updates to key stake holders. It provides integration to IBM Connections by using a Netcool/Impact IBMConnections action function. The IBMConnections action function allows users to query forums and topics lists, create a new forum, create a new topic, and update existing topics. IBM Connections is a leading social software platform that can help your organization to engage the right people, accelerate innovation, and deliver results. This integrated, security-rich platform helps people engage with networks of experts in the context of critical business processes. Now everyone can act with confidence and anticipate and respond to emerging opportunities.

For more information, see “Configuring integration to IBM Connections” on page 283.

Network performance monitoring

Network Performance Insight is a flow-based network traffic performance monitoring system. It provides comprehensive and scalable visibility on network traffic with visualization and reporting of network performance data for complex, multivendor, multi-technology networks. For more information, see <http://www-01.ibm.com/support/knowledgecenter/SSCVHB/welcome>.

IBM Alert Notification

IBM Alert Notification provides instant notification of alerts for any critical IT issues across multiple monitoring tools. It gives IT staff instant notification of alerts for any issues in your IT operations environment. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSY487/com.ibm.netcool_OMNIBusaas.doc_1.2.0/landingpage/product_welcome_alertnotification.html.

IBM Runbook Automation

IBM Runbook Automation empowers IT operations teams to be more efficient and effective. Operators can focus their attention where it is really needed and receive guidance to the best resolution with recommended actions and pre-filled context. With Runbook Automation you can:

- Investigate and delegate problems faster and more efficiently.
- Diagnose and fix problems faster and build operational knowledge.
- Easily create, publish, and manage runbooks and automations.
- Keep score to track achievements and find opportunities for improvement.

For more information, see http://www-01.ibm.com/support/knowledgecenter/SSZQDR/com.ibm.rba.doc/RBA_welcome.html.

Related reference:

“Release notes” on page 289

Supported products and components

Review the products and components included in Netcool Operations Insight.

IBM Netcool Operations Insight V1.4.0.5 includes the product and component versions listed in the following table. Detailed descriptions of each of these components is provided following the table.

Table 1. Netcool Operations Insight V1.4.0.5 product and component versions

Product or component	Netcool Operations Insight V1.4.0.5 (April 2017 GA release)	Change from previous version?
		Netcool Operations Insight V1.4.0.4 (March 2017 GA release)
IBM Tivoli Netcool/OMNIBus core components	V8.1.0.11 (V8.1 fix pack 11)	No
Tivoli Netcool/OMNIBus Web GUI	V8.1.0.9 (V8.1 fix pack 9)	No
IBM Tivoli Netcool/Impact	V7.1.0.9 (V7.1 fix pack 9)	No

Table 1. Netcool Operations Insight V1.4.0.5 product and component versions (continued)

Product or component	Netcool Operations Insight V1.4.0.5 (April 2017 GA release)	Change from previous version? Netcool Operations Insight V1.4.0.4 (March 2017 GA release)
Operations Analytics - Log Analysis	V1.3.5 V1.3.3.1 (V1.3.3 fix pack 1) V1.3.3	No
Event Analytics	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.9 (delivered in Netcool/Impact fix pack) IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI 8.1.0.9 (delivered in Web GUI fix pack)	No
Event Search	Tivoli Netcool/OMNIBus Insight Pack V1.3.0.2 (delivered in Operations Analytics - Log Analysis)	No
Topology Search	Network Manager Insight Pack V1.3.0.0 (delivered in Operations Analytics - Log Analysis)	No
IBM Tivoli Network Manager IP Edition	V4.2.0.3 (V4.2 fix pack 3)	Yes
Device Dashboard	V1.1.0.1 (V1.1 fix pack 1)	No
Network Health Dashboard	V4.2.0.3 (V4.2 fix pack 3)	Yes
IBM Tivoli Netcool Configuration Manager	V6.4.2.4 (V6.4.2 fix pack 4)	Yes
IBM Network Performance Insight	V1.2.0	No
Jazz for Service Management	V1.1.3.0 with Cumulative Patch 1	No
WebSphere Application Server	V8.5.5.9, or later	No

Product and component details

Tivoli Netcool/OMNIBus core components V8.1.0.11

This product includes the following components. It is installed by Installation Manager. It is part of the base Netcool Operations Insight solution, so it must be installed, configured, and running before you can start the Networks for Operations Insight feature setup.

- Server components (includes ObjectServers)
- Probe and gateway feature
- Accelerated Event Notification (AEN) client

For systems requirements, see <https://ibm.biz/BdRNaT>.

Important: The ObjectServer that manages the event data must be at V8.1.

Tivoli Netcool/OMNIBus Web GUI V8.1.0.9

This component includes the following subcomponents and add-ons. It is installed by Installation Manager. It is part of the base Netcool Operations Insight solution. The following extensions to the Web GUI are supplied in Netcool Operations Insight:

- Tools and menus for integration with Operations Analytics - Log Analysis.
- Extensions for Netcool Operations Insight: This supports the Event Analytics capability.

Important: Both the Impact Server Extensions and the Web GUI extensions must be installed for the Event Analytics capability to work.

The Web GUI is installed into Dashboard Application Services Hub, which is part of Jazz for Service Management. Jazz for Service Management is distributed as separate installation features in Installation Manager. For systems requirements, see <https://ibm.biz/BdRNaT>.

DB2® V10.5 Enterprise Server Edition database

DB2 is the default database used for the Netcool Operations Insight solution. Other types of databases are also possible. For more information, see <http://ibm.biz/SysReqsNOI14>.

Gateway for JDBC

This product is required for the base Netcool Operations Insight solution. It is installed by Installation Manager. The system requirements are the same as for Tivoli Netcool/OMNIBus V8.1. It is required for the transfer of event data from the ObjectServer to the IBM DB2 database.

Netcool/Impact V7.1.0.9

This product includes the following components. It is part of the base Netcool Operations Insight solution. It is installed by Installation Manager.

- Impact server
- GUI server
- Impact Server extensions: Includes the policies that are used to create the event analytics algorithms and the integration to IBM Connections.

Important: Both the Impact Server Extensions and the Web GUI extensions must be installed for the Event Analytics capability to work.

For system requirements, see <https://ibm.biz/BdRNLF>.

IBM Operations Analytics - Log Analysis V1.3.3 and V1.3.5

Netcool Operations Insight works with IBM Operations Analytics - Log Analysis V1.3.3 and 1.3.5. IBM Operations Analytics - Log Analysis is part of the base Netcool Operations Insight solution. It is installed by Installation Manager. For system requirements, search for "Hardware and software requirements" within the relevant version of IBM Operations Analytics - Log Analysis at <https://www.ibm.com/support/knowledgecenter/SSPFMY>.

Note: Operations Analytics - Log Analysis Standard Edition is included in Netcool Operations Insight. For more information about Operations Analytics - Log Analysis editions, search for "Editions" at the Operations Analytics - Log Analysis Knowledge Center, at <https://www.ibm.com/support/knowledgecenter/SSPFMY>.

OMNIBusInsightPack_v1.3.0.2 for IBM Operations Analytics - Log Analysis

This product is part of the base Netcool Operations Insight solution. It is required to enable the event search capability in Operations Analytics - Log Analysis. The Insight Pack is installed into Operations Analytics - Log Analysis.

Gateway for Message Bus V7.0

This product is part of the base Netcool Operations Insight solution. It is installed by Installation Manager. The system requirements are the same as for Tivoli Netcool/OMNIBus V8.1. It is used for transferring event data to the IBM Operations Analytics - Log Analysis product.

Jazz for Service Management V1.1.3.0 with Cumulative Patch 1

This component provides the GUI framework for the Netcool Operations Insight solution. It is installed by Installation Manager, and it includes the following subcomponents.

- Dashboard Application Services Hub V3.1.3.0
- Reporting Services (previously called Tivoli Common Reporting V3.1)

For the system requirements for Dashboard Application Services Hub, see <https://ibm.biz/BdHSYG>. The instance of Dashboard Application Services Hub hosts the V8.1 Web GUI and the Seasonal Event Reports portlet. Jazz for Service Management is included in the Web GUI installation package but is installed as separate features.

You can set up Network Manager and Netcool Configuration Manager to work with Reporting Services by installing their respective reports when installing the products. Netcool/OMNIBus V8.1 and later can be integrated with Reporting Services V3.1 to support reporting on events. To configure this integration, connect Reporting Services to a relational database through a gateway. Then, import the report package that is supplied with Netcool/OMNIBus into Reporting Services. For more information about event reporting, see http://www-01.ibm.com/support/knowledgecenter/SSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/omnibus/wip/install/task/omn_con_ext_deploytcrrreports.html.

Network Manager V4.2.0.3

This product includes the core and GUI components for the optional Networks for Operations Insight feature.

For system requirements, see http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/install/task/nmip_pln_planninginst.html.

Network Manager Insight Pack V1.3.0.0 for IBM Operations Analytics - Log Analysis

This product is part of the Networks for Operations Insight feature. It is required to enable the topology search capability in Operations Analytics - Log Analysis. The Insight Pack is installed into Operations Analytics - Log Analysis. It requires that the OMNIBusInsightPack_v1.3.0.2 is installed.

Note: The Network Manager Insight Pack V1.3.0.0 can share a data source with the OMNIBusInsightPack_v1.3.0.2 only. It cannot share a data source with previous versions of the Tivoli Netcool/OMNIBus Insight Pack.

Probe for SNMP

This product is optional for the base Netcool Operations Insight solution. It is used in environments that have SNMP traps. It is required for the Networks for Operations Insight feature. For installations of the probe on

the Tivoli Netcool/OMNIBus V8.1 server, use the instance of the probe that installs with IBM Installation Manager.

Syslog Probe

This product is optional for the base Netcool Operations Insight solution. It is required for the Networks for Operations Insight feature. For installations of the probe on the Tivoli Netcool/OMNIBus V8.1 server, use the instance of the probe that installs with IBM Installation Manager.

Netcool Configuration Manager V6.4.2.4

This product has the following components. It is part of the optional Networks for Operations Insight feature.

- Core components
- Drivers
- OOB component

For system requirements, see <https://ibm.biz/BdRNaN> for the worker server, and see <https://ibm.biz/BdRNGF> for the GUI server.

IBM Network Performance Insight V1.2.0

Network Performance Insight is a flow-based network traffic performance monitoring system. It provides comprehensive and scalable visibility on network traffic with visualization and reporting of network performance data for complex, multivendor, multi-technology networks. For more information, see <http://www-01.ibm.com/support/knowledgecenter/SSCVHB/welcome>.

IBM Alert Notification

IBM Alert Notification provides instant notification of alerts for any critical IT issues across multiple monitoring tools. It gives IT staff instant notification of alerts for any issues in your IT operations environment. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSY487/com.ibm.netcool_OMNIBusaas.doc_1.2.0/landingpage/product_welcome_alertnotification.html.

IBM Runbook Automation

IBM Runbook Automation empowers IT operations teams to be more efficient and effective. Operators can focus their attention where it is really needed and receive guidance to the best resolution with recommended actions and pre-filled context. With Runbook Automation you can:

- Investigate and delegate problems faster and more efficiently.
- Diagnose and fix problems faster and build operational knowledge.
- Easily create, publish, and manage runbooks and automations.
- Keep score to track achievements and find opportunities for improvement.

For more information, see http://www-01.ibm.com/support/knowledgecenter/SSZQDR/com.ibm.rba.doc/RBA_welcome.html.

More information

For more information about the component products of Netcool Operations Insight, see the websites listed in the following table.

Table 2. Product information

Product	Website
IBM Netcool Operations Insight	http://www.ibm.com/support/knowledgecenter/SSTPTP/welcome
IBM Tivoli Netcool/OMNIBus and Web GUI	http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html
IBM Tivoli Netcool/Impact	http://www-01.ibm.com/support/knowledgecenter/SSSHYH/welcome
IBM Operations Analytics - Log Analysis	http://www-01.ibm.com/support/knowledgecenter/SSPFMY/welcome
Netcool/OMNIBus Insight Pack	http://www.ibm.com/developerworks/servicemanagement/ia/log/downloads.html
Netcool/OMNIBus Gateways	http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/gateways/common/Gateways.html
Jazz for Service Management	http://www.ibm.com/support/knowledgecenter/SSEKCU/welcome
IBM Tivoli Network Manager	http://www-01.ibm.com/support/knowledgecenter/SSSHRK/welcome
IBM Tivoli Netcool Configuration Manager	http://www-01.ibm.com/support/knowledgecenter/SS7UH9/welcome
Network Performance Insight	http://www-01.ibm.com/support/knowledgecenter/SSCVHB/welcome
Runbook Automation	http://www-01.ibm.com/support/knowledgecenter/SSZQDR/com.ibm.rba.doc/RBA_welcome.html
Alert Notification	http://www.ibm.com/support/knowledgecenter/SSY487/com.ibm.netcool_OMNIBusaas.doc_1.2.0/landingpage/product_welcome_alertnotification.html

Deployment considerations

How to model your deployment to handle the expected event volumes in Netcool/OMNIBus and to reflect the capacity that you plan for IBM Operations Analytics - Log Analysis, and what to consider if you plan to deploy the Networks for Operations Insight feature.

Related tasks:

“Installing Netcool Operations Insight” on page 27

Deployment considerations for Netcool/OMNIBus and the connection to Operations Analytics - Log Analysis

When you plan a deployment, it is important to consider the relationship between the event volumes that are supported by Netcool/OMNIBus and the capacity of Operations Analytics - Log Analysis to analyze events. The volume of events determines whether a basic, failover, or desktop architecture or a multitier architecture is deployed. The Gateway for Message Bus can be configured to support event inserts only or both inserts and reinserts.

- “Explanation of Netcool/OMNIBus and Operations Analytics - Log Analysis considerations” on page 9
- “Deployment Scenarios” on page 9
- “Illustrations of architectures” on page 11

Explanation of Netcool/OMNIbus and Operations Analytics - Log Analysis considerations

The following explains the architecture and event volume, and the event analysis capacity of Operations Analytics - Log Analysis in more detail.

Note: Operations Analytics - Log Analysis Standard Edition is included in Netcool Operations Insight. For more information about Operations Analytics - Log Analysis editions, search for "Editions" at the Operations Analytics - Log Analysis Knowledge Center, at <https://www.ibm.com/support/knowledgecenter/SSPFMY>.

Event volume

Event inserts are the first occurrence of each event and reinserts are every occurrence of each event. By default, the Gateway for Message Bus is configured to accept only event inserts from ObjectServers through an IDUC channel. To support event inserts and reinserts, you can configure event forwarding through the Accelerated Event Notification (AEN) client. For more information, search for *Integrating with Operations Analytics - Log Analysis* in the *IBM Tivoli Netcool/OMNIbus Gateway for Message Bus Reference Guide*.

Architecture of Netcool/OMNIbus

Basic, failover, and desktop architectures support low and medium capacity for analyzing events. Multitiered architectures support higher Operations Analytics - Log Analysis capacities. In a multitier architecture, the connection to the Gateway for Message Bus supports higher capacity at the collection layer than at the aggregation layer.

For more information about these architectures, see the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* and also the *Netcool/OMNIbus Best Practices Guide*.

Capacity of Operations Analytics - Log Analysis

The capacity of the Operations Analytics - Log Analysis product to handle event volumes. For the hardware levels that are required for expected event volumes, see the Operations Analytics - Log Analysis documentation at <http://www-01.ibm.com/support/knowledgecenter/SSPFMY/welcome>. If capacity is limited, you can use the deletion tool to remove old data.

Connection layer

The connection layer is the layer of the multitier architecture to which the Gateway for Message Bus is connected. This consideration applies only when the Netcool/OMNIbus product is deployed in a multitier architecture. The connection layer depends on the capacity of Operations Analytics - Log Analysis. For more information about multitier architectures, see the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* and also the *Netcool/OMNIbus Best Practices Guide*.

Deployment Scenarios

How to combine the difference considerations that are described in "Explanation of Netcool/OMNIbus and Operations Analytics - Log Analysis considerations" to create a deployment architecture. Possible combinations of these factors, and the event volumes and Operations Analytics - Log Analysis capacity that they support, are explained in the following sections.

- "Deployment scenario 1" on page 10
- "Deployment scenario 2" on page 10
- "Deployment scenario 3" on page 10

- “Deployment scenario 4” on page 11
- “Deployment scenario 5” on page 11
- “Deployment scenario 6” on page 11

Deployment scenario 1

Table 3. Deployment scenario 1: Inserts only, standard architecture, low capacity

Event volume	Architecture of Netcool/OMNIBus	Capacity of Operations Analytics - Log Analysis	Connection layer	IDUC or AEN	Illustration of this architecture
Inserts only	Basic, failover, and desktop architecture	Low	Not applicable	IDUC	See Figure 1 on page 12. Disregard the reference to reinserts in item 1 .

Deployment scenario 2

Table 4. Deployment scenario 2: Inserts and reinserts, standard architecture, low capacity

Event volume	Architecture of Netcool/OMNIBus	Capacity of Operations Analytics - Log Analysis	Connection layer	IDUC or AEN	Illustration of this architecture
Inserts and reinserts	Basic, failover, and desktop architecture	Medium	Not applicable	AEN	See Figure 1 on page 12.

Deployment scenario 3

Table 5. Deployment scenario 3: Inserts only, multitier architecture, medium capacity

Event volume	Architecture of Netcool/OMNIBus	Capacity of Operations Analytics - Log Analysis	Connection layer	IDUC or AEN	Illustration of this architecture
Inserts only	Multitier	Medium	Aggregation layer	IDUC	See Figure 2 on page 13. Disregard the reference to reinserts in item 1 .

Deployment scenario 4

Table 6. Deployment scenario 4: Inserts only, multitier architecture, high capacity

Event volume	Architecture of Netcool/OMNIBus	Capacity of Operations Analytics - Log Analysis	Connection layer	IDUC or AEN	
Inserts only	Multitier	High	Collection layer	IDUC	See Figure 3 on page 14. Disregard the reference to reinserts in item 1 .

Deployment scenario 5

Table 7. Deployment scenario 5: Inserts and reinserts, multitier architecture, high capacity

Event volume	Architecture of Netcool/OMNIBus	Capacity of Operations Analytics - Log Analysis	Connection layer	IDUC or AEN	
Inserts and reinserts	Multitier	High	Aggregation layer	AEN	See Figure 2 on page 13.

Deployment scenario 6

Table 8. Deployment scenario 6: Inserts and reinserts, multitier architecture, very high capacity

Event volume	Architecture of Netcool/OMNIBus	Capacity of Operations Analytics - Log Analysis	Connection layer	IDUC or AEN	
Inserts and reinserts	Multitier	Very high	Collection layer	AEN	See Figure 3 on page 14.

Illustrations of architectures

The following sections show the architecture of Operations Analytics - Log Analysis deployments and how they fit into the various architectures of Netcool/OMNIBus deployments with the Gateway for Message Bus.

The data source that is described in the figures is the raw data that is ingested by the Operations Analytics - Log Analysis product. You define it when you configure the integration between the Operations Analytics - Log Analysis and Netcool/OMNIBus products.

- “Basic, failover, and desktop architectures” on page 12
- “Multitier architecture, events are sent from the Collection layer” on page 14
- “Multitier architecture, events are sent from the Aggregation layer” on page 13

Basic, failover, and desktop architectures

The following figure shows how the integration works in a basic, failover, or desktop Netcool/OMNIBus architecture. This figure is an illustration of the architectures that are described in Table 3 on page 10 and Table 4 on page 10. In the case of the architecture in Table 3 on page 10, disregard item **1** in this figure.

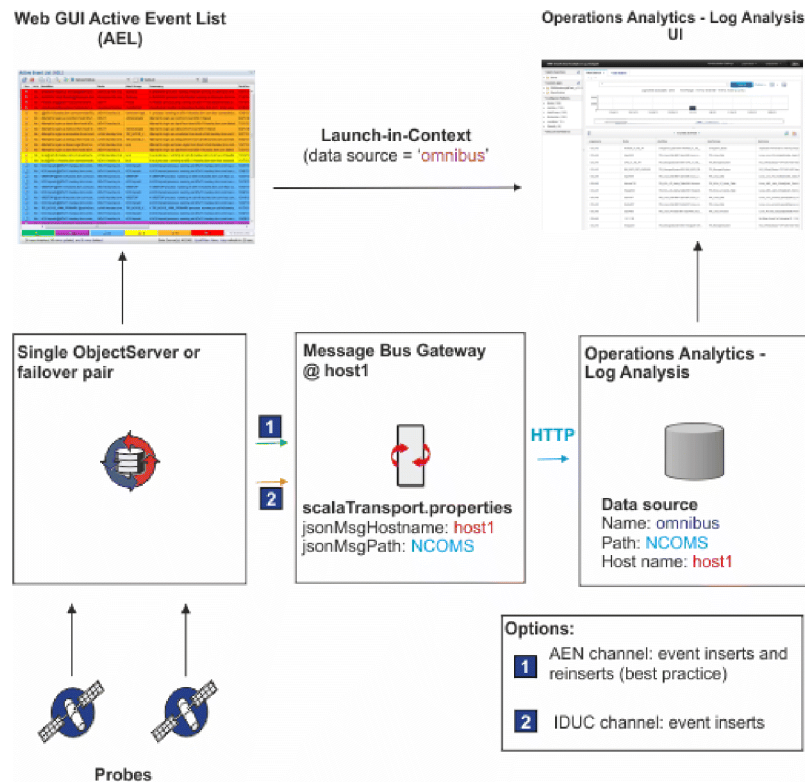


Figure 1. Basic, failover, and desktop deployment architecture

Multitier architecture, events are sent from the Aggregation layer

The following figure shows how the integration works in a multitier Netcool/OMNIbus architecture, with events sent from the Aggregation layer. This figure is an illustration of the architectures that are described in Table 5 on page 10 and Table 7 on page 11. In the case of the architecture in Table 5 on page 10, disregard item **1** in this figure.

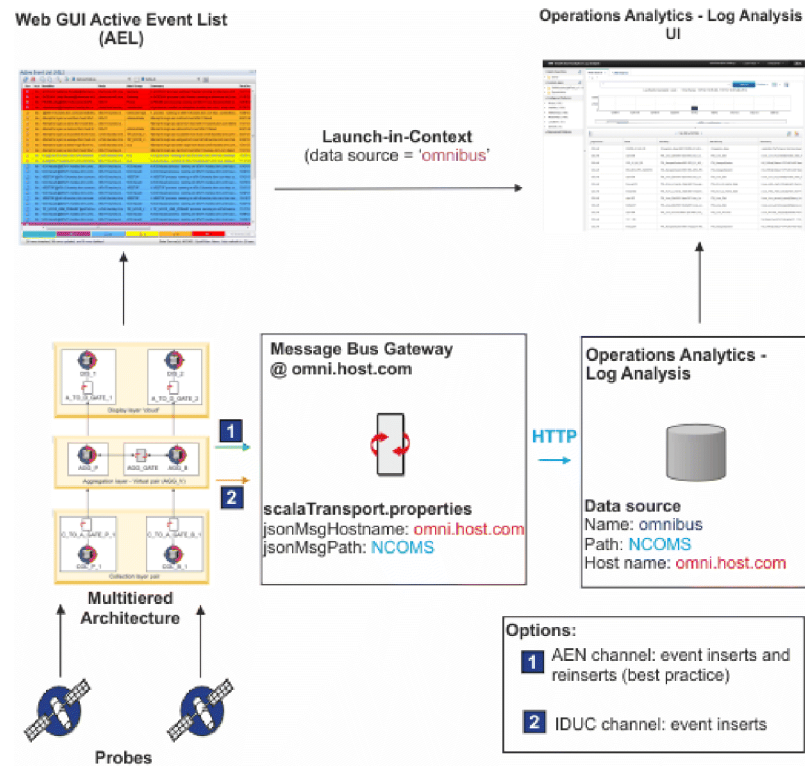


Figure 2. Multitier architecture deployment - Aggregation layer

Multitier architecture, events are sent from the Collection layer

The following figure shows how the integration works in a multitier Netcool/OMNIbus architecture, with events sent from the Collection layer. This is a best practice for integrating the components. This figure is an illustration of the architectures that are described in Table 6 on page 11 and Table 8 on page 11. In the case of the architecture in Table 6 on page 11, disregard item **1** in this figure.

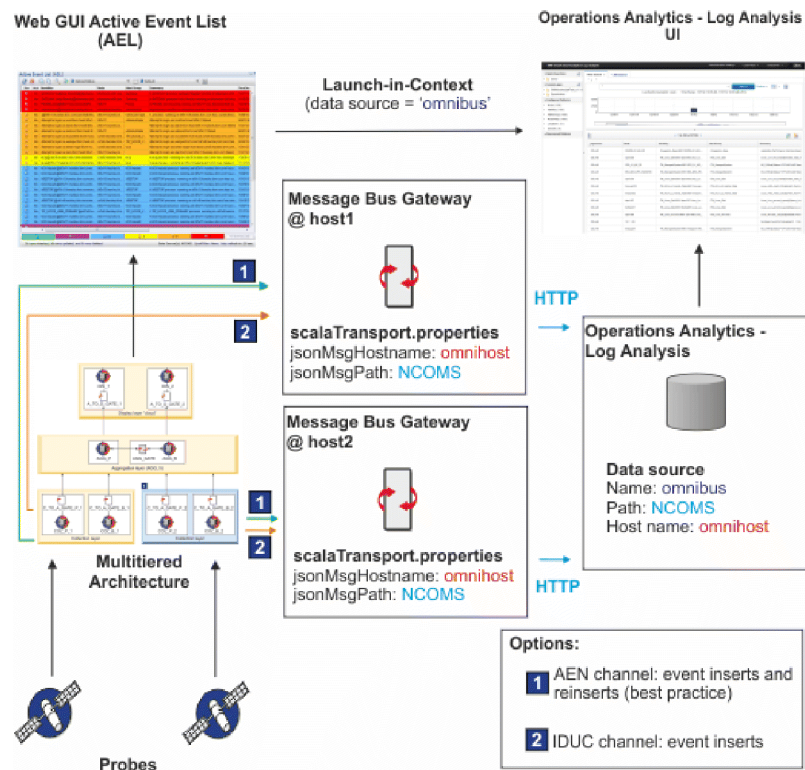


Figure 3. Multitier architecture deployment - Collection layer (best practice)

Related concepts:

- ➡ Overview of the standard multitiered architecture
- ➡ Overview of the AEN client

Related tasks:

- ➡ Sizing your Tivoli Netcool/OMNIbus deployment
- ➡ Configuring and deploying a multitiered architecture
- “Installing Netcool/OMNIbus and Netcool/Impact” on page 40

Related reference:

- ➡ Failover configuration
- ➡ Example Tivoli Netcool/OMNIbus installation scenarios (basic, failover, and desktop architectures)

Related information:

- ➡ Message Bus Gateway documentation
- ➡ IBM Operations Analytics - Log Analysis documentation
- ➡ Tivoli Netcool/OMNIbus Best Practices

Deployment considerations for the Networks for Operations Insight feature

Networks for Operations Insight is an optional feature that integrates network management products with the products of the base Netcool Operations Insight solution.

The Networks for Operations Insight feature includes Network Manager and Netcool Configuration Manager. Deploying these products depends on your environment and the size and complexity of your network. For guidance on deployment options, see guidance provided in the respective product documentation:

- Network Manager: http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/overview/concept/nmip_ovr_deploymenttofitnm.html
- Netcool Configuration Manager: http://www-01.ibm.com/support/knowledgecenter/SS7UH9_6.4.2/ncm/wip/planning/concept/ncm_plan_planninginstallation.html

Ports used by products and components

Use this information to understand which ports are used by the different products and components that make up the Netcool Operations Insight solution.

The following table lists sample ports that you might need to configure, and provides links to Netcool Operations Insight product and component documentation where you can access detailed information.

Table 9. Default port information

Product	Example default ports	Links
Netcool/OMNIbus	Aggregation ObjectServer primary port Process agent ports Gateway server port IBM Eclipse Help System server port Port numbers for individual Netcool/OMNIbus probes	ObjectServer ports can be configured using the Netcool Configuration wizard. See http://ibm.biz/BdskVc . Default ports used by Netcool/OMNIbus. See http://ibm.biz/BdskVr . Ports for a Netcool/OMNIbus basic architecture. See http://ibm.biz/BdsWi9 . Ports for a Netcool/OMNIbus basic failover architecture. See http://ibm.biz/BdsWqw . Ports for a Netcool/OMNIbus desktop server architecture. See http://ibm.biz/BdsWqt .
Netcool/OMNIbus Web GUI	Jazz for Service Management WAS profile • HTTP port • HTTPS port	Jazz for Service Management port availability requirements. See http://ibm.biz/BdsWzf . Firewall Ports to open for DASH Services. See http://www-01.ibm.com/support/docview.wss?uid=swg21687730for technote .

Table 9. Default port information (continued)

Product	Example default ports	Links
Netcool/Impact	Netcool/Impact server • HTTP port • HTTPS port Netcool/Impact GUI • HTTP port • HTTPS port	Assigning Netcool/Impact ports. See http://ibm.biz/BdsWyK . Assigning Netcool/Impact data source and service ports. See http://ibm.biz/BdsWyG . Note: It is not possible to install Netcool/Impact GUI and Jazz for Service Management using the same default port numbers (16310/16311) on the same server. In this case you must modify the port numbers during installation.
Operations Analytics - Log Analysis	Application WebConsole Port Application WebConsole Secure Port Database Server Port Data Collection Server Port	Default ports used by Operations Analytics - Log Analysis: • V1.3.5: see http://ibm.biz/BdsWyn. • V1.3.3: see http://ibm.biz/BdiPy
DB2 Enterprise Server Edition database	Port 50000. Note: This port is also configurable following installation.	
Network Performance Insight	Ports must be assigned for the following Network Performance Insight components: • Ambari Metrics • Hadoop Distributed File System (HDFS) • Apache Kafka	Default ports used by Network Performance Insight. See http://ibm.biz/BdsWyb .

Related concepts:

“Installing DB2 and configuring the REPORTER schema” on page 41

Related tasks:

“Installing Netcool/OMNIBus and Netcool/Impact” on page 40

“Installing IBM Operations Analytics - Log Analysis” on page 42

“Installing Network Performance Insight and configuring integration with Netcool Operations Insight” on page 82

Data flows

How event data is retrieved from your monitored environment and transferred between the products and components of Netcool Operations Insight for analysis. Two sets of data flows are given. The first is for the base Netcool Operations Insight and shows how event data is retrieved from a monitored application environment and transferred between products and components. The second shows the integration with the optional Networks for Operations Insight feature and shows how network event data is retrieved, analyzed and visualized.

Related tasks:

“Installing Netcool Operations Insight” on page 27

Data flows for the base Netcool Operations Insight solution

How event data is retrieved from a monitored application environment and transferred between the products and components of the base Netcool Operations Insight. The explanations of the data flows are simplified to help you understand them. The Networks for Operations Insight feature and Reporting Services are omitted.

The following figure shows a simplified data flow between the products of the base Netcool Operations Insight solution.

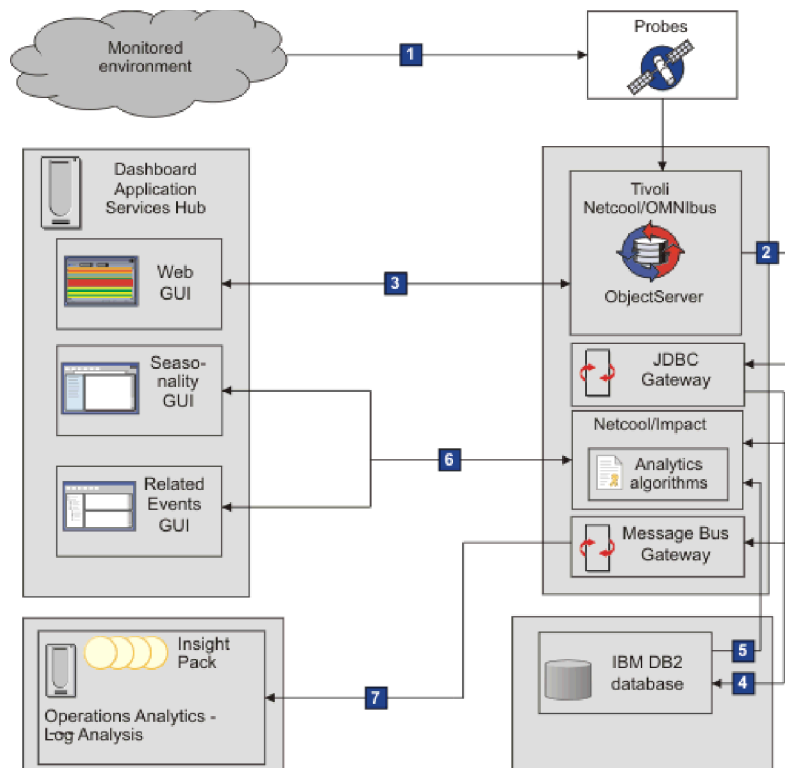


Figure 4. Transfer of event data from the monitored environment to the products and components of the base Netcool Operations Insight solution.

The stages of this data flow are as follows, indicated by the call-out graphics (for example, **1**).

1 : Alerts are received from applications and devices

Probes monitor the devices and applications in the environment. Alert data is captured by the probes and forwarded to the ObjectServer.

2 : Event data is transferred to the gateways and Netcool/Impact

The events are read from the ObjectServer by the Gateway for JDBC and the Message Bus Gateway. Netcool/Impact also reads the event data from the ObjectServer. In Netcool/Impact, the event data is enriched by information retrieved by the policies.

3 : Event data is visualized and managed in the Web GUI

The Tivoli Netcool/OMNIBus Web GUI displays the application events that are in the ObjectServer. From the event lists, you can run tools that changes the event data; these changes are synchronized with the data in the ObjectServer.

4 : Event data is archived

The Gateway for JDBC sends the event data via an HTTP interface to the database. The figure shows an IBM DB2 database but any supported database can be used. The gateway must be configured in reporting mode. This data flow is a prerequisite for the event analytics capability.

5 : Event analytics algorithms run on archived event data

After a set of historical alerts is archived, the seasonality algorithms of the Netcool/Impact policies can generate seasonal reports. The related events function analyzes Tivoli Netcool/OMNIBus historical event data to determine which events have a statistical tendency to occur together.

6 : Analytics data visualized and managed

The seasonality function helps you identify and examine seasonal trends while monitoring and managing events. This capability is delivered in a Seasonal Events Report portlet in Dashboard Application Services Hub. The portlet contains existing seasonal reports, which can be used to identify the seasonal pattern of the events in the Event Viewer. You can create new seasonal reports and edit existing ones. Statistically related groups can be analyzed in the Related Events GUI. Validated event groups can be deployed as Netcool/Impact correlation rules.

7 : Event data transferred for indexing to Operations Analytics - Log Analysis

The Gateway for Message Bus sends the event data via an HTTP interface to the Operations Analytics - Log Analysis product where the event data is indexed. The Tivoli Netcool/OMNIBus Insight Pack V1.3.0.0 parses the event data into a format suitable for use by Operations Analytics - Log Analysis. Figure 4 on page 17 shows the default IDUC connection, which sends only event inserts. For event inserts and reinserts, the Accelerated Event Notification client can be deployed, which can handle greater event volumes. See “Deployment considerations for Netcool/OMNIBus and the connection to Operations Analytics - Log Analysis” on page 8.

Related information:

 [Tivoli Netcool/OMNIBus architecture](#)

 [IBM Operations Analytics - Log Analysis architecture](#)

 [Overview of Netcool/Impact deployments](#)

Networks for Operations Insight data flow

How event data is retrieved from the network and transferred between the products and components of the Networks for Operations Insight feature. The explanations of the data flows are simplified to help you understand them. Not all the products of the base Netcool Operations Insight solution are described.

The data flow starts with the retrieval of information about the network. The events are detected by the probes and by the Network Manager and Netcool Configuration Manager products. The event data is stored and aggregated in the ObjectServer. Network events are enriched with data from the network topology. Events are visualized in event lists and the network topology is visualized in the Network Manager GUIs through the Dashboard Application Services Hub. The event data is archived in a database; this archive is the data set that is used for analysis. The data is ingested by the IBM Operations Analytics - Log Analysis product and the metadata is created that is used for the event search and seasonality functions. You can launch between the event lists and network GUIs. Launch-in-context tools give access from the event lists to the analysis of the application and network event data in the Operations Analytics - Log Analysis. The seasonality function identifies trends so that regularly occurring events are identified.

To help you understand how data flows between the products and how the products are integrated, the following sections are presented:

1. “Data flow for event retrieval” on page 20: Describes how application events, network events, and configuration change and policy violation events are retrieved, stored, and visualized.
2. “Data flow for event archiving” on page 22: Describes how the event data is archived and ingested for analysis.

Data flow for event retrieval

The following figure shows how events are received, enriched, stored, and visualized by the products of the Netcool Operations Insight solution. The sequence of the data flow is indicated by the numbered sections, for example **1**. Each section is explained in the list that follows this figure. The data flow is simplified to make it easy to understand. Some products and components are omitted; these are described in the section “Notes for Figure 5”

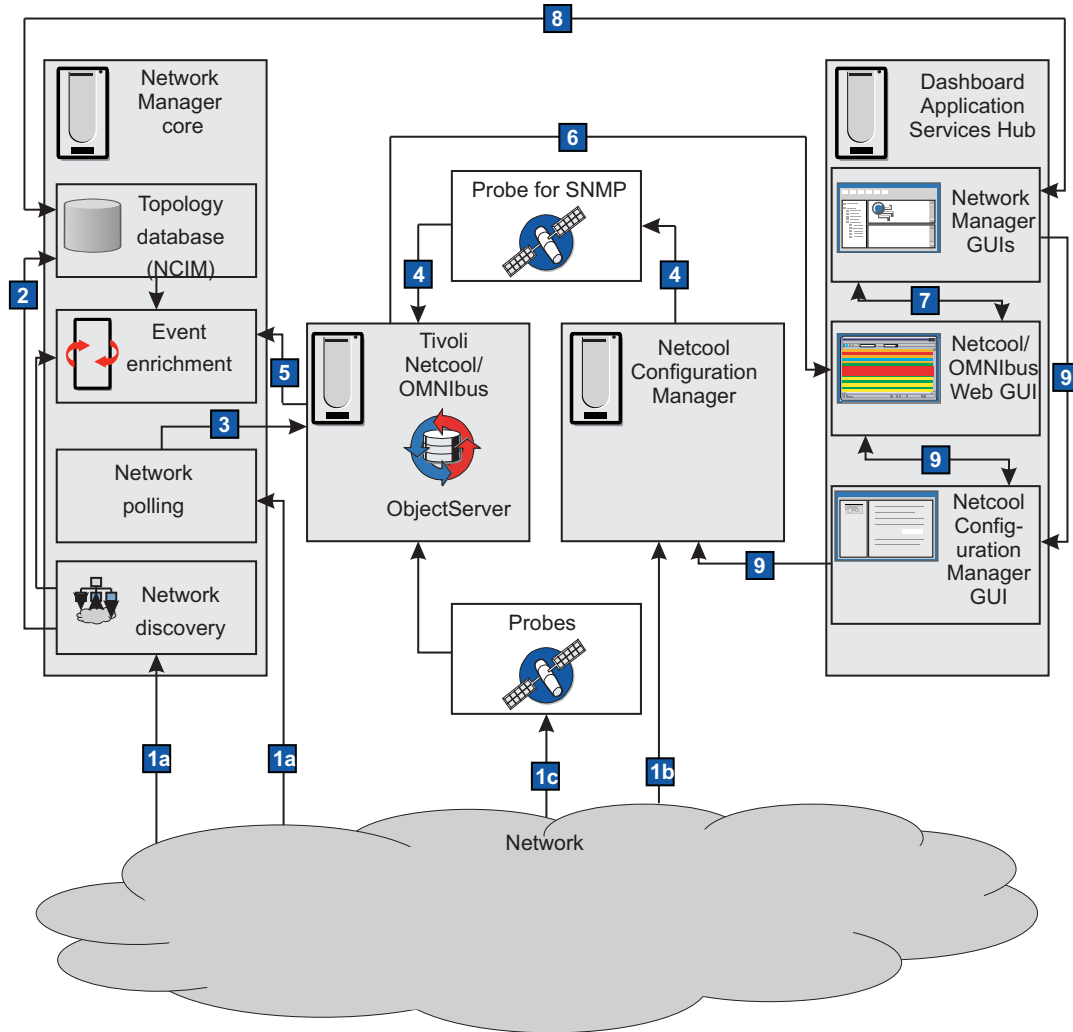


Figure 5. Simplified data flow

The most important points of Figure 5 are as follows:

1a Network discovery and polling of the network

Network Manager gathers data about the network. The discovery function identifies what entities, for example routers and switches, are on the network and interrogates them, for example, for connectivity information. The topology of the network is generated. The network polling determines whether a network device is up or down, whether it exceeds key performance parameters, and identifies inter-device link faults.

1b Detection of changes to device configurations and policy violations

Netcool Configuration Manager receives and stores data about configuration changes and policy violations that occur on network entities.

1c Probes send alerts about the devices that they monitor

Tivoli Netcool/OMNIBus probes that are monitoring devices on the network send alerts to the ObjectServer.

2 Storage of network topology

Network Manager classifies and stores the network topology that was discovered in step **1a** in the NCIM topology database.

3 Generation of network alerts

Network Manager generates fault alerts if network polls (step **1a**) fail. Network Manager converts the results of the relevant polls into events, and sends these network events to the ObjectServer.

4 Generation of configuration change and policy violation events

Netcool Configuration Manager generates events for the configuration changes and policy violations (referred to hereafter as *network configuration events*) that were detected in step **1b**. Configuration change and policy violation events are sent via the Probe for SNMP to the ObjectServer.

5 Event enrichment

Network events and network configuration events (which are generated in steps **3a** and **3b**) are passed to the Event Gateway, where they are enriched with network topology data. For example, the system location, contact information, and product serial number can be added to the events. The events are returned to the ObjectServer.

The ObjectServer now contains the application events from the probes, network events from Network Manager, and the network configuration events from Netcool Configuration Manager.

6 Event visualization and monitoring

The Tivoli Netcool/OMNIBus Web GUI displays the application events, network events, and network configuration events that are in the ObjectServer.¹

7 Different views of events

The event information is shared between the Web GUI and the Network Manager GUIs, for example, the Network Views and Hop View.

8 Visualization and analysis of network topology

The Network Manager GUIs display the network topology data that is in the NCIM database. This data is enriched by the configuration change and policy event information from the ObjectServer.

9 Analysis of network configuration events

Configuration changes and policy violations are displayed in the Network Manager GUIs and Web GUI, and in the Netcool Configuration Manager Activity Viewer, wizards, and other Netcool Configuration Manager UIs for further analysis.²

Notes for Figure 5 on page 20

1. Tivoli Netcool/OMNIBus gateways can be configured to forward alerts to other applications, such as a helpdesk or Customer Relationship Management (CRM) system, and a relational database management system (RDBMS). Gateways are not shown in this figure. The JDBC Gateway can be configured to archive historical events in a database. You configure the archiving of historical events for the Networks for Operations Insight feature. For more information, see Figure 6 on page 22.

2. Using the right-click menus, operators can optionally launch-in-context across into Reporting Services, if it is installed. Reporting Services is not shown on this figure.

Data flow for event archiving

The following figure shows the flow of event data between the products and components of the Networks for Operations Insight feature. To make the figure easy to understand, some products and components of the Netcool Operations Insight solution are omitted. After this data flow first completes, a set of events, that is, application events, network events, and configuration change and policy violation events is ready for visualization and analysis. The sequence of the data flow is indicated by the numbered sections, for example **1**. Each section is explained in the list that follows this figure.

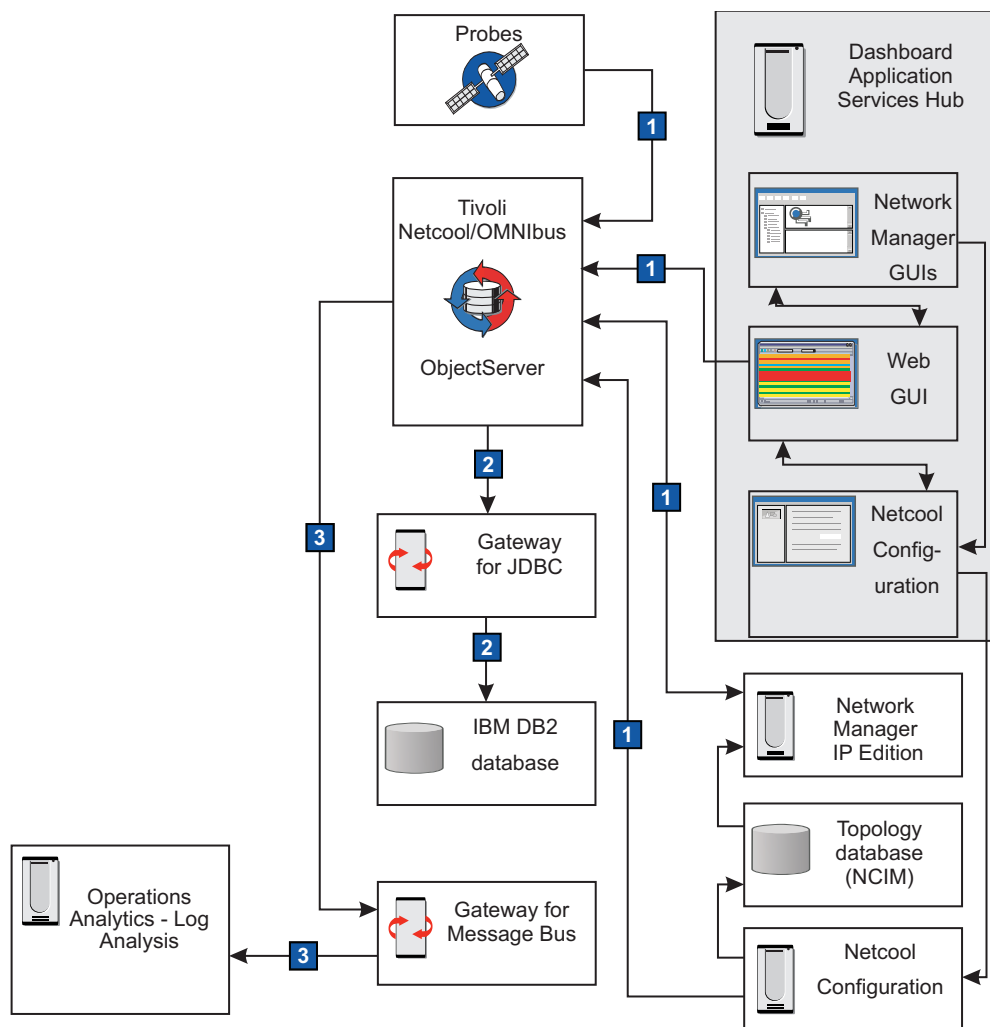


Figure 6. Data flow of the Networks for Operations Insight feature

The most important points of Figure 6 are as follows:

1 Event retrieval

Shows the flow of event data from probes, Network Manager, and Web GUI, to the ObjectServer. If event data is changed by operators who use

the Netcool Configuration Manager event lists, the changes are synchronized with the ObjectServer. This data flow is described in Figure 5 on page 20.

2 Archiving of event data

The Gateway for JDBC reads the events from the ObjectServer and sends them via an HTTP interface to the ObjectServer. The figure shows an IBM DB2 database, but any supported database can be used. The gateway must be configured in reporting mode. The gateway and the database are required for the Netcool Operations Insight solution; they are not specific to the Networks for Operations Insight feature. This data flow is a prerequisite for the event analytics function. After a set of historical alerts is archived, the algorithms of the Netcool/Impact policies can generate seasonal reports and group events based on the statistical likelihood to occur together.

For more information about Gateway for JDBC supported database and about configuring the gateway for reporting mode, see the *IBM Tivoli Netcool/OMNIBus Gateway for JDBC Reference Guide*.

3 Transfer of event data to IBM Operations Analytics - Log Analysis

This data flow is the prerequisite for the event search capability and optionally the topology search capability. Gateway for Message Bus reads the events from the ObjectServer and sends them to Operations Analytics - Log Analysis for indexing. Right-click tools in the event lists in Dashboard Application Services Hub launch the Operations Analytics - Log Analysis product. You can run contextualized searches over current and historical events (event search) and search the network topology for routes along network (topology search).

To support the event search, the OMNIBusInsightPack_v1.3.0.2 is required; for the topology search, you need the Network Manager Insight Pack V1.3.0.0.

For more information about IBM Operations Analytics - Log Analysis, see <http://www-01.ibm.com/support/knowledgecenter/SSPFMY/welcome>. For more information about the Tivoli Netcool/OMNIBus Insight Pack, see the *Tivoli Netcool/OMNIBus Insight Pack README*. For more information about the Network Manager Insight Pack, see the *Network Manager Insight Pack README*. For more information about the Gateway for Message Bus, see the *IBM Tivoli Netcool/OMNIBus Gateway for Message Bus Reference Guide*.

For more information about the Network Manager and Tivoli Netcool/OMNIBus data flow, see the product overview in the Network Manager documentation at http://www-01.ibm.com/support/knowledgecenter/SSSHRK/landingpage/product_welcome_itnm.html.

Related concepts:

 [Netcool Configuration Manager events](#)

Which documentation do I need?

The documentation for the Netcool Operations Insight solution describes scenarios for a fresh installation and upgrades from various existing environments, in varying levels of detail. You do not need to read the entire documentation set to understand how to get started with Netcool Operations Insight. Check here which documentation applies best to your environment and read only the documentation that is useful to you.

The following table describes the installation and upgrade scenarios that are in this documentation and links to each section.

Table 10. Sections of the documentation for installation and upgrade scenarios

Install or upgrade	Scenario	Described here
Fresh installation: no existing products in the environment	At-a-glance overview, for a proof of concept	Quick Start Guide
	Quick reference, to understand in more detail the tasks involved in installing Netcool Operations Insight	"Quick reference to installing" on page 27
	End-to-end overview of installing all the products and components in Netcool Operations Insight, in the recommended order	"Performing a fresh installation" on page 32
Upgrade from previous versions	Quick reference, to upgrading Netcool Operations Insight	"Quick reference to upgrading" on page 87
	End-to-end overview of upgrading all the products and components in Netcool Operations Insight from V1.2, in the recommended order	"Upgrading Netcool Operations Insight" on page 89

The following table shows which documentation to read if you want to find out how to set up one of the individual capabilities that is included in Netcool Operations Insight.

Table 11. Scenarios for setting up Netcool Operations Insight capabilities

Capability	Scenario	Link
Event search	Installing or upgrading the Insight Pack	Installing the Insight Pack
	Configuring the capability	"Configuring event search" on page 94
Event analytics	Adding a new event analytics to an existing environment	"Installing Event Analytics" on page 113
	Upgrading an existing event analytics	"Upgrading Event Analytics" on page 118

Table 11. Scenarios for setting up Netcool Operations Insight capabilities (continued)

Capability	Scenario	Link
Networks for Operations Insight	Adding Networks for Operations Insight to an existing environment	"Installing the Networks for Operations Insight feature" on page 46
Topology search	Installing the Insight Pack	Installing the Insight Pack
	Configuring the capability	"Configuring topology search" on page 276
Integration with IBM Connections	Configuring the capability	"Configuring integration to IBM Connections" on page 283
Network Performance Insight	Network Performance Insight is a flow-based network traffic performance monitoring system. It provides comprehensive and scalable visibility on network traffic with visualization and reporting of network performance data for complex, multivendor, multi-technology networks. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSCVHB/welcome .	
IBM Alert Notification	IBM Alert Notification provides instant notification of alerts for any critical IT issues across multiple monitoring tools. It gives IT staff instant notification of alerts for any issues in your IT operations environment. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSY487/com.ibm.netcool_OMNibusaa.doc_1.2.0/landingpage/product_welcome_alertnotification.html .	
IBM Runbook Automation	IBM Runbook Automation empowers IT operations teams to be more efficient and effective. Operators can focus their attention where it is really needed and receive guidance to the best resolution with recommended actions and pre-filled context. With Runbook Automation you can: • Investigate and delegate problems faster and more efficiently. • Diagnose and fix problems faster and build operational knowledge. • Easily create, publish, and manage runbooks and automations. • Keep score to track achievements and find opportunities for improvement. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSZQDR/com.ibm.rba.doc/RBA_welcome.html.	

Related concepts:

"Supported products and components" on page 3

Installing Netcool Operations Insight

How to install the products and components of Netcool Operations Insight into a new environment, with no existing software. Scenarios are presented here that give a quick reference to installing and also an end-to-end scenario on a simple system architecture.

About this task

Note: The scenarios and examples used assume deployment on UNIX systems.

Related concepts:

“Deployment considerations” on page 8

“Data flows” on page 16

Quick reference to installing

Use this information as a quick reference if you are new to Netcool Operations Insight and want to perform an installation from scratch. This overview assumes detailed knowledge of the products in Netcool Operations Insight. It does not provide all the details. Links are given to more information, either within the Netcool Operations Insight documentation, or in the product documentation of the constituent products of Netcool Operations Insight.

The following table lists the high-level steps for installing Netcool Operations Insight. Steps 1-12 are required for the base Netcool Operations Insight solution. Steps 13-17 are required for the Networks for Operations Insight feature. Steps 18-20 are required if you have Networks for Operations Insight and want to deploy the topology search capability. Steps 21-24 are for additional features you can set up in your Netcool Operations Insight environment. For more information about where to download the documentation as PDF files, see “Where to obtain PDF publications” on page 31.

Tip: To verify the versions of installed packages, select **View Installed Packages** from the File menu on the main IBM Installation Manager screen.

For information on the product and component versions to install, including which fix packs to apply, see “Supported products and components” on page 3.

Table 12. Quick reference for installing Netcool Operations Insight

Item	Action	More information
1	Prepare for the installation by checking the prerequisites.	For information about hardware and software compatibility of each component, and detailed system requirements, see the IBM Software Product Compatibility Reports website: http://www-969.ibm.com/software/reports/compatibility/clarity/index.html “Checking prerequisites” on page 34

Table 12. Quick reference for installing Netcool Operations Insight (continued)

Item	Action	More information
2	Install IBM Installation Manager on each host where components of the Netcool Operations Insight are to be installed. Installation Manager is included in the compressed file distribution of IBM Tivoli Netcool/OMNIBus and Operations Analytics - Log Analysis. Download Installation Manager separately if you are installing directly from an IBM repository or from a local repository. If you need to install Installation Manager separately, you can download it from IBM Fix Central.	http://www.ibm.com/support/fixcentral/ “Obtaining IBM Installation Manager” on page 36 “Installing Installation Manager (GUI or console example)” on page 38
3	Install the Netcool/OMNIBus core components, and apply the latest supported fix pack. Associated tasks include creating and starting ObjectServers, and setting up failover or a multitier architecture.	“Installing Netcool/OMNIBus and Netcool/Impact” on page 40 See “Supported products and components” on page 3 for latest supported fix packs. See the <i>IBM Tivoli Netcool/OMNIBus Installation and Deployment Guide</i>.
4	Install the DB2 database. Apply the REPORTER schema.	“Installing DB2 and configuring the REPORTER schema” on page 41
5	Install the Gateway for JDBC and the Gateway for Message Bus.	See the <i>IBM Tivoli Netcool/OMNIBus Gateway for JDBC Reference Guide</i> and the <i>IBM Tivoli Netcool/OMNIBus Gateway for Message Bus Reference Guide</i>.
6	Install Netcool/Impact, and apply the latest supported fix pack.	“Installing Netcool/OMNIBus and Netcool/Impact” on page 40 See “Supported products and components” on page 3 for latest supported fix packs. See the <i>IBM Tivoli Netcool/Impact Netcool/Impact Installation Guide</i>.
7	Configure the ObjectServer to support the related events function of the Event Analytics capability. Run the <code>nco_sql</code> utility against the <code>relatedevents_objectserver.sql</code> file, which is delivered with Netcool/Impact.	“Configuring the Event Analytics ObjectServer” on page 199
8	Install a supported version of IBM Operations Analytics - Log Analysis. Create a data source called “omnibus”.	http://www-01.ibm.com/support/knowledgecenter/SSPFMY/welcome See step 3 on page 95 in “Configuring event search” on page 94. See “Supported products and components” on page 3 for supported versions.
9	Configure the Gateway for Message Bus as the interface between the ObjectServer and Operations Analytics - Log Analysis. Optionally configure the Accelerated Event Notification Client if you do not want to use the default IDUC channel.	“Configuring the Gateway for JDBC and Gateway for Message Bus” on page 43 See the <i>IBM Tivoli Netcool/OMNIBus Gateway for Message Bus Reference Guide</i>.

Table 12. Quick reference for installing Netcool Operations Insight (continued)

Item	Action	More information
10	To support Event Search, install the latest supported version of Tivoli Netcool/OMNIBus Insight Pack.	See the <i>OMNIBusInsightPack_v1.3.0.2 README</i> Note: You can install both insight packs later, see step 18. See “Supported products and components” on page 3 for latest supported versions.
11	Install the Netcool/OMNIBus Web GUI, and apply the latest supported fix pack. Note: Installation Manager V1.8.4.1 or later is required before Web GUI V8.1.0.7 (fix pack 7) or later installation. During the installation, ensure that the latest supported versions are selected for the following components, based on the information in “Supported products and components” on page 3: • IBM WebSphere® Application Server. • Jazz for Service Management. • Netcool/OMNIBus Web GUI In addition, make the following selections during the installation: • When installing Jazz for Service Management, Installation Manager discovers two required packages in the Jazz™ repository. Select the Jazz for Service Management extension for IBM WebSphere V8.5 and Dashboard Application Services Hub V3.1.3.0 packages for installation. • IBM WebSphere SDK Java Technology Edition V7.0.x. • Install the Netcool Operations Insight Extensions for IBM Tivoli Netcool/OMNIBus Web GUI feature. To install Event Analytics with seasonality reporting, ensure that install Event Analytics is selected.	“Installing Dashboard Application Services Hub and the UI components” on page 44 See “Installing Dashboard Application Services Hub and the UI components” on page 44 and also the <i>IBM Tivoli Netcool/OMNIBus Installation and Deployment Guide</i>. See “Supported products and components” on page 3 for latest supported fix packs.
12	Configure the Web GUI for integration with Operations Analytics - Log Analysis. In the <code>server.init</code> file, set the <code>scala.*</code> properties appropriately.	See “Installing Dashboard Application Services Hub and the UI components” on page 44 and also the <i>IBM Tivoli Netcool/OMNIBus Installation and Deployment Guide</i> .
13	Installing the Probe for SNMP and Syslog Probe for Network Manager	“Installing the Probe for SNMP and Syslog Probe” on page 48

Table 12. Quick reference for installing Netcool Operations Insight (continued)

Item	Action	More information
14	Optional: Configure the ObjectServer for integration with Network Manager by obtaining the ConfigOMNI script from the Network Manager installation package and running it against the ObjectServer.	See “Optional: Preparing the ObjectServer for integration with Network Manager” on page 49 and also the <i>IBM Tivoli Network Manager IP Edition Installation and Configuration Guide</i> . Important: If you have already installed Tivoli Netcool/OMNIBus, the Netcool/OMNIBus Knowledge Library, and the Probe for SNMP, you can now install Network Manager, and do not need to follow the steps in this task. The Network Manager installer configures Tivoli Netcool/OMNIBus for you during the installation process. If the ObjectServer setup changes after you have already installed and configured Network Manager and Tivoli Netcool/OMNIBus, then you must reintegrate the ObjectServer with Network Manager as described in this topic.
15	Prepare the topology database for use by Network Manager	“Preparing the database for Network Manager” on page 49
16	Install Network Manager core and GUI components, and apply the latest supported fix pack.	“Installing Network Manager and Netcool Configuration Manager” on page 50 More information: See “Supported products and components” on page 3 for latest supported fix packs. See the <i>IBM Tivoli Network Manager IP Edition Installation and Configuration Guide</i> .
17	Install and configure Netcool Configuration Manager and apply the latest supported fix pack. This involves configuring the integration with Network Manager.	“Installing Network Manager and Netcool Configuration Manager” on page 50 “Configuring integration with Netcool Configuration Manager” on page 55 More information: For more information about 6.4.2.2 (fix pack 2), see http://www.ibm.com/support/knowledgecenter/SS7UH9_6.4.2/ncm/wip/relnotes/ncm_rn_6422.html . See “Supported products and components” on page 3 for latest supported fix packs. See the <i>IBM Tivoli Netcool Configuration Manager Installation and Configuration Guide</i> and the <i>IBM Tivoli Netcool Configuration Manager Integration Guide</i> .
18	To support Topology Search, install the latest supported version of Network Manager Insight Pack and configure the connection to the NCIM topology database.	Network Manager Insight Pack See the <i>Network Manager Insight Pack V1.3.0.0 README</i> . Note: To install both insight packs at this stage, see summary task “Installing the Insight Packs” on page 79. See “Supported products and components” on page 3 for latest supported versions.

Table 12. Quick reference for installing Netcool Operations Insight (continued)

Item	Action	More information
19	Configure the topology search capability. Run nco_sql against the <code>scala_itnm_configuration.sql</code> file, which is delivered in the Netcool/OMNIBus fix pack. Install the tools and menus to launch the custom apps of the Network Manager Insight Pack in the Operations Analytics - Log Analysis UI from the Web GUI.	"Configuring topology search" on page 276
20	Configure the Web GUI to launch the custom apps of the Network Manager Insight Pack from the event lists.	See step 3 on page 278 of "Configuring topology search" on page 276.
21	To add the performance management feature, set up Network Performance Insight and follow the steps for integrating it with Netcool/OMNIBus and Network Manager.	"Installing Network Performance Insight and configuring integration with Netcool Operations Insight" on page 82
22	Install and configure the Device Dashboard to view performance information.	"Installing and configuring the Device Dashboard" on page 82
23	You can set up event data to be forwarded from Netcool/OMNIBus and Netcool/Impact through the Alert Notification service.	IBM Alert Notification provides instant notification of alerts for any critical IT issues across multiple monitoring tools. It gives IT staff instant notification of alerts for any issues in your IT operations environment. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSY487/com.ibm.netcool_OMNIBusaas.doc_1.2.0/landingpage/product_welcome_alertnotification.html .
24	You can set up Netcool/OMNIBus and Netcool/Impact to integrate with IBM Runbook Automation	IBM Runbook Automation empowers IT operations teams to be more efficient and effective. Operators can focus their attention where it is really needed and receive guidance to the best resolution with recommended actions and pre-filled context. With Runbook Automation you can: • Investigate and delegate problems faster and more efficiently. • Diagnose and fix problems faster and build operational knowledge. • Easily create, publish, and manage runbooks and automations. • Keep score to track achievements and find opportunities for improvement. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSZQDR/com.ibm.rba.doc/RBA_welcome.html .

Where to obtain PDF publications

You can obtain Netcool Operations Insight publications, including the Insight Pack READMEs, in PDF format from http://www-01.ibm.com/support/knowledgecenter/SSTPTP_1.4.0.1/soc/integration/reference/soc_ref_PDFbooks.html.

You can obtain IBM Tivoli Netcool/OMNIBus and Web GUI publications from the FTP download site at <ftp://public.dhe.ibm.com/software/tivoli/Netcool/NetcoolOmnibus/>.

You can obtain IBM Tivoli Netcool/OMNIBus gateway publications from IBM Knowledge Center at <https://ibm.biz/BdE7Lv>. Click the entry in the table of contents for the gateway that you required, for example **Gateway for JDBC** and then click **PDF version**.

You can obtain Netcool/Impact publications from the Netcool/Impact wiki at <https://ibm.biz/BdE79r>.

The Operations Analytics - Log Analysis documentation is available from IBM Knowledge Center only. However, you can use the **My Collections** function to save the documentation and download it as a PDF. For an example of how to do this, see “Creating your own PDF of a subset of topics using My Collections” on page 301.

You can obtain Network Manager publications from http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/common/reference/nmip_ref_pdfbookset.html.

You can obtain Netcool Configuration Manager publications from the IBM Knowledge Center at http://www-01.ibm.com/support/knowledgecenter/SS7UH9_6.4.2/ncm/wip/common/reference/ncm_ref_PDFdocset.dita.

Performing a fresh installation

This installation scenario describes a fresh installation of Netcool Operations Insight. A sample four-server system architecture is presented. This is a simplified sample, for ease of understanding. It can be scaled up and extended for failover, a multitiered architecture, load balancing, and clustering.

This scenario assumes that there are no existing Netcool Operations Insight products in your environment, so no backup, restore, or upgrade information is given. The information supplied in this scenario is high-level and covers the most salient points and possible issues you might encounter that are specific to Netcool Operations Insight. The steps to install the Networks for Operations Insight feature are included, but skip these steps if you want to install only the base solution. This scenario is end-to-end and you must perform the tasks in the specified order.

For more information about each task in this scenario, see the Related concept, task, and information links at the bottom of each page.

The following figure shows the simplified installation architecture that this scenario adheres to.

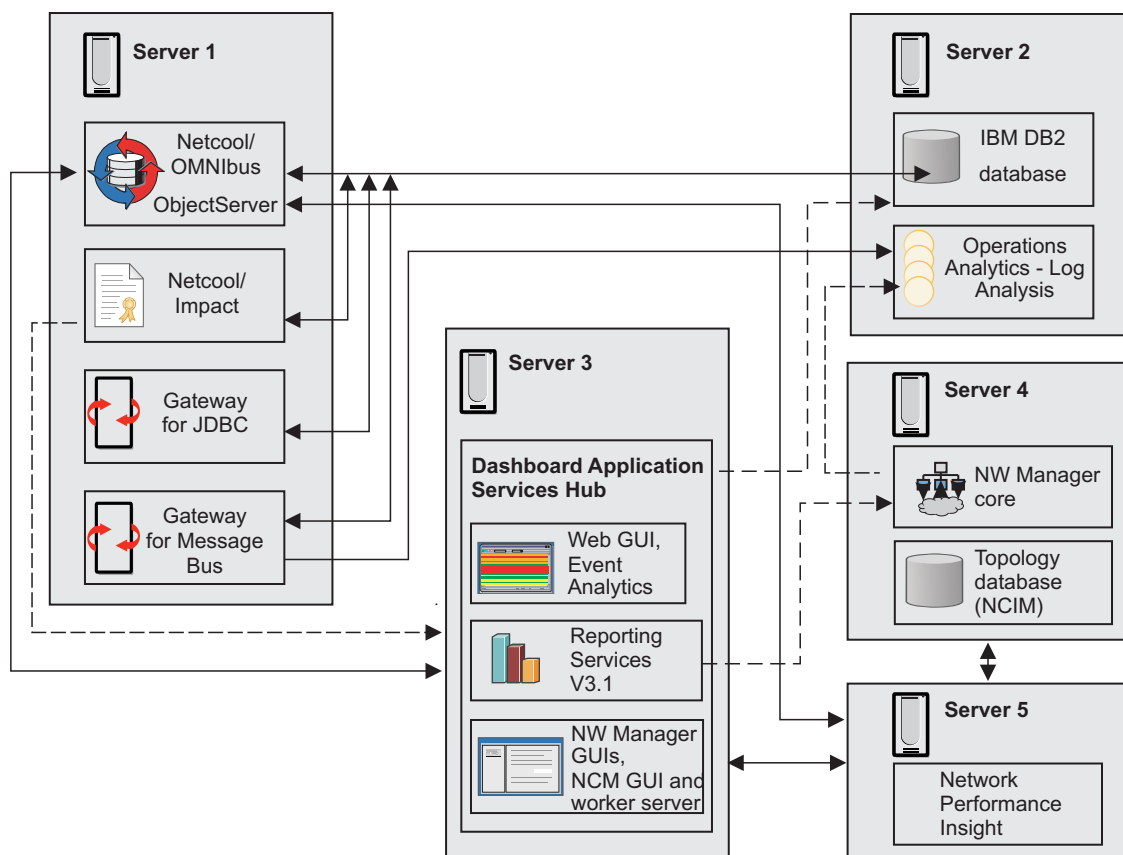


Figure 7. Simplified installation architecture for the installation scenario

For information on the product and component versions supported in the current version of Netcool Operations Insight including supported fix packs, see “Supported products and components” on page 3.

Server 1

Hosts the Netcool/OMNIBus core components, the Gateway for JDBC, Gateway for Message Bus, and Netcool/Impact. Configurations are applied to the ObjectServer to support the event analytics and topology search capabilities. Event analytics is part of the base Netcool Operations Insight solution. Topology search is part of the Networks for Operations Insight feature. The default configuration of the Gateway for Message Bus is to transfer event inserts to Operations Analytics - Log Analysis through an IDUC channel. This connection can be changed to forward events reinserts and inserts through the Accelerated Event Notification client.

Server 2

Hosts an IBM DB2 database and Operations Analytics - Log Analysis. The Tivoli Netcool/OMNIBus Insight Pack and the Network Manager Insight Pack are installed into Operations Analytics - Log Analysis. The Tivoli Netcool/OMNIBus Insight Pack is part of the base Netcool Operations Insight solution. The Network Manager Insight Pack is part of the Networks for Operations Insight feature. The REPORTER schema is applied to the DB2 database so that events can be transferred from the Gateway for JDBC. Various installation methods are possible for DB2. For more information, see <https://ibm.biz/BdEWtm>.

Server 3

Hosts Dashboard Application Services Hub, which is a component of Jazz for Service Management. Jazz for Service Management provides the GUI

framework and the Reporting Services component. The Netcool/OMNIBus Web GUI and the Event Analytics component are installed into Dashboard Application Services Hub. In this setup Reporting Services is also installed on this server, together with parts of the Networks for Operations Insight feature: the Network Manager GUI components and Netcool Configuration Manager. This simplifies the configuration of the GUI server, and provides the reporting engine and the report templates provided by the products on one host.

Note: You can set up Network Manager and Netcool Configuration Manager to work with Reporting Services by installing their respective reports when installing the products. Netcool/OMNIBus V8.1 and later can be integrated with Reporting Services V3.1 to support reporting on events. To configure this integration, connect Reporting Services to a relational database through a gateway. Then, import the report package that is supplied with Netcool/OMNIBus into Reporting Services. For more information about event reporting, see http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/omnibus/wip/install/task/omn_con_ext_deploytcreports.html.

Server 4

Hosts the Network Manager core components and the NCIM topology database, components of the Networks for Operations Insight feature. This setup assumes large networks where discovering the network and creating and maintaining the network topology can require significant system resources.

Server 5

Hosts the Network Performance Insight components that supports the performance management feature. For information on installation and configuration of Network Performance Insight, see “Installing Network Performance Insight and configuring integration with Netcool Operations Insight” on page 82.

Related information:

 Importing event summary reports into Tivoli Common Reporting

Checking prerequisites

Before you install each product, run the IBM Prerequisite Scanner (PRS) to ensure that the target host is suitable, and no installation problems are foreseeable. Also check the maxproc and ulimit settings on the servers you are configuring to ensure they are set to the appropriate minimum values.

Before you begin

- For information about hardware and software compatibility of each component, and detailed system requirements, see the IBM Software Product Compatibility Reports website: <http://www-969.ibm.com/software/reports/compatibility/clarity/index.html>

Tip: When you create a report, search for Netcool Operations Insight and select your version (for example, V1.4). In the report, additional useful information is available through hover help and additional links.

For example, to check the compatibility with an operating system for each component, go to the **Operating Systems** tab, find the row for your operating system, and hover over the icon in the **Components** column. For more detailed information about restrictions, click the **View** link in the **Details** column.

- Download IBM Prerequisite Scanner from IBM Fix Central at <http://www.ibm.com/support/fixcentral/>. Search for “IBM Prerequisite Scanner”.
- After you download the latest available version, decompress the .tar archive into the target directory on all hosts.
- On the IBM Tivoli Netcool/Impact host, set the environment variable `IMPACT_PREREQ_BOTH=True` so that the host is scanned for both the Impact Server and the GUI Server.

For a list of all product codes, see <http://www.ibm.com/support/docview.wss?uid=swg27041454>

About this task

Operations Analytics - Log Analysis and IBM DB2 are not supported by IBM Prerequisite Scanner. For the installation and system requirements for these products, refer to the documentation.

Procedure

Using the IBM Prerequisite Scanner

- On the IBM Tivoli Netcool/OMNIBus and IBM Tivoli Netcool/Impact host, run IBM Prerequisite Scanner as follows:

Product	Command
IBM Tivoli Netcool/OMNIBus	<code>prereq_checker.sh NOC detail</code>
IBM Tivoli Netcool/Impact	<code>prereq_checker.sh NCI detail</code>

- On the host for the GUI components:

Product	Command
Jazz for Service Management	<code>prereq_checker.sh ODP detail</code>
Dashboard Application Services Hub	<code>prereq_checker.sh DSH detail</code>
IBM Tivoli Netcool/OMNIBus Web GUI	<code>prereq_checker.sh NOW detail</code>

- On the Networks for Operations Insight host

Product	Command
IBM Tivoli Network Manager	<code>prereq_checker.sh TNM detail</code>
IBM Tivoli Netcool Configuration Manager	<code>prereq_checker.sh NCM detail</code>
Tivoli Common Reporting	<code>prereq_checker.sh TCR detail</code>

Check the maxproc settings.

- Open the following file: `/etc/security/limits.d/90-nproc.conf`
- Set `nproc` to a value of 131073

Check the ulimit settings.

- Open the following file: `/etc/security/limits.conf`
- Set `nofile` to a value of 131073

Related tasks:

 Installation prerequisites for Operations Analytics - Log Analysis V1.3.5

 Installation prerequisites for Operations Analytics - Log Analysis V1.3.3

➡ System requirements for DB2 products

➡ Installation requirements for DB2 products

Obtaining IBM Installation Manager

Perform this task only if you are installing directly from an IBM repository or a local repository. IBM Installation Manager is required on the computers that host Netcool/OMNIbus, Netcool/Impact, Operations Analytics - Log Analysis, and the products and components that are based on Dashboard Application Services Hub. In this scenario, that is servers 1, 2, and 3. The installation packages of the products include Installation Manager.

Before you begin

Create an IBM ID at <http://www.ibm.com>. You need an IBM ID to download software from IBM Fix Central.

Note:

On Red Hat Enterprise Linux, the GUI mode of the Installation Manager uses the libcairo UI libraries. The latest updates for RHEL 6 contain a known issue that causes the Installation Manager to crash. Before installing Installation Manager on Red Hat Enterprise Linux 6, follow the instructions in the following technote to configure libcairo UI libraries to a supported version: <http://www.ibm.com/support/docview.wss?uid=swg21690056>

If an update is not possible, a workaround to this issue is documented in this technote: <http://www.ibm.com/support/docview.wss?uid=swg21688528>

Remember: The installation image of Netcool/OMNIbus 8.1 available from IBM Passport Advantage and on DVD includes Installation Manager. You only need to download Installation Manager separately if you are installing Netcool/OMNIbus directly from an IBM repository or from a local repository.

You can install Installation Manager in one of three user modes: Administrator mode, Nonadministrator mode, or Group mode. The user modes determine who can run Installation Manager and where product data is stored. The following table shows the supported Installation Manager user modes for products in IBM Netcool Operations Insight.

Table 13. Supported Installation Manager user modes

Product	Administrator mode	Nonadministrator mode	Group mode
IBM Tivoli Netcool/OMNIbus (Includes OMNIbus Core, Web GUI, and the Gateways.)	X	X	X
IBM Tivoli Netcool/Impact	X	X	X

Table 13. Supported Installation Manager user modes (continued)

Product	Administrator mode	Nonadministrator mode	Group mode
IBM Operations Analytics - Log Analysis (Insight Packs are installed by the Operations Analytics - Log Analysis pkg_mgmt command.)		X	

Procedure

The IBM Fix Central website offers two approaches to finding product files: **Select product** and **Find product**. The following instructions apply to the **Find product** option.

- Go to IBM Fix Central at <http://www.ibm.com/support/fixcentral/> and search for **IBM Installation Manager**.
 - On the **Find product** tab, enter IBM Installation Manager in the **Product selector** field.
 - Select V1.8.2.1 (or later) from the **Installed Version** list.
 - Select your intended host operating system from the **Platform** list and click **Continue**.
- On the Identity Fixes page, choose **Browse for fixes** and **Show fixes that apply to this version (1.X.X.X)**. Click **Continue**.
- On the Select Fixes page, select the installation file appropriate to your intended host operating system and click **Continue**.
- When prompted, enter your IBM ID and password.
- If your browser has Java™ enabled, choose the Download Director option. Otherwise, select the HTTP download option.
- Start the installation file download. Make a note of the download location.

What to do next

Install Installation Manager. See <http://www.ibm.com/support/docview.wss?uid=swg24034941>.

Related information:

 [IBM Installation Manager overview](#)

Installing Installation Manager (GUI or console example)

You can install Installation Manager with a wizard-style GUI or an interactive console, as depicted in this example.

Before you begin

Take the following actions:

- Extract the contents of the Installation Manager installation file to a suitable temporary directory.
- Ensure that the necessary user permissions are in place for your intended installation, data, and shared directories.
- The console installer does not report required disk space. Ensure that you have enough free space before you start a console installation.

Before running the Installation Manager installer, create the following target directories and set the file permissions for the designated user and group that Installation Manager will be run as, and any subsequent product installations:

Main installation directory

Location where the product binaries will be installed.

Data directory

Location where Installation Manager stores information about installed products.

Shared directory

Location where Installation Manager stores downloaded packages used for rollback.

Ensure that these directories are separate. For example:

```
mkdir /opt/IBM/NetcoolIM
mkdir /opt/IBM/NetcoolIM/IBMIM
mkdir /opt/IBM/NetcoolIM/IBMIMData
mkdir /opt/IBM/NetcoolIM/IBMIMShared
chown -R netcool:ncadmin /opt/IBM/NetcoolIM
```

About this task

The initial installation steps are different depending on which user mode you use. The steps for completing the installation are common to all user modes and operating systems.

Installation Manager takes account of your current umask settings when it sets the permissions mode of the files and directories that it installs. Using Group mode, Installation Manager ignores any group bits that are set and uses a umask of 2 if the resulting value is 0.

Procedure

1. To install in Group mode:
 - a. Use the `id` utility to verify that your current effective user group is suitable for the installation. If necessary, use the following command to start a new shell with the correct effective group:
`newgrp group_name`
 - b. Use the `umask` utility to check your umask value. If necessary, change the umask value.

- c. Change to the temporary directory that contains the Installation Manager installation files.
- d. Use the following command to start the installation:

GUI installation

```
./groupinst -dL data_location
```

Console installation

```
./groupinstc -c -dL data_location
```

Where *data_location* specifies the data directory. You must specify a data directory that all members of the group can access.

Remember: Each instance of Installation Manager requires a different data directory

2. Follow the installer instructions to complete the installation. The installer requires the following input at different stages of the installation:

GUI installation

- In the first panel, select the Installation Manager package.
- Read and accept the license agreement.
- When prompted, enter an installation directory or accept the default directory.
- Verify that the total installation size does not exceed the available disk space.
- When prompted, restart Installation Manager.

Console installation

- Read and accept the license agreement.
- When prompted, enter an installation directory or accept the default directory.
- If required, generate a response file. Enter the directory path and a file name with a .xml extension. The response file is generated before installation completes.
- When prompted, restart Installation Manager.

Results

Installation Manager is installed and can now be used to install IBM Netcool Operations Insight.

What to do next

If required, add the Installation Manager installation directory path to your PATH environment variable.

Installing Netcool/OMNIBus and Netcool/Impact

Obtain and install the Netcool/OMNIBus core components, Netcool/Impact, and the Gateway for JDBC and Gateway for Message Bus. All these products are installed by IBM Installation Manager. You can use IBM Installation Manager to download the installation packages for these products and install them in a single flow. Extra configuration of each product is required after installation.

Procedure

- Install the Netcool/OMNIBus V8.1 core components. After the installation, you can use the Initial Configuration Wizard (**nco_icw**) to configure the product, for example, create and start ObjectServers, and configure automated failover or a multitier architecture. See related links later for instructions on installing Netcool/OMNIBus.
- Install the Netcool/Impact GUI server and Impact server. See related links later for instructions on installing Netcool/Impact.
- Apply the latest supported Netcool/OMNIBus core and Netcool/Impact fix packs. Also ensure that you apply the appropriate IBM Tivoli Netcool/Impact Server Extensions for Netcool Operations Insight feature. This is delivered in the Netcool/Impact fix pack. For information on the product and component versions supported in the current version of Netcool Operations Insight including supported fix packs, see “Supported products and components” on page 3 The IBM Tivoli Netcool/Impact Server Extensions for Netcool Operations Insight feature is required for the event analytics capability. Fix packs are available from IBM Fix Central, see <http://www.ibm.com/support/fixcentral/>.
- Create the connection from Netcool/Impact to the DB2 database as described in “Configuring DB2 database connection within Impact” on page 202.
- Configure the ObjectServer to support the related events function of the event analytics capability. This requires a ParentIdentifier column in the alerts.status table. Add the column using the SQL utility as described in “Configuring the Event Analytics ObjectServer” on page 199.
- Configure the ObjectServer to support the topology search capability. In `$NCHOME/omnibus/extensions`, run the **nco_sql** utility against the `scala_itnm_configuration.sql` file.

```
./nco_sql -user root -password myp4ss -server NCOMS  
< /opt/IBM/tivoli/netcool/omnibus/extensions/scala/scala_itnm_configuration.sql
```

Triggers are applied to the ObjectServer that delay the storage of events until the events are enriched by Network Manager data from the NCIM database.

- Install the Gateway for JDBC and Gateway for Message Bus. After installation, create the connection between the ObjectServer and the gateways in the Server Editor (**nco_xigen**). See related links later for instructions on creating connections in the Server Editor.
- Configure the integration between Netcool/Impact and IBM Connections. This involves importing the `$IMPACT_HOME/add-ons/IBMConnections/importData` project into Netcool/Impact and adding IBM Connections properties to the `$IMPACT_HOME/etc/NCI_server.props` file. After you edit this file, restart the Netcool/Impact server. See related links later for instructions on configuring integration to IBM Connections and restarting the Impact server.

What to do next

Search on IBM Fix Central for available interim fixes and apply them. See <http://www.ibm.com/support/fixcentral/>.

Related concepts:

➞ Connections in the Server Editor

Related tasks:

➞ Installing Tivoli Netcool/OMNIBus

➞ Creating and running ObjectServers

“Configuring DB2 database connection within Impact” on page 202

“Configuring the Event Analytics ObjectServer” on page 199

“Configuring integration to IBM Connections” on page 283

➞ Restarting the Impact server

Related reference:

“Deployment considerations for Netcool/OMNIBus and the connection to Operations Analytics - Log Analysis” on page 8

➞ Initial configuration wizard

“Ports used by products and components” on page 15

Related information:

➞ Installing Netcool/Impact

Installing DB2 and configuring the REPORTER schema

Netcool Operations Insight requires a DB2 database with the REPORTER schema for historical event archiving.

Tip: For information on the housekeeping of historical DB2 event data, as well as sample SQL scripts, see the 'Historical event archive sizing guidance' section in the *Netcool/OMNIBus Best Practices Guide*, which can be found on the Netcool/OMNIBus best-practice Wiki: http://ibm.biz/nco_bps

Procedure

- Obtain and download the package for the DB2 database and the Gateway configuration scripts.
- Decompress the packages. Then, as the root system user, run the **db2setup** command to install the DB2 database on the host. The **db2setup** command starts the DB2 Setup wizard. Install as the root system user because the setup wizard needs to create a number of users in the process.
- Run IBM Installation Manager on the Netcool/OMNIBus host and install the Gateway configuration scripts. The SQL file that is needed to create the REPORTER schema is installed to `$OMNIBUS_HOME/gates/reporting/db2/db2.reporting.sql`.
- In the `db2.reporting.sql` file, make the following changes.
 - Uncomment the CREATE DATABASE line.
 - Set the default user name and password to match the DB2 installation:

```
CREATE DATABASE reporter @
CONNECT TO reporter USER db2inst1 USING db2inst1 @
```
 - Uncomment the following lines, so that any associated journal and details rows are deleted from the database when the corresponding alerts are deleted:

```
-- Uncomment the line below to enable foreign keys
-- This helps pruning by only requiring the alert to be
-- deleted from the status table
, CONSTRAINT eventref FOREIGN KEY (SERVERNAME, SERVERSERIAL) REFERENCES
REPORTER_STATUS(SERVERNAME, SERVERSERIAL) ON DELETE CASCADE)
```

This SQL appears twice in the SQL file: once in the details table definition and once in the journal table definition. Uncomment both instances.

- Run the SQL file against the DB2 database by running the following command as the db2inst1 system user:
\$ db2 -td@ -vf db2.reporting.sql

Result

The DB2 installer creates a number of users including db2inst1.

Related reference:

“Ports used by products and components” on page 15

Related information:

-  Installing DB2 servers using the DB2 Setup wizard (Linux and UNIX)
-  Gateway for JDBC configuration scripts for Reporting Mode

Installing IBM Operations Analytics - Log Analysis

Operations Analytics - Log Analysis supports GUI, console, and silent installations. The installation process differs for 64-bit and z/OS operating systems.

Procedure

Operations Analytics - Log Analysis can be installed by IBM Installation Manager or you can run the install.sh wrapper script.

Tip: The best practice is to install the Web GUI and Operations Analytics - Log Analysis on separate hosts.

Restriction: Operations Analytics - Log Analysis does not support installation in Group mode of IBM Installation Manager.

What to do next

- If the host locale is not set to English United States, set the locale of the command shell to export LANG=en_US.UTF-8 before you run any Operations Analytics - Log Analysis scripts.
- If you plan to deploy only the base Netcool Operations Insight solution, install the Tivoli Netcool/OMNIBus Insight Pack. See “Installing the Insight Packs” on page 79. Complete only the steps that describe the Tivoli Netcool/OMNIBus Insight Pack.
- Search on IBM Fix Central for available interim fixes and apply them. See <http://www.ibm.com/support/fixcentral/>.

Related tasks:

-  Installing Operations Analytics - Log Analysis V1.3.5
-  Installing Operations Analytics - Log Analysis V1.3.3

Related reference:

“Ports used by products and components” on page 15

Configuring the Gateway for JDBC and Gateway for Message Bus

Configure the Gateway for JDBC to run in reporting mode, so it can forward event data to the DB2 database for archiving. Configure the Gateway for Message Bus gateway to forward event data to Operations Analytics - Log Analysis and run it in Operations Analytics - Log Analysis mode.

Before you begin

- Install the DB2 database and configure the REPORTER schema so that the Gateway for JDBC can connect.
- Install the gateways on the same host as Tivoli Netcool/OMNIBus core components (that is, server 1).
- Install Operations Analytics - Log Analysis and obtain the URL for the connection to the Gateway for Message Bus.

Procedure

- Configure the Gateway for JDBC. This involves the following steps:
 - Obtain the JDBC driver for the target database from the database vendor and install it according to the vendor's instructions. The drivers are usually provided as .jar files.
 - To enable the gateway to communicate with the target database, you must specify values for the **Gate.Jdbc.*** properties in the \$OMNIHOME/etc/G_JDBC.props file. This is the default properties file, which is configured for reporting mode, that is supplied with the gateway.

Here is a sample properties file for the Gateway for JDBC.

```
# Reporting mode properties
Gate.Jdbc.Mode: 'REPORTING'
# Table properties
Gate.Jdbc.StatusTableName: 'REPORTER_STATUS'
Gate.Jdbc.JournalTableName: 'REPORTER_JOURNAL'
Gate.Jdbc.DetailsTableName: 'REPORTER_DETAILS'
# JDBC Connection properties
Gate.Jdbc.Driver: 'com.ibm.db2.jcc.DB2Driver'
Gate.Jdbc.Url: 'jdbc:db2://server3:50000/REPORTER'
Gate.Jdbc.Username: 'db2inst1'
Gate.Jdbc.Password: 'db2inst1'
Gate.Jdbc.ReconnectTimeout: 30
Gate.Jdbc.InitializationString: ''
# ObjectServer Connection properties
Gate.RdrWtr.Username: 'root'
Gate.RdrWtr.Password: 'netcool'
Gate.RdrWtr.Server: 'AGG_V'
```

- Configure the Gateway for Message Bus to forward event data to Operations Analytics - Log Analysis. This involves the following steps:
 - Creating a gateway server in the Netcool/OMNIBus interfaces file
 - Configuring the G_SCALA.props properties file, including specifying the .map mapping file.
 - Configuring the endpoint in the scalaTransformers.xml file
 - Configuring the SSL connection, if required
 - Configuring the transport properties in the scalaTransport.properties file
- If you do not want to use the default configuration of the Gateway for Message Bus (an IDUC channel between the ObjectServer and Operations Analytics - Log

Analysis and supports event inserts only)), configure event forwarding through the AEN client. This support event inserts and reinserts and involves the following steps:

- Configuring AEN event forwarding in the Gateway for Message Bus
- Configuring the AEN channel and triggers in each ObjectServer by enabling the postinsert triggers and trigger group
- Start the Gateway for Message Bus in Operations Analytics - Log Analysis mode. For example:
`$OMNIHOME/bin/nco_g_xml -propsfile $OMNIHOME/etc/G_SCALA.props`

The gateway begins sending events from Tivoli Netcool/OMNIBus to Operations Analytics - Log Analysis.

- Start the Gateway for JDBC in reporter mode. For example:
`$OMNIHOME/bin/nco_g_jdbc -jdbcreporter`
- As an alternative to starting the gateways from the command-line interface, put them under process control. For more information about process control, see the *IBM Tivoli Netcool/OMNIBus Administration Guide*.

Related concepts:

Tivoli Netcool/OMNIBus process control

Related information:

Gateway for JDBC documentation

Gateway for Message Bus documentation

Installing Dashboard Application Services Hub and the UI components

Install the Dashboard Application Services Hub and all the UI components. This applies to the Netcool/OMNIBus Web GUI, the Event Analytics component, fix packs, and optionally Reporting Services.

The UI components are installed in two stages. First, IBM WebSphere Application Server and Jazz for Service Management are installed, which provide the underlying UI technology. Then, the Web GUI and the extension packages that support the Event Analytics component and the event search capability are installed. After installation, configure the Web GUI to integrate with Operations Analytics - Log Analysis and support the topology search capability.

You can optionally install Reporting Services V3.1 into Dashboard Application Services Hub. You can set up Network Manager and Netcool Configuration Manager to work with Reporting Services by installing their respective reports when installing the products. Netcool/OMNIBus V8.1 and later can be integrated with Reporting Services V3.1 to support reporting on events. To configure this integration, connect Reporting Services to a relational database through a gateway. Then, import the report package that is supplied with Netcool/OMNIBus into Reporting Services. For more information about event reporting, see http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/omnibus/wip/install/task/omn_con_ext_deployctrreports.html.

Before you begin

- Obtain the packages from IBM Passport Advantage. For information about the eAssembly numbers you need for the packages, see <http://www-01.ibm.com/support/docview.wss?uid=swg24043517>.

- To install Reporting Services V3.1, ensure that the host meets the extra requirements at http://www.ibm.com/support/knowledgecenter/SSEKCU_1.1.3.0/com.ibm.psc.doc/install/tcr_c_install_prereqs.html.
- IBM Installation Manager V1.8.4.1 or later is required before installing the Web GUI V8.1 fix pack.

Procedure

1. Start Installation Manager and install Jazz for Service Management. The packages that you need to install are as follows.

Package	Description
IBM WebSphere Application Server V8.5.5.9 (or later) for Jazz for Service Management	Select V8.5.5.9 (or later). If V8.0.5 is also identified, clear it.
IBM WebSphere SDK Java Technology Edition V7.0.x.	
Jazz for Service Management V1.1.3.0	Select the following items for installation. • Jazz for Service Management extension for IBM WebSphere V8.5. • Dashboard Application Services Hub V3.1.3.0.
Reporting Services V3.1	This package is optional. Select it if you want to run reports for events and network management.

2. Install the packages that constitute the Web GUI and extensions.

Package	Description
Netcool/OMNIBus Web GUI	This is the base component that installs the Web GUI.
Install tools and menus for event search with IBM SmartCloud Analytics - Log Analysis	This package installs the tools that launch the custom apps of the Tivoli Netcool/OMNIBus Insight Pack from the event lists.
Netcool Operations Insight Extensions for IBM Tivoli Netcool/OMNIBus Web GUI	This package installs the Event Analytics GUIs.
Netcool/OMNIBus Web GUI V8.1 fix pack, as specified in "Supported products and components" on page 3.	This is the fix pack that contains the extensions for the topology search capability.

3. Configure the Web GUI. For example, the connection to a data source (ObjectServer), users, groups, and so on. You can use the Web GUI configuration tool to do this. For more information, see <https://ibm.biz/BdXqcP>.
4. Configure the integration with Operations Analytics - Log Analysis. Ensure that the server.init file has the following properties set:

```
scala.app.keyword=OMNIBus_Keyword_Search
scala.app.static.dashboard=OMNIBus_Static_Dashboard
scala.datasource=omnibus
scala.url=protocol://host:port
scala.version=1.2.0.3
```

If you need to change any of these values, restart the Web GUI server.

5. Set up the Web GUI Administration API client.
6. Install the tools and menus to launch the custom apps of the Network Manager Insight Pack in the Operations Analytics - Log Analysis UI from the Web GUI. In `$WEBGUI_HOME/extensions/LogAnalytics`, run the **runwaapi** command against the `scalaEventTopology.xml` file.

```
$WEBGUI_HOME/waapi/bin/runwaapi -user username -password password -file  
scalaEventTopology.xml
```

Where *username* and *password* are the credentials of the administrator user that are defined in the `$WEBGUI_HOME/waapi/etc/waapi.init` properties file that controls the WAAPI client.

What to do next

- Search on IBM Fix Central for available interim fixes and apply them. See <http://www.ibm.com/support/fixcentral/>.
- Reconfigure your views in the Web GUI event lists to display the **NmosObjInst** column. The tools that launch the custom apps of the Network Manager Insight Pack work only against events that have a value in this column. For more information, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide*.

Related concepts:

"Installing and uninstalling Event Analytics" on page 112

Related tasks:

Installing the Web GUI

Restarting the server

Related reference:

server.init properties

"Ports used by products and components" on page 15

Installing the Networks for Operations Insight feature

This installation scenario describes how to set up the Networks for Operations Insight feature in the Netcool Operations Insight solution. A sample system topology is given on which the installation tasks are based. It is assumed that the core products of the Netcool Operations Insight solution are already installed and running.

The information supplied in this scenario is high-level and covers the most salient points and possible issues you might encounter that are specific to the Networks for Operations Insight feature in the Netcool Operations Insight solution. This scenario is end-to-end and you should perform the tasks in the specified order.

For more information, see the Related concept, task, and information links at the bottom of this topic.

Before you begin

- Install the components of Netcool Operations Insight as described in "Supported products and components" on page 3. The Networks for Operations Insight solution requires that the following products are installed, configured, and running as follows:

- The Tivoli Netcool/OMNIbus V8.1 server components are installed and an ObjectServer is created and running. Ensure that the administrator user of the ObjectServer was changed from the default.
- The Tivoli Netcool/OMNIbus V8.1 Web GUI is installed and running in an instance of Dashboard Application Services Hub. The ObjectServer is defined as the Web GUI data source.
- An IBM DB2 database is installed and configured for event archiving, and the Gateway for JDBC is installed and configured to transfer and synchronize the events from the ObjectServer.
- IBM Operations Analytics - Log Analysis is installed and running, and configured so that events are forwarded from Tivoli Netcool/OMNIbus to Operations Analytics - Log Analysis via the Gateway for Message Bus. See “Configuring event search” on page 94.
- Obtain the following information about the ObjectServer:
 - Host name and port number
 - Installation directory (that is, the value of the \$OMNIHOME environment variable)
 - Name, for example, NCOMS
 - Administrator password
- Install and configure the event search and event seasonality features.

If any of the above products are not installed, or features not configured, they must be configured before you can set up the Networks for Operations Insight feature.

About this task

This task and the sub-tasks describe the scenario of a fresh deployment of the products in the Networks for Operations Insight feature. The system topology is a logical sample. It is not the only system topology that can be used. It is intended for reference and to help you plan your deployment. The system topology is as follows:

- Tivoli Netcool/OMNIbus and Network Manager are installed on separate hosts (that is, a distributed installation). The version of Tivoli Netcool/OMNIbus is 8.1.
- The ObjectServer is configured to be the user repository for the products.

Note: All the products of the Netcool Operations Insight solution also support the use of an LDAP directory as the user repository.

- Network Manager and Netcool Configuration Manager both use the V8.1 ObjectServer to store and manage events.
- In this topology, the default DB2 v10.5 Enterprise Server Edition database is used.

Related concepts:

“Networks for Operations Insight data flow” on page 19

Related tasks:

“Installing Network Performance Insight and configuring integration with Netcool Operations Insight” on page 82

Related reference:

“Release notes” on page 289

Installing the Probe for SNMP and Syslog Probe

The Networks for Operations Insight feature requires the Probe for SNMP and the Syslog Probe. It is important that you install the probes that are included in the entitlement for the Tivoli Netcool/OMNIbus V8.1 product. Although the probes are also available in the Network Manager entitlement, do not install them from Network Manager. The instances of the probes that are available with Tivoli Netcool/OMNIbus V8.1 are installed by IBM Installation Manager.

Procedure

1. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory and run the following command to start Installation Manager:

```
./IBMIM
```

To record the installation steps in a response file for use with silent installations on other computers, use the `-record` option. For example, to record to the `/tmp/install_1.xml` file:

```
./IBMIM -record /tmp/install_1.xml
```

2. Configure Installation Manager to download package repositories from IBM Passport Advantage®.
3. In the main Installation Manager pane, click **Install** and follow the installation wizard instructions to complete the installation. The installer requires the following inputs at different stages of the installation:
 - If prompted, enter your IBM ID user name and password.
 - Read and accept the license agreement.
 - Specify an Installation Manager shared directory or accept the default directory.

Select the `nco-p-syslog` feature for the Syslog Probe, and select the `nco-p-mttrapd` feature for the Probe for SNMP. After the installation completes, click **Finish**.

Results

If the installation is successful, Installation Manager displays a success message and the installation history is updated to record the successful installation. If not, you can use Installation Manager to uninstall or modify the installation.

What to do next

Ensure that both probes are configured:

- For more information about configuring the Probe for SNMP, see http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/probes/snmp/wip/reference/snmp_config.html.
- For more information about configuring the Syslog Probe, see http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/probes/syslog/wip/concept/syslog_intro.html.

Related tasks:

 Installing and configuring IBM Installation Manager

 Installing Tivoli Netcool/OMNIbus V8.1

Related reference:

 Tivoli Netcool/OMNIbus V8.1 installable features

Optional: Preparing the ObjectServer for integration with Network Manager

If you have already installed Tivoli Netcool/OMNIBus, the Netcool/OMNIBus Knowledge Library, and the Probe for SNMP, you can now install Network Manager, and do not need to follow the steps in this task. The Network Manager installer configures Tivoli Netcool/OMNIBus for you during the installation process. If the ObjectServer setup changes after you have already installed and configured Network Manager and Tivoli Netcool/OMNIBus, then you must reintegrate the ObjectServer with Network Manager as described in this topic.

To reintegrate the Network Manager product with the existing Tivoli Netcool/OMNIBus V8.1 ObjectServer, run the **ConfigOMNI** script against the ObjectServer.

Procedure

1. Use the **ConfigOMNI** script to configure an ObjectServer to run with Network Manager.

The script creates the Network Manager triggers and GUI account information. If the ObjectServer is on a remote server, then copy the \$NCHOME/precision/install/scripts/ConfigOMNI script and the support script \$NCHOME/precision/scripts/create_itnm_triggers.sql and put them into the same directory on the remote ObjectServer. If the ObjectServer is local to Network Manager, then you can use both scripts as is.

2. On the ObjectServer host, change to the scripts directory and run the **ConfigOMNI** script.

For example, the following configures the ObjectServer called NCOMS2 using the administrative password NC0M5password, or creates the ObjectServer called NCOMS2 if it does not exist, in the specified directory (OMNIHOME), and creates or modifies the itnadmin and itnmuser users in the ObjectServer.

```
./ConfigOMNI -o NCOMS2 -p NC0M5password -h /opt/ibm/tivoli/netcool  
-u ITNMPassword
```

3. You might also need to update the Network Manager core settings and the Web GUI data source settings. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/install/task/nmip_ins_installingandconfiguringomnibus.html.

Related tasks:

 Installing and configuring Tivoli Netcool/OMNIBus

Preparing the database for Network Manager

After a supported database has been installed, you must install and run the database scripts to configure the topology database for use by Network Manager. You must run the scripts before installing Network Manager.

About this task

If you downloaded the compressed software package from Passport Advantage, the database creation scripts are included at the top level of the uncompressed software file. Copy the scripts to the database server and use them.

You can also install the Network Manager topology database creation scripts using Installation Manager by selecting the **Network Manager topology database creation scripts** package. The database scripts are installed by default in the precision/scripts/ directory in the installation directory (by default, /opt/IBM/netcool/core/precision/scripts/).

Procedure

1. Log in to the server where you installed DB2.
2. Change to the directory where your DB2 instance was installed and then change to the sqllib subdirectory.
3. Set up the environment by typing the following command:

Shell	Command
Bourne	<code>./db2profile</code>
C	<code>source db2cshrc</code>

The Network Manager application wrapper scripts automatically set up the DB2 environment.

4. Locate the compressed database creation file `db2_creation_scripts.tar.gz` and copy it to the server where DB2 is installed. Decompress the file.
5. Change to the `precision/scripts/` directory and run the `create_db2_database.sh` script as the DB2 administrative user for the instance (db2inst1):

```
./create_db2_database.sh database_name user_name -force
```

Where *database_name* is the name of the database, *user_name* is the DB2 user to use to connect to the database, and `-force` an argument that forces any DB2 users off the instance before the database is created.

Important: The *user_name* must not be the administrative user. This user must be an existing operating system and DB2 user.

For example, to create a DB2 database that is called ITNM for the DB2 user `ncim`, type:

```
./create_db2_database.sh ITNM ncim
```

6. After you run `create_db2_database.sh`, restart the database as the DB2 administrative user as follows: **run db2stop** and then **run db2start**.
7. When running the Network Manager installer later on, make sure you select the option to configure an existing DB2 database. The Network Manager installer can then create the tables in the database either on the local or a remote host, depending on where your database is installed.

The installer populates the connection properties in the following files, you can check these files for any problems with your connection to the database:

- The `DbLogins.DOMAIN.cfg` and `MibDbLogin.cfg` files in `$NCHOME/etc/precision`. These files are used by the Network Manager core processes.
- The `tnm.properties` file in `$NMGUI_HOME/profile/etc/tnm`. These files are used by the Network Manager GUI.

Installing Network Manager and Netcool Configuration Manager

Install Network Manager and Netcool Configuration Manager to form the basis of the Networks for Operations Insight feature.

Before you begin

- Ensure you have installed and configured the base products and components of Netcool Operations Insight, including Tivoli Netcool/OMNIBus, Netcool/Impact, and Operations Analytics - Log Analysis, and the associated components and configurations. See Supported products for Networks for Operations Insight.
- Obtain the following information about the ObjectServer:
 - ObjectServer name, for example, NCOMS

- Host name and port number
- Administrator user ID
- Administrator password
- Obtain the following information about your DB2 database:
 - Database name
 - Host name and port number
 - Administrator user ID with permissions to create tables
 - Administrator user password
- Obtain the packages from IBM Passport Advantage. For information about the eAssembly numbers you need for the packages, see <http://www-01.ibm.com/support/docview.wss?uid=swg24043517>.
- Obtain the latest supported fix packs for Network Manager and Netcool Configuration Manager from IBM Fix Central, at <http://www.ibm.com/support/fixcentral/>. For information on the product and component versions supported in the current version of Netcool Operations Insight including supported fix packs, see “Supported products and components” on page 3.
- Ensure that a compatible version of Python is installed on this server before you start. On Linux, Network Manager core components require version 2.6 or 2.7 of Python to be installed on the server where the core components are installed. On AIX, Network Manager requires version 2.7.5 of Python.

About this task

These instructions describe the options that are presented in the Installation Manager in wizard mode. Other modes are also available with equivalent options.

Procedure

1. Start Installation Manager and install the following packages:

Package	Description
Network Manager Core Components Version 4.2.0.1	Installs the Network Manager core components, sets up connection to the specified ObjectServer, sets up connection to the database to be used for the NCIM topology and creates the tables (needs to be selected), creates Network Manager default users, sets up network domain, and configures the details for the poller aggregation. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/install/task/nmip_ins_installingcorecomponents.html. Note: The Network Manager core components can be installed on server 4 of the scenario described in “Performing a fresh installation” on page 32.

Package	Description
Network Manager GUI Components Version 4.2.0.1	Installs the Network Manager GUI components, sets up connection to the specified ObjectServer, sets up connection to the NCIM topology database, and sets up the default users. For more information, see http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/install/task/nmip_ins_installingguicomponents.html. Note: The Network Manager GUI components can be installed on server 3 of the scenario described in “Performing a fresh installation” on page 32. The GUI components of other products in the solution, Netcool Configuration Manager, and Reporting Services would also be on this host.
Network Health Dashboard 4.2.0.1	Installs the Network Health Dashboard. Installing the Network Health Dashboard installs the following roles, which allow users to work with the Network Health Dashboard: • ncp_networkhealth_dashboard • ncp_networkhealth_dashboard_admin • ncp_event_analytics The new 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. A dashboard timeline reports on device configuration changes and event counts, enabling you to correlate events with configuration changes. The dashboard includes the Event Viewer, for more detailed event information. Note: The Network Health Dashboard must be installed on the same host as the Network Manager GUI components.

Package	Description
Network Manager Reports 4.2.0.1	Installs the reports provided by Network Manager that you can use as part of the Reporting Services feature. Note: Reporting Services requires a DB2 database to store its data. This database must be running during installation. If the database is installed on the same server as Reporting Services, the installer configures the database during installation. If the database is on a different server, you must configure the database before you install Reporting Services. In the scenario described in “Performing a fresh installation” on page 32, where the DB2 database is on a different server, you must set up the remote DB2 database for Reporting Services as follows: 1. From the Jazz for Service Management package, copy the <code>TCR_generate_content_store_db2_definition.sh</code> script to the server where DB2 is installed. 2. Run the following command: <pre>./TCR_generate_content_store_db2_definition.sh database_name db2_username</pre> Where <i>database_name</i> is the name you want for the Reporting Services database, and <i>db2_username</i> is the user name to connect to the content store, that is, the database owner (db2inst1). 3. Copy the generated SQL script to a temporary directory and run it against your DB2 instance as the DB2 user (db2inst1), for example: <pre>\$ cp tcr_create_db2_cs.sql /tmp/tcr_create_db2_cs.sql \$ su - db2inst1 -c "db2 -vtf /tmp/tcr_create_db2_cs.sql"</pre>

Package	Description
Netcool Configuration Manager 6.4.2.2	Installs the Netcool Configuration Manager components and loads the required database schema. For Server Installation Type, select Presentation Server and Worker Server to install both the GUI and worker servers. For more information, see http://www-01.ibm.com/support/knowledgecenter/SS7UH9_6.4.2/ncm/wip/install/task/ncm_ins_installingncm.html. Note: The Netcool Configuration Manager components can be installed on server 3 of the scenario described in “Performing a fresh installation” on page 32. For more information about fix pack 2, see http://www.ibm.com/support/knowledgecenter/SS7UH9_6.4.2/ncm/wip/relnotes/ncm_rn_6422.html.
Reporting Services environment	Installs the reports provided by Netcool Configuration Manager (ITNCM-Reports) that you can use as part of the Reporting Services feature.

2. Apply the latest supported Network Manager and Netcool Configuration Manager fix packs. For information on the product and component versions supported in the current version of Netcool Operations Insight including supported fix packs, see “Supported products and components” on page 3
3. On the host where the Network Manager GUI components are installed, install the tools and menus to launch the custom apps of the Network Manager Insight Pack in the Operations Analytics - Log Analysis GUI from the Network Views.
 - a. In \$NMGUI_HOME/profile/etc/tnm/topoviz.properties, set the **topoviz.unity.customappsui** property, which defines the connection to Operations Analytics - Log Analysis. For example:

```
# Defines the LogAnalytics custom App launcher URL
topoviz.unity.customappsui=https://server3:9987/Unity/CustomAppsUI
```
 - b. In the \$NMGUI_HOME/profile/etc/tnm/menus/ncp_topoviz_device_menu.xml file, define the **Event Search** menu item. Add the item `<menu id="Event Search"/>` in the file as shown:

```
<tool id="showConnectivityInformation"/>
    <separator/>
    <menu id="Event Search"/>
```
4. Optional: Follow the steps to configure the integration between Network Manager and Netcool Configuration Manager as described in “Configuring integration with Netcool Configuration Manager” on page 55.

Results

The ports used by each installed product or component are displayed. The ports are also written to the \$NCHOME/log/install/Configuration.log file.

What to do next

- To add the performance management feature, see “Installing Network Performance Insight and configuring integration with Netcool Operations Insight” on page 82.
- To set up the Device Dashboard for the network performance monitoring feature, see “Installing and configuring the Device Dashboard” on page 82.
- Search on IBM Fix Central for available interim fixes and apply them. See <http://www.ibm.com/support/fixcentral/>.

Related reference:

 [Installing Network Manager](#)

Related information:

 [Installing Netcool Configuration Manager](#)

 [V4.2 download document](#)

Configuring integration with Netcool Configuration Manager

After installing the products, you can configure the integration between Network Manager and Netcool Configuration Manager.

Related tasks:

 [Installing Netcool Configuration Manager](#)

Related reference:

 [Netcool Configuration Manager release notes](#)

 [Installation information checklist](#)

Related information:

 [Preparing DB2 databases for Netcool Configuration Manager](#)

User role requirements:

Certain administrative user roles are required for the integration.

Note: For single sign-on information, see the related topic links.

Dashboard Application Services Hub user roles

The following Dashboard Application Services Hub roles are required for access to the Netcool Configuration Manager components that are launched from within Dashboard Application Services Hub, such as the Netcool Configuration Manager Wizards and the Netcool Configuration Manager - Base and Netcool Configuration Manager - Compliance clients.

Either create a Dashboard Application Services Hub user with the same name as an existing Netcool Configuration Manager user who already has the 'IntellidenUser' role, or use an appropriate Network Manager user, such as itnadmin, who is already set up as a Dashboard Application Services Hub user. If you use the Network Manager user, create a corresponding new Netcool Configuration Manager user with the same name (password can differ), and assign the 'IntellidenUser' role to this new user.

Important: If a Dashboard Application Services Hub user is being created on Network Manager with the same name as an existing Netcool Configuration

Manager user. then they also need to be added to an appropriate Network Manager user group, or alternatively be granted any required Network Manager roles manually.

Additionally, assign the following roles to your Dashboard Application Services Hub user:

- ncp_rest_api
- ncmConfigChange
- ncmConfigSynch
- ncmIDTUser
- ncmPolicyCheck
- ncmActivityViewing
- ncmConfigViewing
- ncmConfigEdit
- ncmDashService

The following table cross-references security requirements between user interfaces, Dashboard Application Services Hub roles, Netcool Configuration Manager functionality, and Netcool Configuration Manager realm content permissions. Use this information to assign Dashboard Application Services Hub roles and define realm content permissions.

Table 14. UI security by Dashboard Application Services Hub roles, Netcool Configuration Manager functionality, and realm content permissions

Access	Dashboard Application Services Hub role	Functionality	Realm content permissions
Apply Modelled Command Set	ncmConfigChange	Execute Configuration Change	View, Execute
Apply Native Command Set	ncmConfigChange	Execute Configuration Change, Apply Native Command Sets	View, Execute
Synchronize (ITNCM to Device)	ncmConfigSynch	Execute Configuration Synchronization	View, Execute
Submit Configuration	ncmConfigChange	Execute Configuration Change	View, Execute
Apply Policy	ncmPolicyCheck	Execute Compliance Policy	View
View Configuration	ncmConfigViewing	n/a	View
Edit Configuration	ncmConfigEdit	n/a	View, Modify
Compare Configuration	ncmConfigViewing	n/a	View
IDT Automatic	ncmIDTUser	IDT Access, IDT Allow Auto Login	View
IDT Manual	ncmIDTUser	IDT Access, IDT Allow Manual Login	View

Table 14. UI security by Dashboard Application Services Hub roles, Netcool Configuration Manager functionality, and realm content permissions (continued)

Access	Dashboard Application Services Hub role	Functionality	Realm content permissions
Find Device	n/a	n/a	View
View UOW Log	n/a	n/a	n/a
View IDT Log	n/a	n/a	View
Activity Viewer	ncmActivityViewing	n/a	n/a
Device Synchronization	ncp_rest_api	n/a	n/a
Access Dashboard Application Services Hub services (through right-click menus)	ncmDashServices	n/a	n/a

Reporting Services user roles

Reporting Services and the Netcool Configuration Manager default reports are installed together with the Dashboard Application Services Hub components.

Any user who needs to access reports requires the following permissions:

- The relevant Reporting Services roles for accessing the **Reporting** node in the Dashboard Application Services Hub console. Assign these roles to enable users to run reports to which they are authorized from the Reporting Services GUI.
- The authorization to access the report set, and the relevant Reporting Services roles for working with the reports. Assign these permissions to enable users to run Netcool Configuration Manager reports from Network Manager topology displays, the Active Event List, and the Reporting Services GUI.

For information about authorizing access to a report set and assigning roles by user or group, go to the IBM Tivoli Systems Management Information Center at <http://www-01.ibm.com/support/knowledgecenter/SS3HLM/welcome>, locate the Reporting Services documentation node, and search for *authorization* and *user roles*.

Other user roles

To configure the **Alerts** menu in the Web GUI, the ncw_admin role is required.

Installing the Dashboard Application Services Hub components:

For integrated scenarios, Netcool Configuration Manager provides the following Dashboard Application Services Hub components: The Activity Viewer, the Dashboard Application Services Hub wizards, and the Netcool Configuration Manager thick-client launch portal.

Before you begin

From Version 6.4.2 onwards, Netcool Configuration Manager reporting is no longer installed as part of the Dashboard Application Services Hub components installation, but rather as part of the Netcool Configuration Manager main installation.

Important: Before installing the Dashboard Application Services Hub components, install Netcool Configuration Manager using the 'Integrated' option.

About this task

Restriction: The Netcool Configuration Manager Dashboard Application Services Hub components must be installed as the same user who installed Network Manager.

Procedure

1. Log onto the Dashboard Application Services Hub server.
2. Change to the /eclipse subdirectory of the Installation Manager Group installation directory and use the following command to start Installation Manager:
./IBMIM
To record the installation steps in a response file for use with silent installations on other computers, use the '-record response_file' option. For example:
IBMIM -record C:\response_files\install_1.xml

3. Configure Installation Manager to download package repositories from IBM Passport Advantage:
 - a. From the main menu, choose **File > Preferences**.
You can set preferences for proxy servers in IBM Installation Manager. Proxy servers enable connections to remote servers from behind a firewall.
 - b. In the Preferences window, expand the Internet node and select one of the following options:

FTP Proxy

Select this option to specify a SOCKS proxy host address and a SOCKS proxy port number.

HTTP Proxy

Select this option to enable an HTTP or SOCKS proxy.

- c. Select **Enable proxy server**.
 - d. In the Preferences window, select the **Passport Advantage** panel.
 - e. Select **Connect to Passport Advantage**.
 - f. Click **Apply**, and then click **OK**.
4. In the main Installation Manager window, click **Install**, select **IBM Dashboard Applications for ITNCM**, and then follow the installation wizard instructions to complete the installation.
5. Accept the license agreement, select an installation directory, and supply the following details:

Netcool Configuration Manager database details

Sid/service name/database name(db2)

Database hostname

Port

Username

Password

Dashboard Application Services Hub administrative credentials

Dashboard Application Services Hub administrator username (default is smadmin)

Dashboard Application Services Hub administrator password

Network Manager administrative credentials

Default is `itnadmin` (or the Dashboard Application Services Hub superuser, who must have the 'ncw_admin' role in Dashboard Application Services Hub)

Password

Netcool Configuration Manager presentation server

Connection details to the Netcool Configuration Manager Presentation server

A skip validation option should the Presentation server be unavailable

Reporting Services server

Connection details to the Reporting Services server

A skip validation option should the Reporting Services server be unavailable

6. Complete the installation.

What to do next

Before you can access the Netcool Configuration Manager Dashboard Application Services Hub components, you must set up the Netcool Configuration Manager Dashboard Application Services Hub users and provide them with appropriate access permission.

Once users have been set up, you access the Netcool Configuration Manager Dashboard Application Services Hub components, that is, the Activity Viewer, the Dashboard Application Services Hub wizards, and the thick-client launch portal in the following ways:

- You launch the stand-alone Netcool Configuration Manager UIs (sometimes referred to as the thick-client UIs), from the Dashboard Application Services Hub thick-client launch portal.
- You access the Activity Viewer, the Dashboard Application Services Hub wizards, and a subset of reports **in context** from Network Manager and Tivoli Netcool/OMNIBus.
- You access the complete reports using the Dashboard Application Services Hub Reporting Services GUI.

Configuring separate database types:

Under certain circumstances, such as when different or remote databases are used in an integrated environment, you must perform additional database configuration steps.

About this task

If you are installing Network Manager and ITNCM-Reports together, and if the Network Manager database is DB2 and on a different server, then its component databases must be cataloged.

If Network Manager uses an Informix database in a distributed environment and Dashboard Application Services Hub is not installed on the same server as Network Manager, you ensure that the correct library jars are used.

Procedure

1. Required: If Network Manager and ITNCM-Reports are installed together, and if the Network Manager database is DB2 and on a different server:

- a. To connect to a DB2 database on a server remote from your TCR Installation, ensure that a DB2 client is installed and the remote database cataloged. When the database server is remote to the WebSphere Application Server node where configuration is taking place, enter the following command at the node to add a TCP/IP node entry to the node directory:

```
db2 catalog tcpip node <NODENAME> remote <REMOTE> server <PORT>
```

where

NODENAME

Specifies a local alias for the node to be cataloged.

REMOTE

Specifies the fully qualified domain name of the remote DB server.

PORT Is the port on which the database is accessible, typically port 50000.

```
db2 catalog database <database_name> at node <NODENAME>
```

where

database_name

Specifies the DB2 database name.

NODENAME

Is the local alias specified in the previous step.

- b. Add 'source \$HOME/sqllib/db2profile' to your <install_user>/
.bash_profile. Where \$HOME refers to the home directory of the user
which was configured during the installation of the DB2 client to manage
the client (usually db2inst1), and <install_user> is the user who installed
Netcool Configuration Manager, usually 'icosuser'.

Note: The .bash_profile is only used for bash shell, and it will be different
for sh, csh or ksh.

- c. Restart your reporting server after this update. However, before restarting
the Reporting Server, check that the amended login profile has been
sourced.

Tip: For installations which use a DB2 database, Cognos requires 32 bit DB2
client libraries, which will be installed by the 64 bit DB2 client. However,
there maybe further dependencies on other 32 bit packages being present on
the system; if such errors are reported, you can check this with '**ldd**
\$library_name'.

2. Required: If Network Manager and ITNCM-Reports are installed together, and if the Network Manager database is Oracle:

- a. To connect to an Oracle database from your TCR Installation, ensure that
ITNCM-Reports have been installed, and then update the itncmEnv.sh file
default location:

```
/opt/IBM/tivoli/netcool/nmc/reports/itncmEnv.sh
```

Export the following variables

ORACLE_HOME

```
ORACLE_HOME=<install directory>/reports/oracle export  
ORACLE_HOME
```

TNS_ADMIN

```
TNS_ADMIN=<install directory>/reports/oracle/network/admin  
export TNS_ADMIN
```

LD_LIBRARY_PATH

```
LD_LIBRARY_PATH=<install directory>/reports/  
oracle:$LD_LIBRARY_PATH export LD_LIBRARY_PATH
```

- b. Create a tnsnames.ora file located in <install directory>/reports/oracle/network/admin/
- c. Add the NCIM database to the tnsnames.ora file. For example: NCIM = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(Host = <Database Server>)(Port = 1521))) (CONNECT_DATA = (SERVICE_NAME = NCIM)))
- d. Add 'source <install directory>/reports/itncmEnv.sh' to your <install_user>/.bash_profile.

Note: The .bash_profile is only used for bash shell, and it will be different for sh, csh or ksh.

- e. Restart your reporting server after this update. However, before restarting the Reporting Server, check that the amended login profile has been sourced.

Configuring integration with Tivoli Netcool/OMNIbus:

Ensure that you have Netcool/OMNIbus Knowledge Library (NcKL) Enhanced Probe Rules for Netcool Configuration Manager installed on your Tivoli Netcool/OMNIbus server.

Before you begin

Deploy rules specific to Netcool Configuration Manager. These rules have been bundled with Netcool Configuration Manager and deployed on the Netcool Configuration Manager Presentation server during installation, and are located in the <NCM-INSTALL-DIR>/nckl-rules directory.

Note: This procedure is no longer required for device synchronization with Network Manager, and the mapping of devices between Netcool Configuration Manager and Network Manager.

The standard Netcool/OMNIbus Knowledge Library configuration must have been applied to the ObjectServer and to the Probe for SNMP as part of the prerequisite tasks for the integration. The \$NC_RULES_HOME environment variable must also have been set on the computer where the probe is installed. This environment variable is set to \$NCHOME/etc/rules on UNIX or Linux.

Tip: To source the Network Manager environment script, run the following script: ./opt/IBM/tivoli/netcool/env.sh where opt/IBM/tivoli/netcool is the default Network Manager directory.

Note: If you have existing Probe for SNMP custom rules that you want to preserve, create backups as required before deploying the Netcool/OMNIbus Knowledge Library rules in step two.

About this task

The location denoted by `$NC_RULES_HOME` holds a set of Netcool/OMNIBus Knowledge Library lookup files and rules files within a number of sub-directories. In particular, the `$NC_RULES_HOME/include-snmpttrap/ibm` subdirectory contains files that can be applied to the Probe for SNMP. To support the integration, you must add customized rules for Netcool Configuration Manager to this subdirectory.

Remember: If you have installed Netcool/OMNIBus Knowledge Library (NcKL) Enhanced Probe Rules Version 4.4 Multiplatform English (NcKL4.4) on your Tivoli Netcool/OMNIBus server, which is the recommended option, you do not need to install the ITNCM-specific Rules files, as documented here.

Procedure

Installing rules files specific to Netcool Configuration Manager (not the recommended option)

1. From the server where you have installed Netcool Configuration Manager, copy the following files:
 - `ncm_install_dir/nckl_rules/nckl_rules.zip`
where `ncm_install_dir` represents the installation location of Netcool Configuration Manager, for example `/opt/IBM/tivoli/netcool/ncm`
Copy these files to a temporary location on the computer where the Probe for SNMP is installed.
2. Extract the contents of the `nckl_rules.zip` file, and then copy the extracted files to the `$NC_RULES_HOME/include-snmpttrap/ibm` subdirectory.
3. If object server failover has already been configured, proceed to step 4. Otherwise, perform the following steps:
 - a. Go to the folder in which the `mttrapd.props` has been placed, for example `$NCHOME/omnibus/probes/AIX5`, where `AIX5` is specific to your operating system.
 - b. Edit the `mttrapd.props` file by commenting out the backup object server reference:
`#ServerBackup : ''`
4. To ensure that the probe can reference the enhanced lookup and rules files, edit the `$NC_RULES_HOME/snmpttrap.rules` file by uncommenting the following include statements, as shown:

```
include "$NC_RULES_HOME/include-snmpttrap/ibm/ibm.master.include.lookup"
include "$NC_RULES_HOME/include-snmpttrap/ibm/ibm.master.include.rules"
include "$NC_RULES_HOME/include-snmpttrap/ibm/ibm-preclass.include.snmpttrap.rules"
```
5. Run the probe. If the probe was already running, force the probe to re-read the rules file so that the changes can take effect, for example:
Locate the PID of the probe by running the following command on the server running the probe. Look for a process named - `nco_p_mttrapd`

```
ps -eaf | grep mttrapd
kill -9 PID
```

Note: If the probe is installed on a different computer from Network Manager or the Dashboard Application Services Hub portal, you must restart the probe manually.

Configuring integration with Network Manager:

Copy a number of jar files from the Network Manager GUI server into the Netcool Configuration Manager instance of WebSphere.

About this task

Note: The following default locations may differ depending on where WebSphere was installed on your Network Manager and Netcool Configuration Manager servers.

Procedure

Copy the following jars from the Network Manager GUI server into the corresponding folder in the Netcool Configuration Manager WebSphere instance.

- /opt/IBM/WebSphere/AppServer/etc/vmm4ncos.jks
- /opt/IBM/WebSphere/AppServer/lib/ext/com.ibm.tivoli.ncw.ncosvmm.jar
- /opt/IBM/WebSphere/AppServer/lib/ext/jconn3.jar

Configuring device synchronization:

You configure device synchronization to enable Netcool Configuration Manager to use Network Manager for network device discovery.

Before you begin

During Netcool Configuration Manager 6.4.2 installation you are asked if the product is to be integrated or not. If you select **Yes** the installer will ask the necessary questions to set up the configuration of device synchronization between Netcool Configuration Manager and Network Manager.

A default value of 24 hours (1440mins) is defined in the Netcool Configuration Manager `rseries.properties` file for the periodic synchronization with Network Manager. For the initial synchronization, a large number of devices may already have been discovered by Network Manager, and it can take a considerable time before they are imported into Netcool Configuration Manager. (This also applies in a situation where the discovery scope is widened so that a significant number of new devices are added to Network Manager.) Consequently the devices may not yet appear in the `NMENTITYMAPPING` table in the Netcool Configuration Manager database, and therefore the context tools (right-click tools) from Network Manager will not be available for those devices.

Tip: You can reduce this time by editing the `rseries.properties` file, and changing the mapping period to 60 (for example). This will speed up the process by which devices are added to the autodiscovery queue on Netcool Configuration Manager, but will not change the actual time to import each device configuration.

Tip:

If the password for the itnadmin user has changed on Network Manager, update the locally stored copy on Netcool Configuration Manager as follows:

Use the `icosadmin` script located in `/opt/IBM/tivoli/netcool/ncm/bin`.

For example:

```
icosadmin ChangeNmPassword -u itnadmin -p <new_password>
```

About this task

The configuration is stored in the `rseries.properties` file located in the following directory: `<ncm-install-dir>/config/properties/`

Network Manager:

```
NMEntityMappingComponent/baseUrl=https://nmguiservername:16311
NMEntityMappingComponent/uri=/ibm/console/nm_rest/topology/devices/domain/NCOMS
NMEntityMappingComponent/uriParam=
NMEntityMappingComponent/uriProps=
#####Note: Complete URL = baseUrl+uri+uriProps&uriParam

NMEntityMappingComponent/delay=10 ## delay on startup before first run
NMEntityMappingComponent/importRealm=ITNCM/@DOMAINNAME
NMEntityMappingComponent/maxDevicesPerRealm=50
NMEntityMappingComponent/ncmUser=administrator
NMEntityMappingComponent/period=1440 ## Daily (in minutes)
NMEntityMappingComponent/user=itnadmin
NMEntityMappingComponent/passwd=netcool ## Optional: Install stores securely
```

Note: You can edit this file and the component configuration properties after install if requirements change.

Before device synchronization runs for the first time ensure that the Network Manager Rest API user (in our example 'itnadmin') has the `ncp_rest_api` role in DASH.

Device synchronization is now done by a new core component of Netcool Configuration Manager, and is therefore part of Netcool Configuration Manager Component configuration and started automatically when Netcool Configuration Manager starts. Component start up is configured in `<ncm-install-dir>/config/server/config.xml`

```
<component>
<name>NMEntityMappingComponent</name>
<class>com.intelliden.nmentitymapping.NMEntityMappingComponent</class>
</component>
```

Note: The `NMEntityMappingComponent` is configured by default so if you wish to stop it being started on Netcool Configuration Manager startup you can comment it out in the `config.xml` file.

Note: There is a limit of 50 imported devices per Realm in Netcool Configuration Manager. If there are more devices than this in a Network Manager domain, they will be added to sub-realms (labeled 001, 002, etc) in Netcool Configuration Manager.

Example

Troubleshooting NM Component

Verify that the component has started in file:

```
<NCM_INSTALL_DIR>/logs/Server.out
Fri Jul 31 13:30:06 GMT+00:00 2015 - Starting component : NMEntityMappingComponent
Fri Jul 31 13:30:06 GMT+00:00 2015 - All components started
```

Verify that the `config.xml` file has the component specified for startup

Verify that the `NMEntityMapping` table has the new columns required for the new component implementation:

```

"NMENTITYMAPPING" (
  "UNIQUEKEY" BIGINT NOT NULL,
  "ENTITYID" BIGINT NOT NULL DEFAULT 0,
  "RESOURCEBROWSERID" BIGINT NOT NULL DEFAULT 0,
  "DOMAINNAME" VARCHAR(64),
  "JPAVERSION" BIGINT NOT NULL DEFAULT 1,
  "ENTITYNAME" VARCHAR(255),
  "ACCESSIPADDRESS" VARCHAR(64),
  "SERIALNUMBER" VARCHAR(64),
  "VENDORTYPE" VARCHAR(64),
  "MODELNAME" VARCHAR(64),
  "OSVERSION" VARCHAR(64),
  "OSIMAGE" VARCHAR(255),
  "OSTYPE" VARCHAR(64),
  "HARDWAREVERSION" VARCHAR(64)
)

```

Ensure that the Network Manager Rest API user has the ncp_rest_api role in DASH.

Configuring the Alerts menu of the Active Event List:

You must add access to the Activity Viewer from the Active Event List by configuring the Alerts menu.

Procedure

1. From the navigation pane, click **Administration > Event Management Tools > Menu Configuration**.
2. From the **Available menus** list on the right, select **alerts** and click **Modify**.
3. From the Menus Editor window, select **<separator>** from the drop-down list under **Available items**, and then click **Add selected item** to add the item to the **Current items** list. The **<separator>** item is added as the last item.
4. Under **Available items**, select **menu** from the drop-down list. The list of all menu items that can be added to the **Alerts** menu is shown.
5. Select the **Configuration Management** item and click **Add selected item**. The item is added below the **<separator>** item in the **Current items** list.
6. Click **Save** and then click **OK**.

Results

The **Configuration Management** submenu and tools are now available in the **Alerts** menu of the Active Event List, for use with Netcool Configuration Manager events.

Note: Reports Menu options will not be displayed if the selected event is not enriched.

What to do next

You can optionally create a global filter to restrict the events displayed in the Active Event List to Netcool Configuration Manager events only. You can add this filter to the Web GUI either by using the WAAPI client or by using the Filter Builder. When creating the filter, specify a meaningful name (for example, ITNCMEvents) and define the filter condition by specifying the following SQL WHERE clause:

```
where Class = 87724
```

For further information about creating filters, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide* in the Tivoli Netcool/OMNIBus Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.netcool_OMNIBus.doc_7.3.1/omnibus/wip/welcome.htm.

Migrating reports:

If you have custom Reporting Services reports in an existing Netcool Configuration Manager installation, and are integrating with Network Manager, which has its own Reporting Services solution, you migrate your custom reports from the stand-alone to the integrated version of Reporting Services.

Before you begin

If you are installing Network Manager on the same server as your existing Netcool Configuration Manager installation, you must export your custom reports before installing Network Manager.

About this task

The report migration procedure is different for single and multiple server integrations.

If you are installing Netcool Configuration Manager and Network Manager on the same server

1. Export the custom reports from the existing Netcool Configuration Manager version of Reporting Services and copy them to a safe location.

Note: You export your custom reports before installing Network Manager to prevent the existing reports from being overwritten.

2. Disable and uninstall the existing Netcool Configuration Manager version of Reporting Services.
3. Install Network Manager and integrate it with the existing version of Netcool Configuration Manager as documented.
4. Import the custom reports into the Network Manager version of Reporting Services.

If you are installing Netcool Configuration Manager and Network Manager on different servers

1. Install Network Manager and integrate it with the existing version of Netcool Configuration Manager as documented.
2. Export the custom reports from the existing Netcool Configuration Manager version of Reporting Services and copy them to the Network Manager server.
3. Import the custom reports into the Network Manager version of Reporting Services.
4. Disable the existing Netcool Configuration Manager version of Reporting Services.

Exporting custom reports (distributed integration architecture):

After you have installed Network Manager on a server other than your existing Netcool Configuration Manager installation and performed all integration tasks, you export your custom Reporting Services reports. You also disable and uninstall the existing Netcool Configuration Manager version of Reporting Services.

Before you begin

You export reports **after** installing Network Manager when all of the following circumstances apply to your scenario:

- You are already running Reporting Services as part of an existing, non-integrated Netcool Configuration Manager installation.
- You are deploying a distributed integration architecture and have already installed Network Manager on a server other than your existing version of Netcool Configuration Manager.
- You have customized Netcool Configuration Manager reports that need to be migrated into your planned integrated solution.

About this task

When you install the Network Manager version of Reporting Services on a server other than your existing version of Netcool Configuration Manager, the previous reports as well as the previous version of Reporting Services remain on the Netcool Configuration Manager server. To migrate such reports into an integrated solution, you perform the following tasks:

If you are installing Netcool Configuration Manager and Network Manager on different servers

1. Install Network Manager and integrate it with the existing version of Netcool Configuration Manager as documented.
2. Export the custom reports from the existing Netcool Configuration Manager version of Reporting Services and copy them to the Network Manager server.
3. Import the custom reports into the Network Manager version of Reporting Services.
4. Disable the existing Netcool Configuration Manager version of Reporting Services.

Remember: You do not have to migrate the standard Netcool Configuration Manager reports, because these will be installed together with the Network Manager version of Reporting Services (in addition to a number of Network View reports). You only migrate reports you have customized since installing the standard reports, or new reports you have created.

Procedure

1. Log into the Netcool Configuration Manager version of Reporting Services using the following URL:
`http://hostname:16310/ibm/console`
where *hostname* is the name of your Netcool Configuration Manager server and *16310* is the default port number for Reporting Services.
2. Click **Reporting > Common Reporting**.
3. Click **Launch** on the toolbar, and then select **Administration** from the drop-down menu.

4. Select the **Configuration** tab, then click **Content Administration**.
5. Click **New Export** to launch the New Export wizard.
6. Enter a name and description for the report export, then click **Next**.
7. Accept the default deployment method and click **Next**.
8. Click the **Add** link and select the **ITNCM Reports** checkbox, then move ITNCM Reports to the **Selected Entries** list.
9. Click **OK**, then **Next > Next > Next**, accepting the default values.
10. Select **New archive**, then **Next > Next**, accepting the default values..
11. Click **Finish > Run > OK**. The reports are exported and the new export archive is displayed.
12. Navigate to the following directory:
`/opt/IBM/tivoli/netcool/ncm/tipv2Components/TCRComponent/cognos/deployment,`
 where you can view the report archive, for example:

```
-rw-r--r--    1 icosuser staff      262637 23 Feb 10:27
ncm_export.zip
```

 where `ncm_export.zip` is the report archive.
13. Copy the file to the following directory on the Network Manager server:
`$TIP_HOME/../../TCRComponent/cognos/deployment`

Results

You have exported the custom reports and copied them to the Network Manager server.

What to do next

Next, you import the archived reports into the Network Manager version of Reporting Services, and then disable the Netcool Configuration Manager version of Reporting Services.

Importing reports (distributed integration architecture):

After exporting the custom reports and copying them to the Network Manager server, you import the archived reports into the Network Manager version of Reporting Services, and then disable the Netcool Configuration Manager version of Reporting Services.

Before you begin

You must have exported the custom reports and copied them to the Network Manager server.

About this task

Procedure

1. Log into the Network Manager Dashboard Application Services Hub.
2. Click **Reporting > Common Reporting**.
3. Click **Launch** on the toolbar, and then select **Administration** from the drop-down menu.
4. Select the **Configuration** tab, then click **Content Administration**.
5. Click **New Import** to launch the New Import wizard. A list of available report archives will be displayed.

6. Select the archive that you exported earlier and click **Next**.
7. Select **ITNCM Reports**, then **Next** and **Next** again, accepting the default values.
8. Click **Finish** > **Run** > **OK**. The reports are imported and the new archive is displayed in the list of archives.
9. Close the Common Reporting tab and click the Common Reporting link in the navigation pane. The custom reports will now be available in the Netcool Configuration Manager version of Reporting Services.
10. Navigate to the following directory:
`/opt/IBM/tivoli/netcool/ncm/bin/utls/support`
11. Run the `setPlatform.sh` script: `bash-3.2$ ./setPlatform.sh` and disable Reporting, then exit. When the Netcool Configuration Manager server is restarted, Reporting Services will no longer be running.

Results

You have now completed the migration of custom reports in your distributed custom environment.

Importing reports (single server integration architecture):

After exporting the custom reports, disabling and uninstalling the Netcool Configuration Manager version of Reporting Services, and completing all other integration steps, you import the report archive into the Network Manager version of Reporting Services,

Before you begin

You must have exported the custom reports before installing Network Manager on the same server as your existing Netcool Configuration Manager installation.

About this task

Procedure

1. Log into the Network Manager Dashboard Application Services Hub.
2. Click **Reporting** > **Common Reporting**.
3. Click **Launch** on the toolbar, and then select **Administration** from the drop-down menu.
4. Select the **Configuration** tab, then click **Content Administration**.
5. Click **New Import** to launch the New Import wizard. A list of available report archives will be displayed.
6. Select the archive that you exported earlier and click **Next**.
7. Select **ITNCM Reports**, then **Next** and **Next** again, accepting the default values.
8. Click **Finish** > **Run** > **OK**. The reports are imported and the new archive is displayed in the list of archives.
9. Close the Common Reporting tab and click the **Common Reporting** link in the navigation pane.

Results

The custom reports will now be available in the Netcool Configuration Manager version of Reporting Services.

Configuring Single Sign-On for Netcool Configuration Manager:

The single sign-on (SSO) capability in Tivoli® products means that you can log on to one Tivoli application and then launch to other Tivoli web-based or web-enabled applications without having to re-enter your user credentials.

The repository for the user IDs is the Tivoli Netcool/OMNIbus ObjectServer. A user logs on to one of the participating applications, at which time their credentials are authenticated at a central repository. With the credentials authenticated to a central location, the user can then launch from one application to another to view related data or perform actions. Single sign-on can be achieved between applications deployed to Dashboard Application Services Hub servers on multiple machines.

Single sign-on capabilities require that the participating products use Lightweight Third Party Authentication (LTPA) as the authentication mechanism. When SSO is enabled, a cookie is created containing the LTPA token and inserted into the HTTP response. When the user accesses other Web resources in any other application server process in the same Domain Name Service (DNS) domain, the cookie is sent with the request. The LTPA token is then extracted from the cookie and validated. If the request is between different cells of application servers, you must share the LTPA keys and the user registry between the cells for SSO to work. The realm names on each system in the SSO domain are case sensitive and must match exactly. See *Managing LTPA keys from multiple WebSphere® Application Server cells* on the WebSphere Application Server Information Center.

When configuring ITNCM-Reports for an integrated installation, ensure you configure single sign-on (SSO) on the Reporting Services server. Specifically, you must configure SSO between the instance of WebSphere that is hosting the Network Manager GUI, and the instance of WebSphere that is hosting ITNCM Reports. This will prevent unwanted login prompts when launching reports from within Network Manager. For more information, see *Configuring WebSphere user registry* in the *IBM Tivoli Netcool Configuration Manager Installation and Configuration Guide*.

Creating user groups for Dashboard Application Services Hub:

To configure single sign-on (SSO) between Dashboard Application Services Hub and Netcool Configuration Manager, you must create Netcool Configuration Manager groups and roles for Dashboard Application Services Hub.

Before you begin

Note: For SSO between Dashboard Application Services Hub and Netcool Configuration Manager to work, the user groups specified in this procedure must exist in both Dashboard Application Services Hub and Netcool Configuration Manager.

Network Manager and Netcool Configuration Manager users in Dashboard Application Services Hub should use the same authentication type, for example, ObjectServer.

Note: The **IntellidenUser** role needs to be assigned to the **IntellidenUser** group. Similarly, the **IntellidenAdminUser** role needs to be given to the **IntellidenAdminUser** group.

About this task

Procedure

1. Log onto the WebSphere Administrative console of the Network Manager GUI server as the profile owner (for example, smadmin).
2. Create a group by selecting **Users and Groups > Manage Groups > Create**.
3. Enter **IntellidenUser** in the Group name field.
4. Click **Create**, then click **Create Like**.
5. Enter **IntellidenAdminUser** in the Group name field. **IntellidenAdminUser** is required for access to Account Management in Netcool Configuration Manager.
6. Click **Create**, then click **Close**.
7. Log off from the WebSphere Administrative console, then log on to the Dashboard Application Services Hub GUI.
8. Select **Console Settings > Roles > IntellidenUser**.
9. Click **Users and Groups > Add Groups > Search**, then select the **IntellidenUser** group, and then click **Add**.
10. Select **Console Settings > Roles > IntellidenAdminUser**.
11. Click **Users and Groups > Add Groups > Search**, then select the **IntellidenAdminUser** group, and then click **Add**.

What to do next

After creating Netcool Configuration Manager groups and roles for Dashboard Application Services Hub, you create Netcool Configuration Manager users for Dashboard Application Services Hub.

Creating users for Dashboard Application Services Hub:

This section explains how to create the Netcool Configuration Manager **Intelliden** super-user as well as the default users: **administrator**, **operator**, and **observer** for Dashboard Application Services Hub.

Before you begin

For single sign-on (SSO) between Dashboard Application Services Hub and Netcool Configuration Manager to work, a user must exist (that is, have an account) in both Dashboard Application Services Hub and Netcool Configuration Manager.

At install time Netcool Configuration Manager automatically creates four users: **Intelliden**, **administrator**, **operator**, and **observer**. Of these users, only the **Intelliden** user must be created in Dashboard Application Services Hub. However, it is advisable that the other users are also created.

Note: Only the username must match, it is not necessary that the passwords also match. After single-sign on configuration is complete, the user password entered in Dashboard Application Services Hub will be used to authenticate a Netcool Configuration Manager login.

About this task

This task describes how to create the previously listed Netcool Configuration Manager users for Dashboard Application Services Hub.

Procedure

1. Log onto the WebSphere console of the Network Manager GUI server as the profile owner (for example, smadmin).
2. Click **Users and Groups > Manage Users**, then click **Create**.
3. Enter **Intelliden** in the User ID, First name, and Last Name fields.
4. Enter the Intelliden user's password in the Password and Confirm Password fields.
5. Click on **Group Membership** and select **Search**.
6. Highlight the **IntellidenAdminUser** and **IntellidenUser** groups in the matching groups list, and click **Add**, then click **Close**.
7. Click **Create**, then click **Create Like**.
8. Enter administrator in the following fields:
 - User ID
 - First name
 - Last Name
 - Password
 - Confirm password
9. Click on **Group Membership** and select **Search**.
10. Highlight the **IntellidenAdminUser** and **IntellidenUser** groups in the matching groups list, and click **Add**, then click **Close**.
11. Click **Create** and then **Close**.
12. Click **Create**.
13. Enter operator in the following fields:
 - User ID
 - First name
 - Last Name
 - Password
 - Confirm password
14. Click on **Group Membership** and select **Search**.
15. Highlight the **IntellidenUser** group in the matching groups list, and click **Add** and then **Close**.
16. Click **Create**, then click **Create Like**.
17. Enter observer in the following fields:
 - User ID
 - First name
 - Last Name
 - Password
 - Confirm password
18. Click on **Group Membership** and select **Search**.
19. Highlight the **IntellidenUser** group in the matching groups list, and click **Add**, then click **Close**.
20. Click **Create** and then **Close**.

What to do next

After you have created the Netcool Configuration Manager users for Dashboard Application Services Hub, you export the LTPA keystore to the Netcool Configuration Manager server.

Exporting the Dashboard Application Services Hub LTPA keystore:

For added security the contents of the LTPA token are encrypted and decrypted using a keystore (referred to in the subsequent procedure as the LTPA keystore) maintained by WebSphere. In order for two instances of WebSphere to share authentication information via LTPA tokens they must both use the same LTPA keystore. The IBM Admin Console makes this a simple process of exporting the LTPA keystore on one instance of WebSphere and importing it into another.

About this task

This task describes how to export the LTPA keystore from the instance of WebSphere running on the Network Manager Dashboard Application Services Hub server to the instance of WebSphere running on the Netcool Configuration Manager server for keystore synchronization.

Procedure

1. Launch the Dashboard Application Services Hub Admin Console. For example: http://www.nm_gui_server_ip.com:16310/ibm/console
2. Navigate to **Settings > WebSphere Administrative Console**.
3. Click **Security > Global security**.
4. Under the **Authentication mechanisms and expiration** tab, click **LTPA**.
5. Under the **Cross-cell single sign-on** tab, enter a password in the Password and Confirm password fields. The password will subsequently be used to import the LTPA keystore on the Netcool Configuration Manager server.
6. Enter the directory and filename you want the LTPA keystore to be exported to in the **Fully qualified key file name** field.
7. Complete by clicking **Export keys**.
8. Transfer the LTPA keystore to the Netcool Configuration Manager server.

Results

You will receive a message indicating that the LTPA keystore has been exported successfully.

What to do next

You now configure the SSO attributes for Dashboard Application Services Hub.

Related tasks:

“Importing the Dashboard Application Services Hub LTPA keystore to the Netcool Configuration Manager server” on page 75

Configuring Single Sign-On for Netcool Configuration Manager:

Configuring SSO is a prerequisite to integrating products that are deployed on multiple servers. All Dashboard Application Services Hub server instances must point to the central user registry.

About this task

Use these instructions to configure single sign-on attributes for the Dashboard Application Services Hub.

Procedure

1. Launch the Dashboard Application Services Hub Admin Console. For example: `http://www.nm_gui_server_ip.com:16310/ibm/console`.
2. Navigate to **Settings > WebSphere Administrative Console**.
3. Select **Security**, then click **Global Security > Web and SIP Security > Single sign on (SSO)**.
4. In the **Authentication** area, expand Web security, then click **Global Security > Web and SIP Security (on the Authentication area) > Single sign on (SSO)**.
5. Select the **Enabled** option if SSO is disabled.
6. Deselect **Requires SSL**.
7. Enter the fully-qualified domain names in the Domain name field where SSO is effective. If the domain name is not fully qualified, the Dashboard Application Services Hub server does not set a domain name value for the LTPAToken cookie and SSO is valid only for the server that created the cookie. For SSO to work across Tivoli® applications, their application servers must be installed in the same domain (use the same domain name). See below for an example.
8. Optional: Deselect the **Interoperability Mode** option.
9. Optional: Deselect the **Web inbound security attribute propagation** option.
10. Click **OK**, then save your changes.
11. Stop and restart all the Dashboard Application Services Hub server instances. Log out of the WebSphere Administrative Console.

Example

If Dashboard Application Services Hub is installed on **server1.ibm.com** and Netcool Configuration Manager is installed on **server2.ibm.com**, then enter a value of **.ibm.com**.

What to do next

You enable SSO on Netcool Configuration Manager next.

Related tasks:

“Importing the Dashboard Application Services Hub LTPA keystore to the Netcool Configuration Manager server” on page 75

Enabling SSO for Netcool Configuration Manager:

Both Netcool Configuration Manager and Netcool Configuration Manager WebSphere must be configured to enable SSO.

About this task

This task describes how to enable SSO for Netcool Configuration Manager if it was not enabled during installation.

Procedure

1. Navigate to `$NCM_installation_dir/Utils`.
2. Run the `configSSO.sh` script, for example:

```
cd /opt/IBM/tivoli/netcool/ncm/bin/Utils ./configSSO.sh enable
```

What to do next

When SSO is enabled, the interface to Netcool Configuration Manager must accept an LTPA token as a means of authentication. This is achieved by importing the LTPA keystore to the Netcool Configuration Manager server.

Importing the Dashboard Application Services Hub LTPA keystore to the Netcool Configuration Manager server:

For added security the contents of the LTPA token are encrypted and decrypted using a keystore maintained by WebSphere. In order for two instances of WebSphere to share authentication information via LTPA tokens they must both use the same keystore. The IBM admin console makes this a simple process of exporting the keystore on one instance of WebSphere and importing it into another.

Before you begin

You must have exported the LTPA keystore from the instance of WebSphere running on the Network Manager Dashboard Application Services Hub server and copied it to the Netcool Configuration Manager server in a previous task.

About this task

In this procedure you will import that LTPA keystore to the instance of WebSphere running on the Netcool Configuration Manager server.

Procedure

1. Logon to the WebSphere Administrative Console for the Netcool Configuration Manager Presentation Server using the superuser name and password specified at install time (typically `IntelliDen`).
For example `http://NCM_presentation_server:16316/ibm/console`
2. Click **Security > Global security**.
3. Under **Authentication mechanisms and expiration**, click **LTPA**.
4. Under **Cross-cell single sign-on**, enter the password in the Password and Confirm password fields. This password is the one that was used when the LTPA keystore was exported from Dashboard Application Services Hub.
5. Enter the LTPA keystore file name in the Fully qualified key file name field. This is the LTPA keystore that was exported from Dashboard Application Services Hub.

6. Click **Import keys**.
7. Click **Save directly to the master configuration**.

What to do next

You should now configure single sign-on attributes for the WebSphere instance running on the Netcool Configuration Manager server.

Related tasks:

“Exporting the Dashboard Application Services Hub LTPA keystore” on page 73

“Configuring Single Sign-On for Netcool Configuration Manager” on page 74

Configuring single sign-on attributes for Netcool Configuration Manager WebSphere:

Configuring SSO is a prerequisite to integrating products that are deployed on multiple servers. All eWAS server instances must point to the central user registry.

About this task

This procedure is performed on the Netcool Configuration Manager eWAS instance running on the Netcool Configuration Manager server.

Procedure

1. Logon to the WebSphere Administrative Console for the Netcool Configuration Manager Presentation Server using the superuser name and password specified at install time (typically `Intelliden`).
For example `http://NCM_presentation_server:16316/ibm/console`
2. In the **Authentication** area, expand Web security then click Single sign-on.
3. Select the **Enabled** option if SSO is disabled.
4. Deselect **Requires SSL**.
5. Leave the domain name blank in the **Domain name** field.
6. Optional: Deselect the **Interoperability Mode** option.
7. Optional: Deselect the **Web inbound security attribute propagation** option.
8. Click **Apply** to save your changes.
9. Click **Save Directly to the Master Configuration**.

What to do next

You create a federated user repository for Netcool Configuration Manager next.

Creating and configuring a federated user repository for Netcool Configuration Manager:

The first step for authenticating by using a Tivoli Netcool/OMNIBus ObjectServer is to create a federated user repository for Netcool Configuration Manager.

Before you begin

Important: Before attempting this procedure, complete the following task:
“Configuring integration with Network Manager” on page 63

About this task

A federated user repository is built on Virtual Member Manager (VMM), which provides the ability to map entries from multiple individual user repositories into a

single virtual repository. The federated user repository consists of a single named realm, which is a set of independent user repositories. Each user repository may be an entire external user repository.

This task describes how to create and configure a federated user repository for Netcool Configuration Manager.

Procedure

1. Launch the WebSphere Administrative Console from `http://<ncmserver-hostname-ip>:<16316>/ibm/console` and login using the Netcool Configuration Manager superuser name and password specified during installation.

Note: The port number may be different for a non-standard installation.

2. Select **Security > Global security**.
3. Under the User account repository, select **Federated repositories** from the Available realm definitions field, and click **Configure**.
4. Under Repositories in the realm, select **Add repositories (LDAP, custom, etc)**.
5. Under General Properties, select **New Repository > Custom Repository**
6. Update the ObjectServer VMM properties as described here (or per your custom repository):

Repository identifier

NetcoolObjectServer

Repository adapter class name

com.ibm.tivoli.tip.vmm4ncos.ObjectServerAdapter

Custom Properties

Add the following four properties:

Note: Find the exact details from the repository viewable on the Network Manager Gui Administrative Console.

Table 15. Custom Properties

Name (case-sensitive)	Value
username	ObjectServer administrator user name
password	ObjectServer encrypted administrator user password
port1	Object Server port number
host1	Object Server hostname/IP address

7. Click **Apply** and save your changes directly to the master configuration.
8. Under General properties of Repository Reference, update the Unique distinguished name to `o=netcool0bjectServerRepository`
9. Click **OK** and save your changes directly to the master configuration, then click **OK** again.
10. The local repository may not contain IDs that are also in Netcool Configuration Manager. To mitigate, perform one of the following steps:
 - Remove the local file repository from the federation of repositories.
 - Remove all the conflicting users from the local file repository.
11. If prompted, enter the WebSphere Administrator user password in the **Password** and **Confirm Password** fields, and click **OK**.

12. In Global security under the User account repository, select **Federated Repositories** from the Available realm definitions field, and click **Set as current**.
13. Click **Apply** and save your changes directly to the master configuration.
14. Log out of the Administrative Console.
15. Stop the Netcool Configuration Manager server using the `./itncm.sh stop` command. Then start the Netcool Configuration Manager server using the `./itncm.sh start` command.

What to do next

Netcool Configuration Manager will now authenticate with the ObjectServer VMM.

The Netcool Configuration Manager Superuser has been reverted to the user created during the Dash profile Installation (which is `smadmin` by default)

Getting started with Networks for Operations Insight

After the installation and configuration steps are completed, you can start the components of the Networks for Operations Insight feature and log in to the `ost` using a Web browser.

Procedure

1. Ensure that Tivoli Netcool/OMNIBus ObjectServer is running, see http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/omnibus/wip/admin/task/omn_con_startingobjserv.html?lang=en.
2. Start the Dashboard Application Services Hub server using the `/opt/IBM/JazzSM/profiles/bin/startServer.sh server_name` command.
3. Source the environment variables. On the server where the Network Manager core components are installed, the script is `installation_directory/netcool/core/env.sh`. On the server where the Network Manager GUI components are installed, the script is `installation_directory/nmgui_profile.sh`, for example, `/opt/IBM/netcool/nmgui_profile.sh`.
4. Start the back-end processes for the products. Use the `itnm_start` command to start Network Manager. Do not use this command to start the ObjectServer. The ObjectServer is started and stopped by the Tivoli Netcool/OMNIBus commands. Start Netcool Configuration Manager separately by using the `itncm.sh start` script.
5. Log in at `http://host.domain:16310/ibm/console` or, for a secured environment, at `https://host.domain:16311/ibm/console`, where *host.domain* is the fully qualified host name or IP address of the Jazz for Service Management application server. 16310 and 16311 are the default ports for HTTP and HTTPS respectively. Use the supplied `itnadmin` user with the password that you specified during the installation.
6. You can log in to the Netcool Configuration Manager - Base GUI at `http://ncmserver-hostname:port-number`, where *ncmserver-hostname* is the host name of the computer on which you installed Netcool Configuration Manager. *port-number* is the port that you specified during the installation. Use the default user name and password that you specified during the installation.

Related tasks:

-  Sourcing environment variables
-  Starting Network Manager

➞ Logging in

➞ Launching Netcool Configuration Manager - Base

Related reference:

➞ itncm.sh script

Related information:

➞ Getting started with Network Manager

➞ Getting started with Netcool Configuration Manager

Installing the Insight Packs

The Insight Packs ingest the event data into Operations Analytics - Log Analysis and install the custom apps. Two Insight Packs are supplied. The Tivoli Netcool/OMNIbus Insight Pack is always required. The Network Manager Insight Pack is required only if you deploy the Networks for Operations Insight feature and want to use the topology search capability.

Operations Analytics - Log Analysis can be running while you install the Insight Packs.

Before you begin

If you plan to deploy the topology search capability, obtain information about the NCIM database that you installed in the step “Installing Network Manager and Netcool Configuration Manager” on page 50.

Tip: You can obtain most of the information that is required from the `$NCHOME/etc/precision/DbLogins.cfg` or `DbLogins.DOMAIN.cfg` files (where *DOMAIN* is the name of the domain).

This information is needed for step 6 on page 80 of this procedure.

Procedure

1. Install Python 2.6 or later with the `simplejson` library, which is required by the Custom Apps that are included in Insight Packs.
2. Obtain the required Insight Packs. The Insight Pack images are contained within the Operations Analytics - Log Analysis download, see information about *Event Search integration* and *Topology Search integration* in <http://www-01.ibm.com/support/docview.wss?uid=swg24041694>. The file names of the Insight Packs are:
 - `OMNIbusInsightPack_v1.3.0.2.zip`
 - `NetworkManagerInsightPack_V1.3.0.0.zip`
3. Install the Tivoli Netcool/OMNIbus Insight Pack onto the Operations Analytics - Log Analysis host. For example:

```
$UNITY_HOME/utilities/pkg_mgmt.sh -install $UNITY_HOME/unity_content/OMNIbus/OMNIbusInsightPack_v1.3.0.2.zip
```
4. On the Operations Analytics - Log Analysis UI, use the Data Source Wizard to create a data source into which the event data is ingested. The “omnibus1100” data source can ingest data for both the Tivoli Netcool/OMNIbus Insight Pack and the Network Manager Insight Pack.
 - a. In the Select Location panel, select **Custom** and type the Netcool/OMNIbus server host name. Enter the same host name that was used for the **JsonMsgHostname** transport property of the Gateway for Message Bus.

- b. In the Select Data panel, enter the following field values:

Field	Value
File path	NCOMS. This is the default value of the jsonMsgPath transport property of the Gateway for Message Bus. If you changed this value from the default, change the value of the File path field accordingly.
Type	OMNIBus1100
Collection	OMNIBus1100-Collection

- c. In the Set Attributes panel, enter the following field values:

Field	Value
Name	omnibus. Ensure that the value that you type is the same as the value of the scala.datasource property in the Web GUI <code>server.init</code> file. If the Name field has a value other than omnibus, use the same value for the scala.datasource property.
Group	Leave this field blank.
Description	Type a description of your choice.

5. Optional: Install the Network Manager Insight Pack. For example:

```
$UNITY_HOME/utilities/pkg_mgmt.sh -install $UNITY_HOME/unity_content/
/NetworkManagerNetworkManagerInsightPack_V1.3.0.0.zip
```

6. Optional: In `$UNITY_HOME/AppFramework/Apps/NetworkManagerInsightPack_V1.3.0.0/Network_Topology_Search/NM_EndToEndSearch.properties`, specify the details of the NCIM database.

ncp.dla.ncim.domain

Limits the scope of the topology search capability to a single domain in your topology. For multiple domains, implement the cross-domain discovery function in Network Manager and specify the name of the aggregation domain. For all domains in the topology, comment out this property. Do not leave it blank.

ncp.spf.multipath.maxLinks

Sets a limit on the number of links that are processed when the paths between the two end points are retrieved. If the number of links exceeds the limit, only the first identified path is returned. For example, you specify `ncp.spf.multipath.maxLinks = 1000`. If 999 links are processed, all paths between the two end points are retrieved. If 1001 links are processed, one path is calculated and then processing stops.

ncp.dla.datasource.type

The type of database used to store the Network Manager topology. Possible values are `db2` or `oracle`.

ncp.dla.datasource.driver

The database driver. For DB2, type `com.ibm.db2.jcc.DB2Driver`. For Oracle, type `oracle.jdbc.driver.OracleDriver`.

ncp.dla.datasource.url

The database URL. For DB2, the URL is as follows:

```
jdbc:db2://host:port/name
```

For Oracle the URL is as follows:

`jdbc:oracle:thin:@host:port:name`

In each case, *host* is the database host name, *port* is the port number, and *name* is the database name, for example, NCIM.

`ncp.dla.datasource.schema`

Type the NCIM database schema name. The default is `ncim`.

`ncp.dla.datasource.ncpgui.schema`

Type the NCPGUI database schema name. The default is `ncpgui`.

`ncp.dla.datasource.username`

Type the database user name.

`ncp.dla.datasource.password.`

Type the database password.

`ncp.dla.datasource.encrypted`

If the password is encrypted, type `true`. If not, type `false`.

`ncp.dla.datasource.keyfile`

Type the name of and path to the cryptographic key file, for example `$UNITY_HOME/wlp/usr/servers/Unity/keystore/unity.ks`.

`ncp.dla.datasource.loginTimeout`

Change the number of seconds until the login times out, if required.

What to do next

- Use the **`pkg_mgmt`** command to verify the installations of the Insight Pack. See *Verifying the Tivoli Netcool/OMNIBus Insight Pack* and *Verifying the Network Manager Insight Pack*.
- If you are using an Oracle database for the network topology (the NCIM database), perform the extra configuration for Oracle. See the *Network Manager Insight Pack README*.
- Configure Single Sign-On (SSO) between Operations Analytics - Log Analysis and Dashboard Application Services Hub so that the right-click tools can be launched from the Event Viewer, and if you installed the Network Manager Insight Pack, the right-click tools can be launched from the Network Views. See “Configuring Single Sign-On” on page 84.

Related concepts:

 [Data Source creation in Operations Analytics - Log Analysis V1.3.5](#)

 [Data Source creation in Operations Analytics - Log Analysis V1.3.3](#)

Related information:

 [Gateway for Message Bus documentation](#)

Installing Network Performance Insight and configuring integration with Netcool Operations Insight

To add the performance management feature, install Network Performance Insight and then integrate it with Netcool Operations Insight.

Procedure

1. Install Network Performance Insight by performing the steps in the following topic in the Network Performance Insight documentation: https://www.ibm.com/support/knowledgecenter/SSCVHB_1.2.0/install/cnpi_install_about.html
2. Integrating Network Performance Insight with Netcool Operations Insight by performing the steps in the following topic in the Network Performance Insight documentation: https://www.ibm.com/support/knowledgecenter/SSCVHB_1.2.0/configure/cnpi_configure_about.html. In particular, you must ensure that you perform the following tasks as part of this integration task:
 - Configure Jazz for Service Management for use with Network Performance Insight by running the `npDashIntegration` script.
 - Import and enable the browser certificate to enable single sign-on.
 - Configure data communication between Network Performance Insight and Network Manager by configuring the Kafka bus.
 - Configure the Netcool/OMNIbus Standard Input probe to enable performance anomaly events to be displayed in the Netcool/OMNIbus Event Viewer.

Related reference:

“Ports used by products and components” on page 15

Installing and configuring the Device Dashboard

To integrate with Network Performance Insight and use the Device Dashboard to view performance information about your network, you need to configure the dashboard.

Before you begin

Ensure you have successfully installed Netcool/OMNIbus, Network Manager, and Network Performance Insight.

To add the network performance monitoring feature to your Netcool Operations Insight solution, ensure you also set up the integration between these products as described in http://www.ibm.com/support/knowledgecenter/SSCVHB_1.2.0/configure/cnpi_configure_about.html.

Note: If you do not install Network Performance Insight, you can still install the Device Dashboard, but you will not have the Performance Insights widget. Instead your Device Dashboard will include the Top Performers widget from the Network Health Dashboard.

Procedure

1. On the host where you installed the Network Manager GUI components, start Installation Manager and install the following package: **Netcool Operations Insight Widgets 1.1 -> Netcool Operations Insight Device Dashboard**.

This installs the Device Dashboard you can use to troubleshoot network issues by navigating the network topology and viewing performance anomalies and trends on any device, link, or interface.

Note: The Device Dashboard must be installed on the same host as the Network Manager GUI components.

Note: During the start of Device Dashboard installation, Installation Manager will ask for Ambari credentials. If you installed Network Performance Insight and integrated this as part of your Netcool Operations Insight solution, then at this point you must specify your Ambari credentials. Ambari is configured during the Network Performance Insight installation process and you would have configured Ambari credentials at that time. Default credentials are as follows:

- userid: admin
 - password: admin
2. Apply the latest supported Device Dashboard fix pack. For information on the product and component versions supported in the current version of Netcool Operations Insight including supported fix packs, see “Supported products and components” on page 3. Fix packs are available from IBM Fix Central, see <http://www.ibm.com/support/fixcentral/>. Full update and installation instructions are available in the Device Dashboard fix pack.

Note: You must also specify Ambari credentials when applying Device Dashboard fix packs. See the note in the previous step for more details.

3. Installing the Device Dashboard installs the `noi_npi` and `noi_npi_admin` roles, which allow users to work with the dashboard. Log in as the Dashboard Application Services Hub administrator to assign the roles `noi_npi` and `noi_npi_admin` as follows:
 - a. Go to **Console settings > Roles**.
 - b. In **Users and Groups**, assign roles `noi_npi` and `noi_npi_admin` to the `npiadmin` user, and assign the `noi_npi` role to the `npiuser` user. The `noi_npi` role provides access to view the Device Dashboard, while the `noi_npi_admin` role provides edit access to the Device Dashboard.

Note: You can assign the roles to other individual users or add the role to a group to control access.

Note: If you do not assign the roles and the user selects **Show Device Dashboard** in the right-click tools, the GUI will hang and the user will receive an encoding error message when logging out, requiring the restart of the browser.

- c. Click **Save**.
4. On the same host, save the Network Performance Insight profile as follows: Go to **Console Settings > Console Integrations** and select **NPI**, review the information, and click **Save**. The Network Performance Insight  icon appears on the left in the Navigation bar.
5. Configure the integration with Network Performance Insight as described in Data communication between Network Performance Insight and Network Manager.

What to do next

For more information about roles, see http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itm/ip/wip/admin/concept/nmip_adm_usergroup.html.

Related concepts:

“Device Dashboard” on page 252

Configuring Single Sign-On

Single Sign-On (SSO) can be configured to support the launch of tools between the products and components of Netcool Operations Insight. Different SSO handshakes are supported; which handshake to configure for which capability is described here. Each handshake must be configured separately.

Procedure

Set up the SSO handshake as described in the following table. The table lists which products and components are connected by SSO, which capabilities require which SSO handshake and additional useful information.

Table 16. SSO handshakes for Netcool Operations Insight

SSO handshake can be configured between these products or components		Handshake is configured to support this capability	Additional notes
Operations Analytics - Log Analysis	Dashboard Application Services Hub	Event search	Supports the launch of right-click tools from the event lists(That is, the Event Viewer and Active Event List.) of the Netcool/OMNIBus Web GUI to the custom apps of the Tivoli Netcool/OMNIBus Insight Pack.
Operations Analytics - Log Analysis	Dashboard Application Services Hub	Topology search	Supports the launch of right-click tools from the Web GUI event lists to the custom apps of the Network Manager Insight Pack. Supports the launch of right-click tools from the Network Views in the Network Manager product for the custom apps in the Network Manager Insight Pack.
Netcool Configuration Manager	Dashboard Application Services Hub	Networks for Operations Insight	Supports the launch of right-click tools from the Network Views to the Netcool Configuration Manager GUIs.

Related tasks:

“Configuring single sign-on for the event search capability” on page 97

“Configuring single sign-on for the topology search capability” on page 279

➞ Configuring SSO between Operations Analytics - Log Analysis V1.3.5 and Dashboard Application Services Hub

➞ Configuring SSO between Operations Analytics - Log Analysis V1.3.3 and Dashboard Application Services Hub

“Configuring Single Sign-On for Netcool Configuration Manager” on page 74

Related information:

➞ Configuring Jazz for Service Management for SSO

Getting started with Netcool Operations Insight

This information applies to the base Netcool Operations Insight solution only. If you also installed Networks for Operations Insight, follow the steps in “Getting started with Networks for Operations Insight” on page 78.

About this task

Tip:

You can create start-up scripts to automatically start the various Netcool Operations Insight products. For instructions and an example of how to configure a start-up script, see the 'The Netcool Process Agent and machine start-up' section in the Netcool/OMNIbus *Best Practices Guide*, which can be found on the Netcool/OMNIbus best-practice Wiki: http://ibm.biz/nco_bps

You can configure Jazz not to prompt for user credentials when the stop command is run. After creating a backup, edit the following lines in the `/opt/IBM/JazzSM/profile/properties/soap.client.props` file:

```
com.ibm.SOAP.securityEnabled=true
com.ibm.SOAP.loginUserId=smadmin
com.ibm.SOAP.loginPassword=netcool
```

Run the following command to encrypt the embedded password within the file:

```
/opt/IBM/JazzSM/profile/bin/PropFilePasswordEncoder.sh \
/opt/IBM/JazzSM/profile/properties/soap.client.props \
com.ibm.SOAP.loginPassword
```

For more information, see the following technote: <http://www.ibm.com/support/docview.wss?uid=swg21584635>

Procedure

- Start the Dashboard Application Services Hub server using the `/opt/IBM/JazzSM/profiles/bin/startServer.sh server_name` command.
- Log in at `http://host.domain:16310/ibm/console` or, for a secured environment, at `https://host.domain:16311/ibm/console`, where *host.domain* is the fully qualified host name or IP address of the Jazz for Service Management application server. 16310 and 16311 are the default ports for HTTP and HTTPS respectively.
- Assign roles to users. To give users access to the Event Analytics capability, assign the `ncw_analytics_admin` user.

What to do next

Useful information about how to configure your environment is in the *Netcool Operations Insight Example Guide*, which you can download at <https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli%20Netcool%20OMNIBus/page/Best%20Practices>.

Related tasks:

“Getting started with Networks for Operations Insight” on page 78

Upgrading to the latest Netcool Operations Insight

How to upgrade the products and components of a previous version of Netcool Operations Insight to the latest version. Scenarios are presented here that give a quick reference to upgrading and also an end-to-end scenario that describes an upgrade to the latest version.

Tip: For recommendations for minimizing disruption to production systems, see the Tivoli Netcool/OMNIBus best-practice Wiki at the following location:
http://ibm.biz/nco_bps

As an illustration of the steps that you might have to perform, the following table lists what you have to do on each instance of the products of Netcool Operations Insight V1.4.0.3 to get to V1.4.0.4.

Table 17. Changes to constituent products and components required for an upgrade to the latest Netcool Operations Insight version

Product or component	Action
Tivoli Netcool/OMNIBus	Apply a fix pack, apply configurations.
Jazz for Service Management	Upgrade to latest version provided with Netcool Operations Insight 1.4.0.4.
Tivoli Netcool/OMNIBus Web GUI	Apply a fix pack, apply configurations.
Gateway for JDBC	No upgrade required.
Gateway for Message Bus	No upgrade required.
Netcool/Impact	Apply a fix pack, apply configurations.
Operations Analytics - Log Analysis	No upgrade required. Note: For information on the supported versions, see “Supported products and components” on page 3.
Event Analytics	Upgrade to latest version as provided by Tivoli Netcool/OMNIBus Web GUI and Netcool/Impact extensions.
Tivoli Netcool/OMNIBus Insight Pack	No upgrade required.
Network Manager Insight Pack	No upgrade required.
Network Manager	Apply a fix pack, apply configurations.
Netcool Configuration Manager	Apply a fix pack, apply configurations.

Quick reference to upgrading

The table summarizes how to upgrade from Netcool Operations Insight V1.4.0.3 to V1.4.0.4.

This overview assumes detailed knowledge of the products in Netcool Operations Insight. It does not provide all the details. Links are given to more information, either within the Netcool Operations Insight documentation, or in the product documentation of the constituent products of Netcool Operations Insight.

Tip: To verify the versions of installed packages, select **View Installed Packages** from the File menu on the main IBM Installation Manager screen.

For information on the latest supported fix packs, see “Supported products and components” on page 3.

Remember: All Netcool Operations Insight products require the IBM Installation Manager to be deployed on each server on which products are to be installed.

Table 18. Quick reference for upgrading Netcool Operations Insight

Item	Action	More information
1	Apply the latest supported fix pack for Netcool/OMNIBus core components.	This fix pack is available only from IBM Fix Central: http://www.ibm.com/support/fixcentral/ See “Supported products and components” on page 3 for latest supported fix packs.
2	Download and install the latest supported version of Jazz for Service Management components.	For more information, see “Installing Dashboard Application Services Hub and the UI components” on page 44. See “Supported products and components” on page 3 for latest supported fix packs.
3	Apply the latest supported fix pack for Netcool/Impact. As part of upgrading Event Analytics, select the IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight corresponding to the Netcool/Impact fix pack number.	For more information, see Upgrading Event Analytics. This fix pack is available only from IBM Fix Central: http://www.ibm.com/support/fixcentral/ See “Supported products and components” on page 3 for latest supported fix packs.
4	Apply the latest supported fix pack for Netcool/OMNIBus Web GUI. As part of upgrading Event Analytics, select the IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI corresponding to the current version of Netcool Operations Insight.	For more information, see Upgrading Event Analytics. This fix pack is available only from IBM Fix Central: http://www.ibm.com/support/fixcentral/ See “Supported products and components” on page 3 for latest supported fix packs.
5	Configure the Web GUI for integration with Operations Analytics - Log Analysis. In the <code>server.init</code> file, set the <code>scala.*</code> properties appropriately. Ensure that the settings point to the your Operations Analytics - Log Analysis instance.	See the <i>IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide</i> .
6	Install the latest supported fix pack for Network Manager.	For more information about this fix pack, see http://www.ibm.com/support/knowledgecenter/en/SSSHRK_4.2.0/itnm/ip/wip/relnotes/reference/nmip_rn.html . This fix pack is available from IBM Fix Central: http://www.ibm.com/support/fixcentral/ See “Supported products and components” on page 3 for latest supported fix packs.

Table 18. Quick reference for upgrading Netcool Operations Insight (continued)

Item	Action	More information
7	Install the latest supported fix pack for Netcool Configuration Manager.	For more information about this fix pack, see http://www.ibm.com/support/knowledgecenter/SS7UH9_6.4.2/ncm-gentopic1.html This fix pack is available from IBM Fix Central: http://www.ibm.com/support/fixcentral/ See “Supported products and components” on page 3 for latest supported fix packs.
8	Install the latest supported version of Network Performance Insight.	For installation instructions, see http://www.ibm.com/support/knowledgecenter/SSCVHB Obtain the packages from IBM Passport Advantage. For information about the eAssembly numbers you need for the packages, see http://www-01.ibm.com/support/docview.wss?uid=swg24043517. See “Supported products and components” on page 3 for latest supported fix packs.
9	Install and configure the Device Dashboard	“Installing and configuring the Device Dashboard” on page 82

Upgrading Netcool Operations Insight

This scenario describes how to upgrade Netcool Operations Insight V1.4.0.4.

Before you begin

- Back up all products and components in the environment.
- Go to IBM Fix Central, at <http://www.ibm.com/support/fixcentral/>, to download the latest fix pack versions of Tivoli Netcool/OMNIbus core, Web GUI, and Netcool/Impact. See “Supported products and components” on page 3 for latest supported fix packs.
- Obtain the packages from IBM Passport Advantage. For information about the eAssembly numbers you need for the packages, see <http://www-01.ibm.com/support/docview.wss?uid=swg24043517>.

Because the other products and components stay on the same VRM number, it is assumed that the hosts still meet the installation prerequisites. IBM Installation Manager, product fix packs, and interim fixes are available from IBM Fix Central, at <http://www.ibm.com/support/fixcentral/>.

Procedure

1. On the Netcool/OMNIbus host, apply the latest fix pack for Netcool/OMNIbus core. See “Supported products and components” on page 3 for latest supported fix packs. Start Installation Manager. Change to the `/eclipse` subdirectory of the Installation Manager installation directory and enter the following command to start Installation Manager:
`./IBMIM`

Note: See “Supported products and components” on page 3 for latest supported fix packs.

2. Configure Installation Manager to point to either a local repository or an IBM Passport Advantage repository, where the download package is available. Within the IBM Knowledge Center content for Installation Manager, see the topic that is called *Installing packages by using wizard mode*. See the following URL within the IBM Knowledge Center content for Installation Manager:

http://www-01.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

3. In the main Installation Manager window, click **Update** and complete the following type of installation wizard instructions to complete the installation of your update package:
 - a. In the Update Packages tab, select the product group to find related update packages, and click **Next**. A list of the available update packages displays.
 - b. From the list of available update packages, select the Netcool/OMNIBus fix pack version that you specified in step 1, and click **Next**.
 - c. In the Licenses tab, review the licenses. Select **I accept the terms in the license agreements** and click **Next**.
 - d. In the Features tab, select the features for your update package, and click **Next**.
 - e. Complete the configuration details, and click **Next**.
 - f. In the Summary tab, review summary details. If you need to change any detail click **Back**, but if you are happy with summary details click **Update** and wait for the installation of the update package to complete.
 - g. When the installation of the update package completes, the window updates with details of the installation. Click **Finish**.
4. Configure the ObjectServer to support the topology search capability. In `$NCHOME/omnibus/extensions`, run the `nco_sql` utility against the `scala_itnm_configuration.sql` file.

```
./nco_sql -user root -password myp4ss -server NCOMS  
< /opt/IBM/tivoli/netcool/omnibus/extensions/scala/scala_itnm_configuration.sql
```

Triggers are applied to the ObjectServer that delay the storage of events until the events are enriched by Network Manager data from the NCIM database.

Important: If you are connecting to an ObjectServer instance created before Netcool/OMNIBus core V8.1.0.5 (fix pack 5) being applied, and are using the Operations Analytics - Log Analysis triggers that ship with the ObjectServer, you must run the following SQL file to upgrade the Operations Analytics - Log Analysis AEN triggers:

`$OMNIHOME/etc/update81to81fp5.sql`

If you are using the Operations Analytics - Log Analysis Network Manager triggers in the `$NCHOME/omnibus/extensions/scala` directory, you must apply the `update81to81fp5.sql` file in the `$NCHOME/omnibus/extensions/scala` directory.

5. Download Jazz for Service Management V1.1.3.0 from IBM Passport Advantage. For information about the eAssembly numbers you need for the packages, see <http://www-01.ibm.com/support/docview.wss?uid=swg24043517>. Use Installation Manager to install the Jazz for Service Management packages as described in “Installing Dashboard Application Services Hub and the UI components” on page 44.

6. On the Netcool/Impact host and on the Netcool/OMNIbus Web GUI host apply fix packs as specified in “Supported products and components” on page 3. Then configure Event Analytics as described in “Upgrading Event Analytics” on page 118.
7. On the Network Manager host, apply fix packs as specified in “Supported products and components” on page 3. For more information about this fix pack, see http://www.ibm.com/support/knowledgecenter/en/SSSHRK_4.2.0/itnm/ip/wip/relnotes/reference/nmip_rn.html.
8. On the Netcool Configuration Manager host, apply fix packs as specified in “Supported products and components” on page 3. For more information, see http://www.ibm.com/support/knowledgecenter/SS7UH9_6.4.2/ncm-gentopic1.html.
9. To upgrade from Network Performance Insight v1.1.0 to Network Performance Insight v1.2 perform the following steps.
 - Uninstall Network Performance Insight v 1.1, as described in https://www.ibm.com/support/knowledgecenter/SSCVHB_1.2.0/install/tnpi_uninstalling.html.
 - Obtain the Network Performance Insight v1.2 package from IBM Passport Advantage, and install Network Performance Insight V1.2.0 as described in http://www.ibm.com/support/knowledgecenter/SSCVHB_1.2.0/install/cnpi_install_about.html

For information about the eAssembly numbers you need for the packages, see <http://www-01.ibm.com/support/docview.wss?uid=swg24043517>.

10. Apply the Device Dashboard fix pack as specified in “Supported products and components” on page 3. Upgrade and configure the Device Dashboard as described in “Installing and configuring the Device Dashboard” on page 82. For information about the eAssembly numbers you need for the packages, see <http://www-01.ibm.com/support/docview.wss?uid=swg24043517>.

Related concepts:

 [Connections in the Server Editor](#)

Related tasks:

 [Restarting the Web GUI server](#)

 [Configuring Reporting Services for Network Manager](#)

Related reference:

 [Web GUI server.init file](#)

Related information:

 [Gateway for Message Bus documentation](#)

 [Operations Analytics - Log Analysis Welcome page](#). Roll over link for more information.

Event search

Event search applies the search and analysis capabilities of Operations Analytics - Log Analysis to events that are monitored and managed by Tivoli Netcool/OMNIbus. Events are transferred from the ObjectServer through the Gateway for Message Bus to Operations Analytics - Log Analysis, where they are ingested into a datasource and indexed for searching. After the events are indexed, you can search every occurrence of real-time and historical events. The Tivoli Netcool/OMNIbus Insight Pack is installed into Operations Analytics - Log Analysis and provides custom apps that search the events based on various criteria. The custom apps can generate dashboards that present event information to show how your monitoring environment is performing over time. Keyword searches and dynamic drilldown functions allow you to go deeper into the event data for detailed information. The apps can be run from the Operations Analytics - Log Analysis. Tooling can be installed into the Web GUI that launches the apps from the right-click menus of the Event Viewer and the Active Event List. An “event reduction wizard” is also supplied that includes information and apps that can help you analyze and reduce volumes of events and minimize the “noise” in your monitored environment.

Required products and components

Event search requires the following products and components:

- Operations Analytics - Log Analysis V1.3.3 or V1.3.5. For the system requirements of this product, including supported operating systems, see the following topics:
 - Operations Analytics - Log Analysis V1.3.3: https://www.ibm.com/support/knowledgecenter/SSPFMY_1.3.3/com.ibm.scala.doc/install/iwa_hw_sw_req_scen_c.html
 - Operations Analytics - Log Analysis V1.3.5: https://www.ibm.com/support/knowledgecenter/SSPFMY_1.3.5/com.ibm.scala.doc/install/iwa_hw_sw_req_scen_c.html

Note: Operations Analytics - Log Analysis Standard Edition is included in Netcool Operations Insight. For more information about Operations Analytics - Log Analysis editions, search for "Editions" at the Operations Analytics - Log Analysis Knowledge Center, at <https://www.ibm.com/support/knowledgecenter/SSPFMY>.

- OMNIbusInsightPack_v1.3.0.2
- Gateway for Message Bus V7.0
- Netcool/OMNIbus core components V8.1.0.7 (fix pack 7) or later
- Netcool/OMNIbus Web GUI V8.1.0.5 (fix pack 5) or later

For the system requirements of the core components and Web GUI for Netcool/OMNIbus V8.1, see <https://ibm.biz/BdRNaT>,

Related tasks:

“Configuring event search” on page 94

Related reference:

“Deployment considerations for Netcool/OMNIbus and the connection to Operations Analytics - Log Analysis” on page 8

Configuring event search

This section describes how to configure the integration of the Netcool/OMNIBus and Operations Analytics - Log Analysis products. Events are forwarded from Netcool/OMNIBus to Operations Analytics - Log Analysis by the Gateway for Message Bus.

Before you begin

- Use a supported combination of product versions. For more information, see “Required products and components” on page 93. The best practice is to install the products in the following order:
 1. Netcool/OMNIBus V8.1 and the Web GUI
 2. Gateway for Message Bus. Install the gateway on the same host as the Netcool/OMNIBus product.
 3. Operations Analytics - Log Analysis, see <https://ibm.biz/BdXeZk>
 4. Netcool/OMNIBus Insight Pack, see the *Netcool/OMNIBus Insight Pack README*.

Tip: The best practice is to install the Web GUI and Operations Analytics - Log Analysis on separate hosts.

Restriction: Operations Analytics - Log Analysis does not support installation in Group mode of IBM Installation Manager.

- Ensure that the ObjectServer that forwards event data to Operations Analytics - Log Analysis has the **NmosObjInst** column in the alerts.status table. **NmosObjInst** is supplied by default and is required for this configuration. You can use ObjectServer SQL commands to check for the column and to add it if it is missing, as follows.
 - Use the DESCRIBE command to read the columns of the alerts.status table.
 - Use the ALTER COLUMN setting with the ALTER TABLE command to add **NmosObjInst** to the alerts.status table.

For more information about the alerts.status table and ObjectServer SQL commands, see the *IBM Tivoli Netcool/OMNIBus Administration Guide*.

- Configure the Web GUI server.init file as follows:

Note: The default values do not have to be changed on Web GUI V8.1 fix pack 5 or later.

```
scala.app.keyword=OMNIBus_Keyword_Search
scala.app.static.dashboard=OMNIBus_Static_Dashboard
scala.datasource=omnibus
scala.url=protocol://host:port
scala.version=1.2.0.3
```

Restart the server if you change any of these values. See the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide*.

- Select and plan a deployment scenario. See “Deployment considerations for Netcool/OMNIBus and the connection to Operations Analytics - Log Analysis” on page 8. If your deployment uses the Gateway for Message Bus for forwarding events via the IDUC channel, you can skip step 5 on page 96. If you use the AEN client for forwarding events, complete all steps.
- Start the Operations Analytics - Log Analysis product.

- Familiarize yourself with the configuration of the Gateway for Message Bus. See the *IBM Tivoli Netcool/OMNIBus Reference Guide*. Knowledge of the gateway is required for steps 1, 5 on page 96, and 6 on page 96 of this task.

Procedure

The term *data source* has a different meaning, depending on which product you configure. In the Web GUI, a data source is always an ObjectServer. In the Operations Analytics - Log Analysis product, a data source is a source of raw data, usually log files. In the context of the event search function, the Operations Analytics - Log Analysis data source is Netcool/OMNIBus events.

1. Configure the Gateway for Message Bus. At a high-level, this involves the following:
 - Creating a gateway server in the Netcool/OMNIBus interfaces file
 - Configuring the G_SCALA.props properties file, including specifying the .map mapping file.
 - Configuring the endpoint in the scalaTransformers.xml file
 - Configuring the SSL connection, if required
 - Configuring the transport properties in the scalaTransport.properties file

For more information about configuring the gateway, see the *IBM Tivoli Netcool/OMNIBus Gateway for Message Bus Reference Guide*.

2. If you are ingesting data that is billable, and do not want data ingested into the Netcool Operations Insight data source to be included in the usage statistics, you need to set the Netcool Operations Insight data source as non-billable. Add the path to your data source (default is NCOMS, see following step) to a seed file and restart Operations Analytics - Log Analysis as described in <https://ibm.biz/BdXAbC>.

Note: Ensure you follow this step before you configure an “omnibus” data source for Netcool/OMNIBus events.

3. In Operations Analytics - Log Analysis, start the Add Data Source wizard and configure an “omnibus” data source for Netcool/OMNIBus events. Only a single data source is required. The event management tools in the Web GUI support a single data source only.
 - a. In the Select Location panel, select **Custom** and type the Netcool/OMNIBus server host name. Enter the same host name that was used for the **JsonMsgHostname** transport property of the Gateway for Message Bus.
 - b. In the Select Data panel, enter the following field values:

Field	Value
File path	NCOMS. This is the default value of the jsonMsgPath transport property of the Gateway for Message Bus. If you changed this value from the default, change the value of the File path field accordingly.
Type	OMNIBus1100
Collection	OMNIBus1100-Collection

- c. In the Set Attributes panel, enter the following field values:

Field	Value
Name	omnibus. Ensure that the value that you type is the same as the value of the scala.datasource property in the Web GUI <code>server.init</code> file. If the Name field has a value other than omnibus, use the same value for the scala.datasource property.
Group	Leave this field blank.
Description	Type a description of your choice.

4. Configure access to the data source you set up in the previous step. This involves the following steps in the administrative settings for Operations Analytics - Log Analysis:
 - a. Create a role using the Roles tab, for example, `noirole`, and ensure you assign the role permission to access the data source.
 - b. Add a user, for example, `noiuser`, and assign the role you created that has permissions to access the data source (in this example, `noirole`).

For information about creating and modifying users and roles in Operations Analytics - Log Analysis, see <https://ibm.biz/BdXeYj>.

Note: The contents of the Netcool/OMNIBus Insight Pack dashboards are empty unless you log in with a user that has a role assigned with permissions to access the data source.

5. Configure the Accelerated Event Notification (AEN) client:
 - a. Configure AEN event forwarding in the Gateway for Message Bus.
 - b. Configure the AEN channel and triggers in each ObjectServer by enabling the following postinsert triggers and trigger group:
 - `scala_triggers`
 - `scala_insert`
 - `scala_reinsert`

These items are included in the default configuration of the ObjectServer, as well as the SQL commands to configure the AEN channel, but they are disabled by default. For more information about configuring the AEN client in an integration with the Operations Analytics - Log Analysis product, search for *Configuring event forwarding using AEN* in the *IBM Tivoli Netcool/OMNIBus Gateway for Message Bus Reference Guide*.

6. Start the Gateway for Message Bus in SCA-LA mode. The gateway begins sending Netcool/OMNIBus events to Operations Analytics - Log Analysis.
7. Install the Web GUI with the event search feature. For more information, see the *IBM Tivoli Netcool/OMNIBus Installation and Deployment Guide*.

Results

After the configuration is complete, you can search for Netcool/OMNIBus events in Operations Analytics - Log Analysis. You can also use the Web GUI event management tools to launch into Operations Analytics - Log Analysis to display event data.

What to do next

- Install any available interim fixes and fix packs for the Operations Analytics - Log Analysis product, which are available from IBM Fix Central at <http://www.ibm.com/support/fixcentral/>.
- You can customize event search in the following ways:
 - Change the Operations Analytics - Log Analysis index configuration. For more information, see the Netcool/OMNIBus Insight Pack readme file. If you change the index configuration, also change the map file of the Gateway for Message Bus. After the map file is changed, restart the gateway. For more information, search for *Map definition file* in the Gateway for Message Bus documentation.
 - Customize the Operations Analytics - Log Analysis custom apps that are in the Insight Pack, or create new apps. For more information, see the Netcool/OMNIBus Insight Pack readme file.
 - Customize the Web GUI event list tools. For more information, see “Customizing event management tools” on page 98.
- If the Web GUI and Operations Analytics - Log Analysis are on the same host, configure single sign-on to prevent browser sessions expiring. See “Configuring single sign-on for the event search capability.”

Related tasks:

“Customizing event management tools” on page 98

 [Configuring triggers](#)

“Searching for events” on page 102

Related reference:

 [unity.sh command \(for starting SmartCloud Analytics - Log Analysis V1.3.5\)](#)

 [unity.sh command \(for starting SmartCloud Analytics - Log Analysis V1.3.3\)](#)

Related information:

 [Gateway for Message Bus documentation](#)

Configuring single sign-on for the event search capability

Configure single sign-on (SSO) between Web GUI and Operations Analytics - Log Analysis so that users can switch between the two products without having to log in each time. First, create dedicated users in your LDAP directory, which must be used by both products for user authentication, and then configure the SSO connection.

Procedure

1. Create the dedicated users and groups in your LDAP directory. For example:
 - a. Create a new Organization Unit (OU) named NetworkManagement.
 - b. Under the NetworkManagement OU, create a new group named webguildap.
 - c. Under the NetworkManagement OU, create the following new users: webgui1, webgui2, webgui3, and webgui4.
 - d. Add the new users to the webguildap group.
2. In the Web GUI, assign the ncw_admin and ncw_user roles to the webguildap group that you created in step 1.

3. Configure the SSO connection from the Operations Analytics - Log Analysis product to the Dashboard Application Services Hub instance in which the Web GUI is hosted. The following steps of the Operations Analytics - Log Analysis SSO configuration are important:

- Assign Operations Analytics - Log Analysis roles to the users and groups that you created in step 1 on page 97.
- In the `$SCALAHOME/wlp/usr/servers/Unity/server.xml/server.xml` file, ensure that the `<webAppSecurity>` element has a `httpOnlyCookies="false"` attribute. Add this line before the closing `</server>` element. For example:

```
<webAppSecurity ssoDomainNames="hostname" httpOnlyCookies="false"/>
</server>
```

Where The `httpOnlyCookies="false"` attribute disables the `httponly` flag on the cookie that is generated by Operations Analytics - Log Analysis and is required to enable SSO with the Web GUI.

Related tasks:

-  [Configuring user authentication for the Web GUI against LDAP directories](#)
-  [Assigning roles to Web GUI users and groups](#)
-  [Configuring SSO with Operations Analytics - Log Analysis V1.3.5](#)
-  [Configuring SSO with Operations Analytics - Log Analysis V1.3.3](#)

Related reference:

-  [Web GUI roles](#)
- [“Troubleshooting event search” on page 106](#)

Customizing event management tools

The tools in the Event Viewer and AEL search for event data based on fields from the Netcool/OMNIBus ObjectServer. The fields are specified by URLs that are called when the Operations Analytics - Log Analysis product is started from the tools. You can change the URLs in the tools from the default event fields to search on fields of your choice.

For example, the **Search for similar events > 15 minutes before event** tool filters events on the AlertGroup, Type, and Severity fields. The default URL is:

```
$(SERVER)/integrations/scala/Search?queryFields=AlertGroup,Type,Severity
&queryValuesAlertGroup={${selected_rows.AlertGroup}}
&queryValuesType={CONVERSION(${selected_rows.Type})}
&queryValuesSeverity={CONVERSION(${selected_rows.Severity})}
&firstOccurrences={${selected_rows.FirstOccurrence}}
&timePeriod=15
&timePeriodUnits=minutes
```

About this task

You can change the URLs in the following ways:

- Change the `scalaIntegration.xml` configuration file and apply the changes with the Web GUI **runwaapi** command that is included in the Web GUI Administration API (WAAPI) client.
- Change the tool configuration in the Web GUI Administration console page.

Procedure

As an example, the following steps show how to use each method to change the URLs in the **Search for similar events > 15 minutes before event** tool to search on the AlertKey and Location event fields.

- To change the URLs in the scalaIntegration.xml configuration file:
 1. In *WEBGUI_HOME*/extensions/LogAnalytics/scalaIntegration.xml, or the equivalent XML file if you use a different file, locate the following <tool> element:

```
<tool:tool name="scalaSearchByEvent15Minutes">
```
 2. Change the URL in this element as follows. The changes are shown in **bold** text:

```
<tool:cgiurl foreach="true" windowforeach="false" target="_blank" method="GET"
  url="$(SERVER)/integrations/scala/Search?queryFields=AlertKey,Location
  &queryValuesAlertKey={$selected_rows.AlertKey}
  &queryValuesLocation={$selected_rows.Location}
  &firstOccurrences={$selected_rows.FirstOccurrence}
  &timePeriod=15
  &timePeriodUnits=minutes">
```
 3. Use the **runwaapi** command to reinstall the tools:

```
runwaapi -file scalaIntegration.xml
```
 4. Reinstall the following tool menus to the Event Viewer or AEL **alerts** menu item:
 - scalaStaticDashboard
 - scalaSimilarEvents
 - scalaEventByNode
 - scalaKeywordSearch
- To change the URLs on the Administration page:
 1. In the Web GUI, click **Administration > Event Management Tools > Tool Creation**. Then, on the Tool Creation page, locate the scalaSearchByEvent15Minutes tool.
 2. Change the URL as follows. The changes are shown in **bold** text:

```
$(SERVER)/integrations/scala/Search?queryFields=AlertKey,Location
&queryValuesAlertKey={$selected_rows.AlertKey}
&queryValuesLocation={$selected_rows.Location}
&firstOccurrences={$selected_rows.FirstOccurrence}
&timePeriod=15
&timePeriodUnits=minutes
```
 3. Refresh the Event Viewer or AEL so that the changes to the tool URL are loaded.

What to do next

- The Gateway for Message Bus uses a lookup table to convert the Severity, Type, and Class event field integer values to strings. After a tool is changed or created, use the **CONVERSION** function to change these field values to the strings that are required by Operations Analytics - Log Analysis.
- Change the other tools in the menu so that they search on the same field. It is more efficient to change the configuration file and then use the **runwaapi** command than to change each tool in the UI. The following table lists the names of the event management menu items and tools that are displayed in the Tool Creation and Menu Configuration pages.

Table 19. Web GUI menu and tool names

Menu item	Menu item name	Tool	Tool name
Search for events by node	scalaEventByNode	15 minutes before event	scalaSearchByNode15Minutes
		1 hour before event	scalaSearchByNode1Hour
		1 day before event	scalaSearchByNode1Day
		1 week before event	scalaSearchByNode1Week
		1 month before event	scalaSearchByNode1Month
		1 year before event	scalaSearchByNode1Year
		Custom ...	scalaSearchByNodeCustom
Search for similar events	scalaSimilarEvents	15 minutes before event	scalaSearchByEvent15Minutes
		1 hour before event	scalaSearchByEvent1Hour
		1 day before event	scalaSearchByEvent1Day
		1 week before event	scalaSearchByEvent1Week
		1 month before event	scalaSearchByEvent1Month
		1 year before event	scalaSearchByEvent1Year
		Custom ...	scalaSearchByEventCustom
Show event dashboard by node	scalaStaticDashboard	15 minutes before event	scalaEventDistributionByNode15Minutes
		1 hour before event	scalaEventDistributionByNode1Hour
		1 day before event	scalaEventDistributionByNode1Day
		1 week before event	scalaEventDistributionByNode1Week
		1 month before event	scalaEventDistributionByNode1Month
		1 year before event	scalaEventDistributionByNode1Year
		Custom ...	scalaEventDistributionByNodeCustom
Show keywords and event count	scalaKeywordSearch	15 minutes before event	scalaSetSearchFilter15Minutes
		1 hour before event	scalaSetSearchFilter1Hour
		1 day before event	scalaSetSearchFilter1Day
		1 week before event	scalaSetSearchFilter1Week
		1 month before event	scalaSetSearchFilter1Month
		1 year before event	scalaSetSearchFilter1Year
		Custom ...	scalaSetSearchFilterCustom

- The **Show event dashboard by node** and **Show keywords and event count** tools start the OMNIBus Static Dashboard and OMNIBus Keyword Search custom apps in Operations Analytics - Log Analysis. For more information about customizing the apps, see the Insight Pack documentation at <ftp://public.dhe.ibm.com/software/tivoli/Netcool/NetcoolOperationsInsight/library/opsinsight130/>

Related tasks:

“Searching for events” on page 102

Adding custom apps to the Table View toolbar

To quickly launch custom apps, add them to the Table View toolbar of the Operations Analytics - Log Analysis UI. It is good practice to add the OMNIBus_Keyword_Search.app and OMNIBus_Static_Dashboard.app apps to the toolbar.

Procedure

- To add the OMNIBus_Keyword_Search.app app, use a configuration that is similar to the following example:

```
{
  "url": "https://hostname:9987/Unity/CustomAppsUI?
name=OMNIBus_Keyword_Search&appParameters=[]",
  "icon": "https://hostname:9987/Unity/images/keyword-search.png",
  "tooltip": "OMNIBus Keyword Search"
}
```

Where *hostname* is the fully qualified domain name of the Operations Analytics - Log Analysis host and *keyword-search* is the file name for a .png file that represents the app on the toolbar. Create your own .png file.

- To add the OMNIBus_Static_Dashboard.app app, use a configuration that is similar to the following example:

```
{
  "url": "https://hostname:9987/Unity/CustomAppsUI?
name=OMNIBus_Static_Dashboard&appParameters=[]",
  "icon": "https://hostname:9987/Unity/images/dashboard.png",
  "tooltip": "OMNIBus Static Dashboard"
}
```

Where *hostname* is the fully qualified domain name of the Operations Analytics - Log Analysis host and *dashboard* is the file name for a .png file that represents the app on the toolbar. Create your own .png file.

Related information:

 Adding a shortcut to a Custom App to the Table view toolbar (Operations Analytics - Log Analysis V1.3.5)

 Adding a shortcut to a Custom App to the Table view toolbar (Operations Analytics - Log Analysis V1.3.3)

Searching for events

The event search tools can find the root cause of problems that are generating large numbers of events in your environment. The tools can detect patterns in the event data that, for example, can identify the root cause events that cause event storms. They can save you time that would otherwise be spent manually looking for the event that is causing problems. You can quickly pinpoint the most important events and issues.

The tools are built into the Web GUI event lists (AEL and Event Viewer). They run searches against the event data, based on default criteria, filtered over specific time periods. You can search against large numbers of events. You can change the search criteria and specify different time filters. When run, the tools start the Operations Analytics - Log Analysis product, where the search results are displayed.

Before you begin

- Set up the environment for event search. See “Configuring event search” on page 94.
- Familiarize yourself with the Operations Analytics - Log Analysis search workspace.
 - If you are using V1.3.3, then see http://www-01.ibm.com/support/knowledgecenter/SSPFMY_1.3.3/com.ibm.scala.doc/use/iwa_using_ovw.html.
 - If you are using V1.3.5, then see http://www-01.ibm.com/support/knowledgecenter/SSPFMY_1.3.5/com.ibm.scala.doc/use/iwa_using_ovw.html.
- To understand the event fields that are indexed for use in event searches, familiarize yourself with the ObjectServer alerts.status table. See http://www-01.ibm.com/support/knowledgecenter/SSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/omnibus/wip/common/reference/omn_ref_tab_alertsstatus.html.

Procedure

- To start using the event search tools, select one or more events from an event list and right-click. From the right-click menu, click **Event Search**, click a tool, and click a time filter. The tools are as follows:

Tool	Description
Show event dashboard by node	Searches for all events that originate from the same host name, service name, or IP address, which is equivalent to the Node field of the ObjectServer alerts.status table.
Search for similar events	Searches for all events that have the same failure type, type, and severity as the selected events. The failure type equates to the AlertGroup field of the alerts.status table. The type equates to the Type field. The severity equates to the Severity field.

Tool	Description
Search for events by node	Searches for all events that originate from the same source, that is, host name, service name, or IP address. This is equivalent to the Node field of the alerts.status table. The results are displayed in a list in the Operations Analytics - Log Analysis GUI.
Show keywords and event count	Extracts a list of keywords from the text of the event summary, event source, and failure type. The event summary text equates to the Summary field of the alerts.status table. The event source equates to the Node field. The failure type equates to the AlertGroup field.

The time filters are calculated from the time stamp of the selected event or events. The Operations Analytics - Log Analysis time stamp is equivalent to the FirstOccurrence field of the ObjectServer alerts.status table. The default time filters are as follows. If you click **Custom** specify an integer and unit of time, such as 15 weeks.

- **15 minutes before event**
- **1 hour before event**
- **1 day before event**
- **1 week before event**
- **1 month before event**
- **1 year before event**
- **Custom ...**

If a single event is selected that has the time stamp 8 January 2014 08:15:26 AM, and you click **Search for events by node > 1 hour before event**, the result is filtered on the following time range: (8 January 2014 07:15:26 AM) to (8 January 2014 08:15:26 AM).

If multiple events are selected, the time filter is applied from the earliest to the most recent time stamp. For three events that have the time stamps 1 January 2014 8:28:46 AM, 7 January 2014 8:23:20 AM, and 8 January 2014 8:15:26 AM, the **Search for events by node > 1 week before event**, returns matching events in the following time range: (25 December 2013 08:28:46 AM) to (08 January 2014 08:15:26 AM).

Restriction: The Web GUI and Operations Analytics - Log Analysis process time stamps differently. The Web GUI recognizes hours, minutes, and seconds but Operations Analytics - Log Analysis ignores seconds. This problem affects the **Show event dashboard by node** and **Search for events by node**. If the time stamp 8 January 2014 07:15:26 AM is passed, Operations Analytics - Log Analysis interprets this time stamp as 8 January 2014 07:15 AM. So, the results of subsequent searches might differ from the search that was originally run. The results are displayed differently depending on the tool. The time filter has no effect on how the results are displayed.

Tool	How search results are displayed
Show event dashboard by node	A dashboard is opened for the OMNIBus Static Dashboard custom app that shows the following information about the distribution of the matching events: • Event Trend by Severity • Event Storm by AlertGroup • Event Storm by Node • Hotspot by Node and AlertGroup • Severity Distribution • Top 5 AlertGroups Distribution • Top 5 Nodes Distribution • Hotspot by AlertGroup and Severity For more information about the OMNIBus Static Dashboard custom app, see the Tivoli Netcool/OMNIBus Insight Pack README file.
Search for similar events and Search for events by node	The results are displayed in the search timeline, which shows the distribution of matching events over the specified time period. Below the timeline, the list of results is displayed. Click Table View or List View to change how the results are formatted. Click > or < to move forward and back in the pages of results. Keywords that occur multiple times in the search results are displayed in the Common Patterns area of the navigation pane, with the number of occurrences in parentheses ().
Show keywords and event count	The keywords are displayed in the Configured Patterns area of the Operations Analytics - Log Analysis GUI. Each occurrence of the keyword over the time period is counted and displayed in parentheses () next to the keyword.

- After the results are displayed, you can refine them by performing further searches on the results in the search workspace. For example, click a keyword from the **Configured Patterns** list to add it to the **Search** field.

Important: Because of the difference in handling seconds between the two products, if you run a further search against the keyword counts that result from the **Show keywords and event count** tool, you might see a difference in the count that was returned for a keyword under **Configured Patterns** and in the search that you run in the search workspace.

Above the **Search** field, a sequence of breadcrumbs is displayed to indicate the progression of your search. Click any of the breadcrumb items to return the results of that search.

Example

The **Show keywords and event count** tool can examine what happened before a problematic event in your environment. Assume that high numbers of critical events are being generated in an event storm. A possible work flow is as follows:

- You select a number of critical events and click **Event search > Show keywords and event count > 1 hour before event** so that you can identify any similarities between critical events that occurred in the last hour.
- The most recent time stamp (FirstOccurrence) of an event is 1 January 2014 8:28:00 AM. In the Operations Analytics - Log Analysis GUI, the search results show all keywords from the Summary, Node, and AlertGroup fields and the number of occurrences.
- You notice that the string “swt0001”, which is the host name of a switch in your environment, has a high number of occurrences. You click **swt0001** and run a further search, which reduces the number of results to only the events that contain “swt0001”.
- From this pared-down results list, you quickly notice that one event shows that switch is misconfigured, and that this problem is causing problems downstream in the environment. You can then return to the event list in the Web GUI and take action against this single event.

What to do next

Perform the actions that are appropriate for your environment against the events that are identified by the searches. See http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/webtop/wip/task/web_use_jsel_manageevents.html? for the Event Viewer and http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/webtop/wip/task/web_use_ael_managingevents.html? for the AEL.

Related tasks:

“Configuring event search” on page 94

“Customizing event management tools” on page 98

Related reference:

“Troubleshooting event search” on page 106

Related information:

 Using Operations Analytics - Log Analysis V1.3.5 to search data

 Using Operations Analytics - Log Analysis V1.3.3 to search data

 Event search examples on IBM DeveloperWorks

Event search workflow for operators

A typical workflow to show operators how the event search tools can assist triaging and diagnostics from the event list.

Assume the following situation: An event storm has been triggered but the cause of the storm is unclear. For the past hour, large numbers of critical events have been generated. Run the event search tools against the critical events.

1. To gain an overview of what has happened since the event storm started, select the critical events. Then, right-click and click **Event search > Show event dashboard by node > 1 hour before event**. The charts that are displayed show how the critical events break down, by node, alert group, severity, and so on.
2. Check whether any nodes stand out on the charts. If so, close the Operations Analytics - Log Analysis GUI, return to the event list and find an event that originates on that node. For example, type a filter in the text box on the Event Viewer toolbar like the following example that filters on critical events from the *mynode* node.

```
SELECT * from alerts.status where Node = mynode; and Severity = 5;
```

After the event list refreshes to show only matching events, select an event, right-click, and click **Event search > Search for events by node > 1 hour before event**.

3. In the search results, check whether an event from that node stands out. If so, close the Operations Analytics - Log Analysis GUI, return to the event list, locate the event, for example, by filtering on the summary or serial number:

```
SELECT * from alerts.status where Node = mynode; and Summary like  
"Link Down ( FastEthernet0/13 )";
```

```
SELECT * from alerts.status where Node = mynode; and Serial = 4586967;
```

Action the event.

4. If nothing stands out that identifies the cause of the event storm, close the Operations Analytics - Log Analysis GUI and return to the event list. Select all the critical events again and click **Event searchShow keywords and event count 1 hour before event**.
5. From the results, look in the **Common Patterns** area on the navigation pane. Looks for keywords that are non generic but have a high occurrence, for instance host name or IP addresses.
6. Refine the search results by clicking relevant keywords to copy them to the **Search** field and running the search. All events in which the keyword occurs are displayed, and the **Common Patterns** area is updated.
7. If an event stands out as the cause of the event storm, close the Operations Analytics - Log Analysis GUI, return to the event list, and action the event. If not, continuously refine the search results by searching against keywords until a likely root cause event stands out.

For possible actions from the Event Viewer see http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNibus.doc_8.1.0/webtop/wip/task/web_use_jsel_manageevents.html. For possible actions from the Active Event List, see http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNibus.doc_8.1.0/webtop/wip/task/web_use_ael_manageevents.html. Other actions are possible, depending on the tools that are implemented in your environment.

Related information:

-  Event search examples on IBM DeveloperWorks
-  Using Operations Analytics - Log Analysis V1.3.5 to search data
-  Using Operations Analytics - Log Analysis V1.3.3 to search data

Troubleshooting event search

How to resolve problems with your event search configuration.

- “You must log in each time you switch between interfaces” on page 107
- “Operations Analytics - Log Analysis session times out after 2 hours” on page 107
- “Launch to Operations Analytics - Log Analysis fails on Firefox in non-English locales” on page 108
- “Right-click tool fail to start Operations Analytics - Log Analysis from event lists” on page 108
- “Error message displayed when dynamic dashboard is run” on page 109

- “Error message displayed on “Show event dashboard by node” tool from event lists” on page 109
- “No results found by “Search for similar events” tool” on page 109
- “Chart display in Operations Analytics - Log Analysis changes without warning” on page 109 “Keyword searches return 0 results” on page 109

You must log in each time you switch between interfaces

The problem occurs if single sign-on (SSO) is not configured. If the Web GUI and Operations Analytics - Log Analysis are on the same host computer, you must log in each time you switch between the interfaces in your browser.

This problem happens because each instance of WebSphere Application Server uses the same default name for the LTPA token cookie: LtpaToken2. When you switch between the interfaces, one WebSphere Application Server instance overwrites the cookie of the other and your initial session is ended.

The ways of resolving this problem are as follows:

- Customize the domain name in the Web GUI SSO configuration:
 1. In the administrative console of the WebSphere Application Server that hosts the Web GUI, click **Security > Global security**. Then, click **Authentication > Web security** and click **Single sign-on (SSO)**.
 2. Enter an appropriate domain name for your organization, for example, `ibm.com`. By default, the domain name field is empty and the cookie's domain is the host name. If you also customize the domain name in the Operations Analytics - Log Analysis WebSphere Application Server, to avoid any conflict ensure that the two domain names are different.
 3. Restart the Dashboard Application Services Hub server.
- Use the fully qualified domain name for accessing one instance of WebSphere Application Server and the IP address for accessing the other. For example, always access the Web GUI by the fully qualified domain name and always access Operations Analytics - Log Analysis by the IP address. To configure the Web GUI to access Operations Analytics - Log Analysis by the IP address:
 1. In the `$WEBGUI_HOME/etc/server.init` file, change the value of the `scala.url` property to the IP address of the host, For example:
`https://3.127.46.125:9987/Unity`
 2. Restart the Dashboard Application Services Hub server. See http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/webtop/wip/task/web_adm_server_restart.html.

Operations Analytics - Log Analysis session times out after 2 hours

This problem occurs if SSO is not configured. The first time that you start the Operations Analytics - Log Analysis product from an event list in the Web GUI, you are prompted to log in to Operations Analytics - Log Analysis. You are automatically logged out after 2 hours and must reenter your login credentials every 2 hours. This problem occurs because the default expiration time of the LTPA token is 2 hours.

To resolve this problem, change the session timeout in the Operations Analytics - Log Analysis product as follows:

1. In the `$SCALA_HOME/wlp/usr/servers/Unity/server.xml` file, increase the value of the `<ltpa expiration="120m"/>` attribute to the required value, in minutes. For example, to change the session timeout to 540 minutes:

```
</oauthProvider>
  <ltpa expiration="540"/>
  <webAppSecurity ssoDomainNames="hostname" httpOnlyCookies="false"/>
</server>
```

2. Restart the Operations Analytics - Log Analysis WebSphere Liberty Profile.

Launch to Operations Analytics - Log Analysis fails on Firefox in non-English locales

This problem is a known issue when you launch from the Active Event List (AEL) into the Firefox browser.

If your browser is set to a language other than US English (en_us) or English (en), you might not be able to launch into Operations Analytics - Log Analysis from the Web GUI AEL.

This problem happens because Operations Analytics - Log Analysis does not support all the languages that are supported by Firefox.

To work around this problem, try setting your browser language to an alternative language version. For example, if the problem arises when the browser language is French[fr], set the language to French[fr-fr]. If the problem arises when the browser language is German[de-de], set the language to German[de].

Right-click tool fail to start Operations Analytics - Log Analysis from event lists

The following error is displayed when you start the tools from the right-click menu of an event list:

```
CTGA0026E: The APP name in the query is invalid or it does not exist
```

This error occurs because the custom app that is defined in the `$WEBGUI_HOME/etc/server.init` file does not match the file names in the Tivoli Netcool/OMNIBus Insight Pack.

To resolve this problem, set the **scala.app.keyword** and **scala.app.static.dashboard** properties in the `server.init` file accordingly.

- If the properties are set as follows, the version of the Insight Pack needs to be V1.1.0.2:

```
scala.app.keyword=OMNIBus_Keyword_Search
scala.app.static.dashboard=OMNIBus_Static_Dashboard
```

- If the properties are set as follows, the version of the Insight Pack needs to be V1.1.0.1 or V1.1.0.0:

```
scala.app.keyword= OMNIBus_SetSearchFilter
scala.app.static.dashbaord=OMNIBus_Event_Distribution
```

If you need to change the values of these properties, restart the Dashboard Application Services Hub server afterwards. See http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/webtop/wip/task/web_adm_server_restart.html.

Error message displayed when dynamic dashboard is run

The following error is displayed when you run a dynamic dashboard from the Operations Analytics - Log Analysis product:

```
undefined not found in results data
```

This error is a known defect in the Operations Analytics - Log Analysis product. To resolve, it close and then reopen the dynamic dashboard.

Error message displayed on “Show event dashboard by node” tool from event lists

An error message is displayed when you start the **Show event dashboard by node** tool from an event list.

This error is caused by incompatibility between the version of the Insight Pack and the and the version of the Operations Analytics - Log Analysis product. For example, if Operations Analytics - Log Analysis is at V1.2.0.3 and the Insight Pack is at V1.1.0.1, the error is displayed.

Ensure that the versions are compatible. See “Required products and components” on page 93. For more information about checking which version of the Insight Pack is installed, see Checking the version of the Insight Pack.

No results found by “Search for similar events” tool

No results are returned by the **Search for similar events** tool. A No results found matching the search message is displayed.

This error occurs because the Web GUI is not configured to integrate with V1.2.0.3 of the Operations Analytics - Log Analysis product. The search query that is generated by the tool is not compatible with V1.2.0.3 of Operations Analytics - Log Analysis.

To resolve this problem:

1. Check that the version of the Operations Analytics - Log Analysis is V1.2.0.3.
2. In the file set the **scala.version** property as follows:
`scala.version = 1.2.0.3`
3. Restart the Dashboard Application Services Hub server. See http://www-01.ibm.com/support/knowledgecenter/SSHTQ_8.1.0/com.ibm.netcool_OMNibus.doc_8.1.0/webtop/wip/task/web_adm_server_restart.html.

Chart display in Operations Analytics - Log Analysis changes without warning

The sequence in which charts are displayed on the Operations Analytics - Log Analysis GUI can changes intermittently. This problem is a known defect in the Operations Analytics - Log Analysis product and has no workaround or solution.

Keyword searches return 0 results

This problem occurs only with Operations Analytics - Log Analysis V1.2.0.3. A keyword search returns 0 results. V1.2.0.3 of the Operations Analytics - Log Analysis product uses asynchronous searches. The search result appears to be 0

while data is still being fetched. Wait a few seconds while the data is loaded before checking the results again.

Related tasks:

“Configuring single sign-on for the event search capability” on page 97

“Searching for events” on page 102

 Restarting the Dashboard Application Services server

 WebSphere Application Server Liberty: Starting and stopping a server from the command prompt

Event Analytics

Use Event Analytics to help you analyze seasonal trends and related events, while you monitor and manage events.

Event Analytics overview

Event Analytics allows you to identify seasonal patterns of events and related events within their monitored environment.

Seasonal events

Event Analytics uses statistical analysis of IBM Tivoli Netcool/OMNIBus historical event data to determine the seasonality of events, such as when and how frequently events occur. The results of this analysis are output in both reports and graphs.

The data that is presented in the event seasonality report helps you to identify seasonal event patterns within their infrastructure. For example, an event that periodically occurs at an unscheduled specific time is highlighted. Seasonal Event Rules are grouped by state in the Seasonal Event Rules portlet. You can

- Use the View Seasonal Events UI to analyze seasonal events and associated related events.
- Deploy validated seasonal event rules, without writing new code. Rules that are generated in this way can have various actions applied to them.

Related events

Event Analytics uses statistical analysis of Tivoli Netcool/OMNIBus historical event data to determine which events have a statistical tendency to occur together. Event Analytics outputs the results of this statistical analysis as event groups, on a scheduled basis. You can:

- Use the related events UI to analyze these event groups.
- Deploy validated event groups as Netcool/Impact correlation rules with a single click, without the need to write any code. Correlation rules that are generated in this way act on real-time event data to show a single synthetic event for the events in the event group.
- Present all events in the group as children of this synthetic event. This view decreases the number of events displayed to your operations staff in the Event Viewer.
- Use the Related Event portlet to analyze patterns in groups and deploy correlation rules based on common event types between the groups.

The system uses the most actionable event in the group as the parent event to be set by the correlation rule. By default, the most actionable event in the group is the most ticketed or acknowledged event. Before you deploy the correlation rule, you can change the parent event setting. A synthetic event is created with some of the properties of the parent event, and all the related events are grouped under this synthetic event.

Event groups are generated by scheduled runs of related event configurations. A default related event configuration is provided. You can create your own configurations and specify which historical data to analyze. For example, you can specify a custom time range, an event filter, and schedule. For more information about related events, see “Related events” on page 165.

You can create a pattern based on the related event groups discovered by the related event analytic. Patterns are similar to related event groups but patterns, unlike related event groups are not specific to a resource. You can use an event in the group as the parent event to be set by the correlation rule, or create a synthetic event as the parent. You can also test the performance of a pattern before it is created to check the number of related events groups and events returned for a pattern.

Installing and uninstalling Event Analytics

Read the following topics before you install or uninstall Event Analytics.

Prerequisites

Before you install Event Analytics you must complete the following preinstallation tasks.

Event Archiving

You must be running a database with archived events. Event Analytics supports the DB2 and Oracle databases. Event Analytics support of MS SQL requires a minimum of IBM Tivoli Netcool/Impact 7.1.0.1.

You can use a gateway to archive events to a database. In reporting mode, the gateway archives events to a target database. For more information, see http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/gateways/jdbcgw/wip/concept/jdbcgw_intro.html.

Note: The gateway can operate in two modes: audit mode and reporting mode. Event Analytics only supports reporting mode.

Browser Requirements

To display the Seasonal Event Graphs in Microsoft Internet Explorer, you must install the Microsoft Silverlight plug-in.

Reduced Memory

If you are not running Event Analytics on Solaris, remove the comment from or add the following entry in the `jvm.options` file:

```
#-Xgc:classUnloadingKickoffThreshold=100
```

Removing the comment from or adding that entry dynamically reduces memory requirements.

Installing Event Analytics

You can install Event Analytics with the IBM Installation Manager GUI or console, or do a silent installation. Event Analytics supports IBM Installation Manager 1.7.2 up to 1.8.4.

For more information about installing and using IBM Installation Manager, see the following IBM Knowledge Center:

http://www-01.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

Installing Event Analytics (GUI)

You can install Event Analytics with the IBM Installation Manager GUI.

Before you begin

- Determine which Installation Manager user mode you require.
- Ensure that the necessary user permissions are in place for your intended installation directories.
- Configure localhost on the computer where Event Analytics packages are to be installed.

About this task

The installation of Event Analytics requires you to install product packages for the following product groups:

- IBM Tivoli Netcool/Impact
- IBM Tivoli Netcool/OMNIBus
- IBM Netcool.

The steps for starting Installation Manager are different depending on which user mode you installed it in. The steps for completing the Event Analytics installation with the Installation Manager wizard are common to all user modes and operating systems.

Installation Manager takes account of your current umask settings when it sets the permissions mode of the files and directories that it installs. If you use Administrator mode or Non-administrator mode and your umask is 0, Installation Manager uses a umask of 22. If you use Group mode, Installation Manager ignores any group bits that are set and uses a umask of 2 if the resulting value is 0.

To install the packages and features, complete the following steps.

Procedure

1. Start Installation Manager. Change to the `/eclipse` subdirectory of the Installation Manager installation directory and use the following command to start Installation Manager:

```
./IBMIM
```

To record the installation steps in a response file for use with silent installations on other computers, use the `-record response_file` option. For example:

```
./IBMIM -record /tmp/install_1.xml
```

2. Configure Installation Manager to point to either a local repository or an IBM Passport Advantage repository, where the download packages are available.

Within the IBM Knowledge Center content for Installation Manager, see the topic that is called *Installing packages by using wizard mode*.

3. In the main Installation Manager window, click **Install** and follow the installation wizard instructions to complete the installation.
4. In the Install tab select the following installation packages, and then click **Next**.
 - Packages for IBM Tivoli Netcool/Impact:
 - IBM Tivoli Netcool/Impact GUI Server_7.1.0.5
 - IBM Tivoli Netcool/Impact Server_7.1.0.5
 - IBM Tivoli Netcool/Impact Server Extensions for Netcool Operations Insight_7.1.0.5
 - IBM Tivoli Netcool/Impact GUI Server_7.1.0.9
 - IBM Tivoli Netcool/Impact Server_7.1.0.9
 - IBM Tivoli Netcool/Impact Server Extensions for Netcool Operations Insight_7.1.0.9
 - Packages for IBM Tivoli Netcool/OMNIBus:
 - IBM Tivoli Netcool/OMNIBus_8.1.0.6
 - IBM Tivoli Netcool/OMNIBus_8.1.0.11
 - Packages for IBM Netcool:
 - IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.5
 - IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.9
 - Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_1.4.0.1.
 - Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.9.
5. In the Licenses tab, review the licenses. If you are happy with the license content select **I accept the terms in the license agreements** and click **Next**.
6. In the Location tab, enter information for the Installation Directory and Architecture or progress with the default values, and click **Next**.
 - For IBM Netcool, the default values are /opt/IBM/netcool and 64-bit.
 - For IBM Netcool Impact, the default values are /opt/IBM/tivoli/impact and 64-bit.
7. In the Features tab, select the following features and then click **Next**. Other features are auto-selected.

Table 20. Available features

Feature	Description
IBM Tivoli Netcool/OMNIBus Web GUI 8.1.0.5 > Install base features	To install and run Event Analytics.
Netcool Operations Insight Extensions Web GUI 1.4.0.1 > Install Event Analytics	Contains the Event Analytics components.

Table 21. Available features

Feature	Description
IBM Tivoli Netcool/OMNIBus Web GUI 8.1.0.9 > Install base features	To install and run Event Analytics.
Netcool Operations Insight Extensions Web GUI 8.1.0.9 > Install Event Analytics	Contains the Event Analytics components.

8. In the Summary tab, review summary details. If you are happy with summary details click **Next**, but if you need to change any detail click **Back**.
9. To complete the installation, click **Finish**.

Results

Installation Manager installs Event Analytics.

What to do next

1. Configure the ObjectServer for Event Analytics, see “Configuring the Event Analytics ObjectServer” on page 199.
2. Connect to a valid database from within IBM Tivoli Netcool/Impact. To configure a connection to one of the Event Analytics supported databases, see the following topics:
 - DB2: “Configuring DB2 database connection within Impact” on page 202
 - Oracle: “Configuring Oracle database connection within Impact” on page 200
 - MS SQL: “Configuring MS SQL database connection within Impact” on page 204
3. If you add a cluster to the Impact environment, you must update the data sources in IBM Tivoli Netcool/Impact 7.1.0.4. For more information, see “Adding a cluster to the Netcool/Impact environment” on page 212.
4. If you add a cluster to the Impact environment, you must update the data sources in IBM Tivoli Netcool/Impact 7.1.0.9. For more information, see “Adding a cluster to the Netcool/Impact environment” on page 212.
5. You must set up a remote connection from the Dashboard Application Services Hub to Netcool/Impact. For more information, see “Netcool/Impact remote connection” on page 206.

Installing Event Analytics (Console)

You can install Event Analytics with the IBM Installation Manager console.

Before you begin

Obtain an IBM ID and an entitlement to download Event Analytics from IBM Passport Advantage. The packages that you are entitled to install are listed in Installation Manager.

Take the following actions:

- Determine which Installation Manager user mode you require.
- Ensure that the necessary user permissions are in place for the installation directories.
- Decide which features that you want to install from the installation packages and gather the information that is required for those features.
- Configure localhost on the computer where Event Analytics is to be installed.

About this task

The steps for starting Installation Manager are different depending on which user mode you installed it in. The steps for completing the Event Analytics installation with the Installation Manager console are common to all user modes and operating systems.

Installation Manager takes account of your current umask settings when it sets the permissions mode of the files and directories that it installs. If you use Administrator mode or Non-administrator mode and your umask is 0, Installation Manager uses a umask of 22. If you use Group mode, Installation Manager ignores any group bits that are set and uses a umask of 2 if the resulting value is 0.

Procedure

1. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.
2. Use the following command to start Installation Manager:
 - `./imcl -c` OR `./imcl -consoleMode`
3. Configure Installation Manager to download package repositories from IBM Passport Advantage:
 - a. From the Main Menu, select **Preferences**.
 - b. In the **Preferences** menu, select **Passport Advantage**.
 - c. In the **Passport Advantage** menu, select **Connect to Passport Advantage**.
 - d. When prompted, enter your IBM ID user name and password.
 - e. Return to the Main Menu.
4. From the options that are provided on the installer, add the repository that you want to install.
5. From the Main Menu, select **Install**.

Follow the installer instructions to complete the installation. The installer requires the following inputs at different stages of the installation:

 - Select Event Analytics
 - When prompted, enter an Installation Manager shared directory or accept the default directory.
 - When prompted, enter an installation directory or accept the default directory.
 - Clear the features that you do not require.
 - If required, generate a response file for use with silent installations on other computers. Enter the directory path and a file name with a `.xml` extension. The response file is generated before installation completes.
6. When the installation is complete, select **Finish**.

Results

Installation Manager installs Event Analytics.

What to do next

If you add a cluster to the Impact environment, you must update the data sources in IBM Tivoli Netcool/Impact 7.1. For more information, see “Adding a cluster to the Netcool/Impact environment” on page 212.

Silently installing Event Analytics

You can install Event Analytics silently with IBM Installation Manager. This installation method is useful if you want identical installation configurations on multiple workstations. Silent installation requires a response file that defines the installation configuration.

Before you begin

Take the following actions:

- Create or record an Installation Manager response file.

You can specify a local or remote IBM Tivoli Netcool/OMNIBus package and a Netcool Operations Insight Extensions Web GUI package with a repository in the response file. You can also specify that Installation Manager downloads the packages from IBM Passport Advantage. For more information about specifying authenticated repositories in response files, search for the *Storing credentials* topic in the Installation Manager information center:

http://www-01.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

A default response file is included in the Event Analytics installation package in `responsefiles/platform`, where *platform* can be *unix* or *windows*.

When you record a response file, you can use the `-skipInstall` argument to create a response file for an installation process without performing the installation. For example:

- Create or record a `skipInstall`:

```
IBMIM.exe -record C:\response_files\install_1.xml -skipInstall  
C:\Temp\skipInstall
```

- Determine which Installation Manager user mode you require.
- Read the license agreement. The license agreement file, `license.txt`, is stored in the `/native/license_version.zip` archive, which is contained in the installation package.
- Ensure that the necessary user permissions are in place for your intended installation directories.
- Configure `localhost` on the computer where Event Analytics is to be installed.

Procedure

1. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.
2. To encrypt the password that is used by the administrative user for the initial log-in to Dashboard Application Services Hub, run the following command:
 - `./imutilsc encryptString password`

Where *password* is the password to be encrypted.

3. To install Event Analytics, run the following command:
 - `./imcl -input response_file -silent -log /tmp/install_log.xml -acceptLicense`

Where *response_file* is the directory path to the response file.

Results

Installation Manager installs Event Analytics.

What to do next

If you add a cluster to the Impact environment, you must update the data sources in IBM Tivoli Netcool/Impact 7.1. For more information, see “Adding a cluster to the Netcool/Impact environment” on page 212.

Upgrading Event Analytics

You can upgrade the IBM Netcool Operations Insight packages for Event Analytics by applying the latest fix packs.

About this task

To upgrade to Event Analytics on an IBM Netcool Operations Insight 1.4.0.5 platform, use the IBM Installation Manager **Update** functions to locate update packages, and update your environment with the following product update packages:

- IBM Tivoli Netcool/Impact GUI Server_7.1.0.9
- IBM Tivoli Netcool/Impact Server_7.1.0.9
- IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.9
- IBM Tivoli Netcool/OMNIBus_8.1.0.11
- IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.9
- IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.9

Procedure

The product update packages must be updated individually. Complete steps 1 - 3 for each product update package.

1. Start Installation Manager. Change to the `/eclipse` subdirectory of the Installation Manager installation directory and enter the following command to start Installation Manager:
`./IBMIM`
2. Configure Installation Manager to point to either a local repository or an IBM Passport Advantage repository, where the download package is available. Within the IBM Knowledge Center content for Installation Manager, see the topic that is called *Installing packages by using wizard mode*. See the following URL within the IBM Knowledge Center content for Installation Manager:
http://www-01.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
3. In the main Installation Manager window, click **Update** and complete the following type of installation wizard instructions to complete the installation of your update package:
 - a. In the Update Packages tab, select the product group to find related update packages, and click **Next**. A list of the available update packages displays.
 - b. From the list of available update packages, select one update package that you want to install, and click **Next**. Remember you can install only one update package at a time.
 - c. In the Licenses tab, review the licenses. Select **I accept the terms in the license agreements** and click **Next**.
 - d. In the Features tab, select the features for your update package, and click **Next**.

- e. Complete the configuration details, and click **Next**.
 - f. In the Summary tab, review summary details. If you need to change any detail click **Back**, but if you are happy with summary details click **Update** and wait for the installation of the update package to complete.
 - g. When the installation of the update package completes, the window updates with details of the installation. Click **Finish**.
4. To ensure that the seasonal event reports that were created before upgrading to IBM Netcool Operations Insight 1.4.0.5 are visible, you must run the SE_CLEANUPDATA policy as follows.
 - a. Login as the administrator to the server where IBM Tivoli Netcool/Impact is stored and running.
 - b. Navigate to the policies tab and search for the SE_CLEANUPDATA policy.
 - c. To open the policy, double-click on the policy.
 - d. To run the policy, select the run button on the policy screen toolbar.
 5. To view the event configurations in the View Seasonal Events portlet, rerun the configurations. For more information about running event configurations, see the “Configure Analytics portlet” on page 131 topics.

What to do next

1. Verify that the correct packages are installed. After you update each package, and to ensure that you have the correct environment for Event Analytics on IBM Netcool Operations Insight 1.4.0.5, verify that the following packages are installed.
 - IBM Tivoli Netcool/Impact packages:
 - IBM Tivoli Netcool/Impact GUI Server_7.1.0.9
 - IBM Tivoli Netcool/Impact Server_7.1.0.9
 - IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.9
 - IBM Tivoli Netcool/OMNIBus packages:
 - IBM Tivoli Netcool/OMNIBus_8.1.0.11
 - IBM Netcool® packages.
 - IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.9
 - IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.9
2. Configure the ObjectServer for Event Analytics. For more information about configuring the ObjectServer for Event Analytics, see “Configuring the Event Analytics ObjectServer” on page 199.
3. Connect to a valid database from within IBM Tivoli Netcool/Impact. To configure a connection to one of the Event Analytics supported databases, see the following topics:
 - DB2: “Configuring DB2 database connection within Impact” on page 202
 - Oracle: “Configuring Oracle database connection within Impact” on page 200
 - MS SQL: “Configuring MS SQL database connection within Impact” on page 204
4. If you add a cluster to the Impact environment, you must update the data sources in IBM Tivoli Netcool/Impact 7.1. For more information, see “Adding a cluster to the Netcool/Impact environment” on page 212.
5. If you want to make use of the pattern generalization feature in Event Analytics, you must configure the type properties used for event pattern creation in IBM Tivoli Netcool/Impact. For more information about configuring

the type properties used for event pattern creation in IBM Tivoli Netcool/Impact, see “Configuring the type properties used for event pattern creation in Netcool/Impact” on page 192.

Upgrading Event Analytics from stand-alone installations of IBM Tivoli Netcool/OMNIBus and IBM Tivoli Netcool/Impact

If you have stand-alone installations of IBM Tivoli Netcool/OMNIBus with IBM Netcool/OMNIBus Web GUI and IBM Tivoli Netcool/Impact, you can upgrade to Event Analytics for IBM Netcool Operations Insight 1.4.0.5.

Before you begin

Ensure that the following product packages are already installed:

- IBM Tivoli Netcool/Impact packages:
 - IBM Tivoli Netcool/Impact GUI Server_7.1.0.9
 - IBM Tivoli Netcool/Impact Server_7.1.0.9
- IBM Tivoli Netcool/OMNIBus packages:
 - IBM Tivoli Netcool/OMNIBus_8.1.0.11
- IBM Netcool packages:
 - IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.9

About this task

This upgrade scenario is for users who already use Tivoli Netcool/OMNIBus and Netcool/Impact but do not have the Netcool Operations Insight packages that are needed for the Event Analytics function, and now want the Event Analytics function.

For this upgrade scenario, you must use IBM Installation Manager to **Install** the product packages that are required for the Event Analytics function, then **Update** the product packages. The **Install** of product packages locates and installs the following two packages:

IBM Tivoli Netcool/Impact Server Extensions for Netcool Operations
Insight_7.1.0.9
Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web
GUI_8.1.0.9

To upgrade to IBM Netcool Operations Insight 1.4.0.5 Event Analytics, complete the following steps.

Procedure

1. Start Installation Manager. Change to the `/eclipse` subdirectory of the Installation Manager installation directory and enter the following command to start Installation Manager:
`./IBMIM`
2. Configure Installation Manager to point to either a local repository or an IBM Passport Advantage repository, where the download package is available. Within the IBM Knowledge Center content for Installation Manager, see the topic that is called *Installing packages by using wizard mode*. See the following URL within the IBM Knowledge Center content for Installation Manager:
http://www-01.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

3. To install your packages in the main Installation Manager, click **Install** and complete the steps in the installation wizard to complete the installation of your packages:
 - a. In the Install tab, select the following product groups and product installation packages, and click **Next**.
 - IBM Tivoli Netcool/Impact Server Extensions for Netcool Operations Insight
Version 7.1.0.9
 - Tivoli Netcool/OMNIBus Web GUI
Version 8.1.0.9
 - Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI
Version 8.1.0.9
 - b. In the Licenses tab, review the licenses. When you are happy with the license content select **I accept the terms in the license agreements** and click **Next**.
 - c. In the Location tab, use the existing package group and location.
 - d. In the Features tab, select the features for your packages, and click **Next**.
 - e. In the Summary tab, review summary details. If you need to change any detail click **Back**, but if you are happy with summary details click **Install** and wait for installation of the package to complete.
 - f. When installation of the packages completes, the window updates with details of the installation. Click **Finish**.
4. Migrate the rollup configuration. For more information about updating the rollup configuration, see “Updating Rollup Configuration” on page 122.

What to do next

1. Verify that the correct packages are installed. After you update each package, and to ensure that you have the correct environment for Event Analytics on IBM Netcool Operations Insight 1.4.0.5, verify that the following packages are installed.
 - IBM Tivoli Netcool/Impact packages:
 - IBM Tivoli Netcool/Impact GUI Server_7.1.0.9
 - IBM Tivoli Netcool/Impact Server_7.1.0.9
 - IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.9
 - IBM Tivoli Netcool/OMNIBus packages:
 - IBM Tivoli Netcool/OMNIBus_8.1.0.11
 - IBM Netcool packages.
 - IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.9
 - IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_8.1.0.9
2. Configure the ObjectServer for Event Analytics. For more information about configuring the ObjectServer for Event Analytics, see “Configuring the Event Analytics ObjectServer” on page 199.
3. Connect to a valid database from within IBM Tivoli Netcool/Impact. To configure a connection to one of the Event Analytics supported databases, see the following topics:
 - DB2: “Configuring DB2 database connection within Impact” on page 202

- Oracle: “Configuring Oracle database connection within Impact” on page 200
 - MS SQL: “Configuring MS SQL database connection within Impact” on page 204
4. If you add a cluster to the Impact environment, you must update the data sources in IBM Tivoli Netcool/Impact 7.1. For more information, see “Adding a cluster to the Netcool/Impact environment” on page 212.
 5. If you want to make use of the pattern generalization feature in Event Analytics, you must configure the type properties used for event pattern creation in IBM Tivoli Netcool/Impact. For more information about configuring the type properties used for event pattern creation in IBM Tivoli Netcool/Impact, see “Configuring the type properties used for event pattern creation in Netcool/Impact” on page 192.

Updating Rollup Configuration

You can add columns to Seasonal Event reports and Related Events reports. Update the rollup configuration to add columns to reports.

Before you begin

You must export the current configuration into the properties file.

1. Log in to the server where IBM Tivoli Netcool/Impact is stored and running.
2. Go to the *<Impact install location>/bin* directory.
3. Enter the following command.


```
./nci_trigger NCI <UserID>/<password> NOI_DefaultValues_Export FILENAME
<Full Path to the file name>.properties
```

<UserID>
Specifies the ID of the Impact user.

<password>
Specifies the password of the Impact user.

<Full Path to the file name>
Specifies the directory where the properties file is stored.

About this task

To update the rollup configuration, complete the following steps.

Procedure

1. Update the properties file that you created in the Before you being.
 - a. Specify the number of columns you want to add to the reports:

Increase the value of the `number_of_rollup_configuration=2` parameter for seasonal events.

Increase the value of the `reevent_number_of_rollup_configuration=2` parameter for related events.

For example, to add one column to the reports, increase the parameter value by one from 2 to 3.
 - b. For a new rollup column, add property information.
 - For a new Seasonal Event reports column, add the following properties.


```
rollup_<rollup number>_column_name=<column name>
rollup_<rollup number>_display_name=<display name>
rollup_<rollup number>_type=<type>
```
 - For a new Related Events reports column, add the following properties.


```
reevent_rollup_<rollup number>_column_name=<column name>  
reevent_rollup_<rollup number>_display_name=<display name>  
reevent_rollup_<rollup number>_type=<type>  
reevent_rollup_<rollup number>_actionable=<true/false>
```

<rollup number>

Specifies the new column rollup number.

<column name>

Specifies the new column name. The column name must match the column name in the history table.

<display name>

Specifies the new column display name. The display name must match the column name in the report.

<type>

Specifies one of the following types:

MAX The maximum value observed for the column. If no value is observed, the value defaults to the minimum value of an integer.

MIN The minimum value observed for the column. If no value is observed, the value defaults to the maximum value of an integer.

SUM The sum of all of the values observed for the column.

NON_ZERO

A counting column that counts *nonzero* occurrences of events. This column can be useful to track the proportion of actioned events, or how many events had an associated ticket number.

DISTINCT

The number of distinct values that are seen for this key-value pair.

EXAMPLE

Displays the first non-blank *example* of a field that contained this key. The EXAMPLE type is useful when you are running seasonality on a non-digestible field such as ALERT_IDENTIFIER, and you want an example human readable SUMMARY to demonstrate the type of problem.

actionable=<true/false>

If this property is set to true for a rollup, the rollup is used to determine the probable root cause of a correlation rule. This root cause determination is based on the rollup that has the most actions that are taken against it. For example, if Acknowledge is part of your rollup configuration and has a property value of actionable=true, then the event with the highest occurrence of Acknowledge is determined to be the probable root cause. Probable root cause determination uses the descending order of the actionable rollups, that is, the first actionable rollup is a higher priority than the second actionable rollup. Only four of the possible <type> keywords are valid for root cause: MAX, MIN, SUM, NON_ZERO.

If this property is set to false for a rollup, the rollup is not used to determine the probable root cause of a rule. If all rollup configurations have a property value of actionable=false, the first event that is found is identified as the parent.

To manually change a root cause event for a correlation rule, see
“Selecting a root cause event for a correlation rule” on page 180.

2. Run the following command to update the current configuration:

```
./nci_trigger NCI <UserID>/<password> NOI_DefaultValues_Configure  
FILENAME <Full Path to the file name>.properties
```

Results

The rollup configuration is updated.

Example

Example 1. To add a third column to the Seasonal Event report, change the rollup configuration value to 3, and add the properties.

```
number_of_rollup_configuration=3  
rollup_1_column_name=SEVERITY  
rollup_1_display_name=MINSeverity  
rollup_1_type=MIN  
rollup_2_column_name=SEVERITY  
rollup_2_display_name=MAXSeverity  
rollup_2_type=MAX  
rollup_3_column_name=TYPE  
rollup_3_display_name=TYPE  
rollup_3_type=MAX
```

Example 2. The configuration parameters for a default Related Events report.

```
reevent_rollup_1_column_name=ORIGINALSEVERITY  
reevent_rollup_1_display_name=MINSeverity  
reevent_rollup_1_type=MAX  
reevent_rollup_1_actionable=true  
reevent_rollup_2_column_name=ACKNOWLEDGED  
reevent_rollup_2_display_name=Acknowledged  
reevent_rollup_2_type=NON_ZERO  
reevent_rollup_2_actionable=true  
reevent_rollup_3_column_name=ALERTGROUP  
reevent_rollup_3_display_name=AlertGroup  
reevent_rollup_3_type=EXAMPLE  
reevent_rollup_3_actionable=false
```

What to do next

To add columns to the Seasonal Event reports, Historical Event portlet, Related Eventreports, or Related Event Details portlet complete the following steps:

1. Log in to the Tivoli Netcool/Impact UI.
2. Go to the **Policies** tab.
3. Open the policy that you want to modify. You can modify one policy at a time.
 - For Historical Events, open the **SE_GETHISTORICALEVENTS** policy.
 - For Seasonal Events, open the **SE_GETEVENTDATA** policy.
 - For related events groups, open one of the following policies.

```
RE_GETGROUPS_ACTIVE  
RE_GETGROUPS_ARCHIVED  
RE_GETGROUPS_EXPIRED  
RE_GETGROUPS_NEW  
RE_GETGROUPS_WATCHED
```

Note: Each policy is individually updated. To update two or more policies, you must modify each policy individually.

- For related events, open one of the following policies.

RE_GETGROUPEVENTS_ACTIVE
RE_GETGROUPEVENTS_ARCHIVED
RE_GETGROUPEVENTS_EXPIRED
RE_GETGROUPEVENTS_NEW
RE_GETGROUPEVENTS_WATCHED

Note: Each policy is individually updated. To update two or more policies, you must modify each policy individually.

- For related events details group instances table, open the following policy:

RE_GETGROUPINSTANCEV1

4. Click the **Configure Policy Settings** icon.

5. Under **Policy Output Parameters**, click **Edit**.

6. To create a custom schema definition, open the **Schema Definition Editor** icon.

7. To create a new field, click **New**.

8. Specify the new field name and format.

The new field name must match the display name in the configuration file.

The format must match the format in the **AlertsHistory** Table.

The format must be appropriate for the rollup type added. For example, for numerical types such as SUM or NON_ZERO use a numeric format. Use String for DISTINCT, if the base column is String.

Refresh the **SE_GETHISTORICALEVENTS_DB2** table, or other database model, before you run Event Analytics with the added Historical Event table fields.

For the RE_GETGROUPS_ policies, only rollup columns with a *<type>* value of MAX, MIN, SUM, NON_ZERO are supported. Therefore, add only numeric fields to the schema.

9. To complete the procedure, click **Ok** on each of the open dialog boxes, and **Save** on the **Policies** tab.

Note: Columns that are created for the Related Event Details before Netcool Operations Insight release 1.4.0.1 are displayed as designed. Configurations and groups that are created after you upgrade to Netcool Operations Insight release 1.4.0.1, display the events from the historical event. By adding columns to the Related Event Details, you can display additional information such as the **owner ID** or **ticketnumber**.

10. To add columns to the Related Event Details, update the RE_COLUMN_EVENT_INSTANCES variable in the RE_CONSTANTS policy in Impact. Add or remove fields from the static array. For example,

```
var RE_COLUMN_EVENT_INSTANCES = "NODE,SUMMARY,ALERTGROUP,SEVERITY,OWNERUID,ACKNOWLEDGED,TALLY";
```

You can also add the following columns for group instances in the Related Event Details:

- SERVERSERIAL
- SERVERNAME
- TALLY

- OWNERUID

By default, the previously listed columns are hidden for group instances in the Related Event Details. To display these columns in the Related Event Details, you need to edit the

Policy_RE_GETGROUPINSTANCEV1_RE_GETGROUPINSTANCEV1.properties file, which is located in the following directory: \$IMPACT_HOME/uiproviderconfig/properties.

Specifically, set the following properties in the Policy_RE_GETGROUPINSTANCEV1_RE_GETGROUPINSTANCEV1.properties file from their default values of true to the values false (or comment out the field or fields):

```
SERVERSERIAL.hidden=true
SERVERNAME.hidden=true
TALLY.hidden=true
OWNERUID.hidden=true
```

For example,

```
OWNERUID.hidden=false
```

Or, for example,

```
#OWNERUID.hidden=true
```

Mapping customized columns from the Event History database

You can map any customized columns in your Event History database tables to columns expected by IBM Tivoli Netcool/Impact for Event Analytics.

Before you begin

You must perform this task if you have customized table columns in your Event History database. For example, if you have defined columns called SUMMARYUPDATE and IDENTIFIERSTRING instead of the default names SUMMARY and IDENTIFIER, you must perform this task. You perform the mappings in the IBM Tivoli Netcool/Impact Apache Derby database table called RELATEDEVENTS.RE_MAPPINGS.

About this task

To map customized columns in your Event History database, complete the following steps.

Procedure

1. Log in to the server where IBM Tivoli Netcool/Impact is stored and running.
2. Go to the *<Impact install location>/bin* directory.
3. Run the following commands to connect to the IBM Tivoli Netcool/Impact Apache Derby backend database:

```
./nci_db connect
>connect derby_db
```

Where: *derby_db* specifies the JDBC (Java Database Connectivity) string for the Apache Derby backend database. For example:

```
connect 'jdbc:derby://testserver.ibm.com:1527/
ImpactDB;user=impact;password=derbypass';
```

4. Add the mappings for all of the customized table columns in your Event History database to the RELATEDEVENTS.RE_MAPPINGS Apache Derby database table. For example:

```
insert into RELATEDEVENTS.RE_MAPPINGS values ('SUMMARY','SUMMARYUPDATE');

insert into RELATEDEVENTS.RE_MAPPINGS values ('IDENTIFIER','IDENTIFIERSTRING');
```

Results

Adding the mappings of the customized table columns from the Event History database to the RELATEDEVENTS.RE_MAPPINGS Apache Derby database table will add the expected mappings to the IBM Tivoli Netcool/Impact data base.

What to do next

Ensure that any properties files used to configure Netcool/Impact for Event Analytics use the custom columns specified in the Event History database and not the usual values expected by Netcool/Impact. For example, consider the following column in a properties file:

```
history_column_names_analysis=SUMMARY
```

Given the previous example of a customized column called SUMMARYUPDATE, the following edit would need to be made to the properties file:

```
history_column_names_analysis=SUMMARYUPDATE
```

Ensure that you have refreshed the columns for the Event History database tables in Netcool/Impact prior to using mapped columns.

Configuring columns to display in the More Information panel

You can configure the columns that you want to display in the More Information panel.

About this task

The More Information panel can be started from within the Related Event Details portlet, when you click the hyperlink for either the Group Name or the Pivot Event, and the panel provides more details about the Group Name or the Pivot Event. The Event Analytics installation installs a default configuration of columns that display in the More Information panel, but you can change the configuration of columns that display. Complete the following steps to configure columns to display in the More Information panel.

Procedure

1. Export the current configuration into the properties file.
 - a. Log in to the server where IBM Tivoli Netcool/Impact is stored and running.
 - b. Go to the *<Impact install location>/bin* directory.
 - c. Enter the following command:


```
./nci_trigger NCI <UserID>/<password> NOI_DefaultValues_Export
FILENAME <Full Path to the file name>.properties
```

<UserID>
Specifies the ID of the Impact user.

<password>
Specifies the password of the Impact user.

<Full Path to the file name>
Specifies the directory where the file is stored.

2. Update the properties file with properties for columns you want to display in the More Information panel.

- For columns related to the Group Name in the More Information panel, the following properties are the default properties in the properties file. You can add, remove, and change the default properties.

```
reevent_num_groupinfo=3
reevent_groupinfo_1_column=PROFILE
reevent_groupinfo_2_column=EVENTIDENTITIES
reevent_groupinfo_3_column=INSTANCES
```

reevent_num_groupinfo=3

This property represents the number of group information columns to display. The default value is 3 columns. The value can be any number between 1 and 8, as eight columns are allowed.

reevent_groupinfo_1_column=PROFILE

Enter this property line item for each column. The variables in this property line item are *1* and *PROFILE*.

1 denotes that this column is your first column. This value can increment up to 8 per property line item, as eight columns are allowed.

PROFILE represents the column. The following eight columns are allowed.

PROFILE

Specifies the relationship profile, or strength of the group.

EVENTIDENTITIES

Specifies a comma-separated list that creates the event identity.

INSTANCES

Specifies the total number of group instances.

CONFIGNAME

Specifies the configuration name under which the group was created.

TOTALEVENTS

Specifies the total number of events within the group.

UNIQUEEVENTS

Specifies the total number of unique events within the group.

REVIEWED

Specifies the review status of a group by a user.

GROUPTTL

Specifies the number of seconds the group will stay active after the first event occurs.

- For columns related to the Pivot Event in the More Information panel, the following properties are the default properties in the properties file. You can add, remove, and change the default properties.

```
reevent_num_eventinfo=1
reevent_eventinfo_1_column=INSTANCES
```

reevent_num_eventinfo=1

This property represents the number of group information columns to display. The default value is 1 column. The value can be any number between 1 and 6, as six columns are allowed.

reevent_eventinfo_1_column=INSTANCES

Enter this property line item for each column. The variables in this property line item are *1* and *INSTANCES*.

1 denotes that this column is your first column. This value can increment up to 6 per property line item, as six columns are allowed.

INSTANCES represents the column. The following six columns are allowed:

INSTANCES

Specifies the total number of instances for the related event.

PROFILE

Specifies the relationship profile, or strength of the related event.

EVENTIDENTITY

Specifies the unique event identity for the related event.

EVENTIDENTITIES

Specifies a comma-separated list that creates the event identity.

CONFIGNAME

Specifies the configuration name under which the related event was created.

GROUPNAME

Specifies the group name under which the related event was created.

3. Run the following command to update the current configuration with your updated properties:

```
./nci_trigger NCI <UserID>/<password> NOI_DefaultValues_Configure  
FILENAME <Full Path to the file name>.properties
```

Customization of tables in the Event Analytics UI

You can use the `uiproviderconfig` files to customize the tables in the Event Analytics UI.

To customize how tables are displayed in the Event Analytics UI, you can update the `$IMPACT_HOME/uiproviderconfig/properties` and `$IMPACT_HOME/uiproviderconfig/translation` files that are specific to the policy or data type that you want to update.

If you want to update the `$IMPACT_HOME/uiproviderconfig/properties` and `$IMPACT_HOME/uiproviderconfig/translation` files, make a backup of the files before you do any updates.

Uninstalling Event Analytics

You can uninstall Event Analytics with the IBM Installation Manager GUI or console, or do a silent uninstall.

For more information about installing and using IBM Installation Manager, see the following IBM information center:

<http://pic.dhe.ibm.com/infocenter/install/v1r7/index.jsp>

Uninstalling Event Analytics

Use IBM Installation Manager to remove Event Analytics .

Before you begin

Take the following actions:

- Stop all Event Analytics processes.
- Back up any data or configuration files that you want to retain.
- To do a silent removal, create or record an Installation Manager response file.

Use the `-record response_file` option.

To create a response file without installing the product, use the `-skipInstall` option. For example:

1. Create or record a skipInstall:

```
IBMIM.exe -record C:\response_files\install_1.xml -skipInstall  
C:\Temp\skipInstall
```

2. To create an uninstall response file, using the created skipInstall:

```
IBMIM.exe -record C:\response_files\uninstall_1.xml -skipInstall  
C:\Temp\skipInstall
```

About this task

Note: To uninstall IBM Tivoli Netcool/OMNIbus Web GUI 8.1.0.0, you must first uninstall the IBM Netcool Operations Insight Extensions Web GUI 1.2.0.0 package, including the Event Analytics feature.

Procedure

GUI removal

1. To remove Event Analytics with the Installation Manager GUI:
 - a. Change to the `/eclipse` subdirectory of the Installation Manager installation directory.
 - b. Use the following command to start the Installation Manager wizard:
`./IBMIM`
 - c. In the main Installation Manager window, click **Uninstall**.
 - d. Select the offerings that you want to remove and follow the Installation Manager wizard instructions to complete the removal.

Console removal

2. To remove Event Analytics with the Installation Manager console:
 - a. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.
 - b. Use the following command to start the Installation Manager:
`./imcl -c`
 - c. From the Main Menu, select **Uninstall**.
 - d. Select the offerings that you want to remove and follow the Installation Manager instructions to complete the removal.

Silent removal

3. To silently remove Event Analytics:
 - a. Change to the `/eclipse/tools` subdirectory of the Installation Manager installation directory.

- b. Use the following command to start the Installation Manager:
- ```
./imcl -input response_file -silent -log /tmp/install_log.xml
-acceptLicense
```

Where *response\_file* is the directory path to the response file that defines the removal configuration

## Results

Installation Manager removes the files and directories that it installed.

## What to do next

Files that Installation Manager did not install, and configuration files that were changed, are left in place. Review these files and remove them or back them up as appropriate.

---

## Configure Analytics portlet

The Configure Analytics portlet contains a list of existing event configurations, or reports. Use this portlet to view, create, modify, delete, run, or stop event configurations.

**Note:** To access the Configure Analytics portlet, users must be assigned the `ncw_analytics_admin` role.

You can use the Configure Analytics portlet to determine whether an event recurs and when it recurs most frequently. For example, an event occurs frequently at 9 a.m. every Monday. Knowledge of the type of event and the patterns of recurrence can help to determine the actions that are required to reduce the number of events.

The Configure Analytics table displays the following columns of information for each event configuration.

**Name** Specifies the unique event configuration name.

### Event Identity

Specifies the database fields that identify a unique event in the database. Event seasonality runs on all events selected from the **Event Identity** drop-down list. If the **Event Identity** value is **Using Global Settings**, the Event Identity is set up in the configuration file.

### Seasonality Enabled

Specifies whether the event configuration has seasonality event analytics enabled. This column displays one of the following values:

- True: Seasonality analytics is enabled.
- False: Seasonality analytics is not enabled.

The column displays the value true if seasonality analytics is enabled.

### Related Event Enabled

Specifies whether the event configuration has related event analytics enabled. This column displays one of the following values:

- True: Related event analytics is enabled.
- False: Related event analytics is not enabled.

**Seasonality Status**

Specifies the status of the seasonality event configuration. The column can display one of the following status icons: Waiting, Running, Completed, or Error.

**Related Event Status**

Specifies the status of the related event configuration. The column can display one of the following status icons: Waiting, Running, Completed, or Error.

**Start Time**

Specifies the inclusive start date of historical data for the event configuration.

**End Time**

Specifies the inclusive end date of historical data for the event configuration.

**Seasonality Phase**

Specifies the phase of the seasonality event configuration run. In total, this column displays five phases during the run of the seasonality event configuration. For example, when the seasonality event configuration completion phase occurs, the value Completed displays in the column.

**Seasonality phase progress**

Displays the progress of the seasonality event phase, expressed in terms of percentage. For example, when the seasonality event configuration completion phases finishes, the value 100% displays in the column.

**Related Event Phase**

Specifies the phase of the related event configuration run. In total, this column displays five phases during the run of the related event configuration. For example, when the related event configuration completion phase occurs, the value Completed displays in the column.

**Related Event Phase Progress**

Displays the progress of the related event phase, expressed in terms of percentage. For example, when the related event configuration completion phases finishes, the value 100% displays in the column.

**Scheduled**

Indicates whether the event configuration run is scheduled to run every x number of days, weeks, or months. The value Yes displays in the column if the event configuration run is scheduled.

**Relationship profile**

The entry in this column specifies the strength of the relationship between the events in the event groups that are determined by the algorithm. One value is specified.

**Strong** Represents a high confidence level for relationships between events, but fewer events and fewer event groups. Your event groups might be missing weaker related events.

**Medium** Represents medium confidence level for relationships between events, average number of events and fewer event groups. Your event groups might be missing weakly related events.

**Weak** You see more events and more event groups but potentially more false positives.

**Important:** Netcool/Impact does not support Arabic or Hebrew. Event Analytics users who are working in Arabic or Hebrew see some untranslated English text.

## Setting the Impact data provider and other portlet preferences

If there are multiple connections with the Impact data provider, you must specify which Impact data provider to use.

### About this task

If a single connection with the Impact data provider exists, then that connection is used to compile the list of seasonal reports and display them in a table. If there are multiple connections with the Impact data provider, you must edit your portlet preferences to select one of the options.

### Procedure

1. To edit your portlet preferences, or as an administrator to edit the portlet defaults:

- To edit your portlet preferences, click **Page Actions**  > **Personalize Page** > **Widget** > **Personalize**.
- To edit the portlet defaults of all users, click **Page Actions**  > **Edit Page** > **Widget** > **Edit**.

The Configure Analytics dialog box is displayed.

2. Select a data provider from the **Data Provider** drop-down list.
3. In the **Bidi Settings** tab, specify the settings for the display of bidirectional text.

#### Component direction

Select the arrangement of items in the portlet, left-to-right, or right-to-left. The default setting uses the value that is defined for the page or the console. If the page and console both use the default setting, the locale of your browser determines the layout.

#### Text direction

Select the direction of text on the portlet. The default settings use the value that is defined for the page or the console. If the page and console both use the default setting, the locale of your browser determines the text direction. The Contextual Input setting displays text that you enter in the appropriate direction for your globalization settings.

4. To save your changes, complete the following steps.
  - a. Select **Save** in the Configure Analytics dialog box. The Configure Analytics dialog box is closed.
  - b. Select **Save**, which is in the upper right of the window.

## Viewing current analytics configurations

An Administrator can see the list of current analytics configurations and some basic information about the analytics (related events and seasonal events) related to those configurations.

### About this task

Event Analytics includes a default analytics configuration for you to run a basic configuration with default values. You can run, modify, or delete this analytics configuration. To view your analytics configurations, complete the following steps. This task assumes that you have logged into the Dashboard Application Services Hub as a user with the `ncw_analytics_admin` role.

### Procedure

1. Start the Configure Analytics portlet.
  - a. In the Dashboard Application Services Hub navigation menu, go to the **Insights** menu.
  - b. Select **Configure Analytics**.
2. In the Configure Analytics portlet, a table presents a list of analytics configurations that are already configured. Scroll down the list to view all analytics configurations. The table automatically refreshes every 60 seconds and displays information for select column headings.
  - To view configuration parameters for a specific analytics configuration, select a configuration and then select the **Modify Selected Configuration** icon.
  - To view progress of the latest action that is taken for an analytics configuration, look at the content that is displayed in the following columns:

#### Seasonality Status

Specifies the status of the seasonality event configuration. The column can display one of the following status icons: Waiting, Running, Completed, or Error.

#### Related Event Status

Specifies the status of the related event configuration. The column can display one of the following status icons: Waiting, Running, Completed, or Error.

#### Start Time

Specifies the inclusive start date of historical data for the event configuration.

#### End Time

Specifies the inclusive end date of historical data for the event configuration.

#### Seasonality Phase

Specifies the phase of the seasonality event configuration run. In total, this column displays five phases during the run of the seasonality event configuration. For example, when the seasonality event configuration completion phase occurs, the value **Completed** displays in the column.

#### Seasonality Phase Progress

Displays the progress of the seasonality event phase, expressed in terms of percentage. For example, when the seasonality event configuration completion phases finishes, the value **100%** displays in the column.

**Related Event Phase**

Specifies the phase of the related event configuration run. In total, this column displays five phases during the run of the related event configuration. For example, when the related event configuration completion phase occurs, the value `Completed` displays in the column.

**Related Event Phase Progress**

Displays the progress of the related event phase, expressed in terms of percentage. For example, when the related event configuration completion phases finishes, the value `100%` displays in the column.

- To view other details about the analytics configuration, look at the information displayed in other columns:

**Name**

Specifies the unique event configuration name.

**Event identity**

Specifies the database fields that identify a unique event in the database. Event seasonality runs on all events selected from the **Event Identity** drop-down list.

**Scheduled**

Advises whether the analytics configuration is scheduled to query the historical events database.

**Seasonality Enabled**

Specifies whether the event configuration has seasonality event analytics enabled. This column displays one of the following values:

- `True`: Seasonality analytics is enabled.
- `False`: Seasonality analytics is not enabled.

**Related Event Enabled**

Specifies whether the event configuration has related event analytics enabled. This column displays one of the following values:

- `True`: Related event analytics is enabled.
- `False`: Related event analytics is not enabled.

**Relationship Profile**

The entry in this column specifies the strength of the relationship between the events in the event groups that are determined by the algorithm. One value is specified.

**Strong** Represents a high confidence level for relationships between events, but fewer events and fewer event groups. Your event groups might be missing weaker related events.

**Medium** Represents medium confidence level for relationships between events, average number of events and fewer event groups. Your event groups might be missing weakly related events.

**Weak** You see more events and more event groups but potentially more false positives.

## Creating a new or modifying an existing analytics configuration

An Administrator can create a new analytics configuration or modify an existing analytics configuration. You choose the analytics type (related events, seasonal events, or both) you want to run during the create new analytics configuration operation.

### Before you begin

When you modify an existing analytics configuration, you cannot change the following parameter fields in the dialog box:

- **Name:**
- **Name**
- **Analytics Type**
- **Event identity**
- **Event identity:**
- **Seasonal event analytics**
- **Related event analytics**

### Procedure

1. Start the Configure Analytics portlet. See “Viewing current analytics configurations” on page 134.
2. Select the **Create New Configuration** icon to create a new analytics configuration, or highlight an existing analytics configuration and select the **Modify Selected Configuration** icon to modify an existing analytics configuration. The UI displays a dialog box that contains parameter fields for the new or existing analytics configuration.
3. Populate the parameter fields in the **General** tab of the dialog box with the details applicable to the analytics configuration.

**Name** Enter the name of the analytics configuration. The name should reflect the type of analytics configuration you are creating.

For example, TestSeasonality1 and TestRelatedEvents1 might be names you assign to analytics configurations for seasonality events and related events. The name for an analytics configuration must be unique and not contain certain invalid characters. The invalid character list is the list of characters listed in the *webgui\_home/etc/illegalChar.prop* file.

#### Analytics Type

Select **Seasonal event analytics**, **Related event analytics**, or both.

#### Event identity

From the drop-down list, select the database fields that identify a unique event in the database. Event seasonality runs on all events that are selected from the **Event Identity** drop-down list. For information about how to change the fields in the drop-down list, see “Changing the choice of fields for the Event Identity” on page 141.

#### Date Range

Select either **RelativeFixed date range** or **FixedRelative date range**

**Relative:** Enter the time frame that is to be included in the analytics configuration. The relative time frame is measured in **Months**, **Weeks**, or **Days**.

**Fixed:** The **Start date** and **End date** parameter fields are active. Enter an inclusive **Start date** and **End date** for the analytics configuration.

**Fixed date range:** The **Start date** and **End date** parameter fields are active. Enter an inclusive **Start date** and **End date** for the analytics configuration.

**Relative date range:** Enter the time frame that is to be included in the analytics configuration.

**Run every**

To schedule the analytics configuration to run at specific time intervals, enter how frequently the configuration is to run. When you enter a value greater than zero, the analytics configuration becomes a scheduled configuration.

**Note:** This option applies to the relative date range only. You cannot apply this option to the fixed date range.

**Filter** Detail any filters that are applicable to the analytics configuration. For example, enter Summary NOT LIKE '%maintenance%'.

**\* Select the analytics type you want to run**

Select **Seasonal event analytics**, **Related event analytics**, or both.

4. Populate the parameter fields in the **Related Events** tab of the dialog box with the details applicable to the analytics configuration.

**Relationship Profile**

Select the strength of the relationship between the events in an analytics configuration. If this value is set to Strong, there is more confidence in the result and less number of groups produced.

**Automatically deploy rules discovered by this configuration**

Select this option to automatically deploy rules that are discovered by this analytics configuration.

**Relationship Profile** Select the strength of the relationship between the events in an analytics configuration. If this value is set to Strong, there is more confidence in the result and less number of groups produced.

**Automatically deploy rules discovered by this configuration** Select this option if you want to automatically deploy rules that are discovered by this analytics configuration.

5. Populate the parameter field in the **Advanced** tab of the dialog box with the details applicable to the analytics configuration. You can use the defined event identities, select the **Override global event identity** to identify unique events in the database.

**Override global event identity**

Select this option to enable the **Event identity** drop-down list.

When the **Override global event identity** check box is selected, you cannot create a pattern from a configuration. However, you can deploy a related events group.

**Event identity**

From the **Event identity** drop-down list, select the database fields that identify a unique event in the database. Event seasonality runs on all events that are selected from the **Event Identity** drop-down list. For information about how to change the fields in the drop-down list, see “Changing the choice of fields for the Event Identity” on page 141.

6. Click either **Save** to save the report without running, or click **Save & Run** to save and run the report. You can also cancel the operation by clicking **Cancel**.

## Results

- If no errors are found by the system validation of the analytics configuration content, the new or updated analytics configuration and its parameters are displayed in the table.
- If errors are found by the system validation of the analytics configuration content, you are prevented from saving the configuration and you are asked to reset the invalid parameter.

## Manually running an unscheduled analytics configuration

An Administrator can manually run an unscheduled analytics configuration at any stage. You choose the analytics type (related events or seasonal events) you want to run during the run unscheduled analytics operation.

### Before you begin

The analytics configuration that you try to manually run cannot have a **Related Event Status** or **Seasonality Status** of Running. If you try to manually run an analytics configuration that is already running, the GUI displays a warning message.

**Note:** Sequentially running reports can take longer to complete than parallel running reports in previous releases.

### Procedure

1. Start the Configure Analytics portlet. See “Viewing current analytics configurations” on page 134.
2. Within the list of analytics configurations that are displayed, select one configuration.
3. From the toolbar, click the **Run Selected Configuration** icon. Some columns are updated for your selected analytics configuration.

The icon in the **Seasonality Status** or **Related Event Status** column changes to a time glass icon.

The text in the **Seasonality Phase** or **Related Event Phase** column changes to Waiting to Start.

The percentage in the **Seasonality Phase Progress** or **Related Event Phase Progress** column starts at 0% and changes to reflect the percentage complete for the phase.

## Results

The analytics configuration is put into the queue for the scheduler to run. As the analytics configuration is running, the following columns are updated to communicate the progress of the run:

- **Seasonality Status** or **Related Event Status**
- **Seasonality Phase** or **Related Event Phase**
- **Seasonality Phase Progress** or **Related Event Phase Progress**



## What to do next

If you want to stop an analytics configuration that is in Running status, from the toolbar click the **Stop Selected Configuration** icon.

## Stopping an analytics configuration

You can stop an analytics configuration that is running.

### About this task

If you create an analytics configuration and select to run the configuration, you might realize that some configuration values are incorrect while the configuration is still running. In this situation you can choose to stop the analytics configuration instead of deleting the configuration or waiting for the configuration run to complete. To stop a running analytics configuration, complete the following steps.

### Procedure

1. Start the related events configuration portlet, see “Viewing current analytics configurations” on page 134.
2. Within the list of analytics configurations that are displayed, select the running configuration.
3. From the toolbar, click the **Stop Selected Configuration** icon.

## Deleting an analytics configuration

Analytics configurations can be deleted individually, regardless of their status.

### Procedure

1. Start the Configure Analytics portlet, see “Viewing current analytics configurations” on page 134.
2. Select the name of the analytics configuration that you want to delete and from the toolbar click the **Delete Selected Configuration** icon.
3. Within the confirmation dialog that is displayed, select **OK**. If you attempt to delete an analytics configuration with one or more rules created for it, a text warning dialog box appears with the current rules status for that analytics configuration. The following example illustrates text that the warning dialog box can contain:

Configuration EventAnalytics\_Report\_1 contains the following rules:

Seasonality Rules:

0 watched rules, 1 active rules, 0 expired rules and 0 archived

Related Event Rules:

0 watched rules, 0 active rules, 0 expired rules and 0 archived

Delete the rules manually before deleting the configuration.

As the message indicates, manually delete the rule or rules associated with the specified analytics configuration before deleting the analytics configuration. In the example, the one active rule associated with the analytics configuration called EventAnalytics\_Report\_1 would need to be deleted first.

### Results

- The table of analytics configurations refreshes, and the deleted configuration no longer appears in the list of analytics configurations.

- Deleting the analytics configuration does not delete the related results if the results are in the **Deployed** or **Expired** state. However, deleting the analytics configuration does delete the related results that are in the **New** or **Archived** state.
- You are unable to reuse the name of a deleted analytics configuration until all related event groups that contain the name of the deleted configuration are deleted from the system.

## Changing the expiry time for related events groups

You can modify the expiry time for Watched or Active related events groups. When the expiry time is reached, the expired groups and related events display in the View Related Events portlet, within the Expired tab.

### About this task

Groups that contain an expired group or pattern continues to correlate. The system administrator should review the group and expired group or event.

By default the related events expiry time is 6 months. Complete the following steps to change the related events expiry time.

### Procedure

1. Log in to the Netcool/Impact UI.
2. Select the **Related Events project**.
3. Select the **Policies** tab.
4. Within the Policies tab, select to edit the **RE\_CONSTANTS** policy.
5. Within the RE\_CONSTANTS policy, change the value for the RE\_EXPIRE\_TIME constant. Enter your new value in months.
6. Save the policy.

### Results

This change takes effect only with newly discovered related event groups in the Watched or Active tabs.

### What to do next

If you want to configure the expiry time so that deployed groups never expire, change the value for the RE\_EXPIRE\_TIME constant to 0 and save the policy for this change to take effect. You do not need to restart the Impact Server.

If you want to enable the expiry time at any stage, set this variable back to a value greater than 0.

## Changing the choice of fields for the Event Identity

You can change which fields, from your event history database, are available for selection as the Event Identity.

### About this task

An Event Identity is a database field that identifies a unique event in the event history database. When you configure a related events configuration, you select database fields for the Event Identity from a drop-down list of available fields. Through configuration of an exception list within Netcool/Impact, you can change the fields available for selection in the drop-down list. Fields included in the exception list do not appear in the Configure Analytics portlet.

The Netcool/Impact design displays the following default fields in the Event Identity drop-down list

- Alert Group
- Alert Key
- Node
- Summary
- Identifier
- LOCALNODEALIAS
- LOCALPRIOBJ
- LOCALROOTOBJ
- LOCALSECOBJ
- REMOTENODEALIAS
- REMOTEPRIOBJ
- ROOTEROBJ
- ROTESECOBJ

If you have other database fields that are not in the exception list, these other fields also appear in the drop-down list. Complete the following steps to modify the exception list.

### Procedure

1. Log in to Netcool/Impact.
2. From the list of available projects, select the **RelatedEvents** project.
3. Select the **Policies** tab. Within this tab, select and edit the **RE\_CONSTANTS** policy.
4. Update the RE\_OBJECTSERVER\_EXCLUDEDFIELDS variable. Add or remove fields from the static array. Case sensitivity does not matter.
5. Save the policy.
6. Run the policy. If there is an error, check your syntax.

### Results

The changes occur when the policy is saved. No restart of Netcool/Impact is needed.

---

## View Seasonal Events portlet

The View Seasonal Events portlet contains a list of configurations, a list of seasonal events, and seasonal event details.

In addition to viewing the seasonal events, you can mark events as reviewed and identify the events that were reviewed by others.

The View Seasonal Events portlet displays the following default columns in the group table:

**Configuration**

Displays a list of the seasonal event configurations.

**Event Count**

Displays a count of the number of seasonal events for each seasonal event configuration.

**Node** Displays the managed entity from which the seasonal event originated. The managed entity could be a device or host name, service name, or other entity.

**Summary**

Displays the description of the seasonal event.

**Alert Group**

Displays the Alert Group to which the seasonal event belongs.

**Reviewed by**

Displays the list of user names of the users who reviewed the seasonal event.

**Confidence Level**

Displays icons and text based on the level of confidence that is associated with the seasonal event. The confidence level is displayed as high, medium, or low, indicating that an event has a high, medium, or low seasonality.

**Maximum Severity**

Displays the maximum severity of the events that contribute to the seasonality of the selected seasonal event.

**Rule Created**

Displays the name of the seasonal event rule that was created for the seasonal event.

**Related Events Count**

Displays a count of the number of related events for each seasonal event.

**First Occurrence**

Displays the date and time when the seasonal event first occurred. The time stamp is configurable by users and is displayed in the following format:

`YYYY-MM-DD HH:MM:SS`

For example:

`2012-10-12 09:52:58.0`

## Viewing a list of seasonal event configurations and events

You can view a list of the seasonal event configurations and seasonal events in the View Seasonal Events portlet.

### Before you begin

To access the View Seasonal Events portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To view a list of the seasonal event configurations and seasonal events, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. By default, the Seasonal Event configurations are listed in the **Configuration** table.
3. To view a list of seasonal events associated with the configurations, select one of the following options.
  - a. Select **All** to view of list of the seasonal events for all of the configurations.
  - b. Select a specific configuration to view a list of the seasonal events for that configuration.

The seasonal events are listed in the **Summary** table.

### Results

The seasonal event configurations and associated seasonal events are listed in the View Seasonal Events portlet.

## Reviewing a seasonal event

You can mark or unmark a seasonal event as reviewed.

### About this task

The **Reviewed by** column in the View Seasonal Events portlet displays the user name of the reviewer.

### Procedure

To update the review status of an event, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration or **ALL** in the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Mark as Reviewed** or **Unmark as Reviewed**.

Each seasonal event can be reviewed by multiple users. The reviewers are listed in the **Reviewed by** column.

### Results

The selected seasonal event is marked or unmarked as **Reviewed**. The **Reviewed by** column is updated to display the user name of the reviewer.

## Sorting columns in the View Seasonal Events portlet

You can sort the columns in the View Seasonal Events portlet to organize the displayed data.

### Before you begin

To access the View Seasonal Events portlet, users must be assigned the `ncw_analytics_admin` role.

### About this task

The rows in the View Seasonal Events portlet are sorted by the configuration name. You can change the order of the rows by using the columns to sort the data.

Sorted columns are denoted by an upwards-pointing arrow or downwards-pointing arrow in the column header, depending on whether the column is sorted in ascending or descending order.

### Procedure

To sort the rows by column, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. To sort single columns, complete the following steps.
  - a. To sort a column, click the column header once. The rows are sorted in ascending order.
  - b. To sort in descending order, click the column header again.
  - c. To unsort the column, click the column header a third time.
3. To sort multiple columns, complete the following steps.
  - a. Sort the first column as a single column.
  - b. Move the mouse pointer over the column header of the next column you want to sort. Two icons are displayed. One is a standard sorting icon and the other is a nested sorting icon. The nested sorting icon has a number that represents how many columns are sorted as a result of selecting the option. For example, if this is the second column that you want to sort the number 2 is displayed.
  - c. Click the nested sorting icon. The column is sorted with regard to the first sorted column.

**Tip:** When you move the mouse pointer over the nested sorting icon, the hover help indicates that it is a nested sorting option. For example, the hover help for the icon displays “Nested Sort - Click to sort Ascending”. The resulting sort order is ascending with regard to the previous columns on which a sorting order was placed.

- d. To reverse the order of the nested sort, click the nested sorting icon again. The order is reversed and the nested sorting icon changes to the remove sorting icon.
- e. To remove nested sorting from a column, move the mouse pointer over the column header and click the **Do not sort** icon.

**Note:** In any sortable column after nested sorting is selected, when you click the standard sorting icon, it becomes the only sorted column in the table and any existing sorting, including nested is removed.

## Results

Sorted columns are marked with an upwards-pointing arrow or a downwards-pointing arrow in the column header to indicate whether the column is sorted in ascending or descending order. The sorting is temporary and is not retained.

## Exporting all seasonal events for a specific configuration to Microsoft Excel

You can export all seasonal events for a specific configuration to a Microsoft Excel spreadsheet from a supported browser.

### Before you begin

You view seasonal events for one or more configurations in the **View Seasonal Events** portlet. To access the **View Seasonal Events** portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To export all seasonal events for a specific configuration to a Microsoft Excel spreadsheet, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration from the configuration table.
3. Click the **Export Seasonal Events** button in the toolbar. After a short time, the **Download export results** link displays.
4. Click the link to download and save the Microsoft Excel file.

## Results

The Microsoft Excel file contains a spreadsheet with the following tabs:

- **Report Summary:** This tab contains a summary report of the configuration that you selected.
- **Seasonal Events:** This tab contains the seasonal events for the configuration that you selected.
- **Export Comments:** This tab contains any comments relating to the export for informational purposes (for example, if the spreadsheet headers are truncated, or if the spreadsheet rows are truncated).

## Exporting selected seasonal events for a specific configuration to Microsoft Excel

You can export selected seasonal events for a specific configuration to a Microsoft Excel spreadsheet from a supported browser.

### Before you begin

You view seasonal events for one or more configurations in the **View Seasonal Events** portlet. To access the **View Seasonal Events** portlet, users must be assigned the `ncw_analytics_admin` role.

## Procedure

To export selected seasonal events for a specific configuration to a Microsoft Excel spreadsheet, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration from the configuration table.
3. Select multiple seasonal events by using the Ctrl key and select method. (You can also select multiple seasonal events by using the click and drag method.)
4. After selecting multiple seasonal events, right click on one of the selected seasonal events and select the **Export Selected Events** button in the toolbar. After a short time, the **Download export results** link displays.
5. Click the link to download and save the Microsoft Excel file.

## Results

The Microsoft Excel file contains a spreadsheet with the following tabs:

- **Report Summary:** This tab contains a summary report of the configuration that you selected.
- **Seasonal Events:** This tab contains the seasonal events for the configuration that you selected.
- **Export Comments:** This tab contains any comments relating to the export for informational purposes (for example, if the spreadsheet headers are truncated, or if the spreadsheet rows are truncated).

---

## Seasonal Event Rules

You can use seasonal event rules to apply an action to specific events.

You can choose to apply actions to a selected seasonal event, or to a seasonal event and some or all of its related events.

You can use seasonal event rules to apply actions to suppress and unsuppress an event, to modify or enrich an event, or to create an event if the selected event does not occur when expected.

### Creating a seasonal event rule

You can create a watched or deployed seasonal event rule from the View Seasonal Events portlet.

#### Before you begin

To access the View Seasonal Events portlet, users must be assigned the ncw\_analytics\_admin role.

## Procedure

To create a seasonal event rule in the View Seasonal Events portlet, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration or **ALL** in the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Create Rule**.



5. Input a unique rule name in the **Create Rule** window.
6. Input the following rule criteria for events and actions in the **Create Rule** window.
  - a. To apply rule actions to an event and time condition, see “Applying rule actions to an event and time condition.”
  - b. To apply actions when an event occurs, see “Applying actions when an event occurs” on page 148.
  - c. To Applying actions when an event does not occur, see “Applying actions when an event does not occur” on page 149.
7. To save the seasonal event rule, choose one of the following criteria.
  - a. Select **Watch** to monitor the rule's performance before it is deployed.
  - b. Select **Deploy** to activate the rule.

## Results

A seasonal event rule is created. To view a list of current seasonal event rules, open the **Seasonal Event Rules** portlet.

### Applying rule actions to an event and time condition

To create a seasonal event rule, you must specify the selected events or time conditions, or both in the Create Rule or Modify Existing Rule window.

### Before you begin

Create or modify an existing seasonal event rule. To create a seasonal event rule, see “Creating a seasonal event rule” on page 146. To modify an existing seasonal event rule, see “Modifying an existing seasonal event rule” on page 153.

### About this task

The seasonal event that is selected by default in the Event Selection pane is the seasonal event from which the Create Rule or Modify Existing Rule window was opened.

**Note:** A seasonal event rule suppresses events when they occur for a deployed related event group. The seasonal rule actions do not apply to the synthetic parent event that is created.

**Note:** You can create a seasonal event rule to unsuppress an event or alarm. This rule has no actions if there are no suppressed alarms.

## Procedure

To specify the selected events and time conditions, complete the following steps in the Create Rule window.

1. To select the all, or one or more of the events that are related to the seasonal event, complete the following steps.
  - a. To select all of the related events, select the **Select all related events** check box.
  - b. To edit or select one or more of the related events, click **Edit Selection**, select one or more related events.
2. To save the related eventselection, click **OK**
3. To select a time condition, complete the following steps.

- a. Select one of the following time condition filter conditions.
  - AND** Select **AND** to apply rule actions to each of the selected the time conditions.
  - OR** Select **OR** to apply rule actions to individual time conditions.
- b. Select **Minute of the Hour**, **Hour of the Day**, **Day of Week**, or **Day of Month** from the drop-down menu.
- c. Select **Is** or **Is Not** from the drop-down menu.
- d. Select the appropriate minute, hour, day, or date from the drop-down menu. You can select multiple values from this drop-down menu.

**Note:** High, medium, and low seasonality labels are applied to this time selection drop-down menu to indicate the seasonality of the events occurring at that time.

4. Click the add button to add another time condition.
5. To save the event selection and time conditions, choose one of the following criteria.
  - a. Select **Watch** to monitor the rule's performance before it is deployed.
  - b. Select **Deploy** to activate the rule.

## Results

The seasonal event rule conditions are applied to the selected events, time conditions, or both.

## Applying actions when an event occurs

You can apply specific actions to occur when an event occurs in a specific time window.

## Before you begin

Create or modify an existing seasonal event rule. To create a seasonal event rule, see “Creating a seasonal event rule” on page 146. To modify an existing seasonal event rule, see “Modifying an existing seasonal event rule” on page 153.

**Note:** To suppress or unsuppress events you must update the `noi_default_values` file. For more information about the `noi_default_values` file, see “Updating the NOI\_DefaultValues properties file to suppress and unsuppress events” on page 157.

## About this task

The events that are selected in the Event Selection pane are the events to which the action is applied when the event occurs in a specific time window. For more information about selecting events, see “Applying rule actions to an event and time condition” on page 147.

You can suppress events that do not require you to take any direct action, and unsuppress the events after a specified time period.

You can set a column value on an event occurrence and again set it again after a specified time period.

## Procedure

To specify the actions to apply when an event occurs, complete the following steps in the Actions When Event(s) Occurs in Specified Time Window(s) pane.

1. To suppress an event so that no action is taken when it occurs, complete the following steps.
  - a. Select the **Suppress event(s)** check box.
  - b. (Optional) To select a column value, see step 3 below.
2. To unsuppress an event after an action occurs, complete the following steps.
  - a. To select the time after the action occurs to unsuppress the event, select a number from the **Perform Action(s) After** list, or type an entry in the field. Select **Seconds**, **Minutes**, or **Hours** from the **Perform Action(s) After** drop-down list.
  - b. Select the **Unsuppress event(s)** check box.
  - c. (Optional) To select a column value, see step 4 below.
3. To set the column value after an action occurs, complete the following steps.
  - a. Select the **Set Column Values** check box and click the **Set Column Value** button for **Perform Action(s) on Event Occurrence**.
  - b. In the **Set Column Value** page, input values for the ObjectServer columns.
  - c. To save the column values, click **Ok**.
4. To reset the column value after a specified time period, complete the following steps.
  - a. To specify a time period, select a number from the **Perform Action(s) After** list, or type an entry in the field. Select **Seconds**, **Minutes**, or **Hours** from the **Perform Action(s) After** drop-down list.
  - b. Select the **Set Column Values** check box and click the **Set Column Value** button for **Perform Action(s) After**.
  - c. In the **Set Column Value** page, input values for the ObjectServer columns.
  - d. To save the column values, click **Ok**.
5. To save the seasonal event rule, choose one of the following options.
  - a. Select **Watch** to monitor the rule's performance before it is deployed.
  - b. Select **Deploy** to activate the rule.

## Results

The action to be applied to a rule that occurs in a specific time window is saved.

### Applying actions when an event does not occur

You can apply specific actions to occur when an event does not occur in a specific time window.

### Before you begin

Create or modify an existing seasonal event rule. To create a seasonal event rule, see “Creating a seasonal event rule” on page 146. To modify an existing seasonal event rule, see “Modifying an existing seasonal event rule” on page 153.

### About this task

The events that are selected in the Event Selection pane are the events to which the action is applied if the event does not occur in a specific time window. For more

information about selecting events, see “Applying rule actions to an event and time condition” on page 147.

## Procedure

To specify the actions to apply when an event does not occur, complete the following steps in the Actions When Event(s) Does Not Occur in Specified Time Window(s) pane.

1. To select the time after which the event does not occur to apply the action, complete the following steps.
  - a. Select a number from the **Perform Action(s) After** list, or type an entry in the field.
  - b. Select **Seconds**, **Minutes**, or **Hours** from the **Perform Action(s) After** drop-down list.
2. To create a synthetic event on a non-occurrence, select the **Create event** check box and click **Create event**.
3. To define the event, complete the fields in the new Create Event window.
4. To save the synthetic event, click **Ok**.
5. To save the seasonal event rule, choose one of the following options.
  - a. Select **Watch** to monitor the rule's performance before it is deployed.
  - b. Select **Deploy** to activate the rule.

## Results

The action to be applied to a rule that does not occur in a specific time window is saved.

## Seasonal event rule states

Seasonal event rules are grouped by state in the Seasonal Event Rules portlet.

### Seasonal event rule states

Seasonal event rules are grouped in the following states.

#### Watched

A watched seasonal event rule is not active.

You can watch a seasonal event rule to monitor how the rule performs before you decide whether to deploy it.

Watched seasonal event rules take no actions on events. It is used to collect statistics for rule matches for incoming events.

**Active** A deployed seasonal event rule is active. Active seasonal event rules take defined actions on live events.

#### Expired

An expired seasonal event rule remains active. If triggered, the seasonal event rule takes defined actions on live events. The default expiry time is **6 MONTHS**. To ensure that seasonal event rules are valid, regularly review the state and performance of the rules. You can customize the expiry time of a seasonal event rule. For more information, see “Modifying the default seasonal event rule expiry time” on page 151.

## Archived

An archived seasonal event rule is not active. You can choose to archive a watched, active, or expired seasonal event rule. To delete a seasonal event rule, it must first be archived.

For more information about changing the state of a seasonal event rule, see “Modifying a seasonal event rule state” on page 154.

## Modifying the default seasonal event rule expiry time

You can change the default seasonal event rules expiry time to a specific time or choose no expiry time to ensure that a seasonal event rule does not expire.

### About this task

To ensure that seasonal event rules are valid, you should regularly review and update the state of the rules.

### Procedure

To modify or remove the default seasonal event rules expiry time, complete the following steps.

1. To generate a properties file from the command line interface, use the following command:

```
./nci_trigger SERVER <UserID>/<Password> NOI_DefaultValues_Export FILENAME
directory/filename
```

Where

*SERVER*

The server where Event Analytics is installed.

*<UserID>*

The user name of the Event Analytics user.

*<Password>*

The password of the Event Analytics user.

*directory*

The directory where the file is stored.

*filename*

The name of the properties file.

For example:

```
./nci_trigger NCI impactadmin/impact NOI_DefaultValues_Export FILENAME
/space/noi_default_values
```

2. To modify the default seasonal event rules expiry time, edit the default values of the following parameters.

**seasonality.rules.expiration.time.value=6**

The number of days, hours, or months after which the seasonal event rule expires. The default value is 6.

**seasonality.rules.expiration.time.unit=MONTH**

The seasonal event rules expiry time frequency. The default frequency is *MONTH*. The following time units are supported:

- HOUR
- DAY

- MONTH
3. To import the modified properties file into IBM Tivoli Netcool/Impact, use the following command:
 

```
./nci_trigger SERVER <UserID>/<Password> NOI_DefaultValues_Configure FILENAME
directory/filename
```

For example:

```
./nci_trigger NCI impactadmin/impact NOI_DefaultValues_Configure FILENAME
/space/noi_default_values
```

## Results

The default seasonal event rules expiry time is modified.

## Viewing performance statistics for seasonal event rules

You can view performance statistics for seasonal event rules in the Seasonal Event Rules portlet, within the Watched, Active, or Expired tabs of the group table.

### Columns in the group table

The group table in the View Seasonal Events portlet displays the seasonal event rules that you have created. The left-side of the group table has these columns:

**Configuration:** Displays the list of configuration names for which a seasonal event rule has been created.

**Rule Count:** Displays the number of seasonal event rules created for each particular configuration. This number also indicates the total number of seasonal event rules created for all configurations under the **All** item.

**Rule Name:** Displays the name of the seasonal event rule.

**Last Run:** Displays the date and time when the seasonal event rule was last executed. If the column is blank, the seasonal event rule has not been executed.

**Deployed:** Displays the date and time when the seasonal event rule was deployed. The term deployed means that the seasonal event rule is available for use, is actively accumulating rule statistics, and any actions applied to the rules are being performed.

**Note:** For the Last Run and Deployed columns, the date is expressed as *month, day, year*. Likewise, the time is expressed as *hours:, minutes:, seconds*. The time also indicates whether AM or PM. For example: Apr 13, 2015 4:45:17 PM.

### Performance statistics in the group table

The performance statistics are displayed in the following columns of the group table in the Watched, Active, or Expired tabs in the Seasonal Event Rules portlet.

**Suppressed Events:** Displays the total number of events that the seasonal event rule suppressed since the rule was deployed.

**Unsuppressed Events:** Displays the total number of events that the seasonal event rule unsuppressed since the rule was deployed.

**Enriched/Modified Events:** Displays the total number of events that the seasonal event rule enriched or modified since the rule was deployed.

**Generated Events on Non-occurrence:** Displays the total number of events that the seasonal event rule generated since the rule was deployed for events that do not meet the event selection criteria (that is, for those matching events that fall outside of the event selections condition for the rule).

## Reset performance statistics

You can reset performance statistics to zero for a group in the Watched, Active, or Expired tabs. To reset performance statistics, right-click on the seasonal event rule name (from the Rule Name column) and from the menu select **Reset performance statistics**. A message displays indicating that the operation will reset statistics data for the selected seasonal event rule. The message also indicates that you will not be able to retrieve this data. Click OK to continue with the operation or Cancel to stop the operation. A success message displays after you select OK.

Resetting performance statistics to zero for a seasonal event rule also causes the following columns to be cleared: Last Run and Deployed. Note that performance statistics are not collected for the Archived tab. When a rule is moved between states, the performance statistics are reset. Every time an action is triggered by the rule the performance statistics increase.

## Modifying an existing seasonal event rule

You can modify an existing seasonal event rule to update or change the event selection criteria or actions.

### Before you begin

To access the **Seasonal Event Rules** portlet, users must be assigned the ncw\_analytics\_admin role.

### Procedure

1. Open the Seasonal Event Rules portlet.  
The **Seasonal Event Rules** portlet lists the seasonal event rules configuration in the table on the left side, and the seasonal event rules are listed in the table in the right side.
2. Select the rule that you want to modify from the rule table.
3. Right click and select **Edit Rule**.
4. Modify the event selection criteria or actions in the **Modify Existing Rule** window.
5. To save the seasonal event rule, choose one of the following criteria.
  - a. Select **Watch** to monitor the rule's performance before it is deployed.
  - b. Select **Deploy** to activate the rule.

### Results

The seasonal event rule is modified. To view a list of current seasonal event rules, open the **Seasonal Event Rules** portlet.

## Viewing seasonal event rules grouped by state

You can view seasonal event rules grouped by state in the **Seasonal Event Rules** portlet.

### Before you begin

To access the **Seasonal Event Rules** portlet, users must be assigned the ncw\_analytics\_admin role.

## Procedure

To view seasonal event rules grouped by state, complete the following steps.

1. Open the Seasonal Event Rules portlet.  
The **Seasonal Event Rules** portlet lists the seasonal event rules configuration in the table on the left side, and the seasonal event rules are listed in the table in the right side.
2. Select the seasonal event rule state that you want to view from the status tabs.  
The seasonal event rules are stored in tabs that relate to their status. For example, to view a list of the active seasonal event rules configurations and rules, select the **Active** tab.

## Results

The seasonal event rules configurations and rules for the chosen status are listed in the **Seasonal Event Rules** portlet.

## Modifying a seasonal event rule state

You can change the state of a seasonal event rule to watched, active, or archived from the Seasonal Event Rules portlet.

### Before you begin

To access the **Seasonal Event Rules** portlet, users must be assigned the `ncw_analytics_admin` role.

### About this task

The seasonal event rules are stored in tabs that relate to their state. The total number of rules is displayed on the tabs. For example, when you **Archive** a **Watched** rule, the rule moves from the **Watched** tab to the **Archived** tab in the Seasonal Event Rules portlet and the rules total is updated.

Performance statistics about the rule are logged. You can use performance statistics to verify that a deployed rule is being triggered and that a monitored rule is collecting statistics for rule matches for incoming events. Performance statistics are reset when you change the state of a seasonal event rule.

## Procedure

To change the state of a seasonal event rule in the Seasonal Event Rules portlet, complete the following steps.

1. Open the Seasonal Event Rules portlet.  
The **Seasonal Event Rules** portlet lists the seasonal event rules configuration in the table on the left side, and the seasonal event rules are listed in the table in the right side.
2. To change the state of seasonal event rule, complete one of the following actions:
  - a. To change the state of a watched seasonal event rule, select the **Watched** tab. Select a rule from the rule table. To change the state of the rule right-click the rule and select **Deploy** or **Archive**.



- b. To change the state of an active seasonal event rule, select the **Active** tab. Select a rule from the rule table. To change the state of the rule right-click the rule and select **Watch** or **Archive**.
- c. To change the state of an expired seasonal event rule, select the **Expired** tab. Select a rule from the rule table. To change the state of the rule right-click the rule and select **Validate**, **Watch**, or **Archive**.
- d. To change the state of an archived seasonal event rule, select the **Archived** tab. Select a rule from the rule table. To change the state of the rule right-click the rule and select **Watch** or **Deploy**.

## Results

The seasonal event rule state is changed from its current state to its new state. The rule totals are updated to reflect the new seasonal event rule state.

## Applying rule actions to a list of events

You can apply defined actions to a list of events while you create a seasonal event rule.

### Before you begin

To access the View Seasonal Events portlet, users must be assigned the `ncw_analytics_admin` role.

### About this task

One of the events in the list on the Related Event Selection window is the seasonal event from which you launched the Create Rule dialog box. When the rule you created is fired, the rule is fired on the seasonal event and the related events that you selected. Because the rule is fired on the seasonal event, it is not possible for you to deselect this seasonal event from the list of related events displayed in the Related Event Selection window.

### Procedure

To select a list of events to which the defined action applies, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration or **ALL** in the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Create Rule**.
5. To choose all related events:
  - a. In the **Event Selection** pane of the **Create Rule** page, click the **Select all related events** checkbox.
6. Or, to choose one or more related events:
  - a. In the **Event Selection** pane of the **Create Rule** page, click the **Edit Selection...** control button. The Related Event Selection window displays. Note that the seasonal event from which you launched the Create Rule dialog box has a check mark that you cannot deselect.
  - b. Select one or more related events from the list displayed in the Related Event Selection window.
  - c. Click **OK**.

7. To save your changes, choose one of the following options:
  - a. Select **Watch** to monitor the rule's performance before it is deployed.
  - b. Select **Deploy** to activate the rule.

## Results

The updated seasonal event rule is saved and the defined actions are applied to the selected related events.

## Setting the column value for an event

You can set the column value for an event when you set the actions for a rule.

### Before you begin

To access the View Seasonal Events portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To set the column value, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration or **ALL** in the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Create Rule**.
5. In the **Actions When Event(s) Occurs in Specific Time Window(s)** pane, select from the following options.
  - a. To set the column value to suppress an event, select the **Set Column Values** check box and click the **Set Column Value** button for **Perform Action(s) on Event Occurrence**.
  - b. To set the column value to unsuppress an event, select the **Set Column Values** check box and click the **Set Column Value** button for **Perform Action(s) After**.
6. In the **Set Column Value** page, input values for the ObjectServer columns.
  - a. You can add or remove columns by using the **plus** and **minus** buttons.
7. To save the column values, click **Ok**.
8. To save the seasonal event rule, choose one of the following options.
  - a. Select **Watch** to monitor the rule's performance before it is deployed.
  - b. Select **Deploy** to activate the rule.

## Results

The seasonal event rule that modifies the column values is saved.

## Updating the NOI\_DefaultValues properties file to suppress and unsuppress events

You must add details about suppressing and unsuppressing events to the NOI\_DefaultValues properties file to suppress and unsuppress events.

### About this task

To add details about suppressing and unsuppressing events, you must modify the NOI\_DefaultValues properties file in the *<Impact\_install\_location>/bin* directory.

### Procedure

1. Log in to the server where IBM Tivoli Netcool/Impact is stored and running.
2. Go to the *<Impact\_install\_location>/bin* directory.
3. Enter the following command: `./nci_trigger <server_name>  
<UserID>/<password> NOI_DefaultValues_Export FILENAME <Full Path to the  
file name><name_of_propsfile>`

*<server\_name>*

Specifies the name of the server where Netcool/Impact is stored and running.

*<UserID>*

Specifies the ID of the Netcool/Impact user.

*<password>*

Specifies the password of the Netcool/Impact user.

*<Full Path to the file name><name\_of\_propsfile>*

Specifies the directory where the NOI\_DefaultValues properties file resides. The directory specification includes the name of the NOI\_DefaultValues properties file.

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Configure
/tmp/bin/noi_def_values.props
```

4. Add the following lines of text to the NOI\_DefaultValues properties file:

```
seasonality.supressevent.column.name=SuppressEsc1
seasonality.supressevent.column.type=NUMERIC
seasonality.supressevent.column.value=4
seasonality.unsupressevent.column.name=SuppressEsc1
seasonality.unsupressevent.column.type=NUMERIC
seasonality.unsupressevent.column.value=0
```

5. To update the NOI\_DefaultValues properties file, run the following command:

```
./nci_trigger <server_name> <UserID>/<password> NOI_DefaultValues_Configure
FILENAME <Full Path to the file name><name_of_propsfile>
```

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Configure
FILENAME /tmp/bin/noi_def_values.props
```

---

## Seasonal Event Graphs

The seasonal event graphs display bar charts and confidence level event thresholds for seasonal events.

The **Seasonal Event Graphs** portlet consists of four charts:

**Minute of the hour**

The minute or minutes of the hour that the event occurs.

**Hour of the day**

The hour or hours of the day that the event occurs.

**Day of the week**

The day or days of the week that the event occurs.

**Day of the month**

The date or dates of the month that the event occurs.

The confidence level of the data in the charts is displayed in three ways:

1. The overall distribution score of each chart is displayed as high (red), medium (orange), or low (green) seasonality at the top of each chart.
2. The degree of deviation of the events is indicated by the high (red) and medium (orange) seasonality threshold lines on the charts.
3. The maximum confidence level of each bar is displayed as high (red), medium (orange), or low (green).

The default confidence level thresholds are as follows:

- High: 99-100%
- Medium: 95-99%
- Low: 0-95%

To modify the default confidence level thresholds of the charts, see “Editing confidence thresholds of Seasonal Event Graphs” on page 161.

### Understanding graphs

The four seasonal event graphs illustrate event seasonality. The graphs depict independent observations. For example, if the **Hour of the day** graph indicates a high confidence level for 5 p.m., and the **Minute of the hour** graph indicates a high confidence level for minute 35, it does not necessarily mean that the events all occur at 5:35 p.m. The 5 p.m. value can contain other minute values.

**Note:** In some instances, **Minute of the hour** is indicated as having a high confidence level but the overall confidence level of seasonality is low. This is due to the high-level statistic that does not include minute of the hour due to poll cycle of monitors.

**Note:** In some instances, the overall confidence level of a chart is indicated as high although none of the bars in the graph are in the red zone. An example of this is a system failure due to high load and peak times, with no failure outside of these times.

The seasonal event graphs **Count** refers to the number of observations that are recorded in each graph. There is a maximum of one observation for each minute, hour, day, and date range. Therefore, the count for each of the graphs can differ. For example, if an event occurs at the following times:

10:31 a.m., 1 June 2013

10:31 a.m., 2 June 2013

10:35 a.m., 2 June 2013

There is a count of two observations for 10 a.m., two observations for minute 31, and one observation for minute 35.

## Viewing seasonal event graphs for a seasonal event

You can view seasonal event graphs for the seasonal events that are displayed in the View Seasonal Events portlet.

### Before you begin

To access the View Seasonal Events portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To view seasonal event graphs for a seasonal event, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration or **ALL** in the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Show Seasonal Event Graphs**.

### Results

The Seasonal Event Graphs portlet displays the bar charts and confidence levels for the selected seasonal event. For more information about charts and threshold levels, see the “Seasonal Event Graphs” on page 158 topic.

## Viewing historical events from seasonality graphs

You can view a list of historical events from seasonality graphs.

### Before you begin

To access the View Seasonal Events portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To view a list of historical events from seasonality graphs, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration or **ALL** in the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Show Seasonal Event Graphs**.
5. In the Seasonal Event Graphs tab, you can choose to view all of the historical events for a seasonal event, or filter the historical events by selecting bars in a graph.
  - a. To view all of the historical events for a seasonal event, select **Show Historical Events** in the **Actions** drop-down list.

- b. To view the historical events for specific times, hold down the **Ctrl** key and click the specific bars in the graphs. Select **Show Historical Events for Selected Bars** in the **Actions** drop-down list.

Multiple bars that are selected from one chart are filtered by the **OR** condition. For example, if you select the bars for 9am or 5pm in the **Hour of the Day** graph, all of the events that occurred between 9am and 10am and all events that occurred between 5pm and 6pm are displayed in the Historical Event portlet.

Multiple bar that are selected from more than one graph are filtered by the **AND** condition. For example, if you select the bar for 9am in the **Hour of the Day** graph and Monday in the **Day of the Week** graph, all of the events that occurred between 9am and 10am on Mondays are displayed in the Historical Event portlet.

## Results

The historical events are listed in the **Historical Event** portlet.

## Exporting seasonal event graphs for a specified seasonal event to Microsoft Excel

You can export seasonal event graphs for a specified seasonal event to a Microsoft Excel spreadsheet from a supported browser.

### Before you begin

You view seasonal event graphs for the seasonal events that are displayed in the **View Seasonal Events** portlet. To access the **View Seasonal Events** portlet, users must be assigned the `ncw_analytics_admin` role.

### About this task

In addition to exporting seasonal event graphs to a Microsoft Excel spreadsheet, you also export the historical event data and seasonal event data and confidence levels for the seasonal event that you selected. Currently, there is no way to export only the seasonal event graphs.

### Procedure

To export seasonal event graphs for a specified seasonal event to a Microsoft Excel spreadsheet, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration from the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Show Seasonal Event Graphs**.
5. From the **Actions** menu, select **Export Seasonal Event Graphs**. After a short time, the **Download export results** link displays.
6. Click the link to download and save the Microsoft Excel file.

## Results

The Microsoft Excel file contains a spreadsheet with the following tabs:

- **Seasonal Data:** This tab contains the seasonal event data and confidence levels for the seasonal event that you selected.

- **Seasonality Charts:** This tab contains the seasonal event graphs for the seasonal event that you selected.
- **Historical Events:** This tab contains the historical event data for the seasonal event that you selected.
- **Export Comments:** This tab contains any comments relating to the export for informational purposes (for example, if the spreadsheet headers are truncated, or if the spreadsheet rows are truncated).

For more information about charts and threshold levels, see the “Seasonal Event Graphs” on page 158 topic.

## Editing confidence thresholds of Seasonal Event Graphs

You can edit the default confidence level thresholds of the Seasonal Event Graphs.

### About this task

The confidence level of the data in the charts is displayed in two ways:

1. The overall distribution score of each chart is displayed as high (red), medium (orange), or low (green) seasonality at the top of each chart.
2. The degree of deviation of the events is indicated by the high (red) and medium (orange) seasonality threshold lines on the charts.
3. The maximum confidence level of each bar is displayed as high (red), medium (orange), or low (green).

The default confidence level thresholds are as follows:

- High: 99-100%
- Medium: 95-99%
- Low: 0-95%

To modify the default confidence level thresholds of the charts, see “Editing confidence thresholds of Seasonal Event Graphs.”

### Procedure

To edit the default confidence level threshold, complete the following steps:

1. To generate a properties file from the command-line interface, use the following command:

```
nci_trigger server <UserID>/<password> NOI_DefaultValues_Export
FILENAME directory/filename
```

where

#### **SERVER**

The server where Event Analytics is installed.

#### **<UserID>**

The user name of the Event Analytics user.

#### **<password>**

The password of the Event Analytics user.

#### **directory**

The directory where the file is stored.

#### **filename**

The name of the properties file.

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Export
FILENAME
/tmp/seasonality.props
```

2. To modify the confidence level thresholds, edit the default values of the following parameters:

- level\_threshold\_high = 99
- level\_threshold\_medium = 95
- level\_threshold\_low = 0

**Note:** Other property values are overwritten by the generated properties file. You might need to update other property values. For a full list of properties, see “Generated properties file” on page 206.

3. To import the modified properties file into Netcool/Impact, use the following command:

```
nci_trigger SERVER <UserID>/<password> NOI_DefaultValues_Configure
FILENAME
directory/filename
```

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Configure
FILENAME
/tmp/seasonality.props
```

---

## Historical events

You can view a list of historical events for one or more seasonal events in the table that displays in the **Historical Event** portlet. You can also export the data associated with the list of historical events for the associated seasonal events to a spreadsheet.

The **Historical Event** portlet displays a table with the following default columns:

### Summary

Displays the description of the historical event.

**Node** Displays the managed entity from which the historical event originated. The managed entity could be a device or host name, service name, or other entity.

### Severity

Displays the severity of the historical event. The following list identifies the possible values that can display in the **Severity** column:

- 0: Clear
- 1: Indeterminate
- 2: Warning
- 3: Minor
- 4: Major
- 5: Critical

### FirstOccurrence

Displays the date and time in which the historical event was created or first occurred. The date is expressed as *month, day, year*. The time is expressed as *hours:, minutes:, seconds*. The time also indicates whether AM or PM. For example: Apr 13, 2015 4:45:17 PM.



**LastOccurrence**

Displays the date and time in which the historical event was last updated. The date is expressed as *month, day, year*. The time is expressed as *hours:*, *minutes:*, *seconds*. The time also indicates whether AM or PM. For example: Jun 2, 2015 5:54:49 PM.

**Acknowledged**

Indicates whether the historical event has been acknowledged:

- 0: No
- 1: Yes

The historical event can be acknowledged manually or automatically by setting up a correlation rule.

**Tally** Displays an automatically maintained count of the number of historical events associated with a seasonal event.

## Viewing historical events for a seasonal event

You can view a list of historical events for a seasonal event in the table that displays in the **Historical Event** portlet.

### Before you begin

You view seasonal events for which you want a list of historical events in the **View Seasonal Events** portlet. To access the **View Seasonal Events** portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To view a list of historical events for a seasonal event, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration or **ALL** from the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Show Historical Events**.

### Results

The historical events are listed in the table that displays in the **Historical Event** portlet.

## Exporting historical event data

You can export historical event data to a spreadsheet from Firefox or Internet Explorer.

### Before you begin

You first view seasonal events for which you want a list of historical events in the **View Seasonal Events** portlet. To access the **View Seasonal Events** portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To export historical event data, complete the following steps.

1. Open the **View Seasonal Events** portlet.

2. Select a specific configuration or **ALL** from the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Show Historical Events**. The historical events are listed in the table that displays in the **Historical Event** portlet.
5. Select one or more historical events from the table that displays in the **Historical Event** portlet.
6. To copy the selected historical events:
  - a. In Firefox, to copy the data from the displayed clipboard click **Ctrl+C** followed by **Enter**.
  - b. In Internet Explorer, to copy the data from the displayed clipboard right-click on the selected historical event and select **Copy Ctrl+C** from the drop down menu.
7. Paste the historical event data to your spreadsheet.

## Exporting historical event data for a specified seasonal event to Microsoft Excel

You can export historical event data for a specified seasonal event to a Microsoft Excel spreadsheet from a supported browser.

### Before you begin

You first view seasonal events for which you want a list of historical events in the **View Seasonal Events** portlet. To access the **View Seasonal Events** portlet, users must be assigned the `ncw_analytics_admin` role.

### About this task

In addition to exporting historical event data to a Microsoft Excel spreadsheet, you also export the seasonal event charts and seasonal event data and confidence levels for the seasonal event that you selected. Currently, there is no way to export only the historical event data.

### Procedure

To export historical event data to a Microsoft Excel spreadsheet, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration from the configuration table.
3. Select a seasonal event from the events table.
4. Right-click the seasonal event and select **Show Seasonal Event Graphs**.
5. From the **Actions** menu, select **Export Seasonal Event Graphs**. After a short time, the **Download export results** link displays.
6. Click the link to download and save the Microsoft Excel file.

### Results

The Microsoft Excel file contains a spreadsheet with the following tabs:

- **Seasonal Data:** This tab contains the seasonal event data and confidence levels for the seasonal event that you selected.
- **Seasonality Charts:** This tab contains the seasonal event graphs for the seasonal event that you selected.

- **Historical Events:** This tab contains the historical event data for the seasonal event that you selected.
- **Export Comments:** This tab contains any comments relating to the export for informational purposes (for example, if the spreadsheet headers are truncated, or if the spreadsheet rows are truncated).

---

## Related events

Use the related events function to identify and show events that are historically related and to deploy chosen correlation rules, which are derived from related events configurations. You can create a pattern based on a related events group. The pattern applies the events in the group, which are specific to a resource, to any resource.

The related events function is accessible through three portlets.

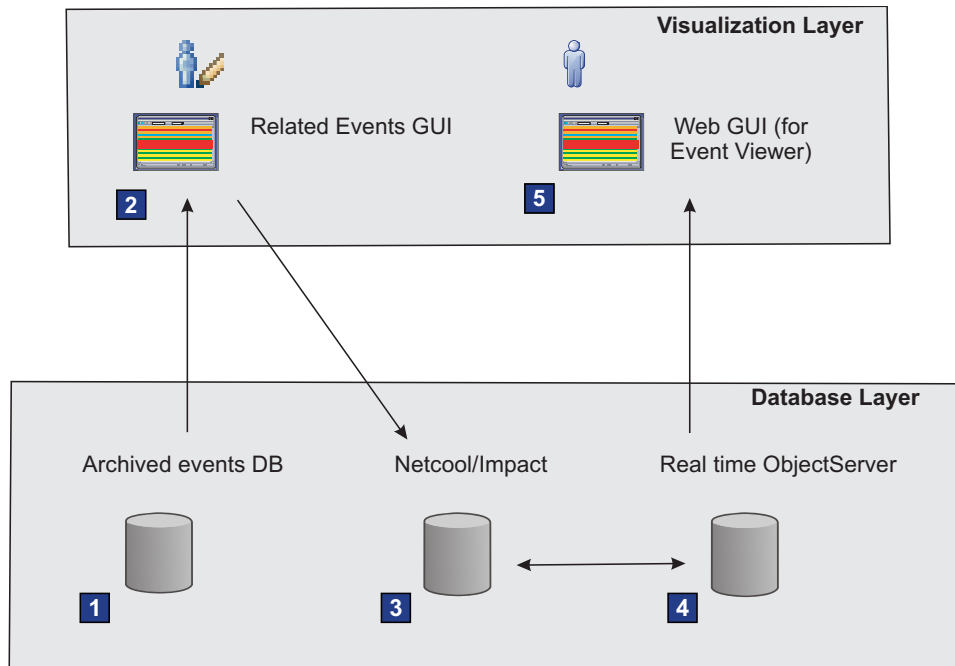
- **The Configure Analytics portlet.** Use this portlet to create, modify, run, and delete related events configurations.
- **The View Related Events portlet.** Use this portlet to review the events and event groups that are derived from a related events configuration and to deploy correlation rules.
- **The Related Event Details portlet.** Use this portlet to access more detail about an event or an event group.

To access the View Related Events portlet, users must be assigned the `ncw_analytics_admin` role.

The related events function uses an algorithm with the event database columns you select to determine relationships between events.

Related events find signatures and patterns that occur together in the historic event stream. This discovery allows subject matter experts to easily review the detected signatures and derive correlation rules from related events configurations, without having to write correlation triggers or policies.

This diagram shows the relationship between the components for the related events functions.



- 1** Netcool/OMNibus continually archives real-time events to an archived events database.
- 2** The Administrator creates a related events configuration. The configuration identifies and groups related events from the archive database and derives correlation rules. The Administrator watches and deploys the rules or configures the configuration to automatically deploy the rules.
- 3** Netcool/Impact policies are automatically created from the deployed correlation rules.
- 4** Netcool/Impact policies take action on real time events and group child events under a synthetic parent event.
- 5** The Operator is presented with a reduced number of events in the Event Viewer.

Figure 8. Related events architecture overview

## Work with related events

Use the View Related Events portlet to work with related events and related event groups that are derived from your related events configuration.

To access the View Related Events portlet, users must be assigned the `ncw_analytics_admin` role.

Within the View Related Events portlet, in the New, Watched, Active, Expired, or Archived tabs, three tables display information about your related events.

**Configuration table.** Displays the All container. Expand this container to see list of related event configurations.

**Group table.** Displays all related event groups or displays the related event groups for a selected configuration.

**Event table.** Displays all related events or displays the related events for a selected configuration or a selected group.

In a table you can right-click on a group, a configuration, or the All container and a menu is displayed. The menu lists some of the following actions for you to select.

**Watch** For more information about this action, see “Watching a correlation rule” on page 181.

**Deploy** For more information about this action, see “Deploying a correlation rule” on page 182.

**Archive** For more information about this action, see “Archiving related events” on page 177.

**Delete** This action is only available from within the Archived tab. If you want to delete event groups from the system, choose this action.

**Reset performance statistics** For more information about this action, see “Viewing performance statistics for a correlation rule” on page 183.

**New** This action is only available from within the Archived tab. If you choose this action, your selected row reinstates into the New tab.

**Copy** Choose this action if you want to copy a row, which you can then paste into another document.

Within the View Related Events portlet, in the New, Watched, Active, Expired, or Archived tabs, four tables display information about your related events.

**Configuration table**

Displays a list of the related event configurations.

**Group Sources table**

Displays the source information for related event groups based on the configuration and created patterns.

**Groups table**

Displays the related event groups for a selected configuration.

**Events table**

Displays the related events for a selected configuration or a selected group.

The information that is listed in the Group Sources, Groups, and Events tables is updated based on the selected configuration in the Configuration table. The information that is listed in the Groups and Events tables is updated based on the selected group source in the Group Sources table. The Events table is further filtered by selecting a group in the Groups table.

Right-click on a configuration in the Configuration table to display a list of menu items. You can select the following actions from the menu list.

**Watch** For more information about this action, see “Watching a correlation rule” on page 181.

**Deploy** For more information about this action, see “Deploying a correlation rule” on page 182.

**Archive** For more information about this action, see “Archiving related events” on page 177.

**Copy** Choose this action if you want to copy a row, which you can then paste into another document.

Right-click on a pattern in the Group Sources table to display a list of menu items. You can select the following actions from the menu list.

**Edit Pattern** For more information about this action, see “Editing an existing pattern” on page 190.

**Delete Pattern** For more information about this action, see “Deleting an existing pattern” on page 191.

**Copy** Choose this action if you want to copy a row, which you can then paste into another document.

Right-click on a group name in the Groups table to display a list of menu items. You can select the following actions from the menu list.

**Show details** For more information about this action, see “Viewing related events details for a seasonal event” on page 169.

**Create Pattern** For more information about this action, see “Creating patterns” on page 184.

**Unmark as reviewed** For more information about this action, see “Marking a related events group as reviewed” on page 170.

**Mark as reviewed** For more information about this action, see “Marking a related events group as reviewed” on page 170.

**Watch** For more information about this action, see “Watching a correlation rule” on page 181.

**Deploy** For more information about this action, see “Deploying a correlation rule” on page 182.

**Archive** For more information about this action, see “Archiving related events” on page 177.

**Delete** This action is only available from within the Archived tab. If you want to delete event groups from the system, choose this action.

**Reset performance statistics** For more information about this action, see “Viewing performance statistics for a correlation rule” on page 183.

**New** This action is only available from within the Archived tab. If you choose this action, your selected row reinstates into the New tab.

**Copy** Choose this action if you want to copy a row, which you can then paste into another document.

Right-click on an event in the Events table to display a list of menu items. You can select the following actions from the menu list.

**Show details** For more information about this action, see “Viewing related events details for a seasonal event” on page 169.

**Copy** Choose this action if you want to copy a row, which you can then paste into another document.

Within the View Related Events portlet, you can also complete the following types of tasks.

- View related events.
- View related events by group.
- Sort a related events view.
- View performance statistics for a deployed correlation rule.

Within the Related Event Details portlet, you can also complete the following types of tasks.

- Change the pivot event.
- Work with correlation rules and related events.
- View events that form a correlation rule.
- Select a root cause event for a correlation rule

## Viewing related events

In the View Related Events portlet, you can view a listing of related events as determined by related events configurations that ran.

### Procedure

1. Log in to the Dashboard Application Services Hub as a user with the `ncw_analytics_admin` role.
2. In the Dashboard Application Services Hub navigation menu, go to the **Insights** menu.
3. Under **View Analytics**, select **View Related Events**.
4. By default, within the View Related Events portlet the New tab opens, this tab lists related events with a status of New.

### What to do next

If you want to see related events with another status, select the relevant toolbar button within the View Related Events portlet toolbar.

## Viewing related events details for a seasonal event

You can view related event details for a seasonal event in the Related Event Details portlet.

### Before you begin

To access the Seasonal Event Rules portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To view a list of historical events for a seasonal event, complete the following steps.

1. Open the **View Seasonal Events** portlet.
2. Select a specific configuration or **ALL** in the configuration table.
3. Select a seasonal event in the events table.
4. Right-click the seasonal event and select **Show Related Event Details**.

### Results

The Related Event Details portlet displays the related event details.

## Viewing related events by group

From the full list of related events, you can view only the related events that are associated to a specific group.

### About this task

A related events configuration can contain one or many related events groups. A related events group is determined by a related events configuration and a related events group can be a child of one or more related events configurations.

**Note:** You might see a different number of **Unique Events** in a related events group when a **Relationship Profile** of Strong has been selected for the events in the configuration. This is caused by the same events being repeated more than once.

## Procedure

1. Start the View Related Events portlet, see “Viewing related events” on page 169.
2. Within any tab, in the Configuration table, expand the root node All. The list of related events configurations display.
3. In the Configuration table, select a related events configuration. The list of related events groups display in the Group table and the related events display in the Event table.
4. In the Configuration table, select a related events configuration. The list of related events groups display in the Group Sources and Groups tables and the related events display in the Events table.
5. In the Group table, select a group. The Event table updates and displays only the events that are associated to the selected group.

## Marking a related events group as reviewed

The review status for a related events group can be updated in the View Related Events portlet.

### About this task

In the View Related Events portlet, within the group table you can modify the review status for a related events group. The review status values that are displayed indicates to Administrators whether related events groups are reviewed or not.

In the View Related Events portlet, in the Groups table you can modify the review status for a related events group. The review status values that are displayed indicates to Administrators the review status of the related events groups.

Related events groups can display these review status values.

Yes. The group is reviewed.

No. The group is not reviewed.

To mark a related events group as reviewed or not reviewed, complete the following steps.

## Procedure

1. View related events, see “Viewing related events” on page 169.
2. In the View Related Events portlet, within the group table, select a line item, which represents a group, and right-click. A menu is displayed.
3. From the menu, select **Mark as Reviewed** or **Unmark as Reviewed**. A success message in a green dialog box displays.

## Results

The values in the Reviewed column are updated, to one of the following values Yes, No.

When you enable sorting for the group table, you can sort on the Yes or No values.



## Sorting a related events view

Within a related events view, it is possible to sort the information that is displayed.

### Before you begin

Within the View Related Events portlet, select the tab view where you want to apply the sorting.

### About this task

Sorting by single column or multiple columns is possible within either the Configuration, Group or Event table. Sorting within the Group or Event table can be done independently or in parallel by using the sorting arrows that display in the table column headings. When you apply sorting within the Configuration table the configuration hierarchy disappears, but the configuration hierarchy reappears when you remove sorting. For more details about rollup information, see “Updating Rollup Configuration” on page 122.

Sorting by single column or multiple columns is possible within the Configuration, Group Sources, Groups or Event table. Sorting within the Groups or Event table can be done independently or in parallel by using the sorting arrows that display in the table column headings. When you apply sorting within the Configuration table the configuration hierarchy disappears, but the configuration hierarchy reappears when you remove sorting. For more details about rollup information, see “Updating Rollup Configuration” on page 122.

### Procedure

1. In either the Configuration, Group or Event table, hover the mouse over a column heading. Arrows are displayed, hover the mouse over the arrow, one of the following sort options is displayed.
  - Click to sort Ascending**
  - Click to sort Descending**
  - Do not sort this column**
2. In either the Configuration, Group Sources, Groups or Event table, hover the mouse over a column heading. Arrows are displayed, hover the mouse over the arrow, one of the following sort options is displayed.
  - Click to sort Ascending**
  - Click to sort Descending**
  - Do not sort this column**
3. Left-click to select and apply your sort option, or left click a second or third time to view and apply one of the other sort options.
4. For sorting by multiple column, apply a sort option to other column headings. Sorting by multiple columns is not limited, as sorting can be applied to all columns.

### Results

The ordering of your applied sort options, is visible when you hover over column headings. The sorting options that you apply are not persistent across portlet sessions when you close the portlet the applied sorting options are lost.

## Filtering related events

Filtering capability is possible on the list of related events within the View Related Events portlet.

### Procedure

1. Start the View Related Events portlet, see “Viewing related events” on page 169
2. Within the toolbar, in the filter text box, enter the filter text that you want to use. Filtering commences as you type.

### Results

The event list is reduced to list only the events that match the filter text in at least one of the displayed columns.

### What to do next

To clear the filter text, click the x in the filter text box. After you clear the filter text, the event list displays all events.

## Exporting related events for a specific configuration to Microsoft Excel

You can export related events for a specific configuration to a Microsoft Excel spreadsheet from a supported browser.

### Before you begin

You view related events for one or more configurations in the **View Related Events** portlet. To access the **View Related Events** portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To export related events for a specific configuration to a Microsoft Excel spreadsheet, complete the following steps.

1. Open the **View Related Events** portlet.
2. Select a specific configuration from the configuration table.
3. Click the **Export Related Events** button in the toolbar. After a short time, the **Download export results** link displays.
4. Click the link to download and save the Microsoft Excel file.

### Results

The Microsoft Excel file contains a spreadsheet with the following tabs:

- **Report Summary:** This tab contains a summary report of the configuration that you selected.
- **Groups Information:** This tab contains the related events groups for the configuration that you selected.
- **Groups Instances:** This tab contains a list of all the related events instances for all of the related events groups for the configuration that you selected.
- **Group Events:** This tab contains a list of all the events that occurred in the related events groups for the configuration that you selected.

- **Instance Events:** This tab contains a list of all the events that occurred in all of the related events instances for all the related events groups for the configuration that you selected.
- **Export Comments:** This tab contains any comments relating to the export for informational purposes (for example, if the spreadsheet headers are truncated, or if the spreadsheet rows are truncated).

## Exporting selected related events groups to Microsoft Excel

You can export related events groups for a specific configuration to a Microsoft Excel spreadsheet from a supported browser.

### Before you begin

You view related events for one or more configurations in the **View Related Events** portlet. To access the **View Related Events** portlet, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To export related events groups for a specific configuration to a Microsoft Excel spreadsheet, complete the following steps.

1. Open the **View Related Events** portlet.
2. Select a specific configuration from the configuration table.
3. Select multiple related event groups by using the `Ctrl` key and select method. (You can also select multiple related events groups by using the click and drag method.)
4. After selecting multiple related event groups, right click on one of the selected groups and select the **Export Selected Groups** button in the toolbar. After a short time, the **Download export results** link displays.
5. Click the link to download and save the Microsoft Excel file.

### Results

The Microsoft Excel file contains a spreadsheet with the following tabs:

- **Report Summary:** This tab contains a summary report of the configuration that you selected.
- **Groups Information:** This tab contains the related events groups for the configuration that you selected.
- **Groups Instances:** This tab contains a list of all the related events instances for all of the related events groups for the configuration that you selected.
- **Group Events:** This tab contains a list of all the events that occurred in the related events groups for the configuration that you selected.
- **Instance Events:** This tab contains a list of all the events that occurred in all of the related events instances for all the related events groups for the configuration that you selected.
- **Export Comments:** This tab contains any comments relating to the export for informational purposes (for example, if the spreadsheet headers are truncated, or if the spreadsheet rows are truncated).

## Expired related events

When the automated expiry time is reached for a related events group, the group and related events are visible in the View Related Events portlet, within the Expired tab.

Even though the expired groups and related events are visible in the Expired tab, you must acknowledge that the group is expired. In the Expired tab, right-click on the group that you want to acknowledge. A menu is displayed, from the menu select **Validate**. The default automated expiry time for an active configuration is six months. To change the expiry time see “Changing the expiry time for related events groups” on page 140.

To perform other actions on related events within the Expired tab, right-click on a group or event and a menu is displayed. From the menu, select the action that you want to take.

## Impacts of newly discovered groups on existing groups

An existing related events group can be replaced by newly discovered related event group, or the newly discovered group can be ignored.

The following bullet points describe the Event Analytics functions for management of newly discovered groups and existing groups.

- If a newly discovered group is a subset or same as an existing group within Watched, Active, Expired, or Archived, then Event Analytics ignores the newly discovered group.
- If a newly discovered group is a superset of an existing group within New, then Event Analytics deletes the existing group and displays the newly discovered group in New. Otherwise, no changes occur with the existing group.
- If a newly discovered group is a superset of an existing group within Watched, Active, or Expired, then Event Analytics moves the existing group to Archived, and displays the newly discovered group in Watched, Active, or Expired.
- If a newly discovered group is a superset of an existing group within Archived, then Event Analytics adds the newly discovered group in to New and leaves the Archived group where it is.

## Extra details about related events

Use the Related Event Details portlet to access extra details about related events.

Within the Related Event Details portlet, you can complete the following types of tasks.

- View the occurrence time of an event.
- Switch between tabulated and charted event information.
- Remove an event from a related events group.

Only one instance of the Related Event Details portlet can be open at any stage. If you select **Show Details** for an event or an event group in the View Related Events portlet and the Related Event Details portlet is already open, the detail in the Related Event Details portlet refreshes to reflect your selected event or event group.

## Viewing the occurrence time of an event

You can get details about the time that an event occurred.

### About this task

When you look at the occurrence time of an event, you might be able to relate this event to some other events that occurred around the same time. Within a particular event group, the same event might occur multiple times. For example, if the group occurs 10 times within the time period over which the related events report is run, then there are 10 instances of the group. The event might occur in each of those group instances, resulting in 10 occurrence times for that event. Events in strong related events groups appear in all group instances, but events in medium or weak related events groups might appear in a subset of the group instances. This information is visible in the Related Event Details portlet by switching between different instances in the Event Group Instance Table as explained in the following procedure.

### Procedure

1. Start the View Related Events portlet, see “Viewing related events” on page 169.
2. Within the View Related Events portlet, in the Events table select an event or in the Group table select an event group, and right-click. A menu is displayed.
3. From the menu, select **Show Details** and a Related Event Details portlet opens.
4. Within the Related Event Details portlet, in the Events tab, two tables are displayed.
  - Event Group Instance Table: This table lists each instance of the event group and the time at which the instance occurred. The time of the group instance is set to the occurrence time of the event that you selected.
    - The Unique Events column shows the number of unique events for each group instance.
  - Events Table: This table lists the events for a selected group instance and the occurrence time of each event.
    - The Offset column displays Not Applicable if the pivot event is not in the selected group instance. However, if the pivot event is in the selected group instance the Offset column displays an offset time that is related to the pivot event. For more information about the pivot event, see “Changing the pivot event” on page 178.
    - The Instances column shows the number of group instances each event participates in.

### What to do next

Within the Event Group Instance Table, select another instance of the event group. The Events Table now displays the events in the newly selected group instance.

## Switching between tabulated and charted event information

Event information is visible in table or chart format, within the Related Event Details portlet.

### About this task

A pivot event is an event that acts as a pivot around which you can extrapolate related event occurrences, in relation to the pivot event occurrence. To view the event distribution of a pivot event, complete the following steps to switch from tabulated event information to charted event information within the Related Event Details portlet.

### Procedure

1. Start the View Related Events portlet, see “Viewing current analytics configurations” on page 134.
2. Within the View Related Events portlet, in the Events table select an event or in the Group table select an event group, and right-click. A menu is displayed.
3. From the menu, select **Show Details** and a Related Event Details portlet opens.
4. Within the Related Event Details portlet, in the Events tab, two tables are displayed.

Event Group Instance Table: This table lists each instance of the event group and the time at which the instance occurred. The time of the group instance is set to the occurrence time of the event that you selected.

Events Table: This table lists the events for a selected group instance.

5. From the Events tab toolbar, select **Timeline**. The event information displays in chart format.

For information about understanding the timeline chart, see “Understanding the timeline chart” on page 215

**Note:** The timeline chart scale is displayed as **seconds (s)**, **minutes (m)**, or **hours (h)**. If many timelines are displayed, users might need to scroll down to view all of the timelines. The timeline chart scale is anchored in place at the top of the **Timeline** view.

### Results

The timeline chart shows the event distribution for each event type in the group, relative to the pivot event. Each comb in the timeline chart represents an event type and the teeth represent the number of instances of the event type. The pivot event is not represented by a comb, but the pivot event instance is always at zero seconds, minutes, or hours. For a selected event group instance, the highlighted tooth on each comb denotes the event type instance relative to the pivot event, in seconds, minutes, or hours.

The long summary labels under the combs in the timeline chart are truncated. Move the mouse cursor over a truncated summary label to see the tooltip that shows the full summary label.

### What to do next

- If there are many event types to view, use the pagination function in addition to scrolling. In the pagination toolbar, select the page to view and the page size.
- If you want to change the pivot event, see “Changing the pivot event” on page 178.

- If you want to revert to the tabulated event information, select **Events** from the Events tab toolbar.

## Removing an event from a related events group

You can remove an event from a related events group.

### About this task

When you believe that an event is no longer related to other events in the related events group, you can remove the event from that events group. When you remove an event from a related events group, the event is hidden from the UI and the correlation process but the event is not deleted from the system. Complete the following steps to remove an event from a related events group.

### Procedure

1. View event groups and events in the View Related Events portlet, see “Viewing related events” on page 169 and “Viewing related events by group” on page 169.
2. Within the View Related Events portlet, in the Group table select an event group or in the Event table select an event, and right click. A menu is displayed.
3. From the menu, select **Show Details** and a Related Event Details portlet opens.
4. Within the Related Event Details portlet, in either the Events tab on the events table or in the Correlation Rule tab, right-click on an event. A menu is displayed.
5. From the menu, select **Remove Event**.
6. A confirmation message is displayed, select **Yes** or **No**.

### Results

The event is removed from the group and no longer appears in the event list in either the Events tab and the Correlation Rule tab.

## Archiving related events

You can archive related events by archiving the related events group.

### Before you begin

View event groups and events in the View Related Events portlet, see “Viewing related events” on page 169 and “Viewing related events by group” on page 169.

### About this task

When you believe that events within a related events group are no longer relevant, you can archive that group. Complete the following steps to archive a related events group.

### Procedure

- To archive a related events group within the View Related Events portlet, complete the following steps.
  1. Within the View Related Events portlet, select the **New**, **Watched**, **Active**, or **Expired** tab.
  2. In your chosen tab, within the Group table select an event group and right click. A menu is displayed.

3. From the menu, select **Archive**.
- To archive a related events group within the Related Event Details portlet, complete the following steps.
  1. Within the View Related Events portlet, select the **New**, **Watched**, **Active**, or **Expired** tab.
  2. In your chosen tab, within the Group table select an event group or within the Event table select an event, and right click. A menu is displayed.
  3. From the menu, select **Show Details**, a Related Event Details portlet opens.
  4. Within the Related Event Details portlet, in either the Events or Correlation Rule tab, select **Archive**. A success message is displayed.

## Results

The related events group moves into the Archived tab in the View Related Events portlet.

## What to do next

Within the Archived tab, from the list of archived groups you can select a group and right click. A menu is displayed with a choice of tasks for your selected group.

- If you want to move a group out of the Archived tab and into the New tab, from the menu select **New**. A number of actions can be performed with groups and events within the New tab, see “Work with related events” on page 166.
- If you want to delete a related events group from the system, from the menu select **Delete**. This is the only way to delete a related events group from the system.

## Changing the pivot event

You can change a pivot event to view related events that are of interest.

## About this task

Use a pivot event as a baseline to determine a sequence of events in the group. A pivot event displays in the Related Event Details portlet. Within the Related Event Details portlet, a pivot event can be changed. Also, a pivot event history, of the 20 most recent pivot events, is available for you to revisit.

- When you open the Related Event Details portlet from an event in the View Related Events portlet, that event becomes the pivot event within the Related Event Details portlet.
- When you open the Related Event Details portlet from a group in the View Related Events portlet, one of the events from that group becomes the pivot event within the Related Event Details portlet. The pivot event is not always the parent event.

Complete the following steps to change the pivot event.

## Procedure

1. Within the View Related Events portlet, right-click on an event or a group. A menu is displayed.
2. From the menu, select **Show Details**. The Related Event Details portlet opens.
3. Within the Related Event Details portlet, information about the pivot event is displayed.



- In the Event Group Instance table, the Contains Pivot Event column reports if a group instance has a pivot event, or not.
  - In the Events table, the pivot event is identifiable by a red border.
  - Next to the Group Name entry, a **Pivot Event** link displays. To see more details about the pivot event, click the **Pivot Event** link and a More Information widow opens displaying details about the pivot event.
4. In the Related Event Details portlet, within the Events tab, in the Events table, right-click on the event you want to identify as the pivot event. A menu is displayed.
  5. From the menu, select **Set as Pivot Event**.

## Results

Your selected event becomes the pivot event with a red border. Data updates in the timeline chart, in the **Pivot Event** link, in the Event Group Instance table and in the Events table.

## What to do next

Within the Related Event Details portlet, you can reselect one of your 20 recent pivot events as your current pivot event. From the Events tab toolbar, select either the forward arrow or back arrow to select one of the 20 recent pivot events.

## Correlation rules and related events

A correlation rule is a mechanism that enables automatic action on real-time events that are received by the ObjectServer, if a trigger condition is met. The result is fewer events in the Event Viewer for the operator to troubleshoot.

Writing a correlation rule in code is complex but the related events function removes the need for administrators to code a correlation rule. Instead, the related events function derives a correlation rule from your related events configuration and deploys a correlation rule, all through the GUI. After the correlation rule is deployed in a live environment and if the trigger condition is met, then automatic action occurs.

- The trigger condition is the occurrence of one or more related event types, from an event group, on the Tivoli Netcool/OMNIBus ObjectServer. Only one event must be the parent event. Related event types are derived from your related events configuration.
- The automatic action is the automatic creation of a synthetic event with some of the properties of the parent event, and the automatic grouping of the event group events under this synthetic event.

## Viewing events that form a correlation rule

You can view the related events that form a correlation rule in the Related Event Details portlet.

## About this task

Administrators can view related events that form a correlation rule to understand associations between events. Complete the following steps to view related events that form a correlation rule.

## Procedure

1. Start the View Related Events portlet, see “Viewing current analytics configurations” on page 134.
2. Within the View Related Events portlet, in the Events table select an event or in the Group table select an event group, and right-click. A menu is displayed.
3. From the menu, select **Show Details** and a Related Event Details portlet opens.
4. In the Related Event Details portlet, select the **Correlation Rule** tab.

## Results

A table displays with a list of the related events that make up the correlation rule.

### Selecting a root cause event for a correlation rule

You can select the root cause event for the correlation rule

## About this task

When you select the root cause event for the correlation rule, the selected event becomes a parent event. A parent synthetic event is created with some of the properties from the parent event and a parent-child relationship is created between the parent synthetic event and the related events. When these events occur in a live environment, they display in the Event Viewer within a group as child events of the parent synthetic event. With this view of events, you can quickly focus on the root cause of the event, rather than looking at other related events.

To select the root cause event for the correlation rule, complete the following steps. If you want to see automated suggestions about the root cause event for a group, see configuration details in “Updating Rollup Configuration” on page 122.

## Procedure

1. View all events that form a correlation rule, see “Viewing events that form a correlation rule” on page 179
2. In the Related Event Details portlet, within the **Correlation Rule** tab, right-click an event and select Use Values in Parent Synthetic Event.

## Results

The table in the **Correlation Rule** tab refreshes and the Use Values in Parent Synthetic Event column for the selected event updates to Yes, which indicates this event is now the parent event.

For a related events group, if all of the children of a parent synthetic event are cleared in the Event Viewer, then the parent synthetic event is also cleared in the Event Viewer. If another related event comes in for that same group, the parent synthetic event either reopens or re-creates in the Event Viewer, depending on the status of the parent synthetic event.

## Watching a correlation rule

You can watch a correlation rule and monitor the rule performance before you deploy the rule for the rule to correlate live data.

### Before you begin

Complete your review of the related events and the parent event that form the correlation rule. If necessary, change the correlation rule or related events configuration.

### About this task

When you are happy with the correlation rule, you can choose to **Watch** the correlation rule.

When you choose to **Watch** the correlation rule, the rule moves out of its existing tab and into the Watched tab within the View Related Events portlet. While the rule is in Watched, the rule is not creating synthetic events or correlating but does record performance statistics. You can check the rule's performance before you deploy the rule for the rule to correlate live data.

Complete the following steps to **Watch** the correlation rule.

### Procedure

- Within the View Related Events portlet.
  1. View related events by group, see “Viewing related events by group” on page 169.
  2. In the View Related Events portlet, within the group table, select either a related events group or a related events configuration and right click. A menu is displayed.
  3. From the menu, select **Watch**.
- Within the Related Event Details portlet for a group or an event.
  1. View related events or related event groups, see “Viewing related events” on page 169 and “Viewing related events by group” on page 169.
  2. Select an event or a related events group.
    - In the View Related Events portlet, within the group table, select a related events group and right click. A menu is displayed.
    - In the View Related Events portlet, within the event table, select an event and right click. A menu is displayed.
  3. From the menu, select **Show Details**. The Related Event Details portlet opens.
  4. In the Related Event Details portlet, within any tab, select **Watch**.

### Results

The rule displays in the Watched tab.

### What to do next

Within the Watched tab, monitor the performance statistics for the rule. When you are happy with the performance statistics consider “Deploying a correlation rule” on page 182.

## Deploying a correlation rule

You can deploy a correlation rule, for the rule to correlate live data.

### Before you begin

Complete your review of the related events and the parent event that form the correlation rule. If necessary, change the correlation rule or related events configuration.

### About this task

When you are happy with the correlation rule, you can choose to **Deploy** the correlation rule.

When you choose to **Deploy** the correlation rule, the rule moves out of its existing tab and into the Active tab within the View Related Events portlet. Active rule algorithm works to identify the related events in the live incoming events and correlates them so the operator knows what event to focus on. Performance statistics about the rule are logged which you can use to verify whether the deployed rule is being triggered.

Complete the following steps to **Deploy** the correlation rule.

### Procedure

- Within the View Related Events portlet.
  1. View related events by group, see “Viewing related events by group” on page 169.
  2. In the View Related Events portlet, within the groups table, select either a related events group or a related events configuration and right click. A menu is displayed.
  3. From the menu, select **Deploy**.
- Within the Related Event Details portlet for a group or an event.
  1. View related events or related event groups, see “Viewing related events” on page 169 and “Viewing related events by group” on page 169.
  2. Select an event or a related events group.
    - In the View Related Events portlet, within the groups table, select a related events group and right click. A menu is displayed.
    - In the View Related Events portlet, within the events table, select an event and right click. A menu is displayed.
  3. From the menu, select **Show Details**. The Related Event Details portlet opens.
  4. In the Related Event Details portlet, within any tab, select **Deploy**.

### Results

The rule moves out of the New tab and into the Active tab within the View Related Events portlet.

### What to do next

When you establish confidence with the rules and groups that are generated by a related events configuration, you might want all the generated groups to be automatically deployed in the future. If you want all the generated groups to be

automatically deployed, return to “Creating a new or modifying an existing analytics configuration” on page 136 and within the Configure Related Events window, tick the option Automatically deploy rules discovered by this configuration.

## Viewing performance statistics for a correlation rule

You can view performance statistics for a correlation rule in the View Related Events portlet, within the Watched, Active, or Expired tabs.

### Performance statistics in the group table

**Times Fired:** The total number of times the rule ran since the rule became active.

**Times Fired in Last Month:** The total number of times that the rule is fired in the current month. Months are calculated from the creation date of the group. At the beginning of a new month, this value resets back to 0.

**Last Fired:** The last date or time that the rule was fired.

**Last Occurrence I:** The percentage of events that occurred from the group, in the last fired rule.

**Last Occurrence II:** The percentage of events that occurred from the group in the second last fired rule.

**Last Occurrence III:** The percentage of events that occurred from the group in the third last fired rule.

### Performance statistics in the event table

**Occurrence:** The number of times the event occurred, for all the times the rule fired.

### Reset performance statistics

You can reset performance statistics to zero for a group in the Watched, Active, or Expired tabs. To reset performance statistics, right-click on the group name and from the menu select **Reset performance statistics**. A message displays indicating that the operation will reset statistics data for the selected correlation rule. The message also indicates that you will not be able to retrieve this data. Click Yes to continue with the operation or No to stop the operation. A success message displays after you select Yes.

Resetting performance statistics to zero for a group also causes the following columns to be cleared: Times Fired, Times Fired in Last Month, and Last Fired. Note that performance statistics are not collected for the Archived tab. When a rule is moved between states, the performance statistics are reset. Every time an action is triggered by the rule the performance statistics increase.

### Related Events statistics

When sending some events a synthetic event is created, but the statistics can appear not to be updated.

This is because there are delays in updating the related events statistics. These delays are due to the time window during which the related event groups are open, so that events can be correlated.

The statistics (Times Fired, Times Fired in last month, last fired) are updated only when the **Group Time to Live** has expired. The sequence is; synthetic event is triggered, action is done, and the statistics are calculated later.

Take the following query as an example:

```
SELECT GROUPTTL FROM RELATEDEVENTS.RE_GROUPS WHERE GROUPNAME = 'XXX';
```

There was an occurrence of the GROUPTTL being equal to 82800000 milliseconds, this is 23 hours. In this instance an update to the statistics wouldn't be visible to the user for 23 hours. If GROUPTTL is reduced to 10 seconds by running the following command:

```
UPDATE RELATEDEVENTS.RE_GROUPS SET GROUPTTL = 10000 WHERE GROUPNAME = 'XXX';
```

Subsequent tests will show that the statistics are updated promptly.

An algorithm creates GROUPTTL based on historical occurrences of the events. There is no default value for GROUPTTL and no best practice recommendation. GROUPTTL should be determined and set on a per case basis.

---

## Creating patterns

Groups of related events are discovered using Related Event analytics. Automatically discovered groups in the View Related Events portlet can be used to create patterns.

While the discovered groups are specific to a particular resource, the event patterns are not specific to one single resource. A resource can be a host name ("server name"), and is usually a Node field in the ObjectServer events.

For example, assume that Link up and Link down regularly occurs on Node A. Analytics detects the occurrence in the historical data and generates a specific grouping of those two events for Node A. Likewise, if Link up and Link down also regularly occurs on Node B, a grouping of those two events will be generated but specifically for Node B.

With generalization, the association of such events is encapsulated by the system as a pattern: Link up / Link down on any Node. In generalization terms, Link Up / Link Down represents the event type and Node\* represents the resource.

A created pattern has the following advantages over a related event group:

- For any instance of a pattern, not all of the events in the definition have to occur for the pattern to apply. This is dependent on the Trigger Action settings. For more information about Trigger Action setting, see "Creating an event pattern" on page 186.
- The pattern definition encompasses groups of events with the defined event types.
- A single pattern can capture the occurrence of events on any resource. For example, with discovered groups, analytics only found historical events that occurred on a specific host name, and created groups for each host name. If real time events happen on different host names in the future, the discovered groups will not capture them. However, patterns will discover the events because the event type is the same.
- A pattern can encompass event groupings that were not previously seen in the event history. An event group that did not previously occur on a specific resource is identified by the pattern, as the pattern is not resource dependent, but event type specific.
- A single pattern definition can encompass multiple event groups. Patterns will act on event types for different host names which might have occurred

historically (discovered groups) or will happen in future real time events. For example, an event type could be *"Server Shutting Down"*, *"Server Starting Up"*, *"Interface Ping Failure"*, and so on. Each group is resource specific, but an event pattern is event type specific. Therefore, an environment might have multiple groups for different resources, and an event pattern will encompass all of those different groups since their event type is the same.

## Starting the Events Pattern portlet

The administrator can start the Events Pattern portlet from a number of locations on the Event Analytics UI.

### Before you begin

To access the View Related Events, Related Event Details, and Events Pattern portlets, users must be assigned the `ncw_analytics_admin` role.

### About this task

You can start the Events Pattern portlet from the View Related Events portlet or the Related Event Details portlet. Starting the Events Pattern portlet directly from the Related Event Details portlet ensures that you do not need to return to the View Related Events portlet to start the Events Pattern portlet after you review the details of a group.

### Procedure

You can start the Events Pattern portlet from the View Related Events portlet or the Related Event Details portlet.

1. To start the Events Pattern portlet from the View Related Events portlet, start the View Related Events portlet and select one of the following options. For more information about starting the View Related Events portlet, see "Viewing related events" on page 169.
  - a. To create a pattern, complete the following steps.
    - 1) Select a related events group in the Groups table.
    - 2) Right-click the related events group and select **Create Pattern**.
  - b. To edit an existing pattern, complete the following steps.
    - 1) Select a pattern in the Group Sources table.
    - 2) Right-click the pattern and select **Edit Pattern**.
2. To start the Events Pattern portlet from the Related Event Details portlet, complete the following steps.
  - a. Start the Related Event Details portlet. For more information, see "Viewing related events details for a seasonal event" on page 169
  - b. Click **Create Pattern**.

**Note:** The Events Pattern portlet is updated with each newly selected group.

3.

### What to do next

Input the details of the pattern in the Events Pattern portlet. For more information about completing the Events Pattern portlet, see "Creating an event pattern" on page 186

## Creating an event pattern

You can create a pattern based on the automatically discovered groups.

### Before you begin

To access the View Related Events and Events Pattern portlets, users must be assigned the `ncw_analytics_admin` role.

### About this task

A related events configuration automatically discovers groups of events that apply to specific managed resources. You can create an event pattern that is not specific to resources based on an automatically discovered group.

### Procedure

1. Start the Events Pattern portlet for a group. For more information about starting the portlet, see “Starting the Events Pattern portlet” on page 185.
2. Complete the parameter fields in the **Pattern Criteria** tab of the Events Pattern portlet.

#### Merge into

Merge a Related Event Group into an existing pattern or select **NONE** to create new pattern. To merge a group into a pattern, select from the list of patterns with one or more event types in common. **NONE** is the default option.

**Name** The name of the pattern. The name must contain alphanumeric characters. Special characters are not permitted.

#### Pattern Filter

The ObjectServer SQL filters that are applied to the pattern. This filter is used to restrict the events to which the pattern is applied. For example, enter `Summary NOT LIKE '%maintenance%'`.

#### Time between first and last event

The maximum time that can elapse between the occurrence of the first event and the last event in this pattern, which is measured in minutes. The default value is determined by the Related Events Group on which the pattern is based. Events that occur outside of this time window are not considered part of this group.

#### Trigger Action

Select the **Trigger Action** check box to group the live events when the selected event comes into the ObjectServer. When an event with the selected event type occurs, the grouping is triggered to start. The created grouping includes events that contain all of the selected event types.

For example, if the following three event types are part of the pattern criteria, A, B, and C, with only the **Trigger Action** check box for event C selected, the grouping only occurs when an event with event type C occurs. The grouping contains events that contain all three event types.

#### Event Type

The event type or types that are included in the pattern. The **Event Type** is pre-populated with existing event types for the selected pattern, and can be modified.



**Resource Column(s)**

The resource or resources to which the action is applied. The **Resource Column(s)** is pre-populated with existing event type resources for the selected pattern, and can be modified.

**Note:** The triangle, circle, and square icons signify where the event types originate from when a group is merged into an exiting pattern.

**Triangle**

Common to both the existing pattern and the group.

**Circle** Part of the group.

**Square**

Part of the existing pattern.

**Note:** Duplicate **Event Type** and **Resource Columns** pairs are not permitted.

**Regular Expression**

(Optional) Click the regular expression icon to provide the regular expression pattern for extracting the resource information from the selected column.

**Note:** To configure the regular expression for a resource, select one resource in the resource column.

For example, the application abc on : myhost.xxxxxxx.xxx.com : encountered an unrecoverable error.

Assuming that the resource information is always located between colons (:), and the host name ends with xxx.com, the following regular expression extracts this resource information while the Events Pattern is created.

```
[^:]*.com
```

For more information about creating and editing regular expressions, see “Applying a regular expression to the pattern criteria” on page 188 and “Editing a pattern criteria regular expression” on page 189.

3. In the **Parent Event** tab of the Events Pattern portlet, select one of the following parent event options.

**Most Important Event by Type**

The system checks the events as they occur. The events are ranked based on the order defined in the UI. The highest ranking event is the parent. The parent event changes if a higher ranking event occurs after a lower ranking event. To prevent a dynamically changing parent event, select **Synthetic Event**.

You can manually reorder the ranking by selecting an event and clicking the **Move Up** and **Move Down** arrows.

**Synthetic Event**

Create an event to act as the parent event or select **Use Selected Event as Template** to use an existing event as the parent event.

To create or modify a synthetic event, populate the following parameter fields, as required. All of the synthetic event fields are optional.

**Node** The managed entity from which the event originated. Displays the managed entity from which the seasonal event originated.

**Summary**

The event description.

**Severity**

The severity of the event. Select one of the following values from the **Severity** drop-down list.

Critical  
Major  
Minor  
Warning  
Indeterminate  
Clear

**Alert Group**

The Alert Group to which the event belongs.

**Add additional fields**

Select the **Add additional fields** check box to add more fields to the synthetic parent event.

4. In the **Test** tab of the Events Pattern portlet, you can run a test to display the existing auto-discovered groups that match the pattern criteria. The test displays the types of events that are matched by the chosen criteria. To run the test, select **Run Test**. To cancel the test at any time, select **Cancel Test**.
5. To save, watch, or deploy the pattern, select one of the following options.
  - Select **Save** to save the pattern details to the View Related Events **New** tab.
  - Select **Watch** to add the pattern to the View Related Events **Watched** tab.
  - Select **Deploy** to add the pattern to the View Related Events **Active** tab.

**Results**

The events pattern is created and displayed in the Group Sources table in the View Related Events portlet.

**Note:** If the patterns display 0 group and 0 events, the pattern creation process is not finished. To confirm that the process is running,

1. Append the policy name to the policy logger file from the **Services** tab, **Policy Logger** service. For more information about configuring the Policy logger, see [Configuring the Policy logger service](#).
2. Check the following log file.

`$IMPACT_HOME/logs/<serverName>_policylogger_PG_ALLOCATE_PATTERNS_GROUPS.log`

If the process is not running, see the [Troubleshooting Event Analytics](#) guide.

## Applying a regular expression to the pattern criteria

You can apply a regular expression to the pattern criteria to extract information from unstructured data in the selected resource column.

**Before you begin**

To access the View Related Events and Events Pattern portlets, users must be assigned the `ncw_analytics_admin` role.

## About this task

The regular expression extracts specific information from unstructured data in the selected resource column.

### Procedure

1. Start the Events Pattern portlet for a group. For more information about starting the portlet, see “Starting the Events Pattern portlet” on page 185.
2. Select the regular expression symbol in the **Pattern Criteria** tab of the Events Pattern portlet. The Regular Expression dialog box is displayed.
3. Insert the regular expression in the **Expression** field.
4. To change or select the event type to which the regular expression is applied, select an event type from the drop-down list in the **Test Data** field.
5. To test the regular expression, select **Test**. The test results are displayed in the **Result** field.

**Note:** If there are multiple matches for the given regular expression, the matches are displayed in the **Result** field as a comma-separated list.

6. To save and apply the regular expression, select **Save**. The Regular Expression dialog box is closed. A confirm symbol is displayed beside the Resource Column.

## Editing a pattern criteria regular expression

You can edit an existing regular expression that was applied to a pattern criteria to extract information from unstructured data in the selected resource column.

### Before you begin

To access the View Related Events and Events Pattern portlets, users must be assigned the `ncw_analytics_admin` role.

## About this task

The regular expression extracts specific information from unstructured data in the selected resource column.

### Procedure

1. Start the Events Pattern portlet for a group. For more information about starting the portlet, see “Starting the Events Pattern portlet” on page 185.
2. Select the confirm symbol in the **Pattern Criteria** tab of the Events Pattern portlet. The Regular Expression dialog box is displayed.
3. Edit the regular expression in the **Expression** field.
4. To change or select the event type to which the regular expression is applied, select an event type from the drop-down list in the **Test Data** field.
5. To test the regular expression, select **Test**. The test results are displayed in the **Result** field.

**Note:** If there are multiple matches for the given regular expression, the matches are displayed in the **Result** field as a comma-separated list.

6. To save and apply the regular expression, select **Save**. The Regular Expression dialog box is closed. A confirm symbol is displayed beside the Resource Column.

## Viewing related event details in the Events Pattern portlet

You can view the related event details for a selected related events group in the Events Pattern portlet, when you create a new pattern for the group.

### Before you begin

To access the View Related Events and Events Pattern portlets, users must be assigned the `ncw_analytics_admin` role.

### Procedure

To view the related event details in the Events Pattern portlet, complete the following steps.

1. Open the View Related Events portlet.
2. Select a related events group in the Groups table.
3. Right-click the related events group and select **Create Pattern**. The Events Pattern portlet is displayed.

### Results

The related event details are displayed in the Group instances and Events tables in the **Pattern Criteria** tab of the Events Pattern portlet.

**Note:** The related event details columns in the **Pattern Criteria** tab of the Events Pattern portlet matches the Related Event Details portlet columns.

## Editing an existing pattern

You can edit an existing pattern to modify the pattern criteria.

### Before you begin

To access the View Related Events and Events Pattern portlets, users must be assigned the `ncw_analytics_admin` role.

### Procedure

1. Start the View Related Events portlet. For more information about starting the View Related Events portlet, see “Viewing related events” on page 169.
2. Select a pattern in the Group Sources table.
3. Right-click the pattern and select **Edit Pattern**.
4. Modify the parameter fields in the **Pattern Criteria** and **Parent Event** tabs. For more information about modifying the parameters, see “Creating an event pattern” on page 186.
5. To save, watch, or deploy the pattern, select one of the following options.
  - Select **Save** to save the pattern details to the View Related Events **New** tab.
  - Select **Watch** to add the pattern to the View Related Events **Watched** tab.
  - Select **Deploy** to add the pattern to the View Related Events **Active** tab.

## Deleting an existing pattern

You can delete an existing pattern to remove it from the Group Sources table.

### Before you begin

To access the View Related Events and Events Pattern portlets, users must be assigned the `ncw_analytics_admin` role.

### Procedure

1. Start the View Related Events portlet. For more information about starting the View Related Events portlet, see “Viewing related events” on page 169.
2. Select the pattern you want to delete in the Group Sources table.
3. Right-click the pattern and select **Delete Pattern**.
4. To delete the pattern, select **Yes** in the confirmation dialog window.

### Results

The selected pattern is deleted.

## Exporting pattern generalization test results to Microsoft Excel

You can export pattern generalization test results for a specific configuration to a Microsoft Excel spreadsheet from a supported browser.

### Before you begin

To access the View Related Events, Related Event Details, and Events Pattern portlets, users must be assigned the `ncw_analytics_admin` role.

### About this task

You can start the Events Pattern portlet from the View Related Events portlet or the Related Event Details portlet. Starting the Events Pattern portlet directly from the Related Event Details portlet ensures that you do not need to return to the View Related Events portlet to start the Events Pattern portlet after you review the details of a group.

### Procedure

To export pattern generalization test results for a specific configuration to a Microsoft Excel spreadsheet, complete the following steps.

1. Open the **View Related Events** portlet.
2. Select a specific configuration from the configuration table.
3. Enter the pattern criteria and navigate to the **Test** tab of the Events Pattern portlet and select **Run Test**.
4. Click the **Export Generalization Test Results** button in the toolbar. After a short time, the **Download export results** link displays.
5. Click the link to download and save the Microsoft Excel file.

### Results

The Microsoft Excel file contains a spreadsheet with the following tabs:

- **Groups Information:** This tab contains the related events groups for the configuration that you selected.
- **Groups Instances:** This tab contains a list of all the related events instances for all of the related events groups for the configuration that you selected.
- **Group Events:** This tab contains a list of all the events that occurred in the related events groups for the configuration that you selected.
- **Instance Events:** This tab contains a list of all the events that occurred in all of the related events instances for all the related events groups for the configuration that you selected.
- **Export Comments:** This tab contains any comments relating to the export for informational purposes (for example, if the spreadsheet headers are truncated, or if the spreadsheet rows are truncated).

## Configuring the type properties used for event pattern creation in Netcool/Impact

You can configure how Netcool/Impact handles the creation of event patterns by editing properties in the generated NOI Shared Configuration properties file.

### Before you begin

**Note:** You should perform this configuration task prior to running any related events configurations that use the global type properties associated with event pattern creation. It is expected that you will perform this configuration task only when something in your environment changes that affects where type information is found in events.

The default NOI Shared Configuration properties file is divided into sections, where each section contains a number of properties that allow you to instruct how Netcool/Impact handles a variety of operations, such as how it should handle event pattern creation. There are three categories of event pattern creation properties defined in the NOI Shared Configuration properties file:

- Properties related to configuring which table columns in the Event History database that Netcool/Impact should use in performing the event pattern analysis.
- Properties related to configuring the default unique event identifier and event type in the Event History database that you want Netcool/Impact to use when there is no match in the event type index related properties.
- Properties related to configuring one or more event identity and event type indexes.

Table 22 describes the event pattern creation properties defined in the NOI Shared Configuration properties file. Use these descriptions to help you configure the values appropriate for your environment.

*Table 22. Event pattern creation properties*

| Global type                                                                   | Description | Example |
|-------------------------------------------------------------------------------|-------------|---------|
| Properties related to configuring table columns in the Event History database |             |         |

Table 22. Event pattern creation properties (continued)

| Global type                                                                                                               | Description                                                                                                                                                                                                                                       | Example                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type.resourcelist                                                                                                         | Specifies the name of the table column or columns in the Event History database that Netcool/Impact should use in performing the event pattern analysis.                                                                                          | <p>The NOI Shared Configuration properties file that you generate with the nci_trigger command provides the following default value:</p> <pre>type.resourcelist=NODE</pre> <p><b>Note:</b> You should use the default value, NODE.</p>                                        |
| type.servername.column                                                                                                    | Specifies the name of the table column in the Event History database that contains the name of the server associated with any particular event that arrives in the Event History database.                                                        | <p>The NOI Shared Configuration properties file that you generate with the nci_trigger command provides the following default value:</p> <pre>type.servername.column=SERVERNAME</pre> <p><b>Note:</b> You should use the default value, SERVERNAME, where possible.</p>       |
| type.serverserial.column                                                                                                  | Specifies the name of the table column in the Event History database that contains the server serial number associated with any particular event that arrives in the Event History database. Note that the server serial number should be unique. | <p>The NOI Shared Configuration properties file that you generate with the nci_trigger command provides the following default value:</p> <pre>type.serverserial.column=SERVERSERIAL</pre> <p><b>Note:</b> You should use the default value, SERVERSERIAL, where possible.</p> |
| <b>Properties related to configuring the default unique event identifier and event type in the Event History database</b> |                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                               |

Table 22. Event pattern creation properties (continued)

| Global type                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Example                                                                                                                                                                                           |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>type.default.eventid</code> | <p>This property contains the database field in the Event History database that you want to specify as the default Event Identity. An Event Identity is a database field that identifies a unique event in the Event History database. When you configure a related events configuration, you select database fields for the Event Identity from a drop-down list of available fields. In the User Interface, you perform this from the <b>Advanced</b> tab when you want to override the settings in the configuration file.</p> <p>Netcool/Impact uses the database field specified in this property as the default Event Identity when there is no match in the value specified in the <code>type.index.eventid</code> property.</p> <p><b>Note:</b> The database field specified for this property should not contain a timestamp component.</p> | <p>The NOI Shared Configuration properties file that you generate with the <code>nci_trigger</code> command provides the following default value:</p> <pre>type.default.eventid= IDENTIFIER</pre> |



Table 22. Event pattern creation properties (continued)

| Global type                                                                                                                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Example                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type.default.eventtype                                                                                                                                                      | <p>Specifies the default related events type to use when creating an event pattern to generalize.</p> <p>Netcool/Impact uses this default related events type when there is no match in the <code>type.index.eventtype</code> property.</p> <p><b>Note:</b> You choose the related events type values based on the fields for which you want to create a generalized pattern. For example, if you want to create a pattern and generalize it based on the EVENTID for an event, you would specify that value in this property.</p> <p>When the related events configuration completes and you create a pattern for generalization, the pattern generalization screen will contain a drop down menu that lists all of the EVENTIDs found in the Event History database. You can then create a pattern/rule that will be applied to all EVENTIDs selected for that pattern. This means that you can expand the definition of the pattern to include all types, not just the types in the Related Events Group.</p> | <p>The NOI Shared Configuration properties file that you generate with the <code>nci_trigger</code> command provides the following default value:</p> <pre>type.default.eventtype= EVENTID</pre> |
| <b>Properties related to configuring one or more event identity and event type indexes. You should specify values for each of the properties described in this section.</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                  |

Table 22. Event pattern creation properties (continued)

| Global type                        | Description                                                                                                                                                                                       | Example                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| type_number_of_type_configurations | Specifies the number of types to use in the NOI Shared Configuration properties file for the global type configuration. There is no limit on how many types you can configure.                    | <p>The following example specifies two types for the global type configuration:</p> <pre>type_number_of_type_configurations=2</pre> <p>Thus, you would define the other type.index related properties as follows. Note that the index numbering starts with 0 (zero).</p> <pre>type.0.eventid=Identifier type.0.eventtype=ACMEType type.0.filterclause=Vendor='ACME' type.0.osfilterclause=Vendor='ACME' type.1.eventid=SUMMARY, NODE type.1.eventtype=TAURUSType type.1.filterclause=Vendor = 'TAURUS' type.1.osfilterclause=Vendor = 'TAURUS'</pre> |
| type.index.eventid                 | Specifies the database field in the Event History database that you want to specify as the Event Identity. Multiple fields are separated by commas.                                               | <p>The following shows an example of a database field used as the Event Identity:</p> <pre>type.0.eventid=SUMMARY</pre> <p>The following shows an example of multiple database fields used as the Event Identity:</p> <pre>type.0.eventid=NODE, SUMMARY, ALERTGROUP</pre>                                                                                                                                                                                                                                                                             |
| type.index.eventtype               | <p>Specifies the event type to return for pattern generalization.</p> <p><b>Note:</b> The returned event types display in the event type drop down menu in the pattern generalization screen.</p> | <p>The following example shows an event type to return for pattern generalization:</p> <pre>type.0.eventtype=EVENTID</pre>                                                                                                                                                                                                                                                                                                                                                                                                                            |

Table 22. Event pattern creation properties (continued)

| Global type                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         | Example                                            |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| <code>type.index.filterclause</code>   | <p>Specifies an Event History database filter that defines a set of events. For the set of events defined by this filter, the event type will be found in the table column or columns in the <code>type.index.eventtype</code> property.</p> <p><b>Note:</b> It is recommended that you create one or more database indexes on the reporter status table for the fields used in the <code>type.index.filterclause</code> to speed up the query.</p> | <code>type.0.filterclause=Vendor = 'ACME'</code>   |
| <code>type.index.osfilterclause</code> | <p>Specifies an ObjectServer filter to filter matching event types.</p> <p><b>Note:</b> The filter that you specify for the <code>type.index.osfilterclause</code> property should be semantically identical to the filter that you specify for the <code>type.index.filterclause</code> property, except for this property you use the ObjectServer syntax.</p>                                                                                    | <code>type.0.osfilterclause=Vendor = 'ACME'</code> |

## About this task

To configure the event pattern creation properties that Netcool/Impact uses for generalization, you must modify the default NOI Shared Configuration properties file in the `<Impact_install_location>/bin` directory.

## Procedure

1. Log in to the server where IBM Tivoli Netcool/Impact is stored and running.
2. Go to the `<Impact_install_location>/bin` directory.
3. Enter the following command: `./nci_trigger <server_name> <UserID>/<password> NOI_DefaultValues_Export FILENAME <Full Path to the file name><name_of_propsfile>`
  - `<server_name>`  
Specifies the name of the server where Netcool/Impact is stored and running.
  - `<UserID>`  
Specifies the ID of the Netcool/Impact user.
  - `<password>`  
Specifies the password of the Netcool/Impact user.

*<Full Path to the file name><name\_of\_propsfile>*

Specifies the directory where the default NOI Shared Configuration properties file resides. The directory specification includes the name of the default NOI Shared Configuration properties file.

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Export
/tmp/bin/noi_def_values.props
```

4. Go to the directory where you generated the NOI Shared Configuration properties file and open it for editing.
5. Create a backup copy of the generated NOI Shared Configuration properties file.
6. Using the editor of your choice open the generated NOI Shared Configuration properties file for editing.
7. Using the information about the event pattern creation properties described in Table 22 on page 192, specify values appropriate to your environment. Remember that the following properties have default values that you should not change:
  - type.resourcelist
  - type.servername.column
  - type.serverserial.column
8. After specifying appropriate values to the event pattern creation properties, write and then quit the NOI Shared Configuration properties file.
9. To update the values that you specified for the event pattern creation properties in the default NOI Shared Configuration properties file, run the following command:

```
./nci_trigger <server_name> <UserID>/<password> NOI_DefaultValues_Configure
FILENAME <Full Path to the file name><name_of_propsfile>
```

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Configure
FILENAME /tmp/bin/noi_def_values.props
```

## Example

The following example sets the Event Identity, defines a set of events, and finds the type information in the specified table column or columns in the Event History database:

```
type_number_of_type_configurations=1
type.0.eventid=NODE,SUMMARY,ALERTGROUP
type.0.eventtype=ACMEType
type.0.filterclause=Vendor = 'ACME'
type.0.osfilterclause=Vendor = 'ACME'
```

More specifically, the examples shows that if there is an event and the value for Vendor for that event is ACME, then look in the table column called ACMEType to find the event type.

The following example expands on the previous example by showing two configurations (as indicated by the value 2 in the type\_number\_of\_type\_configurations property:

```
type_number_of_type_configurations=2
type.0.eventid=NODE
type.0.eventtype=ACMEType
type.0.filterclause=Vendor = 'ACME'
type.0.osfilterclause=Vendor = 'ACME'
```

```
type.1.eventid=NODE,SUMMARY,ALERTGROUP
type.1.eventtype=TAURUSType
type.1.filterclause=Vendor = 'TAURUS'
type.1.osfilterclause=Vendor = 'TAURUS'
```

**Note:** Netcool/Impact attempts to match each event to the filter defined in configuration 0 first. If the event matches the filter defined in configuration 0, then Netcool/Impact defines the event's type as defined in the filter. If the event does not match the filter defined in configuration 0, Netcool/Impact attempts to match the event to the filter defined in configuration 1. If the event matches the filter defined in configuration 1, then Netcool/Impact defines the event's type as defined in the filter. Netcool/Impact continues this processing sequence for as many configuration types you define.

If no events match the filters defined in the defined configuration types you define, Netcool/Impact uses the default configuration to determine where type and identity are to be found.

---

## Reference

Review reference information for Event Analytics.

### Netcool/Impact installation components

Select the components of Netcool/Impact that you want to install.

If you purchased IBM Netcool Operations Insight the Impact Server Extensions component is displayed in the list and is selected automatically. This component contains extra Impact Server features that work with IBM Netcool Operations Insight.

If you accept the default selection, both the GUI Server and the Impact Server are installed on the same computer. In a production environment, install the Impact Server and the GUI Server on separate computers. So, for example, if you already installed the Impact Server on another computer, you can choose to install the GUI Server alone.

The component Installation Manager is selected automatically on the system that is not already installed with Installation Manager.

Netcool/Impact does not support Arabic or Hebrew, therefore Event Analytics users, who are working in Arabic or Hebrew, see some untranslated English text.

### Configuring the Event Analytics ObjectServer

You must run SQL to update the Event Analytics ObjectServer for the Related Events function.

#### About this task

The SQL provides commands for creating and modifying ObjectServer objects and data. Complete the following steps to run the SQL to update the ObjectServer.

#### Procedure

1. Copy the SQL file `IMPACT_HOME/add-ons/RelatedEvents/db/relatedevents_objectserver.sql` from Netcool/Impact into the `tmp` directory on your ObjectServer.

2. Run the SQL against your ObjectServer, enter the following command.  
 On Windows, enter the command %OMNIHOME%\..\bin\redist\isql -U <username> -P <password> -S <server\_name> < C:\tmp\relatedevents\_objectserver.sql  
 On Linux and UNIX, enter the command \$OMNIHOME/bin/nco\_sql -user <username> -password <password> -server <server\_name> < /tmp/relatedevents\_objectserver.sql
3. If you have not previously configured the Event Analytics ObjectServer, you must enter the following command.  
 On Windows, enter the command %OMNIHOME%\..\bin\redist\isql -U <username> -P <password> -S <server\_name> < C:\tmp\relatedevents\_objectserver.sql  
 On Linux and UNIX, enter the command \$OMNIHOME/bin/nco\_sql -user <username> -password <password> -server <server\_name> < /tmp/relatedevents\_objectserver.sql
4. All users must run the SQL against your ObjectServer, enter the following command.  
 On Windows, enter the command %OMNIHOME%\..\bin\redist\isql -U <username> -P <password> -S <server\_name> < C:\tmp\relatedevents\_objectserver\_update\_fp5.sql  
 On Linux and UNIX, enter the command \$OMNIHOME/bin/nco\_sql -user <username> -password <password> -server <server\_name> < /tmp/relatedevents\_objectserver\_update\_fp5.sql

## What to do next

Event correlation for the related events function in Event Analytics, uses a ParentIdentifier column that is added to the ObjectServer. If the size of this identifier field changes in your installation, you must change the value of the ParentIdentifier column within the ObjectServer SQL file that creates the event grouping automation relatedevents\_objectserver.sql, to ensure that both values are the same. The updated SQL is automatically picked up.

### Related tasks:

“Installing Netcool/OMNIbus and Netcool/Impact” on page 40

## Configuring Oracle database connection within Impact

You can configure a connection to a valid Oracle database from within IBM Tivoli Netcool/Impact.

### Before you begin

To use Oracle as the archive database, you must set up a remote connection to Netcool/Impact. For more information, see “Netcool/Impact remote connection” on page 206.

### About this task

Users can run seasonality event reports and related event configurations, specifying the time range and name with Oracle. Complete the following steps to configure the ObjectServer data source or data type.

## Procedure

1. Log in to the Netcool/Impact UI.  
`https://impacthost:port/ibm/console`
2. Configure the ObjectServer data source and data type.
  - a. In the Netcool/Impact UI, from the list of available projects, select the **NOI project**.
  - b. Select the **Data Model** tab, and select **ObjectServerForNOI**.
    - 1) Click **Edit** and enter information for `<username>`, `<password>`, `<host name>`, and `<port>`.
    - 2) Save the Netcool/Impact data source. Click **Test Connection**, followed by the **Save** icon.
  - c. Edit the data type. Expand the data source **ObjectServerForNOI** and edit the data type to correspond to the ObjectServer event history database type. For example, `AlertsForNOITable`.
  - d. For Base Table, select `<database table>`.
  - e. To update the schema and table, click **Refresh** and then click **Save**.
  - f. Select the **Data Model** tab, and select **ObjectServerHistoryOrclForNOI**.
    - 1) Click **Edit** and enter information for `<username>`, `<password>`, `<host name>`, `<port>`, and `<sid>`.
    - 2) Save the Netcool/Impact data source. Click **Test Connection**, followed by the **Save** icon.
  - g. Edit the data type. Expand the data source **ObjectServerHistoryOrclForNOI** and edit the `AlertsHistoryOrclTable` data type.
  - h. For Base Table, select `<database name>` and `<database table name>`.
  - i. To update the schema and table, click **Refresh** and then click **Save**.
  - j. Select the **Services** tab and ensure that following services are started:
    - ProcessRelatedEvents
    - ProcessSeasonalityEvents
    - ProcessRelatedEventConfig
3. Configure the report generation to use the Oracle database. Export the default properties, change the default configuration, and update the properties.
  - a. Generate a properties file. Go to the `<Impact install location>/bin` directory to locate the `nci_trigger` utility, and run the following command from the command-line interface:

```
nci_trigger <server> <username>/<password> NOI_DefaultValues_Export
FILENAME directory/filename
```

Where

`<server>`

The server where Event Analytics is installed.

`<user name>`

The user name of the Event Analytics user.

`<password>`

The password of the Event Analytics user.

`directory`

The directory where the properties file is stored.

*filename*

The name of the properties file.

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Export
FILENAME /tmp/seasonality.props
```

- b. You need to modify the property values that are overwritten by the generated properties file. For a full list of properties, see “Generated properties file” on page 206.
  - If you do not have the following values for these properties, update your properties file to reflect these property values:

```
history_datasource_name=ObjectServerHistory0rc1ForNOI
history_datatype_name=AlertsHistory0rc1Table
history_database_table=<database table name>
history_database_type=Oracle
```
  - Enter the following value, which is the Oracle database timestamp format from the policy, to the `history_db_timestampformat` property:

```
history_db_timestampformat=yyyy-mm-dd hh24:mi:ss
```

**Note:** The `history_db_timestampformat` property delivers with the properties file with a default value of `yyyy-MM-dd HH:mm:ss.SSS`. This default timestamp format for the `history_db_timestampformat` property does not work with Oracle. Thus, you need to perform the previous step to change the default value to the Oracle database timestamp format from the policy (`yyyy-mm-dd hh24:mi:ss`).

- c. Import the modified properties file into Netcool/Impact using the following command:

```
nci_trigger <Server> <username>/<password> NOI_DefaultValues_Configure
FILENAME directory/filename
```

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Configure
FILENAME /tmp/seasonality.props
```

## Configuring DB2 database connection within Impact

You can configure a connection to a valid DB2 database from within IBM Tivoli Netcool/Impact.

### About this task

Users can run seasonality event reports and related event configurations, specifying the time range and name with DB2. Complete the following steps to configure the ObjectServer data source or data type.

### Procedure

1. Log in to the Netcool/Impact UI.

```
https://impacthost:port/ibm/console
```
2. Configure the ObjectServer data source and data type.
  - a. In the Netcool/Impact UI, from the list of available projects, select the **NOI project**.
  - b. Select the **Data Model** tab and select **ObjectServerForNOI**.
    - 1) Click **Edit** and enter information for `<username>`, `<password>`, `<host name>`, `<port>`.



- 2) To save the Netcool/Impact data source, click **Test Connection**, followed by the **Save** icon.
  - c. Edit the data type. Expand the data source and edit the data type to correspond to the ObjectServer event history database type. For example, AlertsForNOITable
  - d. For Base Table, select *<database table>*.
  - e. To update the schema and table, click **Refresh** and then click **Save**.
  - f. Select the **Data Model** tab and select **ObjectServerHistoryDB2ForNOI**.
    - 1) Click **Edit** and enter information for *<username>*, *<password>*, *<host name>*, *<port>*.
    - 2) To save the Netcool/Impact data source, click **Test Connection**, followed by the **Save** icon.
  - g. Edit the data type. Expand the **ObjectServerHistoryDB2ForNOI** data source and edit AlertsHistoryDB2Table.
  - h. For Base Table, select *<database name>* and *<database table name>*
  - i. To update the schema and table, click **Refresh** and then click **Save**.
  - j. Select the **Services** tab and ensure that the following services are started.
    - ProcessRelatedEvents
    - ProcessSeasonalityEvents
    - ProcessRelatedEventConfig
3. Configure the DB2 database connection within Netcool/Impact if it was previously configured for Oracle or MSSQL. The following steps configure the report generation to use the DB2 database. Export the default properties, change the default configuration, and update the properties.
- a. Generate a properties file, go to the *<Impact install location>/bin* directory to locate the nci\_trigger, and run the following command from the command-line interface.
 

```
nci_trigger <server> <username>/<password> NOI_DefaultValues_Export
FILENAME directory/filename
```

where

*<server>*  
The server where Event Analytics is installed.

*<user name>*  
The user name of the Event Analytics user.

*<password>*  
The password of the Event Analytics user.

*directory*  
The directory where the file is stored.

*filename*  
The name of the properties file.

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Export
FILENAME /tmp/seasonality.props
```
  - b. Update the properties file. Some property values are overwritten by the generated properties file, you might need to update other property values in the generated properties file. For a full list of effected properties, see “Generated properties file” on page 206.

- If you do not have the following parameter values, update your properties file to reflect these parameter values.
 

```
history_datasource_name=ObjectServerHistoryDB2ForNOI
history_datatype_name=AlertsHistoryDB2Table
history_database_table=<database table name>
history_database_type=DB2
```
- c. Import the modified properties file into Netcool/Impact, enter the following command.
 

```
nci_trigger <Server> <username>/<password> NOI_DefaultValues_Configure
FILENAME <directory/filename>
```

For example:

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Configure
FILENAME /tmp/seasonality.props
```

#### Related tasks:

“Installing Netcool/OMNIbus and Netcool/Impact” on page 40

## Configuring MS SQL database connection within Impact

You can configure a connection to a valid MS SQL database from within IBM Tivoli Netcool/Impact.

### Before you begin

MS SQL support requires, at minimum, IBM Tivoli Netcool/Impact 7.1.0.1.

To use MS SQL as the archive database, you must set up a remote connection to Netcool/Impact. For more information, see “Netcool/Impact remote connection” on page 206.

### About this task

Users can run seasonality event reports and related event configurations, specifying the time range and name with MS SQL. Complete the following steps to configure the ObjectServer data source and data type.

### Procedure

1. Log in to the Netcool/Impact UI.
 

```
https://impacthost:port/ibm/console
```
2. Configure the ObjectServer data source and data type.
  - a. In the Netcool/Impact UI, from the list of available projects, select the **NOI project**.
  - b. Select the **Data Model** tab and select **ObjectServerForNOI**.
    - 1) Click **Edit** and enter the following information **<username>**, **<password>**, **<host name>**, **<port>**.
    - 2) Save the Netcool/Impact data source. Click **Test Connection**, followed by the **Save** icon.
  - c. Edit the data type, expand the data source and edit the data type to correspond to the ObjectServer event history database type. For example, **AlertsForNOITable**
  - d. For Base Table, select **<database table>**.
  - e. To update the schema and table, click **Refresh** and then click **Save**.
  - f. Select the **Data Model** tab and select **ObjectServerHistoryMSSQLForNOI**.

- 1) Click **Edit** and enter the following information *<username>*, *<password>*, *<host name>*, *<port>*, *<sid>*.
- 2) Save the Netcool/Impact data source. Click **Test Connection**, followed by the **Save** icon.
- g. Edit the data type. Expand the data source **ObjectServerHistoryMSSQLForNOI** and edit AlertsHistoryMSSQLTable.
- h. For Base Table, select *<database table name>*.
- i. To update the schema and table, click **Refresh** and then click **Save**.
- j. Select the **Services** tab and ensure that the following services are started.
  - ProcessRelatedEvents
  - ProcessSeasonalityEvents
  - ProcessRelatedEventConfig
3. Configure the report generation to use the MS SQL database.
  - a. Generate a properties file, go to the *<Impact install location>/bin* directory to locate the nci\_trigger and in the command-line interface enter the following command.
 

```
nci_trigger <server> <username>/<password> NOI_DefaultValues_Export
FILENAME directory/filename
```

    - <server>*  
The server where Event Analytics is installed.
    - <user name>*  
The user name of the Event Analytics user.
    - <password>*  
The password of the Event Analytics user.
    - directory*  
The directory where the file is stored.
    - filename*  
The name of the properties file.

For example, `./nci_trigger NCI impactadmin/impactpass  
NOI_DefaultValues_Export FILENAME /tmp/seasonality.props.`

- b. Update the properties file. Some property values are overwritten by the generated properties file, you might need to update other property values in the generated properties file. For a full list of effected properties, see “Generated properties file” on page 206.
  - If you do not have the following parameter values, update your properties file to reflect these parameter values.
 

```
history_datasource_name=ObjectServerHistoryMSSQLForNOI
history_datatype_name=AlertsHistoryMSSQLTable
history_database_table=<database table name>
history_database_type=MSSQL
```
- c. Import the modified properties file into Netcool/Impact, enter the command.
 

```
nci_trigger <Server> <username>/<password> NOI_DefaultValues_Configure
FILENAME directory/filename
```

For example,

```
./nci_trigger NCI impactadmin/impactpass NOI_DefaultValues_Configure
FILENAME /tmp/seasonality.props
```

## Netcool/Impact remote connection

DB2 is the default archive database. To use Oracle or MS SQL as the archive database, you must set up a remote connection to Netcool/Impact.

### About this task

The IBM Dashboard console Netcool/Impact connection should use HTTPS.

### Procedure

1. Log in to the IBM Dashboard console. If you fail to connect to the Dashboard console, ensure that the firewall on your computer is disabled.
2. Click the **Console** icon.
3. Select **Connections**.
4. Click the **Create new remote provider** icon.
5. Enter the Netcool/Impact UI server *Host name*, *Port*, *Name* and *Password*.
6. Click **Search**.
7. Select **Impact\_NCICLUSTER** as your data provider.
8. Click **OK**.

## Generated properties file

Overwritten property values can be updated in the generated properties file.

You can edit the generated properties file to set up and customize Netcool/Impact for seasonal events and related events. The following properties are in the generated properties file.

```
#
#####
NOI Shared Configuration
#####
#
If you are updating the Rollup configuration, go to
The end of the file
Following section holds the configuration for accessing
Alerts historical information and storing results
history_datasource_name Contains the Impact datasource name
history_datatype_name Contains the Impact datatype name
history_database_type Contains the Impact datasource type (DB2, Oracle, MSSQL)
history_database_table Contains the database table and if required, the schema,
to access the event history
results_database_type Contains the database type for storing results.
#
Most likely you do not have to change this configuration
#
history_datasource_name=ObjectServerHistoryDB2ForNOI
history_datatype_name=AlertsHistoryDB2Table
history_database_table=DB2INST1.REPORTER_STATUS
history_database_type=DB2
#
#
results_database_type=DERBY
#
Column name for the analysis
#
history_column_names_analysis=SUMMARY
#
The column name where the timestamp associated with the records is stored
#
```

```

history_column_name_timestamp=FIRSTOCCURRENCE
#
#
#
history_db_timestampformat=yyyy-MM-dd HH:mm:ss.SSS
configuration_db_timestampformat=yyyy-MM-dd HH:mm:ss.SSS
#
#####
Seasonality Only Configuration
#####
#
Will only save and process events of this confidence level or higher
#
save_event_threshold=.85
#
Used in determining the confidentiality level ranges, by determining the
threshold values.
level_threshold_high Level is high, when confidentiality is greater than
or equal to
level_threshold_medium Level is medium, when confidentiality is greater
than or equal to
level_threshold_low Level is low, when confidentiality is greater than or
equal to
If the confidentiality doesn't meet any of these conditions, level will be
set to unknown.
#
level_threshold_high=99
level_threshold_medium=95
level_threshold_low=0
#
Rollup configuration adds additional information to the Seasonal Report data
number_of_rollup_configuration Contains the number of additional rollup
configuration
rollup_ <number where its 1 to n >_column_name Contains the column name from
which the data is retrieved
rollup_ <number where its 1 to n >_type Contains the type value
rollup_ <number where its 1 to n >_display_name A name that needs to be
defined in the UI
Types can be defined as follows :
MAX, MIN, SUM, NON_ZERO, DISTINCT and EXAMPLE
MAX: The maximum value observed for the column, if no value is ever seen
this will default to Integer.MIN_VALUE
MIN: The minimum value observed for the column, if no value is ever seen
this will default to Integer.MAX_VALUE
SUM: The sum of the values observed for the column.
NON_ZERO: A counting column, that counts "Non-Zero"/"Non-Blank"
occurrences of events, this can be useful to
track the proportion of events that have been actioned,
or how many events had a ticket number associated
with them.
DISTINCT: The number of distinct values that have been seen for this key,
value pair
EXAMPLE: Show the first non-blank "example" of a field that contained this
key, useful when running seasonality on a
non-digestible field such as ALERT_IDENTIFIER, and you want an
example human readable
SUMMARY to let you understand the type of problem
#
number_of_rollup_configuration=2
rollup_1_column_name=SEVERITY
rollup_1_type=MIN
rollup_1_display_name=MINSeverity
rollup_2_column_name=SEVERITY
rollup_2_type=MAX
rollup_2_display_name=MAXSeverity
#
#####

```

```

Related Events Only Configuration
#####
#
Rollup configuration adds additional information to the Related Events data
reevent_number_of_rollup_configuration Contains the number of additional
rollup configuration
reevent_rollup_ <number where its 1 to n >_column_name Contains the column
name from which the data is retrieved
reevent_rollup_ <number where its 1 to n >_type Contains the type value
reevent_rollup_ <number where its 1 to n >_display_name A name that needs
to be defined in the UI
reevent_rollup_ <number where its 1 to n >_actionable Numeric only column
that determines the weight for probable root cause
Types can be defined as follows :
MAX, MIN, SUM, NON_ZERO, DISTINCT and EXAMPLE
MAX: The maximum value observed for the column, if no value is ever
seen this will default to Integer.MIN_VALUE
MIN: The minimum value observed for the column, if no value is ever
seen this will default to Integer.MAX_VALUE
SUM: The sum of the values observed for the column.
NON_ZERO: A counting column, that counts "Non-Zero"/"Non-Blank"
occurrences of events, this can be useful to
track the proportion of events that have been actioned, or
how many events had a ticket number associated
with them.
DISTINCT: The number of distinct values that have been seen for this
key, value pair
EXAMPLE: Show the first non-blank "example" of a field that contained
this key, useful when running Seasonality on a
non-digestible field such as ALERT_IDENTIFIER, and you want
an example human readable
SUMMARY to let you understand the type of problem
#
reevent_number_of_rollup_configuration=3
reevent_rollup_1_column_name=ORIGINALSEVERITY
reevent_rollup_1_type=MAX
reevent_rollup_1_display_name=MAXSeverity
reevent_rollup_1_actionable=true
reevent_rollup_2_column_name=ACKNOWLEDGED
reevent_rollup_2_type=NON_ZERO
reevent_rollup_2_display_name=Acknowledged
reevent_rollup_2_actionable=true
reevent_rollup_3_column_name=ALERTGROUP
reevent_rollup_3_type=EXAMPLE
reevent_rollup_3_display_name=AlertGroup
reevent_rollup_3_actionable=false
#
Group Information adds additional group information under the Show Details ->
Group More Information portion of the UI
reevent_num_groupinfo Contains the number of group information columns to
display
reevent_groupinfo_ <number where its 1 to n >_column Contains the column
name from which the data is retrieved
The following columns are allowed :
PROFILE, EVENTIDENTITIES, INSTANCES, CONFIGNAME, TOTALEVENTS,
UNIQUEEVENTS, REVIEWED, GROUPTTL
PROFILE: The relationship profile, or strength of the group.
EVENTIDENTITIES: A comma separated list that creates the event identity.
INSTANCES: The total number of group instances.
CONFIGNAME: The configuration name the group was created under.
TOTALEVENTS: The total number of events within the group.
UNIQUEEVENTS: The total number of unique events within the group.
REVIEWED: Whether the group has been reviewed by a user or not.
GROUPTTL: The number of seconds the group will stay active after the
first event occurs.
#
reevent_num_groupinfo=3

```

```

reevent_groupinfo_1_column=PROFILE
reevent_groupinfo_2_column=EVENTIDENTITIES
reevent_groupinfo_3_column=INSTANCES
#
Event Information adds additional event information under the Show Details ->
Event More Information portion of the UI
reevent_num_eventinfo Contains the number of event information columns to
display
reevent_eventinfo_ <number where its 1 to n >_columnContains the column name
from which the data is retrieved
The following columns are allowed :
PROFILE, INSTANCES, EVENTIDENTITY, EVENTIDENTITIES, CONFIGNAME, and GROUPNAME
PROFILE: The relationship profile, or strength of the related event.
INSTANCES: Total number of instance for the related event.
EVENTIDENTITY: The unique event identity for the related event.
EVENTIDENTITIES: A comma separated list that creates the event identity.
CONFIGNAME: The configuration name the related event was created under.
GROUPNAME: The group name the related event is created under.
#
reevent_num_eventinfo=1
reevent_eventinfo_1_column=INSTANCES
#
#####
NOI Shared Configuration
#####
#
If you are updating the Rollup configuration, go to
The end of the file
Following section holds the configuration for accessing
Alerts historical information and storing results
history_datasource_name Contains the Impact datasourcename
history_datatype_name Contains the Impact datatype name
history_database_type Contains the Impact datasource type (DB2, Oracle, MSSQL)
history_database_table Contains the database table and if required, the schema,
to access the event history
results_database_type Contains the database type for storing results.
#
Most likely you do not have to change this configuration
#
history_datasource_name=ObjectServerHistoryDB2ForNOI
history_datatype_name=AlertsHistoryDB2Table
history_database_table=DB2INST1.REPORTER_STATUS
history_database_type=DB2
#
#
#
results_database_type=DERBY
#
Column name for the analysis
#
history_column_names_analysis=SUMMARY
#
The column name where the timestamp associated with the records is stored
#
history_column_name_timestamp=FIRSTOCCURRENCE
#
#
#
history_db_timestampformat=yyyy-MM-dd HH:mm:ss.SSS
configuration_db_timestampformat=yyyy-MM-dd HH:mm:ss.SSS
#
#####
Seasonality Only Configuration
#####
#
Will only save and process events of this confidence level or higher
#

```

```

save_event_threshold=.85
#
Used in determining the confidentiality level ranges, by determining the
threshold values.
level_threshold_high Level is high, when confidentiality is greater than
or equal to
level_threshold_medium Level is medium, when confidentiality is greater
than or equal to
level_threshold_low Level is low, when confidentiality is greater than or
equal to
If the confidentiality doesn't meet any of these conditions, level will be
set to unknown.
#
level_threshold_high=99
level_threshold_medium=95
level_threshold_low=0
#
Rollup configuration adds additional information to the Seasonal Report data
number_of_rollup_configuration Contains the number of additional rollup
configuration
rollup_ <number where its 1 to n >_column_name Contains the column name from
which the data is retrieved
rollup_ <number where its 1 to n >_type Contains the type value
rollup_ <number where its 1 to n >_display_name A name that needs to be
defined in the UI
Types can be defined as follows :
MAX, MIN, SUM, NON_ZERO, DISTINCT and EXAMPLE
MAX: The maximum value observed for the column, if no value is ever seen
this will default to Integer.MIN_VALUE
MIN: The minimum value observed for the column, if no value is ever seen
this will default to Integer.MAX_VALUE
SUM: The sum of the values observed for the column.
NON_ZERO: A counting column, that counts "Non-Zero"/"Non-Blank"
occurrences of events, this can be useful to
track the proportion of events that have been actioned,
or how many events had a ticket number associated
with them.
DISTINCT: The number of distinct values that have been seen for this key,
value pair
EXAMPLE: Show the first non-blank "example" of a field that contained this
key, useful when running seasonality on a
non-digestible field such as ALERT_IDENTIFIER, and you want an
example human readable
SUMMARY to let you understand the type of problem
#
number_of_rollup_configuration=2
rollup_1_column_name=SEVERITY
rollup_1_type=MIN
rollup_1_display_name=MINSeverity
rollup_2_column_name=SEVERITY
rollup_2_type=MAX
rollup_2_display_name=MAXSeverity
#
#####
Related Events Only Configuration
#####
#
Rollup configuration adds additional information to the Related Events data
reevent_number_of_rollup_configuration Contains the number of additional
rollup configuration
reevent_rollup_ <number where its 1 to n >_column_name Contains the column
name from which the data is retrieved
reevent_rollup_ <number where its 1 to n >_type Contains the type value
reevent_rollup_ <number where its 1 to n >_display_name A name that needs
to be defined in the UI
reevent_rollup_ <number where its 1 to n >_actionable Numeric only column
that determines the weight for probable root cause

```



```

Types can be defined as follows :
MAX, MIN, SUM, NON_ZERO, DISTINCT and EXAMPLE
MAX: The maximum value observed for the column, if no value is ever
seen this will default to Integer.MIN_VALUE
MIN: The minimum value observed for the column, if no value is ever
seen this will default to Integer.MAX_VALUE
SUM: The sum of the values observed for the column.
NON_ZERO: A counting column, that counts "Non-Zero"/"Non-Blank"
occurrences of events, this can be useful to
track the proportion of events that have been actioned, or
how many events had a ticket number associated
with them.
DISTINCT: The number of distinct values that have been seen for this
key, value pair
EXAMPLE: Show the first non-blank "example" of a field that contained
this key, useful when running Seasonality on a
non-digestible field such as ALERT_IDENTIFIER, and you want
an example human readable
SUMMARY to let you understand the type of problem
#
reevent_number_of_rollup_configuration=3
reevent_rollup_1_column_name=ORIGINALSEVERITY
reevent_rollup_1_type=MAX
reevent_rollup_1_display_name=MAXSeverity
reevent_rollup_1_actionable=true
reevent_rollup_2_column_name=ACKNOWLEDGED
reevent_rollup_2_type=NON_ZERO
reevent_rollup_2_display_name=Acknowledged
reevent_rollup_2_actionable=true
reevent_rollup_3_column_name=ALERTGROUP
reevent_rollup_3_type=EXAMPLE
reevent_rollup_3_display_name=AlertGroup
reevent_rollup_3_actionable=false
#
Group Information adds additional group information under the Show Details ->
Group More Information portion of the UI
reevent_num_groupinfo Contains the number of group information columns to
display
reevent_groupinfo_ <number where its 1 to n >_columnContains the column
name from which the data is retrieved
The following columns are allowed :
PROFILE, EVENTIDENTITIES, INSTANCES, CONFIGNAME, TOTALEVENTS,
UNIQUEEVENTS, REVIEWED, GROUPTTL
PROFILE: The relationship profile, or strength of the group.
EVENTIDENTITIES: A comma separated list that creates the event identity.
INSTANCES: The total number of group instances.
CONFIGNAME: The configuration name the group was created under.
TOTALEVENTS: The total number of events within the group.
UNIQUEEVENTS: The total number of unique events within the group.
REVIEWED: Whether the group has been reviewed by a user or not.
GROUPTTL: The number of seconds the group will stay active after the
first event occurs.
#
reevent_num_groupinfo=3
reevent_groupinfo_1_column=PROFILE
reevent_groupinfo_2_column=EVENTIDENTITIES
reevent_groupinfo_3_column=INSTANCES
#
Event Information adds additional event information under the Show Details ->
Event More Information portion of the UI
reevent_num_eventinfo Contains the number of event information columns to
display
reevent_eventinfo_ <number where its 1 to n >_columnContains the column name
from which the data is retrieved
The following columns are allowed :
PROFILE, INSTANCES, EVENTIDENTITY, EVENTIDENTITIES, CONFIGNAME, and GROUPNAME
PROFILE: The relationship profile, or strength of the related event.

```

```

INSTANCES: Total number of instance for the related event.
EVENTIDENTITY: The unique event identity for the related event.
EVENTIDENTITIES: A comma separated list that creates the event identity.
CONFIGNAME: The configuration name the related event was created under.
GROUPNAME: The group name the related event is created under.
#
reevent_num_eventinfo=1
reevent_eventinfo_1_column=INSTANCES
#
#####
The following properties are used to configure event pattern creation
type.resourcelist=<columns include information. Comma separated list >
type.servername.column=<SERVERNAME column name if different than default>
type.serverserial.column=<SERVERSERIAL column name if different than default>
type.default.eventid=<default event identities when there is no match
found in the types configuration. Comma separated list
The id should not include a timestamp component.
type.default.eventtype=<default event type when there is no match
found in the types configuration.
type index starts with 0
type_number_of_type_configurations=number of type configurations
type.index.eventid=event identity column name
type.index.eventtype=event column includes the type to use
type.index.filterclause=History DB filter to filter events to find the types
type.index.osfilterclause=ObjectServer filter tp filter matching events types
##
##
NOTE : It is recommended to create database index(s) on the reporter status
table for the fields used in the filtercaluse to speed the query(s).
Example to create an index:
create index types_index on db2inst1.reporter_stuats (Severity)
##
##
#Use the following as an example creating one type only ##
##
#type_number_of_type_configurations=1 ##
#type.0.eventid=NODE,SUMMARY,ALERTGROUP ##
#type.0.eventtype=ACMEType ##
#type.0.filterclause=Vendor = 'ACME' ##
#type.0.osfilterclause=Vendor = 'ACME' ##
#####
type.resourcelist=NODE
type.default.eventid=IDENTIFIER
type.default.eventtype=ALERTGROUP
type.servername.column=SERVERNAME
type.serverserial.column=SERVERSERIAL

type_number_of_type_configurations=1
type.0.eventid=SUMMARY
type.0.eventtype=ALERTGROUP
type.0.filterclause=Severity >=3
type.0.osfilterclause=Severity >=3

```

## Adding a cluster to the Netcool/Impact environment

If you add a cluster to the Netcool/Impact environment, you must update the data sources in IBM Tivoli Netcool/Impact.

### About this task

Update the following data sources when you add a cluster to the Netcool/Impact environment.

```

seasonalReportDataSource
RelatedEventsDataSource

```

Complete the following steps to update the data sources.

## Procedure

1. In Netcool/Impact, go to the **Database Failure Policy**.
2. Select *Fail over* or *Fail back* depending on the high availability type you want. For more information, see the failover and failback descriptions.
3. Go to **Backup Source**.
4. Enter the secondary Impact Server's Derby *Host Name*, *Port*, and *Database* information.

### Standard failover

Standard failover is a configuration in which an SQL database DSA switches to a secondary database server when the primary server becomes unavailable and then continues by using the secondary until Netcool/Impact is restarted.

### Failback

Failback is a configuration in which an SQL database DSA switches to a secondary database server when the primary server becomes unavailable and then tries to reconnect to the primary at intervals to determine whether it returned to availability.

## What to do next

If you encounter error ATKRST132E, see details in “Troubleshooting Event Analytics” on page 215

If you want your Netcool/Impact cluster that is processing events to contain the same cache and update the cache, at or around the same time, you must run the file `relatedevents_objectserver.sql` with `nco_sql`. The `relatedevents_objectserver.sql` file contains the following commands.

```
create database relatedevents;
create table relatedevents.cacheupdates persistent (name varchar (20) primary key,
updates integer);
insert into relatedevents.cacheupdates (name, updates) values ('RE_CACHE', 0);
```

## Extra failover capabilities

Related events use standard ObjectServer components to provide a high availability solution. These ObjectServer components require extra configuration to ensure high availability where there is an ObjectServer pair and the primary ObjectServer goes down before the cache on the Netcool/Impact node refreshes.

In this scenario, if you deploy a correlation rule, the rule is picked up if you have replication setup between the ObjectServer tables. Otherwise, the new rule is not picked up and this state continues until you deploy another new rule. Complete the following steps to setup replication between the ObjectServer tables.

- In the `.GATE.map` file, add the following lines.

```
CREATE MAPPING RE_CACHMAP
(
 'name' = '@name' ON INSERT ONLY,
 'updates' = '@updates'
);
```

- If your configuration does not use the standard StatusMap file, add the following line to the StatusMap file that you use to control alerts.status, you can find the StatusMap file in the .tblrep.def file.

```
'ParentIdentifier' = '@ParentIdentifier'
```

- In the .tblrep.def file, add the following lines.

```
REPLICATE ALL FROM TABLE 'relatedevents.cacheupdates'
USING map 'RE_CACHEMAP';
```

For more information about adding collection ObjectServers and display ObjectServers to your environment, see the following topics within IBM Knowledge Center for IBM Tivoli Netcool/OMNIBus, <http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html?lang=en>.

*Setting up the standard multitiered environment*

*Configuring the bidirectional aggregation ObjectServer Gateway*

*Configuring the unidirectional primary collection ObjectServer Gateway*

## Viewing historical events in the Event Viewer

You can view historical events in the Event Viewer.

### About this task

To view historical events in the Event Viewer, you must create a connection to the historical database in IBM Tivoli Netcool/Impact. Complete the following steps.

### Procedure

1. Log in to the Netcool/Impact GUI and select the **NOI project**.
2. Select the **Data Model** tab, and click the **New Data Source** icon.
3. Point to **Database SQL** and select your database type. For example, DB2.
4. In the **Data Source Name** field, enter historicalEventsDatasource.
5. Enter your user name and password in the fields that are provided and click the **Save** icon.
6. In the navigation pane, right-click **historicalEventsDatasource** and select **New Data Type**.
7. In the **Data Type Name** field, enter historicalEventData.
8. Enable the **Access the data through UI data provider** check box.
9. Click **Refresh** and the table description is updated.
10. From the table description, select at least one field as the key field. Then, click the **Save** icon.
11. Within IBM Tivoli Netcool/OMNIBus Web GUI, use the Event Viewer personalize screen to change the data provider for the Event Viewer. For more information about customizing event displays in the Web GUI, see [http://www-01.ibm.com/support/knowledgecenter/SSSHTQ\\_8.1.0/com.ibm.netcool\\_OMNIBus.doc\\_8.1.0/webtop/wip/task/web\\_cust\\_jsel\\_settingportletpreferences.html](http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIBus.doc_8.1.0/webtop/wip/task/web_cust_jsel_settingportletpreferences.html).

## Understanding the timeline chart

Event information in the Related Event Details portlet is available in chart format.

You can use the Related Event Details portlet to view more information about related events. For example, you can view charted event information on a timeline chart. For more information about how to view the charted event information, see “Switching between tabulated and charted event information” on page 176

The timeline chart shows the event distribution for each event type in the group, relative to the pivot event. The pivot event is always at zero seconds, minutes, or hours.

Each comb in the timeline chart represents an event type and the teeth represent the number of instances of the event type. The blue event markers represent all the times the event occurred relative to the pivot event. The red event markers indicate the time that the event occurred in the selected group instance.

---

## Troubleshooting Event Analytics

Use the following troubleshooting information to resolve problems with your Event Analytics configuration.

### Improving Event Analytics performance due to large search results

If you are performing an upgrade of Event Analytics from an earlier version, the upgrade repopulates the existing data from the previous version and aligns this data with the new schema, tables, and views. It is possible that you might see degradation in the performance of Event Analytics operations. Examples of degradation in performance include but are not limited to:

- Reports can hang.
- Reports complete, but no data is displaying for seasonal events.

To improve any degradation in the performance of Event Analytics operations due to the upgrade to 1.3.1 or later releases, run the SE\_CLEANUPDATA policy as follows:

1. Log in to the server where IBM Tivoli Netcool/Impact is stored and running. You must log in as the administrator (that is, you must be assigned the ncw\_analytics\_admin role).
2. Navigate to the policies tab and search for the SE\_CLEANUPDATA policy.
3. Open this policy by double-clicking it.
4. Select to run the policy by using the run button on the policy screen toolbar.

The SE\_CLEANUPDATA policy cleans up the data. Specifically, the SE\_CLEANUPDATA policy:

- Does not remove or delete any data from the results tables. The results tables hold all the original information about the analysis.
- Provides some additional views and tables on top of the original tables to enhance performance.
- Combines some information from related events, seasonal events, rules, and statistics.
- Cleans up only the additional tables and views.

## **The Seasonal Event Report stops running before completion.**

The Seasonal Event Report does not complete running. No errors are displayed. The report progress does not increase.

This problem occurs if a Seasonal Event Report is running when the Netcool/Impact back-end server goes offline while the Impact UI server is still available. No errors are displayed in the Impact UI and no data is displayed in the widgets/dashboards.

To resolve this problem, ensure that the Netcool/Impact servers are running. Edit and rerun the Seasonal Event Report.

## **The Netcool/Impact back-end server fails when you run multiple Seasonal Event Reports**

The Seasonal Event Reports do not complete running. No errors are displayed. The report progress does not increase.

This problem occurs when multiple Seasonal Event Reports are run simultaneously without increasing the default heap size settings for Netcool/Impact. The default heap size setting for Netcool/Impact is 1200 MB. If the heap size is exceeded, the Netcool/Impact back-end server fails.

To resolve this problem, increase the heap size settings. As a guideline, increase the heap size settings to 80% of the free memory on your system.

For more information, see the *Increasing the memory for the Java virtual machine on the Impact profile* and *Setting the memory for the Java virtual machine on the Impact profile* Netcool/Impact topics. You can access these publications from the IBM Tivoli Network Management IBM Knowledge Center (<http://www-01.ibm.com/support/knowledgecenter/SSSHYH/welcome>).

## **Error displaying Seasonal Event Graphs in Microsoft Internet Explorer browser**

The Seasonal Event Graphs do not display in a Microsoft Internet Explorer browser.

This problem happens because Microsoft Internet Explorer requires the Microsoft Silverlight plug-in to display the Seasonal Event Graphs.

To resolve this problem, install the Microsoft Silverlight plug-in.

## **Submitted Seasonal Event Report remains at 0%**

The Seasonal Event Report does not run. It remains at 0%.

This problem occurs when Event Analytics cannot access the ProcessSeasonalityEvents Service. You cannot create a Seasonal Event Report without access to the ProcessSeasonalityEvents Service.

To resolve this issue, ensure that the ProcessSeasonalityEvents Service is running on the Impact Server.

## Creating a Seasonal Event Report displays error message Error creating report. Seasonality configuration is invalid

The Seasonal Event Report does not run. An error message is displayed.

Error creating report.

Seasonality configuration is invalid. Verify settings and retry.

This problem occurs when Event Analytics is not correctly configured before you run a Seasonal Event Report.

To resolve this problem, review the Event Analytics installation and configuration guides to ensure that all of the prerequisites and configuration steps are complete. Also, if you use a table name that is not the standard REPORTER\_STATUS, you must verify the settings that are documented in the following configuration topics.

“Configuring DB2 database connection within Impact” on page 202

“Configuring Oracle database connection within Impact” on page 200

“Configuring MS SQL database connection within Impact” on page 204

## Missing Event Analytics files and directories

The stand-alone Netcool/Impact GUI server contains incorrect column names and untranslated text strings.

This problem occurs when a stand-alone Netcool/Impact GUI server is installed. Some of the Event Analytics files and directories are not installed correctly.

To resolve this problem, copy the files and directories in the following directory in the backend server to the stand-alone Netcool/Impact GUI server:

`$IMPACT_HOME/uiproviderconfig`

## The seasonality report times out when you use large data sets

Before the seasonality policy starts to process a report, the seasonality policy issues a database query to find out how many rows of data need to be processed. This database query has a timeout when the database contains many rows and the database is not tuned to process the query. Within the `<impact install>/logs/impact_server.log` file, the following message is displayed.

```
02 Sep 2014 13:00:28,485 ERROR [JDBCVirtualConnectionWithFailOver] JDBC Connection
Pool recieved
error trying to connect to data source at: jdbc:db2://localhost:50000/database
02 Sep 2014 13:02:28,500 ERROR [JDBCVirtualStatement] JDBC execute failed twice.
com.micromuse.common.util.NetcoolTimeoutException: TransBlock [Executing SQL query:
select count(*)
as COUNT from DBINST1.PRU_REPORTER where ((Severity >= 4) AND (FIRSTOCCURRENCE >
'2007-
09-02 00:00:00.000')) AND (FIRSTOCCURRENCE < '2014-09-02 00:00:00.000')] timed
out after
120000ms.
```

Check that you have indexes for the FIRSTOCCURRENCE field and any additional filter fields that you specified, for example, Severity. Use a database tuning utility, or refresh the database statistics, or contact your database administrator for help. Increase the impact.server timeout to a value greater than the default of 120s, see <http://www-01.ibm.com/support/docview.wss?uid=swg21621488>.

## The seasonality report stays at 0% complete and does not progress

Within `<install>/impact/logs/NCO_policylogger.log`, the following trace entry is visible with no latter trace entries.

```
12 Sep 2014 11:23:08,817: [ConfigureResults][pool-3-thread-18]Parser log: About to Add a new Data
```

This problem occurs if the seasonality services are not started.

To resolve this problem, complete the following steps.

1. In the Netcool/Impact UI, select the **Seasonality** project.
2. Within the **Seasonality** project, select the **Services** tab.
3. In the **Services** tab, start the following policies.

StartSeasonalityProcessing

ProcessSeasonalityEvents

## Seasonality reports or related events configurations hang, with error ATKRST132E logged

When you start cluster members, replication starts and the Netcool/Impact database goes down. Any running seasonality reports or related events configurations hang and this error message is logged in the Netcool/Impact server log.

```
ATKRST132E An error occurred while transferring a request to the following remote provider: 'Impact_NCICLUSTER.server.company.com'. Error Message is 'Cannot access data provider - Impact_NCICLUSTER.server.company.com'.
```

To resolve this problem, do a manual restart or a scheduled restart of the affected reports or configurations.

## Within the event viewer, you are unable to view seasonal events and error ATKRST103E is logged

When you complete the following type of steps, then within the event viewer the seasonal events are not viewable and error ATKRST103E is logged.

1. Open the event viewer and select to edit the widget from the widget menu.
2. From the list on the edit screen, select the Impact Cluster data provider.
3. Select to view either the seasonality report and the report name.
4. Save the configuration.

To resolve the problem, view seasonal events by using the provided seasonal events pages and view related events parent to child relationships by using the Tivoli Netcool/OMNIBus data provider.

## Configuring Netcool/Impact for ObjectServer failover

Netcool/Impact does not process new events for Event Analytics after ObjectServer failover. Seasonal event rule actions are not applied if the Netcool/Impact server is not configured correctly for ObjectServer failover as new events are processed. For example, if a seasonal event rule creates a synthetic event, the synthetic event does not appear in the event list, or if a seasonal event rule changes the column value for an event, the value is unchanged.



This problem occurs when Netcool/Impact is incorrectly configured for ObjectServer failover.

To resolve this problem, extra Netcool/Impact configuration is required for ObjectServer failover. To correctly configure Netcool/Impact, complete the steps in the *Managing the OMNIBusEventReader with an ObjectServer pair for New Events or Inserts* topic in the Netcool/Impact V 7.1.0.3 documentation: [https://www-01.ibm.com/support/knowledgecenter/SSSHYH\\_7.1.0.3/com.ibm.netcoolimpact.doc/common/dita/ts\\_serial\\_value\\_omnibus\\_eventreader\\_failover\\_failback.html](https://www-01.ibm.com/support/knowledgecenter/SSSHYH_7.1.0.3/com.ibm.netcoolimpact.doc/common/dita/ts_serial_value_omnibus_eventreader_failover_failback.html)

When configured, Netcool/Impact uses the failover ObjectServer to process the event.

### **Update the Seasonal Event date range after you upgrade from 7.1.0.2 to 7.1.0.3 or later**

After you upgrade from 7.1.0.2 to 7.1.0.3 or later for Netcool/Impact and web GUI, you must update the seasonal event configuration date range. In 7.1.0.2 a seasonal event configuration has a fixed date range. In 7.1.0.3 or later, the default date range is relative.

To update the date range after you upgrade to 7.1.0.3 or later, complete the following steps:

- Select the seasonal event configuration in the Configure Analytics portlet.
- Click the fixed date range radio button.
- Click **Save** to save the configuration without running, or **Save & Run** to save and run the configuration.

The correct fixed date range values are imported from 7.1.0.2.

### **Seasonal report missing information after you upgrade to Netcool/Impact 7.1.0.3 or later**

After you upgrade from Netcool/Impact 7.1.0.1 and 7.1.0.2 to Netcool/Impact 7.1.0.3 or later, information is missing from columns in the group table in the **View Seasonal Events** portlet.

Information is missing from specific columns in the group table that is displayed in the **View Seasonal Events** portlet after you upgrade. The information that is missing in 7.1.0.3 or later was not displayed in earlier versions of Netcool/Impact and Netcool Operations Insight.

To display the missing information in the columns, rerun the migrated configuration in the latest build.

**Note:** Rerunning the migrated configuration in the latest build overwrites data that existed for the previously run configuration.

### **Unable to create patterns for configurations created before you upgraded to Netcool Operations Insight 1.4.0.1 or later**

Configurations that are created before you upgrade to Netcool Operations Insight 1.4.0.1 or later used the override global event identity setting, which is defined in the analytics configuration file. You cannot create patterns for groups in this analytics configuration.

After you upgrade to Netcool Operations Insight 1.4.0.1 or later, ensure that the event history database is indexed based on the SERVERSERIAL and SERVERNAME, or equivalent used, fields. If the historical database is created from the default historical database, the index is in place.

To apply patterns to existing configurations, re-create the configurations in Netcool Operations Insight 1.4.0.1 or later using the original configuration settings and the global event identity.

### **Warning message related to configuring seasonality event analytics**

When you are configuring an event configuration and seasonality event analytics is enabled, the following warning message appears in the log file.

WARNING: Follow this instruction: This error is after the analysis is done. The last step is to reinsert the data for UI views.

You login to the Impact UI, go to the Policies tab, and execute the following policy:

```
SE_CLEANUPDATA
```

Following these steps corrects the error and reinserts the data.

Typically, the previous warning message appears in the log file when the seasonality configuration is complete and an error occurred.

To correct the error and reinsert the data, run the SE\_CLEANUPDATA policy as follows.

**Note:** Before you run the SE\_CLEANUPDATA policy, it is recommended that you increase the value specified for the `impact.server.timeout` property defined in the `$IMPACT_HOME/etc/ServerName_server.props` properties file. Specifically, replace `impact.server.timeout=120000` with `impact.server.timeout=3600000`. The value 3600000 allows for 60 minutes to give more time for the Apache Derby database to work in the complex query. You will need to restart the Netcool/Impact server after you edit the `impact.server.timeout` property.

1. Log in to the server where IBM Tivoli Netcool/Impact is stored and running. You must log in as the administrator (that is, you must be assigned the `ncw_analytics_admin` role).
2. Navigate to the policies tab and search for the SE\_CLEANUPDATA policy.
3. Open this policy by double-clicking it.
4. Select to run the policy by using the run button on the policy screen toolbar.

The SE\_CLEANUPDATA policy cleans up the data. Specifically, the SE\_CLEANUPDATA policy:

- Does not remove or delete any data from the results tables. The results tables hold all the original information about the analysis.
- Provides some additional views and tables on top of the original tables to enhance performance.
- Combines some information from related events, seasonal events, rules, and statistics.
- Cleans up only the additional tables and views.

## Unable to run SE\_CLEANUPDATA policy

If the Netcool/Impact server timeout is reached when you are running a seasonality report, the following message displays on the Configure Analytics portlet:

Finished with Errors

If you then try to run the SE\_CLEANUPDATA policy, the policy locks on the Netcool/Impact server. To work around this issue, you must manually unlock the file that contains the SE\_CLEANUPDATA policy. Then, run the SE\_CLEANUPDATA policy again. To unlock the SE\_CLEANUPDATA policy, follow these steps:

1. Log in to the server where IBM Tivoli Netcool/Impact is stored and running. You must log in as the administrator (that is, you must be assigned the ncw\_analytics\_admin role).
2. Navigate to the policies tab and search for the SE\_CLEANUPDATA policy.
3. Right-click the SE\_CLEANUPDATA policy and select unlock from the drop-down menu.

## No type configuration found error message

After you upgrade Event Analytics to IBM Netcool Operations Insight 1.4.0.1, you can use the pattern generalization feature in Event Analytics. To use the pattern generalization feature in Event Analytics, you must configure the type properties used for event pattern creation in IBM Tivoli Netcool/Impact. If you do not configure the type properties for event pattern creation in IBM Tivoli Netcool/Impact, any attempts to create and run a configuration causes the following error message to display:

No type configuration found

For more information about configuring the type properties that are used for event pattern creation in IBM Tivoli Netcool/Impact, see “Configuring the type properties used for event pattern creation in Netcool/Impact” on page 192.

## The pattern displays 0 groups and 0 events

The events pattern that is created and displayed in the Group Sources table in the View Related Events portlet displays 0 groups and 0 events

The pattern displays 0 groups and 0 events for one of the following reasons.

- The pattern creation process is not finished. The pattern creation process can take a long time to complete due to large datasets and high numbers of suggested patterns.
- The pattern creation process was stopped before it completed.

To confirm the reason that the pattern displays 0 groups and 0 events, complete the following steps.

1. To confirm that the process is running,
  - a. Append the policy name to the policy logger file from the **Services** tab, **Policy Logger** service. For more information about configuring the Policy logger, see Configuring the Policy logger service.
  - b. Check the following log file.  
\$IMPACT\_HOME/logs/<serverName>\_policylogger\_PG\_ALLOCATE\_PATTERNS\_GROUPS.log

If the log file shows that the process is running, wait for the process to complete. If the log file shows that the process stopped without completing, proceed to step 2.

2. To force reallocation for all configurations and patterns run the `PG_ALLOCATE_PATTERNS_GROUPS_FORCE` from Global projects policy with no parameters from the UI.
3. Monitor the `$IMPACT_HOME/logs/<serverName>_policylogger_PG_ALLOCATE_PATTERNS_GROUPS_FORCE.log` log file to track the completion of the process.

## Incomplete, stopped, and uninitiated configurations

Configurations do not complete, are stalled on the Configure Analytics portlet, or fail to start.

These problems occur if the services are not started after Event Analytics is installed, or the Netcool/Impact server is restarted.

To resolve these problems, complete the following steps.

1. In the Netcool/Impact UI, select the **Impact Services** tab.
2. Ensure that each of the following services is started. To start a service, right-click the service and select **Start**.
  - ProcessClosedPatternInstances
  - ProcessPatternGroupsAllocation
  - ProcessRelatedEventConfig
  - ProcessRelatedEventPatterns
  - ProcessRelatedEventTypes
  - ProcessRelatedEvents
  - ProcessSeasonalityAfterAction
  - ProcessSeasonalityConfig
  - ProcessSeasonalityEvents
  - ProcessSeasonalityNonOccurrence
  - UpdateSeasonalityExpiredRules

## Event Analytics: Reports fail to run due to event count queries that take too long.

Reports fail to run due to large or unoptimized datasets that cause the Netcool/Impact server to timeout and reports fails to complete.

To resolve this issue, increase the Netcool/Impact server timeout value to ensure that the Netcool/Impact server processes these events before it times out. As a result of increasing this server timeout value, the Netcool/Impact server waits for the events to be counted, thus ensuring that the reports complete and display in the appropriate portlet.

Edit the Netcool/Impact `impact.server.timeout` value, at `$IMPACT_HOME/etc/ServerName_server.props`

By default, the `impact.server.timeout` property is set to 120000 milliseconds, which is equal to 2 minutes. The recommendation is to specify a server timeout value of at least 5 minutes. If the issue continues, increase the server timeout value

until the reports successfully complete and display in the appropriate portlet.

## Backup the Apache Derby database before upgrading to Event Analytics 1.4.0.1

Before you upgrade Event Analytics to Netcool Operations Insight 1.4.0.1, create a backup of the Apache Derby database.

To back up the Apache Derby database, complete the following steps.

1. Stop the ImpactDatabase service.
2. Back up the files from the `$NCHOME/db/<SERVER_NAME>/derby` directory.
3. Start the ImpactDatabase service again.

To restore the Apache Derby database from a backup file, complete the following steps.

1. Stop the ImpactDatabase service. Make a copy of the existing ImpactDB database before you restore the backup file.
2. Copy the backup file to the `$NCHOME/db/<SERVER_NAME>/derby` directory.
3. Start the ImpactDatabase service again.

To restore an older version of the Apache Derby database, after a failure complete the following steps, based on the upgrade version.

1. Change to the following directory:  
`cd $IMPACT_HOME/add-ons/NOI/db`
2. List the files that reside in the `$IMPACT_HOME/add-ons/NOI/db` directory. For example:

```
ls
.
.
.
noi_derby_updatefp03.sql
noi_derby_updatefp04.sql
noi_derby_updatefp05.sql
noi_derby_upgrade_71fp2.sql
.
.
.
```

3. Make backup copies to each file before editing.
4. Using a text editor, open each file for editing and find the following line:

```
connect 'jdbc:derby://__PRIMARY_HOST__:__
PRIMARY_PORT__/
__PRIMARY_DB__';
user=__DBUSER__;password=__DBPASSWORD__';
```

5. Change the connection parameters in each of the files.
6. Write and close each file.
7. Run the following command:

```
$IMPACT_HOME/bin/nci_db connect -sqlfile <one of the sql files>
```

**Note:** You execute all previous versions of the files until Fix Pack 5 as follows:

- `noi_derby_upgrade_71fp2.sql` -- Start here if you are upgrading Fix Pack 1.
- `noi_derby_updatefp03.sql` -- Start here if you are upgrading Fix Pack 2.
- `noi_derby_updatefp04.sql` -- Start here if you are upgrading Fix Pack 3.
- `noi_derby_updatefp05.sql`

8. Restart the Netcool/Impact server.

### **Event pattern with the same criteria already exists (error message)**

An error message is displayed if you create a pattern that has a duplicate pattern criteria selected. Check the following log file to determine which pattern is the duplicate:

```
$IMPACT_HOME/logs/<serverName>_policylogger_PG_SAVEPATTERN.log
```

## **Event relationships display in the Event Viewer, only if the parent and child events match the filter**

The Event Viewer is only able to show relationships between events if the parent and the child events are all events that match the filter. There are some use cases for related events where parent or child events might not match the filter.

### **Background**

Netcool/OMNIbus Web GUI is able to show the relationships between events in the Event Viewer, if the Event Viewer view in use has an associated Web GUI relationship. This relationship defines which field in an event contains the identifier of the event's parent, and which field contains the identifier for the current event. For more information about defining event relationships, see [http://www-01.ibm.com/support/knowledgecenter/SSSHTQ\\_8.1.0/com.ibm.netcool\\_OMNIbus.doc\\_8.1.0/webtop/wip/task/web\\_cust\\_jsel\\_evtrelationshipmanage.html](http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_8.1.0/com.ibm.netcool_OMNIbus.doc_8.1.0/webtop/wip/task/web_cust_jsel_evtrelationshipmanage.html).

The relationship function works from the set of events that are included in the event list, and the event list displays the events that match the relevant Web GUI filter. See the following example. If you have a filter that is called *Critical* to show all critical events, the filter clause is *Severity = 5*, then relationships between these events are shown provided the parent and child events in the relationships all have *Severity = 5*. If you have a parent event that matches the filter *Severity = 5* but has relationships to child events that have a major severity *Severity = 4*, these child relations are not seen in the event list because the child events do not match the filter. Furthermore, these child relations are not included in the set of events that are returned to the Event Viewer by the server.

### **Resolution**

To resolve this problem, you must define your filter with appropriate filter conditions that ensures that related events are included in the data that is returned to the Event Viewer by the server. See the following example, this example builds on the example that is used in the *Background* section.

1. Make a copy of the *Critical* filter and name the copy *CriticalAndRelated*. You now have two filters. Use the original filter when you want to see only critical events. You use the new filter to see related events, even if events are not critical.
2. Manually modify the filter condition of the *CriticalAndRelated* filter to include the related events. To manually modify this filter condition, use the advanced mode of the Web GUI filter builder. The following example conditions are based on the current example.

The main filter condition is *Severity = 5*.

In an event, the field that denotes the identifier of the parent event is called `ParentSerial`.

The value of the `ParentSerial` field, where populated, is the `Serial` of an event.

If `ParentSerial` is 0, this value is a default value and does not reference another event.

- Including related child events. To include events that are the immediate child events of events that match the main filter, set this filter condition.

```
Severity = 5
```

```
OR
```

```
ParentSerial IN (SELECT Serial FROM alerts.status WHERE Severity = 5)
```

- Including related parent events. To include events that are the immediate parent of events that match the main filter, set this filter condition.

```
Severity = 5
```

```
OR
```

```
Serial IN (SELECT ParentSerial from alerts.status WHERE Severity = 5)
```

- Including related sibling events. To include events that are the other child events of the immediate parents of the event that matches the main filter (the siblings of the events that match the main filter), set this filter condition.

```
Severity = 5
```

```
OR
```

```
ParentSerial IN (SELECT ParentSerial from alerts.status WHERE
Severity = 5 AND ParentSerial > 0)
```

- Including related parents, children, and siblings together. Combine the previous types of filter conditions so that the new `CriticalAndRelated` filter retrieves critical events, and the immediate children of the critical events, and the immediate parents of the critical events, and the immediate children of those parent events (the siblings). You must have this filter condition.

```
Severity = 5
```

```
OR
```

```
ParentSerial IN (SELECT Serial FROM alerts.status WHERE Severity = 5)
```

```
OR
```

```
Serial IN (SELECT ParentSerial from alerts.status WHERE Severity = 5)
```

```
OR
```

```
ParentSerial IN (SELECT ParentSerial from alerts.status WHERE
Severity = 5 AND ParentSerial > 0)
```

- Including related events that are more than one generation away. In the previous examples, the new filter conditions go up to only one level, up or down, from the initial set of critical events. However, you can add more filter conditions to retrieve events that are more than one generation away from the events that match the main filter. If you want to retrieve grandchildren of the critical events (that is, two levels down from the events that match the main filter condition) and immediate children, set this filter condition.

```
-- The initial set of Critical events
```

```
Severity = 5
```

```
OR
```

```
-- Children of the Critical events
```

```
ParentSerial IN (SELECT Serial FROM alerts.status WHERE Severity = 5)
```

```
-- Children of the previous "child events"
```

```
OR
```

```
ParentSerial IN (SELECT Serial FROM alerts.status WHERE
```

```
 ParentSerial IN (SELECT Serial FROM alerts.status WHERE Severity = 5))
```

Use a similar principal to retrieve parent events that are two levels up, and siblings of the parent events. To pull this scenario together, set this filter condition.

```

-- The initial set of Critical events
Severity = 5

OR

-- Children of the Critical events
ParentSerial IN (SELECT Serial FROM alerts.status WHERE
Severity = 5)

OR

-- Children of the previous "child events"
ParentSerial IN (SELECT Serial FROM alerts.status WHERE
 ParentSerial IN (SELECT Serial FROM alerts.status WHERE
Severity = 5))

OR

-- Parents of the Critical events
Serial IN (SELECT ParentSerial from alerts.status WHERE Severity = 5)

OR

-- Parents of the previous "parent events"
Serial IN (SELECT ParentSerial from alerts.status WHERE
 Serial IN (SELECT ParentSerial from alerts.status WHERE Severity = 5))
OR

-- Other children of the Critical events' parents
ParentSerial IN (SELECT ParentSerial from alerts.status WHERE
Severity = 5 AND ParentSerial > 0)

OR

-- Other children of the Critical events' grandparents
ParentSerial IN (SELECT ParentSerial from alerts.status WHERE
 Serial IN (SELECT ParentSerial from alerts.status WHERE
Severity = 5 AND ParentSerial > 0) AND ParentSerial > 0)

```

You can continue this principal to go beyond two levels in the hierarchy. However, with each additional clause the performance of the query degrades due to the embedded subquerying. Therefore, there might be a practical limit to how far away the related events can be.



---

## IBM Networks for Operations Insight

Networks for Operations Insight adds network management capabilities to the Netcool Operations Insight solution. These capabilities provide network discovery, visualization, event correlation and root-cause analysis, and configuration and compliance management that provide service assurance in dynamic network infrastructures. It contributes to overall operational insight into application and network performance management.

For documentation that describes how to install Networks for Operations Insight, see “Performing a fresh installation” on page 32. For documentation that describes how to upgrade from an existing Networks for Operations Insight, or transition to Networks for Operations Insight, see “Upgrading to the latest Netcool Operations Insight” on page 87.

### Before you begin

The Networks for Operations Insight capability is provided through setting up the following products in Netcool Operations Insight:

- Network Manager, see [http://www-01.ibm.com/support/knowledgecenter/SSSHRK/landingpage/product\\_welcome\\_itnm.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK/landingpage/product_welcome_itnm.html)
- Netcool Configuration Manager, see <http://www-01.ibm.com/support/knowledgecenter/SS7UH9/welcome>

In addition, you can optionally add on performance management capability by setting up the Network Performance Insight product and integrating it with Netcool Operations Insight. Performance management capability includes the ability to display and drill into performance anomaly and flow data. For more information on Network Performance Insight, see <https://www.ibm.com/support/knowledgecenter/SSCVHB>.

---

## Network Health Dashboard

Use the Network Health Dashboard to monitor a selected network view, and display availability, performance, and event data, as well as configuration and event history for all devices in that network view.

### Administering the Network Health Dashboard

Perform these tasks to configure and maintain the Network Health Dashboard for users.

#### Before you begin

Device configuration change data can only be displayed in the Configuration and Event Timeline if the integration with Netcool Configuration Manager has been set up. For more information on the integration with Netcool Configuration Manager, see the following topic in the Network Manager Knowledge Center: [http://www-01.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/install/task/nmip\\_con\\_configintegrationwithncm.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/install/task/nmip_con_configintegrationwithncm.html)

## About this task

**Note:** The minimum screen resolution for display of the Network Health Dashboard is 1536 x 864. If your screen is less than this minimum resolution, then you will see scroll bars on one or more of the widgets in the Network Health Dashboard.

## Configuring the Network Health Dashboard

As an administrator, you can configure how data is displayed, and which data is displayed in the Network Health Dashboard.

## About this task

To fit the quantity of widgets onto a single screen, customers need a minimum resolution of 1536 x 864, or higher.

As an administrator, you can configure the Network Health Dashboard in a number of ways to meet the needs of your operators.

### Changing the layout of the dashboard

You can change the layout of the dashboard. For example, you can reposition, or resize widgets. For more information, see the following topic on the Network Manager Knowledge Center: [http://www-01.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/isc/edit\\_page.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/isc/edit_page.html)

### Change the refresh period for all widgets on the Network Health Dashboard

The Network Manager widgets within the Network Health Dashboard update by default every 20 seconds. You can change this update frequency by performing the following steps.

**Note:** The Event Viewer widget updates every 60 seconds by default.

1. Edit the the following configuration file: `$NMGUI_HOME/profile/etc/tnm/nethealth.properties`.
2. Find the following line and update the refresh period to the desired value in seconds.  
`nethealth.refresh.period=60`
3. Save the file.
4. Close and reopen the Network Health Dashboard tab to put the changes into effect.

### Change the colors associated with event severity values used in the Configuration and Event Timeline

You can update the colors associated with event severity values used in the Configuration and Event Timeline, by performing the following steps:

1. Edit the following configuration file: `$NMGUI_HOME/profile/etc/tnm/status.properties`.
2. Find the properties `status.color.background.severity_number`, where *severity\_number* corresponds to the severity number. For example 5 corresponds to Critical severity.
3. Change the RGB values for the severity values, as desired.
4. Save the file.

### Disable launch of the Network View tab when selecting a network view in the Network Health Dashboard

When a user selects a network view in the Network Health Dashboard, by default a second tab is opened, called "Network View". This tab contains a

dashboard comprised of the Network Views GUI, the **Event Viewer**, and the Structure Browser, and displaying the selected network view. If your network views are very large, then displaying this second tab can have an impact on system performance. To avoid this performance impact, you can disable the launch of the Network View tab by performing the following steps:

1. Edit the following configuration file: `$NMGUI_HOME/profile/etc/tnm/topoviz.properties`.
2. Find the following lines:  

```
Defines whether the dashboard network view tree fires a launchPage
event when the user clicks a view in the tree
topoviz.networkview.dashboardTree.launchpage.enabled=true
```
3. Set the property  
`topoviz.networkview.dashboardTree.launchpage.enabled` to `false`.
4. Save the file.

## Troubleshooting the Network Health Dashboard

Use this information to troubleshoot the Network Health Dashboard.

### Network Health Dashboard log files:

Review the Network Health Dashboard log files to support troubleshooting activity.

The Network Health Dashboard log files can be found at the following locations:

*Table 23. Locations of Network Health Dashboard log files*

| File       | Location                                                         |
|------------|------------------------------------------------------------------|
| Log file   | <code>\$NMGUI_HOME/profile/logs/tnm/ncp_nethealth.0.log</code>   |
| Trace file | <code>\$NMGUI_HOME/profile/logs/tnm/ncp_nethealth.0.trace</code> |

### Data sources for the Network Health Dashboard widgets:

Use this information to understand from where the Network Health Dashboard widgets retrieve data. This information might be useful for troubleshooting data presentation issues in the Network Health Dashboard.

### Configuration and Event Timeline widget

This widget is populated by the following integrations:

- Tivoli Netcool/OMNIBus integration that analyzes Tivoli Netcool/OMNIBus events and shows a count based on event severity in a specified period.
- Netcool Configuration Manager integration that retrieves configuration change distribution.

### Percentage Availability widget

The data source for this widget is the historical poll data table `pdEwmaForDay`. The widget displays data from the device poll `PingResult` from the `pdEwmaForDay` table, scoped as follows:

- Scope is the selected network view if called from the Network Health Dashboard
- Scope is the in-context devices or interfaces if called from a right-click command within a topology map.

**Note:** The widget is updated only at the end of the hour to which the data applies.

### **Top Performers widget**

The data sources for this widgets are the various historical poll data tables:

- pdEwmaForDay
- pdEwmaForWeek
- pdEwmaForMonth
- pdEwmaForYear

The scope of the data is as follows:

- Scope is the selected network view if called from the Network Health Dashboard
- Scope is the in-context devices or interfaces if called from a right-click command within a topology map.

### **Unavailable Resources widget**

This widget is populated by a Tivoli Netcool/OMNIBus integration that analyzes Tivoli Netcool/OMNIBus events and uses the event data to determine whether a device or interface is affected, and whether the issue is ICMP or SNMP-based.

### **Investigating data display issues in the Network Health Dashboard:**

If any of the widgets in the Network Health Dashboard are not displaying data, this could mean that there is no data to display. However, it could mean that there is an underlying problem that needs to be resolved. As an administrator, you can configure poll policies and poll definition so that users are able to display the data that they need to see in the Network Health Dashboard. You can also explore other potential underlying issues, such as problems with the underlying systems that process and store historical poll data.

### **About this task**

To configure poll policies, see the following topic in the Network Manager Knowledge Center: [http://www-01.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/poll/task/nmip\\_poll\\_creatingpollswithmultiplepolldefinitions.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/poll/task/nmip_poll_creatingpollswithmultiplepolldefinitions.html).

When editing a poll policy editor, the following operations in the Poll Policy Editor are important for determining whether data from the poll policy will be available for display in the Network Health Dashboard:

#### **Poll Enabled**

Check this option to enable the poll policy.

**Store?** Check this option to store historical data for the poll policy.

**Note:** Checking this option will activate the historical poll data storage system, which will store large amounts of data on your system. For more information on the historical poll data storage system, see the following topic in the Network Manager Knowledge Center: [http://www-01.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/poll/task/nmip\\_poll\\_administeringstorm.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/poll/task/nmip_poll_administeringstorm.html)

## Network Views

In this tab, ensure that the poll policy is active in the network views that you want to monitor in the Network Health Dashboard.

Configure poll policies as follows in order to make data available in the various widgets of the Network Health Dashboard.

For information on the different Network Manager poll policies and poll definitions, see the following topic on the Network Manager Knowledge Center: [http://www-01.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/ref/reference/nmip\\_ref\\_pollingref.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/ref/reference/nmip_ref_pollingref.html)

## Unavailable Resources widget

Configure the following poll policies in order to make data available in the Unavailable Resources widget:

Table 24. Unavailable Resources widget: which poll policies to configure

| If you want to show response data for | Then ensure that one or more of the following poll policies is enabled in the appropriate network views                                                  |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chassis devices based on ping polling | Any poll policy that uses one or more chassis ping poll definitions. An example of a poll policy of this type is the Default Chassis Ping poll policy    |
| Interfaces based on ping polling      | Any poll policy that uses one or more chassis ping poll definitions. An example of a poll policy of this type is the Default Interface Ping poll policy. |
| Chassis devices based on SNMP polling | Any poll policy that uses one or more SNMP poll definitions. An example of a poll policy of this type is the snmpInBandwidth poll policy.                |
| Interfaces based on SNMP polling      | SNMP Link State poll policy.                                                                                                                             |

## Percentage Availability widget

Enable the Default Chassis Ping poll policy in order to display overall chassis availability data in the Percentage Availability widget.

## Top Performers widget

### Metrics in the Top Performers widget

To show a specific metric in the Top Performers widget **Metric** drop-down list, you must enable the poll policy that contains a poll definition related to that metric. Alternatively, create a new poll definition and add it to an enabled poll policy.

**Note:** These must be poll definition that can be stored and that falls into one of the following types:

- Basic threshold
- Ping
- SnmpLinkState

For example, using the default poll policies and poll definitions provided with Network Manager, here are examples of poll policies to enable and the corresponding metric that will be made available in the **Metric** drop-down list:

Table 25. Top Performers widget: examples of poll policies to configure

| To display this metric | Enable this poll policy | Which contains this poll definition |
|------------------------|-------------------------|-------------------------------------|
| ifInDiscards           | ifInDiscards            | ifInDiscards                        |
| ifOutDiscards          | ifOutDiscards           | ifOutDiscards                       |
| snmpInBandwidth        | snmpInBandwidth         | snmpInBandwidth                     |

#### Historical poll data in the Top Performers widget

You can display historical poll data for a metric in the Top Performers widget by clicking the **Last Day**, **Last Week**, **Last Month**, and **Last Year** buttons. To collect historical poll data to display in this way, you must select the option to store historical data for the related poll definition related to the metric. For example, using the default poll policies and poll definitions provided with Network Manager, here are examples of poll definitions to configure.

**Note:** Historical data will only be viewable in the Top Performers once it has been collected, processed, and stored in the NCPOLLDATA database. For example, if at the time of reading this you had selected the option to store poll data for a poll definition one month ago, then you will only see one month's worth of data in the **Last Year** option.

Table 26. Top Performers widget: examples of poll definitions to configure

| To display historical data for this metric | Select the Store? option for this poll definition | Within this poll policy |
|--------------------------------------------|---------------------------------------------------|-------------------------|
| ifInDiscards                               | ifInDiscards                                      | ifInDiscards            |
| ifOutDiscards                              | ifOutDiscards                                     | ifOutDiscards           |
| snmpInBandwidth                            | snmpInBandwidth                                   | snmpInBandwidth         |

**Important:** If you have correctly configured storage of historical poll data for the metrics you are interested in, but when you click any of the the **Last Day**, **Last Week**, **Last Month**, and **Last Year** buttons you are not seeing any data, then there might be a problem with the underlying systems that process and store historical poll data. In particular, the Apache Storm system that processes historical poll data, might not be running, or Apache Storm might have lost connection to the NCPOLLDATA database, where historical poll data is stored. For more information, see the following topic in the Network Manager Knowledge Center: [http://www-01.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itm/ip/wip/poll/task/nmip\\_poll\\_administeringstorm.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itm/ip/wip/poll/task/nmip_poll_administeringstorm.html)

#### Configuration and Event Timeline

If a configuration with Netcool Configuration Manager was set up at installation time, but configuration change data does not appear in the Configuration and Event Timeline this might be due to integration issues. For more information on the integration with Netcool Configuration Manager, see the following topic in the Network Manager Knowledge Center: <http://www-01.ibm.com/support/knowledgecenter/>

### Top Performers widget is unable to display values greater than 32 bit:

The Top Performers widget is unable to display values greater than 32 bit. If no data is being displayed in the Top Performers widget for a selected metric, then this might be due to a number of factors. One possibility is that the value of data in that metric is greater than 32 bit.

If no data is being displayed in the Top Performers widget for a selected metric, then run the following SQL query to determine if there is an error, and if, what the error code is.

```
SELECT errorcode, value, datalabel
FROM ncpolldata.polldata pd
INNER JOIN ncpolldata.monitoredobject mo ON mo.monitoredobjectid = pd.monitoredobjectid
WHERE datalabel =poll_of_interest
```

Error codes are listed in the ERROR\_CODE values in KNP\_POLL\_DATA\_COLLECTION Support document, at the following location: <http://www-01.ibm.com/support/docview.wss?uid=swg21422092>. The error code 112 indicates that metric contains a polled value that was greater than can be stored in a 32-bit integer field.

### Percentage Availability widget takes a long time to refresh:

If the Percentage Availability widget is taking a long time to refresh then one possible solution is to increase the number of threads available for this widget. This solution is most suitable for customers with large networks.

### About this task

Increase the number of threads available by performing the following steps:

#### Procedure

1. Edit the the following configuration file: \$NMGUI\_HOME/profile/etc/tnm//nethealth.properties.
2. Find the following lines:  

```
Widget thread count for availability widget
nethealth.threads.availability=5
```
3. Increase the value of the nethealth.threads.availability property. The maximum possible value is 10.
4. Save the file.

## Developing custom dashboards

You can create pages that act as "dashboards" for displaying information on the status of parts of your network or edit existing dashboards, such as the Network Health Dashboard. You can select from the widgets that are provided with Network Manager, Tivoli Netcool/OMNIBus Web GUI, and also from other products that are deployed in your Dashboard Application Services Hub environment.

## About this task

For basic information on creating and editing pages in the Dashboard Application Services Hub see the following topic on the Network Manager Knowledge Center: [http://www-01.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/isc/edit\\_page.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/isc/edit_page.html). For more detailed information about Dashboard Application Services Hub, see the Jazz for Service Management information center at <http://www-01.ibm.com/support/knowledgecenter/SSEKCU/welcome>.

### Before you begin

- - Determine which widgets you want on the page.
  - If you want a custom Web GUI gauge on the page, develop the metric that will feed the gauge display.
  - Decide which users, groups, or user roles you want to have access to the page and assign the roles accordingly.
  - If you want the widgets to communicate in a custom wire, develop the wires that will control the communications between the widgets.

## Displaying an event-driven view of the network

You can configure a dashboard to contain a Dashboard Network Views widget and other widgets that are driven by network alert data. Under the configuration described here, when a user clicks a node in the network view tree in the Dashboard Network Views widget, the other widgets in the dashboard update to show data based on events for entities in the selected network view. This dashboard is useful for network operations centers that want to see the real-time situation on the network, as it provides a real-time view of network alerts and of the availability of devices and interfaces. No historical polling data is used by any of the widgets in this dashboard, so this provides an alternative to the Network Health Dashboard if polling data is not being stored.

### Before you begin

Depending on the requirements you have of the page, perform some or all of the tasks described in “Developing custom dashboards” on page 233.

## About this task

To develop a page that wires a Dashboard Network Views widget and other widgets that are driven by network alert data:

### Procedure

1. Log in as a user that has the iscadmins role.
2. Create the page, assign it to a location in the navigation, and specify the roles that users need to view the page. The default location is **Default**, and in this task it is assumed that this default location is used. If you use a different location, then substitute your chosen location wherever you see the location **Default** used in this task.
3. Add the Dashboard Network Views widget to the page.
4. Add the Configuration and Event Timeline to the page. If you have configured the Network Manager integration with Netcool Configuration Manager then this widget displays a timeline up to a period of 24 hours, showing



configuration change data and event data by first occurrence of the event. If you have not set up the integration, then the widget still displays event data on the timeline.

5. Add the Unavailable Resources widget to the page. This widget displays how many devices and interfaces within the selected network view are unavailable.
6. Add the Event Viewer to the page.
7. Click **Save and Exit** to save the page.

**Note:** This page does not require any wires. The Dashboard Network Views widget automatically broadcasts the NodeClickedOn event, and the other widgets automatically subscribe to this event and update their data accordingly.

## Results

You can now click a network view in the network view tree in the Dashboard Network Views widget and the other widgets automatically update to show event data:

- The Unavailable Resources widget displays a bar chart showing how many devices and interfaces within the selected network view are unavailable. The exact data shown in this widget depends on whether the following poll policies are enabled:
  - Devices: Default Chassis Ping and SNMP Poll Fail poll policies must be enabled.
  - Interfaces: Default Interface Ping and SNMP Link State poll policies must be enabled.
- The Configuration and Event Timeline displays a timeline showing events by first occurrence, and, if the Netcool Configuration Manager integration is configured, configuration change data, for all entities in the network view.
- The Event Viewer shows events for all entities in the network view.

**Note:** Clicking a bar in the Unavailable Resources widget further filters the Event Viewer to show only the availability events related to the devices or interfaces in that bar.

## Displaying and comparing top performer data for entities in a network view

Create a dashboard containing multiple Top Performers widgets to enable you to compare historical poll data across multiple entities and metrics in a selected network view. This dashboard is particularly useful for background investigation and analysis in order to determine how devices and interfaces are performing over time and whether there are any underlying issues.

### Before you begin

Depending on the requirements you have of the page, perform some or all of the tasks described in “Developing custom dashboards” on page 233.

### About this task

To develop a page that wires a Network Views widget and multiple Top Performers widgets to enable you to compare historical poll data across multiple entities and metrics in a selected network view:

## Procedure

1. Log in as a user that has the iscadmins role.
2. Create the page, assign it to a location in the navigation, and specify the roles that users need to view the page. The default location is **Default**, and in this task it is assumed that this default location is used. If you use a different location, then substitute your chosen location wherever you see the location **Default** used in this task.
3. Add the Network Views widget to the page.
4. Add two Top Performers widgets to the page.

**Note:** Adding two Top Performers widgets enables you to perform basic comparisons, such as displaying metric traces on the same device or interface over two different time periods. You can add more than two Top Performers widgets, and this will provide the ability to perform comparisons across a wider range of data; for example, adding four Top Performers widgets enables you to display metric traces on the same device or interface over four different time periods.

5. Click **Save and Exit** to save the page.

**Note:** This page does not requires any wires. The Network Views widget automatically broadcasts the NodeClickedOn event, and the other widgets automatically subscribe to this event and update their data accordingly.

## What to do next

You can use this dashboard to compare metric traces or charts.

### Example: comparing metric traces on the same device or interface over different time periods:

Use the custom dashboard that contains the two Top Performers widgets to compare metric traces on the same device or interface over different time periods; for example, you might see a spike in the current raw data trace for a metric such as snmpInBandwidth on a specific interface. To determine if this is just an isolated spike or a more serious ongoing issue, you can, on the same dashboard, also display a trace for the same snmpInBandwidth metric on the same interface over a longer time period, such as the last day or last week, and then visually determine if there have been continual incidences of high snmpInBandwidth on this interface over the last day or week.

## About this task

To use the dashboard to compare metric traces on the same device or interface over different time periods, proceed as follows:

## Procedure

1. In the Network Views widget, select a network view. The two Top Performers widgets update to show data for the selected network view.
2. From each of the Top Performers widgets, click the **Metric** drop-down list and select a metric of interest; for example snmpInBandwidth. Select the same metric on both Top Performers widgets; this ensures that the top entity in both chart is always the same.

3. In one of the Top Performers widgets, click the top bar to show the trace for the entity with the top value in that chart. This displays a time-based trace of current raw data for the snmpInBandwidth metric.
4. In the other Top Performers widget, click the top bar to show the trace for the entity with the top value in that chart. You are now showing the identical time trace in both widgets.
5. In the second Top Performers widget, change the timeframe; for example, click **Last Day**. You are now showing a current raw data trace of snmpInBandwidth data in the first widget, and a trace of the last day's worth of snmpInBandwidth data for the same interface in the second widget, and you can compare the more transient raw data in the first widget with data averages over last day.

#### **Example: comparing different metric traces on the same device or interface:**

Use the custom dashboard that contains the two Top Performers widgets to compare different metric traces on the same device or interface; for example, you might see a number of incidences of high snmpInBandwidth on a specific interface over the last day. To determine if the high incoming SNMP bandwidth usage on this interface is affecting the outgoing SNMP bandwidth usage on that same interface, you can, on the same dashboard, also display a trace for the snmpOutBandwidth metric on the same interface and also over the last day, and then visually compare the two traces.

#### **About this task**

To use the dashboard to compare different metric traces on the same device or interface, proceed as follows:

#### **Procedure**

1. In the Network Views widget, select a network view.
2. From each of the Top Performers widgets, click the **Metric** drop-down list and select a metric of interest; for example snmpInBandwidth. Select the same metric on both Top Performers widgets; this ensures that the top entity in both chart is always the same.
3. In one of the Top Performers widgets, click the top bar to show the trace for the entity with the top value in that chart. This displays a time-based trace of current raw data for the snmpInBandwidth metric.
4. In the other Top Performers widget, click the top bar to show the trace for the entity with the top value in that chart. You are now showing the identical time trace in both widgets.
5. In the second Top Performers widget, click the **Metric** drop-down list and select snmpOutBandwidth. You are now displaying a trace of incoming SNMP bandwidth usage on the interface with the highest incoming SNMP bandwidth usage in the network view on one widget, and a trace of outgoing SNMP bandwidth usage on that same interface. You can now visually compare the two traces to see if there is any correlation.

### Example: comparing different Top 10 metric charts:

Use the custom dashboard that contains the two Top Performers widgets to compare different Top 10 metric charts. This enables you to see the potential impact of one metric on another across the devices that are showing the highest performance degradation on the first metric. For example, you might want to compare the chart showing those devices showing the highest ten incoming SNMP bandwidth usage values, with the chart showing those devices showing the highest ten outgoing SNMP bandwidth usage values.

### About this task

To use the dashboard to compare different Top 10 metric charts, proceed as follows:

#### Procedure

1. In the Network Views widget, select a network view.
2. In one of the Top Performers widgets, click the **Metric** drop-down list and select a metric of interest; for example `snmpInBandwidth`. The Top Performers widget updates to show a bar chart of the ten interfaces in the network view with the highest incoming SNMP bandwidth usage values.
3. In the other Top Performers widget, click the **Metric** drop-down list and select a second metric of interest; for example `snmpOutBandwidth`. The Top Performers widget updates to show a bar chart of the ten interfaces in the network view with the highest outgoing SNMP bandwidth usage values.

### Results

You can now compare the two charts to see if there is any correlation between the data.

### Displaying network view event data in a gauge group

You can use wires to configure a Network Views widget and a Dashboard Application Services Hub gauge group to pass data between each other. Under the configuration described here, when a user clicks a node in the network view tree in the Network Views widget, the gauge group updates to show a number of status gauges: you can configure as many status gauges as desired. In the example described here, three gauges are configured: Severity 3 (minor), Severity 4 (major), and Severity 5 (critical), together with a number within each status gauge indicating how many events at that severity are currently present on the devices in that network view. The instructions in this topic describe a possible option for wiring the two widgets.

### Before you begin

Depending on the requirements you have of the page, perform some or all of the tasks described in “Developing custom dashboards” on page 233.

### About this task

To develop a page that wires a Network Views widget and a Dashboard Application Services Hub gauge group:

#### Procedure

1. Log in as a user that has the `iscadmins` role.

2. Create the page, assign it to a location in the navigation, and specify the roles that users need to view the page. The default location is **Default**, and in this task it is assumed that this default location is used. If you use a different location, then substitute your chosen location wherever you see the location **Default** used in this task.
3. Add the Network Views widget to the page.
4. Add the Dashboard Application Services Hub gauge group to the page.
5. Edit the gauge group widget.
6. Select a dataset for the gauge group. In the Gauge Group: Select a Dataset window, search for the **Netcool/OMNIBus WebGUI > All data > Filter Summary** dataset. One way to do this is as follows:
  - a. In the search textbox at the top left of the Gauge Group: Select a Dataset window, type **filter**.
  - b. Click **Search**. This search retrieves two **Filter Summary** datasets.
  - c. Select the dataset that has a provider title labeled **Provider: Netcool/OMNIBus WebGUI > Datasource: All data**.
7. Configure how you want the gauge group to be displayed. In the Gauge Group: Visualization Settings window, add three value status gauges by performing the following steps:
  - a. Click **Choose Widget** and select **ValueStatus Gauge** from the drop-down list. Then click **Add**.
  - b. Add two more **ValueStatus Gauge** widgets, following the instruction in the previous step.

There should now be three **ValueStatus Gauge** widgets listed in the **Selected Widgets** list.

8. Configure the three value status gauges to show the following:
  - First value status gauge will display the number of Severity 3 (minor) events, within the Severity 3 (minor) symbol, .
  - Second value status gauge will display the number of Severity 4 (major) events, within the Severity 4 (major) symbol, .
  - Third value status gauge will display the number of Severity 5 (critical) events, within the Severity 5 (critical) symbol, .

Perform the following steps to configure the Severity 3 (minor) value status gauge:

- a. Select the first value status gauge item in the **Selected Widgets** list.
- b. Click **Required Settings**.
- c. Click the **Value** drop-down list and select **Severity 3 Event Count** from the drop-down list.
- d. Click **Optional Settings**.
- e. Click the **Label above Gauge** drop-down list and select **Severity 3 Event Count Name** from the drop-down list.
- f. In the  **Minor** spinner set a threshold value of 0 by typing 0. This threshold value causes any number of Severity 3 (minor) events to generate a Severity 3 value status gauge.

Perform the following steps to configure the Severity 4 (major) value status gauge:

- a. Select the first value status gauge item in the **Selected Widgets** list.

- b. Click **Required Settings**.
- c. Click the **Value** drop-down list and select **Severity 4 Event Count** from the drop-down list.
- d. Click **Optional Settings**.
- e. Click the **Label above Gauge** drop-down list and select **Severity 4 Event Count Name** from the drop-down list.
- f. In the  **Major** spinner set a threshold value of 0 by typing 0. This threshold value causes any number of Severity 4 (major) events to generate a Severity 4 value status gauge.

Perform the following steps to configure the Severity 5 (critical) value status gauge:

- a. Select the first value status gauge item in the **Selected Widgets** list.
  - b. Click **Required Settings**.
  - c. Click the **Value** drop-down list and select **Severity 5 Event Count** from the drop-down list.
  - d. Click **Optional Settings**.
  - e. Click the **Label above Gauge** drop-down list and select **Severity 5 Event Count Name** from the drop-down list.
  - f. In the  **Critical** spinner set a threshold value of 0 by typing 0. This threshold value causes any number of Severity 5 (critical) events to generate a Severity 5 value status gauge.
9. Click **Save and Exit** to save the page.
  10. From the page action list, select **Edit Page**.
  11. Click **Show Wires**  and then, in the Summary of wires section of the window, click **New Wire**.
  12. Specify the wires that connect the Network Views widget to the Dashboard Application Services Hub gauge group.
    - In the Select Source Event for New Wire window, click **Network Views > NodeClickedOn**, and then click **OK**.
    - In the Select Target for New Wire window, click **Default > This page name\_of\_page > Event Viewer**, where *name\_of\_page* is the name of the page that you created in step 2.
    - In the Transformation window, select **Show Gauge Events**, and then click **OK**.
  13. Close the Summary of wires section of the window by clicking the X symbol at the top right corner.
  14. Click **Save and Exit** to save the page.

## Results

You can now click a network view in the network view tree in the Network Views widget and have the gauge group update to show three status values: Severity 3 (minor), Severity 4 (major), and Severity 5 (critical), together with a number within each status gauge indicating how many events at that severity are currently present on the devices in the selected network view.

## Event information for Network Health Dashboard widgets

Refer to this table to get information about the publish events and subscribe events for Network Health Dashboard widgets. Use this event information when you create a new custom widget and you want to wire your custom widget with an existing Network Health Dashboard widget.

Table 27. Event information for Network Health Dashboard widgets

| Widget name                      | Event type      | Event name    | Event description                                                                                                              |
|----------------------------------|-----------------|---------------|--------------------------------------------------------------------------------------------------------------------------------|
| Configuration and Event Timeline | Subscribe event | NodeClickedOn | Subscribes to a NodeClickedOn event and displays data based on the events <i>ViewId</i> and the <i>datasource</i> .            |
| Percentage Availability          | Subscribe event | NodeClickedOn | Subscribes to a NodeClickedOn event and displays data based on the events <i>ViewId</i> and the <i>datasource</i> .            |
| Network Manager Polling Chart    | Subscribe event | NodeClickedOn | Subscribes to a NodeClickedOn event and displays data based on the events <i>ViewId</i> and the <i>datasource</i> .            |
| Unavailable Resources            | Publish event   | showEvents    | Click a bar in the displayed graph and the widget publishes a showEvents event that contains the name of the transient filter. |
|                                  | Subscribe event | NodeClickedOn | Subscribes to a NodeClickedOn event and displays data based on the events <i>ViewId</i> and the <i>datasource</i> .            |

## Monitoring the network using the Network Health Dashboard

Use this information to understand how to use the Network Health Dashboard to determine if there are any network issues, and how to navigate from the dashboard to other parts of the product for more detailed information.

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. A dashboard timeline reports on device configuration changes and event counts, enabling you to correlate events with configuration changes. The dashboard includes the event viewer, for more detailed event information.

## Monitoring the Network Health Dashboard

Monitor the Network Health Dashboard by selecting a network view within your area of responsibility, such as a geographical area, or a specific network service such as BGP or VPN, and reviewing the data that appears in the other widgets on the dashboard. If you have set up a default network view bookmark that contains the network views within your area of responsibility, then the network views in that bookmark will appear in the network view tree within the dashboard.

### Before you begin

For more information about the network view tree in the Network Health Dashboard, see “Configuring the network view tree to display in the Network Health Dashboard” on page 250

### About this task

**Note:** The minimum screen resolution for display of the Network Health Dashboard is 1536 x 864. If your screen is less than this minimum resolution, then you will see scroll bars on one or more of the widgets in the Network Health Dashboard.

### Displaying device and interface availability in a network view:

Using the Unavailable Resources widget you can monitor, within a selected network view, the number of device and interface availability alerts that have been open for more than a configurable amount of time. By default this widget charts the number of device and interface availability alerts that have been open for up to 10 minutes, for more than ten minutes but less than one hour, and for more than one hour.

### About this task

To monitor the number of open device and interface availability alerts within a selected network view, proceed as follows:

#### Procedure

1. Click the **Incident** icon and select **Network Availability > Network Health Dashboard**.
2. In the Network Health Dashboard, select a network view from the network view tree in the Network Views at the top left. The other widgets update to show information based on the network view that you selected. In particular, the Unavailable Resources widget updates to show device and interface availability in the selected network view. A second tab, called "Network View", opens. This tab contains a dashboard comprised of the Network Views GUI, the **Event Viewer**, and the Structure Browser, and it displays the selected network view. You can use this second tab to explore the topology of the network view that you are displaying in the Network Health Dashboard.  
  
For information about specifying which network view tree to display in the Network Health Dashboard, see “Configuring the network view tree to display in the Network Health Dashboard” on page 250.
3. In the Unavailable Resources widget, proceed as follows:

To determine the number of unavailable devices and interface alerts, use the following sections of the chart and note the colors of the stacked bar segments and the number inside each segment.



**Restriction:** By default, all of the bars described below are configured to display. However, you can configure the Unavailable Resources widget to display only specific bars. For example, if you configure the widget to display only the **Device Ping** and the **Interface Ping** bars, then only those bars will be displayed in the widget.

**Note:** By default the data in the Unavailable Resources widget is updated every 20 seconds.

#### **SNMP Poll Fail**

Uses color-coded stacked bars to display the number of SNMP Poll Fail alerts within the specified timeframe.

#### **SNMP Link State**

Uses color-coded stacked bars to display the number of SNMP Link State alerts within the specified timeframe.

#### **Interface Ping**

Uses color-coded stacked bars to display the number of Interface Ping alerts within the specified timeframe.

#### **Device Ping**

Uses color-coded stacked bars to display the number of Device Ping alerts within the specified timeframe.

Color coding of the stacked bars is as follows:

*Table 28. Color coding in the Unavailable Resources widget*

|                                                                                     |               |                                                                                   |
|-------------------------------------------------------------------------------------|---------------|-----------------------------------------------------------------------------------|
|   | <b>Yellow</b> | Number of alerts that have been open for up to 10 minutes.                        |
|  | <b>Pink</b>   | Number of alerts that have been open for more than 10 minutes and up to one hour. |
|  | <b>Blue</b>   | Number of alerts that have been open for more than one hour.                      |

Click any one of these bars to show the corresponding alerts for the devices and interfaces in the Event Viewer at the bottom of the Network Health Dashboard.

**Note:** You can change the time thresholds that are displayed in this widget. The default threshold settings are 10 minutes and one hour. If your availability requirements are less stringent, then you could change this, for example, to 30 minutes and 3 hours. The change applies on a per-user basis. If none of the devices in the current network view is being polled by any one of these polls, then the corresponding stacked bar will always displays zero values. For example, If none of the devices in the current network view is being polled by the SNMP Poll Fail poll, then the **SNMP Poll Fail** bar will always displays zero values. If you are able to access the Configure Poll Policies panel in the Network Polling GUI, then you can use the **Device Membership** field on that table to see a list all of devices across all network views that are polled by the various poll policies.

## Displaying overall network view availability:

You can monitor overall availability of chassis devices within a selected network view using the Percentage Availability widget.

### About this task

To display overall availability of chassis devices within a selected network view, proceed as follows:

#### Procedure

1. Click the **Incident** icon and select **Network Availability > Network Health Dashboard**.
2. In the Network Health Dashboard, select a network view from the network view tree in the Network Views at the top left. The other widgets update to show information based on the network view that you selected. In particular, the Percentage Availability widget updates to show overall availability of chassis devices in network view. A second tab, called "Network View", opens. This tab contains a dashboard comprised of the Network Views GUI, the **Event Viewer**, and the Structure Browser, and it displays the selected network view. You can use this second tab to explore the topology of the network view that you are displaying in the Network Health Dashboard.

For information about specifying which network view tree to display in the Network Health Dashboard, see "Configuring the network view tree to display in the Network Health Dashboard" on page 250.

3. In the Percentage Availability widget, proceed as follows:

The Percentage Availability widget displays 24 individual hour bars. Each bar displays a value, which is an exponentially weighted moving average of ping results in the past hour; the bar only appears on the completion of the hour. The bar value represents a percentage availability rate rather than a total count within that hour. The color of the bar varies as follows:

- Green: 80% or more.
- Orange: Between 50% and 80%.
- Red: Less than 50%.

## Displaying highest and lowest performers in a network view:

You can monitor highest and lowest poll data metrics across all devices and interfaces within a selected network view using the Top Performers widget.

### About this task

To display highest and lowest poll data metrics across all devices and interfaces within a selected network view, proceed as follows:

#### Procedure

1. Click the **Incident** icon and select **Network Availability > Network Health Dashboard**.
2. In the Network Health Dashboard, select a network view from the network view tree in the Network Views at the top left. The other widgets update to show information based on the network view that you selected. In particular, the Top Performers widget updates to show overall availability of chassis devices in network view. A second tab, called "Network View", opens. This tab contains a dashboard comprised of the Network Views GUI, the **Event Viewer**,

and the Structure Browser, and it displays the selected network view. You can use this second tab to explore the topology of the network view that you are displaying in the Network Health Dashboard.

For information about specifying which network view tree to display in the Network Health Dashboard, see “Configuring the network view tree to display in the Network Health Dashboard” on page 250.

3. In the Top Performers widget, proceed as follows:

Select from the following controls to display chart, table, or trace data in the Top Performers widget.

**Metric** Click this drop-down list to display a selected set of poll data metrics. The metrics that are displayed in the drop-down list depend on which poll policies are enabled for the selected network view. Select one of these metrics to display associated data in the main part of the window.

**Order** Click this drop-down list to display what statistic to apply to the selected poll data metric.

- Statistics available for all metrics, except the SnmpLinkStatus metric.

**From Top:** Displays a bar chart or table that shows the 10 highest values for the selected metric. The devices or interfaces with these maximum values are listed in the bar chart or table.

**From Bottom:** Displays a bar chart or table that shows the 10 lowest values for the selected metric. The devices or interfaces with these minimum values are listed in the bar chart or table.

- Statistics available for the SnmpLinkStatus metric. In each case, a bar chart or table displays and shows devices for the selected statistic.

**Unavailable:** This statistic displays by default. Devices with this statistic are problematic.

**Admin Down** Devices with this statistic are not problematic as Administrators change devices to this state.

**Available** Devices with this statistic are not problematic.

**Note:** The widget lists devices or interfaces depending on which metric was selected:

- If the metric selected applies to a device, such as memoryUtilization, then the top 10 list contains devices.
- If the metric selected applies to an interface, such as ifInDiscards, then the top 10 list contains interfaces.



#### Show Chart

Displays a bar chart with the 10 highest or lowest values. Show Chart is the display option when you first open the widget.



#### Show Table

Displays a table of data associated with the 10 highest or lowest values.



#### Define Filter

This button only appears if you are in **Show Table**  mode. Click here to define a filter to apply to the Top Performers table data.

The main part of the window contains the data in one of the following formats:

- Chart** Bar chart with the 10 highest or lowest values. Click any bar in the chart to show a time trace for the corresponding device or interface.
- Table** Table of data associated with the 10 highest or lowest values. The table contains the following columns:
- **Entity Name:** Name of the device or interface.
  - **Show Trace:** Click a link in one of the rows to show a time trace for the corresponding device or interface.
  - **Last Poll Time:** Last time this entity was polled.
  - **Value:** Value of the metric the last time this entity was polled.
- Trace** Time trace of the data for a single device or interface. Navigate within this trace by performing the following operations:
- Zoom into the trace by moving your mouse wheel forward.
  - Zoom out of the trace by moving your mouse wheel backward.
  - Double click to restore the normal zoom level.
  - Click within the trace area for a movable vertical line that displays the exact value at any point in time.

Click one of the following buttons to specify which current or historical poll data to display in the main part of the window. This button updates the data regardless of which mode is currently being presented: bar chart, table, or time trace.

**Restriction:** If your administrator has opted not to store poll data for any of the poll data metrics in the **Metric** drop-down list, then historical poll data will not be available when you click any of the following buttons:

- **Last Day**
- **Last Week**
- **Last Month**
- **Last Year**

#### **Current**

Click this button to display current raw poll data. When in time trace mode, depending on the frequency of polling of the associated poll policy, the time trace shows anything up to two hours of data.

#### **Last Day**

Click this button to show data based on a regularly calculated daily average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a daily exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 24 hours is shown, based on the average values.

In the **Last Day** section of the widget EWMA values are calculated by default every 15 minutes and are based on the previous 15 minutes of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every 15 minutes.

#### **Last Week**

Click this button to show data based on a regularly calculated weekly average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a weekly exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 7 days is shown, based on the average values.

In the **Last Week** section of the widget EWMA values are calculated by default every 30 minutes and are based on the previous 30 minutes of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every 30 minutes.

#### **Last Month**

Click this button to show data based on a regularly calculated monthly average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a monthly exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 30 days is shown, based on the average values.

In the **Last Month** section of the widget EWMA values are calculated by default every two hours and are based on the previous two hours of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every two hours.

#### **Last Year**

Click this button to show data based on a regularly calculated yearly average.

- In bar chart or table mode, the top 10 highest or lowest values are shown based on a yearly exponentially weighted moving average (EWMA).
- In time trace mode, a time trace of the last 365 days is shown, based on the average values.

In the **Last Year** section of the widget EWMA values are calculated by default every day and are based on the previous 24 hours of raw poll data. The data presented in this section of the widget is then updated with the latest EWMA value every day.

### **Displaying the Configuration and Event Timeline:**

You can display a timeline showing, for all devices in a selected network view, device configuration changes and network alert data over a time period of up to 24 hours using the Configuration and Event Timeline widget. Correlation between device configuration changes and network alerts on this timeline can help you identify where configuration changes might have led to network issues.

#### **About this task**

To display a timeline showing device configuration changes and network alert data for all devices in a selected network view, proceed as follows:

#### **Procedure**

1. Click the **Incident** icon and select **Network Availability > Network Health Dashboard**.
2. In the Network Health Dashboard, select a network view from the network view tree in the Network Views at the top left. The other widgets update to

show information based on the network view that you selected. In particular, the Configuration and Event Timeline updates to show configuration change and event data for the selected network view. A second tab, called "Network View", opens. This tab contains a dashboard comprised of the Network Views GUI, the **Event Viewer**, and the Structure Browser, and it displays the selected network view. You can use this second tab to explore the topology of the network view that you are displaying in the Network Health Dashboard.

For information about specifying which network view tree to display in the Network Health Dashboard, see "Configuring the network view tree to display in the Network Health Dashboard" on page 250.

3. In the Configuration and Event Timeline widget, proceed as follows:

Configuration changes displayed in the Configuration and Event Timeline can be any of the following. Move your mouse over the configuration change bars to view a tooltip listing the different types of configuration change made at any time on the timeline.

**Note:** If you do not have Netcool Configuration Manager installed, then no configuration data is displayed in the timeline.

#### **Changes managed by Netcool Configuration Manager**

These changes are made under full Netcool Configuration Manager control. The timeline differentiates between scheduled or policy-based changes, which can be successful (Applied) or unsuccessful (Not Applied), and one-time changes made using the IDT Audited terminal facility within Netcool Configuration Manager.

##### **Applied**

A successful scheduled or policy-based set of device configuration changes made under the control of Netcool Configuration Manager.

##### **Not Applied**

An unsuccessful scheduled or policy-based set of device configuration changes made under the control of Netcool Configuration Manager.

**IDT** Device configuration changes made using the audited terminal facility within Netcool Configuration Manager that allows one-time command-line based configuration changes to devices.

#### **Unmanaged changes**

##### **OABC**

Out-of-band-change. Manual configuration change made to device where that change is outside of the control of Netcool Configuration Manager.

Events are displayed in the timeline as stacked bars, where the color of each element in the stacked bar indicates the severity of the corresponding events. Move your mouse over the stacked bars to view a tooltip listing the number of events at each severity level. The X-axis granularity for both events and configuration changes varies depending on the time range that you select for the timeline.

*Table 29. X axis granularity in the Configuration and Event Timeline*

| If you select this time range | Then the X axis granularity is |
|-------------------------------|--------------------------------|
| 6 hours                       | 15 minutes                     |

Table 29. X axis granularity in the Configuration and Event Timeline (continued)

| If you select this time range | Then the X axis granularity is |
|-------------------------------|--------------------------------|
| 12 hours                      | 30 minutes                     |
| 24 hours                      | 1 hour                         |

For more detailed information on the different types of configuration change, see the Netcool Configuration Manager knowledge center at <http://www-01.ibm.com/support/knowledgecenter/SS7UH9/welcome>.

Select from the following controls to define what data to display in the Configuration and Event Timeline.

**Time** Select the duration of the timeline:

- **6 Hours:** Click to set a timeline duration of 6 hours.
- **12 Hours:** Click to set a timeline duration of 12 hours.
- **24 Hours:** Click to set a timeline duration of 24 hours.

**Events by Occurrence**

- **First Occurrence:** Click to display events on the timeline based on the first occurrence time of the events.
- **Last Occurrence:** Click to display events on the timeline based on the last occurrence time of the events.



#### Show Table

Displays the configuration change data in tabular form. The table contains the following columns.

**Note:** If you do not have Netcool Configuration Manager installed, then this button is not displayed.

- **Number:** Serial value indicating the row number.
- **Device:** Host name or IP address of the affected device.
- **Unit of Work (UoW):** In the case of automated Netcool Configuration Manager configuration changes, the Netcool Configuration Manager unit of work under which this configuration change was processed.
- **Result:** Indicates whether the change was successful.
- **Start Time:** The time at which the configuration change began.
- **End Time:** The time at which the configuration change completed.
- **User:** The user who applied the change.
- **Description:** Textual description associated with this change.



#### Show Chart

Click here to switch back to the default graph view.

**Note:** If you do not have Netcool Configuration Manager installed, then this button is not displayed.

Use the sliders under the timeline to zoom in and out of the timeline. The legend under the timeline shows the colors used in the timeline to display the following items:

- Event severity values.
- Configuration change types.

**Note:** If the integration with Netcool Configuration Manager has been set up but there is a problem with data retrieval from Netcool Configuration Manager, then the configuration change types shown in the legend are

marked with the following icon: 

## Configuring the Network Health Dashboard

As an end user, you can configure the Network Health Dashboard to display the data you want to see.

### Configuring the network view tree to display in the Network Health Dashboard:

As a user of the Network Health Dashboard, you can configure a default bookmark to ensure that you limit the data that is displayed in the Network Health Dashboard to the network views within your area of responsibility.

#### About this task

The network views tree in the Network Health Dashboard automatically displays the network views in your default network view bookmark. If there are no network views in your default bookmark, then a message is displayed with a link to the Network Views GUI, where you can add network views to your default bookmark. The network views that you add to your default bookmark will be displayed in the network tree within the Network Health Dashboard.

Complete the following steps to add network views to your default bookmark.

#### Procedure

1. Within the displayed message, click the link that is provided. The Network Views GUI opens in a second tab.
2. Follow the instructions in the following topic in the Network Manager Knowledge Center: [http://www-01.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/visualize/task/nmip\\_vis\\_addingnetworkviewstobookmark.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/visualize/task/nmip_vis_addingnetworkviewstobookmark.html)

#### Results

The network views tree in the Network Health Dashboard displays the network views in your newly configured default bookmark.

### Configuring the Unavailable Resources widget:

As a user of the Network Health Dashboard, you can configure which availability data is displayed in the Network Health Dashboard by the Unavailable Resources widget. For example you can configure the widget to display availability data based on ping polls only, and not based on SNMP polls. You can also configure the time duration thresholds to apply to availability data displayed in this widget. For example, by default the widget charts the number of device and interface availability alerts that have been open for up to 10 minutes, more than 10 minutes, and more than one hour. You can change these thresholds.

#### About this task

To configure which availability data is displayed by the Unavailable Resources widget, proceed as follows:



## Procedure

1. Click the **Incident** icon and select **Network Availability > Network Health Dashboard**.
2. In the Unavailable Resources widget, click **User Preferences** .
3. To configure the Unavailable Resources widget, use the following checkboxes and number steppers:

### Device

Configure which device alerts to monitor in the Unavailable Resources widget in order to retrieve information on device availability. By default all of these boxes are checked.

#### Device Ping

Check the box to monitor Default Chassis Ping alerts. Selecting this option causes the Unavailable Resources widget to provide an indication of the number of open device ICMP (ping) polling alerts.

#### SNMP Poll Fail

Check the box to monitor SNMP Poll Fail alerts. Selecting this option causes the Unavailable Resources widget to provide an indication of the number of open SNMP Poll Fail alerts.

### Interface

Configure which interface alerts to monitor in the Unavailable Resources widget in order to retrieve information on interface availability. By default all of these boxes are checked.

#### Interface Ping

Check the box to monitor Default Interface Ping alerts. Selecting this option causes the Unavailable Resources widget to provide an indication of the number of open interface ICMP (ping) polling alerts.

#### Link State

Check the box to monitor SNMP Link State alerts. Selecting this option causes the Unavailable Resources widget to provide an indication of the number of open SNMP Link State alerts.

### Thresholds

**Upper** Specify an upper threshold in hours and minutes. By default, the upper threshold is set to one hour. This threshold causes the chart in the Unavailable Resources widget to update as follows: when the amount of time that any availability alert in the selected network view remains open exceeds the one hour threshold, then the relevant bar in the Unavailable Resources chart updates to show this unavailability as a blue color-coded bar section.

**Lower** Specify a lower threshold in hours and minutes. By default, the lower threshold is set to 10 minutes. This threshold causes the chart in the Unavailable Resources widget to update as follows: when the amount of time that any availability alert in the selected network view remains open exceeds the 10 minute threshold, then the relevant bar in the Unavailable Resources chart updates to show this unavailability as a as a pink color-coded bar section.

## Configuring the Configuration and Event Timeline:

You can configure which event severity values to display on the Configuration and Event Timeline.

### About this task

To configure which event severity values to display on the Configuration and Event Timeline:

### Procedure

1. Click the **Incident** icon and select **Network Availability > Network Health Dashboard**.
2. In the Configuration and Event Timeline widget, click **User Preferences** .
3. To configure the Configuration and Event Timeline, use the following lists:

#### Available Severities

By default, lists all event severity values and these event severity values are all displayed in the Configuration and Event Timeline.

To remove an item from this list, select the item and click the right-pointing arrow. You can select and move multiple values at the same time.

#### Selected Severities

By default, no event severity values are displayed in this list. Move items from the **Available Severities** list to this list to show just those values in the Configuration and Event Timeline. For example, to show only Critical and Major in the Configuration and Event Timeline, move the Critical and Major items from the **Available Severities** list to the **Selected Severities** list.

To remove an item from this list, select the item and click the left-pointing arrow. You can select and move multiple values at the same time.

---

## Device Dashboard

Use the Device Dashboard to troubleshoot network issues by navigating the network topology and seeing performance anomalies and trends on any device, link, or interface.

## Troubleshooting network issues using the Device Dashboard

Use the Device Dashboard to troubleshoot any network issue on a device, link, or interface.

## Starting the Device Dashboard

You can start the Device Dashboard from an event in the Event Viewer, from a device in the Network Views, Network Hop View, or Path Views. You can also start the Device Dashboard from the Top Performers widget within the Network Health Dashboard.

### About this task

The content of the Device Dashboard varies depending on whether you installed Network Performance Insight (NPI).

- If NPI is installed, then the Device Dashboard includes the Performance Insights widget. The Performance Insights widget shows performance measure values, anomalies, and trends for the selected entity. For more information, see “Monitoring performance data” on page 254.
- If NPI is not installed, then the Device Dashboard does not include the Performance Insights widget. Instead, it displays the Top Performers widget, showing performance measure values only for the selected entity. For more information, see “Displaying highest and lowest performers in a network view” on page 244.

Open the Device Dashboard using one of the following options:

- Open the Device Dashboard from the Top Performers widget in the Network Health Dashboard, by completing one of the following tasks.
  - Press **Ctrl** and click a bar in the Chart view.
  - Click an entity name in the Table view.

The Device Dashboard opens in a new Dashboard Application Services Hub tab. The Device Dashboard opens in the context of the device or interface that is associated with the element that you clicked.

- Open the Device Dashboard from any of the topology GUIs. Right-click a device, link, or interface and click **Performance Insight > Show Device Dashboard**.

The topology GUIs include the Network Views, Network Hop View, Path Views GUI, and Structure Browser.

The Device Dashboard opens in a new tab, in the context of the device, link, or interface associated with the element that you clicked.

- To open the Device Dashboard from the Event Viewer, right-click an event and click **Performance Insight > Show Device Dashboard**.

The Device Dashboard opens in a new tab, in the context of the device or interface that is associated with the element that you clicked.

## Changing Device Dashboard focus

You can change the Device Dashboard focus to a different device, link, or interface.

### Procedure

1. To switch focus to a device, click the device in the **Device** tab in the **Topology** widget. If the device is not shown in the **Topology** widget, complete the following steps.
  - a. Search for the device by using the Network Hop View search feature. For more information, see [http://www.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/visualize/task/nmip\\_vis\\_searchfordevices.html](http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/visualize/task/nmip_vis_searchfordevices.html). The **Topology** widget is updated to center on the device that is selected in the search results.
  - b. In the **Topology** widget, click the device of interest.

2. To switch focus to a link, click the link in the **Device** tab in the **Topology** widget. If the link is not shown in the **Topology** widget, complete the following steps.
  - a. Search for a device at one end of the link by using the Network Hop View search feature. For more information, see [http://www.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/visualize/task/nmip\\_vis\\_searchfordevices.html](http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/visualize/task/nmip_vis_searchfordevices.html). The **Topology** widget is updated to center on the device that is selected in the search results.
  - b. In the **Topology** widget, click the link of interest.
3. To switch focus to an interface, click the device that contains the interface of interest in the **Topology** widget. If the interface is not shown in the **Topology** widget, complete the following steps.
  - a. Search for the device that contains the interface of interest by using the Network Hop View search feature. For more information, see [http://www.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/visualize/task/nmip\\_vis\\_searchfordevices.html](http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/visualize/task/nmip_vis_searchfordevices.html). The **Topology** widget is updated to center on the device that is selected in the search results.
  - b. Click the **Structure** tab.
  - c. Click **Show Interfaces**  .
  - d. Select the interface of interest from the list.

## Results

All the widgets on the Device Dashboard update to show data for the device, interface, or link.

## Monitoring performance data

You can monitor performance metrics for a device, link, or interface using the Performance Insights widget within the Device Dashboard.

## Procedure

1. Launch the Device Dashboard as described in “Starting the Device Dashboard” on page 253.
2. Ensure that the device, link, or interface of interest is selected. To change the dashboard context, see “Changing Device Dashboard focus” on page 253.
3. In the Performance Insights widget, proceed as follows:  
Select from the following controls to display performance metric values, anomalies, and trends in the Performance Insights widget.

**Note:** Performance anomalies are determined based on the application of static thresholds to performance data. Anomaly detection is an early warning system that indicates that a device, interface, or link, needs attention.

### Devices

This tab contains performance data for the devices that you selected in the **Topology** portlet. If you selected interfaces, it shows the devices that contain them. If you selected links, it shows the devices at either end.

If there are performance anomalies associated with any of the metrics, then the number of the worst severity anomalies is shown in a colored square in the tab header.

- A number in a red square indicates that there are higher severity anomalies, and indicates the number of higher severity anomalies. If a red square is showing, there might also be lower severity anomalies.
- A number in an orange square indicates that there are lower severity anomalies, but no higher severity anomalies, and indicates the number of lower severity anomalies.

**Filter** Type any string to filter the rows displayed in the table.

**Device**

Lists the device or devices selected in the **Topology** widget. Expand the device node to see the metrics associated with the device.

**Metric** Lists the performance metrics available for the associated device.

**Last 30 Minutes**

Displays a sparkline showing the trend of the performance metric over the last 30 minutes. The current value is shown using a colored dot at the end of the sparkline. The color of the dot indicates whether there is an anomaly associated with this performance metric.

- Red: indicates a higher severity anomaly.
- Orange: indicates a lower severity anomaly.
- Black: no anomaly.

**Severity**

Bullet graph, showing a central bar in a color that indicates the anomaly severity. The thresholds that have been applied to the performance metric are shown in different levels of gray shading in the wider bar. The color of the central bar specifies the anomaly severity.

- Red: indicates a higher severity anomaly.
- Orange: indicates a lower severity anomaly.
- Black: no anomaly.

**Value** Indicates the value of the performance metric based on the most recent poll action.

**Links** This tab contains performance metric anomaly and trend data for one or more links. In particular, it displays data for each connection on each of the selected links.

**Note:** The **Links** tab only appears if you selected one or more links in the **Topology** widget.

If there are performance anomalies associated with any of the metrics, then the number of the worst severity anomalies is shown in a colored square in the tab header.

- A number in a red square indicates that there are higher severity anomalies, and indicates the number of higher severity anomalies. If a red square is showing, there might also be lower severity anomalies.
- A number in an orange square indicates that there are lower severity anomalies, but no higher severity anomalies, and indicates the number of lower severity anomalies.

- Filter** Type any string to filter the rows displayed in the table.
- Links** For each link displays the NCIM topology database entity identifiers of the devices at either end of the link. Roll over this field for more details of the devices, such as hostname and IP address.

#### Connections

Within each link, lists the connections that make up the link. Each connection is identified using the NCIM topology database entity identifiers of the interfaces at either end of the link. Roll over this field for more details of the interfaces, such as interface name, and interface description.

- Metric** Lists the performance metrics available for the associated connection.

#### Last 30 Minutes

Displays a sparkline showing the trend of the performance metric over the last 30 minutes. The current value is shown using a colored dot at the end of the sparkline. The color of the dot indicates whether there is an anomaly associated with this performance metric.

- Red: indicates a higher severity anomaly.
- Orange: indicates a lower severity anomaly.
- Black: no anomaly.

#### Severity

This takes the form of a square in a color that indicates the anomaly severity for this performance metric.

- Red: indicates a higher severity anomaly.
- Orange: indicates a lower severity anomaly.
- Green: no anomaly.

- Value** Indicates the value of the performance metric based on the most recent poll action.

#### Interfaces

Depending on the selection in the **Topology** widget, this tab contains performance data for the following interfaces:

| If you selected in the Topology widget | Then this tab displays performance metric anomaly and trend data for      | For more information, see                                                             |
|----------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| One or more devices                    | All the interfaces on these devices.                                      | Interfaces tab: Content when a device or interface is selected in the Topology widget |
| One or more interfaces                 | The selected interfaces.                                                  |                                                                                       |
| One or more links                      | The interfaces at either end of the connections that make up these links. | Interfaces tab: Content when a link is selected in the Topology widget                |

If there are performance anomalies associated with any of the metrics, then the number of the worst severity anomalies is shown in a colored square in the tab header.

- A number in a red square indicates that there are higher severity anomalies, and indicates the number of higher severity anomalies. If a red square is showing, there might also be lower severity anomalies.
- A number in an orange square indicates that there are lower severity anomalies, but no higher severity anomalies, and indicates the number of lower severity anomalies.

If there is performance data associated with the interface, you can view it by opening the Traffic Details widget in a new tab. Right-click an interface and select **Show Traffic Details**.

#### **Interfaces tab: Content when a device or interface is selected in the Topology widget**

**Filter** Type any string to filter the rows displayed in the table.

**Metric** Drop-down list that lists all of the metrics available on the selected interfaces.

##### **Device**

Lists the device or devices that contain the interfaces selected in the **Topology** widget. Expand the device node to see the all the interfaces in that device and associated status and metric data.

##### **Interface**

Interface name of the selected interfaces or of the interfaces on the selected devices.

**Metric** Performance metric selected from the **Metric** drop-down list.

##### **Last 30 Minutes**

Displays a sparkline showing the trend of the performance metric over the last 30 minutes. The current value is shown using a colored dot at the end of the sparkline. The color of the dot indicates whether there is an anomaly associated with this performance metric.

- Red: indicates a higher severity anomaly.
- Orange: indicates a lower severity anomaly.
- Black: no anomaly.

##### **Severity**

This takes the form of a square in a color that indicates the anomaly severity for this performance metric.

- Red: indicates a higher severity anomaly.
- Orange: indicates a lower severity anomaly.
- Green: no anomaly.

**Value** Indicates the value of the performance metric based on the most recent poll action.

#### **Interfaces tab: Content when a link is selected in the Topology widget**

**Filter** Type any string to filter the rows displayed in the table.

**Links** For each link displays the NCIM topology database entity identifiers of the devices at either end of the link.

Roll over this field for more details of the devices, such as hostname and IP address.

**Connections**

Within each link, lists the connections that make up the link. Each connection is identified using the NCIM topology database entity identifiers of the interfaces at either end of the link. Roll over this field for more details of the interfaces, such as interface name, and interface description.

**Device**

Specifies the device at each end of the connection.

**Interface**

Specifies the interface at each end of the connection.

**Metric** Performance metric selected from the **Metric** drop-down list.

**Last 30 Minutes**

Displays a sparkline showing the trend of the performance metric over the last 30 minutes. The current value is shown using a colored dot at the end of the sparkline. The color of the dot indicates whether there is an anomaly associated with this performance metric.

- Red: indicates a higher severity anomaly.
- Orange: indicates a lower severity anomaly.
- Black: no anomaly.

**Severity**

This takes the form of a square in a color that indicates the anomaly severity for this performance metric.

- Red: indicates a higher severity anomaly.
- Orange: indicates a lower severity anomaly.
- Green: no anomaly.

**Value** Indicates the value of the performance metric based on the most recent poll action.

## Configuring the Performance Insights widget

Both administrators and end users can configure the Performance Insights widget within the Device Dashboard.

### About this task

To configure the Performance Insights widget, perform the following steps.

### Procedure

1. In the Performance Insights widget, click **Edit Preferences** .
2. To configure communication between the Performance Insights widget and Network Performance Insight, use the following controls:

**NPI Hostname**

Specify the hostname of Network Performance Insight server that provides performance data for this widget.



- Port** Specify the port on the Network Performance Insight host. This is usually either 8080 or 9443.
3. To configure presentation and refresh of data on the Performance Insights widget, use the following controls:
- Time Period**  
Specify how many minutes of sparkline data to display for each performance metric in the Performance Insights widget. Default value is 30 minutes.
- Refresh Rate**  
Specify how often to refresh the data in the Performance Insights widget. Default value is 60 seconds.
4. Click **OK**.

## Configuring thresholds

You can configure thresholds that determine when anomalies or events are raised.

### About this task

You can configure anomaly thresholds for performance measures. Anomaly thresholds use data from Network Manager.

### Defining performance thresholds for anomaly detection

If your Netcool Operations Insight solution is integrated with Network Performance Insight, then you can define static thresholds for anomaly detection. You define a static threshold for a given KPI within the poll definition that polls for that KPI.

### About this task

For full information on how to configure poll definitions, see the following topic in the Network Manager Knowledge Center: [http://www.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itm/ip/wip/poll/task/nmip\\_crtpolldef.html](http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itm/ip/wip/poll/task/nmip_crtpolldef.html).

### About poll definitions and static thresholds:

You specify static thresholds on performance measures on devices and interfaces, by defining the thresholds within the relevant poll definition. If these static thresholds are violated for any given performance measure on a device or interface, Tivoli Netcool/OMNIbus events will be generated at an appropriate severity level, and if the context of the Device Dashboard is switched to the relevant device or interface, then the anomaly value and any associated performance measure trends will be shown on the dashboard.

*Poll definition parameters:*

Use this information to understand the parameters of a poll definition.

Network Manager provides default poll policies and definitions.

Use the poll definition to define the following parameters:

- Poll definition name
- Poll definition type: This determines the *polling mechanism* that the poll definition uses. The following polling mechanisms are used:

- Ping polling
- SNMP polling
- Severity level of the event that is generated

**Important:** The severity level must correspond to a valid severity level as defined in IBM Tivoli Netcool/OMNIBus. For a listing of available severity levels, refer to the *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*.

- Short description of the poll definition.
- Basic threshold poll definition type only: data label. A label used to associate the data collected by a basic threshold poll definition with a report. When defining the report, you pick the data to present in the report using the data label. This enables a report to present data tagged with the same data label but collected by more than one poll definition. For a listing of summary reports, refer to the *IBM Tivoli Network Manager IP Edition Administration Guide*.
- Scope of the poll definition: optionally which device class and interface filters to apply.
- Threshold poll definitions only: the threshold settings for generating and clearing an alert.

#### *Threshold polling:*

During threshold polling, predefined formulas are applied to the selected MIB variables, and if the threshold is exceeded by the MIB variable, then an event is generated. A Clear event is generated when the value of the MIB variable either falls below the threshold value, or falls below a different clear value.

You can set two thresholds:

#### **Trigger threshold**

Required: An event is generated when the value of the MIB variable or variables exceeds the threshold.

#### **Clear threshold**

Optional: A clear-event is generated when the value of the MIB variable falls below the threshold.

If you do not specify a clear threshold, the raised event is cleared automatically when the value of the MIB variable or variables no longer exceeds the value of the trigger threshold.

#### **Example of threshold polling**

The Monitoring Administrator wants to identify all Cisco 29xx routers that have CPU usage greater than 75%. Using SNMP polling, the administrator can monitor the behavior of all Cisco 29xx routers in the network, and define that an event is generated for each of these routers when their CPU usage exceeds 75%. A clear threshold can also be set to generate a notification when CPU usage drops below 60%; if no clear threshold is specified, a clear event is generated when the CPU usage no longer exceeds 75%.

#### **Basic and generic threshold polling**

Use *basic threshold polling* to apply simple formulas to the MIB variables, or for filtering the scope at device and interface level. To filter at interface level, the poll definition must be set up for interface filtering.

Use *generic threshold polling* for complex formulas, or for filtering the scope at device level only.

#### *Anomaly detection:*

By defining static thresholds for a performance measure in the Network Manager Poll Definition Editor, you can optionally specify definitive threshold values. If these threshold values are overridden for the specified number of consecutive occurrences, then a performance anomaly with the appropriate severity level is generated.

#### **Defining anomaly thresholds:**

Define anomaly thresholds to detect anomalies in performance measures on devices, links, and interfaces, and display these anomalies in the Device Dashboard.

#### **Before you begin**

Anomaly thresholds are defined within poll definitions.

#### **Restriction:**

You can define anomaly thresholds only for Basic threshold, Chassis Ping, and Interface Ping poll definitions. The poll definition must be set to store historical data and specified within an active poll policy.

#### **About this task**

To define an anomaly threshold, complete the following steps:

#### **Procedure**

1. Create a poll definition, or modify an existing poll definition.
  - To apply anomaly thresholds to performance measures such as CPU and memory utilization on devices, and incoming and outgoing bandwidth utilization on interfaces, create or modify a basic threshold poll definition. Creating a basic threshold poll definition is described in [http://www.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/poll/task/nmip\\_poll\\_crtbasictholddef.html](http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/poll/task/nmip_poll_crtbasictholddef.html).
  - To apply anomaly thresholds to performance measures associated with ping operations against devices and interfaces, such as packet loss and ping time, create or modify a chassis or interface ping poll definition. Creating a chassis or interface ping poll definition is described in [http://www.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/poll/task/nmip\\_poll\\_creatingchassisandifpingpolldefs.html](http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/poll/task/nmip_poll_creatingchassisandifpingpolldefs.html).

When you define a new poll definition, all of the tabs in the Poll Definition Editor are editable, except for the **NPI Anomaly Threshold** tab, which is blank. Complete the other tabs but do not complete the **NPI Anomaly Threshold**. Complete this tab later in the procedure.

2. Ensure that the poll definition is specified in an active poll policy.
  - a. If necessary, create a poll policy. For more information about creating poll policies, see [http://www.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/poll/task/nmip\\_poll\\_crtpoll.html](http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/poll/task/nmip_poll_crtpoll.html).

- b. Set the poll definition to store historical data, by selecting the **Poll Policy Properties** tab in the Poll Policy Editor and clicking the **Store?** check box next to the name of the poll definition.
  - c. Enable the poll policy. For more information about enabling poll policies, see [http://www.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/poll/task/nmip\\_poll\\_enablepoll.html](http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/poll/task/nmip_poll_enablepoll.html).
3. Open the poll definition and define anomaly thresholds by following the instructions in the next step.
4. Click the **NPI Anomaly Threshold** tab and specify static thresholds for triggering performance measurement anomalies in the Device Dashboard, and associated Tivoli Netcool/OMNIBus events.
  - a. In the **Raise violation if the metric value is:** list, specify the conditions for an anomaly to be created. You can select from three types of threshold.

#### Too High

Creates an anomaly if the performance measure goes over either of the limits, for the specified number of times or more.

- If the current value exceeds the **Major Limit** but is less than the **Critical Limit**, a lesser severity (orange) anomaly is generated on the Device Dashboard, and a Major Tivoli Netcool/OMNIBus event is generated.
- If the current value exceeds the **Critical Limit**, a higher severity (red) anomaly is generated on the Device Dashboard, and a Critical Tivoli Netcool/OMNIBus event is generated.

#### Too Low

Creates an anomaly if the performance measure is less than either of the limits, for the specified number of times or more.

- If the current value is less than the **Major Limit** but is more than the **Critical Limit**, a lesser severity (orange) anomaly is generated on the Device Dashboard, and a Major Tivoli Netcool/OMNIBus event is generated.
- If the current value is less than the **Critical Limit**, a higher severity (red) anomaly is generated on the Device Dashboard, and a Critical Tivoli Netcool/OMNIBus event is generated.

#### Outside Band

Creates an anomaly if the performance measure goes outside the band that is defined by the limits, for the specified number of times or more. A higher severity (red) anomaly is generated on the Device Dashboard, and a Critical Tivoli Netcool/OMNIBus event is generated.

- b. For **Too High** and **Too Low** thresholds, specify the **Critical Limit** and **Major Limit**.
  - c. For **Outside Band** type thresholds, specify the band limits in the **Upper Limit** and **Lower Limit** fields.
  - d. In the **Consecutive Occurrences Before Generating Anomaly** spinner, specify the number of consecutive threshold violations that must occur before an anomaly and an event are generated.
5. Click **Save**.

---

## Monitoring traffic flow

Using Network Performance Insight, you can monitor your network's performance.

### Before you begin

To use Network Performance Insight to monitor network performance, you must have successfully installed Network Manager and run a discovery. For more information, see [http://www.ibm.com/support/knowledgecenter/SSSHRK\\_4.2.0/itnm/ip/wip/disco/task/nmip\\_dsc\\_admdsc.html](http://www.ibm.com/support/knowledgecenter/SSSHRK_4.2.0/itnm/ip/wip/disco/task/nmip_dsc_admdsc.html).

### Traffic Details dashboard

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

You can launch the Traffic Details dashboard from the following dashboards:

- From Network Health Dashboard.

The traffic details for an interface are populated in the Network View page, from a selected network view.

- From Event Viewer or AEL

Right-click any event from the Event Viewer or the AEL and select **Flow Dashboard**, to view the traffic details for the event.

#### Related tasks:

“Launching Traffic Details dashboard from Network Health dashboard” on page 272

“Monitoring network performance from Event Viewer” on page 273

### Monitoring Flow data with Traffic Details dashboard

The Traffic Details dashboard displays the network information at an interface level.

#### About this task

By default, the **Traffic Details** page displays the data about the top ingress, top egress, or both flows for an interface

#### 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 265.
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 the check box for a particular interface.  
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 30. Grouping

| Grouping Key | Description                                                                                                                                          |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol     | 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. |
| Source       | Each data series in the donut chart represents the source that is sending the traffic.                                                               |
| Application  | Applications are mapped based on port, protocol, and IP address or network.                                                                          |
| Destination  | Destination can be a host computer to which the network flow comes from a source computer.                                                           |

**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.

#### Related information:

 Built-in aggregation definitions

 Data storage

## Traffic Details dashboard views:

Use this information to see the list of views that are available in The Traffic Details dashboard.

### Top Sources

Displays the details about top Sources for a particular entity. The report shows the topmost sources for ingress, egress and both. The table at the bottom of the view displays the following details:

Table 31. *SOURCE\_IP*

| Name       | Description                                                       |
|------------|-------------------------------------------------------------------|
| Rank       | Displays the number in ascending order.                           |
| Source     | Identity of the source                                            |
| Octets     | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage | Percentage of traffic on the grouping that occupies the traffic.  |

### Top Sources with Application

Displays the traffic details for top Sources and top Applications for a particular entity. The reports show the conversation between top most source and applications for ingress, egress, and both. The table at the bottom of the view displays the following details:

Table 32. *SOURCE\_IP+ APPLICATION\_NAME*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Application | Name of the application                                           |
| Source      | Identity of the source                                            |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

### Top Applications

Displays the traffic details for top Applications for a particular entity. The reports show the topmost Applications for ingress, egress and both. The table at the bottom of the view displays the following details:

Table 33. *APPLICATION\_NAME*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Application | Name of the application                                           |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

### 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 of the view displays the following details:

*Table 34. APPLICATION\_NAME + SOURCE\_IP*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Application | Name of the application                                           |
| Source      | Identity of the source                                            |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

#### **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. The table at the bottom of the view displays the following details:

*Table 35. APPLICATION\_NAME + DESTINATION\_IP*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Application | Name of the application                                           |
| Destination | Identity of the destination                                       |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

#### **Top Applications with Conversation**

Displays the traffic details for top Applications with top Conversations for a particular entity. The reports show the conversation between top most Applications, Sources, and Destinations for ingress, egress and both. The table at the bottom of the view displays the following details:

*Table 36. APPLICATION\_NAME + SOURCE\_IP + DESTINATION\_IP*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Application | Name of the application                                           |
| Source      | Identity of the source                                            |
| Destination | Identity of the destination                                       |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

#### **Top Protocols**

Displays the traffic details for top Protocols for a particular entity. The reports show top most Protocols for ingress, egress and both. The table at the bottom of the view displays the following details:



Table 37. *PROTOCOL\_ID*

| Name       | Description                                                       |
|------------|-------------------------------------------------------------------|
| Rank       | Displays the number in ascending order.                           |
| Protocol   | Identity of the protocol                                          |
| Octets     | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage | Percentage of traffic on the grouping that occupies the traffic.  |

#### Top Protocols with Source

Displays the traffic details for top Protocols with top Sources for a particular entity. The reports show the conversation between top most Protocols with Sources for ingress, egress and both. The table at the bottom of the view displays the following details:

Table 38. *PROTOCOL\_ID + SOURCE\_IP*

| Name       | Description                                                       |
|------------|-------------------------------------------------------------------|
| Rank       | Displays the number in ascending order.                           |
| Protocol   | Identity of the protocol                                          |
| Source     | Identity of the source                                            |
| Octets     | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage | Percentage of traffic on the grouping that occupies the traffic.  |

#### Top Protocols with Application

Displays the traffic details for top Protocols with top Applications for a particular entity. The reports show the conversation between top most Protocols with Applications for ingress, egress and both. The table at the bottom of the view displays the following details:

Table 39. *PROTOCOL\_ID + APPLICATION\_NAME*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Protocol    | Identity of the protocol                                          |
| Application | Name of the application                                           |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

#### Top Protocols with Conversation

Displays the traffic details for top Protocols with top Conversations for a particular entity. The reports show the conversation between top most applications, sources, and destinations for ingress, egress and both. The table at the bottom of the view displays the following details:

Table 40. *PROTOCOL\_ID + SOURCE\_IP + DESTINATION\_IP*

| Name | Description                             |
|------|-----------------------------------------|
| Rank | Displays the number in ascending order. |

Table 40. *PROTOCOL\_ID + SOURCE\_IP + DESTINATION\_IP* (continued)

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Protocol    | Identity of the protocol                                          |
| Source      | Identity of the source                                            |
| Destination | Identity of the destination                                       |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

### 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. The table at the bottom of the view displays the following details:

Table 41. *PROTOCOL\_ID + DESTINATION\_IP*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Protocol    | Identity of the protocol                                          |
| Destination | Identity of the destination                                       |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

### Top Conversations

Displays the traffic details for top Conversations for a particular entity. The reports show the topmost conversations for ingress, egress and both. The table at the bottom of the view displays the following details:

Table 42. *SOURCE\_IP + DESTINATION\_IP*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Source      | Identity of the source                                            |
| Destination | Identity of the destination                                       |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

### Top Conversations with Application

Displays the traffic details for top Conversations and top Applications for a particular entity. The reports show the conversation between top most source, destination, and applications for ingress, egress and both. The table at the bottom of the view displays the following details:

Table 43. *SOURCE\_IP + DESTINATION\_IP + APPLICATION\_NAME*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Application | Name of the application                                           |
| Source      | Identity of the source                                            |
| Destination | Identity of the destination                                       |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

### Top Destinations

Displays the traffic details for top Destinations for a particular entity for a particular entity. The reports show the topmost Destinations for ingress, egress and both. The table at the bottom of the view displays the following details:

Table 44. *DESTINATION\_IP*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Destination | Identity of the destination                                       |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

### Top Destinations with Application

Displays the traffic details for top Destinations with top Applications for a particular entity. The reports show the conversation between top most Destinations and Applications for ingress, egress, and both. The table at the bottom of the view displays the following details:

Table 45. *DESTINATION\_IP + APPLICATION\_NAME*

| Name        | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Rank        | Displays the number in ascending order.                           |
| Application | Name of the application                                           |
| Destination | Identity of the destination                                       |
| Octets      | Displays the amount of data that is used in Bytes, KB, and so on. |
| Percentage  | Percentage of traffic on the grouping that occupies the traffic.  |

## 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 that is 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 46. Mappings table

| Flow table         | NCIM view                |
|--------------------|--------------------------|
| <i>exporter ip</i> | <i>device ip address</i> |
| <i>if index</i>    | <i>interface index</i>   |

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 47. SNMP fields in Traffic Details dashboard

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

### Related concepts:

"Traffic Details dashboard views" on page 265

## Related information:

 Data storage

## 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 that is created for Network Performance Insight. For more information, see *Configuring launch-in-context integration with Network Performance Insight*.

The **NPI** folder name is based on the launch-in-context tool that is 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:

"Launching Traffic Details dashboard from Network Health dashboard" on page 272

## Related information:

 Editing dashboard content and layout

## Launching Traffic Details dashboard 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 Flow data with Traffic Details dashboard” on page 263.

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 information:

 [About the Structure Browser](#)

## Monitoring network performance from Event Viewer

You can monitor and manage network performance from events that are generated by Tivoli Netcool/OMNIBus on Web GUI.

### About this task

You can access the events from the following widgets:

- 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.

2. In the navigation bar, click **Incident** () > **Events** > **Event Viewer**.
3. Right-click any event from the **Event Viewer** page and select **Flow Dashboard**.  
The Traffic Details dashboard that is associated with the selected event is displayed in another window.

**Note:** You can launch the Traffic Details dashboard from Flow thresholds only.

4. Optional: In the navigation bar, click **Incident** () > **Events** > **Active Event List (AEL)**.
5. 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.
6. Right-click any event from the **Event Viewer** page and select **Performance Insight** > **Show Traffic**.  
The Traffic Details dashboard that is associated with the selected event is displayed in another window.

**Note:** You can launch the Traffic Details dashboard from Flow thresholds only.

### Related information:

-  [Monitoring events in the Web GUI](#)
-  [Configuring launch-in-context menu](#)

## 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.

| Level | Threshold type | Color  |
|-------|----------------|--------|
| 0     | Clear          | Green  |
| 1     | Intermediate   | Gray   |
| 2     | Warning        | Blue   |
| 3     | Minor          | Yellow |
| 4     | Major          | Orange |
| 5     | Critical       | Red    |

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

### Related information:

 [Customizing event displays in the Web GUI](#)



---

## Topology search

The topology search capability is an extension of the Networks for Operations Insight feature. It applies the search and analysis capabilities of Operations Analytics - Log Analysis to give insight into network performance. Events that have been enriched with network data are analyzed by the Network Manager Insight Pack and are used to calculate the lowest-cost routes between two endpoints on the network topology over time. The events that occurred along the routes over the specified time period are identified and shown by severity. The topology search requires the Networks for Operations Insight feature to be installed and configured. The topology search capability can plot the lowest-cost route across a network between two end points and display all the events that occur on the devices on the routes.

The Network Manager product enriches all the event data that is generated by the devices on the network topology. It is stored in Tivoli Netcool/OMNIbus, so that the Operations Analytics - Log Analysis product can cross-reference devices and events. The Gateway for Message Bus is used to pass event data from Tivoli Netcool/OMNIbus to Operations Analytics - Log Analysis. Also, the Network Manager Insight Pack reads topology data from the NCIM database in Network Manager to identify the paths in the topology between the devices.

The scope of the topology search capability is that of the entire topology network, which includes all NCIM domains. To restrict the topology search to a single domain, you can configure a properties file that is included in the Network Manager Insight Pack.

After the Insight Pack is installed, you can run the apps from the Operations Analytics - Log Analysis UI. With Network Manager installed and configured, the apps can also be run as right-click tools from the Network Views. With Tivoli Netcool/OMNIbus Web GUI installed and configured, the apps can be run as right-click tools from the Event Viewer and Active Event List (AEL).

The custom apps use the network-enriched event data and the topology data from the Network Manager NCIM database. They plot the lowest-cost routes across the network between two nodes (that is, network entities) and count the events that occurred on the nodes along the routes. You can specify different time periods for the route and events. The algorithm uses the speed of the interfaces along the routes to calculate the routes that are lowest-cost. That is, the fastest routes from start to end along which a packet can be sent. The network topology is based on the most recent discovery. Historical routes are not accounted for. If your network topology is changeable, the routes between the nodes can change over time. If the network is stable, the routes stay current.

### Before you begin

Ensure that you have a good knowledge of your network before you implement the topology search capability. Over large network topologies, the topology search can be performance intensive. It is therefore important to determine which parts of your network you want to use the topology search on. You can define those parts of the network into a single domain. Alternatively, implement the cross-domain discovery function in Network Manager to create a single aggregation domain of the domains that you want to search. You can restrict the scope of the topology

search to that domain or aggregation domain. For more information about deploying Network Manager to monitor networks of small, medium, and larger networks, see the *IBM Tivoli Network Manager IP Edition Product Overview*. For more information about the cross-domain discovery function, see the *IBM Tivoli Network Manager IP Edition Discovery Guide*.

---

## Supported products and components

The topology search capability is supported on a specific combination of products and components. Ensure that your environment has the requisite support before you enable topology search. These requirements apply to both new and upgraded environments.

The topology search capability requires the following products and components.

- Operations Analytics - Log Analysis V1.3 or later with the OMNIBusInsightPack\_v1.3.0.2 and the NetworkManagerInsightPack\_V1.3.0.0.
- Tivoli Netcool/OMNIBus Core V8.1.0.2 and Tivoli Netcool/OMNIBus Web GUI V8.1.0.2 or later. Install the **Install tools and menus for event search with IBM SmartCloud Analytics - Log Analysis** feature as part of the Web GUI installation.
- Gateway for Message Bus package version 6.0 or later. Earlier package versions do not include the configurations that are required for the topology search capability.
- Network Manager V4.1.1.1 or later. The topology search capability requires that the NCIM database for the network topology is IBM DB2 9.7 or 10.1. Oracle 10g or 11g is also supported, but requires more configuration than DB2. Although the Network Manager product supports other databases for storing the topology, the topology search capability is supported only on these databases.

### Related tasks:

“Installing Netcool Operations Insight” on page 27

---

## Configuring topology search

Before you can use the topology search capability, configure the Tivoli Netcool/OMNIBus core and Web GUI components, the Gateway for Message Bus and Network Manager.

### Before you begin

Set up the environment for each product as follows:

- Ensure you have a combination of supported products and components. See “Supported products and components.”
- Configure the event search capability, including the Gateway for Message Bus. See “Configuring event search” on page 94. The topology search capability requires that the Gateway for Message Bus is configured to forward event data to Operations Analytics - Log Analysis.
- If your Operations Analytics - Log Analysis is upgraded from a previous version, migrate the data to your V1.3 instance. See <https://ibm.biz/BdEQmi>.
- Ensure that the ObjectServer that forwards event data to Operations Analytics - Log Analysis has the **NmosObjInst** column in the alerts.status table. **NmosObjInst** is supplied by default and is required for this configuration. You can use ObjectServer SQL commands to check for the column and to add it if it is missing, as follows.

- Use the DESCRIBE command to read the columns of the alerts.status table.
- Use the ALTER COLUMN setting with the ALTER TABLE command to add **NmosObjInst** to the alerts.status table.

For more information about the alerts.status table and ObjectServer SQL commands, see the *IBM Tivoli Netcool/OMNIBus Administration Guide*.

- Configure the Tivoli Netcool/OMNIBus Web GUI V8.1.0.4 as follows:
    - Install the **Netcool Operations Insight Extensions for IBM Tivoli Netcool/OMNIBus Web GUI** package. IBM Installation Manager installs this package separately from the Web GUI. It needs to be explicitly selected.
    - Check the server.init file to ensure that the **scala\*** properties are set as follows:
 

```
scala.app.keyword=OMNIBus_Keyword_Search
scala.app.static.dashboard=OMNIBus_Static_Dashboard
scala.datasource=omnibus
scala.url=protocol://host:port
scala.version=1.2.0.3
```
- This configuration needed for new environments and for environments that are upgraded from versions of Operations Analytics - Log Analysis that are earlier than 1.2.0.3.
- Set up the Web GUI Administration API client, which is needed to install the event list tooling that launches Operations Analytics - Log Analysis. See the *IBM Tivoli Netcool/OMNIBus Installation and Deployment Guide*.
  - Install and configure the Insight Packs as follows:
    1. Install the OMNIBusInsightPack\_v1.3.0.2. If your environment is upgraded from a previous version of Netcool Operations Insight, upgrade to this version of the Insight Pack. See Netcool/OMNIBus Insight Pack.
    2. Create a data source.
    3. Obtain and install the Network Manager Insight Pack V1.3.0.0. See Installing the Insight Pack.

## Procedure

1. In \$NCHOME/omnibus/extensions, run the **nco\_sql** utility against the scala\_itnm\_configuration.sql file.
 

```
./nco_sql -user root -password myp4ss -server NCOMS
< /opt/IBM/tivoli/netcool/omnibus/extensions/scala/scala_itnm_configuration.sql
```

Triggers are applied to the ObjectServer that delay the storage of events until the events are enriched by Network Manager data from the NCIM database.

2. If the Gateway for Message Bus is not configured to forward event data to Operations Analytics - Log Analysis, perform the required configurations.<sup>1</sup>

---

1. At a high-level, this involves the following:

- Creating a gateway server in the Netcool/OMNIBus interfaces file
- Configuring the G\_SCALA.props properties file, including specifying the xml1302.map
- Configuring the endpoint in the scalaTransformers.xml file
- Configuring the SSL connection, if required
- Configuring the transport properties in the scalaTransport.properties file

3. Install the tools and menus to launch the custom apps of the Network Manager Insight Pack in the Operations Analytics - Log Analysis UI from the Web GUI. In `$WEBGUI_HOME/extensions/LogAnalytics`, run the **runwaapi** command against the `scalaEventTopology.xml` file.

```
$WEBGUI_HOME/waapi/bin/runwaapi -user username -password password -file
scalaEventTopology.xml
```

Where *username* and *password* are the credentials of the administrator user that are defined in the `$WEBGUI_HOME/waapi/etc/waapi.init` properties file that controls the WAAPI client.

4. On the host where the Network Manager GUI components are installed, install the tools and menus to launch the custom apps of the Network Manager Insight Pack in the Operations Analytics - Log Analysis GUI from the Network Views.

- a. In `$NMGUI_HOME/profile/etc/tnm/topoviz.properties`, set the **topoviz.unity.customappsui** property, which defines the connection to Operations Analytics - Log Analysis. For example:

```
Defines the LogAnalytics custom App launcher URL
topoviz.unity.customappsui=https://server3:9987/Unity/CustomAppsUI
```

- b. In the `$NMGUI_HOME/profile/etc/tnm/menus/ncp_topoviz_device_menu.xml` file, define the **Event Search** menu item. Add the item `<menu id="Event Search"/>` in the file as shown:

```
<tool id="showConnectivityInformation"/>
 <separator/>
 <menu id="Event Search"/>
```

5. Start the Gateway for Message Bus in Operations Analytics - Log Analysis mode. For example:

```
$OMNIHOME/bin/nco_g_xml -propsfile $OMNIHOME/etc/G_SCALA.props
```

The gateway begins sending events from Tivoli Netcool/OMNIBus to Operations Analytics - Log Analysis.

## What to do next

- Configure single sign-on (SSO) between the products.
- Reconfigure your views in the Web GUI to display the **NmosObjInst** column. The tools that launch the custom apps of the Network Manager Insight Pack work only against events that have a value in this column. For more information, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide*.

### Related reference:

"Supported products and components" on page 276

### Related information:

 Gateway for Message Bus documentation

## Configuring single sign-on for the topology search capability

Configure single sign-on (SSO) between the Dashboard Application Services Hub that hosts the Network Manager GUI components and Operations Analytics - Log Analysis so that users can switch between the two products without having to log in each time. First, create dedicated users in your LDAP directory, which must be used by both products for user authentication, and then configure the SSO connection.

### Procedure

1. Create the dedicated users and groups in your LDAP directory. For example:
  - a. Create a new Organization Unit (OU) named NetworkManagement.
  - b. Under the NetworkManagement OU, create a new group named itnmlldap.
  - c. Under the NetworkManagement OU, create the following new users: itnm1, itnm2, itnm3, and itnm4.
  - d. Add the new users to the itnmlldap group.
2. In Dashboard Application Services Hub, assign the itnmlldap group that you created in step 1 to a Network Manager user group that can access the Network Views. Network Manager user roles are controlled by assignments to user groups. Possible user groups that can access the Network Views are Network\_Manager\_IP\_Admin and Network\_Manager\_User.
3. Configure the SSO connection from the Operations Analytics - Log Analysis product to the Dashboard Application Services Hub instance in which Network Manager is hosted. For more information about configuring SSO for Operations Analytics - Log Analysis, see the Operations Analytics - Log Analysis documentation. The following steps of the Operations Analytics - Log Analysis SSO configuration are important:
  - Assign Operations Analytics - Log Analysis roles to the users and groups that you created in step 1.
  - In the `$SCALAHOME/wlp/usr/servers/Unity/server.xml/server.xml` file, ensure that the `<webAppSecurity>` element has a `httpOnlyCookies="false"` attribute. Add this line before the closing `</server>` element. For example:

```
<webAppSecurity ssoDomainNames="hostname" httpOnlyCookies="false"/>
</server>
```

The `httpOnlyCookies="false"` attribute disables the `httponly` flag on the cookie that is generated by Operations Analytics - Log Analysis and is required to enable SSO with Network Manager GUI.

### Related tasks:

 [Configuring SSO between Operations Analytics - Log Analysis V1.3.5 and Dashboard Application Services Hub](#)

 [Configuring SSO between Operations Analytics - Log Analysis V1.3.3 and Dashboard Application Services Hub](#)

---

## Searching the topology

After the topology search capability is configured, you can have Operations Analytics - Log Analysis show you the events that occurred within a specific time period on routes between two devices in the network topology. This capability is useful to pinpoint problems on the network, for example, in response to a denial of service attack on a PE device.

The custom apps of the Network Manager Insight Pack can be run from the Operations Analytics - Log Analysis and, depending on your configuration, from the Network Views in Network Manager and the event lists in the Web GUI. The custom apps support searches on Layer 2 and Layer 3 of the topology. The custom apps use the network-enriched event data and the topology data from the Network Manager NCIM database. They plot the lowest-cost routes across the network between two nodes (that is, network entities) and count the events that occurred on the nodes along the routes. You can specify different time periods for the route and events. The algorithm uses the speed of the interfaces along the routes to calculate the routes that are lowest-cost. That is, the fastest routes from start to end along which a packet can be sent. The network topology is based on the most recent discovery. Historical routes are not accounted for. If your network topology is changeable, the routes between the nodes can change over time. If the network is stable, the routes stay current.

### Before you begin

- Knowledge of the events in your topology is required to obtain meaningful results from the topology search, for example, how devices are named in your environment, or with what information devices are enriched. Device names are usually indicative of their functions. This level of understanding helps you run searches in Operations Analytics - Log Analysis.
- Configure the products to enable the topology search capability. See “Configuring topology search” on page 276.
- To avoid reentering user credentials when launching between products, configure SSO.
- Create the network views that visualize the parts of the network that you are responsible for and want to search. See [http://www-01.ibm.com/support/knowledgecenter/SSSHRK\\_4.1.1/com.ibm.networkmanagerip.doc\\_4.1.1/itnm/ip/wip/admin/task/nmip\\_adm\\_crtnwview.html](http://www-01.ibm.com/support/knowledgecenter/SSSHRK_4.1.1/com.ibm.networkmanagerip.doc_4.1.1/itnm/ip/wip/admin/task/nmip_adm_crtnwview.html).
- Reconfigure your views in the Web GUI to display the **NmosObjInst** column. The tools that launch the custom apps of the Network Manager Insight Pack work only against events that have a value in this column. For more information, see the *IBM Tivoli Netcool/OMNIBus Web GUI Administration and User's Guide*.

### Procedure

The flow of this procedure is to select the two nodes, select the tool and a time period over which the tool searches the historical event data. Then, in the Operations Analytics - Log Analysis UI, select the route that you are interested in and view the events. You can run searches on the events to refine the results.

1. Run the topology search from one of the products, as follows:
  - Web GUI event lists:
    - a. In an Event Viewer or AEL, select two rows that have a value in the **NmosObjInst** column.

- b. Right click and click **Event Search > Find events between two nodes > Layer 2 Topology** or **Event Search > Find events between two nodes > Layer 3 Topology**, depending on which layer of the topology you want to search.
  - c. Click a time filter, or click **Custom** and select one.
- Network Manager network views:
  - a. Select two devices.
  - b. Click **Event Search > Find Events Between 2 Nodes > Layer 2 Topology** or **Event Search > Find Events Between 2 Nodes > Layer 3 Topology** depending on which layer of the topology you want to search.
  - c. Click a time filter, or click **Custom** and select one.
- Operations Analytics - Log Analysis UI. In the Operations Analytics - Log Analysis UI, the app requires search results before you can run it. In the search results, select the **NmosObjInst** column. The app finds the events between the two nodes on which each selected event originated.

**Important:** Select the **NmosObjInst** cells only. Do not select the entire rows. If you select the entire rows, no results are found, or incorrect routes between the entities on the network are found.

In the **Search Dashboards** section of the UI, click

**NetworkManagerInsightPack > Find events between two nodes on layer 2 topology** or **Find events between two nodes on layer 3 topology**, depending which network layer you want to view.

See “Example” on page 282 for an example of how to run the apps from the Operations Analytics - Log Analysis UI.

The results of the search are displayed on the Operations Analytics - Log Analysis UI as follows:

#### **Find alerts between two nodes on layer 2 topology**

This app shows the distribution of alerts on the least-cost routes between two network end points in a layer 2 topology. Charts show the alert distribution by severity and alert group for each route over the specified time period. The ObjectServer field for the alert group is AlertGroup. A list of the routes is displayed from which you can search the events that occurred on each route over the specified time period.

#### **Find alerts between two nodes on layer 3 topology**

This app shows the distribution of alerts on the least-cost routes between two network end points in a layer 3 topology. Charts show the alert distribution by severity and alert group for each route over the specified time period. The ObjectServer field for the alert group is AlertGroup. A list of the routes is displayed from which you can search the events that occurred on each route over the specified time period.

The apps count the events that occurred over predefined periods of time, relative to the current time, or over a custom time period that you can specify. For the predefined time periods, the current time is calculated differently, depending on which product you run the apps from. Network Manager uses the current time stamp. The Tivoli Netcool/OMNIBus Web GUI uses the time that is specified in the FirstOccurrence field of the events.

**Restriction:** The Web GUI and Operations Analytics - Log Analysis process time stamps differently. The Web GUI recognizes hours, minutes, and seconds but Operations Analytics - Log Analysis ignores seconds. This problem affects the **Show event dashboard by node** and **Search for events by node**. If the time stamp 8 January 2014 07:15:26 AM is passed, Operations Analytics - Log

Analysis interprets this time stamp as 8 January 2014 07:15 AM. So, the results of subsequent searches might differ from the search that was originally run.

2. From the bar charts, identify the route that is of most interest. Then, on the right side of the UI, click the link that corresponds to that route. A search result is returned that shows all the events that occurred within the specified time frame on that network route.
3. Refine the search results. You can use the patterns that are listed in **Search Patterns**. For example, to search the results for critical events, click **Search Patterns > Severity > Critical**. A search string is copied to the search field. Then, click **Search**.
4. Extend and refine the search as required. For more information about searches in Operations Analytics - Log Analysis, see [http://www-01.ibm.com/support/knowledgecenter/SSPFMY\\_1.3.1/com.ibm.scala\\_1.3.1.doc/use/iwa\\_using\\_ovw.html](http://www-01.ibm.com/support/knowledgecenter/SSPFMY_1.3.1/com.ibm.scala_1.3.1.doc/use/iwa_using_ovw.html).

## Example

An example of how to run the custom apps from the Operations Analytics - Log Analysis UI. This example searches between 2 IP addresses: 172.20.1.3 and 172.20.1.5.

1. To run a new search, click **Add search** and type `NodeAlias:"172.20.1.3" OR NodeAlias:"172.20.1.5"`. Operations Analytics - Log Analysis returns all events that have the NodeAlias 172.20.1.3, or the NodeAlias 172.20.1.5.
2. In the results display, switch to grid view. Scroll across until you see the **NmosObjInst** column. Identify 2 rows that have different **NmosObjInst** values.
3. For these rows, select the cells in the **NmosObjInst** column.
4. In the **Search Dashboards** section of the UI, click **NetworkManagerInsightPack > Find events between two nodes on layer 2 topology** or **Find events between two nodes on layer 3 topology**, depending which network layer you want to view.



---

## Configuring integration to IBM Connections

IBM Tivoli Netcool/Impact provides integration to IBM Connections by using a Netcool/Impact IBMConnections action function. The IBMConnections action function allows users to query forums and topics lists, create a new forum, create a new topic, and update existing topics. The IBMConnections action function package is available in the directory `$IMPACT_HOME/integrations/IBMConnections`.

### About this task

Complete the following steps to configure Netcool/Impact to integrate with the IBM Connections Server.

### Procedure

1. Go to the directory `$IMPACT_HOME/add-ons/IBMConnections`, this directory is the IBM Connections integration package. The package includes the following subdirectory:

#### **importData**

A project that includes policies, data source, data type, and a service. The project serves an example to show how to connect, create, update, and topics in IBM Connections

2. Import the project `$IMPACT_HOME/bin/nci_import <ServerName> __Extraction_Directory__/importData`.
3. Within the `$IMPACT_HOME/etc/<NCI>_server.props` file, add the following parameters:
  - `impact.ibmconnections.forum.title.maxsize= number`. Default value is 0. Any string size can be used.
  - `impact.ibmconnections.forum.content.maxsize= number`. Default value is 0. Any string size can be used
  - `impact.ibmconnections.topic.title.maxsize= number`. Default value is 255, for a topic and a reply.
  - `impact.ibmconnections.topic.content.maxsize = number`. Default value is 0. Any string size can be used
4. Restart Netcool/Impact servers.

#### **Related tasks:**

"Installing Netcool/OMNIBus and Netcool/Impact" on page 40

---

## IBM Connections Overview

IBM Connections is a leading social software platform that can help your organization to engage the right people, accelerate innovation, and deliver results.

This integrated, security-rich platform helps people engage with networks of experts in the context of critical business processes. Now everyone can act with confidence and anticipate and respond to emerging opportunities

For information about IBM Connections, refer to

<http://www-03.ibm.com/software/products/en/conn>

---

## Parameters for the IBMConnections function

The integration between Netcool/Impact and IBM Connections uses a new policy action function that is called the IBMConnections function. The IBMConnections function can be used within any policy to connect to the IBM Connections Server and to perform an action on the IBM Connections Server. The function accepts two input parameters, the **Action Option** parameter and the **Impact Object** parameter.

### Action Option Parameter

The **Action Option** parameter accepts one of the following action entries, which are case insensitive. Some action entries require property information that is case-sensitive.

In the content of an IBM Connections forum, topic, or reply, you can use HTML formatting tags `br`, `b`, and `a`. For more information about the supported HTML tags, see <http://www-03.ibm.com/software/products/en/conn>.

#### CREATEFORUM

Creates a forum.

Enter the following property information that is case-sensitive. The tags must be created before they pass to a variable name.

```
props.ForumTitle=title;
props.ForumContent=full text of the body;
props.ForumTags=List_Of_Tags; Is optional, the object must be a
Netcool/Impact object.
Tags=NewObject();
Tags.Tag1=some tag;
Tags.Tag2=some tag2; Is optional if want more than one tag.
```

#### CREATETOPIC

Creates a topic.

Enter the following property information that is case-sensitive:

```
props.TopicTitle=title;
props.TopicContent=full text of the body;
props.ForumId=forum id: Where the forum id is an ID and not a forum
name.
```

#### DELETEFORUM

Deletes the forum name that was created by the logged in user and any topic or reply belonging to it.

Enter the following property information that is case-sensitive:

```
props.ForumId=forumId; Or props.ForumId=forumTitle;
props.FirstMatchOnly=true; Or props.FirstMatchOnly=false; The
props.FirstMatchOnly property deletes the first matching forum or
matching topic that it finds, or else it deletes any matching forum or
matching topic and its default value is true.
```

#### DELETEPUBLICFORUM

Deletes the given public forum name and any topic or reply belonging to it.

Enter the following property information that is case-sensitive:

```
props.ForumId=forumId; Or props.ForumId=forumTitle;
```

`props.FirstMatchOnly=true`; Or `props.FirstMatchOnly=false`; The `props.FirstMatchOnly` property deletes the first matching forum or matching topic that it finds, or else it deletes any matching forum or matching topic and its default value is true.

#### **DELETEREPLY**

Deletes a topic reply in the topic in the forum id.

Enter the following property information that is case-sensitive:

`props.ForumId=forumId`; Where the *forumId* is an ID and not a title.  
`props.TopicTitle=title`; Or `props.TopicTitle=id`;  
`props.ReplyTitle=replytitle`; Or `props.ReplyTitle=replyid`;  
`props.FirstMatchOnly=true`; Or `props.FirstMatchOnly=false`; The `props.FirstMatchOnly` property deletes the first matching forum or matching topic that it finds, or else it deletes any matching forum or matching topic and its default value is true.

#### **DELETETOPIC**

Deletes a topic in the forum id.

Enter the following property information that is case-sensitive:

`props.ForumId=forumId`; Where the *forumId* is an ID and not a title.  
`props.TopicTitle=title`; Or `props.TopicTitle=id`;  
`props.FirstMatchOnly=true`; Or `props.FirstMatchOnly=false`; The `props.FirstMatchOnly` property deletes the first matching forum or matching topic that it finds, or else it deletes any matching forum or matching topic and its default value is true.

#### **GETCOMMUNITYFORUMID**

Gets the ID of the community that is created by the logged in user

Enter the following property information that is case-sensitive:

`props.CommunityName=Community name`;  
`props.ForumName=forum name`;

#### **GETFORUMTOPICS**

Gets list of topics for the forum id

Enter the following property information that is case-sensitive:

`props.ForumId=forum id`;

#### **GETMYCOMMUNITYID**

Gets the ID of the community for the logged in user

Enter the following property information that is case-sensitive:

`props.CommunityName=Community name`;

#### **GETMYFORUMID**

Gets the ID of the forum that is created by the logged in user.

Enter the following property information that is case-sensitive:

`props.ForumName=actual forum name that is created by the logged in user`

#### **GETMYFORUMS**

Gets all the forums for the logged in user

#### **GETPUBLICCOMMUNITYID**

Gets the ID of the given public community ID

Enter the following property information that is case-sensitive:

```
props.CommunityName=Community name;
```

#### **GETPUBLICFORUMID**

Gets the ID of the given public forum name

Enter the following property information that is case-sensitive:

```
props.ForumName=actual public forum name
```

#### **GETPUBLICFORUMS**

Gets list of all public forums

#### **GETTOPICREPLIES**

Gets list of replies for a topic

Enter the following property information that is case-sensitive:

```
props.TopicId=topic id; Where topic id must be the topic id not the topic name.
```

#### **REPLYTOTOPIC**

Creates a reply to an existing topic

Enter the following property information that is case-sensitive:

```
props.TopicId=topic id; Where topic id is a topic ID not a topic name
props.ReplyTitle=title;
props.ReplyContent=full text of the body;
```

### **Impact Object Parameter**

The **Impact Object** parameter accepts the following property information. The authentication, and connection property information is mandatory.

```
props = NewObject();
props.Protocol=https;
props.Host=IBM Connections Server Host/IP;
props.Port=_PORT_;
props.Username=userName;
props.Password=password; The password can be encrypted by using either the
Netcool/Impact nci_crypt tool or the policy function Encrypt(). If the
password is encrypted, you must use the property
props.DecryptPassword=true;
```

---

## **IBMConnections Project and artifacts**

The imported IBMConnections project includes artifacts that are categorized into four categories.

### **Data sources**

- IBMConnectionsObjectServerDSA
- Internal

### **Data types**

- TopicCreationTracker
  - An internal data type that is used to track the topic creation to avoid duplicate names.

- InternetOutageEvents
  - ObjectServer data type that can be used to view the critical events in the UI Data Provider widgets. It populates the severity as status data type to show colorful images.

## Policies

- IBMConnectionsUtils
  - Includes a utility function to extract value from a data item.
- IBMConnectionsUtilsCaller
  - Shows how to call the utility function in IBMConnectionsUtils.
- IBMConnectionsUtilsJS
  - For JavaScript policies.
- IBMConnectionsUtilsCallerJS
  - For JavaScript policies.
- NetworkMonitorExample
  - Example policy that is run by an event reader to create and update topics.
- NetworkMonitorForOpView
  - Example policy that is run by the operator view from the ObjectServer Event List tool.
- Opview\_IBMConnectionsOpView
  - Is run by the AEL tool.

## Services

- NetworkMonitorExample
  - Connects to the object server data source and uses a default filter of Node in ('US','France','UK') and Identifier Like 'Monitoring Network for'. You can change the default filter at any time. It runs the policy NetworkMonitorExample.

---

## Automatic topic management

The IBM Connections integration package includes NetworkMonitorExample event reader service that connects to the Netcool/OMNIBus Object Server and filters for specific events. When there is a match, the service runs the policy that either updates the topic by sending a reply to the topic, or creates a topic if a topic does not exist.

The forum that is used in this example is the same name as the AlertKey in the Object Server event, forumName = @IBMConnections\_Forum

You can use the sql scripts in the \$IMPACT\_HOME/integrations/IBMConnections/db directory to create extra fields in the Object Server or you can use existing fields.

The topic title is created as a combination of a hardcoded string and the node field from the event:

```
topicTitleVar="Network Monitor is down on node: @Node@" ;
IBMConnectionsUtils.extractParametersAndSubstitute
(topicTitleVar,EventContainer,result);
topicTitle = result;
```

The policy checks if the topic was created by querying the internal data type TopicCreationTracker. If the topic exists, the policy sends a reply instead of creating a new one.

---

## Automatic topic management with event management tools

The operator view policy is updated to run the NetworkMonitorForOpView policy that automatically updates an existing topic or creates a new topic.

### Procedure

1. Create the event management tool, refer to the Netcool/OMNIBus documentation.
2. In the event management tool, select the executable box tab and enter the following text: `start "" "https://<impactgui_server>:<port>/opview/displays/NCICLUSTER-IBMConnectionsOpView.html?Node=@Node&Serial=@Serial&Severity=@Severity&Acknowledged=@Acknowledged&AlertKey=@AlertKey&AlertGroup=@AlertGroup&Summary=@Summary"`

NCICLUSTER is the default cluster but if you are using a different cluster name then update the URL with your cluster name.

The above text is an example of text to enter for an Object Server on Windows.

3. Add the new event management tool to the AlertsStatus tools menu, refer to the Netcool/OMNIBus documentation.
4. When you right-click on an event, click the tool to start the URL and run the policy. The operator view is started and gives a notification that the topic is created or updated, along with a link to the topic URL to use.

### Related information:

 [Creating event management tools](#)

---

## Enabling historical events

Create a connection to the historical database in Impact to view historical events in the Event Viewer.

### Procedure

1. Log in to Dashboard Application Services Hub and select the **Data Model** tab.
2. Click the **New Data Source** icon.
3. Point to **Database SQL** and select your database type. For example **DB2**.
4. In the **Data Source Name** field enter: **historicalEventsDataSource**.
5. Enter your Username and Password in the fields provided and click the **Save** icon.
6. In the left-hand navigation pane, right-click **ImpactHistoricalEventData** and select **New Data Type**.
7. In the **Data Type Name** field enter: **historicalEventData**.
8. Click **Refresh**.

---

## Release notes

IBM Netcool Operations Insight V1.4.0.5 is available. Compatibility, installation, and other getting-started issues are addressed in these release notes.

### Contents

- “Description”
- “Compatibility”
- “System requirements” on page 293
- “New features” on page 293
- “Known problems at eGA” on page 294
- “Support” on page 300

### Description

Netcool Operations Insight combines real-time event consolidation and correlation capabilities of Netcool Operations Insight with Event Search and Event Analytics. It further delivers seasonality analysis to assist in detecting regularly occurring issues. Netcool Operations Insight also enables real-time enrichment and correlation to enable agile responses to alerts raised across disparate systems including application topology.

### Compatibility

The IBM Netcool Operations Insight V1.4.0.5 includes the product and component versions listed in the following table.

*Table 48. Netcool Operations Insight V1.4.0.5 product and component versions*

Product or component	Netcool Operations Insight V1.4.0.5 (April 2017 GA release)	Change from previous version?
		Netcool Operations Insight V1.4.0.4 (March 2017 GA release)
IBM Tivoli Netcool/OMNIBus core components	V8.1.0.11 (V8.1 fix pack 11)	No
Tivoli Netcool/OMNIBus Web GUI	V8.1.0.9 (V8.1 fix pack 9)	No
IBM Tivoli Netcool/Impact	V7.1.0.9 (V7.1 fix pack 9)	No
Operations Analytics - Log Analysis	V1.3.5 V1.3.3.1 (V1.3.3 fix pack 1) V1.3.3	No
Event Analytics	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.9 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI 8.1.0.9 (delivered in Web GUI fix pack)	No

Table 48. Netcool Operations Insight V1.4.0.5 product and component versions (continued)

Product or component	Netcool Operations Insight V1.4.0.5 (April 2017 GA release)	Change from previous version?
		Netcool Operations Insight V1.4.0.4 (March 2017 GA release)
Event Search	Tivoli Netcool/OMNIbus Insight Pack V1.3.0.2  (delivered in Operations Analytics - Log Analysis)	No
Topology Search	Network Manager Insight Pack V1.3.0.0  (delivered in Operations Analytics - Log Analysis)	No
IBM Tivoli Network Manager IP Edition	V4.2.0.3 (V4.2 fix pack 3)	Yes
Device Dashboard	V1.1.0.1 (V1.1 fix pack 1)	No
Network Health Dashboard	V4.2.0.3 (V4.2 fix pack 3)	Yes
IBM Tivoli Netcool Configuration Manager	V6.4.2.4 (V6.4.2 fix pack 4)	Yes
IBM Network Performance Insight	V1.2.0	No
Jazz for Service Management	V1.1.3.0 with Cumulative Patch 1	No
WebSphere Application Server	V8.5.5.9, or later	No

The previous IBM Netcool Operations Insight V1.4.x and V1.3.x releases include the following product and component versions.

- Table 49
- Table 50 on page 292

For more information about the Netcool Operations Insight products and components, see “Supported products and components” on page 3.

Table 49. Netcool Operations Insight Previous 1.4.x product and component versions with GA release date

Product or component	V1.4 (February 2016 )	V1.4.0.1 (March 2016 )	V1.4.0.2 (June 2016 )	V1.4.0.3 (September 2016 )	V1.4.0.4 (December 2016)	V1.4.0.4 (March 2017)
IBM Tivoli Netcool/OMNIbus core components	V8.1.0.5	V8.1.0.7	V8.1.0.8	V8.1.0.9	V8.1.0.10	V8.1.0.11
Tivoli Netcool/OMNIbus Web GUI	V8.1.0.4	V8.1.0.5	V8.1.0.6	V8.1.0.7	V8.1.0.8	V8.1.0.9
IBM Tivoli Netcool/Impact	V7.1.0.4	V7.1.0.5	V7.1.0.6	V7.1.0.7	V7.1.0.8	V7.1.0.9



Table 49. Netcool Operations Insight Previous 1.4.x product and component versions with GA release date (continued)

Product or component	V1.4 (February 2016 )	V1.4.0.1 (March 2016 )	V1.4.0.2 (June 2016 )	V1.4.0.3 (September 2016 )	V1.4.0.4 (December 2016)	V1.4.0.4 (March 2017)
Operations Analytics - Log Analysis	V1.3.2 <b>Note:</b> V1.3.1 is also supported.	V1.3.2 <b>Note:</b> V1.3.3 is also supported. <b>Note:</b> Netcool Operations Insight V1.4.0.2 and later also support Operations Analytics - Log Analysis V1.3.3 fix pack 1.		V1.3.3  V1.3.2	V1.3.3.1  V1.3.3  V1.3.2	1.3.5  V1.3.3.1  V1.3.3  V1.3.2
Event Analytics	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.4 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_1.3.1 (delivered in Web GUI fix pack)	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.5 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_1.4.0.1 (delivered in Web GUI fix pack)	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.6 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_1.4.0.2 (delivered in Web GUI fix pack)	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.7 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_1.4.0.3 (delivered in Web GUI fix pack)	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.8 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_1.4.0.4 (delivered in Web GUI fix pack)	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.9 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI 8.1.0.9 (delivered in Web GUI fix pack)
Event Search	Tivoli Netcool/OMNIBus Insight Pack V1.3.0.2 (delivered in Operations Analytics - Log Analysis)					
Topology Search	Network Manager Insight Pack V1.3.0.0 (delivered in Operations Analytics - Log Analysis)					
IBM Tivoli Network Manager IP Edition	V4.2			V4.2.0.1	V4.2.0.2	
IBM Tivoli Netcool Configuration Manager	V6.4.2		V6.4.2.1	V6.4.2.2	V6.4.2.3	
Device Dashboard	Not yet released	Not yet released	Not yet released	V1.1.0.0	V1.1.0.1	
Network Health Dashboard	V4.2	V4.2	V4.2	V4.2.0.1	V4.2.0.2	
IBM Network Performance Insight	V1.1.1			V1.2.0		

Table 49. Netcool Operations Insight Previous 1.4.x product and component versions with GA release date (continued)

Product or component	V1.4 (February 2016 )	V1.4.0.1 (March 2016 )	V1.4.0.2 (June 2016 )	V1.4.0.3 (September 2016 )	V1.4.0.4 (December 2016)	V1.4.0.4 (March 2017)
Jazz for Service Management	V1.1.2.1			V1.1.3.0	V1.1.3.0 with Cumulative Patch 1  V1.1.2.1 with Cumulative Patch 6	V1.1.3.0 with Cumulative Patch 1
WebSphere Application Server	V8.5.0.1, or later			V8.5.5.9, or later		

The IBM Netcool Operations Insight V1.3.x release includes the following product and component versions.

Table 50. Netcool Operations Insight 1.3.x product and component versions

Product or component	Netcool Operations Insight V1.3 (March 2015 GA release)	Netcool Operations Insight V1.3 (September 2015 update)	Netcool Operations Insight V1.3.1 (December 2015 GA release)
IBM Tivoli Netcool/OMNIBus core components	V8.1.0.3	V8.1.0.4	V8.1.0.5
Tivoli Netcool/OMNIBus Web GUI	V8.1.0.2	V8.1.0.3	V8.1.0.4
IBM Tivoli Netcool/Impact	V7.1.0.2	V7.1.0.3	V7.1.0.4
Operations Analytics - Log Analysis	V1.3.0	V1.3.1	V1.3.2 <b>Note:</b> V1.3.1 is also supported.
Event Analytics	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.2 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_1.3.0 (delivered in Web GUI fix pack)	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.3 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_1.3.0.1 (delivered in Web GUI fix pack)	IBM Tivoli Netcool/Impact Server Extensions for IBM Netcool Operations Insight_7.1.0.4 (delivered in Netcool/Impact fix pack)  IBM Netcool Operations Insight Extension for IBM Tivoli Netcool/OMNIBus Web GUI_1.3.1 (delivered in Web GUI fix pack)
Event Search	Tivoli Netcool/OMNIBus Insight Pack V1.3.0.0  (delivered in Operations Analytics - Log Analysis)	Tivoli Netcool/OMNIBus Insight Pack V1.3.0.1  (delivered in Operations Analytics - Log Analysis)	Tivoli Netcool/OMNIBus Insight Pack V1.3.0.2  (delivered in Operations Analytics - Log Analysis)
Topology Search	Network Manager Insight Pack V1.3.0.0 (delivered in Operations Analytics - Log Analysis)		
IBM Tivoli Network Manager IP Edition	V3.9.0.4  V4.1.1.1		

Table 50. Netcool Operations Insight 1.3.x product and component versions (continued)

Product or component	Netcool Operations Insight V1.3 (March 2015 GA release)	Netcool Operations Insight V1.3 (September 2015 update)	Netcool Operations Insight V1.3.1 (December 2015 GA release)
IBM Tivoli Netcool Configuration Manager	V6.4.1		
IBM Network Performance Insight	N/A		
Jazz for Service Management	V1.1.0.3		V1.1.2.1
WebSphere Application Server	V8.5.0.1		V8.5.0.1, or later

## System requirements

For information about hardware and software compatibility of each component, and detailed system requirements, see the IBM Software Product Compatibility Reports website:

<http://www-969.ibm.com/software/reports/compatibility/clarity/index.html>

**Tip:** When you create a report, search for Netcool Operations Insight and select your version (for example, V1.4). In the report, additional useful information is available through hover help and additional links.

For example, to check the compatibility with an operating system for each component, go to the **Operating Systems** tab, find the row for your operating system, and hover over the icon in the **Components** column. For more detailed information about restrictions, click the **View** link in the **Details** column.

## New features

IBM Netcool Operations Insight V1.4.0.5 offers the following new features. After you install all the products, components, and fixes that are included in Netcool Operations Insight, you can benefit from all these features.

### Updated product versions for the Netcool Operations Insight 1.4.0.5 release

The Netcool Operations Insight V1.4.0.5 solution includes features delivered by the fix packs and fix pack extensions of the following products and versions:

- Network Manager V4.2.0.3
- Network Health Dashboard V4.2.0.3
- Netcool Configuration Manager V6.4.2.4

All of the other products and components are unchanged from the Networks for Operations Insight 1.4.0.4 March 2017 release.

The products are available on Passport Advantage and Fix Central. See <http://www.ibm.com/support/fixcentral/>

More information: “Supported products and components” on page 3

## Known problems at eGA

The following problems with IBM Netcool Operations Insight V1.4.0.4 March release were known at the time of eGA.

- “Device Dashboard”
- “Event Analytics” on page 295
- “Event Search” on page 297
- “Globalization” on page 298
- “Network Health Dashboard” on page 299
- “Operations Analytics - Log Analysis” on page 300

### Device Dashboard

#### Structured configuration browser error

When you open the **Device Dashboard**, you receive a content encoding error message. This is harmless error message that can be ignored.

#### Widget does not refresh when right-clicking Event Viewer from within Device Dashboard

When right-clicking and selecting **Show Device Dashboard**, the widget does not refresh with the device details. To work around this issue, go to the **Event Viewer** and select the device or the relevant event, and right-click and select **Show Device Dashboard**.

#### Integration problem: Widgets do not open when selecting "Show Traffic"

When right-clicking and selecting **Show Traffic** from any network topology (for example, Hop View), widgets do not open. To work around this issue, find the device in **Event Viewer**, right-click and select **Show Traffic**.

#### Following refresh, the sparkline graph within Performance widget does not display correct values

Following automatic refresh of the Device Dashboard, the sparkline graph within Performance widget disappears. To work around this issue, close the Device Dashboard and relaunch it.

#### Device Dashboard does not launch from a Network Hop View opened within a new browser tab

If you launch a Network Hop View within a new browser tab by running the **Find in > Network Hop View** from any other GUI, then you will not be able to launch the Device Dashboard from that Network Hop View.

#### Changing the target Network Performance Insight server requires a back-end file change and modification of the settings within each user's Device Dashboard

If you need to change the target NPI server, then you must perform the following steps:

1. Edit the npι.properties file. This file is located by default at \$NMGUI\_HOME/profile/etc/tnm/npι.properties, where \$NMGUI\_HOME is by default /opt/IBM/netcool/gui/precision\_gui.
2. In the npι.properties file change the following properties to point to the new target NPI server:
  - npι.server.name
  - npι.host.name

3. Instruct each end user to go to the Device Dashboard and change the portlet preferences there to point to the new target NPI server. End users must do this because the portlet preferences override the properties defined in the `npi.properties` file.
4. Stop and then restart the WebSphere Application Server.

**On first launch the Device Dashboard sometimes does not display data**

When you first launch the Device Dashboard, the dashboard widgets sometimes do not populate with data. If this happens, select a device in the **Topology** widget within the Device Dashboard to populate the dashboard.

## Event Analytics

**When displaying seasonal events, sorting the list causes previously applied filter to disappear**

When displaying seasonal events in the Seasonal Events portlet, if you first apply a filter to see a restricted set of seasonal events, and then you subsequently sort the filtered list by any of the currently displayed columns, the sort removes the filter. The filter is still shown in the filter box, but the sort now applies to an unrestricted set of seasonal events.

**Unable to export Event Analytics report using the load balanced ImpactUI configuration**

It is not possible to export Event Analytics reports in the Dashboard Application Services Hub when the ImpactUI data provider connection is using a HTTP server for ImpactUI Load Balancing. In this scenario, the export is prepared for download, but on clicking the download link the export fails with the following browser error message:

*Error 500: java.io.IOException: Unable to validate authorization*

To avoid this issue, provide a direct connection to the ImpactUI data provider in the Dashboard Application Services Hub connections page and export the report using this Netcool/Impact data provider connection.

**After exporting Event Analytics reports you might need to log back in**

After exporting an Event Analytics report, if the browser cache that was used to run the export is emptied or cleared prior to the export, then you will be logged out of Dashboard Application Services Hub automatically, immediately following the report export. You will need to log back in on the main Dashboard Application Services Hub screen in order to get back into the system.

**As of the Netcool Operations Insight V1.4.0.4 March 2017 release indexes are no longer automatically created on the events history table**

As of the Netcool Operations Insight V1.4.0.4 March 2017 release, Netcool/Impact no longer automatically creates indexes on the events history table for the filter date column (FIRSTOCCURRENCE by default) and the Identity field for seasonality.

Instead it is the responsibility of the database administrator to construct (and maintain) appropriate indexes on the REPORTER

history database. The database administrator should review the filter fields for the reports as a basis for an index, and should also review if an index is required for Identity fields.

**Blank fields during creation of synthetic event on non-occurrence.**

Users are given the option to supply one or more values for additional columns by selecting **Set additional fields**. With the exception of the values specified in the **Create Event** window, only the values of Node and Summary are copied into the synthetic event.

**Removing Netcool/Impact data models that are no longer needed.**

This issue refers to the following Netcool/Impact data models that are no longer needed after you upgrade to the IBM Netcool Operations Insight fix pack. Use the Netcool/Impact GUI to remove these data models:

**ObjectServerHistoryDB2ForSeasonality**

**ObjectServerHistoryOrclForSeasonality**

**ObjectServerHistoryMSSQLForSeasonality**

**Note:** If you choose not to remove these data models, there is no impact to the Event Analytics functionality. You would remove these data models only for cosmetic purposes.

**Note:** See **Notes on upgrading** in the “New features” on page 293 section of these Release Notes for information about upgrading.

**Event summary is truncated**

The event summary is occasionally truncated in the **Related Events Details** portlet Timeline view. To view the event summary, modify the screen resolution temporarily.

**Seasonal event rule with time condition does not run**

A seasonal event rule, with an action to run after a specific time that is more than 25 seconds, is not run. To ensure that a seasonal event rule that is scheduled to run after a specific time runs correctly, select a time condition of less than or equal to 25 seconds.

**Edit selection window hangs when 'selecting all' for a large number of related events during seasonal event rule creation**

When creating a seasonal event rule for an event with a large number of related events, you can check the **Select all related events** check box to associate all the related events with the seasonal event rule. The problem occurs when a large number of related events, on the order of 1000 or more, are selected and **Edit selection** is clicked. The **Edit selection** window is displayed but it remains in a loading state.

To avoid this issue, split the report into smaller reports and create rules around reports with fewer related events.

**Incorrectly displaying 'No event selected' error message**

When creating a pattern for related events and clicking **Use Selected Event as Template**, if you have not selected an event, the system correctly displays the 'No event selected' error message. However, if you then do select an event and click **Use Selected Event as Template** again, the error message persists

In this case, you can disregard and close the error message. It will not affect the creation of the pattern.

### **When testing an event pattern collapsed sections do not display correctly when reopened**

Following testing of an event pattern, if you collapse the **Groups**, **Group Instances**, and **Events** sections in the **Test** tab of the **Events Patten GUI** using the splitters provided and then you expand the sections again, the data columns in the **Groups** and **Events** panels become very narrow and the data cannot be read.

To work around this issue, you can do one of the following:

- Resize the window frame. This causes the columns to resize so that the data becomes visible.
- Manually resize the column widths or refresh the page. Either of these actions causes the columns to be displayed correctly again

## **Event Search**

### **HeatMap chart types do not render correctly**

The HeatMap type charts fail to render when using IBM Operations Analytics - Log Analysis V1.3.3, displaying the following error: Parameter category is invalid for Heat Map. The error is caused by a difference in the way charts are defined in Operations Analytics - Log Analysis 1.3.2 and 1.3.3.

The following charts are affected:

- In **OMNIBusInsightPack > Last Day > Dynamic Event Dashboard**:
  - Hotspots by Node and Alert Group
  - Hotspot by AlertGroup and Severity
- In **OMNIBus\_Static\_Dashboard**, opened from the Web GUI **EventSearch** tab by right-clicking and selecting **Show Event Dashboard by Node**:
  - Hotspots by Node and AlertGroup
  - Hotspots by AlertGroup and Severity

To correct this problem, edit the following chart specification files, and search for all instances of category and change them to categories:

- \$UNITY\_HOME/AppFramework/Apps/OMNIBusInsightPack\_v1.3.0.2/Last\_Day/OMNIBus\_Dynamic\_Dashboard.app
- \$UNITY\_HOME/AppFramework/Apps/OMNIBusInsightPack\_V1.3.0.2/OMNIBus\_Static\_Dashboard.app

### **Right-click keyword search results hidden by default**

This issue affects Event Search prior to Operations Analytics - Log Analysis version 1.3.5. When using the Event Search right-click menu within Web GUI and selecting **Show keywords and event count**, the search results in Event Search are empty. The problem is caused by the **Search Patterns** pane being hidden by default in the Operations Analytics - Log Analysis user interface.

To view the **Show keywords and event count** results, click the **Restore Section** triangle icon on the left side of the Event Search user interface.

### **Hotspots by Node, AlertKey not displaying.**

If the **Hotspots by Node, Alert Group and AlertKey** chart fails to display in the Last\_Month->Operational Status Dashboard the SOLR heap size might need increasing.

**Note:** The **Hotspots by Node, Alert Group and AlertKey** chart is CPU intensive and can be slow to render for systems with a large amount of data.

More information: Search runtime exceptions and IBM SmartCloud Analytics - Log Analysis Performance and Tuning Guide.

### **Hover values for the Event Trend by Severity charts do not appear to match the axes.**

When hovering over a point on a particular severity the values returned might not appear to match the axes on the chart. It is because the hover values represent that severity only, whereas the values on the axes are cumulative. For example, if there are 20 Intermediate severity events and 26 Major severity events displayed on the line above, the Major events will appear against 46 on the Y-axis.

### **Drill down does not return results.**

The drill down function is not available for the type Omnibus Tree Map. This affects some of the charts in the Operational Efficiency dashboard in the Last Month folder, and in the OMNIBus Operations Manager and OMNIBus Spot Important Alerts dashboards in the Last Hour folder.

If drill down is required for these charts you can use the default **Tree Map** specification instead. To change specification, click the chart settings icon on the right of the chart and change **Chart Type** from **OMNIBus Tree Map** to **Tree Map**.

### **Help text not rendered correctly for Event Analysis and Reduction in bi-directional locales.**

This affects the help text in the **Event Analysis and Reduction** dashboards for **Analyze and Reduce Event Volumes**, **Introduction to the Apps**, and **Helpful Links**. The help text is not rendered correctly in the Arabic and Hebrew locales.

You can view text directly as an HTML file in a browser that supports bi-directional locales. The relevant files are `Analyze_and_reduce_event_volumes.html`, `Introduction_to_the_Apps.html`, and `Helpful_links.html`. The files are located in `$UNITY_HOME/AppFramework/Apps/OMNIBusInsightPack_v1.3.0.2/locale/<LOCALE>/LC_MESSAGES`.

## **Globalization**

The following issues affect the non-English language versions of Netcool Operations Insight.

### **Event Search: count and time stamp hover help are not translated in some charts**

This issue affects the OMNIBusInsightPack\_v1.3.0.2. The following texts are not translated and appear in English only:

- Hover help for time stamp and count in stacked bar charts, heat maps and pie charts



- Legend for the **Count** field in the “Hotspots by Node and AlertGroup” chart and “Hotspots by AlertGroup and Severity” chart of the xxxOMNIBus Static Dashboard custom app
- Legend for the **Count** field in the “Last Day - Hotspots by AlertGroup and Severity” chart, “Last Day - Event Storm by Node” chart, and “Last Day - Hotspots by Node and AlertGroup” of the OMNIBus Dynamic Dashboard custom app

**Network Health Dashboard: In the Top Performers widget, the Japanese translation of the time to refresh is not displayed correctly**

In the Top Performers widget, the Japanese translation of the time to refresh is not displayed correctly. The correct word order in Japanese has the number preceding the text; however, the word order displayed has the number following the text.

**Topology Search: error message only partially translated**

This issue affects the Network Manager Insight Pack V1.3.0.0. If you attempt to run a topology search between two nodes on the same device, the error message that is displayed is only partially translated. The error message in full is as follows:

An error occurred calculating the path between 'X' and 'X',  
The source and destination Node's cannot be the same

(Where X is the value of the **NmosObjInst** for the device. The first half of the message, An error occurred calculating the path between 'X' and 'X', is translated. The second half of the message The source and destination Node's cannot be the same is not translated and always appears in English.

## **IBM Installation Manager**

**Console mode: cannot install Netcool/OMNIBus core and Web GUI or Netcool/Impact at the same time.**

When you install Netcool/OMNIBus core and Web GUI or Netcool/Impact at the same time with Installation Manager - console mode, the installation paths for Web GUI and Netcool/Impact are not prompted for and the installation fails. If you are performing the installation with Installation Manager - console mode, you must install the components separately.

**Note:** Installing Jazz for Service Management and IBM WebSphere Application Server is not supported for Installation Manager - console mode.

## **Network Health Dashboard**

**You must install the Network Health Dashboard with the Network Manager GUI Components**

If you want to install the Network Health Dashboard, you must install it in the same IBM Installation Manager session as the Network Manager GUI Components. Otherwise, some interaction between widgets and pages might not work.

**You must roll back the Network Manager GUI Components and the Network Health Dashboard packages together**

If you have installed the Network Manager 4.2 GA release and the Network Health Dashboard, and you then updated to 4.2 Fix Pack 1, and at this point you want to roll back one or more packages, then you must roll back the Network Manager GUI Components

and the Network Health Dashboard packages together. If you roll back one of these packages without the other, there is a risk that your system will become corrupted.

### **Operations Analytics - Log Analysis**

#### **Operations Analytics - Log Analysis installation fails**

Operations Analytics - Log Analysis V1.3.x requires a minimum 5 GB disk space on all supported operating systems. If less than 5 GB is found, the installer hangs. No error message is displayed. If this problem occurs, terminate the installer.

### **Support**

IBM Electronic Support offers a portfolio of online support tools and resources that provides comprehensive technical information to diagnose and resolve problems and maintain your IBM products. IBM has many smart online tools and proactive features that can help you prevent problems from occurring in the first place, or quickly and easily troubleshoot problems when they occur. For more information, see:

<http://www.ibm.com/support/electronicssupport>

#### **Related concepts:**

“Solution overview” on page 1

---

## Creating your own PDF of a subset of topics using My Collections

When you sign in to IBM Knowledge Center, you can save individual topics, groups of topics, or entire collections. After you save content by adding it to My Collections, you can rearrange topics, delete them, rename them, and then format them as PDF files.

### To add a topic to a collection:

In the table of contents, right-click a topic and select **Add this topic to an existing collection** or **Add this topic to a new collection**. Alternatively, you can click **Add to Collection**.

### To change the order of topics in a collection:

In the My Collections pane, select a collection and click **Edit**. Use the arrow keys to move the topic up or down in the collection hierarchy.

### To remove a topic from a collection:

In the My Collections pane, select a collection and click **Edit**. Then, click the X next to the topic title.

### To rename a collection:

In the My Collections pane, select a collection and click **Edit**. Click the collection title and enter a new name for the collection.

### To create a PDF file of the collection:

In the My Collections pane, select a collection and click **Create PDF File**.



---

## Notices

This information was developed for products and services offered in the U.S.A. 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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (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.  
1623-14, Shimotsuruma, Yamato-shi  
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

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 states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply 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 Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758 U.S.A.

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://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.



Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

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

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

Other product and service names might be trademarks of IBM or other companies.