

Course Guide

IBM Netcool Operations Insight 1.6 Implementation and Configuration

Course code TN522 ERC 1.0



August 2019 edition

NOTICES

This information was developed for products and services offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America*

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 may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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.

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.

TRADEMARKS

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

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

IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

Linux is a registered 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.

© Copyright International Business Machines Corporation 2016.

This document may not be reproduced in whole or in part without the prior written permission of IBM.

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

Contents

About this course	ix
About the student	x
Learning objectives	xi
Course agenda	xii
1 Netcool Operations Insight introduction and overview	1
Objectives	2
Lesson 1 Overview	3
Netcool Operations Insight base features	4
Networks for Operations Insight	5
Additional optional components	6
Event search (1)	8
Event search (2)	9
Event Analytics: Related Events	10
Event Analytics: Seasonality	11
Networks for Operations Insight	12
Topology search	13
Network Health Dashboard	14
Base solution components	15
Optional network management components	16
Lesson 2 Architecture	17
Netcool Operations Insight 1.6 with Network option	18
Data flows for the base Netcool Operations Insight solution	19
Netcool Operations Insight user interface technology	20
Data flow with network manager option	21
Student exercises	23
Summary	24
2 Installing IBM Netcool Operations Insight base	25
Objectives	26
Lesson 1 Overview	27
Complete installation	28
IBM Prerequisite Scanner	29
Checking maxproc and ulimit settings	30
Installing IBM Installation Manager	31
Lesson 2 Netcool/OMNIbus core	32
Netcool/OMNIbus core component requirements	33
Installing Netcool/OMNIbus core	34
Installation	35
Installing JDBC gateway	36

Configuring the gateway	37
Postinstallation configuration	38
Lesson 3 Netcool/OMNibus Web GUI	39
Installing Netcool/OMNibus Web GUI	40
Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub	41
Installing Web GUI and extensions	42
Installing Web GUI and extensions (2)	43
Postinstallation configuration	44
Configuring LDAP as an authentication source	45
Lesson 4 Netcool/Impact	47
Installing Netcool/Impact 7.1.0.16	48
Installation (1)	49
Installation (2)	50
Configuring single sign-on between Jazz and Netcool/Impact	51
Integrating the Netcool/Impact console (1)	52
Integrating the Netcool/Impact console (2)	53
Integrating the Netcool/Impact console (3)	54
Lesson 5 IBM Operations Analytics Log Analysis	55
Installing Log Analysis 1.3.5.3	56
Installation	57
Configuring single sign-on between Jazz and Log Analysis	58
User administration basics	59
Enabling Log Analysis product key	62
Student exercises	63
Summary	64
3 Configuring IBM Netcool Operations Insight base	65
Objectives	66
Lesson 1 Configuring Event Search	67
Event Search overview	68
OMNIBus Insight Pack	69
Installing the OMNIBus Insight Pack	70
Creating the event data source (1)	71
Creating the event data source (2)	72
Creating the event data source (3)	73
Log Analysis Gateway	74
Configuring SSL (1)	75
Configuring SSL (2)	76
ObjectServer modifications	77
Installing the message bus gateway	78
Configuring the gateway (1)	79
Configuring the gateway (2)	80
Configuring the gateway (3)	81
Configuring the gateway (4)	82
Lesson 2 Verifying Event Search	83
Running a search	84
Verifying launch-in-context	85

Verifying search results	86
Lesson 3 Configuring Event Analytics	87
Feature overview	88
Viewing related events	89
How seasonality is determined	90
Example seasonal report	91
Event Analytics administration	92
Related Events workflow	93
Prerequisite	94
Configuration (1)	95
Configuration (2)	96
Postinstallation configuration: ObjectServer data source	97
Postinstallation configuration: Event archive data source	98
Postinstallation configuration (1)	99
Postinstallation configuration (2)	100
Postinstallation configuration (3)	101
Student exercises	102
Summary	103
4 IBM Tivoli Network Manager	104
Objectives	105
Lesson 1 Installing Network Manager	106
Installation overview	107
Installing database creation scripts	108
Creating the topology database	109
Installing Network Manager core components	110
ObjectServer Configuration	111
Network Manager users	112
Network domain name	113
Topology Database	114
Poller Aggregation	115
Installing Network Manager GUI components	116
Jazz for Service Management	117
ObjectServer Configuration	118
Network Manager users	119
Topology Database	120
Installing Network Manager Reports	121
Jazz for Service Management	122
Administrator Credentials	123
Topology Database	124
Installing Network Health Dashboard	125
Jazz for Service Management	126
Administrator Credentials	127
Lesson 2 Post installation configuration	128
Configuring Web GUI data source name	129
Configuring core components to run as non-root user	130
Configuring processes to start automatically	131
Configuring Network Manager environment variables	132

Starting Network Manager	133
Lesson 3 Installing and configuring Topology Search	134
Feature overview	135
Implementation summary	136
Installing the Network Manager Insight Pack	137
Configuring the Network Manager Insight Pack	138
Configuring Network Manager users for Log Analysis access (1)	140
Configuring Network Manager users for Log Analysis access (2)	141
Configuring Network Manager users for Log Analysis access (3)	142
Modifying the ObjectServer	143
Adding topology search tools to Web GUI	144
Adding topology search tools to Network Manager GUI (1)	145
Adding topology search tools to Network Manager GUI (2)	146
Configuring users for access to topology search tools	147
Student exercises	148
Summary	149
5 IBM Tivoli Netcool Configuration Manager	151
Objectives	152
Lesson 1 Overview	153
Network configuration and change control manager	154
Deployment architecture	155
Presentation server tasks	156
Worker server tasks	157
Evaluation server tasks	158
Relational database tasks	159
Installation prerequisites	160
Lesson 2 Creating the database	161
Operating system users	162
Creating the database	163
Modifying the database transaction log size	164
Adding user defined functions to the database	165
Lesson 3 Installing Jazz for Service Management	166
Coexisting with Netcool Operations Insight	167
Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (1)	169
Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (2)	170
Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (3)	171
Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (4)	172
Change installation directory (1)	173
Change installation directory (2)	174
Complete the installation	175
Verifying access	176
Lesson 4 Installing Netcool Configuration Manager	177
Installation	178

Installation directory	179
Features	180
Database Configuration	181
Server Configuration (1)	182
Server Configuration (2)	183
NCM JazzSM Details	184
Installation complete	185
Installing GUI components	186
Features	187
Jazz for Service Management	188
Administrator Credentials	189
Database Configuration	190
ITNCM Presentation Server	191
ITNCM Reporting Server	192
Installation complete	193
Installing Common Reporting reports	194
Features	195
Database Configuration	196
TCR properties	197
Installation complete	198
Starting the server	199
Stopping the server	200
Lesson 5 Installing Device Drivers	201
Preparing for driver installation	202
Installing the standard drivers	203
Installing the Smart Model drivers	204
Installing Autodiscovery	205
Lesson 6 Post installation configuration	206
Configuring Java Webstart (1)	207
Configuring Java Webstart (2)	208
Configuring Java Webstart (3)	209
Configuring Java Webstart (4)	210
Configuring SNMP trap destination	211
Updating Work Distribution Resource	212
Adding a realm	213
Configuring device passwords (1)	214
Configuring device passwords (2)	215
Lesson 7 Configuring integration with Network Manager	216
Integration overview	217
Configuring groups and users in WebSphere	218
Adding existing users to Configuration Manager groups	219
Assigning Dashboard Application Services Hub roles	220
Configuring the presentation server to use LDAP	221
Adding LDAP to the Virtual Member Manager realm: Step 1	222
Adding LDAP to the Virtual Member Manager realm: Step 2	223
Adding LDAP to the Virtual Member Manager realm: Step 3	224
Adding LDAP to the Virtual Member Manager realm: Step 4	225
Adding LDAP to the Virtual Member Manager realm: Step 5	226

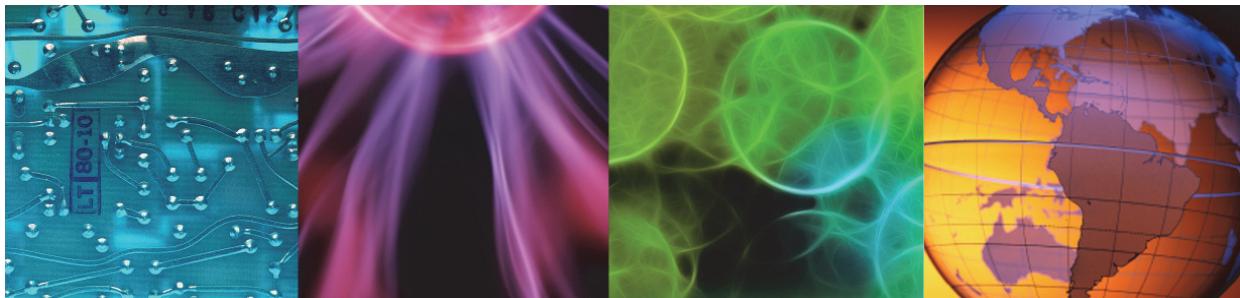
Adding LDAP to the Virtual Member Manager realm: step 6227
Configuring the presentation server for single sign-on228
Importing the Dashboard Application Services Hub LTPA keys229
Configuring single sign-on attributes230
Importing the Dashboard Application Services Hub SSL certificate (1)231
Importing the Dashboard Application Services Hub SSL certificate (2)232
Enabling single sign-on for Configuration Manager233
Configuring access rights for existing users (1)234
Configuring access rights for existing users (2)235
Configuring access rights for existing users (3)236
Configuring integration with Netcool/OMNIbus (1)237
Configuring integration with Netcool/OMNIbus (2)238
Configuring device synchronization239
Lesson 8 Out-of-band change240
Reasons for out-of-band change241
Out-of-band change242
OOBC process243
Installation prerequisites244
Installing the OOBC software245
Installation questions246
Files in the execution directory248
Configuring OOBC249
Startup and shutdown250
Student exercises251
Summary252
6 Verifying Networks for Operations Insight253
Objectives254
Lesson 1 Solution verification255
Configuring network discovery256
Running a network discovery257
Discovery complete258
Network view259
Verifying integration with Configuration Manager260
Imported devices261
Device configuration262
Verifying Compliance Management263
Compliance results264
Verifying compliance remediation265
Remediation results266
Verify remediation267
Configuration Manager traps268
Device Activity Viewer269
Topology search270
Student exercises271
Summary272



About this course



IBM Netcool Operations Insight 1.6 Implementation and Configuration



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This 4-day class teaches you how to install the Netcool for Operations Insight components, including Networks for Operations Insight.

On Day 1 and Day 2 of this class, you install Netcool/OMNIbus, Netcool/OMNIbus Web GUI, Netcool/Impact, and IBM Operations Analytics Log Analysis. In addition, you install and configure the event search and event analytics features that are unique to Netcool Operations Insight. On Day 3, you install IBM Tivoli Network Manager IP Edition and the topology search feature. On Day 4, you install IBM Tivoli Netcool Configuration Manager and verify the solution.

The lab environment for this course uses the Red Hat Enterprise Linux platform.

For information about other related courses, visit the Cloud & Smarter Infrastructure education training paths website:

ibm.com/software/software/tivoli/education/

Details	
Delivery method	Classroom or instructor-led online (ILO)
Course level	ERC 1.0 This course is a new course.
Product and version	Netcool Operations Insight V1.6
Duration	4 days
Skill level	Intermediate

About the student

This course is designed for administrators who must install Netcool Operations Insight.

Before taking this course, make sure that you have the following skills:

- Install and configure Netcool/OMNIBus core
- Install and configure Netcool/OMNIBus Web GUI
- Install and configure Netcool/Impact
- Install and configure IBM Operations Analytics Log Analysis
- Install and configure IBM Tivoli Network Manager IP Edition
- Install and configure IBM Tivoli Netcool Configuration Manager

Before taking this course, make sure that you take the following courses:

- TN025 IBM Netcool/OMNIBus 8.1 Installation and Configuration
- TN045 IBM Tivoli Netcool/Impact Administration and Implementation
- TN325 IBM Tivoli Network Manager IP Edition 4.2 Operations and Administration
- TN630 IBM Operations Analytics Log Analysis 1.3 Administration
- TOD44 IBM Tivoli Netcool Configuration Manager 6.4.2: Operations and Configuration

Learning objectives

Objectives

In this course, you learn to perform the following tasks:

- Install the following components of IBM Netcool Operations Insight base, among others:
 - Netcool/OMNIbus core V8.1.0.19
 - Netcool/OMNIbus Web GUI V8.1.0.16
 - Netcool/Impact V7.1.0.16
 - IBM Operations Analytics Log Analysis V1.3.5.3
- Configure event search and event analytics features
- Install the following components of Networks for Operations Insight, among others:
 - IBM Tivoli Network Manager IP Edition V4.2.0.7
 - IBM Tivoli Netcool Configuration Manager V6.4.2.8
 - Install and configure the topology search feature

© Copyright IBM Corporation 2019

Course agenda

The course contains the following units:

1. [Netcool Operations Insight introduction and overview](#)

This unit provides an introduction to the features, and functions of Netcool Operations Insight.

2. [Installing IBM Netcool Operations Insight base](#)

This unit provides an overview of the installation of the products that are used in Netcool Operations Insight.

3. [Configuring IBM Netcool Operations Insight base](#)

In this unit, you complete the installation of Netcool Operations Insight base components, configure the components, and verify their function.

4. [IBM Tivoli Network Manager](#)

In this unit, you learn how to install and configure IBM Tivoli Network Manager.

5. [IBM Tivoli Netcool Configuration Manager](#)

In this unit, you learn how to install and configure Netcool Configuration Manager.

6. [Verifying Networks for Operations Insight](#)

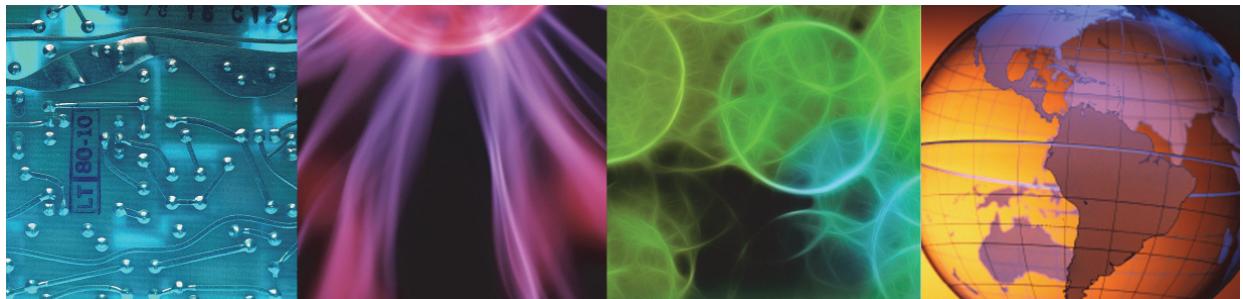
In this unit, you verify the basic features of the Networks for Operations Insights solution.



1 Netcool Operations Insight introduction and overview



Netcool Operations Insight introduction and overview



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This unit provides an introduction to the features, and functions of Netcool Operations Insight.

Objectives

In this unit, you learn to perform the following tasks:

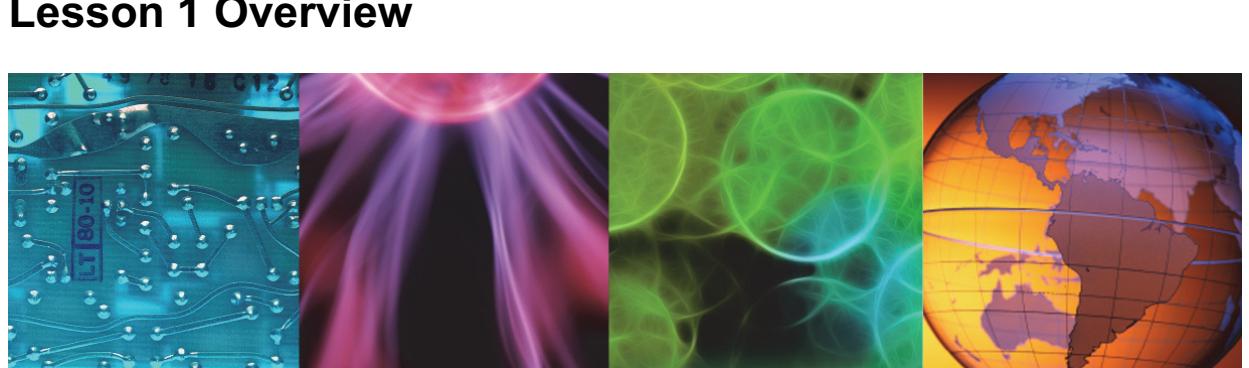
- Describe the major functions of Netcool Operations Insight
- Explain the concept of Event Search
- Explain the concept of Event Analytics
- Describe the deployment architecture

© Copyright IBM Corporation 2019

Objectives



Lesson 1 Overview



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn about the features and functions of Netcool Operations Insight.

Netcool Operations Insight base features

- Event search
 - Applies the search and analysis capabilities of Operations Analytics Log Analysis to events that are monitored and managed by Tivoli Netcool/OMNibus
 - ObjectServer events ingested by Log Analysis and indexed for searching
- Event Analytics
 - Netcool/Impact performs statistical analyses of Tivoli Netcool/OMNibus historical event data

© Copyright IBM Corporation 2019

Netcool Operations Insight base features

IBM Netcool Operations Insight uses real-time alarm and alert analytics, which are combined with broader historic data analytics. Netcool Operations Insight uses 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.

The main features of the base solution are as follows:

- Event search

Combines the features of Netcool/OMNibus for comprehensive event management with the search capabilities of IBM Operations Analytics Log Analysis.

- Event Analytics

Netcool/Impact analyzes events from the Netcool/OMNibus event archive database. The analysis looks for events that repeat and events that are related.

Networks for Operations Insight

- Optional feature that can be added to a deployment of the base Netcool Operations Insight solution
 - Integrates IBM Tivoli Network Manager and IBM Tivoli Netcool Configuration Manager
- Topology search
 - An extension of the Networks for Operations Insight feature
 - Applies the search and analysis capabilities of Operations Analytics Log Analysis to give insight into network diagnostics
- Network Health Dashboard
 - Monitors a selected network view
 - Displays device and interface availability within the selected view
 - Reports on performance by presenting graphs, tables, and traces of KPI data for monitored devices and interfaces

© Copyright IBM Corporation 2019

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.

Additional optional components **

Network Performance Insight

- SNMP and Flow-based network traffic performance monitoring system
- Provides comprehensive and scalable visibility on network traffic with visualization and reporting of network performance data for complex, multivendor, multi-technology networks

IBM Cloud Event Management

- Provides instant notification of alerts for any critical IT issues across multiple monitoring tools
- Easily create, publish, and manage runbooks and automations
- Quickly connect to cloud-based alert sources

IBM Agile Service Manager

- Provides operations teams with up-to-date visibility and control over dynamic infrastructure and services
- Maintain a historical view of resources and relationships so you can compare topologies at two points in time to understand how resources, relationships and state has changed

** These products are not covered in this course

© Copyright IBM Corporation 2019

Additional optional components

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

https://www.ibm.com/support/knowledgecenter/SSCVHB_1.3.1/npi_kc_welcome.html.

IBM Cloud Event Management

IBM Cloud Event Management can receive events from various monitoring sources, either on-prem or in the cloud, then consolidate related events into a manageable number of incidents. For more information, see

https://www.ibm.com/support/knowledgecenter/SSURRN/com.ibm.cem.doc/em_overview.html.

IBM Agile Service Manager

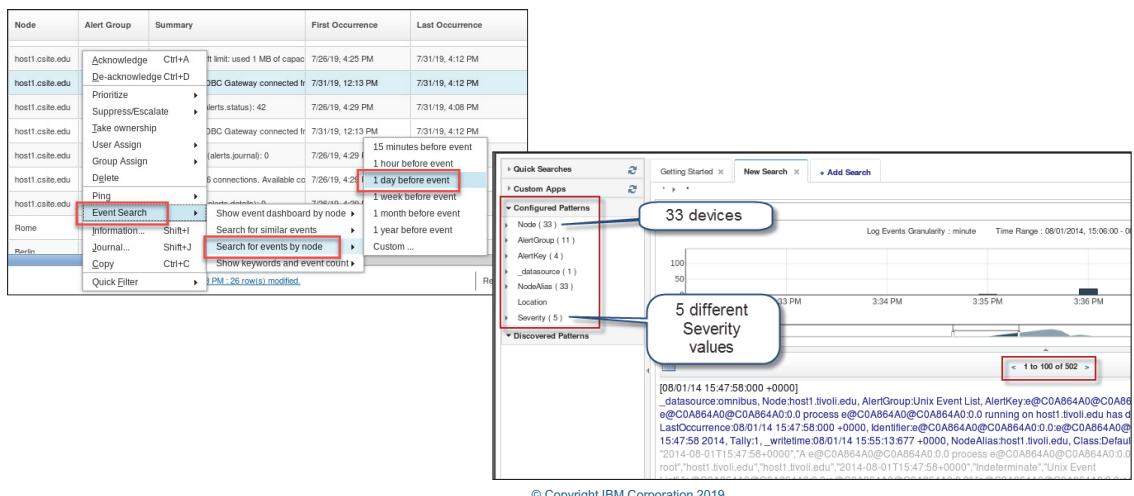
When a fault occurs in your IT infrastructure, you need to see more than just the current conditions of the environment; you need a way to go back in time and understand how the environment behaved up to and during an incident as part of your postmortem activities. IBM Agile Service Manager lets you query a specific networked resource, and then presents a configurable topology view of it within its ecosystem of relationships and states, both in real time and within a definable time window. IBM Agile Service Manager provides visibility of current behavior and, crucially, the ability to view historical topology.

For more information, see

https://www.ibm.com/support/knowledgecenter/en/SS9LQB_1.1.5/ProductOverview/c_asm_productoverview.html.

Event search (1)

- Log Analysis tools launch from right-click menus of the Event Viewer and the Active Event List
- Passes context to configure Log Analysis search



Event search (1)

Event search applies the search and analysis capabilities of Operations Analytics Log Analysis to events that Tivoli Netcool/OMNibus monitors and manages. Events are transferred from the ObjectServer through the Gateway for Message Bus to Operations Analytics Log Analysis, where they are processed into a data source 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 that shows how your monitoring environment is performing over time. You use keyword searches and dynamic drill-down functions to go deeper into the event data for detailed information. You can run the apps run from the Operations Analytics Log Analysis. You can install the tools into the Web GUI that starts the apps from the right-click menus of the Event Viewer and the Active Event List. An *event reduction wizard* is also supplied, which includes information and apps that can help you analyze and reduce volumes of events and minimize the *noise* in your monitored environment.

Event search (2)

- Custom apps generate dashboards that present event information about how your monitoring environment is performing over time



© Copyright IBM Corporation 2019

Event search (2)

Custom applications provide a one-click mechanism to retrieve events based on a defined time frame and generate comprehensive dashboards.

Event Analytics: Related Events

- Netcool/Impact evaluates historical event
- Determines which events have a statistical tendency to occur together
- Outputs the results on a scheduled basis as event groups
- You 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

Severity	Node	ScopeID	TicketNumber	Summary
	TLCO-TLCO/BPT-47495	TLCO-TLCO/BPT-47495	55784	INCIDENT: TLCO-TLCO/BPT-47495: 3 sites affected
	RT0748	TLCO-TLCO/BPT-47495	55784	RT0748: CAUSE AND IMPACT: Operational Warning, inc running on ba
	RT1297	TLCO-TLCO/BPT-47495	55784	RT1297: Service delivery reported as non-Functional caused by Perform
	RT1297	TLCO-TLCO/BPT-47495	55784	7705 *- LAPD FAILURE
	RT1297	TLCO-TLCO/BPT-47495	55784	7705 *- LAPD FAILURE
	RT1297	TLCO-TLCO/BPT-47495	55784	7767 ***- BCCH MISSING
	VC4282	TLCO-TLCO/BPT-47495	55784	VC4282: CAUSE AND IMPACT: Operational Warning, inc running on ba

© Copyright IBM Corporation 2019

Event Analytics: Related Events

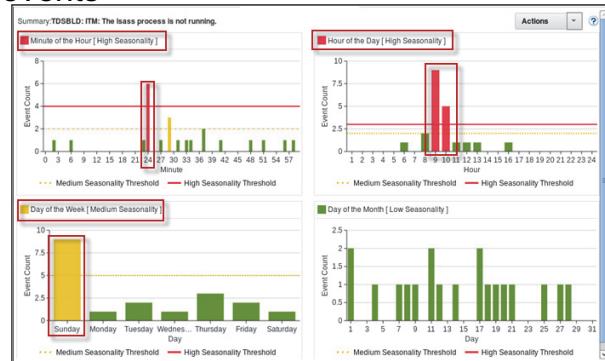
Event Analytics uses Netcool/Impact to perform statistical analyses of Tivoli Netcool/OMNibus historical event data. The results of the analysis are used in two manners. The first analytic feature is called Related Events.

The Related Events analysis determines which events have a statistical tendency to occur together and publishes the results on a scheduled basis as event groups. You can deploy 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 grouping reduces the number of events that are presented to operators.

Event Analytics: Seasonality

- Identifies seasonal patterns, such as when and how frequently events occur
- Seasonality analyses are published 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
- Use the information from the seasonality reports to create network, device, or suppression rules to reduce the number of events

Node	Summary	Alert Group	Reviewed By	Confidence Level
ducttape.tivlab.rule	TDSBLD: ITM: The lsass process is not running.	ITM_NT_Process		100%
s3w2k.tivlab.austin	Show Seasonal Event Graphs			100%
fw2w2k.tivlab.aust	Show Historical Events			100%
fw3w2k.tivlab.aust	Show Related Event Details			100%
rtpbwin1.tivlab.rule	Create Rule...			100%
rtpbwin1.tivlab.rule	Mark as Reviewed			100%
rtpbwin3b.tivlab.ral	Unmark as Reviewed			100%



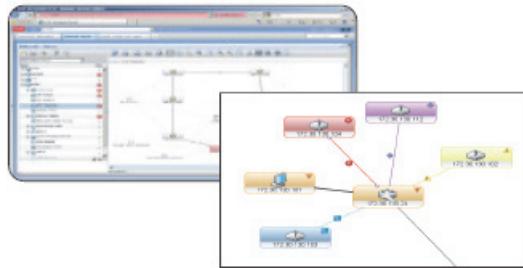
© Copyright IBM Corporation 2019

Event Analytics: Seasonality

The second type of analysis is called Seasonal Events, which identify seasonal patterns, such as when and how frequently events occur. Seasonality analyses are published 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.

Networks for Operations Insight

- IBM Tivoli Network Manager
 - Network discovery, visualization and automated root cause analysis



- Tivoli Netcool Configuration Manager
 - Network configuration and change management
 - Evaluate device configurations against a defined set of compliance policies



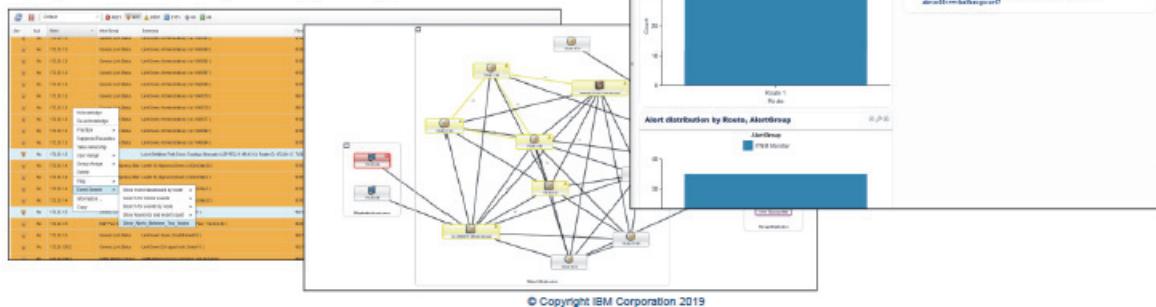
© Copyright IBM Corporation 2019

Networks for Operations Insight

Networks for Operations Insight is an optional feature that you can add 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. Networks for Operations Insight includes the Network Manager and Netcool Configuration Manager products.

Topology search

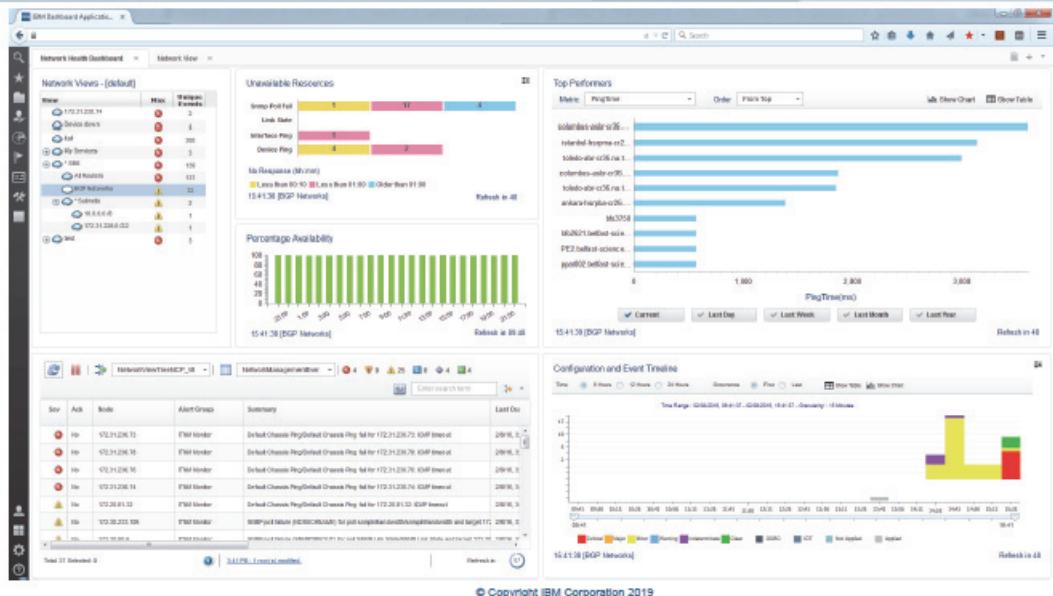
- Quickly identifies the routes between two devices from the network topology
- Generates a graph showing event severity summary for each route, revealing problematic routes
- Can be launched from
 - IBM Tivoli Network Manager topology view
 - Netcool/OMNIBUS Web GUI Event Viewer
 - Operations Analytics Log Analysis



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 diagnostics. The Network Manager Insight Pack analyzes events that are enriched with network data and calculates event statistics between two endpoints in the network topology over time. Topology search identifies the events that occurred along the routes over the specified time period and shows them by severity. The topology search requires the Networks for Operations Insight feature to be installed and configured.

Network Health Dashboard



Network Health Dashboard

A main feature that is provided by Networks for Operations Insight is the Network Health Dashboard. The Network Health Dashboard is only available if you have Network Manager as part of Netcool Operations Insight. The Network Health Dashboard monitors a selected network view, and displays device and interface availability within that network view. It also reports on performance by presenting graphs, tables, and traces of KPI data for monitored devices and interfaces. A dashboard timeline reports on device configuration changes and event counts, which you can use to correlate events with configuration changes. The dashboard includes the event viewer, for more detailed event information.

Base solution components

- Tivoli Netcool/OMNibus core V8.1.0.19
- Gateway for JDBC
 - Used to populate event archive database
- Tivoli Netcool/OMNibus Web GUI V8.1.0.16
 - With Netcool Operations Insight extensions
- Netcool/Impact V7.1.0.16
 - With Netcool Operations Insight extensions
- IBM Operations Analytics Log Analysis V1.3.5.3
- Tivoli Netcool/OMNibus Insight Pack V1.3.1 for IBM Operations Analytics Log Analysis
- Gateway for Message Bus V10.0
- Jazz for Service Management V1.1.2.1

© Copyright IBM Corporation 2019

Base solution components

The Netcool Operations Insight solution consists of the products that are shown on this slide. Each of these products is available for purchase individually. The Netcool Operations Insight solution includes features that are not available with the individual products when you purchase the products individually. The extensions are not available when the product is purchased individually.

Optional network management components

- IBM Tivoli Network Manager V4.2.0.7
- Probe for SNMP
- Syslog Probe
- Network Manager Insight Pack V1.3.5.0 for IBM Operations Analytics Log Analysis
- IBM Tivoli Netcool Configuration Manager V6.4.2.8
- Network Health Dashboard V4.2.0.1

© Copyright IBM Corporation 2019

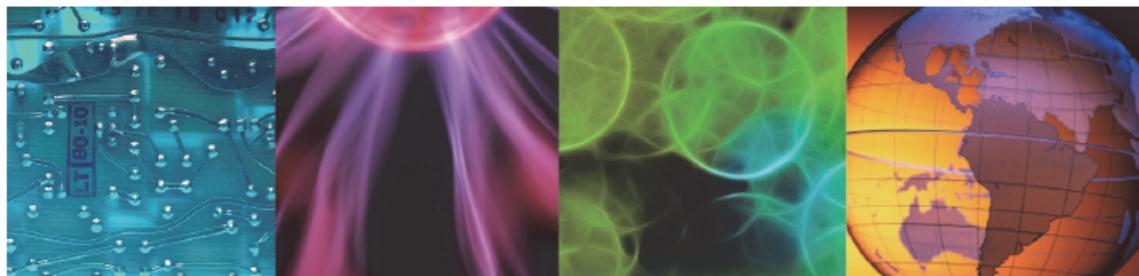
Optional network management components

This slide shows the products that comprise the network management option for Netcool Operations Insight.

Lesson 2 Architecture



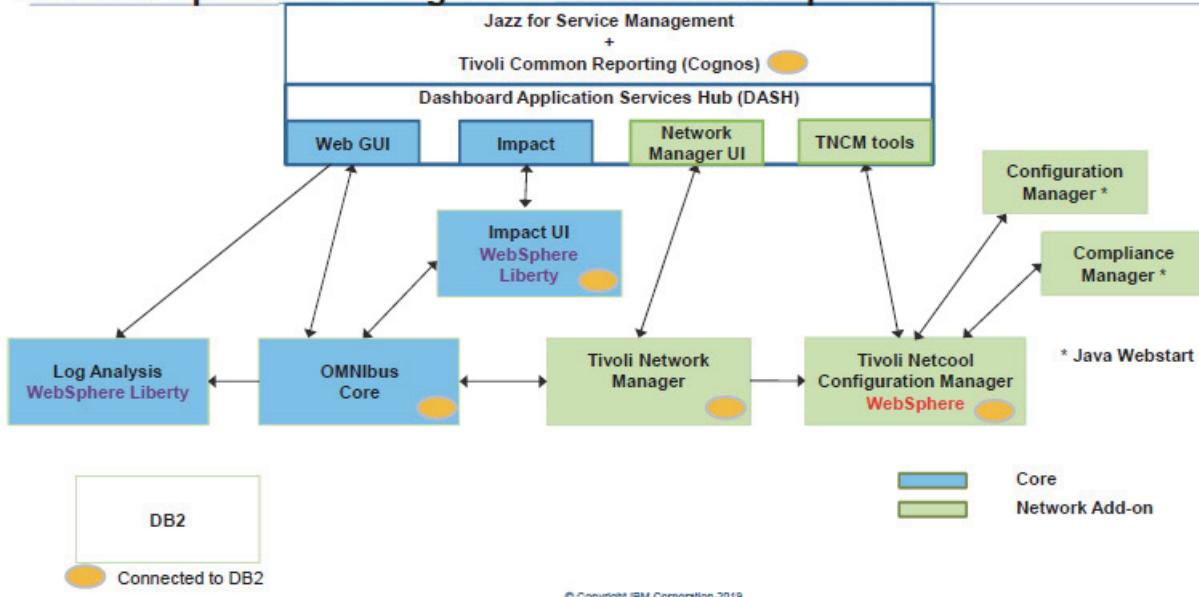
Lesson 2 Architecture



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to describe the architecture of the Netcool Operations Insight solution.

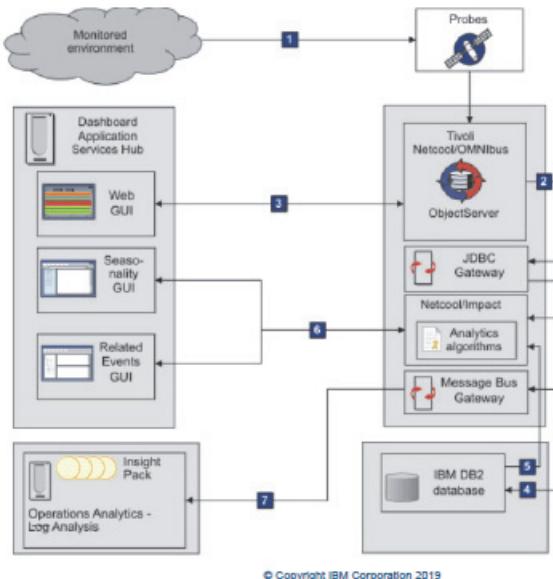
Netcool Operations Insight 1.6 with Network option



Netcool Operations Insight 1.6 with Network option

This slide illustrates the component architecture of the solution. The components in blue, on the left, represent the base solution and the components in green, on the right, represent the network option.

Data flows for the base Netcool Operations Insight solution



Data flows for the base Netcool Operations Insight solution

This slide illustrates the major steps in the flow of data within the solution.

1. Netcool/OMNibus probes receive status information from the monitored infrastructure. The probes normalize the information into a common format and send the data to an ObjectServer. The data is represented in the ObjectServer as an event.
2. The event records are periodically read from the ObjectServer by the following components:
 - JDBC Gateway
 - Netcool/Impact
 - Message Bus Gateway
3. The Web GUI server accesses the event records. Web GUI users can view event records and modify event records when they have the appropriate authority.
4. The JDBC Gateway reads events from the ObjectServer and writes the data to the event archive database. The archive database is supported on DB2, Oracle, and MSSQL.
5. Netcool/Impact reads records from the archive database for Event Analytics.
6. Web GUI provides administrative tools for configuring, running, and evaluating the results of Event Analytics.
7. The Message Bus Gateway reads events from the ObjectServer and converts the events into a format that is suitable for IBM Operations Analytics Log Analysis.

Netcool Operations Insight user interface technology

- **Base**

- *Netcool/OMNibus*

- Natively supports Dashboard Application Services Hub

- *Netcool Impact*

- Provides a Dashboard Application Services Hub widget for Operator View and CURI provider for data integration
 - Uses a separate Admin Server via WebSphere liberty

- *Log Analytics*

- Built on IBM Rave and uses WebSphere Liberty
 - Integration is driven via launch in context from Netcool/OMNibus Event Viewer

- **Network add-on**

- *IBM Tivoli Network Manager*

- Natively supports Dashboard Application Services Hub

- *Tivoli Netcool Configuration Manager*

- Uses WebSphere Application Server as main interface and also Java Web Start for full client

- Widgets are integrated into Dashboard Application Services Hub by a Netcool Operations Insight integration tool

© Copyright IBM Corporation 2019

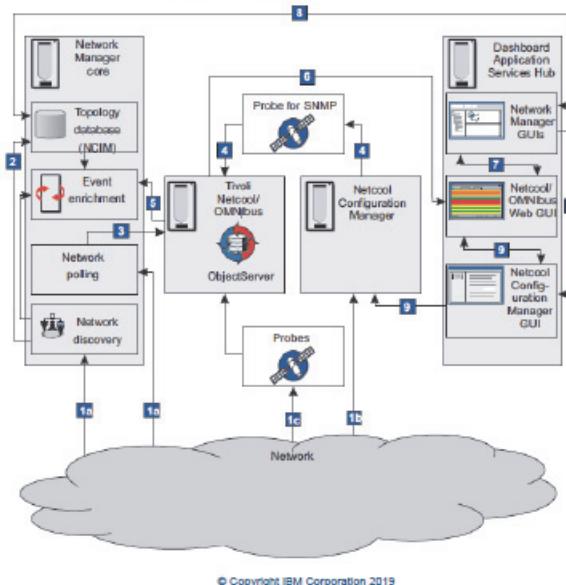
Netcool Operations Insight user interface technology

An important aspect of the Netcool Operations Insight solution is the combination of technologies that provide user access to the various products, including these examples:

- Dashboard Application Services Hub
- WebSphere Liberty

The solution incorporates single sign-on and other techniques to provide integration between the user interfaces without the need for multiple user names and passwords.

Data flow with network manager option



Data flow with network manager option

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 topology database.

3 Generation of network alerts

Network Manager generates fault alerts when 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 that are detected in Step 1b. Configuration change and policy violation events are sent with the Probe for SNMP to the ObjectServer.

5 Event enrichment

Network events, which are generated in Step 3, 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.

Configuration Manager events, which are generated in Step 4, are passed to the SNMP Probe. The probe can optionally add more data to the events.

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 Netcool/OMNIbus Web GUI displays the application events, network events, and network configuration events that are in the ObjectServer.

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 topology database.

9 Analysis of network configuration events

Configuration changes and policy violations are displayed in the Web GUI, the Netcool Configuration Manager Activity Viewer, wizards, and other Netcool Configuration Manager UIs.

Student exercises



© Copyright IBM Corporation 2019

Student exercises

Refer to the exercises for Unit 1 in the *Student Exercise Guide*.

Summary

You now should be able to perform the following tasks:

- Describe the major functions of Netcool Operations Insight
- Explain the concept of Event Search
- Explain the concept of Event Analytics
- Describe the deployment architecture

© Copyright IBM Corporation 2019

Summary



2 Installing IBM Netcool Operations Insight base



Installing IBM Netcool Operations Insight base



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

This unit provides an overview of the installation of the products that are used in Netcool Operations Insight.

Objectives

In this unit, you learn to perform the following tasks:

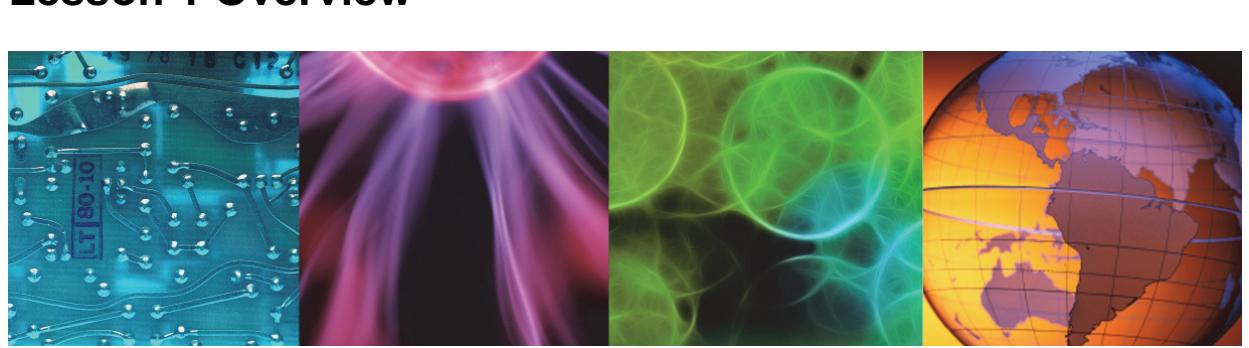
- Use the prerequisite scanner to verify the system requirements
- Install and configure Netcool/OMNIbus core components
- Install and configure Netcool/OMNIbus Web GUI
- Install and configure Netcool/Impact
- Install and configure IBM Operations Analytics Log Analysis

© Copyright IBM Corporation 2019

Objectives



Lesson 1 Overview



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to install Netcool Operations Insight V1.6.

Complete installation

A high-level list of the steps are as follows:

1. Verify hardware and software prerequisites
2. Install IBM Installation Manager on all target machines
3. Install Netcool/OMNibus Core
4. Install Netcool/OMNibus Web GUI
5. Install Netcool/Impact
6. Apply Event Analytics configuration and create Seasonality reports
7. Install IBM Operations Analytics Log Analysis
8. Install Networks for Operational Insights integration (optional)
9. Install and configure Tivoli Common Reporting and Event List tools (optional)
10. Configure processes to automatically start on machine boot (optional)

© Copyright IBM Corporation 2019

Complete installation

A complete installation requires the installation of the individual products and some additional steps that are unique to Netcool Operations Insight. The hardware and software requirements for the individual products is the same when used with the Netcool Operations Insight deployment. The solution also supports the high availability configurations that each product supports. This slide illustrates the major steps that are required for a complete installation.

Detailed instructions for a complete installation can be found here:

https://www.ibm.com/support/knowledgecenter/SSTPTP_1.6.0/com.ibm.netcool_ops.doc/soc/integration/task/int_installing-onprem.html

This course assumes that the student meets the prerequisites and is experienced with installing each of the base products. The focus of this course is on the installation and configuration of the additional components that comprise the Netcool Operations Insight solution.

IBM Prerequisite Scanner

The IBM Prerequisite Scanner must be run with each of the component codes as follows, where appropriate:

- prereq_checker.sh NOC detail (for IBM Netcool/OMNIbus)
- prereq_checker.sh NOW detail (for IBM Netcool/OMNIbus Web GUI)
- prereq_checker.sh NCI detail (for IBM Netcool/Impact)
- prereq_checker.sh ODP detail (for IBM Jazz for Service Management)
- prereq_checker.sh DSH detail (for IBM Dashboard Application Services Hub)
- prereq_checker.sh TNM detail (for IBM Tivoli Network Manager)
- prereq_checker.sh NCM detail (for IBM Tivoli Netcool Configuration Manager)
- prereq_checker.sh ILA detail (for IBM Operations Analytics Log Analysis)
- prereq_checker.sh TCR detail (for IBM Tivoli Common Reporting)

© Copyright IBM Corporation 2019

IBM Prerequisite Scanner

The prerequisite scanner provides a convenient mechanism to automatically verify most of the requirements for the Netcool Operations Insight solution. The scanner does not provide a single check for all requirements. Instead, you must run the scanner multiple times to verify the requirements for the individual products. In a production environment, the products are distributed across multiple servers. In that environment, you run the scanner on each server and verify the requirements for only the products that are hosted on each server. You install all components on one server in this course.

Checking maxproc and ulimit settings

Make sure that the maxproc and ulimit settings are set to the following minimum values:

- **maxproc**

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

- **ulimit**

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

© Copyright IBM Corporation 2019

Checking maxproc and ulimit settings

This slide illustrates the minimum values for two system parameters. The values that are shown here set these parameters to an *unlimited* maximum. The setting of unlimited is not a requirement but rather a recommendation.

Installing IBM Installation Manager

1. Download the software
 - a. Download it from IBM Fix Central from the following location
 - b. Expand the file to a temporary directory
2. Install the IBM Installation Manager
 - IBM Installation Manager is installed in user mode
 - userinst

© Copyright IBM Corporation 2019

Installing IBM Installation Manager

Every product in the solution is installed with IBM Installation Manager. Most, if not all, products bundle a copy of IBM Installation Manager with their respective installation file. In many cases, the versions of IBM Installation Manager that are bundled with the products are not the same. The recommendation is to manually install a copy of the current version of IBM Installation Manager before you install the individual products. You use that copy of IBM Installation Manager to install every product.

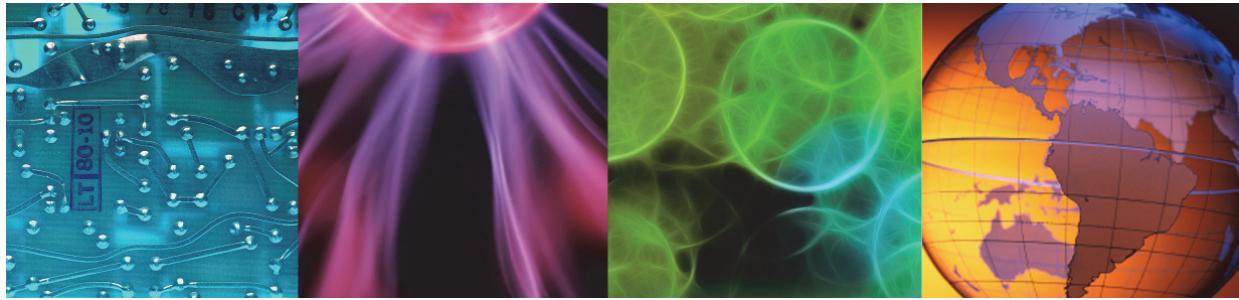


Important: Some product documentation suggests that you use the *group* mode when you install IBM Installation Manager. IBM Operations Analytics Log Analysis cannot be installed with IBM Installation Manager in *group* mode. You must use *user* mode when you install IBM Installation Manager.

Lesson 2 Netcool/OMNIbus core



Lesson 2 Netcool/OMNIbus core



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to install Netcool/OMNIbus core components.



Important: A prerequisite for this class is completion of the IBM Netcool/OMNIbus 8.1 Installation and Configuration course. The material in this unit is not a comprehensive description of how to install Netcool/OMNIbus core.

Netcool/OMNibus core component requirements

The following is the minimum feature set that is required for Netcool Operations Insight:

- Server components (includes ObjectServers)
- Probe and gateway feature
- Accelerated Event Notification (AEN) client
- Gateway for JDBC
 - Required for the base Netcool Operations Insight solution
 - It is installed by Installation Manager
 - It is required for the transfer of event data from the ObjectServer to the IBM® DB2 database
- Gateway for Message Bus
 - Required for the base Netcool Operations Insight solution
 - It is installed by Installation Manager
 - It is required for the transfer of event data from the ObjectServer to IBM Operations Analytics Log Analysis

© Copyright IBM Corporation 2019

Netcool/OMNibus core component requirements

Netcool/OMNibus core components are categorized into various features. Some of the features are required for other components. For example, the Probe Support feature is a requirement for the subsequent installation of one or more probes. The Netcool Operations Insight solution requires the features that are shown on this slide.

- Server components
- Probe and gateway
- Accelerated Event Notification

In addition to the core features that are listed, the Netcool Operations Insight solution also requires the Gateway for JDBC and the Gateway for Message Bus.

Installing Netcool/OMNIbus core

1. Download the software

- IBM Tivoli Netcool OMNIbus 8.1.0.19 Core - Linux 64bit Multilingual (CC28ZML)
- Expand to some temporary directory, for example:
/tmp/omnibus_core

2. Define the target installation directory

For example:

```
mkdir /opt/IBM/tivoli/netcool  
chown -R netcool:ncoadmin /opt/IBM/tivoli/netcool
```

3. Install Netcool/OMNIbus core with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
. ./IBMMIM
```

* Assumes that IBM Installation Manager is installed by the **netcool** user

© Copyright IBM Corporation 2019

Installing Netcool/OMNIbus core

This slide illustrates the basics steps that are required for the installation of Netcool/OMNIbus core. The material on the slide assumes that the software is installed as the **netcool** user.

Installation

1. Define software repository

/tmp/omnibus_core/OMNIbusRepository/repository.config

2. Select installation package

IBM Tivoli Netcool/OMNIbus Version 8.1.0.19

3. Default Netcool/OMNIbus installation directory

/opt/IBM/tivoli/netcool

4. Accept the default to install all features

Note the minimum required features from the previous slide

Note: Installation runs for approximately 10 minutes

5. Create the initial configuration

- Use the Initial Configuration Wizard
- Create an aggregation ObjectServer

© Copyright IBM Corporation 2019

Installation

The use of the Initial Configuration Wizard after the installation is suggested. Netcool Operations Insight supports Netcool/OMNIbus high availability and the multitier options. For the class exercise, you create a single ObjectServer.

Installing JDBC gateway

1. Download the software to a temporary directory

- Netcool/OMNIbus 8 Plus JDBC Gateway Configuration Scripts (Reporting Mode: nco-g-jdbc-reporting-scripts 1_0) Multiplatform English (CN1FLEN)
- Netcool/OMNIbus 8 Plus Gateway for JDBC (nco-g-jdbc 6_0) Multiplatform English (CN1FMEN)

Note: It is not necessary to expand the installation files

2. Install JDBC gateway with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
./IBMIM
```

3. Define software repositories

```
/tmp/jdbc/NCOMNI_GTW_JDBC.zip  
/tmp/jdbc/im-nco-g-jdbc-rpt-scripts-1_0.zip
```

4. Select installation packages

```
Netcool/OMNIbus Gateway nco-g-jdbc  
Netcool/OMNIbus Gateway nco-g-jdbc-reporting-scripts
```

© Copyright IBM Corporation 2019

Installing JDBC gateway

You use the Gateway for JDBC to save ObjectServer event records in an archive database. The event archive is a requirement for the Event Analytics feature of Netcool Operations Insight.

Configuring the gateway

1. Create database structure

Import supplied SQL file with the user that *owns the database*

```
cd /opt/IBM/tivoli/netcool/omnibus/gates/reporting/db2  
db2 -td@ -vf db2.reporting.old.sql
```

2. Configure the gateway

- a. Add the gateway name to the interfaces file
- b. Copy and rename to gateway configuration files
- c. Modify the gateway property file
- d. Modify the gateway startup file

3. Test the gateway and verify correct operation

© Copyright IBM Corporation 2019

Configuring the gateway

The gateway configuration does not require any steps that are unique to Netcool Operations Insight. The only requirement for Netcool Operations Insight is that the archive database must be implemented in *reporter* mode. Netcool Operations Insight does not support an archive database that is implemented in *audit* mode.

Post-installation configuration

1. Configure process activity agent

- The ObjectServer is configured by the Initial Configuration wizard
- Modify the configuration to run as non-root user
- Add an entry to start the JDBC gateway

2. Configure autostart

- Add script to server start files, for example:
`/etc/init.d/nco`

© Copyright IBM Corporation 2019

Postinstallation configuration

You typically configure process activity to manage all Netcool/OMNibus core components as a standard practice.



Lesson 3 Netcool/OMNIbus Web GUI



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to install Netcool/OMNIbus Web GUI components.



Important: A prerequisite for this class is the IBM Netcool/OMNIbus 8.1 Installation and Configuration course. The material in this unit is not a comprehensive description of how to install Netcool/OMNIbus Web GUI.

Installing Netcool/OMNIbus Web GUI

1. Download the software:

- IBM WebSphere Application Server V8.5.5.15 for Jazz for Service Management for Linux Multilingual (CC29KML)
- Jazz for Service Management 1.1.3.3 for Linux ML (Launchpad, PRS, Jazz Repository, TDI) Multilingual (CC29GML)
- IBM Tivoli Netcool OMNIbus 8.1.0.16 WebGUI & Extensions for Netcool Operations Insight Linux 64bit English (CC293EN)
- IBM Tivoli Common Reporting 3.1.3.0 for Linux Multilingual (CNC1TML)

2. Expand to some temporary directory, for example:

/tmp/omnibus_webgui

3. Define the target installation directories

```
mkdir /opt/IBM/JazzSM  
chown -R netcool:ncoadmin /opt/IBM/JazzSM  
mkdir /opt/IBM/WebSphere  
chown -R netcool:ncoadmin /opt/IBM/WebSphere  
mkdir /opt/IBM/netcool  
chown -R netcool:ncoadmin /opt/IBM/netcool
```

© Copyright IBM Corporation 2019

Installing Netcool/OMNIbus Web GUI

Netcool Operations Insight uses a version of Netcool/OMNIbus Web GUI that contains some custom extensions. Be sure that you download the correct Netcool/OMNIbus Web GUI installation file.

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub

1. Install Jazz for Service Management with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
.IBMIM
```

2. Define software repositories

```
/tmp/omnibus_webgui/WASRepository/disk1/diskTag.inf  
/tmp/omnibus_webgui/JazzSMRepository/disk1/diskTag.inf  
/tmp/omnibus_webgui/repository.config
```

3. Select the following packages:

- IBM WebSphere Application Server Version 8.5.5.15
- IBM WebSphere SDK Java Technology Edition (Optional) Version 7.0.9.30
- Jazz for Service Management extension for IBM WebSphere 8.5 Version 1.1.2.1
- IBM Dashboard Application Services Hub Version 3.1.3.3
- Reporting Services Version 3.1.3.0

4. Accept the default features

5. Configure WebSphere administrator user name and password

6. Change port numbers if desired

© Copyright IBM Corporation 2019

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub

The installation does not require anything that is unique to Netcool Operations Insight.

Installing Web GUI and extensions

1. Install Netcool/OMNIbus 8.1.0.16 Web GUI with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
. ./IBMMIM
```

2. Define software repositories

```
/tmp/omnibus_webgui/OMNIbusWebGUIRepository/repository.config  
/tmp/omnibus_webgui/OMNIbusWebGUI_NOIExtensionsRepository/repository.config
```

3. Select the following packages:

- IBM Tivoli Netcool/OMNIbus Web GUI
- Netcool Operations Insight Extensions for IBM Tivoli Netcool/OMNIbus Web GUI

4. Define Web GUI installation directory

```
/opt/IBM/netcool/gui
```

5. Configure WebSphere administrator user name and password

© Copyright IBM Corporation 2019

Installing Web GUI and extensions

When you install Netcool/OMNIbus Web GUI, you must define two software repositories. The installation assumes that you use a local installation file. If you configure IBM Installation Manager to connect to Passport Advantage, the correct repositories are automatically configured. You must also select both packages during the installation process.

Installing Web GUI and extensions (2)

6. Configure Log Analysis access information

- Protocol: https
- URL host name: < location of Log Analysis server >
- URL port number: 9987 [default]
- URL context root: Unity
- Data source name: omnibus

Note: Installation runs for approximately 15 minutes

Configuration for IBM Tivoli Netcool/OMNibus Web GUI 8.1.0.16	
Integrate with IBM Operations Analytics - Log Analysis	
URL protocol type	https
URL host name	host1.csite.edu
URL port number	9987
URL context root	Unity
Data source name	omnibus
User name	unityadmin
Password

© Copyright IBM Corporation 2019

Installing Web GUI and extensions (2)

The screen capture that is shown on this slide is unique to Netcool Operations Insight. If you do not define both software repositories or fail to select both installation packages, you do not see this screen during the installation. The information on this screen is used to configure Netcool/OMNibus Web GUI event search tools. The event search tools are used to access IBM Operations Analytics Log Analysis.

Post-installation configuration

1. Configure IBM Tivoli Netcool/OMNibus Web GUI

- Select this option on the end of installation
- Can also be run manually after the installation

```
cd /opt/IBM/netcool/gui/omnibus_webgui/configtool/linux.gtk.x86_64  
.ncwConfigUI -WASUserID <WAS_ADMIN_ID> -WASPassword <WAS_ADMIN_PASSWORD>
```

2. Select configuration option

- Configure a single server setup using default settings
 - Single ObjectServer
 - ObjectServer defined as default user repository
 - Create default groups and users
- Configure an advanced setup
 - High availability pair of ObjectServers
 - ObjectServer or file-based repository
 - Create default groups and users

© Copyright IBM Corporation 2019

Postinstallation configuration

When the installation completes, you can select the option to run the postinstallation configuration wizard, which is suggested.

Configuring LDAP as an authentication source

The steps to configure user authentication against an LDAP directory are as follows:

1. Remove the ObjectServer from the Virtual Member Manager realm
You cannot use ObjectServer and LDAP simultaneously as user repositories
2. Add the LDAP directory to the Virtual Member Manager realm
3. Configure the Virtual Member Manager realm to write new users to the LDAP directory

The following information is required for the configuration:

- Host name and port number for the LDAP directory
- Type and version of LDAP directory, for example, IBM Security Directory Server V6.2
- The user ID and password that are used to bind to the LDAP server
- Subtree of the LDAP directory that is used for authenticating users

Important: To create users and groups through the Web GUI, the LDAP bind ID must have the appropriate permissions in the LDAP directory

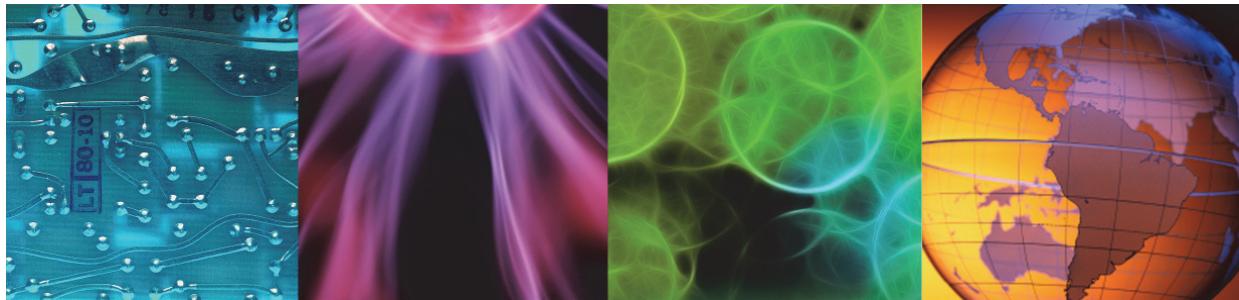
© Copyright IBM Corporation 2019

Configuring LDAP as an authentication source

The use of a Lightweight Directory Access Protocol (LDAP) server is not a specific requirement of Netcool Operations Insight. Rather, the use of LDAP facilitates the use of Netcool Operations Insight. You configure the components to use LDAP, which enables the use of single sign-on. Single sign-on eliminates the need for multiple login and authentication steps when a user switches between components.



Lesson 4 Netcool/Impact



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.



Lesson 4 Netcool/Impact



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to install Netcool/Impact components.



Important: A prerequisite for this class is completion of the IBM Tivoli Netcool/Impact 7.1 Administration and Implementation course. The material in this unit is not a comprehensive description of how to install Netcool/Impact.

Installing Netcool/Impact 7.1.0.16

1. Download the software

- IBM Tivoli Netcool/Impact 7.1.0.16 - Linux 64 bit English (CC298EN)
- Expand to a temporary directory, for example:
/tmp/impact

2. Define the target installation directory

```
mkdir /opt/IBM/tivoli/impact  
chown -R netcool:ncoadmin /opt/IBM/Impact
```

3. Install Netcool/Impact 7.1.0.16 with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
. /IBMMIM
```

© Copyright IBM Corporation 2019

Installing Netcool/Impact 7.1.0.16

Netcool Operations Insight uses a version of Netcool/Impact that contains some custom extensions. You must ensure that you download the correct Netcool/Impact installation file.

Installation (1)

1. Define software repositories

```
/tmp/impact/ImpactExtRepository/disk1/diskTag.inf  
/tmp/impact/ImpactRepository/disk1/diskTag.inf
```

2. Select installation packages

IBM Tivoli Netcool/Impact GUI Server Version 7.1.0.16

IBM Tivoli Netcool/Impact Server Version 7.1.0.16

IBM Tivoli Netcool/Impact Server Extensions for Netcool Operations Insight Version 7.1.0.16

3. Define the installation directory

```
/opt/IBM/tivoli/impact
```

4. Select all features

5. Select user repository type

- ObjectServer
- LDAP
- File-based, recommended

© Copyright IBM Corporation 2019

Installation (1)

When you install Netcool/Impact, you must define two software repositories. The installation assumes that you use a local installation file. If you configure IBM Installation Manager to connect to Passport Advantage, the correct repositories are automatically configured. You must also ensure that you select all three packages during the installation process.

The installation requests a choice of user repository. The choices are ObjectServer, LDAP, or file-based. The class exercises use an LDAP instance as a common user repository for all components. It is not possible to configure the use of LDAP during the installation. You configure LDAP after you install Netcool/Impact.

Installation (2)

6. Define Impact administrator user name and password
7. Define starting port numbers
 - Starting port number for the Impact Server: **9080** [default]
 - Starting port number for the GUI Server: **16310** [default]
8. Accept the default settings for the Impact Nameserver
 - Host name: localhost [default]
Use fully qualified host name for single sign-on (SSO)
 - Port number: 9080 [default]
9. Accept the default settings for the Impact server instance
 - Instance name: NCI [default]
 - Cluster name: NCICLUSTER [default]
 - Command line port: 2000 [default]
10. Define access details for embedded Derby database

Note: Installation runs approximately 45 minutes

© Copyright IBM Corporation 2019

Installation (2)

Netcool/Impact uses a copy of WebSphere Liberty for the user interface. The default start port number, 16310, is the same default start number as Dashboard Application Services Hub. In a production environment, you typically install Netcool/Impact on a dedicated server. In the class exercises, you install all components on a single server. You must change the default start port number during the installation of Netcool/Impact to eliminate a port conflict with Dashboard Application Services Hub.

Configuring single sign-on between Jazz and Netcool/Impact

- Not required for Event Analytics
- Single sign-on is required for DASH console integration
 - Console integration is not required for Event Analytics
- Steps for configuring SSO are found [here](#)
https://www.ibm.com/support/knowledgecenter/SSSHYH_7.1.0.16/com.ibm.netcoolimpact.doc/admin/imag_configure_single_signon.html
SSO requires common user repository between Impact and DASH
 - Use LDAP for the repository
 - ObjectServer is an option, but Log Analysis does not support the ObjectServer as a user repository
- Steps for configuring LDAP are found [here](#)
(https://www.ibm.com/support/knowledgecenter/SSSHYH_7.1.0.16/com.ibm.netcoolimpact.doc/admin/imag_ldap_c.html)

© Copyright IBM Corporation 2019

Configuring single sign-on between Jazz and Netcool/Impact

Netcool Operations Insight does not require the use of single sign-on to access Netcool/Impact. It is suggested that you configure Netcool/Impact for single sign-on. When you enable single sign-on, you can integrate the Netcool/Impact console into Dashboard Application Services Hub. The Netcool/Impact console access is not a requirement for Netcool Operations Insight. It merely facilitates user access to the Netcool/Impact user interface. The class exercises demonstrate how to configure Netcool/Impact to enable single sign-on.

Integrating the Netcool/Impact console (1)

- Log in to Dashboard Application Services Hub
 - User must be a valid Netcool/Impact user
- Select Console Integrations



- Click the icon to create a new connection



© Copyright IBM Corporation 2019

Integrating the Netcool/Impact console (1)

Integrating the Netcool/Impact console into Dashboard Application Services Hub is not a requirement for Netcool Operations Insight. The integration is an operational convenience. Single sign-on is a requirement for the integration.

You connect to Dashboard Application Services Hub as a valid Netcool/Impact user, for example, **impactadmin**. The user must also possess the **iscadmins** role.

Integrating the Netcool/Impact console (2)

- Enter a value for the name
- Enter the URL

`https://<host name>:16311/ibm/console/rest`

Console Integrations

General information regarding the Console Integration being created or edited. Specify the name of your integration and the URL of the Netcool/Impact server.

Required field

Console Integration ID:

Console Integration Name:

Console Integration URL:

Integration Location:

Test →

Status: **Connection Successful**

The following tasks will be integrated into this console. Pages will be added to the navigation tree under NetcoolImpact.

Name	ID	Roles
Impact	i1-impactView	impactAdminUser, impactFullAccessUser, impactOpViewUser

- Test the connection

- Save the connection

© Copyright IBM Corporation 2019

Integrating the Netcool/Impact console (2)

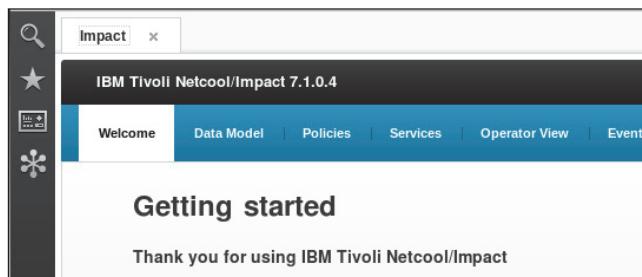
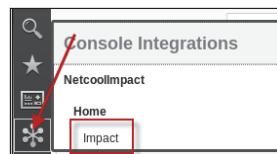
Enter a Console Integration Name and a Console integration URL that points to your Netcool/Impact GUI Server. Use the fully qualified domain name for the server. For example,

`https://<impactui_fqdn>/ibm/console/rest`.

Select Test and verify that the connection is successful.

Integrating the Netcool/Impact console (3)

- Log in to Dashboard Application Services Hub
 - User must be a valid Netcool/Impact user
- Click the icon and select Impact
- Console opens



© Copyright IBM Corporation 2019

Integrating the Netcool/Impact console (3)

In the navigation tree, a new console integrations icon is displayed for Netcool/Impact. All the console integrations are stored here along with their tasks. You can click any of these integrated tasks to start the task inside the Dashboard Applications Services Hub console content area.

Due to security requirements on some browsers, you might need to accept the Netcool/Impact SSL certificate in your browser to be able to view Netcool/Impact related views inside the Dashboard Applications Services Hub.

Lesson 5 IBM Operations Analytics Log Analysis



Lesson 5 IBM Operations Analytics Log Analysis



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to install IBM Operations Analytics Log Analysis.



Important: A prerequisite for this class is completion of the IBM Operations Analytics Log Analysis 1.3 Administration course. The administration course does not cover installation. The material in this unit provides the basic description of how to install Log Analysis.

Installing Log Analysis 1.3.5.3

1. Download the software

- IBM Operations Analytics Log Analysis Managed - Device based v1.3.5.3 Linux 64 bit ALL editions English (CC29CEN)
- IBM Operations Analytics Log Analysis v1.3.5 - Device based Enablement Key to Standard Edition Multiplatform English (CNE6FEN)
- IBM Operations Analytics - Log Analysis 1.3 Big Insights Tooling English Linux (CN6WREN)
Note: Tooling is required only to create new insight packs
- Expand the Log Analysis installation file to some temporary directory, for example:
`/tmp/la`

2. Define the target installation directory

```
mkdir /opt/IBM/LogAnalysis  
chown -R netcool:ncoadmin /opt/IBM/LogAnalysis
```

3. Install Log Analysis

```
cd /home/netcool/InstallationManager/eclipse  
. /IBMMIM
```

© Copyright IBM Corporation 2019

Installing Log Analysis 1.3.5.3

IBM Operations Analytics Log Analysis is available for use as a stand-alone product. Netcool Operations Insight uses the same version of Log Analysis. What makes the Log Analysis product unique to Netcool Operations Insights is some additional components. Those components are covered in the next unit of this course.

IBM Operations Analytics Log Analysis is distributed as three installation files. One of these files contains the Log Analysis software. One file contains a license key. The third file contains a software development toolkit that is used to create an insight pack. The third file is not required for Netcool Operations Insights.



Note: The toolkit is not covered in this class.

Installation

1. Define software repository

/tmp/la/diskTag.inf

2. Accept default installation packages

IBM Operations Analytics - Log Analysis Version 1.3.5.3

3. Define the installation directory

/opt/IBM/LogAnalysis

4. Accept the default installation features

IBM Operations Analytics - Log Analysis Version 1.3.5.3

Apache Solr 7.5.0

IBM Tivoli Log File Agent 06.30.02.00

5. Accept the default port numbers

6. Leave the option selected to install a local Indexing Engine instance

Note: Installation runs approximately 20 minutes

© Copyright IBM Corporation 2019

Installation

When you expand the installation file, you find a single software repository. The installation process assumes that you install the software in the home directory of the user that you use to install the software. It is suggested that you change the installation directory.

Configuring single sign-on between Jazz and Log Analysis

- Required for Event Search
 - Single sign-on is required for event search tool launch from Web GUI to Log Analysis
- Steps for configuring SSO are found [here](#)
https://www.ibm.com/support/knowledgecenter/SSPFMY_1.3.5/com.ibm.scala.doc/install/iwa_pinstall_sso_dash_t.html
- SSO requires common user repository between Log Analysis and DASH
 - Use LDAP for the repository
 - Log Analysis does not support the ObjectServer as a user repository
- Steps for configuring LDAP are found [here](#)
https://www.ibm.com/support/knowledgecenter/SSPFMY_1.3.5/com.ibm.scala.doc/install/iwa_install_ldapconfig_ovw.html

© Copyright IBM Corporation 2019

Configuring single sign-on between Jazz and Log Analysis

Again, single sign-on is not a specific requirement of Netcool Operations Insight. Access to Log Analysis search features is implemented as a tool launch from Netcool/OMNIbus Web GUI. The user interface for Log Analysis is implemented through WebSphere Liberty. If single sign-on is enabled, when a Web GUI user initiates an event search tool, the user does not have to authenticate to Log Analysis.

A requirement for single sign-on is a common user repository between products. Netcool/Impact can use an ObjectServer or LDAP as a user repository. Log Analysis cannot use an ObjectServer. The class exercises demonstrate how to configure Log Analysis to use LDAP and enable single sign-on.

User administration basics

- Access to Log Analysis features is controlled through roles and groups
 - UnityAdmins for administrative access
 - UnityUsers for basic user access
- Default role and group associations defined in a file
`/opt/IBM/LogAnalysis/wlp/usr/servers/Unity/unityConfig.xml`
- When using LDAP, perform these steps:
 - Create group names in LDAP
 - Create users in LDAP
 - Add users to groups
- More information regarding user administration can be found [here](#):
`https://www.ibm.com/support/knowledgecenter/SSPFMY_1.3.5/com.ibm.scala.doc/config/iwa_config_pinstall_userrole_ovw_c.html`

© Copyright IBM Corporation 2019

User administration basics

The default configuration of Log Analysis uses a simple file-based repository for authentication. Two files implement the repository.

`/opt/IBM/LogAnalysis/wlp/usr/servers/Unity/unityConfig.xml`
`/opt/IBM/LogAnalysis/wlp/usr/servers/Unity/unityUserRegistry.xml`

The first file contains the group names, and the roles that are associated with each group. The second file contains the user names, passwords, and the group to which the user belongs. When Log Analysis is configured to use LDAP, the use of these files changes slightly. LDAP replaces the use of the second file. LDAP contains the user names, passwords, and group associations.

The first file is used to define group names and the roles that are assigned. The same group names must be used in LDAP. Log Analysis authenticates the user with LDAP and retrieves the associated group name. Log Analysis uses the first file to determine which role is associated with the corresponding group name. If you have an existing user that you want to enable access to Log Analysis, you modify the user in LDAP and add the user to the appropriate Log Analysis group.

If your organization uses LDAP and group names already exist, you can enable those groups for access to Log Analysis by modifying the `unityConfig.xml` file. You merely add the group name to the appropriate role.

The default `unityConfig.xml` file contains the following lines:

```
<server>
  <application type="war" id="Unity" name="Unity"
    location="${server.config.dir}/apps/Unity.war">
    <application-bnd>
```

```
<security-role name="UnityUser">
    <group name="UnityUsers" />
    <group name="UnityAdmins" />
</security-role>
<security-role name="UnityAdmin">
    <group name="UnityAdmins" />
</security-role>
</application-bnd>

</application>

<oauth-roles>
    <authenticated>
        <group name="UnityUsers"/>
    </authenticated>
</oauth-roles>
</server>
```

Two roles control access to Log Analysis.

- UnityUser
- UnityAdmin



Important: A user must have the UnityUser role to access the Log Analysis user interface.

The roles are assigned to groups.

- UnityUsers belongs to the UnityUser role
- UnityAdmins belongs to the UnityUser and UnityAdmin roles

The default unityUserRegistry.xml file contains the following lines:

```
<server>
    <basicRegistry id="basic" realm="UnityRealm">
        <user name="unityuser" password="{xor}KjE2KyYqLDot" />
        <user name="unityadmin" password="{xor}KjE2KyY+OzI2MQ==" />
        <group name="UnityUsers">
            <member name="unityuser" />
            <member name="unityadmin" />
        </group>
        <group name="UnityAdmins">
            <member name="unityadmin" />
        </group>
    </basicRegistry>
</server>
```

The default user names are as follows:

- unityadmin
- unityuser

LDAP replaces the use of this file.

Enabling Log Analysis product key

1. Copy the license file to the Log Analysis server, for example:

```
/software/la/IOALA_ENABMT_KEY_STD_ED.swttag
```

2. Run the utility to change editions:

```
cd /opt/IBM/LogAnalysis/utilities/  
.unity_change_edition_util.sh -p /software/la/IOALA_ENABMT_KEY_STD_ED.swttag
```

3. Restart Log Analysis

```
/opt/IBM/LogAnalysis/utilities/unity.sh -restart
```

© Copyright IBM Corporation 2019

Enabling Log Analysis product key

You must download a license file to activate IBM Operations Analytics Log Analysis. Use the `unity_change_edition_util.sh` tool to apply the license. Restart Log Analysis after you activate the license. You can see your Log Analysis license version in the output of the Log Analysis start-up script.

Student exercises



© Copyright IBM Corporation 2019

Student exercises

Refer to the exercises for Unit 2 in the student exercises guide.

Summary

You now should be able to perform the following tasks:

- Use the prerequisite scanner to verify the system requirements
- Install and configure Netcool/OMNIbus core components
- Install and configure Netcool/OMNIbus Web GUI
- Install and configure Netcool/Impact
- Install and configure IBM Operations Analytics Log Analysis

© Copyright IBM Corporation 2019

Summary



3 Configuring IBM Netcool Operations Insight base



Configuring IBM Netcool Operations Insight base



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this unit, you learn how to install and configure the remaining elements of the Netcool Operations Insight solution.

Objectives

In this unit, you learn to perform the following tasks:

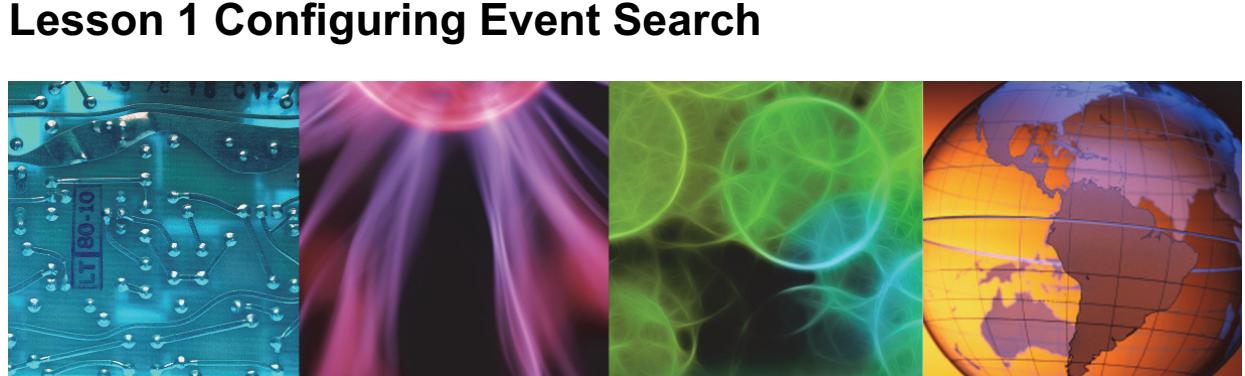
- Install the event search components
- Verify the event search feature
- Configure the event analytics features

© Copyright IBM Corporation 2019

Objectives



Lesson 1 Configuring Event Search



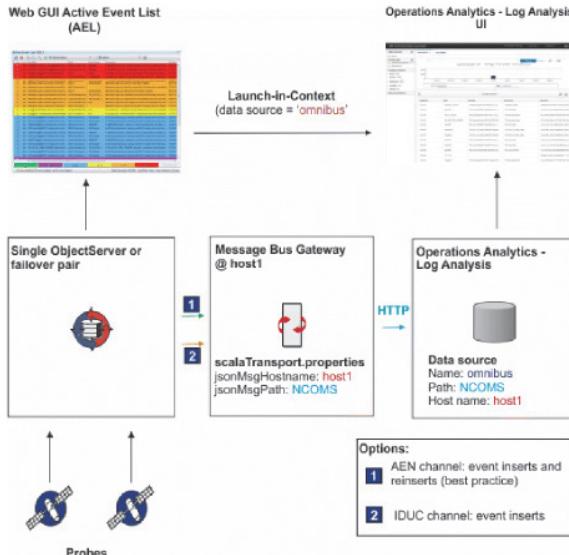
© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to perform the following tasks:

- Install the OMNIbus Insight Pack
- Create an event data source
- Install and configure the Log Analysis gateway

Event Search overview

- OMNIbus events in the ObjectServer are sent to Log Analysis by the Message Bus Gateway
- OMNIbus event data is stored in Log Analysis in the context of a data source
Default name is omnibus
- OMNIbus events are indexed in Log Analysis
- OMNIbus events are searchable in Log Analysis
A search is performed against a data source



© Copyright IBM Corporation 2019

Event Search overview

The Event Search feature applies the search and analysis capabilities of Operations Analytics Log Analysis to events that Netcool/OMNIbus monitors and manages. Events are transferred from the ObjectServer through the Gateway for Message Bus to Operations Analytics Log Analysis, where they are processed into a data source and indexed for searching. After the events are indexed, you can search every occurrence of real-time and historical events. The 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 that shows how your monitoring environment is performing over time. You can go deeper into the event data with keyword searches and dynamic drill-down functions. The apps can be run from the Operations Analytics Log Analysis. Tools are installed into the Web GUI that start 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.

OMNIbus Insight Pack

- Log Analysis Insight Pack defined
 - A set of related artifacts to ingest data or to develop applications are packaged together as an installable package called an Insight Pack
- The OMNIbus Insight Pack provides the following data ingestion artifacts:
 - A *rule set* with annotator and splitter that parses Netcool/OMNIbus event data into delimiter separated value (DSV) format
 - A *source type* that matches the event fields in the Gateway for Message Bus map file
 - A *collection* that contains the provided source type
 - Custom apps
 - Two custom apps to support launch-in-context from Web GUI
 - OMNIbus_Keyword_Search.app
 - OMNIbus_Static_Dashboard.app
 - Two custom apps to provide event insight
 - OMNIbus_Dynamic_Dashboard.app
 - OMNIbus_Operational_Efficiency.app

© Copyright IBM Corporation 2019

OMNIbus Insight Pack

After you install the Tivoli Netcool/OMNIbus Insight Pack, you can view and search both historical and real-time event data from Tivoli Netcool/OMNIbus in the IBM Operations Analytics Log Analysis product.

The Insight Pack parses Tivoli Netcool/OMNIbus event data into a format suitable for use by Operations Analytics Log Analysis. The event data is transferred from Tivoli Netcool/OMNIbus to Operations Analytics Log Analysis by the IBM Tivoli Netcool/OMNIbus Gateway for Message Bus (`nco_g_xml`).

Installing the OMNIbus Insight Pack

1. Create a directory for the Insight Pack

```
cd /opt/IBM/LogAnalysis/unity_content/  
mkdir OMNIbus
```

2. Copy the Insight Pack to the new directory

```
cp /tmp/la/OMNIbusInsightPack_v1.3.1.0.zip OMNIbus
```

3. Install the Insight Pack

```
/opt/IBM/LogAnalysis/utilities/pkg_mgmt.sh -install OMNIbusInsightPack_v1.3.1.0.zip
```

After the installation is complete, the rule set, source type, and collection that are required for working with Netcool/OMNIbus events are in place

© Copyright IBM Corporation 2019

Installing the OMNIbus Insight Pack

The insight pack is distributed as a separate installation file:

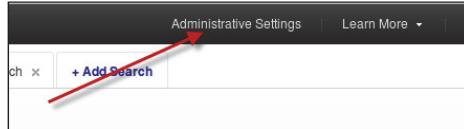
IBM Tivoli Netcool/OMNIbus Insight Pack V1.3.1 for IBM Operations Analytics - Log Analysis
V1.3 English (CNS6GEN)

The insight pack is not installed with IBM Installation Manager. Instead, the insight pack is installed with a Log Analysis utility.

Creating the event data source (1)

1. You define the data source with the Log Analysis administrative interface

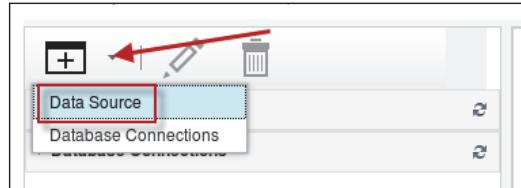
- Log in to Log Analysis
 - <https://<Log Analysis host>:9987/Unity/>
 - Open the administrative interface



2. Select data sources

You can use the Data Sources workspace to define your Data Sources and Databases by converting the file contents into a structured format. You can use a Database Connection in the application database. Click Add and choose the Data Source that you want to add.

3. Create a new data source



© Copyright IBM Corporation 2019

Creating the event data source (1)

A data source is a configuration object that Log Analysis uses to process the contents of a log file. You create data sources to start processing a specific log source. After you create a data source, it is available in the user interface for users to select.

The best practice is to consolidate all Netcool/OMNIbus events into one data source. If you have several ObjectServers, use separate instances of the Gateway for Message Bus to connect to each ObjectServer. The best practice is for each gateway to send events to a single data source.

Creating the event data source (2)

4. Select Custom

5. Enter the host name

The host name is the location of the Log Analysis receiver

* Select Location * Select Data * Set Attributes

If you want to ingest data into the Log Analytics server, use the wizard to configure to monitor changes to a file. Select Custom when data is sent to the Log Analytics remote log file agent, Logstash, or the data collector client. [Learn More...](#)

Local file
 Remote file
 Custom

* Host name: host1.tivoli.edu

6. Enter a value for File path

7. Select OMNIbus1100 for the Type

8. Select OMNIbus1100-Collection for the Collection

The Type and Collection values are created by the Insight Pack installation

* Select Location * Select Data * Set Attributes

Enter the location and type of data for this data source. The file path is not validated when you [More...](#)

* File path: NOI_AGG_P

* Type: OMNIbus1100 →

* Collection: OMNIbus1100-Collection →

* Required

© Copyright IBM Corporation 2019

Creating the event data source (2)

The type and collection values are created when you install the insight pack. Log Analysis is designed to process various types of log files. The Log Analysis product contains insight packs for various log file types. When you click the arrow to select the type, you see a long list of values. These values are associated with the other log file types that Log Analysis supports.



Important: The value for File path is used later when you configure the gateway.

Creating the event data source (3)

9. Enter **omnibus** for the name
10. Click **OK** to save the definition

The screenshot shows a dialog box titled 'Set Attributes'. At the top, there are three tabs: 'Select Location', 'Select Data', and 'Set Attributes', with 'Set Attributes' being the active tab. Below the tabs, a message says 'Enter a name for the new data source. Optionally, set a description and assign the source to a group.' There are three input fields: 'Name:' containing 'omnibus', 'Description:' (empty), and 'Group:' (empty). The 'Name:' field is highlighted with a red border.

© Copyright IBM Corporation 2019

Creating the event data source (3)

The value for **Name** is merely text. However, the value is also used in the configuration of the gateway.

Log Analysis Gateway

- There is no Log Analysis Gateway binary
 - The Log Analysis Gateway is a new transport of the Message Bus (XML) Gateway
 - Follows the same setup and structure as other transports of this gateway
- Configuring SSL connections
 - The gateway uses HTTPS as the transport mechanism for Log Analysis
 - You must create a truststore to store the Message Bus digital certificate and point the gateway to the location of the truststore
 - The process consists of two tasks:
 1. Creating a client keystore
 2. Creating a truststore for the target application to which the gateway is connecting

© Copyright IBM Corporation 2019

Log Analysis Gateway

Netcool Operations Insight uses the Message Bus Gateway to collect events from the ObjectServer. The gateway extracts events from the ObjectServer and formats the event data into a delimited string. The gateway passes this string to the Log Analysis receiver with the HTTPS protocol. Because the gateway uses HTTPS, part of the configuration process involves the exchange and storage of digital certificates.

Configuring SSL (1)

1. Create a client keystore on the Netcool/OMNIbus server

```
mkdir /opt/IBM/tivoli/netcool/omnibus/java/security  
cd /opt/IBM/tivoli/netcool/platform/linux2x86/jre_1.8.0/jre/bin/  
  
.keytool -genkey -alias newkey -keystore  
/opt/IBM/tivoli/netcool/omnibus/java/security/client.jks
```

2. Export the server certificate from the host running IBM Operations Analytics Log Analysis

a. Open a Firefox browser and connect to the following URL:

<https://< Log Analysis host >:9987/Unity>

b. Click **Edit** and select **Preferences**

c. Click **Advanced**, click **Encryption**, click **View Certificates**

d. Click **Servers**, select the Log Analysis host, and click **Export**

e. Save the file to a temporary location, for example:

/tmp/loganalysis.crt

© Copyright IBM Corporation 2019

Configuring SSL (1)

You create a client keystore that is named client.jks and store in it a certificate for your client. Run the following keytool command from the \$NCHOME/platform/arch/jre_directory/jre/bin/ directory:

```
keytool -genkey -alias youralias -keystore $OMNIHOME/java/security/client.jks
```

 **Note:** You are prompted to create a keystore password. Then, keytool prompts you for the details of the certificate to be entered; for each prompt enter something appropriate for your organization.

You can export the certificate from the Firefox browser to a file as shown on the slide.

Configuring SSL (2)

3. Copy the Log Analysis certificate to the Netcool/OMNIbus server
4. Import the certificate

```
cd /opt/IBM/tivoli/netcool/platform/linux2x86/jre_1.8.0/jre/bin  
  
./keytool -import -keystore  
/opt/IBM/tivoli/netcool/omnibus/java/security/cacerts.jks  
-file /tmp/loganalysis.crt -alias mykey
```

© Copyright IBM Corporation 2019

Configuring SSL (2)

Copy the server certificate file to the host where the gateway is running. Run the following keytool command from the \$NCHOME/platform/arch/jre_directory/jre/bin/ directory:

```
keytool -import -keystore $OMNIHOME/java/security/cacerts.jks -file scala-host.crt  
-alias scala-host
```

ObjectServer modifications

- Event analytics is interested in the generated events as they occurred in the environment and not the changes to an event that occur by operator actions
 - As provided with the product, the gateway replicates only new events to Log Analysis by standard IDUC
 - Event instances that deduplicate are not sent to Log Analysis
- To send newly inserted events and deduplicated inserts, you must additionally customize the ObjectServer and configure the solution to use the Accelerated Event Notification (AEN) system
- ObjectServer modifications
 - Trigger group
 - scala_triggers
 - Triggers
 - scala_reinsert
 - scala_insert
 - Enable the trigger group and triggers

© Copyright IBM Corporation 2019

ObjectServer modifications

The gateway processes only new event records by default. The recommendation is to implement a modified behavior to cause the gateway to process both new and deduplicated event records. The behavior is based on the Accelerated Event Notification (AEN) feature. In previous versions of Netcool Operations Insight, you implemented this behavior by importing a supplied SQL file. The modifications are now implemented automatically.

The modifications include a custom trigger group and custom triggers. The triggers are database triggers that activate based on an *insert* or *reinsert* to the alerts.status table. Each trigger runs a command to send an AEN notification on a custom channel that is called *scala*. The gateway is configured to receive notifications on this channel. The notification causes the gateway to process the corresponding event.

The ObjectServer modifications are included, but you must enable the trigger group and triggers to implement the behavior.

Installing the message bus gateway

1. Download the software

- Netcool/OMNIbus 8 Plus Gateway for Message Bus (nco-g-xml 10_0) Multi-Platform English (CC194EN)

2. Install with IBM Installation Manager

```
cd /opt/IBM/InstallationManager/eclipse  
. /IBMIM
```

3. Define software repository

```
/tmp/gateway/NCLOM_8P_GTY_FOR_MB_MPL_EN.zip  
Note: you do not have to expand the gateway installation file
```

4. Select installation packages

```
Netcool/OMNIbus Gateway nco-g-xml Version 1.10.0.0
```

5. Select all features

© Copyright IBM Corporation 2019

Installing the message bus gateway

The gateway is installed with IBM Installation Manager.

Configuring the gateway (1)

1. Add the gateway to the Netcool/OMNIbus communications file

LA_GATE

2. Copy and rename the configuration files

```
cp xml1302.map $OMNIHOME/etc/LA_GATE.1302.map
cp G_SCALA.props $OMNIHOME/etc/LA_GATE.props
cp xml.reader.tblrep.def $OMNIHOME/etc/LA_GATE.reader.tblrep.def
cp xml.startup.cmd $OMNIHOME/etc/LA_GATE.startup.cmd
```

3. Modify the gateway property file

\$OMNIHOME/gates/xml/scala/G_SCALA.props

```
Name : 'LA_GATE'
Gate.Reader.Description : 'SCALA Gateway Reader'
Gate.Reader.Server : 'NCOMS'
Gate.Reader.Username : 'root'
Gate.Reader.Password : 'EDEAAPAIANFMCHCB'
```

Note: The password is encrypted with nco_g_crypt

© Copyright IBM Corporation 2019

Configuring the gateway (1)

Part of the gateway configuration is generic to all Netcool/OMNIbus gateways and part is unique to Netcool Operations Insight. The generic configuration steps include:

- Assigning a name to the gateway and configuring the name in the interfaces file
- Configuring the map file, property file, table replication file, and startup command file



Important: The value for the gateway description must be **SCALA Gateway Reader**. It is this value that configures the gateway to receive the AEN messages.

Configuring the gateway (2)

4. Modify the gateway reader file

\$OMNIHOME/gates/xml.reader.tblrep.def

a. Locate the following line:

REPLICATE **INSERT** FROM TABLE 'alerts.status'

b. Change as follows:

REPLICATE **FT_INSERT,FT_UPDATE** FROM TABLE 'alerts.status'

Note: This change is required to use the AEN mechanism that is described on a previous slide

© Copyright IBM Corporation 2019

Configuring the gateway (2)

You must change the default settings in the gateway reader file. You remove the word INSERT from the replicate command. You add FT_INSERT and FT_UPDATE. This change is required for the AEN notification behavior.



Hint: FT_INSERT and FT_UPDATE are references to *Fast Track*. The AEN mechanism implements the *Fast Track* behavior.

Configuring the gateway (3)

5. Modify the scalaTransport.properties file

\$OMNIHOME/java/conf/scalaTransport.properties

```
scalaURL=https://< Log Analysis host >:9987/Unity/DataCollector
keyStore=/opt/IBM/tivoli/netcool/omnibus/java/security/client.jks
keyStorePassword=object00
trustStore=/opt/IBM/tivoli/netcool/omnibus/java/security/cacerts.jks
trustStorePassword=object00
username=unityadmin
password =unityadmin
jsonMsgPath = NOI_ AGG _ P
```

6. Modify the scalaTransformers.xml file

\$OMNIHOME/java/conf/scalaTransformers.xml

```
endpoint="https://< Log Analysis host >:9987/Unity/DataCollector"
```

© Copyright IBM Corporation 2019

Configuring the gateway (3)

The configuration steps that are unique to Netcool Operations involve two files:

- scalaTransport.properties
- scalaTransformers.xml

The properties that you modify in the scalaTransport.properties files are as follows:

- scalaURL: Change the name to the host where Log Analysis is installed.
- keyStore: Enter the full path for the name and location of the keystore.
- keyStorePassword: Enter the password for the keystore.
- trustStore: Enter the full path for the name and location of the truststore.
- trustStorePassword: Enter the password for the truststore.
- username: The default is **unityadmin**.
- password: The default password for the **unityadmin** user.
- jsonMsgPath: Enter the same value that you used for the **File** setting when you created the Log Analysis data source.

The only change that is required in the `scalaTransformers.xml` file is to enter the name for the Log Analysis host.

Configuring the gateway (4)

7. Start the gateway

```
$OMNIHOME/bin/nco_g_xml -name LA_GATE &
```

Hint: Run the gateway with messagelevel debug initially

8. Check the gateway log for issues

```
$OMNIHOME/log/LA_GATE.log
```

9. Check the Log Analysis receiver log for issues

```
/opt/IBM/LogAnalysis/logs/GenericReceiver.log
```

10. Diagnose connectivity issues

Set the transport property enableTrace to True to turn on Log Analysis diagnostic logging

```
$OMNIHOME/java/conf/scalaTransport.properties
```

- Allows connectivity problems to the data collector to be examined
- HTTP Responses are dumped to the log file

© Copyright IBM Corporation 2019

Configuring the gateway (4)

You start the gateway as shown on the slide. You can run the gateway initially in debug mode to facilitate the resolution of any issues. Check the gateway log file for issues. Also, check the Log Analysis receiver log file for issues.

After the gateway is functioning correctly, you can add the gateway to process activity.



Lesson 2 Verifying Event Search



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to verify the Event Search feature.

Running a search

1. Log in to Dashboard Application Services Hub

User must be a valid Log Analysis user

2. Select Event Viewer

3. Right-click an event and select Event Search > Search for events by node > 1 day before event

The screenshot shows a table of event records with a context menu open over a record for 'London'. The menu path 'Event Search' -> 'Search for events by node' is highlighted with a red box. A secondary dropdown menu for 'Search for events by node' is also shown, with the option '1 day before event' highlighted with a red box. Other options in this dropdown include '15 minutes before event', '1 hour before event', '1 week before event', '1 month before event', '1 year before event', and 'Custom ...'. The main table columns are Ack, Node, Alert Group, and Summary.

Ack	Node	Alert Group	Summary
No	London		Machine has gone offline
No	Tokyo		Diskspace alert
No	Beijing		Diskspace alert
No	Washington		Machine has gone offline
No	Moscow		Machine has gone offline
No	Sydney		Machine has gone offline
No	link1		Link Down on port
No	link4		Link Down on port
No	Tokyo	Event Search	Show event dashboard by node
No	Beijing		Search for similar events
No	Tokyo		Search for events by node

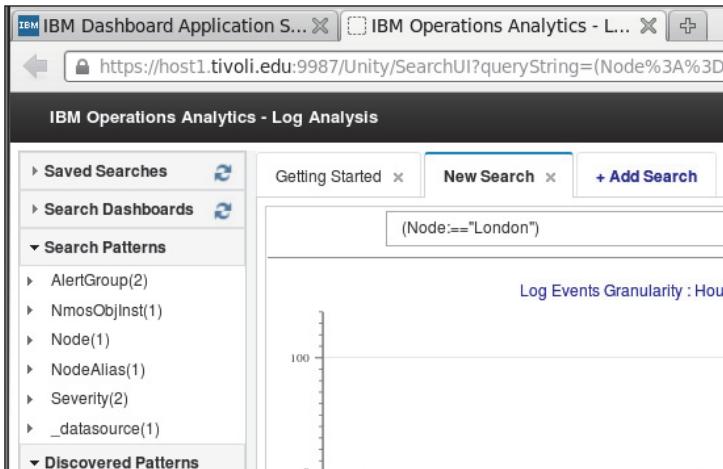
Running a search

You access the Log Analysis tools with the Active Event List or the Event Viewer. The user must be a valid Log Analysis user. All Netcool/OMNIbus Web GUI users can see the event search tools in the various event viewers and they can start the tools. However, if the user is not a valid Log Analysis user, the Log Analysis user interfaces fails to open and an error is generated.

The Event Search tool uses the value from the FirstOccurrence column in the selected event record to determine the required *search window*, for example, 1 hour before event. The class image contains a limited number of event records. When you select a record to use for the event search, make sure that the event occurred multiple times. If the event record contains a count of 1, which indicates a single occurrence, the search does not find any events in Log Analysis. Also, use one of the longer time spans, like day or week, to maximize the probability of finding event records in Log Analysis.

Verifying launch-in-context

- The Log Analysis user interface opens in a new tab
- You are logged in as the same user



© Copyright IBM Corporation 2019

Verifying launch-in-context

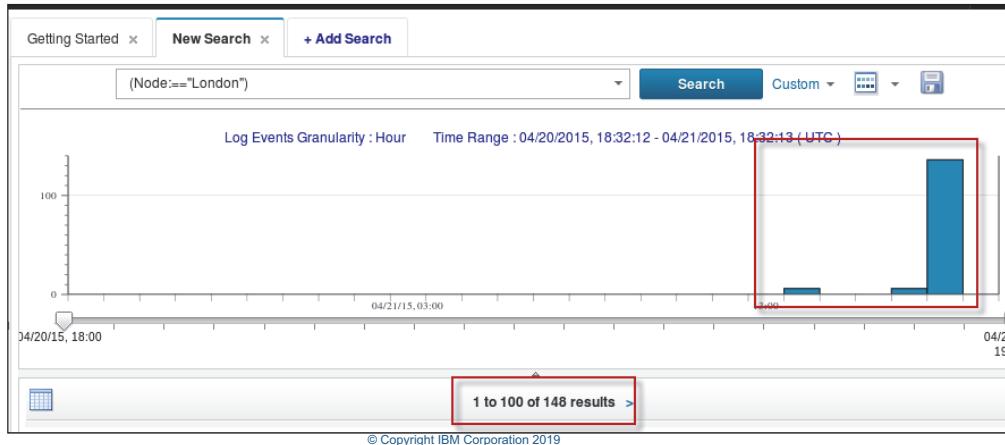
After you start the tool from Web GUI, a new Firefox tab opens. The new tab connects to the Log Analysis URL. If you do not use a valid Log Analysis user to start the tool, the Log Analysis user interface does not open. You see a message that indicates a user authorization failure.

If the Log Analysis login screen opens and prompts for a user name and password, there is an issue with the single sign-on configuration. Examine the end of the Log Analysis message log for error messages:

```
/opt/IBM/LogAnalysis/wlp/usr/server/Unity/logs/message.log
```

Verifying search results

- The search results are displayed
- This action verifies several performance points:
 - The search context is passed correctly from Web GUI
 - Log Analysis is ingesting ObjectServer events



Verifying search results

If the search does not find any records, select a different event record and repeat the process. Or use a longer time period.



Lesson 3 Configuring Event Analytics



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to configure Event Analytics.

Feature overview

- Event Analytics consists of the following components:
 - Related Events
 - Seasonal Events
- Related Events
 - Correlates *unknown* related events and shows them grouped as parent-child in the Event Viewer
 - Reduces actionable events presented to the operator
 - Looks for relationship between events in the historical event database
- Seasonal Events
 - Discovers events that occur in a non-random pattern over time
 - Produces a summary of events that are likely to be seasonal, including a confidence score
 - Analyzes events in the historical event database

© Copyright IBM Corporation 2019

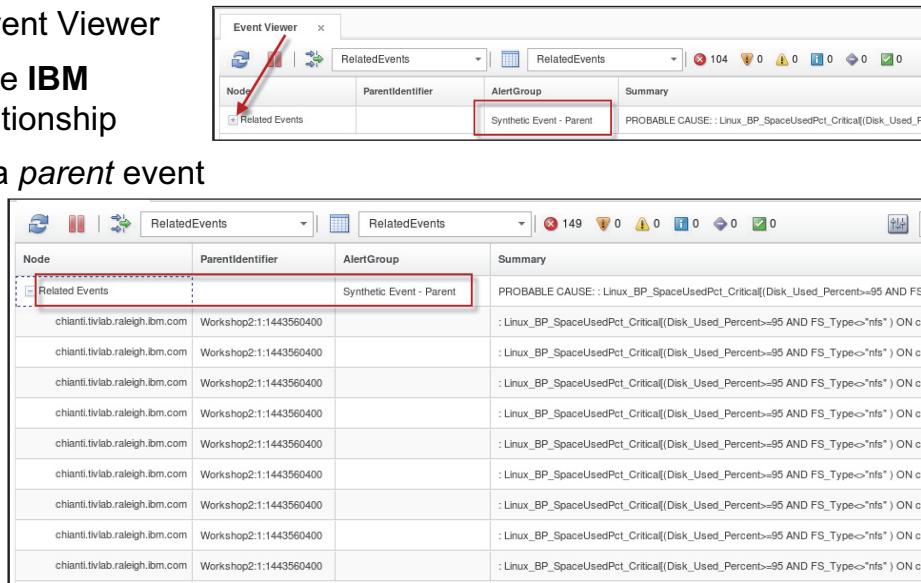
Feature overview

The Event Analytics feature contains two functions. One function is called Related Events, and the other function is called Seasonal Events. The Related Events function analyzes events in the Netcool/OMNIbus event archive database. The analysis determines whether the events are related in some manner. The output from the analysis is used to group new ObjectServer events in a parent-child hierarchy.

The Seasonal Events function also analyzes events in the Netcool/OMNIbus event archive. The analysis identifies events that occur in a non-random pattern. The output from the analysis is used to implement operational changes to eliminate the same events from recurring.

Viewing related events

1. Open a Web GUI Event Viewer
 2. Select a view with the **IBM Related Events** relationship
 3. Locate and expand a *parent* event
 4. View the grouped events



© Copyright IBM Corporation 2019

Viewing related events

A user monitors event records with the Web GUI Event Viewer. The user sees an event record that is preceded with a plus sign. Netcool/Impact generates this event record, which is the parent for a deployed group. The plus sign indicates that additional event records exist that are related to the parent. The user can click the plus sign to expand the list of children.

Event grouping provides an effective means to reduce the number of events that a user sees in the Event Viewer. In the example that is shown here, the user sees a single parent event. The group contains 157 event records. The other records are hidden as children of the parent. The user can expand the list and see the child events if necessary.

How seasonality is determined

- Seasonality is determined by counting event observations in time period bins
- Events are identified as unique if their SUMMARY is the same
 - The choice of column name is configurable
- The number of actual observations in each time period bin is compared with a uniform distribution of events
- The difference is a measure of probable seasonality
- An **observation** is a count of whether or not the event arrived in each bin

© Copyright IBM Corporation 2019

How seasonality is determined

The Seasonal Events feature analyzes events in the archive database. The analysis uses the value of the SUMMARY column to identify the same events. The column name can be changed when you create the analysis request. The analysis counts events based on four time periods. The analysis compares the events for each time period against the uniform distribution of events. Any deviation from normal is considered potentially seasonal.

Example seasonal report

- The analysis identifies potential seasonal time frames
- The example event analysis indicates:
 - High confidence for minute of the hour
 - High confidence for hour of the day
 - Medium confidence for day of the week

The event repeats every Sunday, at 24 minutes past the hours of 9 and 10 AM



© Copyright IBM Corporation 2019

Example seasonal report

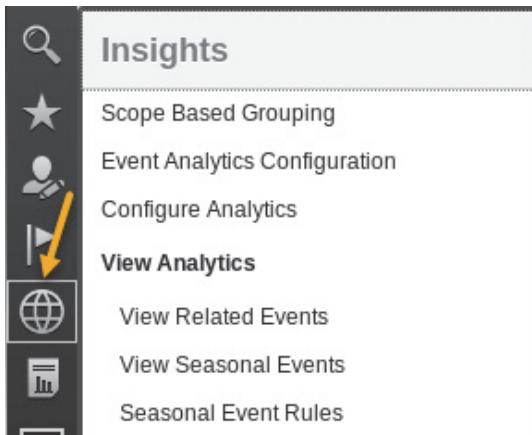
The graphs present the observation counts in the context of the four analysis windows:

- Minute of the hour
- Hour of the day
- Day of the week
- Day of the month

The green areas show the expected observation threshold (count). The yellow and red shaded areas show when the actual count exceeds the expected value.

Event Analytics administration

- User interface is provided by Web GUI
- Feature consists of 6 portlets
 - Insights > Scope Based Grouping
 - Insights > Event Analytics Configuration
 - Insights > Configure Analytics
 - Insights > View Analytics
 - View Related Events
 - View Seasonal Events
 - View Seasonal Event Rules
- All portlets require the user to have **ncw_analytics_admin** role



© Copyright IBM Corporation 2019

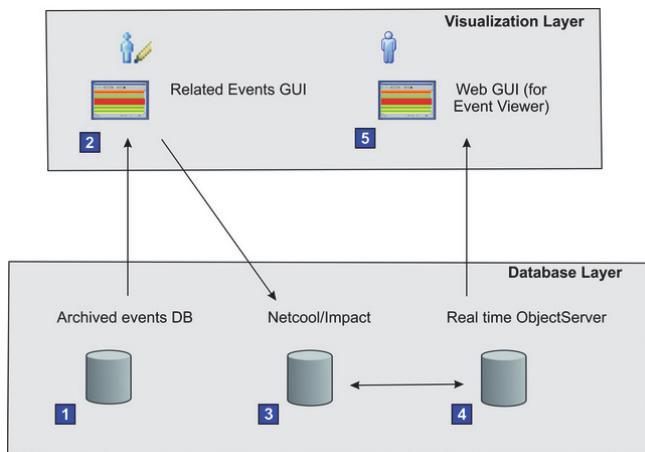
Event Analytics administration

Event Analytics has two functional users. One functional user is the administrator. The administrator is responsible for configuring event analytics and running the analysis. The administrator requires the **ncw_analytics_admin** role. The administrator has access to the features that are illustrated on this slide.

The second functional user is a normal user. The normal user views the results of event analytics. The normal user does not require any special role. The normal user does not have access to the features that are shown on this slide.

Related Events workflow

1. Netcool/OMNIbus continuously archives real time events to an archived events database
2. The administrator creates a related events analysis
 - a) The analysis identifies and groups related events from the archive database and derives correlation rules
 - b) The Administrator watches and deploys 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



© Copyright IBM Corporation 2019

Related Events workflow

The Related Events feature is implemented in a series of tasks. A user with the *ncw_analytics_admin* role creates a related events analysis request. The analysis request contains a time period for historical events, and a time period for when the analysis is run. In most cases, the configuration runs on a defined frequency, for example, every week. The result of the analysis is one or more event groups.

The administrator views the event groups. The group information includes a list of the historical events that are considered members of the group. The administrator examines the events in the group and determines whether the group is valid. If the group is considered valid, the administrator *deploys* the group.

When a group is deployed, Netcool/Impact policies are initiated. The policies create a *synthetic parent* event in the ObjectServer. As new or deduplicated events reach the ObjectServer, Netcool/Impact retrieves the events and evaluates the events against the deployed group criteria. When Netcool/Impact determines that an event is related to a group, the event record is enriched with data that identifies the event as a *child* of the group. The enriched event is written to the ObjectServer. In addition, Netcool/Impact computes statistics that are related to the use of deployed groups.

A Netcool/OMNIbus Web GUI user views events with the Event Viewer. The Event Viewer is configured to use an event view that references a relationship. The enriched events from Netcool/Impact appear in a hierarchical manner based on the relationship. The user sees the synthetic parent event and all children events.

Prerequisite

Event Archiving:

- A database with archived events in *reporter* mode
Event Analytics supports DB2, Oracle, or MSSQL
- Additional fields are supported within the historical database
- Indexing is automatically created on database:

CREATE INDEX RE_FIRSTOCCURRENCE on DB2INST1.REPORTER_STATUS (FIRSTOCCURRENCE ASC)

© Copyright IBM Corporation 2019

Prerequisite

You can create an Netcool/OMNIbus archive in either audit mode or reporter mode. The Event Analytics feature supports only an archive database that is created in reporter mode. The Event Analytics feature supports the use of custom event columns in the archive database.

Configuration (1)

- ObjectServer configuration:
 - Import \$IMPACT_HOME/add-ons/RelatedEvents/db/relatedevents_objectserver.sql
 - Adds the following objects:
 - ParentIdentifier field is added to alerts.status table
 - ParentIdentifierIndex is created on alerts.status table
 - Database relatedevents.cacheupdates is created on ObjectServer
 - Trigger Group ibm_re_triggers is created
 - Trigger re_remove_dangling_parentEvent is created in trigger group
- Note: Required by Related Events
- Web GUI Configuration:
 - Create remote connection to Impact CURI service
 - Handling multiple Impact CURI connections
 - If there are multiple Impact CURI connections created, then the connection to use can be selected in the Personalize mode of the Related Events portlets

© Copyright IBM Corporation 2019

Configuration (1)

The Related Events function requires modifications to the ObjectServer. The modifications are supplied in an SQL file. You use the nco_sql utility to import the file.

You must create a connection to the Netcool/Impact server in Dashboard Application Services Hub. Related Events and Seasonal Events require the Netcool/Impact connection.

Configuration (2)

- Impact configuration:
 - ObjectServer definition:
 - Update DataSource: ObjectServerForNOI
 - Refresh DataType: AlertsForNOITable
 - Event archive database:
 - For DB2 Event History Database:
Update DataSource: ObjectServerHistoryDB2ForNOI and refresh DataType: AlertsHistoryDB2Table
 - For Oracle Event History Database:
Update DataSource: ObjectServerHistoryOrclForNOI and refresh DataType: AlertsHistoryOrclTable
 - For MSSQL Event History Database:
Update DataSource: ObjectServerHistoryMSSQLForNOI and refresh DataType: AlertsHistoryMSSQLTable
 - Ensure Impact services are started

© Copyright IBM Corporation 2019

Configuration (2)

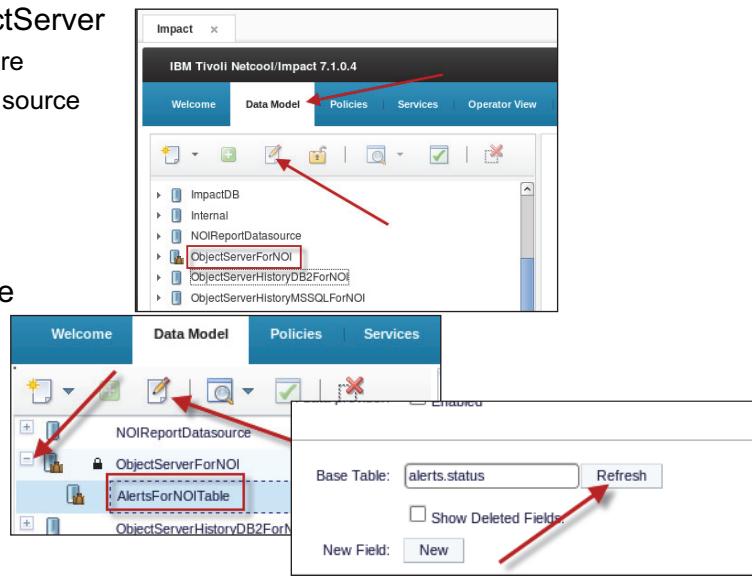
A number of Netcool/Impact objects must be configured for Event Analytics. Related Events and Seasonal Events share some of the objects. Other objects are unique to each function.

Both functions access the Netcool/OMNIbus event archive database. One Netcool/Impact data source defines the access credentials to the archive database for both features. The archive database is supported on DB2, Oracle, and MSSQL. The default configuration assumes the use of DB2. You must edit the data source definition, and configure the access information.

The Related Events feature requires two Netcool/Impact services, and Seasonal Events requires six services. You must start all of these services.

Post-installation configuration: ObjectServer data source

- Configure access to the ObjectServer
 - Required for Related Events feature
 - Update *ObjectServerForNOI* data source
 - ObjectServer host
 - ObjectServer port number
 - ObjectServer user name
 - ObjectServer password
- Update ObjectServer data type
 - Expand *ObjectServerForNOI*
 - Edit *AlertsForNOITable*
 - Refresh the column information

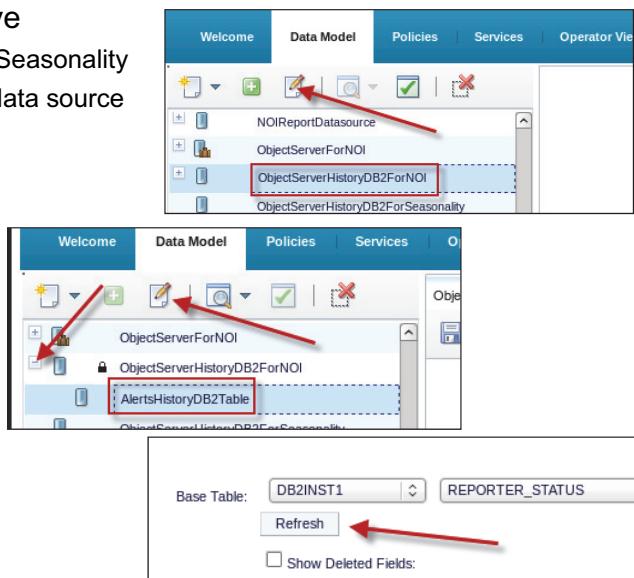


Postinstallation configuration: ObjectServer data source

The Events Analytics functions process events from the archive database and events from the ObjectServer. You must configure a Netcool/Impact data source for the ObjectServer with the appropriate access information. In addition, open the data type that is associated with the *alerts.status* table and refresh the column names. This action updates the data type with any custom columns.

Post-installation configuration: Event archive data source

- Configure access to the event archive
 - Required for Related Events feature and Seasonality
 - Update *ObjectServerHistoryDB2ForNOI* data source
 - Database host,
 - Port number
 - User name
 - Password
 - Database name [REPORTER]
- Update event archive data type
 - Expand *ObjectServerHistoryDB2ForNOI*
 - Edit *AlertsHistoryDB2Table*
 - Refresh the column information



Postinstallation configuration: Event archive data source

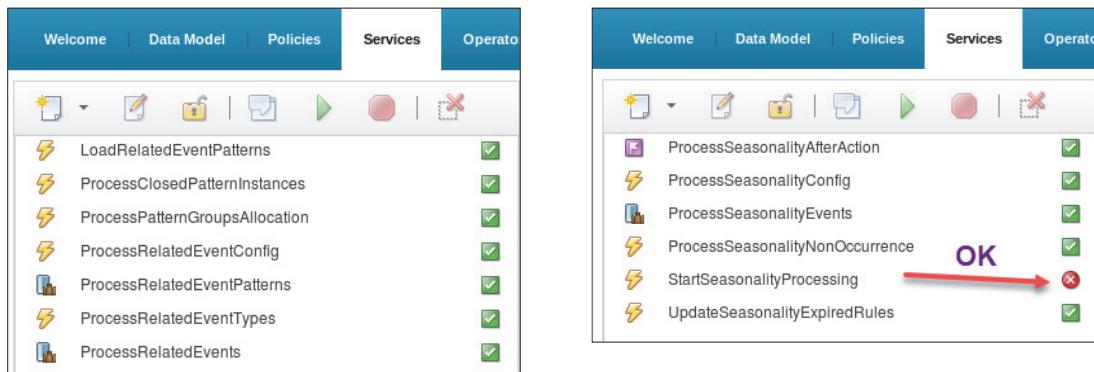
Related Events and Seasonal Events share the data type that defines the access to the event archive database. You must configure a Netcool/Impact data source for the archive database with the appropriate access information. In addition, open the data type that is associated with the REPORTER_STATUS table and refresh the column names. This action updates the data type with any custom columns.



Important: You might notice a data type that is labeled *ObjectServerHistoryDB2ForSeasonality*. That data type is no longer used by the Seasonal Events feature.

Post-installation configuration (1)

- Verify Netcool/Impact services for Related Events
- Verify Netcool/Impact services for Seasonality



© Copyright IBM Corporation 2019

Postinstallation configuration (1)

Netcool/Impact services are runnable components of the Impact Server that you start and stop using both the GUI and the CLI. This slide illustrates the process to verify the Netcool/Impact services for Related Events and Seasonality.

Post-installation configuration (2)

- Create a new Impact Data Provider in DASH
 - Required for Event Analytics feature

Name	Type	Description	Connection
Impact_NCICLUSTER	Impact_NCICLUSTER	Impact_NCICLUSTER	Remote
Tivoli Directory Integrator	TDI	TDI Generic Data Provider (1.0.26)	Local

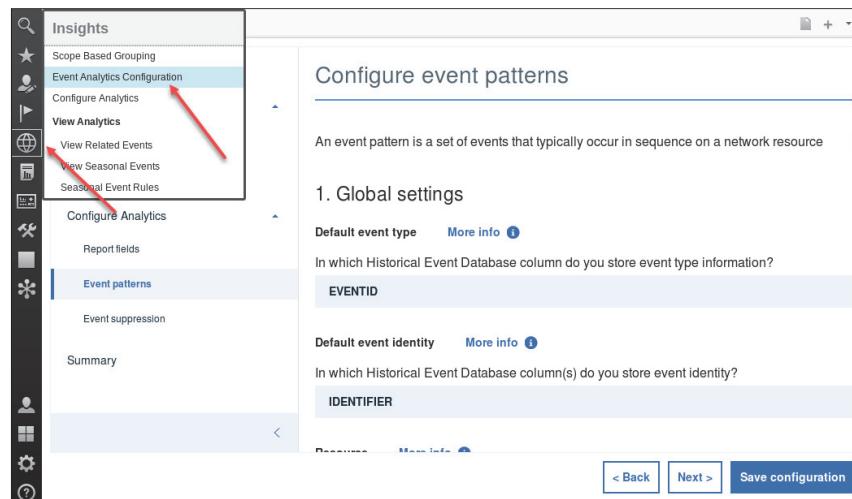
© Copyright IBM Corporation 2019

Postinstallation configuration (2)

This slide shows a configure Netcool/Impact connection in Dashboard Application Services Hub.

Post-installation configuration (3)

Run the Event Analytics Configuration wizard



© Copyright IBM Corporation 2019

Postinstallation configuration (3)

Use the Event Analytics Configuration wizard to finish setting up the related events and seasonality features. You can also use this wizard to change your configuration after installation is complete.

Student exercises



© Copyright IBM Corporation 2019

Student exercises

Refer to the exercises for Unit 3 in the student exercises guide.

Summary

You now should be able to perform the following tasks:

- Install the event search components
- Verify the event search feature
- Configure the event analytics features

© Copyright IBM Corporation 2019

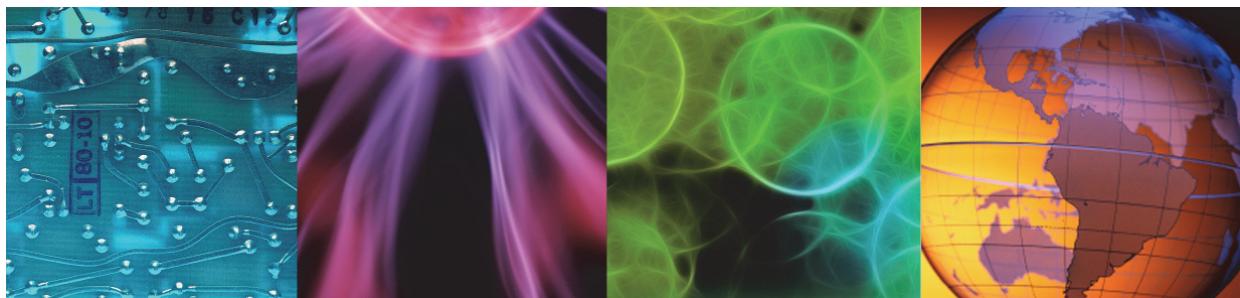
Summary



4 IBM Tivoli Network Manager



IBM Tivoli Network Manager



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this unit, you learn how to install IBM Tivoli Network Manager and the Topology Search feature.

Objectives

In this unit, you learn to perform the following tasks:

- Install and configure IBM Tivoli Network Manager
- Install and configure the Topology Search feature

© Copyright IBM Corporation 2019

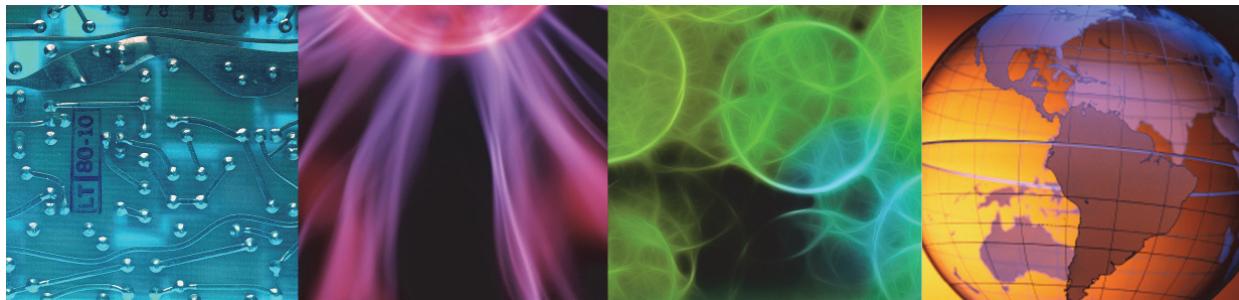
Objectives



Lesson 1 Installing Network Manager



Lesson 1 Installing Network Manager



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to install IBM Tivoli Network Manager on a single server.

Installation overview

1. Install Netcool Operations Insight
2. Install Network Manager database creation scripts
3. Create the topology database
4. Install Network Manager core components
 - Modifies the ObjectServer
 - Creates topology database table structure
5. Install Network Manager GUI components
6. Install Network Manager reports
7. Install Network Health Dashboard
8. Post-installation configuration
9. Install the Network Manager Insight Pack and configure the connection to the NCIM topology database

© Copyright IBM Corporation 2019

Installation overview

This slide contains a list of the basic steps to install IBM Tivoli Network Manager as an add-on to Netcool Operations Insight.

Installing database creation scripts

1. Download the software

- IBM Tivoli Network Manager IP Edition 4.2.0.7 Linux Multilingual (CC29QML)
- Expand to some temporary directory, for example:
`/tmp/itnm
unzip ITNMIPREV4.2.0.7LNXML.zip`

Note: all Network Manager components are bundled in the same installation file

2. Install with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
.IBMIM
```

* Assumes that IBM Installation Manager is installed by the **netcool** user

3. Define software repository

```
/tmp/itnm/repositories/disk1/diskTag.inf
```

4. Select installation package

```
Network Manager topology database creation scripts Version 4.2.0.7
```

© Copyright IBM Corporation 2019

Installing database creation scripts

Network Manager requires a database to use to store the network topology.

Network Manager 4.2.0.7 supports the following topology databases:

- IBM Db2 version 10.1 Enterprise Server Edition
- IBM Db2 version 10.5 Workgroup Server Edition
- IBM Db2 version 10.5 Enterprise Server Edition
- IBM Db2 version 11.1 Enterprise Server Edition
- IBM Db2 version 11.1 Advance Enterprise Server Edition
- Oracle Database version 11g, Enterprise Edition with Partitioning option
- Oracle Database version 12c, Enterprise Edition with Partitioning option

You install the database software separately. The steps on this slide assume that you use DB2 for the topology database.

The installation process that is described on this slide creates an SQL file. You use that SQL to create the topology database.

Creating the topology database

1. Create a user
 - The user owns the topology database
 - For example, ncim
 - The user must belong to the db2iadm1 group
2. Add the DB2 environment settings to the user

Source /home/db2inst1/sqllin/db2profile

3. Create the topology database

Use the db2inst1 user for this step

```
cd /opt/IBM/tivoli/netcool/precision/scripts/sql/db2
./create_db2_database.sh <database name> <database owner>
```

For example:

```
./create_db2_database.sh NCIM ncim
```

- Creates the NCIM database
- Assigns ownership to the ncim user

© Copyright IBM Corporation 2019

Creating the topology database

The steps on this slide assume that you install DB2 as the db2inst1 user. You create a new operating system user. The new user must be configured with DB2 administrator authority.

You run the database creation script as the **db2inst1** user. The script creates the database, and assigns ownership to the operating system user that you created previously.

Installing Network Manager core components

1. Install with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse
```

```
./IBMIM
```

* Assumes that IBM Installation Manager is installed by the **netcool** user

2. Define software repository

Uses the same software repository that you configured previously

3. Select installation package

Network Manager Core Components Version 4.2.0.7

© Copyright IBM Corporation 2019

Installing Network Manager core components

As mentioned previously, the Network Manager components are bundled in one installation file. You use the same software repository for all Network Manager components.

ObjectServer Configuration

- Enter these ObjectServer values:
 - Name
 - Host
 - Port
 - User ID
 - Password

ObjectServer Configuration

Network Manager needs to be configured to report events to a Netcool/OMNibus ObjectServer. The Netcool/OMNibus ObjectServer should already be running. Additional configuration required by Network Manager in the Netcool/OMNibus ObjectServer will be automatically added as part of this installation. Enter connection details of the Netcool/OMNibus ObjectServer that Network Manager will use.

Name:	NOI_AGG_P
Host:	host1.csite.edu
Port:	4100
Super user ID:	root
Password:	*****

Skip ObjectServer connection details verification and configuration.

- The installation process modifies the ObjectServer
- Do not* select the box to skip the verification

© Copyright IBM Corporation 2019

ObjectServer Configuration

IBM Tivoli Network Manager requires access to an ObjectServer. When you install Network Manager with Netcool Operations Insight, you configure Network Manager to use the existing ObjectServer.

The installation process connects to the ObjectServer, and makes several modifications.



Important: Do not select the option to skip the ObjectServer verification. If you select this option, the installation process does not modify the ObjectServer.

Network Manager users

- The installation process creates two default users:

- **itnmadmin**
- **itnmuser**

Network Manager users

Network Manager needs dedicated users to be created in the Netcool/OMNibus ObjectServer. Enter a password for the default Network Manager users itnmadmin and itnmuser. The same password will be assigned to the two users.

Password:

Confirm password:

- Enter a value for the password
- The installer creates the users in the ObjectServer

© Copyright IBM Corporation 2019

Network Manager users

The installation process creates two Network Manager users in the ObjectServer: **itnmadmin** and **itnmuser**. The password that you enter on this screen is used for both users.

Network domain name

- Enter a value for the domain name

Network domain name
The initial name of the network domain. A network domain represents a collection of network entities to be discovered and managed.
Network domain name: NOI_AGG_P

- The name is just text
- Use the ObjectServer name to avoid confusion

© Copyright IBM Corporation 2019

Network domain name

Enter a name for the network domain. This name is visible to network operators and product administrators. You can add, remove, and change domains later. Record the name that you choose. You need this name to start Network Manager components.



Hint: You can use any valid text string for the domain name. If you use the ObjectServer name, you might avoid some confusion.

Topology Database

- Select the type of database
 - DB2
 - Oracle
- Enter values for these fields:
 - Database name
 - Host
 - Port
 - User ID
 - Password

Topology Database

Network Manager needs a topology database to store discovery results. Please configure the type of database and the connection details.

Database server type

DB2 (default)
 Oracle

Database name: NCIM

Server host: host1.csite.edu

Server port: 50000

User ID: ncim

Password: *****

Create tables to hold topology data in selected database.

Skip database connection details verification.

- The installation process validates the access information
- The installation process creates the table structure

© Copyright IBM Corporation 2019

Topology Database

Enter the access information for the topology database. When you created the database previously, you did not populate the database with structure. When you install the Network Manager core components, the installation process adds the table structure to the database.

Poller Aggregation

Enter the location for Python

Poller Aggregation

The poller aggregation engine requires Python version 2.6 or 2.7 to be installed on this server. Enter the path to the Python installation.

Python path:

Next steps:

- Review the installation summary
- Click **Install**

© Copyright IBM Corporation 2019

Poller Aggregation

Enter the fully qualified path for the Python software.

After this page in the wizard, you can review an installation summary, and click **Install**. The core components take about 15 minutes to install.

Installing Network Manager GUI components

1. Install with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse
```

```
./IBMIM
```

* Assumes that IBM Installation Manager is installed by the **netcool** user

2. Define software repository

Uses the same software repository that you configured previously

3. Select installation package

Network Manager GUI Components Version 4.2.0.7

© Copyright IBM Corporation 2019

Installing Network Manager GUI components

As mentioned previously, the Network Manager components are bundled in one installation file. You use the same software repository for all Network Manager components.

Jazz for Service Management

- Enter values for these fields:
 - Installation directory
 - User ID
 - Password

Jazz for Service Management properties

Network Manager needs to deploy a Web Application into the IBM Dashboard Application Service Hub. Please confirm the install location of the Jazz for Service Management instance you want to use.

Installation directory details

/opt/IBM/JazzSM

Enter the credentials of an existing Jazz for Service Management user that has administrative permissions

JazzSM user credentials

User name smadmin

Password

- The user must be a Jazz for Service Management administrator
- The user must also be capable of running Web GUI Administrative API (WAAPI)
 - Add the `ncw_admin` role to the **smadmin** user

© Copyright IBM Corporation 2019

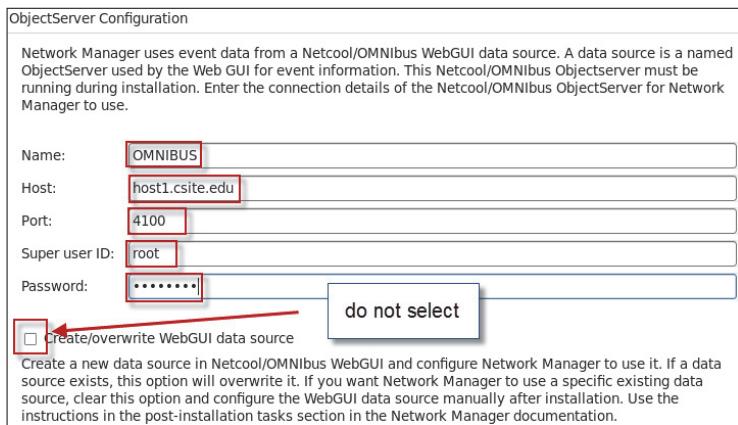
Jazz for Service Management

When you install the Network Manager GUI components, you modify Jazz for Service Management. The installation process requires a user with Jazz for Service Management administrative authority.

The installation process also modifies Web GUI. The process makes the modifications with the Web GUI API utility. By default, the Jazz for Service Management administrative user cannot use the Web GUI API utility. You must add the `ncw_admin` role to the user before you install the GUI components.

ObjectServer Configuration

- Enter ObjectServer values for these fields:
 - Name
 - Host
 - Port
 - User ID
 - Password
- Do not select the box to overwrite the Web GUI data source*
- If you do, the installer will replace the existing data that was created when Web GUI was installed



© Copyright IBM Corporation 2019

ObjectServer Configuration

When you install the Network Manager GUI components, the installation process requires access information for the ObjectServer. The installation process uses this information to create a Web GUI data source definition.

When you install Network Manager with Netcool Operations Insight, a Web GUI data source definition exists. The definition was created when you installed Web GUI. Do not select the option to overwrite the Web GUI data source. If you select this option, the installation process removes the existing data source, and configures WebSphere to use the ObjectServer as the Virtual Member Manager user repository. WebSphere is configured to use LDAP as the user repository.

Network Manager users

- The installation process creates *three* default users:

- **itnadmin**
- **Itnmuser**
- **itnmclient**

Network Manager users

Network Manager needs dedicated users to be created in the Netcool/OMNibus ObjectServer (itnadmin, itnmuser) and the WebSphere users repository (itnmclient). Enter the initial password for these three users. The same password will be assigned to all three users. The password of an already existing user will not be changed.

Password:

Confirm password:|

- Enter a value for the password
- The installer creates these users in Dashboard Application Services Hub

© Copyright IBM Corporation 2019

Network Manager users

When you install Network Manager core components, the installation process creates users in the ObjectServer. When you install Network Manager GUI components, the installation process creates the same users in WebSphere, and assigns the Network Manager Dashboard Application Services Hub roles. In the class exercises, WebSphere is configured to use LDAP, and WebSphere is configured to write new users and groups to LDAP. When you install the Network Manager GUI components, the installation process creates the sample users in LDAP.

Topology Database

- Select the type of database:

- DB2
 - Oracle

- Enter values for these fields:

- Database name
 - Host
 - Port
 - User ID
 - Password

- Next steps:

- Review the installation summary
 - Click **Install**

Topology Database

Network Manager needs a topology database to store discovery results. Please configure the type of database and the connection details.

Database server type

DB2 (default)
 Oracle

Database name: NCIM

Server host: host1.csuite.edu

Server port: 50000

User ID: ncim

Password: *****

Skip database connection details verification.

© Copyright IBM Corporation 2019

Topology Database

When you install the Network Manager GUI components, the installation process creates more tables in the topology database.

After this page in the wizard, you can review an installation summary, and click **Install**. The GUI components take about 50 minutes to install.

Installing Network Manager Reports

1. Install with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse
```

```
./IBMIM
```

* Assumes that IBM Installation Manager is installed by the **netcool** user

2. Define software repository

Uses the same software repository that you configured previously

3. Select installation package

Network Manager Reports Version 4.2.0.7

Tivoli Common Reporting is installed separately

The Network Manager Reports installation adds the reports to Tivoli Common Reporting

© Copyright IBM Corporation 2019

Installing Network Manager Reports

You must install the Tivoli Common Reporting software separately. The software is not bundled with Network Manager.

When you install Network Manager Reports, the installation process imports the report package into Tivoli Common Reporting, and creates the necessary data sources.

Jazz for Service Management

- Enter values for these fields:
 - Installation directory**
 - User ID**
 - Password**

Jazz for Service Management properties

Network Manager needs to deploy reports into the Jazz for Service Management Reporting Service. Please confirm the install location of the Jazz for Service Management instance you want to use.

Installation directory details

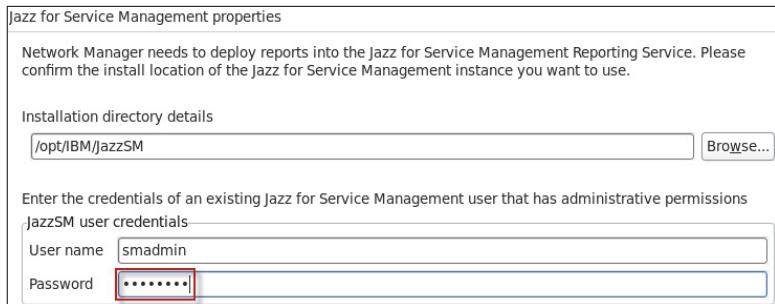
/opt/IBM/JazzSM

Enter the credentials of an existing Jazz for Service Management user that has administrative permissions

JazzSM user credentials

User name

Password



- The user must be a Jazz for Service Management administrator

© Copyright IBM Corporation 2019

Jazz for Service Management

The installation process uses the Jazz for Service Management administrator user to add the Network Manager reports to Tivoli Common Reporting.

Administrator Credentials

- Enter values for these fields:

- User ID
 - Password

Administrator Credentials

IBM Installation Manager needs the credentials of an OMNIBUS WebGUI administrative user (for example, itnadmin) to manage filters and views. The user must have the ncw_admin role and privileges to run the Netcool WebGUI waapi command. Ensure that the user authentication repository is accessible from this server before continuing.

User ID:

Password:

- The user must be capable of running Web GUI Administrative API (WAAPI)
 - Add the ncw_admin role to the **itnadmin** user

© Copyright IBM Corporation 2019

Administrator Credentials

The installation process requires a user who can run the Web GUI API utility.

Topology Database

- Select the type of database
 - DB2
 - Oracle
- Enter values for these fields
 - Database name
 - Host
 - Port
 - User ID
 - Password
- Next steps:
 - Review the installation summary
 - Click **Install**

Topology Database

Network Manager needs a topology database to store discovery results. Please configure the type of database and the connection details.

Database server type

DB2 (default)
 Oracle

Database name: NCIM

Server host: host1.csuite.edu

Server port: 50000

User ID: ncim

Password: *****

Skip database connection details verification.

© Copyright IBM Corporation 2019

Topology Database

The installation process requires the access information for the topology database. The installation process uses this information to create the Tivoli Common Reporting data source definitions.

After this page in the wizard, you can review an installation summary, and click **Install**. The reports take about 30 minutes to install.

Installing Network Health Dashboard

1. Download the software

- Network Health Dashboard v4.2 Linux English (CNEK1EN)
- Expand to some temporary directory, for example:
/tmp/dashboard
unzip NETWORK_HEALTH_DASHBOARD_V4.2_LIN.zip

2. Install with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
.IBMIM
```

* Assumes that IBM Installation Manager is installed by the **netcool** user

3. Define software repository

```
/tmp/dashboard/repositories/disk1/diskTag.inf
```

4. Select installation package

```
Network Health Dashboard Version 4.2.0.1
```

© Copyright IBM Corporation 2019

Installing Network Health Dashboard

The Network Health Dashboard application is distributed as a separate installation file. You must download the file, and expand the file in some temporary directory. The Network Health Dashboard application is installed with IBM Installation Manager.

Jazz for Service Management

- Enter values for these fields:

- User ID

- Password

Jazz for Service Management properties	
WebSphere Application Server administrator permissions are required to perform this operation. Enter the credentials of an existing Jazz for Service Management user that has administrative permissions.	
User name	smadmin
Password	*****

- The user must be a Jazz for Service Management administrator

© Copyright IBM Corporation 2019

Jazz for Service Management

The installation process uses the Jazz for Service Management administrator user to add the software to Dashboard Application Services Hub.

Administrator Credentials

- Enter values for these fields:

- User ID
- Password

Administrator Credentials	
IBM Installation Manager needs the credentials of an OMNIBUS WebGUI administrative user (for example, itnmadmin) to manage filters and views. The user must have the ncw_admin role and privileges to run the Netcool WebGUI waapi command. Ensure that the user authentication repository is accessible from this server before continuing.	
User ID:	itnmadmin
Password:	*****

- The user must be capable of running Web GUI Administrative API (WAAPI)
 - Add the ncw_admin role to the itnmadmin user
- Next steps:
 - Review the installation summary
 - Click **Install**

© Copyright IBM Corporation 2019

Administrator Credentials

The installation process requires a user who can run the Web GUI API utility.

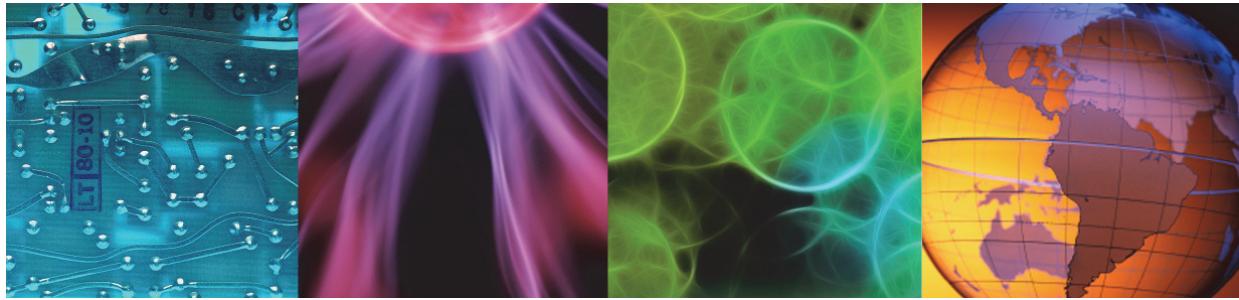
After this page in the wizard, you can review an installation summary, and click **Install**. The dashboard takes about 20 minutes to install.



Lesson 2 Post installation configuration



Lesson 2 Post-installation configuration



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to complete the post installation tasks.

Configuring Web GUI data source name

If you installed the Network Manager GUI components and chose not to create a new Web GUI data source, you must configure Network Manager to use an existing data source.

- The existing data source name is OMNIBUS
- You change the data source name in a property file

/opt/IBM/tivoli/netcool/etc/precision/ModelNcimDb.<Domain>.cfg

```
values
(
    "enumGroup in ('ASN' , 'sysServices', 'ifAdminStatus', 'ifOperStatus',
'sysServices', 'ifType', 'ifOperStatusToOperationalStatus',
'entPhysicalClass', 'cefcFRUPowerAdminStatus', 'cefcFRUPowerOperStatus',
'TruthValue', 'TruthValueString', 'entSensorType', 'entSensorScale',
'entSensorStatus', 'cefcModuleAdminStatus', 'cefcModuleOperStatus',
'ipForwarding', 'cefcPowerRedundancyMode', 'EntityType', 'ospfIfstate',
'ospfIfType', 'dot3statsDuplexStatus', 'accessProtocol', 'cdmDuplex',
'OperationalStatusEnum', 'RttMonRttType', 'RttMonCodecType',
'rttMonCtrlOperStateToStdOperStatus', 'RowStatusToStdAdminStatus',
'NqaType', 'nqaAdminParaCodecType', 'nqaScheduleOperStatusToStdOperStatus')",
    500
    "OMNIBUS"
);
create table dbModel.entityDetails
```

© Copyright IBM Corporation 2019

Configuring Web GUI data source name

The Web GUI data source name is embedded in a Network Manager configuration file. When you install Network Manager with Netcool Operations Insight, and reuse the existing Web GUI instance, you must modify the Network Manager configuration file and change the data source name.

Configuring core components to run as non-root user

- Some processes use ports under 1024
- These processes must run with the **setuid** bit set so that they can run as a root-level equivalent
- You must run the following instructions as the **root** user

1. Change to the location of the required script

```
cd /opt/IBM/tivoli/netcool/precision/scripts
```

2. Run the script

```
./setup_run_as_setuid_root.sh
```

© Copyright IBM Corporation 2019

Configuring core components to run as non-root user

On UNIX, if you installed Network Manager as a non-root user, and you want to allow that user permissions to run the core components, you must log in as root and complete more configuration.

Configuring processes to start automatically

You must run the following instructions as the **root** user

1. Change to the location of the required script

```
cd /opt/IBM/tivoli/netcool/precision/install/scripts
```

2. Create the ncp startup script

```
./create_itnm_control_scripts.sh ncp -auto_only
```

3. Create the Apache Storm startup script

```
./create_itnm_control_scripts.sh storm -auto_only
```

© Copyright IBM Corporation 2019

Configuring processes to start automatically

On UNIX systems, as a post installation task for non-root installations you can configure your Network Manager processes to start automatically when your system is started or restarted.

You must run two separate scripts. One script creates the startup process for the core components, and the second script creates the startup process for the Apache Storm components.

The two scripts create these two files:

```
/etc/init.d/ncp  
/etc/init.d/storm
```

Configuring Network Manager environment variables

- You installed Network Manager as a non-root user
- You run Network Manager as a non-root user

1. Change to the home directory

```
cd /home/netcool
```

2. Open the environment file for edit

```
gedit .bashrc
```

3. Add the following line to the end of the file

```
source $NCHOME/env.sh
```

© Copyright IBM Corporation 2019

Configuring Network Manager environment variables

The user that you use to install and run Network Manager components requires some environment variables. A file contains the required settings. You must include that file as part of the existing environment configuration.

Starting Network Manager

You run Network Manager as a non-root user

1. Start all components

itnm_start

2. Verify component status

itnm_status

[netcool@host1 ~]\$ itnm_status			
Network Manager:			
Domain: NOI_AGG_P			
ncp_ctrl	RUNNING	PID=9138	NOI_AGG_P
ncp_store	RUNNING	PID=9248	NOI_AGG_P
ncp_class	RUNNING	PID=9249	NOI_AGG_P
ncp_model	RUNNING	PID=9452	NOI_AGG_P
ncp_disco	RUNNING	PID=9592	NOI_AGG_P
ncp_d_helpserv	RUNNING	PID=9250	NOI_AGG_P
ncp_config	RUNNING	PID=9251	NOI_AGG_P
ncp_poller_default	RUNNING	PID=9984	NOI_AGG_P
ncp_poller_admin	RUNNING	PID=9985	NOI_AGG_P
nco_p_ncpmonitor	RUNNING	PID=9252	NOI_AGG_P
ncp_g_event	RUNNING	PID=9705	NOI_AGG_P
ncp_webtool	RUNNING	PID=9253	NOI_AGG_P
ncp_virtualdomain	RUNNING	PID=10401	NOI_AGG_P
Apache Storm:			
supervisord	RUNNING	PID=9652	
storm_nimbus	RUNNING	PID=9655	
storm_supervisor	RUNNING	PID=9656	
zookeeper	RUNNING	PID=9654	
Storm topologies:			
NMStormTopology	ACTIVE		

© Copyright IBM Corporation 2019

Starting Network Manager

The installation process configures several utility commands that you use to start, stop, and verify the status of Network Manager components.

Use the following command syntax to start Network Manager components:

itnm_start [ncp | storm]

Use the following command syntax to stop Network Manager components:

itnm_stop [ncp | storm]

Use the following command syntax to verify the status of Network Manager components:

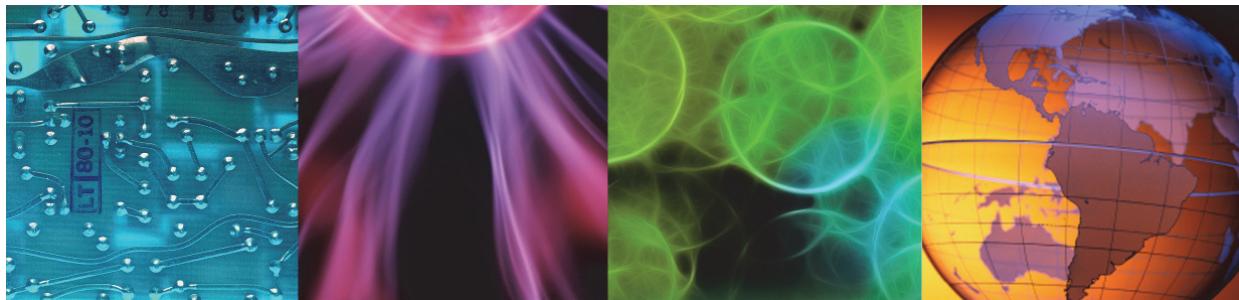
itnm_status [ncp | storm]

The component name is optional for each of the commands. If you run the command with no component name, the command assumes both ncp and storm components.

Lesson 3 Installing and configuring Topology Search



Lesson 3 Installing and configuring Topology Search



© Copyright IBM Corporation 2019

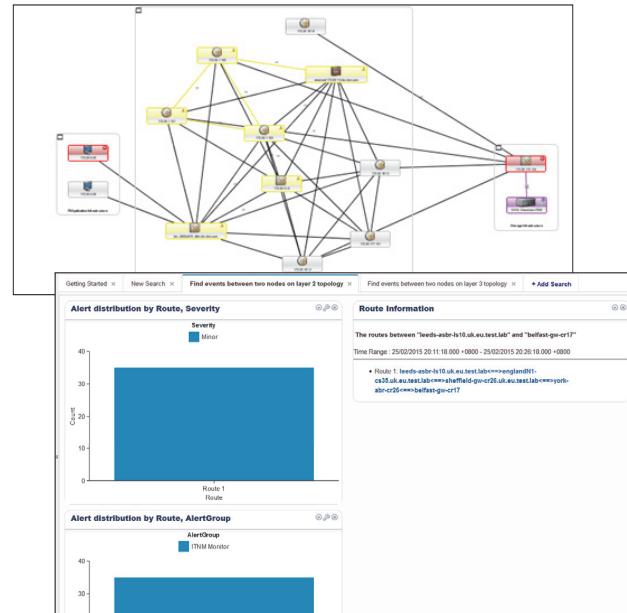
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to perform the following tasks:

- Install the Network Manager Insight Pack
- Configure the Topology Search feature

Feature overview

- Custom Log Analysis application
- Searches Network Manager topology database
 - Locates all devices in a network route
- Searches Log Analysis event history
 - Locates events for the devices in the network route
- Presents the event summary in the Log Analysis user interface



© Copyright IBM Corporation 2019

Feature overview

The Topology Search feature consists of a custom Log Analysis application, and several tools that you use to run the application. You install tools in the Web GUI Event Viewer, Network Manager topology viewer, and the Log Analysis user interface.

To use the application, you use one of the tools to select two devices. The tool passes the device names to the Log Analysis topology search application. The application queries the Network Manager topology database, and locates all devices in the path between the two selected devices. The application uses the list of devices names to search the event history. The application retrieves the event records for all devices and presents the summarized results in the Log Analysis user interface.

Implementation summary

1. Install the Network Manager Insight Pack
2. Configure the insight pack
3. Modify the Web GUI server.init file
4. Configure Network Manager users for access to Log Analysis
5. Modify the ObjectServer to add custom triggers
6. Add topology search tools to Web GUI
7. Add topology search tools to the Network Manager topology GUI
8. Configure Network Manager users for access to topology search tools

© Copyright IBM Corporation 2019

Implementation summary

This slide contains a list of the steps that you must perform to complete the installation and configuration of topology search.

Installing the Network Manager Insight Pack

1. Create a directory for the Insight Pack

```
cd /opt/IBM/LogAnalysis/unity_content/
mkdir NetworkManager
```
2. Copy the Insight Pack to the new directory

```
cp /tmp/la/NetworkManagerInsightPack_v1.3.5.0.zip NetworkManager/
```

3. Install the Insight Pack

```
/opt/IBM/LogAnalysis/utilities/pkg_mgmt.sh -install NetworkManagerInsightPack_v1.3.5.0.zip
```

© Copyright IBM Corporation 2019

.Installing the Network Manager Insight Pack

The insight pack is distributed as a separate installation file:

IBM Tivoli Netcool/Network Insight Pack V1.3.0.0 for IBM Operations Analytics - Log Analysis V1.3 English Linux (CNZ43EN). This package contains the installation archive file: NetworkManagerInsightPack_v1.3.5.0.zip.

The insight pack is not installed with IBM Installation Manager. Instead, the insight pack is installed with a Log Analysis utility.

Configuring the Network Manager Insight Pack

- The topology search application needs access information for the topology database

- Change to the target directory:

```
cd /opt/IBM/LogAnalysis/AppFramework/Apps/NetworkManagerInsightPack_v1.3.5.0/Network_Topo
```

- Open the property in a text editor:

```
gedit NM_EndToEndSearch.properties
```

- Modify the following properties:

```
ncp.dla.datasource.type = db2  
ncp.dla.datasource.driver = com.ibm.db2.jcc.DB2Driver  
ncp.dla.datasource.url = jdbc:db2://host1.csite.edu:50000/NCIM  
ncp.dla.datasource.schema = ncim  
ncp.dla.datasource.ncpgui.schema = ncpgui  
ncp.dla.datasource.username = ncim  
ncp.dla.datasource.password = object00  
ncp.dla.datasource.encrypted = false  
ncp.dla.datasource.keyFile = /opt/IBM/LogAnalysis/wlp/usr/servers/Unity/keystore/unity.ks  
ncp.dla.datasource.loginTimeout = 5
```

© Copyright IBM Corporation 2019

Configuring the Network Manager Insight Pack

The topology search application requires access to two types of data. The first type of data is the Log Analysis event history. The topology search application uses a Log Analysis data source to access the event history.



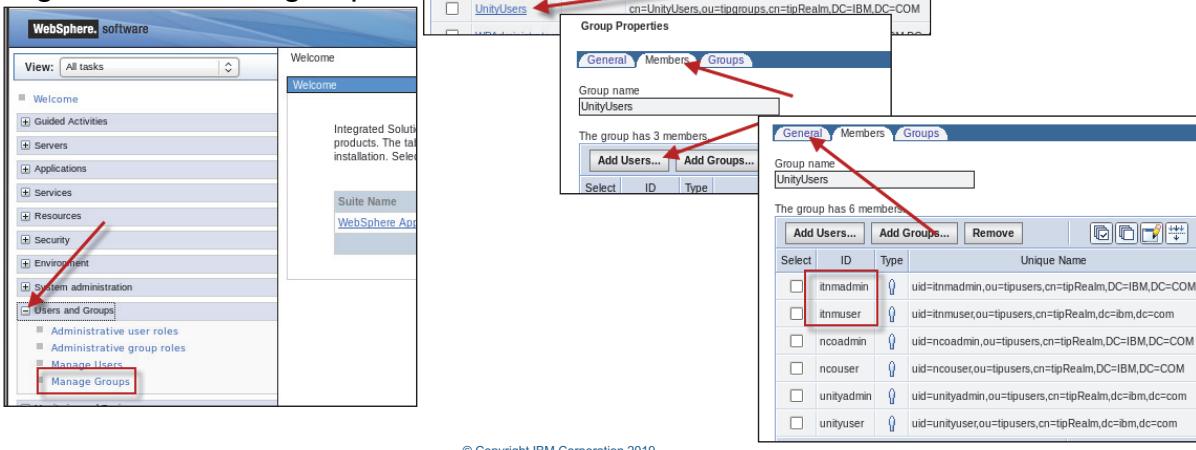
Note: The application uses the same data source that you defined previously when you installed the Netcool/OMNIbus Insight Pack in a previous unit.

The second type of data is the Network Manager topology database. You configure the access information in a property file. The topology database access information is found in a Network Manager configuration file:

```
/opt/IBM/tivoli/netcool/etc/precision/DbLogins.NOI_AGG_P.cfg
//*****
//
// File: DbLogins.NOI_AGG_P.cfg
//
// Automatically generated on: Wed Jul 31 19:35:57 2019
// by '' on the domain 'NOI_AGG_P' using ncp_config.
//
//*****
insert into config.dbserver
(
    m_DbId,
    m_Server,
    m_DbName,
    m_OracleService,
    m_Schema,
    m_Hostname,
    m_Username,
    m_Password,
    m_PortNum,
    m_EncryptedPwd
)
values
(
    "NCIM",
    "db2",
    "NCIM",
    1,
    "ncim",
    "host1.csuite.edu",
    "ncim",
    "@44:XmmVSTB+rM/E5Yliq/S2VG2PCuk7sUwRtGd2G1IjMhY=@",
    50000,
    1
);
```

Configuring Network Manager users for Log Analysis access (1)

- A valid Log Analysis user belongs to the UnityUsers group
- You must add the Network Manager users to this group



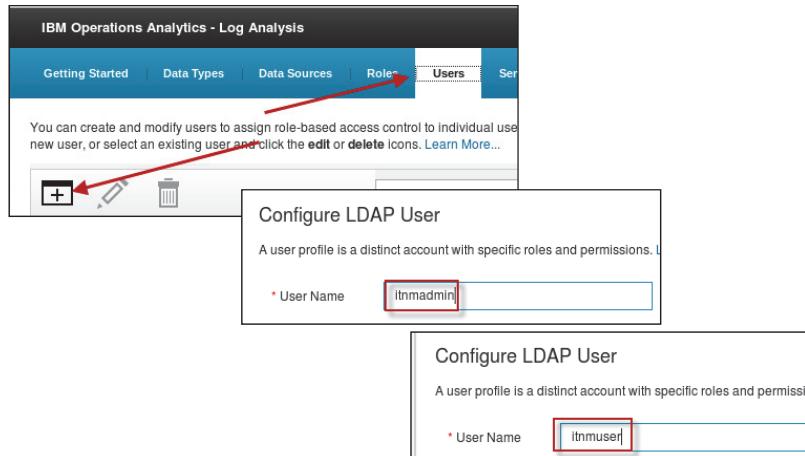
Configuring Network Manager users for Log Analysis access (1)

You must enable Network Manager users to allow access to Log Analysis. In the first step, you add Network Manager users to the UnityUsers group. Membership in the UnityUsers group allows access to the Log Analysis user interface.

You can add individual users to the group, or you add a group of users to the group. The group option is easier and more efficient.

Configuring Network Manager users for Log Analysis access (2)

- You must add the Network Manager users to Log Analysis



© Copyright IBM Corporation 2019

Configuring Network Manager users for Log Analysis access (2)

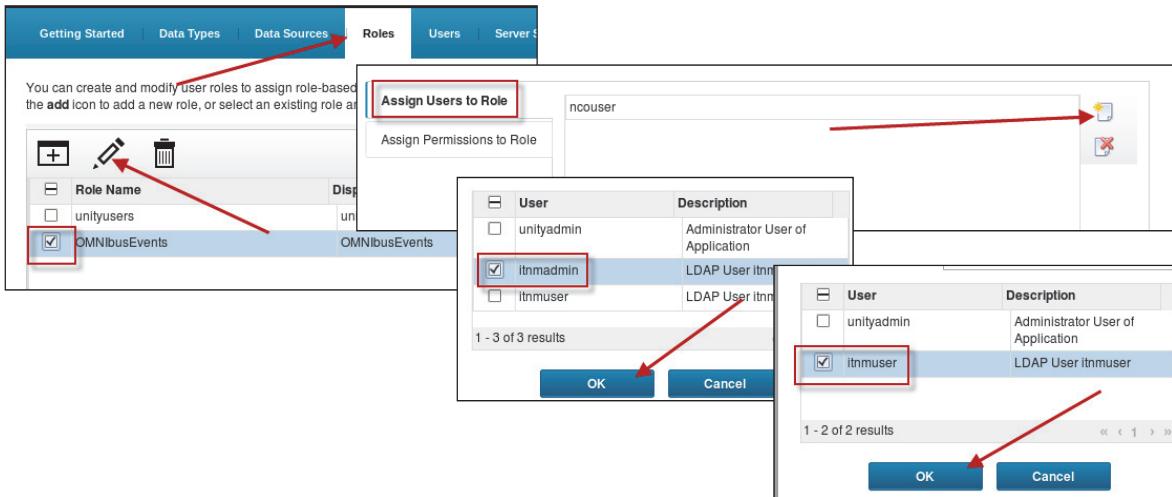
The Log Analysis application implements a role-based access control mechanism. This access mechanism controls access to Log Analysis data sources. You configure access to data sources on a user basis. You must add the Network Manager users to the Log Analysis role-based access mechanism.



Note: Currently, the access mechanism supports only users, not groups.

Configuring Network Manager users for Log Analysis access (3)

- You must add the Network Manager users to the Log Analysis role



© Copyright IBM Corporation 2019

Configuring Network Manager users for Log Analysis access (3)

The Log Analysis role defines access to one or more data sources. The role definition contains a list of data sources, and a list of users who can access those data sources.

When you installed the Netcool/OMNIbus Insight Pack in a previous unit, you created a role that controls access to the event history data source. You must modify the existing role, and add the Network Manager users.

Modifying the ObjectServer

- You must modify the ObjectServer when you use the Network Manager Insight Pack
- The modifications are included in an SQL file
- The SQL file adds a custom trigger to the ObjectServer
- The trigger ensures that an event is enriched with a value for NmosObjInst before it passes to Log Analysis
 - The trigger runs every 5 seconds
 - If the events are not enriched 20 seconds after the trigger runs, the events are forwarded to IBM Operations Analytics Log Analysis without NmosObjInst data.
- The topology search application requires a value for NmosObjInst

1. Change to the directory location of the supplied file.

```
cd $OMNIHOME/extensions/scala
```

2. Import the file into the ObjectServer.

```
nco_sql -server NOI_ AGG_P -user root -password object00 < scala_itnm_configuration.sql
```

© Copyright IBM Corporation 2019

Modifying the ObjectServer

The topology search application uses the value found in the NmosObjInst ObjectServer event record column to search the Network Manager topology database. Network Manager enriches ObjectServer event records and populates the value for the NmosObjInst column. When a new event is created in the ObjectServer, a short delay results before Network Manager enriches the new event with a value for NmosObjInst.

When you implement the topology search feature, you add a custom trigger to the ObjectServer. The trigger keeps the Message Bus gateway from processing an event record until the Network Manager enrichment populates the NmosObjInst column. The trigger ensures that event records that the gateway sends to Log Analysis contain values for the NmosObjInst column.

You create the trigger when you import an SQL file into the ObjectServer.

Adding topology search tools to Web GUI

- Install the tools and menus to start the custom apps from the Web GUI
- The configuration for these tools is included in the Web GUI instance
- You use the Web GUI Administration API utility to add the tools

1.Change to the WAPPI bin directory:

```
cd /opt/IBM/netcool/gui/omnibus_webgui/waapi/bin
```

2.Run the following command to install the tools:

```
./runwaapi -file  
/opt/IBM/netcool/gui/omnibus_webgui/extensions/LogAnalytics/scalaEventTopology.xml
```

© Copyright IBM Corporation 2019

Adding topology search tools to Web GUI

You use the Web GUI API utility to add the topology search tools and menus to the Event Viewer.

Adding topology search tools to Network Manager GUI (1)

- 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
- Modify the topoviz property settings

1. Change to the target directory:

```
cd /opt/IBM/netcool/gui/precision_gui/profile/etc/tnm
```

2. Open the property file in a text editor:

```
gedit topoviz.properties
```

3. Add the following line on the end of the file:

```
topoviz.unity.customappsui=https://<Log Analysis host>:9987/Unity/CustomAppsUI
```

© Copyright IBM Corporation 2019

Adding topology search tools to Network Manager GUI (1)

You must modify the configuration of the Network Manager topology visualization user interface to add the topology search tools. The configuration requires two steps. In the first step, you modify a property file, and configure a property that defines the URL for the Log Analysis application.

Adding topology search tools to Network Manager GUI (2)

Modify the device menu file:

1. Change to the target directory:

```
cd /opt/IBM/netcool/gui/precision_gui/profile/etc/tnm/menus
```

2. Open the file for edit:

```
gedit ncp_topoviz_device_menu.xml
```

3. Add the following line: <menu id="ncp_topo_e2esearch" />

```
<?xml version="1.0" ?>
<ncp_menu id="ncp_topoviz_device_menu" key="ncp_topoviz_device_menu"
           label="Right Click Menu">
    <definition>
        <tool id="recenterTopo" />
        <separator />
        <menu id="ncp_events_submenu" />
        <separator />
        <tool id="showDeviceStructure" />
        <tool id="showConnectivityInformation" />
        <tool id="showDeviceView" />
        <separator />
        <menu id="ncp_topo_e2esearch"/>
        <menu id="ncp_findIn_submenu" />
        <separator />
```

© Copyright IBM Corporation 2019

Adding topology search tools to Network Manager GUI (2)

To complete the configuration of the Network Manager topology visualization component, you must modify an XML file and add a reference to the topology search menu as shown on this slide.

Configuring users for access to topology search tools

- Access to the topology search tools requires the *ncp_event_analytics* role
- Add this role to the Network Manager groups
 - Network_Manager_IP_Admin
 - Network_Manager_user

The screenshot shows the 'Roles' section of the Network Manager interface. On the left, there's a sidebar with icons for Roles, Group Roles, and User Roles. A red arrow points from the 'User Roles' icon to the main configuration area. The main area displays two tables: one for 'Network_Manager_IP_Admin' and one for 'Network_Manager_User'. Both tables have columns for 'Group Name' and 'Roles'. In the 'Roles' column, the 'ncp_event_analytics' role is checked for both groups, indicated by a red box around the checked checkbox.

Group Name	Roles
Network_Manager_IP_Admin	ncp_oql_editor, ncp_networkview_admin, ncp_event_analytics
Network_Manager_User	ncp_miner, ncp_event_analytics, ncp_hopview

© Copyright IBM Corporation 2019

Configuring users for access to topology search tools

Access to tools from the Network Manager topology visualization is controlled with Dashboard Application Services Hub roles. You must add the *ncp_event_analytics* role to users or groups that require access to the topology search tools from Network Manager network views.

Student exercises



© Copyright IBM Corporation 2019

Student exercises

Refer to the exercises for Unit 4 in the student exercise guide.

Summary

You now should be able to perform the following tasks:

- Install and configure IBM Tivoli Network Manager
- Install and configure the Topology Search feature

© Copyright IBM Corporation 2019

Summary



5 IBM Tivoli Netcool Configuration Manager



IBM Tivoli Netcool Configuration Manager



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this unit, you learn how to install and configure Netcool Configuration Manager.

Objectives

In this unit, you learn to perform the following tasks:

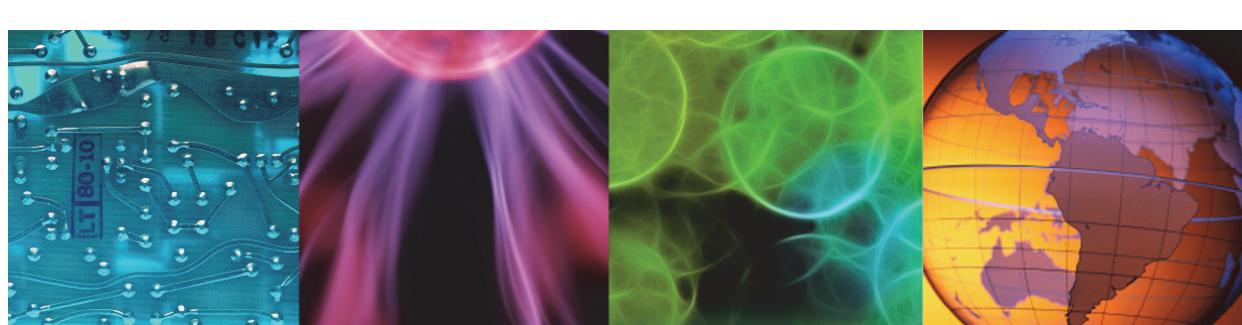
- Describe the major functions of Netcool Configuration Manager
- Describe the deployment architecture
- Install and configure Netcool Configuration Manager

© Copyright IBM Corporation 2019

Objectives



Lesson 1 Overview



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to perform the following tasks:

- Describe the deployment architecture
- Describe the system prerequisites

Network configuration and change control manager

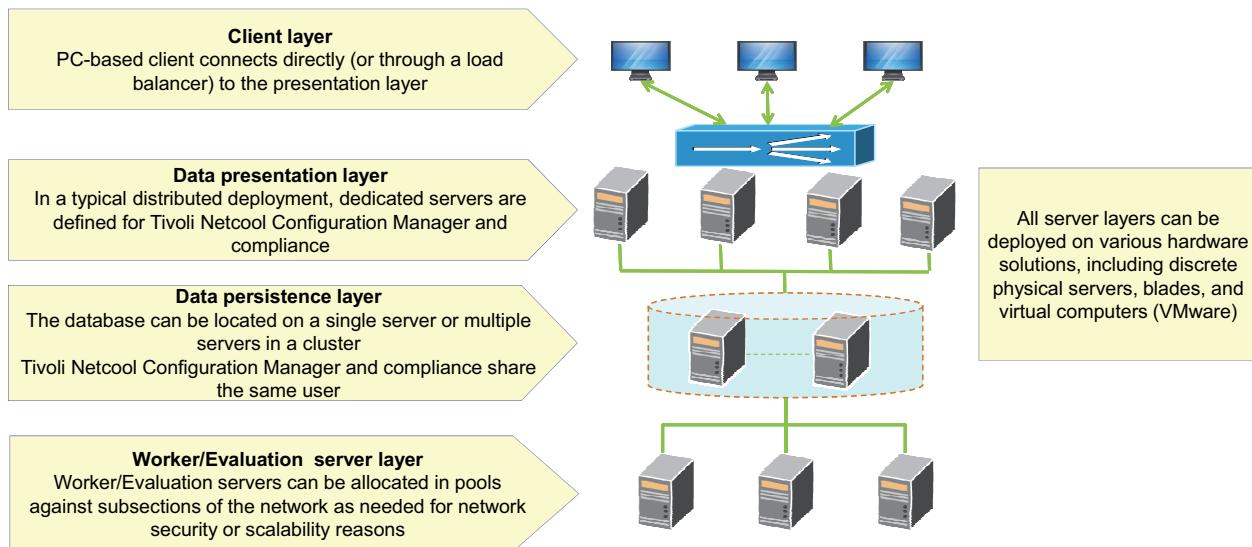
- Maintain current configurations on all network devices
- Implement network changes in a controlled and orderly fashion
- Provide an audit trail of all network device access
- Create standard configuration change templates
 - Standardize change operations
 - Provide procedural uniformity
- Analyze configurations to ensure corporate standards

© Copyright IBM Corporation 2019

Network configuration and change control manager

The value of IBM Tivoli Netcool Configuration Manager is based in its configuration management and change control philosophy. You can use it to maintain current copies of information, including network device configurations. You can track and audit state changes for future needs. For fine-tuned access control, you can quickly configure steps to approve changes and move them into production. You can also define templates to apply standard changes to the devices that are managed. Finally, you can use the data that is captured about the device and analyze it to ensure that it meets the corporate standards for documentation, security, and any other industry best practices.

Deployment architecture



© Copyright IBM Corporation 2019

Deployment architecture

The deployment architecture consists of the following layers:

The client layer uses a centrally managed thick client that supports automatic updates to the desktop software. Based on Java Web Start technology, the client layer is supported on any desktop that is operating the correct Java Runtime Environment.

The data presentation layer can be distributed across many servers to support both user interaction and integration needs. This layer enforces the security architecture and ensures that the client does not view any unauthorized data.

The data persistence layer is where all unique data about the implementation is stored. This layer can be designed to meet whatever data scalability and resiliency that the customer requires. Currently, the product supports Oracle and DB2 database servers.

The worker/evaluation server layer is where most of the processing of the application occurs. This pool of processing power can be scaled up and down, depending on the needs for network change and compliance. The evaluation server is designed for compliance analysis task. The worker server directly accesses network devices, converts native languages into XML, and applies changes.

Presentation server tasks

Serves as a security layer between the user and database of devices and configuration

Displays units of work, devices, and configurations with appropriate security setting, compliance policies and results

Sets up, schedules, and approves tasks

Processes XML to command-line interface (CLI) for GUI

Processes differences between configurations for GUI

Sends SNMP traps

© Copyright IBM Corporation 2019

Presentation server tasks

The presentation server is the main security layer for defining what users can see and do with the GUI application. It applies all the view, add, modify, and delete rights that are assigned to the groups to which users belong.

Using the security layer as a guide, it shows all the *units of work* (UOW) and devices that a user can see within the GUI. It is where units of work are created, scheduled, and approved for execution by the worker servers. It converts XML-based configurations back into CLI for users to view. Security features can limit what the user sees in a configuration file. It can compare two configurations and show the differences between them.

You can configure the presentation server to send SNMP traps to appropriate servers when various changes occur inside the application. For instance, a trap can be sent when a unit of work begins on a device.

Worker server tasks

Converts CLI to XML and XML to CLI

Decomposes units of work into tasks for optimal processing

Processes tasks based on security settings, defined by worker server resources

Communicates with network resource

Sends FTP files to appropriate locations

Holds temporary files for configurations and changes

© Copyright IBM Corporation 2019

Worker server tasks

The worker server is designed to take device drivers and use them to convert raw configuration text (CLI) and convert it into an XML representation.

The worker server takes units of work that users submit to the database from the presentation server and decomposes them into tasks. A task is a major operation against an individual device. The worker server receives tasks and processes the commands against devices.

In an implementation with multiple worker servers, the workers can be assigned which devices they can process. Workers can be restricted to processing only the devices they access because of the network design.

Workers communicate directly with network devices, typically through Telnet or SSH sessions. Workers can also employ SNMP when that is the only protocol that a device supports. This communication is used to support task execution or to provide the device when users are establishing interactive sessions.

The workers host and move change files to the appropriate locations to support the network change mechanisms.

Evaluation server tasks

Similar to worker server

Evaluates compliance policies against devices

- Review device configuration
- Cached hardware data
- Requests configuration manager to gather live data

Determines if device is compliant or not

© Copyright IBM Corporation 2019

Evaluation server tasks

An evaluation server is designed for compliance. Its main purpose is to evaluate compliance policies against devices. Using either device configurations, cached hardware information, or live data that is retrieved from the device, it determines whether the device meets a specific compliance criteria or not.

Relational database tasks

- Supports both Oracle and DB2 databases
- Holds all the important items about the solution
- Is used by all other servers
- Is a single point of failure

© Copyright IBM Corporation 2019

Relational database tasks

Configuration Manager supports both Oracle and DB2 databases. The database saves all important data for the solution, which includes the following information:

- Users and groups
- Devices and their configurations
- Generalized resources that are used for device interaction and security
- Units of work and their logs
- Keystroke logs for device interactions
- Scratch or tmp space to process UOWs

The database is a single point of failure for the entire solution, and its implementation needs serious consideration from an architectural standpoint. You must consider how long the database can be down before it seriously impacts operations. To help this decision, you can determine what tools are used in the application and other integration points. For example, if the device terminal solution is the main point of access into the network, then its unavailability is a serious problem for users.

Installation prerequisites

- Database
 - DB2 10.1, 10.5, or 11.1
 - Oracle 11G R2 and 12C
- Operating Systems
 - Linux RHEL 6 & 7, SUSE 11 & 12, or AIX 6.1 & 7.1
- Presentation Server
 - WebSphere
 - Jazz for Service Management
 - Dashboard Application Services Hub
- Reporting Services
 - WebSphere
 - Jazz for Service Management
 - Dashboard Application Services Hub
 - Reporting Services

The presentation server requires a separate installation of WebSphere, Jazz for Service Management, and Dashboard Application Services Hub

© Copyright IBM Corporation 2019

Installation prerequisites

This slide contains the software that is required in addition to the software that is bundled with Configuration Manager.

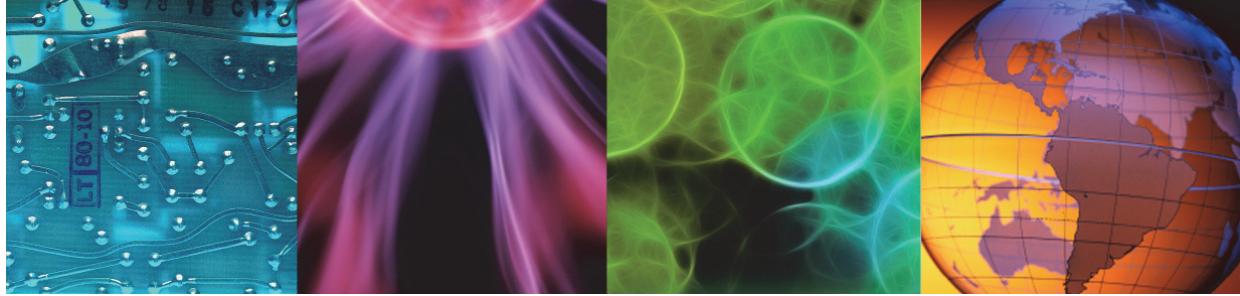
Configuration Manager requires two separate installations of WebSphere, Jazz for Service Management, and Dashboard Application Services Hub. One instance of this software is used for the Configuration Manager presentation server. The second instance is used by Network Manager and Tivoli Common Reporting. In the documentation, this instance is typically referred to as the NM GUI server.

In a production environment, Configuration Manager is typically installed on a dedicated server, which does not include Network Manager. In the class exercises, you install all components on a single server.



Lesson 2 Creating the database

Lesson 2 Creating the database



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to create the Configuration Manager database.

Operating system users

Tivoli Netcool Configuration Manager uses several operating system user IDs

- The application software is installed, and runs, as a non-root user
- The configuration database is owned by a non-root user
- A non-root user is required for FTP access to move configuration files

1. Create a user for the database

- The user must be a database administrator
For DB2, the user must belong to the db2iadm1 group
- The user requires the database environment settings

2. Create a user for FTP use

© Copyright IBM Corporation 2019

Operating system users

Configuration Manager requires three operating system users. You use one user to install and run the Configuration Manager software. You use the second user to create the Configuration Manager database. The database user must be defined with database administration privileges.

Configuration Manager uses the third user for FTP access. Configuration Manager uses the FTP user to move changes to network devices.

Creating the database

- You create the DB2 database with the **db2inst1** user ID
- You use additional SQL commands to grant access to the database by the custom user ID that you created previously

1. Create the database as the **db2inst1** user

```
db2 create database ITNCM automatic storage yes pagesize 32768 dft_extent_sz 32
```

2. Connect to the database

```
db2 connect to itncm
```

3. Issue the GRANT command

```
db2 "GRANT  
BINDADD,CONNECT,CREATE_NOT_FENCED_ROUTINE,CREATE_EXTERNAL_ROUTINE,QUIESCE_CONNECT  
ON DATABASE TO USER tncmdb"
```

In this example, the database owner user ID is **tncmdb**

© Copyright IBM Corporation 2019

Creating the database

This slide contains the commands that you use to create the Configuration Manager database with DB2. DB2 is typically installed as the root user, and the **db2inst1** user owns the software. The **db2inst1** user has database administration privileges. You use the **db2inst1** user to create the Configuration Manager database. After you create the database, you use more commands to grant access rights to the database for the Configuration Manager database user. After you grant access, you complete all subsequent database actions as the Configuration Manager database user.

Modifying the database transaction log size

Enter additional commands to update the transaction log size

```
db2 update db cfg using logfilsiz 5000  
db2 update db cfg for itncm using logprimary 200  
db2 update db cfg for itncm using logsecond 50  
db2 update db cfg for itncm using LOCKLIST 8192  
db2 commit  
db2 connect reset
```

© Copyright IBM Corporation 2019

Modifying the database transaction log size

You run more commands as the Configuration Manager database owner. These commands increase the transaction log size, and increase database storage that is used for locking.

Adding user-defined functions to the database

Install Netcool Configuration Manager user-defined functions to your database user to prevent the schema installation from reporting errors

1. Connect to the database

```
db2 connect to itncm
```

2. Install the jar file

```
db2 "CALL SQLJ.INSTALL_JAR('ibm_tivoli-ncm_db2_udf.jar', ncm_db2_udf)"
```

3. Refresh the classes

```
db2 "CALL SQLJ.REFRESH_CLASSES()"
```

© Copyright IBM Corporation 2019

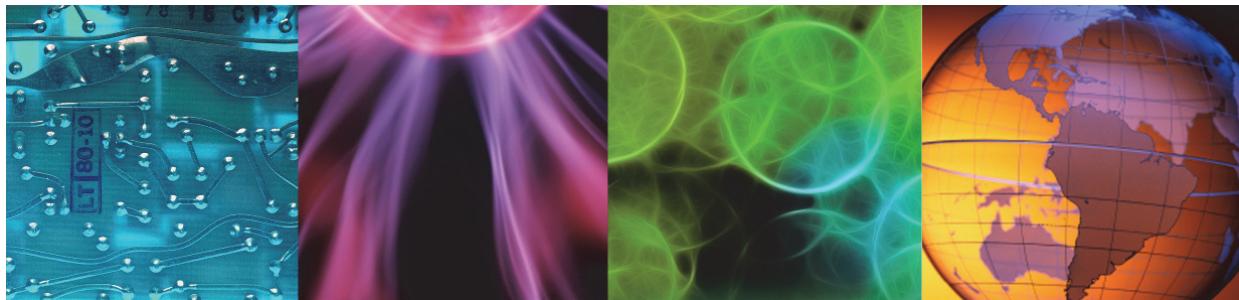
Adding user defined functions to the database

The JAR file that you use to install the user-defined functions is bundled with the Configuration Manager installation file.

Lesson 3 Installing Jazz for Service Management



Lesson 3 Installing Jazz for Service Management



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to perform the following tasks:

- Install Jazz for Service Management
- Install WebSphere Application Server
- Install Dashboard Application Services Hub

Coexisting with Netcool Operations Insight

- The Netcool Configuration Manager presentation server is based on
 - Jazz for Service Management
 - WebSphere Application Server
 - Dashboard Application Services Hub
- You cannot reuse the Netcool Operations Insight copy of Jazz for Service Management
- You must install separate copies for Netcool Configuration Manager
- If you install the software on the same server as Netcool Operations Insight, you must perform the following tasks:
 - Install the software into different directories
 - Configure the software to use different port numbers

Note: In a production environment, this is typically not the case

The following slides assume that you use a single server

© Copyright IBM Corporation 2019

Coexisting with Netcool Operations Insight

When you deploy Configuration Manager as part of the Netcool Operations Insight solution, you must be aware of the user interface requirements. Netcool Operations Insight uses Jazz for Service Management and Dashboard Application Services Hub as the primary user interface. The user interfaces for various components are integrated into Dashboard Application services Hub, including:

- Web GUI
- Netcool/Impact
- Network Manager
- Common Reporting

When you deploy Configuration Manager, you integrate extra components into Dashboard Application Services Hub, including:

- Web GUI tools that run Configuration Manager applications
- Network Manager tools that run Configuration Manager applications
- Common Reporting reports for Configuration Manager

The Configuration Manager presentation server is based on WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub. You cannot not reuse existing copies of that software. Configuration Manager requires separate copies of those products.

In a production environment, you typically install Configuration Manager on a dedicated server. In the class exercises, you install all components on a single server. In this type of deployment, you

must install the additional copies of software in separate directories, and configure the products to use different port numbers.

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (1)

1. Download the software:

- IBM WebSphere Application Server V8.5.5.15 for Jazz for Service Management for Linux Multilingual
- (CC29KML)
- Jazz for Service Management 1.1.3.3 for Linux ML (Launchpad, PRS, Jazz Repository, TDI) Multilingual
- (CC29GML)

2. Expand to some temporary directory, for example:

```
/tmp/jazz_install
```

3. Define the target installation directories

```
mkdir /opt/IBM/JazzSM_ncm
chown -R netcool:ncoadmin /opt/IBM/JazzSM_ncm
mkdir /opt/IBM/WebSphere/AppServer_ncm
chown -R netcool:ncoadmin /opt/IBM/WebSphere/AppServer_ncm
```

© Copyright IBM Corporation 2019

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (1)

Configuration Manager requires the same versions of WebSphere, Jazz for Service Management, and Dashboard Application Services Hub that you use for Netcool Operations Insight. The primary difference in the installation process is that you must install the software into different directories when you deploy the components on a single server.

For the student exercise, you use the following directories:

```
/opt/IBM/JazzSM_ncm
/opt/IBM/WebSphere/AppServer_ncm
```

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (2)

1. Install Jazz for Service Management with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
.IBMIM
```

2. Define software repositories

```
/tmp/omnibus_webgui/WASRepository/disk1/diskTag.inf  
/tmp/omnibus_webgui/JazzSMRepository/disk1/diskTag.inf  
/tmp/omnibus_webgui/repository.config
```

Note: The required packages have already been installed

Installation Packages	Status
IBM WebSphere Application Server	Installed
Version 8.5.5.15	Installed
IBM WebSphere SDK Java Technology Edition (Optional)	Installed
Version 7.0.9.30	Installed
Jazz for Service Management extension for IBM WebSphere 8.0	Installed
Version 1.1.0.2	Installed
Jazz for Service Management extension for IBM WebSphere 8.5	Installed
Version 1.1.2.1	Installed
IBM Dashboard Application Services Hub	Installed
Version 3.1.3.3	Installed
Reporting Services	Installed

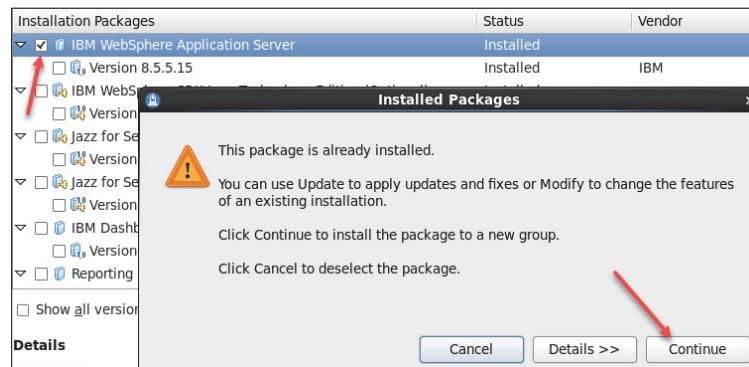
© Copyright IBM Corporation 2019

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (2)

When you start IBM Installation Manager, the application indicates that the components are already installed.

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (3)

3. Select IBM WebSphere Application Server, and click Continue



4. Select IBM WebSphere SDK, and click Continue
5. Select Jazz for Service Management extension, and click Continue
6. Select IBM Dashboard Application Services Hub, and click Continue

© Copyright IBM Corporation 2019

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (3)

You select the first component, and the application generates a warning message. You click **Continue** to ignore the warning. You repeat this process for the remaining components.

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (4)

7. Verify that you have selected the required packages, and click **Next**

Installation Packages	Status
IBM WebSphere Application Server Version 8.5.5.15	Installed
IBM WebSphere SDK Java Technology Edition (Optional) Version 7.0.9.30	Installed
Jazz for Service Management extension for IBM WebSphere 8.0 Version 1.1.0.2	Installed
Jazz for Service Management extension for IBM WebSphere 8.5 Version 1.1.2.1	Installed
IBM Dashboard Application Services Hub Version 3.1.3.3	Installed

8. Accept the license agreement and click **Next**

© Copyright IBM Corporation 2019

Installing WebSphere Application Server, Jazz for Service Management, and Dashboard Application Services Hub (4)

Verify that you selected the required components, and click **Next**. Accept the license agreement, and click **Next**.

Change installation directory (1)

9. Click the package name **IBM WebSphere Application Server V8.5_1** to select it

10. Change the Installation Directory to

/opt/IBM/WebSphere/AppServer_ncm

Package Group Name	Installation Directory
IBM WebSphere Application Server V8.5_1	/opt/IBM/WebSphere/AppServer_ncm
IBM WebSphere Application Server 8.5.5.15	
IBM WebSphere SDK Java Technology Edition (Optional)	
Jazz for Service Management extension for IBM WebS	
Core services in Jazz for Service Management_1	/home/netcool/IBM/JazzSM
IBM Dashboard Application Services Hub 3.1.3.3	

Package Group Name: IBM WebSphere Application Server V8.5_1
Installation Directory: /opt/IBM/WebSphere/AppServer_ncm

© Copyright IBM Corporation 2019

Change installation directory (1)

You must change the installation directory for WebSphere. Click the package name to select it, and change the installation directory name.

Change installation directory (2)

11. Click the package name **Core services in Jazz for Service Management_1** to select it

12. Change the Installation Directory to

/opt/IBM/JazzSM_ncm

Package Group Name	Installation Directory
IBM WebSphere Application Server V8.5_1	/opt/IBM/WebSphere/AppServer_ncm
IBM WebSphere Application Server 8.5.5.15	
IBM WebSphere SDK Java Technology Edition (Options)	
Jazz for Service Management extension for IBM Webs	
Core services in Jazz for Service Management_1	/opt/IBM/JazzSM_ncm
IBM Dashboard Application Services Hub 3.1.3.3	

Package Group Name: Core services in Jazz for Service Management_1
Installation Directory: /opt/IBM/JazzSM_ncm

13. Click **Next**

© Copyright IBM Corporation 2019

Change installation directory (2)

Change the name for the Jazz for Service Management installation directory. Click **Next**.

Complete the installation

14. Accept the default list of features
15. Enter the user name and password for the administrator
16. Change the default starting port number to 15310
Netcool Operations Insight uses 16310
17. Accept the default value for the context root
18. Review the installation summary and click **Install**
The installation runs approximately 40 minutes

© Copyright IBM Corporation 2019

Complete the installation

You click **Next** to continue through the installation options until you come to the port numbers. You must change the starting port number to something other than 16310. You can accept the default settings for the remaining options, and click **Install**. The installation runs approximately 40 minutes.

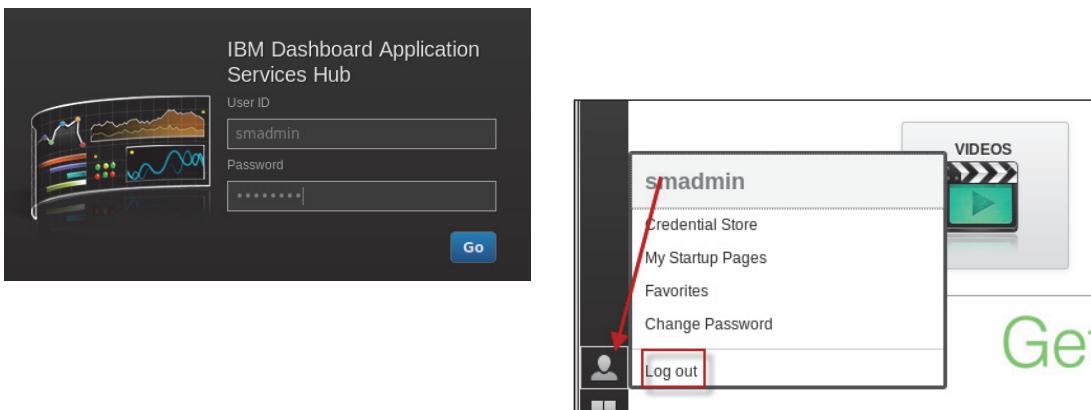
When the installation is complete, leave the option set to log in to Dashboard Application Services Hub, and click **Finish**.

Verifying access

A Firefox browser opens and connects to IBM Dashboard Application Services Hub:

<https://host1.csuite.edu:15311/ibm/console/logon.jsp>

Log in as **smadmin** with password **object00**



© Copyright IBM Corporation 2019

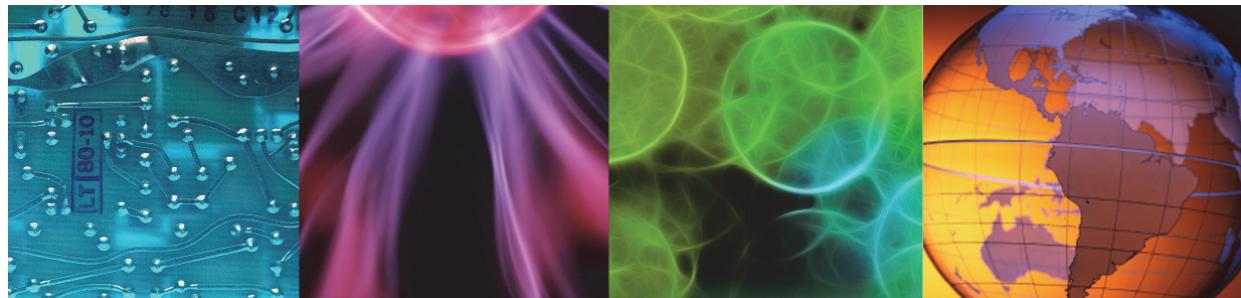
Verifying access

A Firefox browser opens, and you see the login screen for Dashboard Application Services Hub. Remember that this application is the Configuration Manager presentation server. The only discernible difference is the port number in the URL, which is 15311 in this example.



Lesson 4 Installing Netcool Configuration Manager

Lesson 4 Installing Netcool Configuration Manager



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to perform the following tasks:

- Install Configuration Manager core components
- Install Configuration Manager GUI components
- Install Configuration Manager reports

Installation

1. Expand the software

Note: You expanded the software installation file previously

2. Install with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
./IBMIM
```

* Assumes that IBM Installation Manager is installed by the **netcool** user

3. Define software repository

```
/tmp/tncm/ITNCM-Installer-6.4.2.8.zip
```

4. Select installation package

```
Netcool Configuration Manager Version 6.4.2.8
```

© Copyright IBM Corporation 2019

Installation

You install the core components with IBM Installation Manager.

Installation directory

5. Select the entry for **Netcool Configuration Manager**

6. Change the installation directory to:

/opt/IBM/ncm

7. Click **Next**

<input type="radio"/> Use the existing package group					
<input checked="" type="radio"/> Create a new package group					
<table border="1"><thead><tr><th>Package Group Name</th><th>Installation Directory</th></tr></thead><tbody><tr><td>Netcool Configuration Manager</td><td>/opt/IBM/ncm</td></tr></tbody></table>		Package Group Name	Installation Directory	Netcool Configuration Manager	/opt/IBM/ncm
Package Group Name	Installation Directory				
Netcool Configuration Manager	/opt/IBM/ncm				
Package Group Name: Netcool Configuration Manager					
Installation Directory: /opt/IBM/ncm					

© Copyright IBM Corporation 2019

Installation directory

Change the installation directory.

Features

8. Accept the default list of features
9. Click **Next**

Note: The Reports feature is not selected

You install the reports later

© Copyright IBM Corporation 2019

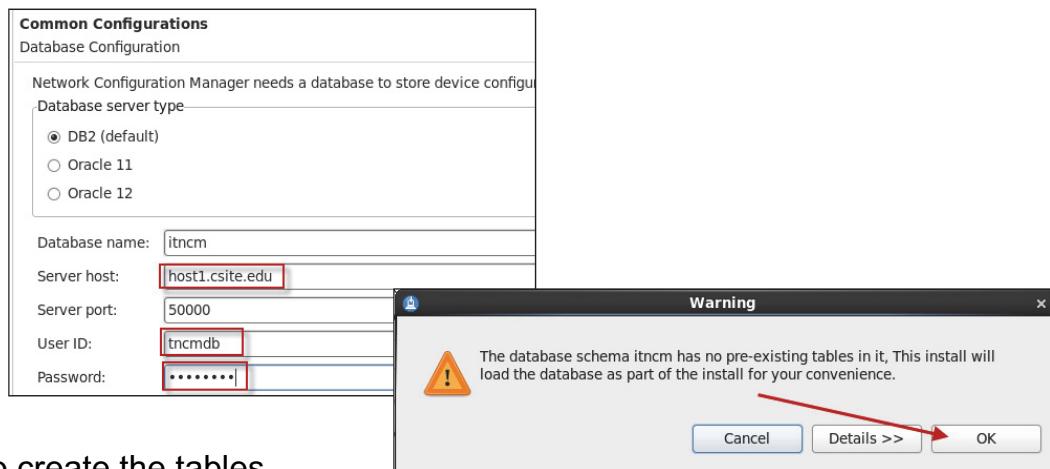
Features

Accept the default list of features. You see an option for reports. Do not select that feature. You install the reports in a subsequent step.

Database Configuration

10. Enter the access information for the database

11. Click **Next**



12. Click **OK** to create the tables

© Copyright IBM Corporation 2019

Database Configuration

In a previous unit, you created the Configuration Manager database. When you created the database, you did not create any table structure. This installation step creates the table structure.

Server Configuration (1)

13. Enter the details for FTP access

You created the FTP user ID in a previous exercise

Common Configurations for Network Configuration Manager	
ITNCM Server Configuration	
Root Realm	ITNCM
FTP Server	host1.csite.edu
FTP User Account	tncm_ftp
FTP user Password	*****
FTP User Password Confirmation	*****
FTP User Account Directory	/home/tncm_ftp
SMTP Server	localhost

Scroll down in the pane

© Copyright IBM Corporation 2019

Server Configuration (1)

The Server Configuration page is long. This slide highlights part of the configuration options.

Enter the information for the FTP user. You created an operating system user in a previous exercise.

Server Configuration (2)

14. Select the option for an integrated installation
15. Configure the access details for Network Manager

Is This the main IDT Server
 Yes
 No

Select the type of install you require.
 Activate Configuration-Core
 Activate Compliance-Core

Is this an integrated NCM - NM Install?

The NM Hostname: host1.csuite.edu

The port to connect to: 16311

The NM User: itnmadmin

The NM User Password:
.....
.....

NM User Password Confirmation: ITNCM/NOI_AGG_P

16. Click Next

© Copyright IBM Corporation 2019

Server Configuration (2)

Make sure that you select the option for an integrated Network Manager installation. When you select this option, the installation process installs and configures the process that accesses the Network Manager topology database to retrieve device information. This information is used by Configuration Manager to import the device configuration files for all devices that Network Manager discovers.



Note: You can configure the integration manually after installation if necessary.

NCM JazzSM Details

17. Change the value for the installation directory
18. Enter the administrator user name and password

Common Configurations
NCM JazzSM Details

Network Configuration Manager needs to deploy a Web Application into the IBM Dashboard Application Services Hub. Please confirm the install location of the Jazz for Service Management to use.

Installation Directory Details

JazzSM user credentials

User name	smadmin
Password	*****
Password Confirmation	*****

19. Click **Next**

© Copyright IBM Corporation 2019

NCM JazzSM Details

As mentioned previously, you use separate copies of Jazz for Service Management, WebSphere, and Dashboard Application Services Hub. The installation process refers to one copy as NCM, and the other copy as NM. The NCM copy is the Configuration Manager presentation server. The NM copy is what you use for Netcool Operations Insight. Pay careful attention to the references during the installation. It is easy to confuse the choices.

The screen capture that is shown here is looking for the attributes for the Configuration Manager presentation server. Make sure that you change the installation directory name.

The installation process modifies the configuration of Jazz for Service Management, WebSphere, and Dashboard Application Services Hub. The process adds the components that comprise the presentation server.

Installation complete

Review the installation summary, and click **Install**

The installation takes about 25 minutes

 The packages are installed. [View Log File](#)

The following package was installed:

▽  Netcool Configuration Manager
 Netcool Configuration Manager 6.4.2.8

© Copyright IBM Corporation 2019

Installation complete

Installing GUI components

1. Expand the software

Note: You expanded the software installation file previously

2. Install with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
.IBMIM
```

* Assumes that IBM Installation Manager is installed by the **netcool** user

3. Define software repository

Note: You defined the repository previously

4. Select installation package

```
IBM Dashboard Applications for ITNCM Version 6.4.2.8
```

© Copyright IBM Corporation 2019

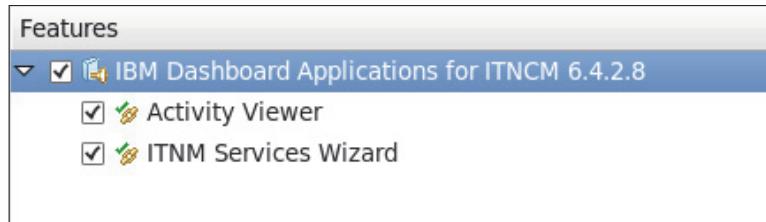
Installing GUI components

You use IBM Installation Manager to install the Configuration Manager GUI components. You use the same installation software, and the same software repository that you used when you installed the core components.

This installation process adds Configuration Manager objects to the copy of WebSphere that is used by Netcool Operations Insight.

Features

5. Accept the default package group, and click **Next**
6. Accept the default list of features, and click **Next**



© Copyright IBM Corporation 2019

Features

Accept the default list of features.

Jazz for Service Management

7. Enter the administrator user name and password. Click **Next**

Common Configurations
Jazz for Service Management properties

WebSphere user credentials are required to perform this operation. Please enter the username and password details used to Administer the IBM Dashboard Application Service Hub.

User name

Password

The user must be a Jazz for Service Management administrator

© Copyright IBM Corporation 2019

Jazz for Service Management

The reference on this page is to the copy of Jazz for Service Management that Netcool Operations Insight uses. In the class exercise, the administrator user and password are the same for both copies of WebSphere. In a production environment, you typically use different values for different users.

Administrator Credentials

8. Enter the user name and password

Click **Next**

Common Configurations	
Administrator Credentials	
To change filters and views, enter the credentials of an administrative user (for example, itnmadmin). The user must have the ncw_admin role and privileges to run the Netcool WebGUI waapi command. Ensure that the user authentication repository is accessible from this server before continuing.	
User ID:	<input type="text" value="itnmadmin"/>
Password:	<input type="password" value="*****"/>

The user must be capable of running Web GUI Administrative API (WAAPI)

© Copyright IBM Corporation 2019

Administrator Credentials

Again, the reference on this page is to the copy of Jazz for Service Management that Netcool Operations Insight uses. You must enter a user name that can run the Web GUI API utility. The user must have the *ncw_admin* role.

Database Configuration

9. Enter the access information for the database

Click **Next**

Common Configurations
ITNCM Database Server

Connectivity to ITNCM Database

Database server type

DB2 (default)
 Oracle 11
 Oracle 12

ITNCM database schema

ITNCM database hostname

ITNCM database port

ITNCM database username

ITNCM database password

© Copyright IBM Corporation 2019

Database Configuration

The installation process references several database uses. Configuration Manager uses a database, and Common Reporting uses a database. In the class exercise, you use a single copy of DB2 for all database uses. In a production environment, that might not be the case.

The reference on this page is for the Configuration Manager database.

ITNCM Presentation Server

10. Configure the access details for the presentation server

Click **Next**

Common Configurations
ITNCM Presentation Server

Connectivity to ITNCM Presentation server

ITNCM presentation server scheme 

ITNCM presentation server hostname 

ITNCM presentation server web port 

Tick this box to skip full validation if the presentation server is currently unavailable



© Copyright IBM Corporation 2019

ITNCM Presentation Server

The information on this page refers to the Configuration Manager presentation server. The installation process uses this information to configure several Dashboard Application Services Hub tools.

ITNCM Reporting Server

11. Configure the access details for the reporting server

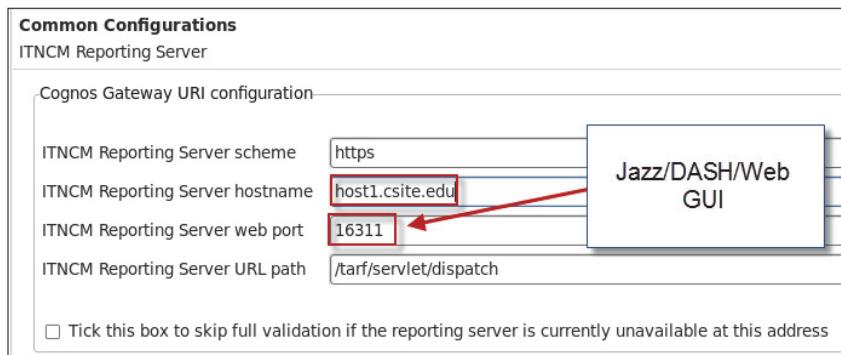
Click **Next**

Common Configurations
ITNCM Reporting Server

Cognos Gateway URI configuration-

ITNCM Reporting Server scheme	https
ITNCM Reporting Server hostname	host1.csuite.edu
ITNCM Reporting Server web port	16311
ITNCM Reporting Server URL path	/tarf/servlet/dispatch

Tick this box to skip full validation if the reporting server is currently unavailable at this address



© Copyright IBM Corporation 2019

ITNCM Reporting Server

The installation process needs the access information for the server that hosts Common Reporting. In the student exercise, Common reporting is installed in the copy of Jazz for Service Management that Netcool Operations Insight uses. In a production environment, you might use a dedicated copy of Jazz for Service Management just for Common Reporting.

The installation process uses this information to configure several Dashboard Application Services Hub tools.

Installation complete

The installation runs for approximately 20 minutes

 The packages are installed. [View Log File](#)

The following package was installed:

▽  IBM Netcool GUI Components
 IBM Dashboard Applications for ITNCM 6.4.2.8

© Copyright IBM Corporation 2019

Installation complete

Installing Common Reporting reports

1. Expand the software

Note: You expanded the software installation file previously

2. Install with IBM Installation Manager

```
cd /home/netcool/InstallationManager/eclipse  
.IBMIM
```

* Assumes that IBM Installation Manager is installed by the **netcool** user

3. Define software repository

Note: You defined the repository previously

4. Select the **Modify** option

5. Select installation package

Netcool Configuration Manager

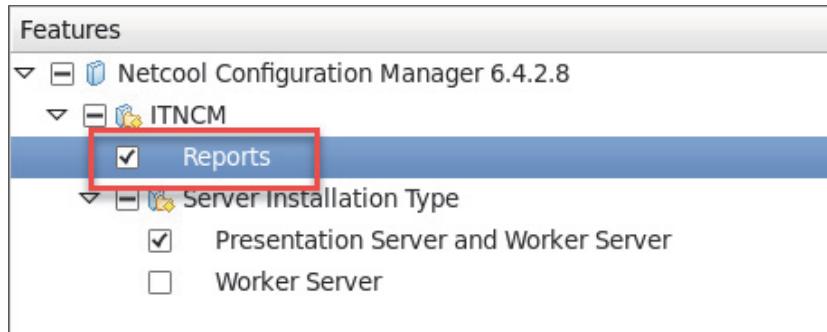
© Copyright IBM Corporation 2019

Installing Common Reporting reports

In the final installation step, you install the Common Reporting report package. The report package is a feature of the core components package. Because you installed the core component package previously, you must *modify* the installation to add the reports feature.

Features

6. Accept the default package group, and click **Next**
7. Select **Reports**, and click **Next**



Features

Make sure that you select the **Reports** feature.

Database Configuration

8. Enter the access information for the database

Click **Next**

Common Configurations

Database Configuration

Network Configuration Manager needs a database to store device configuration type of database and the connection details.

Database server type

DB2 (default)
 Oracle 11
 Oracle 12

Database name:

Server host:

Server port:

User ID:

Password:

© Copyright IBM Corporation 2019

Database Configuration

Configuration Manager reports reference data that is stored in the Configuration Manager database. The installation process requires the Configuration Manager database access credentials to define a Common Reporting data source.

Tivoli Common Reporting properties

9. Select the option to install reports
10. Enter the user name and password and click **Next**

The screenshot shows the 'Common Configurations' tab of the TCR properties window. It includes the following sections:

- Network Configuration Manager needs to deploy a Web Application into the IBM Dashboard location of the Jazz for Service Management instance you want to use.**
- Install the NM-NCM Integrated Reports.**:
An input field with two radio button options: "No (default)" and "Yes". The "Yes" option is selected and highlighted with a red box.
- Installation Directory Details**:
A text input field containing the value "/opt/IBM/JazzSM".
- JazzSM user credentials**:
Three input fields:
 - User name: smadmin
 - Password: [REDACTED]
 - Password Confirmation: [REDACTED]The password and confirmation fields are highlighted with a red box.

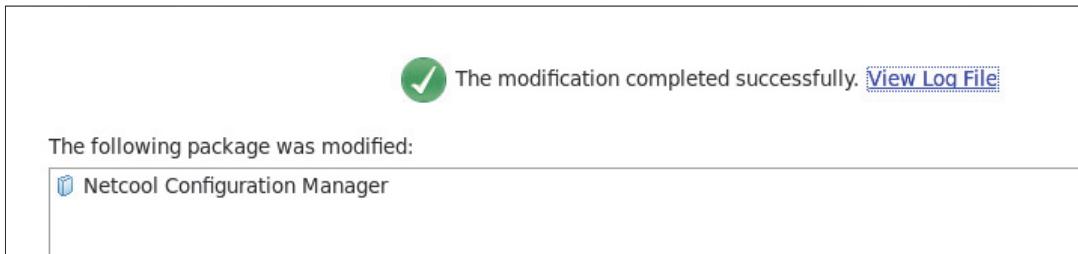
At the bottom of the window, there is a copyright notice: © Copyright IBM Corporation 2019

TCR properties

Make sure that you select the option to install the integrated reports.

Installation complete

The installation runs for approximately 10 minutes



© Copyright IBM Corporation 2019

Installation complete

Starting the server

\$INSTALL-DIR/bin/itncm.sh start

```
cd /opt/IBM/ncm/bin
./itncm.sh start
IBM Tivoli Netcool Configuration Manager
-----
Starting Worker Server
Worker Server = RUNNING
Starting Compliance Server
Compliance Server = RUNNING
Starting GUI Server
GUI Server = RUNNING
```

© Copyright IBM Corporation 2019

Starting the server

You start the application with the following commands:

```
cd /opt/IBM/ncm/bin
./itncm.sh start
```

In the lab exercise, all Configuration Manager components are installed on a single server. This script starts all three components.

Stopping the server

\$INSTALL-DIR/bin/itncm.sh stop

Stopping presentation server requires super user credentials

```
/opt/IBM/ncm/bin/itncm.sh stop¶
¶
IBM Tivoli Netcool Configuration Manager¶
-----¶
¶
Stopping GUI Server¶
¶
Please enter the Intelliden Super User and password if prompted below:¶
```



© Copyright IBM Corporation 2019

Stopping the server

You stop the application with the following commands:

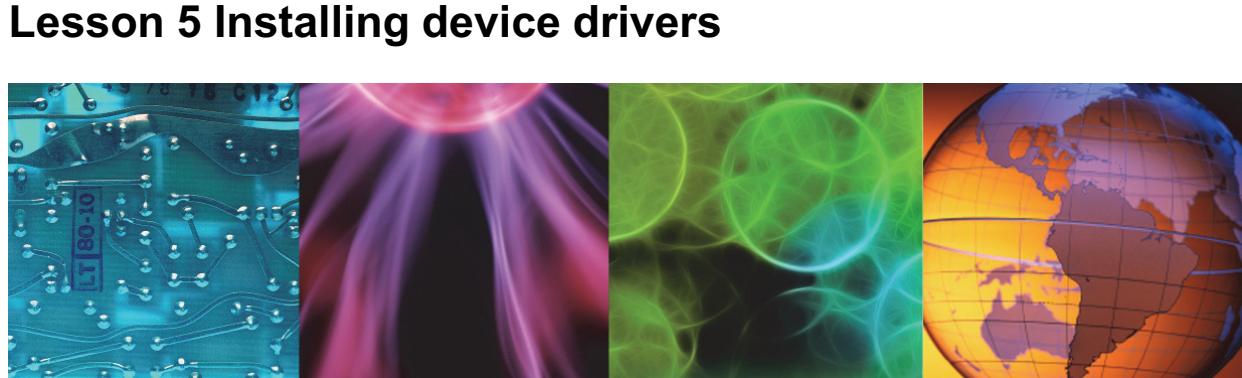
```
cd /opt/IBM/ncm/bin
./itncm.sh start
```

You must enter the Configuration Manager super user name and password to stop the presentation server. The super user name is **Intelliden**.

In the class exercise, all Configuration Manager components are installed on a single server. This script stops all three components.



Lesson 5 Installing Device Drivers



© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to perform the following tasks:

- Install the Standard device drivers
- Install the SmartModel device drivers
- Install the Auto-discovery drivers

Preparing for driver installation

Have 8 GB of free space for installation

Download the driver installation files:

IBM Netcool Configuration Manager Drivers 19 SmartModel Device v6.4 Full Installer Multiplatform English (CN15XEN)

IBM Netcool Configuration Manager Drivers 19 Standard Device Full Installer v6.4 Multiplatform English (CN15TEN)

Autodiscovery Driver Multiplatform English (CN15UEN)

Expand the archives

Install as same user who installed base software

Stop Configuration Manager components before you install the drivers

© Copyright IBM Corporation 2019

Preparing for driver installation

The driver files are distributed in separate installation files. The installation process requires a minimum of 8 GB of free disk space. You must stop the Configuration Manager components before you install the drivers.

Installing the standard drivers

1. Expand the Standard drivers installation file

```
unzip NCM-6.4.2-Drivers19-Standard.zip
```

2. Change to the installation location

```
cd NCM-6.4.2-Drivers19-Standard
```

3. Change file permissions to allow execution

```
chmod +x ITNCMDrivers.bin
```

4. Run the installation utility

```
./ITNCMDrivers.bin
```

© Copyright IBM Corporation 2019

Installing the standard drivers

The driver software does not use IBM Installation Manager.

Installing the Smart Model drivers

1. Expand the Smart Model drivers installation file

```
unzip NCM-6.4.2-Drivers19-SmartModel.zip
```

2. Change to the installation location

```
cd NCM-6.4.2-Drivers19-SmartModel/Disk1/InstData
```

3. Run the installation utility

```
chmod +x ITNCMDrivers.bin
```

```
./ITNCMDrivers.bin
```

4. Start the components

```
/opt/IBM/ncm/bin/itncm.sh start
```

5. Change SmartModel drivers from Standard to SmartModel mode

```
cd /opt/IBM/ncm/drivers/bin
```

```
./SmartModelUpgrade.sh -all
```

© Copyright IBM Corporation 2019

Installing the Smart Model drivers

You can install SmartModel driver packages by using the full installer or by using individual driver installers, depending on the installer that you download. You can also use SmartModel driver packages to upgrade standard drivers to SmartModel drivers.

Installing Autodiscovery

1. Stop the components

```
/opt/IBM/ncm/bin/itncm.sh stop
```

2. Expand the installation file

```
tar -xvf ITNCM_Autodiscovery.tar
```

3. Change file permissions to allow execution

```
chmod +x autodiscovery-aa85.bin
```

4. Run the installation utility

```
./autodiscovery-aa85.bin
```

5. Start the components

```
/opt/IBM/ncm/bin/itncm.sh start
```

© Copyright IBM Corporation 2019

Installing Autodiscovery

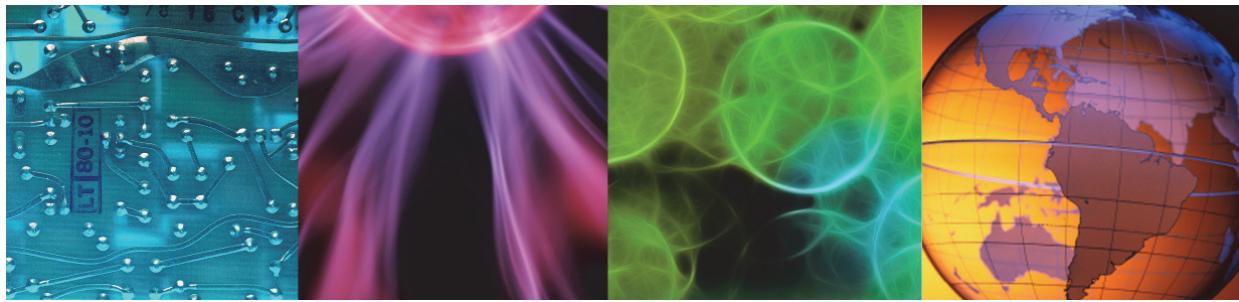
The Netcool Configuration Manager auto-discovery component determines the network resource Vendor, Type, Model, and Operating System (VTMOS), by sending a series of queries with TELNET, SNMP, or SSH to each network resource.

You must install the most current drivers before installing auto-discovery.

Lesson 6 Post installation configuration



Lesson 6 Post-installation configuration



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to perform the following tasks:

- Configure the Firefox browser to open the Java Webstart application
- Configure SNMP trap destination
- Update the Work Distribution resource
- Add a realm
- Configure device passwords

Configuring Java Webstart (1)

1. Open a Firefox browser
2. Connect to the following URL:
`http://host1.csuite.edu:15310/security/login.jsp`
3. Log in as **administrator**
4. Select **ITNCM Webstart GUI**

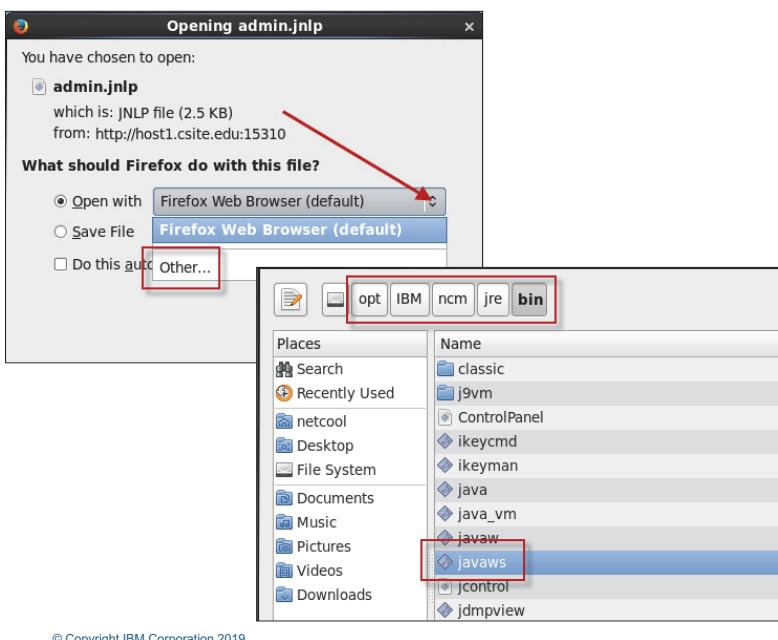


Configuring Java Webstart (1)

The Configuration Manager client is a Java Webstart application. You must configure the Firefox browser to open the Java Webstart file with the correct application.

Configuring Java Webstart (2)

1. Click the arrow and select Other



2. Navigate to **/opt/IBM/ncm/jre/bin**, and select **javaws**

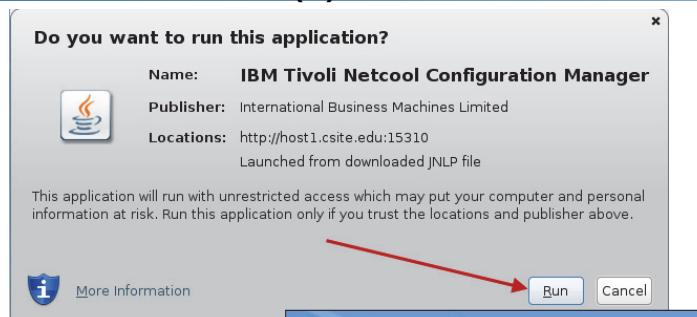
Configuring Java Webstart (2)

The first time that you attempt to open the Configuration Manager client, the Firefox browser asks for the location of a compatible application. You select the copy of Java Webstart that is bundled with Configuration Manager.

You complete this step only the first time you access the application.

Configuring Java Webstart (3)

1. Click Run



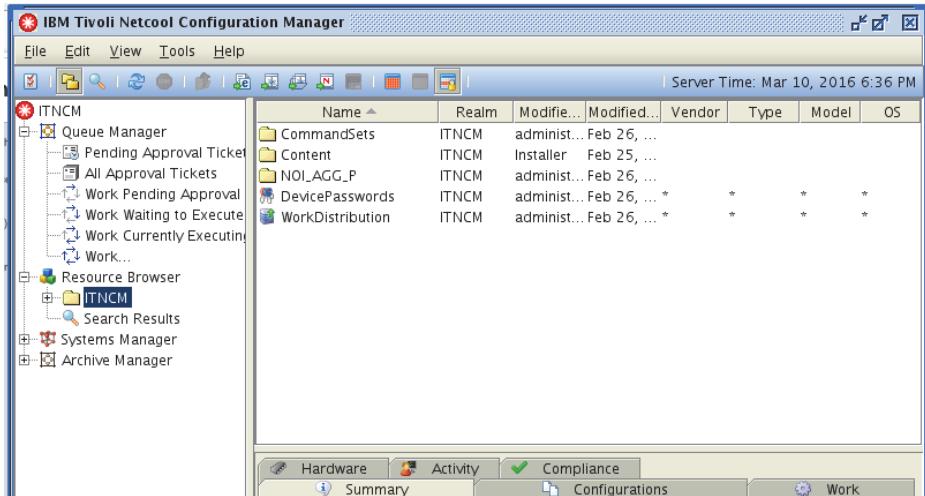
2. Log in as administrator



Configuring Java Webstart (3)

The Firefox browser presents a security challenge. You must click **Run** to proceed.

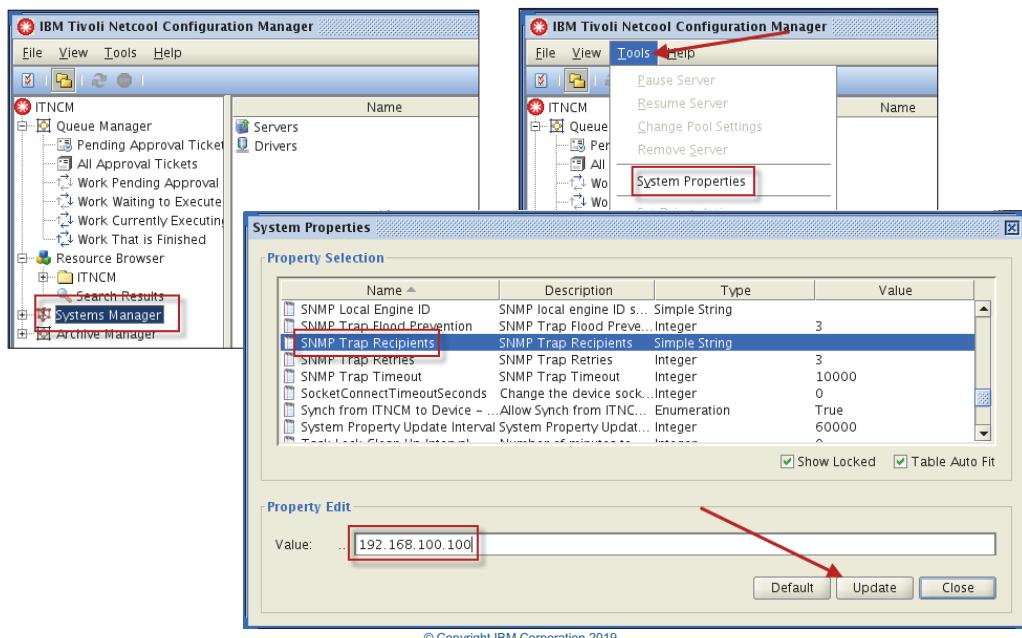
Configuring Java Webstart (4)



Configuring Java Webstart (4)

The Configuration Manager client opens.

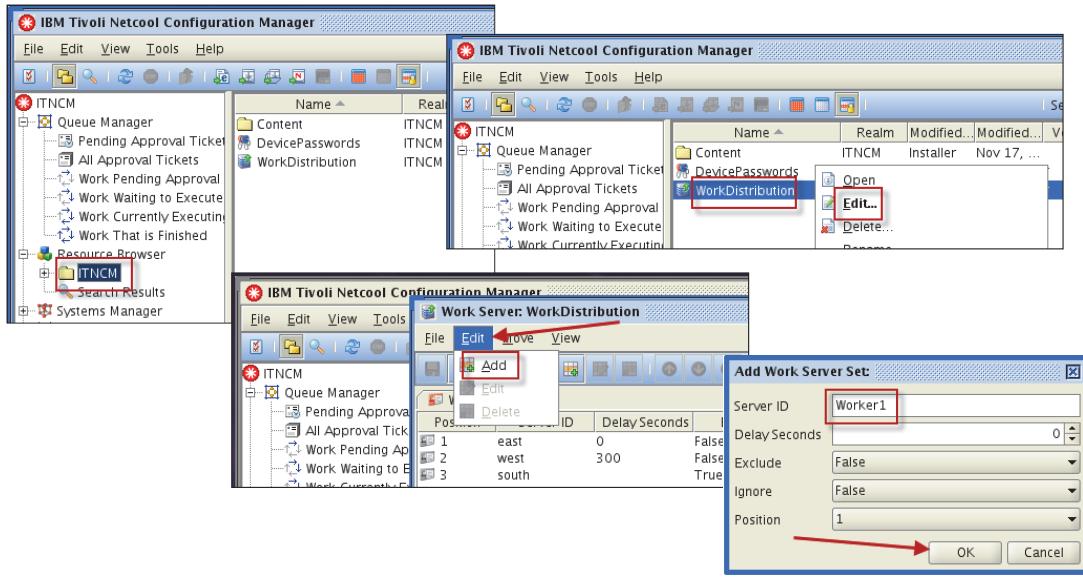
Configuring SNMP trap destination



Configuring SNMP trap destination

You configure a trap destination with the Configuration Manager client. Under Resource Browser, click **Systems Manager** to select it. Click **Tools**, and select System Properties. Scroll down in the list, and locate SNMP Trap Recipients. Click the entry, and enter the IP address as the value. Click **Update** to save the change.

Updating Work Distribution resource



© Copyright IBM Corporation 2019

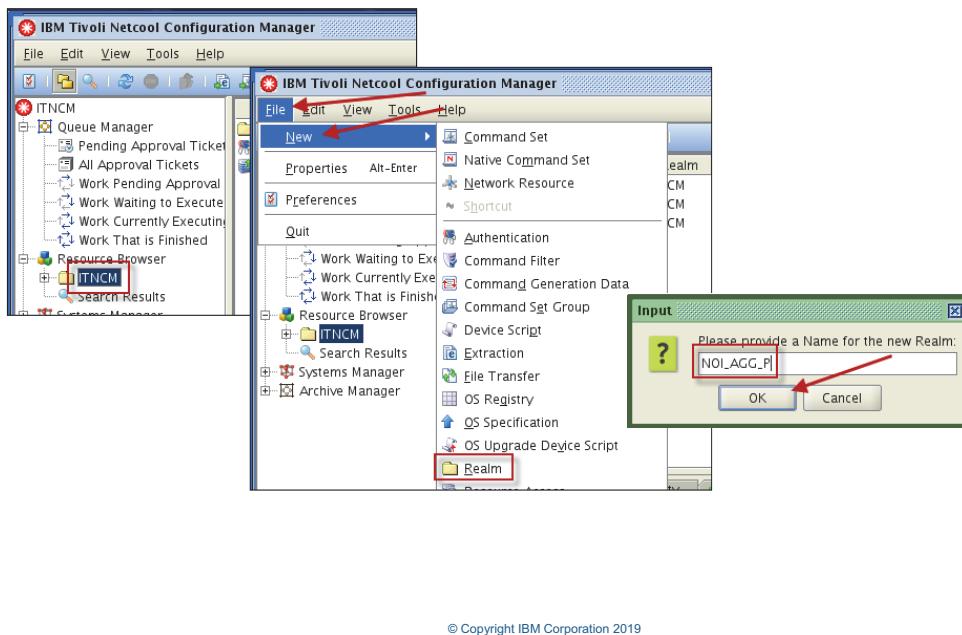
Updating Work Distribution Resource

You configure a Work Distribution Resource with the Configuration Manager client. Under Resource Browser, click **ITNCM** to select it. Click **WorkDistribution**, right-click, and select **Edit**. Click **Edit**, and select **Add**. Enter Worker1 for the Server ID, and click **OK**.



Note: You do not use any of the existing entries. You can delete the existing entries if you want.

Adding a realm

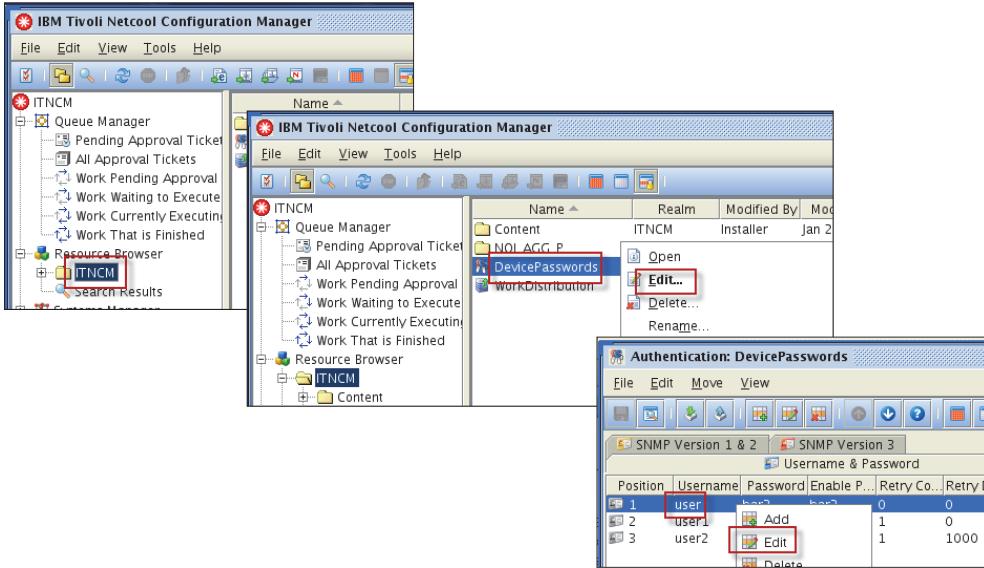


Adding a realm

When you installed the core components, you selected an option for an integrated Network Manager configuration. You also provided a realm name. Configuration Manager imports devices from Network Manager and saves the device information under that realm name. You must create that realm entry.

You configure a realm with the Configuration Manager client. Under Resource Browser, click **ITNCM** to select it. **Click File > New > Realm**. Enter NOI_AGG_P for name, and click **OK**.

Configuring device passwords (1)



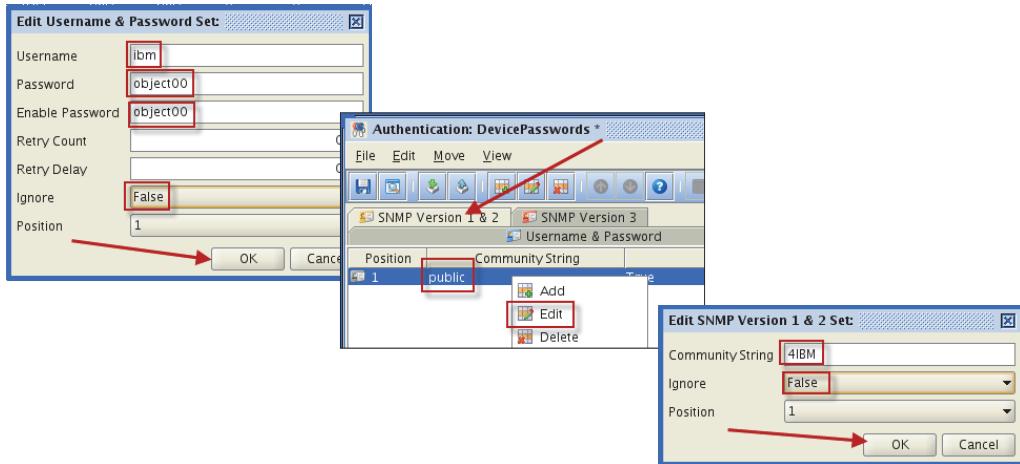
© Copyright IBM Corporation 2019

Configuring device passwords (1)

You configure device passwords with the Configuration Manager client. Under Resource Browser, click **ITNCM** to select it. Click **DevicePasswords**, right-click, and select **Edit**. Click the first entry to select it, right-click, and select **Edit**.

Note: These steps describe how you modify an existing entry. You can add a new entry instead.

Configuring device passwords (2)



© Copyright IBM Corporation 2019

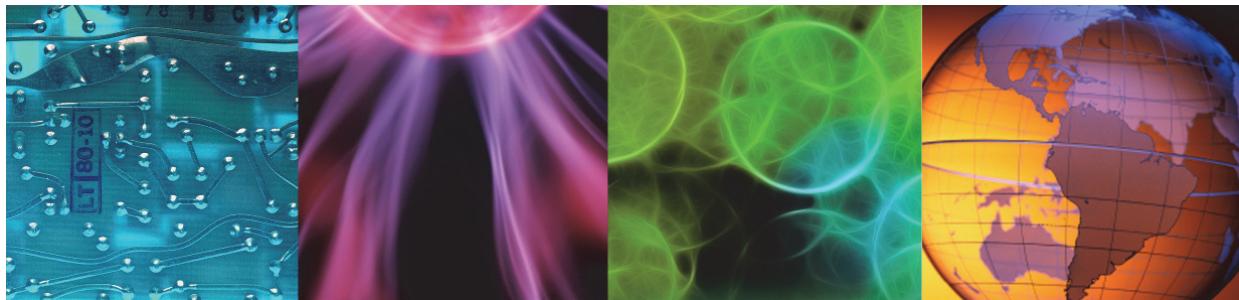
Configuring device passwords (2)

Enter the device user name, password, and enable password. Click the **SNMP** tab, and enter an SNMP community string. Click **OK** to save the changes.

Lesson 7 Configuring integration with Network Manager



Lesson 7 Configuring integration with Network Manager



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to configure the integration with Network Manager.

Integration overview

1. Create Configuration Manager groups and users in WebSphere
2. Add existing users to Configuration Manager groups
3. Assign roles in Dashboard Application Services Hub
4. Configure presentation server to use LDAP
5. Configure presentation server to use single sign-on (SSO)
6. Configure Configuration Manager access rights
7. Configure integration with Netcool/OMNIbus
8. Configure device synchronization

© Copyright IBM Corporation 2019

Integration overview

The integration with Network Manager encompasses several applications. The integration requires that single sign-on is enabled between the Configuration Manager presentation server, and Dashboard Application Services Hub. To enable single sign-on, you must first create Configuration Manager users and groups in the common user repository. In the student exercise, the common repository is LDAP. Next, you configure the Configuration Manager presentation server to use the LDAP repository. Next, you configure Configuration Manager access rights. Next, you configure the Netcool/OMNIbus SNMP probe to understand Configuration Manager traps. Finally, you configure device synchronization.

Configuring groups and users in WebSphere

- Integration with Netcool Operations Insight requires single sign-on
- Single sign-on requires a common user repository
 - The ObjectServer is an option
 - LDAP is a better option for Netcool Operations Insight
- Add Configuration Manager groups to WebSphere
 - IntellidenAdminUser
 - IntellidenUser
- Add Configuration Manager users to WebSphere
 - Intelliden
 - administrator
 - operator (optional)
 - observer (optional)

© Copyright IBM Corporation 2019

Configuring groups and users in WebSphere

Access to Configuration Manager is controlled with two group names. Any user that belongs to the IntellidenAdminUser group is granted access to Configuration Manager administration features. Any user that belongs to the IntellidenUser group is granted access to normal user features, including the use of the Java Webstart clients.

You must manually create the two groups in the common user repository. You must also create the Configuration Manager default users, and assign them to the correct groups.

Adding existing users to Configuration Manager groups

- Netcool Operations Insight has a number of users
 - **itnmadmin**
 - **itnmuser**
 - **ncoadmin**
 - **ncouser**
- Add those users to Configuration Manager groups (optional)
 - IntellidenAdminUser
 - itnmadmin
 - ncoadmin
 - IntellidenUser
 - itnmadmin
 - itnmuser
 - ncoadmin
 - ncouser

© Copyright IBM Corporation 2019

Adding existing users to Configuration Manager groups

When you deploy Configuration Manager with Netcool Operations Insight, you must configure a number of existing users for access to Configuration Manager features. You make this configuration to facilitate product integration. When a Netcool/OMNIbus user, like **ncoadmin**, accesses Dashboard Application Services Hub, the user can run Configuration Manager tools. The user must be a valid Configuration Manager for those tools to function correctly.

To provide the necessary access, you modify the Configuration Manager groups, and add the existing users as members.

Assigning Dashboard Application Services Hub roles

- Access to Configuration Manager features in Dashboard Application Services Hub requires specific roles
- The installation of Configuration Manager GUI components added the roles to Dashboard Application Services Hub
- Add the required roles to each Configuration Manager group
 - IntellidenAdminUser
 - IntellidenUser

© Copyright IBM Corporation 2019

Assigning Dashboard Application Services Hub roles

The Configuration Manager groups control access to Configuration Manager features. However, roles control access to Dashboard Application Services Hub features, like pages, tools, and menus. You must manually add the required roles to the respective Configuration Manager groups.

Configuring the presentation server to use LDAP

The steps to configure user authentication against an LDAP directory are as follows:

- Add the LDAP directory to the Virtual Member Manager realm
- Configure the Virtual Member Manager realm to write new users to the LDAP directory
- Remove the internal repository from the Virtual Member Manager realm

The following information is required for the configuration:

- Host name and port number for the LDAP directory
- Type and version of LDAP directory, for example, IBM Security Directory Server V6.2
- The user ID and password that are used to bind to the LDAP server
- Subtree of the LDAP directory that is used for authenticating users

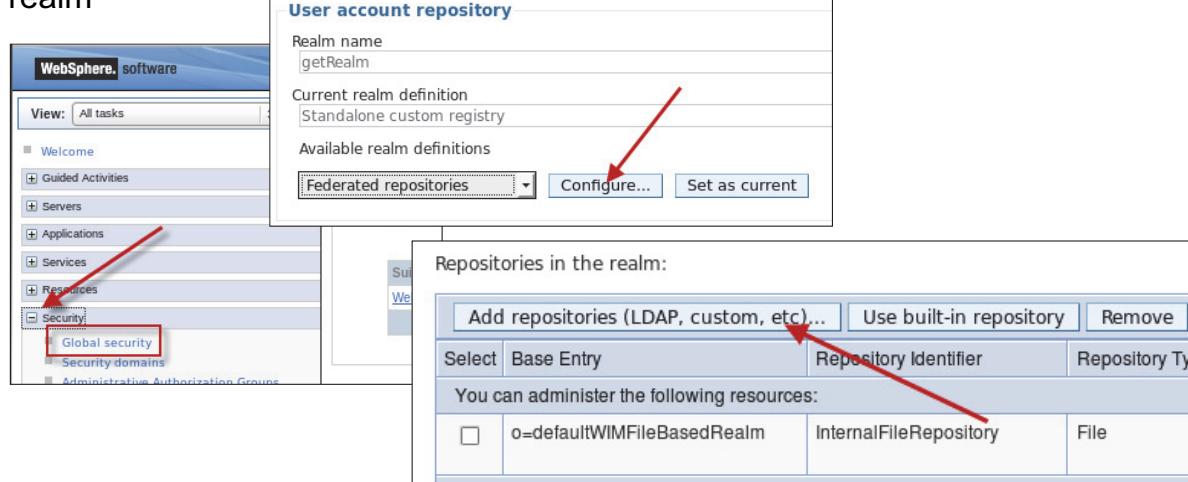
© Copyright IBM Corporation 2019

Configuring the presentation server to use LDAP

After you create the users and groups, you configure the presentation server to use LDAP.

Adding LDAP to the Virtual Member Manager realm: Step 1

The WebSphere Administrative Console is used to add the LDAP definition to the realm



Adding LDAP to the Virtual Member Manager realm: Step 1

In a previous exercise, you installed Netcool/OMNibus Web GUI. After you installed Web GUI, you configured WebSphere to use LDAP as a federated user repository. You use the same procedure to configure the presentation server to use LDAP.

Note: By default, the presentation server uses an internal file-based repository. You remove that repository in a subsequent step.

Adding LDAP to the Virtual Member Manager realm: Step 2

Configure the access criteria for the LDAP server

The screenshot shows two configuration panels side-by-side.

General Properties:

- * Repository: none defined → New Repository... (highlighted with a red arrow)
- * Unique distinguished name: TIVIDS (highlighted with a red box)
- Repository adapter class name: com.ibm.ws.wim.adapter.ldap.LdapAdapter

LDAP server:

- * Directory type: IBM Tivoli Directory Server
- * Primary host name: host1.csite.edu
- Port: 389
- Failover server used when primary is not available: (empty)

Security:

- Bind distinguished name: cn=root (highlighted with a red box)
- Bind password: (redacted)
- Federated repository properties for login uid (highlighted with a red box)
- LDAP attribute for Kerberos principal name (highlighted with a red box)

© Copyright IBM Corporation 2019

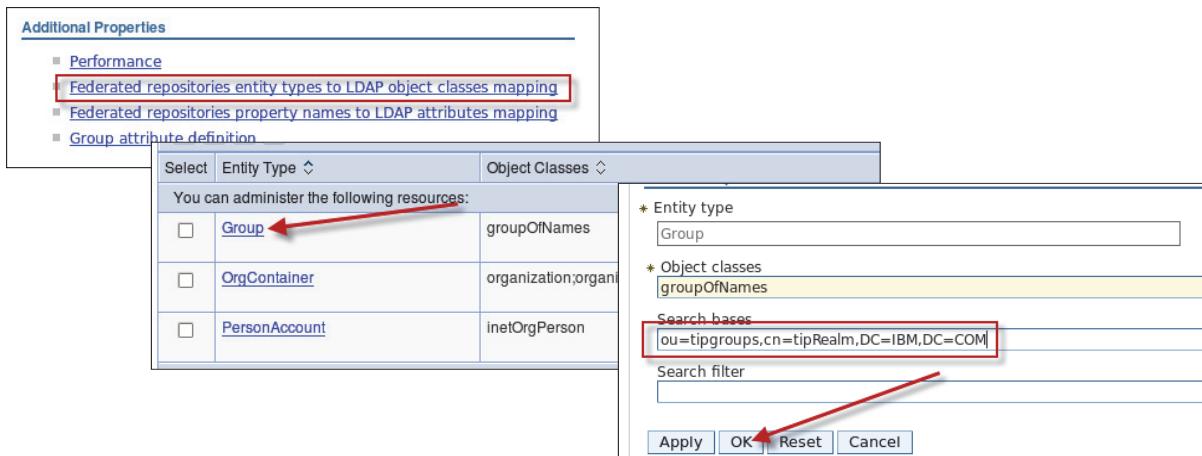
Adding LDAP to the Virtual Member Manager realm: Step 2

You create a new LDAP repository entry. In that entry, you specify the access criteria for the LDAP server.

Adding LDAP to the Virtual Member Manager realm: Step 3

Configure the LDAP search criteria

- Limits the LDAP data to a specific subtree within the directory
- Defined for Group, OrgContainer, and PersonAccount



© Copyright IBM Corporation 2019

Adding LDAP to the Virtual Member Manager realm: Step 3

In the next step, you configure how the LDAP object names are mapped to each corresponding Virtual Member Manager resource type. You configure each resource type to specify search criteria. The search criteria are used to locate values for each of the object classes. These definitions essentially define the LDAP subtree where the user information is located.

Adding LDAP to the Virtual Member Manager realm: Step 4

Configure the Virtual Member Manager to write new users to LDAP

Defined for Group, OrgContainer, and PersonAccount

The screenshot shows the 'Repositories in the realm' configuration page. In the 'You can administer the following resources:' section, 'Group' is selected. A configuration dialog is open over the page, showing the 'Entity type' set to 'Group', 'Base entry for the default parent' set to 'ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM', and 'Relative Distinguished Name properties' set to 'cn'. The 'OK' button in the dialog is highlighted with a red arrow.

© Copyright IBM Corporation 2019

Adding LDAP to the Virtual Member Manager realm: Step 4

In the next step, you configure the presentation server to write new users and groups to the LDAP directory. This configuration process is similar to the previous steps. You define which LDAP object classes are modified when you create a new user or group.

Adding LDAP to the Virtual Member Manager realm: Step 5

Remove the internal repository

The screenshot shows the 'Global security > Federated repositories > Supported entity types' page. The page title is 'Global security > Federated repositories > Supported entity types'. Below the title, a sub-header says 'Use this page to configure entity types that are supported by the member repositories.' There is a 'Preferences' link and a toolbar with icons for add, edit, and delete. A table titled 'Repositories in the realm:' lists resources. The first row has columns for 'Select', 'Base Entry', 'Repository Identifier', and 'Repository Type'. The second row contains 'dc=ibm,dc=com' (unchecked), 'TIVIDS', 'LDAP:IDS', and 'File'. The third row contains 'o=defaultWIMFileBasedRealm' (checked), 'InternalFileRepository', and 'File'. A red box highlights the checked checkbox in the third row. A red arrow points from the breadcrumb 'Federated repositories' to the 'Remove' button in the top right of the table. The bottom of the page has a copyright notice: '© Copyright IBM Corporation 2019'.

Adding LDAP to the Virtual Member Manager realm: Step 5

In the last step, you remove the existing internal file-based repository.

Adding LDAP to the Virtual Member Manager realm: step 6

LDAP users known to the presentation server

- All users within the defined LDAP search subtree appear automatically
- You must add roles to configure access to Dashboard Application Services Hub features

Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	Intelliden	TNCM Super	User		uid=Intelliden,ou=tipusers,cn=tipRealm,DC=IBM,DC=IB
<input type="checkbox"/>	abraman	Ariana Braman	Braman	abraman@ibm.com	cn=Ariana Braman,ou=tipusers,cn=tipRealm,DC=IBM,
<input type="checkbox"/>	administrator	TNCM Admin	User		uid=administrator,ou=tipusers,cn=tipRealm,DC=IBM,D
<input type="checkbox"/>	adurling	Adeline Durling	Durling	adurling@ibm.com	cn=Adeline Durling,ou=tipusers,cn=tipRealm,DC=IBM,
<input type="checkbox"/>	bwinebarger	Bart Winebarger	Winebarger	bwinebarger@ibm.com	cn=Bart Winebarger,ou=tipusers,cn=tipRealm,DC=IBM
<input type="checkbox"/>	dselan	Dick Selan	Selan	dselan@ibm.com	cn=Dick Selan,ou=tipusers,cn=tipRealm,DC=IBM,DC=IB
<input type="checkbox"/>	eange	Earline Ange	Ange	eange@ibm.com	cn=Earline Ange,ou=tipusers,cn=tipRealm,DC=IBM,D
<input type="checkbox"/>	elotempio	Emelda Lotempio	Lotempio	elotempio@ibm.com	cn=Emelda Lotempio,ou=tipusers,cn=tipRealm,DC=IB
<input type="checkbox"/>	ezegarelli	Else Zegarelli	Zegarelli	ezegarelli@ibm.com	cn=Else Zegarelli,ou=tipusers,cn=tipRealm,DC=IBM,D

© Copyright IBM Corporation 2019

Adding LDAP to the Virtual Member Manager realm: step 6

After you complete the required configuration steps, you must restart the Configuration Manager components. After you restart the components, the presentation server has access to LDAP, and is aware of all users and groups.

Configuring the presentation server for single sign-on

1. Import the Dashboard Application Services Hub LTPA keys
 2. Configure single sign-on attributes
 3. Import the Dashboard Application Services Hub SSL certificate
 4. Enable single sign-on for Configuration Manager
- Additional steps are required for Dashboard Application Services Hub
Those steps were outlined in a previous unit

Detailed steps to configure single sign-on can be found here:

https://www.ibm.com/support/knowledgecenter/SS7UH9_6.4.2/ncm/wip/noi-ncm/concept/ncm_int_sso.html

© Copyright IBM Corporation 2019

Configuring the presentation server for single sign-on

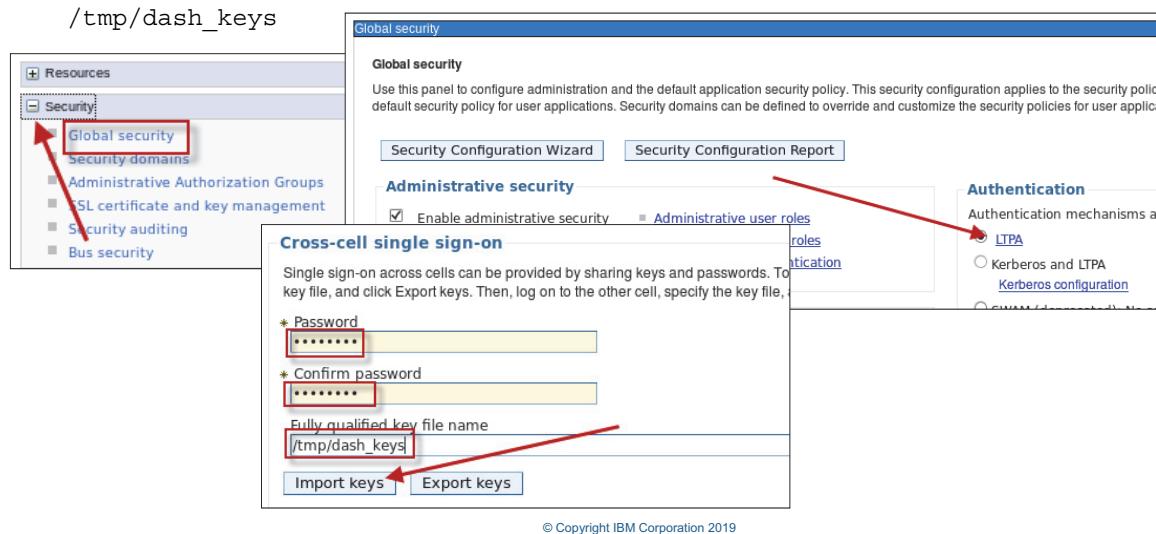
To enable single sign-on, you complete configuration steps on Dashboard Application Services Hub and on the presentation server. You already completed the required configuration on Dashboard Application Services Hub. You did this configuration after you installed Netcool/Impact in a previous unit.

The following slides describe the configuration steps for the presentation server.

Importing the Dashboard Application Services Hub LTPA keys

The WebSphere Administrative Console is used to import the keys

This slide assumes that the keys are exported to



Importing the Dashboard Application Services Hub LTPA keys

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.

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 with LTPA tokens, they must both use the same LTPA keystore.

You exported the keystore from Dashboard Application Services Hub in a previous unit. This slide describes the process that you use to import the keystore into the presentation server.

Configuring single sign-on attributes

The WebSphere Administrative Console is used to configure the attributes

Authentication
Authentication mechanisms and expiration
 [LTPA](#)
 Kerberos and LTPA
[Kerberos configuration](#)
 SWAM (deprecated): No authenticated communication

Authentication cache settings
 [Web and SIP security](#)
 [General settings](#)
 [Single sign-on \(SSO\)](#) **(This link is highlighted with a red box)**
 [SPNEGO web authentication](#)

General Properties

Enabled
 Requires SSL
Domain name **jcsite.edu** **(This field is highlighted with a red box)**
 Interoperability mode
LTPA V1 cookie name
LTPA V2 cookie name **LtpaToken2** **(This field is highlighted with a red box)**
 Web inbound security attribute propagation
 Set security cookies to HTTPOnly to help prevent cross-site scripting attacks
Apply **OK** **Reset** **Cancel** **(The 'Reset' button is highlighted with a red box)**

© Copyright IBM Corporation 2019

Configuring single sign-on attributes

This slide describes how to specify the domain name and LTPA cookie name. These entries must match exactly the entries in Dashboard Application Services Hub.

Importing the Dashboard Application Services Hub SSL certificate (1)

The WebSphere Administrative Console is used to import the certificate

The screenshot shows the 'Security' section of the WebSphere Administrative Console. The left sidebar lists 'Global security', 'Security domains', 'Administrative Authorization Groups', 'SSL certificate and key management' (which is highlighted with a red box), 'Security auditing', and 'Bus security'. The main content area displays information about SSL configurations, including establishing secure connections between applications and configuring each endpoint. It also mentions migration utilities and key sets. A 'Related Items' sidebar on the right lists 'SSL configurations', 'Dynamic outbound endpoint SSL configurations', 'Key stores and certificates' (which is highlighted with a red box), and 'Key sets'. Below this is a table titled 'You can administer the following resources:' containing two entries:

Select	Name	Description	
<input type="checkbox"/>	NodeDefaultKeyStore	Default key store for JazzSMNode01	(ce... (nc...)
<input type="checkbox"/>	NodeDefaultTrustStore	Default trust store for JazzSMNode01	(ce... (nc...)

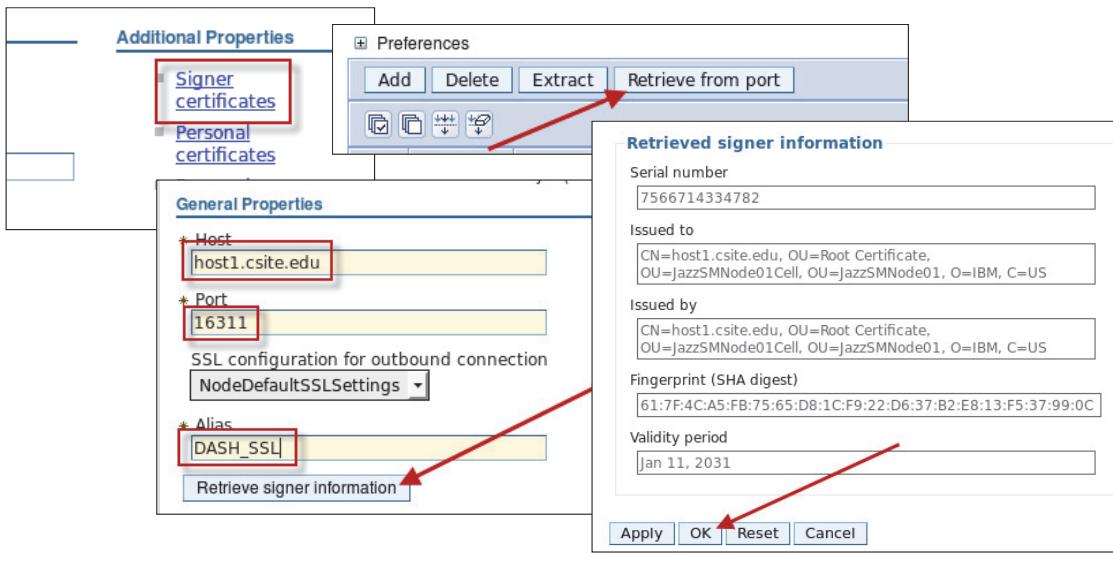
© Copyright IBM Corporation 2019

Importing the Dashboard Application Services Hub SSL certificate (1)

You install a Dashboard Application Services Hub SSL certificate in the presentation.

Importing the Dashboard Application Services Hub SSL certificate (2)

The WebSphere Administrative Console is used to import the certificate



© Copyright IBM Corporation 2019

Importing the Dashboard Application Services Hub SSL certificate (2)

Enter the SSL port number for Dashboard Application Services Hub, and click **Retrieve from port**. Click **OK** to save the certificate.

Enabling single sign-on for Configuration Manager

- Both Configuration Manager and Configuration Manager WebSphere must be configured to enable SSO
The previous steps configured WebSphere for SSO
- The following step configures Configuration Manager for SSO

1. Change to the target directory

```
cd /opt/IBM/ncm/bin/utils
```

2. Run the utility

```
./configSSO.sh enable
```

```
-----  
ITNCM - DATABASE SQL RUNNER  
-----
```

```
Loading database property file: /opt/IBM/ncm/bin/utils/database/dbload.properties  
Processing file /opt/IBM/ncm/database/sql/ncm_enableSSO.sql  
.  
1 of 1 statement(s) processed successfully.
```

© Copyright IBM Corporation 2019

Enabling single sign-on for Configuration Manager

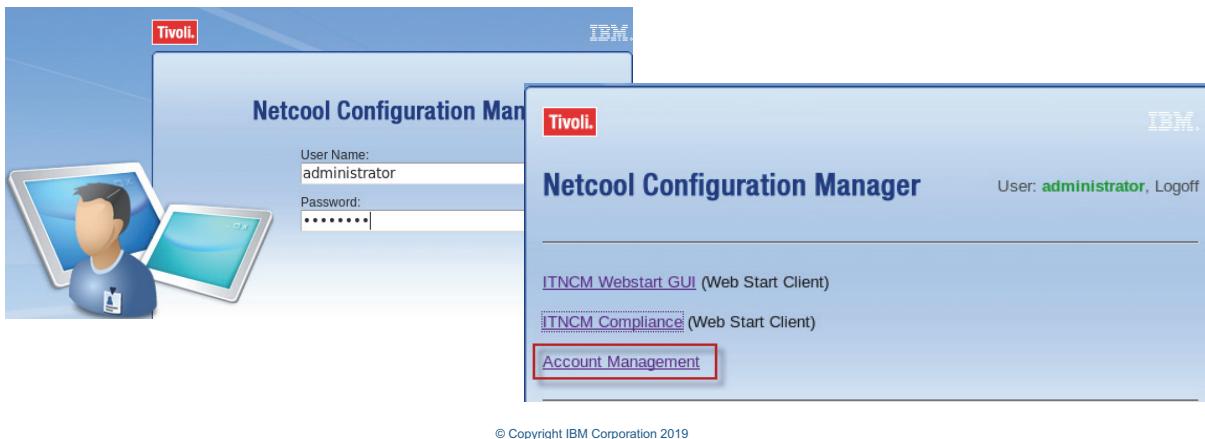
In the previous steps, you configure the WebSphere application to enable single sign-on. You must also run a command that configures the Configuration Manager to enable single sign-on.

Configuring access rights for existing users (1)

You added Netcool/OMNIbus and Network Manager users to Configuration Manager groups in a previous step

The group access grants access to certain Configuration Manager features

The following steps configure the user access rights within Configuration Manager



© Copyright IBM Corporation 2019

Configuring access rights for existing users (1)

When you created the Configuration Manager groups, you assigned roles in Dashboard Application Services Hub. These roles grant access to Dashboard Application Services Hub features, like pages, tools, and menus. You must also complete more configuration to enable access to Configuration Manager features. You use the Account Management feature of Configuration Manager for this configuration.



Note: A user must belong to the IntellidenAdminUser group to use the Account Manager feature.

Configuring access rights for existing users (2)

The operator group has full access to the ITNCM realm

The screenshot shows the 'Account Administration' interface. On the left, there's a tree view with 'Groups' and 'Users'. Under 'Groups', 'operator' is selected and highlighted with a red box. Under 'Users', several entries like 'itnadmin', 'itnmuser', 'ncoadmin', and 'ncouser' are listed, with 'itnadmin' and 'itnmuser' also highlighted with red boxes. A note at the bottom left says 'User data is managed via remote user registry'. In the center, a 'Modify Group: operator' dialog is open. It has tabs for General, Activities, Users, Workflow, and Security. A red arrow points to the Security tab. Below it is a table:

Realm	View	Add	Modify	Delete	All
ITNCM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ITNCM/NOI_AGG_P	<input checked="" type="checkbox"/>				

© Copyright IBM Corporation 2019

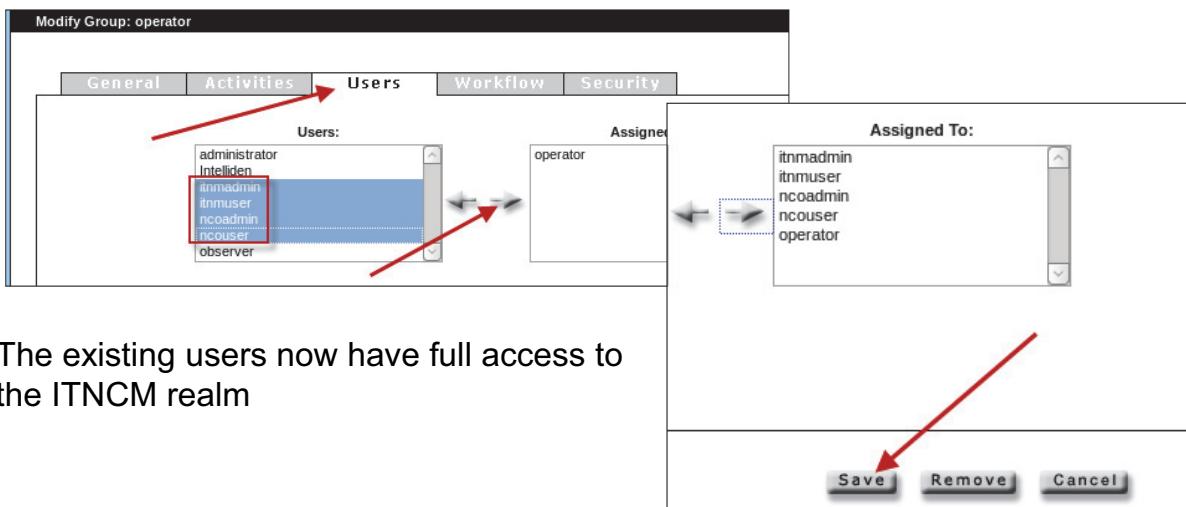
Configuring access rights for existing users (2)

When the Account Management user interface opens, you see a list of groups and a list of users. The group names are internal to Configuration Manager, and are not the same groups that exist in LDAP. However, the user names are defined in LDAP. The Account Management utility sees only those users that are members of one of the Configuration Manager groups: IntellidenAdminUser or IntellidenUser.

This slide highlights the access rights that exist for the operator group. Any member of the operator group has full access to the ITNCM realm, and any subrealms.

Configuring access rights for existing users (3)

Add the existing users to the operator group



The existing users now have full access to the ITNCM realm

© Copyright IBM Corporation 2019

Configuring access rights for existing users (3)

This slide describes how you add users to the operator group. After you add the users to the group, the users have full access rights to the ITNCM realm.

Configuring integration with Netcool/OMNIbus (1)

Netcool Configuration Manager generates SNMP traps for various situations

The SNMP probe rules that decode the Configuration Manager traps are included in the Netcool Knowledge Library collection of rules files

You must uncomment a few lines to activate the Configuration Manager rules.

1. Edit the following file:

/opt/IBM/tivoli/NcKL/rules/snmptrap.rules

2. Uncomment the following lines:

```
#include "$NC_RULES_HOME/include-snmptrap/ibm/ibm.master.include.lookup"  
#include "$NC_RULES_HOME/include-snmptrap/ibm/ibm.master.include.rules"  
#include "$NC_RULES_HOME/include-snmptrap/ibm/ibm-preclass.include.snmptrap.rules"  
include "$NC_RULES_HOME/include-snmptrap/ibm/ibm-preclass.include.snmptrap.rules"
```

These lines may already be uncommented, depending on your version of the Netcool Knowledge Library

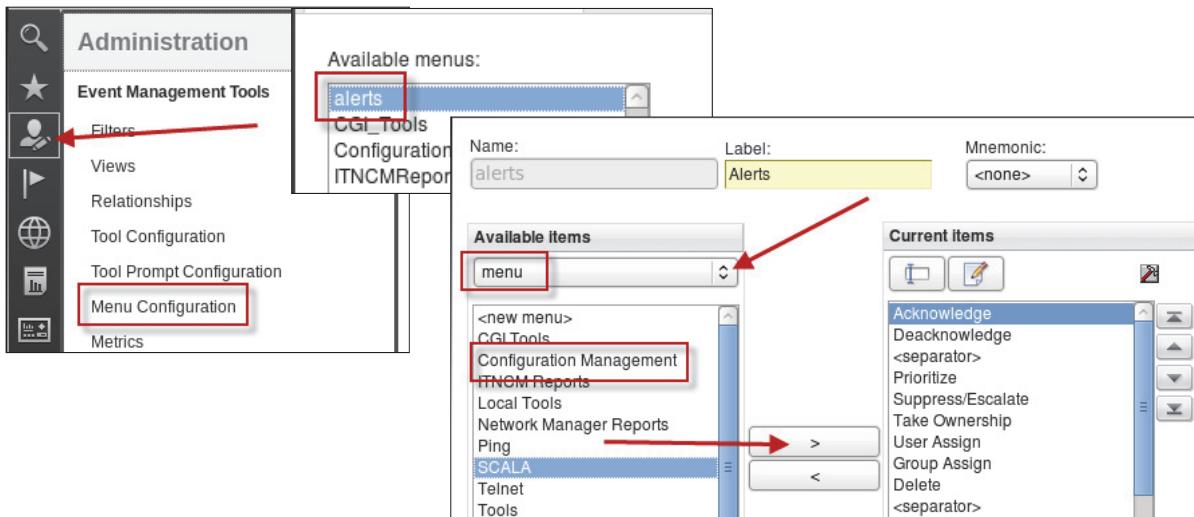
© Copyright IBM Corporation 2019

Configuring integration with Netcool/OMNIbus (1)

The SNMP probe rules to interpret Configuration Manager traps are bundled with the current version of the Netcool Knowledge Library. You must modify a file, and uncomment several lines to enable those rules.

Configuring integration with Netcool/OMNibus (2)

Add the Configuration Manager menu to the Web GUI alert menu



© Copyright IBM Corporation 2019

Configuring integration with Netcool/OMNibus (2)

When you installed the Configuration Manager GUI components, you added some Web GUI tools and a menu definition. You must manually add that menu to the existing alerts menu. After you add the entry, users can see the Configuration Manager tools from the Event Viewer.

Configuring device synchronization

Netcool Configuration Manager automatically imports devices that are discovered by Network Manager

The installation configures this synchronization process

By default, the synchronization runs once every day

The following steps demonstrate how to modify that frequency

1. Edit the following file:

/opt/IBM/ncm/config/properties/rseries.properties

2. Change the following property:

```
#  
# Label: 1440 is a Daily (in minutes) delay. Update time in minutes.  
#  
NMEntityMappingComponent/period=1440
```

Note: This change is optional

© Copyright IBM Corporation 2019

Configuring device synchronization

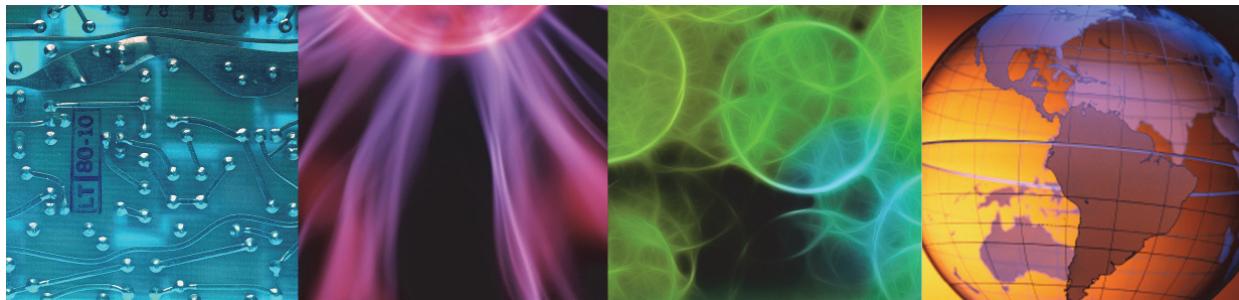
Device synchronization between Network Manager and Configuration Manager is automatic. Configuration Manager queries the Network Manager topology database periodically and looks for devices that Network Manager discovers. When it finds new devices, Configuration Manager retrieves the device configuration files.

The synchronization configuration is accomplished during the core installation process. No further configuration is required. However, the automatic frequency that the process uses is configured for one time each day. For the class exercise, you modify a property file and change the frequency.

Lesson 8 Out-of-band change



Lesson 8 Out-of-band change



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to install the Out-of-band change feature.

Reasons for out-of-band change

You use out-of-band change for several reasons:

- Not all changes are processed by Configuration Manager worker servers
- Not all VTY connections are made by the Configuration Manager device terminal
- You can ensure that the configurations are always current within the database

© Copyright IBM Corporation 2019

Reasons for out-of-band change

The out-of-band change (OOBC) daemon is a tool that can be implemented with the Configuration Manager software. OOBC addresses the following issues:

- Configuration Manager is initially implemented as a change mechanism in only one portion of the infrastructure of a customer. If not all stakeholders in a network change use the solution, then Configuration Manager does not manage a certain set of changes.
- The Configuration Manager device terminal does not manage all manual interactions with devices. When device interactions are processed with other VTY clients, no monitoring of the sessions occur.

The issue that arises from not using the Configuration Manager architecture for device interaction is that configurations can change, but the application is not aware of the change. Having the configurations always current in the database is important. This issue is especially the case when Configuration Manager implements changes, and the database and device must be synchronized for the change to be successful.

Out-of-band change

A **syslog** event that comes from one of these sources:

- A nonworker server IP address
- An unauthorized user

An out-of-band change differs from an in-band change

- Out-of-band change syslog message

Jul 14 10:08:46 Sales_Lab_2600-3 11566: 7w6d: %SYS-5-CONFIG_I: Configured from console by **lkoeser** on vty0 (**9.3.86.27**)

- In-band change syslog message

Jul 14 15:28:53 Sales_Lab_2600-5 11567: 7w6d: %SYS-5-CONFIG_I: Configured from ftp://ftp:password@12.41.186.55/intelliden-Cisco1025558934493.cfg by **itncm** on vty0 (**12.41.186.55**)

© Copyright IBM Corporation 2019

Out-of-band change

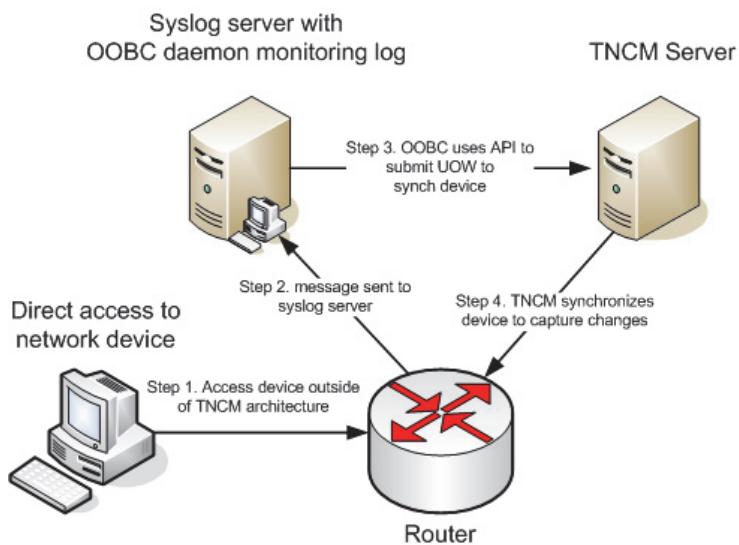
The OOBC daemon is a utility that monitors syslog events. Syslog events are UDP logging events that can be captured in a flat text file on a server that devices are sending messages to. When logging is enabled on network devices, you can configure various logging levels. The various levels mean that many log messages can be received from any one device that can reference many different issues the device is reporting on. Only a small subset of these messages indicates that the configuration state that the device configuration changed.

When a message of interest is found, it is parsed for various data items. These items include the user name of the individual who accessed the device and the IP address from which the connection was made. Using this information, this logic is used:

- If the IP address is present, then it is compared to a list of worker server addresses. If it matches one of those addresses, the daemon assumes that the device was synchronized. If it does not match a worker server IP, then the daemon schedules that device to synchronize.
- If the syslog event does not have a connection IP address, then the user name is selected and compared against a list of authorized user names. If the user name is authorized, it is assumed that device synchronization occurred, and the message is ignored. If that user name is not authorized, the event is noted and the daemon schedules a synchronization.
- If neither of these data items is in the message, the event is noted and the daemon schedules a synchronization as a precaution to ensure that the changes are saved to the database.

Notice the difference between the out-of-band change and the in-band change messages. The assumption is that the worker server IP address is 12.41.186.55, and the authorized user is **itncm**.

OOBC process



© Copyright IBM Corporation 2019

OOBC process

From an external perspective, the OOBC daemon is a piece of Java code that is run as a service on the server that collects syslog messages throughout the network. It is rare that the OOBC daemon runs on a Configuration Manager server because most organizations use a dedicated syslog server.

The process begins by a user or application logging in to a network device from a client computer that is not a worker server. This action can be from a desktop computer or an application server that applies changes to device configurations.

The network device is configured to send log messages when a change to the configuration is detected. This action has two implications:

- The device was configured to send log messages and is sending them to the correct server.
- The server is receiving the log messages. If the message is using UDP, it has an unreliable method of transmission.

The OOBC daemon uses its list of rules to parse through all log messages to find ones that are interesting. It finds the message that the router generated and parses information from the message. Using its logic, it notes that the message is an out-of-band change. It eventually connects to the Configuration Manager server through the API and submits a unit of work to ensure that the configuration is synchronized.

So configuration Manager processes the UOW, obtains the configuration from the device, and updates its database.

Installation prerequisites

You must install the OOBC where it has read access to a text-based syslog file

Each installation can read only one syslog file

You can have multiple installations on a syslog server

Each installation requires 500 MB of space

Each installation requires 1 GB of memory

Application must connect to a Configuration Manager presentation server

Requires a Configuration Manager user name and password

© Copyright IBM Corporation 2019

Installation prerequisites

The OOBC daemon must be able to read the text-based syslog file. You typically install the daemon on the same server where the syslog messages are being captured. If the syslog file is an NFS mount point, it is possible to read it from a separate server.

Each OOBC process can monitor only one file at a time. A server can have multiple installations to monitor multiple log files.

Each installation takes about 500 MB of space. Most of this space (400 MB) is for logging. The installation also requires up to 1 GB of memory. This value is negotiable, depending on how many syslog messages must be parsed in any given second.

The OOBC process must be able to connect up to a Configuration Manager presentation server to use the API.

Finally, you need a user name and password to log in to the presentation server. Ensure that the user name and password are unique and reflect that the OOBC process submitted the UOWs, in other words, OOBCUser. By having a unique user for running an OOBC task, you can find those tasks in the queue manager. This method makes it easy to generate reports on how much OOBC activity is being generated.

Ensure that the user belongs to a group that has limited capabilities. The OOBC user needs only synchronization activities and a workflow policy of zero so that UOWs require no approval. The group requires view rights on realms and view and run privileges on resources.

Installing the OOBC software

1. Find the oobc.zip software
Included in the Configuration Manager installation file
2. Move it to syslog server and extract to the appropriate location
3. Change directory to install
4. Run the install.sh script as **root**
Installs the executable software under a **run1** directory

© Copyright IBM Corporation 2019

Installing the OOBC software

To install the application, you must locate the OOBC software. This software is in the Configuration Manager base archive file that you downloaded and used to install the Configuration Manager application. Move the oobc.zip file to the syslog server where it is installed.

Determine where the base file system is located, and extract the file. This action creates a directory called OutOfBandChange. This file system is where all the executable files are built during the installation process.

Move into the installation directory and run the install.sh script as the root user. Root privileges are required because startup and shutdown scripts are placed in the RC directories. This step ensures that OOBC is restarted if the syslog server is rebooted. While not a hard requirement, running the installer as a different user causes the installation to generate a message that it failed. This failure is probably a false positive, and the OOBC can start. If you install as root, the permissions on all the files are changed to reflect the user and group prompted for by the installer.

This installation creates a run1 directory, where all the executable files are placed. If subsequent installations are necessary to monitor more than one file, a run2 directory is created.

Installation questions

User and group owner of the software installation
Configuration Manager presentation server host name and port
Configuration Manager user name and password
User name for Configuration Manager access to network devices
IP address of the worker server
Authorized user name of who can access network devices
Full path to the syslog file that is monitored
Full path to a file that saves all interesting syslog events

You can modify these details in the oobc.properties.xml file

© Copyright IBM Corporation 2019

Installation questions

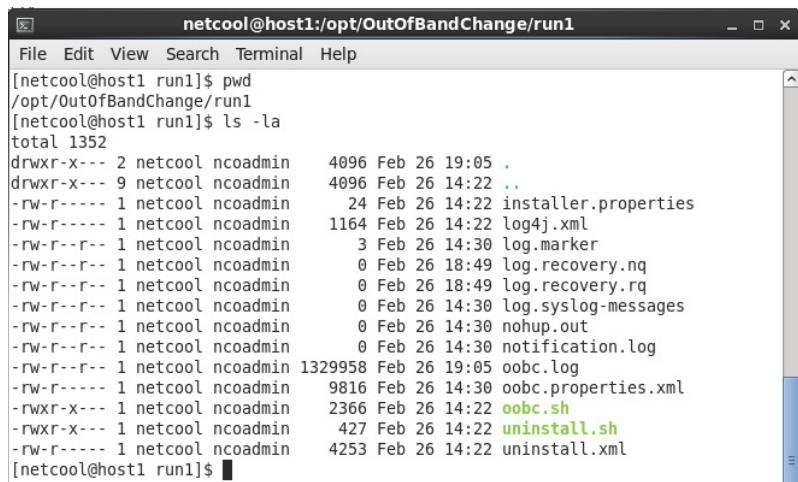
In the installer, you are prompted to answer a series of questions:

- User and Group owner of the software installation: This value defines a Linux user and group that is already configured on the server. This user and group require read access to the monitored syslog file. If installed as root, the permissions of all installation files are changed to these values.
- Configuration Manager presentation server host name and port: This data directs the OOBC daemon to the Configuration Manager installation. The default port is 16310.
- Configuration Manager user name and password: These values are the credentials that are used to log in to Configuration Manager and submit the UOW.
- User name used for Configuration Manager access to network devices: This value is the user name that Configuration Manager uses to log in to network devices. Typically, it is a TACACS

user name. If more than one user name is used for device connectivity, the oobc.properties.xml file can be manually configured after this installation.

- IP address of the worker server: This value is the IP address of the worker server.
- User names that generate synchronizations but not notifications: These user names complete modifications that must be synchronized but do not send messages to notification.log. The installer refers to them as 3rdPartyUsers.
- Full path to the syslog file that is monitored: This path is the location of the syslog file that the OOBC daemon monitors.
- Full path to a file that saves all interesting syslog events that generated UOWs: This file is used to capture all syslog events of interest.

Files in the execution directory



```
netcool@host1:/opt/OutOfBandChange/run1
File Edit View Search Terminal Help
[netcool@host1 run1]$ pwd
/opt/OutOfBandChange/run1
[netcool@host1 run1]$ ls -la
total 1352
drwxr-x--- 2 netcool ncoadmin 4096 Feb 26 19:05 .
drwxr-x--- 9 netcool ncoadmin 4096 Feb 26 14:22 ..
-rw-r----- 1 netcool ncoadmin 24 Feb 26 14:22 installer.properties
-rw-r----- 1 netcool ncoadmin 1164 Feb 26 14:22 log4j.xml
-rw-r---- 1 netcool ncoadmin 3 Feb 26 14:30 log.marker
-rw-r---- 1 netcool ncoadmin 0 Feb 26 18:49 log.recovery.ng
-rw-r---- 1 netcool ncoadmin 0 Feb 26 18:49 log.recovery.rq
-rw-r---- 1 netcool ncoadmin 0 Feb 26 14:30 log.syslog-messages
-rw-r---- 1 netcool ncoadmin 0 Feb 26 14:30 nohup.out
-rw-r---- 1 netcool ncoadmin 0 Feb 26 14:30 notification.log
-rw-r---- 1 netcool ncoadmin 1329958 Feb 26 19:05 oobc.log
-rw-r----- 1 netcool ncoadmin 9816 Feb 26 14:30 oobc.properties.xml
-rwxr-x--- 1 netcool ncoadmin 2366 Feb 26 14:22 oobc.sh
-rwxr-x--- 1 netcool ncoadmin 427 Feb 26 14:22 uninstall.sh
-rw-r----- 1 netcool ncoadmin 4253 Feb 26 14:22 uninstall.xml
[netcool@host1 run1]$
```

© Copyright IBM Corporation 2019

Files in the execution directory

The run1 directory holds all the files needed for review and troubleshooting, including the following files:

- oobc.sh is used to start and stop the daemon
- oobc.log file that notes any trouble with the daemon and messages it found interesting in the syslog file
- oobc.properties.xml file is important as it has all the configuration settings used by the daemon

Configuring OOBC

Most configuration is in the **oobc.properties.xml** file:

- Specific syslog file is for monitoring and how often to monitor
- Consolidation algorithm and timeouts
- Presentation server details, user name, and password
- Worker server addresses
- Authorized users who log in to network devices
- The regular expressions used to find syslog messages of interest

© Copyright IBM Corporation 2019

Configuring OOBC

After the installation is complete, you might require more configuration to include extra worker servers and user names.

For this extra configuration, you use the **oobc.properties.xml** file. This file is an XML file that defines everything that is important about the OOBC daemon. Any changes to this file require restarting the daemon.

This file contains the following properties:

- Location of the syslog file to monitor
- The timeout value and consolidation algorithm to use
- The credentials and location of the presentation server
- The worker server IP address
- Device user names
- The regular expressions used to parse the syslog server file for interesting messages.

These items typically require little change when correctly defined after installation.

Startup and shutdown

- Single script for each runtime configuration
- \$OOBC_Install_Home/run1/oobc.sh {start | stop | restart}
- Creates and uses \$OOBC_Install_Home/run1/oobc.pid
- Simple kill causes an orderly shutdown

Starting the daemon

```
cd /opt/OutOfBandChange/run1  
./oobc.sh start  
Monitor $OOBC_home/run1/oobc.log for any errors
```

Stopping the daemon

```
cd /opt/OutOfBandChange/run1  
./oobc.sh stop
```

© Copyright IBM Corporation 2019

Startup and shutdown

After modifying the oobc.properties.xml file, you can start the application by using the oobc.sh script. It takes the options of start, stop, and restart. Upon starting the daemon, a file with the process ID is created and kept in the run1 directory until the process is shut down.

Student exercises



© Copyright IBM Corporation 2019

Student exercises

Summary

You now should be able to perform the following tasks:

- Describe the major functions of Netcool Configuration Manager
- Describe the deployment architecture
- Install and configure Netcool Configuration Manager

© Copyright IBM Corporation 2019

Summary



6 Verifying Networks for Operations Insight



Verifying networks for Operations Insight



© Copyright IBM Corporation 2019

Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this unit, you verify the basic features of the Networks for Operations Insights solution.

Objectives

In this unit, you learn to perform the following tasks:

- Discover devices with Network Manager
- Import devices into Netcool Configuration Manager based on Network Manager discovery
- Verify network compliance evaluation and perform remediation
- Verify of launch-in-context tool launch from Dashboard Application Services Hub

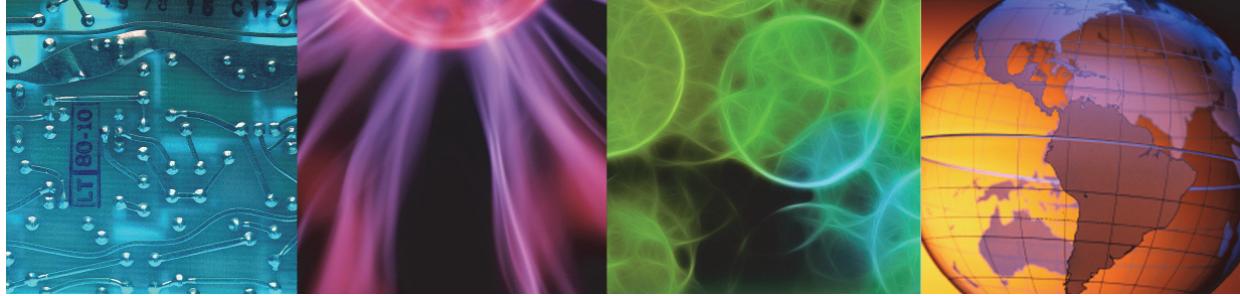
© Copyright IBM Corporation 2019

Objectives



Lesson 1 Solution verification

Lesson 1 Solution verification



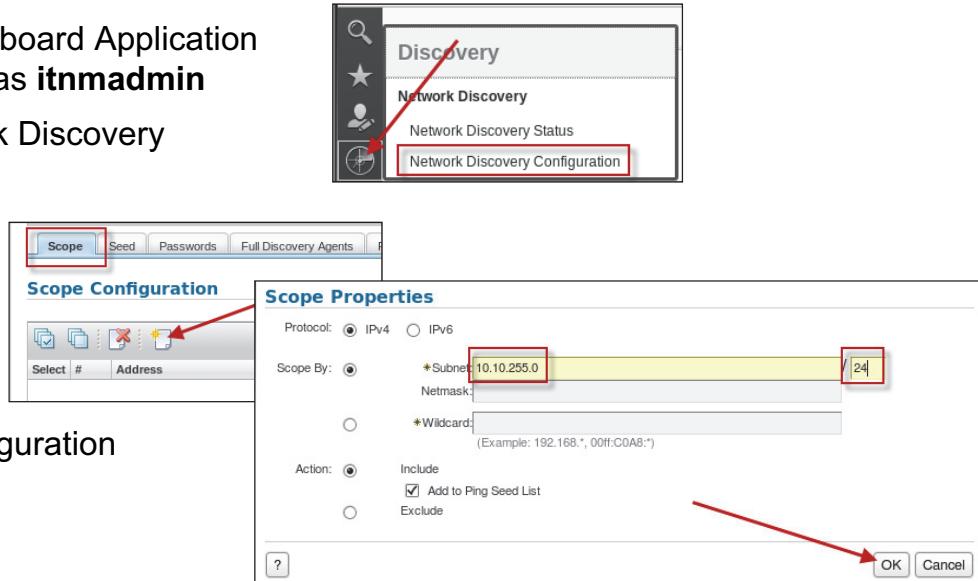
© Copyright IBM Corporation 2019
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

In this lesson, you learn how to perform the following tasks:

- Perform a network discovery with Network Manager
- Import device configurations into Configuration Manager
- Perform compliance evaluation and remediation
- Verify tool capability

Configuring network discovery

1. Log in to Dashboard Application Services Hub as **itnmadmin**
2. Select Network Discovery Configuration
3. Add a subnet



4. Save the configuration

© Copyright IBM Corporation 2019

Configuring network discovery

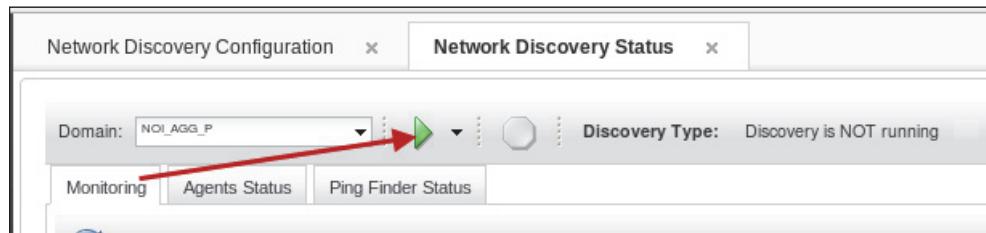
The lab exercises for this unit use a network simulator. The simulator simulates 15 network devices. In the exercise, you add the subnet for the simulated devices.

Running a network discovery

1. Select Network Discovery Status



2. Click the green arrow



© Copyright IBM Corporation 2019

Running a network discovery

To start the network discovery, click the **green arrow** icon.

Discovery complete

Phase	Status	Elapsed Time (H:MM:SS)	
		Current	Previous
Interrogating Devices	✓	0:02:34	-
Resolving Addresses	✓	0:00:08	-
Downloading Connections	✓	-	-
Correlating Connectivity	✓	0:00:03	-

© Copyright IBM Corporation 2019

Discovery complete

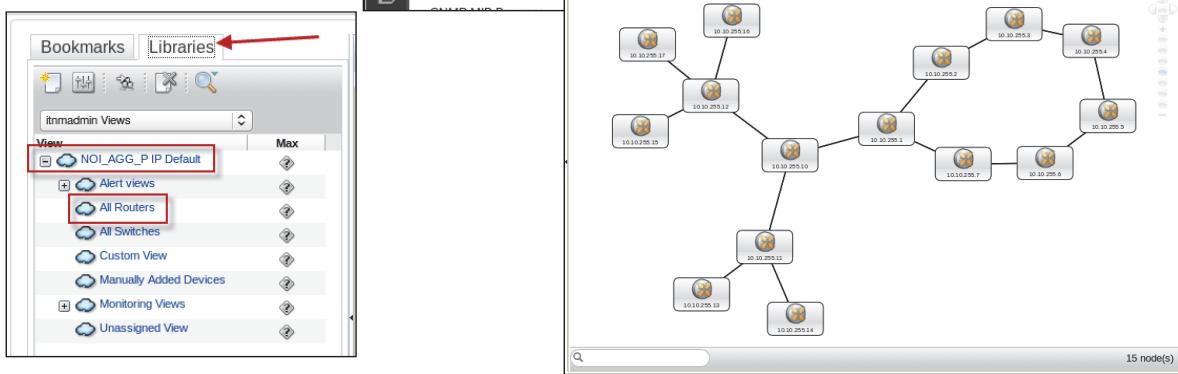
The discovery runs approximately 3 minutes. The four green check marks indicate that the discovery is complete.

Network view

1. Select Network Views



2. Click All Routers



© Copyright IBM Corporation 2019

Network view

Select Network Views, and click the **Libraries** tab. The discovery process populates the entries in this tab automatically. Click **All Routers**, and the discovered topology opens in a new pane.

Verifying integration with Configuration Manager

1. Select Client Launch



2. Click ITNCM-Base

UOW ID	Type	Submitter	Request Type	Execution Status
1	UOW	administrator	Run Autodiscovery	SUCCESS
2	UOW	administrator	Run Autodiscovery	SUCCESS
3	UOW	administrator	Run Autodiscovery	SUCCESS
4	UOW	administrator	Run Autodiscovery	SUCCESS
5	UOW	administrator	Run Autodiscovery	SUCCESS
6	UOW	administrator	Run Autodiscovery	SUCCESS
7	UOW	administrator	Run Autodiscovery	SUCCESS
8	UOW	administrator	Run Autodiscovery	SUCCESS
9	UOW	administrator	Run Autodiscovery	SUCCESS
10	UOW	administrator	Run Autodiscovery	SUCCESS
11	UOW	administrator	Run Autodiscovery	SUCCESS
12	UOW	administrator	Run Autodiscovery	SUCCESS
13	UOW	administrator	Run Autodiscovery	SUCCESS
14	UOW	administrator	Run Autodiscovery	SUCCESS
15	UOW	administrator	Run Autodiscovery	SUCCESS

Verifying integration with Configuration Manager

Configuration Manager is configured to retrieve device information from the Network Manager topology database automatically. The retrieval process runs periodically. The default frequency is one time per day. In the student exercises, you modify the frequency and set the value to every 5 minutes.

You click **ITNCM-Base** in Dashboard Application Services Hub which starts the Java Webstart client for Configuration Manager. The client opens, and you log in without entering a user name and password, which verifies that single sign-on is functioning correctly.

The automatic import process creates a *unit of work* for each device that Network Manager discovers. You can check the status of the unit of work processing under Queue Manager.

Imported devices

The screenshot shows the IBM Tivoli Netcool Configuration Manager interface. The left pane displays a tree view of resources under 'ITNCM'. A red box highlights the 'ITNCM' node. Below it, 'Queue Manager' is expanded, showing 'Pending Approval Tickets', 'All Approval Tickets', 'Work Pending Approval', 'Work Waiting to Execute', 'Work Currently Executing', and 'Work That is Finished'. Another red box highlights the 'Content' node under 'Resource Browser', which contains 'CommandSets', 'ModeledCommands', 'NativeCommands', and 'NOI_AGG_P'. A third red box highlights the 'Search Results' node. The right pane is a grid table titled 'Server Time: Mar 2, 2016 10:01 AM'. It lists 14 Cisco routers (Type: Router) with names ranging from 10.10.255.1 to 10.10.255.7. The columns are: Name, Realm, Modified..., Vendor, Type, Model, and OS.

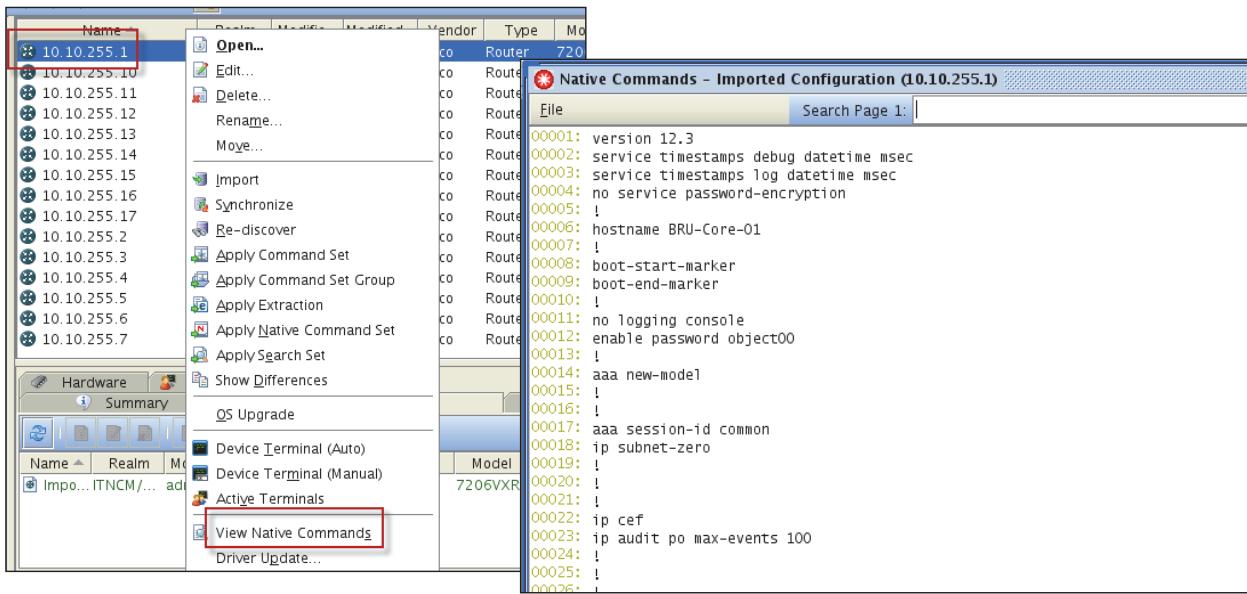
Name	Realm	Modified...	Vendor	Type	Model	OS
10.10.255.1	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	7206...	C720...
10.10.255.10	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	3660	C366...
10.10.255.11	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	3640	C364...
10.10.255.12	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	3640	C364...
10.10.255.13	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	3640	C364...
10.10.255.14	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	3640	C364...
10.10.255.15	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	3640	C364...
10.10.255.16	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	3640	C364...
10.10.255.17	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	3640	C364...
10.10.255.2	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	7206...	C720...
10.10.255.3	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	7206...	C720...
10.10.255.4	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	7206...	C720...
10.10.255.5	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	7206...	C720...
10.10.255.6	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	7206...	C720...
10.10.255.7	ITNCM/...	administ... Mar 1, 2...	Cisco	Router	7206...	C720...

© Copyright IBM Corporation 2019

Imported devices

After the processing for the units of work is complete, you can see the entries for the imported devices.

Device configuration



© Copyright IBM Corporation 2019

Device configuration

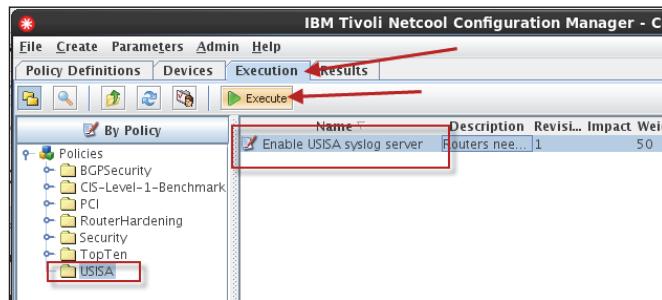
Click a device entry to select it, right-click, and select **View Native Commands**. A new window opens, and you see the contents of the device configuration file.

Verifying compliance management

1. Select ITNCM-Compliance



2. Click Execute



Verifying Compliance Management

After you import the device configuration files, you can evaluate the files for compliance. You click **ITNCM-Compliance** in Dashboard Application Services Hub which starts the Java Webstart client for Compliance Manager. The client opens, and you log in without entering a user name and password, which verifies that single sign-on is functioning correctly.

Select the **Execution** tab, select a compliance policy, and click **Execute**. The compliance wizard opens, and you select the devices for evaluation.

Compliance results

The screenshot shows two tables from a compliance reporting interface.

Process Execution Summary:

Name	State	Executed By	Devices	Process Type	Execution Type	Start Time
AdHoc_02-Ma...	Finished	itnmadmin	15	Compliance	AdHoc	02-Mar-2016

Policy Validation Summary:

Policy Name	Severity	Revision	Date	Passed	Failed	Not Assess
Enable USISA s...	3	1	02-Mar-2016 12:00:00	Passed	15 Failed	0

© Copyright IBM Corporation 2019

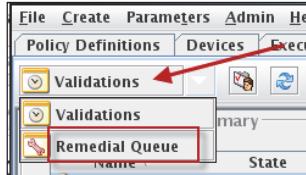
Compliance results

The compliance evaluation process does not examine the physical devices. The evaluation process examines the device configuration files. After the process completes, you see the results of the compliance testing. In the example that is shown here, the process evaluates 15 devices, and every device fails the compliance test.

In the student exercise, the compliance policy checks the device configuration for the presence of a command to configure a syslog server IP address. The policy check fails because none of the devices contain the required command.

Verifying compliance remediation

1. Click Remedial Queue



2. Approve the requests

A screenshot of the Remedial Queue list view. The table has columns: Co..., Com..., Policy, Device, Realm, Status, Occur..., Para..., Result, UOW There are 15 rows, each representing a failed configuration. The last column in each row contains three buttons: 'Approve' (highlighted with a red box), 'Reject', and 'Delete'. The footer of the table area says '© Copyright IBM Corporation 2019'.

Co...	Com...	Policy	Device	Realm	Status	Occur...	Para...	Result	UOW ...
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		
3...	ITNC...	Enabl...	10.1...	ITNC...	Pendi...	02-M...	SYSLO...		

Verifying compliance remediation

The compliance policy is configured to correct any failed configurations. The compliance policy creates 15 units of work, one for each failed device. You must approve the units of work.

Remediation results

UOW ID	Type	Submitter	Request Type	Execution Status
31	UOW	administrator	Native Command Set	SUCCESS
32	UOW	administrator	Native Command Set	SUCCESS
33	UOW	administrator	Native Command Set	SUCCESS
34	UOW	administrator	Native Command Set	SUCCESS
35	UOW	administrator	Native Command Set	SUCCESS
36	UOW	administrator	Native Command Set	SUCCESS
37	UOW	administrator	Native Command Set	SUCCESS
38	UOW	administrator	Native Command Set	SUCCESS
39	UOW	administrator	Native Command Set	SUCCESS
40	UOW	administrator	Native Command Set	SUCCESS
41	UOW	administrator	Native Command Set	SUCCESS
42	UOW	administrator	Native Command Set	SUCCESS
43	UOW	administrator	Native Command Set	SUCCESS
44	UOW	administrator	Native Command Set	SUCCESS
45	UOW	administrator	Native Command Set	SUCCESS

Remediation results

After you approve the units of work, the worker server processes each one. You verify the completion status under the Queue Manager.

Verify remediation

The screenshot shows the Compliance Manager interface with the 'Results' tab selected. A red arrow points to the 'Execute' button in the toolbar. The main pane displays a table of policy results:

Name	Description	Revised	Impact	Weight	Excluded
Enable USISA	Route...	1	50	P	

Below this is the 'Process Execution Summary' table:

Name	State	Executed By	Devices	Process Type	Execution Type	Start Date
AdHoc_02-Main	Finished	itnmadmin	15	Compliance	AdHoc	02-Mar-16
AdHoc_02-Main	Finished	itnmadmin	15	Compliance	AdHoc	02-Mar-16

At the bottom, the 'Policy Validation Summary' table shows:

Policy Name	Severity	Revision	Date	Passed	Failed	Not As
Enable USISA	3	1	02-Mar-2016 13:15	Passed	0	0

Verify remediation

You return to the Compliance Manager user interface, and rerun the same policy. The policy checks the configuration files and all 15 devices pass the check.

Configuration Manager traps

Sev	Ack	Node	Alert Group	Summary
⚠️	No	10.10.255.12	Policy Trap	10.10.255.12 is in violation of policy Enable USISA syslog server
⚠️	No	10.10.255.2	Policy Trap	10.10.255.2 is in violation of policy Enable USISA syslog server
⚠️	No	10.10.255.14	Policy Trap	10.10.255.14 is in violation of policy Enable USISA syslog server
⚠️	No	10.10.255.11	Policy Trap	10.10.255.11 is in violation of policy Enable USISA syslog server
⚠️	No	10.10.255.15	Policy Trap	10.10.255.15 is in violation of policy Enable USISA syslog server
⚠️	No	10.10.255.7	Policy Trap	10.10.255.7 is in violation of policy Enable USISA syslog server
⚠️	No	10.10.255.6	Policy Trap	10.10.255.6 is in violation of policy Enable USISA syslog server

Node	Alert Group	Summary
192.168.100.100	UOW trap	Apply Native Commandset UOW '35' submitted by administrator is executing (531658018)
192.168.100.100	UOW trap	Apply Native Commandset UOW '37' submitted by administrator is executing (531658023)
192.168.100.100	UOW trap	Apply Native Commandset UOW '41' submitted by administrator is executing (531669050)
host1.csite.edu	DBStatus	Last 5 mins alerts.details (inserts): 0
192.168.100.100	UOW trap	Import UOW '17' submitted by administrator is executing (531557597) 61 days, 12:32:55.9

© Copyright IBM Corporation 2019

Configuration Manager traps

Configuration Manager generates SNMP traps for various activities, including the compliance testing. Configuration Manager is configured to forward traps to the Netcool/OMNibus SNMP probe. The probe is configured with the Netcool Knowledge Library collection of rules files. The Netcool Knowledge Library contains rules that interpret Configuration Manager traps and generate Netcool/OMNibus event records.

Open the Event Viewer in Dashboard Application Services Hub, and you see the Configuration Manager events. The correct event records verify that Configuration Manager forwards SNMP traps correctly, and that the SNMP probe is configured correctly to decode the traps.

Device Activity Viewer

The screenshot shows the ITNCM Activity Viewer interface. At the top, there are filter options for Start Date (01/02/2016, 13:38), End Date (02/03/2016, 13:38), Users (Select All, administrator), and Activity Status (Select All, Successful). A 'Search' button is also present. Below the filter section, a timeline displays five events for the device 10.10.255.1 (SmartModel) on 02/03/2016:

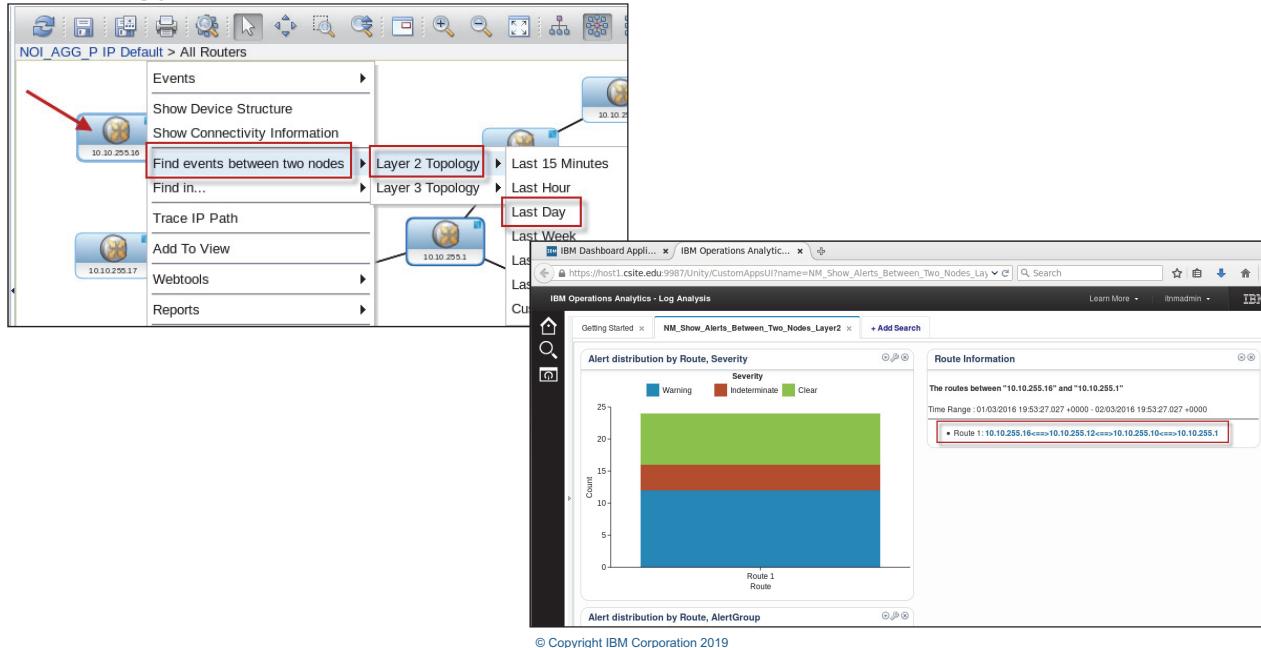
- Run Autodiscovery: User : administrator 02/03/2016 12:30:55
- Import Configuration: User : administrator 02/03/2016 12:32:52
- Imported Configuration: User : administrator Support : SmartModel 02/03/2016 12:34:18
- Native Command Set: User : administrator 02/03/2016 12:47:39
- Native command set Modified Configuration (3.1.55 enable logging to syslog server): User : administrator Support : SmartModel 02/03/2016 12:51:15

Each event is represented by a box with a gear icon and a timestamp. Arrows indicate the sequence of events.

Device Activity Viewer

Activity Viewer is an application available in Dashboard Application services Hub. The application is typically started in the context of a Netcool/OMNibus event list. The Activity Viewer shows a series of graphical icons. Each icon represents an action that Configuration Manager completed. The icons provide a graphical summary of what device configuration changes occurred during a defined time frame. When used in the context of a Netcool/OMNibus event, it provides a convenient mechanism for determining whether the event is directly related to a recent device modification.

Topology search



Topology search

You can run the topology search application from:

- Event Viewer
- Network Manager topology view
- Log Analytics user interface

In each case, you must select two devices. In the Event Viewer, you select two event records. In the Network Manager topology view, you select two device icons. Next, you run the application, and select a time frame. The information passes to the topology search application. The application queries the Network Manager topology database, and locates all devices in the network path between the selected devices. Next, the list of device names is used to query the event history in Log Analytics, and return a summary of event records.

Student exercises



© Copyright IBM Corporation 2019

Student exercises

Summary

You now should be able to perform the following tasks:

- Discover devices with Network Manager
- Import devices into Netcool Configuration Manager based on Network Manager discovery
- Verify network compliance evaluation and perform remediation
- Verify of launch-in-context tool launch from Dashboard Application Services Hub

© Copyright IBM Corporation 2019

Summary

