



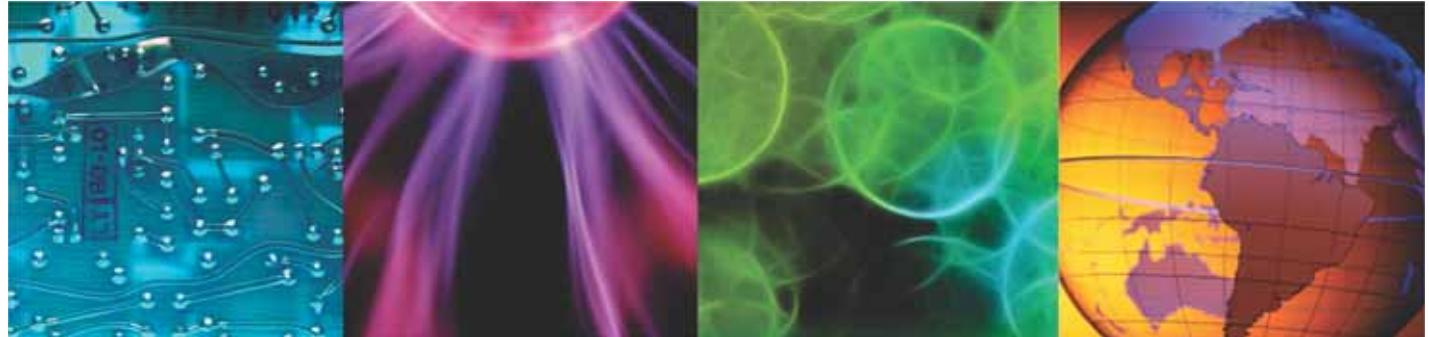
IBM Training

IBM Netcool Operations Insight 1.4 Implementation and Configuration

Student Exercises

Course code TN521 ERC 1.0

May 2016



All files and material for this course are IBM copyright property covered by the following copyright notice.

© Copyright IBM Corp. 2016. All Rights Reserved.

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

IBM, the IBM logo, and ibm.com are 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.

Trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

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

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

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

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

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

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

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results.



Contents

1 Netcool Operations Insight introduction and overview exercise	1
Exercise 1 Validating the host1 server configuration	1
2 Installing IBM Netcool Operations Insight base exercises.....	13
Exercise 1 DB2	13
Installing DB2	13
Configuring DB2 to start at system start	16
Installing the DB2 license file	16
Exercise 2 Netcool/OMNibus core	18
Installing IBM Installation Manager	18
Installing Netcool/OMNibus core	20
Creating the ObjectServer	23
Verifying the initial configuration	26
Verifying basic ObjectServer function	27
Adding a password to the root ObjectServer user	29
Configuring event archiving	29
Configuring Netcool/OMNibus to start at system start	39
Exercise 3 Netcool/OMNibus Web GUI	40
Installing Jazz for Service Management	40
Installing the cumulative patch	49
Tivoli Common Reporting workaround	51
Installing Web GUI	51
Configuring Netcool/OMNibus Web GUI to start at system start	57
Exercise 4 Configuring LDAP as an authentication source	58
Removing the ObjectServer user repository	58
Adding the LDAP user repository	64
Configuring Dashboard Application Services Hub to allow logins when LDAP is down	73
Configuring ObjectServer synchronization	76
Configuring default users and groups	77
Configuring Tivoli Common Reporting	84
Exercise 5 Netcool/Impact	99
Installing the software	99
Configuring Netcool/Impact to use LDAP	102
Configuring Netcool/Impact to use single sign-on	107
Integrating the Netcool/Impact console	112
Enabling users for access to the Netcool/Impact console	115
Configuring Netcool/Impact to start at system start	117
Exercise 6 IBM Operations Analytics Log Analysis	119
Verifying prerequisites	119

Installing the software	121
Configuring Log Analysis to use LDAP	124
Configuring Log Analysis to use single sign-on	130
Updating passwords in configuration files	133
Configuring Log Analysis to start at system start	135
Enabling the Log Analysis product key	137
Configuring Network Manager workaround	137
3 Configuring IBM Netcool Operations Insight base exercises	141
Exercise 1 Netcool/OMNIbus Insight Pack	141
Installing the Insight Pack	142
Creating the Log Analysis data source	143
Configuring Web GUI	146
Exercise 2 Message Bus Gateway	148
Configuring SSL	148
Installing the gateway	152
Configuring the ObjectServer	153
Configuring the gateway	155
Verifying the gateway operation	159
Configuring user access to the Event Search feature	163
Exercise 3 Configuring Event Analytics	169
Configuring the Related Events feature	169
Configuring seasonality	185
Loading the sample database	187
Installing Netcool/Impact policies	188
Installing updated Netcool/Impact policy	190
Exercise 4 Verifying Netcool Operations Insight features	193
Verifying Related Events	193
Verifying the Seasonal Events feature	199
Creating a seasonal event rule	204
Verifying the Event Search feature	209
4 IBM Tivoli Network Manager exercises	213
Exercise 1 Installing the SNMP probe	213
Exercise 2 Installing and configuring a topology database	222
Installing the database creation scripts	222
Creating the topology database	225
Exercise 3 Installing Tivoli Network Manager	228
Updating smadmin roles	228
Installing Network Manager core components	229
Installing Network Manager GUI components	233
Installing Network Manager Reports	237
Installing Network Health Dashboard	239
Configuring the Network Health Dashboard	242
Exercise 4 Performing postinstallation configuration	243
Configuring the Tivoli Netcool/OMNIbus Web GUI data source name	243
Configuring the core components to run as a non-root user	244
Configuring processes to start automatically	245
Adding Network Manager environment variables to the netcool user	247

Removing the ObjectServer users	247
Installing the hot fix	249
Verifying the installation	251
Exercise 5 Installing the Network Manager Insight Pack	260
Installing the Insight Pack	260
Configuring the Insight Pack	261
Modifying the ObjectServer	269
Installing the tools in Web GUI	269
Configuring the tools in Network Manager	270
5 IBM Tivoli Netcool Configuration Manager exercises	274
Exercise 1 Creating users	274
Creating the database user ID	274
Creating the FTP user ID	275
Exercise 2 Creating the database	276
Exercise 3 Installing Jazz for Service Management	279
Exercise 4 Installing Netcool Configuration Manager	289
Installing the presentation server	289
Installing the Netcool Configuration Manager GUI components	296
Installing Common Reporting reports	300
Exercise 5 Installing device drivers	303
Installing the standard device drivers	304
Installing the Smart Model device drivers	306
Installing auto-discovery	309
Exercise 6 Post-installation configuration	312
Changing passwords	312
Configuring Java Webstart	314
Configuring SNMP trap destination	322
Updating the Work Distribution resource	324
Creating resources to support device import	326
Exercise 7 Configuring integration with Tivoli Network Manager	330
Creating users and groups	330
Adding existing users to Netcool Configuration Manager groups	336
Assigning roles in Dashboard Application Services Hub	339
Configuring the presentation server to use LDAP	341
Configuring the presentation server for single sign-on	353
Configuring access rights for existing users	357
Verifying single sign-on	360
Installing sample policy packs	362
Importing sample command sets	368
Configuring integration with Netcool/OMNIbus	375
Configuring device synchronization	378
Configuring the Network Health Dashboard	379
Exercise 8 Configuring Out-of-Band Change (OOBC) daemon	380
Modifying the start script	384
Configuring auto-start	385
Verifying auto-start	386

6 Verifying Networks for Operations Insight exercises	389
Exercise 1 Starting the network simulator	389
Exercise 2 Solution verification	391
Discovering devices with Network Manager	391
Verifying integration with Configuration Manager	395
Verifying Compliance Management	400
Verifying tool launch	408



1 Netcool Operations Insight introduction and overview exercise

The exercises in this unit validate the host configuration before installing the IBM Netcool Operations Insight components.



Important: The exercise guide includes instructions at various points for deleting installation files. You must delete these files as you progress through the exercises. Otherwise, you exhaust the available disk space on the image.

Exercise 1 Validating the host1 server configuration

IBM® Netcool® Operations Insight consists of several products that are integrated into a common solution. Each of the products in the solution has system requirements that must be met before the software is installed. These requirements include such things as the following examples:

- Server disk and memory capacity
- Operating system
- System patches
- Third-party software

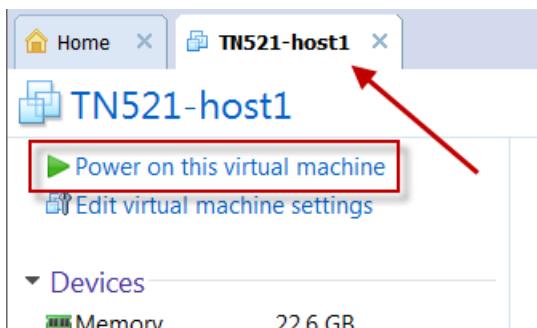
The requirements vary by operating system, and are detailed in the installation guide for the respective product.

To automate the validation process, IBM provides the *Prerequisite Scanner*. IBM Prerequisite Scanner is a stand-alone prerequisite checking tool that analyzes system environments before the installation or upgrade of a Tivoli® product or IBM solution.

Task 1 Starting the image

Depending on how this course is delivered, the host1 image might already be running. If the image is running, skip the steps for powering on the images. If the image is not running, use the following steps to start the image:

1. Locate the **TN521-host1** tab in the VMware console.
 - a. Click the **TN521-host1** tab to select it.
 - b. Click the line that is labeled **Power on this virtual machine**.

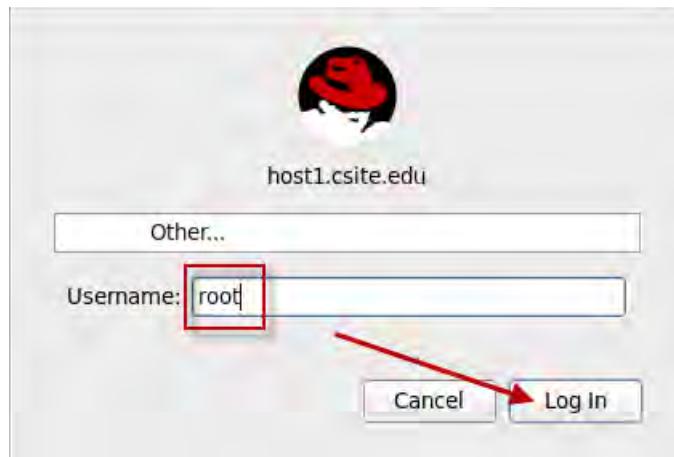


The image takes several minutes to initialize. The login screen opens when the image is available.

2. Log in as the root user:
 - a. Click **Other**.



- b. Enter **root** as the user name and click **Log In**.

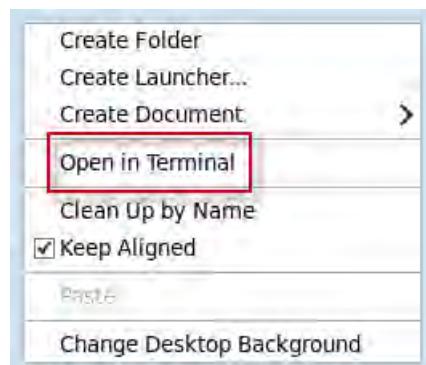


The password is **object00**.

The Linux console window opens.

3. Open a terminal window:

- Place your cursor anywhere in the console window.
- Right-click and select **Open in Terminal**.



A terminal window opens.

 Hint: Repeat the previous steps if you want more terminal windows.

Task 2 Installing the prerequisite scanner

The prerequisite scanner is not bundled with IBM Netcool Operations Insight. It is distributed as a UNIX compressed file. Perform the following steps to install the prerequisite scanner.

1. Change to the required directory:

```
cd /software/prs
```

2. Expand the compressed file:

```
tar -xvf precheck_unix_20150827.tar
```

Task 3 Running the prerequisite scanner

All Netcool Operations Insight components are installed on the host1 server in this course.



Important: In a production environment, the components are typically distributed across multiple servers.

Checking prerequisites for Netcool/OMNIbus core components

1. Change to the required directory:

```
cd /software/prs
```

2. Run the scanner to check Netcool/OMNIbus core requirements:

```
./prereq_checker.sh NOC detail
```

```
IBM Prerequisite Scanner
```

```
Version: 1.2.0.17
```

```
Build : 20150827
```

```
OS name: Linux
```

```
User name: root
```

```
.
```

```
.
```

```
.
```

```
Aggregated Properties for Scanned Products:
```

Property	Result	Found
----------	--------	-------

Expected	=====	=====
----------	-------	-------

=====	=====	=====
-------	-------	-------

/	PASS	49152.00MB
---	------	------------

910MB		
-------	--	--

Memory	PASS	6.98GB
--------	------	--------

4.00GB		
--------	--	--

Overall result: PASS (NOC 08010000: PASS)

Detailed results are also available in /tmp/prs/result.txt

The scanner presents its detailed output. Verify that all checks are flagged as PASS. The output verifies that the host system meets all of the requirements to install Netcool/OMNIbus core, desktop, and server components.

Checking prerequisites for Netcool/OMNIbus Web GUI components

1. Run the scanner to check Netcool/OMNIbus Web GUI requirements:

```
./prereq_checker.sh NOW detail
```

IBM Prerequisite Scanner

Version: 1.2.0.17

Build : 20150827

OS name: Linux

User name: root

.

.

.

Aggregated Properties for Scanned Products:

Property	Result	Found
Expected	=====	=====
=====	=====	=====
/	PASS	49152.00MB
800MB		

Overall result: PASS (NOW 08010000: PASS)

Detailed results are also available in /tmp/prs/result.txt

Checking prerequisites for Netcool/Impact components

1. Run the scanner to check Netcool/Impact requirements:

```
export IMPACT_PREREQ_BOTH=True
```

```
./prereq_checker.sh NCI detail
```

```
IBM Prerequisite Scanner
```

```
Version: 1.2.0.17
```

```
Build : 20150827
```

```
OS name: Linux
```

```
User name: root
```

```
.
```

```
.
```

```
Aggregated Properties for Scanned Products:
```

Property	Result	Found
Expected	=====	=====
=====	=====	=====
/	PASS	45.00GB
30.68GB		

```
Overall result: FAIL (NCI 07010001: FAIL)
```



Important: The scan on host1 fails due to swap space. The failure is not an issue in the classroom environment.

Checking prerequisites for Jazz for Service Management components

1. Run the scanner to check Jazz™ for Service Management requirements:

```
export JazzSM_FreshInstall=True
export Include_TCR=True
export JazzSM_TYPICAL=True
./prereq_checker.sh ODP detail
```

Overall result: PASS (ODP 01010002: PASS)

IBM Prerequisite Scanner

Version: 1.2.0.17
Build : 20150827
OS name: Linux
User name: root

.

.

.

Aggregated Properties for Scanned Products:

Property	Result	Found
<u>Expected</u>	<u>=====</u>	<u>=====</u>
<u>=====</u>	<u>=====</u>	<u>=====</u>
/	PASS	48.00GB
4.68GB		

Overall result: PASS (ODP 01010200: PASS)

Checking prerequisites for Dashboard Application Services Hub components

1. Run the scanner to check IBM Dashboard Application Services Hub requirements:

```
./prereq_checker.sh DSH detail
```

IBM Prerequisite Scanner

Version: 1.2.0.17

Build : 20150827

OS name: Linux

User name: root

.

.

.

Aggregated Properties for Scanned Products:

Property	Result	Found
<u>Expected</u>	=====	=====
=====	=====	=====
/	PASS	48.00GB
6.33GB		

Overall result: PASS (DSH 03010200: PASS)

Environment variable settings: [JazzSM_FreshInstall=True]

Detailed results are also available in /tmp/prs/result.txt

Checking prerequisites for Tivoli Common Reporting components

1. Run the scanner to check Tivoli Common Reporting requirements:

```
./prereq_checker.sh TCR detail
```

IBM Prerequisite Scanner

Version: 1.2.0.17

Build : 20150827

OS name: Linux

User name: root

.

.

.

Aggregated Properties for Scanned Products:

Property	Result	Found
Expected		
=====	=====	=====
=====		
/	PASS	48.00GB
7.50GB		

Overall result: PASS (TCR 03010200: PASS)

Checking prerequisites for IBM Operations Analytics Log Analysis components

- Run the scanner to check Log Analysis requirements:

```
./prereq_checker.sh ILA detail
```

```
IBM Prerequisite Scanner
Version: 1.2.0.17
Build : 20150827
OS name: Linux
User name: root
```

.

.

.

	FAIL	True
user.isAdmin	FAIL	True
False		
os.SELinux	PASS	Disabled
[source:Command]Disabled		
os.ksh	PASS	Available
Available		
os.package.python	PASS	python-2.6.6-52.el6.x86_64
python-2.4.3+		
os.package.unzip	PASS	unzip-6.0-1.el6.x86_64
unzip+		
os.package.sed	PASS	sed-4.2.1-10.el6.x86_64
sed+		
os.package.perl	PASS	perl-5.10.1-136.el6.x86_64
perl-5.8.8+		
network.dns	PASS	True
True		
os.ulimit	PASS	131073
[type:filedescriptorlimit]4096+,unlimited		
os.ulimit	PASS	unlimited
[type:maxmemoriesizelimit]unlimited		
os.package.libstdc++.x86_64	PASS	libstdc++-4.4.7-16.el6.x86_64
libstdc++-4.4.4-13.el6+		

Overall result: FAIL (ILA 01320000: FAIL)



Important: The scan fails because you ran the check as the root user. This failure is not an issue for the class environment.

Checking prerequisites for IBM Tivoli Network Manager components

- Run the scanner to check IBM Tivoli Network Manager requirements:



Important: An updated configuration file is provided for Network Manager V4.2. This file is not currently included with the prerequisite scanner software. The configuration file is included with this workshop.

- Copy the workshop file to the correct location.

```
cd /software/prs  
cp TNM_04200000.cfg /software/prs/UNIX_Linux
```

- Run the prerequisite checker.

```
export tnmCORE=True  
export tnmDB=True  
export tnmEvents=True  
export tnmGUI=True
```

```
./prereq_checker.sh TNM detail
```

```
IBM Prerequisite Scanner  
Version: 1.2.0.17  
Build : 20150827  
OS name: Linux  
User name: root
```

```
.
```

```
.
```

Aggregated Properties for Scanned Products:

Property	Result	Found
Expected	=====	=====
=====	=====	=====
/	FAIL	45.00GB
142.00GB		
Memory	PASS	17.69GB
2.00-8.00GB		

Overall result: FAIL (TNM 04200000: FAIL)



Important: The scan fails due to available disk space. This failure is not an issue for the class environment.

Checking prerequisites for Netcool Configuration Manager components

At the time that this class was created, an updated prerequisite check for Netcool Configuration Manager 6.4.2 did not exist.

Task 4 Verifying the user environment

The software is installed as the **netcool** user. The **netcool** user belongs to the ncoadmin group. To facilitate the workshop, the **netcool** user and the ncoadmin group are already created.

1. Examine the **ncoadmin** group:

```
more /etc/group | grep ncoadmin
```

```
ncoadmin:x:501:
```

The ncoadmin group is a requirement of Netcool/OMNIbus Process Activity. The group ID number (GID) is not important. Only the name ncoadmin is important.

2. Examine the **netcool** user:

```
more /etc/passwd | grep netcool
```

```
netcool:x:500:501::/home/netcool:/bin/bash
```

The **netcool** user does not possess any special authority or privileges. The only unique characteristic is that the user is a member of the ncoadmin group.

3. Verify the target directory as follows:

```
cd /opt  
ls -la  
drwxr-xr-x  6 netcool ncoadmin 4096 Oct 21 18:04 IBM
```

The directory exists and the **netcool** user owns it.

The following list is a summary of the accomplishments from this unit:

- Started images
- Verified system prerequisites



2 Installing IBM Netcool Operations Insight base exercises

In this unit, you learn how to install the Netcool Operations Insight base components.

Exercise 1 DB2

DB2® is a requirement for several components, including the Netcool/OMNIbus event archive and Tivoli Common Reporting report store databases.

Installing DB2



Important: You are currently the root user. You must install DB2 as the root user.

1. Expand the installation software.

```
cd /software/db2  
gunzip DB2_Svr_10.5.0.3_Linux_x86-64.tar.gz  
tar -xvf DB2_Svr_10.5.0.3_Linux_x86-64.tar
```

2. Install DB2 with the setup wizard.

```
cd server  
. ./db2setup
```

The setup wizard is a graphical utility. The following instructions do not contain all of the screen captures of the wizard.



Important: It takes several minutes for the launchpad to open.

- Select **Install a Product**, scroll down, and select **Install New**.



- Click Next.**
- Accept the license agreement and click Next.**
- Leave the option set to Typical and click Next.**
- Leave the option set to Install DB2 Server Edition and save my settings in response file, and click Next.**
- Retain the default installation directory and click Next.**
- Accept the default information to create the DAS admin user, type in the password: **object00**, and click Next.**

<input checked="" type="radio"/> New user	
User name	dasusr1
UID	
Group name	dasadm1
GID	
Password	***** (highlighted with a red box)
Confirm password	***** (highlighted with a blue box)
Home directory	/home/dasusr1

- Retain the option to create an instance and click Next.**
- Retain the option to create a single partition and click Next.**

- j. Retain the default to create a DB2 instance owner, type in the password **object00**, and click **Next**.

<input checked="" type="radio"/> New user	User name	db2inst1
	UID	
	Group name	db2iadm1
	GID	
	Password	***** *****
	Confirm password	***** *****
	Home directory	/home/db2inst1

- k. Retain the default information for the **db2 fenced** user, type in the password **object00**, and click **Next**.

<input checked="" type="radio"/> New user	User name	db2fenc1
	UID	
	Group name	db2fadm1
	GID	
	Password	***** *****
	Confirm password	***** *****
	Home directory	/home/db2fenc1

- l. Select the option **Do not set up your DB2 server to send notifications at this time** and click **Next**.



- m. Review the settings and click **Finish**.

The installation starts and a window displays the progress.



Note: The installation runs for approximately ten minutes.

The installation completes and a window displays the status of the setup.

- n. Click **Finish** to exit the setup wizard.

Configuring DB2 to start at system start

Several ways exist to configure DB2 to start at system start time. The following steps use a start script in /etc/init.d.

1. Configure DB2 to automatically start:

- a. Copy the supplied start script:

```
cd /workshop/etc/init.d  
cp db2_tcr /etc/init.d
```

- b. Change the file permissions to allow execution:

```
cd /etc/init.d  
chmod +x db2_tcr
```

- c. Create the logical links to enable the autostart feature:

```
chkconfig db2_tcr on
```

2. Verify DB2 autostart:

- a. Stop DB2.

```
/etc/init.d/db2_tcr stop
```

- b. Start DB2.

```
/etc/init.d/db2_tcr start
```

- c. Change to the **db2inst1** user.

```
su - db2inst1
```

- d. Attempt to start DB2 by entering the following command:

```
db2start
```

SQL1026N The database manager is already active.

This message verifies that the DB2 instance is running.



Important: The **db2start** command must return the message that indicates that DB2 is already running. If this message is not returned, and the command starts DB2, it means that the autostart feature is not configured correctly. Return to the previous section and verify the steps.

Installing the DB2 license file

The copy of DB2 that is provided with Netcool/OMNIbus is a restricted version with a limited license. The software includes a license file that is used to extend the expiration date.



Important: You are currently the **db2inst1** user.

1. Expand the license installation files.

```
cd /tmp
```

```
mkdir db2
```

```
cd db2
```

```
unzip /software/db2/DB2_ESE_Restricted_QS_Act_10.5.0.1.zip
```

2. Install the license file as the **db2inst1** user.

```
cd /tmp/db2/ese_o/db2/license
```

```
db2licm -a db2ese_o.lic
```

```
LIC1402I License added successfully.
```

```
LIC1426I This product is now licensed for use as outlined in your License  
Agreement. USE OF THE PRODUCT CONSTITUTES ACCEPTANCE OF THE TERMS OF THE IBM  
LICENSE AGREEMENT, LOCATED IN THE FOLLOWING DIRECTORY:  
"/opt/ibm/db2/V10.5/license/en_US.iso88591"
```

3. Verify the license information.

```
db2licm -l
```

Product name:	"DB2 Enterprise Server Edition"
License type:	"Restricted"
Expiry date:	"Permanent"
Product identifier:	"db2ese"
Version information:	"10.5"

4. Remove the DB2 installation files:

- a. Exit the **db2inst1** user back to the root user.

```
exit
```

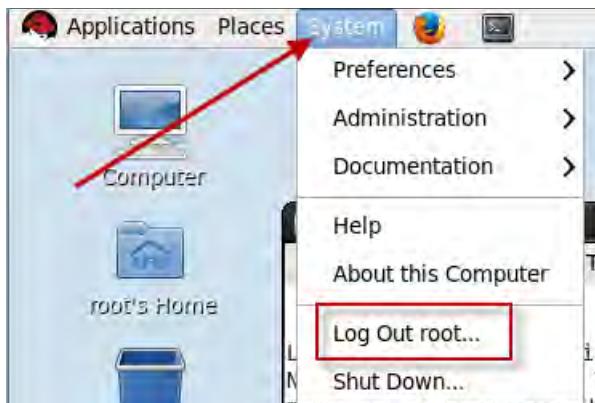
- b. Remove the DB2 installation files:

```
cd /software  
/bin/rm -R db2
```

- c. Remove the license files.

```
cd /tmp  
/bin/rm -R db2
```

5. Log out of the image as the root user.
 - a. Click **System**, and select **Log Out root**.



- b. Click **Log Out**.



Exercise 2 Netcool/OMNIbus core

Installing IBM Installation Manager

1. Log in as the **netcool** user with password **object00**.

The Linux console window opens.

2. Open a terminal window:

3. Configure environment variables:

```
cd /workshop/netcool
```

```
cat .bashrc >> /home/netcool/.bashrc
```

```
source /home/netcool/.bashrc
```

4. Verify environment variables:

```
env | grep IBM
```

```
PATH=/opt/IBM/tivoli/netcool/bin:/opt/IBM/tivoli/netcool/omnibus/bin:/opt/IBM/tivoli/netcool/omnibus/probes:/usr/lib64/qt-3.3/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin:/home/netcool/bin
NCHOME=/opt/IBM/tivoli/netcool
OMNIHOME=/opt/IBM/tivoli/netcool/omnibus
```

The following steps demonstrate how to install IBM Installation Manager, and use IBM Installation Manager to install Netcool/OMNIbus.



Note: The other option available is to use an installation utility that is bundled with the Netcool/OMNIbus installation files. The utility installs the version of IBM Installation Manager that is bundled with Netcool/OMNIbus. However, that version is old.

5. Expand the installation file as follows:

```
cd /software/iim
```

```
unzip agent.installer.linux.gtk.x86_64_1.8.4000.20151125_0201.zip
```

6. Install IBM Installation Manager as follows:

```
./userinst
```

a. Verify that the IBM Installation Manager package is selected for installation and click **Next**.

Installation Packages	Status	Vendor
IBM® Installation Manager	Will be installed	IBM
Version 1.8.4	Will be installed	IBM

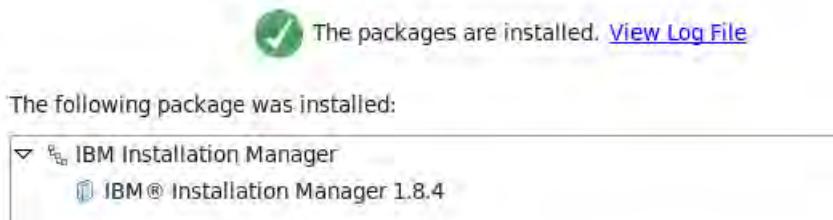
b. Accept the license agreement and click **Next**.

c. Leave the default location for Installation Manager, and click **Next**.

Installation Manager Directory:

d. Review the installation summary and click **Install**.

- e. Verify that the installation is successful. Click **Restart Installation Manager**.



IBM Installation Manager stops and restarts.

- f. Click **File** and select **Exit** to close IBM Installation Manager.

7. Remove the installation files.

```
cd /software
/bin/rm -R iim
```

Installing Netcool/OMNIbus core

In this exercise, you install the Netcool/OMNIbus core components. You install all of Netcool/OMNIbus core on a single server, which is not typically done in a production environment.

1. Expand the installation file as follows:

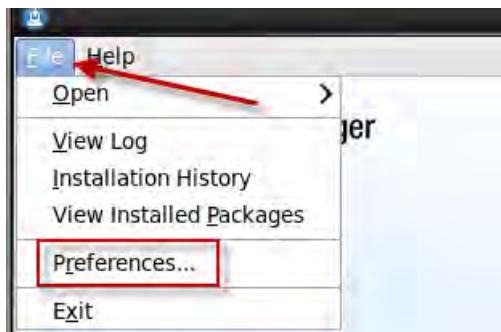
```
cd /software/omnibus
```

```
unzip OMNIbus-v8.1.0.5-Core.linux64.zip
```

2. Install the software:

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

- a. Click **File** and select **Preferences**.

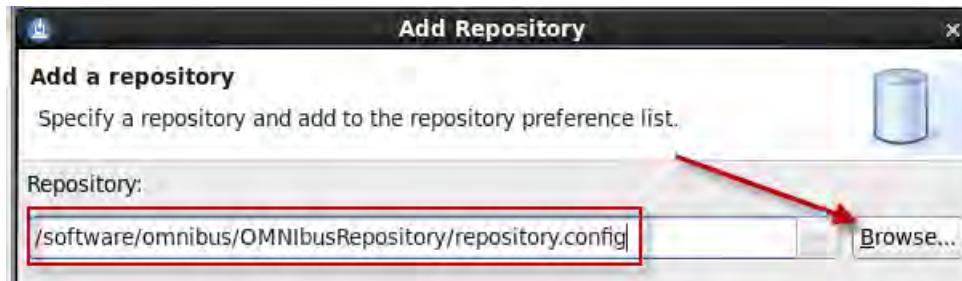


- b. Click **Add Repository**.



- c. Click **Browse** and locate the following file:

/software/omnibus/OMNIbusRepository/repository.config



- d. Click **OK** to add the repository.

- e. Verify that the repository is listed and click **OK**.



- f. Click **Install**.



- g. Select the Netcool/OMNIbus package and click **Next**.

Installation Packages	Status	Vendor
<input checked="" type="checkbox"/> IBM Tivoli Netcool/OMNIbus		
<input checked="" type="checkbox"/> Version 8.1.0.5	Will be installed	IBM

- h. Accept the license agreement and click **Next**.

- i. Leave the default directory location for Installation Manager, and click **Next**.

Shared Resources Directory: /home/netcool/IBM/IBMIMShared

- j. Leave the option set to create a new package group.

- k. Leave the default installation directory, and click **Next**.

Package Group Name: IBM Tivoli Netcool OMNIbus

Installation Directory: /opt/IBM/tivoli/netcool

Architecture Selection: 32-bit 64-bit

- I. Leave all of the features selected, and click **Next**.
- m. Leave the option for **Data migration** cleared, and click **Next**.



Hint: The option is used when you upgrade from a previous version of Netcool/OMNIBus.

- n. Review the installation summary and click **Install**.



Hint: An installation on most servers runs approximately 10 minutes.

- o. Leave the option selected to run the configuration wizard and click **Finish**.



- p. Verify that the installation is successful.
- q. Click **Finish** to exit the installation wizard.

Creating the ObjectServer

At the conclusion of the installation process, the installation wizard starts automatically.



Hint: You start the configuration wizard manually with the following command:

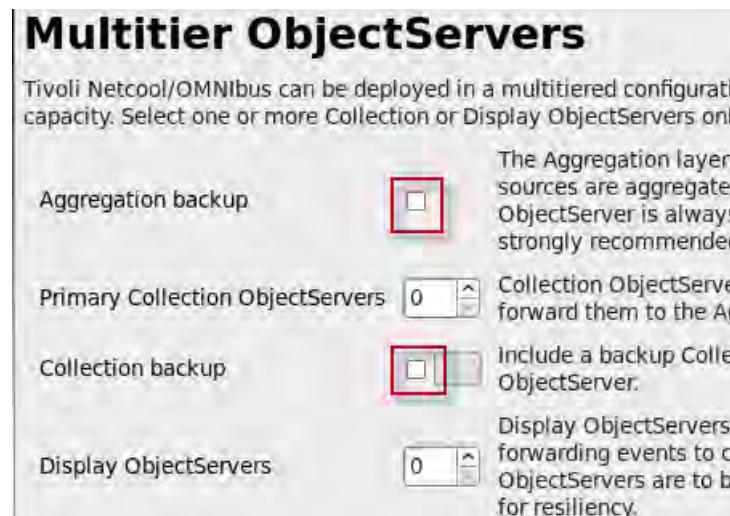
```
/opt/IBM/tivoli/netcool/omnibus/bin/nco_icw
```

1. Complete the configuration with the wizard as follows:

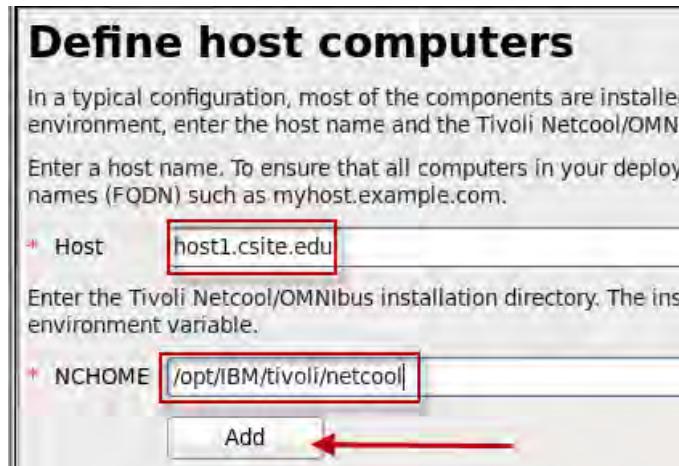
- a. Scroll to the bottom of the view and click **Next**.



- b. Leave the option selected to create a new configuration and click **Next**.
- c. Clear the check for **Aggregation backup** and clear the check for **Collection backup**. Click **Next**.



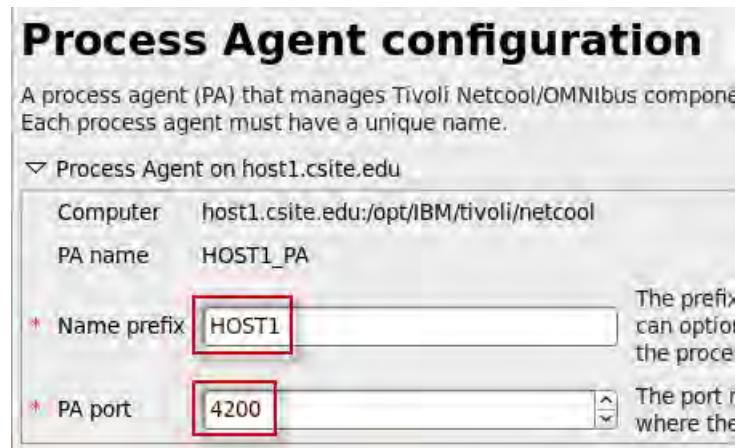
- d. Enter **host1.csite.edu** and **/opt/IBM/tivoli/netcool**. Click **Add**.



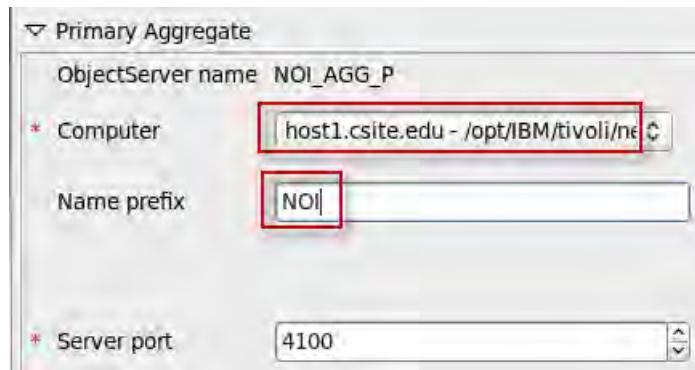
- e. Verify that the entry looks like this example and click **Next**.

host1.csite.edu - /opt/IBM/tivoli/netcool

- f. Verify that the settings for Process Agents look like this example and click **Next**.

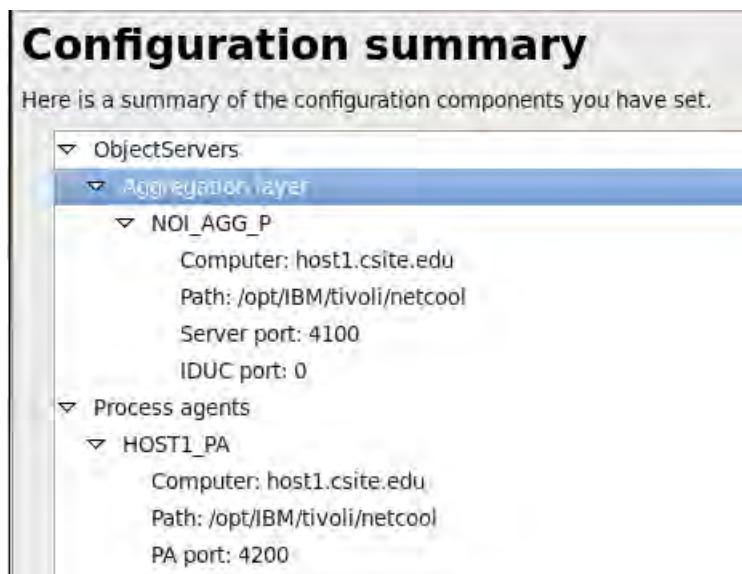


- g. Select **host1.csite.edu** for Computer and enter **NOI** in the **Name prefix** field.



The primary ObjectServer name is set to AGG_P and cannot be changed. You can enter text in the **Name prefix** field, and that text adds a prefix to AGG_P. In this example, the ObjectServer name is NOI_AGG_P.

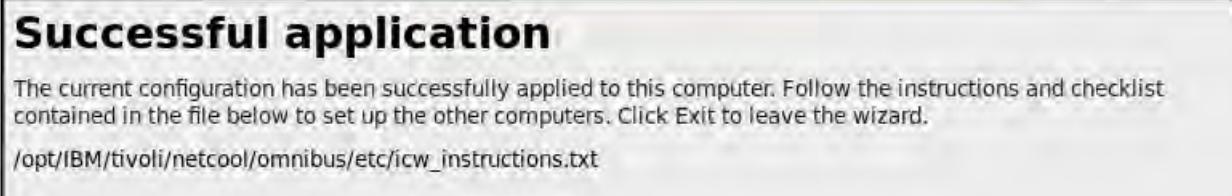
- h. Scroll down in the view and click **Next**.
- i. Review the configuration summary and click **Next**.



- j. Click **Next**.
- k. Click **Next** to apply the configuration.



- l. Verify that the configuration is successfully applied and click **Exit**.



The configuration is applied to the system.

- m. Click **File** and select **Exit** to close IBM Installation Manager.

2. Remove the Netcool/OMNIbus core installation files.

```
cd /software  
/bin/rm -R omnibus
```

Verifying the initial configuration

The wizard creates the process agent configuration file. The wizard assumes that the processes under the control of the process agent are run as the root user. Most users want to limit the processes that run as root. In the next step, you modify the configuration file to run the ObjectServer as the **netcool** user.

1. Determine the UID value of the **netcool** user.

```
more /etc/passwd | grep netcool
```

```
netcool:x:501:501::/home/netcool:/bin/bash
```

In this example, the UID for the **netcool** user is 501.

2. Modify the process activity configuration file:

```
cd /opt/IBM/tivoli/netcool/omnibus/etc  
gedit nco_pa.conf
```

- a. Locate the following line:

```
Command '$OMNIHOME/bin/nco_objserv -name NOI_AGG_P -pa HOST1_PA' run as 0
```

- b. Change run as 0 to run as 501.

```
Command '$OMNIHOME/bin/nco_objserv -name NOI_AGG_P -pa HOST1_PA' run as 501
```

- c. Save the changes and exit gedit.

3. Start the process agent:

```
nco_pad -name HOST1_PA
```



Hint: The directory is not required because the PATH environment variable contains this path:

```
/opt/IBM/tivoli/netcool/omnibus/bin
```

4. Verify that the ObjectServer is running:

```
nco_ping NOI_AGG_P
```

```
NCO_PING: Server available.
```

Verifying basic ObjectServer function

You can set up the Simnet probe, to automatically generate incidents to simulate network events. The probe provides a convenient mechanism for verifying basic ObjectServer functions.



Important: The Simnet probe is bundled with Netcool/OMNibus. You must install all other probes individually.

1. Start the probe, and send events to the NOI_AGG_P ObjectServer as follows:

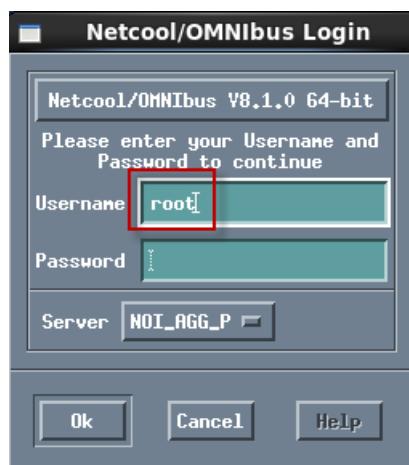
```
nco_p_simnet -server NOI_AGG_P &
```

2. Examine the simulated events.

- a. Start the native event list:

```
nco_event &
```

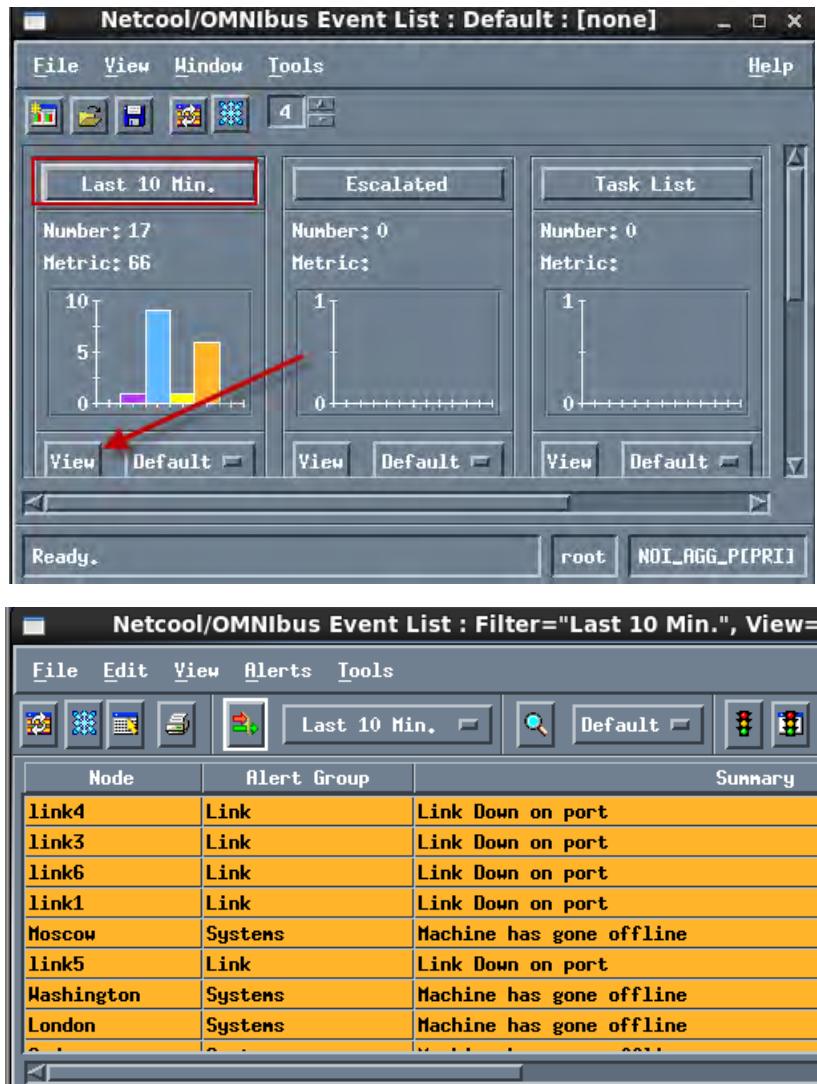
- b. Connect to the NOI_AGG_P ObjectServer as the root user, with no password.



- c. Click **OK**.

The **Event List** window opens.

- d. Locate the box that is labeled **Last 10 Mins.**, and click **View**:



The Sub-Event List view opens. The Simnet probe generates the events in this view. These steps verify that the ObjectServer is active, the Simnet probe can connect, and the ObjectServer generates events that are based on data that is provided by the probe.

- e. Click **File > Close** to close the Sub-Event List window.
 f. Click **File > Exit** to close the Event List window.
 g. Click **Yes** to abandon the changes.

Adding a password to the root ObjectServer user

When an ObjectServer is created, the root user is defined with no password. The following steps use a command-line utility to add a password to that user.

1. Add a password to the NOI_AGG_P root user as follows.

- a. Connect to the ObjectServer with the nco_sql utility:

```
nco_sql -server NOI_AGG_P -user root -password ''
```



Important: The value for password in the command that is shown is *two single quotation marks* (' '). This syntax indicates a *blank* password.

- b. Enter the following commands that are shown in bold text:

```
1> alter user 'root' set password 'object00';
2> go
(0 rows affected)
1> quit
```

The password for the root user is now **object00** on the NOI_AGG_P ObjectServer.

- c. Verify that the password is correct:

```
nco_sql -server NOI_AGG_P -user root -password 'object00'

1> quit
```

The prompt characters (1>) indicate that the utility is able to connect to the ObjectServer with the revised password. Enter quit to exit the utility.

Configuring event archiving

An event archive database is a requirement for event analytics. In this section, you create the event archive database and install the JDBC gateway.

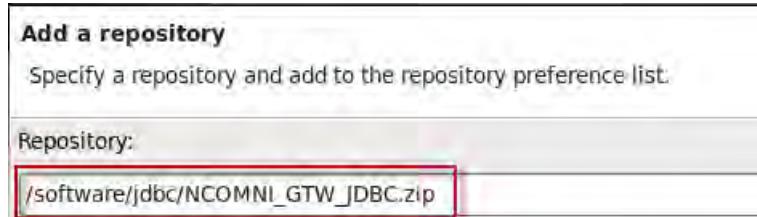
1. Install the gateway components.

- a. Start IBM Installation Manager:

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

- b. Add the gateway installation compressed file as a repository:

/software/jdbc/NCOMNI_GTW_JDBC.zip



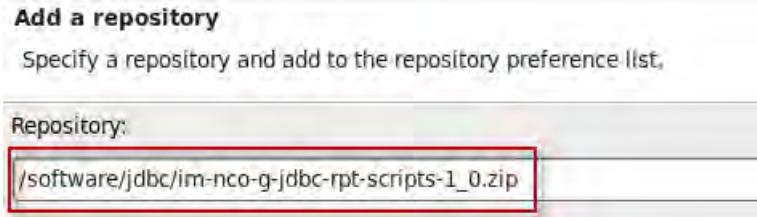
- c. Click **OK** to add the repository.



Note: It is not necessary to expand the compressed file.

- d. Add the gateway scripts installation compressed file as a repository:

/software/jdbc/im-nco-g-jdbc-rpt-scripts-1_0.zip



- e. Clear the check marks for the Netcool/OMNIbus repository.

Repositories:	
Location	Connection
<input checked="" type="checkbox"/> /software/omnibus/OMNIbusRepository/repository.config	?
<input checked="" type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	?
<input checked="" type="checkbox"/> /software/jdbc/im-nco-g-jdbc-rpt-scripts-1_0.zip	?



Hint: You removed the files at the end of the previous step. If you do not remove the check marks, you receive a warning message that the files are missing.

- f. Verify that the repositories are listed and click **OK**.

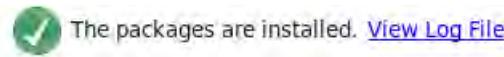
Repositories:	
Location	Connect
<input type="checkbox"/> /software/omnibus/OMNIbusRepository/repository.config	?
<input checked="" type="checkbox"/> /software/omnibus/fb2/OMNIbusRepository/composite/repository.config	?
<input checked="" type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	?
<input checked="" type="checkbox"/> /software/jdbc/im-nco-g-jdbc-rpt-scripts-1_0.zip	?

- g. Click **Install**.

- h. Select the two packages to install and click **Next**.

Installation Packages	Status	Vendor
Netcool/OMNibus Gateway nco-g-jdbc Version 1.6.0.0	Will be installed	IBM
Netcool/OMNibus Gateway nco-g-jdbc-reporting-scripts Version 1.1.0.0	Will be installed	IBM

- i. Accept the license agreement and click **Next**.
- j. Leave the option selected to use the existing package group and click **Next**.
- k. Leave the features selected and click **Next**.
- l. Review the installation summary and click **Install**.
- m. Verify that the installation is successful and click **Finish**.



The following packages were installed:

IBM Tivoli Netcool OMNibus
Netcool/OMNibus Gateway nco-g-jdbc 1.6.0.0
Netcool/OMNibus Gateway nco-g-jdbc-reporting-scripts 1.1.0.0

- n. Click **File** and select **Exit** to close IBM Installation Manager.
2. Create the DB2 structure.

DB2 is running as the **db2inst1** user. You must use this user to create the database structure.

- a. Change to the **db2inst1** user:

```
su - db2inst1
Password: object00
```

- b. Change to the required directory:

```
cd /opt/IBM/tivoli/netcool/omnibus/gates/reporting/db2
```



Hint: The *reporting* directory is created when the gateway package is installed.

- c. Import the SQL file:

```
db2 -td@ -vf db2.reporting.old.sql
```



Note: This command runs for several minutes.

```

.
.
.

COMMIT WORK

DB20000I  The SQL command completed successfully.
```

3. Verify the DB2 structure.

The SQL file creates a database (REPORTER), and numerous tables.

a. Connect to the REPORTER database:

```
db2 connect to reporter
```

Database Connection Information

```

Database server      = DB2/LINUXX8664 10.5.3
SQL authorization ID = DB2INST1
Local database alias = REPORTER
```



Hint: DB2 is not case-sensitive. You can use uppercase or lowercase characters for any DB2 object.

b. Verify the table structure:

```
db2 list tables
```

Table/View	Schema	Type	Creation time
REPORTER_CLASSES	DB2INST1	T	2014-10-01-17.54.12.151628
REPORTER_CONVERSIONS	DB2INST1	T	2014-10-01-17.54.12.268367
REPORTER_DETAILS	DB2INST1	T	2014-10-01-17.54.09.595508
REPORTER_GROUPS	DB2INST1	T	2014-10-01-17.54.11.970445
REPORTER_JOURNAL	DB2INST1	T	2014-10-01-17.54.10.911528
REPORTER_MEMBERS	DB2INST1	T	2014-10-01-17.54.12.073987
REPORTER_NAMES	DB2INST1	T	2014-10-01-17.54.11.828164
REPORTER_STATUS	DB2INST1	T	2014-10-01-17.54.11.121974
REP_AUDIT	DB2INST1	V	2014-10-01-17.54.13.372712
REP_AUDIT_ACK	DB2INST1	T	2014-10-01-17.54.11.630816
REP_AUDIT_OWNERRID	DB2INST1	T	2014-10-01-17.54.11.415751
REP_AUDIT_OWNERUID	DB2INST1	T	2014-10-01-17.54.11.339441
REP_AUDIT_SEVERITY	DB2INST1	T	2014-10-01-17.54.11.499096
REP_REFERENCE_DATE	DB2INST1	V	2014-10-01-17.54.13.125819
REP_SEVERITY_TYPES	DB2INST1	T	2014-10-01-17.54.12.414987
REP_TIME_PERIODS	DB2INST1	T	2014-10-01-17.54.12.629815
STATUS_VW	DB2INST1	V	2014-10-01-17.54.13.319413

17 record(s) selected.

c. Verify that 17 tables and views are created.

- d. Exit the **db2inst1** user to return to the **netcool** user.

```
exit
```



Important: Make sure that you are the **netcool** user before proceeding.

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

The gateway must have a name. For this exercise, use **JDBC_GATE**. You must add that name to the Netcool/OMNIbus communications file.

- a. Run the **Server Editor** utility:

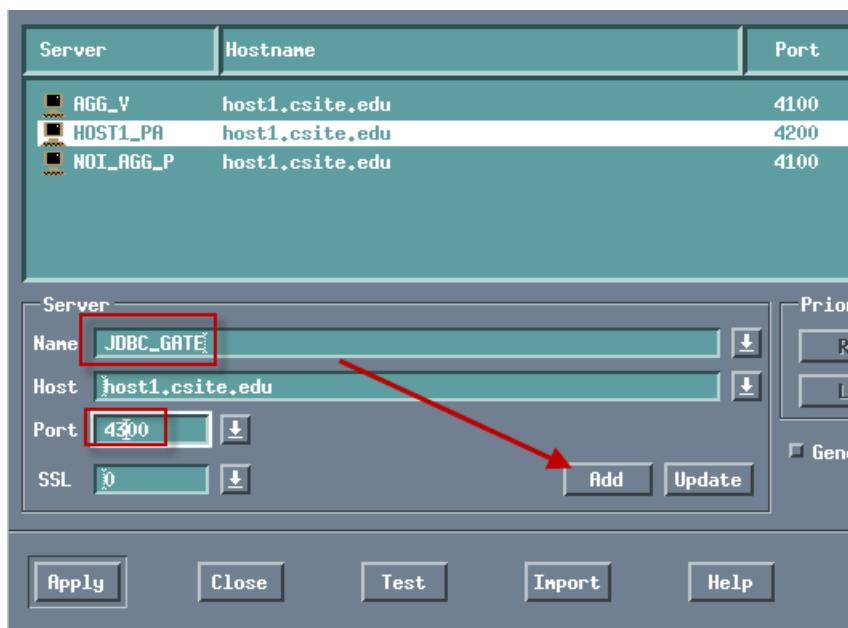
```
nco_xigen &
```

- b. Click the entry **HOST1_PA** to select it.

- c. Change the Name to **JDBC_GATE**.

- d. Change the Port to **4300**.

- e. Click **Add**.



Important: Make sure that you click **Add** because you want to create a new entry. If you click **Update**, you *change* the entry for HOST1_PA to JDBC_GATE.

- f. Verify that the entry for JDBC_GATE is listed. Click **Apply** and click **Close**.

Server	Hostname	Port
AGG_V	host1.csuite.edu	4100
NOCT1_P0	host1.csuite.edu	4200
JDBC_GATE	host1.csuite.edu	4300
NOT_AGG_P	host1.csuite.edu	4100

5. Configure the gateway.

The gateway is configured with several text files. The installation process creates these files in a specific directory. Copy the default files from that location to **\$OMNIHOME/etc**, and rename the files to include the gateway name, JDBC_GATE.

- a. Change to the required directory:

```
cd $OMNIHOME/gates/jdbc
```

- b. Copy and rename the files:

```
cp reporting.jdbc.map $OMNIHOME/etc/JDBC_GATE.map
cp reporting.G_JDBC.props $OMNIHOME/etc/JDBC_GATE.props
cp jdbc.rdrwtr.tblrep.def $OMNIHOME/etc/JDBC_GATE.rdrwtr.tblrep.def
cp jdbc.startup.cmd $OMNIHOME/etc/JDBC_GATE.startup.cmd
```

- c. Verify that the files are correctly renamed:

```
cd $OMNIHOME/etc
ls -1 JDBC_GATE.*
```

JDBC_GATE.map
JDBC_GATE.props
JDBC_GATE.rdrwtr.tblrep.def
JDBC_GATE.startup.cmd

- d. Modify the property file.

You must modify the property file to define things like ObjectServer name, DB2 database user, and the password for that user.



Hint: When modifying the file, be sure to place all changes on the end of the file.

- i. Enter the following command to begin editing the file:

```
gedit JDBC_GATE.props
```

- ii. Scroll to the bottom of the file. Numerous properties values are already defined. Some of the property values must be modified, and more lines must be added.

iii. Modify the following *existing* lines as shown:

```
# JDBC Connection properties
Gate.Jdbc.Driver: 'com.ibm.db2.jcc.DB2Driver' # STRING (JDBC Driver)
Gate.Jdbc.Url: 'jdbc:db2://host1.csite.edu:50000/reporter' # STRING (JDBC connection URL)
Gate.Jdbc.Username: 'db2inst1' # STRING (JDBC username)
Gate.Jdbc.Password: 'object00' # STRING (JDBC password)
Gate.Jdbc.ReconnectTimeout: 30 # INTEGER (JDBC database reconnection timeout)
Gate.Jdbc.InitializationString: '' # STRING (JDBC connection initialization string)
```

iv. Comment out the following two *existing* lines:

```
# ObjectServer Connection properties
#Gate.RdrWtr.Username: 'root' # STRING ([RdrWtr] Name of the user to connect as.)
#Gate.RdrWtr.Password: '' # STRING ([RdrWtr] Password of the user to connect as.)
```

An ObjectServer user name and password is required only if the ObjectServer is running in secure mode.

v. Add the following lines:

```
# New lines
# Log file name
MessageLog : '$OMNIHOME/log/JDBC_GATE.log'
# Gateway name
Name : 'JDBC_GATE'
# Property file name
PropsFile : '$OMNIHOME/etc/JDBC_GATE.props'
# Map file name
Gate.MapFile : '$OMNIHOME/etc/JDBC_GATE.map'
# Name of ObjectServer
Gate.RdrWtr.Server : 'NOI_001_P'
# Table replication file name
Gate.RdrWtr.TblRepDefFile :
'$OMNIHOME/etc/JDBC_GATE.rdrwtr.tblrep.def'
# Startup command file name
Gate.StartupCmdFile : '$OMNIHOME/etc/JDBC_GATE.startup.cmd'
# Description name - this value appears in the list of ObjectServer connections
Gate.RdrWtr.Description : 'JDBC Gateway'
```



Hint: Each of the new property statements is in the upper part of the file. You can copy the property value from the top of the file and paste the line. Remove the comment character, and modify the value.

e. Save the changes and exit the gedit utility.

f. Modify the startup command file.

i. Enter the following command:

```
gedit JDBC_GATE.startup.cmd
```

ii. Remove the comment character (#) from the beginning of each TRANSFER command as follows:

```
TRANSFER FROM 'alerts.conversions' TO 'REPORTER_CONVERSIONS' DELETE USING
TRANSFER_MAP ConversionsMap;
TRANSFER FROM 'alerts.objclass' TO 'REPORTER_CLASSES' DELETE USING
TRANSFER_MAP ObjectClassesMap;
TRANSFER FROM 'master.groups' TO 'REPORTER_GROUPS' DELETE USING
TRANSFER_MAP GroupsMap;
TRANSFER FROM 'master.members' TO 'REPORTER_MEMBERS' DELETE USING
TRANSFER_MAP MembersMap;
TRANSFER FROM 'master.names' TO 'REPORTER_NAMES' DELETE USING
TRANSFER_MAP NamesMap;
```

g. Save the changes and exit the gedit utility.

6. Install the DB2 JDBC driver files.

```
cd /opt/ibm/db2/V10.5/java
cp db2jcc.jar $OMNIHOME/gates/java
cp db2jcc_license_cu.jar $OMNIHOME/gates/java
```

7. Start the gateway.

```
nco_g_jdbc -name JDBC_GATE &
```

Wait a short time, and verify that the gateway is running. If the gateway fails, examine the log file for issues:

```
more $OMNIHOME/log/JDBC_GATE.log
```



Hint: One of the primary reasons for the gateway to fail to start is an issue with the DB2 connection information. If the gateway fails to start, examine the gateway property file, and verify the host name, port number, user name, and password.

8. Verify gateway operation.

If the gateway is functioning correctly, the REPORTER database contains data.

- Change to the **db2inst1** user:

```
su - db2inst1
Password: object00
```

- Connect to the REPORTER database:

```
db2 connect to reporter
```

- Examine the event archive table:

```
db2 select node from reporter_status
```

```
NODE
```

```
host2.tivoli.edu
host2.tivoli.edu
host2.tivoli.edu
host1
host1
host2.tivoli.edu
host1
host1
host1
host1
```

The values that are shown for NODE indicate that the gateway is archiving event records to DB2.

- Examine the alternative tables.

Verify that the following commands return data:

```
db2 select name from reporter_classes
db2 select column_name from reporter_conversions
db2 select name from reporter_names
db2 select name from reporter_groups
db2 select owneruid from reporter_members
```

These tables are all populated when the gateway starts. Data in these tables indicates that the gateway startup command file is correct.

- Exit the **db2inst1** user to return to the **netcool** user.

```
exit
```

9. Stop the gateway.

- Find the PID of the running event gateway:

```
ps -ef | grep jdbc
netcool 15861 4777 1 14:38 pts/1    00:00:04
/opt/IBM/tivoli/netcool/omnibus/platform/linux2x86/bin64/nco_g_jdbc -name
JDBC_GATE
```

- b. Find the PID of the running event gateway:

```
kill -9 15861
```

10. Add the gateway to process activity.

- a. Change to the target directory:

```
cd $OMNIHOME/etc
```

- b. Modify the process activity configuration file.

```
gedit nco_pa.conf
```

- c. Add the following lines to the process section:

```
nco_process 'ArchiveGateway'  
{  
    Command '$OMNIHOME/bin/nco_g_jdbc -name JDBC_GATE' run as 501  
    Host='host1.csite.edu'  
    Managed=True  
    RestartMsg='${NAME} running as ${EUID} has been restored on ${HOST}.'  
    AlertMsg='${NAME} running as ${EUID} has died on ${HOST}.'  
    RetryCount=0  
    ProcessType=PaPA_AWARE  
}
```

- d. Add the following line to the service section:

```
process 'ArchiveGateway' 20
```

- e. Save the changes and exit the gedit utility.

11. Stop process activity.

```
nco_pa_shutdown -server HOST1_PA -password object00  
Connected To PA Server [HOST1_PA] Shutdown Options :-
```

- 1) Shutdown Server leaving managed processes running.
- 2) Shutdown Server and stop all managed processes.
- 3) Exit shutdown interface.

Select Option [1-3]

Enter 2.

12. Start process activity:

```
nco_pad -name HOST1_PA
```

13. Verify process status:

```
nco_pa_status -server HOST1_PA -password object00
```

Service Name	Process Name	Hostname	User	Status	PID
Core	MasterObjectServer	host1.csuite.edunetcool	object00	RUNNING	14164
	ArchiveGateway	host1.csuite.edunetcool	object00	RUNNING	14273



Important: The gateway is configured with a 20-second delay. You might have to run the status command a few times before the gateway shows as running.

14. Remove the installation files:

```
cd /software  
/bin/rm -R jdbc
```

Configuring Netcool/OMNibus to start at system start

Several ways exist to configure Netcool process activity to start at system start time. The following steps use a start script in /etc/init.d.

1. Configure process activity to auto-start:

- a. Change to the root user.

```
su -  
Password: object00
```

- b. Copy the supplied start script:

```
cd /workshop/etc/init.d  
cp nco /etc/init.d
```

- c. Change the file permissions to allow execution:

```
cd /etc/init.d  
chmod +x nco
```

- d. Create the logical links to enable auto-start:

```
chkconfig nco on
```

2. Verify the autostart feature by restarting the image:

- a. Stop the process control agent.

```
/etc/init.d/nco stop
```

- b. Start the process control agent.

```
/etc/init.d/nco start
```

- c. Exit the root user back to the netcool user.

```
exit
```

- 3. Verify the status of process activity.

```
nco_pa_status -server HOST1_PA -password object00
```

Service Name	Process Name	Hostname	User	Status	PID
Core	MasterObjectServer	host1.tivoli.edunetcool		RUNNING	2191
	ArchiveGateway	host1.tivoli.edunetcool		RUNNING	2532

The ObjectServer and database gateway are running.

Exercise 3 Netcool/OMNIbus Web GUI

Installing Jazz for Service Management

In this step, you install Jazz for Service Management, WebSphere Application Server, Dashboard Application Services Hub, and Tivoli Common Reporting.



Important: A known issue exists when you install Tivoli Common Reporting as a non-root user. The issue and workaround are documented in the following technote.

<http://www-01.ibm.com/support/docview.wss?uid=swg21902346>

1. Set up the Tivoli Common Reporting installation work-around:

- a. Change to the root user.

```
su -
Password: object00
```

- b. Add the **netcool** user to the db2iadm1 group.

```
usermod -a -G db2iadm1 netcool
```

- c. Exit the root user.

```
exit
```

2. Create a directory to hold the Jazz for Service Management installation files:

```
mkdir /tmp/jazz_install
```

3. Expand the Jazz installation file into the target directory:

```
cd /tmp/jazz_install
unzip /software/jazz/JAZZ_FOR_SM_1.1.2.1_FOR_LNX.zip
```

4. Create a directory to hold the WebSphere installation files:

```
mkdir /tmp/was_install
```

5. Expand the WebSphere installation file into the target directory:

```
cd /tmp/was_install  
unzip /software/jazz/WAS_FOR_LINUX.zip
```

6. Create a directory to hold the Tivoli Common Reporting installation files:

```
mkdir /tmp/tcr_install
```

7. Expand the Tivoli Common Reporting installation file into the target directory:

```
cd /tmp/tcr_install  
gunzip /software/tcr/ITCR_3.1.2.1_FOR_LINUX.tar.gz  
tar -xvf /software/tcr/ITCR_3.1.2.1_FOR_LINUX.tar
```

8. Start IBM Installation Manager:

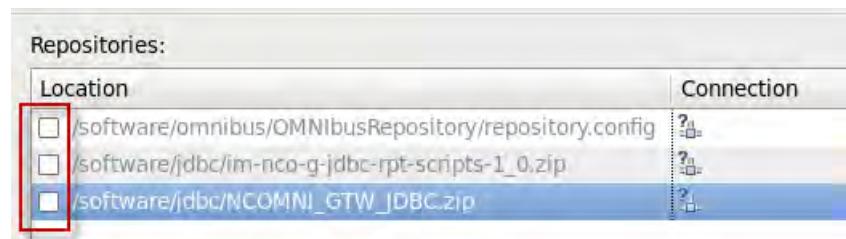
```
cd /home/netcool/IBM/InstallationManager/eclipse  
. ./IBMMIM
```

IBM Installation Manager opens.

9. Define the Jazz for Service Management repository.

a. Click **File** and select **Preferences**. Select **Repositories**.

b. Remove the check marks from the existing entries.

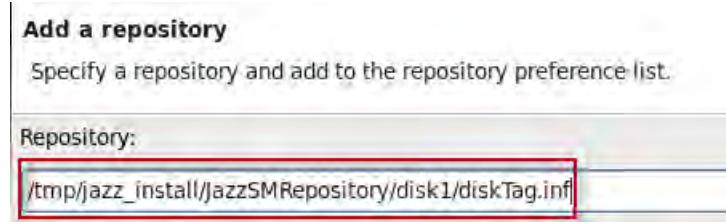


Note: You can remove the old repository entries instead of clearing the check marks.

c. Click **Add Repository**.

d. Click **Browse** and select the following repository:

```
/tmp/jazz_install/JazzSMRepository/disk1/diskTag.inf
```



e. Click **OK** to add the repository.

- f. Verify that the repository is listed.

Repositories:	
Location	Connection
<input type="checkbox"/> /software/omnibus/OMNIbusRepository/repository.config	?
<input type="checkbox"/> /software/jdbc/iM-nco-g-jdbc-rpt-scripts-1_0.zip	?
<input type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	?
<input checked="" type="checkbox"/> /tmp/jazz_install/repositories/disk1/diskTag.inf	?

10. Define the WebSphere repository.

- a. Click **Add Repository**.

- b. Click **Browse** and select the following repository:

/tmp/was_install/disk1/diskTag.inf

Add a repository
Specify a repository and add to the repository preference list.

Repository:

- c. Click **OK** to add the repository.

- d. Verify that the repository is listed, and click **OK**.

Repositories:	
Location	Connection
<input type="checkbox"/> /software/omnibus/OMNIbusRepository/repository.config	?
<input type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	?
<input type="checkbox"/> /software/jdbc/iM-nco-g-jdbc-rpt-scripts-1_0.zip	?
<input checked="" type="checkbox"/> /tmp/jazz_install/jazzSMRepository/disk1/diskTag.inf	?
<input checked="" type="checkbox"/> /tmp/was_install/disk1/diskTag.inf	?

11. Start the installation.

- Click **Install**.
- Select the following packages:

Installation Packages	Status	Vendor
IBM WebSphere Application Server	Will be installed	IBM
Version 8.5.5.7		
Pluggable Application Client for IBM WebSphere Application Server		
Web Server Plug-ins for IBM WebSphere Application Server		IBM
Version 8.5.5.7		
IBM WebSphere SDK Java Technology Edition (Optional)	Will be installed	IBM
Version 7.0.9.10		
Jazz for Service Management extension for IBM WebSphere 8.0		IBM
Version 1.1.0.2		
Jazz for Service Management extension for IBM WebSphere 8.5	Will be installed	IBM
Version 1.1.2.1		

- Scroll down, and select the following packages:

Installation Packages	Status	Vendor
Version 1.1.2.1		IBM
Administration Services		IBM
Version 1.1.2.1		
Reporting Services	Will be installed	IBM
Version 3.1.2.1		
Security Services		IBM
Version 1.1.2.1		
IBM Dashboard Application Services Hub	Will be installed	IBM
Version 3.1.2.1		
Administration Services UI		IBM
Version 1.1.2.1		

- Click **Next**.
- Accept the license agreement and click **Next**.
- Click the package name **IBM WebSphere Application Server V8.5** to select it.

- g. Change the Installation Directory to

/opt/IBM/WebSphere/AppServer

The screenshot shows the 'Package Group Name' column with several options. The first option, 'IBM WebSphere Application Server V8.5', is highlighted with a red box. Below it, other options like 'IBM WebSphere Application Server 8.5.5.7' and 'Core services in Jazz for Service Management' are listed. The 'Installation Directory' column shows the path '/opt/IBM/WebSphere/AppServer' for the selected package group.

Package Group Name	Installation Directory
IBM WebSphere Application Server V8.5	/opt/IBM/WebSphere/AppServer
IBM WebSphere Application Server 8.5.5.7	
IBM WebSphere SDK Java Technology Edition (Optional)	
Jazz for Service Management extension for IBM WebS	
Core services in Jazz for Service Management	/home/netcool/IBM/JazzSM
IBM Dashboard Application Services Hub 3.1.2.1	
Reporting Services 3.1.2.1	

Below the table, there are two input fields:

- 'Package Group Name: IBM WebSphere Application Server V8.5'
- 'Installation Directory: /opt/IBM/WebSphere/AppServer'

- h. Click the package name **Core services in Jazz for Service Management** to select it.

- i. Change the Installation Directory to

/opt/IBM/JazzSM

The screenshot shows the 'Package Group Name' column with the 'Core services in jazz for Service Management' package group selected, highlighted with a red box. Below it, other options like 'IBM WebSphere Application Server 8.5.5.7' and 'Jazz for Service Management extension for IBM WebS' are listed. The 'Installation Directory' column shows the path '/opt/IBM/jazzSM' for the selected package group.

Package Group Name	Installation Directory
IBM WebSphere Application Server V8.5	/opt/IBM/WebSphere/AppServer
IBM WebSphere Application Server 8.5.5.7	
IBM WebSphere SDK Java Technology Edition (Optional)	
Jazz for Service Management extension for IBM WebS	
Core services in jazz for Service Management	/opt/IBM/jazzSM
IBM Dashboard Application Services Hub 3.1.2.1	
Reporting Services 3.1.2.1	

Below the table, there are two input fields:

- 'Package Group Name: Core services in Jazz for Service Management'
- 'Installation Directory: /opt/IBM/JazzSM'

- j. Click **Next**.

- k. Accept the default translation setting, and click **Next**.

- l. Review the list of features and click **Next**.

The screenshot shows a tree view of installed features under the 'IBM WebSphere Application Server 8.5.5.7' package group. Several features are checked, including 'WebSphere Application Server Full Profile', 'IBM WebSphere SDK for Java Technology Edition 6', 'IBM WebSphere SDK Java Technology Edition (Optional) 7.0.9.10', 'Jazz for Service Management extension for IBM WebSphere 8.5 1.1.2.1', 'IBM Dashboard Application Services Hub 3.1.2.1', and 'Reporting Services 3.1.2.1'. The 'IBM WebSphere Application Server 8.5.5.7' package group itself is also expanded.

- m. Enter **object00** as the password and click **Validate**.

Common Configurations

WebSphere Configuration

WebSphere installation location /opt/IBM/WebSphere/AppServer

Profile deployment type Create WebSphere profile

Profile details

Profile location	/opt/IBM/JazzSM/profile
Profile name	JazzSMPProfile
Node name	JazzSMNode01
Server name	server1 <i>not the host name</i>
User name	smadmin
Password	*****
Password confirmation	*****

Validate...



Important: You cannot proceed until you validate the password.

- n. Verify that the validation is successful and click **Next**.

Install Packages

① Click Next to continue.



Hint: No message indicates success. If the validation is successful, the **Next** option is available.

- o. Accept all of the default port values and click **Next**.

Common Configurations	
Ports Configuration	
HTTP transport port	16310
HTTPS transport secure port	16311
Bootstrap port	16312
SOAP connector port	16313
IPC connector port	16314
Administrative console port	16315
Administrative console secure port	16316
High availability manager communication port	16318
ORB listener port	16320
SAS SSL server authentication port	16321
CSIV2 client authentication listener port	16322
CSIV2 server authentication listener port	16323
REST notification port	16324

- p. Accept the default value for context root and click **Next**.

Configuration for IBM Dashboard Application Services Hub 3.1.2.1	
Context Root	
Context Root	/ibm/console

- q. Change the user name to **netcool**. Enter **object00** as the password and click **Test connection**.



Important: As part of the Tivoli Common Report installation work around, you must use the **netcool** user to create the tcrdb database.

Configuration for Reporting Services 3.1.2.1

Database Configuration

Select DB2 instance	db2inst1
IBM Cognos Content Store	Create database
New database name	tcrdb
User name	netcool
Password	*****
Database port number	50000
<input type="button" value="Test connection"/> ←	



Important: You cannot proceed until you validate the connection.

- r. Verify that the connection is successful and click **Next**.

Install Packages

① Test connection is successful. Click Next to continue.

Install Licences Location Features

- s. Enter **/tmp/tcr_install/TCRCognos** as the location of the Cognos installation file and click **Validate**.

Configuration for Reporting Services 3.1.2.1

Cognos Install Image Location

Note: Specify the complete path upto TCRCognos (ex: <Extracted Location>/TCRCognos)

Cognos Install Image	/tmp/tcr_install/TCRCognos
<input type="button" value="Validate..."/> ←	



Important: You cannot proceed until you validate the path.

- t. Verify that the validation is successful and click **Next**.



- u. Review the installation summary and click **Install**.

 **Note:** The installation process runs approximately 50 minutes.

- v. Verify that the installation is successful. Leave the option set to Log on to IBM Dashboard Application Services Hub and click **Finish**.

The following packages were installed:

- IBM WebSphere Application Server V8.5
 - IBM WebSphere Application Server 8.5.5.7
 - IBM WebSphere SDK Java Technology Edition (Optional) 7
 - Jazz for Service Management extension for IBM WebSphere
- Core services in Jazz for Service Management
 - IBM Dashboard Application Services Hub 3.1.2.1
 - Reporting Services 3.1.2.1

Which program do you want to start?

- Log on to IBM Dashboard Application Services
- Profile Management Tool to create a profile.
- Profile Management Tool to create an application
- None

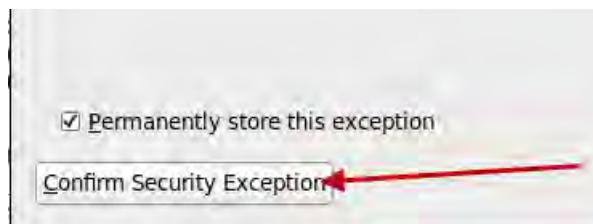
A Firefox browser opens and connects to IBM Dashboard Application Services Hub:

<https://host1.csuite.edu:16311/ibm/console/logon.jsp>

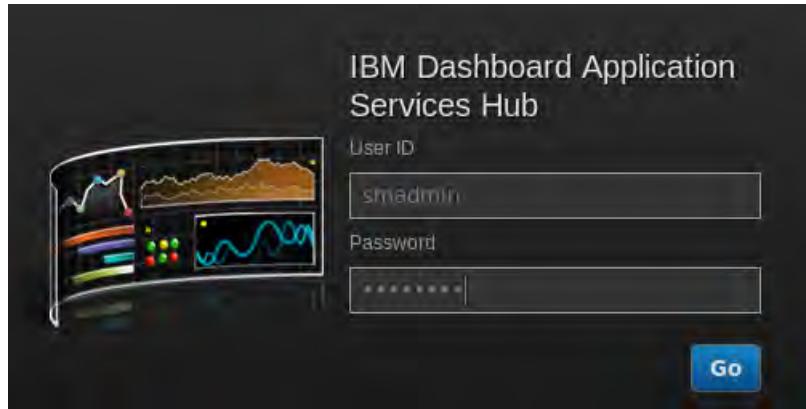
12. Expand **I Understand the Risks**, and click **Add Exception**.



13. Click **Confirm Security Exception**.



14. Log in as user **smadmin** with password **object00**.



15. Verify successful access. Click the icon and select **Log out**.



Hint: Set the Dashboard Application Services Hub login page as the default browser home page.

16. Close the Firefox browser.

Installing the cumulative patch

When this class was created, a known issue with Web GUI existed. The twistie (+) feature in the Event Viewer has an issue with Dashboard Application Services Hub v3.1.2.1. The issue is resolved with the installation of a Dashboard Application Services Hub cumulative patch.

1. Stop Dashboard Application Services Hub:

```
cd /opt/IBM/JazzSM/profile/bin
./stopServer.sh server1 -username smadmin -password object00
```

2. Expand the patch file.

a. Create a temporary directory.

```
mkdir /tmp/cum_patch
```

- b. Expand the patch file into the temporary directory.

```
cd /tmp/cum_patch  
unzip /software/jazz/3.1.2.1CumulativePatch4.zip
```

3. Change file permissions.

```
cd /tmp/cum_patch/3.1.2.1CumulativePatch4  
chmod +x applyPatch.sh
```

4. Install the patch.

```
./applyPatch.sh -username smadmin -password object00 -dashHome  
/opt/IBM/JazzSM/ui
```

```
Installing DASH version 3.1.2.1 cumulative patch 201511051349  
Checking DASH version...  
Checking DASH patch level...  
Checking server status...  
Preparing patch...  
Backing up original files from profileinstalledApps...  
Backing up original files from DASH...  
Creating rollback script...  
Installing patch files to profile/installedApps...  
Installing patch files to DASH...  
Executing patch deploy commands...  
Setting patch level...  
Patch 201511051349 successfully installed.
```

5. Start Dashboard Application Services Hub:

```
cd /opt/IBM/JazzSM/profile/bin  
. ./startServer.sh server1
```

6. Remove the installation files to conserve disk space.

```
cd /software  
/bin/rm -R jazz
```

```
cd /software  
/bin/rm -R tcr
```

```
cd /tmp  
/bin/rm -R cum_patch
```

```
cd /tmp  
/bin/rm -R tcr_install
```



Important: Leave the installation files in `/tmp/jazz_install`, and `/tmp/was_install`. You use the files again in a subsequent unit.

Tivoli Common Reporting workaround

When you open the administration feature of Tivoli Common Reporting, you experience the following error:

```
PF-VAL-6171 Error retrieving metadata for the target fragment.
```

The workaround is to rename or remove a JAR file.

1. Change to the location of the file.

```
cd /opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/lib
```

2. Rename the file.

```
mv BirtAdapterB.jar BirtAdapterB.jar.orig
```

To complete the workaround, you must restart Dashboard Application Services Hub. You restart the application in a subsequent step.

Installing Web GUI

1. Expand the installation file:

```
cd /software/webgui  
unzip OMNIBus-v8.1.0.4-WebGUI.Linux64.zip
```

2. Start IBM Installation Manager:

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

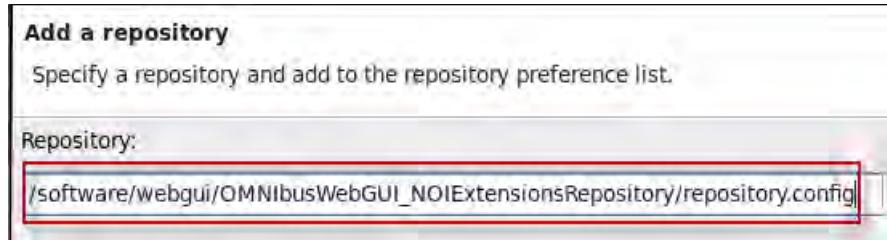
IBM Installation Manager opens.

3. Define the Web GUI repository.

- a. Click **File** and select **Preferences**.
- b. Remove the check marks from the existing entries.
- c. Select **Repositories** and click **Add Repository**.

- d. Click **Browse** and select the following repository:

/software/webgui/OMNIBusWebGUI_NOIExtensionsRepository/repository.config

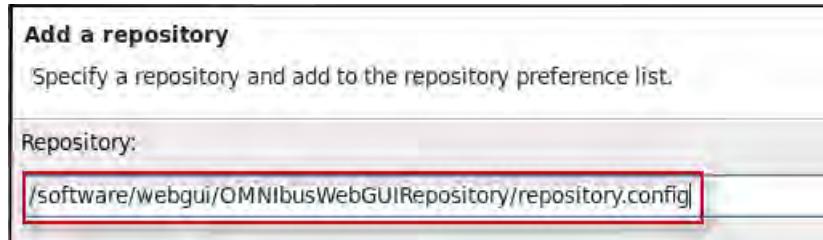


- e. Click **OK** to add the repository.

- f. Click **Add Repository**.

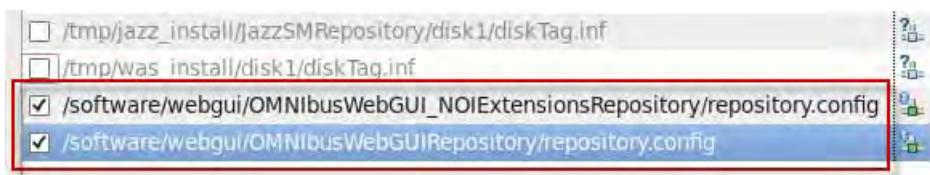
- g. Click **Browse** and select the following repository:

/software/webgui/OMNIBusWebGUICoreRepository/repository.config



- h. Click **OK** to add the repository.

- i. Verify that the repositories are listed and click **OK**.



4. Start the installation.

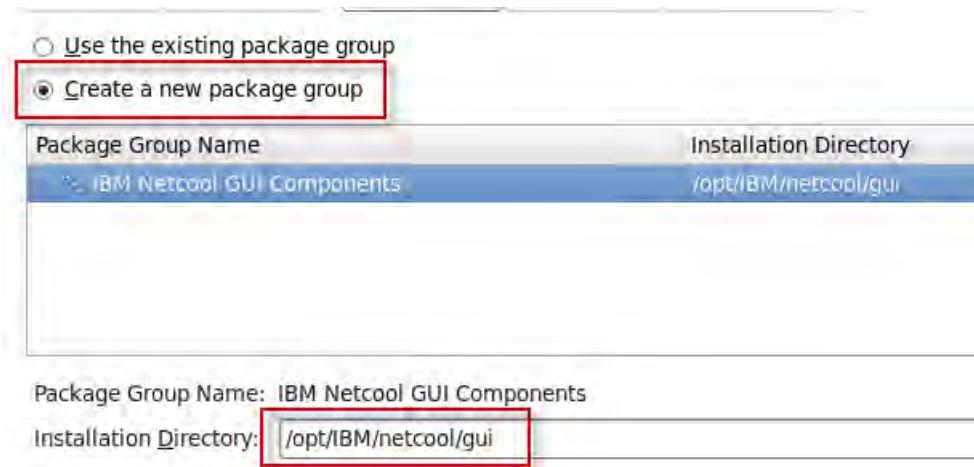
- a. Click **Install**.

- b. Select the two packages and click **Next**.

Installation Packages	Status
<input checked="" type="checkbox"/> IBM Tivoli Netcool/OMNIBus Web GUI	
<input checked="" type="checkbox"/> Version 8.1.0.4	Will be installed
<input checked="" type="checkbox"/> Netcool Operations Insight Extensions for IBM Tivoli Netcool/OM	
<input checked="" type="checkbox"/> Version 1.4.0.0	Will be installed

- c. Accept the license agreement and click **Next**.

- d. Accept the option to create a new package group. Click **Next**.



- e. Expand the list of features and verify that they are all selected. Click **Next**.



- f. Enter **object00** as the password and click **Next**.

The screenshot shows the 'Common Configurations' and 'Profile Details' sections of the installer. In the 'Common Configurations' section, there are tabs for 'WebSphere Application Server' and 'Jazz for Service Management properties'. In the 'Profile Details' section, there are fields for 'Server name' (set to 'server1'), 'User name' (set to 'smadmin'), and 'Password' (set to 'object00', which is highlighted with a red box).



Important: The value **server1** is the name of the WebSphere internal server. It is not the UNIX host name.

The installer verifies that the user name and password provide access to Dashboard Application Services Hub.

- g. Enter **host1.csuite.edu** for the host name and click **Next**.

Configuration for IBM Tivoli Netcool/OMNibus Web GUI 8.1.0.4

Integrate with IBM SmartCloud Analytics - Log Analysis

URL protocol type	https
URL host name	host1.csuite.edu
URL port number	9987
URL context root	Unity
Data source name	omnibus

- h. Review the installation summary and click **Install**.



Note: The installation process runs approximately 25 minutes.

- i. Verify that the installation is successful. Leave the option set to configure Web GUI and click **Finish**.

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

The following packages were installed:

- IBM Netcool
- IBM Tivoli Netcool/OMNibus Web GUI 8.1.0.0
- Netcool Operations Insight Extensions for IBM T

Which program do you want to start?

Configure IBM Tivoli Netcool/OMNibus Web GUI

Log on to IBM Tivoli Netcool/OMNibus Web GUI

None

Web GUI postinstallation configuration

The installation process starts the Web GUI Post-Installation Configuration Tool.

1. Leave the default and click **Next**.

IBM Tivoli Netcool/OMNibus Web GUI Post-Installation Configuration Tool

This tool allows you to configure the Tivoli Netcool/OMNibus Web GUI and get your system up and running as quickly as possible.

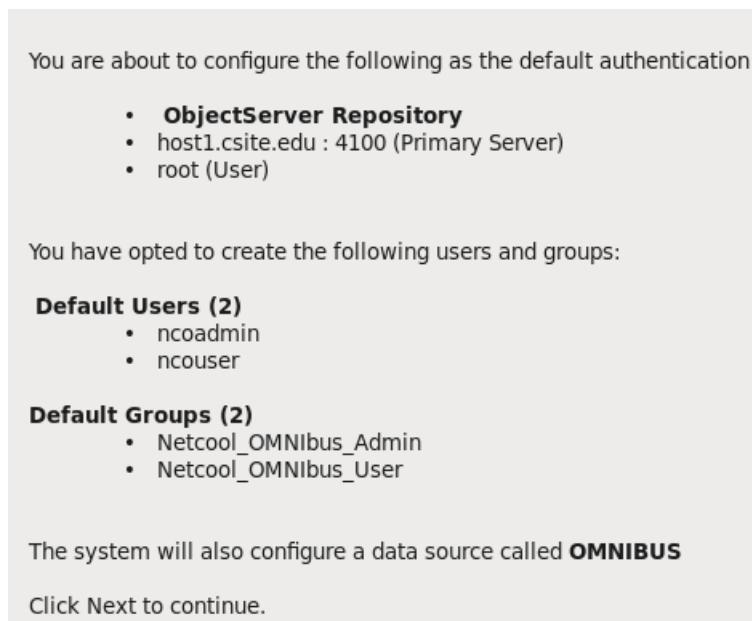
Configure a single server setup using default settings.

Configure an advanced setup.

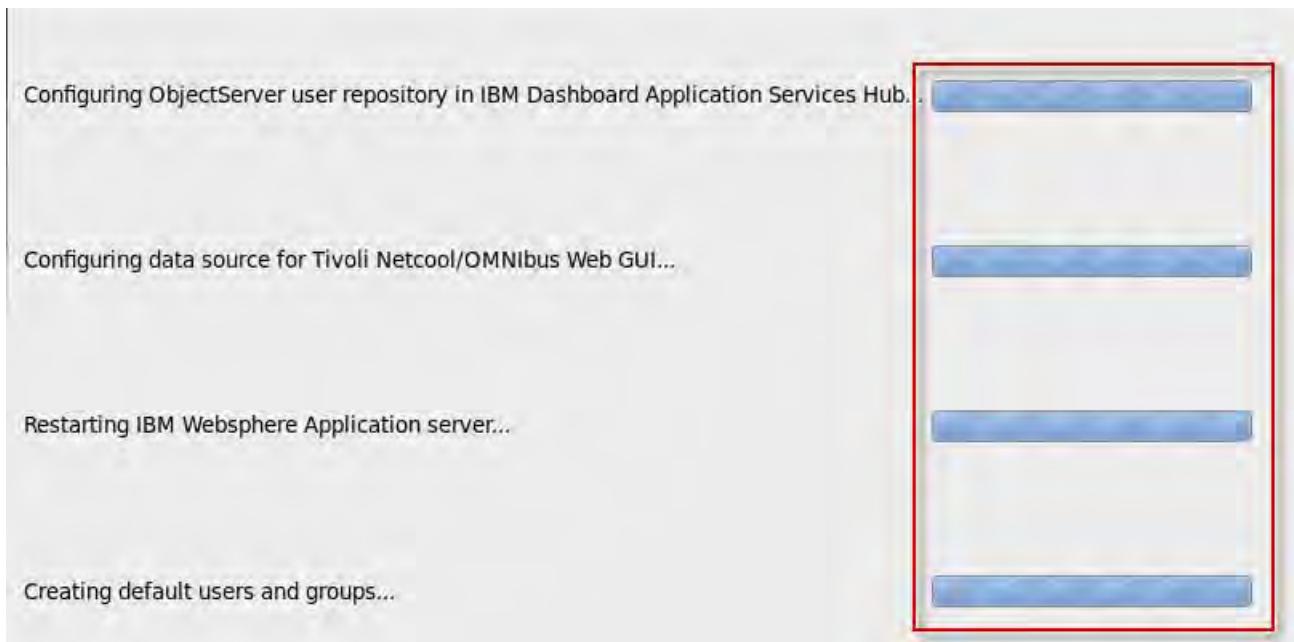
2. Change the Host to **host1.csite.edu**, enter **object00** for the password, and click **Next**.



3. Review the summary and click **Next**.



4. Verify that the steps are complete and click **Next**.



5. Review the configuration results and click **Finish**.

You have successfully configured IBM Tivoli Netcool/OMNibus Web GUI.

- **ObjectServer Repository**
- host1.csite.edu : 4100 (Primary Server)
- root (User)

Following users and groups have been created:

Default Users (2)

- ncoadmin
- ncouser

Default Groups (2)

- Netcool_OMNibus_Admin
- Netcool_OMNibus_User

The system has also configured a data source called **OMNIBUS**

Note: You can run the Configuration tool manually as follows:

```
cd /opt/IBM/netcool/omnibus_webgui/configtool/linux.gtk.x86_64  
./ncwConfigUI -WASUserID smadmin -WASPassword object00
```

6. Click **File** and select **Exit** to close IBM Installation Manager.

7. Remove the installation files to conserve disk space.

```
cd /software  
/bin/rm -R webgui
```

Configuring Netcool/OMNibus Web GUI to start at system start

The following steps use a start script in /etc/init.d.

1. Configure process activity to automatically start:

- a. Change to the root user:

```
su -  
Password: object00
```

- b. Copy the supplied start script:

```
cd /workshop/etc/init.d  
cp jazz /etc/init.d
```

- c. Change the file permissions to allow execution:

```
cd /etc/init.d  
chmod +x jazz
```

- d. Create the logical links to enable the autostart feature:

```
chkconfig jazz on
```

2. Verify autostart.

- a. Stop Jazz for Service Management.

```
/etc/init.d/jazz stop  
ADMU0116I: Tool information is being logged in file  
          /opt/IBM/JazzSM/profile/logs/server1/stopServer.log  
ADMU0128I: Starting tool with the JazzSMProfile profile  
ADMU3100I: Reading configuration for server: server1  
ADMU3201I: Server stop request issued. Waiting for stop status.  
ADMU4000I: Server server1 stop completed.
```



Important: The Cognos reporting engine takes a few minutes to stop. Verify that the process is stopped before proceeding.

- b. Check for a running Cognos process.

```
ps -ef | grep cognos
```

If the command finds a running process, wait a short time and check again.

- c. Start Jazz for Service Management.

```
/etc/init.d/jazz start
```

ADMU0116I: Tool information is being logged in file

/opt/IBM/JazzSM/profile/logs/server1/startServer.log

ADMU0128I: Starting tool with the JazzSMProfile profile

ADMU3100I: Reading configuration for server: server1

ADMU3200I: Server launched. Waiting for initialization status.

ADMU3000I: Server server1 open for e-business; process id is 14535



Note: The process is submitted in the background. The application is ready when you see the open for e-business message. Press enter to see the cursor.

- d. Exit the root user back to the netcool user.

```
exit
```

3. Verify the status of Dashboard Application Services Hub.

```
cd /opt/IBM/JazzSM/profile/bin
```

```
./serverStatus.sh server1 -username smadmin -password object00
```

ADMU0116I: Tool information is being logged in file

/opt/IBM/JazzSM/profile/logs/server1/serverStatus.log

ADMU0128I: Starting tool with the JazzSMProfile profile

ADMU0500I: Retrieving server status for server1

ADMU0508I: The Application Server "server1" is **STARTED**

Exercise 4 Configuring LDAP as an authentication source

The following steps demonstrate how to modify the existing configuration to use LDAP as an authentication source for Dashboard Application Services Hub.

Removing the ObjectServer user repository

The configuration for the Virtual Member Manager component is defined in an XML file. Save a copy of this file before you modify the existing configuration.

1. Save a copy of the VMM configuration file:

```
cd /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/wim/config
cp wimconfig.xml /home/netcool
```



Important: If any of the following configuration steps fail, you can recover the original configuration by copying the saved file back to the original location, and restarting Dashboard Application Services Hub.

2. Connect to WebSphere administrative console as follows:

- a. Open a Firefox browser and connect to Dashboard Application Services Hub.

<http://host1.csite.edu:16310/ibm/console>



Hint: If you did not set the default home page previously, do so now.

- b. Log in as the **smadmin** user with password **object00**.
 - c. Click the icon and select **WebSphere Administrative Console**.



- d. Click **Launch WebSphere administrative console**.



- e. Accept all security messages.

The administrative console opens in a new Firefox tab.

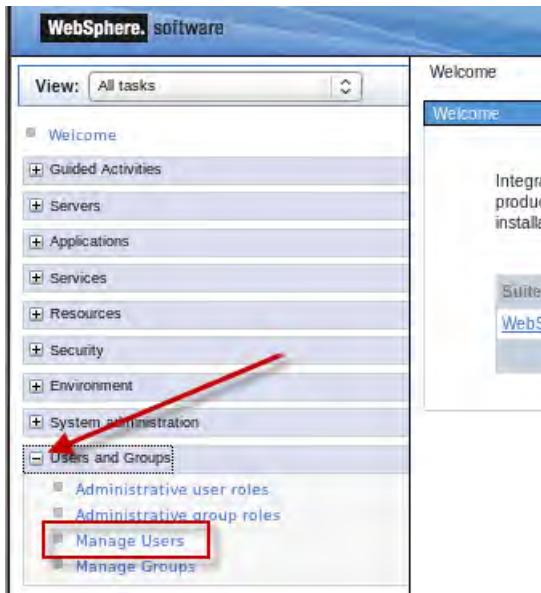
3. Remove the default users and groups.

Two users and two groups were created when you installed Web GUI. Remove those entries before changing the user repositories. You add them again in a subsequent step.

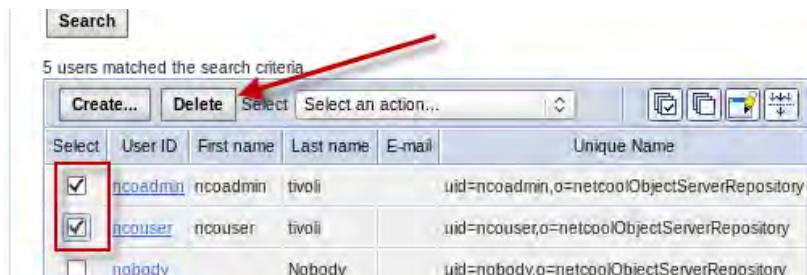


Important: The users and groups are created in the ObjectServer when you run the Web GUI post installation configuration wizard. When you remove the users and groups below, you remove them from the ObjectServer.

- Expand **Users and Groups** and click **Manage Users**.



- Click the boxes to select the two users and click **Delete**.



- Click **Delete**.

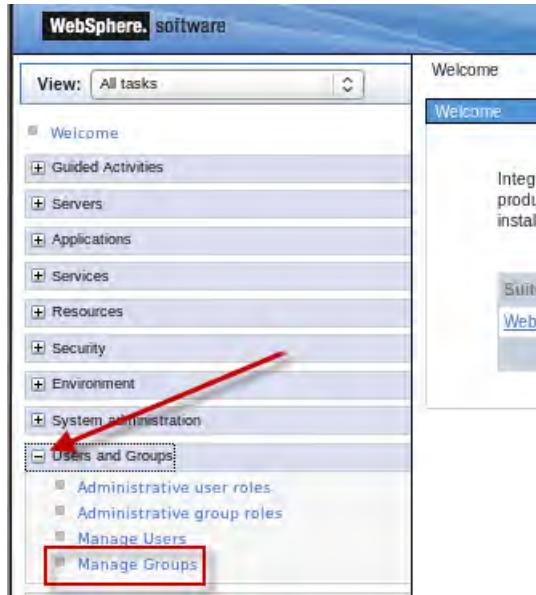


Important: Do not remove any of the other users.



The **ncoadmin** and **ncouser** IDs are deleted from the ObjectServer.

d. Click **Manage Groups**.



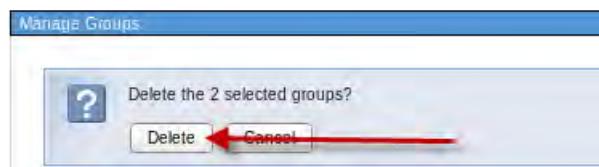
e. Click the boxes to select the two groups and click **Delete**.

10 groups matched the search criteria.		
	Create...	Delete
Select	Group name	Description
<input type="checkbox"/>	Administrator	Admin Group cn=Administrator,o=netco
<input type="checkbox"/>	Gateway	Permissions required for a gateway user cn=Gateway,o=netcoolO
<input type="checkbox"/>	ISQL	Read only ISQL access cn=ISQL,o=netcoolObjec
<input type="checkbox"/>	ISQLWrite	Write ISQL access cn=ISQLWrite,o=netcoolC
<input checked="" type="checkbox"/>	Netcool_OMNIbus_Admin	cn=Netcool_OMNIbus_Ad
<input checked="" type="checkbox"/>	Netcool_OMNIbus_User	cn=Netcool_OMNIbus_Us
<input type="checkbox"/>	Normal	Normal Group cn=NormalGroup,ou=netco

f. Click **Delete**.



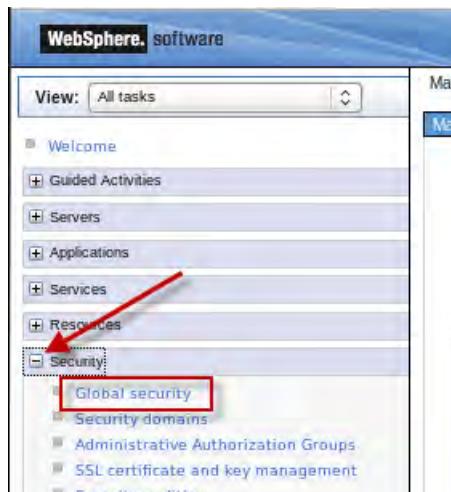
Important: Do not remove any of the other groups.



The Netcool_OMNIbus_Admin and Netcool_OMNIbus_User groups are deleted.

4. Removing the ObjectServer definition.

- Expand **Security** and click **Global security**.



- Scroll down on the page to the *User account repository* section and click **Configure**.

User account repository

Realm name: defaultWIMFileBasedRealm

Current realm definition: Federated repositories

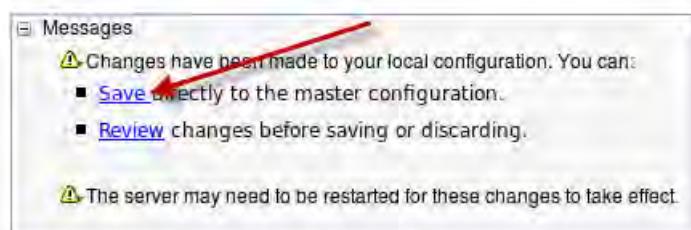
Available realm definitions:

- Federated repositories
- Configure...
- Set as current

- Scroll down on the page to the *Repositories in the realm*, select the check box for the ObjectServer entry, and click **Remove**.

Add repositories (LDAP, custom, etc)...		Use built-in repository	Remove
Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File
<input checked="" type="checkbox"/>	o=netcoolObjectServerRepository	NetcoolObjectServer	Custom
Total 2			

- Click **Save**.



- e. Scroll down on the page to the *Related Items* section and click **Manage repositories**.

The screenshot shows a table titled "You can administer the following resources:" with one entry: "o=defaultWIMFileBasedRealm" (File type). Below this, the "Related Items" section is visible, featuring tabs for "Additional Properties" (selected), "Manage repositories" (highlighted with a red box), and "Trusted authentication realms -".

- f. Check the box to select the ObjectServer entry and click **Delete**.

The screenshot shows a confirmation dialog with "Add" and "Delete" buttons. A red arrow points to the "Delete" button. Below it is a table titled "You can administer the following resources:" with two entries: "InternalFileRepository" (File type) and "NetcoolObjectServer" (Custom type). A red box highlights the checkbox next to "NetcoolObjectServer".

- g. Click **Save**.

The screenshot shows a "Messages" dialog with a warning icon. It says: "Changes have been made to your local configuration. You can: [] Save directly to the master configuration. [] Review changes before saving or discarding." A red arrow points to the "Save directly" link.

- h. Log out of administrative console.

The screenshot shows the top navigation bar of the administrative console. It includes "Welcome smadmin", "Help", "Logout" (highlighted with a red arrow), and the IBM logo. Below the main menu is a toolbar with "Close pag", "Help", and "Field help".

Leave the Firefox tab open. You use it again shortly.

- i. Log out of Dashboard Application Services Hub.

The screenshot shows the user profile menu for "smadmin". It includes "Credential Store", "Favorites", "My Startup Pages", "Change Password", and a "Log out" option (highlighted with a red box).

The ObjectServer is removed as a Virtual Member Manager user repository. You must restart Dashboard Applications Services Hub to complete the removal.

5. Stop Dashboard Application Services Hub.

```
cd /opt/IBM/JazzSM/profile/bin
./stopServer.sh server1 -username smadmin -password object00
```



Important: The Cognos reporting engine takes a few minutes to stop. Verify that the process is stopped before proceeding.

6. Check for a running Cognos process.

```
ps -ef | grep cognos
```

If the command finds a running process, wait a short time and check again.

7. Start Dashboard Application Services Hub.

```
./startServer.sh server1
```

Dashboard Application Services Hub is now configured with a single user repository, internal file-based. The only valid user ID is **smadmin** because that user is defined in the file-based repository.

8. Save another copy of the VMM configuration file.

```
cd /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/wim/config
cp wimconfig.xml /home/netcool/wimconfig.xml.fileonly
```

Adding the LDAP user repository

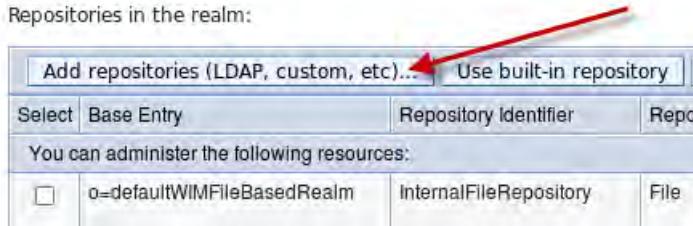
1. Return to WebSphere Integrated Solutions Console in the Firefox tab.
2. Log in as **smadmin** with password **object00**.
3. Adding the LDAP directory as a user repository.
 - a. Expand **Security** and click **Global Security**.



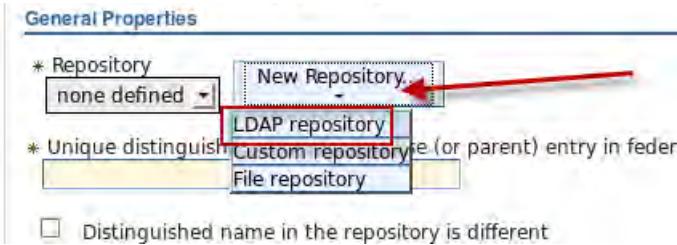
- b. Scroll down on the page to the *User account repository* section and click **Configure**.



- c. Scroll down on the page to the *Repositories in the realm*, and click **Add repositories**.



- d. Click **New Repository** and select **LDAP repository**.



- e. Change the repository identifier to **TIVIDS**.
f. Set the primary host name to **host1.csite.edu**.
g. Verify that the port is set to **389**.
h. Set the **Bind distinguished name** field to **cn=root**.
i. Set the **Bind password** field to **object00**.
j. Set the **Federated repository properties for login** field to **uid;cn**.

- k. Scroll to the bottom of the page and click **OK**.

* Repository identifier
TIVIDS

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:

Security

Bind distinguished name
cn=root

Bind password

Federated repository properties for
uid;cn

I LDAP attribute for Kerberos principal

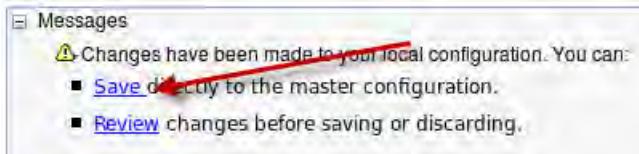
- l. Enter **dc=ibm,dc=com** for the Unique distinguished name field, and click **OK**.

General Properties

* Repository
TIVIDS New Repository...

* Unique distinguished name of the base (or parent) entry
repositories
dc=ibm,dc=com

- m. Click **Save**.



Important: The base entry is mapped to the root of the LDAP directory. All operations are completed as root, which causes errors on most LDAP servers. More configuration is required.

The next step is to 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 is used to locate values for each of the object classes. These definitions essentially define the LDAP subtree where the Netcool user information is located.

4. Defining LDAP object class mappings.
 - a. Scroll down on the page and click **TIVIDS**.

Repositories in the realm:

Select	Base Entry	Repository Identifier	Re...
<input type="checkbox"/>	dc=ibm,dc=com	TIVIDS	L...
<input type="checkbox"/>	o-defaultWIMFileBasedRealm	InternalFileRepository	F...

- b. Scroll down and click **Federated repositories entity types to LDAP object classes mapping**.

Additional Properties

- [Performance](#)
- [**Federated repositories entity types to LDAP object classes mapping**](#)
- [Federated repositories property names to LDAP attributes mapping](#)
- [Group attribute definition](#)



Important: The following steps are unique to the configuration of the classroom LDAP server. The steps that are shown here are relevant to the LDAP configuration that is used for the class. The process is the same regardless of the LDAP configuration. The values that are used in these steps must change for another LDAP server.

- c. Click **Group**.

Select	Entity Type	Object Classes
<input type="checkbox"/>	Group	groupOfNames
<input type="checkbox"/>	OrgContainer	organization;organizationalUnit;domain;container
<input type="checkbox"/>	PersonAccount	inetOrgPerson

- d. Enter **ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM** for **Search bases** and click **OK**.

General Properties

- * Entity type: Group
- * Object classes: groupOfNames
- Search bases: ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
- Search filter

e. Click **OrgContainer**.

Select	Entity Type ▾	Object Classes ▾
You can administer the following resources:		
<input type="checkbox"/>	Group	groupOfNames
<input type="checkbox"/>	OrgContainer	organization;organizationalUnit;domain;container
<input type="checkbox"/>	PersonAccount	inetOrgPerson

f. Verify that the **Search bases** field is empty and click **OK**.

General Properties

* Entity type

* Object classes

Search bases

Search filter

g. Click **PersonAccount**.

Select	Entity Type ▾	Object Classes ▾
You can administer the following resources:		
<input type="checkbox"/>	Group	groupOfNames
<input type="checkbox"/>	OrgContainer	organization;organizationalUnit;domain;container
<input type="checkbox"/>	PersonAccount	inetOrgPerson

h. Enter **ou=tipusers,cn=tipRealm,DC=IBM,DC=COM** for the **Search bases** field and click **OK**.

General Properties

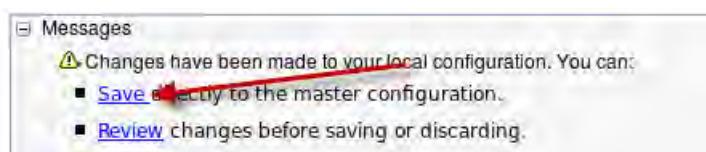
* Entity type

* Object classes

Search bases

Search filter

i. Click **Save**.



Now the Virtual Member Manager is configured to retrieve user information from a specific subtree within LDAP.

The last step is to configure Dashboard Application Services Hub 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 a new user or group is created.

5. Configure IBM Dashboard Application Services Hub to write to LDAP as follows:

- Click **Federated repositories**.

Global security

Global security > Federated repositories > TIVIDS > Federated repositories entity types mapping

Use this page to list federated repositories entity types that are supported by the LI entity type to view or change its configuration properties, or to add or remove the entity type.

- Scroll to the bottom of the page and click **Supported entity types**.

Additional Properties

- Property extension repository
- Entry mapping repository
- Supported entity types**
- User repository attribute

Related Items

- Manage repositories
- Trusted authentication realms - inbound

- Click **Group**.

Entity Type	Base Entry for the Default Parent	Relative Distinguished Name
You can administer the following resources:		
Group	o=netcoolObjectServerRepository	cn
OrgContainer	o=netcoolObjectServerRepository	o;ou;dc;cn
PersonAccount	o=netcoolObjectServerRepository	uid



Important: Observe the values in the table that say *o=netcoolObjectServerRepository*. In the present state, if a new user is added to Dashboard Application Services Hub, an attempt is made to write the entry to the netcoolObjectServerRepository. This repository was removed in a previous step. Until the following steps are completed, it is not possible to add new Dashboard Application Services Hub users.

- d. Enter **ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM** for **Base entry for the default parent** and click **OK**.

General Properties

* Entity type
Group

* Base entry for the default parent
ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM

* Relative Distinguished Name properties
cn

- e. Click **OrgContainer**.

Entity Type	Base Entry for the Default Parent	Relative DN
You can administer the following resources:		
Group	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn
OrgContainer	dc=netcoolObjectServerRepository	o;ou
PersonAccount	o=netcoolObjectServerRepository	uid

- f. Enter **dc=ibm,dc=com** for **Base entry for the default parent** and click **OK**.

General Properties

* Entity type
OrgContainer

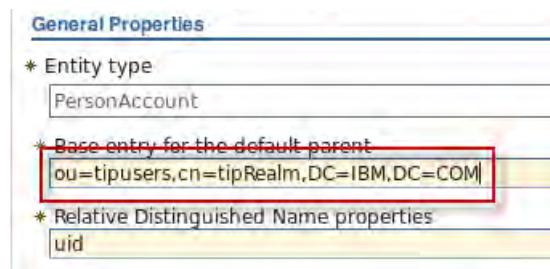
* Base entry for the default parent
dc=ibm,dc=com

* Relative Distinguished Name properties
o;ou;dc;cn

- g. Click **PersonAccount**.

Entity Type	Base Entry for the Default Parent	Relative DN
You can administer the following resources:		
Group	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn
OrgContainer	dc=ibm,dc=com	o;ou;dc;cr
PersonAccount	o=netcoolObjectServerRepository	uid

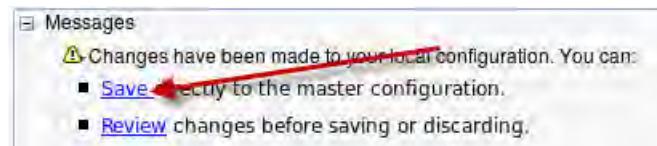
- h. Enter **ou=tipusers,cn=tipRealm,DC=IBM,DC=COM** for **Base entry for the default parent** and click **OK**.



The revised entries are listed as shown.

Entity Type	Base Entry for the Default Parent	Relative Distinguished
You can administer the following resources:		
Group	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn
OrgContainer	dc=ibm,dc=com	o;ou;dc;cn
PersonAccount	ou=tipusers,cn=tipRealm,DC=IBM,DC=COM	uid

- i. Click **Save**.



6. Log out of administrative console.

Leave the Firefox tab open. You use it again shortly.

7. Stop Dashboard Application Services Hub.

```
cd /opt/IBM/JazzSM/profile/bin
./stopServer.sh server1 -username smadmin -password object00
```



Important: The Cognos reporting engine takes a few minutes to stop. Verify that the process is stopped before proceeding.

8. Check for a running Cognos process.

```
ps -ef | grep cognos
```

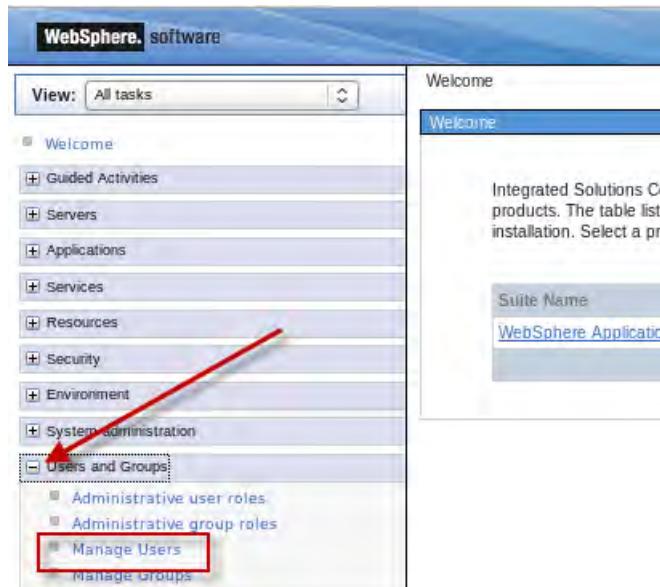
If the command finds a running process, wait a short time and check again.

9. Start Dashboard Application Services Hub.

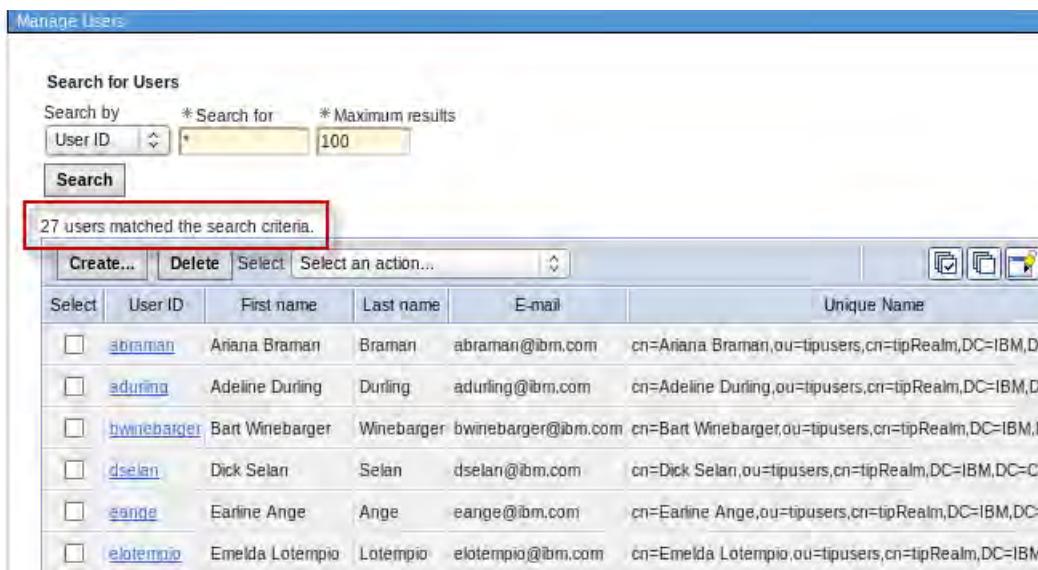
```
./startServer.sh server1
```

Dashboard Application Services Hub is now configured with two user repositories: internal file-based and LDAP. The LDAP users and groups that are located within the defined subtree are available within Dashboard Application Services Hub.

10. Return to WebSphere Integrated Solutions Console in the Firefox tab.
 11. Log in as **smadmin** with password **object00**.
 12. Verify that the LDAP users are available within Dashboard Application Services Hub.
 - a. Expand **Users and Groups** and click **Manage Users**.



- b. Observe the list of users.



Dashboard Application Services Hub is now aware of 27 users. Note the values in the Unique Name column of the table. These values indicate that the user is defined in the LDAP directory. When one of these users logs in to Dashboard Application Services Hub, the Virtual Member Manager component uses the password that is defined in LDAP to authenticate the login.

The users are known to Dashboard Application Services Hub, but they do not belong to any group, and they do not have any roles that are assigned yet. Therefore, they cannot perform

any useful functions within Dashboard Application Services Hub. You add roles to some of these users in a subsequent unit.

Configuring Dashboard Application Services Hub to allow logins when LDAP is down

Dashboard Application Services Hub is configured to use two user repositories:

internal file-based
LDAP

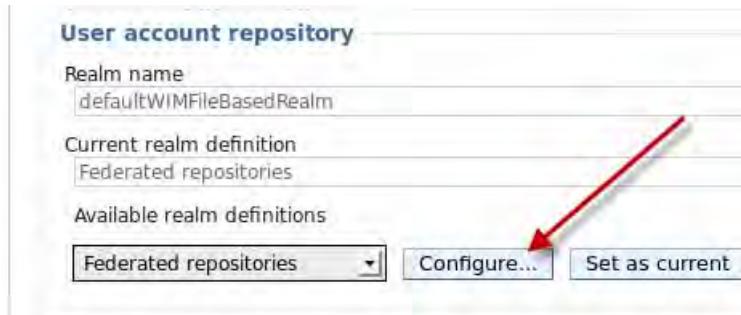
Dashboard Application Services Hub is based on WebSphere. WebSphere uses a property called *allowOperationIfReposDown*. The default setting for this property is False. When set to False, when one of the repositories is not available, users cannot log in to Dashboard Application Services Hub. If the property is True, and the LDAP server goes down, you can log in to Dashboard Application Services Hub as the **smadmin** user because that user is defined in the file-based repository.

To facilitate this exercise, a script is provided which runs a utility to change the value of the property to true.

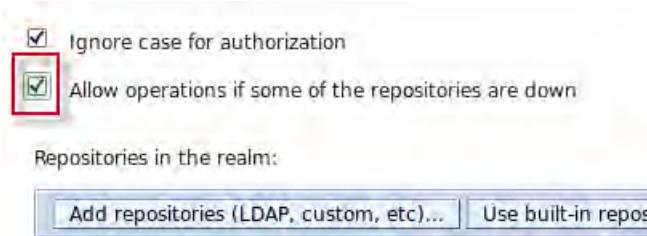
1. Expand **Security** and click **Global security**.



2. Scroll down on the page to the *User account repository* section and click **Configure**.

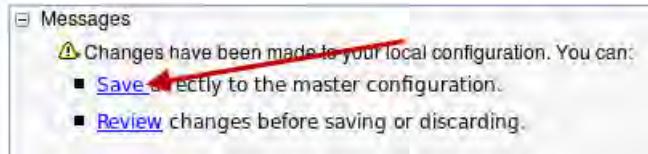


3. Scroll down and select **Allow operations if some repositories are down**.



4. Scroll to the bottom of the page and click **OK**.

5. Click **Save**.



6. Log out of WebSphere administrative console.

7. Log out of Dashboard Applications Services Hub.

8. Stop Dashboard Application Services Hub.

```
cd /opt/IBM/JazzSM/profile/bin
./stopServer.sh server1 -username smadmin -password object00
```

9. Check for a running Cognos process.

```
ps -ef | grep cognos
```

If the command finds a running process, wait a short time and check again.

10. Start Dashboard Application Services Hub.

```
./startServer.sh server1
```

Dashboard Application Services Hub is now configured with two user repositories: internal file-based and LDAP. The LDAP users and groups that are located within the defined subtree are available within Dashboard Application Services Hub.

To verify that the change works, you must temporarily stop the LDAP server.

11. Stop the LDAP server as follows:

a. Change to the root user.

```
su -
Password: object00
```

b. Stop LDAP.

```
/etc/init.d/ibmslapd stop
```

```
Stopping SDS instance dsrdbm01 Stopping SDS Admin Server instance dsrdbm01
[root]
```



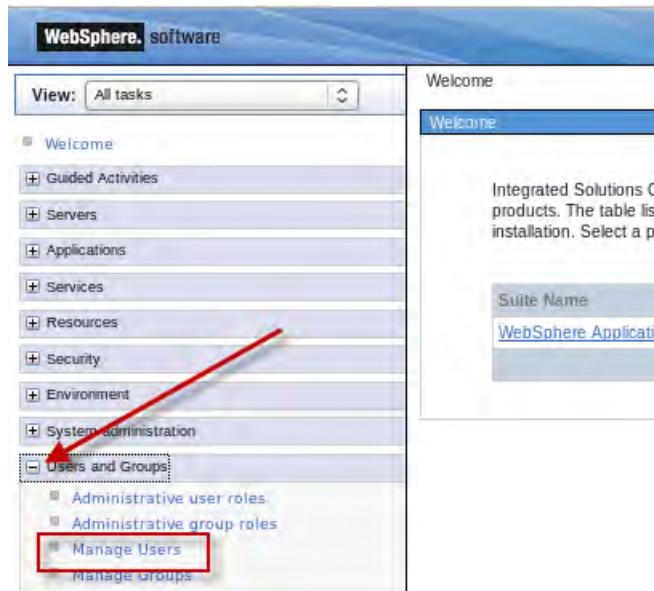
Important: Leave the terminal window as is. You return shortly and use it to restart the LDAP server.

12. Return to WebSphere Integrated Solutions Console in the Firefox tab.

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

The successful login verifies that the property change is correct.

14. Expand **Users and Groups** and click **Manage Users**.



15. Observe the list of users.

Search					
1 users matched the search criteria.					
Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	smadmin	smadmin	smadmin		uid=smadmin,o=defaultWIMFileBasedRealm

Dashboard Application Services Hub is aware of only one user: **smadmin**.



Important: Leave the browser session as is. You return to it shortly.

16. Restart the LDAP server as follows:

- Start the LDAP server.

```
/etc/init.d/ibmslapd start
```

```
Starting SDS instance dsrdbm01 Starting SDS Admin Server instance dsrdbm01
[root]
```

- Exit the **root** user and return to the **netcool** user:

```
exit
```

17. Return to the administrative console session and click **Search**.

The screenshot shows a search interface with the following details:

- Search by: User ID
- Search for: (empty field)
- Maximum results: 100
- Search button: A red arrow points to this button.
- Message: "27 users matched the search criteria."
- Table headers: Select, User ID, First name, Last name, E-mail, Unique Name.
- Data rows:
 - Ariana Braman: Braman, abraman@ibm.com, cn=Ariana Braman,ou=tipusers,cn=tipRealm
 - Adeline Durling: Durling, adurling@ibm.com, cn=Adeline Durling,ou=tipusers,cn=tipRealm
 - Bart Winebarger: Winebarger, bwinebarger@ibm.com, cn=Bart Winebarger,ou=tipusers,cn=tipRealm
 - Dick Selan: Selan, dselan@ibm.com, cn=Dick Selan,ou=tipusers,cn=tipRealm,D
 - Earline Ange: Ange, eange@ibm.com, cn=Earline Ange,ou=tipusers,cn=tipRealm

All 27 users are again available.

18. Log out of administrative console.

Configuring ObjectServer synchronization

1. Enable ObjectServer synchronization as follows:

- a. Change to the required directory:

```
cd /opt/IBM/netcool/gui/omnibus_webgui/etc
```

- b. Modify the Web GUI initialization file:

```
gedit server.init
```

- c. Locate the following line:

```
users.credentials.sync:false
```



Note: The line is at approximately line number 185 in the file.

- d. Change the property value to true:

```
users.credentials.sync:true
```

- e. Save the file.

Synchronization is performed at a defined frequency. The default frequency is every 3600 seconds. To facilitate the class exercises, you modify that setting and reduce the frequency.

- f. Change to the required directory:

```
cd /opt/IBM/netcool/gui/omnibus_webgui/etc/datasources
```

- g. Modify the Web GUI initialization file:

```
gedit ncwDataSourceDefinitions.xml
```

- h. Locate the following line:

```
<config maxAge="3600" />
```
 - i. Change the property value to 600:

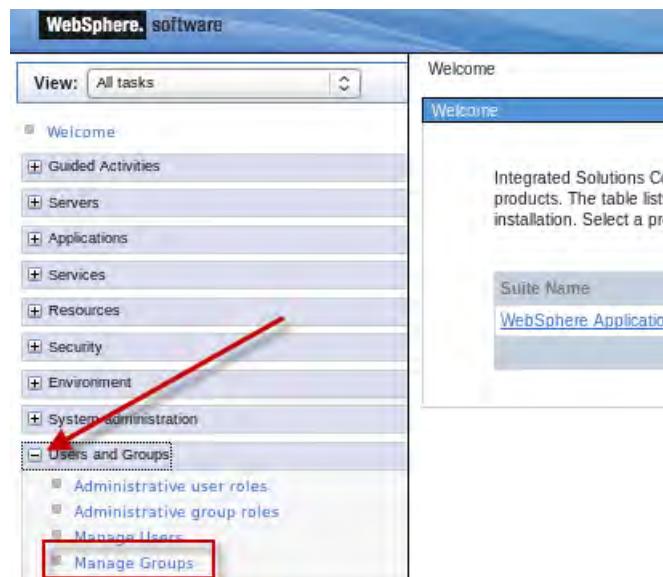
```
<config maxAge="600" />
```
 - j. Save the file.
2. Stop Dashboard Application Services Hub:
- ```
cd /opt/IBM/JazzSM/profile/bin
.stopServer.sh server1 -username smadmin -password object00
```
3. Check for a running Cognos process.
- ```
ps -ef | grep cognos
```
- If the command finds a running process, wait a short time and check again.
4. Start Dashboard Application Services Hub:
- ```
./startServer.sh server1
```

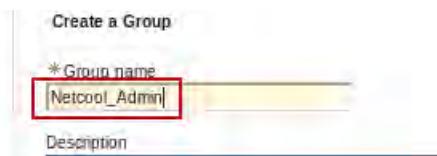
## Configuring default users and groups

Now that the synchronization process is configured, you must re-create the default users and groups. You create the users and groups in Dashboard Application Services Hub. The synchronization process creates the same entries in the ObjectServer.

1. Log in to Dashboard Application Services Hub as user **smadmin** with password **object00**.
2. Start WebSphere administrative console.
3. Add the default groups as follows:

- a. Expand **Users and Groups** and click **Manage Groups**.



b. Click **Create**.c. Enter **Netcool\_Admin** as the group name and click **Create**.d. Click **Close**.e. Repeat the previous steps and create the **Netcool\_User** group.

When complete, the groups are listed as follows:



3 groups matched the search criteria.

| Select                   | Group name       | Description                             | Unique Na |
|--------------------------|------------------|-----------------------------------------|-----------|
| <input type="checkbox"/> | Netcool_Admin    | cn=Netcool_Admin,ou=tipgroups,cn=       |           |
| <input type="checkbox"/> | Netcool_User     | cn=Netcool_User,ou=tipgroups,cn=tip     |           |
| <input type="checkbox"/> | WPAdministrators | cn=WPAdministrators,ou=tipgroups,cn=tip |           |

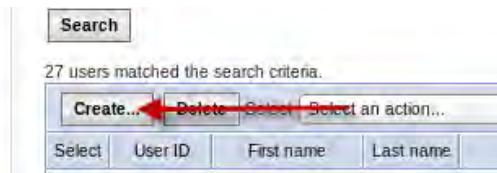


**Note:** The two groups are created in the LDAP directory.

## 4. Add the default users as follows:

a. Click **Manage Users**.

b. Click **Create**.



- c. Enter **ncoadmin** as the user ID.
- d. Enter values for first and last names.
- e. Enter **object00** for the password and click **Group Membership**.

Create a User

\*User ID: ncoadmin

\*First name: Netcool

\*Last name: Admin

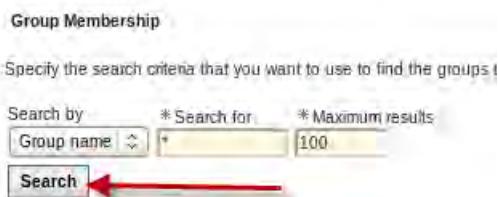
E-mail: ncoadmin

\*Password: object00

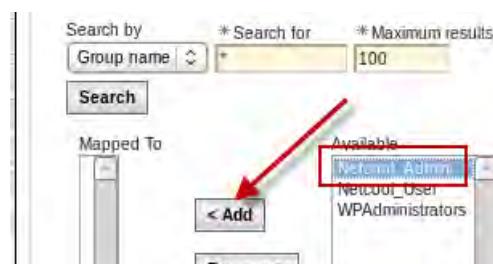
\*Confirm password: object00

Group Membership

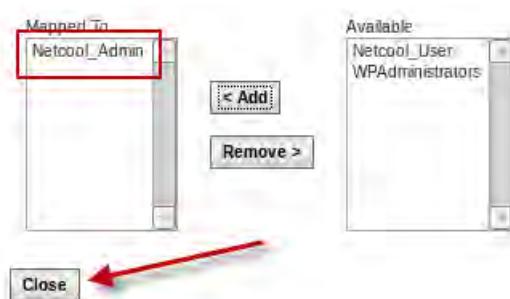
f. Click **Search**.



g. Click **Netcool\_Admin** to select it and click **Add**.



h. Click **Close**.



- i. Click Create.



- j. Click Close.



- k. Repeat the previous steps to create the **ncouser** user and assign the user to the **Netcool\_User** group.

When complete, the user entries are listed as follows:

| Select                   | User ID  | First name | Last name | E-mail   | Unique Name                                        |
|--------------------------|----------|------------|-----------|----------|----------------------------------------------------|
| <input type="checkbox"/> | ncoadmin | Netcool    | Admin     | ncoadmin | uid=ncoadmin,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM |
| <input type="checkbox"/> | ncouser  | Netcool    | User      | ncouser  | uid=ncouser,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM  |

- l. Log out of administrative console.

- m. Close the **Firefox** tab.

The users and groups are created in the LDAP directory and are now known to Dashboard Application Services Hub. However, no Dashboard Application Services Hub roles are assigned to either the users or the groups yet.

5. Assign Dashboard Application Services Hub roles to the default groups as follows.

- a. Click the icon and select **Group Roles**.



- b. Click **Search**.



- c. Click **Netcool\_Admin**.

| Group Name    | Roles | Unique Name  |
|---------------|-------|--------------|
| Netcool_Admin |       | cn=Netcool_A |
| Netcool_User  |       | cn=Netcool_U |

- d. Scroll down and select the following roles:

iscadmins  
ncw\_admin  
ncw\_dashboard\_editor  
ncw\_gauges\_editor  
netcool\_rw



**Important:** The example screen capture does not show all required roles.

- e. Scroll to the bottom of the page and click **Save**.



- f. Click **Netcool\_User**.

| Group Name    | Roles                                                                     |
|---------------|---------------------------------------------------------------------------|
| Netcool_Admin | ncw_gauges_editor, ncw_admin, ncw_dashboard_editor, iscadmins, netcool_rw |
| Netcool_User  |                                                                           |

- g. Scroll down and select the following roles:

ncw\_user  
ncw\_gauges\_viewer  
netcool\_rw

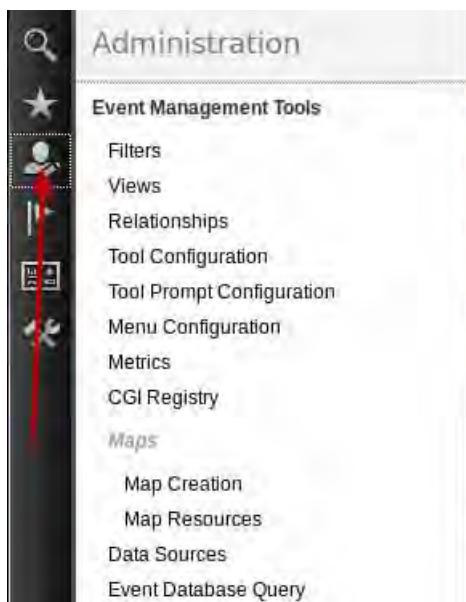


- h. Scroll to the bottom of the page and click **Save**.

The role assignments are listed as follows:

| Group Name    | Roles                                                                     | Uniq |
|---------------|---------------------------------------------------------------------------|------|
| Netcool_Admin | ncw_gauges_editor, ntw_admin, ntw_dashboard_editor, iscadmins, netcool_rw | cn=1 |
| Netcool_User  | ncw_user, ntw_gauges_viewer, netcool_rw                                   | cn=1 |

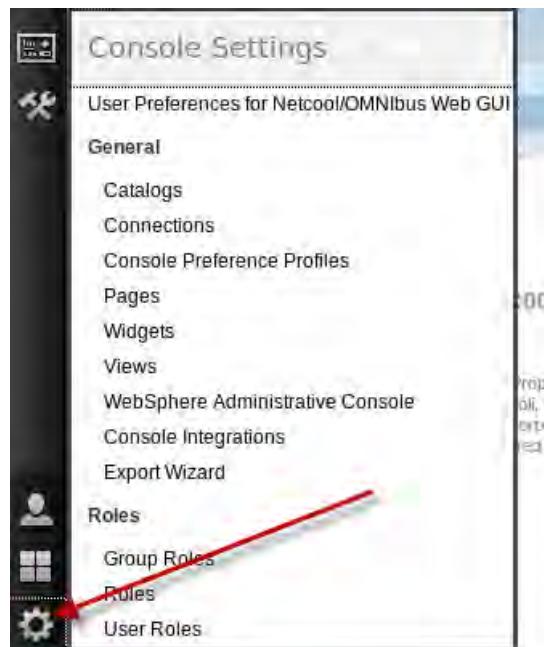
6. Log out of Dashboard Application Services Hub as the **smadmin** user.
7. Log in to Dashboard Application Services Hub as user **ncoadmin** with password **object00**.
8. Click the icon and verify access to Netcool administrative features.



9. Click the icon and verify access to Netcool user features.



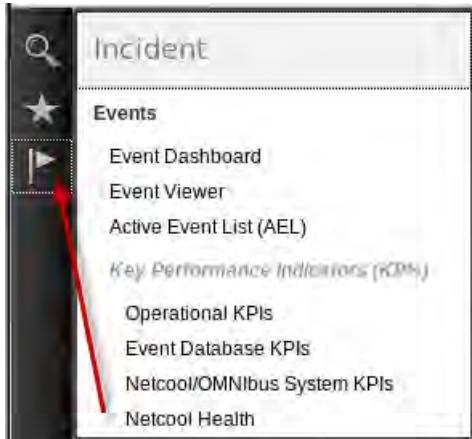
10. Click the icon and verify access to Dashboard Application Services Hub administrative features.



11. Log out of Dashboard Application Services Hub as the **ncoadmin** user.

12. Log in to Dashboard Application Services Hub as user **ncouser** with password **object00**.

13. Click the icon and verify access to Netcool user features.



14. Log out of Dashboard Application Services Hub.

## Configuring Tivoli Common Reporting

The following steps demonstrate how to import the Netcool/OMNibus Common Reporting reports, and configure Common Reporting for user access.

1. Log in to Dashboard Application Services Hub as user **smadmin** with password **object00**.

2. Update groups to allow access to Tivoli Common Reporting.

Access to Tivoli Common Reporting requires a specific Dashboard Application Services Hub role. The installation process adds that role to the **smadmin** user. Add the role to other user groups.

- a. Click the icon and select **Group Roles**.



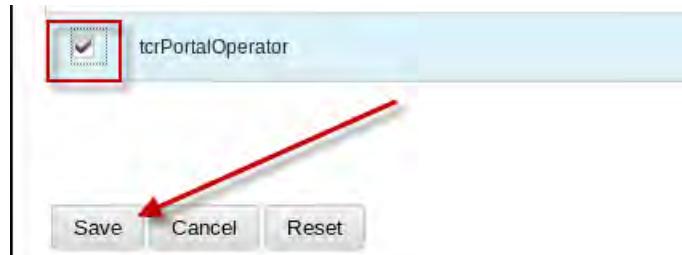
- b. Enter **Netcool\*** and click **Search**.

The screenshot shows a search interface for group roles. It includes fields for 'Group ID' (containing 'Netcool\*' highlighted with a red box), 'Number of results to display' (set to 20), and a 'Search' button (highlighted with a red arrow).

c. Click **Netcool\_Admin**.

| Group Name    | Roles                                                                     |
|---------------|---------------------------------------------------------------------------|
| Netcool_Admin | ncw_gauges_editor, ncw_admin, ncw_dashboard_editor, iscadmins, netcool_rw |
| Netcool_User  | ncw_user, ncw_gauges_viewer, netcool_rw                                   |

d. Scroll to the bottom of the page, select **tcrPortalOperator**, and click **Save**.



e. Repeat the previous steps to add **tcrPortalOperator** to the **Netcool\_User** group.

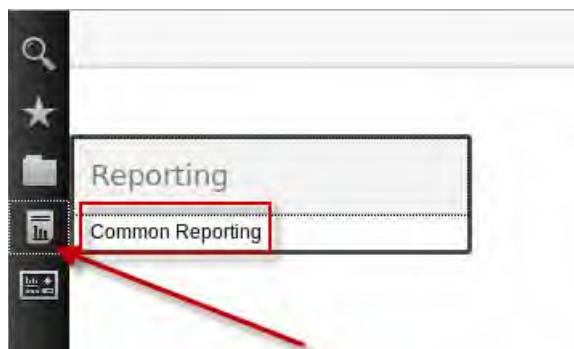
| Group Name    | Roles                                                                                        |
|---------------|----------------------------------------------------------------------------------------------|
| Netcool_Admin | ncw_gauges_editor, ncw_admin, tcrPortalOperator, ncw_dashboard_editor, iscadmins, netcool_rw |
| Netcool_User  | ncw_user, tcrPortalOperator, ncw_gauges_viewer, netcool_rw                                   |

f. Click the X to close the Group Roles page.



3. Verify basic Tivoli Common Reporting function.

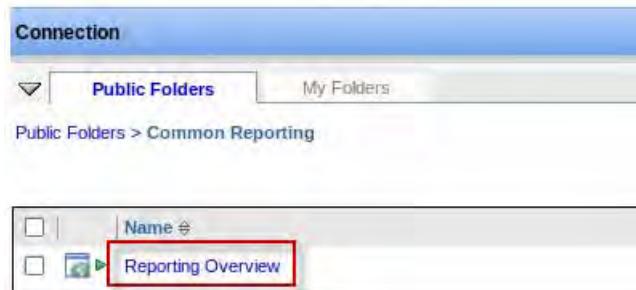
a. Click the icon and select **Common Reporting**.



- b. Click the report package **Common Reporting**.

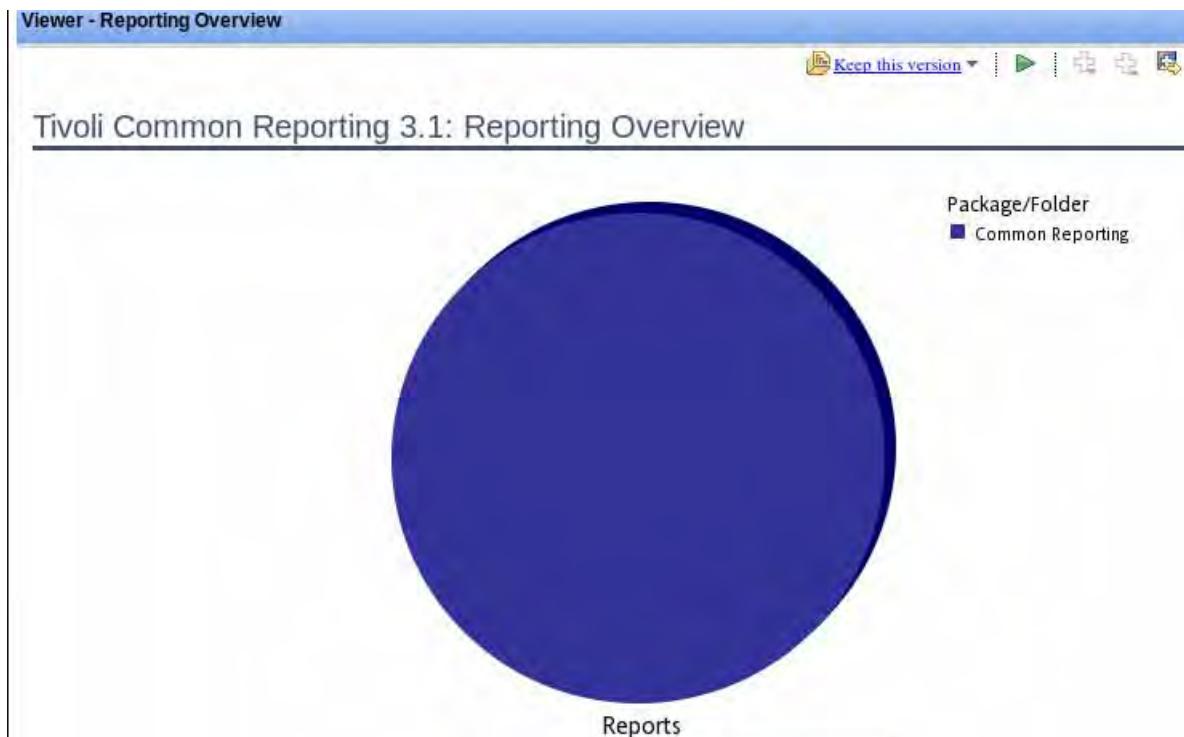


- c. Click **Reporting Overview** to run the report.



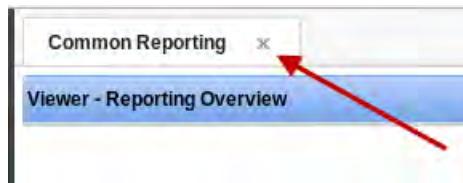
- d. Leave the default settings on the prompt page and click **Finish**.

The completed report opens.



This report lists all of the report templates that currently exist in the Tivoli Common Reporting report store database. Currently, there is only one, which is this report. This report verifies that Tivoli Common Reporting is able to generate a basic report.

4. Click the X to close the tab.



5. Modify environment settings for the **netcool** user.

The Cognos reporting engine for Tivoli Common Reporting requires access to various DB2 library files. This change is necessary only if you are creating reports from a DB2 data source. The Cognos reporting engine is started when Dashboard Application Services Hub starts. The engine runs as the same user that starts Dashboard Application Services Hub. For the class room environment that is the *netcool* user. The simplest way to make the library files available to the Cognos reporting engine is to modify the *netcool* user environment.

- a. Open the *netcool* user environment file for edit.

```
cd /home/netcool
```

```
gedit .bashrc
```

- b. Scroll down in the file and remove the comment character from the following line:

```
#source /home/db2inst1/sqlllib/db2profile
```

The modified line is shown as follows:

```
source /home/db2inst1/sqlllib/db2profile
```

- c. Save the file and exit gedit.



**Note:** The file **/home/db2inst1/sqlllib/db2profile** contains a definition for the **LD\_LIBRARY\_PATH** environment variable. This variable definition is what implements the required environment.

6. Verify the environment change.

- a. Source the modified file.

```
source .bashrc
```

- b. Test the change.

```
which db2
```

```
/home/db2inst1/sqlllib/bin/db2
```



**Important:** The command must return the correct path as shown here.

7. Log out of Dashboard Application Services Hub.

8. Close the Firefox browser.
9. Restart Dashboard Application Services Hub.

- a. Stop the server.

```
cd /opt/IBM/JazzSM/profile/bin
.stopServer.sh server1 -username smadmin -password object00
```

Wait for the server to stop.

- b. Check for a remaining Cognos process.

```
ps -ef | grep cognos
```

If you find a Cognos process, wait a short time and repeat the previous command.

- c. Start the server.

```
./startServer.sh server1
```

You restart Dashboard Application Services Hub to incorporate the environment setting changes.

A set of Tivoli Common Reporting reports are bundled with Netcool/OMNibus. The report package must be imported into Tivoli Common Reporting.

10. Copy the report package.

The report package file must be placed in a specific directory.

- a. Change to the source directory:

```
cd $OMNIHOME/extensions/tcr_event_reports
```

- b. Copy the file to the target directory:

```
cp Netcool_OMNIbus.zip /opt/IBM/JazzSM/reporting/cognos/deployment
```

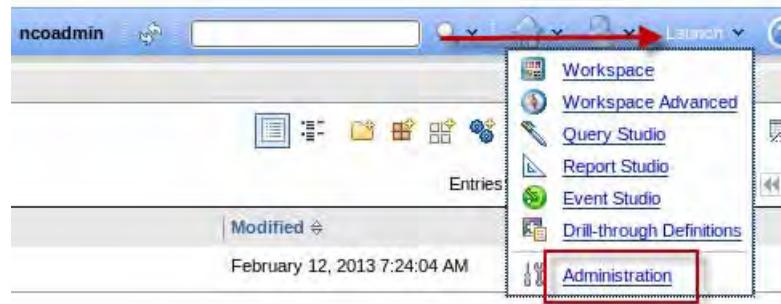
11. Import the package.

- a. Return to the browser.

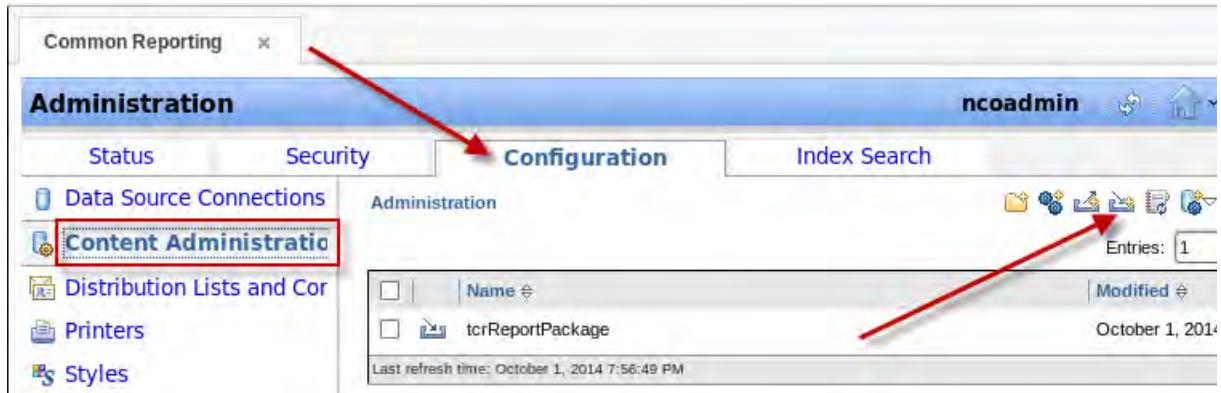
- b. Click the icon and select Common Reporting.



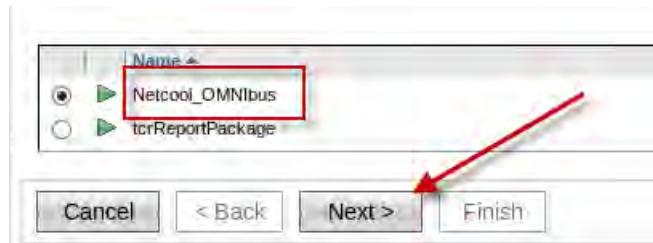
- c. Click **Launch** and select **Administration**.



- d. Click the **Configuration** tab.  
e. Click **Content Administration**.  
f. Click the indicated icon to start a **New Import**.

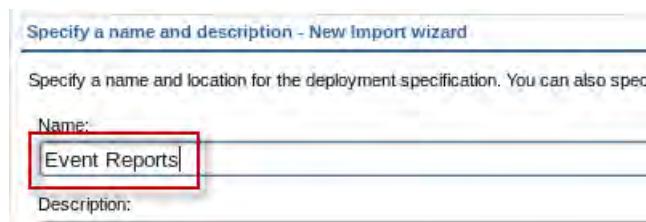


- g. Verify that the Netcool\_OMNIbus package is selected and click **Next**.



**Important:** If the Netcool\_OMNIbus package is not listed, it means that it was not copied to the correct location.

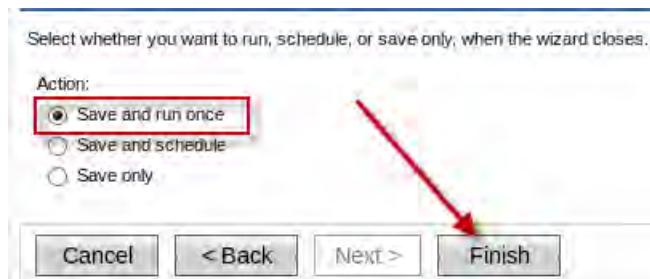
- h. Enter a name, and click **Next**.



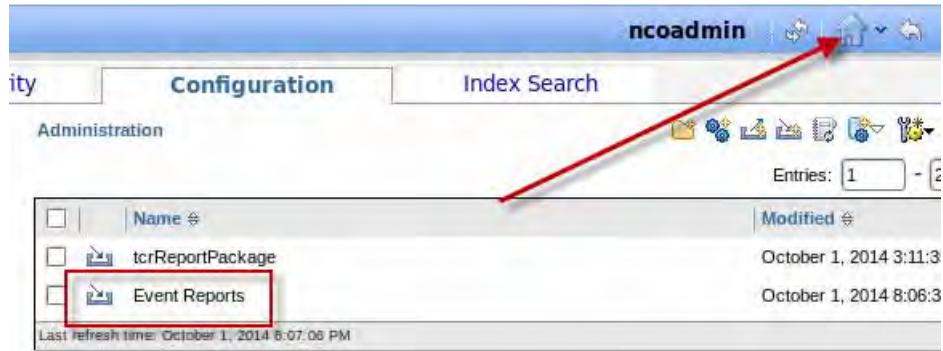
- i. Click the box to select the Netcool\_OMNIbus package and click **Next**.



- j. Scroll to the bottom of the page, and click **Next**.
- k. Scroll to the bottom of the page, and click **Next**.
- l. Leave the option set as shown and click **Finish**.



- m. Scroll to the bottom of the page, and click **Run**.
- n. Click **OK**.
- o. Click the icon to return to the home page.



The import process is complete.

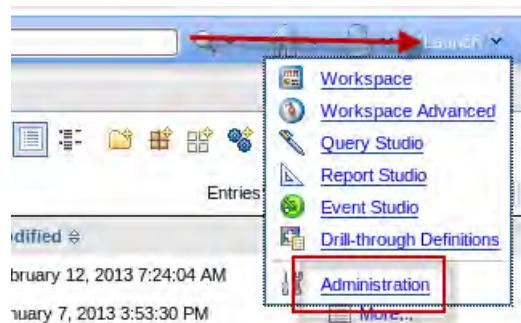


The Netcool/OMNibus report package is now available.

12. Create a data source.

A Tivoli Common Reporting data source defines the location of the database that reports use.

- Click **Launch** and select **Administration**.

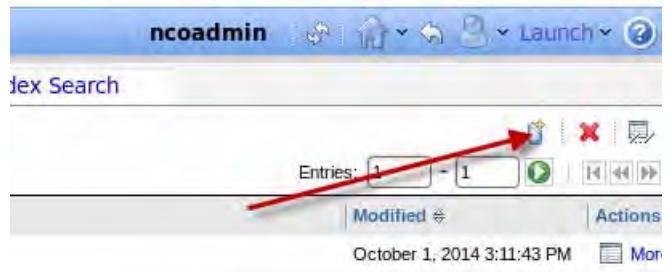


- Click the **Configuration** tab.
- Click **Data Source Connections**.



The available data sources are listed. The entry that is shown defines the location of the Tivoli Common Reporting report store database. The overview report run previously uses this data source.

- d. Click the indicated icon to create a new data source.



- e. Enter **Reporter** for the name and click **Next**.

Specify a name and description - New Data Source wizard

Specify a name and location for this entry. You can also specify a description.

Name: **Reporter**

Description:



**Important:** The name *must* be Reporter because this value is defined in the report templates.

- f. Select IBM DB2 for the database type.

- g. Remove the check mark to configure a JDBC connection and click **Next**.

Specify the parameters for the connection of this new data source. The name is Reporter.

Type: **IBM DB2**

Isolation level:

- Use the default object gateway
- Specify a value: **com.ibm.jdbc4**

Configure JDBC connection



**Note:** In a production environment, the database might be on a remote server. In that case, you can define a JDBC connection.

- h. Enter REPORTER for the DB2 database name.

Specify the IBM DB2 connection string - New Data Source wizard

Edit the parameters to build a DB2 connection string.

DB2 database name: **REPORTER**

DB2 connect string:

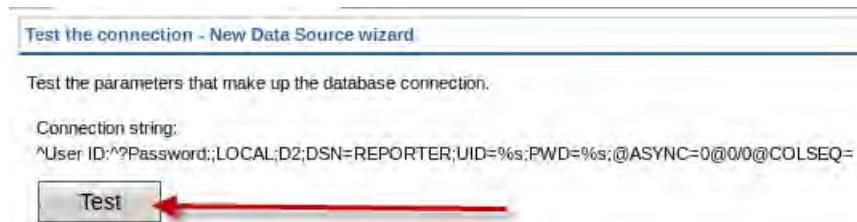


**Important:** This value must be REPORTER because it is the database name that is cataloged in DB2.

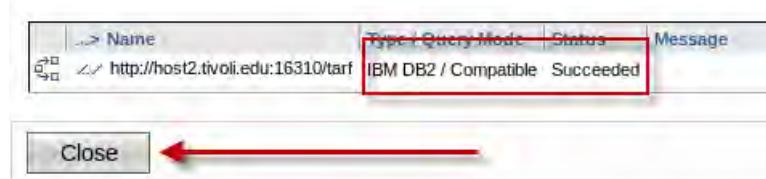
- i. Scroll down to the bottom of the page.
- j. Select the **Password** check box.
- k. Enter **db2inst1** for the user ID and **object00** for the password.
- l. Click the line that is labeled **Test the connection**.



- m. Click **Test**.



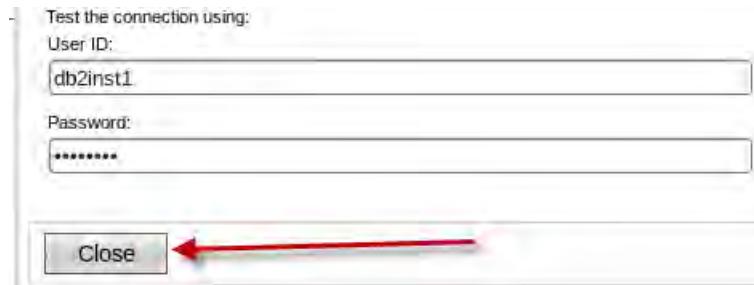
- n. Verify that the test is successful and click **Close**.



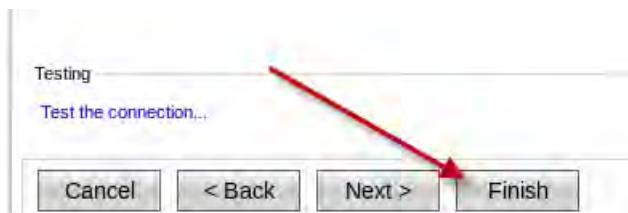


**Important:** If the test fails with QE-DEF-0285, it typically means that either the user ID or password is incorrect, or the **netcool** user environment variables are not correct.

- o. Scroll to the bottom of the page, and click **Close**.

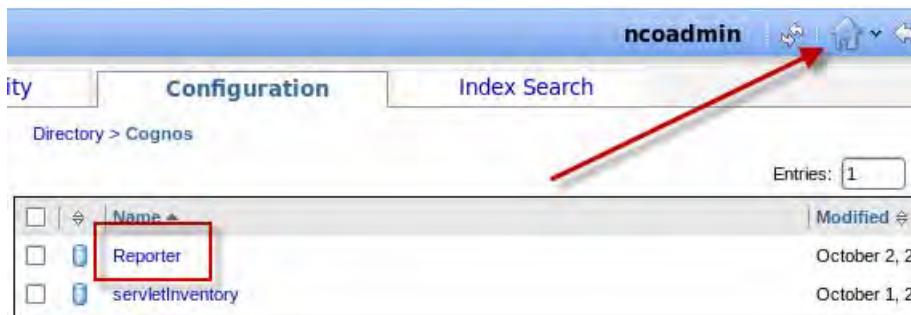


- p. Scroll to the bottom of the page, and click **Finish**.



The **Reporter** data source is shown in the list of available data sources.

- q. Click the icon to return to the report packages.



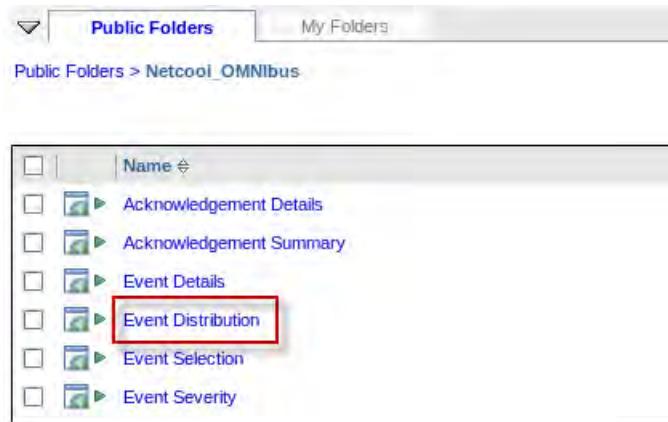
### 13. Verify the Netcool/OMNIbus reports.

- a. Click **Netcool\_OMNIbus** to view the report templates.

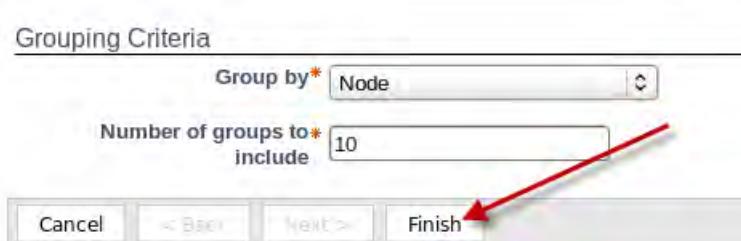


The list of reports opens.

b. Click **Event Distribution**.



- c. Leave all the default values on the prompt page, scroll to the bottom of the page, and click **Finish**.

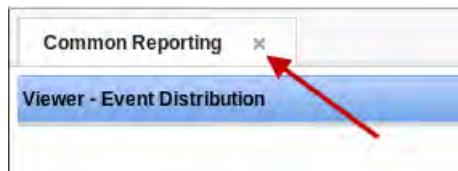


The report is generated.



The event distribution report opens.

14. Click the X to close the tab.



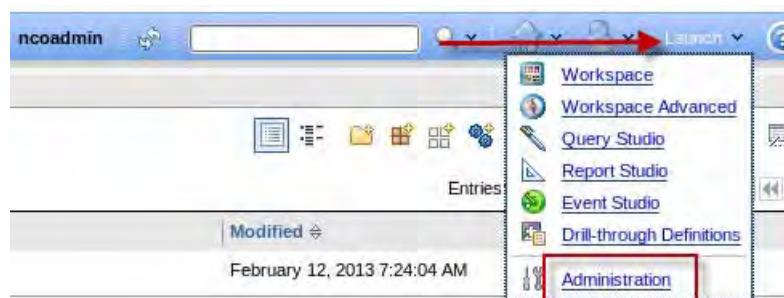
The smadmin user is configured with full access to Common Reporting features.

15. Modify Common Reporting to allow access for all other users.

a. Click the icon and select Common Reporting.



b. Click Launch and select Administration.



c. Click the Security tab.

d. Click Cognos.



16. Select **Authors**, and click the icon to set properties.

| Name                              | Modified                     | Actions |
|-----------------------------------|------------------------------|---------|
| Adaptive Analytics Administrators | February 23, 2016 1:33:09 AM |         |
| Adaptive Analytics Users          | February 23, 2016 1:34:52 AM |         |
| All Authenticated Users           | February 23, 2016 1:33:07 AM |         |
| Analysis Users                    | February 23, 2016 1:34:51 AM |         |
| Anonymous                         | February 23, 2016 1:33:16 AM |         |
| <b>Authors</b>                    | February 23, 2016 1:34:51 AM |         |
| Cognos Insight Users              | February 23, 2016 1:34:52 AM |         |

17. Click the **Members** tab, and click Add.

Set properties - Authors

General Members Permissions

Select the members of this entry.

Entries: [ ] - [ ]

| Name        | Type |
|-------------|------|
| No entries. |      |

Add... Remove

18. Click **Cognos**.

Available entries

Directory

Show users in the list

Entries: [1] - [2]

| Name        |
|-------------|
| Cognos      |
| VMMProvider |

19. Select All Authenticated Users. Click the green arrow icon to add the entry.

Available entries

Directory > Cognos

Show users in the list

Entries: [1] - [15]

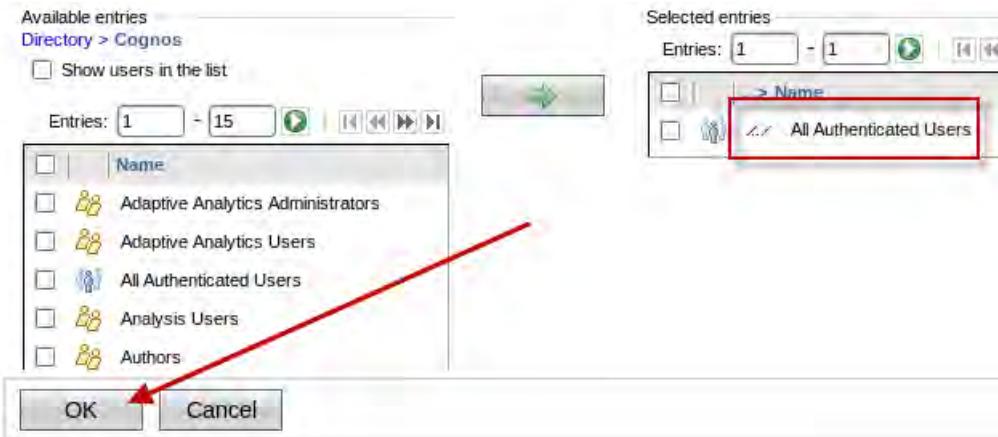
| Name                              |
|-----------------------------------|
| Adaptive Analytics Administrators |
| Adaptive Analytics Users          |
| <b>All Authenticated Users</b>    |

Selected entries

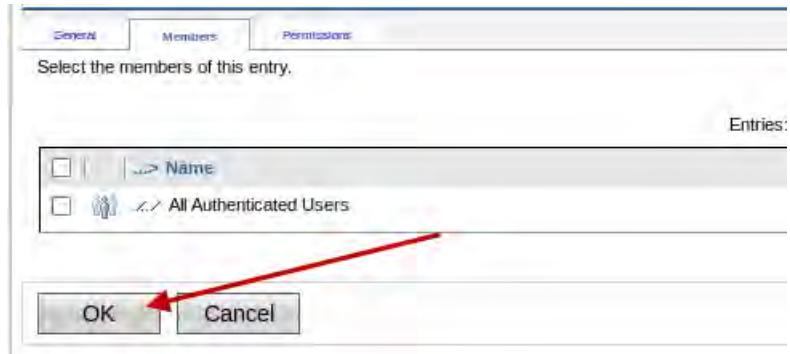
Entries: [ ] - [ ]

| Name        |
|-------------|
| No entries. |

20. Scroll to the bottom of the page and click **OK**.



21. Click **OK**.



**Note:** The tcrPortalOperator role grants access to the Common Reporting feature. The previous steps grant access to features within Common Reporting.

22. Log out of Dashboard Application Services Hub.

23. Close the Firefox browser.

# Exercise 5 Netcool/Impact

## Installing the software

In this exercise, you install the Netcool/Impact components. You are installing all of Netcool Operations Insight on a single server, which is not typically done in a production environment.

1. Expand the installation file as follows:

```
cd /software/impact
```

```
unzip Impact-v7.1.0.4 NOI.linux64.zip
```

2. Start IBM Installation Manager:

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

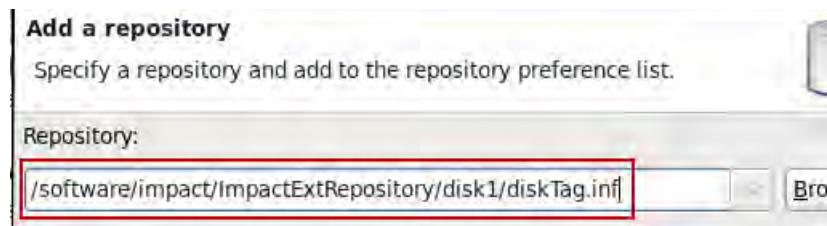
```
./IBMMIM
```

IBM Installation Manager opens.

3. Define the Impact repositories.

- a. Click **File** and select **Preferences**.
- b. Select **Repositories** and clear the check marks for all entries.
- c. Click **Add Repository**.
- d. Click **Browse** and select the following repository:

```
/software/impact/ImpactExtRepository/disk1/diskTag.inf
```



- e. Click **OK** to add the repository.
- f. Click **Add Repository**.
- g. Click **Browse** and select the following repository:

```
/software/impact/ImpactRepository/disk1/diskTag.inf
```



- h. Click **OK** to add the repository.
- i. Verify that the repositories are listed and click **OK**.



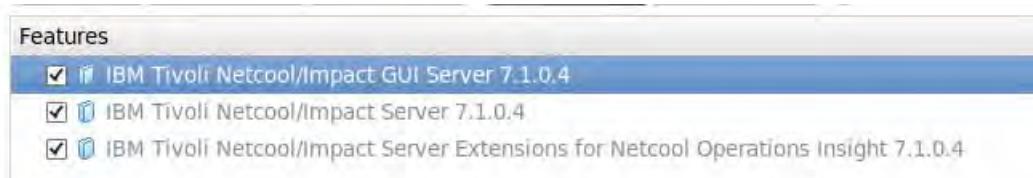
4. Start the installation.
- a. Click **Install**.
- b. Select all three packages and click **Next**.

| Installation Packages                                                                         | Status            | Vendor |
|-----------------------------------------------------------------------------------------------|-------------------|--------|
| IBM Tivoli Netcool/Impact GUI Server<br>Version 7.1.0.4                                       | Will be installed | IBM    |
| IBM Tivoli Netcool/Impact Server<br>Version 7.1.0.4                                           | Will be installed | IBM    |
| IBM Tivoli Netcool/Impact Server Extensions for Netcool Operations Insight<br>Version 7.1.0.4 | Will be installed | IBM    |

- c. Accept the license agreement and click **Next**.
- d. Leave the option set to **Create a new package group** and click **Next**.

The screenshot shows a configuration dialog for creating a new package group. It has two radio button options: "Use the existing package group" (unchecked) and "Create a new package group" (checked). Below the radio buttons, there is a table with two columns: "Package Group Name" containing "IBM Tivoli Netcool Impact" and "Installation Directory" containing "/opt/IBM/tivoli/impact".

- e. Accept the default list of features and click **Next**.



- f. Select **Local File Based** and click **Next**.



- g. Click **OK**.



- h. Enter **object00** for the password and click **Next**.

Provide an administrative user ID and password for Impact

Impact User ID  
impactadmin

Impact Password (Minimum 6 characters)  
[REDACTED]

Confirm Impact Password  
[REDACTED]

- i. Change the starting port number for the GUI Server to **17310** and click **Next**.

Common Configurations

Profile Ports

Impact requires a range of ports to run. Specify the starting port of the range.

Starting port number for Impact Server  
9080

Starting port number for GUI Server  
17310



**Important:** You must change the default start port number to avoid a conflict with Dashboard Application Services Hub.

- j. Accept the default values for the host name and port number. Click **Next**.
- k. Accept the default values for the instance name, cluster name, and command-line port. Click **Next**.
- l. Accept the default values for the Derby database and click **Next**.
- m. Review the installation summary and click **Install**.



**Note:** The installation runs approximately 15 minutes.

- n. Verify that the installation is successful and click **Finish**.



The screenshot shows the IBM Installation Manager interface after a successful installation. A green checkmark icon indicates success. The message "The packages are installed. [View Log File](#)" is displayed. The log window shows the following text:

```
IMPACTIN212I Local file based user authentication is the basic and the least secured user authentication configuration.
After installing Impact, you can reconfigure to an LDAP repository or ObjectServer repository.
The following packages were installed:
 ▾ IBM Tivoli Netcool Impact
 IBM Tivoli Netcool/Impact GUI Server 7.1.0.4
 IBM Tivoli Netcool/Impact Server 7.1.0.4
 IBM Tivoli Netcool/Impact Server Extensions for Netcool Operations Insight 7.1.0.4
```

5. Click **File** and select **Exit** to close IBM Installation Manager.
6. Remove the installation files.

```
cd /software
/bin/rm -R impact
```

## Configuring Netcool/Impact to use LDAP

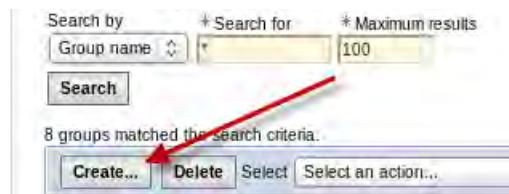
LDAP configuration is completed by updating a properties file and running a script, which are both provided by Netcool/Impact. Before you configure Netcool/Impact to use LDAP, you must create an Impact administrator user in LDAP.

1. Open a Firefox browser.
2. Log in to Dashboard Application Services Hub as the **smadmin** user with password **object00**.

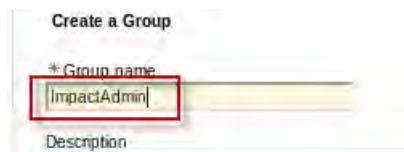
3. Open the WebSphere administrative console.
4. Expand **Users and Groups** and click **Manage Groups**.



5. Click **Create**.



6. Enter **ImpactAdmin** for the Group name. Click **Create**.



**Important:** The group name must be ImpactAdmin.

7. Click **Close**.



8. Expand **Users and Groups** and click **Manage Users**.



9. Click **Create**.



10. Enter **impactadmin** for the user ID. Enter values for the first and last name fields. Enter **object00** for the password. Click **Groups**.

The screenshot shows the 'General' tab of a user creation dialog. The 'User ID' field contains 'impactadmin'. The 'First name' field contains 'Impact' and the 'Last name' field contains 'Admin'. The 'Password' and 'Confirm password' fields both contain '\*\*\*\*\*'. At the bottom are 'OK', 'Apply', and 'Cancel' buttons. A red arrow points from the text above to the 'Groups' tab at the top right.

11. Click **Add**.

The screenshot shows a user profile page with a 'Groups' section. It displays the message 'The user is a member of 0 groups.' Below this are 'Add...' and 'Remove' buttons. A red arrow points to the 'Add...' button.

12. Enter **Impact\*** and click **Search**.

The screenshot shows the 'Add a User to Groups' search interface. The 'User ID' field contains 'impactadmin'. The 'Search by' dropdown is set to 'Group name'. The 'Search for' field contains 'Impact\*'. The 'Maximum results' field is set to '100'. A red arrow points to the 'Search' button.

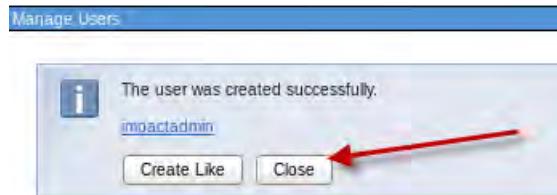
13. Click **ImpactAdmin** to select it. Click **Add**.

The screenshot shows the search results for 'Impact\*'. It displays a single result: 'ImpactAdmin'. This result is highlighted with a red box. At the bottom of the screen, there is an 'Add' button.

14. Click **Close**.

15. Click **Create**.

16. Click **Close**.



17. Log out of WebSphere administrative console.

18. Close the Firefox tab.

19. Log out of Dashboard Application Services Hub.

20. Modify the property file as follows.

a. Change to the target directory:

```
cd /opt/IBM/tivoli/impact/install/security
```

b. Save a copy of the original file:

```
cp impactdap.properties impactdap.properties.orig
```

c. Modify the file:

```
gedit impactdap.properties
```

- d. Configure the following property values:

```
LDAPServerType="IBM Tivoli Directory Server"
LDAPHost="host1.csuite.edu"
LDAPPort="389"
LDAPBindDN="cn=root"
LDAPBaseEntry="DC=IBM,DC=COM"
LDAPSSLEnabled="false"
LDAPSSORealm="defaultWIMFileBasedRealm"
```

- e. Save the file and exit the gedit utility.

21. Run the configuration script.

```
./confAuth4LDAP.sh enable impactadmin object00 object00 object00
.
.
.
startNCI:
[echo] Attempting to start the Impact NCI Server...
[exec] Starting server NCI.
[exec] Server NCI started with process ID 6283.
.
.
.
startGUI:
[echo] Attempting to start the Impact GUI Server...
[exec] Starting server ImpactUI.
[exec] Server ImpactUI started with process ID 6745.
.
.
.
BUILD SUCCESSFUL
Total time: 2 minutes 45 seconds
```



**Important:** The build must be successful before you continue.

22. Verify that the **impactadmin** user can access Netcool/Impact.

- Open a Firefox browser, if necessary.
- Enter the following URL:

```
http://host1.csuite.edu:17310/ibm/console
```



**Note:** If prompted, accept all security messages.

- c. Log in with user **impactadmin** and password **object00**.  
Verify that the user can access Netcool/Impact.
  - d. Log out.
23. Close the Firefox browser.

## Configuring Netcool/Impact to use single sign-on

You must configure single sign-on to allow federation or console integration between Netcool/Impact and the IBM Dashboard Applications Services Hub (DASH). For single sign-on (SSO) to work, you need a common user repository between your products, for example LDAP or ObjectServer. Also, your SSO parameter settings must be consistent between your products. For this class, you use LDAP as the common user repository.

1. Open a Firefox browser.
2. Log in to Dashboard Application Services Hub as user **smadmin** with password **object00**.
3. Start WebSphere administrative console.
4. Enable single sign-on as follows:
  - a. Expand **Security** and click **Global security**.



- b. Locate the *Authentication* section on the Global security page. Expand **Web and SIP security**. Click **Single sign-on (SSO)**.

**Authentication**  
Authentication mechanisms and expiration

[LTPA](#)  
 [Kerberos and LTPA](#)  
[Kerberos configuration](#)  
 [SWAM \(deprecated\): No authenticated communication between](#)  
[Authentication cache settings](#)

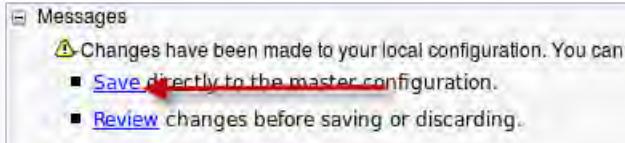
[Web and SIP security](#)

[General settings](#)  
**[Single sign-on \(SSO\)](#)**  
[SPNEGO web authentication](#)

- c. Verify that SSO is enabled. Enter **.csite.edu** for the domain name. Enter **LtpaToken2** for the cookie name. Click **OK**.



- d. Click **Save**.



5. Import the Netcool/Impact SSL certificate into the Dashboard Applications Services Hub truststore.

- a. Under **Security**, click **SSL certificate and key management**.



- b. Under the *Related Items* section, select the **Key stores and certificates** link.



- c. Select the **NodeDefaultTrustStore** keystore.

| Select                                      | Name                                  | Description                          | Management Scope                             |
|---------------------------------------------|---------------------------------------|--------------------------------------|----------------------------------------------|
| You can administer the following resources: |                                       |                                      |                                              |
| <input type="checkbox"/>                    | <a href="#">NodeDefaultKeyStore</a>   | Default key-store for JazzSMNode01   | (cell):JazzSMNode01Cell; (node):JazzSMNode01 |
| <input type="checkbox"/>                    | <a href="#">NodeDefaultTrustStore</a> | Default trust store for JazzSMNode01 | (cell):JazzSMNode01Cell; (node):JazzSMNode01 |

- d. Under the *Additional Properties* section, select the **Signer certificates** link.



- e. Select **Retrieve from port**.



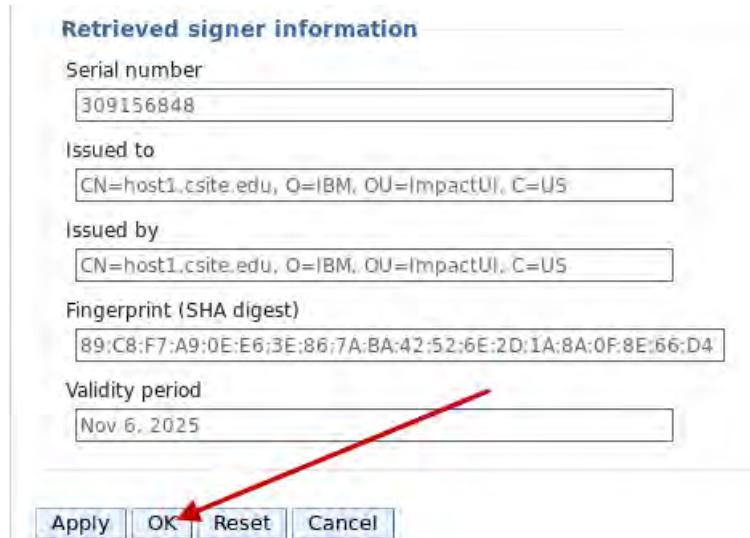
- f. Enter **host1.csuite.edu** for the host. Enter **17311** for the port. Enter **Impact\_SSL** for the alias. Click **Retrieve signer information**.

The screenshot shows the **General Properties** dialog with the following fields:

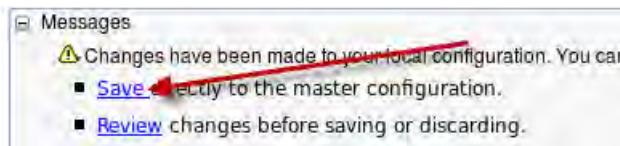
- \* Host: **host1.csuite.edu**
- \* Port: **17311**
- SSL configuration for outbound connection: **NodeDefaultSSLSettings**
- \* Alias: **Impact\_SSL**

A red arrow points to the **Retrieve signer information** button at the bottom right of the dialog.

- g. Review the certificate details, and click **OK**.



- h. Click **Save**.

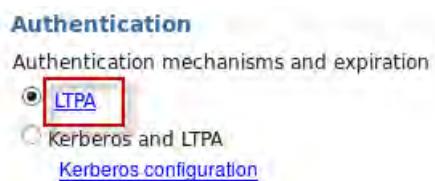


6. Export the ltpa.keys file from the Dashboard Applications Services Hub.

- a. Under **Security**, click **Global security**.



- b. Under **Authentication**, click **LTPA**.



- c. Enter **object00** for the password. Enter **/tmp/dash\_keys** for the file name. Click **Export keys**.

**Cross-cell single sign-on**

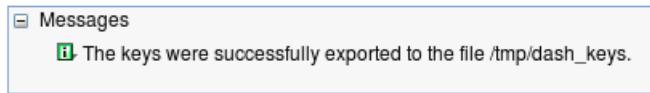
Single sign-on across cells can be provided by sharing keys and password files. To do this, enter a password and click Export keys. Then, log on to the other cell, specify the password and key file, and click Import keys. Then, log on to the other cell, specify the password and key file, and click Import keys.

\* Password  \*\*\*\*\*

\* Confirm password  \*\*\*\*\*

Fully qualified key file name  /tmp/dash\_keys

- d. Verify that the keys are exported.



7. Log out of WebSphere administrative console
8. Close the Firefox tab.
9. Log out of Dashboard Application Services Hub.
10. Copy the exported keys file into Netcool/Impact:

```
cp /tmp/dash_keys
/opt/IBM/tivoli/impact/wlp/usr/servers/ImpactUI/resources/security/ltpa.keys
```

```
cp /tmp/dash_keys
/opt/IBM/tivoli/impact/wlp/usr/servers/NCI/resources/security/ltpa.keys
```

11. Run the Netcool/Impact single sign-on configuration script.

```
cd /opt/IBM/tivoli/impact/install/security

. ./configImpactSSO.sh "defaultWIMFileBasedRealm" "LtpaToken2" ".csite.edu"
object00 object00

.
.
.

startNCI:
[echo] Attempting to start the Impact NCI Server...
[exec] Starting server NCI.
[exec] Server NCI started with process ID 8891.

.
.
.

startGUI:
```

```
[echo] Attempting to start the Impact GUI Server...
[exec] Starting server ImpactUI.
[exec] Server ImpactUI started with process ID 9014.

.
.
.

BUILD SUCCESSFUL
Total time: 1 minute 36 seconds
```



**Important:** The build must be successful before you continue.

12. Verify that the **impactadmin** user can access Netcool/Impact.

a. Open a Firefox browser, if necessary.

b. Enter the following URL:

<http://host1.csite.edu:17310/ibm/console>

c. Log in with user **impactadmin** and password **object00**.

Verify that the user can access Netcool/Impact.

d. Log out.

13. Close the Firefox browser.

## Integrating the Netcool/Impact console

In this step, you define a console integration for Netcool/Impact. With this feature defined, a user can log in to Dashboard Application Services Hub and access Netcool/Impact.



**Important:** The user that adds the console integration must be a valid Netcool/Impact user. The user must also have access to Dashboard Application Services Hub administration.

Add the **iscadmins** role to the **impactadmin** user to grant Dashboard Application Services Hub administration access to the user.

1. Open a Firefox browser.

2. Log in to Dashboard Application Services Hub as user **smadmin** with password **object00**.

- Click the icon and select **User Roles**.



- Enter **impactadmin** and click **Search**.

User ID: impactadmin  
Number of results to display: 20  
Search

- Click **impactadmin**.

| Select | User ID     | Active     | First Name |
|--------|-------------|------------|------------|
|        | impactadmin | Not Active | Impact     |

- Scroll down and select **iscadmins**. Click **Save**.



- Log out as user **smadmin**.

- Log in to Dashboard Application Services Hub as user **impactadmin** with password **object00**.

- Click the icon and select **Console Integrations**.



10. Click the icon to create a new entry.



11. Enter **NetcoolImpact** for the name. Enter the following value for the URL:

`https://host1.csuite.edu:17311/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 external system.

\* Required field

|                           |                                                              |
|---------------------------|--------------------------------------------------------------|
| Console Integration ID:   |                                                              |
| Console Integration Name: | NetcoolImpact                                                |
| Console Integration URL:  | <code>https://host1.csuite.edu:17311/ibm/console/rest</code> |
| Integration Location:     | console/Console Integrations                                 |

12. Click **Test** to verify the connection.

Test your UI to see which tasks will be integrated into this console.

**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 |

13. Click **Save** to create the entry.

The entry is included in the list.

| Select | Name          | Status                |
|--------|---------------|-----------------------|
|        | NetcoolImpact | Connection Successful |

Access to the Impact console is shown as a new icon on the navigation bar.



**Important:** The icon is visible only for users that are valid Netcool/Impact users.

14. Click the **snowflake** icon and select **Impact**.



The Netcool/Impact console opens.



15. Log out of Dashboard Application Services Hub.

## Enabling users for access to the Netcool/Impact console

Access to Netcool/Impact features is controlled through Netcool/Impact roles. The Netcool/Impact roles are separate from Dashboard Application Services Hub roles and are managed with a command-line utility. The best way to implement access is to assign the required role to a group. In a production environment, you typically create a special group for this purpose. In the student exercise, you use the existing Netcool\_Admin group. The following steps demonstrate how to add the Netcool/Impact role to the Netcool\_Admin group.

1. List the available Netcool/Impact roles as follows:

```
cd /opt/IBM/tivoli/impact/install/security/
```

```
./mapRoles.sh -list -all
```

Roles:

```
impactOSLCDDataProviderUser
impactEmailUser
impactAdminUser
impactFullAccessUser
impactOpViewUser
impactUIDataProviderUser
impactEmailUser
ConsoleUser
```

WriteAdmin

ReadAdmin

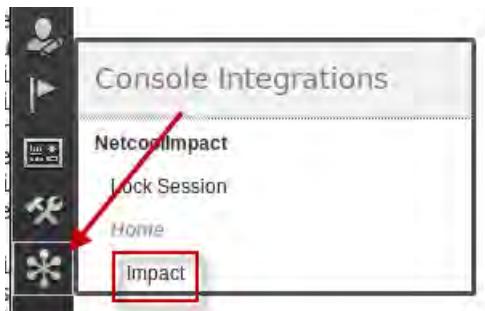
2. Add the impactAdminUser role to the Netcool\_Admin group as follows:

```
./mapRoles.sh -add -group Netcool_Admin -roles "impactAdminUser"
```

```
Adding group Netcool_Admin to role impactAdminUser
```

The change takes place immediately. You do not need to restart Netcool/Impact.

3. Log in to Dashboard Application Services Hub as the **ncoadmin** user with password **object00**.
4. Click the *snowflake* icon and select Impact.



The Netcool/Impact console opens.



5. Log out of Dashboard Application Services Hub.



**Hint:** If you receive a connection error message, log out of Dashboard Application Services Hub. Close the browser, open a new browser, and repeat the steps.

# Configuring Netcool/Impact to start at system start

Several ways exist to configure Netcool/Impact to start at system start time. The following steps use a start script in `/etc/init.d`.

1. Configure Netcool/Impact to automatically start:

- a. Change to the root user.

```
su -
Password: object00
```

- b. Copy the supplied start script:

```
cd /workshop/etc/init.d
cp impact /etc/init.d
cp impact_gui /etc/init.d
```

- c. Change the file permissions to allow execution:

```
cd /etc/init.d
chmod +x impact
chmod +x impact_gui
```

- d. Create the logical links to enable the autostart feature:

```
chkconfig impact on
chkconfig impact_gui on
```

2. Restart the Netcool/Impact components.

- a. Stop the NCI server component.

```
/etc/init.d/impact stop
```

```
Stopping server NCI.
Server NCI stopped.
```

- b. Stop the GUI server component.

```
/etc/init.d/impact_gui stop
```

```
Stopping server ImpactUI.
Server ImpactUI stopped.
```

- c. Start the GUI server component.

```
/etc/init.d/impact_gui start
```

```
Starting server ImpactUI.
Server ImpactUI started with process ID 19568.
```



**Note:** The command is submitted to the background. The server is started when you see the message ImpactUI started. Press Enter to see the cursor.

- d. Start the NCI server component.

```
/etc/init.d/impact start
```

Starting server NCI.

Server NCI started with process ID 20101.



**Note:** The command is submitted to the background. The server is started when you see the message NCI started. Press Enter to see the cursor.

- e. Exit the root user back to the netcool user.

```
exit
```

3. Open a Firefox browser.

4. Enter the following URL:

```
http://host1.csite.edu:17310/ibm/console
```

5. Log in with user **impactadmin** and password **object00**.

A successful login verifies that Netcool/Impact started when the server started.



6. Log out of Netcool/Impact.

7. Close the Firefox browser.

# Exercise 6 IBM Operations Analytics Log Analysis

## Verifying prerequisites

Before you install IBM Operations Analytics Log Analysis, ensure that the system meets the hardware and software requirements and complete the prerequisite tasks.

1. Open a terminal window if necessary.

2. Change to the **root** user:

```
su -
Password: object00
```

3. Verify the version of RHEL as follows:

```
cat /etc/redhat-release
```

Red Hat Enterprise Linux Server release 6.5 (Santiago)

IBM Operations Analytics Log Analysis requires Red Hat Enterprise (RHEL) for Linux version 5 or 6.

4. Verify 64-bit library requirement as follows:

```
rpm -qa | grep compat-libstdc++
compat-libstdc++-33-3.2.3-69.el6.i686
compat-libstdc++-33-3.2.3-69.el6.x86_64
compat-libstdc++-296-2.96-144.el6.i686
```

For Red Hat Enterprise Linux, IBM Operations Analytics Log Analysis requires the 64-bit `compat-libstdc++` library.

5. Verify Security-Enhanced Linux mode as follows:

```
more /etc/selinux/config
```

```
This file controls the state of SELinux on the system.
SELINUX= can take one of these three values:
enforcing - SELinux security policy is enforced.
permissive - SELinux prints warnings instead of enforcing.
disabled - SELinux is fully disabled.
SELINUX=disabled
```

If SELinux is in enforcing mode, an exception occurs during the installation of IBM Operations Analytics Log Analysis. Ensure that the SELinux policy is set to a permissive or disabled state.

6. Verify Python as follows:

```
rpm -qa | grep "python-2"
```

**python-2.6.6-52.el6.x86\_64**

IBM Operations Analytics Log Analysis supports Python Version 2.6.6 to 2.6.8.

7. Verify host server IP address and names as follows:

- To verify that the host name is configured correctly, enter the following command:

```
hostname
```

**host1.csuite.edu**

- To verify that the host name uses the fully qualified host name, enter the following command:

```
hostname -f
```

**host1.csuite.edu**

- To confirm that the IP address is configured correctly, ping the host name:

```
ping -c 3 host1.csuite.edu
```

```
PING host1.csuite.edu (192.168.100.100) 56(84) bytes of data.
```

```
64 bytes from host1.csuite.edu (192.168.100.100): icmp_seq=1 ttl=64
```

```
time=0.015 ms
```

```
64 bytes from host1.csuite.edu (192.168.100.100): icmp_seq=2 ttl=64
```

```
time=0.051 ms
```

```
64 bytes from host1.csuite.edu (192.168.100.100): icmp_seq=3 ttl=64
```

```
time=0.024 ms
```

8. Exit the root user to return to the **netcool** user.

```
exit
```

9. Verify the default number of open files limit as follows:

```
ulimit -n
```

**131073**

10. Verify the virtual memory limit as follows:

```
ulimit -v
```

**unlimited**

The suggested `ulimit -v` setting, which limits the virtual memory for processes, is **unlimited**.

11. Verify the locale setting as follows:

```
env | grep ^LANG
```

LANG=en\_US.UTF-8

You must set the locale of the command shell to export LANG=en\_US.UTF-8 before you run any IBM Operations Analytics Log Analysis scripts.

## Installing the software

IBM Operations Analytics Log Analysis is installed with IBM Installation Manager.

1. Expand the installation file as follows:

```
cd /software/la
```

```
gunzip OALA_1.3.2_ENTRY_LINUX_64_BIT.tar.gz
```

```
mkdir lacore
```

```
cd lacore
```

```
tar -xvf ../OALA_1.3.2_ENTRY_LINUX_64_BIT.tar
```

2. Start IBM Installation Manager:

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

IBM Installation Manager opens.

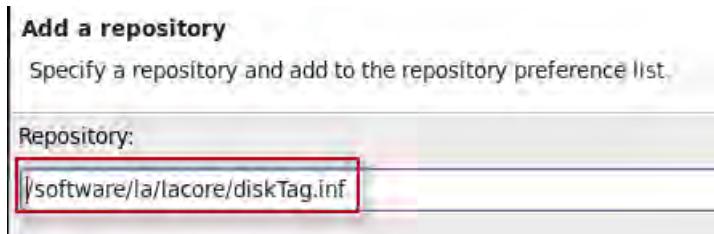
3. Define the Log Analysis repository.

- a. Click **File** and select **Preferences**.

- b. Select **Repositories** and remove all of the existing repository entries. Click **Add Repository**.

- c. Click **Browse** and select the following repository:

```
/software/la/lacore/diskTag.inf
```



- d. Click **OK** to add the repository.

- e. Verify that the repository is listed and click **OK**.

4. Start the installation.

a. Click **Install**.



b. Select the package and click **Next**.

| Installation Packages                                                                                                                      | Status            | Vendor |
|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------|
| <input checked="" type="checkbox"/> IBM Operations Analytics - Log Analysis<br><input checked="" type="checkbox"/> 1.3.2.0 Version 1.3.2.0 | Will be installed | IBM    |

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

d. Leave the option set to **Create a new package group**.

e. Change the installation directory to **/opt/IBM/LogAnalysis** and click **Next**.

Create a new package group

| Package Group Name                      | Installation Directory |
|-----------------------------------------|------------------------|
| IBM Operations Analytics - Log Analysis | /opt/IBM/LogAnalysis   |

Package Group Name: IBM Operations Analytics - Log Analysis  
Installation Directory:   
Architecture Selection:  32-bit  64-bit

f. Accept the default list of features and click **Next**.

| Features                                                                            |
|-------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> IBM Operations Analytics - Log Analysis 1.3.2.0 |
| <input checked="" type="checkbox"/> IBM Operations Analytics - Log Analysis 1.3.2.0 |
| <input checked="" type="checkbox"/> Apache Solr 5.2.1                               |
| <input checked="" type="checkbox"/> IBM Tivoli Log File Agent 06.30.00.04           |

- g. Accept the default port numbers and click **Next**.

**Configuration for IBM Operations Analytics - Log Analysis 1.3.1.0**

IBM Operations Analytics - Log Analysis Port Configuration:

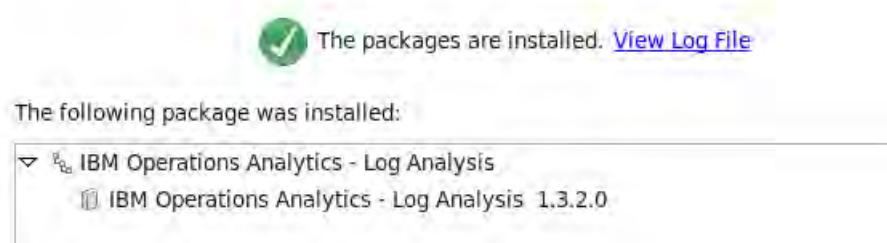
|                                     |       |
|-------------------------------------|-------|
| Application WebConsole Port:        | 9988  |
| Application WebConsole Secure Port: | 9987  |
| Database Server Port:               | 1627  |
| EIF Receiver Port:                  | 5529  |
| ZooKeeper Port:                     | 12181 |
| Apache Solr Search Port:            | 8983  |
| Apache Solr Stop Port:              | 7205  |

- h. Review the installation summary and click **Install**.



**Note:** The installation runs approximately 15 minutes.

- i. Verify that the installation is successful and click **Finish**.



5. Click **File** and select **Exit** to close IBM Installation Manager.
6. Open a Firefox browser if necessary.
7. Connect to the following URL:  
<https://host1.csite.edu:9987/Unity/>
8. Accept the security warnings and import the certificate.
9. Log in as **unityadmin** with password **unityadmin**.

10. Verify access and log out.

The screenshot shows the IBM Operations Analytics Log Analysis interface. At the top, there's a navigation bar with links for 'New Search' and '+ Add Search'. On the right side of the header, there are buttons for 'Administrative Settings', 'Learn More', and a dropdown menu for the user 'unityadmin'. The 'unityadmin' dropdown menu has options for 'Change Password' and 'Logout', with 'Logout' also highlighted by a red box and a red arrow pointing to it from the top right.

11. Close the Firefox browser.

## Configuring Log Analysis to use LDAP

LDAP configuration is completed by updating a properties file and running a script, which are both provided by Log Analysis. Before you configure Log Analysis to use LDAP, you must set the default Log Analysis users and groups in LDAP.

1. Open a Firefox browser.
2. Log in to Dashboard Application Services Hub as the **smadmin** user with password **object00**.
3. Open the WebSphere administrative console.
4. Expand **Users and Groups** and click **Manage Groups**.



5. Click **Create**.



6. Enter **UnityAdmins** for the Group Name. Click **Create**.



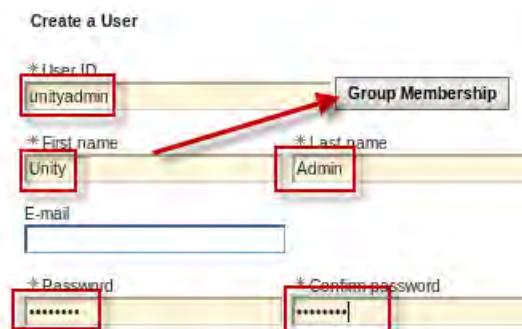
7. Click **Close**.
8. Repeat the previous step and create the **UnityUsers** group.
9. Expand **Users and Groups** and click **Manage Users**.



10. Click **Create**.



11. Enter **unityadmin** for the User ID. Enter values for the first and last name fields. Enter **object00** for the password. Click **Group Membership**.

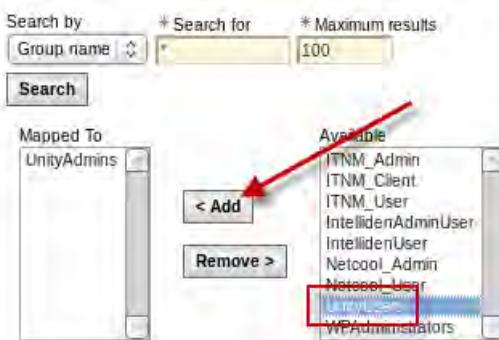


12. Click **Search** to display the available groups.

13. Click **UnityAdmins** to select the entry. Click **Add**.



14. Click **UnityUsers** to select the entry. Click **Add**. Click **Close**.



The **unityadmin** user is now a member of the UnityAdmins and UnityUsers groups.

15. Click **Create**.

16. Click **Close**.

17. Repeat the previous steps to create the **unityuser** user ID and assign the user to the UnityUsers group.

18. Log out of WebSphere administrative console.

19. Close the Firefox tab.

20. Log out of Dashboard Application Services Hub.

21. Modify the property file as follows.

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/utilities
```

- b. Save a copy of the original file:

```
cp ldapRegistryHelper.properties ldapRegistryHelper.properties.orig
```

- c. Modify the file:

```
gedit ldapRegistryHelper.properties
```

- d. Configure the following property values:

```
ldap_type_property=IBM Tivoli Directory Server
ldap_hostname_property=host1.csite.edu
ldap_port_property=389
ldap_baseDN_property=DC=IBM,DC=COM
ldap_bindDN_property=cn=root
ldap_bindPassword_property=object00
ldap_realm_property=defaultWIMFileBasedRealm
ldap_id_property=LdapRegistryId
ldap_ignoreCase_property=true
```

- e. Save the file and exit the gedit utility.

22. Run the configuration script to *create* the `ldapRegistry.xml` file.

```
./ldapRegistryHelper.sh config
```

```
.
```

```
Calling ldapRegistryHelper ant script.
```

```
Buildfile: /opt/IBM/LogAnalysis/utilities/xml/ldapRegistryHelper_config.xml
```

```
.
```

```
.
```

```
.
```

```
BUILD SUCCESSFUL
```

```
Total time: 6 seconds
```



**Important:** The build must be successful before you proceed.

23. Run the configuration script to *enable* the `ldapRegistry.xml` file.

```
./ldapRegistryHelper.sh enable
```

```
.
```

```
Calling ldapRegistryHelper ant script.
```

```
Buildfile: /opt/IBM/LogAnalysis/utilities/xml/ldapRegistryHelper_enabler.xml
```

```
.
```

```
.
```

```
.
```

```
BUILD SUCCESSFUL
```

```
Total time: 0 seconds
```



**Important:** The build must be successful before you proceed.

24. Verify that LDAP is configured for use as follows:

```
more /opt/IBM/LogAnalysis/wlp/usr/servers/Unity/server.xml
```

```
</httpEndpoint>
```

```
<!-- Include the basic registry predefined with default users and groups -->
```

```
<!--<include optional="true" location="${server.config.dir}/unityUserRegistry.xml"/>
```

```
<!-- Include the LDAP registry -->
```

```
<!--<include optional="true" location="${server.config.dir}/ldapRegistry.xml"/>
```

```
<!-- Include the Unity configuration for war control and role mapping -->
```

25. Verify that the line that references the `unityUserRegistry.xml` file is commented out. Verify that the file contains a line that references the `ldapRegistry.xml` file.

26. Stop Log Analysis as follows:

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

```
IBM Operations Analytics Log Analysis v1.3.2.0 Application Services Status:
```

No.	Service	Status	Process ID
<hr/>			
1	Derby Network Server	UP	25912
2	ZooKeeper	UP	26021
3	Websphere Liberty Profile	UP	26516
4	EIF Receiver	UP	26880
5	Log File Agent instance	UP	27711
<hr/>			

Getting status of Solr on host1.tivoli.edu

Status of Solr Nodes:

No.	Instance Name	Host	Status	State
<hr/>				
1	SOLR_NODE_LOCAL	host1.csuite.edu	UP	ACTIVE
<hr/>				

All Application Services are in Running State

Checking server initialization status: Server has initialized!

Stopping IBM Operations Analytics v1.3.2.0 Application Services...

Stopping Log File Agent...

Processing. Please wait...

Stopping Tivoli Log File Agent ...

Product Tivoli Log File Agent was stopped gracefully.

Agent stopped...

Stopped Log File Agent Process...

Stopping EIF Receiver Process...

Waiting for EIF Receiver stop...

Stopped EIF Receiver...

Stopping Websphere Liberty Profile...

Stopping server Unity.

Server Unity stopped.

Stopped Websphere Liberty Profile...

Stopping Solr on host1.tivoli.edu

Stopped Solr

Stopping ZooKeeper Service...

JMX enabled by default

Using config: /opt/IBM/LogAnalysis/zookeeper-3.4.6/bin/..../conf/zoo.cfg

Stopped ZooKeeper Service...

Stopping Derby Network Server...

Mon Apr 06 20:33:37 UTC 2015 : Apache Derby Network Server - 10.10.2.1 - (1643489) shutdown

Stopped All Services...

27. Start Log Analysis as follows:

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

IBM Operations Analytics Log Analysis v1.3.2.0 Application Services Status:

No.	Service	Status	Process ID
1	Derby Network Server	DOWN	
2	ZooKeeper	DOWN	
3	Websphere Liberty Profile	DOWN	
4	EIF Receiver	DOWN	
5	Log File Agent instance	DOWN	

Getting status of Solr on host1.tivoli.edu

Status of Solr Nodes:

No.	Instance Name	Host	Status	State
1	SOLR_NODE_LOCAL	host1.csuite.edu	DOWN	ACTIVE

All Application Services are in Stopped State

Starting IBM Operations Analytics Log Analysis v1.3.2.0 Application Services...

Starting Derby Network Server...

Started Derby Network Server...

Starting ZooKeeper Service...

JMX enabled by default

Using config: /opt/IBM/LogAnalysis/zookeeper-3.4.6/bin/..../conf/zoo.cfg

Started ZooKeeper Service...

Starting Solr on host1.tivoli.edu

Started Solr with PID 6262

Starting Websphere Liberty Profile...

Starting server Unity.

Server Unity started with process ID 6324.

Started Websphere Liberty Profile...

Starting EIF Receiver...

Started Data Collection Application...

Starting Log File Agent Instance - default\_workload\_instance...

Processing. Please wait...

Starting Tivoli Log File Agent ...

Tivoli Log File Agent started

Started Log File Agent Instance - default\_workload\_instance...

Started All Services...

28. Open a Firefox browser if necessary.

29. Connect to the following URL:

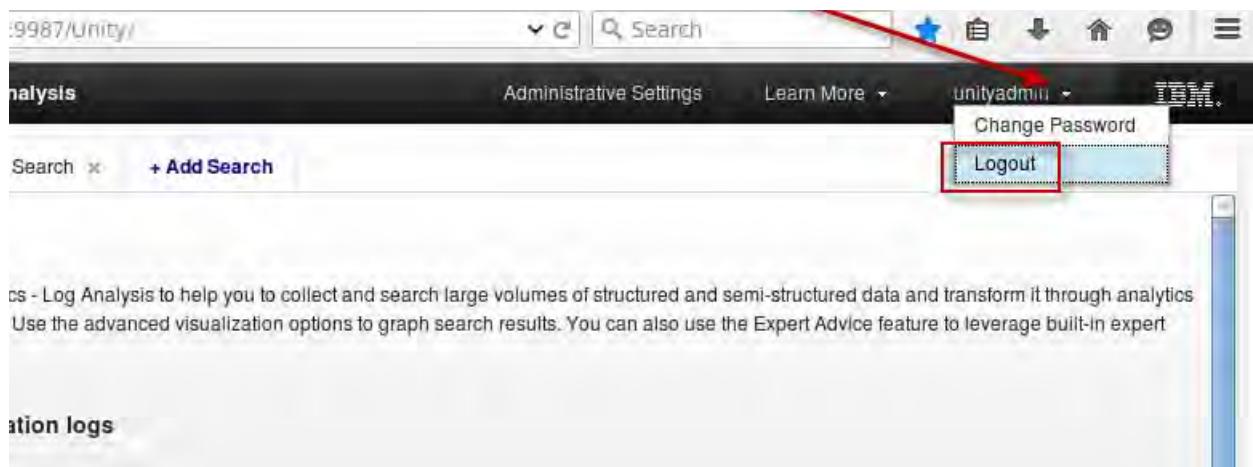
<https://host1.csite.edu:9987/Unity/>

30. Log in as **unityadmin** with password **object00**.



**Important:** You must use **object00** for the password. The password for the **unityadmin** user is **object00** in LDAP. The default password in the file-based repository is **unityadmin**.

31. Verify access and log out.



32. Close the Firefox browser.

## Configuring Log Analysis to use single sign-on

If you want to integrate data from IBM Operations Analytics Log Analysis with the Dashboard Application Services Hub component of Jazz for Service Management, you need to configure SSO between IBM Operations Analytics Log Analysis and Jazz for Service Management.

The first step in this process is to export the `ltpa_keys` file from the Jazz for Service Management server. You exported the file in the previous unit. The keys file is saved at the following location:

`/tmp/dash_keys`

The next step in the process is to add the Jazz for Service Management LDAP realm to the IBM Operations Analytics Log Analysis LDAP configuration. The realm name is configured in the following file:

`/opt/IBM/LogAnalysis/utilities/ldapRegistryHelper.properties`

The value is defined in the following property:

`ldap_realm_property=defaultWIMFileBasedRealm`

You defined this property in the previous exercise in this unit.

The last step in this procedure is to configure LTPA on the Liberty Profile for the WebSphere Application Server.

1. Copy the LTPA keys file that you exported from the Jazz for Service Management server to Log Analysis.

```
cp /tmp/dash_keys /opt/IBM/LogAnalysis/wlp/usr/servers/Unity/resources/security
```

2. Generate the encrypted text for the password **object00** for access to the key file:

```
cd /opt/IBM/LogAnalysis/wlp/bin/
../securityUtility encode object00
```

{xor}MD01Ojwrb28=

3. Copy the output test string.

4. Modify the Log Analysis server.xml file as follows:

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/wlp/usr/servers/Unity
```

- b. Save a copy of the file before modification:

```
cp server.xml server.xml.orig
```

- c. Open the file for edit:

```
gedit server.xml
```

- d. Modify the file as follows:

```
</oauthProvider>
 <webAppSecurity ssoDomainNames="DashDomain" />
 <ltpa keysFileName="${server.output.dir}/resources/security/dash_keys"
keysPassword="{xor}MD01Ojwrb28=" expiration="1440" />
</server>
```

Add the two lines that are shown here in bold face. The value for `keysPassword` is the text from the utility in the previous step. The lines are inserted between `oauth` and `/server`.

- e. Save the file and exit the gedit utility.

5. Stop Log Analysis as follows:

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

```
.
. .
```

Stopped All Services...

6. Start Log Analysis as follows:

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

.

.

.

Started All Services...

7. Open a Firefox browser if necessary.

8. Connect to Dashboard Application Services Hub.

9. Log in as **unityadmin** with password **object00**.

10. Open a new Firefox tab while still logged in to Dashboard Application Services Hub.



11. Connect to the following URL in the new tab:

<https://host1.csuite.edu:9987/Unity/>

If you are not prompted for the user name and password, the SSO connection is set up correctly. If you are prompted for the login details, the SSO connection is not configured correctly.

12. Verify access and click the X to close the tab.



13. Log out of Dashboard Application Services Hub.

14. Close the Firefox browser.

# Updating passwords in configuration files

After you create or change a user or password in your Lightweight Directory Access Protocol (LDAP) application, you must add the changed or new user information to several IBM Operations Analytics Log Analysis configuration files.

1. Encrypt the password string as follows:

```
cd /opt/IBM/LogAnalysis/utilities
```

```
./unity_securityUtility.sh encode object00
```

```
Using keystore file unity.ks.
```

```
/opt/IBM/LogAnalysis/utilities/..../wlp/usr/servers/Unity/keystore/unity.ks
```

```
{aes}FFAC4A5CBA0A3CC785330D7F5B1DFF25
```



**Important:** Your password string does not match the example that is shown here. Be sure to use the output from your utility in the following steps.

2. Copy the encrypted text.

If you change the password that is used by the **unityuser**, you must update the password in the following files to match the updated password.

3. Modify the data collector file as follows:

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/utilities/datacollector-client
```

- b. Save a copy of the file before modification:

```
cp javaDatacollector.properties javaDatacollector.properties.orig
```

- c. Open the file for edit:

```
gedit javaDatacollector.properties
```

- d. Locate the line with the existing password as shown here:

```
#The password to use to access the unity rest service
password = {aes}2E60564877892EDA85433985CCFC5615
```

- e. Replace the password text with the output from the unity\_securityUtility as shown here:

```
password = {aes}FFAC4A5CBA0A3CC785330D7F5B1DFF25
```

- f. Save the file and exit the gedit utility.

4. Modify the rest-api file as follows:

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/remote_install_tool/config
```

- b. Save a copy of the file before modification:

```
cp rest-api.properties rest-api.properties.orig
```

- c. Open the file for edit:

```
gedit rest-api.properties
```

- d. Locate the line with the existing password as shown here:

```
ibm.scala.rest.password={aes}2E60564877892EDA85433985CCFC5615
```

- e. Replace the password text with the output from the unity\_securityUtility as shown here:

```
ibm.scala.rest.password={aes}FFAC4A5CBA0A3CC785330D7F5B1DFF25
```

- f. Save the file and exit the gedit utility.

5. Modify the EIF receiver file as follows:

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/UnityEIFReceiver/config
```

- b. Save a copy of the file before modification:

```
cp unity.conf unity.conf.orig
```

- c. Open the file for edit:

```
gedit unity.conf
```

- d. Locate the line with the existing password as shown here:

```
unity.data.collector.password={aes}2E60564877892EDA85433985CCFC5615
```

- e. Replace the password text with the output from the unity\_securityUtility as shown here:

```
unity.data.collector.password={aes}FFAC4A5CBA0A3CC785330D7F5B1DFF25
```

- f. Save the file and exit the gedit utility.

6. Modify the Solr register file as follows:

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/solr_install_tool/scripts
```

- b. Save a copy of the file before modification:

```
cp register_solr_instance.sh register_solr_instance.sh.orig
```

- c. Change file permissions to allow modifications:

```
chmod +w register_solr_instance.sh
```

- d. Open the file for edit:

```
gedit register_solr_instance.sh
```

- e. Locate the line with the existing password as shown here:

```
PASSWD={aes}2E60564877892EDA85433985CCFC5615
```

- f. Replace the password text with the output from the unity\_securityUtility as shown here:  
`PASSWD={aes}FFAC4A5CBA0A3CC785330D7F5B1DFF25`
- g. Save the file and exit the gedit utility.

If you change the password that is used by the **unityadmin** user, you must update the password in the following file to match the updated password:

7. Modify the package management file as follows:

- a. Change to the target directory.

```
cd /opt/IBM/LogAnalysis/utilities
```

- b. Save a copy of the file before modification:

```
cp pkg_mgmt.sh pkg_mgmt.sh.orig
```

- c. Change file permissions to allow modifications:

```
chmod +w pkg_mgmt.sh
```

- d. Open the file for edit:

```
gedit pkg_mgmt.sh
```

- e. Locate the line with the existing password as shown here:

```
username=unityadmin
password={aes}928D7851BC5FAB69EFCAD4C3E8CC18CA
```

- f. Replace the password text with the output from the unity\_securityUtility as shown here:

```
password={aes}FFAC4A5CBA0A3CC785330D7F5B1DFF25
```

- g. Save the file and exit the gedit utility.



**Important:** You must restart Log Analysis after you change the password values. You restart Log Analysis in the next step.

## Configuring Log Analysis to start at system start

The following steps use a start script in `/etc/init.d`.

1. Configure Log Analysis to automatically start:

- a. Change to the root user.

```
su -
Password: object00
```

- b. Copy the supplied start script:

```
cd /workshop/etc/init.d
cp iola /etc/init.d
```

- c. Change the file permissions to allow execution:

```
cd /etc/init.d
chmod +x iola
```

- d. Create the logical links to enable the autostart feature:

```
chkconfig iola on
```

2. Stop the Log Analysis components.

```
/etc/init.d/iola stop
```

Wait for the components to stop.

3. Start the Log Analysis components.

```
/etc/init.d/iola start
```

.

.

.

```
Starting Log File Agent Instance - default_workload_instance...
Processing. Please wait...
Starting Tivoli Log File Agent ...
Tivoli Log File Agent started
Started Log File Agent Instance - default_workload_instance...

Started All Services...
```

4. Wait for the components to start.



**Note:** The command is submitted to the background. The components are started when you see the message Started All Services. Press Enter to see the cursor.

5. Exit the root user back to the **netcool** user.

```
exit
```

6. Open a Firefox browser.

7. Enter the following URL:

```
https://host1.csite.edu:9987/Unity/
```

8. Log in with user **unityadmin** and password **object00**.

A successful login verifies that Log Analysis started when the server started.

9. Log out of Log Analysis.

10. Close the browser.

## Enabling the Log Analysis product key

To continue to use IBM Operations Analytics Log Analysis beyond the trial period, you must enable the product key to set up the licensed version of IBM Operations Analytics Log Analysis.

1. Create the key directory as follows:

```
cd /opt/IBM/LogAnalysis
mkdir properties
cd properties
mkdir version
```

2. Copy the license file to the new directory.

```
cd /software/la
cp OALA_1.3.2_ED_ENABLEMENT_KEY.swttag /opt/IBM/LogAnalysis/properties/version
```

3. Rename the license key file.

```
cd /opt/IBM/LogAnalysis/properties/version
mv OALA_1.3.2_ED_ENABLEMENT_KEY.swttag IBM_OPERATIONS_ANALYTICS_1.3_KEY.swttag
```

The change takes effect immediately. You do not need to restart Log Analysis.

## Configuring Network Manager workaround

IBM Tivoli Network Manager v4.2 now uses the Apache Zoo Keeper application. If you install Network Manager on the same server as Log Analysis, you encounter a configuration conflict. The current workaround for this conflict is to add some environment variable settings to the Log Analysis start script.

1. Change to the directory of the start script.

```
cd /opt/IBM/LogAnalysis/utilities
```

2. Save a copy of the script before changes.

```
cp unity.sh unity.sh.orig
```

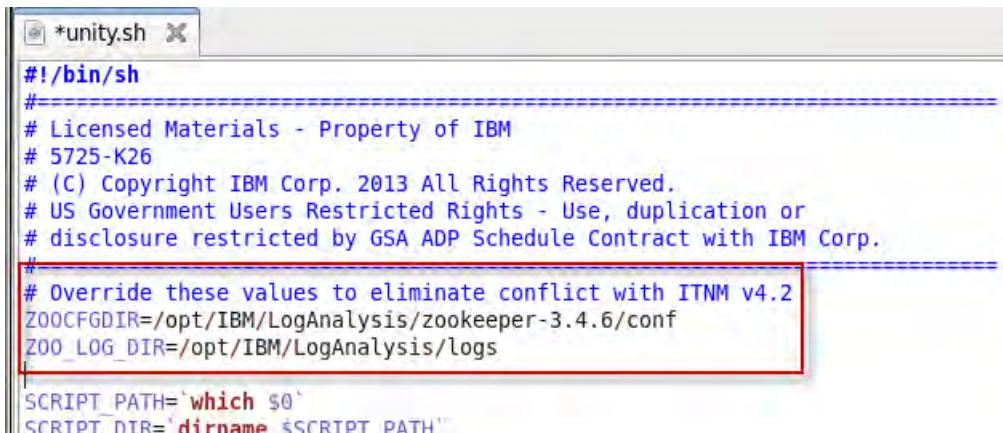
3. Modify the file as follows.

- a. Open the file for edit.

```
gedit unity.sh
```

- b. Add the following lines to the top of the file.

```
Override these values to eliminate conflict with ITNM v4.2
ZOOCFGDIR=/opt/IBM/LogAnalysis/zookeeper-3.4.6/conf
ZOO_LOG_DIR=/opt/IBM/LogAnalysis/logs
```



```
*unity.sh
#!/bin/sh
#-----
Licensed Materials - Property of IBM
5725-K26
(C) Copyright IBM Corp. 2013 All Rights Reserved.
US Government Users Restricted Rights - Use, duplication or
disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#-----
Override these values to eliminate conflict with ITNM v4.2
ZOOCFGDIR=/opt/IBM/LogAnalysis/zookeeper-3.4.6/conf
ZOO_LOG_DIR=/opt/IBM/LogAnalysis/logs

SCRIPT_PATH=`which $0`
SCRIPT_DIR=`dirname $SCRIPT_PATH`
```

- c. Save the file and exit the gedit utility.

4. Test the revised script.

- a. Stop the Log Analysis components.

```
./unity.sh -stop
```

Wait for the components to stop.

- b. Start the Log Analysis components.

```
./unity.sh -start
```

Wait for the components to start.

c. Verify the status of the Log Analysis components.

```
./unity.sh -status
```

```
Mon Jan 18 15:07:02 UTC 2016
```

```
IBM Operations Analytics - Log Analysis v1.3.2.0 ENTRY EDITION Application
Services Status:
```

No.	Service	Status	Process ID
1	Derby Network Server	UP	8609
2	ZooKeeper	UP	8655
3	Websphere Liberty Profile	UP	8989
4	EIF Receiver	UP	9220
5	Log File Agent instance	UP	9485

```
Getting status of Solr on host1.csuite.edu
```

```
Status of Solr Nodes:
```

No.	Instance Name	Host	Status	State
1	SOLR_NODE_LOCAL	host1.csuite.edu	UP	ACTIVE

**All Application Services are in Running State**

Checking server initialization status: Server has initialized!

Verify that all the components start correctly.

The following list is a summary of the accomplishments from this unit:

- Installed Netcool/OMNIbus core component
- Created and run the primary ObjectServer
- The root user has a valid password in the ObjectServer
- Verified basic ObjectServer functions
- Installed the gateway for JDBC and configured event archiving
- Installed Dashboard Application Services Hub
- Installed Netcool/OMNIbus Web GUI component
- Verified basic Web GUI functions
- Configured Dashboard Application Services Hub to use LDAP as a user repository
- Installed Netcool/Impact
- Configured Netcool/Impact to use LDAP as a user repository
- Configured single sign-on between Dashboard Application Services Hub and Netcool/Impact
- Configured Netcool/Impact console integration in Dashboard Application Services Hub
- Installed IBM Operations Analytics Log Analysis
- Configured Log Analysis to use LDAP as a user repository
- Configured single sign-on between Dashboard Application Services Hub and Log Analysis
- Configured all components to start when the server starts



## 3 Configuring IBM Netcool Operations Insight base exercises

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

### Exercise 1 Netcool/OMNibus Insight Pack

The Netcool/OMNibus Insight Pack is used to view and search both historical and real-time event data from Netcool/OMNibus in the IBM Operations Analytics Log Analysis product. The Insight Pack parses Netcool/OMNibus event data into a format suitable for use by Operations Analytics Log Analysis.

# Installing the Insight Pack



**Important:** The Operations Analytics Log Analysis components must be running when the insight pack is installed.

1. Verify the status of the Log Analysis components:

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

```
IBM Operations Analytics - Log Analysis v1.3.0.0 Application Services Status:

No. Service Status Process ID

1 Derby Network Server UP 3687
2 ZooKeeper UP 3727
3 Websphere Liberty Profile UP 3855
4 EIF Receiver UP 3960
5 Log File Agent instance UP 4229

Getting status of Solr on host1.tivoli.edu
Status of Solr Nodes:

No. Instance Name Host Status State

1 SOLR_NODE_LOCAL host1.tivoli.edu UP ACTIVE

All Application Services are in Running State
Checking server initialization status: Server has initialized!
```

2. Create a directory to hold the insight pack files.

```
cd /opt/IBM/LogAnalysis/unity_content/
```

```
mkdir OMNIbus
```

3. Copy the insight pack installation file to the new directory:

```
cp /software/la/OMNIbusInsightPack_v1.3.0.2.zip OMNIbus
```

4. Install the insight pack as follows:

```
cd OMNIbus
```



**Note:** Enter the following text as one line.

```
/opt/IBM/LogAnalysis/utilities/pkg_mgmt.sh
-install OMNIbusInsightPack_v1.3.0.2.zip
.
.
.

[packagemanager] 04/09/15 14:00:38:163 UTC [main] INFO - ContentPackManager :
CTGLC0023I : Install of OMNIbusInsightPack_v1.3.0.2 completed successfully

BUILD SUCCESSFUL
Total time: 7 seconds
```



**Important:** The build must complete successfully before you proceed. If the build fails with an authentication issue, the problem is likely due to a bad password. Verify the password change to the package management utility from the previous exercise.

## Creating the Log Analysis data source

Use the IBM Operations Analytics Log Analysis administrative user interface to add a data source for Netcool/OMNibus events.

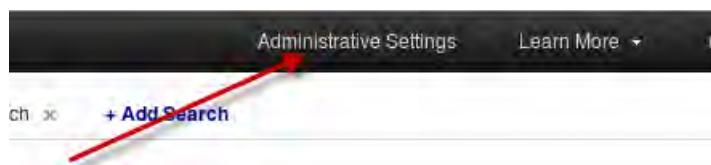
1. Open a Firefox browser if necessary.

2. Connect to the following URL:

<https://host1.csite.edu:9987/Unity/>

3. Log in with user **unityadmin** and password **object00**.

4. Click **Administrative Settings**.



The administrative user interface opens in a new Firefox tab.

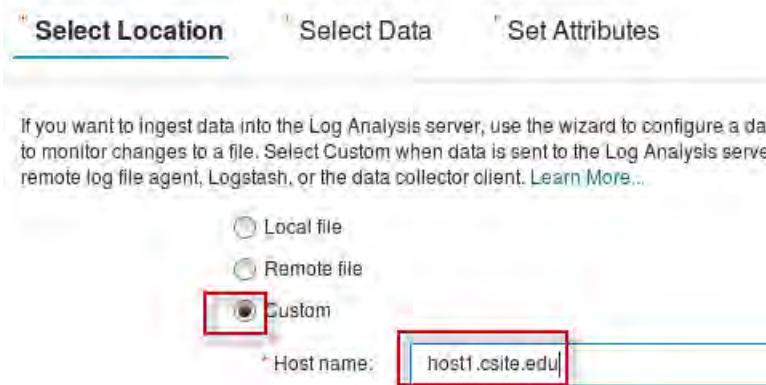
5. Click the **Data Sources** tab.



6. Click the arrow and select **Data Source** to add a data source.



7. Select **Custom** and enter **host1.csite.edu** as the host name. Click **Next**.



8. Enter **NOI\_AGG\_P** for the **File path** field.



**Important:** The value for **File Path** must match a property in the Message Bus gateway configuration. You configure the gateway in a subsequent step.

9. Click the arrow and select **OMNIbus1100** for the type.

10. Click the arrow and select **OMNibus1100-Collection** for Collection. Click **Next**.

\* 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 click Next.

More...

\* File path: NOI\_AGG\_P

\* Type: OMNibus1100 

Collection: OMNibus1100-Collection 

\* Required

11. Enter **omnibus** for the **Name** field and click **Finish**.



**Important:** The data source name must be **omnibus**. This name must match the `scala.datasource` property in the Web GUI server session properties file, `server.init`  
`scala.datasource=omnibus`

\* Select Location      \* Select Data      \* **Set Attributes**

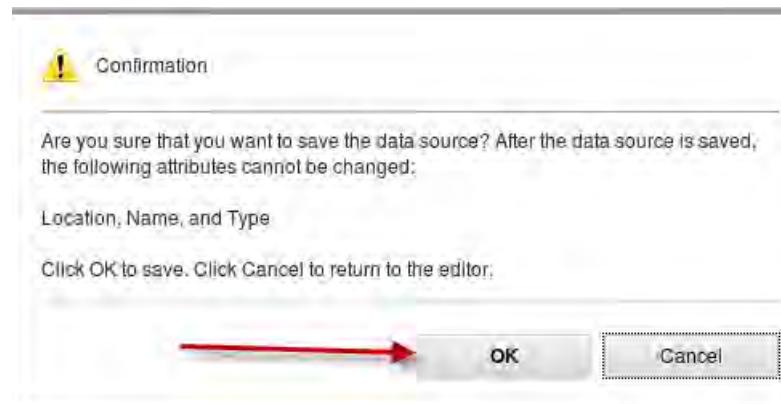
Enter a name for the new data source. Optionally, set a description and assign the source to a group.

\* Name: omnibus

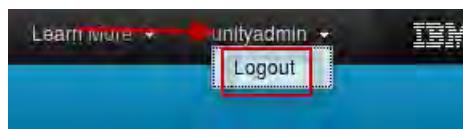
Description:

Group:

12. Click **OK** to confirm the save.

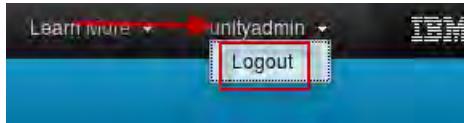


13. Log out of the administration user interface.



14. Close the Firefox tab.

15. Log out of Log Analysis.

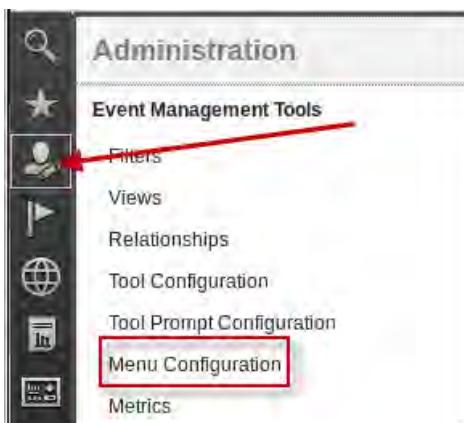


16. Close the Firefox browser.

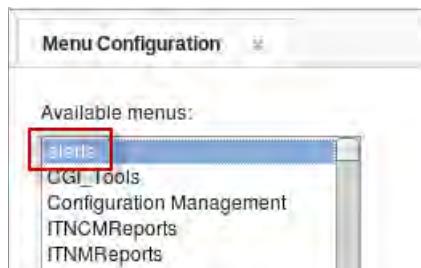
## Configuring Web GUI

The installation process creates Web GUI tools and a menu for the Log Analysis utilities. You must add the Log Analysis menu to an existing menu to make the Log Analysis tools visible to users.

1. Open a Firefox browser if necessary.
2. Log in to Dashboard Application Services Hub as user **ncoadmin** and password **object00**.
3. Click the icon and select **Menu Configuration**.

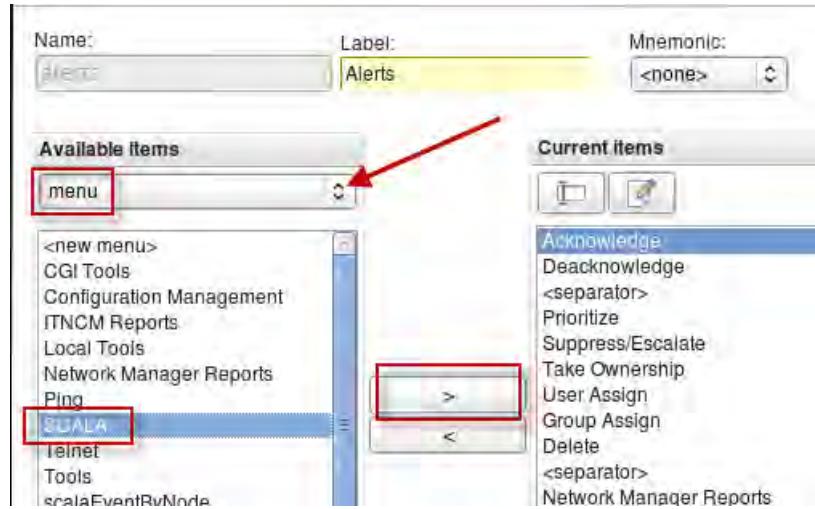


4. Click **alerts** to select it. Click **Modify**.



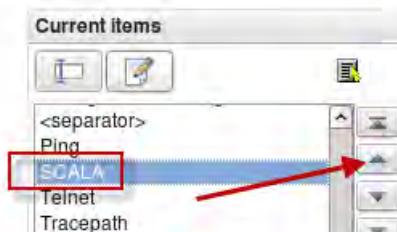
5. Click the arrow and select menu.

6. Click **SCALA** to select it, and click the *right arrow* icon to add the menu.



The menu is added to the bottom of the list.

7. Click **SCALA** to select it. Click the *up arrow* icon several times to move up the menu in the list.



8. Click **Save**.

9. Log out of Dashboard Application Services Hub.

10. Close the **Firefox** browser.

The Log Analysis tools use several parameter settings in the Web GUI initialization file. You must change some of these parameters.

11. Open a Terminal window if necessary.

12. Change to the target directory.

```
cd /opt/IBM/netcool/gui/omnibus_webgui/etc
```

13. Open the file for edit.

```
gedit server.init
```

14. Locate the following line:

```
scala.version=1.2.0.2
```

15. Change the value as follows:

```
scala.version=1.2.0.3
```

16. Locate the following line:

```
scala.app.keyword=OMNIBUS_SetSearchFilter
```

17. Change the value as follows:

```
scala.app.keyword=OMNIBUS_Keyword_Search
```

18. Save the changes and exit the gedit utility.

## Exercise 2 Message Bus Gateway

In the integration uses an HTTPS/SSL connection between the Netcool/OMNIbus gateway and the HTTP interface of IBM Operations Analytics Log Analysis. You must create a truststore to store the Log Analysis digital certificate and then point the gateway to the location of the truststore. You then install and configure the Netcool/OMNIbus message bus gateway. The message bus gateway extracts Netcool/OMNIbus events and formats them for Log Analysis.

## Configuring SSL

1. Use the following steps to create a client keystore.

a. Run the following command to create the directory where the keystore is saved.

```
mkdir /opt/IBM/tivoli/netcool/omnibus/java/security
```

b. Change to the JRE bin directory where the keytool utility is located.

```
cd /opt/IBM/tivoli/netcool/platform/linux2x86/jre_1.7.0/jre/bin
```

c. Use the keytool utility to create a new keystore.



**Note:** Enter the following text that starts with `./keytool` as one line.

```
./keytool -genkey -alias host1key -keystore
/opt/IBM/tivoli/netcool/omnibus/java/security/client.jks
```

Enter keystore password: **object00**

Re-enter new password: **object00**

What is your first and last name?

[Unknown]:

What is the name of your organizational unit?

[Unknown]: **IBM**

What is the name of your organization?

[Unknown]: **Netcool**

What is the name of your City or Locality?

[Unknown]:

What is the name of your State or Province?

[Unknown]:

What is the two-letter country code for this unit?

[Unknown]: **US**

Is CN=Unknown, OU=IBM, O=Netcool, L=Unknown, ST=Unknown, C=US correct? (type "yes" or "no")**yes**

Enter key password for <host1key>:

(RETURN if same as keystore password):

## 2. Check keystore contents.



**Note:** Enter the following text that starts with `./keytool` as one line.

```
./keytool -list -keystore
/opt/IBM/tivoli/netcool/omnibus/java/security/client.jks
```

Enter keystore password: **object00**

Keystore type: jks

Keystore provider: IBMJCE

Your keystore contains 1 entry

host1key, Apr 8, 2015, keyEntry,

Certificate fingerprint (SHA1):

3D:13:94:06:CE:35:BE:B6:D0:EF:5F:73:5B:99:CF:8F:EC:39:AD:C7

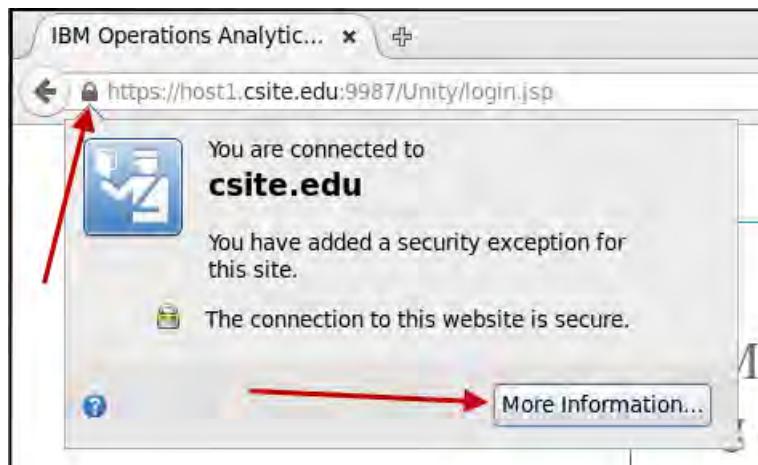
3. Export the server certificate from the host that runs IBM Operations Analytics Log Analysis with Firefox.

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

<https://host1.csite.edu:9987/Unity>

You see the IBM Operations Analytics Log Analysis login page. It is not necessary to log in with any user.

- b. Click the **padlock** icon and click **More Information**.



- c. Click **Security** and click **View Certificate**.



- d. Select the **Details** tab.

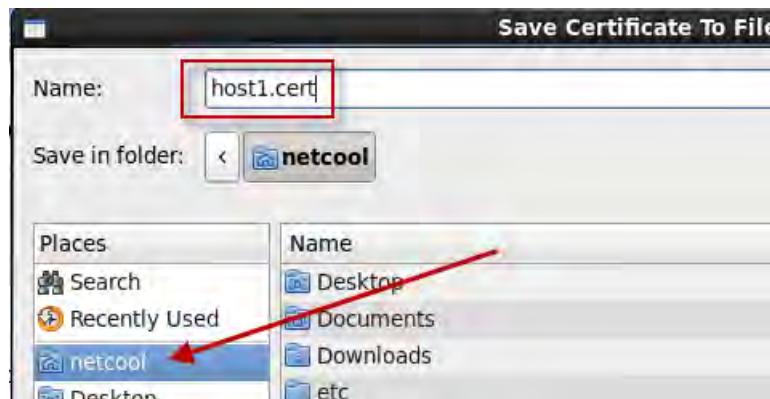


- e. Scroll to the bottom of the page and click **Export**.

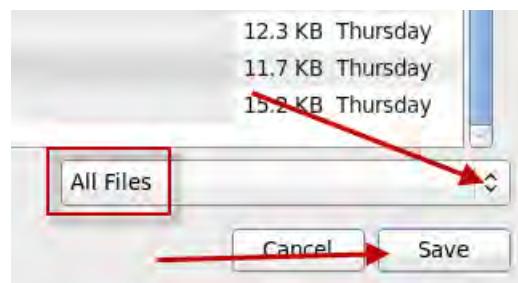


- f. Enter the following name for the file and click **netcool** to select the destination folder.

**host1.cert**



- g. Scroll down on the page. Select **All Files** for the output format. Click **Save** to export the file.



The file is saved as /home/netcool/host1.cert.

- h. Click **Close**.



- i. Click the X to close the information page.



- j. Close the Firefox browser.

4. Import the Log Analysis server certificate and create the Netcool/OMNIbus truststore.

```
cd /opt/IBM/tivoli/netcool/platform/linux2x86/jre_1.7.0/jre/bin
```



**Note:** Enter the following text that starts with `./keytool` as one line.

```
./keytool -import -keystore $OMNIHOME/java/security/cacerts.jks
-file /home/netcool/host1.cert -alias loganalysis
```

Enter keystore password: **object00**

Re-enter new password: **object00**

.

.

.

Trust this certificate? [no]: **yes**

Certificate was added to keystore

Enter **object00** for the password when prompted.

Enter **yes** to trust the certificate when prompted.

## Installing the gateway

The message bus gateway is installed with IBM Installation Manager.

1. Start IBM Installation Manager:

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

IBM Installation Manager opens.

2. Define the gateway repository.

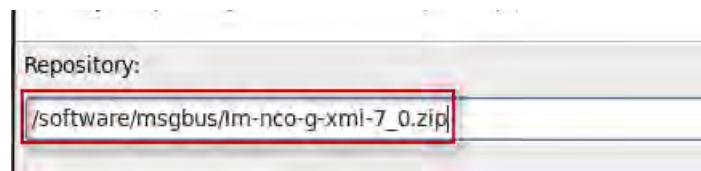
a. Click **File** and select **Preferences**.

b. Remove the check marks from all of the existing repository entries.

c. Select **Repositories** and click **Add Repository**.

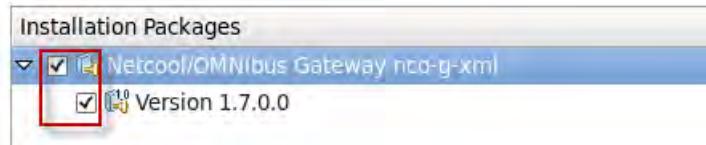
d. Click **Browse** and select the following repository:

```
/software/msgbus/Im-nco-g-xml-7_0.zip
```



e. Click **OK** to add the entry.

- f. Verify that the repository is listed and click **OK**.
3. Start the installation.
  - a. Click **Install**.
  - b. Select the package and click **Next**.



- d. Accept the license agreement and click **Next**.
- e. Leave the option set to use the existing package group.
- f. Accept the default list of features and click **Next**.
- g. Review the installation summary and click **Install**.
- h. Verify that the installation is successful and click **Finish**.



4. Click **File** and select **Exit** to close IBM Installation Manager.
5. Remove the installation file.

```
cd /software
/bin/rm -R msgbus
```

## Configuring the ObjectServer

As provided with the product, the gateway replicates only new events to Log Analysis with standard IDUC. Event instances that deduplicate do not get sent to Log Analysis, because no configuration is in place to replicate these events without sending all updates.

Additionally, to send newly inserted events and deduplicated inserts, you must customize the ObjectServer and configure the solution to use the Accelerated Event Notification (AEN) system. You must enable a trigger group and two triggers.

1. Start the Netcool/OMNibus Administrator utility:

```
nco_config &
```

- Click Yes.



- Click Finish.

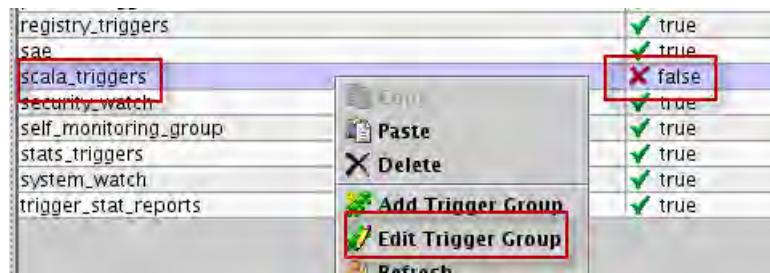


- Connect to the NOI\_AGG\_P ObjectServer as the root user with password object00.

- Expand Automation and select Trigger Groups.



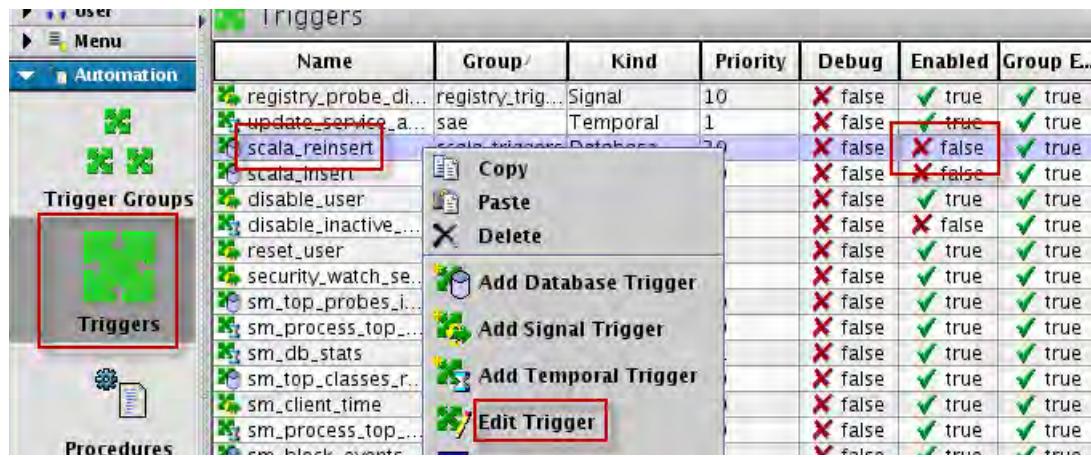
- Right-click scala-triggers and select Edit Trigger Group.



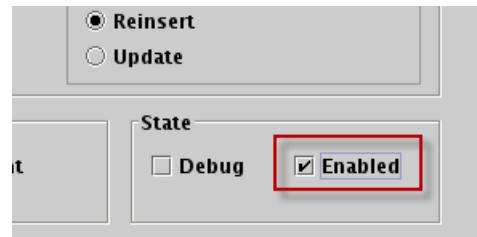
- Select Enabled and click OK.



- Select **Triggers**. Scroll down and locate the two scala triggers. Right-click **scala\_reinsert** and select **Edit Trigger**.



- Select **Enabled** and click **OK**.



- Repeat this step to enable the **scala\_insert** trigger.

- Verify that the triggers are both enabled.

Name	Group	Kind	Priority	Debug	Enabled	Group E..
registry_probe_d...	registry_trig...	Signal	10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
update_service_a...	sae	Temporal	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
scala_reinsert	scala_triggers	Database	20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
scala_insert	scala_triggers	Database	20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
disable_user	security_wa...	Signal	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- Click **File** and select **Exit** to close the administrator utility.

## Configuring the gateway

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

The gateway must have a name. For this exercise, use **LA\_GATE**. The name must be added to the Netcool/OMNIbus communications file.

- Run the **Server Editor** utility:

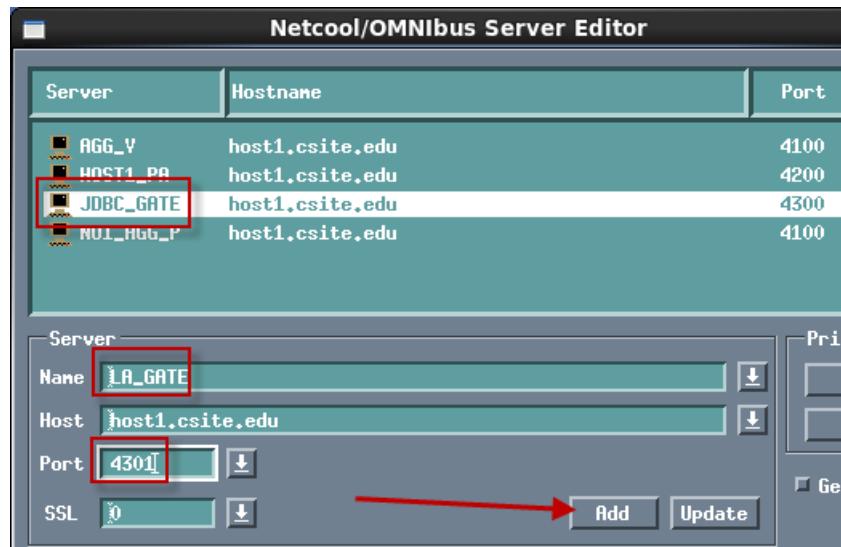
```
nco_xigen &
```

- Click the entry **JDBC\_GATE** to select it.

- Change the Name to **LA\_GATE**.

- Change the Port to **4301**.

## e. Click Add.



**Important:** Make sure that you click **Add** because you want to create a new entry. If you click **Update**, you *change* the entry for JDBC\_GATE to LA\_GATE.

f. Click **Apply** and click **Close**.

Server	Hostname	Port
AGG_V	host1.csuite.edu	4100
HOST1_PA	host1.csuite.edu	4200
JDBC_GATE	host1.csuite.edu	4300
<b>LA_GATE</b>	<b>host1.csuite.edu</b>	<b>4301</b>
NOI_HUB_P	host1.csuite.edu	4100

Verify that the entry for LA\_GATE is listed.

## 2. Configure the gateway.

Part of the gateway configuration is generic to the message bus gateway. Separate configuration files that are used with Netcool Operations Insight. The gateway is configured with several text files. The installation process creates these files in a specific directory. Copy the generic configuration files from that location to **\$OMNIHOME/etc** and rename the files to include the gateway name **LA\_GATE**.

## a. Change to the required directory:

```
cd $OMNIHOME/gates/xml/scala
```

## b. Copy and rename the 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
```

- c. Verify that the files are correctly renamed:

```
cd $OMNIHOME/etc
```

```
ls -l LA_GATE.*
```

LA\_GATE.1302.map

LA\_GATE.props

LA\_GATE.reader.tblrep.def

LA\_GATE.startup.cmd

3. Modify the property file as follows:

- a. Open the file for edit.

```
gedit LA_GATE.props
```

- b. Locate the following lines near the top of the file:

```
MessageLog : '$OMNIHOME/log/G_SCALA.log'
```

```
Name : 'G_SCALA'
```

- c. Comment out these lines as shown:

```
#MessageLog : '$OMNIHOME/log/G_SCALA.log'
```

```
#Name : 'G_SCALA'
```

- d. Locate the following lines near the bottom of the file:

```
#####
SCALA configuration
#####
```

- e. Add the following lines as shown in bold face:

```
#####
SCALA configuration
#####
```

```
Gate.Reader.Description : 'SCALA Gateway Reader'
```

```
Gate.Reader.Server : 'NOI_AGG_P'
```

```
Gate.Reader.Username : 'root'
```

```
Gate.Reader.Password : 'EDEAAPAIANFMCHCB'
```



**Note:** The text **EDEAAPAIANFMCHCB** is the output from nco\_g\_crypt object00.

- f. Locate the existing reader table replication definition:

```
Gate.Reader.TblReplicateDefFile:
```

```
'$OMNIHOME/gates/xml/scala/xml.reader.tblrep.def'
```

- g. Modify the name as shown here:

```
Gate.Reader.TblReplicateDefFile: '$OMNIHOME/etc/LA_GATE.reader.tblrep.def'
```

- h. Locate the existing map file definition:

```
Gate.MapFile : '$OMNIHOME/gates/xml/scala/xml.map'
```

- i. Modify the name as shown here:

```
Gate.MapFile : '$OMNIHOME/etc/LA_GATE.1302.map'
```

- j. Locate the existing startup file definition:

```
Gate.StartupCmdFile: '$OMNIHOME/gates/xml/scala/xml.startup.cmd'
```

- k. Modify the name as shown here:

```
Gate.StartupCmdFile: '$OMNIHOME/etc/LA_GATE.startup.cmd'
```

- l. Save the file and exit the gedit utility.

#### 4. Edit the reader table replication file.

You must edit one line in this file.

- a. Edit the file.

```
gedit LA_GATE.reader.tblrep.def
```

- b. Locate the following line:

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

- c. Change as follows:

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

- d. Save the file and exit the gedit utility.

#### 5. Copy the Log Analysis gateway configuration files.

- a. Change to the required directory:

```
cd $OMNIHOME/gates/xml/scala
```

- b. Copy the files:

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

```
cp scalaTransformers.xml $OMNIHOME/java/conf/
```

- c. Verify that the files are correctly renamed:

```
cd $OMNIHOME/java/conf/
```

```
ls -1 scala*
```

```
scalaTransformers.xml
```

```
scalaTransport.properties
```

#### 6. Edit the scalaTransport.properties file.

- a. Edit the file.

```
gedit scalaTransport.properties
```

- b. Add the following lines to the bottom of the file:

```
scalaURL=https://host1.csuite.edu: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 =object00
jsonMsgPath = NOI_ AGG_P
```



**Important:** The value for jsonMsgPath must match the value for file path in the Log Analysis data source definition. You created the data source in a previous exercise.

- c. Save the file and exit the gedit utility.
7. Edit the `scalaTransformers.xml` file.
  - a. Edit the file:  
`gedit scalaTransformers.xml`
  - b. Locate the following text:  
`endpoint="https://localhost:9987/Unity/DataCollector"`
  - c. Change as follows:  
`endpoint="https://host1.csuite.edu:9987/Unity/DataCollector"`
  - d. Save the file and exit the gedit utility.

## Verifying the gateway operation

To verify the gateway operation, you run the gateway in debug mode and examine the contents of 2 log files. You examine the gateway log file and the log file for the Log Analysis receiver. You use the UNIX `tail` command to examine the log files.

1. Open a terminal window.
2. Start the Simnet probe to produce some test event records.

```
nco_p_simnet -server NOI_ AGG_P &
```

3. Examine the Log Analysis receiver log file as follows:

- a. Change to the log directory.

```
cd /opt/IBM/LogAnalysis/logs
```

- b. Start the `tail` operation.

```
tail -f GenericReceiver.log
```



**Hint:** Press Enter a few times to create some blank lines.

Leave this terminal window as is.

4. Open a terminal window.

5. Start the gateway in debug mode.

```
nco_g_xml -name LA_GATE -messagelevel debug&
```

6. Examine the gateway log file as follows:

- a. Change to the log directory.

```
cd /opt/IBM/tivoli/netcool/omnibus/log
```

- b. Start the *tail* operation.

```
tail -f LA_GATE.log
```

- c. Look for messages that are similar to the following example:

```
2015-04-21T15:07:13: Debug: D-GJA-000-000: [ngjava]: XMLGateway:
Transforming XML message - [<?xml version="1.0"
encoding="UTF-8"?><tns:netcoolEvent type="insert"
xmlns:tns="http://item.tivoli.ibm.com/omnibus/netcool">
<tns:netcoolField name="FirstOccurrence"
type="utc">2015-04-14T15:49:58+0000</tns:netcoolField>
<tns:netcoolField name="Summary" type="string">Diskspace
alert</tns:netcoolField>
<tns:netcoolField name="NmOsObjInst" type="integer">0</tns:netcoolField>
<tns:netcoolField name="Node" type="string">Beijing</tns:netcoolField>
<tns:netcoolField name="NodeAlias" type="string">Beijing</tns:netcoolField>
<tns:netcoolField name="LastOccurrence"
type="utc">2015-04-21T15:07:13+0000</tns:netcoolField>
<tns:netcoolField name="Severity" type="string">Major</tns:netcoolField>
<tns:netcoolField name="AlertGroup" type="string">Stats</tns:netcoolField>
<tns:netcoolField name="AlertKey" type="string">97% full</tns:netcoolField>
<tns:netcoolField name="Identifier"
type="string">BeijingMachineStats4Stats</tns:netcoolField>
<tns:netcoolField name="Location" type="string"/>
<tns:netcoolField name="Type" type="string">Type Not Set</tns:netcoolField>
<tns:netcoolField name="Tally" type="integer">293</tns:netcoolField>
<tns:netcoolField name="Class" type="string">SimNet Probe</tns:netcoolField>
<tns:netcoolField name="OmniText" type="string">Simnet Probe
MachineStats</tns:netcoolField>
</tns:netcoolEvent>]
```

This message indicates that the gateway converted an event record into the format that the Log Analysis receiver expects.

- d. Look for messages similar to the following example:

```
2015-04-21T15:07:13: Debug: D-GOB-105-289: [ngobjserv]: Mapper: Post-Mapping
insert/update iduc data from 'NOI_AGG_P', table 'alerts.status' of '1'
item(s). [Inserts=1][Updates=0]
2015-04-21T15:07:13: Debug: D-GOB-105-147: [ngobjserv]: Mapper: Sending '1'
mapped insert table item(s) from 'NOI_AGG_P', table 'alerts.status', to table
'alerts.status', to writer.
```

These messages indicate that the gateway forwarded a formatted record to the Log Analysis receiver.



**Important:** If you see the following message in the GenericReceiver log file, restart the Log Analysis processes:

```
11/09/15 15:07:22:862 UTC [Default Executor-thread-1545] ERROR - SolrUtil : CTGLA5556E :
Error occurred while creating collection "UnityCollection_09_11_2015_00_00_00_UTC"
org.apache.solr.client.solrj.SolrServerException: No live SolrServers available to handle this
request:[http://192.168.100.100:8983/solr]
```

- e. Press Ctrl+C to exit the *tail* operation.

7. Return to the terminal window with the Log Analysis receiver log file.

8. Look for messages that are similar to the following example:

```
04/21/15 15:13:45:533 UTC [Default Executor-thread-51] INFO -
UnityFlowController : Batch Status for -> OMNIbus1100-Collection , Size: 200 ,
Num successful: 200 , Num failures: 0 , Indexed Source volume: 43596
04/21/15 15:13:45:533 UTC [Default Executor-thread-51] INFO -
DataCollectorRestServlet : Batch of Size 200 processed and encountered 0
failures
04/21/15 15:13:45:954 UTC [Thread-63] INFO - IndexStatusChecker : Updating
statistics for data source [omnibus], stream [_unity_default_stream], ingested
bytes [44155], write date [Tue Apr 21 15:13:45 UTC 2015].
```

These messages indicate that the receiver processed a batch of messages from the gateway, and that no errors occurred.



**Important:** Both gateways process events based on a frequency. The gateways do not process events in real time. You might need to wait several minutes before you see activity in each log file.

9. Press Ctrl+C to exit the *tail* operation.

## 10. Stop the gateway.

- Find the PID of the running event gateway:

```
ps -ef | grep nco_g_xml
netcool 25406 8221 0 15:26 pts/1 00:01:50
/opt/IBM/tivoli/netcool/omnibus/platform/linux2x86/bin64/nco_g_xml -name
LA_GATE
```

- Find the PID of the running event gateway:

```
kill -9 25406
```

## 11. Add the gateway to process activity.

- Change to the target directory:

```
cd $OMNIHOME/etc
```

- Modify the process activity configuration file.

```
gedit nco_pa.conf
```

- Add the following lines to the *process* section.

```
nco_process 'LogAnalysisGateway'
{
 Command '$OMNIHOME/bin/nco_g_xml -name LA_GATE' run as 501
 Host='host1.csite.edu'
 Managed=True
 RestartMsg='${NAME} running as ${EUID} has been restored on ${HOST}.'
 AlertMsg='${NAME} running as ${EUID} has died on ${HOST}.'
 RetryCount=0
 ProcessType=PaPA_AWARE
}
```

- Add the following line to the *service* section.

```
process 'LogAnalysisGateway' 20
```

- Save the changes and exit the gedit utility.

12. Stop process activity. Enter **2** when prompted.

```
nco_pa_shutdown -server HOST1_PA -password object00
```

```
Connected To PA Server [HOST1_PA] Shutdown Options :-
1) Shutdown Server leaving managed processes running.
2) Shutdown Server and stop all managed processes.
3) Exit shutdown interface.

Select Option [1-3] 2

Shutdown PA and stop processes.
```

## 13. Start process activity:

```
nco_pad -name HOST1_PA
```

14. Verify process status:

```
nco_pa_status -server HOST1_PA -password object00
```

Service Name	Process Name	Hostname	User	Status	PID
Core	MasterObjectServer	host1.csuite.edunetcool		RUNNING	11965
	ArchiveGateway	host1.csuite.edunetcool		RUNNING	12124
	LogAnalysisGateway	host1.csuite.edunetcool		RUNNING	12125



**Important:** The gateway is configured with a 20-second delay. You might need to run the status command a few times before the gateway shows up as running.

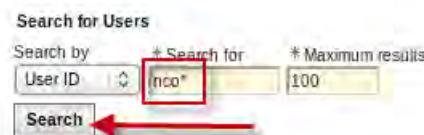
## Configuring user access to the Event Search feature

The Event Search capability is implemented with Log Analysis. A user requires access to Netcool/OMNIbus event records, and Log Analysis. In the following steps, you modify an existing Netcool/OMNIbus user to add access to Log Analysis. A user must be a member of the UnityUsers group to access Log Analysis. You must add a user to the group before you verify the feature.

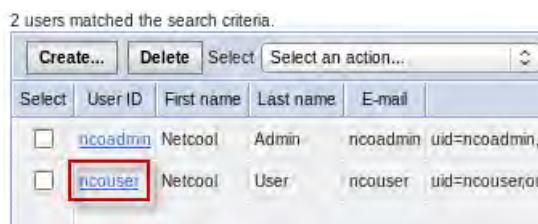
1. Log in to Dashboard Application Services Hub as the **smadmin** user with password **object00**.
2. Open WebSphere administrative console.
3. Expand **Users and Groups**. Select **Manage Users**.



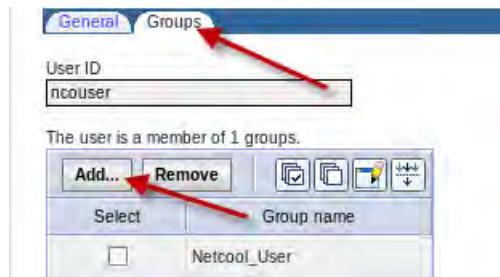
4. Enter **nco\*** in the search box and click **Search**.



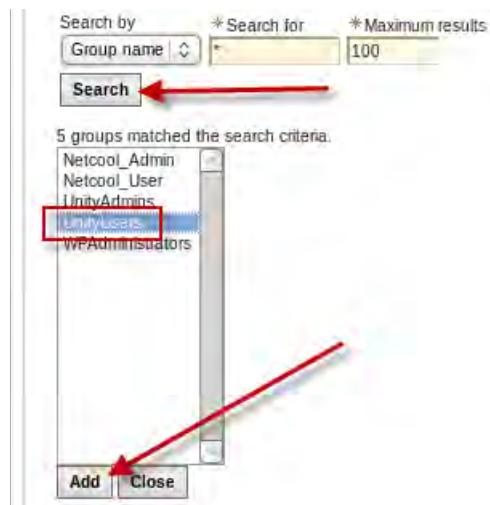
5. Click **ncouser**.



6. Select the **Groups** tab and click **Add**.



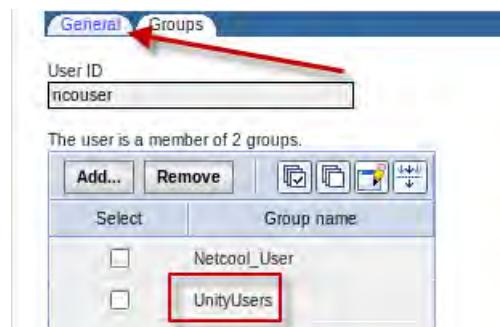
7. Click **Search** to display the list of groups. Click **UnityUsers** to select it. Click **Add**.



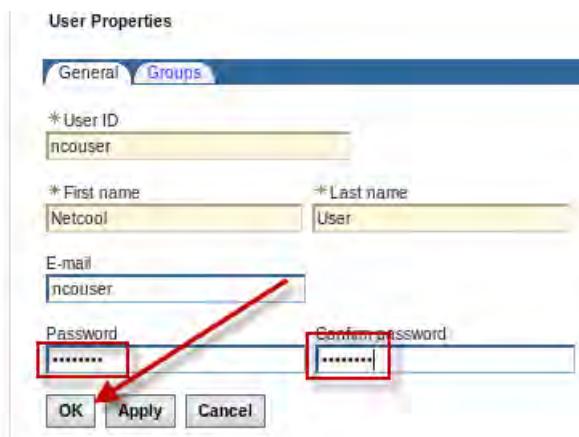
8. Click **Close**.



9. Verify that the group is listed and select the **General** tab.



10. Enter **object00** for the password and click **OK** to update the user record.



11. Log out of WebSphere administrative console.

12. Close the Firefox tab.

13. Log out of Dashboard Application Services Hub as the **smadmin** user.

After you add the ncouser to the UnityUsers group, the user can now access Log Analysis features. However, Log Analysis limits access to log data by controlling access to each data source. In a previous exercise, you installed the Netcool/OMNIbus Event Insight pack, and created a Log Analysis data source for event records. You must configure Log Analysis to allow the ncouser user to access that data source.

14. Connect the Firefox browser to the following URL

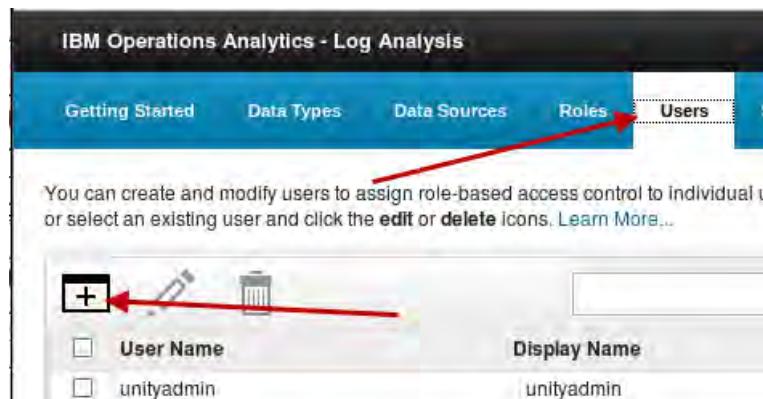
<https://host1.csite.edu:9987/Unity>

15. Log in as **unityadmin** with password **object00**.

16. Click **Administrative Settings**.



17. Select Users, and click the icon to add a user.



18. Enter **ncouser**, scroll down, and click **OK**.

Add User x

Configure LDAP User

A user profile is a distinct account with specific roles and permissions. L

\* User Name  ncouser

\* Display Name



**Important:** The user name field is the only required value. The other fields are gray, and you cannot enter values.

19. Click **OK** to confirm the new user.



20. Select Roles, and click the icon to create a new role.

IBM Operations Analytics - Log Analysis

Getting Started Data Types Data Sources **Roles** Users

You can create and modify user roles to assign role-based access control to icons to add a new role, or select an existing role and click the edit or delete icon

**+**

Role Name	Display Name
<input type="checkbox"/> unityusers	unity users

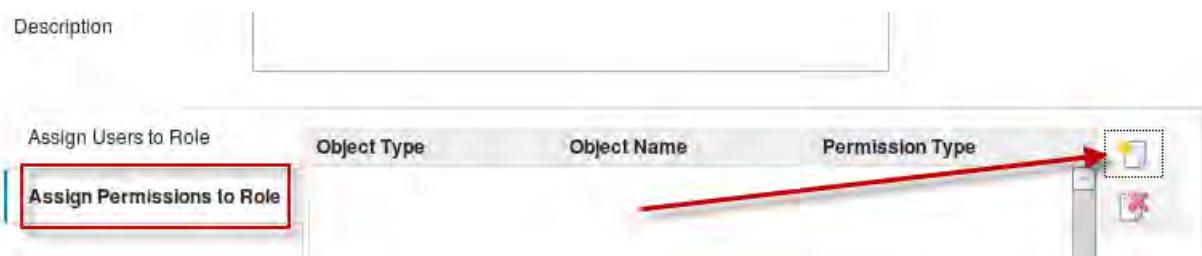
21. Enter **OMNIbusEvents** for both name values.

Add Role

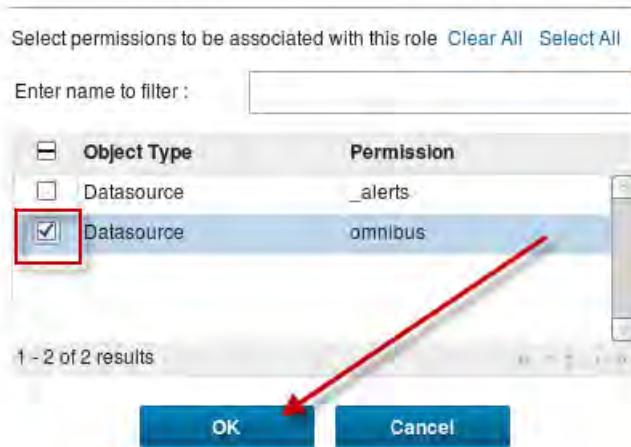
A user role specifies a set of permissions that are assigned to a role. [Learn More...](#)

Name:	OMNIbusEvents
Display Name:	OMNIbusEvents
Description:	

22. Scroll down, and select **Assign Permission to Role**. Click the icon to add a permission.



23. Select the **omnibus** Data Source, and click **OK**.



24. Select **Assign Users to Role**. Click the icon to add a user.



25. select **ncouser**, and click **OK**.



26. Scroll to the bottom of the page and click **OK** to create the role.

27. Click **OK** to confirm the new role.



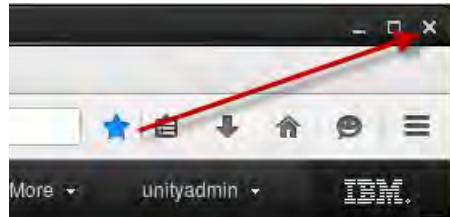
The new role is available, and the ncouser has access to the role.



28. Click the X to close the Administrative Settings tab.



29. Click the X to close the Firefox browser.



## Exercise 3 Configuring Event Analytics

### Configuring the Related Events feature

Netcool/Impact determines related events. Netcool/Impact evaluates the events from the archive database and automatically identifies relationships. You must complete customization steps to enable the Related Events feature.

#### ***ObjectServer modifications***

Configure the ObjectServer with customizations that are used by the related events feature. The solution includes an SQL to make the necessary changes.

1. Change to the directory where the SQL file is found:

```
cd /opt/IBM/tivoli/impact/add-ons/RelatedEvents/db/
```

2. Import the SQL file as follows:



**Note:** Enter the following text that starts with nco\_sql as one line.

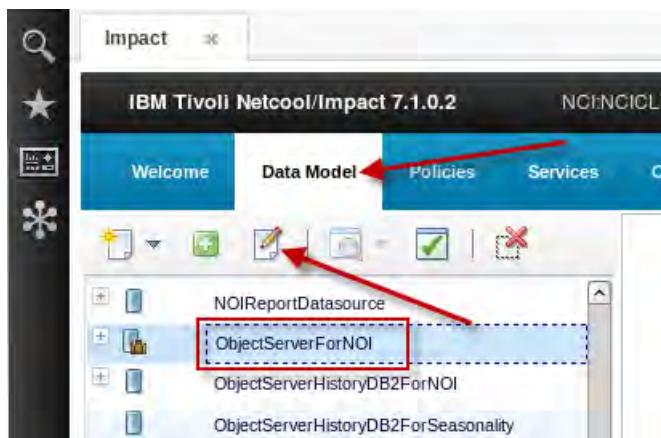
```
nco_sql -server NOI_AGG_P -user root -password object00 <
relatedevents_objectserver.sql

(0 rows affected)
```

## Impact configuration

The components that support event analytics are contained in Netcool/Impact. You must configure and enable several components.

1. Open a Firefox browser, if necessary.
2. Log in to Dashboard Application Services Hub as the **impactadmin** user with password **object00**.
3. Click the *snowflake* icon and select **Impact** to open the Netcool/Impact console.
4. Click the **Data Model** tab. Click **ObjectServerForNOI** to select it. Click the *pencil* icon to open the data source definition.



5. Enter **object00** for the password.

**ObjectServer Data Source Editor**

General Settings:

Provide general information which describes the data source. An \* indicates required fields.

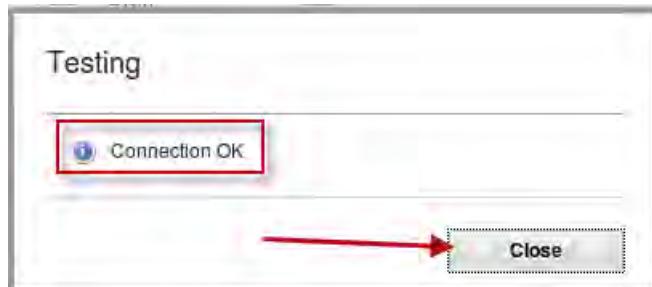
* Data Source Name:	ObjectServerForNOI
* Username:	root
Password:	*****
Maximum SQL Connection:	30

6. Scroll down and enter **host1.csite.edu** for the host name. Click **Test Connection**.

Provide information on the primary database. \* marks a required field.

* Host Name:	host1.csite.edu
* Port:	4100
<input type="checkbox"/> SSL Mode	
<b>Test Connection</b>	

- Verify that the connection is successful and click **Close** to close the window.

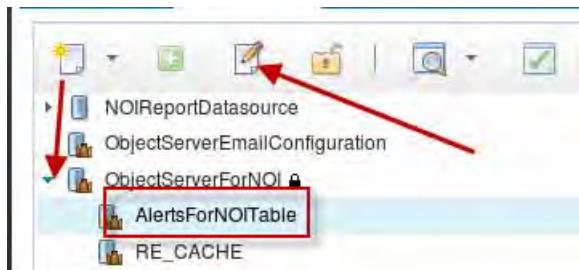


- Click the icon to save the changes.



**Note:** The data source page remains open after it is saved.

- Click the plus sign to expand **ObjectServerForNOI**. Click **AlertsForNOITable** to select it. Click the *pencil* icon to open the data type.

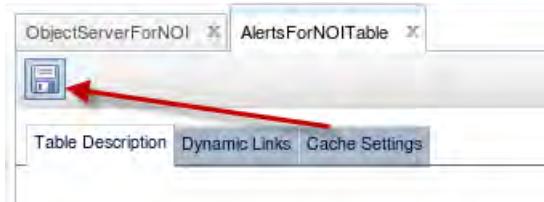


- Scroll down and click **Refresh**.



You added columns to the event record table in previous steps. When you click Refresh, it causes Netcool/Impact to discover the table changes.

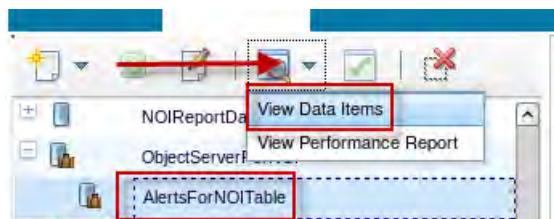
- Click the icon to save the data type changes.



12. Click the X on each tab to close the data source page and the data type page.



13. Click the plus sign to expand **ObjectServerForNOI**. Click **AlertsForNOITable** to select it. Click the *magnifying glass* icon and select **View Data Items**.



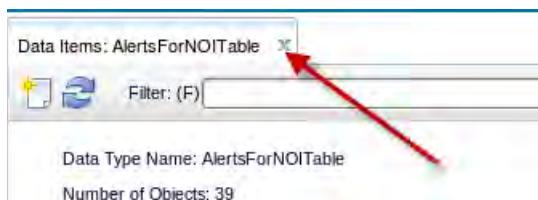
14. Verify that you are able to see event records.

Select:	(all)	Identifier
<input type="checkbox"/>	TokyoMachineStats4Stats	
<input type="checkbox"/>	OMNIBus ObjectServer : Total SQL time for all clients NOI_	AGG_P:
<input type="checkbox"/>	NCI:Impact:@host1.tivoli.educonnectedThu Apr 16 20:13:07 2015	



**Important:** If you receive an error message, repeat the previous steps to refresh the list of event columns and save the data type.

15. Click the X on the tab to close the page.

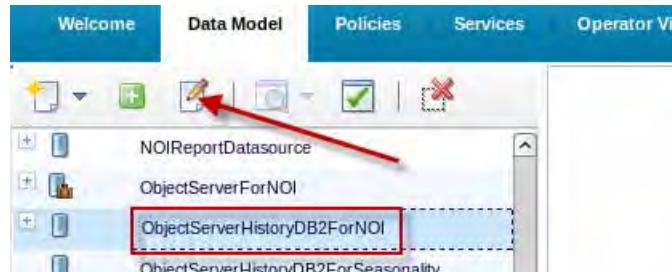


Netcool/Impact processes events from the event archive database to determine event relationships. You must configure the access credential for the event archive.



**Important:** The following steps are unique to an event archive on DB2. The event archive is supported on other database types. For an event archive on a different database type, you configure a different data source.

16. Click **ObjectServerHistoryDB2ForNOI** to select it. Click the *pencil* icon to open the data source definition.



17. Enter **db2inst1** for the user and **object00** for the password.

DB2 Data Source Editor

General Settings:

Provide general information which describes the data source. An \* indicates required fields.

* Data Source Name:	ObjectServerHistoryDB2ForNOI
* Username:	db2inst1
Password:	*****
Maximum SQL Connection:	5

18. Scroll down and enter **host1.csite.edu** for the host name. Click **Test Connection**.

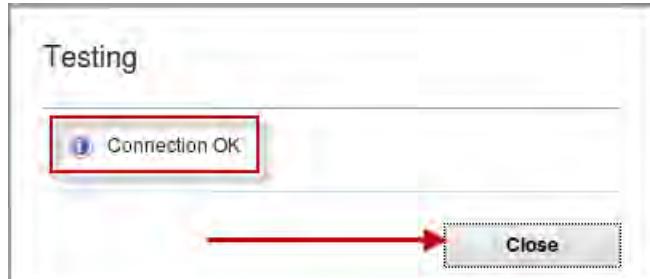
Primary Source:

Provide information on the primary database. \* marks a required field.

* Host Name:	host1.csite.edu
* Port:	50000
* Database:	REPORTER

**Test Connection**

19. Verify that the connection is successful and click **Close** to close the window.

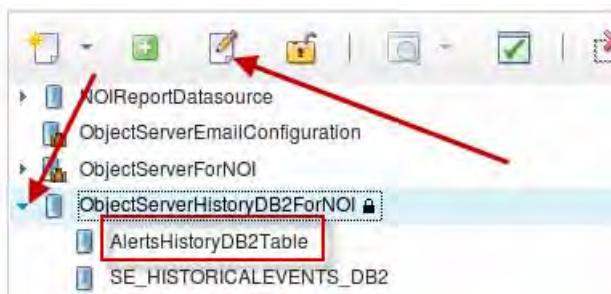


20. Click the icon to save the changes.



**Note:** The data source page remains open after it is saved.

21. Click the plus sign to expand **ObjectServerHistoryDB2ForNOI**. Click **AlertsHistoryDB2Table** to select it. Click the *pencil* icon to open the data type.

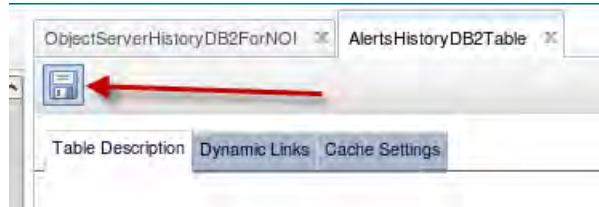


22. Scroll down and click **Refresh**.



**Note:** The refresh is required only if you add columns to the event record table in the archive database. You do not add columns in this class, but it is typical in a production environment.

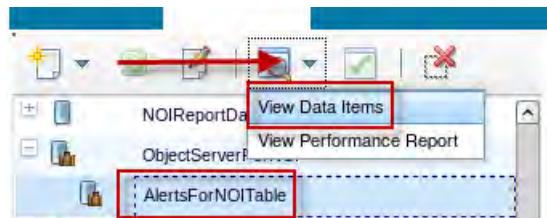
23. Click the icon to save the data type changes.



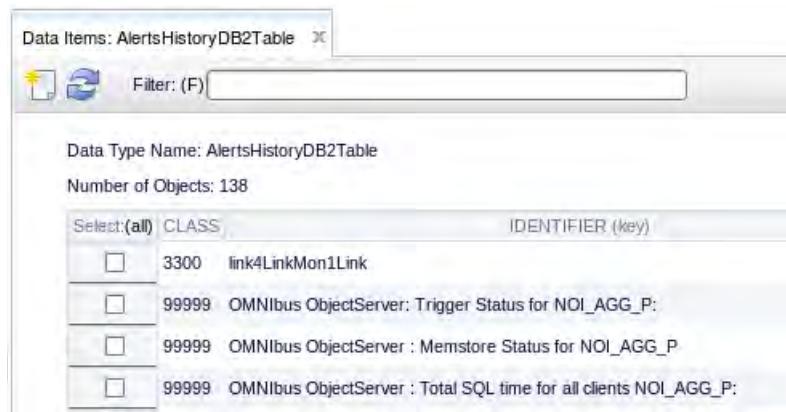
24. Click the X on each tab to close the data source page and the data type page.



25. Click the plus sign to expand **ObjectServerHistoryDB2ForNOI**. Click **AlertsHistoryDB2Table** to select it. Click the *magnifying glass* icon and select **View Data Items**.

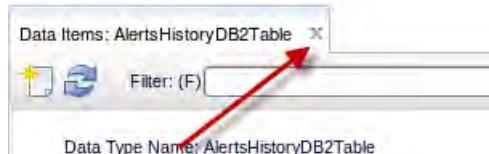


26. Verify that you are able to see records from the DB2 table.



**Important:** If you receive an error message, repeat the previous steps to refresh the list of event columns and save the data type.

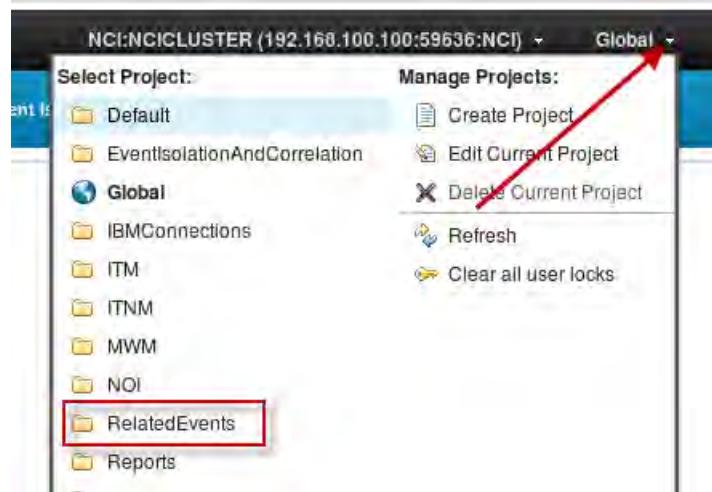
27. Click the X on the tab to close the page.



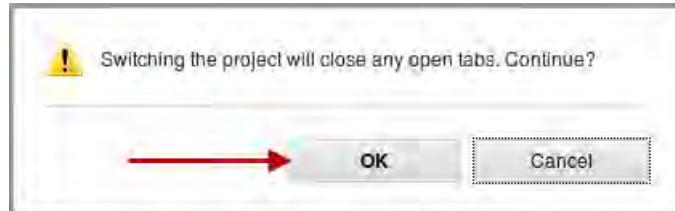
The related events feature uses two Netcool/Impact services. Verify that the services are started.

28. Click the **Services** tab.

29. Click the arrow and select the **RelatedEvents** project.

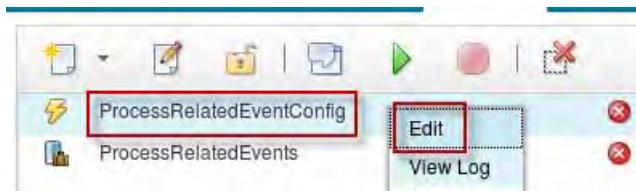


30. Click **OK** to confirm the change.

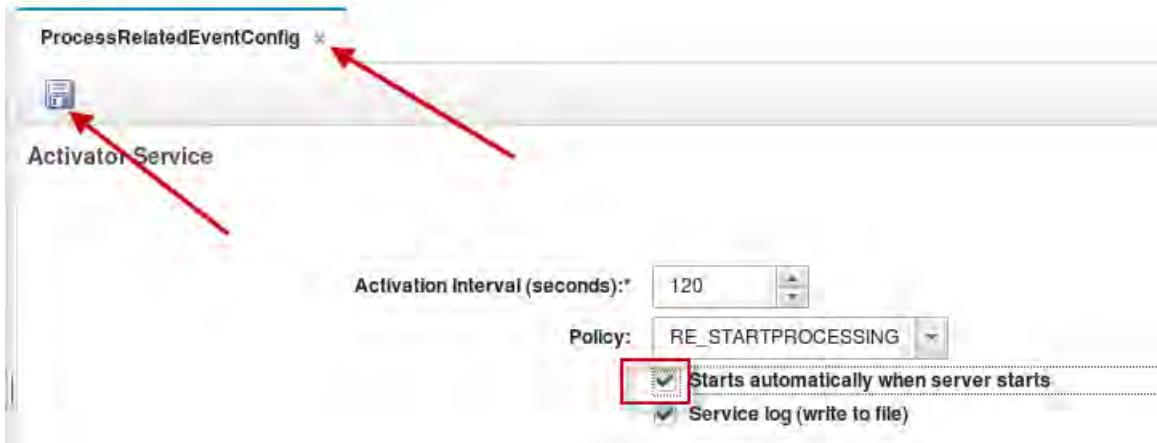


31. Start the required services as follows:

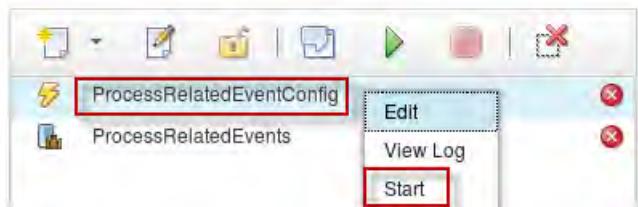
a. Right-click **ProcessRelatedEventConfig** and select **Edit**.



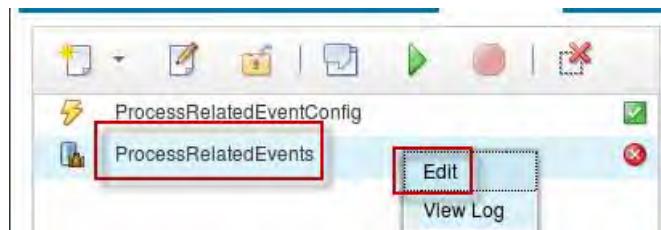
- b. Select the option to **Start automatically**. Click the icon to save the change. Click the X to close the page.



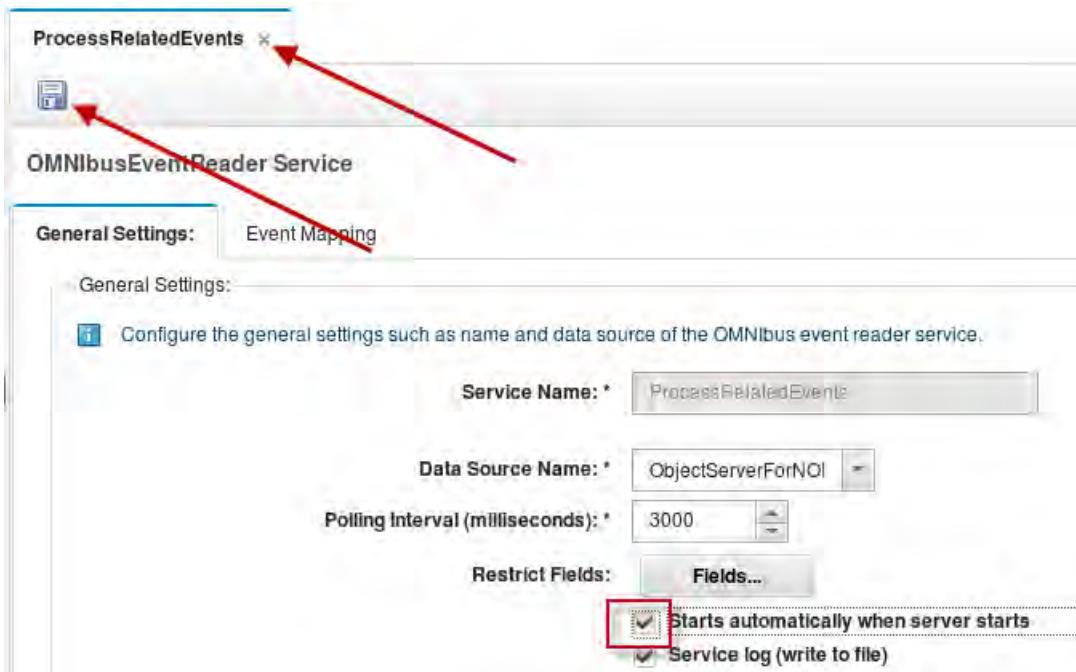
- c. Right-click **ProcessRelatedEventConfig** and select **Start**.



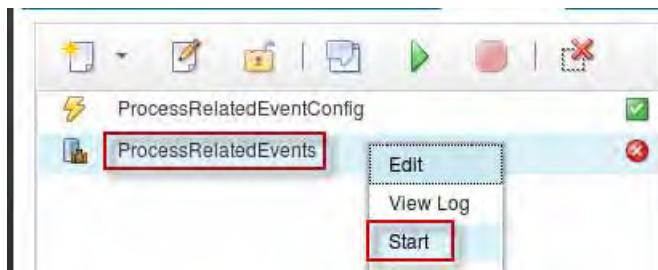
- d. Right-click **ProcessRelatedEvents** and select **Edit**.



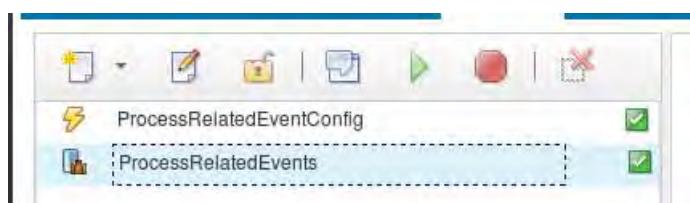
- e. Select the option to **Start automatically**. Click the icon to save the change. Click the X to close the page.



- f. Right-click **ProcessRelatedEvents** and select **Start**.



32. Verify that **ProcessRelatedEventConfig** and **ProcessRelatedEvents** are both started.



The green check marks indicate that the services are running.

33. Click the X to close the Impact console page.

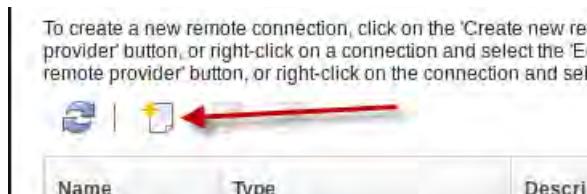


## Dashboard Application Services Hub modifications

1. Create a CURI connection to Netcool/Impact as follows:
  - a. Click the icon and select **Connections**.



- b. Click the icon to create a connection.



- c. Change the protocol to **HTTP**. Enter **host1.csite.edu** for the host. Enter **17310** for the port. Enter **impactadmin** for the user and **object00** for the password. Click **Search**.

**Server information**

\* Protocol: **HTTP** \* Host name: **host1.csite.edu** \* Port: **17310**

\* Path: **/ibm/tivoli/rest**

Connection goes through a firewall

Firewall address: \_\_\_\_\_ Firewall port: \_\_\_\_\_

Use the following credentials to query the remote data providers:

\* Name: **impactadmin** \* Password: **\*\*\*\*\***

\* Confirm password: **\*\*\*\*\***

**Search**

If the access information is correct, the Netcool/Impact cluster is shown in the bottom of the window.

- d. Select the cluster, scroll to the bottom of the page, and click **OK** to save the connection.

Name	Description
<b>Impact_NCICLUSTER</b>	

Total: 1 Selected: 1

**Connection information**

\* Name: **Impact\_NCICLUSTER**

2. Verify that the connection is shown for Netcool/Impact.

Name	Type	Description
<b>Impact_NCICLUSTER</b>	Impact_NCICLUSTER	Impact_NCICLUSTEF
Tivoli Directory Integrator	TDI	TDI Generic Data Pro

3. Click the X to close the Connections page.



A role controls user access to the related events feature. You must add the role to a group to enable access.

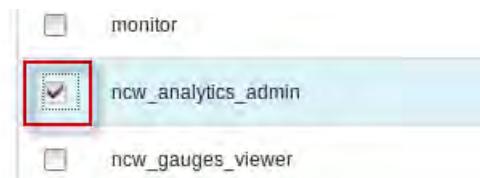
4. Click the icon and select **Group Roles**.



5. Click **Search** to display the available groups. Click **Netcool\_Admin**.



6. Scroll down and select **ncw\_analytics\_admin**. Click **Save**.



7. Log out of Dashboard Application Services Hub.

8. Log in to Dashboard Application Services Hub as **ncoadmin** with password **object00**.

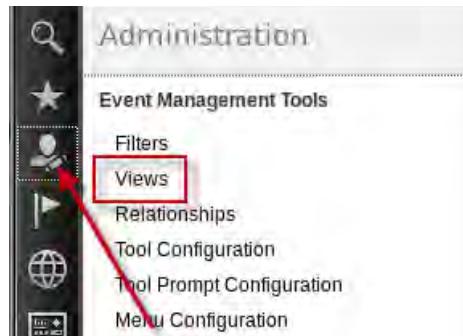
- Click the icon and observe the features.



**Note:** The `ncw_analytics_admin` role provides access to the related events user interface and seasonality.

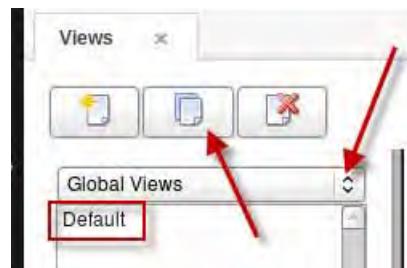
The next step is to create an event view and add the relationship definition.

- Click the icon and select Views.

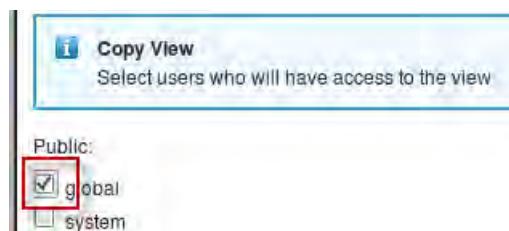


The View Builder opens.

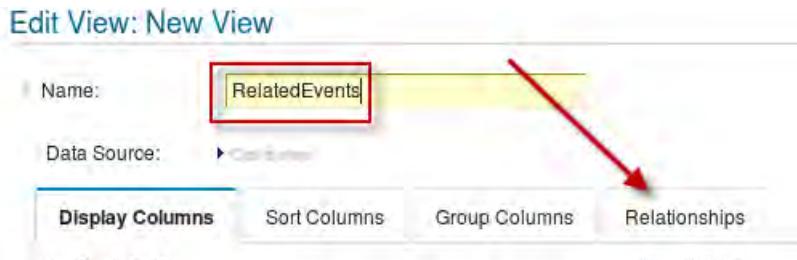
- Click the arrow and select Global Views. Click Default to select it. Click the icon to copy the view.



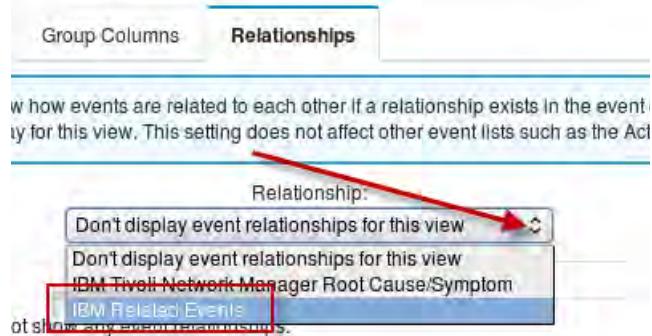
- Select global and click OK.



13. Enter **RelatedEvents** for the name and click the **Relationships** tab.



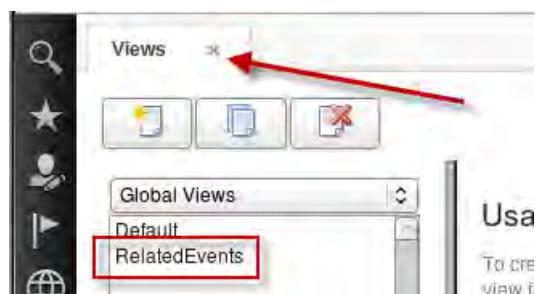
14. Click the arrow and select **IBM Related Events**.



15. Click **Save and Close**.



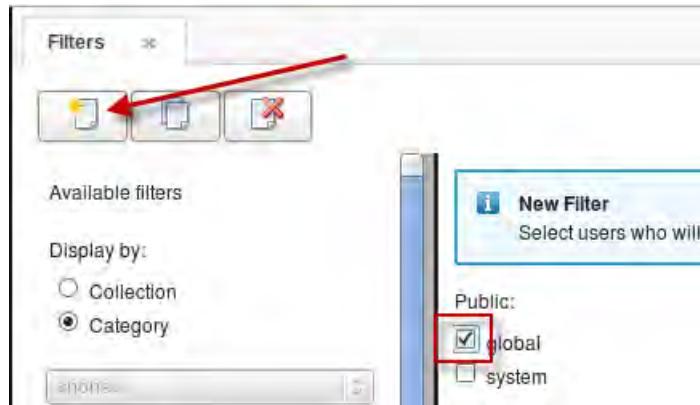
16. Click the X to close the Views page.



17. Click the icon and select **Filters**.



18. Click the icon to create a new filter. Select **global**, scroll to the bottom, and click **OK**.



19. Enter **RelatedEvents** for the name. Click the arrow and select the **RelatedEvents** view.

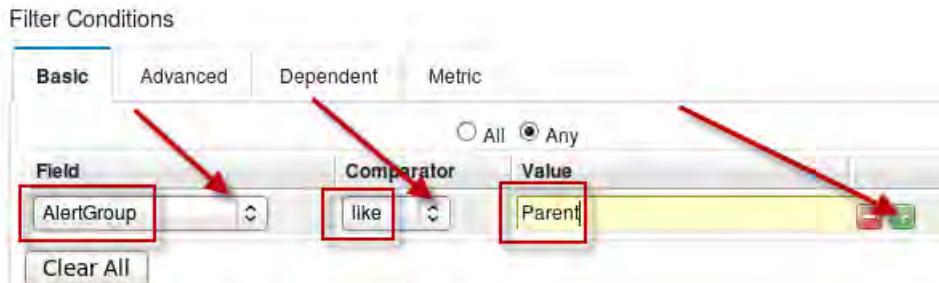
#### Edit Filter: New Filter

##### Filter Attributes

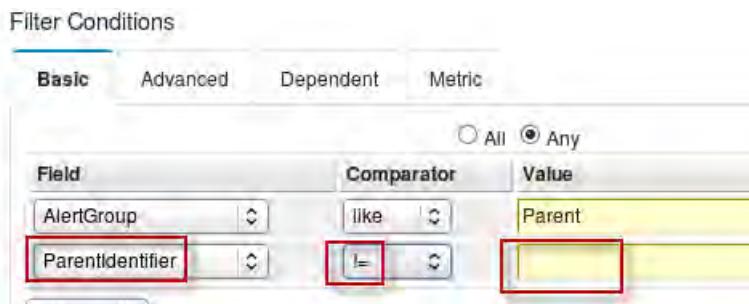
Name: **RelatedEvents**

Default view: **RelatedEvents**

20. Click the arrow under **Field** and select **AlertGroup**. Click the arrow under **Comparator** and select **like**. Enter **Parent** for Value. Click the green plus sign (+) to add another condition.



21. Click the arrow under **Field** and select **ParentIdentifier**. Click the arrow under **Comparator** and select **!=**. Leave Value empty.



The filter conditions select any event where the text Parent is shown in the value of the AlertGroup column or the value of the ParentIdentifier column is not equal to a blank.

22. Click **Save and Close**.

23. Click the X to close the Filter page.



The configuration for related events is complete.

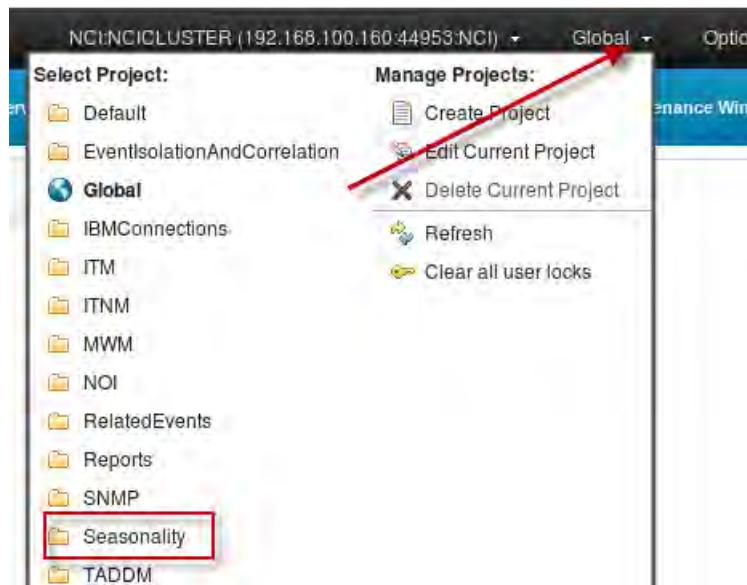
## Configuring seasonality

Event seasonality is also implemented with Netcool/Impact. The Seasonality feature also uses the event archive database. The Seasonality feature uses the same Netcool/Impact data source definition as the Related Events feature. You configured the data source in the previous step. The only Netcool/Impact components that require verification for seasonality are services.



**Note:** You are currently logged in to Dashboard Application Services Hub as the **ncoadmin** user. You configured the ncoadmin user for access to Netcool/Impact in a previous exercise.

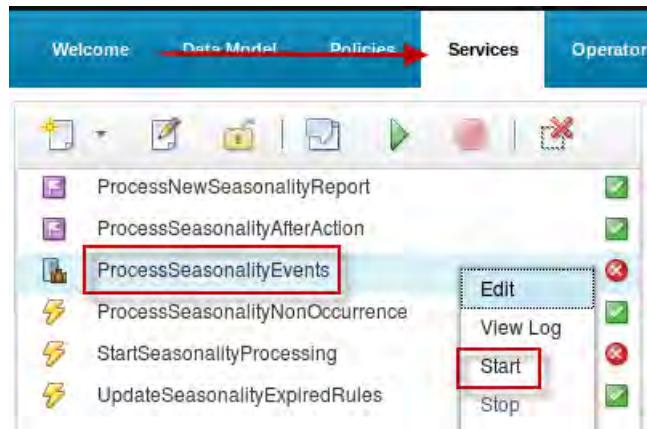
1. Click the **snowflake** icon and select **Impact** to open the Netcool/Impact console.
2. Change the project to **Seasonality**.



- Click **OK** to confirm the change.



- Click the **Services** tab and scroll down in the list of services.
- Right-click **ProcessSeasonalityEvents**, and select **Start**.



- Verify that the required services are started.



The green check marks indicate that the service is running.



**Important:** The **StartSeasonalityProcessing** service is stopped, which is normal.

The configuration for Event Seasonality is complete.

- Click the **X** to close the Netcool/Impact console page.

# Loading the sample database

Event analytics requires a reasonable number of historical event records. The course image includes a file that contains over 1 million records. In the following steps, you import the file into the existing event archive database.

1. Open a terminal window if necessary.
2. Switch to the DB2 instance owner.

```
su - db2inst1
Password: object00
```

3. Change to the location of the DB2 file.

```
cd /workshop/relatedevents
```

4. Connect to the REPORTER database.

```
db2 connect to REPORTER
```

Database Connection Information

```
Database server = DB2/LINUXX8664 10.5.3
SQL authorization ID = DB2INST1
Local database alias = REPORTER
```

5. Import the file.

```
db2 load from reporter_status_export_data.ixf of ixr insert into reporter_status
. . .
SQL3515W The utility has finished the "BUILD" phase at time "11/09/2015
18:25:39.616905".
```

```
Number of rows read = 1321112
Number of rows skipped = 0
Number of rows loaded = 1321112
Number of rows rejected = 0
Number of rows deleted = 0
Number of rows committed = 1321112
```



**Important:** The command runs for several minutes.

6. Exit the **db2inst1** user.

```
exit
```

7. Remove the file to save disk space.

```
cd /workshop/relatedevents
/bin/rm reporter_*
```

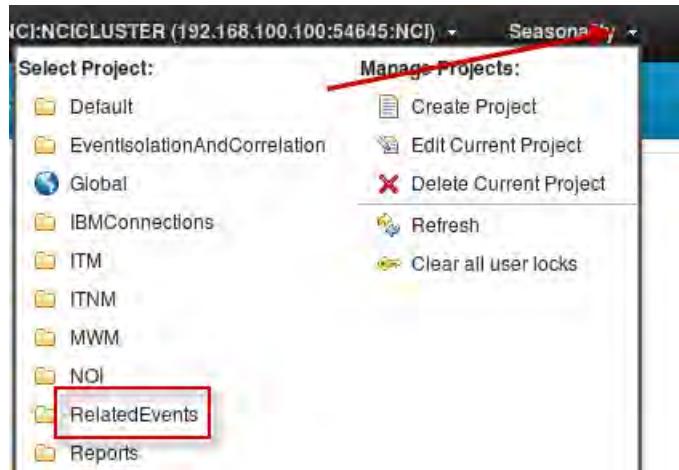
## Installing Netcool/Impact policies

The workshop image contains a Netcool/Impact policy and parameter file. You use the policy to generate synthetic Netcool/OMNIbus event records to demonstrate related event grouping.

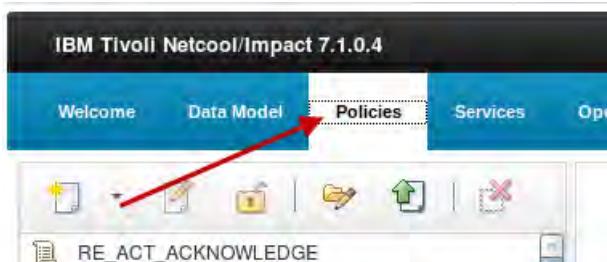


**Note:** You are currently logged in to Dashboard Application Services Hub as the **ncoadmin** user.

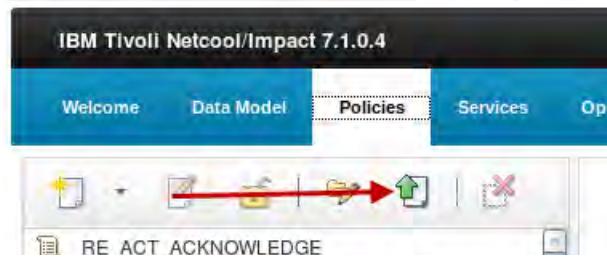
1. Click the *snowflake* icon and select **Impact** to open the Netcool/Impact console.
2. Change the project to **RelatedEvents**.



3. Click the **Policies** tab.



4. Click the indicated icon to upload a policy file.



5. Click **Browse**.

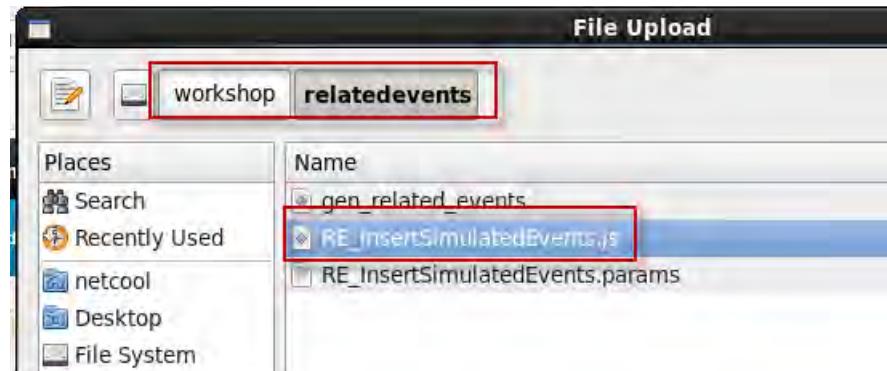
### Upload Policy

Select a policy or parameters file to upload.

Policy file (.ipl or .js)

**Browse ...** No file selected

6. Navigate to **/workshop/relatedevents**, and select **RE\_InsertSimulatedEvents.js**. Click **Open**.



7. Select **Parameters file**. Click **Browse**.

### Upload Policy

Select a policy or parameters file to upload.

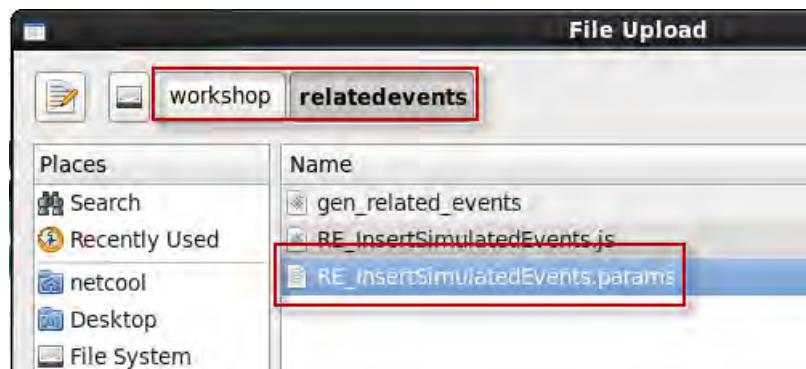
Policy file (.ipl or .js)

**Browse ...** File to upload: RE\_InsertSimulatedEvents.js

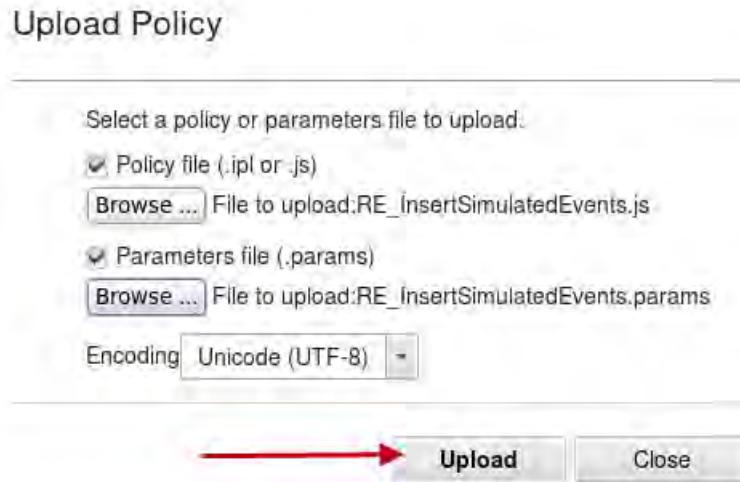
Parameters file (.params)

**Browse ...** No file selected

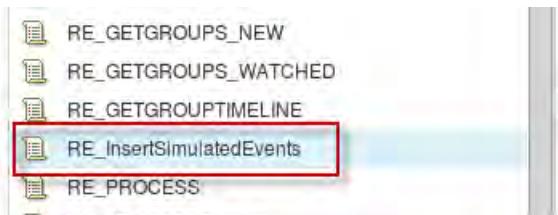
8. Navigate to **/workshop/relatedevents**, and select **RE\_InsertSimulatedEvents.params**. Click **Open**.



9. Click **Upload**.



10. Verify that the policy appears.

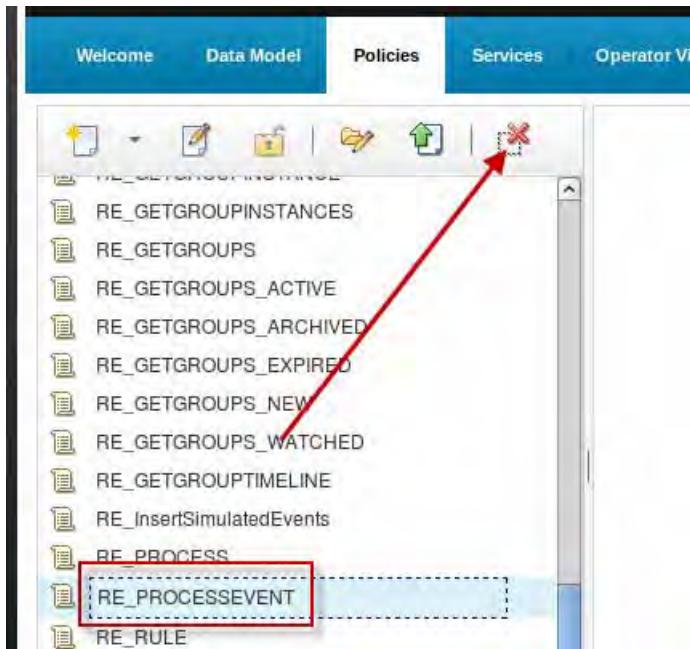


## Installing updated Netcool/Impact policy

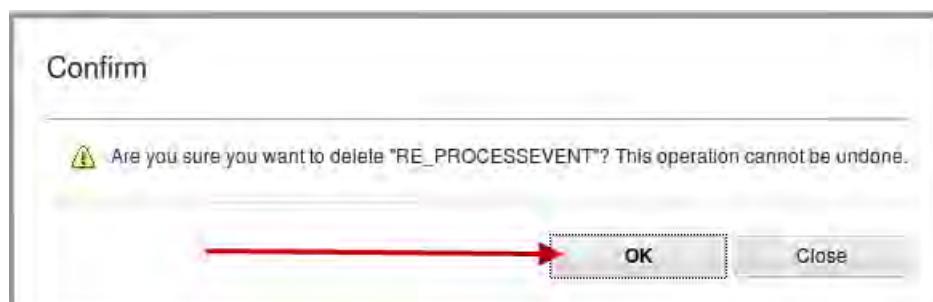
When the workshop was created, an issue with an existing Netcool/Impact policy existed. This policy processes Netcool/OMNIbus event records for related events analysis. The workshop

contains an updated copy of the policy. You must remove the existing policy, and install the updated version.

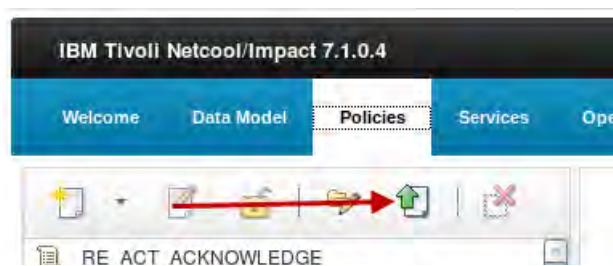
1. Click policy **RE\_PROCESSEVENT** to select it. Click the red X icon to delete the policy.



2. Click **OK** to confirm the delete.



3. Click the indicated icon to upload a policy file.



4. Click **Browse**.

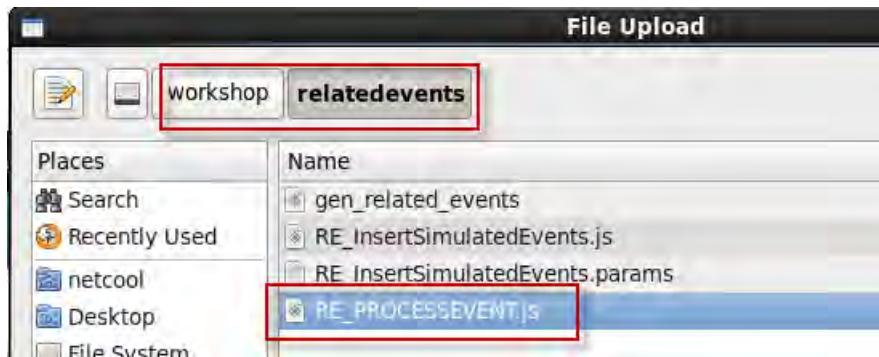
### Upload Policy

Select a policy or parameters file to upload.

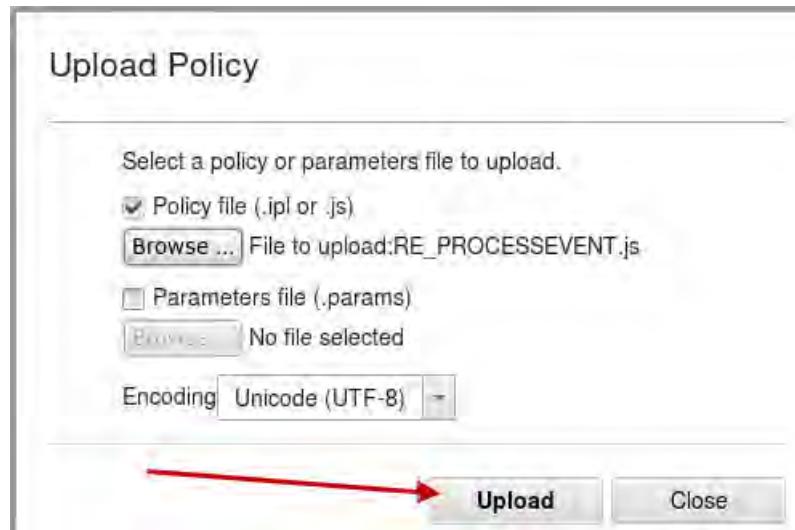
Policy file (.ipl or .js)

No file selected

5. Navigate to **/workshop/relatedevents**, and select **RE\_PROCESSEVENT.js**. Click **Open**.



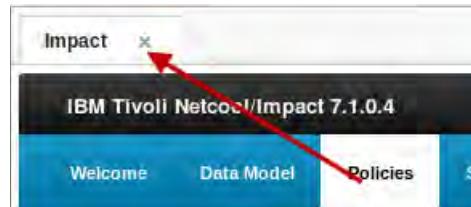
6. Click **Upload**.



7. Verify that the policy appears.



8. Click the X to close the Impact page.

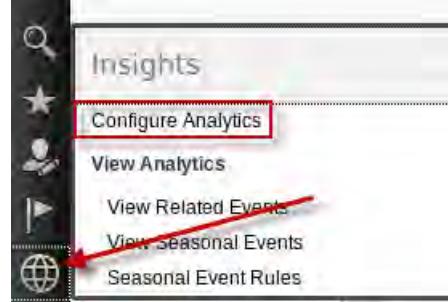


9. Log out as **ncoadmin**.

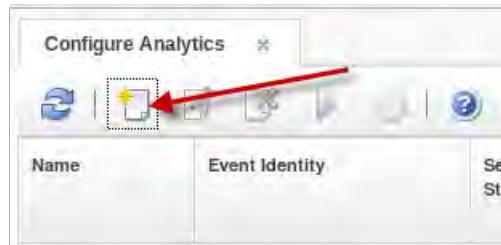
## Exercise 4 Verifying Netcool Operations Insight features

### Verifying Related Events

1. Log in to Dashboard Application Services Hub as the **ncoadmin** user with password **object00**.
2. Click the icon and select **Configure Analytics**.

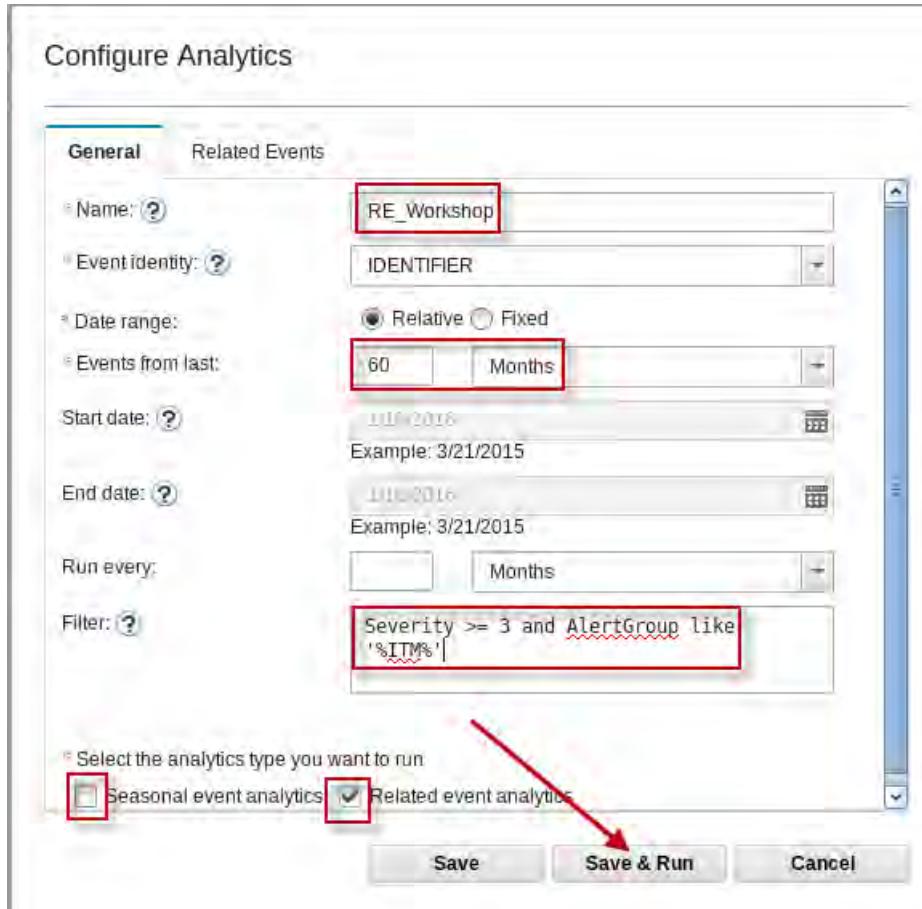


3. Click the icon to create a new request.



4. Configure the rule settings.
  - a. Enter **RE\_Workshop** for the name.
  - b. Select **60 Months** for the date range.
  - c. Enter **Severity >= 3 and AlertGroup like '%ITM%'** for the filter.

- d. Clear **Seasonal event analytics**.
- e. Select **Related event analytics**.
- f. Click **Save and Run**.



The workshop image contains a collection of historical event records. The records are taken from a lab environment, and are old. In a production environment, you typically perform the analysis based on more recent data.

You select events where Severity  $\geq 3$  because you want events that constitute an issue. You limit the events based on the AlertGroup column to only IBM Tivoli Monitoring events.

Netcool/Impact schedules the associated policies to process the rule and sets the Phase to *Waiting to run*.

	Seasonality Phase	Seasonality Phase Progress	Related Event Phase	Related Event Phase Progress
31:23 A	Saved, Waiting for user ac	0%	Saved, Waiting for user ac	0%
7:20 PM	Not Enabled	0%	Queued, Waiting to run	0%

After a short time, you see the phase change to indicate that the analysis is started.

Phase	Seasonality Phase Progress	Related Event Phase	Related Event Phase Progress	Schedule
or user action	0%	Saved, Waiting for user action	0%	No
	0%	Step 1 of 5: Retrieving events	33%	No

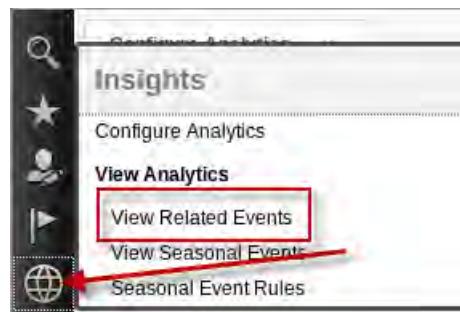
When the analysis is complete, you see the following result.

Phase	Seasonality Phase Progress	Related Event Phase	Related Event Phase Progress	Schedule
er action	0%	Saved, Waiting for user action	0%	No
	0%	Completed	100%	No



**Important:** Related event analytics requests run every 2 minutes by default. It might take a few moments before the status changes to processing. The analysis runs for several minutes.

5. Click the icon and select **View Related Events**.



A page opens with the results of the analysis.

Configuration	Strength	Groups	Events	Node	Summary
All	---	87	501		
RE_Workshop	Strong	87	501	tabantest.tivlab.raleigh.ibm.com	TDSBLD: ITM: The
				tabantest.tivlab.raleigh.ibm.com	TDSBLD: ITM: The
				tabantest.tivlab.raleigh.ibm.com	TDSBLD: ITM: The
				tabantest.tivlab.raleigh.ibm.com	TDSBLD: ITM: The
				fluid.tivlab.raleigh.ibm.com	TDSBLD: ITM: The
				fluid.tivlab.raleigh.ibm.com	TDSBLD: ITM: The
				fw2w2k.tivlab.austin.ibm.com	TDSBLD: ITM: The
				fw2w2k.tivlab.austin.ibm.com	TDSBLD: ITM: The
				rtpbwin7a.tivlab.raleigh.ibm.com	TDSBLD: ITM: The

The analysis determines that 87 potential event groups exist. The group names are shown in the lower portion of the pane. The number of events for each group is listed after the group name.

6. Scroll down, if necessary, and click the entry with 157 events and 6 instances. The event records are listed in the view on the right.

Configuration	Strength	Groups	Events	Node	Sum
All	---	87	501	chianti,tivlab,raleigh.ibm.com	: Lin
RE_Workshop	Strong	87	501	chianti,tivlab,raleigh.ibm.com	: Lin
Group Name	Strength	Events	Instances	Reviewed	
RE_Workshop:1	Strong	157	8	No	
RE_Workshop:7	Strong	15	19	No	
RE_Workshop:20	Strong	11	26	No	



- Right-click **RE\_Workshop:1** and select **Deploy**.

Group Name	Strength	Events ▾	Instances	Reviewer
RE_Workshop:1	Strong	157	6	
RE_Workshop:7	Strong	15	19	
RE_Workshop:20	Strong	11	20	
RE_Workshop:65	Strong	8	8	



**Important:** Use the group in your example with 157 events.

The group entry is removed from the list and one active group exists.

- Click **Active[1]** to view the active group.

Configuration	Time Fired	Time Fired in Last Month	Last Fired	Last Occurred I	Last Occurred II	Last Occurred III
- All	0	0		0%	0%	0%
RE_Workshop	0	0		0%	0%	0%

Group Name	Time Fired	Time Fired in Last Month	Last Fired	Last Occurred I	Last Occurred II	Last Occurred III
RE_Workshop:1	0	0		0%	0%	0%

The page now contains statistics that are related to the active group. The statistics are based on real-time events as they arrive in the ObjectServer.

The image includes a custom script that you can use to generate simulated events for the active group.

- In a terminal window, change to the location of the script.

```
cd /workshop/relatedevents
```

- Generate simulated events.

```
./gen_related_events RE_Workshop:1
```

```
Generating related events for group: RE_Workshop:1
RE_InsertSimulatedEvents Policy completed successfully
```

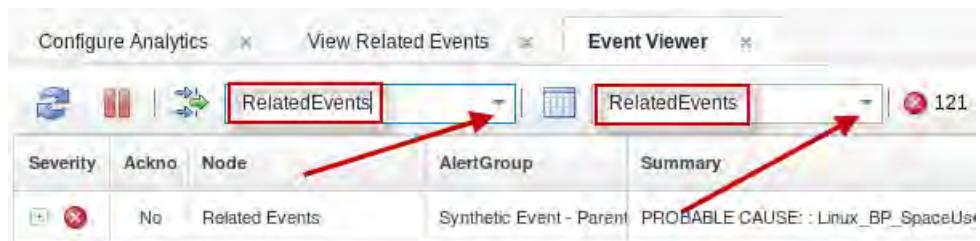


**Important:** Use the group in your example with 157 events.

11. Return to the browser, click the icon and select **Event Viewer**.



12. Click the arrow and select the **RelatedEvents** filter. Click the arrow and select the **RelatedEvents** view.



The event list contains a single record. This event is the synthetic parent event that Netcool/Impact generated.

13. Click the *plus sign* to expand the group.

Severity	Ackno	Node	AlertGroup	Summary
[+]	No	Related Events	Synthetic Event - Parent	PROBABLE CAUSE: Linux_BP_SpaceUsedPct_Critical(Disk_Used_Percent>=95 AND FS_Type<=1)

The related events are listed under the parent.

Severity	Ackno	Node	AlertGroup	Summary
[+]	No	Related Events	Synthetic Event - Parent	PROBABLE CAUSE: Linux_BP_SpaceUsedPct_Critical(Disk_Used_Percent>=95 AND FS_Type<=1)
(x)	No	chianti.tivlab.raleigh.ibm.com		: Linux_BP_SpaceUsedPct_Critical(Disk_Used_Percent>=95 AND FS_Type<=1)
(x)	No	chianti.tivlab.raleigh.ibm.com		: Linux_BP_SpaceUsedPct_Critical(Disk_Used_Percent>=95 AND FS_Type<=1)
(x)	No	chianti.tivlab.raleigh.ibm.com		: Linux_BP_SpaceUsedPct_Critical(Disk_Used_Percent>=95 AND FS_Type<=1)
(x)	No	chianti.tivlab.raleigh.ibm.com		: Linux_BP_SpaceUsedPct_Critical(Disk_Used_Percent>=95 AND FS_Type<=1)
(x)	No	chianti.tivlab.raleigh.ibm.com		: Linux_BP_SpaceUsedPct_Critical(Disk_Used_Percent>=95 AND FS_Type<=1)

## Verifying the Seasonal Events feature

You are currently logged in as the **ncoadmin** user.

1. Click the icon and select **Configure Analytics**.



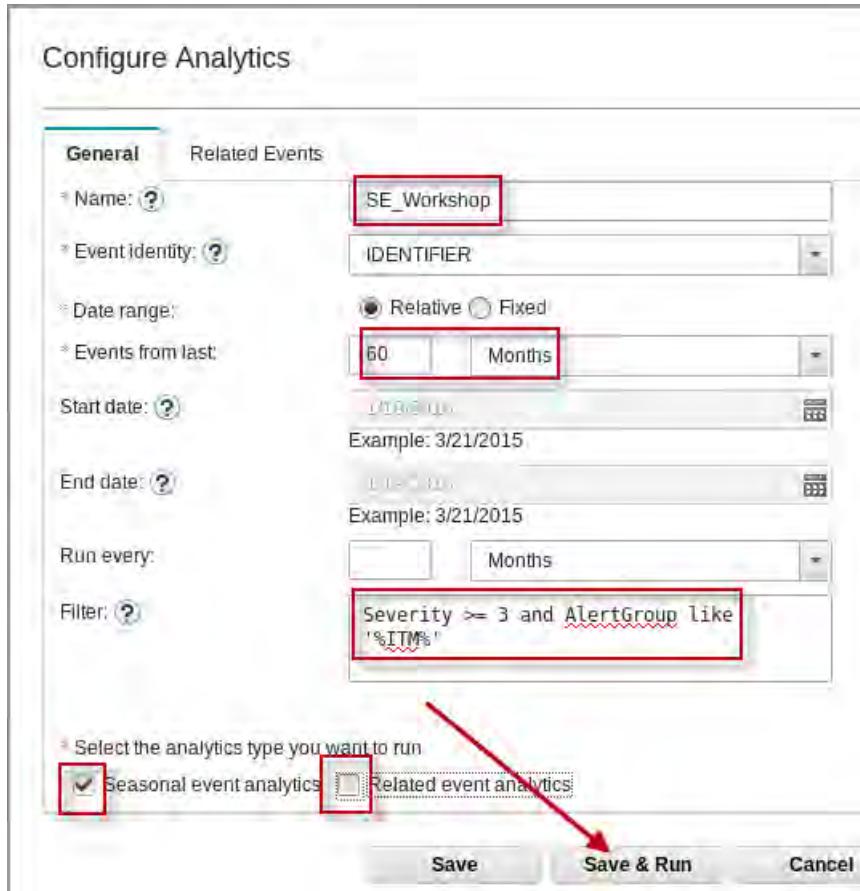
2. Click the icon to create a new configuration.



3. Configure the rule settings.

- a. Enter **SE\_Workshop** for the name.
- b. Select **60 Months** for the date range.
- c. Enter **Severity >= 3 and AlertGroup like '%ITM%'** for the filter.
- d. Select **Seasonal event analytics**.
- e. Clear **Related event analytics**.

f. Click Save and Run.



The workshop image contains a collection of historical event records. The records are taken from a lab environment, and are old. In a production environment, you typically perform the analysis based on more recent data.

You select events where Severity  $\geq 3$  because you want events that constitute an issue. You limit the events based on the AlertGroup column to only IBM Tivoli Monitoring events.

Netcool/Impact schedules the associated policies to process the rule and sets the Phase to *Waiting to run*.

	End Time	Seasonality Phase	Seasonality Phase Progress
2 PM	Jan 19, 2016 12:18:12 PM	Saved, Waiting for user action	0%
PM	Jan 19, 2016 9:49:24 PM	Queued, Waiting to run	0%
PM	Jan 19, 2016 8:42:53 PM	Not Enabled	0%

After a short time, you see the phase change to indicate that the analysis is started.

Phase	Seasonality Phase Progress	Related Event Phase	Related Event Phase Progress	%
For user ac	0%	Saved, Waiting for user ac	0%	N
	0%	Step 1 of 5: Retrieving eve	33%	N

When the analysis is complete, you see the following result.

End Time	Seasonality Phase	Seasonality Phase Progress	Rel
Nov 9, 2015 3:00:01 PM	Saved, Waiting for user ac	0%	Sav
Nov 9, 2015 6:40:32 PM	Not Enabled	0%	Cor
Nov 9, 2015 8:03:12 PM	Completed	100%	Not



**Important:** Seasonal event analytics requests run every 2 minutes by default. It might take a few moments before the status changes to processing. The analysis runs for several minutes.

- Click the icon and select **View Seasonal Events**.



A page opens with the results of the analysis.

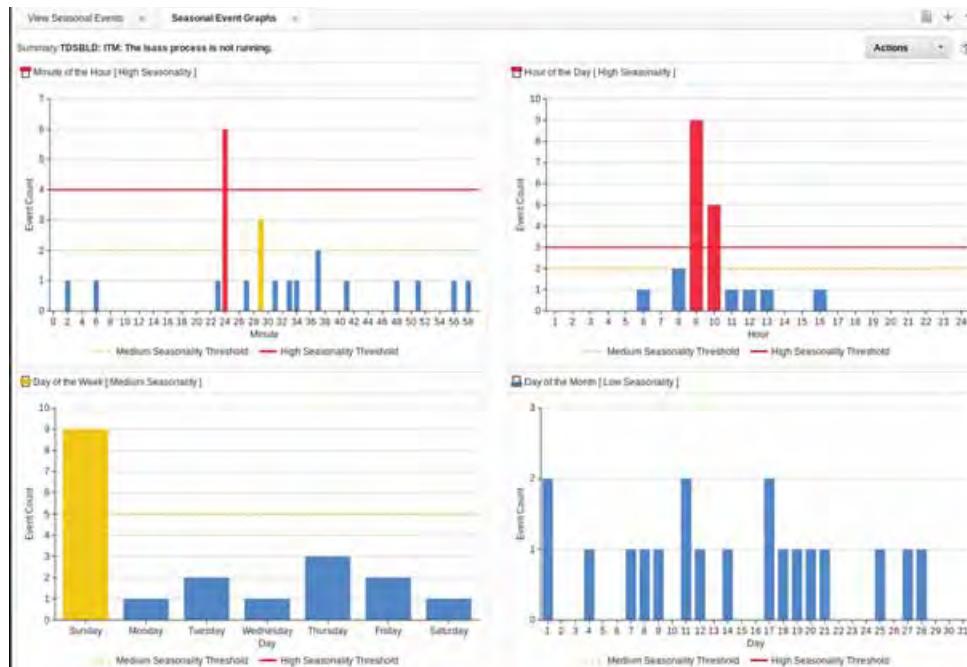
Configure Analytics		View Seasonal Events	
Configuration	Event Count	Node	Summary
ALL	265	plaix61-64.tivlab.austin.ibm.com	TDSBLD; UNIX
SE_Workshop	265	leghorn.tivlab.raleigh.ibm.com	TDSBLD; UNIX
		goldeneye.tivlab.raleigh.ibm.com	TDSBLD; UNIX
		kobol.tivlab.raleigh.ibm.com	TDSBLD; Linux

The analysis determines that there are over 260 potential seasonal events. The right side lists each of the events.

- Right-click the first event record, and select **Show Seasonal Event Graphs**.

Event Count	Node	Summary	Alert Group
265	ducttape.tivlab.raleigh.ibm.com	TDSBLD: ITM: The lsass process is not running	
265	s3w2k.tivlab.austin.ibm.com	TDSBLD: ITM: The lsass process is not running	
	p3aix53-32.tivlab.austin.ibm.com	TDSBLD: UNIX: The lsass process is not running	

The results open in a new tab.



The results are presented in four graphs:

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

The results are color-coded based on the statistical confidence that the event is considered seasonal. In the example that is shown here, the graphs for Minute of the Hour and Hour of the Day are labeled in red. The color red is an indication of a high statistical confidence that this event repeats consistently based on minute and hour. The Day of the Week graph is labeled in yellow. The yellow color is an indication that the event most likely repeats consistently on Sundays. The Day of the Month graph is labeled green. The blue is an indication that the event does not appear to repeat consistently on any day of the month.

Users can use the output in these graphs for several purposes.

- Validate expected behavior.

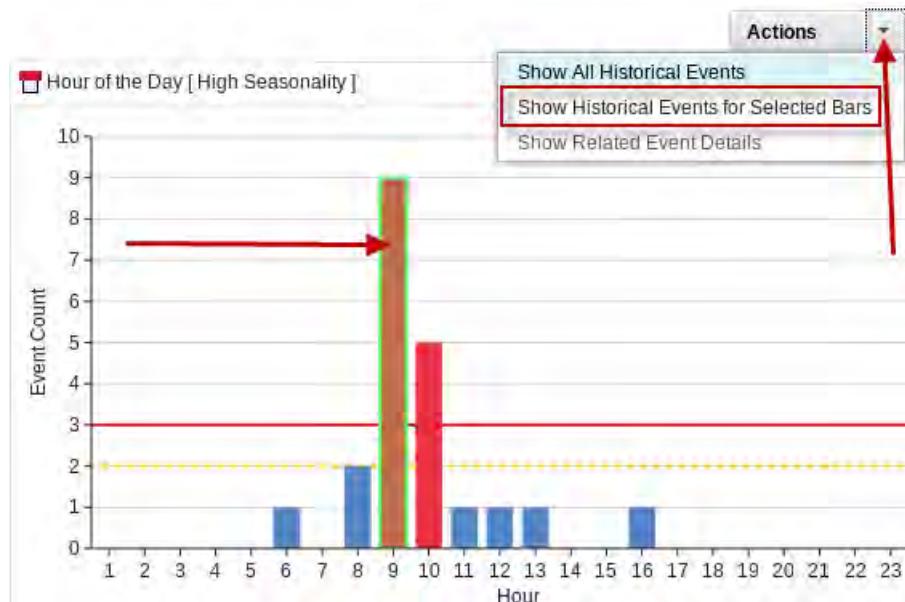
In most production environments, some events occur in a pattern. For example, server instrumentation might indicate excessive disk I/O activity at the same time every night. Disk backups are the cause of this known condition. You can use seasonal reports to verify that the activity occurs as expected.

- Identify unexpected behavior.

Given the same scenario that was presented previously, a seasonal report can identify those periods where excessive disk I/O occurs during times that are outside of normal backup windows.

The seasonality feature provides a number of tools that can be used to investigate the event records.

6. Click the bar for hour 10 to select it. Click the arrow next to **Actions** and select **Show Historical Events for Selected Bars**.



The results open in a new tab.



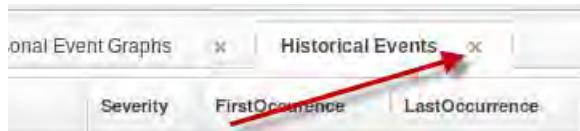
**Important:** Make sure that you do not select more than one column. If you select more than one column, the result is a logical AND of the selected values. For example, all values equal to hour 9 AND all values equal to hour 10. It is impossible for values of hour 9 and hour 10, so the result is empty.

7. Examine the values for FirstOccurrence.

Summary	Node	Severity	FirstOccurrence	LastOccurrence
TDSBLD: ITM: The lsass process is not running.	ducttape.tivlab.raleigh.ibm.com	5	Jul 11, 2013 9:58:45 AM	Jul 11, 2013 9:58:45 AM
TDSBLD: ITM: The lsass process is not running.	ducttape.tivlab.raleigh.ibm.com	5	Jul 21, 2013 9:29:29 AM	Jul 21, 2013 10:06:12 AM
TDSBLD: ITM: The lsass process is not running.	ducttape.tivlab.raleigh.ibm.com	5	Jul 28, 2013 9:29:33 AM	Jul 28, 2013 10:06:13 AM
TDSBLD: ITM: The lsass process is not running.	ducttape.tivlab.raleigh.ibm.com	5	Aug 4, 2013 9:29:33 AM	Aug 4, 2013 10:06:10 AM
TDSBLD: ITM: The lsass process is not running.	ducttape.tivlab.raleigh.ibm.com	5	Aug 11, 2013 9:24:32 AM	Aug 11, 2013 10:06:16 AM
TDSBLD: ITM: The lsass process is not running.	ducttape.tivlab.raleigh.ibm.com	5	Aug 18, 2013 9:24:31 AM	Aug 18, 2013 10:06:06 AM
TDSBLD: ITM: The lsass process is not running.	ducttape.tivlab.raleigh.ibm.com	5	Aug 25, 2013 9:24:23 AM	Aug 25, 2013 10:06:52 AM
TDSBLD: ITM: The lsass process is not running.	ducttape.tivlab.raleigh.ibm.com	5	Sep 1, 2013 9:24:27 AM	Sep 1, 2013 10:06:55 AM
TDSBLD: ITM: The lsass process is not running.	ducttape.tivlab.raleigh.ibm.com	5	Sep 8, 2013 9:24:18 AM	Sep 8, 2013 10:06:51 AM

The events occurred on different days, but always during the 9:00 AM hour.

8. Click the X to close the **HistoricalEvents** tab.



9. Click the X to close the **SeasonalEventGraph** tab.



After evaluating the event results, the administrator can decide to perform an automated action for one or more identified events.

## Creating a seasonal event rule

You can use seasonal event rules to apply an action to specific events.

You can choose to apply actions to a selected seasonal event, or to a seasonal event and some or all of its related events.

You can use seasonal event rules to apply actions to suppress and unsuppress an event to modify or enrich an event, or to create an event when the selected event does not occur when expected.

In this exercise, you create a rule that generates an event when the seasonal event does not occur at the designated time. The seasonal event in this example is expected to occur on Sunday, at 9:00 AM. In a production environment, you use those parameters to create the rule. However, in the

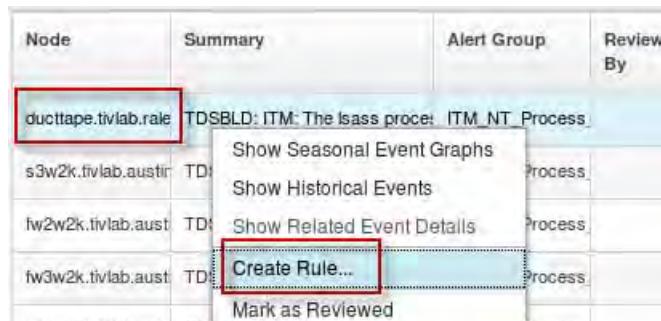
workshop environment you cannot use Sunday, or possibly even 9:00 AM. You must use a day and time that is close to the current day and time in order to observe the expected result.

1. Open a Terminal window, and enter the **date** command to determine the current date and time.

```
File Edit View Search Terminal Help
[netcool@host1 relatedevents]$ date
Wed Jan 20 12:26:01 UTC 2016
[netcool@host1 relatedevents]$
```

In the example that is shown here, the current day of the week is Wednesday, and the current time is 12:26. In the following steps, you create a rule that generates an artificial event if a seasonal event does not occur on Wednesday, at 12:35. You must allow some time to create and activate the rule.

2. Right-click an event and select **Create Rule**.



3. Enter **SE\_Workshop\_Rule** for the name.
4. Click the arrow and select **Day of Week**.
5. Click the arrow and select **Is**.
6. Click the arrow and select **Wednesday**.



**Important:** You select the appropriate day of the week based on your local date and time.

7. Click the green plus sign to add another rule.

8. Click the arrow and select **Hour of Day**.

9. Click the arrow and select **Is**.

10. Click the arrow and select **12**.



**Important:** You select the appropriate hour of the day based on your local date and time.

11. Click the green plus sign to add another rule.

Event(s) Selected: TDSBLD: ITM: The lsass process i...      Select all related events [0]      Edit Selection...

Time Condition(s)  AND  OR

Day of Week	Is	Wednesday [Low]		
Hour of Day	Is	12 [Low]		

12. Click the arrow and select **Minute of Hour**.

13. Click the arrow and select **Is**.

14. Click the arrow and select **35**.



**Important:** You select the appropriate minute based on your local date and time. Make sure to select a value that is several minutes in the future. You need time to complete the rule configuration.

Event(s) Selected: TDSBLD: ITM: The lsass process i...      Select all related events [0]      Edit Selection...

Time Condition(s)  AND  OR

Day of Week	Is	Wednesday [Low]		
Hour of Day	Is	12 [Low]		
Minute of Hour	Is	35		

15. Scroll down in the window and locate the section for **Actions When Event Does Not Occur**.

16. Select the option to create an event. Click **Create Event**.

Actions When Event(s) Does Not Occur in Specified Time Window(s)

Perform Action(s) After  Seconds

17. Enter **SE\_Auto** for AlertGroup and Manager. Click **OK**.

Create Event

Identifier Prefix	NON-OCCUR_
Identifier	NON-OCCUR_TDSBLD; ITM: The lsass process is not running
Summary Prefix	NON-OCCUR_
Summary	NON-OCCUR_TDSBLD; ITM: The lsass process is not running
* Severity	Major
* Alert Group	<b>SE_Auto</b>
* Manager	<b>SE_Auto</b>
<input type="checkbox"/> Set additional fields:	
Acknowledged	No

You use this window to configure how the artificial event is constructed. You can adjust the values for Summary, Severity, AlertGroup, and Manager. You can also set the values for more columns within the event record when you select **Set additional fields**.

18. Return to the Terminal window and repeat the date command.

```
File Edit View Search Terminal Help
[netcool@host1 relatedevents]$ date
Wed Jan 20 12:26:01 UTC 2016
[netcool@host1 relatedevents]$ date
Wed Jan 20 12:32:09 UTC 2016
[netcool@host1 relatedevents]$
```



**Important:** Make sure that the current time is not beyond the time that is configured in your rule.

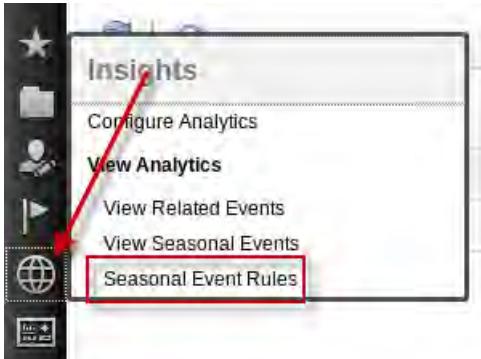
19. Click **Deploy** to activate the rule.



20. Verify that the event shows that a rule exists.

	Summary	Alert Group	Reviewed By	Seasonality	Maximum Severity	Rule Created
e.tivlab.raleigh.ibm	TDSBLD; ITM: The lsass process is not running	ITM_NT_Process_64		<input checked="" type="checkbox"/> High	<input checked="" type="checkbox"/> Critical	<b>SE_Workshop_Rule</b>
tivlab.austin.ibm.ibm	TDSBLD; ITM: The services process is not running	ITM_NT_Process_64		<input checked="" type="checkbox"/> High	<input checked="" type="checkbox"/> Critical	

21. Click the icon and select **Seasonal Event Rules**.



22. Verify that **one Active rule exists**.

Seasonal Event Rules			
	Watched [0]	Active [1]	Expired [0]
Configuration	Rule Count	Rule Name	
All	1	SE_Workshop_Rule	
SE_Workshop	1		

23. Return to the Terminal window, and repeat the date command until the current time exceeds the configured time in your rule.

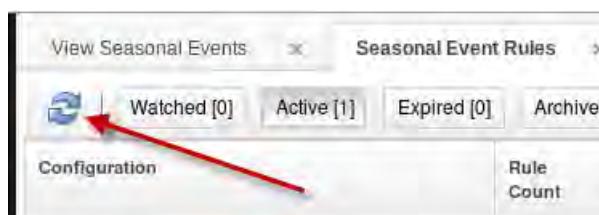
```

File Edit View Search Terminal Help
[netcool@host1 relatedevents]$ date
Wed Jan 20 12:26:01 UTC 2016
[netcool@host1 relatedevents]$ date
Wed Jan 20 12:32:09 UTC 2016
[netcool@host1 relatedevents]$ date
Wed Jan 20 12:36:15 UTC 2016
[netcool@host1 relatedevents]$ █

```

24. Return to the Firefox browser.

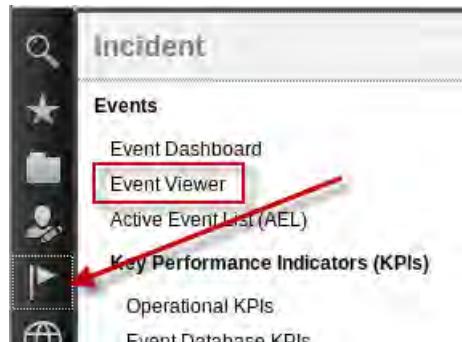
25. Click the blue arrows to refresh the view.



26. Scroll to the right and verify that the rule generated an event.

Rule Name	Last Run	Deployed	Suppressed Events	Unsuppress Events	Enriched/M Events	Generated Events on Non-occurr
SE_Workshop_Rule	Jan 20, 2016 12:36:46 PM	Jan 20, 2016 12:33:24 PM	0	0	0	1

27. Click the icon and select Event Viewer.



28. Click the icon to select only events with Severity of Major.

Sev	Ack	Node	Alert Group	Summary
!	No	link6	Link	Link Down on port
!	No	ducttape.tivlab.raleigh.ibm.com	SE_Auto	NON-OCCUR_1_ {"IDENTIFIER": "NT_BP_ProcMissing_Critical:Primary:DUCT"}

The artificial event that is created by the seasonality rule is displayed.

In this exercise, you created a rule to test for the absence of an event at a predetermined time. The process is the same to create a rule to suppress an event that occurs at a predetermined time.

If time allows, you can examine some of the other seasonal events.

29. Log out of Dashboard Application Services Hub.

## Verifying the Event Search feature

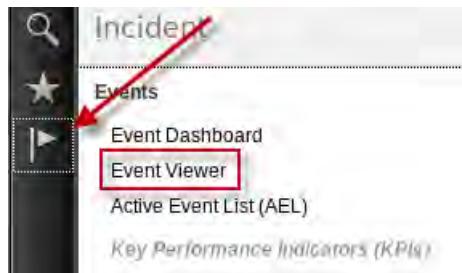
In a previous exercise, you configured the ncouser user for access to Log Analysis. In the following steps, you verify the event search feature with the ncouser user.

1. Log in to Dashboard Application Services Hub as the **ncouser** user with password **object00**.



**Important:** In a previous exercise, you configured the ncouser user with access to Log Analysis features.

2. Click the icon and select **Event Viewer**.

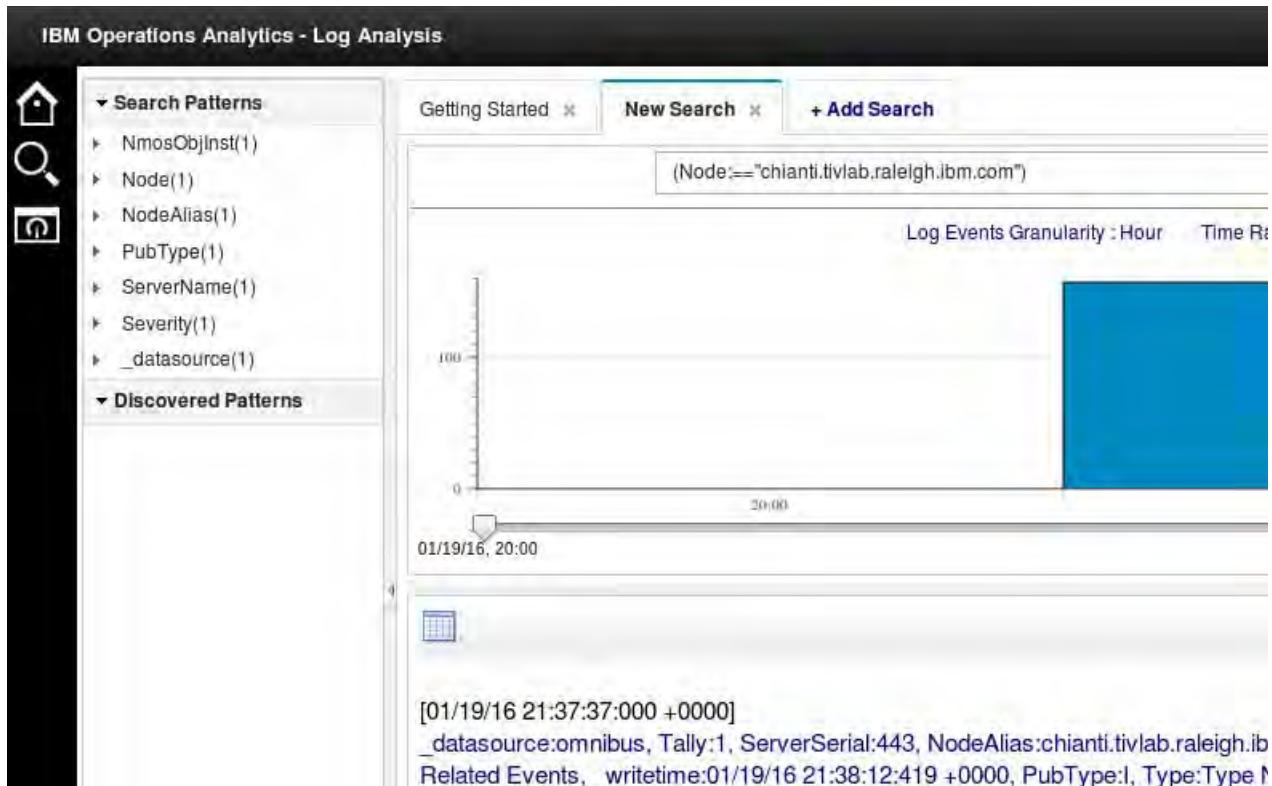


3. Right-click any event and select **Event Search > Search for events by node > 1 hour before event**.

This screenshot shows a context menu for an event in the list. The menu items include Acknowledge, De-acknowledge, Prioritize, Suppress/Escalate, Take ownership, User Assign, Group Assign, Delete, Ping, and Event Search. The Event Search option is highlighted with a red box. The submenu for Event Search shows options like Search for similar events, Search for events by node, Show keywords and event count, and Quick Filter. The 'Search for events by node' option is also highlighted with a red box. A third-level submenu for 'Search for events by node' shows time ranges: 15 minutes before event, 1 hour before event (which is highlighted with a red box), 1 day before event, and 1 week before event.

Node	Alert Group	Summary
chianti.tivlab.raleigh.ibm.com		Acknowledge Ctrl+A De-acknowledge Ctrl+D Prioritize Suppress/Escalate Take ownership User Assign Group Assign Delete Ping Event Search Information... Shift+I Journal... Shift+J Copy Ctrl+C Quick Filter
chianti.tivlab.raleigh.ibm.com		=UsedPct_Critical((Disk_Used_Percent>=95 AND FS_Type<>"nfs") ON chianti.tivlab.raleigh.ibm.com 15 minutes before event
chianti.tivlab.raleigh.ibm.com		=UsedPct_Critical((Disk_Used_Percent>=95 AND FS_Type<>"nfs") ON chianti.tivlab.raleigh.ibm.com 1 hour before event (highlighted)
chianti.tivlab.raleigh.ibm.com		=UsedPct_Critical((Disk_Used_Percent>=95 AND FS_Type<>"nfs") ON chianti.tivlab.raleigh.ibm.com 1 day before event
chianti.tivlab.raleigh.ibm.com		=UsedPct_Critical((Disk_Used_Percent>=95 AND FS_Type<>"nfs") ON chianti.tivlab.raleigh.ibm.com 1 week before event

The Log Analysis user interface opens in a new Firefox tab. You are logged in as the **ncouser** user. The authentication is performed through single sign-on.



The Node name and time span are passed to Log Analysis from the Event Viewer. The results of the search open.

The results verify the following aspects of the event search feature:

- Adding a user to the **UnityUsers** group provides access to Log Analysis
- The tool launch from Event Viewer to Log Analysis works correctly
- Log Analysis processes the event records and they are available for search
- Single sign-on between Dashboard Application Services Hub and Log Analysis works

4. As time allows, you can test the other options for event search launch from the Event Viewer.

The following list is a summary of the accomplishments from this unit:

- Installed Log Analysis
- Installed and configured the Message Bus Gateway
- Installed the Netcool/OMNIbus events insight pack
- Configured and verified the Related Events feature
- Configured and verified Event Seasonality
- Configured the ncouser for access to Log Analysis
- Verified the Event Search feature





## 4 IBM Tivoli Network Manager exercises

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

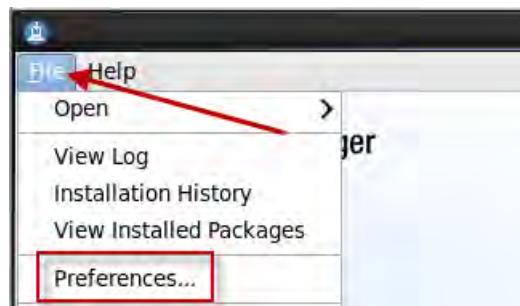
### Exercise 1 Installing the SNMP probe

Tivoli Network Manager requires the SNMP probe and the Netcool Knowledge Library. The following steps demonstrate how to install those components.

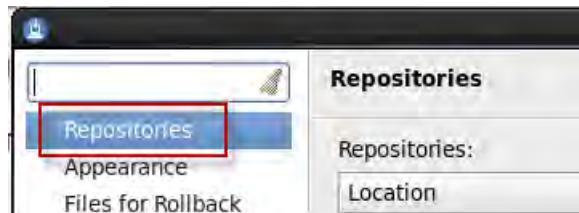
1. Open a terminal window if necessary.
2. Start IBM Installation Manager.

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

3. Click **File** and select **Preferences**.



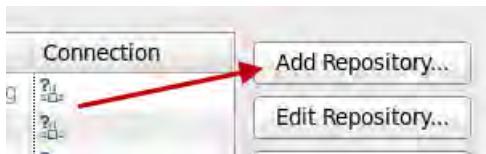
4. Select **Repositories**.



5. Remove all check marks from any existing repository entries.

Repositories:	
Location	Connection
<input type="checkbox"/> /software/omnibus/OMNIbusRepository/repository.config	?
<input type="checkbox"/> /software/jdbc/lm-nca-g-jdbc-rpt-scripts-1_0.zip	?
<input type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	?
<input type="checkbox"/> /tmp/jazz_install/repositories/disk1/diskTag.ini	?
<input type="checkbox"/> /software/webgui/OMNIbus/WebGUIRepository/repository.config	?

6. Click **Add Repository**.



7. Click **Browse** and locate the following file:

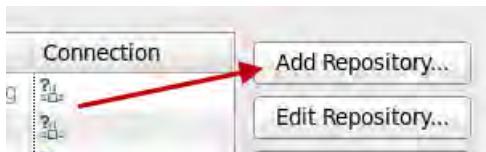
/software/nckl/NcKL\_4.5.0.zip

**Add a repository**  
Specify a repository and add to the repository preference list.

Repository:

8. Click **OK** to add the repository.

9. Click **Add Repository**.



10. Click **Browse** and locate the following file:

/software/snmp/NCOMNI\_PROBE\_FOR\_SNMP.zip

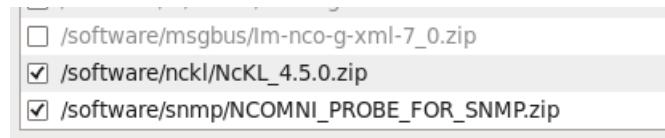
**Add a repository**  
Specify a repository and add to the repository preference list.

Repository:

**Browse...**

11. Click **OK** to add the repository.

12. Verify that the repositories are selected, and click **OK**.



13. Click **Install**.



14. Select both packages. Click **Next**.

Installation Packages		Status
<input checked="" type="checkbox"/>	Netcool/OMNibus Knowledge Library	
<input checked="" type="checkbox"/>	Version 4.5.2	Will be installed
<input checked="" type="checkbox"/>	Netcool/OMNibus Probe nco-p-mttrapd	
<input checked="" type="checkbox"/>	Version 1.20.0.0	Will be installed

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

16. Change the installation directory for the Netcool Knowledge Library.

- a. Click the entry for **IBM Netcool Knowledge Library** to select it.
- b. Change the installation directory to **/opt/IBM/tivoli/NcKL**.
- c. Click **Next**.

Package Group Name	Installation Directory
IBM Netcool Core Components	/opt/IBM/tivoli/netcool
Netcool/OMNibus Probe nco-p-mttrapd 1.20.0.0	
<b>IBM Netcool Knowledge Library</b>	
Netcool/OMNibus Knowledge Library 4.5.2	/opt/IBM/tivoli/NcKL

Package Group Name: IBM Netcool Knowledge Library  
Installation Directory: **/opt/IBM/tivoli/NcKL**

17. Verify that all features are selected, and click **Next**.

Features
<input checked="" type="checkbox"/> Netcool/OMNibus Probe nco-p-mttrapd 1.20.0.0
<input checked="" type="checkbox"/> Netcool/OMNibus Knowledge Library 4.5.2
<input checked="" type="checkbox"/> IBM Tivoli Netcool/OMNibus Knowledge Library

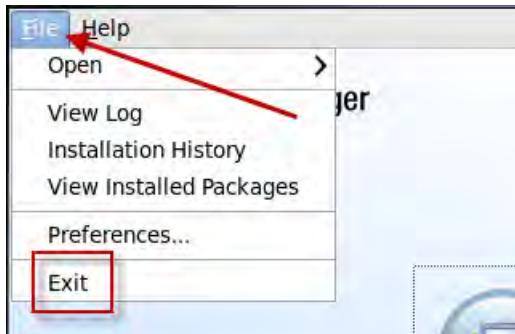
18. Review the summary, and click **Install**.

Packages	Installation Directory
IBM Netcool Core Components	/opt/IBM/tivoli/netcool
Netcool/OMNibus Probe nco-p-mttrapd 1.20.0.0	
IBM Netcool Knowledge Library	/opt/IBM/tivoli/NcKL
Netcool/OMNibus Knowledge Library 4.5.2	
IBM Tivoli Netcool/OMNibus Knowledge Library	

19. Verify that the installation is successful, and click **Finish**.



20. Click **File** and select **Exit** to close IBM Installation Manager.



21. Remove the installation files to save disk space.

```
cd /software/
/bin/rm -R nckl
/bin/rm -R snmp
```

22. Import the Netcool Knowledge Library ObjectServer modifications.

a. Change to the location of the sql file.

```
cd /opt/IBM/tivoli/NcKL
```

b. Import the modifications.

```
nco_sql -server NOI_AGG_P -user root -password object00 < advcorr.sql
```

ERROR=Object not found on line 114 of statement

```
'--#####
#####... ', at or near 'AdvCorr_SetCauseType'
```

```
ERROR=Object not found on line 1 of statement 'drop trigger
AdvCorr_LPC_RC;...', at or near 'AdvCorr_LPC_RC'
ERROR=Object not found on line 1 of statement 'drop trigger
AdvCorr_LPC_Sym;...', at or near 'AdvCorr_LPC_Sym'
ERROR=Object not found on line 4 of statement '-- Drop tables in case they
already exists from a previous installation...', at or near
'AdvCorrLpcSymCand'
ERROR=Object not found on line 1 of statement 'drop table
alerts.AdvCorrLpcRcCand;...', at or near 'AdvCorrLpcRcCand'
(0 rows affected)
(10 rows affected)
(0 rows affected)
```



**Note:** The error messages are normal and can be ignored.

23. Modify the SNMP probe property settings.

- Change to the location of the property file.

```
cd /opt/IBM/tivoli/netcool/omnibus/probes/linux2x86
```

- Open the property file for edit.

```
gedit mttrapd.props
```

- Add the following lines to the end of the file:

```
Server: 'NOI_AGG_P'
```

```
RulesFile: '/opt/IBM/tivoli/NcKL/rules/snmptrap.rules'
```

- Save the file and exit the gedit utility.

24. Define required Netcool Knowledge Library environment variable.



**Important:** The environment variable is required for the SNMP probe. The probe runs as the root user. You must define the environment variable for the root user. The root user needs the same variables as the **netcool** user, and one extra variable.

- Change to the root user.

```
su -
```

```
Password: object00
```

- Change to the root user home directory.

```
cd /root
```

- Append the **netcool** user environment settings to the end of the root user file.

```
cat /home/netcool/.bashrc >> .bashrc
```

- Open the environment file for edit.

```
gedit .bashrc
```

```
*.bashrc
fi
.bashrc

Source global definitions
if [-f /etc/bashrc]; then
 . /etc/bashrc
fi

User specific aliases and functions
#
Environment variables for Netcool / OMNIbus
#
NCHOME=/opt/IBM/tivoli/netcool
export NCHOME
OMNIHOME=$NCHOME/omnibus
export OMNIHOME
PATH=$NCHOME/bin:$OMNIHOME/bin:$OMNIHOME/probes:$PATH
export PATH
End Netcool/OMNIbus

The following line is required for Tivoli Common Reporting
source /home/db2inst1/sqllib/db2profile
```

- Verify that the **netcool** user settings are listed in the file.

- Add the following lines to the end of the file:

```
Required for Netcool KN owledge Library
NC_RULES_HOME=/opt/IBM/tivoli/NcKL/rules
export NC_RULES_HOME
```

- Save the file and exit the gedit utility.

- Source the modified environment file.

```
source .bashrc
```

- i. Verify the settings.

```
which nco_p_mttrapd
```

```
/opt/IBM/tivoli/netcool/omnibus/probes/nco_p_mttrapd
```



**Important:** The command must return the correct directory before you can proceed.

- j. Verify the syntax of the rules file.

```
cd $NC_RULES_HOME
```

```
nco_p_syntax -server NOI_AGG_P -rulesfile snmptrap.rules
```

```
.
```

```
.
```

```
2015-11-11T14:05:01: Debug: D-UNK-000-000: Auto-resizing lookup table
'syslogCorrScore' with 10271 entries from 127 to 513
```

```
2015-11-11T14:05:01: Information: I-UNK-000-000: Rules file syntax OK
```

```
2015-11-11T14:05:01: Information: I-UNK-000-000: Disconnecting ...
```

```
2015-11-11T14:05:01: Debug: D-UNK-000-000: Shutting down Probewatch
heartbeat thread.
```

```
.
```

```
.
```

```
.
```

- k. Start the probe as the root user.

```
nco_p_mttrapd &
```

- l. Verify that the probe is running.

```
ps -ef | grep nco_p_mttrapd
```

```
root 15011 13026 0 14:06 pts/0 00:00:00
```

```
/opt/IBM/tivoli/netcool/omnibus/platform/linux2x86/probes64/nco_p_mttrapd
```

After you verify that the probe starts correctly, you stop the probe.

- m. Stop the probe.

```
kill -9 15011
```

- n. Exit the root user back to the **netcool** user.

```
exit
```

## 25. Add the probe to process activity.

- a. Change to the location of the process activity configuration file.

```
cd /opt/IBM/tivoli/netcool/omnibus/etc
```

- b. Save a copy of the existing file.

```
cp nco_pa.conf nco_pa.conf.orig
```

- c. Open the configuration file for edit.

```
gedit nco_pa.conf
```

- d. Add the following lines to the *nco\_process* section of the file.

```
nco_process 'SnmpProbe'
{
 Command '$OMNIHOME/probes/nco_p_mttrapd' run as 0
 Host='host1.csite.edu'
 Managed=True
 RestartMsg='${NAME} running as ${EUID} has been restored on ${HOST}.'
 AlertMsg='${NAME} running as ${EUID} has died on ${HOST}.'
 RetryCount=0
 ProcessType=PaPA_AWARE
}
```



**Important:** Make sure that you configure the probe to run as the root user.

- e. Add the following highlighted line to the *nco\_service* section of the file.

```
nco_service 'Core'
{
 ServiceType=Master
 ServiceStart=Auto
 process 'MasterObjectServer' NONE
 process 'ArchiveGateway' 20
 process 'LogAnalysisGateway' 20
 process 'SnmpProbe' 20
}
```

- f. Save the file and exit the gedit utility.

## 26. Stop process activity.

```
nco_pa_shutdown -server HOST1_PA -password object00
```

Connected To PA Server [HOST1\_PA] Shutdown Options :-

- 1) Shutdown Server leaving managed processes running.
- 2) Shutdown Server and stop all managed processes.
- 3) Exit shutdown interface.

Select Option [1-3] 2

Shutdown PA and stop processes.

27. Enter **2** to shut down process activity.

28. Start process activity.



**Important:** The process activity daemon must run as the root user.

a. Change to the root user.

```
su -
Password: object00
```

b. Start process activity.

```
/etc/init.d/nco start
```

c. Exit the root user back to the **netcool** user.

```
exit
```

29. Verify the status of processes.

```
nco_pa_status -server HOST1_PA -password object00
```

```
[netcool@host1 log]$ nco_pa_status -server HOST1_PA -password object00

Service Name Process Name Hostname User Status PID

Core MasterObjectServer host1.csite.edunetcool RUNNING 18800
 ArchiveGateway host1.csite.edunetcool RUNNING 18970
 LogAnalysisGateway host1.csite.edunetcool RUNNING 18971
 SnmpProbe host1.csite.eduroot RUNNING 18972

```

# Exercise 2 Installing and configuring a topology database

In this exercise, you install the database creation scripts, and then run the scripts to create the topology database. You use the existing DB2 installation.

## Installing the database creation scripts



**Important:** Make sure that you are the **netcool** user before proceeding.

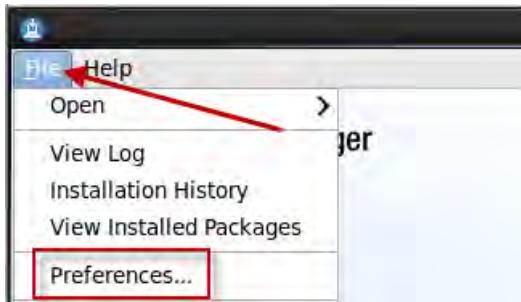
1. Expand the Network Manager installation file.

```
cd /software/itnm
unzip ITNP_IP_LIN.zip
```

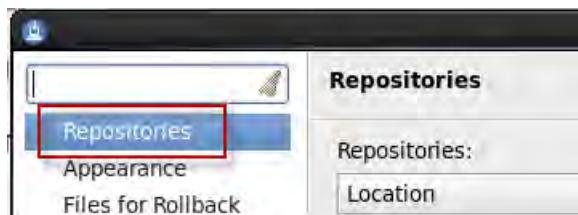
2. Start IBM Installation Manager.

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

3. Click **File** and select **Preferences**.



4. Select **Repositories**.



5. Remove all check marks from any existing repository entries.

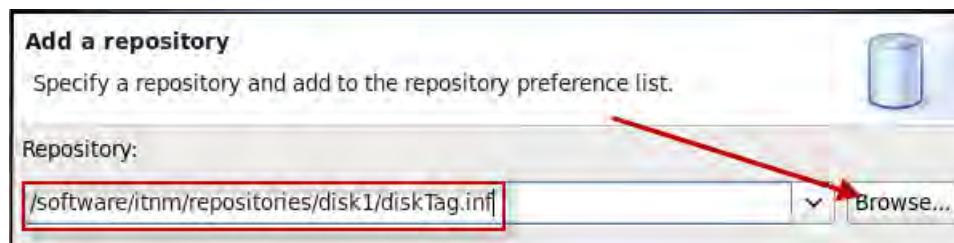
Repositories:	
Location	Connection
<input type="checkbox"/> /software/omnibus/OMNIbusRepository/repository.config	?
<input type="checkbox"/> /software/jdbc/lm-nca-q-jdbc-rpt-scripts-1_0.zip	?
<input type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	?
<input type="checkbox"/> /tmp/azz_install/repositories/disk1/diskTag.inf	?
<input type="checkbox"/> /software/webgui/OMNIbus/WebGUIRepository/repository.c	?

6. Click **Add Repository**.



7. Click **Browse** and locate the following file:

/software/itnm/repositories/disk1/diskTag.inf



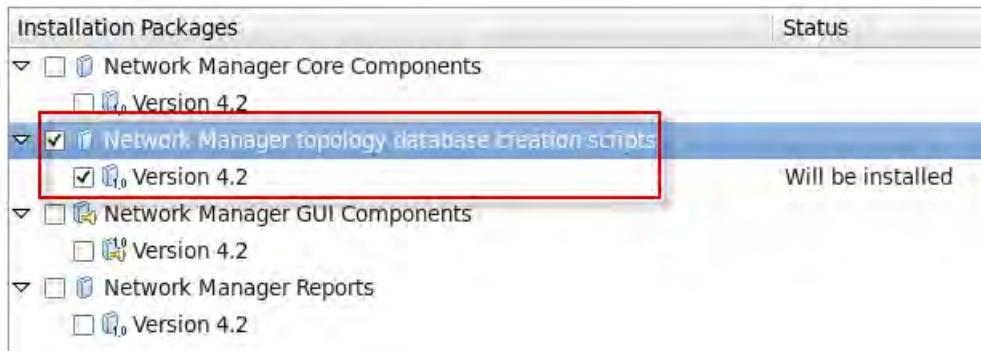
8. Click **OK** to add the repository.

9. Verify that the repository is selected, and click **OK**.



10. Click **Install**.



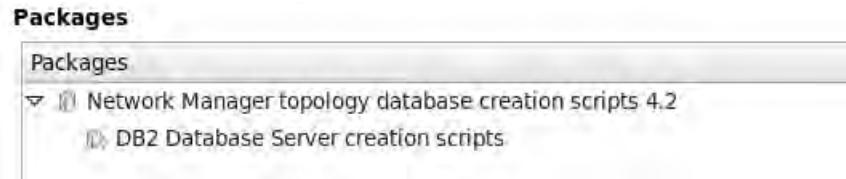
11. Select **Network Manager topology database creation scripts**. Click **Next**.

**Important:** Do not select any other packages.

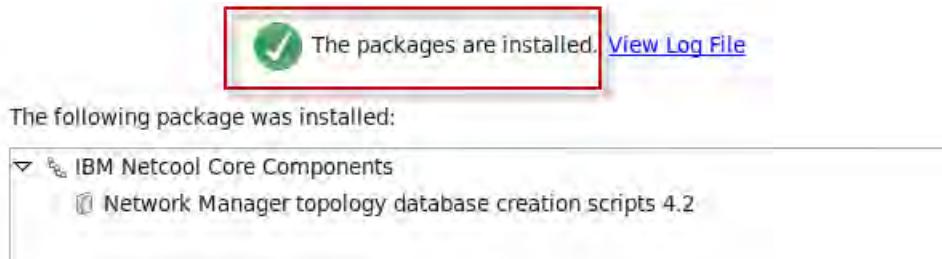
12. Accept the license agreement and click **Next**.13. Leave the default option to use the existing package group, and click **Next**.14. Clear **Oracle Database Server creation scripts**, and click **Next**.

**Note:** You use DB2 for the class exercises.

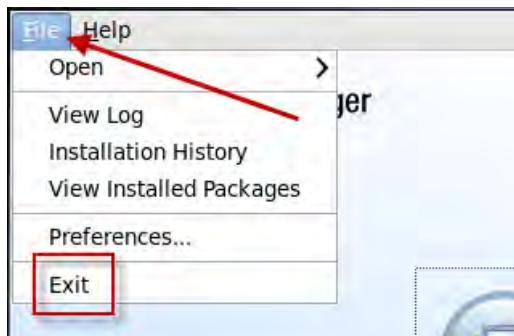
15. Review the summary, and click **Install**.



16. Verify that the package installation is successful, and click **Finish**.



17. Click **File** and select **Exit** to close IBM Installation Manager.



The database creation scripts are installed in this location:

/opt/IBM/tivoli/netcool/precision/scripts

## Creating the topology database

You create a user with DB2 access authority. You use that user to create the topology database.

1. Switch to the root user.

```
su -
Password: object00
```

2. Create the database user as follows.

```
useradd -g db2iadm1 -m ncim
```

The **ncim** user is created as a member of the db2iadm1 group.

3. Set the password for the **ncim** user.

```
passwd ncim
```

Changing password for user ncim.

New password: **object00**

BAD PASSWORD: it is based on a dictionary word

Retype new password: **object00**

passwd: all authentication tokens updated successfully.

The password is set to **object00**.

4. Exit from the root user back to the **netcool** user.

```
exit
```

5. Switch to the **ncim** user.

```
su - ncim
```

Password: **object00**

6. Add the DB2 environment settings to the **ncim** user.

- a. Open the environment file for edit.

```
cd /home/ncim
```

```
gedit .bashrc
```

- b. Add the following line to the end of the file.

```
source /home/db2inst1/sqllib/db2profile
```

- c. Save the file and exit the gedit utility.

7. Source the updated file.

```
source .bashrc
```

8. Verify settings.

```
which db2
```

/home/db2inst1/sqllib/bin/db2



**Important:** The command must return the correct location before you can proceed.

9. Exit the **ncim** user back to the **netcool** user.

```
exit
```

10. Change to the DB2 instance owner.

```
su - db2inst1
```

Password: **object00**

11. Change to location of the database creation scripts.

```
cd /opt/IBM/tivoli/netcool/precision/scripts/sql/db2
```

12. Verify that you are the **db2inst1** user.

```
whoami
```

```
db2inst1
```

13. Run the database creation script.



**Note:** The value NCIM is the database name, and **ncim** is the database owner.

```
./create_db2_database.sh NCIM ncim
.
.
.
db2 => DB20000I The QUIT command completed successfully.
```

```
Database Connection Information
```

```
Database server = DB2/LINUXX8664 10.5.3
SQL authorization ID = DB2INST1
Local database alias = NCIM
```

```
DB20000I The SQL DISCONNECT command completed successfully.
```



**Important:** The script runs for several minutes, and seems to stop periodically. You must wait until the script completes before you proceed.

14. Exit the **db2inst1** user back to the **netcool** user.

```
exit
```

15. Switch to the **ncim** user.

```
su - ncim
Password: object00
```

16. Verify access to the IBM Tivoli Network Manager database.

```
db2 connect to NCIM
```

```
Database Connection Information
```

```
Database server = DB2/LINUXX8664 10.5.3
SQL authorization ID = NCIM
Local database alias = NCIM
```

17. Exit the **ncim** user back to the **netcool** user.

```
exit
```

Several database parameters cannot be changed dynamically. You must restart the database before you proceed. Several components use DB2. The easiest option is to restart the image.

18. Change to the root user and restart the image.

```
su -
Password: object00
init 6
```

19. Wait for the image to restart.

20. Log in as the **netcool** user with password **object00**.

## Exercise 3 Installing Tivoli Network Manager

### Updating smadmin roles

You use the **smadmin** user to modify the Web GUI configuration during the Network Manager installation process. The **smadmin** user must be able to run the WAAPI utility. The user requires the **ncw\_admin** role to use this utility.

1. Open a Firefox browser.
2. Log in to Dashboard Application Services Hub as the **smadmin** user with password **object00**.
3. Click the icon and select **User Roles**.



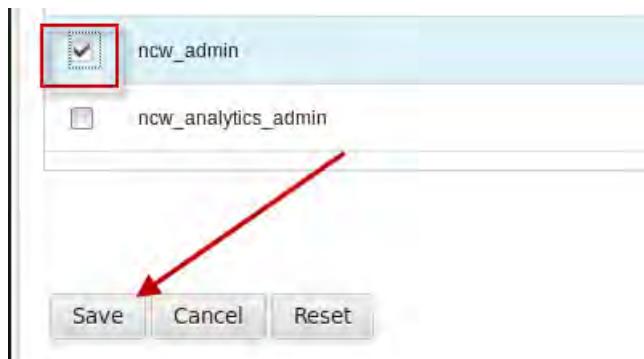
4. Enter **smadmin** and click **Search**.

A screenshot of a search interface. It has fields for 'Firstname', 'Lastname', 'User ID' (containing 'smadmin'), and 'E-mail'. Below these is a dropdown for 'Number of results to display' set to 20. A large red arrow points from the 'User ID' field to the 'Search' button.

5. Click **smadmin**.

Select	User ID	Active	First Name	Last Name
	smadmin	1	smadmin	smadmin

6. Select **ncw\_admin**, and click **Save**.



7. Log out of Dashboard Application Services Hub.

8. Close the Firefox browser.

## Installing Network Manager core components

In the previous exercise, you expanded the Tivoli Network Manager installation, and defined the appropriate software repository to IBM Installation Manager.

1. Start IBM Installation Manager.

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

2. Click **Install**.



### 3. Select Network Manager Core Components.

Installation Packages	Status
<input checked="" type="checkbox"/> Network Manager Core Components	
<input checked="" type="checkbox"/> Version 4.2	Will be installed
<input type="checkbox"/> Network Manager topology database creation scripts	Installed
<input type="checkbox"/> Version 4.2	Installed
<input type="checkbox"/> Network Manager GUI Components	
<input type="checkbox"/> Version 4.2	
<input type="checkbox"/> Network Manager Reports	
<input type="checkbox"/> Version 4.2	



**Important:** Make sure that no other packages are selected. The packages must be installed in separate steps.

### 4. Accept the license agreement and click **Next**.

### 5. Leave the default option to use the existing package group, and click **Next**.

Install    Licenses    Location    Features    Summary

Use the existing package group  
 Create a new package group

Package Group Name	Installation Directory
IBM Netcool Core Components	/opt/IBM/tivoli/netcool
CORE SERVICES in JAZZ for Service Management	/opt/IBM/jazzSM
IBM Netcool GUI Components	/opt/IBM/netcool

Package Group Name: IBM Netcool Core Components  
 Installation Directory: /opt/IBM/tivoli/netcool

### 6. Verify that all features are selected, and click **Next**.

Install Packages  
 Select the features to install.

Install    Licenses    Location    **Features**    Summary

Features

<input checked="" type="checkbox"/> Network Manager Core Components 4.2
<input checked="" type="checkbox"/> Core components
<input checked="" type="checkbox"/> Additional cryptographic routines

### 7. Enter the following values, and click **Next**.

- Enter NOI\_AGG\_P for the ObjectServer name.
- Enter host1.csite.edu for the host name.

- c. Enter port number **4100**.
- d. Enter user name **root**.
- e. Enter **object00** for the password.

#### Configuration for Network Manager Core Components 4.2

##### 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.csuite.edu
Port:	4100
Super user ID:	root
Password:	*****

Skip ObjectServer connection details verification and configuration.

8. Enter **object00** for the default users password, and click **Next**.

#### Configuration for Network Manager Core Components 4.2

##### 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:	*****

9. Enter **NOI\_AGG\_P** for the domain name, and click **Next**.

#### Configuration for Network Manager Core Components 4.2

##### 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

10. Enter the following values, and click **Next**.

- a. Enter **host1.csuite.edu** for the host name.
- b. Enter **ncim** for the user name.

- c. Enter **object00** for the password.

**Configuration for Network Manager Core Components 4.2**

**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 utility validates the access to DB2.

11. Accept the default location for Python, and click **Next**.

**Configuration for Network Manager Core Components 4.2**

**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:

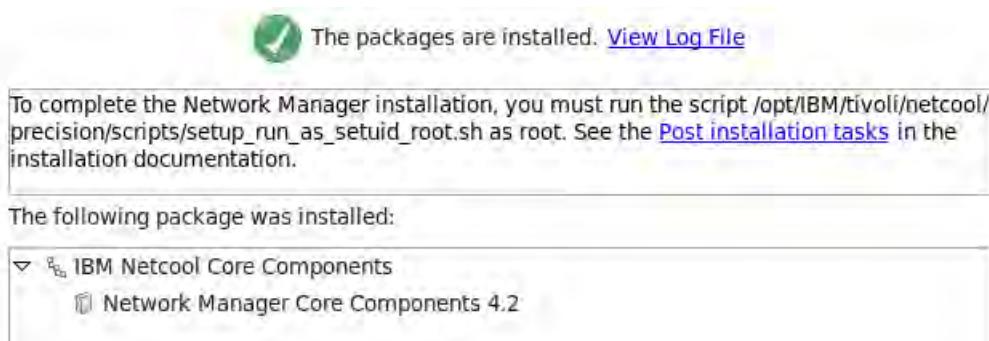
/usr/bin/python

12. Review the summary, and click **Install**.



**Important:** The installation runs approximately 15 minutes.

13. Verify that the installation is successful, and click **Finish**.



14. Leave IBM Installation Manager open.

## Installing Network Manager GUI components

1. Click **Install**.



2. Select **Network Manager GUI Components**.

Installation Packages	Status
Network Manager Core Components	Installed
Version 4.2	Installed
Network Manager topology database creation scripts	Installed
Version 4.2	Installed
Network Manager GUI Components	Will be installed
Version 4.2	
Network Manager Reports	
Version 4.2	



**Important:** Make sure that no other packages are selected. The packages must be installed in separate steps.

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

4. Leave the default option to use the existing package group, and click **Next**.

Use the existing package group

Create a new package group

Package Group Name	Installation Directory
IBM Netcool GUI Components	/opt/IBM/netcool/gui
Core services in jazz for Service Management	/opt/IBM/jazzSM
IBM Netcool Core Components	/opt/IBM/tivoli/netcool

Package Group Name: IBM Netcool GUI Components

Installation Directory: /opt/IBM/netcool/gui

5. Verify that all features are selected, and click **Next**.



6. Enter **object00** for the password, and click **Next**.

**Configuration for Network Manager GUI Components 4.2**

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	*****



**Important:** The **smadmin** user must have the *ncw\_admin* role. The role is required because the **smadmin** user must be able to run the WAAPI utility.

The installer validates access to Jazz for Service Management.

7. Enter the following values, and click **Next**.

- Enter **OMNIBUS** for the ObjectServer name.
- Enter **host1.csite.edu** for the host name.

- c. Enter port number **4100**.
- d. Enter user name **root**.
- e. Enter **object00** for the password.

#### Configuration for Network Manager GUI Components 4.2

##### ObjectServer Configuration

Network Manager uses event data from a Netcool/OMNibus WebGUI data source. A data source is a named ObjectServer used by the Web GUI for event information. This Netcool/OMNibus Objectserver must be running during installation. Enter the connection details of the Netcool/OMNibus ObjectServer for Network Manager to use.

Name:	OMNIBUS
Host:	host1.csuite.edu
Port:	4100
Super user ID:	root
Password:	*****

Create/overwrite WebGUI data source      do not select

Create a new data source in Netcool/OMNibus WebGUI and configure Network Manager to use it. If a data source exists, this option will overwrite it. If you want Network Manager to use a specific existing data source, clear this option and configure the WebGUI data source manually after installation. Use the instructions in the post-installation tasks section in the Network Manager documentation.



**Important:** Do not select the option to create a data source. Change the name to OMNIBUS because Web GUI is configured with that data source name.

8. Enter **object00** for the default users password, and click **Next**.

#### Configuration for Network Manager GUI Components 4.2

##### Network Manager Users

Network Manager needs dedicated users to be created in the Netcool/OMNibus ObjectServer (itnmadmin, 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:	*****

9. Enter the following values, and click **Next**.

- a. Enter **host1.csuite.edu** for the host name.
- b. Enter **ncim** for the user name.

- c. Enter **object00** for the password.

#### Configuration for Network Manager GUI Components 4.2

##### 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: **\*\*\*\*\***

Skip database connection details verification.

The installation utility validates the access to DB2.

10. Review the summary, and click **Install**.



**Important:** The installation runs approximately 50 minutes.

11. Verify that the installation is successful, and click **Finish**.



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

Skipping Registration of the OMNIBUS ObjectServer datasource with JazzSM.

The following package was installed:

▽ IBM Netcool GUI Components  
   Network Manager GUI Components 4.2

12. Leave IBM Installation Manager open.

# Installing Network Manager Reports

1. Click **Install**.



2. Select **Network Manager Reports**.

Installation Packages	Status
Network Manager Core Components	Installed
Version 4.2	Installed
Network Manager topology database creation scripts	Installed
Version 4.2	Installed
Network Manager GUI Components	Installed
Version 4.2	Installed
Network Manager Reports	Will be installed
Version 4.2	



**Important:** Make sure that no other packages are selected. The packages must be installed in separate steps.

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

4. Leave the default option to use the existing package group, and click **Next**.

- Use the existing package group  
 Create a new package group

Package Group Name	Installation Directory
IBM Netcool GUI Components	/opt/IBM/netcool/gui
Core services in jazz for Service Management	/opt/IBM/jazzSM
IBM Netcool Core Components	/opt/IBM/tivoli/netcool

Package Group Name: IBM Netcool GUI Components

Installation Directory: /opt/IBM/netcool/gui

5. Verify that all features are selected, and click **Next**.

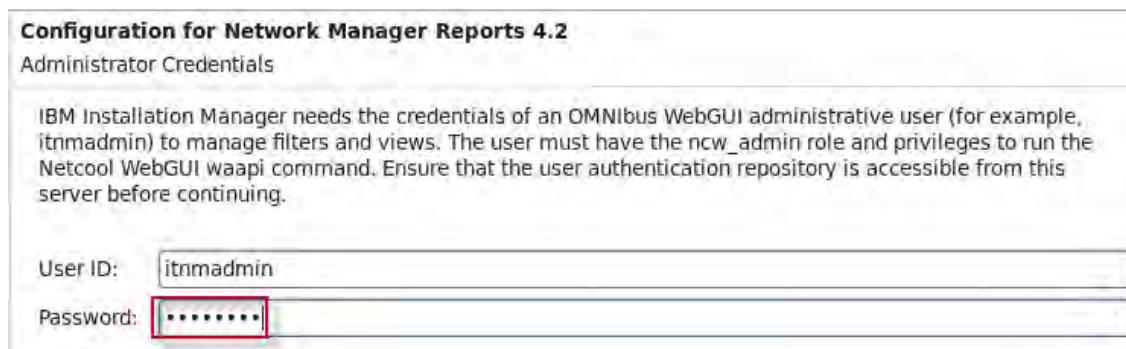
Install	Licenses	Location	Features	Summary
Features				
<input checked="" type="checkbox"/>	Network Manager Reports 4.2			
	<input checked="" type="checkbox"/>	Network Manager Reports		

6. Enter **object00** for the password, and click **Next**.



The installer validates access to Jazz for Service Management.

7. Enter **object00** for the password, and click **Next**.



8. Enter the following values, and click **Next**.

- Enter **host1.csite.edu** for the host name.
- Enter **ncim** for the user name.

- c. Enter **object00** for the password.

**Configuration for Network Manager Reports 4.2**

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.

The installation utility validates the access to DB2.

9. Review the summary, and click **Install**.



**Important:** The installation runs approximately 30 minutes.

10. Verify that the installation is successful, and click **Finish**.



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

The following package was installed:

IBM Netcool GUI Components  
Network Manager Reports 4.2

11. Click **File** and select **Exit** to close IBM Installation Manager.

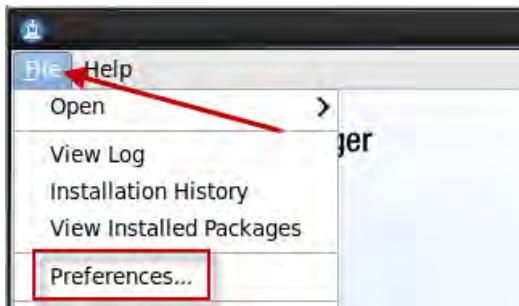
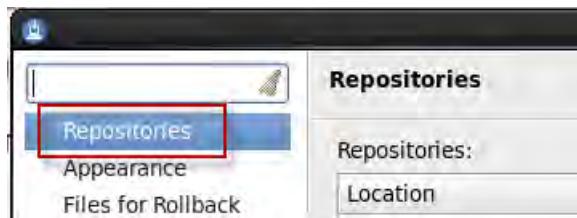
## Installing Network Health Dashboard

1. Expand the Network Manager installation file.

```
cd /software/itnm
mkdir dashboard
cd dashboard
unzip ../NTWRK_HLTH_DSHBRD_V4.2_LNX.zip
```

## 2. Start IBM Installation Manager.

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

3. Click **File** and select **Preferences**.4. Select **Repositories**.

## 5. Remove all check marks from any existing repository entries.

Repositories:	
Location	Connection
<input type="checkbox"/> /software/omnibus/OMNIbusRepository/repository.config	?
<input type="checkbox"/> /software/jdbc/lm-nco-g-jdbc-rpt-scripts-1_0.zip	?
<input type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	?
<input type="checkbox"/> /tmp/jazz_install/repositories/disk1/diskTag.inf	?
<input type="checkbox"/> /software/webgui/OMNIbus/WebGUIRepository/repository.c	?

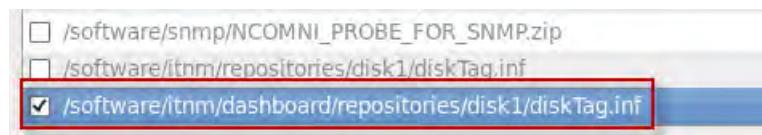
6. Click **Add Repository**.7. Click **Browse** and locate the following file:

```
/software/itnm/dashboard/repositories/disk1/diskTag.inf
```

**Add a repository**  
Specify a repository and add to the repository preference list.

**Repository:**

8. Click **OK** to add the repository.
9. Verify that the repository is selected, and click **OK**.



10. Click **Install**.



11. Select **Network Health Dashboard**.



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

13. Leave the default option to use the existing package group, and click **Next**.

- Use the existing package group  
 Create a new package group

Package Group Name	Installation Directory
IBM Netcool GUI Components	/opt/IBM/netcool/gui
Core services in Jazz for Service Management	/opt/IBM/JazzSM
IBM Netcool Core Components	/opt/IBM/tivoli/netcool

Package Group Name: IBM Netcool GUI Components  
Installation Directory: /opt/IBM/netcool/gui

14. Verify that all features are selected, and click **Next**.



15. Enter **object00** for the password, and click **Next**.

**Configuration for Network Health Dashboard 4.2**

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: **\*\*\*\*\***

16. Enter **object00** for the password, and click **Next**.

**Configuration for Network Health Dashboard 4.2**

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: **\*\*\*\*\***

17. Review the summary, and click **Install**.



**Important:** The installation runs approximately 15 minutes.

18. Verify that the installation is successful, and click **Finish**.

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

The following package was installed:

- IBM Netcool GUI Components
  - Network Health Dashboard 4.2

19. Click **File** and select **Exit** to close IBM Installation Manager.

## Configuring the Network Health Dashboard

Install the tools and menus to start 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 for edit:

```
gedit topoviz.properties
```

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

```
topoviz.unity.customappsui=https://host1.csuite.edu:9987/Unity/CustomAppsUI
```

4. Save the file and exit the gedit utility.

## Exercise 4 Performing postinstallation configuration

You must perform several postinstallation steps to complete the configuration.

### Configuring the Tivoli Netcool/OMNibus 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.

1. Change to the location of the property file.

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

2. Save a copy of the existing file.

```
cp ModelNcimDb.NOI_AGG_P.cfg ModelNcimDb.NOI_AGG_P.cfg.orig
```

3. Open the file for edit with the gedit utility.

```
gedit ModelNcimDb.NOI_AGG_P.cfg
```

- Locate the existing data source name as shown here.

```

insert into dbModel.access
(
 EnumGroupFilter,
 TransactionLength,
 WebTopDataSource
)
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')",
 500,
 "NOI_AGG_P"
);

```

Web GUI data source name

"NOI\_AGG\_P"

- Change the value to **OMNIBUS**.

```

insert into dbModel.access
(
 EnumGroupFilter,
 TransactionLength,
 WebTopDataSource
)
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')",
 500,
 "OMNIBUS"
);

```

"OMNIBUS"

- Save the file and exit the gedit utility.

## Configuring the core components to run as a non-root user

- Switch to the root user.

```

su -
Password: object00

```

- Change to the location of the required script.

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

3. Run the script.

```
./setup_run_as_setuid_root.sh
.
.
.
```

In order for this script to work correctly, you must be logged on as root when you run it.

**Press return to continue**, or <CTRL> + C to abort

```
.
. .
.
```

Changing ownership of nco\_p\_mttrapd to root  
Enabling setuid on execution permission on nco\_p\_mttrapd

Changing ownership of nco\_p\_mttrapd to root  
Enabling setuid on execution permission on nco\_p\_mttrapd

## Configuring processes to start automatically



**Important:** You are still 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
```

Installing automated startup and shutdown scripts for ncp only.

ITNMHOME is not set in the environment.

Guessing ITNMHOME=/opt/IBM/tivoli/netcool/precision.

Rerun -auto\_only if not satisfactory.

PRECISION\_DOMAIN is not set in the environment.

Guessing PRECISION\_DOMAIN=NOI\_AGG\_P.

Rerun -auto\_only if not satisfactory.

Creating control script /etc/init.d/ncp

Creating startup/shutdown links

Creating control script

```
/opt/IBM/tivoli/netcool/precision/custom/control/init.d/ncp
```

3. Create the storm startup script.

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

Installing automated startup and shutdown scripts for storm only.

ITNMHOME is not set in the environment.

Guessing ITNMHOME=/opt/IBM/tivoli/netcool/precision.

Rerun -auto\_only if not satisfactory.

PRECISION\_DOMAIN is not set in the environment.

Guessing PRECISION\_DOMAIN=NOI\_AGG\_P.

Rerun -auto\_only if not satisfactory.

Creating control script /etc/init.d/storm

Creating startup/shutdown links

**service storm does not support chkconfig**

Creating control script

```
/opt/IBM/tivoli/netcool/precision/custom/control/init.d/storm
```



**Important:** The script that creates the storm startup script has an issue. You must manually correct the issue.

4. Correct the issue with the storm startup script.

a. Change to the startup directory.

```
cd /etc/init.d
```

b. Open the storm file for edit.

```
gedit storm
```

c. Locate the chkconfig line as shown here:

```
#!/bin/sh
#####
#
chkconfig: 35 99
description: Automatic startup/shutdown script for
Netcool/Precision for IP Networks Storm supervisor
#
```

- d. Change the line as shown here:

```
#!/bin/sh
#####
#
chkconfig: 35 85 65
description: Automatic startup/shutdown script for
Netcool/Precision for IP Networks Storm supervisor
```

- e. Save the file and exit the gedit utility.
- f. Create the symbolic links for startup.  
chkconfig storm on
5. Exit the root user and return to the **netcool** user.

```
exit
```

## Adding Network Manager environment variables to the netcool 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
4. Save the file and exit the gedit utility.

5. Source the modified file.

```
source .bashrc
```

6. Verify the settings.  
which itnm\_status

```
/opt/IBM/tivoli/netcool/precision/bin
```



**Important:** The command must return the correct path before you can proceed.

## Removing the ObjectServer users

The Tivoli Network Manager installation process creates sample users in the ObjectServer. In addition, the process adds the same users and two groups to WebSphere. Because WebSphere is

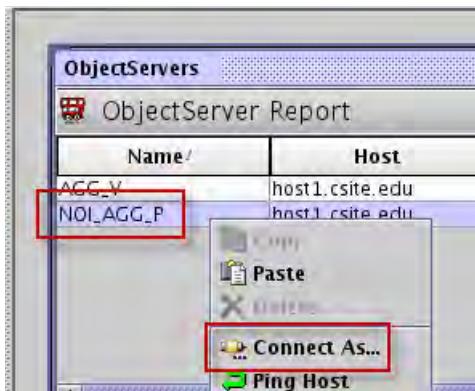
configured to write new users and groups to LDAP, the process creates the sample users and groups in LDAP. In the following steps, you manually remove the users from the ObjectServer. The Web GUI synchronization process adds the users and sample groups to the ObjectServer.

1. Open the Netcool/OMNIbus Administrator utility.

```
nco_config &
```

**Note:** If the utility wants to import the omni.dat file, click **Yes**. When the import wizard opens, click **Finish**.

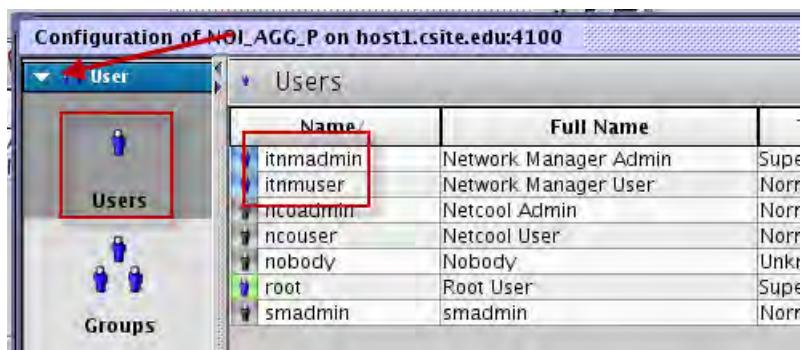
2. Right-click **NOI\_AGG\_P**, and select **Connect As...**



3. Enter **root** for the user and **object00** for the password. Click **OK**.



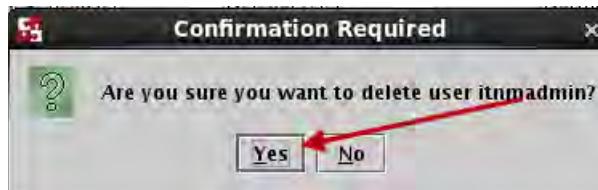
4. Expand **User**, and select **Users**.



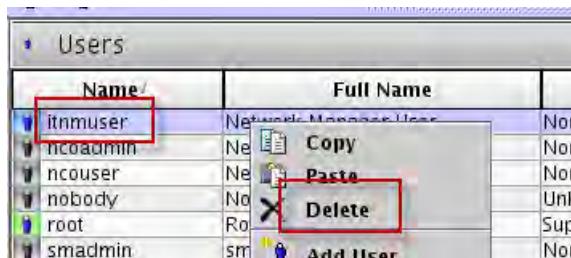
5. Right-click **itnmadmin** and select **Delete**.



6. Click **Yes** to confirm.



7. Right-click **itnmuser** and select **Delete**.



8. Click **Yes** to confirm.



9. Click **File**, and select **Exit** to close the administrator utility.

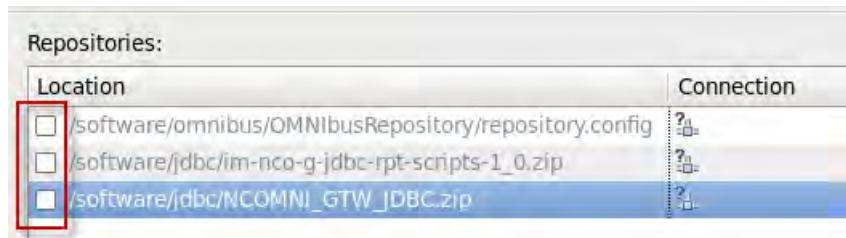
## Installing the hot fix

The hot fix resolves some performance and functional issues in Bookmarks and Libraries for IBM Tivoli Network Manager IP Edition version 4.2.

1. Start IBM Installation Manager.

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

2. Install the hot fix.
  - a. Click **File** and select **Preferences**. Select **Repositories**.
  - b. Remove the check marks from the existing entries.

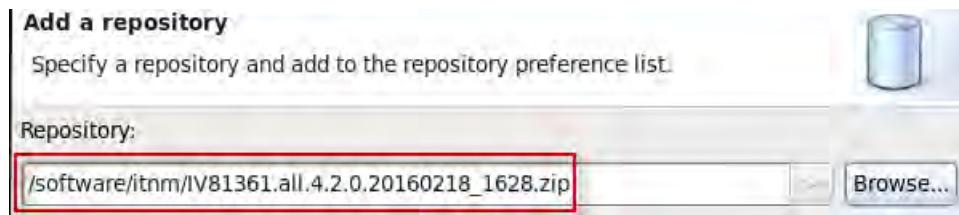


- c. Click **Add Repository**.



- d. Click **Browse** and locate the following file:

/software/itnm/IV81361.all.4.2.0.20160218\_1628.zip



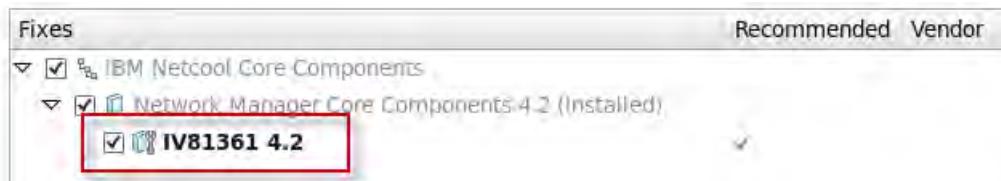
- e. Click **OK** to add the repository.
- f. Verify that the repository is listed and click **OK**.
- g. Click **Update**.



- h. Select the IBM Netcool Core Components package and click **Next**.

Package Group Name	Directory
IBM Netcool Core Components	/opt/IBM/tivoli/netcool
IBM Netcool Knowledge Library	/opt/IBM/tivoli/NcKL
IBM Operations Analytics - Log Analysis	/opt/IBM/LogAnalysis

- i. Verify that the hot fix is selected, and click **Next**.



- j. Review the summary, and click **Update**.



- k. Verify that the installation is successful, and click **Finish**.



- l. Click **File**, and select **Exit** to close installation manager.

## Verifying the installation

In the following steps, you start the Network Manager processes and verify that the users have the necessary access authority.

1. Start the Network Manager processes.

```
itnm_start
```

After the command completes, wait a short time, and check the status of the processes. It takes several minutes for all processes to start.

## 2. Check the status.

```
itnm_status
```

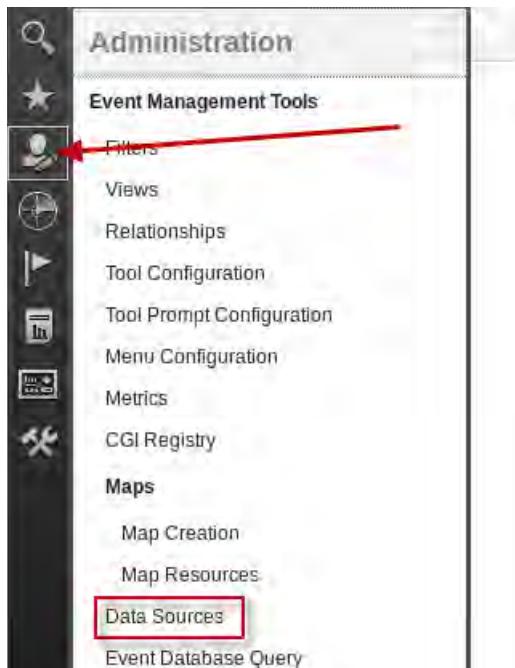
[netcool@host1 ~]\$ itnm_status		
Network Manager:		
Domain: NOI_AGG_P		
ncp_ctrl	RUNNING	PID=9138 NOI_AGG_P
ncp_store	RUNNING	PID=9248 NOI_AGG_P
ncp_class	RUNNING	PID=9249 NOI_AGG_P
ncp_model	RUNNING	PID=9452 NOI_AGG_P
ncp_disco	RUNNING	PID=9592 NOI_AGG_P
ncp_d_helpserv	RUNNING	PID=9250 NOI_AGG_P
ncp_config	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	

3. Repeat the status command until all processes are running.
4. Open a Firefox browser.
5. Log in to Dashboard Application Services Hub as user **itnmadmin** with password **object00**.
6. Create a data source for the ObjectServer.

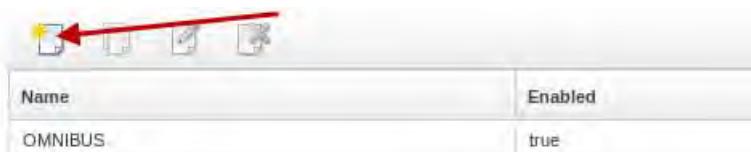


**Note:** Apparently Network Manager expects a particular ObjectServer data source. You must create that data source entry.

- a. Click the icon and select **Data Sources**.



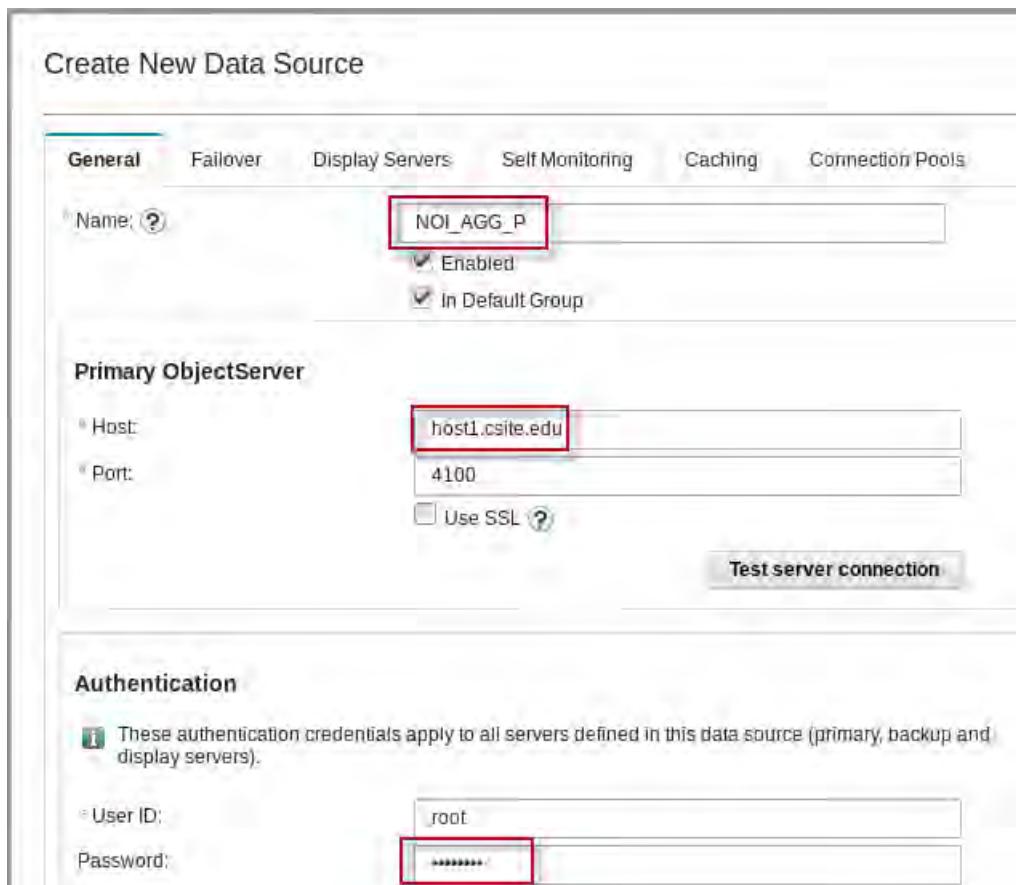
- b. Click the icon to create a new data source.



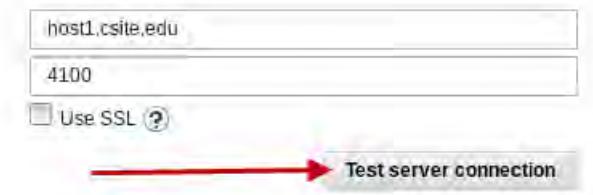
**Note:** The OMNIBUS entry was created when you installed Web GUI in a previous unit.

- c. Enter **NOI\_AGG\_P** for the name.  
d. Enter **host1.csite.edu** for the host.

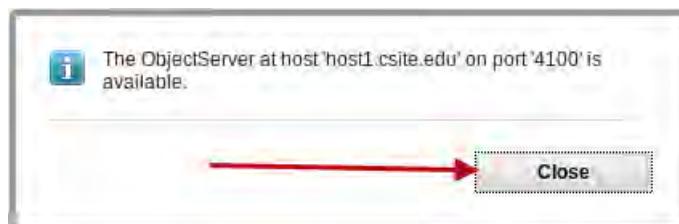
- e. Enter **object00** for the password.



- f. Click **Test server connection**.



- g. Verify that the ObjectServer is available, and click **Close**.



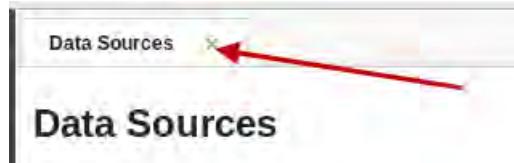
- h. Scroll to the bottom of the page and click **Save Datasource**.



- i. Verify that the new data source is in the list.

Name	Enabled
OMNIBUS	true
NOI_AGG_P	true

- j. Click the X to close the tab.

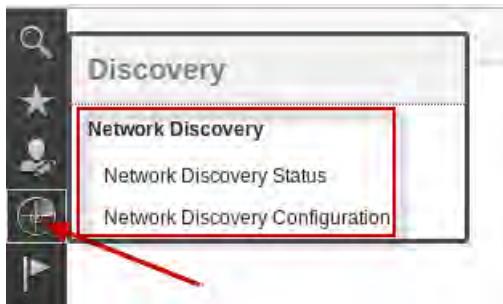


7. Click the icon and verify the items.

The screenshot shows the 'Administration' menu on the left. The 'Network' section is expanded and highlighted with a red box. Inside the 'Network' box, the following items are listed: Database Access Configuration, Network Polling, Path View Administration, and Management Database Access. The 'User' icon in the sidebar is also highlighted with a red box.

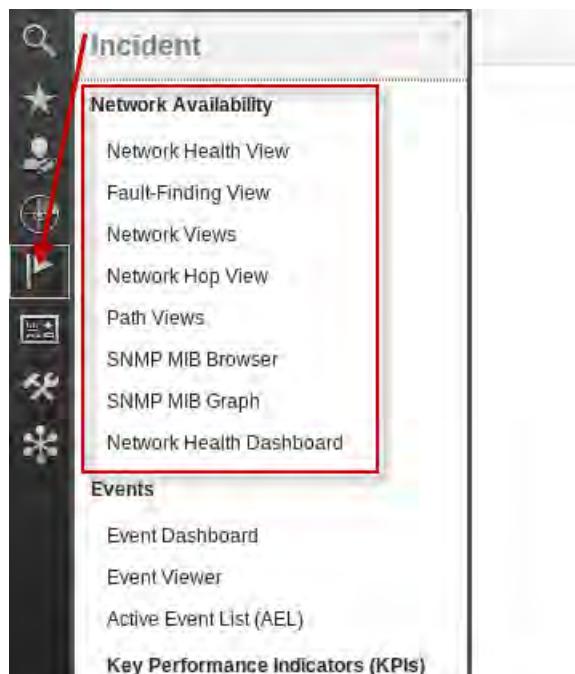
Verify that the user has access to the Network administration features.

8. Click the icon and verify the items.



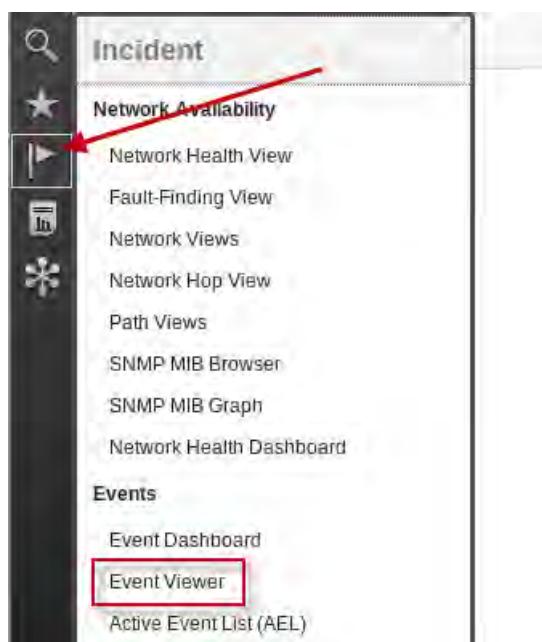
Verify that the user has access to the Network Discovery features.

9. Click the icon and verify the items.

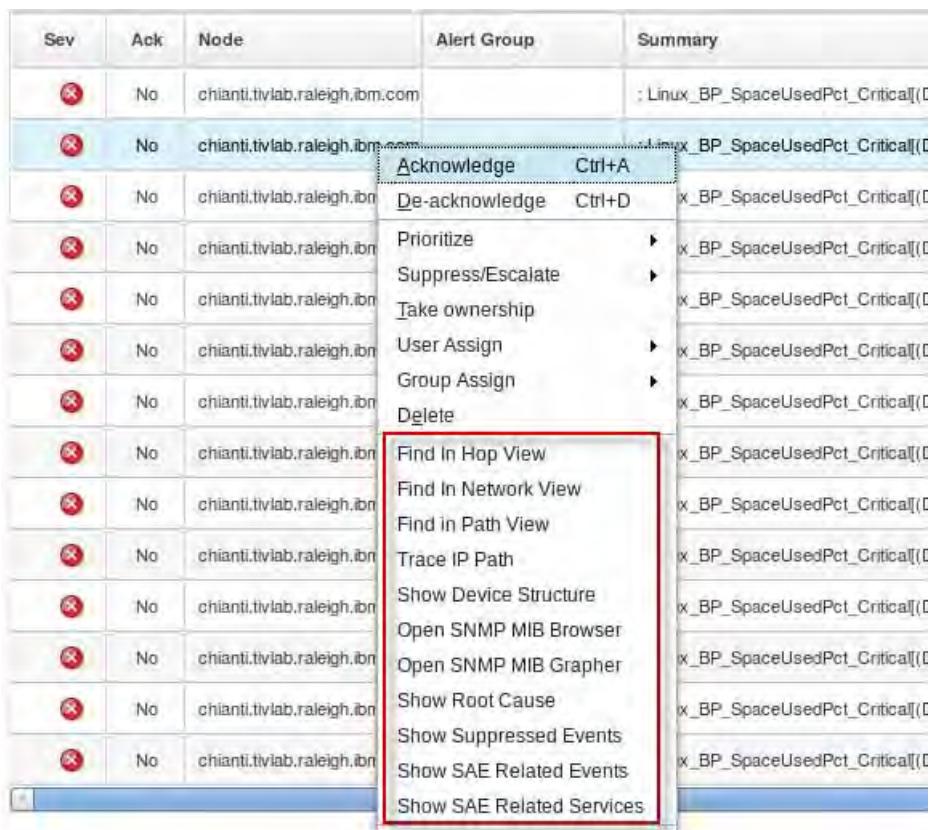


Verify that the user has access to the Network Availability features.

10. Click the icon and select **Event Viewer**.



11. Right-click any event and examine the available tools.

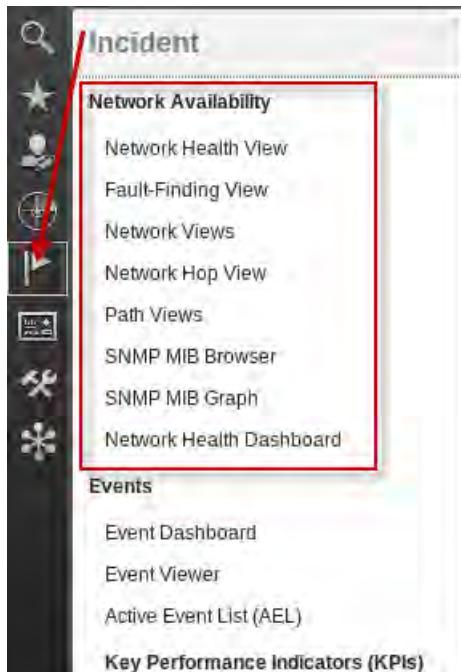


The itnmadmin user is defined with the *netcool\_rw* role. This role allows access to all tools, including the Network Manager tools.

## 12. Log out as the **itnmadmin** user.

13. Log in to Dashboard Application Services Hub as user **itnmuser** with password **object00**.

14. Click the icon and verify the items.



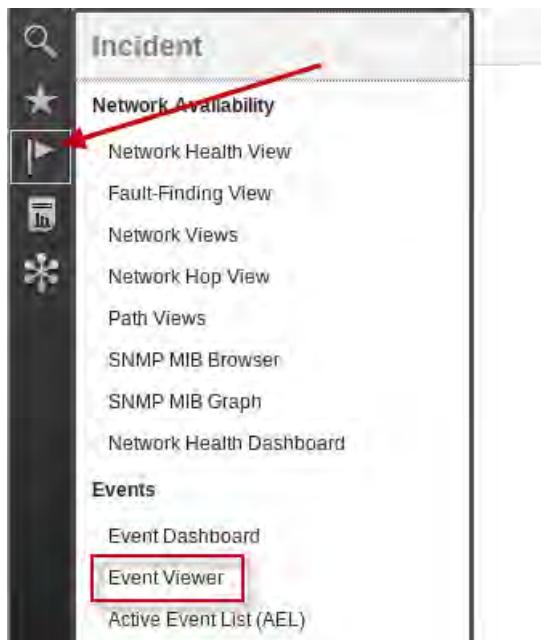
Verify that the user has access to the Network Availability features.

15. Click the icon and verify the items.



Verify that the user has access to the Common Reporting features.

16. Click the icon and select Event Viewer.



17. Right-click any event and examine the available tools.

Sev	Ack	Node	Alert Group	Summary
critical	No	chianti.tivlab.raleigh.ibm.com	: Linux_BP.	
critical	No	chianti.tivlab.raleigh.ibm.com	: Linux_BP.	
critical	No	chianti.tivlab.raleigh.ibm.com	: Linux_BP.	
critical	No	chianti.tivlab.raleigh.ibm.com	: Linux_BP.	
critical	No	chianti.tivlab.raleigh.ibm.com	: Linux_BP.	

A context menu is open over the third row of events, showing options: Information... Shift+I, Journal... Shift+J, Copy Ctrl+C, and Quick Filter. The 'Information...' option is highlighted with a red box.

The itnmuser user is defined with the *netcool\_ro* role. This role restricts access to most tools.

18. Log out as the **itnmuser** user.

19. Close the Firefox browser.

# Exercise 5 Installing the Network Manager Insight Pack

The Network Manager Insight Pack reads event data and network topology data so that it can be searched and visualized in the IBM Operations Analytics Log Analysis product.

## Installing the Insight Pack

1. Verify the status of the Log Analysis components.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -status
[netcool@host1 ~]$ /opt/IBM/LogAnalysis/utilities/unity.sh -status
Wed Feb 24 22:29:28 UTC 2016
IBM Operations Analytics - Log Analysis v1.3.2.0 ENTRY EDITION Application Services Status:

No. Service Status Process ID

1 Derby Network Server UP 4144
2 ZooKeeper UP 4191
9654
3 Websphere Liberty Profile UP 5687
4 EIF Receiver UP 6182
5 Log File Agent instance UP 6562

Getting status of Solr on host1.csuite.edu
Status of Solr Nodes:

No. Instance Name Host Status State

1 SOLR_NODE_LOCAL host1.csuite.edu UP ACTIVE

All Application Services are in Running State
Checking server initialization status: Server has initialized!
```

2. Create a directory to hold the Insight Pack files.

```
cd /opt/IBM/LogAnalysis/unity_content/
```

```
mkdir NetworkManager
```

3. Copy the Insight Pack installation file to the new directory:

```
cp /software/la/NetworkManagerInsightPack_v1.3.0.0.zip NetworkManager/
```

4. Install the Insight Pack as follows:

```
cd NetworkManager
```

 **Note:** Enter the following text as one line.

```
/opt/IBM/LogAnalysis/utilities/pkg_mgmt.sh
-install NetworkManagerInsightPack_v1.3.0.0.zip
.
.
.

C0047I : Unity apps deployment completed successfully
[packagemanager] 05/11/15 17:36:36:702 UTC [main] INFO - ContentPackManager : C
TGLC0023I : Install of NetworkManagerInsightPack_v1.3.0.0 completed
successfully

BUILD SUCCESSFUL
Total time: 17 seconds
```



**Important:** The build must complete successfully before you proceed.

5. Remove installation files.

```
cd /software
/bin/rm -R itnm
/bin/rm -R la
```

## Configuring the Insight Pack

The Insight Pack has two primary components. One component is Netcool/OMNibus events. The events are configured as a Log Analysis data source. The Network Manager insight pack can use the same data source as the OMNIBus Event insight pack that was configured previously.

The second component is the Network Manager topology database. The next series of steps describe how to configure the access to the topology database. You need some information about the database. Most of this information can be found in the following Network Manager property file:

```
/opt/IBM/tivoli/netcool/etc/precision/DbLogins.NOI_AGG_P.cfg
```

1. Open a terminal window if necessary.
2. Examine the property file.

```
more /opt/IBM/tivoli/netcool/etc/precision/DbLogins.NOI_AGG_P.cfg
//*****
//
// File: DbLogins.NOI_AGG_P.cfg
//
// Automatically generated on: Wed Feb 24 13:11:38 2016
// 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
);

```

3. Configure the Log Analysis property file as follows:

a. Change to the target directory:

```

cd
/opt/IBM/LogAnalysis/AppFramework/Apps/NetworkManagerInsightPack_v1.3.0.0/Ne
twork_Topoology_Search

```

b. Open the property for edit with the gedit utility:

```
gedit NM_EndToEndSearch.properties
```

c. Modify the property settings as shown here:

ncp.dla.datasource.type	= db2
ncp.dla.datasource.driver	= com.ibm.db2.jcc.DB2Driver
ncp.dla.datasource.url	= jdbc:db2://host1.csuite.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

- d. Save the changes and exit the gedit utility.

4. Restart the server.

- a. Stop Dashboard Application Services Hub.

```
cd /opt/IBM/JazzSM/profile/bin
.stopServer.sh server1 -username smadmin -password object00
Wait for the components to stop.
```

- b. Check for the Cognos process.

```
ps -ef | grep cognos
Repeat this command until the process is not running.
```

- c. Start the server.

```
./startServer.sh server1
Wait for the components to start.
```

A user requires access to Log Analysis to use the Network Manager topology search feature. The **ncouser** user ID is configured for access to Log Analysis. Configure the existing Network Manager users for access to Log Analysis.

5. Open a Firefox browser if necessary.

6. Log in to Dashboard Application Services Hub as **smadmin** with password **object00**.

7. Start WebSphere administrative console.

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

**8. Expand Users and Groups. Click Manage Groups.**



**9. Click UnityUsers.**

<input type="checkbox"/>	<a href="#">ITNM User</a>	cn=ITNM_User,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	<a href="#">Netcool Admin</a>	cn=Netcool_Admin,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	<a href="#">Netcool User</a>	cn=Netcool_User,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	<a href="#">UnityAdmins</a>	cn=UnityAdmins,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	<a href="#">UnityUsers</a>	cn=UnityUsers,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM

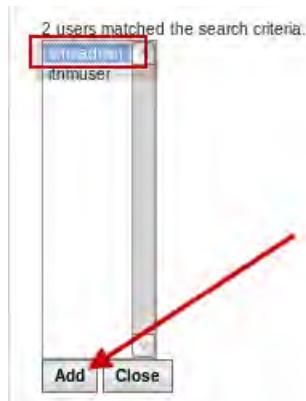
**10. Select the Members tab and click Add Users.**

The screenshot shows the 'Group Properties' window. At the top, there are three tabs: General (selected), Members, and Groups. The 'Members' tab is highlighted with a red arrow. Below the tabs, the 'Group name' is set to 'UnityUsers'. Underneath, it says 'The group has 3 members.' There are three buttons: 'Add Users...', 'Add Groups...', and 'Remove'. The 'Add Users...' button is highlighted with a red arrow. At the bottom, there are buttons for 'Select', 'ID', 'Type', and 'Unique Name'.

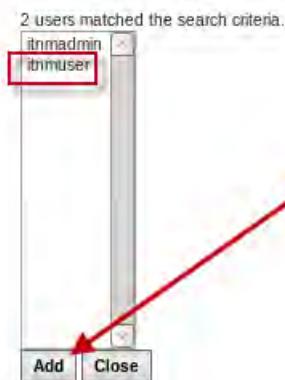
**11. Enter itnm\* and click Search.**

The screenshot shows a search interface. The 'Group name' is set to 'UnityUsers'. Below it, there is a search bar with the placeholder 'Search for users that will be members of this group.' Underneath, there are dropdown menus for 'Search by' (User ID) and 'Maximum results' (set to 100). The search term 'itnm\*' is entered into the search field and is highlighted with a red box. A 'Search' button is at the bottom.

12. Select **itnadmin** and click **Add**.



13. Select **itnmuser** and click **Add**.



14. Click **Close**.



15. Verify that the users are listed and click the **General** tab.

The screenshot shows the "General" tab of a group configuration window. The "Members" tab is also visible. The group name is "UnityUsers". The members list shows six entries:

Select	ID	Type	Unique Name
<input type="checkbox"/>	itnadmin	uid=itnadmin,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM	
<input type="checkbox"/>	itnmuser	uid=itnmuser,ou=tipusers,cn=tipRealm,dc=ibm,dc=com	
<input type="checkbox"/>	ncoadmin	uid=ncoadmin,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM	
<input type="checkbox"/>	ncouser	uid=ncouser,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM	
<input type="checkbox"/>	unityadmin	uid=unityadmin,ou=tipusers,cn=tipRealm,dc=ibm,dc=com	
<input type="checkbox"/>	unityuser	uid=unityuser,ou=tipusers,cn=tipRealm,dc=ibm,dc=com	

16. Click **OK** to save the group modifications.

17. Log out of WebSphere administrative console.

18. Close the Firefox tab.

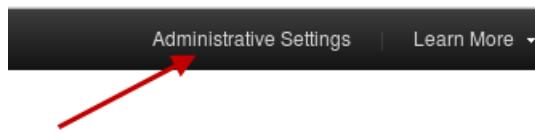
19. Log out of Dashboard Application Services Hub.

20. Connect to Log Analysis with the following URL:

<https://host1.csite.edu:9987/Unity>

21. Log in to Log Analysis as **unityadmin** with password **object00**.

22. Click **Administrative Settings**.



23. Click the **Users** tab. Click the icon to add a user.



24. Enter **itnmadmin** and click **OK**.

#### Configure LDAP User

A user profile is a distinct account with specific roles and permissions

\* User Name  itnmadmin

25. Click **OK** to confirm.



26. Click the icon to add a user.



27. Enter **itnmuser** and click **OK**.



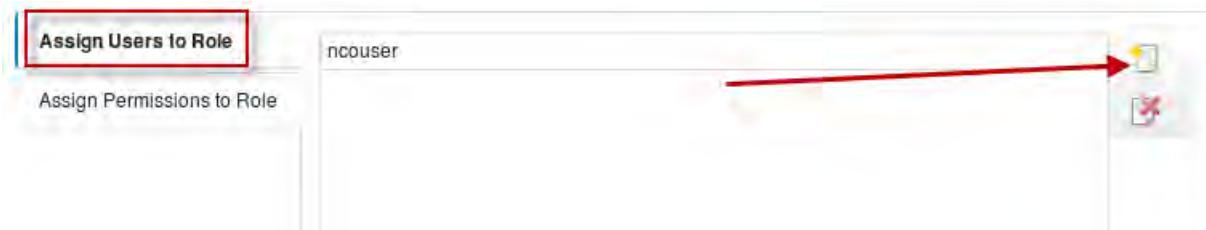
28. Click **OK** to confirm.



29. Click the **Roles** tab. Select **OMNIbusEvents**, and click the icon to edit the role.



30. Select **Assign Users to Role**. Click the icon to add a user.



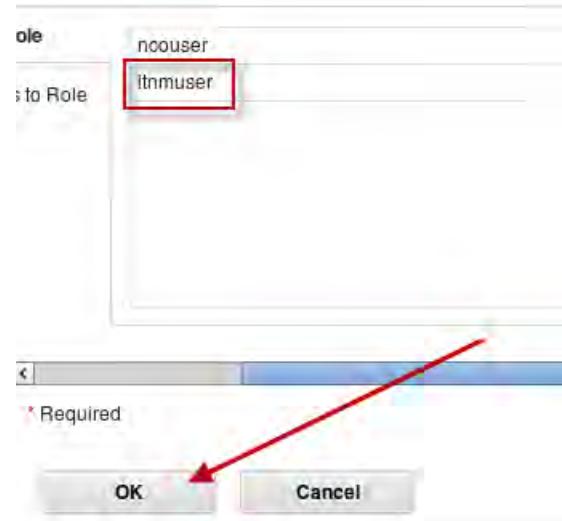
31. Select **itnmadmin**, and click **OK** to add the user to the role.



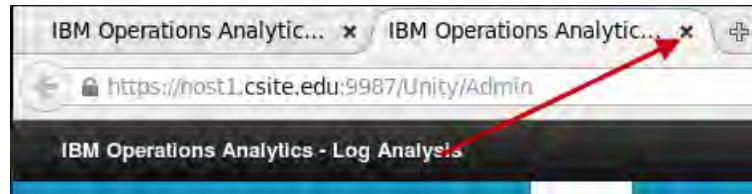
32. Select **itnmuser**, and click **OK** to add the user to the role.



33. Click **OK** to update the role.



34. Close the Firefox tab.



35. Log out of Log Analysis.

## Modifying the ObjectServer

You must modify the ObjectServer when you use the Network Manager Insight Pack. The modifications are included in an SQL file. After you apply this file, the triggers prevent events from being forwarded to IBM Operations Analytics Log Analysis until the Network Manager product enriches the events. To enrich events, Network Manager populates the NmosObjInst column of the ObjectServer alerts.status table during event processing; the Insight Pack requires that the NmosObjInst column is populated.

A publish 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.

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
```

```
(0 rows affected)
(2 rows affected)
(0 rows affected)
(0 rows affected)
(0 rows affected)
(0 rows affected)
```

## Installing the tools in Web GUI

Install the tools and menus to start the custom apps of the Network Manager Insight Pack in the Operations Analytics Log Analysis UI from the Web GUI. The configuration for these tools is included in the V8.1 Web GUI instance. You use the Web GUI Administration API utility to add the tools. You must add a user ID and password to a configuration file to complete the configuration of the Web GUI Administration API utility.

1. Configure the Web GUI Administration API utility.

- a. Change to the target directory:

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

- b. Open the file for edit:

```
gedit waapi.init
```

- c. Locate the following lines:

```
waapi.user:root
waapi.password:
```

- Change the lines as follows:

```
waapi.user:ncoadmin
waapi.password:object00
```

- Save the changes and exit the gedit utility.

## 2. Test the Web GUI Administration API utility:

```
cd /opt/IBM/netcool/gui/omnibus_webgui/bin
./webtop_report
.
.
.

Tivoli Netcool/OMNIBUS Web GUI DATA REPORT END


```

WAAPIClient: 0 method was fully executed.

## 3. Install the tools as follows:

- Change to the WAPPI bin directory:

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

- Run the following command to install the tools:

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

```

WAAPIClient: Request sent to server on
http://localhost:16310/ibm/console/webtop/...
Wed Jun 03 21:09:18 UTC 2015


```

WAAPIClient: 3 methods were fully executed.

# Configuring the tools in Network Manager

Install the tools and menus to start the custom apps of the Network Manager Insight Pack in the Operations Analytics Log Analysis GUI from the Network Views.

## 1. Modify the topoviz property settings.

- Change to the target directory:

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

- Open the property file for edit:

```
gedit topoviz.properties
```

- c. Add the following line on the end of the file.  

```
topoviz.unity.customappsui=https://host1.csuite.edu:9987/Unity/CustomAppsUI
```
  - d. Save the file and exit the gedit utility.
2. Modify the device menu file.
- a. Change to the target directory:  

```
cd /opt/IBM/netcool/gui/precision_gui/profile/etc/tnm/menus
```
  - b. Open the file for edit:  

```
gedit ncp_topoviz_device_menu.xml
```
  - c. Add the following line as shown here:  

```
<menu id="ncp_topo_e2esearch"/>
```


  - d. Save the file and exit the gedit utility.
3. Restart the server.
- a. Stop Dashboard Application Services Hub.  

```
cd /opt/IBM/JazzSM/profile/bin
.stopServer.sh server1 -username smadmin -password object00
```

Wait for the components to stop.
  - b. Check for the Cognos process.  

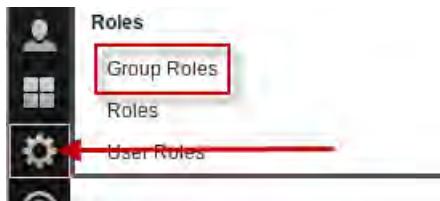
```
ps -ef | grep cognos
```

Repeat this command until the process is not running.
  - c. Start the server.  

```
./startServer.sh server1
```

Wait for the components to start.
4. Add the required role.
- Access to the topology search tools requires the *ncp\_event\_analytics* role.
- a. Open a Firefox browser.
  - b. Log in to Dashboard Application Services Hub as **smadmin** with password **object00**.

- c. Click the icon and select **Group Roles**.



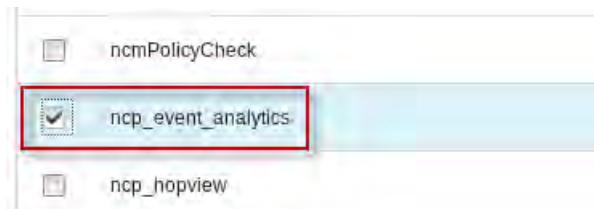
- d. Enter **Network\***, and click **Search**.

<b>Group ID:</b>	<input style="border: 2px solid red;" type="text" value="Network*"/>	<b>Desc:</b>
<b>Number of results to display:</b>		20
<input style="background-color: #e0e0e0; border: 1px solid #ccc; padding: 5px;" type="button" value="Search"/>		

- e. Click **Network\_Manager\_IP\_Admin**.

Group Name	Roles
<b>Network_Manager_IP_Admin</b>	ncp_oql_editor, ncp_networkview_admin_;
Network_Manager_User	ncp_mibbrowser, ncp_webtools, ncp_mibg

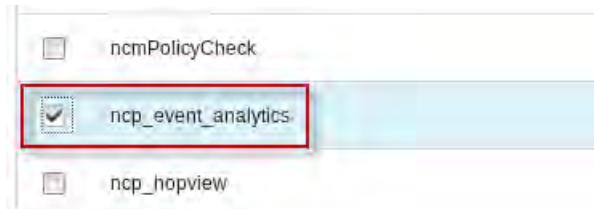
- f. Scroll down and select **ncp\_event\_analytics**. Click **Save**.



- g. Click **Network\_Manager\_User**.

Group Name	Roles
Network_Manager_IP_Admin	ncp_oql_editor, ncp_networkview_admin_;
<b>Network_Manager_User</b>	ncp_mibbrowser, ncp_webtools, ncp_mibg

- h. Scroll down and select **ncp\_event\_analytics**. Click **Save**.



- i. Log out of Dashboard Application Services Hub.

j. Close the Firefox browser.

The following list is a summary of the accomplishments from this unit:

- Installed Network Manager
- Installed the Network Manager Insight Pack
- Configured the topology search feature



## 5 IBM Tivoli Netcool Configuration Manager exercises

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

### Exercise 1 Creating users

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 created, and owned, by a non-root user. A non-root user is required for FTP access to move configuration files.

#### Creating the database user ID

You create a user with DB2 access authority. You use that user to create the topology database.

1. Switch to the root user.

```
su -
Password: object00
```

2. Create the database user as follows.

```
useradd -g db2iadm1 -m tncmdb
```

The **tncmdb** user is created as a member of the db2iadm1 group.

3. Set the password for the **tncmdb** user.

```
passwd tncmdb
Changing password for user tncmdb.
New password: object00
BAD PASSWORD: it is based on a dictionary word
Retype new password: object00
passwd: all authentication tokens updated successfully.
```

The password is set to **object00**.

4. Exit out of the root user back to the **netcool** user.

```
exit
```

5. Switch to the **tncmdb** user.

```
su - tncmdb
Password: object00
```

6. Add the DB2 environment settings to the **tncmdb** user.

- Open the environment file for edit.

```
cd /home/tncmdb
gedit .bashrc
```

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

```
source /home/db2inst1/sqllib/db2profile
```

- Save the file and exit the gedit utility.

7. Source the updated file.

```
source .bashrc
```

8. Verify settings.

```
which db2
/home/db2inst1/sqllib/bin/db2
```



**Important:** The command must return the correct location before you can proceed.

9. Exit the **tncmdb** user back to the **netcool** user.

```
exit
```

## Creating the FTP user ID

1. Switch to the root user.

```
su -
Password: object00
```

2. Create the database user as follows.

```
useradd -m tncm_ftp
```

3. Set the password for the **tncm\_ftp** user.

```
passwd tncm_ftp
Changing password for user tncm_ftp.
New password: object00
BAD PASSWORD: it is based on a dictionary word
Retype new password: object00
passwd: all authentication tokens updated successfully.
```

The password is set to **object00**.

4. Update file permissions for **tncm\_ftp** user.

```
cd /home
chmod -R a+r tncm_ftp
chmod -R a+w tncm_ftp
chmod -R a+x tncm_ftp
```

5. Exit out of the root user back to the **netcool** user.

```
exit
```



**Important:** In a production environment, you must verify that the FTP service is enabled on the Configuration Manager server.

## Exercise 2 Creating the database

This process is slightly different than the process used to create the Network Manager DB2 environment. With Network Manager, the DB2 environment is created as the **ncim** user. With Netcool Configuration Manager, the DB2 environment is created as the **db2inst1** user. Then, you use SQL commands to grant access to that environment by the **tncmdb** user.

1. Expand the Netcool Configuration Manager installation file.

```
cd /software/tncm
mkdir base
cd base
tar -xvf ../ITNCM_Base_Linux.tar
```

2. Change file permissions on the temp directory and contents.

```
chmod -R a+r *
```

3. Switch to the **db2inst1** user.

```
su - db2inst1
Password: object00
```

4. Create the database as follows.

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

```
DB20000I The CREATE DATABASE command completed successfully.
```

**Note:** The command runs for several minutes.

5. Configure database user privileges.

- a. Connect to the database.

```
db2 connect to itncm
```

Database Connection Information

```
Database server = DB2/LINUXX8664 10.5.3
SQL authorization ID = DB2INST1
Local database alias = ITNCM
```

- b. Issue the GRANT command.



**Important:** Enter the following command as one continuous line.

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

```
DB20000I The SQL command completed successfully.
```

- c. Enter the highlighted commands to update the transaction log size.

```
db2 update db cfg using logfilsiz 5000
```

DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database

must be shutdown and reactivated before the configuration parameter changes become effective.

```
db2 update db cfg for itncm using logprimary 200
```

DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database

must be shutdown and reactivated before the configuration parameter changes become effective.

```
db2 update db cfg for itncm using logsecond 50
```

DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

```
db2 update db cfg for itncm using LOCKLIST 8192
```

DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

- d. Commit changes.

```
db2 commit
```

DB20000I The SQL command completed successfully.

- e. Reset the database connection.

```
db2 connect reset
```

DB20000I The SQL command completed successfully.

- f. Exit the **db2inst1** user back to the **netcool** user.

```
exit
```

6. Add user-defined functions as follows.

- a. Switch to the Netcool Configuration Manager database user.

```
su - tncmdb
```

```
Password: object00
```

- b. Change to the location of the JAR file.

```
cd /software/tncm/base/
```

- c. Copy the JAR file.

```
cp ibm_tivoli-ncm_db2_udf.jar /home/tncmdb
```

- d. Connect to the Netcool Configuration Manager database.

```
db2 connect to itncm
```



**Important:** The first connect request with the **tncmdb** user might take several minutes to complete.

- e. Install the JAR file.

```
db2 "CALL SQLJ.INSTALL_JAR('file:/home/tncmdb/ibm_tivoli-ncm_db2_udf.jar',
ncm_db2_udf)"
```

```
DB20000I The CALL command completed successfully.
```

- f. Refresh the classes.

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

```
DB20000I The CALL command completed successfully.
```

- g. Exit out of the **tncmdb** user back to the **netcool** user:

```
exit
```

## Exercise 3 Installing Jazz for Service Management

In this step, you install Jazz for Service Management, WebSphere Application Server, and Dashboard Application Services Hub. These components are required for the Netcool Configuration Manager presentation server component.



**Important:** You cannot reuse the existing installation of Jazz for Service Management. You must install a separate copy, into separate directories, and configure the components to use unique port numbers. You must follow the instructions **very carefully** for the following exercises. If you make a mistake in any step, you might destroy the existing copy of Dashboard Application Services Hub.

1. Start IBM Installation Manager:

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

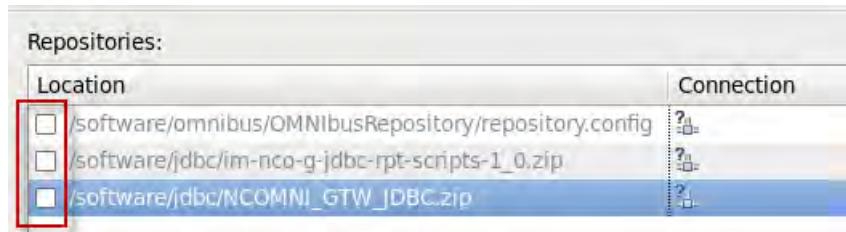
2. Define the repositories.



**Note:** The installation files are still in **/tmp**, and the repository entries are still defined in IBM Installation Manager.

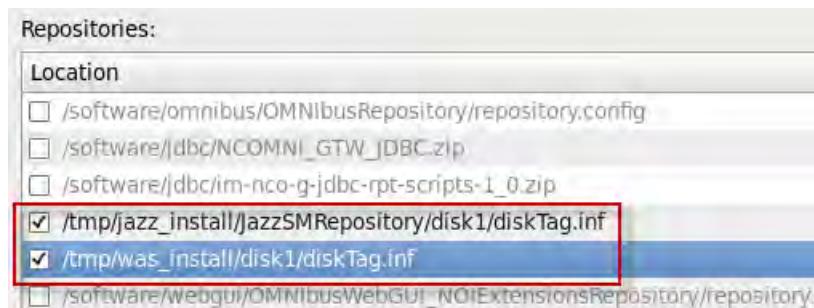
- a. Click **File** and select **Preferences**. Select **Repositories**.

- b. Remove the check marks from the existing entries.



**Note:** You added the Jazz and WebSphere repositories in a previous unit. You must locate the entries and select them.

- c. Select the Jazz repository entry. Select the WebSphere entry, and click **OK**.



3. Start the installation.

- a. Click **Install**.

The next window shows that some of the packages are currently installed.

Installation Packages	Status	Ve
IBM WebSphere Application Server	Installed	IBI
Version 8.5.5.7	Installed	IBI
Pluggable Application Client for IBM WebSphere Application Se		
Web Server Plug-ins for IBM WebSphere Application Server		
Version 8.5.5.7		
IBM WebSphere SDK Java Technology Edition (Optional)	Installed	IBI
Version 7.0.9.10	Installed	IBI
Jazz for Service Management extension for IBM WebSphere 8.0		
Version 1.1.0.2		
Jazz for Service Management extension for IBM WebSphere 8.5	Installed	IBI
Version 1.1.2.1	Installed	IBI

- b. Select **IBM WebSphere Application Server**, and click **Continue**.



- c. Select **IBM WebSphere SDK**, and click **Continue**.



- d. Select **Jazz for Service Management extension**, and click **Continue**.



- e. Select **IBM Dashboard Application Services Hub**, and click **Continue**.



- f. Verify that you selected the required packages, and click **Next**.

Installation Packages		Status
► <input type="checkbox"/>	Application Client for IBM WebSphere Application Server	
► <input type="checkbox"/>	IBM HTTP Server for WebSphere Application Server	
► <input checked="" type="checkbox"/>	IBM WebSphere Application Server	Installed
<input checked="" type="checkbox"/>	Version 8.5.5.7	Installed
<input type="checkbox"/>	Pluggable Application Client for IBM WebSphere Application Se	
► <input type="checkbox"/>	Web Server Plug-ins for IBM WebSphere Application Server	
► <input checked="" type="checkbox"/>	IBM WebSphere SDK Java Technology Edition (Optional)	Installed
<input checked="" type="checkbox"/>	Version 7.0.9.10	Installed
► <input type="checkbox"/>	Jazz for Service Management extension for IBM WebSphere 8.0	
► <input checked="" type="checkbox"/>	Jazz for Service Management extension for IBM WebSphere 8.5	Installed
<input checked="" type="checkbox"/>	Version 1.1.2.1	Installed
► <input type="checkbox"/>	Registry Services	
► <input type="checkbox"/>	Administration Services	
► <input type="checkbox"/>	Reporting Services	Installed
► <input type="checkbox"/>	Security Services	
► <input checked="" type="checkbox"/>	IBM Dashboard Application Services Hub	Installed
<input checked="" type="checkbox"/>	Version 3.1.2.1	Installed
► <input type="checkbox"/>	Administration Services UI	



**Important:** Do not select the **Reporting Services** package.

- g. Accept the license agreement and click **Next**.

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

- i. 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 8.5.5.7	
IBM WebSphere SDK Java Technology Edition (Optional) 7.0.9.10	
Jazz for Service Management extension for IBM WebSphere 8.5 1.1.2.1	
Core services in Jazz for Service Management_1	/home/netcool/IBM/JazzSM
IBM Dashboard Application Services Hub 3.1.2.1	

Package Group Name: IBM WebSphere Application Server V8.5\_1

Installation Directory: `/opt/IBM/WebSphere/AppServer_ncm`

- j. Click the package name **Core services in Jazz for Service Management\_1** to select it.

- k. 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
IBM WebSphere Application Server 8.5.5.7	
IBM WebSphere SDK Java Technology Edition (Optional) 7.0.9.10	
Jazz for Service Management extension for IBM WebSphere 8.5 1.1.2.1	
Core services in Jazz for Service Management_1	/opt/IBM/JazzSM_ncm
IBM Dashboard Application Services Hub 3.1.2.1	

Package Group Name: Core services in Jazz for Service Management\_1

Installation Directory: `/opt/IBM/JazzSM_ncm`

- l. Click **Next**.

- m. Accept the default translation setting, and click **Next**.

n. Accept the default list of features. Click **Next**.



o. Enter **object00** as the password and click **Validate**.

The screenshot displays the 'Common Configurations' screen. In the 'WebSphere Configuration' section, the 'WebSphere installation location' is set to '/opt/IBM/WebSphere/AppServer\_ncm' and the 'Profile deployment type' is set to 'Create WebSphere profile'. In the 'Profile details' section, the 'Profile location' is set to '/opt/IBM/JazzSM\_ncm/profile', 'Profile name' is 'JazzSMProfile', 'Node name' is 'JazzSMNode01', 'Server name' is 'server1', and 'User name' is 'smadmin'. The 'Password' and 'Password confirmation' fields are both redacted with dots. A red arrow points from the 'Validate...' button to the 'Password confirmation' field.



**Important:** You cannot proceed until you validate the password.

p. Verify that the validation is successful and click **Next**.





**Hint:** No message indicates success. If the validation is successful, the **Next** option is available.

- q. Change the default HTTP port value to **15310** and click **Next**.

**Common Configurations**

Ports Configuration

Configure the various network ports to which the WebSphere Application Server provides services.

HTTP transport port	15310
HTTPS transport secure port	15311
Bootstrap port	15312
SOAP connector port	15313
IPC connector port	15314
Administrative console port	15315
Administrative console secure port	15316
High availability manager communication port	15318
ORB listener port	15320
SAS SSL server authentication port	15321
CSIV2 client authentication listener port	15322



**Note:** When you change the value for the HTTP port number, the remaining port numbers change automatically.

- r. Accept the default value for context root and click **Next**.

**Configuration for IBM Dashboard Application Services Hub 3.1.2.1**

Context Root

Context Root /ibm/console

- s. Review the installation summary and click **Install**.

**Install Packages**  
Review the summary information.

Install Licenses Location Features Summary

**Target Location**  
Shared Resources Directory: /home/netcool/IBM/IBMIMShared

**Packages**

Packages	Installation Directory
IBM WebSphere Application Server V8.5_1	/opt/IBM/WebSphere/AppServer_ncm
IBM WebSphere Application Server 8.5.5.7	
WebSphere Application Server Full Profile	
IBM WebSphere SDK for Java Technology Edition	
IBM WebSphere SDK Java Technology Edition (Optional)	
Jazz for Service Management extension for IBM WebSphere	
Install JazzSM WebSphere Extension	
Core services in Jazz for Service Management_1	/opt/IBM/JazzSM_ncm
IBM Dashboard Application Services Hub 3.1.2.1	



**Note:** The installation process runs approximately 40 minutes.

- t. Verify that the installation is successful. Leave the option set to log on to IBM Dashboard Application Services Hub and click **Finish**.

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

following packages were installed:

- IBM WebSphere Application Server V8.5\_1
- IBM WebSphere Application Server 8.5.5.7
- IBM WebSphere SDK Java Technology Edition (Optional)
- Jazz for Service Management extension for IBM WebSphere
- Core services in Jazz for Service Management\_1
- IBM Dashboard Application Services Hub 3.1.2.1

Which program do you want to start?

Log on to IBM Dashboard Application Services Hub

Profile Management Tool to create a profile.

Profile Management Tool to create an application server

None

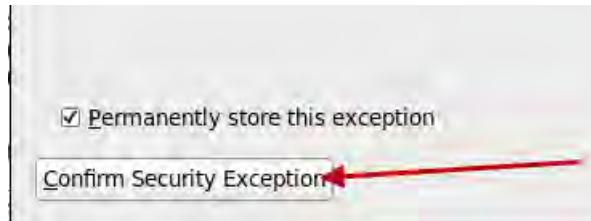
A Firefox browser opens and connects to IBM Dashboard Application Services Hub:

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

4. Expand I Understand the Risks, and click Add Exception.



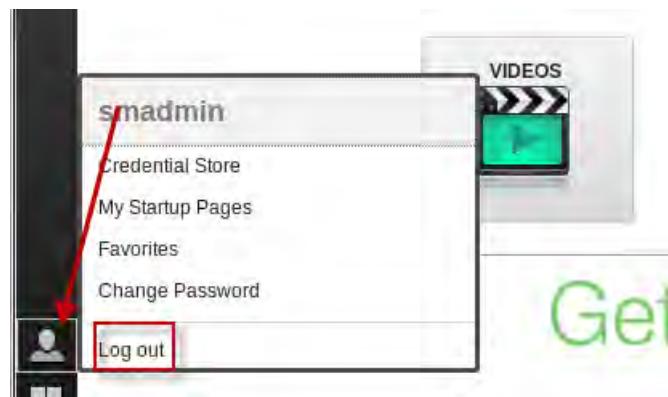
5. Click Confirm Security Exception.



6. Log in as user **smadmin** with password **object00**.



7. Verify successful access. Click the icon and select Log out.



8. Close the Firefox browser.

9. Remove the installation files to conserve disk space.

```
cd /tmp
/bin/rm -R jazz_install
/bin/rm -R was_install
```

You now have two complete copies of Jazz for Service Management installed and running. One copy is used for the Netcool Operations Insight components. The second copy is configured in the following exercise for use with Netcool Configuration Manager.

## Exercise 4 Installing Netcool Configuration Manager

### Installing the presentation server

You expanded the installation file in a previous exercise.

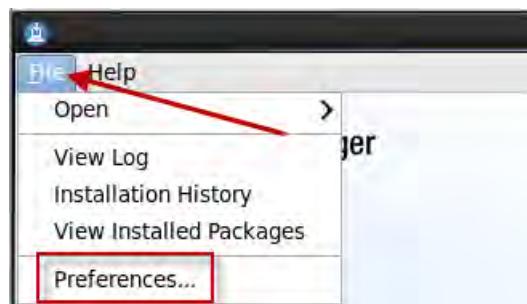
1. Start IBM Installation Manager.



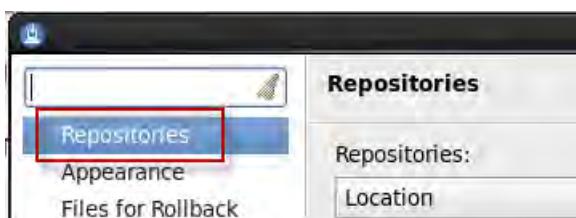
**Note:** IBM Installation Manager might still be open from the previous exercise.

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

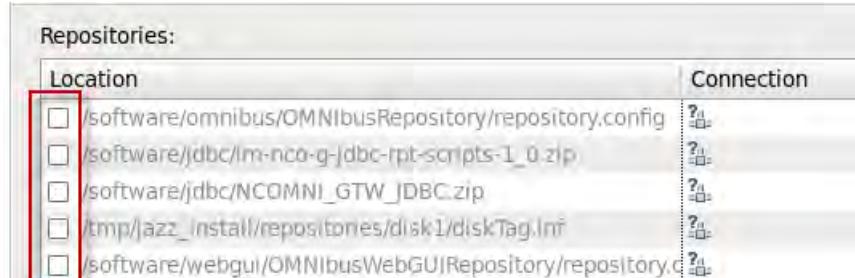
2. Click **File** and select **Preferences**.



3. Select **Repositories**.

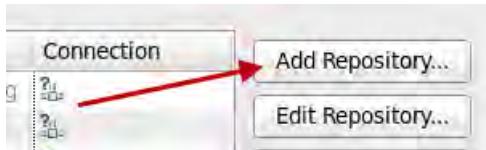


- Remove all check marks from any existing repository entries.



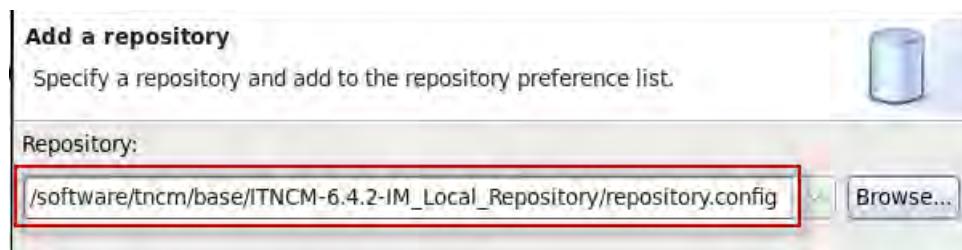
Repositories:	
Location	Connection
<input type="checkbox"/> /software/omnibus/OMNIbusRepository/repository.config	?
<input type="checkbox"/> /software/jdbc/lm-nco-g-jdbc-rpt-scripts-1_0.zip	?
<input type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	?
<input type="checkbox"/> /tmp/jazz_install/repositories/disk1/diskTag.ini	?
<input type="checkbox"/> /software/webgui/OMNIbus/WebGUIRepository/repository.config	?

- Click **Add Repository**.



- Click **Browse** and locate the following file:

/software/tncm/base/ITNCM-6.4.2-IM\_Local\_Repository/repository.config



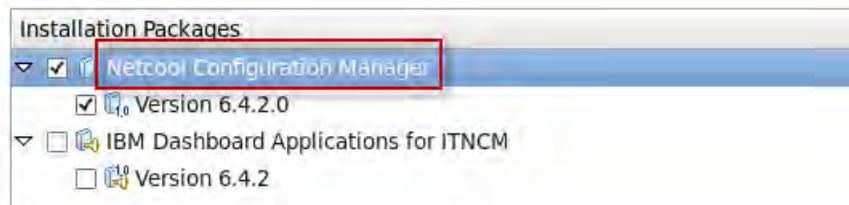
- Click **OK** to add the repository.

- Verify that the repository is selected, and click **OK**.

- Click **Install**.



- Select the **Netcool Configuration Manager** package. Click **Next**.



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

12. Select the entry for **Netcool Configuration Manager**. Change the installation directory to **/opt/IBM/ncm**. Click **Next**.



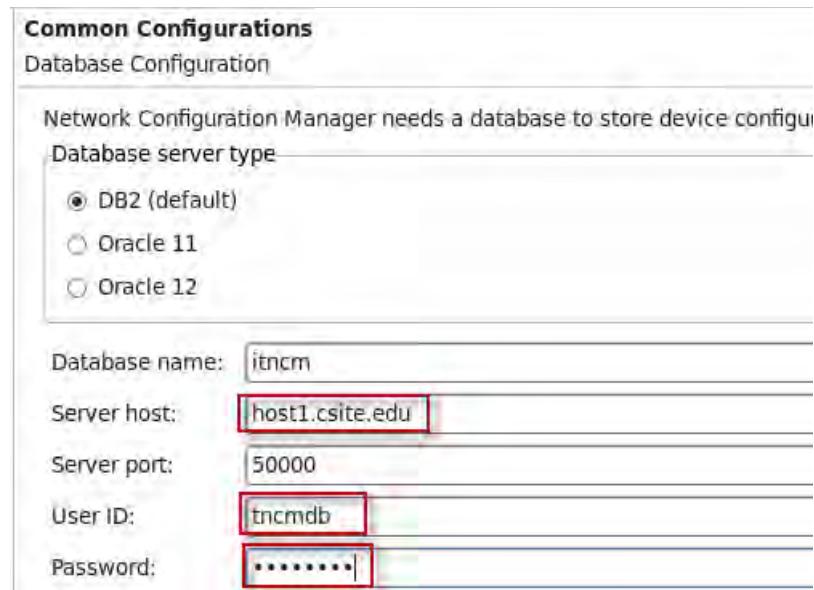
13. Accept the default list of features. Click **Next**.



14. Enter the db2 access information as follows, and click **Next**.

- Enter **host1.csite.edu** for the host name.
- Enter **50000** for the port number.
- Enter **tncmdb** for the database user.

- d. Enter **object00** for the password.



15. Click **OK** to accept the option to create the database tables.



16. Enter the FTP access information as follows, and scroll down.



**Important:** Make certain that you scroll down and complete the next step before you click Next.

- a. Enter **host1.csite.edu** for the host name.
- b. Enter **tncm\_ftp** for the user.
- c. Enter **object00** for the password.

- d. Enter **/home/tncm\_ftp** for the account directory.

**Common Configurations for Network Configuration Manager**

ITNCM Server Configuration

Root Realm	ITNCM
FTP Server	host1.csuite.edu
FTP User Account	tncm_ftp
FTP user Password	*****
FTP User Password Confirmation	*****
FTP User Account Directory	/home/tncm_ftp
SMTP Server	localhost

- e. Select the option for integrated NCM - NM install.  
f. Enter **host1.csuite.edu** for the host name.  
g. Enter **16311** for the port number.  
h. Enter **itnmadmin** for the user name.  
i. Enter **object00** for the password.  
j. Enter **ITNCM/NOI\_AGG\_P** for the realm.  
k. Click **Next**.

Is This the main IDT Server

Yes  
 No

Select the type of install you require

Activate Configuration-Core  
 Activate Compliance-Core

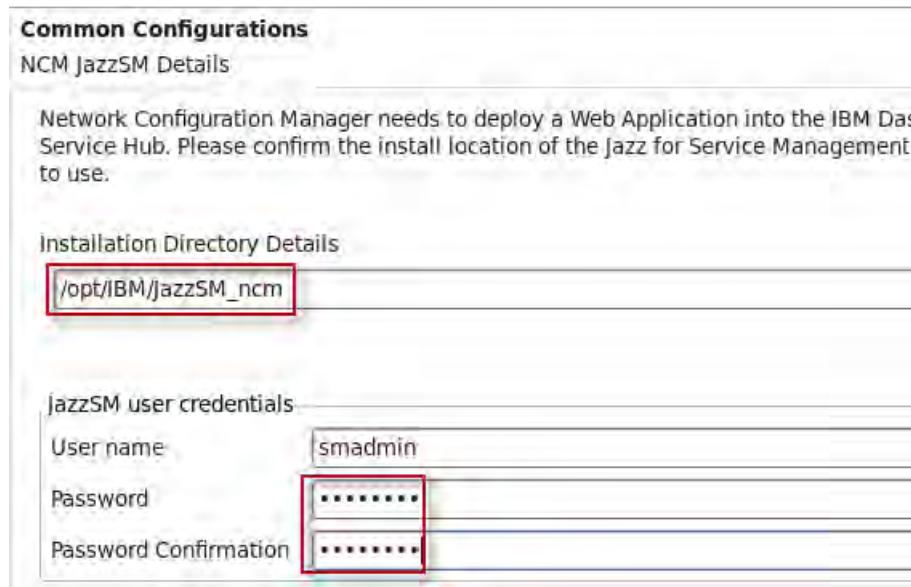
Is this an integrated NCM - NM Install?

The NM Hostname: host1.csuite.edu  
The port to connect to: 16311  
The NM User: itnmadmin  
The NM User Password: \*\*\*\*\*  
NM User Password Confirmation: \*\*\*\*\*  
The realm to import the devices to remove the @ symbol if specifying an exact domain: ITNCM/NOI\_AGG\_P



**Note:** NOI\_AGG\_P is the Network Manager domain name.

17. Change the installation directory to **/opt/IBM/JazzSM\_ncm**. Enter **object00** for the password, and click **Next**.



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

**Install Packages**  
Review the summary information.

Install    Licenses    Location    Features    Summary

**Target Location**

Package Group Name: Network Configuration Manager  
Installation Directory: /opt/IBM/ncm  
Shared Resources Directory: /home/netcool/IBM/IBMMIMShared

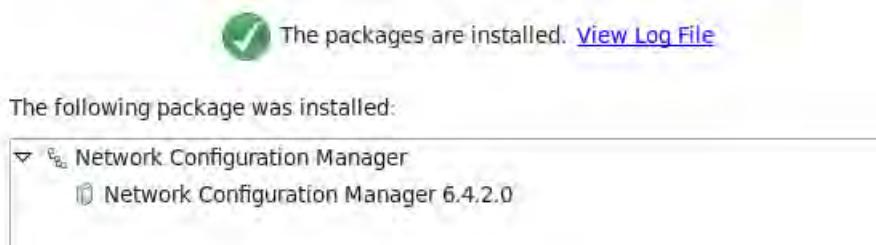
**Packages**

Packages	
▼	Network Configuration Manager 6.4.2.0
▼	ITNCM
▼	Server Installation Type
	Presentation Server and Worker Server

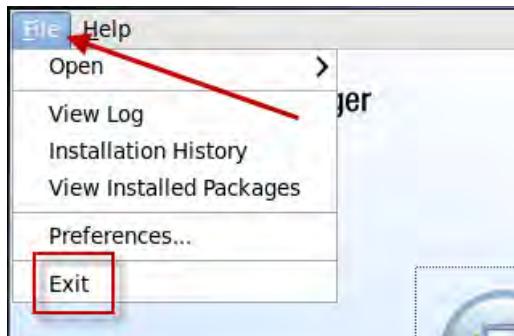


**Note:** The installation runs for approximately 25 minutes.

19. Verify that the package installation is successful, and click **Finish**.



20. Click **File** and select **Exit** to close IBM Installation Manager.



21. Start the Netcool Configuration Manager components.

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

22. Open a Firefox browser.

23. Connect to the presentation server at the following URL.

```
http://host1.csite.edu:15310/security/login.jsp
```

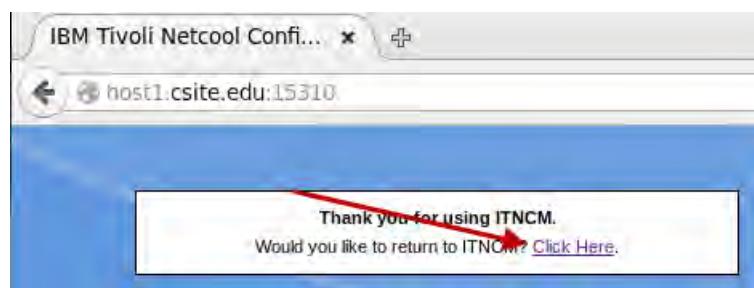
24. Log in as user **Intelliden** with password **object00**.



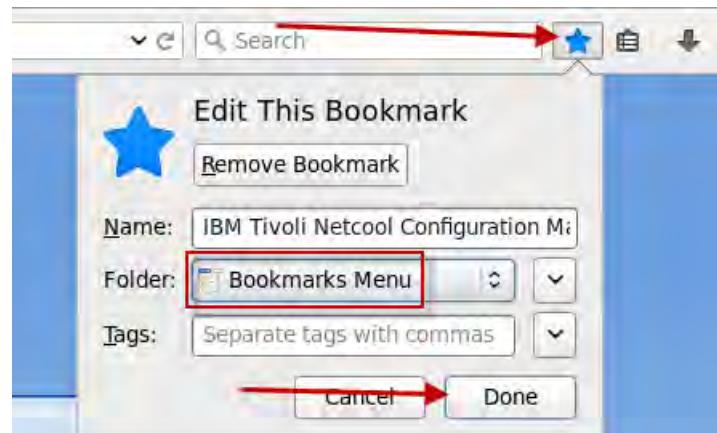
25. Verify access, and click **Logoff**.



26. Select **Click here** to return to the login screen.



27. Click the *star* icon twice to save the page as a bookmark.



28. Close the browser.

## Installing the Netcool Configuration Manager GUI components.

You expanded the installation file in a previous exercise, and defined the software repository.

1. Start IBM Installation Manager.

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

2. Click **Install**.



3. Select **IBM Dashboard Applications for ITNCM**, and click **Next**.

Installation Packages	Status
Netcool Configuration Manager	Installed
Version 6.4.2.0	Installed
IBM Dashboard Applications for ITNCM	Will be installed
Version 6.4.2	Will be installed

4. Accept the default package group, and click **Next**.

Install   Location   Features   Summary

Use the existing package group  
 Create a new package group

Package Group Name	Installation Directory
IBM Netcool GUI Components	/opt/IBM/netcool
Core services in Jazz for Service Management	/opt/IBM/jazzSM
Core services in Jazz for Service Management_1	/opt/IBM/jazzSM_ncm
IBM Netcool Core Components	/opt/IBM/tivoli/netcool

Package Group Name: IBM Netcool GUI Components  
Installation Directory: /opt/IBM/netcool  
Architecture Selection:  32-bit  64-bit

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

Install   Location   Features   Summary

Features

IBM Dashboard Applications for ITNCM 6.4.2

- Activity Viewer
- ITNM Services Wizard

6. Enter **object00** for the password, and 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: smadmin  
Password: **\*\*\*\*\***

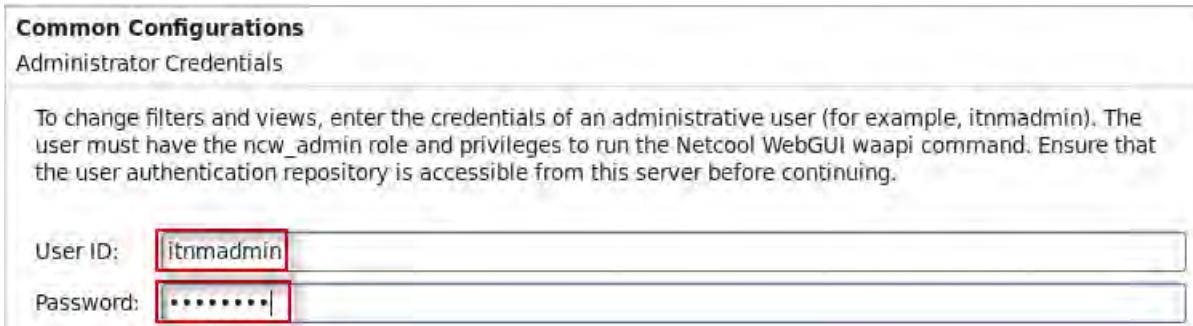


7. Enter **itnadmin** for the user, and **object00** for the password. Click **Next**.

**Common Configurations**  
Administrator Credentials

To change filters and views, enter the credentials of an administrative user (for example, itnadmin). 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: **itnadmin**  
Password: **\*\*\*\*\***



8. Enter the DB2 access information as shown here, and click **Next**.

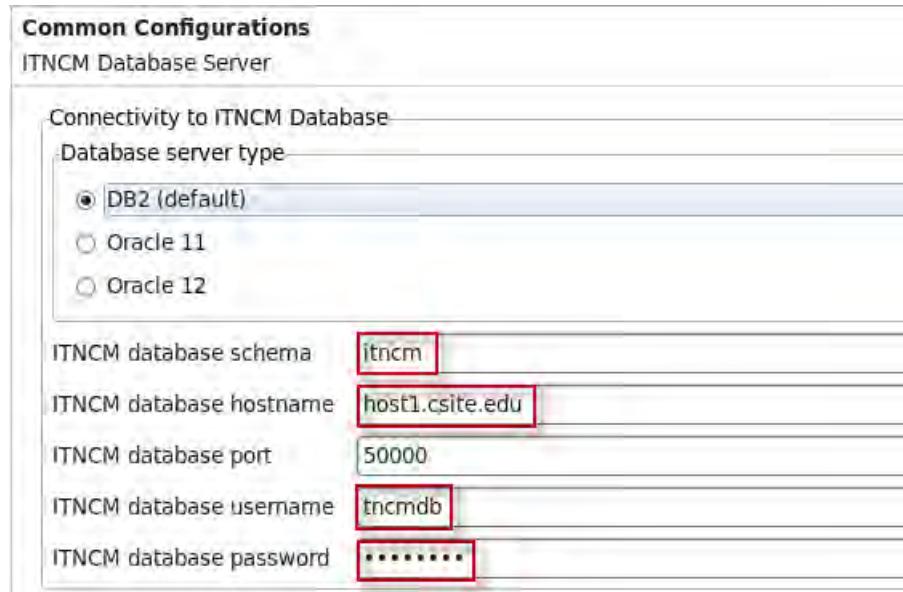
- Enter **itncm** for the database schema.
- Enter **host1.csite.edu** for the host name.
- Enter **tncmdb** for the user name.
- Enter **object00** for the password.

**Common Configurations**  
ITNCM Database Server

Connectivity to ITNCM Database

Database server type:  
 DB2 (default)  
 Oracle 11  
 Oracle 12

ITNCM database schema: **itncm**  
ITNCM database hostname: **host1.csite.edu**  
ITNCM database port: **50000**  
ITNCM database username: **tncmdb**  
ITNCM database password: **\*\*\*\*\***



9. Enter the presentation server access information as follows, and click **Next**.
  - a. Enter **host1.csuite.edu** for the host name.
  - b. Enter **15311** for the port number.

**Common Configurations**  
ITNCM Presentation Server

Connectivity to ITNCM Presentation server

ITNCM presentation server scheme https  
ITNCM presentation server hostname host1.csuite.edu  
ITNCM presentation server web port 15311

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

```
graph LR; ITNCM[ITNCM presentation server] -- https --> NCM[Netcool Configuration Manager]; ITNCM -- host1.csuite.edu --> NCM; ITNCM -- 15311 --> NCM
```

The installation process verifies access to the presentation server.

10. Enter the Common Reporting server access information as follows, and click **Next**.
  - a. Enter **host1.csuite.edu** for the host name.
  - b. Enter **16311** for the port number.

**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

```
graph LR; ITNCM[ITNCM Reporting Server] -- https --> JDWGUI[Jazz/DASH/Web GUI]; ITNCM -- host1.csuite.edu --> JDWGUI; ITNCM -- 16311 --> JDWGUI
```

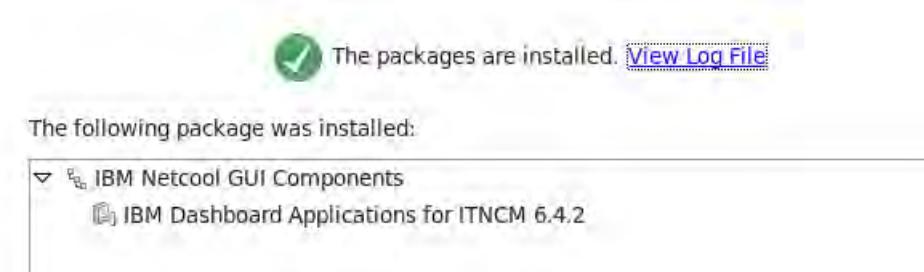
The installation process verifies access to the Common Reporting server.

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



**Important:** The installation runs approximately 20 minutes.

- Verify that the installation is successful, and click **Finish**.



Leave the IBM Installation Manager open.

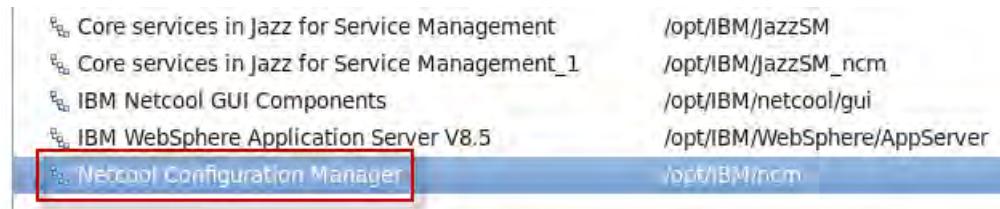
## Installing Common Reporting reports

You expanded the installation file in a previous exercise.

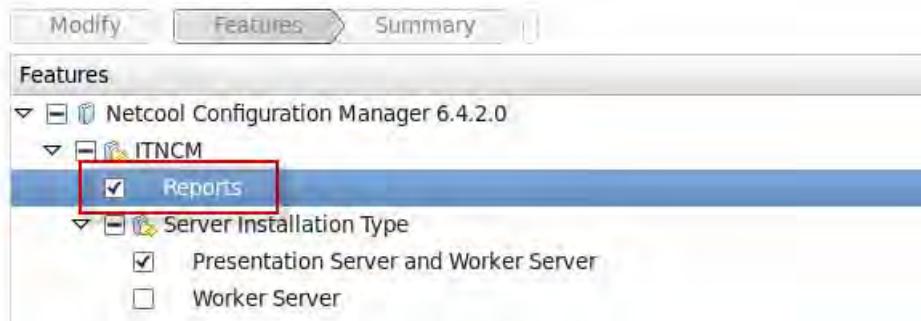
- Click **Modify**.



- Select the **Netcool Configuration Manager** package. Click **Next**.



- Select **Reports**, and click **Next**.



- Enter the db2 access information as follows, and click **Next**.

- Enter **host1.csite.edu** for the host name.
- Enter **50000** for the port number.
- Enter **tncmdb** for the database user.

- d. Enter **object00** for the password.

**Common Configurations**

Database Configuration

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

Database server type

DB2 (default)  
 Oracle 11  
 Oracle 12

Database name: itncm

Server host: host1.csite.edu

Server port: 50000

User ID: tncmdb

Password: **\*\*\*\*\***

5. Select the option to install reports. Enter **object00** for the password. Click **Next**.

**Common Configurations**

TCR properties

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.

No (default)  
 Yes

Installation Directory Details:  
/opt/IBM/JazzSM

JazzSM user credentials

User name: smadmin

Password: **\*\*\*\*\***

Password Confirmation: **\*\*\*\*\***



**Important:** You currently have two copies of Jazz for Service Management installed. One copy is used for the Netcool Configuration Manager. This copy is installed in **/opt/IBM/JazzSM\_ncm**. The second copy is used for the primary user interface for the Netcool Operations Insight components. This copy is installed in **/opt/IBM/JazzSM**. The second copy is what you select in this window.

6. Verify that the **Reports** feature is listed, and click **Modify**.

**Target Location**

Package Group Name: Network Configuration Manager  
Installation Directory: /opt/IBM/ncm  
Shared Resources Directory: /home/netcool/IBM/IBMIMShared

**Features**

Adding Feature	Removing Feature
Network Configuration Manager 6.4.2.0	
ITNCM	
Reports	

 **Note:** The process runs approximately 10 minutes.

7. Verify that the modification is successful. Click **Finish**.

The modification completed successfully. [View Log File](#)

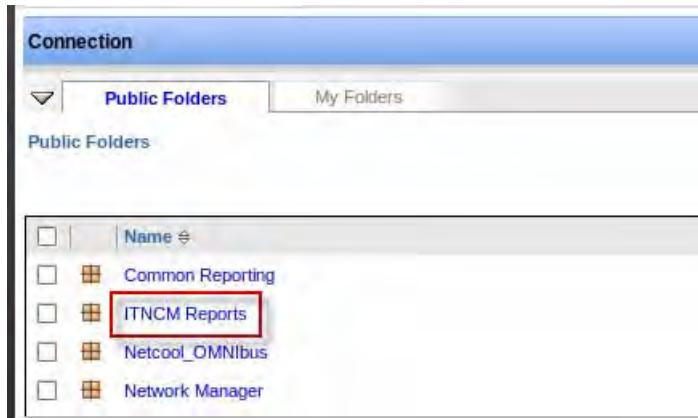
The following package was modified:

Netcool Configuration Manager
-------------------------------

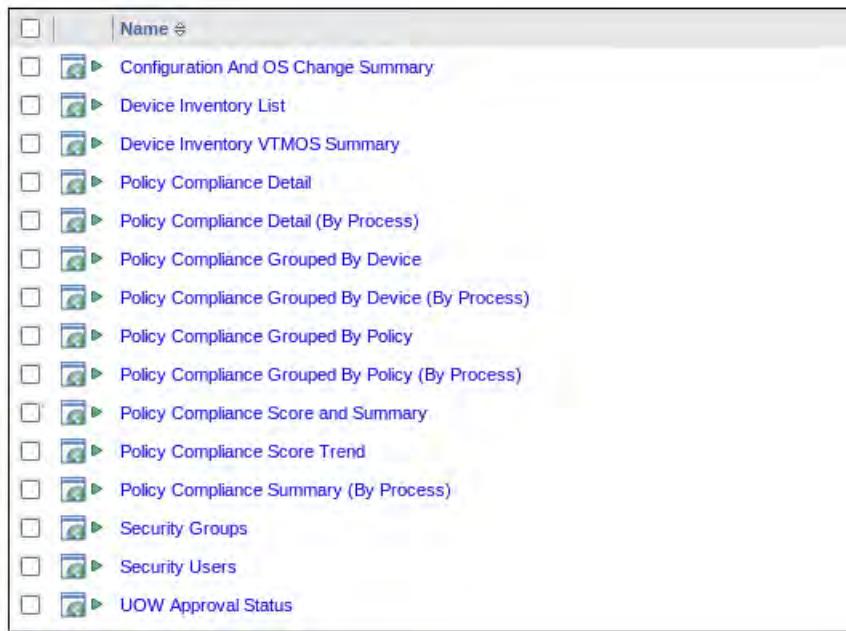
8. Click **File** and select **Exit** to close IBM Installation Manager.
9. Open a Firefox browser.
10. Log in to Dashboard Application Services Hub as **ncoadmin** with password **object00**.
11. Click the icon and select **Common Reporting**.



12. Click ITNCM Reports.



The list of Netcool Configuration Manager reports opens.



13. Log out of Dashboard Application Services Hub.

14. Close the Firefox browser.

## Exercise 5 Installing device drivers

In this exercise, you install a set of Standard device drivers and a set of Smart Model device drivers.

# Installing the standard device drivers



**Note:** You must stop the Netcool Configuration Manager components before you install device drivers.

1. Stop the components.

```
/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:

2. Enter **Intelliden** for the user and **object00** for the password. Click **OK**.



3. Expand the Standard drivers install file.

```
cd /software/tncm
mkdir Standard
cd Standard
unzip ../NCM-6.4.2-Drivers19-Standard.zip
```

4. Install the Standard drivers.

- a. Change to the installation location.

```
cd /software/tncm/Standard/NCM-6.4.2-Drivers19-Standard
```

- b. Change file permissions to allow the drivers to run.

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

- c. Run the installation utility.

```
./ITNCMDrivers.bin LAX_VM /opt/IBM/ncm/jre/bin/java -i console
```

.

.

.

PRESS <ENTER> TO CONTINUE:

.

.

.

Press Enter to continue viewing the license agreement, or enter "1" to accept the agreement, "2" to decline it, "3" to print it, or "99" to go back to the previous screen.: 1



**Note:** Enter 1 to accept the license agreement.

.

.

.

Where would you like to install?

Default Install Folder: /opt/IBM/ncm

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT

:



**Note:** Press Enter to accept the default.

.

.

.

Disk Space Information (for Installation Target):

Required: 104 MegaBytes

Available: 25,642 MegaBytes

PRESS <ENTER> TO CONTINUE:



**Note:** Press Enter to accept the default.

.

.

.

Installation Complete

-----

Congratulations. ITNCM Standard Drivers support version 6.4.0.0 has been successfully installed.

PRESS <ENTER> TO EXIT THE INSTALLER:

5. Remove the installation files.

```
cd /software/tncm
/bin/rm -R Standard

/bin/rm NCM-6.4.2-Drivers19-Standard.zip
```

## Installing the Smart Model device drivers

1. Expand the Smart Model drivers install file.

```
cd /software/tncm
mkdir SM
cd SM
unzip ../NCM-6.4.2-Drivers19-SmartModel.zip
```

2. Install the Smart Model drivers.

- a. Change to the installation location.

```
cd /software/tncm/SM/NCM-6.4.2-Drivers19-SmartModel/Disk1/InstData
```

- b. Change file permissions to allow the drivers to run.

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

- c. Run the installation utility.

```
./ITNCMDrivers.bin
```

.

.

.

PRESS <ENTER> TO CONTINUE:



**Note:** Press Enter to continue.

.

.

.

Press Enter to continue viewing the license agreement, or enter "1" to accept the agreement, "2" to decline it, "3" to print it, or "99" to go back to the previous screen.: **1**



**Note:** Enter 1 to accept the license agreement.

.

.

.

Where would you like to install?

Default Install Folder: /opt/IBM/ncm

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT



**Note:** Press Enter to accept the default path.

.

.

.

18- SNMP Devices

19- VMware Devices

->20- Exit Installer

21- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT  
: **1**



**Note:** Enter 1 to install all of the drivers.

.

.

.

Disk Space Information (for Installation Target):

Required: 13,738,673,199 Bytes

Available: 22,215,008,256 Bytes

PRESS <ENTER> TO CONTINUE:



**Note:** Press Enter to continue.

.

.

.

Installation Complete

-----

Congratulations. IBM Tivoli Netcool Configuration Manager SmartModel Drivers support version 6.4.0.0 has been successfully installed.

PRESS <ENTER> TO EXIT THE INSTALLER:

3. Start the components.

```
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

4. Change the SmartModel drivers from Standard to SmartModel mode.

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

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

```

SmartModel Upgrade
```

```

Enabled SmartModel mode for all drivers.
```

```
Your drivers will be dynamically reloaded automatically.
```

5. Remove the installation files.

```
cd /software/tncm
/bin/rm -R SM
```

```
/bin/rm NCM-6.4.2-Drivers19-SmartModel.zip
```

## Installing auto-discovery

1. Stop the components.

```
/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:
```

2. Enter **Intelliden** for the user and **object00** for the password. Click **OK**.



3. Expand the first installation file.

```
cd /software/tncm
mkdir auto
cd auto
tar -xvf ../ITNCM_Autodiscovery.tar
```

4. Expand the second installation file.

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



**Note:** The installation file is a tar file within a tar file.

5. Change the file permissions to allow autodiscovery to run.

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

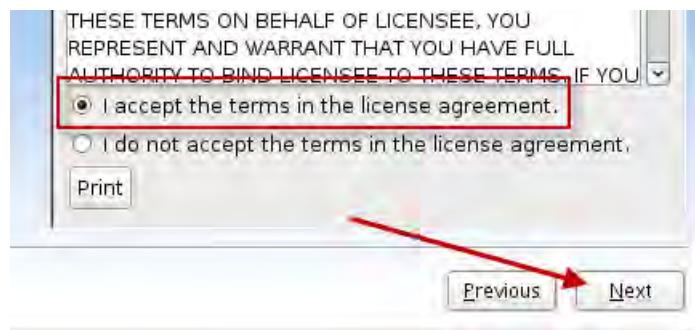
6. Run the installation utility.

```
./autodiscovery-aa85.bin LAX_VM /opt/IBM/ncm/jre/bin/java -i gui
```

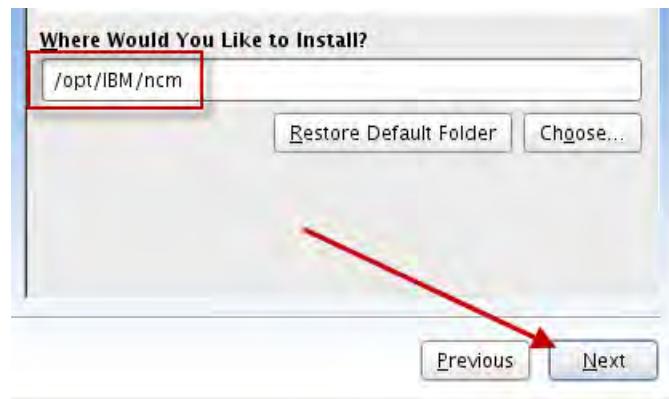
7. Click **Next**.



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



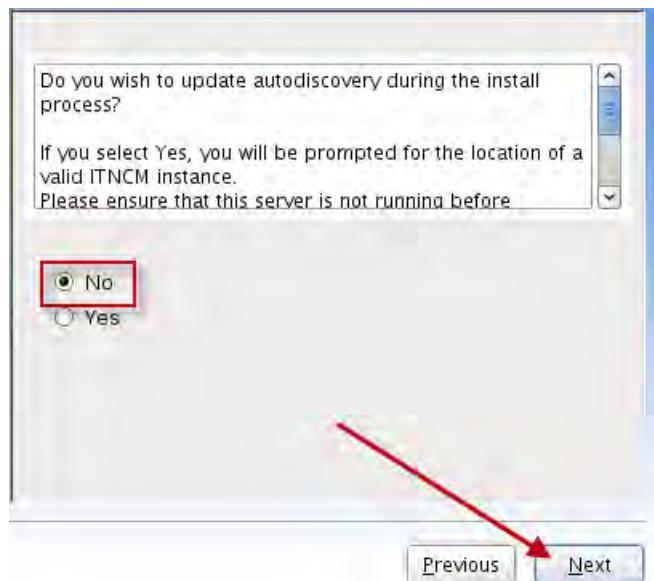
9. Accept the default folder, and click **Next**.



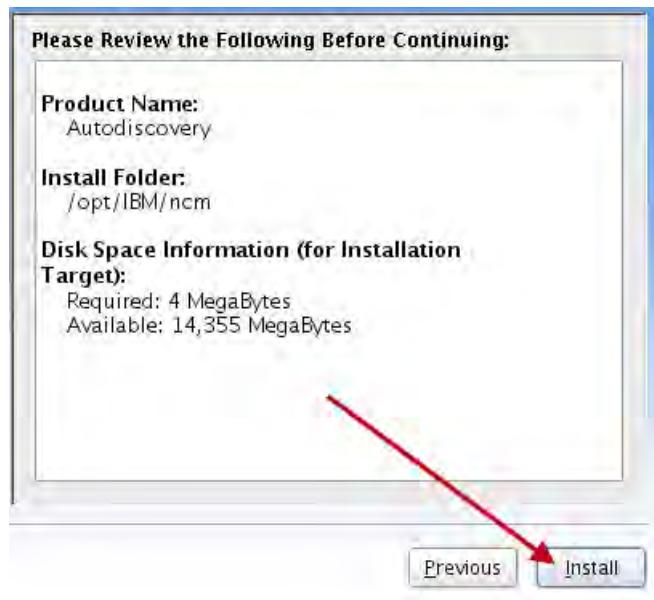
10. Ignore the warning message, and click **Continue**.



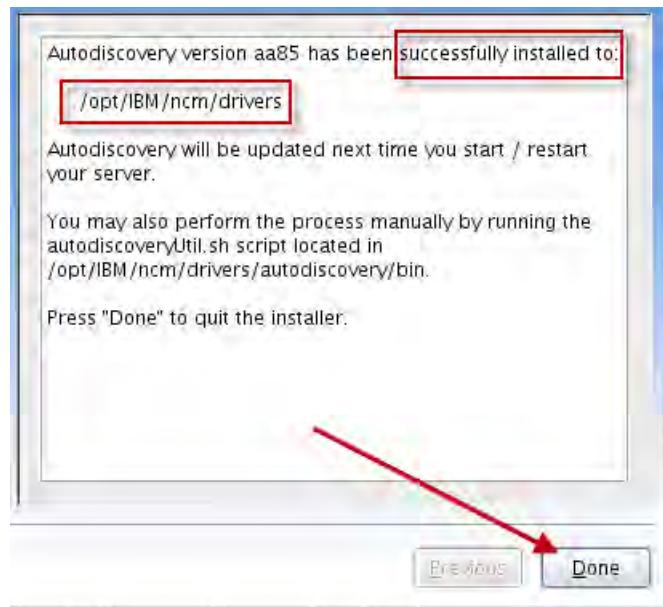
11. Accept the default, and click **Next**.



12. Click **Install**.



13. Verify that the installation is successful, and click **Done**.



14. Start the components.

```
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
```

## Exercise 6 Post-installation configuration

### Changing passwords

1. Open a Firefox browser.
2. Connect to the presentation server at the following URL.

<http://host1.csuite.edu:15310/security/login.jsp>



**Hint:** Use the bookmark that you created previously to open the URL for the presentation server.

3. Log in as user **Intelliden** with password **object00**.

The screenshot shows the Netcool Configuration Manager login page. It features a blue header with the Tivoli logo on the left and the IBM logo on the right. Below the header is a cartoon illustration of a person sitting at a desk with two monitors. The main area has a light blue background with the title "Netcool Configuration Manager". There are two input fields: "User Name:" containing "Intelliden" and "Password:" containing "\*\*\*\*\*". A "Login" button is located on the right side of the form.

4. Click Account Management.

The screenshot shows the Netcool Configuration Manager dashboard after logging in. The top navigation bar includes the Tivoli logo, a search bar, and a user status message "User: Intelliden, Logoff". Below the navigation is a horizontal menu bar with several items. The "Account Management" item is highlighted with a red rectangular box.

5. Under Users, click **administrator**.

The screenshot shows the "Accounts" section of the Netcool Configuration Manager interface. The left pane displays a tree view under "Account Administration" with "Groups" and "Users" expanded. Under "Groups", there are entries for "administrator", "observer", "operator", and "Super User Group". Under "Users", there are entries for "administrator", "Installer", and "Intelliden". The "administrator" entry under "Users" is selected and highlighted with a red rectangular box. The right pane shows a detailed view for "Modify User: administrator" with tabs for "General" and "Details".

6. Change the password to **object00**, and click **Save**.

The screenshot shows a user management interface with the following fields:

- User Name: administrator
- Remote User:
- Two Factor User:
- \*Password:  (highlighted with a red box)
- \*Validate Password:  (highlighted with a red box)
- First Name: administrator
- Middle Initial:
- \*Last Name: administrator
- \*E-mail: administrator
- Telephone Number:
- Identification:

At the bottom right are three buttons: Save, Remove, and Cancel. A red arrow points from the bottom right towards the Save button.

7. Repeat these steps for the remaining Users:

observer

operator

8. Click the *running man* icon to log out.



9. Close the Firefox browser.

## Configuring Java Webstart

The current version of IBM Java includes some security checks that cause Java Webstart to fail under certain conditions. To eliminate this issue, you must modify some Java property settings.

1. Change to the location of Java.

```
cd /opt/IBM/ncm/jre/bin
```

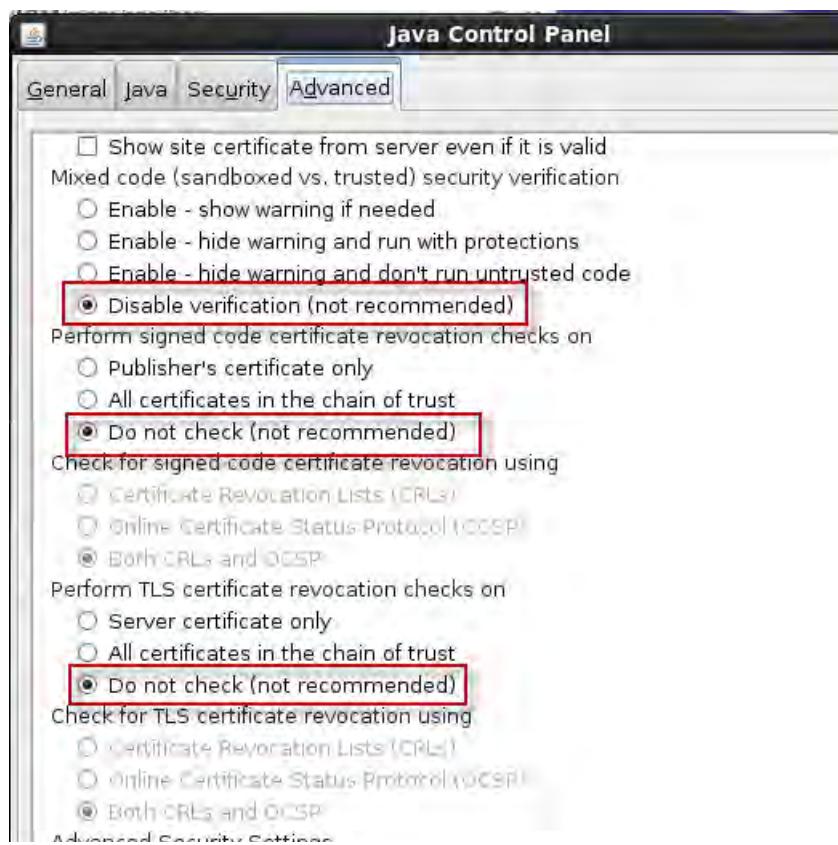
2. Open the Java control panel.

```
./ControlPanel
```

3. Click Advanced.



4. Select the **three** options as shown here.



5. Click OK to save the changes.



6. Change to the target directory.

```
cd /home/netcool/.java/deployment
```

7. Open the property file for edit.

```
gedit deployment.properties
```

8. Add the following line to the file.

```
deployment.expiration.check.enabled=false
```

9. Save the changes and exit the gedit utility.

The following steps configure the Firefox browser to run the Java Webstart application.

10. Open a Firefox browser.

11. Connect to the following URL:

<http://host1.csite.edu:15310/security/login.jsp>

12. Log in as **administrator** with password **object00**.



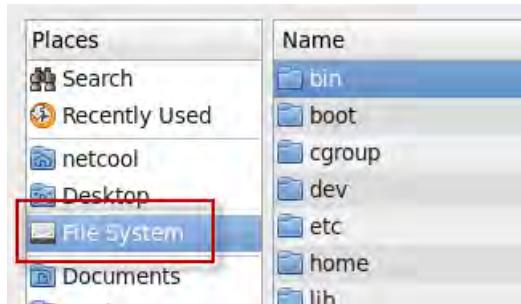
13. Select **ITNCM Webstart GUI**.



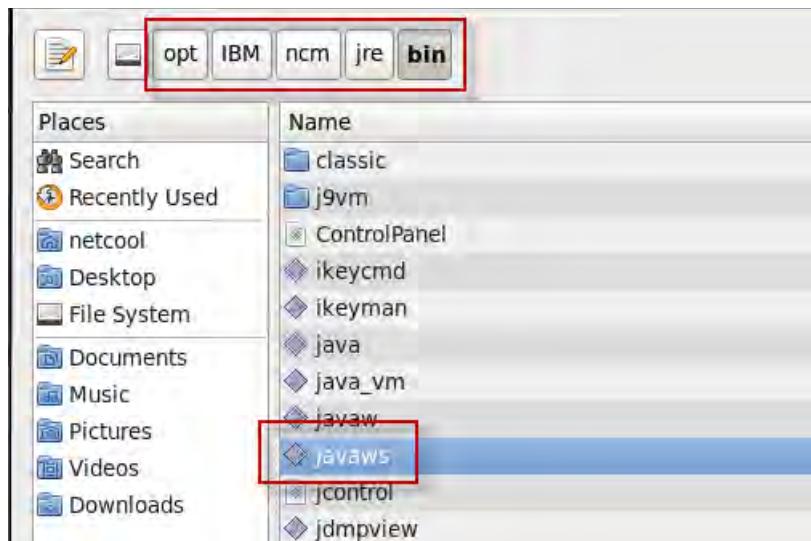
14. Click the arrow and select **Other**.



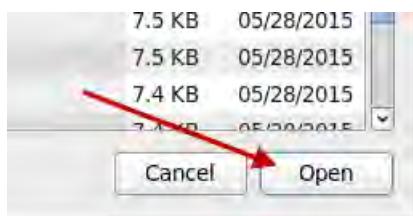
15. Click **File System**.



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



17. Click **Open**.



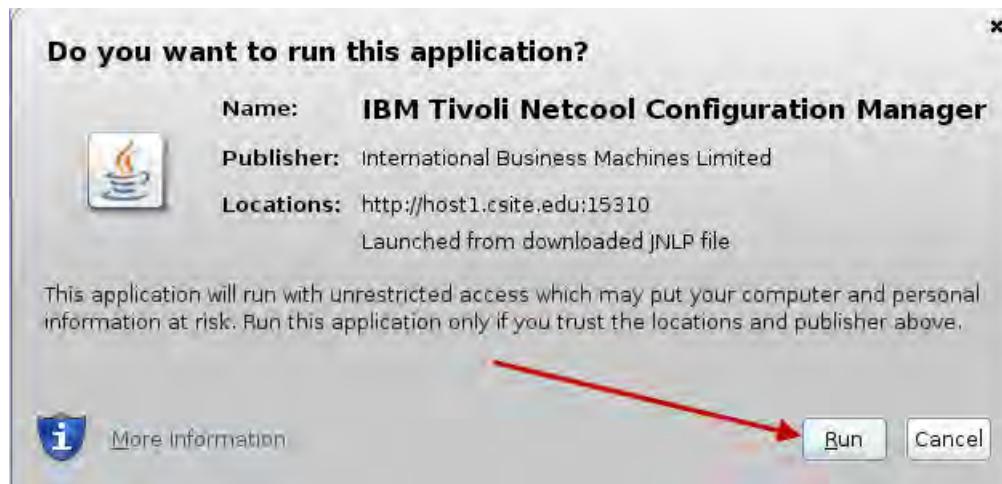
18. Select the option to do this automatically, and click **OK**.



19. Select the option to not ask again, and click **Continue**.



20. Click Run.



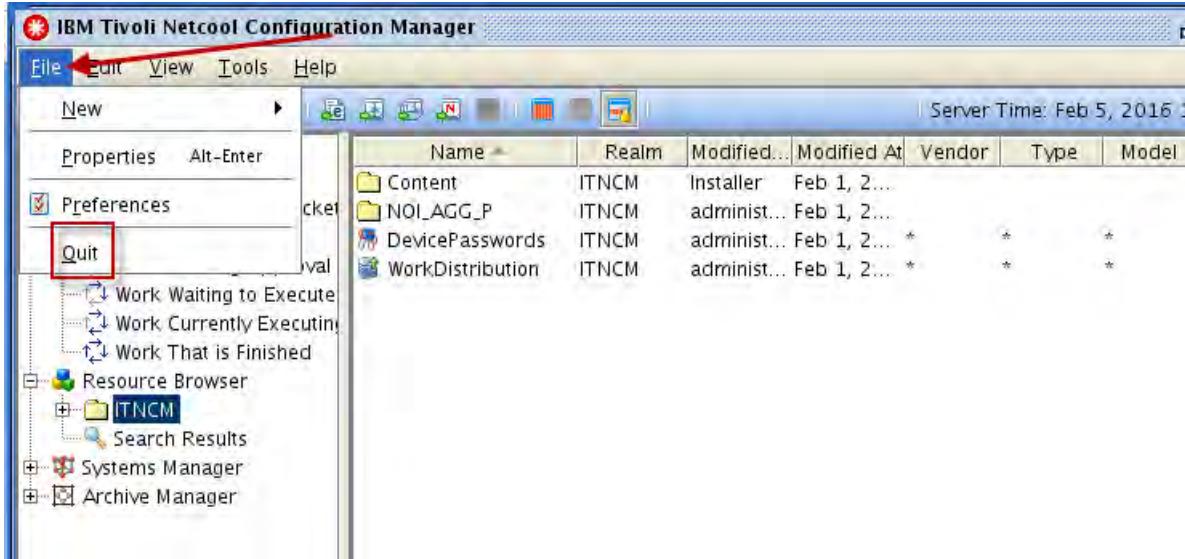
21. Select the option to not ask again, and click **Install**.



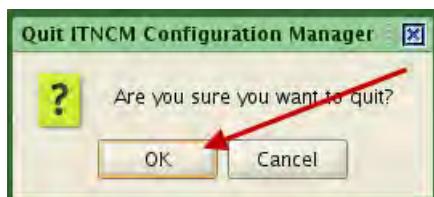
22. Enter **administrator** for the user name and **object00** for the password. Click **Login**.



23. Verify that the application opens correctly. Click **File** and select **Quit** to close the application.



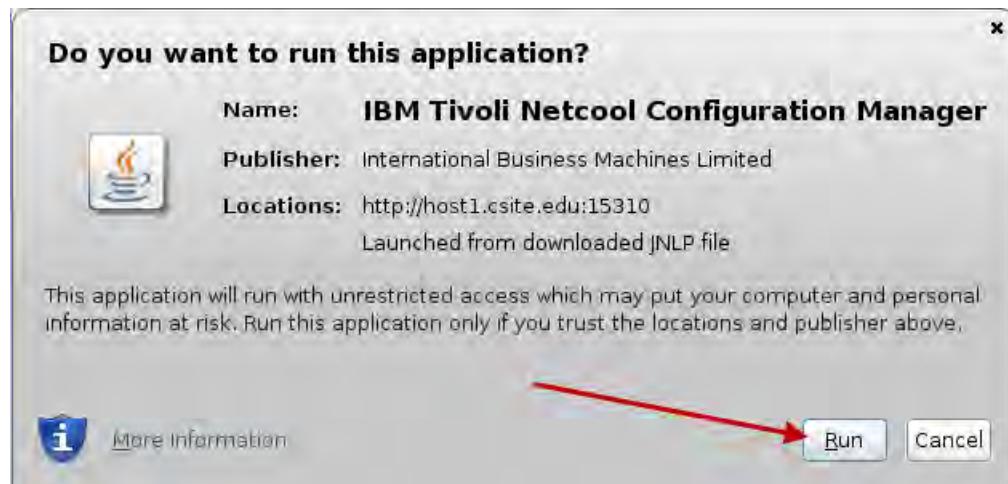
24. Click **OK** to confirm exit.



25. Click **ITNCM Compliance**.



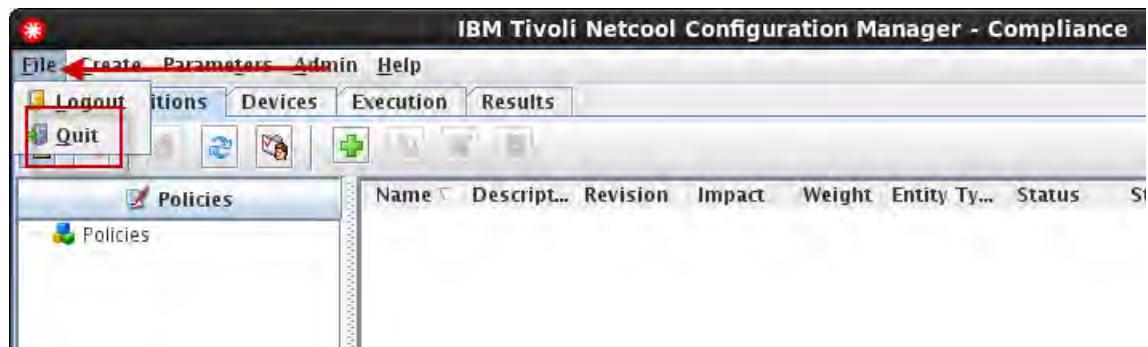
26. Click Run.



27. Enter **administrator** for the user name and **object00** for the password. Click **Login**.



28. Verify that the application loads correctly. Click **File** and select **Quit** to close the application.



29. Click **Yes** to confirm exit.



## Configuring SNMP trap destination

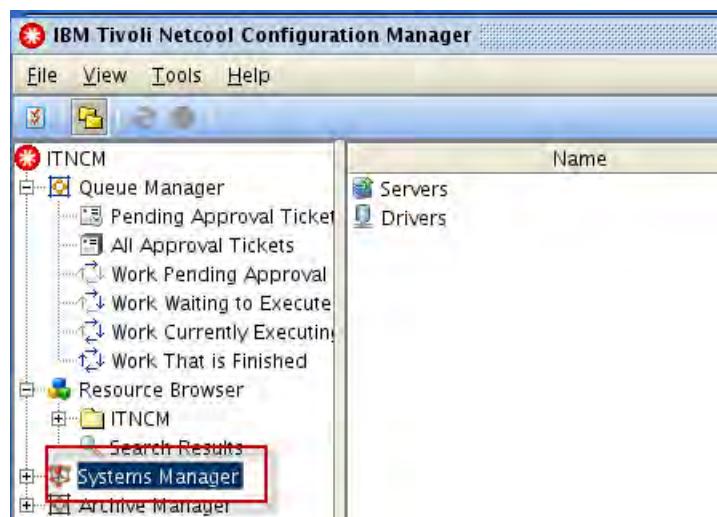
1. Click **ITNCM Webstart GUI**.



2. Enter **administrator** for the user name and **object00** for the password. Click **Login**.



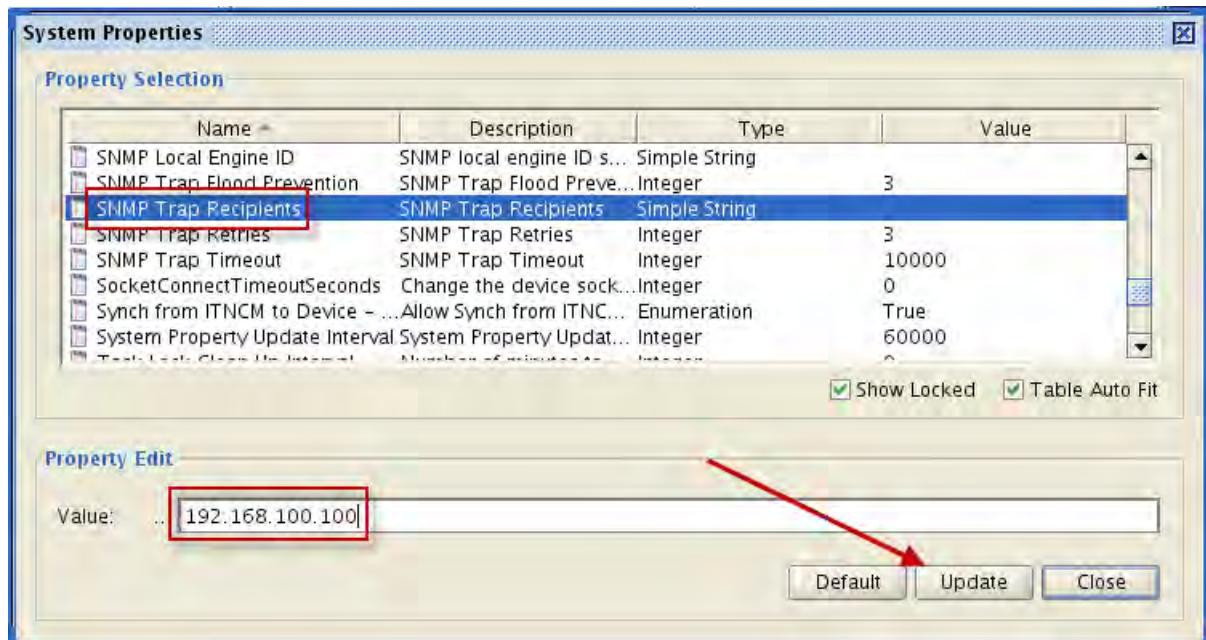
3. Click **Systems Manager** to select it.



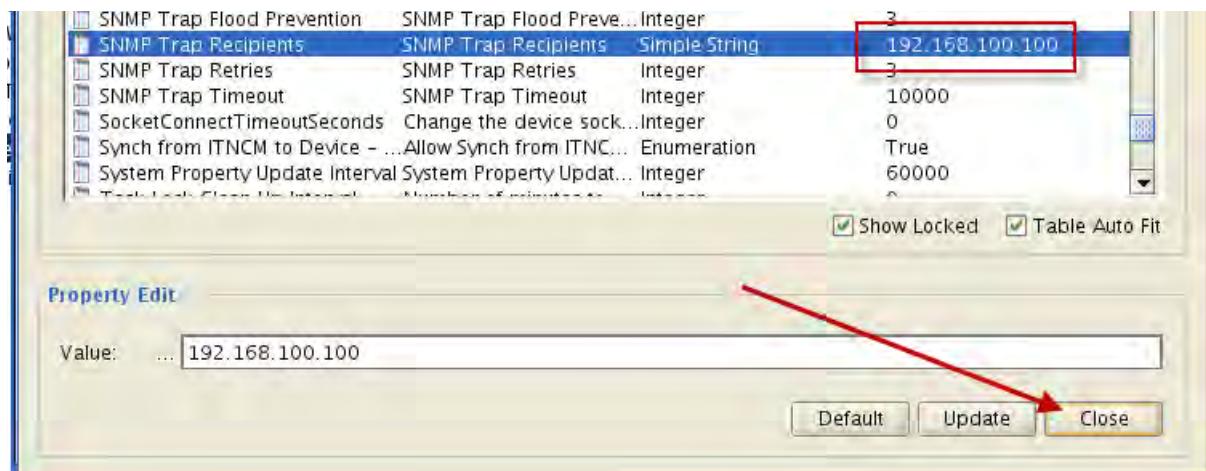
4. Click **Tools**, and select **System Properties**.



5. Click **SNMP Trap Recipients** to select it. Enter **192.168.100.100** for the value. Click **Update**.



6. Verify that the value is correct. Click **Close**.



## Updating the Work Distribution resource

- Determine the value for the Server ID.

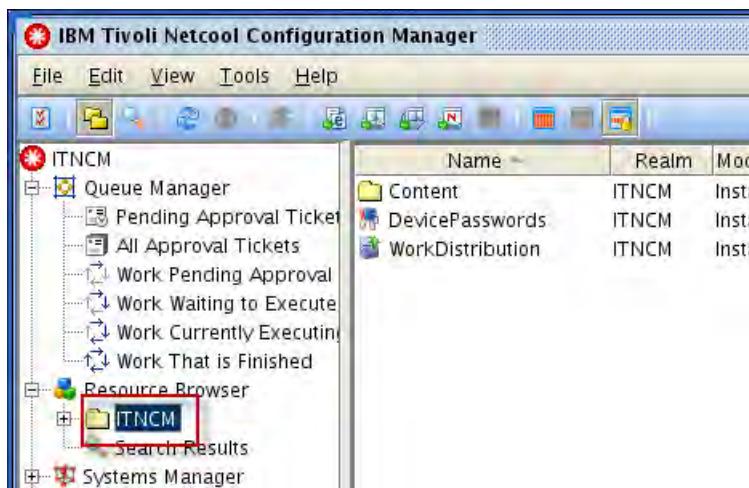
```
cat /opt/IBM/ncm/ITNCM.properties | grep ServerName
```

AdminManager/ServerName=Worker1

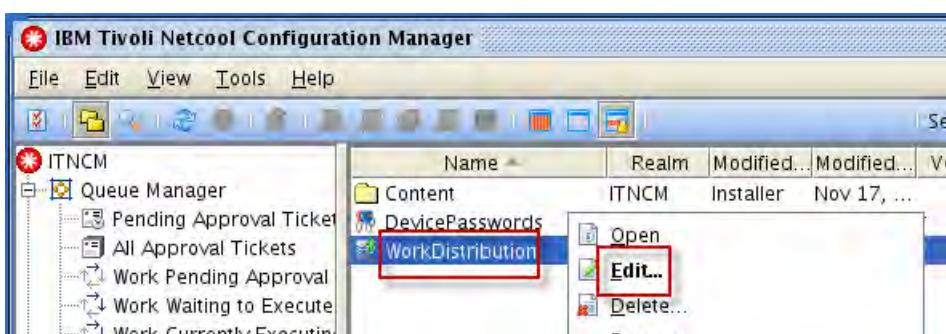


**Note:** The value for the Server ID is defined during installation of Netcool Configuration Manager.

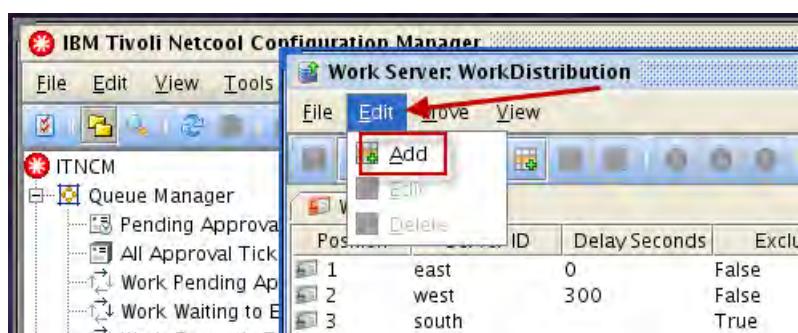
- Under Resource Browser, click ITNCM to select it.



- Click WorkDistribution to select it, right-click and select Edit.



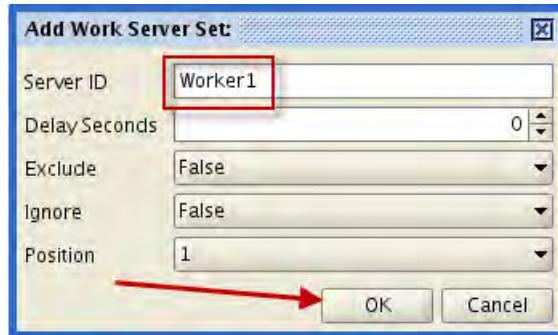
- Click Edit and select Add.



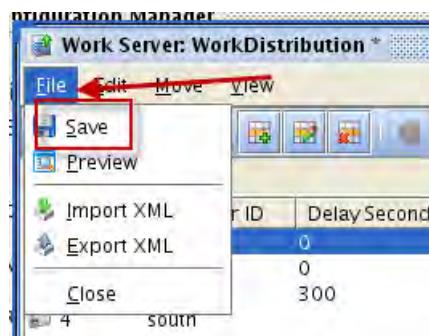


**Note:** None of the current entries are required. You can select one of the existing ones and modify it or create a new entry.

5. Enter **Worker1** and click **OK**.



6. Click **File** and select **Save**.

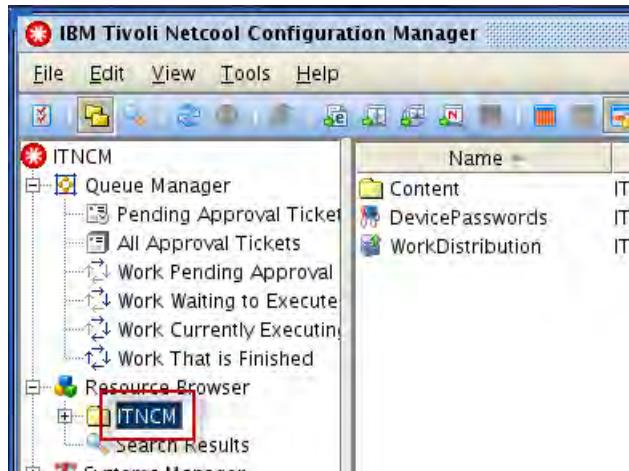


7. Click **File** and select **Close**.

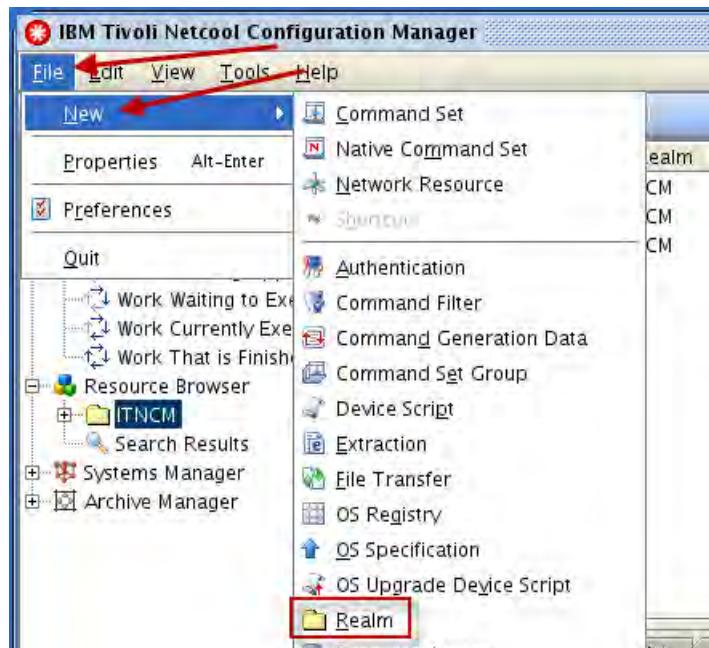
## Creating resources to support device import

The following steps configure various Netcool Configuration Manager objects that are used for device import.

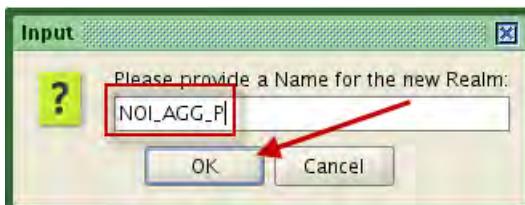
- Under **Resource Browser**, click **ITNCM** to select it.



- Click **File**, **New**, and select **Realm**.



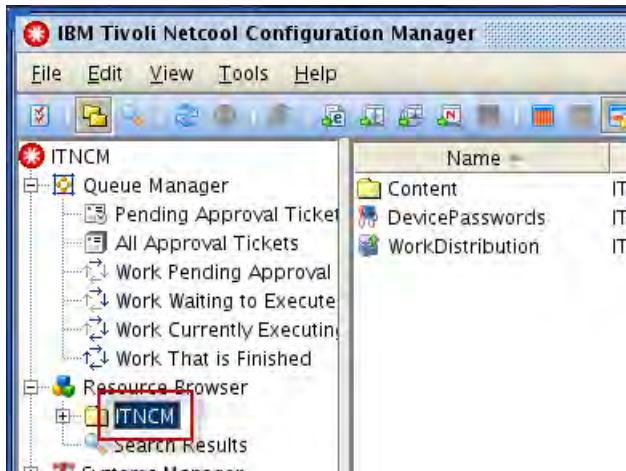
- Enter **NOI\_AGG\_P** for the realm name and click **OK**.



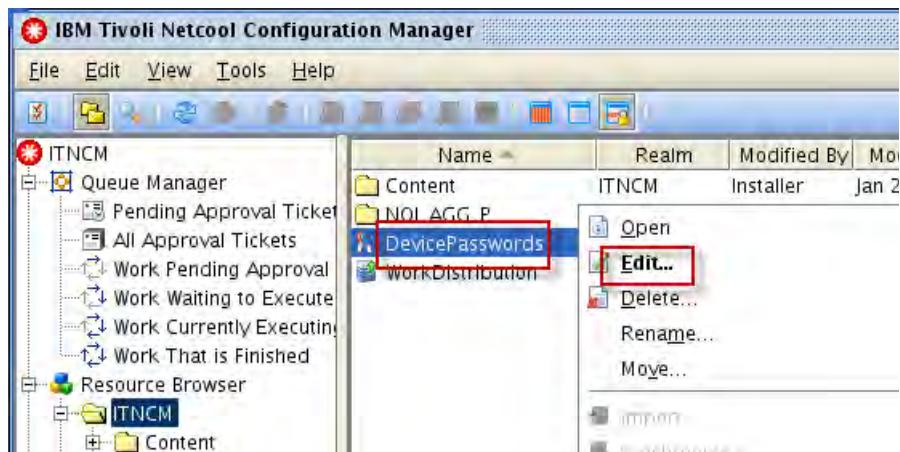


**Hint:** The realm name can be any valid value. If you use the same value as the Network Manager domain name, it can potentially avoid confusion.

- Under Resource Browser, click ITNCM to select it.

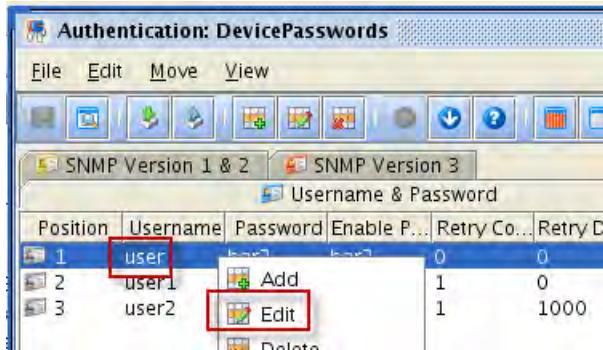


- Click DevicePasswords to select it, right-click and select Edit.



**Important:** The following steps describe how to configure access credentials for devices that Netcool Configuration Manager manages. The values that are used in the exercise are unique to the class environment.

6. Click the entry for **user** to select it, right-click and select **Edit**.



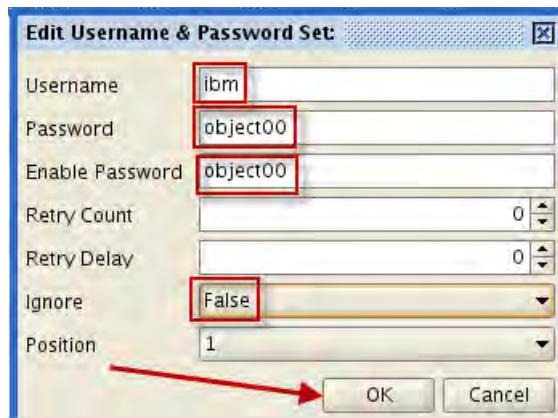
7. Enter the following values, and click **OK**.

Username: **ibm**

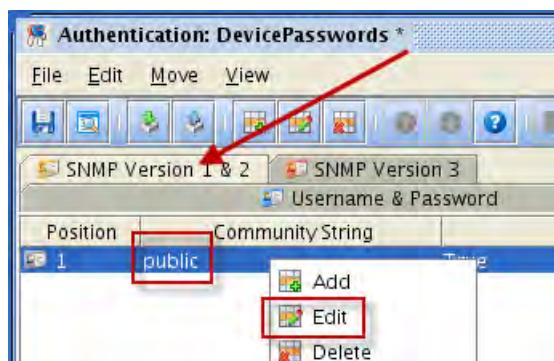
Password: **object00**

Enable Password: **object00**

Ignore: **False**



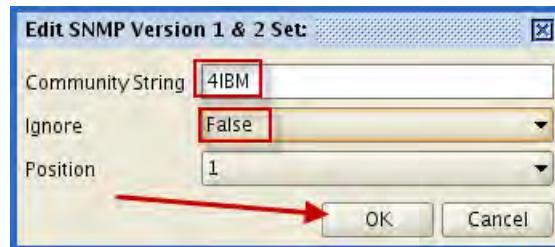
8. Click the SNMP Version 1 & 2 tab. Click the entry for **public** to select it. Right-click and select **Edit**.



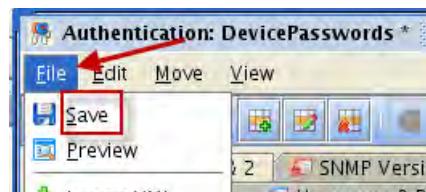
9. Enter the following values, and click **OK**.

Community String: **4IBM**

Ignore: **False**

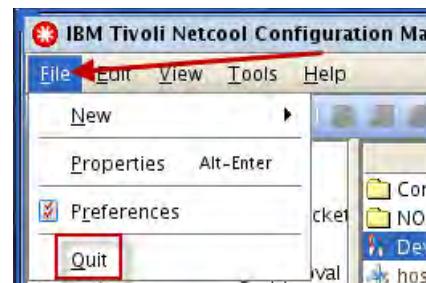


10. Click **File**, and select **Save**.



11. Click **File**, and select **Close**.

12. Click **File** and select **Quit** to exit the ITNCM client.



13. Click **OK** to confirm exit.

14. Click **Logoff**.



15. Close the Firefox browser.

# Exercise 7 Configuring integration with Tivoli Network Manager

In this step, you configure the integration between Tivoli Network Manager and Netcool Configuration Manager.

## Creating users and groups

Netcool Configuration Manager users and groups are currently defined in a file-based user repository in the presentation server. To configure single sign-on (SSO) between Dashboard Application Services Hub and Netcool Configuration Manager, you must create Netcool Configuration Manager users and groups in LDAP. In the following steps, you add the users and groups to LDAP, and then remove the file-base repository. In the last step, you configure the presentation server to use the LDAP repository.

1. Save copies of the Virtual Member Management configuration files.

- a. Save the Dashboard Application Services Hub file.

```
cd /opt/IBM/JazzSM/profile/config/cells/JazzSMNode01Cell/wim/config
```

```
cp wimconfig.xml /home/netcool/wimconfig.xml_dash
```

- b. Save the presentation server file.

```
cd /opt/IBM/JazzSM_ncm/profile/config/cells/JazzSMNode01Cell/wim/config
```

```
cp wimconfig.xml /home/netcool/wimconfig.xml_tncm
```



**Important:** If any of the following configuration steps fail, you can recover the original configurations by copying the saved files back to the original locations, and restarting Dashboard Application Services Hub, and the presentation server.

2. Open a Firefox browser.
3. Log in to Dashboard Application Services Hub as **smadmin** with password **object00**.

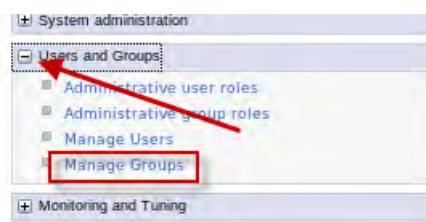
4. Click the icon and select **WebSphere Administrative Console**.



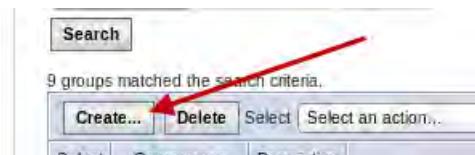
5. Click **Launch WebSphere administrative console**.



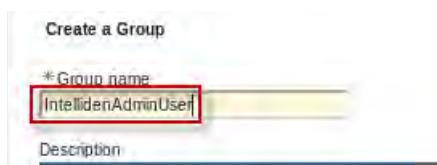
6. Expand **Users and Groups**. Select **Manage Groups**.



7. Click **Create**.



8. Enter **IntellidenAdminUser** for the name, click **Create**.



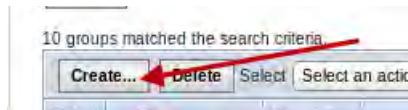


**Important:** Enter the group name exactly as shown.

9. Click **Close**.



10. Click **Create**.



11. Enter **IntellidenUser** for the name, click **Create**.

\* Group name  
 IntellidenUser

Description

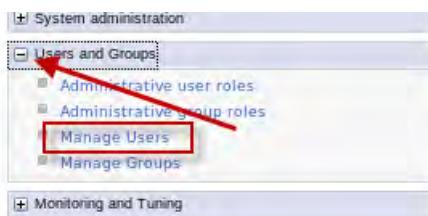


**Important:** Enter the group name exactly as shown.

12. Click **Close**.



13. Expand **Users and Groups**. Select **Manage Users**.



14. Click **Create**.



15. Create a user as follows.

- Enter **Intelliden** for the user ID.
- Enter **TNCM Super** for the first name, and **User** for the last name.
- Enter **object00** for the password.
- Click **Group Membership**.

Create a User

\*User ID: Intelliden

\*First name: TNCM Super

\*Last name: User

E-mail:

\*Password: \*\*\*\*\*

\*Confirm password: \*\*\*\*\*

Group Membership

16. Click **Search**.

Search by

\* Search for

\* Maximum results

Group name

100

Search

17. Select **IntellidenAdminUser** and click **Add**.

Search by

\* Search for

\* Maximum results

Group name

100

Search

Mapped To

< Add

Available

- ImpactAdmin
- IntellidenAdminUser
- Netcool\_Admin
- Netcool\_User

18. Select **IntellidenUser** and click **Add**. Click **Close**.

Search by

\* Search for

\* Maximum results

Group name

100

Search

Mapped To

IntellidenAdminUser

< Add

Available

- ImpactAdmin
- IntellidenUser
- Netcool\_Admin
- Netcool\_User

19. Click **Create**.

20. Click **Create Like**.



21. Create a user as follows.

- Enter **administrator** for the user ID.
- Enter **TNCM Admin** for the first name, and **User** for the last name.
- Enter **object00** for the password.
- Click **Create**.

The screenshot shows a user creation form. The fields are as follows:

- \* User ID: administrator
- \* First name: TNCM Admin
- \* Last name: User
- E-mail: (empty)
- \* Password: object00
- \* Confirm password: object00

At the bottom are two buttons: **Create** and **Cancel**. Red arrows point from the text instructions above to the User ID, First name, Last name, and Password fields.

**Hint:** The **administrator** user is assigned to the same groups by using the Create Like feature.

22. Click **Close**.



23. Click **Create**.



24. Create a user as follows.

- Enter **observer** for the user ID.
- Enter **TNCM Observer** for the first name, and **User** for the last name.
- Enter **object00** for the password.

d. Click **Group Membership**.

A user creation form with fields for User ID (observer), First name (TNCM Observer), Last name (User), E-mail, Password, and Confirm password. A red arrow points to the 'Group Membership' button.

25. Click **Search**.

A search interface with fields for Search by (Group name), Search for (\*), and Maximum results (100). A red arrow points to the 'Search' button.

26. Select **IntellidenUser** and click **Add**. Click **Close**.

A search results interface showing 'Available' users: ImpactAdmin, IntellidenAdminUser, IntellidenUser, Netcool\_Admin, and Netcool\_User. A red arrow points to the '< Add' button.

27. Click **Create**.

28. Click **Create Like**.



29. Create a user as follows.

- Enter **operator** for the user ID.
- Enter **TNCM Oper** for the first name, and **User** for the last name.
- Enter **object00** for the password.

d. Click **Create**.

The screenshot shows a user creation form. The fields are labeled as follows: \*User ID (operator), \*First name (TNCM Oper), \*Last name (User), E-mail (empty), Password (redacted), \*Confirm password (redacted). At the bottom are 'Create' and 'Cancel' buttons, with a red arrow pointing to the 'Create' button.



**Hint:** The **operator** user is assigned to the same groups by using the Create Like feature.

30. Click **Close**.



## Adding existing users to Netcool Configuration Manager groups

In the following steps, you add existing users to Netcool Configuration Manager groups. After you add the users, the users have access to Netcool Configuration Manager features.

1. Expand **Users and Groups**. Select **Manage Groups**.



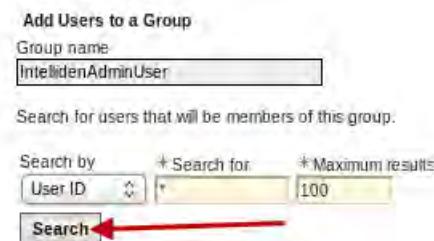
2. Select **IntellidenAdminUser**.

11 groups matched the search criteria.			
Select	Group name	Description	
<input type="checkbox"/>	ImpactAdmin	cn=ImpactAd	
<input type="checkbox"/>	IntellidenAdminUser	cn=Intelliden.	
<input type="checkbox"/>	IntellidenUser	cn=Intelliden	

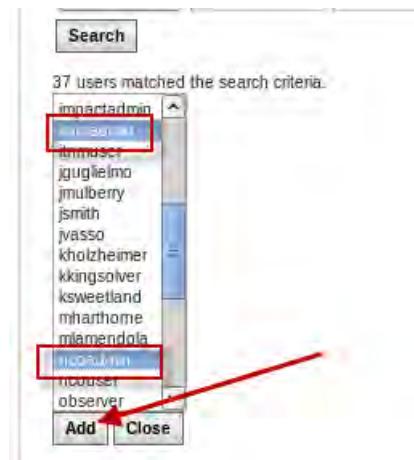
3. Select the Members tab. Click Add Users.



4. Click Search.

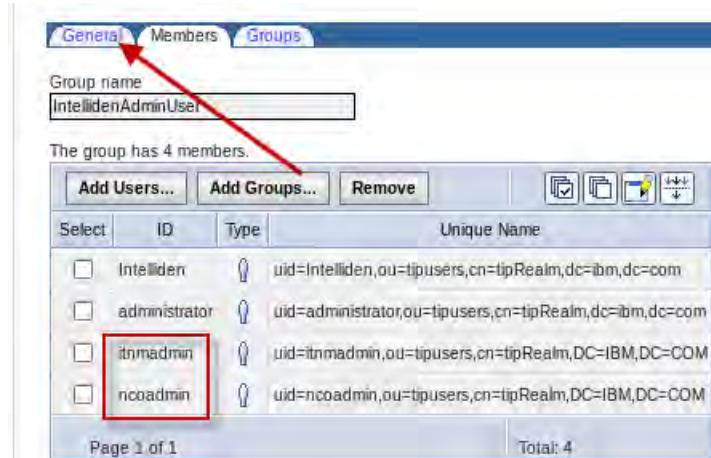


5. Select **itnadmin**. Hold the *Ctrl* key and select **ncoadmin**, and click **Add**.



6. Click Close.

7. Verify that the user names appear, and click General.



8. Click OK to save the group changes.

9. Select **IntellidenUser**.

11 groups matched the search criteria.

Select	Group name	Description
<input type="checkbox"/>	ImpactAdmin	cn=ImpactAdmin,ou=tppro
<input type="checkbox"/>	IntellidenAdminUser	cn=IntellidenAdminUser,ou=tppro
<input type="checkbox"/>	IntellidenUser	cn=IntellidenUser,ou=tppro

10. Select the Members tab. Click **Add Users**.

General Members Groups

Group name  
IntellidenUser

The group has 4 members.

Add Users... Add Groups... Remove



11. Click **Search**.

Add Users to a Group

Group name  
IntellidenUser

Search for users that will be members of this group.

Search by \* Search for \* Maximum results  
User ID \* 100

Search

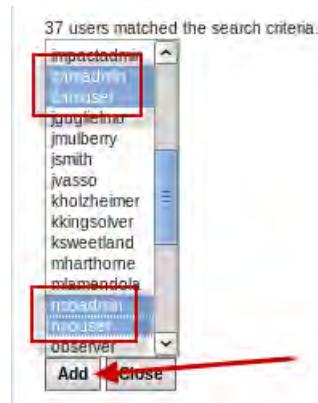


12. Select **itnmadmin**. Hold the Ctrl key and select **itnmuser**. Hold the Ctrl key and select **ncoadmin**. Hold the Ctrl key and select **ncouser**, and click **Add**.

37 users matched the search criteria.

ImpactAdmin
itadmin
itmuser
itngilman
jmulberry
jsmith
javasso
kholzheime
kkingsolver
ksweetland
mharthome
mlamendola
ntnadmin
ntnuser
ooserver

Add Close



13. Click **Close**.

14. Verify that the user names are shown, and click General.

The screenshot shows a list of users under the 'General' tab of a group named 'IntellidenUser'. The 'itnmadmin' user is selected and highlighted with a red box. The list includes:

Select	ID	Type	Unique Name
<input type="checkbox"/>	Intelliden		uid=Intelliden,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
<input type="checkbox"/>	administrator		uid=administrator,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
<input checked="" type="checkbox"/>	itnmadmin		uid=itnmadmin,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
<input type="checkbox"/>	itnmuser		uid=itnmuser,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
<input type="checkbox"/>	ncoadmin		uid=ncoadmin,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
<input type="checkbox"/>	ncouser		uid=ncouser,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
<input type="checkbox"/>	observer		uid=observer,ou=tipusers,cn=tipRealm,dc=ibm,dc=com
<input type="checkbox"/>	operator		uid=operator,ou=tipusers,cn=tipRealm,dc=ibm,dc=com

15. Click **OK** to save the group changes.

16. Log out of WebSphere administrative console.

## Assigning roles in Dashboard Application Services Hub

In the following steps, you assign Netcool Configuration Manager roles to the groups that you created in the previous step.

1. Click the tab to select Dashboard Application Services Hub.
2. Click the icon and select **Group Roles**.



3. Enter **Intelliden\*** and click **Search**.

The screenshot shows a search interface with a 'Group ID' input field containing 'Intelliden\*'. Below it is a 'Number of results to display' dropdown set to 20. A large red arrow points to the 'Search' button at the bottom.

4. Select **IntellidenAdminUser**.

Group Name	Role
IntellidenAdminUser	
IntellidenUser	

5. Select the following roles, and click **Save**.

IntellidenAdminUser  
IntellidenUser  
ncmActivityViewing  
ncmConfigChange  
ncmConfigEdit  
ncmConfigSynch  
ncmConfigViewing  
ncmDashService  
ncmIDTUser  
ncmPolicyCheck

6. Verify that the roles appear as follows.

Group Name	Roles
IntellidenAdminUser	IntellidenAdminUser, ncmConfigChange, ncmConfigEdit, ncmConfigSynch, ncmDashService, IntellidenUser, ncmIDTUser, ncmPolicyCheck, ncmActivityViewing, ncmConfigViewing

7. Select **IntellidenUser**.

IntellidenAdminUser	IntellidenAdminUser, ncmConfigChange, ncmDashService, IntellidenUser, ncmIDTUser, ncmPolicyCheck, ncmActivityViewing, ncmConfigViewing
IntellidenUser	

8. Select the following roles, and click **Save**.

IntellidenUser  
ncmActivityViewing  
ncmConfigViewing  
ncmDashService

9. Verify that the roles appear as follows.

IntellidenAdminUser	IntellidenAdminUser, ncmConfigChange, ncmConfigEdit, ncmConfigSynch, ncmDashService, IntellidenUser, ncmIDTUser, ncmPolicyCheck, ncmActivityViewing, ncmConfigViewing
IntellidenUser	ncmDashService, IntellidenUser, ncmActivityViewing, ncmConfigViewing

10. Log out of Dashboard Application Services Hub.

11. Close the Firefox browser.

## Configuring the presentation server to use LDAP

In the following steps, you configure the presentation server to use the LDAP repository. In the last step, you remove the file-based repository from the presentation server.

1. Open a Firefox browser.
2. Connect to the following URL:  
<https://host1.csite.edu:15316/ibm/console/logon.jsp>
3. Accept all of the security warnings.
4. Log in as **Intelliden** with password **object00**.



**Important:** This application is the WebSphere administrative console for the Netcool Configuration Manager presentation server.

5. Adding the LDAP directory as a user repository.
  - a. Expand **Security** and click **Global Security**.



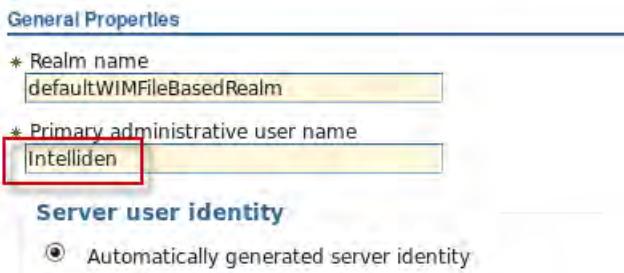
- b. Scroll down on the page to the *User account repository* section, click the arrow, and select **Federated repositories**.



- c. Click **Configure**.



- d. Change the user name to **Intelliden**.

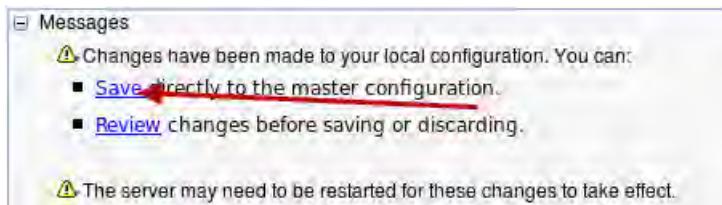


- e. Scroll to the bottom of the page and click **Apply**.

- f. Enter **object00** for the password, and click **OK**.



g. Click **Save**.



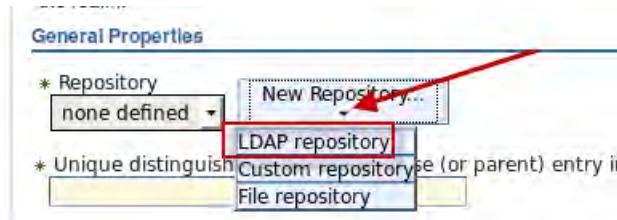
h. Scroll down on the page to the *Repositories in the realm*, and click **Add repositories**.

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

[Add repositories \(LDAP, custom, etc\)...](#)
[Use built-in repository](#)
[Remove](#)

i. Click **New Repository** and select **LDAP repository**.



j. Change the repository identifier to **TIVIDS**.

k. Set the primary host name to **host1.csite.edu**.

l. Verify that the port is set to **389**.

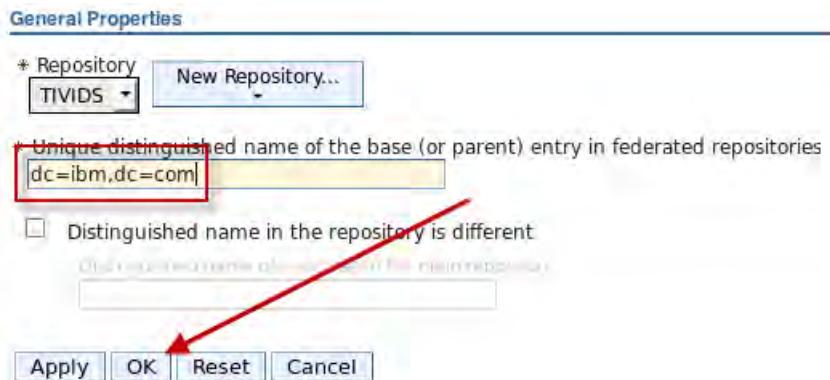
m. Set the **Bind distinguished name** field to **cn=root**.

n. Set the **Bind password** field to **object00**.

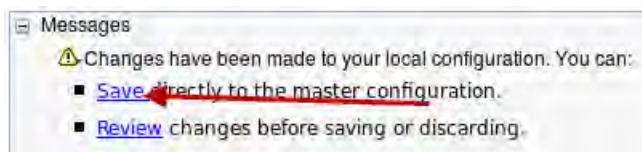
o. Scroll to the bottom of the page and click **OK**.

<b>General Properties</b>	
* Repository identifier <input style="width: 100%;" type="text" value="TIVIDS"/>	
Repository adapter class name <input type="text" value="com.ibm.ws.wim.adapter.ldap.LdapAdapter"/>	
<b>LDAP server</b>	
* Directory type <input type="text" value="IBM Tivoli Directory Server"/>	
* Primary host name <input type="text" value="host1.csite.edu"/>	
	Port <input type="text" value="389"/>
Failover server used when primary is not available: <input type="text"/>	
<b>Security</b>	
Bind distinguished name <input type="text" value="cn=root"/>	
Bind password <input type="password" value="*****"/>	
Federated repository properties for login <input type="text" value="uid"/>	
LDAP attribute for Kerberos principal name <input type="text"/>	

- p. Enter **dc=ibm,dc=com** for the Unique distinguished name field, and click **OK**.



- q. Click **Save**.



**Important:** The base entry is mapped to the root of the LDAP directory. All operations are completed as root, which causes errors on most LDAP servers. More configuration is required.

The next step is to 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 Netcool user information is located.

6. Defining LDAP object class mappings.  
a. Scroll down on the page and click **TIVIDS**.

Repositories in the realm:			
Add repositories (LDAP, custom, etc)...		Use built-in repository	Remove
Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
<input type="checkbox"/>	<a href="#">dc=ibm,dc=com</a>	<a href="#">TIVIDS</a>	LDAP:IDS
<input type="checkbox"/>	<a href="#">o=defaultWIMFileBasedRealm</a>	InternalFileRepository	File

- b. Scroll down and click **Federated repositories entity types to LDAP object classes mapping**.

Additional Properties

- Performance
- Federated repositories entity types to LDAP object classes mapping
- Federated repositories property names to LDAP attributes mapping
- Group attribute definition



**Important:** The following steps are unique to the configuration of the classroom LDAP server. The steps that are shown here are relevant to the LDAP configuration that is used for the class. The process is the same regardless of the LDAP configuration. The values that are used in these steps are different for another LDAP server.

- c. Click **Group**.

Select	Entity Type	Object Classes
You can administer the following resources:		
<input type="checkbox"/>	<a href="#">Group</a>	groupOfNames
<input type="checkbox"/>	<a href="#">OrgContainer</a>	organization;organizationalUnit;domain;container
<input type="checkbox"/>	<a href="#">PersonAccount</a>	inetOrgPerson

- d. Enter **ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM** for **Search bases** and click **OK**.

General Properties

\* Entity type:

\* Object classes:

Search bases:  (highlighted)

Search filter:

- e. Click **OrgContainer**.

Select	Entity Type	Object Classes
You can administer the following resources:		
<input type="checkbox"/>	<a href="#">Group</a>	groupOfNames
<input type="checkbox"/>	<a href="#">OrgContainer</a>	organization;organizationalUnit;domain;container
<input type="checkbox"/>	<a href="#">PersonAccount</a>	inetOrgPerson

- f. Verify that the **Search bases** field is empty and click **OK**.

**General Properties**

* Entity type	OrgContainer
* Object classes	organization;organizationalUnit;domain;container
Search bases	
Search filter	

- g. Click **PersonAccount**.

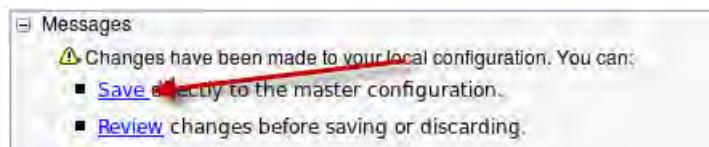
Select	Entity Type	Object Classes
You can administer the following resources:		
<input type="checkbox"/>	<a href="#">Group</a>	groupOfNames
<input type="checkbox"/>	<a href="#">OrgContainer</a>	organization;organizationalUnit;domain;container
<input type="checkbox"/>	<a href="#">PersonAccount</a>	inetOrgPerson

- h. Enter **ou=tipusers,cn=tipRealm,DC=IBM,DC=COM** for the **Search bases** field and click **OK**.

**General Properties**

* Entity type	PersonAccount
* Object classes	inetOrgPerson
Search bases	ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
Search filter	

- i. Click **Save**.



Now the Virtual Member Manager is configured to retrieve user information from a specific subtree within LDAP.

The next step is to configure Dashboard Application Services Hub 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 a new user or group is created.

7. Configure IBM Dashboard Application Services Hub to write to LDAP as follows:
  - a. Click **Federated repositories**.

**Global security > Federated repositories > TIVIDS > Federated repositories and classes mapping**

Use this page to list federated repositories entity types that are supported by the LI entity type to view or change its configuration properties, or to add or remove the entity type.

- b. Scroll to the bottom of the page and click **Supported entity types**.

**Additional Properties**

- [Property extension repository](#)
- [Entry mapping repository](#)
- **Supported entity types**
- [User repository attribute](#)

**Related Items**

- [Manage repositories](#)
- [Trusted authentication realms - inbound](#)

- c. Click **Group**.

Entity Type	Base Entry for the Default Parent	Relative Distinguished Name
You can administer the following resources:		
<a href="#">Group</a>	<a href="#">o=defaultWIMFileBasedRealm</a>	cn
<a href="#">OrgContainer</a>	<a href="#">o=defaultWIMFileBasedRealm</a>	o;ou;dc;cn
<a href="#">PersonAccount</a>	<a href="#">o=defaultWIMFileBasedRealm</a>	uid



**Important:** Observe the values in the table that say `o=defaultWIMFileBasedRealm`. In the present state, if a new user is added to Dashboard Application Services Hub, an attempt is made to write the entry to the file-based repository.

- d. Enter `ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM` for **Base entry for the default parent** and click **OK**.

**General Properties**

\* Entity type

\* Base entry for the default parent

\* Relative Distinguished Name properties

e. Click OrgContainer.

Entity Type	Base Entry for the Default Parent	Rel
You can administer the following resources:		
<a href="#">Group</a>	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn
<a href="#">OrgContainer</a>	o=defaultWIMFileBasedRealm	o;o
<a href="#">PersonAccount</a>	o=defaultWIMFileBasedRealm	uid

f. Enter dc=ibm,dc=com for Base entry for the default parent and click OK.

General Properties

\* Entity type

\* Base entry for the default parent

\* Relative Distinguished Name properties

g. Click PersonAccount.

Entity Type	Base Entry for the Default Parent	Rel
You can administer the following resources:		
<a href="#">Group</a>	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn
<a href="#">OrgContainer</a>	dc=ibm,dc=com	o;o
<a href="#">PersonAccount</a>	o=defaultWIMFileBasedRealm	uid

h. Enter ou=tipusers,cn=tipRealm,DC=IBM,DC=COM for Base entry for the default parent and click OK.

General Properties

\* Entity type

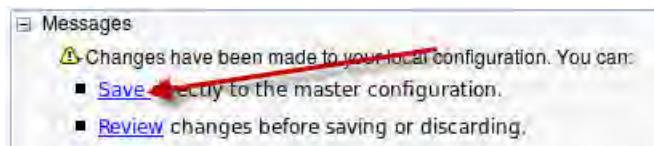
\* Base entry for the default parent

\* Relative Distinguished Name properties

The revised entries are listed as shown.

Entity Type	Base Entry for the Default Parent	Relative Distinguishing Name
You can administer the following resources:		
<a href="#">Group</a>	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn
<a href="#">OrgContainer</a>	dc=ibm,dc=com	o:objectCategory
<a href="#">PersonAccount</a>	ou=tipusers,cn=tipRealm,DC=IBM,DC=COM	uid

- i. Click **Save**.



## 8. Click **Federated repositories**.

**Global security**

[Global security](#) > [Federated repositories](#) > **Supported entity types**

Use this page to configure entity types that are supported by the member repositories.

[Preferences](#)

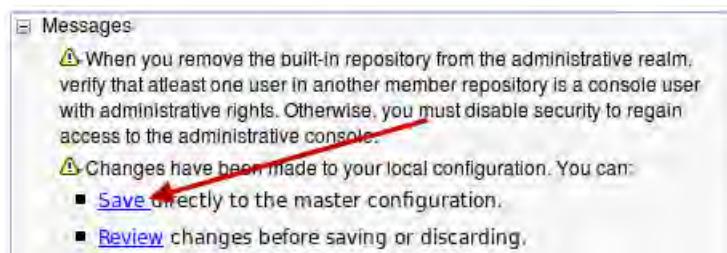
Entity Type	Base Entry for the Default Parent	Relative Distinguishing Name
<a href="#">Group</a>	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn

## 9. Select the entry for the file-based repository and click **Remove**.

Repositories in the realm:

Add repositories (LDAP, custom, etc)...	Use built-in repository	Remove	
Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
<input type="checkbox"/>	<a href="#">dc=ibm,dc=com</a>	TIVIDS	LDAP:IDS
<input checked="" type="checkbox"/>	<a href="#">o=defaultWIMFileBasedRealm</a>	InternalFileRepository	File

## 10. Click **Save**.



11. Click **Global security**.

The screenshot shows the 'Global security' page with a blue header bar. Below it, a red arrow points to the 'Federated repositories' link under the 'Global security > Federated repositories' heading. The text below explains federating repositories and mentions built-in and external repositories.

12. Click the arrow and select **Federated repositories**.

The screenshot shows the 'User account repository' page. A red arrow points to the 'Available realm definitions' dropdown menu, which contains 'Federated repositories'. Below the dropdown are 'Configure...' and 'Set as current' buttons.

13. Click **Set as current**.

The screenshot shows the 'User account repository' page again. A red arrow points to the 'Set as current' button, which is highlighted in blue.

14. Click **Apply**.

15. Click **Save**.

The screenshot shows a 'Messages' dialog box. A red arrow points to the 'Save' button, which is highlighted in blue. The dialog also contains other messages about saving changes and restarting the server.

16. Log out of the administrative console.

Leave the Firefox tab open. You use it again shortly.

17. Restart Netcool Configuration Manager.

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



Wait for the components to restart.

18. Return to WebSphere Integrated Solutions Console in the Firefox tab.

19. Log in as **Intelliden** with password **object00**.

20. Verify that the LDAP users are available within the presentation server.

- Expand **Users and Groups** and click **Manage Users**.

A screenshot of the WebSphere Integrated Solutions Console interface. The left sidebar shows a tree view with nodes like "Welcome", "Guided Activities", "Servers", "Applications", "Services", "Resources", "Security", "Environment", "System administration", and "Users and Groups". Under "Users and Groups", there are three sub-nodes: "Administrative user roles", "Administrative group roles", and "Manage Users". A red arrow points from the text above to the "Manage Users" node, which is highlighted with a red box. The right panel displays a "Welcome" message and a "Suite Name" section with "WebSphere Application Server" selected.

b. Observe the list of users.

The screenshot shows a table titled "User Management" with columns: Select, User ID, First name, Last name, E-mail, and Unique Name. A red box highlights the header row and the first three user entries. The first entry is "Intelliden TNCM Super". The second entry is "abraman Ariana Braman". The third entry is "administrator TNCM Admin".

Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	Intelliden	TNCM Super			uid=Intelliden,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	abraman	Ariana	Braman	abraman@ibm.com	cn=Ariana Braman,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	administrator	TNCM Admin			uid=administrator,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	aduring	Adeline	During	aduring@ibm.com	cn=Adeline During,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	bwinebarger	Bart	Winebarger	bwinebarger@ibm.com	cn=Bart Winebarger,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	dselan	Dick	Selan	dselan@ibm.com	cn=Dick Selan,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	eange	Earline	Ange	eange@ibm.com	cn=Earline Ange,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	elotempio	Emelda	Lotempio	elotempio@ibm.com	cn=Emelda Lotempio,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	ezegarelli	Else	Zegarelli	ezegarelli@ibm.com	cn=Else Zegarelli,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM

c. Expand **Users and Groups** and click **Manage Groups**.



d. Observe the list of groups.

The screenshot shows a table titled "Group Management" with columns: Select, Group name, Description, and Unique Name. A red box highlights the header row and the first three group entries. The first entry is "ISQLWrite". The second entry is "ImpactAdmin". The third entry is "IntellidenAdminUser".

Select	Group name	Description	Unique Name
<input type="checkbox"/>	ISQLWrite		cn=ISQLWrite,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	ImpactAdmin		cn=ImpactAdmin,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	IntellidenAdminUser		cn=IntellidenAdminUser,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	IntellidenUser		cn=IntellidenUser,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	Netcool_Admin		cn=Netcool_Admin,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	Netcool_User		cn=Netcool_User,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	Network_Manager_IP_Admin		cn=Network_Manager_IP_Admin,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	Network_Manager_User		cn=Network_Manager_User,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	Normal		cn=Normal,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	System		cn=System,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	UnityAdmins		cn=UnityAdmins,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	UnityUsers		cn=UnityUsers,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	WPAdministrators		cn=WPAdministrators,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM

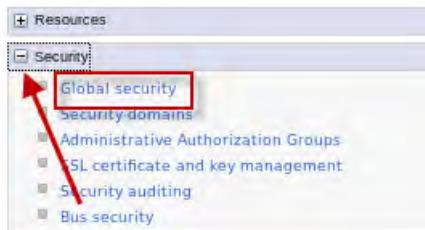
The Netcool Configuration Manager presentation server is configured to use the LDAP repository.

## Configuring the presentation server for single sign-on

You exported LTPA keys from Dashboard Application Services Hub in a previous unit. In the following steps, you import those keys into the presentation server. Then, you enable single sign-on in the presentation server.

You are currently logged in to WebSphere administrative console as the **Intelliden** user.

1. Expand **Security** and select **Global security**.



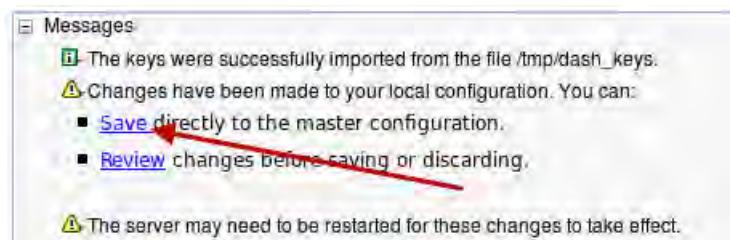
2. Click **LTPA**.

A screenshot of the 'Global security' configuration page. Under 'Administrative security', there is a checked checkbox for 'Enable administrative security'. On the right side, under 'Authentication', there is a section titled 'Authentication mechanisms' with two radio buttons: 'LTPA' (which is selected) and 'Kerberos and LTPA'. Below these buttons are links for 'LTPA configuration' and 'Kerberos configuration'. A red arrow points from the 'LTPA' button to the 'Import keys' step below.

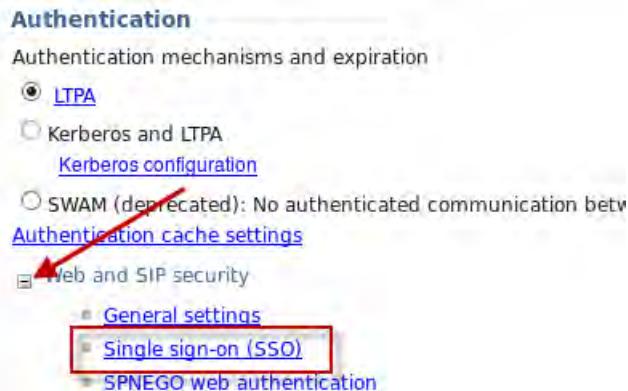
3. Enter **object00** for the password. Enter **/tmp/dash\_keys** for the file name. Click **Import keys**.

A screenshot of the 'Cross-cell single sign-on' configuration page. It shows fields for 'Password' (containing '\*\*\*\*\*') and 'Confirm password' (also containing '\*\*\*\*\*'). Below these is a field for 'Fully qualified key file name' containing '/tmp/dash\_keys'. At the bottom are two buttons: 'Import keys' (highlighted with a red arrow) and 'Export keys'.

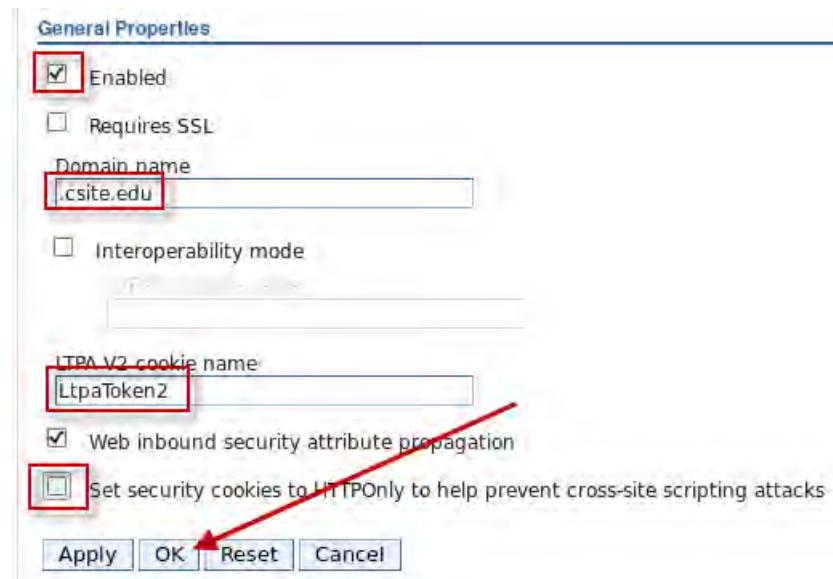
4. Click **Save**.



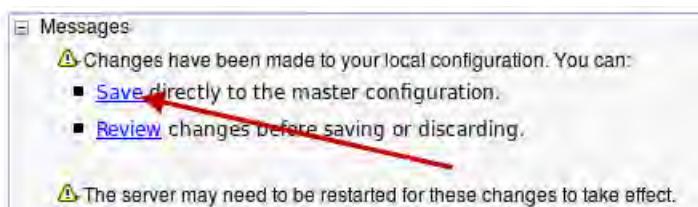
5. Expand **Web and SIP security**. Select **Single sign-on (SSO)**.



6. Verify that SSO is enabled. Enter **.csite.edu** for the domain name. Enter **LtpaToken2** for the cookie name. Clear the option for **HTTPOnly**. Click **OK**.



7. Click **Save**.



8. Add the Dashboard Application Services Hub SSL certificate into the presentation server truststore.
  - a. Under **Security**, click **SSL certificate and key management**.



- b. Under the *Related Items* section, select the **Key stores and certificates**.

The screenshot shows the 'Related Items' section on the right side of the screen. It contains the following links:

- SSL configurations
- Dynamic outbound endpoint SSL configurations
- Key stores and certificates** (highlighted with a red box)
- Key sets
- Key set groups
- Key managers
- Trust managers
- Certificate Authority (CA) client configurations

- c. Select **NodeDefaultTrustStore**.

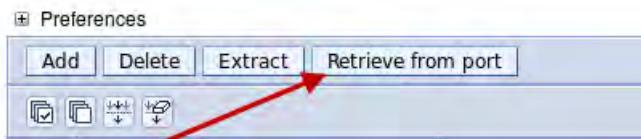
Select	Name	Description	
You can administer the following resources:			
<input type="checkbox"/>	<a href="#">NodeDefaultKeyStore</a>	Default key store for JazzSMNode01	(optional)
<input type="checkbox"/>	<a href="#">NodeDefaultTrustStore</a>	Default trust store for JazzSMNode01	(optional)

- d. Under the *Additional Properties* section, select **Signer Certificates**.

The screenshot shows the 'Additional Properties' section on the right side of the screen. It contains the following links:

- Signer certificates** (highlighted with a red box)
- Personal certificates
- Personal certificate

e. Click **Retrieve from port**.



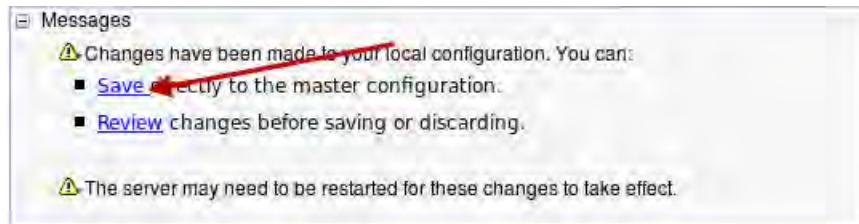
f. Enter **host1.csuite.edu** for the host. Enter **16311** for the port. Enter **DASH\_SSL** for the alias.  
Click **Retrieve signer information**.

A screenshot of a 'General Properties' dialog. It contains three required fields: 'Host' (host1.csuite.edu), 'Port' (16311), and 'Alias' (DASH\_SSL). Below these is a dropdown menu for 'SSL configuration for outbound connection' set to 'NodeDefaultSSLSettings'. At the bottom is a blue button labeled 'Retrieve signer information' with a red arrow pointing to it.

g. Review the certificate details, and click **OK**.

A screenshot of a 'Retrieved signer information' dialog. It displays several fields: 'Serial number' (7566714334782), 'Issued to' (CN=host1.csuite.edu, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US), 'Issued by' (CN=host1.csuite.edu, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US), 'Fingerprint (SHA digest)' (61:7F:4C:A5:FB:75:65:D8:1C:F9:22:D6:37:B2:E8:13:F5:37:99:0C), and 'Validity period' (Jan 11, 2031). At the bottom are four buttons: 'Apply', 'OK', 'Reset', and 'Cancel', with a red arrow pointing to the 'OK' button.

h. Click **Save**.



9. Log out of the WebSphere administrative console.

10. Close the Firefox browser.

11. Run the single sign-on enable script.

```
cd /opt/IBM/ncm/bin/utils
```

```
./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.
```

12. Restart Netcool Configuration Manager.

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



Wait for the components to restart.

## Configuring access rights for existing users

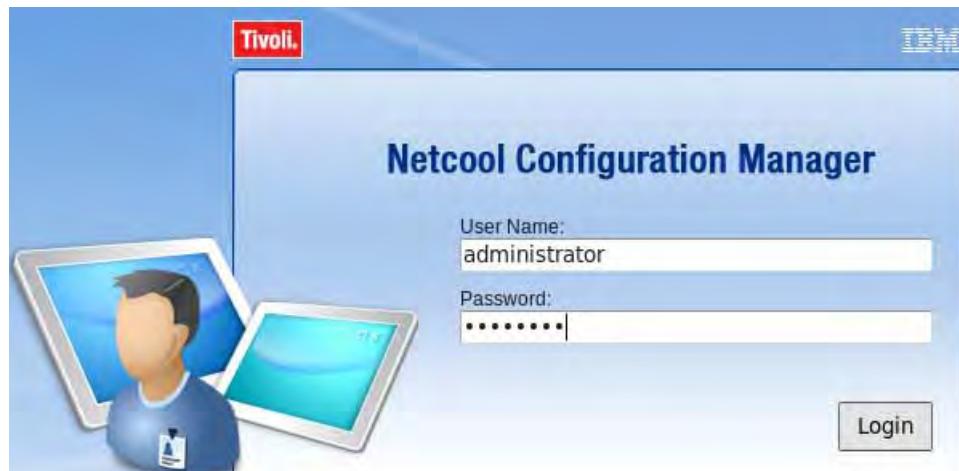
You added Netcool/OMNIbus and Network Manager users to Configuration Manager groups in a previous step. The group access grants access to certain Configuration Manager features. The following steps configure the user access rights within Configuration Manager.

1. Open a Firefox browser.

2. Connect to the following URL:

```
http://host1.csite.edu:15310/security/login.jsp
```

3. Log in as **administrator** with password **object00**.



4. Select **Account Management**.



5. Observe the list of users.

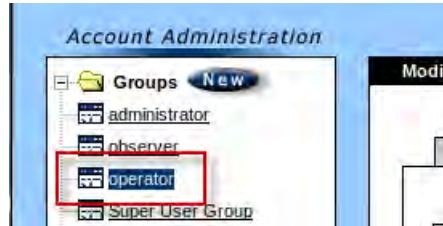
A screenshot of the "Accounts" screen in the Netcool Configuration Manager. The title bar says "Accounts" and the sub-header is "Account Administration". On the left, there's a tree view with "Groups" expanded, showing "administrator", "observer", "operator", and "Super User Group". Under "Users", there are several entries: "Intelliden", "itmadmin", "itmuser", "ncoadmin", "ncouser", "observer", and "operator". The entries "itmadmin", "itmuser", "ncoadmin", and "ncouser" are highlighted with a red box. A note at the bottom left says "User data is managed via remote user registry". On the right, there are two empty boxes labeled "Groups: Click" and "Users: Click".

The Netcool/OMNIbus and Network Manager users appear in the list because they belong to one of the Configuration Manager groups: IntellidenAdminUser or IntellidenUser.

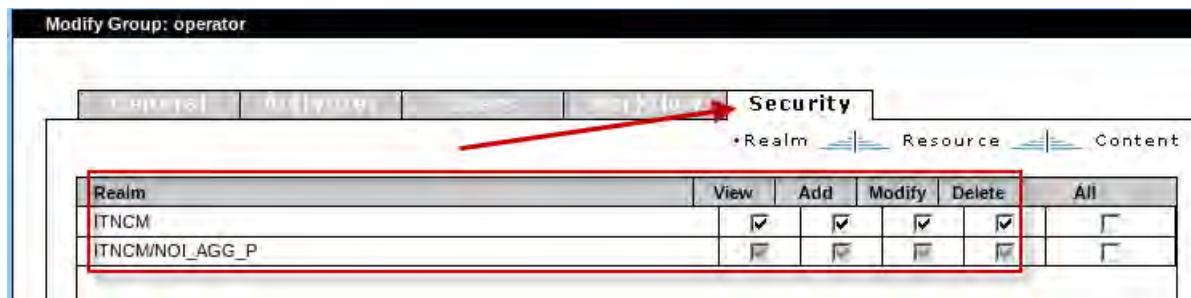


**Note:** No option is available to create new users within account management. Users are created or deleted within LDAP.

6. Select the **operator** group.



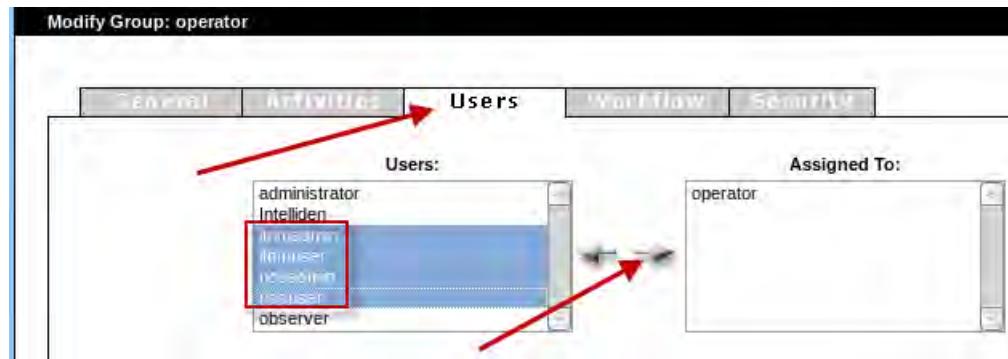
7. Select the **Security** tab.



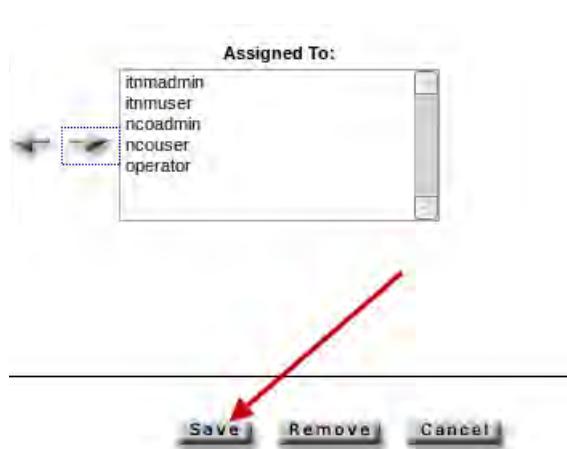
Users that belong to the operator group have full access rights to the ITNCM realm.

8. Select the **Users** tab.

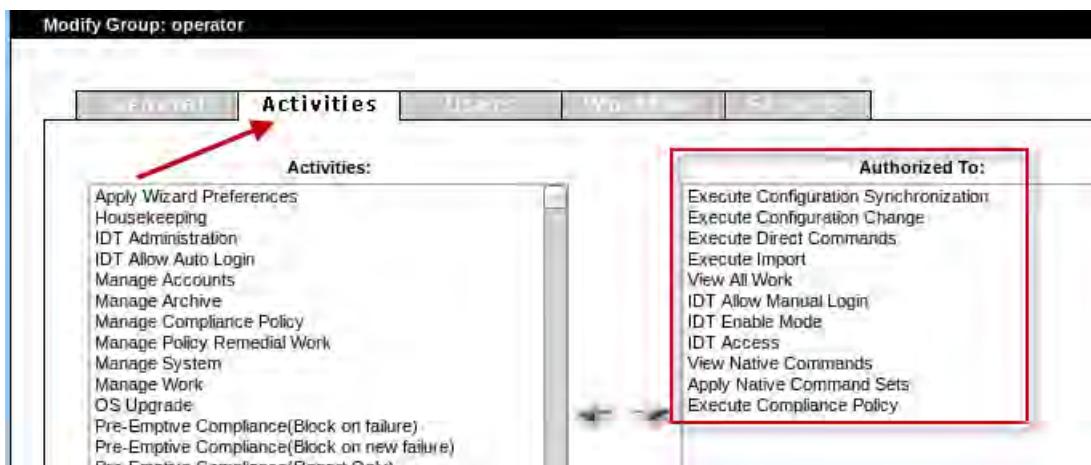
9. Click **itnadmin** to select the entry. Hold the Ctrl key and select **itnmuser**, **ncoadmin**, and **ncouser**. Click the *right arrow* icon to add the users to the group.



10. Click **Save**.



11. Click the **Activities** tab.



The members of the operator group are authorized to use these Configuration Management functions.

12. Click the *running person* icon to log out.

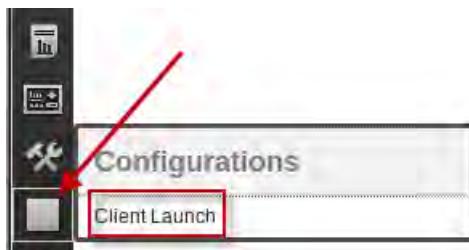


13. Close the Firefox browser.

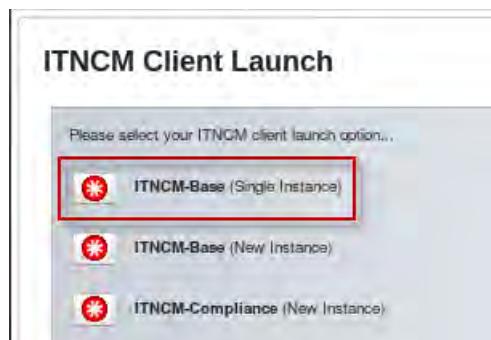
## Verifying single sign-on

1. Open a Firefox browser.
2. Log in to Dashboard Application Services Hub as **ncoadmin** with password **object00**.

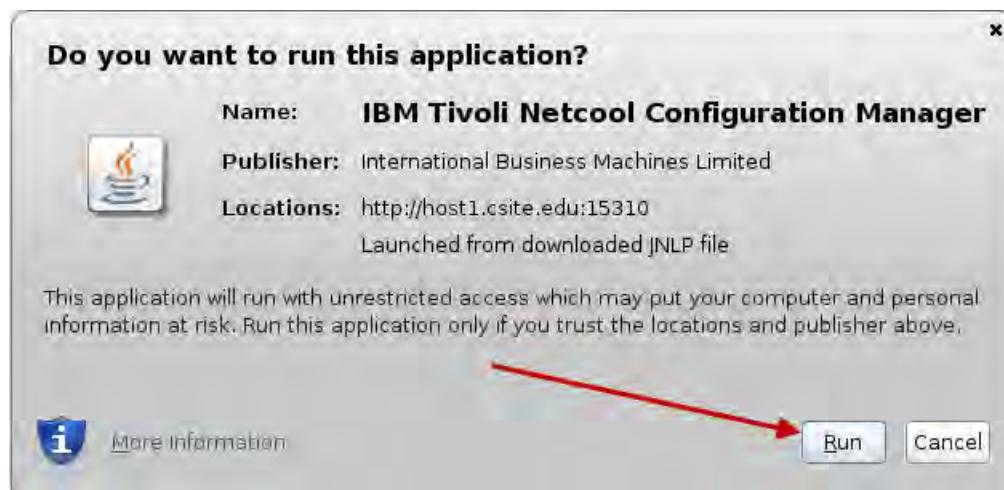
3. Click the indicated icon, and select **Client Launch**.



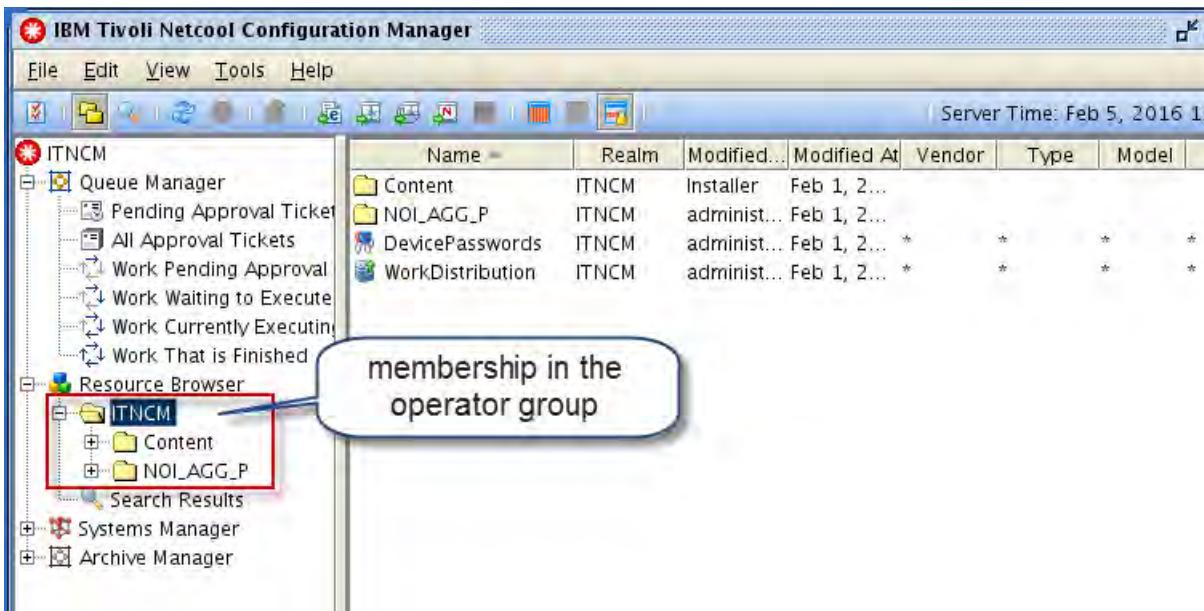
4. Click **ITNCM-Base (Single Instance)**.



5. Click **Run** when prompted.

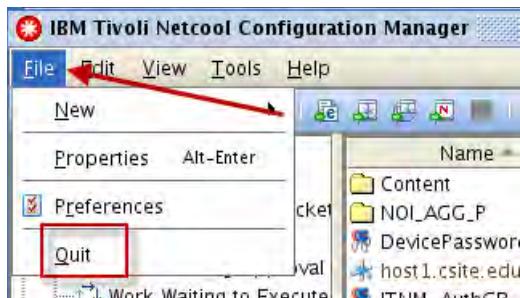


6. Verify that the login is successful.



The ncoadmin user has access to the ITNCM realm because the user belongs to the operator group.

7. Click **File** and select **Quit** to exit the client.



8. Click **OK** to confirm.



9. Log out of Dashboard Application Services Hub.

## Installing sample policy packs

The following steps describe how to install a collection of prebuilt compliance policies, and command sets that are used with the policies.



**Note:** At the time of this writing, some of the policy packs were available from the Integrated Service Management Library (ISML) website. A few samples are specific to the lab exercises.

1. Expand the policy file.

```
cd /software/tncm/
```

```
unzip ITNCM6.4BETAPolicyPacks_II.zip
```

2. Copy the policy files.

```
cd /software/tncm/ITNCM6.4BETAPolicyPacks_II
```

```
cp *.zip /opt/IBM/ncm/compliance/db/export/policies
```

The samples include five sets of policies. Each of the policies is distributed in a separate zip file. You must import each one individually.

3. Import BGPSecurity policies.

```
cd /opt/IBM/ncm/compliance/bin/utils
```

```
./policyImport.sh BGPSecurity.zip
```

```
.
```

```
Checking Parameters...
```

```
Results...
```

```
19 policies successfully imported.
```

```
0 Parameter warnings
```

4. Import PCI policies.

```
./policyImport.sh PCI.zip
```

```
.
```

```
Checking Parameters...
```

```
Results...
```

```
30 policies successfully imported.
```

```
0 Parameter warnings
```

5. Import RouterHardening policies.

```
./policyImport.sh RouterHardening.zip
. . .
Checking Parameters...
```

Results...

25 policies successfully imported.  
0 Parameter warnings

6. Import Security policies.

```
./policyImport.sh Security.zip
. . .
Checking Parameters...
```

Results...

47 policies successfully imported.  
0 Parameter warnings

7. Import TopTen policies.

```
./policyImport.sh TopTen.zip
. . .
Checking Parameters...
```

Results...

10 policies successfully imported.  
0 Parameter warnings

The following sample policies are unique to the lab exercises.

8. Copy the policy files.

```
cd /workshop/tncm
cp *.zip /opt/IBM/ncm/compliance/db/export/policies
```

9. Install the USISA workshop policies.

```
cd /opt/IBM/ncm/compliance/bin/utils
```

```
./policyImport.sh usisa_policies.zip
Extracting Policies...
```

Importing Policies...

```
Success: Policy Enable USISA syslog server|1 successfully imported.
```

Results...

```
1 policy successfully imported.
```

10. Install the CIS workshop policies.

```
./policyImport.sh cis_policies.zip
Extracting Policies...
```

Importing Policies...

.

.

.

Results...

```
38 policies successfully imported.
```

11. Grant access to the policies.

a. Open a Firefox browser.

b. Connect to the following URL:

```
http://host1.csite.edu:15310/security/login.jsp
```

c. Log in as **administrator** with password **object00**.



d. Select **ITNCM Compliance**.



e. Click **Admin**, and select **User Security Options**.



f. Click the **Realm Access Control** tab.

g. Click **BGPSecurity** to select it.

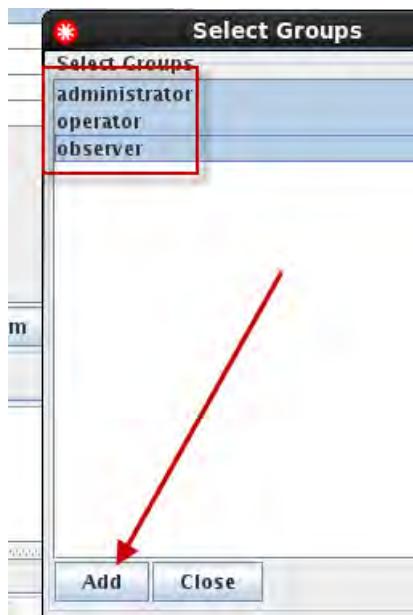
h. Click **Add Group(s)**.



i. Click **administrator** to select it.

j. Hold down the *Ctrl* key, and click the other two group names to select them all.

k. Click **Add**.



l. Verify that the three groups are added to the **BGPSecurity** realm.



m. Repeat these steps to add the same groups to the other realms in the list.

n. Click **Close**.

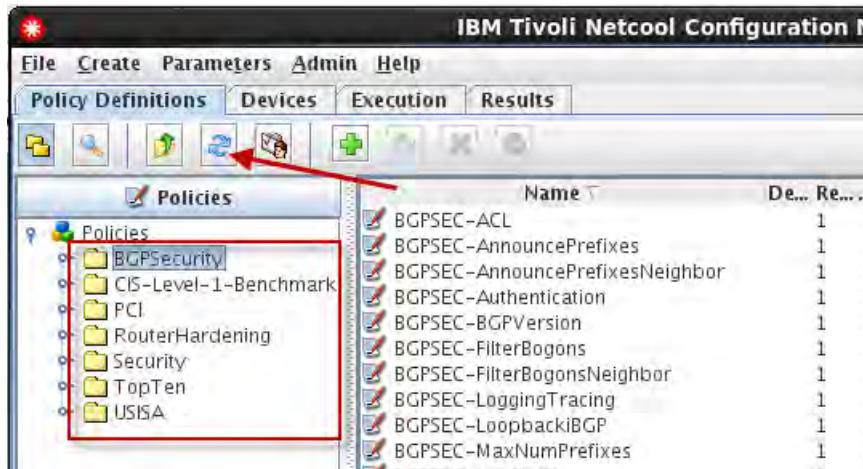


12. Verify access to the policies.

a. Click the icon with the two blue arrows to refresh the view.

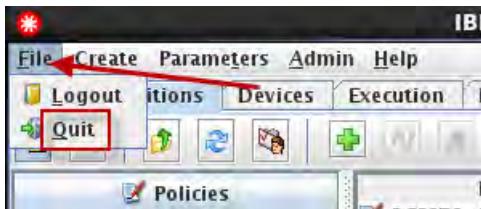


The realms for the policy packs now appear in the list.



The **administrator** user belongs to the administrator group. The previous steps granted access for the members of the administrator group to the policy realms.

- Click **File** and select **Quit** to exit the compliance client.



## Importing sample command sets

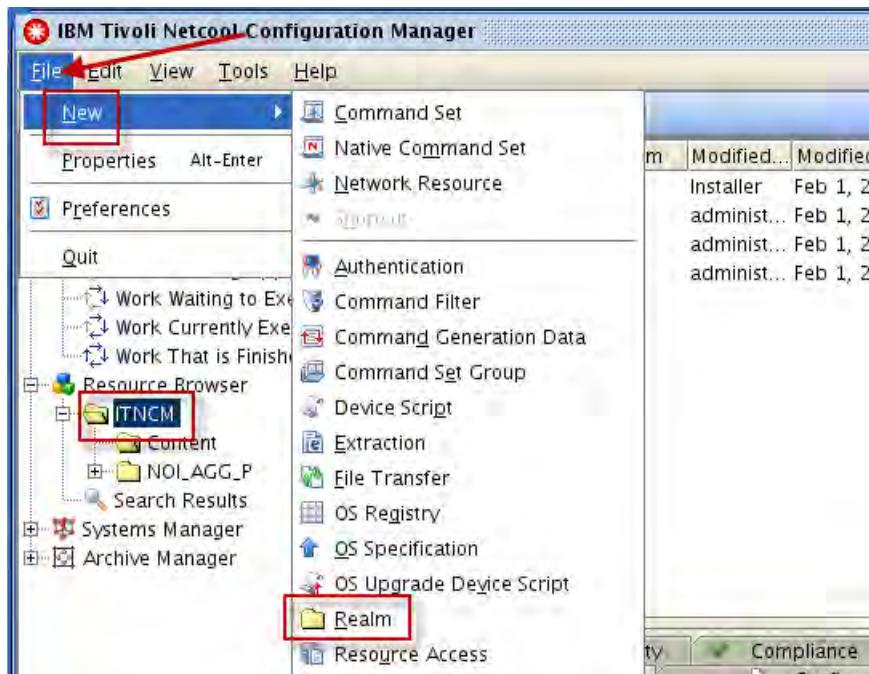
The workshop includes a small collection of sample command sets. The workshop compliance policies that you installed in the previous step reference these command sets.

- Select **ITNCM Webstart GUI**.

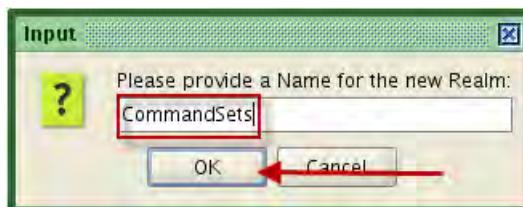


- Click **Run**.

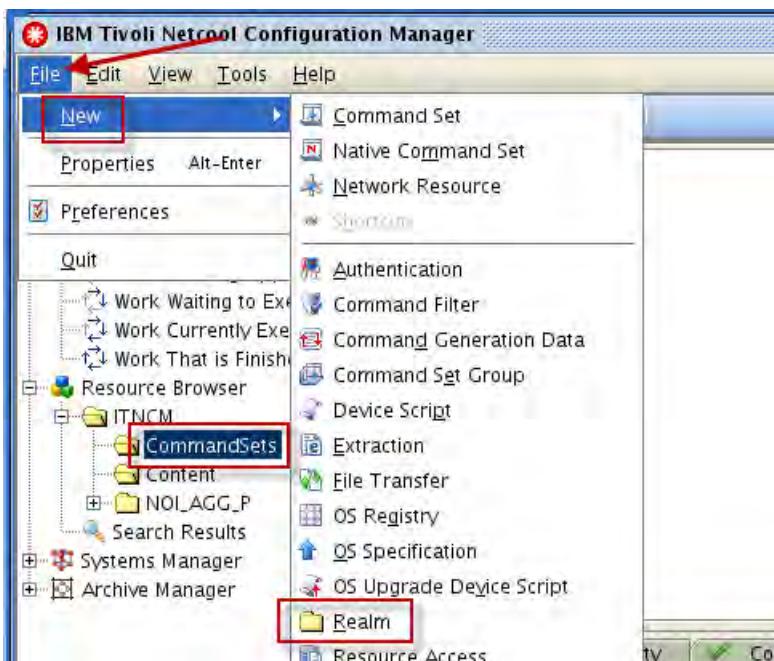
3. Under Resource Browser, click **ITNCM** to select it. Click **File**, and select **New > Realm**.



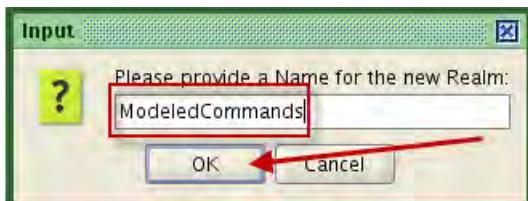
4. Enter **CommandSets** for the name, and click **OK**.



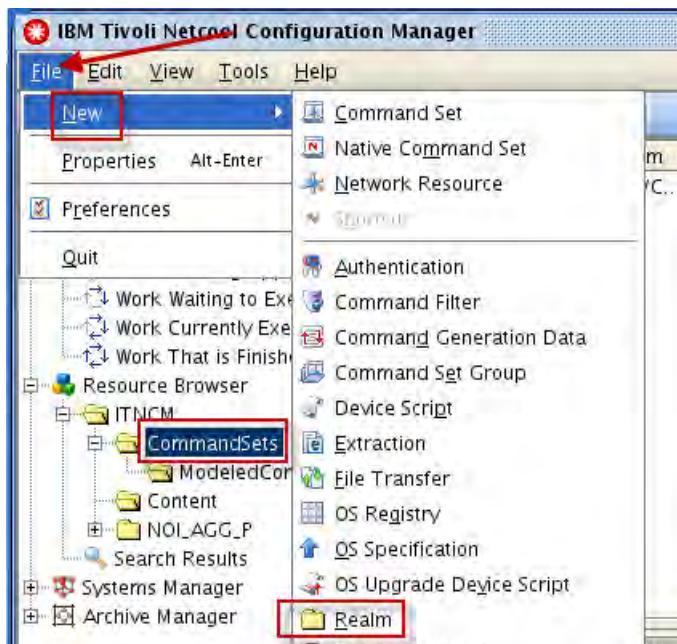
5. Under **ITNCM**, click **CommandSets** to select it. Click **File**, and select **New > Realm**.



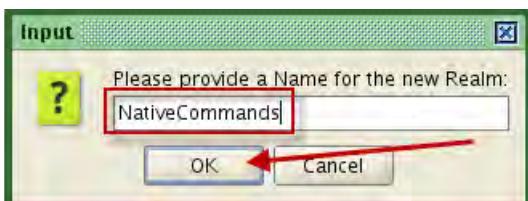
6. Enter **ModeledCommands** for the name, and click **OK**.



7. Under ITNCM, click **CommandSets** to select it. Click **File**, and select **New > Realm**.

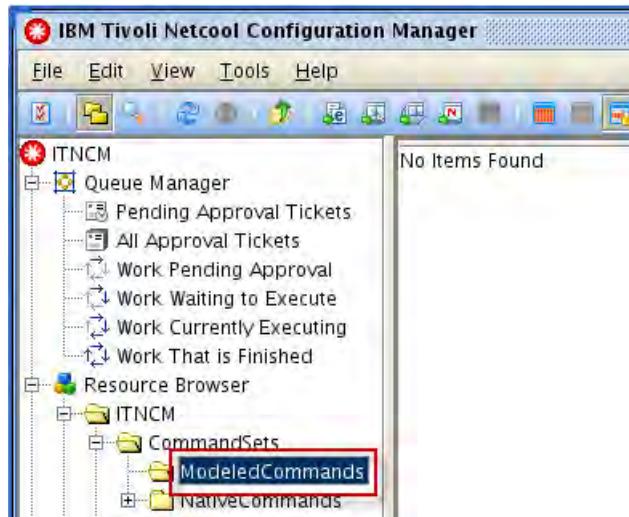


8. Enter **NativeCommands** for the name, and click **OK**.

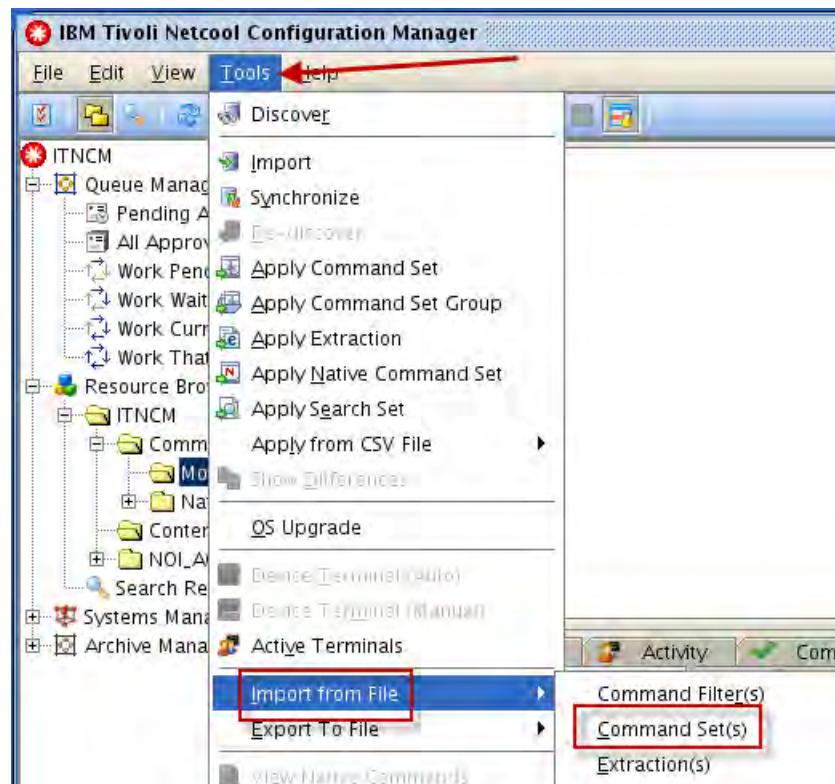


**Note:** The realm names are not significant. You create the realms to organize the command sets.

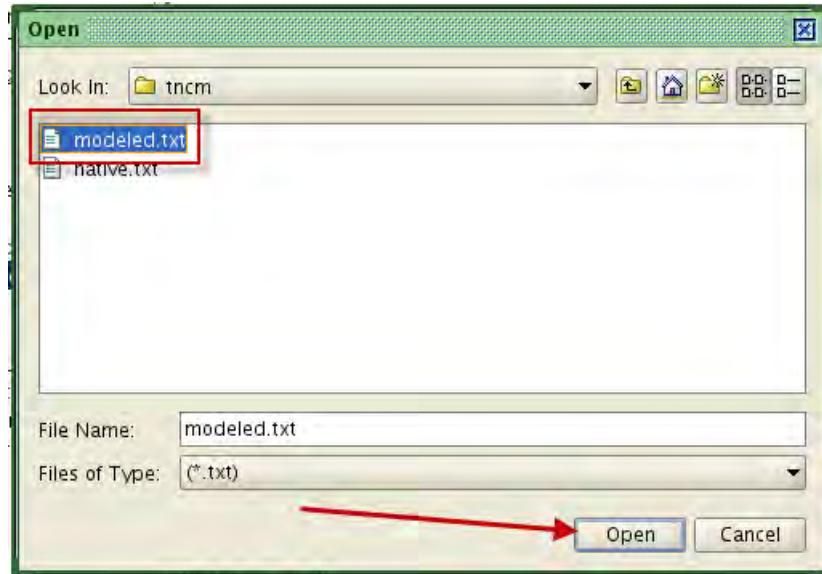
9. Under **CommandSets**, click **ModeledCommands** to select it.



10. Click **Tools**, and select **Import from File > Command Set(s)**.

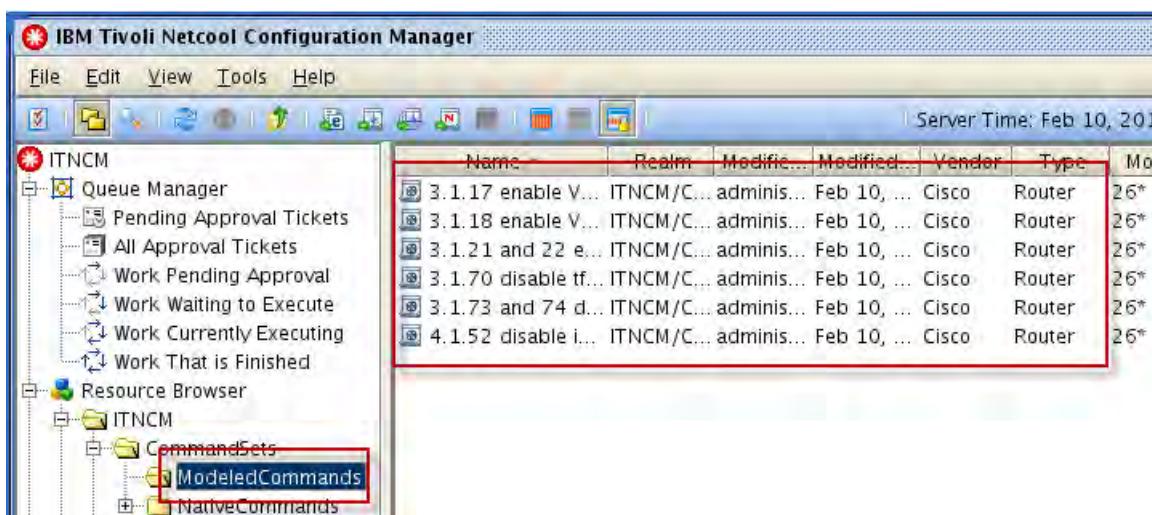


11. Navigate to **/workshop/tncm**, and select **modeled.txt**. Click Open.



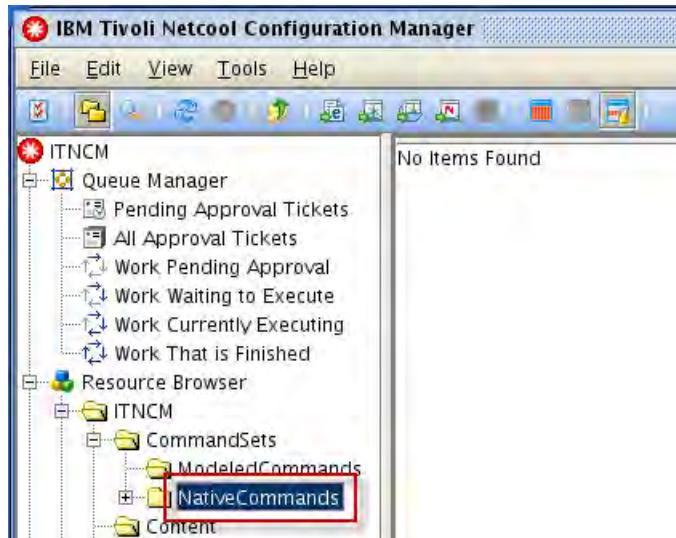
12. Wait a short time.

13. Verify that the command sets are listed.

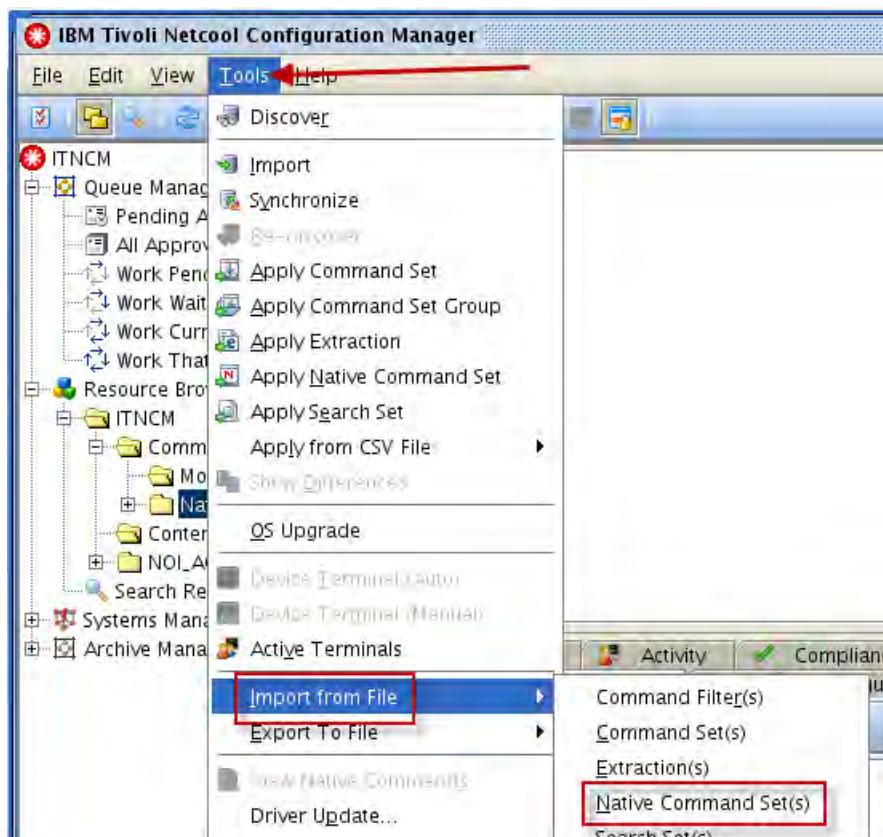


Name	Realm	Modified...	Modified...	Vendor	Type	Mo
3.1.17 enable V...	ITNCM/C...	adminis...	Feb 10, ...	Cisco	Router	26*
3.1.18 enable V...	ITNCM/C...	adminis...	Feb 10, ...	Cisco	Router	26*
3.1.21 and 22 e...	ITNCM/C...	adminis...	Feb 10, ...	Cisco	Router	26*
3.1.70 disable tf...	ITNCM/C...	adminis...	Feb 10, ...	Cisco	Router	26*
3.1.73 and 74 d...	ITNCM/C...	adminis...	Feb 10, ...	Cisco	Router	26*
4.1.52 disable i...	ITNCM/C...	adminis...	Feb 10, ...	Cisco	Router	26*

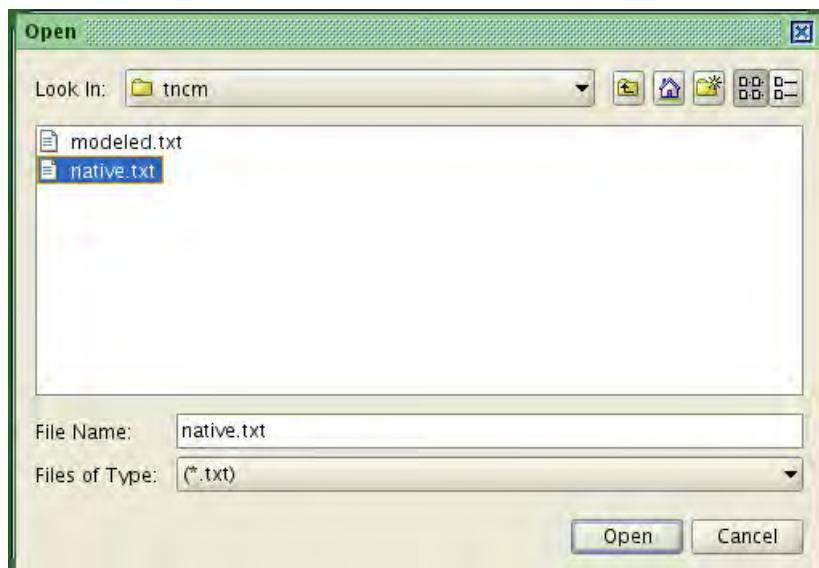
14. Under **CommandSets**, click **NativeCommands** to select it.



15. Click **Tools**, and select **Import from File > Native Command Set(s)**.

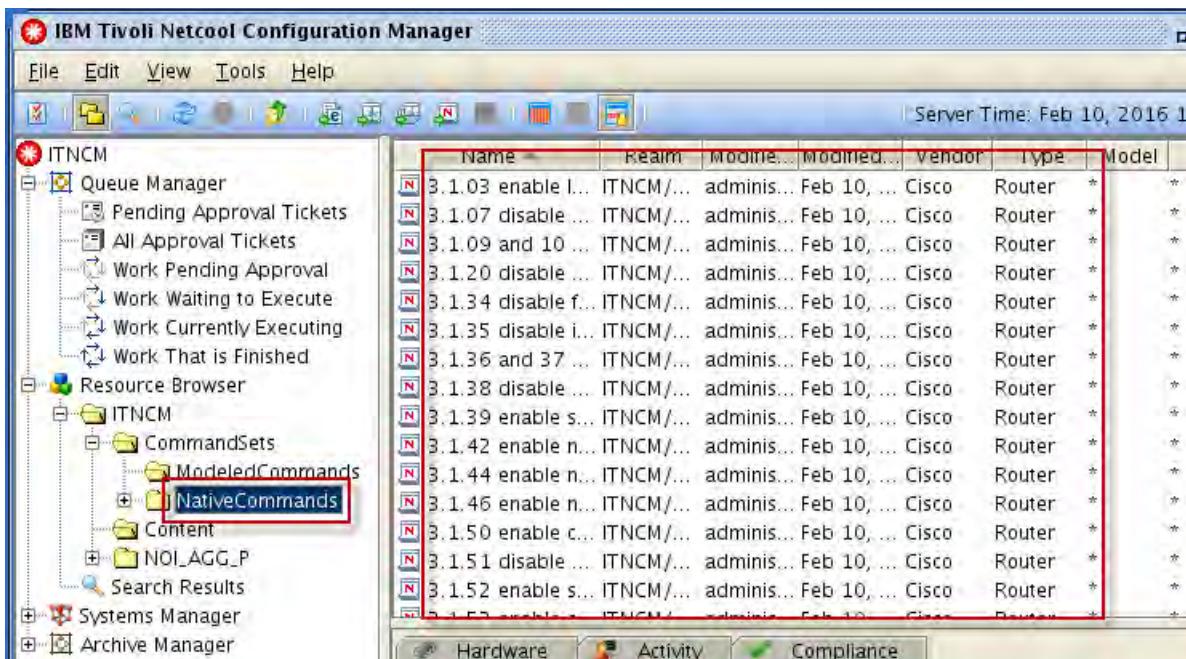


16. Navigate to **/workshop/tncm**, and select **native.txt**. Click **Open**.



17. Wait a short time.

18. Verify that the command sets are listed.



Name	Realm	Modified...	Vendor	Type	Model
3.1.03 enable I...	ITNCM/...	adminis...	Cisco	Router	*
3.1.07 disable ...	ITNCM/...	adminis...	Cisco	Router	*
3.1.09 and 10 ...	ITNCM/...	adminis...	Cisco	Router	*
3.1.20 disable ...	ITNCM/...	adminis...	Cisco	Router	*
3.1.34 disable f...	ITNCM/...	adminis...	Cisco	Router	*
3.1.35 disable i...	ITNCM/...	adminis...	Cisco	Router	*
3.1.36 and 37 ...	ITNCM/...	adminis...	Cisco	Router	*
3.1.38 disable ...	ITNCM/...	adminis...	Cisco	Router	*
3.1.39 enable s...	ITNCM/...	adminis...	Cisco	Router	*
3.1.42 enable n...	ITNCM/...	adminis...	Cisco	Router	*
3.1.44 enable n...	ITNCM/...	adminis...	Cisco	Router	*
3.1.46 enable n...	ITNCM/...	adminis...	Cisco	Router	*
3.1.50 enable c...	ITNCM/...	adminis...	Cisco	Router	*
3.1.51 disable ...	ITNCM/...	adminis...	Cisco	Router	*
3.1.52 enable s...	ITNCM/...	adminis...	Cisco	Router	*
3.1.53 enable ...	ITNCM/...	adminis...	Cisco	Router	*

19. Click **File** and select **Exit** to close the client.

20. Click **OK** to confirm the exit.

21. Click Logoff.



22. Close the Firefox browser.

## Configuring integration with Netcool/OMNibus

Netcool Configuration Manager generates SNMP traps for various situations during normal operations. In a previous exercise, you configured Configuration Manager to forward trap messages to an IP address. The Netcool/OMNibus SNMP probe is configured to listen for traps on that IP address. 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. Modify the master rules file.

a. Change to the location of the Netcool Knowledge Library.

```
cd /opt/IBM/tivoli/NcKL/rules
```

b. Open the master rules file for edit.

```
gedit snmptrap.rules
```

c. Scroll down in the file and locate the following line:

```
#include "$NC_RULES_HOME/include-snmptrap/ibm/ibm.master.include.lookup"
```

d. Uncomment the line by removing the # character.

```
include "$NC_RULES_HOME/include-snmptrap/ibm/ibm.master.include.lookup"
```

e. Scroll down in the file and locate the following line:

```
#include "$NC_RULES_HOME/include-snmptrap/ibm/ibm.master.include.rules"
```

f. Uncomment the line by removing the # character.

```
include "$NC_RULES_HOME/include-snmptrap/ibm/ibm.master.include.rules"
```

g. Scroll down in the file and locate the following line:

```
#include
"$NC_RULES_HOME/include-snmptrap/ibm/ibm-preclass.include.snmptrap.rules"
```

 Hint: This line is near the bottom of the file.

- h. Uncomment the line by removing the # character.

```
include
"${NC_RULES_HOME}/include-snmptrap/ibm/ibm-preclass.include.snmptrap.rules"
```

- i. Save the file and exit the gedit utility.

2. Test the syntax of the modified file.

- a. Define the Knowledge Library environment variable

```
export NC_RULES_HOME=/opt/IBM/tivoli/NcKL/rules
```

- b. Run the Syntax probe.

```
cd $NC_RULES_HOME
```

```
nco_p_syntax -server NOI_AGG_P -rulesfile snmptrap.rules
```

```
.
```

```
.
```

```
.
```

```
2016-02-05T13:42:02: Information: I-UNK-000-000: Rules file syntax OK
```

```
2016-02-05T13:42:02: Information: I-UNK-000-000: Disconnecting ...
```

```
2016-02-05T13:42:02: Debug: D-UNK-000-000: Shutting down Probewatch
heartbeat thread.
```

```
.
```

```
.
```

```
.
```

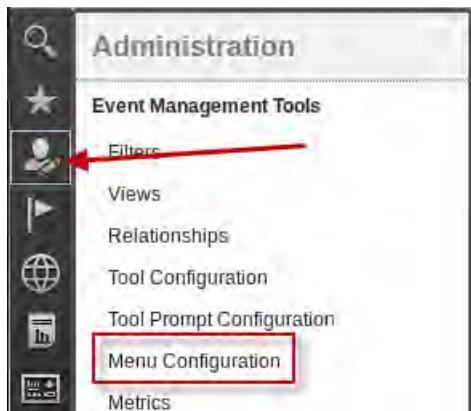
Scroll back in the terminal window output and locate the message that indicates no errors.

3. Add the Configuration Manager menu to the Web GUI alert menu.

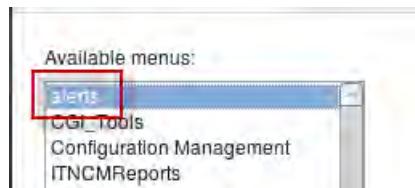
- a. Open a Firefox browser.

- b. Log in to Dashboard Application Services Hub as **ncoadmin** with password **object00**.

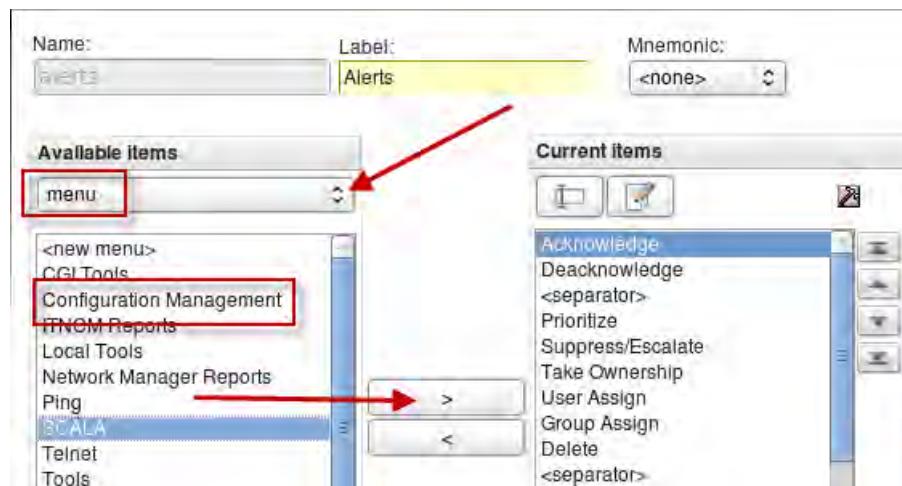
- c. Click the icon and select **Menu Configuration**.



- d. Click **alerts** to select it. Scroll to the bottom and click **Modify**.

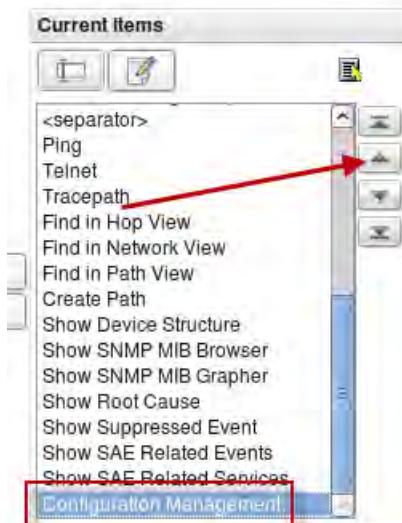


- e. Click the arrow and select **menu**. Click **Configuration Management** to select it. Click the **right arrow icon** to add the menu to the list.

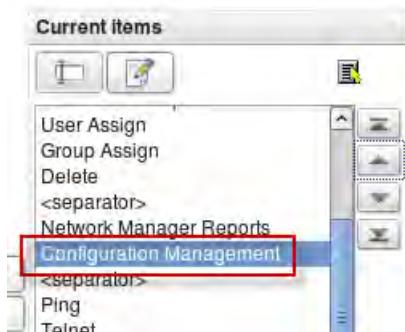


The Configuration Management menu is added to the bottom of the list.

- f. Scroll to the bottom of the list and select **Configuration Management**. Click the **up arrow icon** several times.



- g. Click the *up arrow* icon until **Configuration Management** appears below the entry for Network Manager Reports.



- h. Click **Save**. Click **OK**.



- i. Log out of Dashboard Application Services Hub.  
j. Close the Firefox browser.

## Configuring device synchronization

Netcool Configuration Manager automatically imports devices that Network Manager discovers. The installation configures this synchronization process. By default, the synchronization runs one time every day. The following steps demonstrate how to modify that frequency.

1. Change to the location of the property file.

```
cd /opt/IBM/ncm/config/properties
```

2. Save a copy of the original file.

```
cp rseries.properties rseries.properties.orig
```

3. Open the file for edit.

```
gedit rseries.properties
```

4. Locate the following lines:

```

Label: 1440 is a Daily (in minutes) delay. Update time in minutes.

NMEntityMappingComponent/period=1440
```

5. Change 1440 to 5 as shown here:

```

Label: 1440 is a Daily (in minutes) delay. Update time in minutes.

NMEntityMappingComponent/period=5
```

6. Save the file and exit the gedit utility.



**Important:** You change this property to facilitate a subsequent workshop exercise. You do not typically change this value in a production environment.

## Configuring the Network Health Dashboard

You installed the Network Health Dashboard in a previous unit. You must modify a property file to complete the dashboard configuration.

1. Change to the target directory:

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

2. Open the property file for edit:

```
gedit ncm.properties
```

3. Locate the following lines:

```
ncm.properties
Local URL to ITNCM REST services provided by 'ncmdashservice'
ncm.protocol=https
ncm.server=localhost
ncm.port=16311
ncm.contextroot=/ibm/console
ncm.service.context=/ncmdashservice/rest
ncm.service.devices=/ncm/device
```

4. Modify the following lines:

```
*ncm.properties
Local URL to ITNCM REST services provided by 'ncmdashservice'
ncm.protocol=https
ncm.server=host1.csuite.edu
ncm.port=15311
ncm.contextroot=/ibm/console
ncm.service.context=/ncmdashservice/rest
ncm.service.devices=/ncm/device
```

5. Save the file and exit the gedit utility

# Exercise 8 Configuring Out-of-Band Change (OOBC) daemon

The OOBC daemon detects network device configuration changes by looking for messages in the system Syslog file. Network devices are configured to forward their console logs to the local Syslog server. The Syslog daemon is modified to route specific categories of messages to a separate file. The OOBC daemon is configured to examine that file.

1. Examine the Rsyslog configuration.



**Note:** To facilitate the workshop, the Rsyslog configuration is already modified.

- a. Change to the root user.

```
su -
Password: object00
```

- b. Examine the revised configuration file.

```
cd /workshop/etc/rsyslog
```

```
more rsyslog.conf
```

- c. Locate the following lines:

```
Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

The lines are uncommented so that the Rsyslog daemon listens on UDP port 514 for messages. This property is required to receive messages from network devices.

- d. Scroll to the end of the file, and locate the following lines:

```
Save local* messages for TNCM OOBC daemon
local0.*;local1.*;local2.*;local3.*;local4.*;local5.*;local6.*;local7.*
/var/log/tncm_oobc.log
```

These lines configure the Rsyslog daemon to direct messages for the *local* facility to */var/log/tncm\_oobc.log*.

2. Create the TNCM log file.

```
cd /var/log
```

```
touch tncm_oobc.log
```

```
chown netcool:ncoadmin tncm_oobc.log
```

3. Modify the Rsyslog daemon.

- a. Replace the existing Rsyslog file with the workshop copy.

```
cp /workshop/etc/rsyslog/rsyslog.conf /etc/rsyslog.conf
```

```
cp: overwrite `'/etc/rsyslog.conf'? y
```

Enter **y** to overwrite the existing file.

- b. Restart the Rsyslog daemon.

```
service rsyslog restart
```

```
Shutting down system logger:
```

```
[OK]
```

```
Starting system logger:
```

```
[OK]
```

The Rsyslog daemon is configured to forward messages to local\* facility to the TNCM log file.

4. Verify that the revised daemon works as expected.

- a. Generate a test message.

```
logger -p local0.info 'this is a test'
```

- b. Check the TNCM log file.

```
tail /var/log/tncm_oobc.log
```

```
Feb 2 21:32:36 host1 netcool: this is a test
```

5. Install the OOBC software.

- a. Expand the installation.

```
cd /opt
```

```
unzip /software/tncm/base/oobc.zip
```

- b. Install the daemon.

```
cd /opt/OutOfBandChange/install
```

```
./install.sh
```

Enter **1** to accept the license

```
Enter the Unix owner of the OOBC software? [icosuser:icosgrp]
```

Enter **netcool:ncoadmin**

```
Enter the servername of ITNCM? [intelliden]
```

Enter **host1.csite.edu**

```
Is ITNCM running a secure connection (https)? [no]
```

Press enter to accept the default

```
What port is ITNCM running on [16310]?
```

Enter **15310**

What user do you want to login to ITNCM as [OOBCUser]?

Enter **administrator**

Enter clear text password:

Enter **object00**

Enter the worker user id ITNCM executes work as [intelliden]?

Enter **administrator**

Enter the worker server address [intelliden]?

Enter **host1.csite.edu**

Enter an authorized 3rd party user id that does not require notification when activity is recorded in the syslog [3rdPartyUser]?

Press enter to accept the default

Enter the full path to the syslog file to be parsed:

[ /opt/OutOfBandChange/run1/local7.log ]

Enter **/var/log/tncm\_oobc.log**

Enter the full path to the syslog saver file:

[ /opt/OutOfBandChange/run1/log.syslog-messages ]

Press enter to accept the default

Intelliden OOBC Install Properties:

Install Owner: netcool:ncoadmin

Install Directory: /opt/OutOfBandChange/run1

Intelliden URL: iiop://TNCMHOST:7001/

Syslog File: /var/log/tncm\_oobc.log

OOBC User: administrator

User Password: f705040e2b8f43e8b3f49d8923e67d3d

Intelliden Worker: administrator

3rd Party User: 3rdPartyUser

Worker Server: host1.csite.edu

Syslog Message Storage File:/opt/OutOfBandChange/run1/log.syslog-messages

Is this OK? (yes, no)

Enter yes

```
Copying Configuration Files
Setting permissions
Creating symbolic links for Linux
/etc/rc.d/rc0.d/K8700BCDaemon_run1
/etc/rc.d/rc1.d/K8700BCDaemon_run1
/etc/rc.d/rc2.d/S1300BCDaemon_run1
/etc/rc.d/rc3.d/S1300BCDaemon_run1
/etc/rc.d/rc4.d/S1300BCDaemon_run1
/etc/rc.d/rc5.d/S1300BCDaemon_run1
/etc/rc.d/rc6.d/K8700BCDaemon_run1
BUILD SUCCESSFUL
Total time: 3 minutes 59 seconds
```

- c. Remove symbolic links.

```
cd /etc/rc.d
rm rc*/*OOBCDaemon_run1
```

Enter **y** to confirm delete for each file.



**Note:** The default configuration runs the OOBC daemon as the root user. You want the daemon to run as the **netcool** user.

- d. Exit the root user.

```
exit
```



**Important:** The OOBC installation process creates the oobc.properties.xml file. However, a regular expression command contained within that file has an issue. This command is used by the OOBC daemon to locate messages in the Syslog file. The workshop provides a file with the correct regular expression configured.

6. Replace the property file with the workshop copy.

```
cd /opt/OutOfBandChange/run1
cp /workshop/tncm/oobc.properties.xml .
```

7. Start the oobc daemon.

```
cd /opt/OutOfBandChange/run1
./oobc.sh start
```

```
Started OOBC daemon: 25440
nohup: redirecting stderr to stdout
```

8. Verify operation.

```
tail -2001 oobc.log
```

```
WARN 02 Feb 2016 22:28:15 Activating com.intelliden.oobc.OutOfBandChangeDaemon
INFO 02 Feb 2016 22:28:17 Recovered 0 PRE rolled-up Events (with 0 child events)
from last run.
INFO 02 Feb 2016 22:28:17 Recovered 0 POST rolled-up Events (with 0 child
events) from last run.
INFO 02 Feb 2016 22:28:17 Started com.intelliden.oobc.NotifierThread
INFO 02 Feb 2016 22:28:17 Started com.intelliden.oobc.RollupThread
INFO 02 Feb 2016 22:28:17 Started com.intelliden.oobc.ParserThread
WARN 02 Feb 2016 22:28:17 com.intelliden.oobc.OutOfBandChangeDaemon now Active.
WARN 02 Feb 2016 22:28:17 Starting log parsing with new marker file:
/opt/OutOfBandChange/run1/log.marker
INFO 02 Feb 2016 22:28:17
```

```
=====
ITNCM Host: host1.csite.edu
ITNCM Port: 15310
ITNCM Protocol: iiop
ITNCM User: administrator
Ignored host(Worker Server): host1.csite.edu
Input Log File: /var/log/tncm_oobc.log
Input Log File Poll Seconds: 5
Marker File: /opt/OutOfBandChange/run1/log.marker
Recovery File(s) Prefix: /opt/OutOfBandChange/run1/log.recovery
Notify on Unmanaged Device: true
Event Consolidation Algorithm: IdleTimeout
Consolidation Freq Seconds: 60
Fatal Restart Seconds: 15
ITNCM User: administrator
3rd Party User: 3rdPartyUser
Number of Log pattern rules: 6
Number of Notification Rules: 1
Number of Action Rules: 4
=====
```

## Modifying the start script

When you use the existing script to stop the Netcool Configuration Manager Components, you are prompted for a user name and password. Modify the script to eliminate the need for the prompt.

1. Change to the location of the start script.

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

2. Save a copy of the file before changes.

```
cp itncm.sh itncm.sh.orig
```

3. Open the file for edit.

```
gedit itncm.sh
```

4. Locate the following lines.

```
echo "Stopping GUI Server"
echo
echo "Please enter the Intelliden Super User and password if prompted
below:"
echo
$WAS_BIN/stopServer.sh server1 -quiet
```

5. Modify the line as high-lighted.

```
$WAS_BIN/stopServer.sh server1 -quiet -username Intelliden -password object00
```

6. Save the file and exit the gedit utility.

7. Test the modification.

```
./itncm.sh stop
```

IBM Tivoli Netcool Configuration Manager

---

Stopping GUI Server

Please enter the Intelliden Super User and password if prompted below:



**Important:** The prompt message appears, but the script stops the components without requesting the user name and password.

## Configuring auto-start

1. Change to the root user:

```
su -
```

```
Password: object00
```

2. Generate the auto-start script:

```
cd /opt/IBM/ncm/bin/utils/
```

```
./createAutoStart.sh
```

```
itncm 0:off1:off2:on3:on4:on5:on6:off
```

This command creates a script that is called itncm and places the file in the **/etc/init.d** directory. However, the script is configured to start the components by using a user ID called **icosuser**. Change the user to **netcool**.

3. Modify itncm start-up script as follows:

```
cd /etc/init.d
gedit itncm
```

4. Locate all two instances of **icosuser** and change them to **netcool** as shown here:

```
case "$1" in
 'start')
 if [-f /opt/IBM/ncm/bin/itncm.sh]; then
 su - netcool -c "/opt/IBM/ncm/bin/itncm.sh start"
 touch /var/lock/subsys/itncm
 fi
 ;;

 'stop')
 if [-f /opt/IBM/ncm/bin/itncm.sh]; then
 su - netcool -c "/opt/IBM/ncm/bin/itncm.sh stop"
 if [-f /var/lock/subsys/itncm]; then
 rm /var/lock/subsys/itncm
 fi
```

5. Save the file and exit the gedit utility.

6. Change the file permission to allow execute.

```
chmod +x itncm
```

## Verifying auto-start

1. Start the components.

```
/etc/init.d/itncm start
```

Wait for the components to start.

2. Exit the root user.

```
exit
```

3. Check the status of the Netcool Configuration Manager components.

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

```

IBM Tivoli Netcool Configuration Manager Status

```

```
Deployment Type = GUI + Worker Server
```

```
Base Worker Server = Enabled
Compliance Core = Enabled
```

```
Components
```

```

Worker Server = RUNNING
Compliance Core = RUNNING
GUI Server = RUNNING
```

```
Logging level
```

```

Current log level = WARN
```

```
Load version
```

```

6.4.2.0-0-167
```

```
Database
```

```

Hostname/IP Address = host1.csite.edu
Database Name = itncm
```

```
Driver Currency
```

```

This NCM instance can support the latest installed drivers
```

4. Remove the installation files.

```
cd /software
```

```
/bin/rm -R tncm
```

The following list is a summary of the accomplishments from this unit:

- Installed Tivoli Netcool Configuration Manager
- Installed the Standard device drivers
- Installed the SmartModel device drivers
- Configured the presentation server to use LDAP
- Configured single sign-on between the presentation server and Dashboard Application Services Hub
- Imported sample policy packs
- Installed and configured the Out of Band daemon



## 6 Verifying Networks for Operations Insight exercises

In this unit, you learn how to verify the functions of the networks portion of the solution. Some basic verification was completed during the installation and configuration exercises. The following steps perform a more comprehensive verification.

### Exercise 1 Starting the network simulator

The verification steps use another VMware image. This image contains a network simulator.

1. Click the GNS3 tab. Click **Power on this virtual machine**.

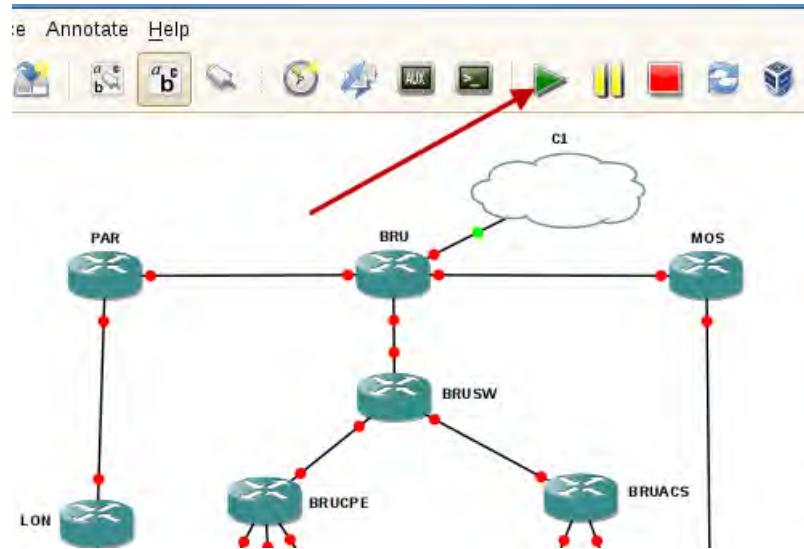


The image takes a few minutes to initialize.

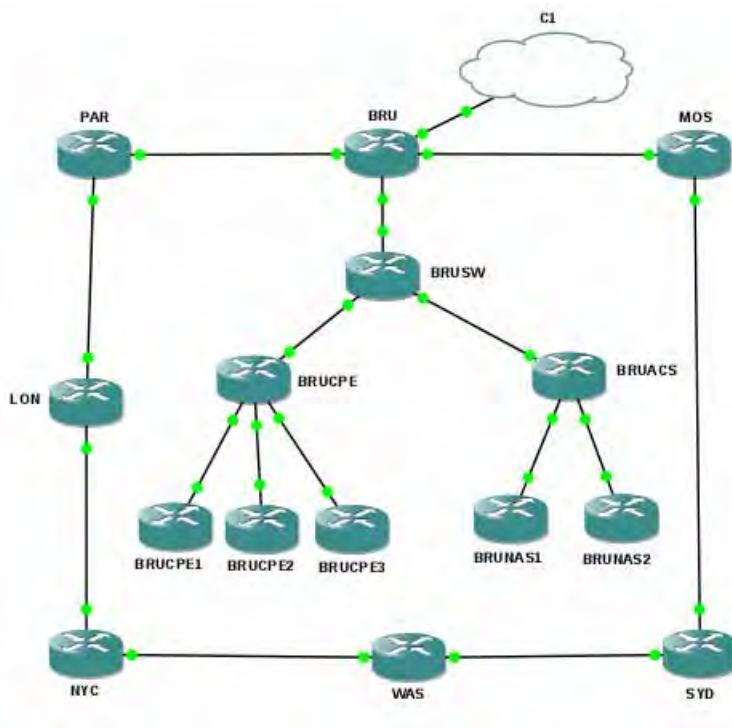
2. Log in as **root** with password **object00**.
3. Start the simulated devices.
  - a. Double-click the desktop icon labeled **RouterSim-lab1**.



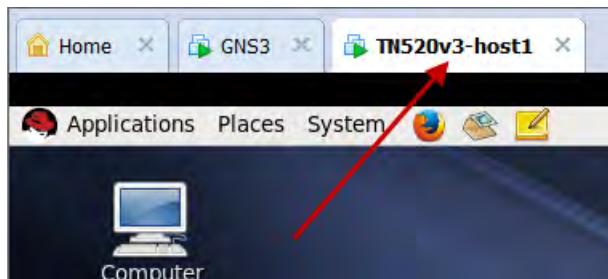
- b. Click the green arrow icon to start the simulated devices.



- c. Wait until all of the dots turn green.



4. Click the TN520-host1 tab to return to the NOI image.



5. Verify access to the simulated devices.

```
ping -c 3 10.10.255.1
```

```
PING 10.10.255.1 (10.10.255.1) 56(84) bytes of data.
64 bytes from 10.10.255.1: icmp_seq=2 ttl=255 time=7.04 ms
64 bytes from 10.10.255.1: icmp_seq=3 ttl=255 time=10.5 ms

--- 10.10.255.1 ping statistics ---
3 packets transmitted, 2 received, 33% packet loss, time 3001ms
rtt min/avg/max/mdev = 7.049/8.821/10.593/1.772 ms
```

6. Remove all events from the ObjectServer:

```
nco_sql -server NOI_AGG_P -user root -password object00
```

```
1> delete from alerts.status;
2> go
(20 rows affected)
1> quit
```

## Exercise 2 Solution verification

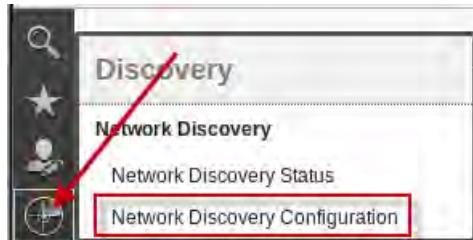
In this exercise, you verify many of the functions provided by the Networks for Operations Insight solution, including these items:

- Discovering devices with Network Manager
- Netcool Configuration Manager client launch from Dashboard Application Services Hub
- Verification of single sign-on
- Importing devices into Netcool Configuration Manager based on Network Manager discovery
- Verification of network compliance evaluation and remediation
- Verification of launch-in-context tool launch from Dashboard Application Services Hub

## Discovering devices with Network Manager

1. Open a Firefox browser.
2. Log in to Dashboard Application Services Hub as **itnadmin** with password **object00**.

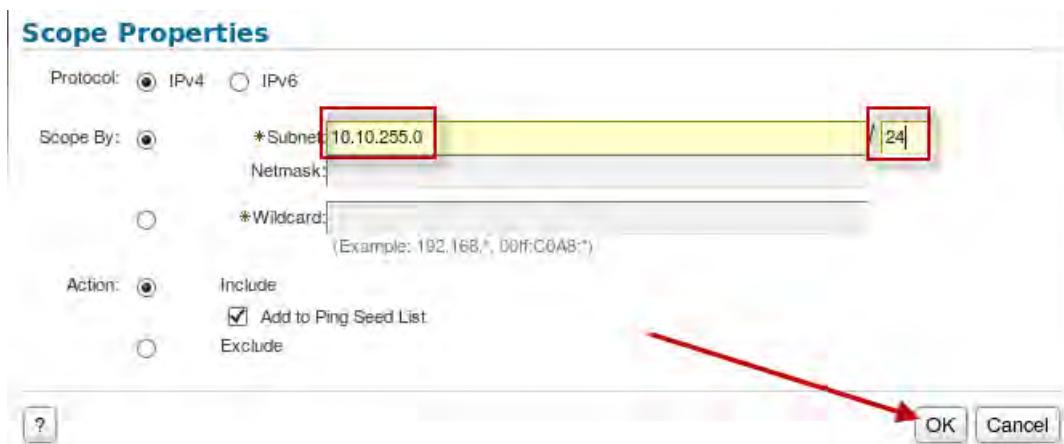
3. Click the icon and select Network Discovery Configuration.



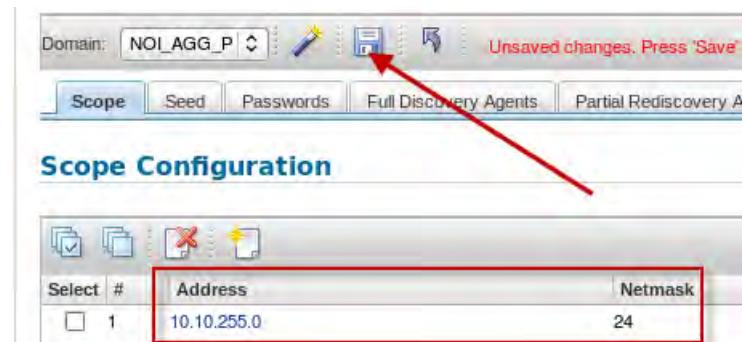
4. Click the icon to add a subnet.



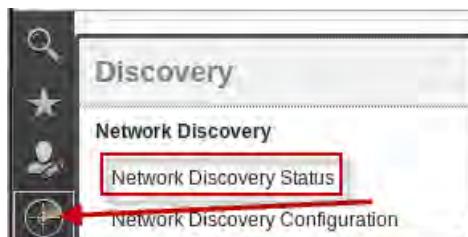
5. Enter 10.10.255.0 / 24. Click OK.



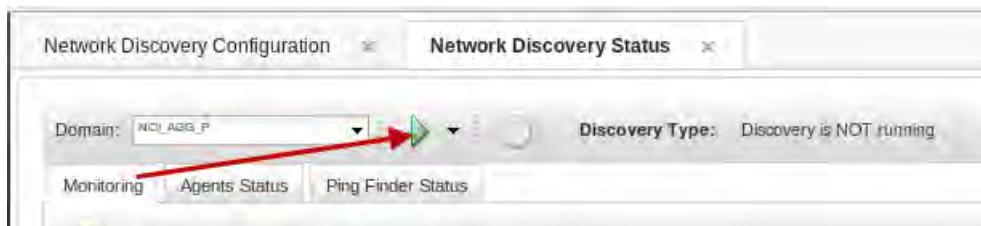
6. Click the icon to save the configuration.



7. Click the icon and select Network Discovery Status.



8. Click the green arrow icon to start the discovery.



**Note:** The discovery runs for approximately 3 minutes.

9. Verify that discovery is complete.

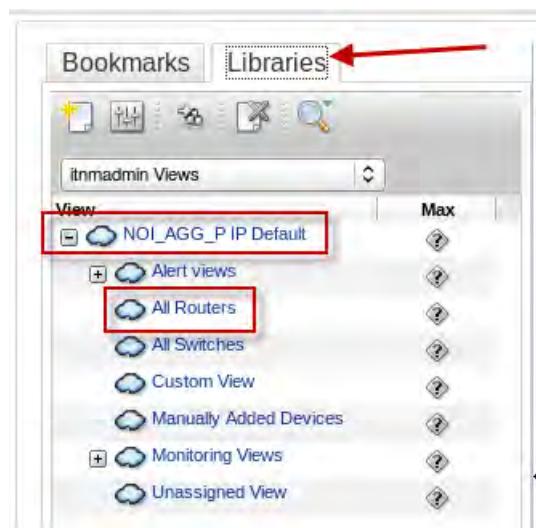
Phase	Status	Elapsed Time (H:MM:SS)	
		Current	Previous
Interrogating Devices	<input checked="" type="checkbox"/>	0:02:34	-
Resolving Addresses	<input checked="" type="checkbox"/>	0:00:08	-
Downloading Connections	<input checked="" type="checkbox"/>	-	-
Correlating Connectivity	<input checked="" type="checkbox"/>	0:00:03	-
Last status received:	Discovery is NOT running		

10. Examine the devices.

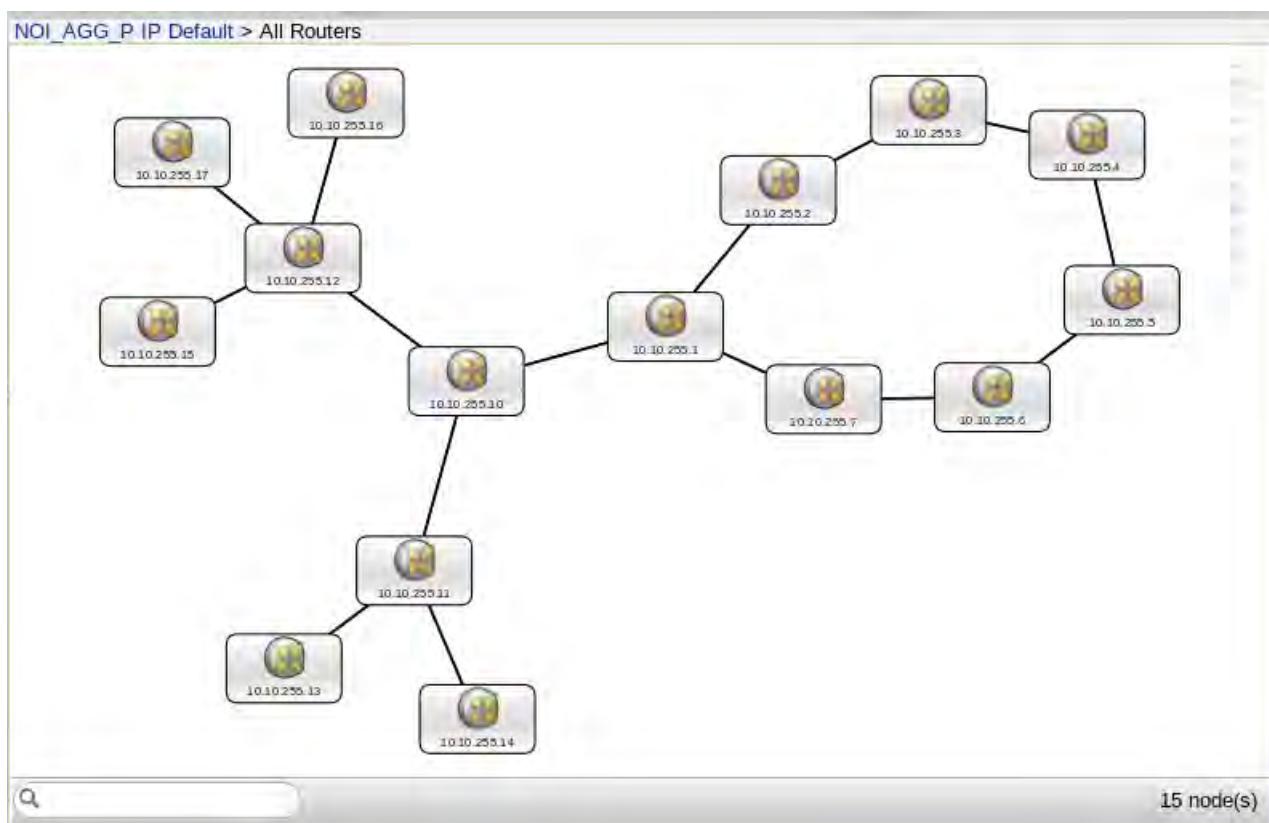
- a. Click the icon and select Network Views.



- b. Click **Libraries**. Expand **NOI\_ AGG\_P IP Default**. Click **All Routers**.



- c. Verify that the topology looks like the example shown here.



Leave the browser session as is. You return to it shortly.

# Verifying integration with Configuration Manager

Netcool Configuration Manager imports discovered devices periodically. You configured the frequency of this import in the previous unit. You set the value to every 5 minutes.

1. Check the log file to verify the import.

- a. Change to the target directory.

```
cd /opt/IBM/ncm/logs
```

- b. Check the file.

```
tail Intelliden.log
```

.

.

.

```
NMEntityMappingTimerTask,THR:71,WARN,NM Entity Mapping is running...
2016/03/01,22:42:16.820,com.intelliden.nmentitymapping.NMEntityMappingCompon
ent$NMEntityMappingTimerTask,THR:71,WARN,NM Entity Mapping returned 15
devices
```

This message indicates that Configuration Manager found 15 devices to import.

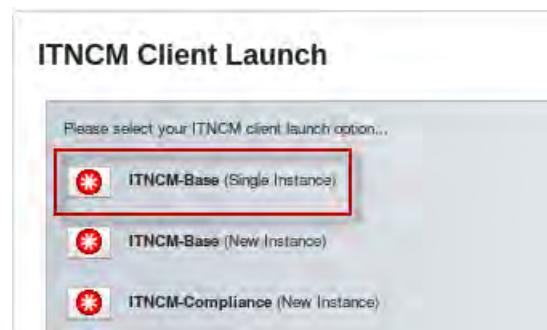


**Important:** You might need to repeat the tail command several times before the correct message appears.

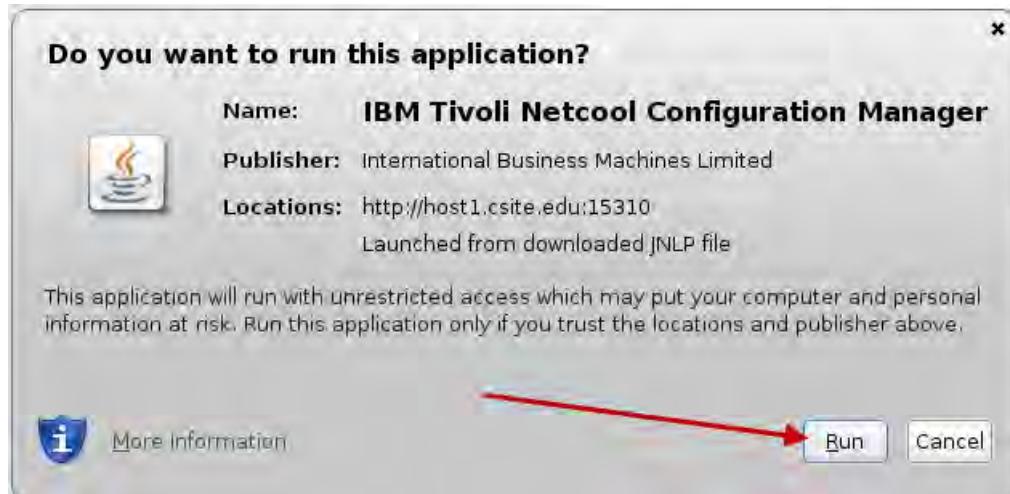
2. Return to the Firefox browser.
3. Click the icon and select **Client Launch**.



4. Click **ITNCM-Base (Single Instance)**.



## 5. Click Run.



The Configuration Manager client opens, and you are logged in as the **itnmadmin** user, which verifies that single sign-on works.

6. Under Queue Manager, click **Work That is Finished**.

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

7. Verify that you have 30 *units of work* (UOW) under **Work That is Finished**.

The screenshot shows the IBM Tivoli Netcool Configuration Manager interface. The left pane displays a tree view of the system structure, including ITNCM, Queue Manager, Resource Browser (with sub-folders like ITNCM, CommandSets, NativeCommands, Content, and NOI\_AGG\_P), and Systems Manager. The right pane is a table titled 'UOW ID' showing 30 rows of data. The columns are UOW ID, Type, Submitter, Request Type, and Execution Status. All entries show 'UOW' as the type, 'administrator' as the submitter, 'Import Configuration' as the request type, and 'SUCCESS' as the execution status. The table includes navigation buttons for page size (100), page number (1 / 1), and row selection (1 - 30 (30)).

UOW ID	Type	Submitter	Request Type	Execution Status
16	UOW	administrator	Import Configuration	SUCCESS
17	UOW	administrator	Import Configuration	SUCCESS
18	UOW	administrator	Import Configuration	SUCCESS
19	UOW	administrator	Import Configuration	SUCCESS
20	UOW	administrator	Import Configuration	SUCCESS
21	UOW	administrator	Import Configuration	SUCCESS
22	UOW	administrator	Import Configuration	SUCCESS
23	UOW	administrator	Import Configuration	SUCCESS
24	UOW	administrator	Import Configuration	SUCCESS
25	UOW	administrator	Import Configuration	SUCCESS
26	UOW	administrator	Import Configuration	SUCCESS
27	UOW	administrator	Import Configuration	SUCCESS
28	UOW	administrator	Import Configuration	SUCCESS
29	UOW	administrator	Import Configuration	SUCCESS
30	UOW	administrator	Import Configuration	SUCCESS

If you do not see 30 *units of work*, click the blue arrows icon to refresh the display. Wait until you see 30 complete *units of work* before you proceed.

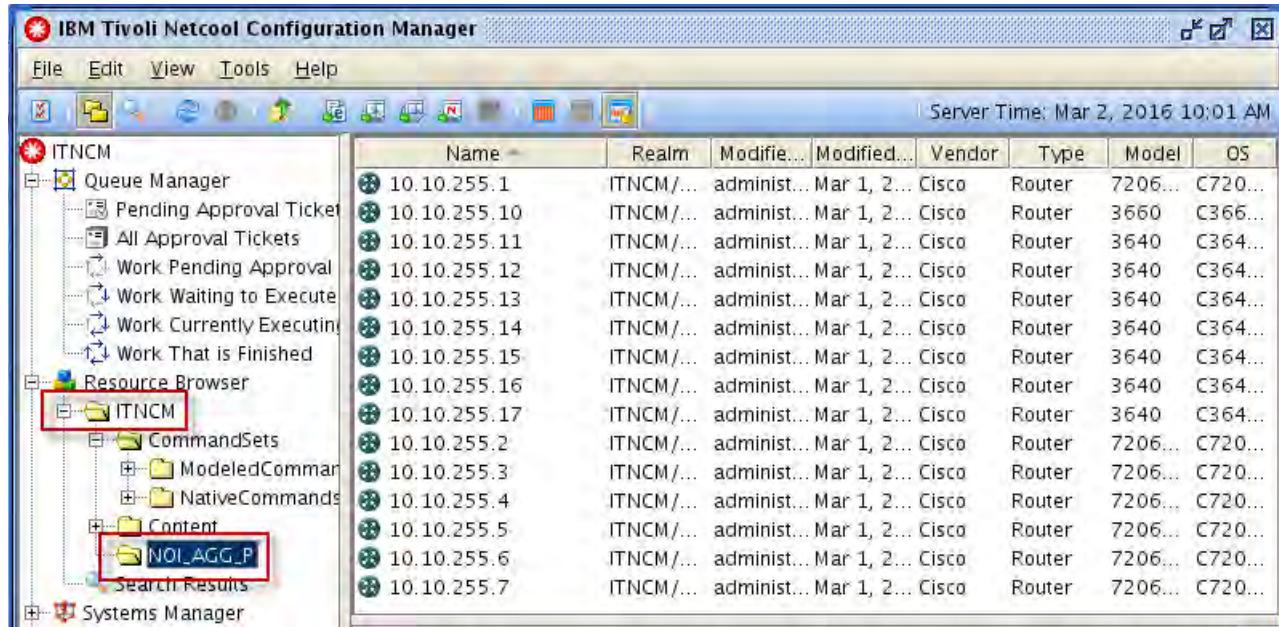
The units of work verify that device synchronization between Network Manager and Configuration Manager works.

8. Under Resource Browser, click **NOI\_AGG\_P**.

The screenshot shows the IBM Tivoli Netcool Configuration Manager interface. The left pane displays a tree view of the system structure, including ITNCM, Queue Manager, Resource Browser (with sub-folders like ITNCM, CommandSets, NativeCommands, Content, and NOI\_AGG\_P), and Systems Manager. The right pane is a table showing 10 entries of imported routers. The columns are Name, Realm, Modified..., Modified..., Vendor, Type, Model, and OS. All entries show 'ITNCM/...' as the realm, 'Mar 1, 2...' as the modified date, 'Cisco' as the vendor, 'Router' as the type, '7206...' as the model, and 'C720...' as the OS. The table includes navigation buttons for page size (100), page number (1 / 1), and row selection (1 - 10 (10)).

Name	Realm	Modified...	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...

Observe the entries for the imported routers.

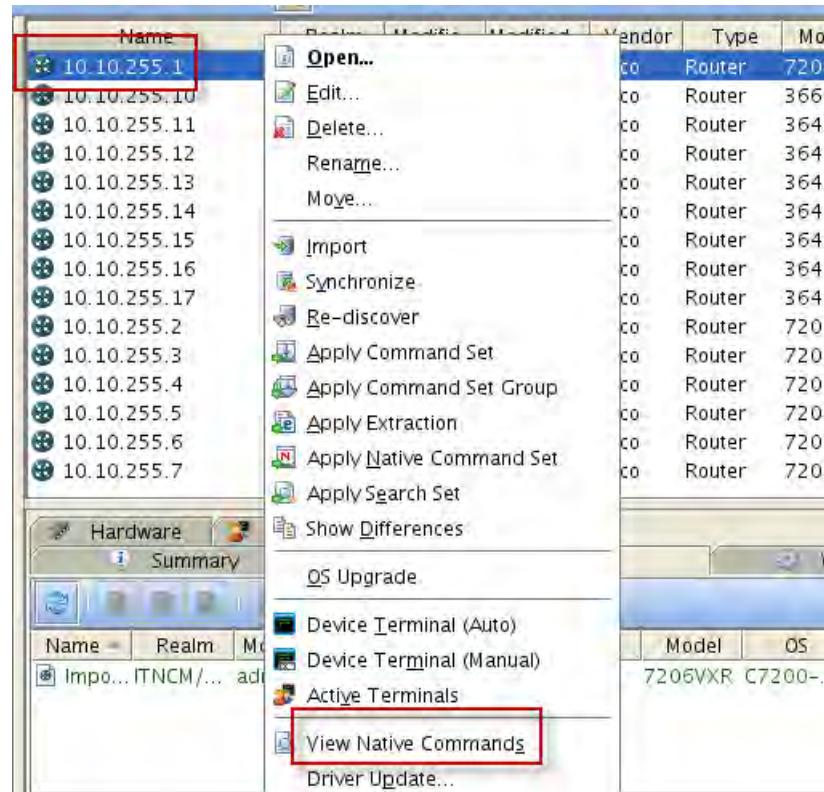
9. Under Resource Browser, click **NOI\_AGG\_P**.10. Click any entry to select it. Click the **Configurations** tab.

The screenshot shows the Resource Browser with two entries selected: '10.10.255.1' and '10.10.255.10', both highlighted with red boxes. Below the table, a navigation bar has tabs: 'Hardware', 'Activity', 'Compliance', 'Summary', 'Configurations' (which is highlighted with a red arrow), and 'Work'. At the bottom, there is another table with one row, also highlighted with a red box. This bottom table represents the configuration for the selected device.

Name	Realm	Modified...	Modified...	Vendor	Type	Model	OS
Impo...	ITNCM/...	administ...	Mar 1, 2...	Cisco	Router	7206VXR	C7200-...

The entry in the bottom view represents the configuration for the selected device.

11. Click any entry to select it. Right-click and select **View Native Commands**.



12. Observe the actual device configuration. Close the view.

```

Native Commands - Imported Configuration (10.10.255.1)
File Search Page 1: | 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

00001: version 12.3
00002: service timestamps debug datetime msec
00003: service timestamps log datetime msec
00004: no service password-encryption
00005: !
00006: hostname BRU-Core-01
00007: !
00008: boot-start-marker
00009: boot-end-marker
00010: !
00011: no logging console
00012: enable password object00
00013: !
00014: aaa new-model
00015: !
00016: !
00017: aaa session-id common
00018: ip subnet-zero
00019: !
00020: !
00021: !
00022: ip cef
00023: ip audit po max-events 100
00024: !
00025: !
00026: !

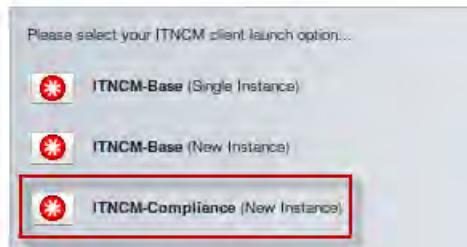
```

Leave the configuration client open. You use it again shortly.

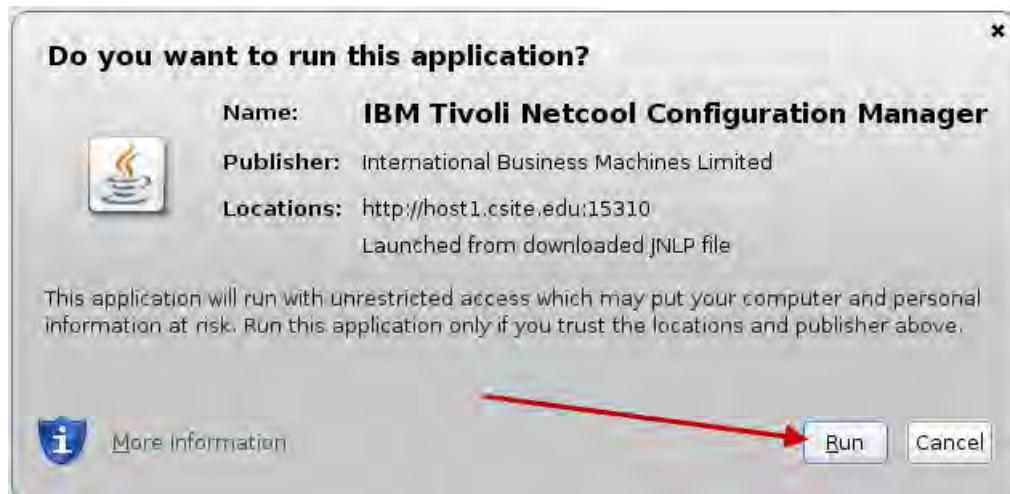
# Verifying Compliance Management

1. Return to the Firefox browser.
2. Click **ITNCM-Compliance (New Instance)**.

## ITNCM Client Launch



3. Click **Run**.

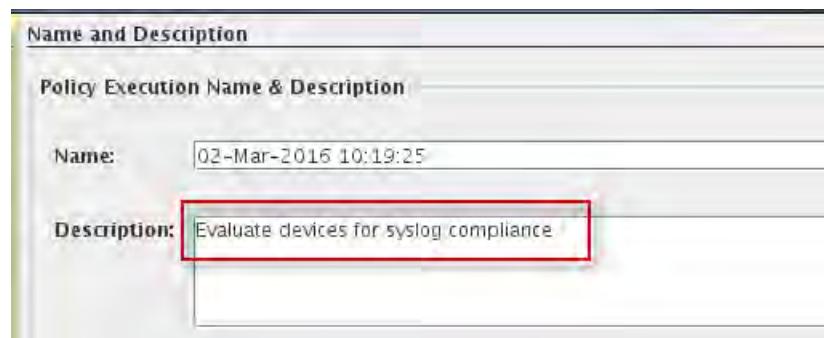


4. Evaluate the imported devices for compliance.
  - a. Select the **Execution** tab.
  - b. Under Policies, click **USISA**.
  - c. Click **Enable USISA syslog server**.

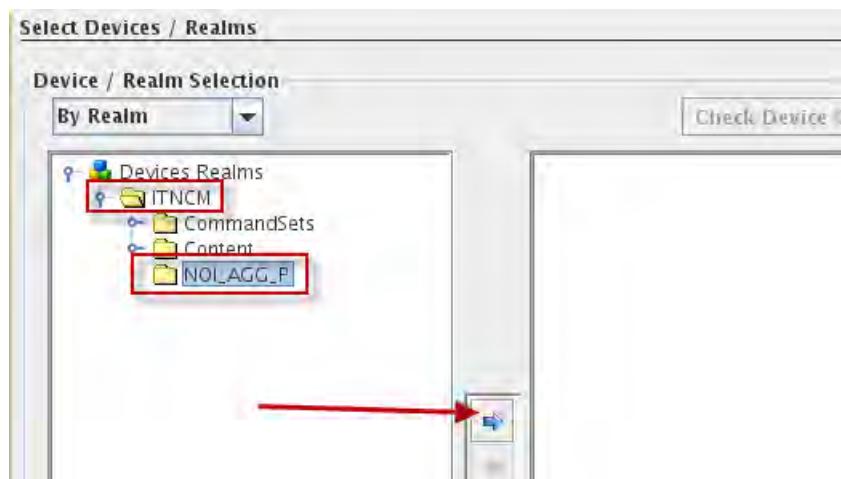
d. Click **Execute**.



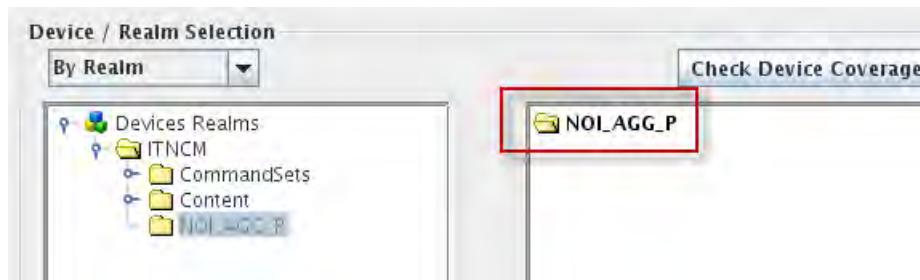
5. Enter a value for description, and click **Next**.



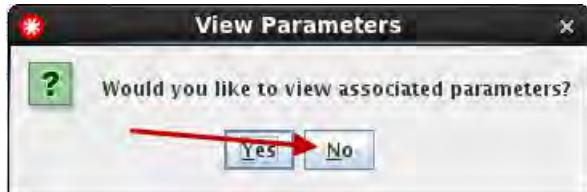
6. Expand the **ITNCM** realm. Click **NOI\_AGG\_P** to select it. Click the *right arrow* icon to select the devices in the realm.



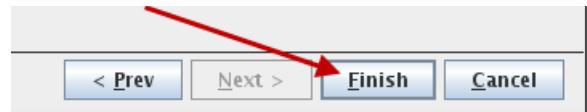
7. Click **Next**.



8. Click **No**.

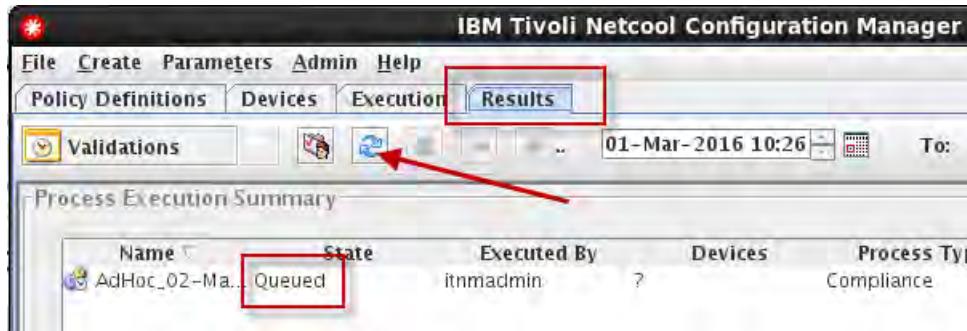


9. Click **Finish**.



The **Results** tab opens automatically. You see an entry in the Queued state.

10. Click the *blue arrows* icon to refresh the display.



11. Repeat the refresh until the state shows **Finished**.

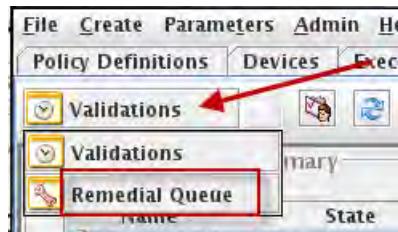


12. Click the entry to select it. Observe the results in the lower pane.

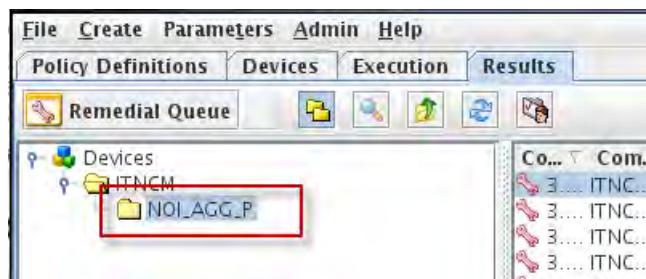
The screenshot shows two windows side-by-side. The top window is titled 'Process Execution Summary' and lists a single entry: 'AdHoc\_02-Mail...', State: 'Finished', Executed By: 'ithmadmin', Devices: '15', Process Type: 'Compliance', Execution Type: 'AdHoc', and Start Date: '02-Mar-'. The bottom window is titled 'Policy Validation Summary' and shows a table with one row: Policy Name 'Enable USISA s...', Severity '3', Revision '1', Date '02-Mar-2016 12:00:0', Status: 'Passed' (highlighted with a red box), Failed count '15' (highlighted with a red box), and Not Assessed count '0'.

The compliance policy evaluated 15 devices and they all failed.

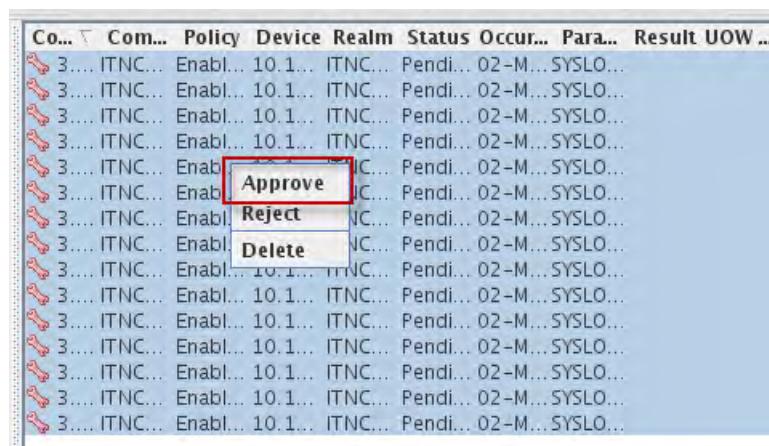
13. Click **Validations**, and select Remedial Queue.



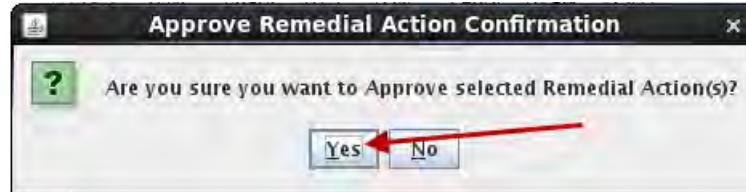
14. Expand **ITNCM**, and click **NOI\_AGG\_P**.



15. Select all of the entries. Right-click, and select **Approve**.

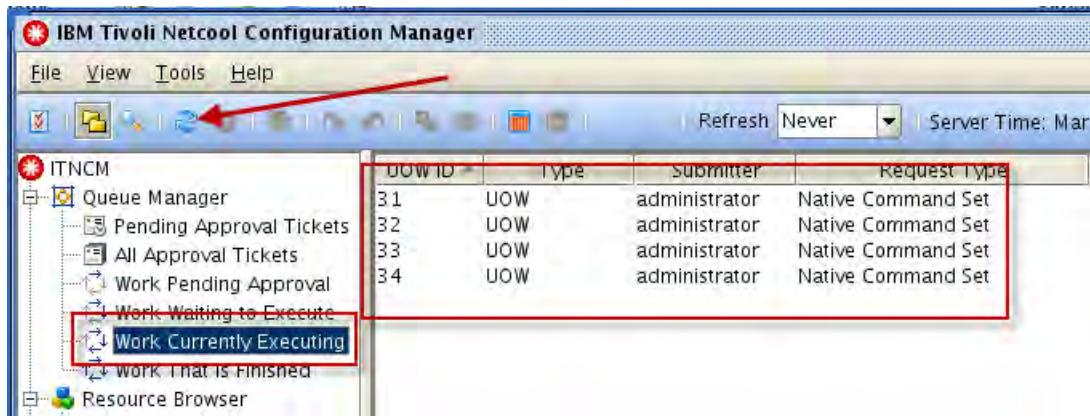


16. Click **Yes** to confirm the approval.



17. Return to the configuration manager client.

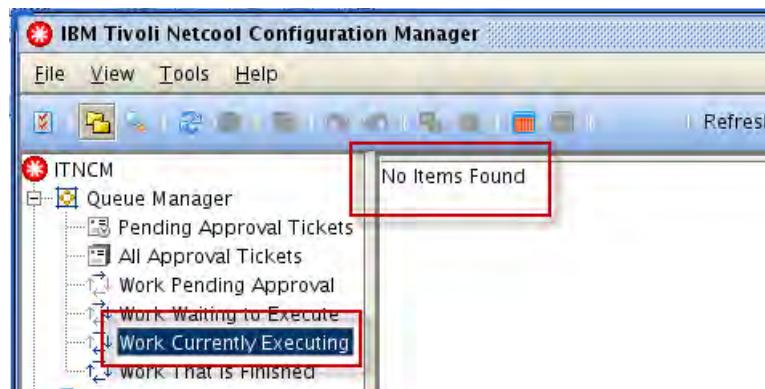
18. Under Queue Manager, click **Work Currently Executing**.



You see four *units of work*.

 Hint: Click the blue arrows icon to refresh the display if you do not see any *units of work*.

19. Click the *blue arrows* icon to refresh the display until the units of work are complete.



20. Under Queue Manager, click **Work That is Finished**. Verify that all *units of work* completed successfully.

The screenshot shows the IBM Tivoli Netcool Configuration Manager interface. On the left, the navigation tree under 'ITNCM' includes 'Queue Manager' with several sub-options like 'Pending Approval Tickets', 'All Approval Tickets', 'Work Pending Approval', 'Work Waiting to Execute', 'Work Currently Executing', and 'Work That is Finished'. The 'Work That is Finished' option is highlighted with a red box. On the right, a table lists 45 completed units of work (UOW). The columns are UOW ID, Type, Submitter, Request Type, and Execution Status. All entries show 'Native Command Set' as the Request Type and 'SUCCESS' as the Execution Status. A red box highlights the entire table area.

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

21. Under Resource Browser, click **NOI\_AGG\_P**. Click any device entry to select it. Click the **Configurations** tab.

The screenshot shows the IBM Tivoli Netcool Configuration Manager interface. On the left, the navigation tree under 'ITNCM' includes 'Queue Manager' and 'Resource Browser'. In 'Resource Browser', the 'Content' folder contains a sub-item 'NOI\_AGG\_P', which is highlighted with a red box. The main pane displays a table of devices, with the first entry '10.10.255.1' highlighted with a red box. At the bottom, a navigation bar has tabs for 'Hardware', 'Activity', 'Compliance', and 'Configurations'. An arrow points from the text in step 21 to the 'Configurations' tab. Below the table, another table shows two configuration files: 'Imp...' and 'Nati...', both listed as 'Versioned'.

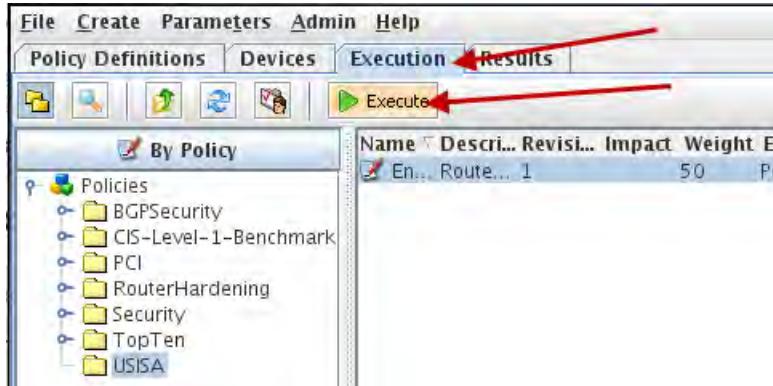
Name	Realm	Modific...	Modific...	Vendor	Type	Model	OS
10.10.255.1	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	7206...	C720...
10.10.255.10	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	3660	C366...
10.10.255.11	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	3640	C364...
10.10.255.12	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	3640	C364...
10.10.255.13	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	3640	C364...
10.10.255.14	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	3640	C364...
10.10.255.15	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	3640	C364...
10.10.255.16	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	3640	C364...
10.10.255.17	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	3640	C364...
10.10.255.2	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	7206...	C720...
10.10.255.3	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	7206...	C720...
10.10.255.4	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	7206...	C720...
10.10.255.5	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	7206...	C720...
10.10.255.6	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	7206...	C720...
10.10.255.7	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	7206...	C720...

Name	Realm	Modific...	Modific...	Vendor	Type	Model	OS	State
Imp...	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	7206VXR	C7200-...	Versioned
Nati...	ITNCM/...	adminis...	Mar 2, ...	Cisco	Router	7206VXR	C7200-...	Current

You see two configuration files. One file is from the original import. The second file was retrieved after compliance remediation modified the device.

22. Return to the compliance manager client.

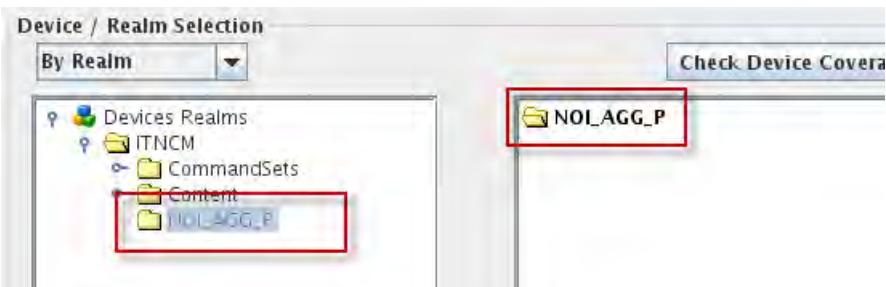
23. Click the **Execution** tab. Click **Execute**.



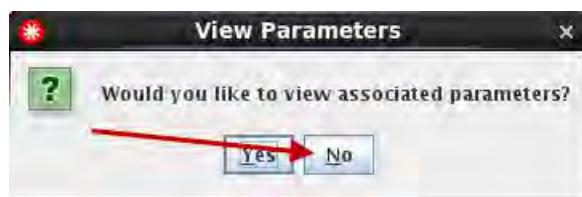
24. Enter a value for description, and click **Next**.

Name and Description	
Policy Execution Name & Description	
Name:	02-Mar-2016 13:03:22
Description:	Re-check syslog compliance.

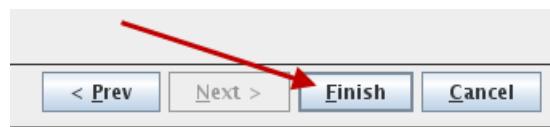
25. Select the **NOI\_AGG\_P** realm, and click **Next**.



26. Click **No**.

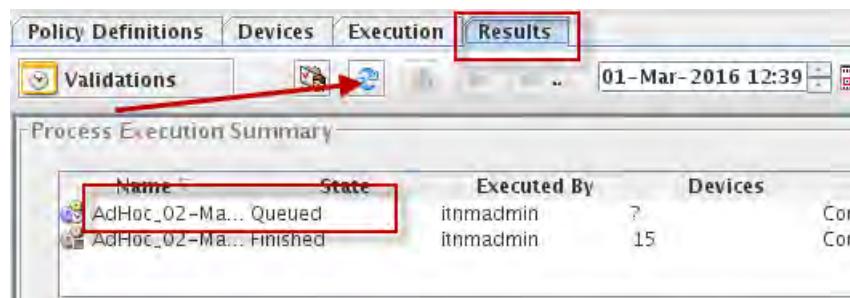


27. Click **Finish**.



The results view opens automatically. You see a second entry.

28. Click the *blue arrows* icon to refresh the display.



29. After the entry completes, click the entry to select it, and observe the results.

Name	State	Executed By	Devices	Process Type	Execution Type	Status
AdHoc_02-Ma...	Finished	itmadmin	15	Compliance	AdHoc	02-Mar
AdHoc_02-Ma...	Finished	itmadmin	15	Compliance	AdHoc	02-Mar

Policy Name	Severity	Revision	Date	Passed	Failed	Not A
Enable USISA s...	3	1	02-Mar-2016 13...	15	0	0

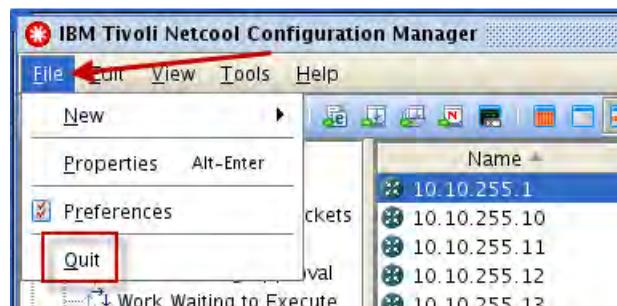
All 15 devices are compliant.

30. Click **File**, and select **Quit** to close the compliance manager client.



31. Click **Yes** to confirm the exit.

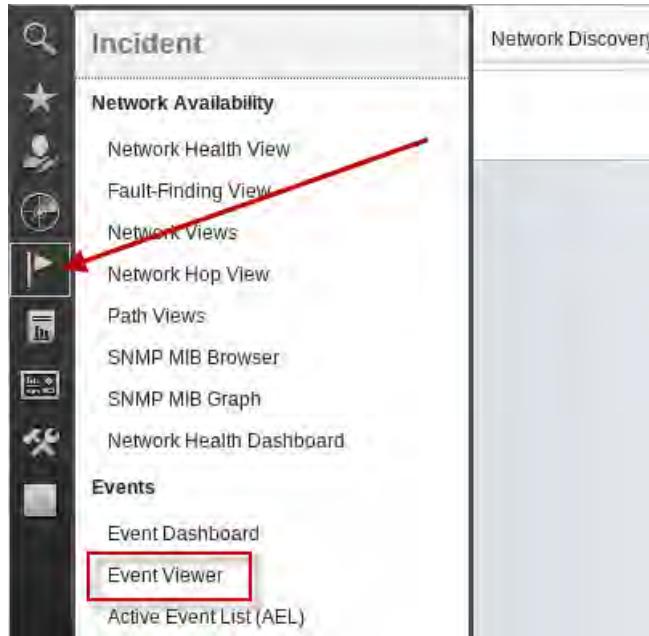
32. Click **File**, and select **Quit** to close the configuration manager client.



33. Click **OK** to confirm the exit.

## Verifying tool launch

1. Return to the Firefox browser.
2. Click the icon, and select Event Viewer.



3. Observe the events with Alert Group of Policy Trap.

The screenshot shows the 'Event Viewer' interface. At the top, there are various status indicators and a summary bar showing 0 errors, 0 warnings, 17 alerts, and 85 information messages. Below this is a table with columns: Sev, Ack, Node, Alert Group, and Summary. The 'Alert Group' column is highlighted with a red border. The table data is as follows:

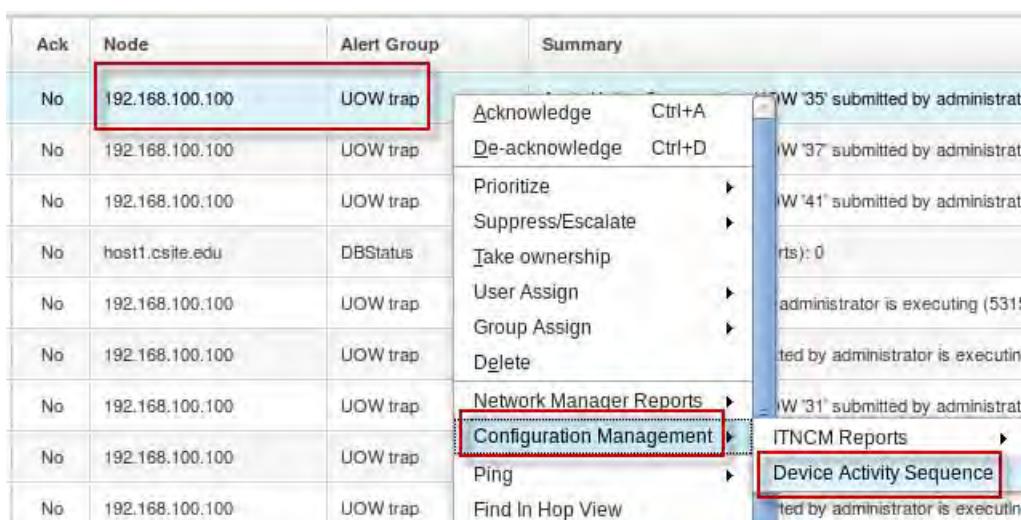
Sev	Ack	Node	Alert Group	Summary
!	No	10.10.255.12	Policy Trap	10.10.255.12 is in violation of policy Enable USISA syslog server
!	No	10.10.255.2	Policy Trap	10.10.255.2 is in violation of policy Enable USISA syslog server
!	No	10.10.255.14	Policy Trap	10.10.255.14 is in violation of policy Enable USISA 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

The Policy Trap events verify several features. First, Configuration Manager is sending traps to the SNMP Probe. Second, the probe is configured correctly to interpret the Configuration Manager traps.

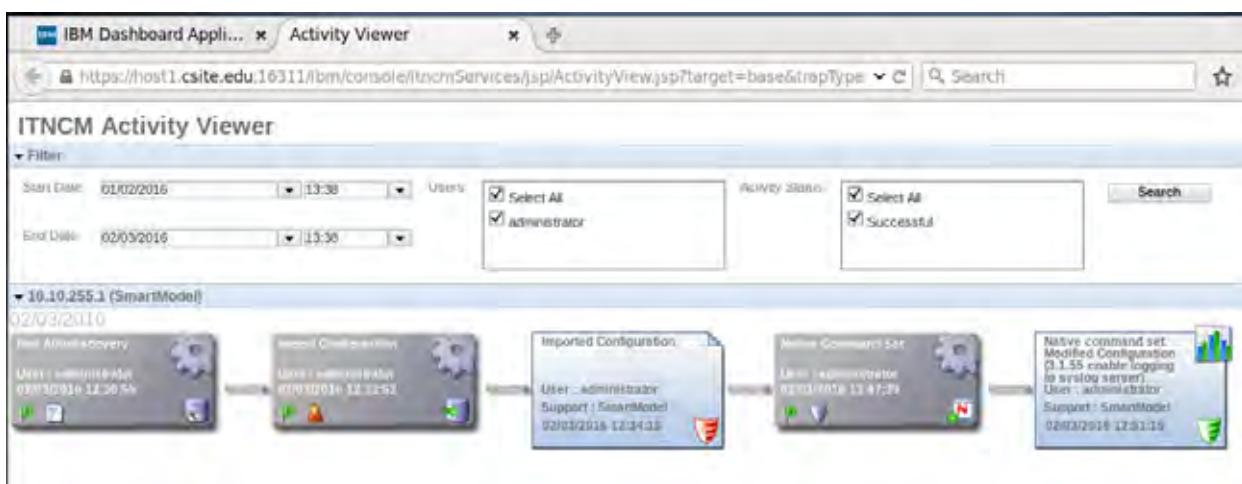
4. Scroll down within the event list until you find a **UOW trap**.

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, 12:32:55.5

5. Click any UOW trap event to select it. Right-click and select **Configuration Management > Device Activity Sequence**.



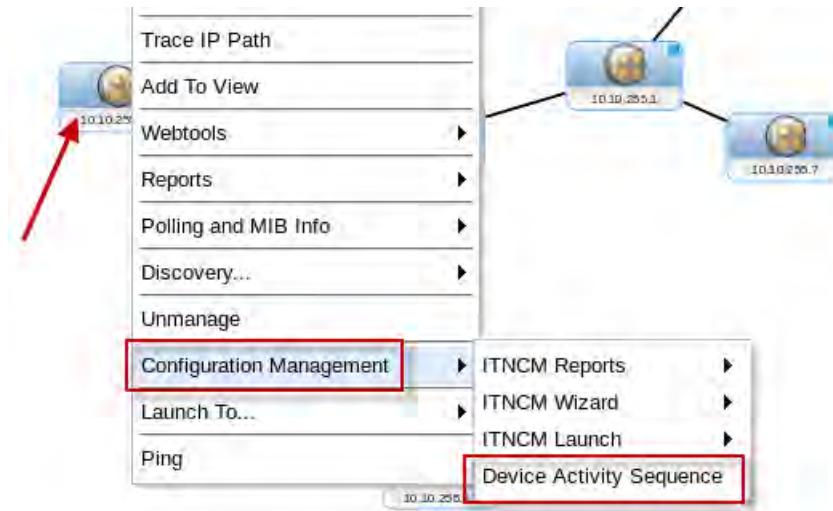
The Activity Viewer opens in a new tab.



Each box represents a separate Configuration Manager action.

6. Click the X to close the **Activity Viewer** tab.
7. Return to the Network Views page.

8. Click any device icon to select it. Right-click and select **Configuration Management > Device Activity Sequence**.



9. Change the **End Date** field to tomorrow, and click **Search**.

The screenshot shows the ITNCM Activity Viewer interface. The search filters are set to:

- Start Date: 01/02/2016 19:38
- End Date: 03/03/2016 19:38
- Users: Select All, administrator

The results section for device 10.10.255.16 (SmartModel) displays the message: "No data found for the selected device(s)".

**Note:** The default date range is not wide enough to locate all of the recent activities.

10. Observe the result. Click the X to close the tab.

The screenshot shows the ITNCM Activity Viewer interface with the following search parameters:

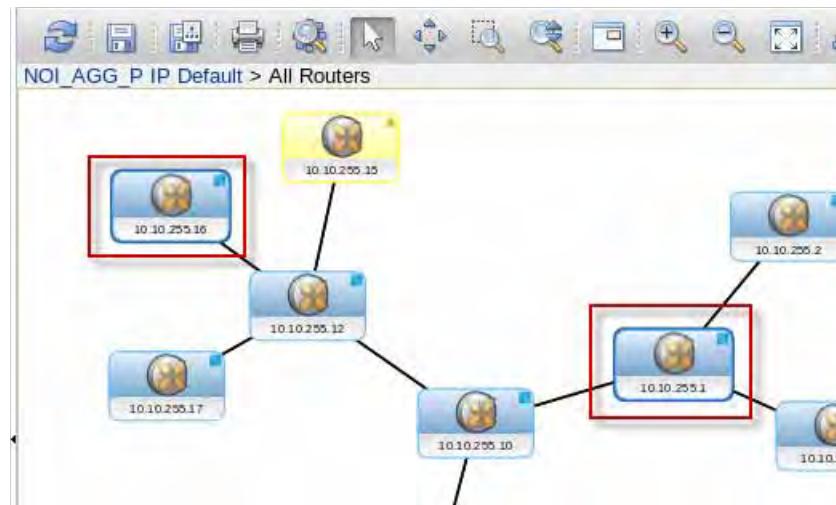
- Start Date: 01/02/2016 19:38
- End Date: 03/03/2016 19:38
- Users: Select All, administrator
- Activity Status: Select All, Successful

The results section for device 10.10.255.16 (SmartModel) shows a sequence of five activity boxes:

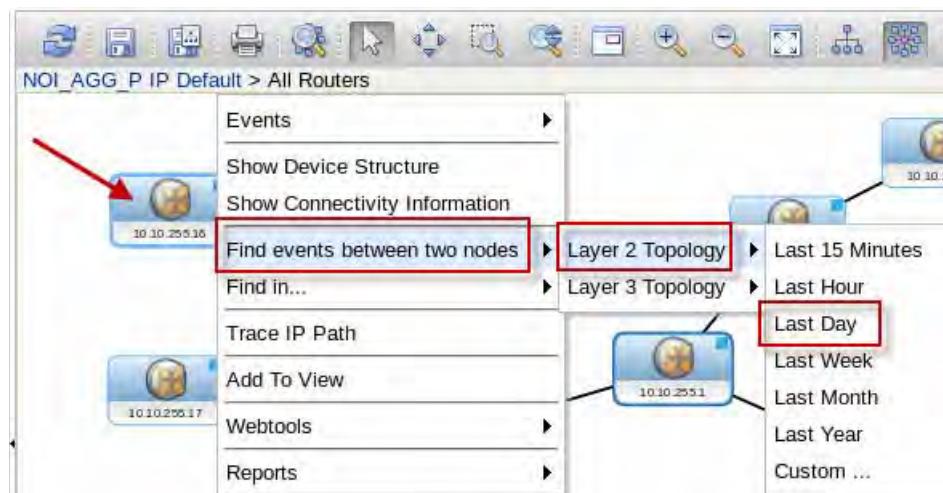
- Post Configuration: User: administrator, Support: SmartModel, 02/03/2016 12:30:55
- Import Configuration: User: administrator, Support: SmartModel, 02/03/2016 12:30:55
- Imported Configuration: User: administrator, Support: SmartModel, 02/03/2016 12:30:55
- Native Command Set: Modified Configuration (2.1.55 enable logging to syslog server), User: administrator, Support: SmartModel, 02/03/2016 12:31:10
- Native command set: Modified Configuration (2.1.55 enable logging to syslog server), User: administrator, Support: SmartModel, 02/03/2016 12:31:10

11. Return to the Network Views page.

12. Click a device icon to select it. Hold the Ctrl key, and click a second device icon to select it.

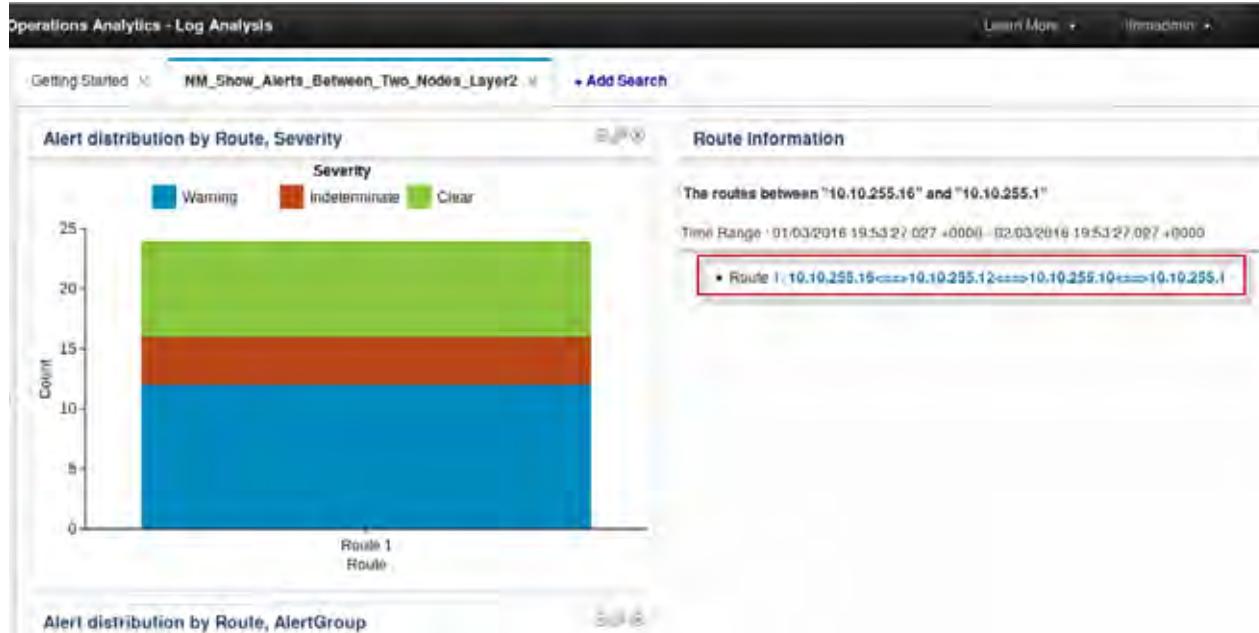


13. Right-click either device icon, and select **Find events between two nodes > Layer 2 Topology > Last Day**.

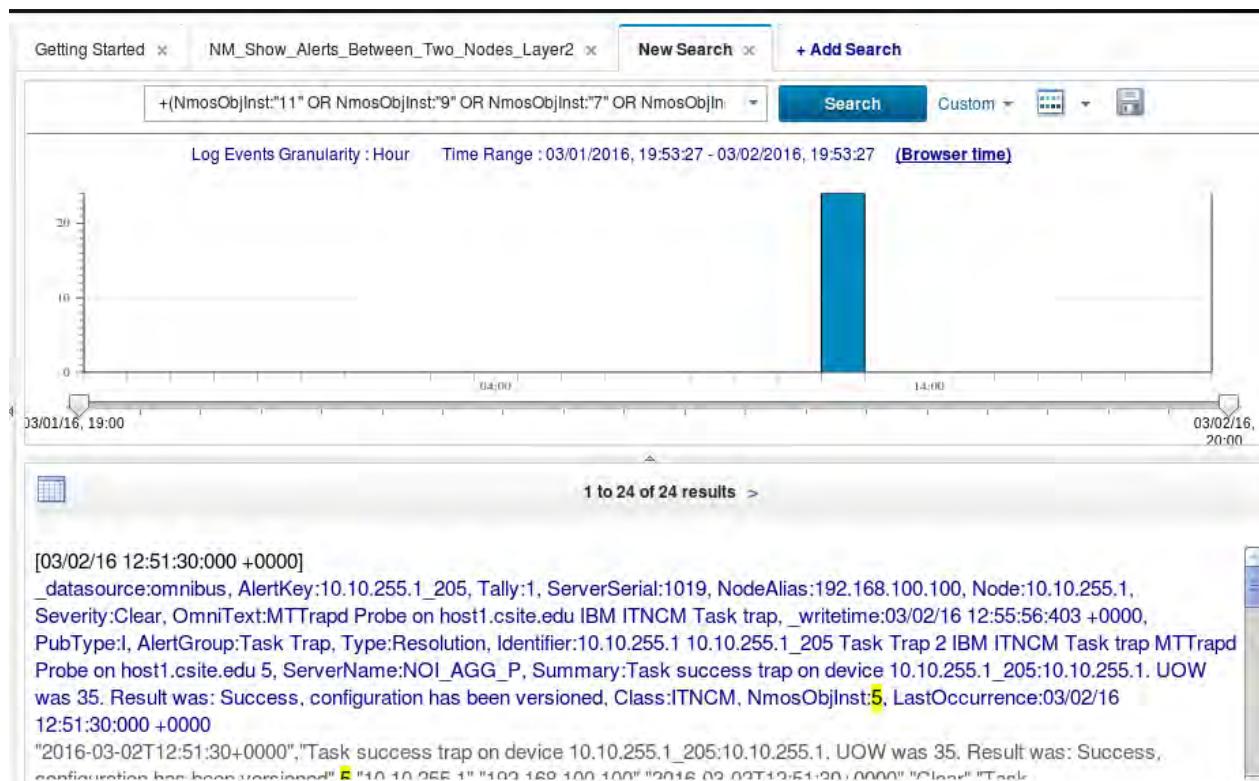


The Log Analysis user interface opens in a new Firefox tab. The topology search runs, and the event summary is displayed.

14. Click the Route 1 entry.



The event details are displayed.



15. Close the Log Analysis tab.

16. Log out of Dashboard Application Services Hub.

17. Close the Firefox browser.

The following list is a summary of the accomplishments from this unit:

- Discovered simulated routers with Network Manager
- Imported router configurations into Configuration Manager
- Evaluated the routers for compliance
- Modified the router configurations to make them compliant
- Verified tool launch capabilities





TN521 1.0



[ibm.com/training](http://ibm.com/training)

Authorized  
**IBM | Training**