

Course Exercises

IBM Netcool Operations Insight 1.6 Implementation and Configuration

Course code TN522 ERC 1.0



August 2019 edition

NOTICES

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

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

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

TRADEMARKS

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

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

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

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

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

ITIL is a Registered Trade Mark of AXELOS Limited.

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

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

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

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

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

© Copyright International Business Machines Corporation 2019.

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

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

Contents

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.....	14
Exercise 1 DB2	14
Installing DB2	14
Configuring DB2 to start at system start	16
Installing the DB2 license file	17
Exercise 2 Netcool/OMNibus core	19
Installing IBM Installation Manager	19
Installing Netcool/OMNibus core	20
Creating the ObjectServer	23
Verifying the initial configuration	27
Verifying basic ObjectServer function	28
Adding a password to the root ObjectServer user	30
Configuring event archiving	30
Configuring Netcool/OMNibus to start at system start	40
Exercise 3 Netcool/OMNibus Web GUI	42
Installing Jazz for Service Management	42
Installing Web GUI	52
Configuring Netcool/OMNibus Web GUI to start at system start	58
Exercise 4 Configuring LDAP as an authentication source	59
Removing the ObjectServer user repository	59
Adding the LDAP user repository	65
Configuring Dashboard Application Services Hub to allow logins when LDAP is down	74
Configuring ObjectServer synchronization	77
Configuring default users and groups	78
Configuring Tivoli Common Reporting	85
Exercise 5 Netcool/Impact	100
Installing the software	100
Configuring Netcool/Impact to use LDAP	104
Configuring Netcool/Impact to use single sign-on	109
Integrating the Netcool/Impact console	114
Enabling users for access to the Netcool/Impact console	117
Configuring Netcool/Impact to start at system start	118
Exercise 6 IBM Operations Analytics Log Analysis	120
Verifying prerequisites	120
Installing the software	122
Configuring Log Analysis to use LDAP	125
Configuring Log Analysis to use single sign-on	130

Updating passwords in configuration files	132
Configuring Log Analysis to start at system start	135
Enabling the Log Analysis product key	136
Configuring the Network Manager workaround	137
3 Configuring IBM Netcool Operations Insight base exercises	140
Exercise 1 Netcool/OMNibus Insight Pack	140
Installing the OMNibus Insight Pack	140
Creating the Log Analysis data source	141
Configuring Web GUI	144
Exercise 2 Message Bus Gateway	145
Configuring SSL	146
Installing the gateway	150
Configuring the ObjectServer	151
Configuring the gateway	154
Verifying the gateway operation	158
Configuring user access to the Event Search feature	161
Verifying the Event Search feature	167
Exercise 3 Configuring Event Analytics	169
Configuring the Related Events feature	169
Configuring seasonality	184
Running the analytics wizard	186
4 IBM Tivoli Network Manager exercises	189
Exercise 1 Installing the SNMP probe	189
Exercise 2 Installing and configuring a topology database	198
Installing the database creation scripts	198
Creating the topology database	201
Exercise 3 Installing Tivoli Network Manager	204
Updating smadmin roles	204
Installing Network Manager core components	205
Installing Network Manager GUI components	209
Installing Network Manager Reports	213
Installing Network Health Dashboard	215
Configuring the Network Health Dashboard	218
Exercise 4 Performing post-installation configuration	219
Configuring the Tivoli Netcool/OMNibus Web GUI data source name	219
Configuring the core components to run as a non-root user	220
Configuring processes to start automatically	221
Adding Network Manager environment variables to the netcool user	222
Adding MIB files	223
Removing the ObjectServer users	223
Verifying the installation	225
Exercise 5 Installing the Network Manager Insight Pack	234
Installing the Insight Pack	234
Configuring the Insight Pack	235
Modifying the ObjectServer	242
Installing the tools in Web GUI	243

Configuring the tools in Network Manager244
5 IBM Tivoli Netcool Configuration Manager exercises	247
Exercise 1 Creating users	247
Creating the database user ID	247
Creating the FTP user ID	248
Exercise 2 Creating the database	249
Exercise 3 Installing Jazz for Service Management	252
Exercise 4 Installing Netcool Configuration Manager	261
Installing the presentation server	261
Installing the Netcool Configuration Manager GUI components	268
Installing Common Reporting reports	272
Exercise 5 Installing device drivers	276
Installing the standard device drivers	276
Installing the Smart Model device drivers	278
Installing auto-discovery	280
Exercise 6 Post-installation configuration	283
Copying required Java files	283
Changing passwords	284
Configuring Java Webstart	286
Configuring SNMP trap destination	293
Updating the Work Distribution resource	295
Creating resources to support device import	297
Exercise 7 Configuring integration with Tivoli Network Manager	301
Creating users and groups	301
Adding existing users to Netcool Configuration Manager groups	307
Assigning roles in Dashboard Application Services Hub	310
Configuring the presentation server to use LDAP	312
Configuring the presentation server for single sign-on	324
Configuring access rights for existing users	329
Verifying single sign-on	333
Installing sample policy packs	335
Importing sample command sets	341
Configuring integration with Netcool/OMNIbus	348
Configuring device synchronization	350
Configuring the Network Health Dashboard	351
Setting the compliance user	351
Exercise 8 Configuring Out-of-Band Change (OOBC) daemon	352
Modifying the start script	356
Configuring auto-start	357
Verifying auto-start	358
6 Verifying Networks for Operations Insight exercises	361
Exercise 1 Starting the network simulator	361
Exercise 2 Solution verification	363
Discovering devices with Network Manager	363
Verifying integration with Configuration Manager	367
Verifying Compliance Management	371

Verifying tool launch	380
---------------------------------	-----



1 Netcool Operations Insight introduction and overview exercise

Before you install IBM Netcool Operations Insight, you must validate the target host. The exercises in this unit show you how to validate the host and operating system in your lab environment.



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

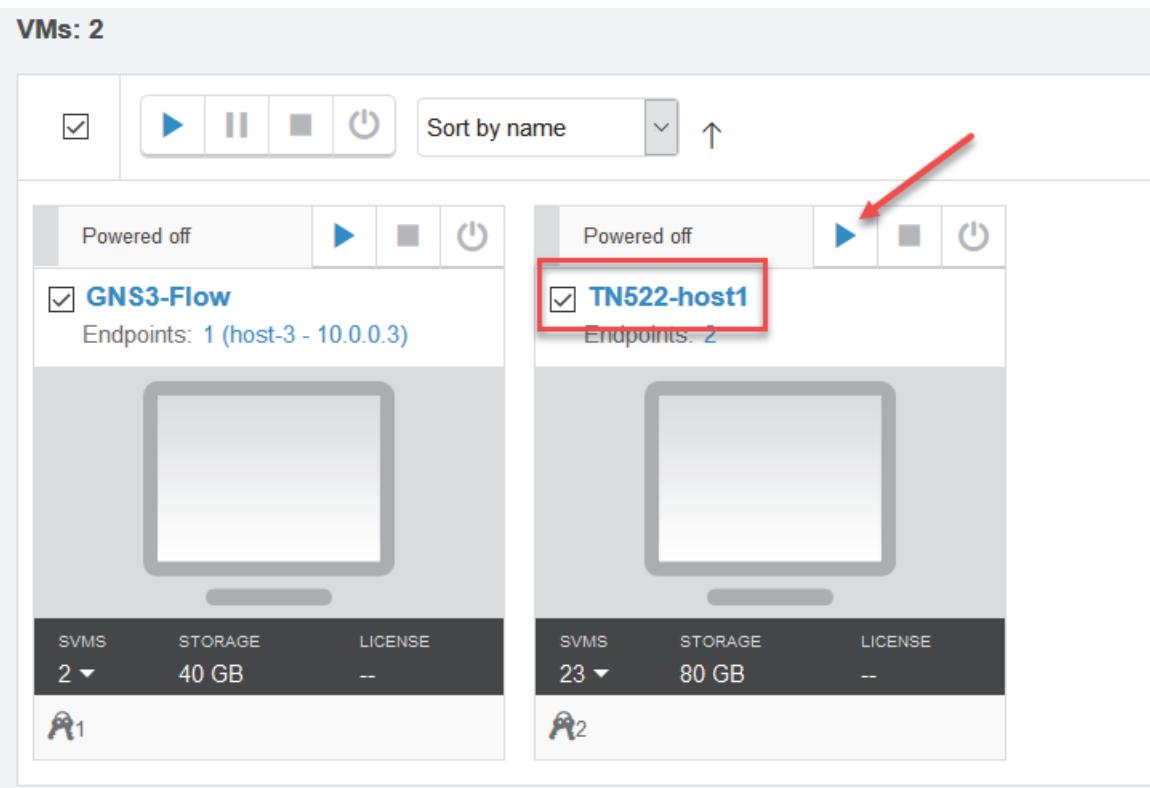
The requirements vary by operating system, and are detailed in the installation guide for the respective product.

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.

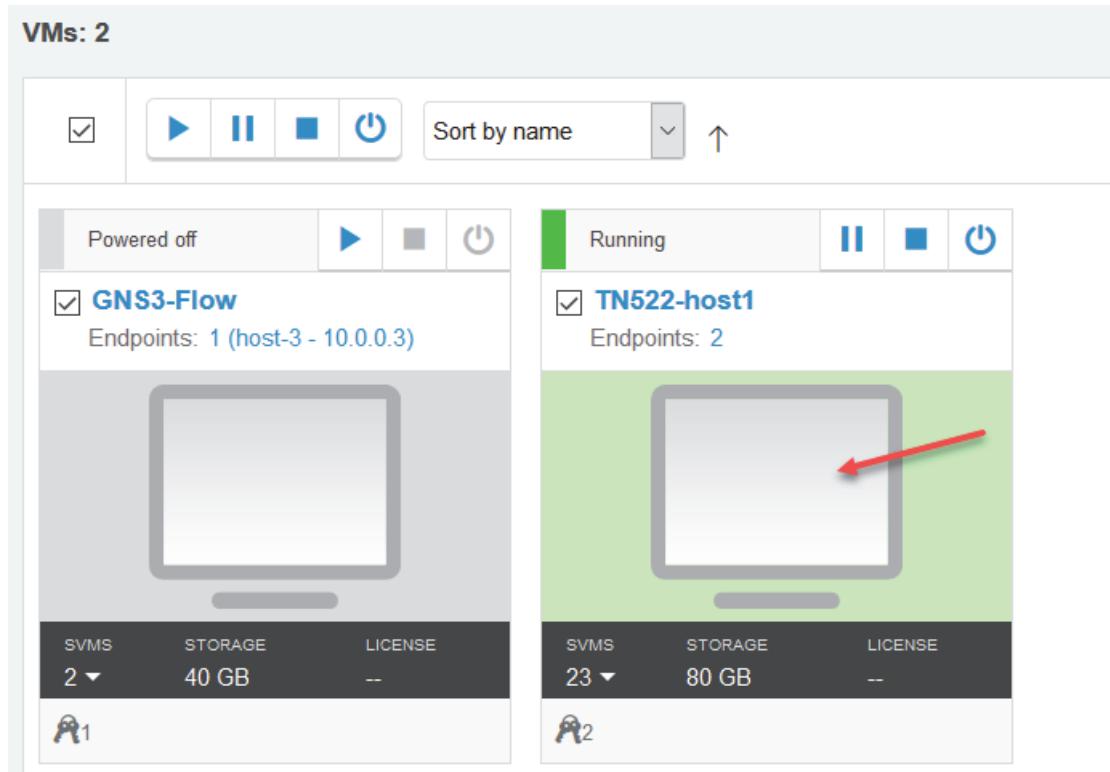
Task 1 Starting the image

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. Find the **TN522-host1** tile in the list of VMs. Click the Run button.



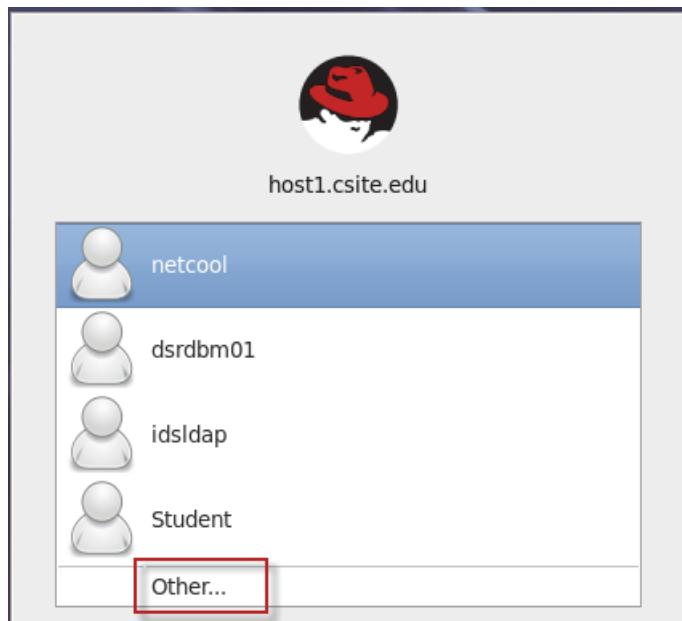
2. The image takes several minutes to start. After a few moments, click the **TN522-host1** tile to connect to the console of the virtual machine.



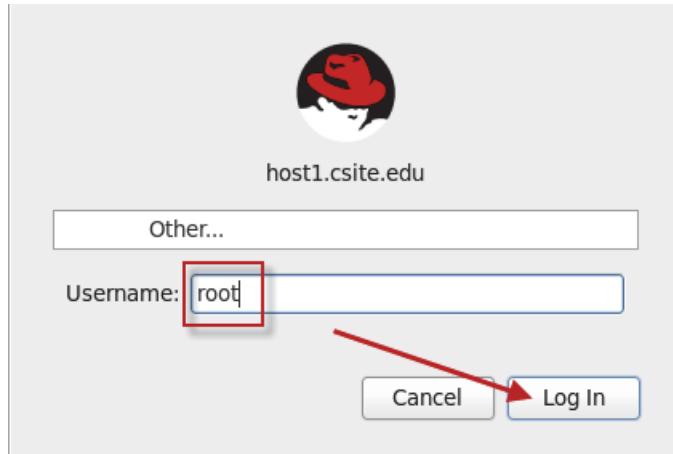
The image takes several minutes to start. The login screen opens when the image is available.

3. Log in as the root user:

- a. Click **Other**.



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

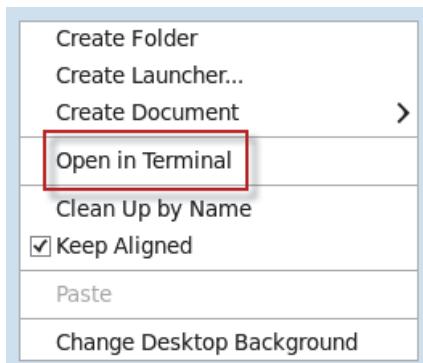


The password is **object00**.

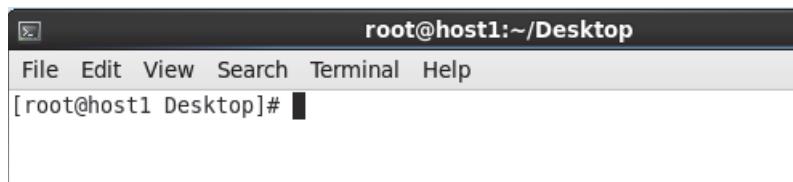
The Linux console window opens.

4. 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 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 1.2.0.18-Tivoli-PRS-Unix-fp0001.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: 1.2.0.18

Build : 20160602

OS name: Linux

User name: root

.

.

.

Aggregated Properties for Scanned Products:

Property	Result	Found
Expected	=====	=====
/	PASS	40960.00MB
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: 1.2.0.18

Build : 20160602

OS name: Linux

User name: root

.

.

Aggregated Properties for Scanned Products:

Property	Result	Found
Expected	=====	=====
	=====	=====
/	PASS	40960.00MB
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.
 - a. Export the required environment variable.

```
export IMPACT_PREREQ_BOTH=True
```

- b. Run the scanner to check Netcool/Impact requirements:

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

IBM Prerequisite Scanner

Version: 1.2.0.18

Build : 20160602

OS name: Linux

User name: root

...

Aggregated Properties for Scanned Products:

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

Overall result: FAIL (NCI 07010005: 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:

- a. Export the required environment variables.

```
export JazzSM_FreshInstall=True
export Include_TCR=True
export JazzSM_TYPICAL=True
```

Exercise 1 Validating the host1 server configuration

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

```
./prereq_checker.sh ODP detail
```

```
IBM Prerequisite Scanner
```

```
Version: 1.2.0.18
```

```
Build : 20160602
```

```
OS name: Linux
```

```
User name: root
```

```
.
```

```
.
```

```
.
```

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

Property	Result	Found
Expected	=====	=====
=====	=====	=====
/	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: 1.2.0.18

Build : 20160602

OS name: Linux

User name: root

.

.

.

Aggregated Properties for Scanned Products:

Property	Result	Found
Expected	=====	=====
/	PASS	48.00GB
6.33GB		

Overall result: PASS (DSH 03010300: 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: 1.2.0.18

Build : 20160602

OS name: Linux

User name: root

.

.

.

Aggregated Properties for Scanned Products:

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

Overall result: PASS (TCR 03010300: 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: 1.2.0.18
Build : 20160602
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

1. Run the scanner to check IBM Tivoli Network Manager requirements.

- a. Export the required environment variables.

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

- b. Run the prerequisite checker.

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

IBM Prerequisite Scanner

Version: 1.2.0.18

Build : 20160602

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

- Run the scanner to check IBM Tivoli Netcool Configuration Manager requirements.

- a. Export the required environment variables.

```
export TNCM_COMPLIANCE_CORE=true
export TNCM_COMPLIANCE_EVALUATION=true
export TNCM_PRESENTATION_SERVER=true
export TNCM_REPORTING=true
export TNCM_WORKER_SERVER=true
```

- b. Run the prerequisite checker.

```
./prereq_checker.sh NCM detail
```

```
IBM Prerequisite Scanner
Version: 1.2.0.18
Build : 20160602
OS name: Linux
User name: root

.
.
.

Property          Result    Found
Expected
=====
=====      =====      =====

CpuArchitecture      PASS      x86_64
i386,i686,x86,x86_64,AMD64
os.RAMSize           PASS      22.GB
8GB
network.fqdn         FAIL      False
True
network.UDPPortsInUse.NetworkTimeProtocol FAIL
PortsInUse:813,794,783,631,57959,45... 123
.
.
.

Aggregated Properties for Scanned Products:
Property          Result    Found
Expected
=====
=====      =====      =====

/                  PASS      40.00GB
10.00GB

Overall result: FAIL (NCM 06040100: FAIL)
```



Important: The scan fails due to host domain name and network time protocol requirements. This failure is not an issue for the class environment.

Task 4 Verifying the user environment

You install the software 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:501:501::/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 that the **/opt/IBM** directory exists and the netcool user owns it:

```
cd /opt  
ls -la  
drwxr-xr-x    6 netcool ncoadmin 4096 Aug 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  
tar -zxvf DB2_AWSE_REST_Svr_11.1_Lnx_86-64.tar.gz
```

2. Install DB2 with the setup wizard.

- a. Start the setup wizard.

```
cd server_awse_o/  
./db2setup -f sysreq
```

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. You can ignore any errors about prerequisites that are not met.

- b. Click **New Install**.

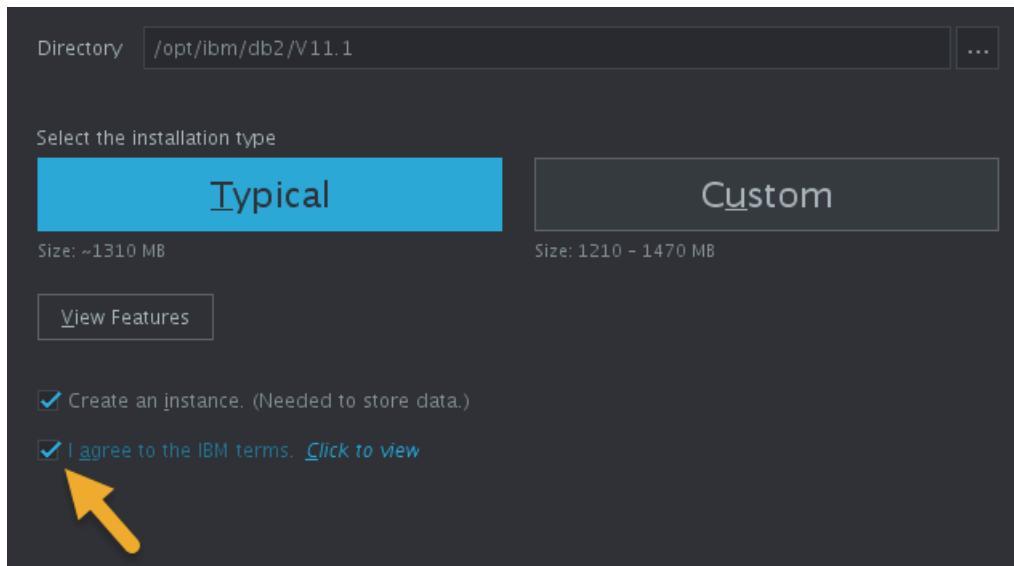
- c. Select **DB2 Version 11.1.0.0 Workgroup, Enterprise and Advanced Editions** and click **Next**.



d. Select **Typical**.

e. Select **I agree**.

f. Click **Next**.



- g. On the Instance Owner page, enter **object00** in both password fields, then click **Next**.



- h. On the Fenced User page, enter **object00** in both password fields, then click **Next**.



- i. Click **Finish**.



Note: The installation runs for approximately ten minutes.

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

Configuring DB2 to start at system start

Several methods 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
```

```
SQL1064N DB2STOP processing was successful.
```

- b. Start DB2.

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

```
SQL1063N DB2START processing was successful.
```

- 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. Run the following commands to expand the license installation files.

```
cd /tmp  
mkdir db2  
cd db2  
unzip /software/db2/DB2_AWSE_Restricted_Activation_11.1.zip
```

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

```
cd /tmp/db2/awse_o/db2/license/  
db2licm -a db2awse_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/V11.1/license/en_US.iso88591"

3. Verify the license information.

```
db2licm -l
```

Product name:	"DB2 Advanced Workgroup Server Edition"
License type:	"Restricted"
Expiry date:	"Permanent"
Product identifier:	"db2awse"
Version information:	"11.1"
Max amount of memory (GB):	"128"

4. Remove the DB2 installation files:

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

```
exit
```

- Remove the DB2 installation files:

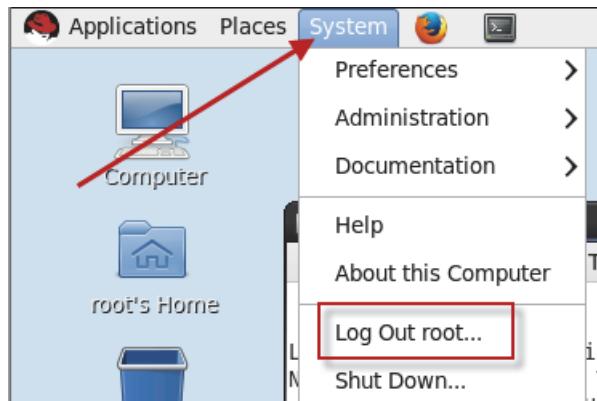
```
cd /software  
/bin/rm -R db2
```

- Remove the license files.

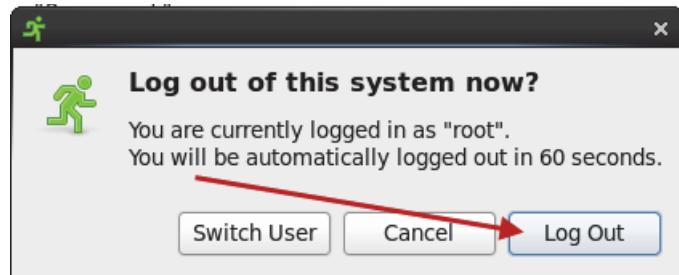
```
cd /tmp  
/bin/rm -R db2
```

5. Log out of the image as the root user.

- Click **System**, and select **Log Out root**.



- 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, then 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.

1. Expand the installation archive.

```
cd /software/iim
```

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

2. Install IBM Installation Manager.

```
./userinst
```

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

Installation Packages	Status	Vendor
IBM® Installation Manager		
IBM® Installation Manager 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: /home/netcool/IBM/InstallationManager/eclipse

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

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



The following package was installed:

IBM Installation Manager
IBM® Installation Manager 1.8.4

IBM Installation Manager stops and restarts.

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

3. 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 archive file.

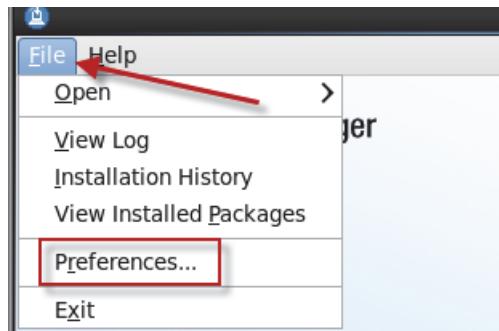
```
cd /software/omnibus
```

```
unzip TVL_NTCL_OMN_V8.1.0.19_CORE_LNX_M.zip
```

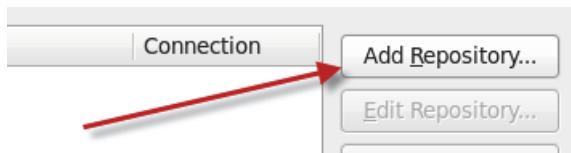
2. Install the software.

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

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

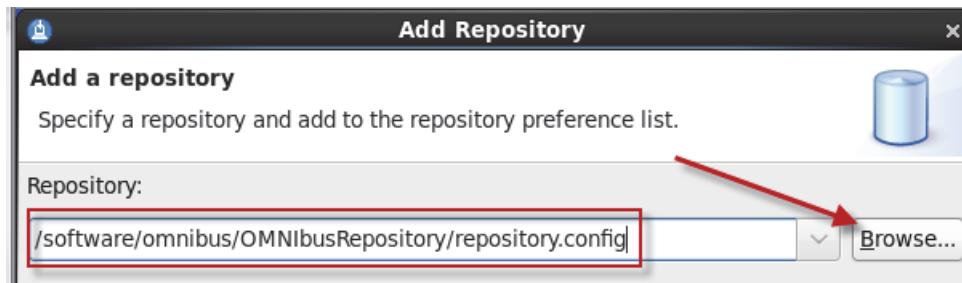


b. Click **Add Repository**.



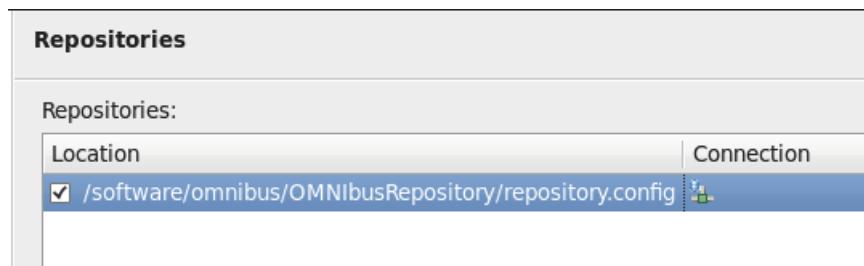
c. Click **Browse** and find the following file:

/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**.



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

- i. Leave the default directory location for shared resources, and click **Next**.

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

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

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

- Use the existing package group
 Create a new package group

Package Group Name	Installation Directory
IBM Netcool Core Components	/opt/IBM/tivoli/netcool

Package Group Name: IBM Netcool Core Components

Installation Directory: /opt/IBM/tivoli/netcool

Architecture Selection: 32-bit 64-bit

- l. Leave all of the features selected, and click **Next**.

- m. Leave the option for **Data migration** cleared, and click **Next**.



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

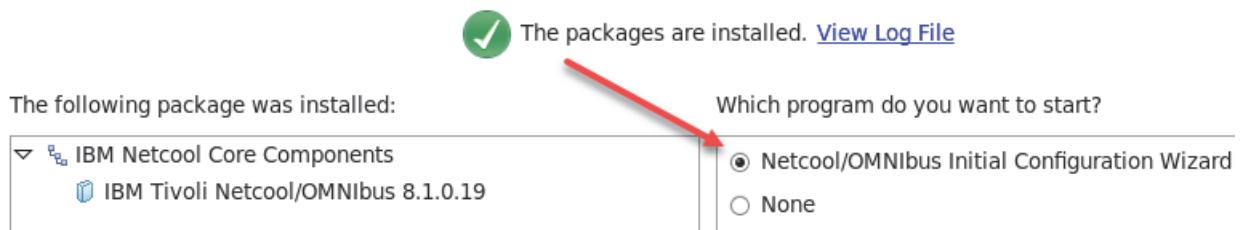
- n. Review the installation summary and click **Install**.



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

- o. Verify that the installation is successful.

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



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:

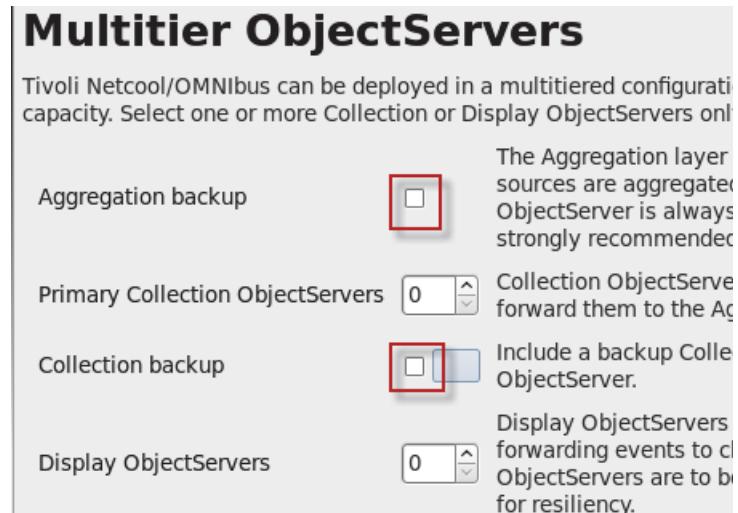
```
/opt/IBM/tivoli/netcool/omnibus/bin/nco_icw
```

1. Complete the configuration with the wizard as follows:
 - a. Scroll to the bottom of the page and click **Next**.

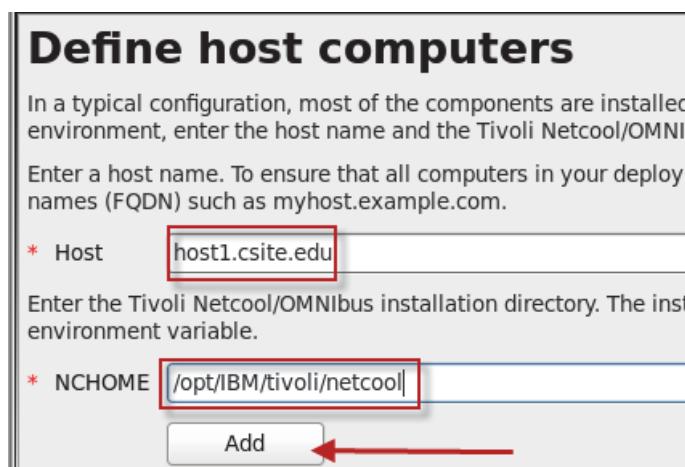


- b. Leave the option selected to create a new configuration and click **Next**.

- 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 the following example and click **Next**.

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

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

Process Agent configuration

A process agent (PA) that manages Tivoli Netcool/OMNibus components. Each process agent must have a unique name.

▼ Process Agent on host1.csuite.edu

Computer	host1.csuite.edu:/opt/IBM/tivoli/netcool
PA name	HOST1_PA
* Name prefix	HOST1
* PA port	4200

The prefix can optionally be used by the process agent.

The port number where the process agent runs.

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

▼ Primary Aggregate

ObjectServer name	NOI_AGG_P
* Computer	host1.csuite.edu - /opt/IBM/tivoli/netcool
Name prefix	NOI
* Server port	4100

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 on the page and click **Next**.

- Review the configuration summary and click **Next**.

Configuration summary

Here is a summary of the configuration components you have set.

- ObjectServers
 - Aggregation layer
 - NOI_AGG_P
 - Computer: host1.csuite.edu
 - Path: /opt/IBM/tivoli/netcool
 - Server port: 4100
 - IDUC port: 0
 - Process agents
 - HOST1_PA
 - Computer: host1.csuite.edu
 - Path: /opt/IBM/tivoli/netcool
 - PA port: 4200

- Click **Next** on the Save Configuration page.
- Click **Next** to apply the configuration.

Apply the configuration

The deployment descriptor has been saved. Now you must apply the configuration to each computer in your configuration. This wizard will guide you through the process. The file contains the required instructions and a checklist of the computers in your configuration.

/opt/IBM/tivoli/netcool/omnibus/etc/icw_instructions.txt

If you are ready to apply the configuration to this computer click **Next** now. If you prefer to apply the configuration to other computers later click **Exit** now, and follow the instructions when you are ready. The following components will be applied to this computer.

Component	Action
Interfaces file	Update /opt/IBM/tivoli/netcool/etc/omni.dat and run nco_igen
Process agent	Create configuration for this computer
Process agent	Add entry for ObjectServer NOI_AGG_P
ObjectServer	Create properties file and database for NOI_AGG_P

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

Successful application

The current configuration has been successfully applied to this computer. Follow the instructions and checklist contained in the file below to set up the other computers. Click **Exit** to leave the wizard.

/opt/IBM/tivoli/netcool/omnibus/etc/icw_instructions.txt

The configuration is applied to the system.

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

Forking to a Daemon Process.....



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:

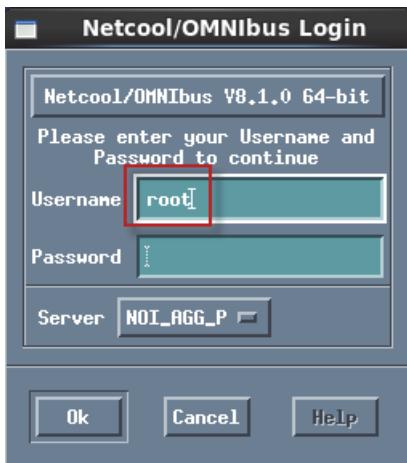
```
nco_p_simnet -server NOI_AGG_P &
```

2. Examine the simulated events.

- a. Start the native event list:

```
nco_event &
```

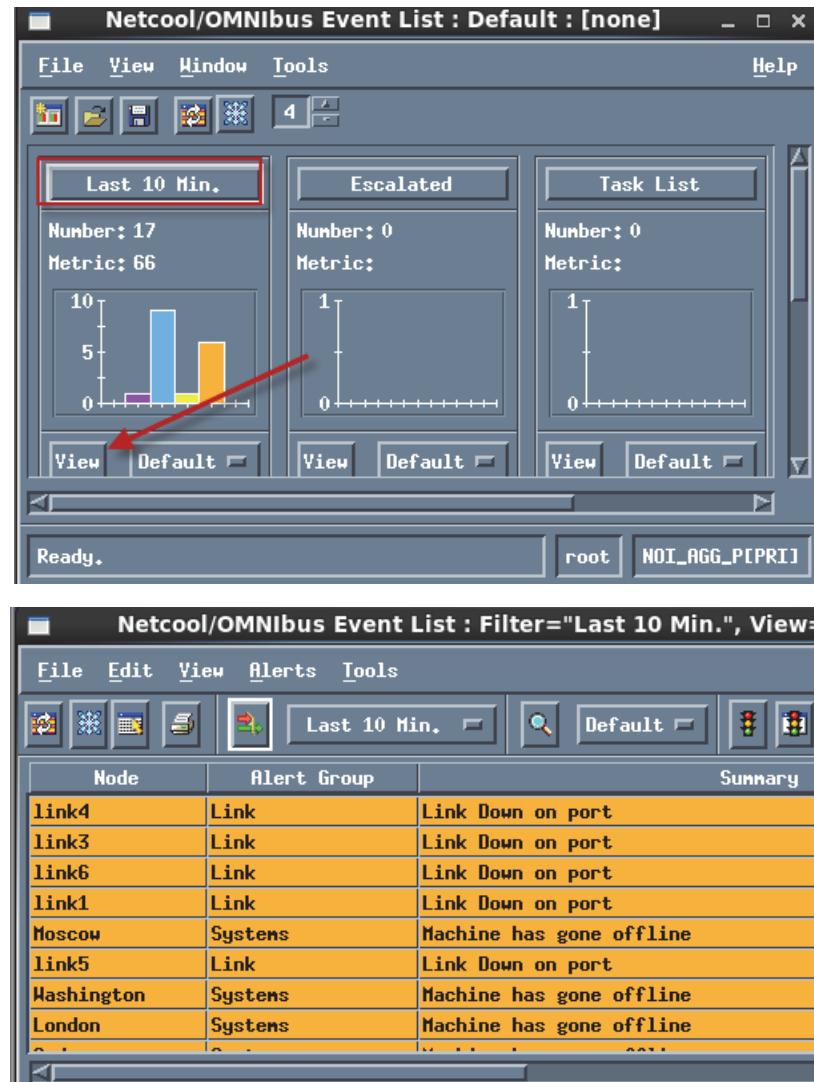
- b. Connect to the NOI_AGG_P ObjectServer as the root user, with no password.



- c. Click OK.

The **Event List** window opens.

- d. Find 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.

- 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
./IBMMIM
```

- b. Click **File > Preferences > Repositories**.

- c. Click **Add Repository**.

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

/software/jdbc/NCOMNI_GTW_JDBC.zip

Add a repository

Specify a repository and add to the repository preference list.

Repository:

/software/jdbc/NCOMNI_GTW_JDBC.zip

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



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

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

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

Add a repository

Specify a repository and add to the repository preference list.

Repository:

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

- g. Clear the check marks for the Netcool/OMNibus repository.

Repositories:	
Location	Connection
<input 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.

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

Repositories:	
Location	Connection
<input type="checkbox"/> /software/omnibus/OMNibusRepository/repository.config	
<input type="checkbox"/> /software/omnibus/fp2/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	

- i. Click **Install**.

- j. 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

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

- l. Leave the option selected to use the existing package group and click **Next**.

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

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

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

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

- o. 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 11.1.0
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	2019-07-26-16.40.59.446166
REPORTER_CONVERSIONS	DB2INST1	T	2019-07-26-16.40.59.454708
REPORTER_DETAILS	DB2INST1	T	2019-07-26-16.40.59.303762
REPORTER_GROUPS	DB2INST1	T	2019-07-26-16.40.59.434099
REPORTER_JOURNAL	DB2INST1	T	2019-07-26-16.40.59.360836
REPORTER_MEMBERS	DB2INST1	T	2019-07-26-16.40.59.440101
REPORTER_NAMES	DB2INST1	T	2019-07-26-16.40.59.428443
REPORTER_STATUS	DB2INST1	T	2019-07-26-16.40.59.373936
REP_AUDIT	DB2INST1	V	2019-07-26-16.40.59.569008
REP_AUDIT_ACK	DB2INST1	T	2019-07-26-16.40.59.415307
REP_AUDIT_OWNERGID	DB2INST1	T	2019-07-26-16.40.59.396828
REP_AUDIT_OWNERUID	DB2INST1	T	2019-07-26-16.40.59.389136
REP_AUDIT_SEVERITY	DB2INST1	T	2019-07-26-16.40.59.404155
REP_REFERENCE_DATE	DB2INST1	V	2019-07-26-16.40.59.552508
REP_SEVERITY_TYPES	DB2INST1	T	2019-07-26-16.40.59.470961
REP_TIME_PERIODS	DB2INST1	T	2019-07-26-16.40.59.491611
STATUS_VW	DB2INST1	V	2019-07-26-16.40.59.562198

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:

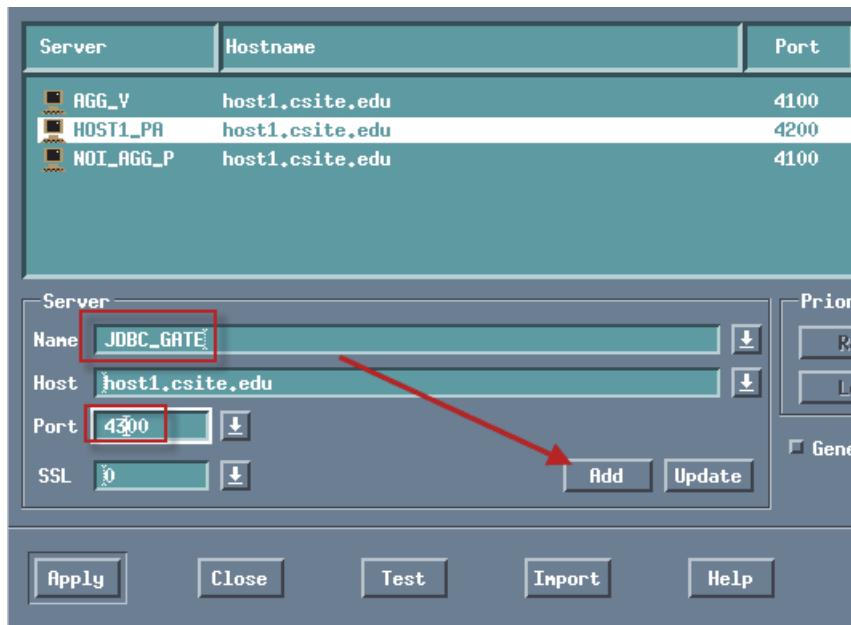
```
nco_xigen &
```

- 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
NETCO1_P0	host1.csuite.edu	4200
JDBC_GATE	host1.csuite.edu	4300
NOI_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 -l 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 at the end of the file.

- i. Enter the following command to edit 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 by adding the comment character (#) at the front of the line:

```
# 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.)
```



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

- v. Add the following lines to the bottom the file.

```
# 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 : '$OMNIHOME/etc/JDBC_GATE.map'
# Name of ObjectServer
Gate.RdrWtr.Server : 'NOI_ AGG_P'
# Table replication file name
Gate.RdrWtr.TblRepDefFile :
'$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/V11.1/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. If the log file is empty, the gateway is functioning correctly.

```
more $OMNIHOME/log/JDBC_GATE.log
```
8. Verify gateway operation.



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.

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

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

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

- b. Connect to the REPORTER database:

```
db2 connect to reporter
```

- c. Examine the event archive table:

```
db2 select node from reporter_status
```

NODE

```
host1.csuite.edu  
host1.csuite.edu  
host1.csuite.edu  
link4  
link4  
host1.csuite.edu  
Berlin  
London  
link3  
link1
```

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

- d. Examine the alternative tables.

Verify that each of 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.

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

```
exit
```

9. Stop the gateway.

- a. 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. Stop the gateway with a command like the following example. Use the PID you found in the previous step.

```
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, under the **MasterObjectServer** line.

```
process 'ArchiveGateway' 20
```

- e. The **service** section now looks like the following example.

```
{  
    ServiceType=Master  
    ServiceStart=Auto  
    process 'MasterObjectServer' NONE  
    process 'ArchiveGateway' 20  
}
```

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

11. Run the following command to 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
```

...

Forking to a Daemon Process.....

13. Verify that the gateway process starts:

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

[netcool@host1 etc]\$ 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 methods 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 process control agent:

- a. Stop the process control agent.

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

Netcool/OMNibus : Stopping Process Control ... [OK]

- b. Start the process control agent.

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

Netcool/OMNibus : Starting Process Control ... [OK]

- 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
```

[netcool@host1 Desktop]\$ 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 archive gateway are running.

Exercise 3 Netcool/OMNIbus Web GUI

Installing Jazz for Service Management

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

1. Prepare the host for the Tivoli Common Reporting installation.

- a. Change to the root user.

```
su -  
Password: object00
```

- b. Add the **netcool** user to the db2iadm1 group. This action allows you to install Tivoli Common Reporting as a non-root user.

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

- c. Add the DB2 client library path to the dynamically linked libraries. Open the /etc/ld.so.conf file in a text editor.

```
gedit /etc/ld.so.conf
```

- d. Add the following line to the end of the file.

```
/opt/ibm/db2/V11.1/lib32/
```

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

- f. Run the following command to regenerate the dynamically linked libraries.

```
ldconfig
```

- g. 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/JSM1.1.3.3_FOR_LNX_ML.zip
```

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

```
mkdir /tmp/was_install
```

5. Expand the WebSphere installation archive files into the target directory:

```
cd /tmp/was_install  
tar -zxvf /software/jazz/WSPAS8.5.5.15_FOR_JSM_LNX_ML.tar.gz
```

6. Expand the individual installation files.

```
unzip IBM-was-8.5.5.9-linux64.zip
```

```
unzip 8.5.5-WS-WAS-FP015-part1.zip
```

```
unzip 8.5.5-WS-WAS-FP015-part2.zip
```

```
unzip 8.5.5-WS-WAS-FP015-part3.zip
```

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

```
mkdir /tmp/tcr_install
```

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

```
cd /tmp/tcr_install  
tar -zxvf /software/tcr/ITCR_3.1.3.0_FOR_LINUX.tar.gz
```

9. Start IBM Installation Manager:

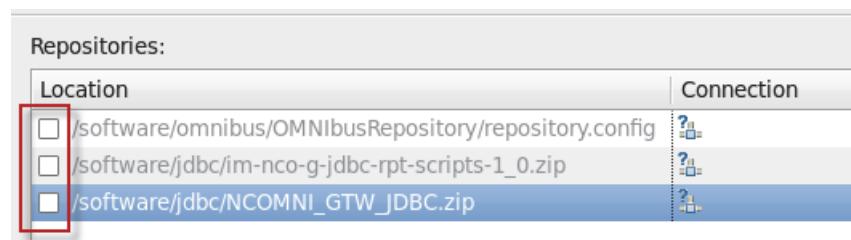
```
cd /home/netcool/IBM/InstallationManager/eclipse  
.IBMIM
```

IBM Installation Manager opens.

10. Define the Jazz for Service Management repository.

a. Click **File > Preferences**. Select **Repositories**.

b. Remove the check marks from the existing entries.

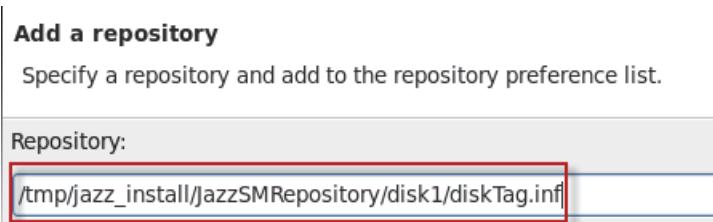


Note: You can remove the old repository entries instead of clearing the check marks.

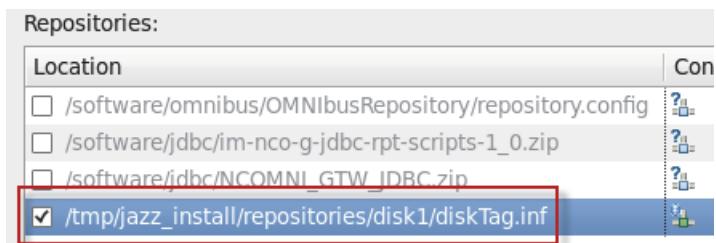
c. Click **Add Repository**.

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

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



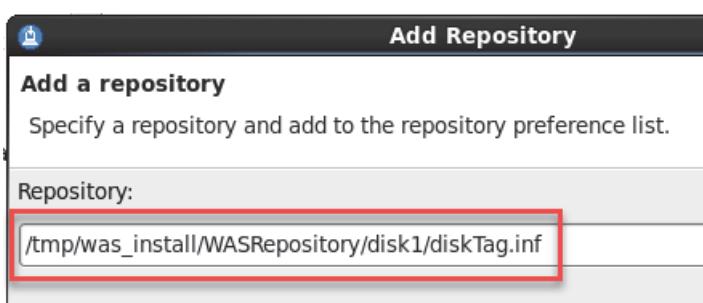
- e. Click **OK** to add the repository.
- f. Verify that the repository is listed.



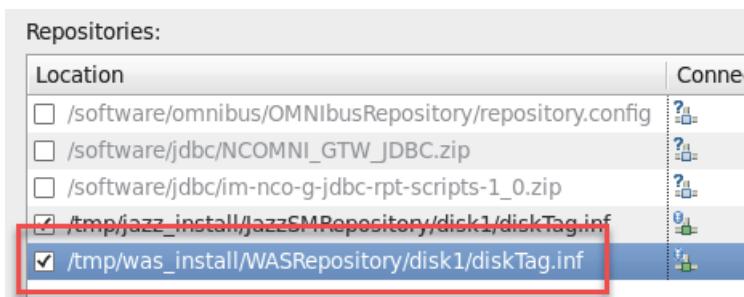
11. Define the WebSphere repository.

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

/tmp/was_install/WASRepository/disk1/diskTag.inf



- c. Click **OK** to add the repository.
- d. Verify that the repository is listed.



12. Define the WebSphere fix pack repository.

a. Click **Add Repository**.

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

/tmp/was_install/repository.config



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

d. Verify that all three repositories are listed, then click **OK**.

Repositories:	
Location	Connect
<input type="checkbox"/> /software/omnibus/OMNIBusRepository/repository.config	
<input type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	
<input type="checkbox"/> /software/jdbc/im-nco-q-jdbc-rpt-scripts-1.0.zip	
<input checked="" type="checkbox"/> /tmp/jazz_install/JazzSMRepository/disk1/diskTag.inf	
<input checked="" type="checkbox"/> /tmp/was_install/WASRepository/disk1/diskTag.inf	
<input checked="" type="checkbox"/> /tmp/was_install/repository.config	

13. Start the installation.

a. Click **Install**.

b. Select the following packages:

Installation Packages		Status	Vendor
<input checked="" type="checkbox"/> IBM WebSphere Application Server	<input checked="" type="checkbox"/> Version 8.5.5.15	Will be installed	IBM
<input checked="" type="checkbox"/> IBM WebSphere SDK Java Technology Edition (Optional)	<input checked="" type="checkbox"/> Version 7.0.9.30	Will be installed	IBM
<input type="checkbox"/> Jazz for Service Management extension for IBM WebSphere 8.0	<input type="checkbox"/> Version 1.1.0.2		IBM
<input checked="" type="checkbox"/> Jazz for Service Management extension for IBM WebSphere 8.5	<input checked="" type="checkbox"/> Version 1.1.2.1	Will be installed	IBM

c. Scroll down, and select the following packages:

<input checked="" type="checkbox"/> IBM Dashboard Application Services Hub	<input checked="" type="checkbox"/> Version 3.1.3.3	Will be installed	IBM
<input checked="" type="checkbox"/> Reporting Services	<input checked="" type="checkbox"/> Version 3.1.3.0	Will be installed	IBM



Important: Select five packages on this page. Do not select Jazz for Service Management extension for WebSphere **8.0**.

- d. Click **Next**.
- e. Accept the license agreement and click **Next**.
- f. Click the package named **IBM WebSphere Application Server V8.5** to select it.
- g. Change the Installation Directory to:

/opt/IBM/WebSphere/AppServer

Package Group Name	Installation Directory
IBM WebSphere Application Server V8.5	/opt/IBM/WebSphere/AppServer
IBM WebSphere Application Server 8.5.5.15	
IBM WebSphere SDK Java Technology Edition (Optional)	
Jazz for Service Management extension for IBM WebS	
Core services in Jazz for Service Management	/home/netcool/IBM/JazzSM
IBM Dashboard Application Services Hub 3.1.3.3	
Reporting Services 3.1.3.0	

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

- h. Click the package named **Core services in Jazz for Service Management** to select it.
- i. Change the Installation Directory to:

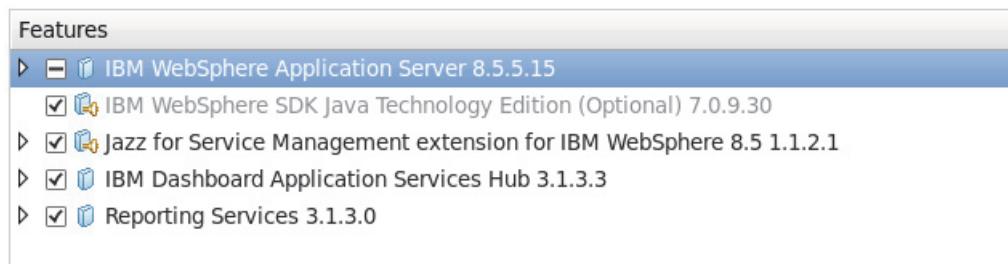
/opt/IBM/JazzSM

Package Group Name	Installation Directory
IBM WebSphere Application Server V8.5	/opt/IBM/WebSphere/AppServer
IBM WebSphere Application Server 8.5.5.15	
IBM WebSphere SDK Java Technology Edition (Optional)	
Jazz for Service Management extension for IBM WebS	
Core services in Jazz for Service Management	/opt/IBM/JazzSM
IBM Dashboard Application Services Hub 3.1.3.3	
Reporting Services 3.1.3.0	

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**.

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



- 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

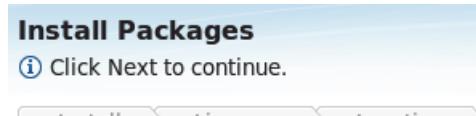
Profile location	/opt/IBM/JazzSM/profile
Profile name	JazzSMPProfile
Node name	JazzSMNode01
Server name	server1
User name	smadmin
Password	*****
Password confirmation	*****

Validate... ←



Important: You cannot proceed until you validate the password.

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



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 3.1.1	
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 3.1.3.0

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**.



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

Configuration for Reporting Services 3.1.3.0

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

The following packages were installed:

- ▽ IBM WebSphere Application Server V8.5
 - IBM WebSphere Application Server 8.5.5.15
 - 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 3.1.3.3
 - Reporting Services 3.1.3.0

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
- None

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

14. Open a Firefox browser and connect to the IBM Dashboard Application Services Hub URL:

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

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

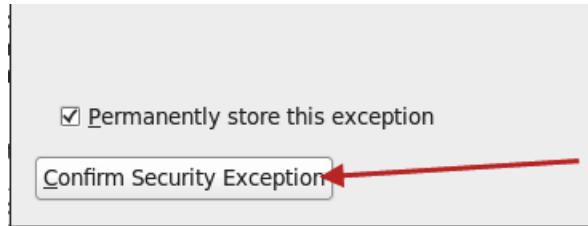
▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

[Add Exception...](#)

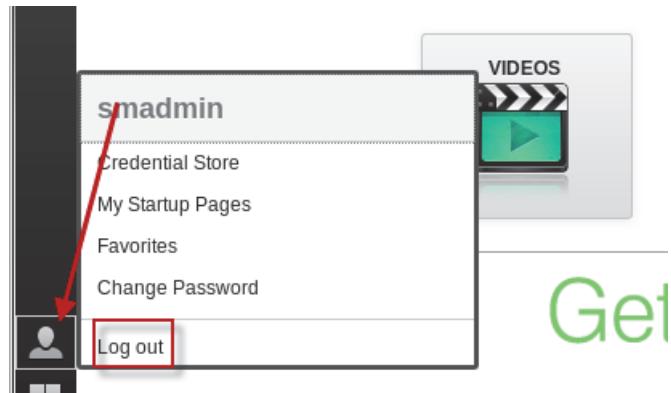
16. Click Confirm Security Exception.



17. Login as user **smadmin** with password **object00**.



18. 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.

19. Close the Firefox browser.

20. 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 tcr_install
```

```
cd /tmp/was_install/  
/bin/rm IBM-was-8.5.5.9-linux64.zip  
/bin/rm 8.5.5-WS-WAS-FP015-part1.zip  
/bin/rm 8.5.5-WS-WAS-FP015-part2.zip  
/bin/rm 8.5.5-WS-WAS-FP015-part3.zip
```



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

Installing Web GUI

1. Expand the installation file:

```
cd /software/webgui  
unzip TNOMN_V8.1.0.16_WBGEFOR_NOI_LNX_E.zip
```

2. Start IBM Installation Manager:

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

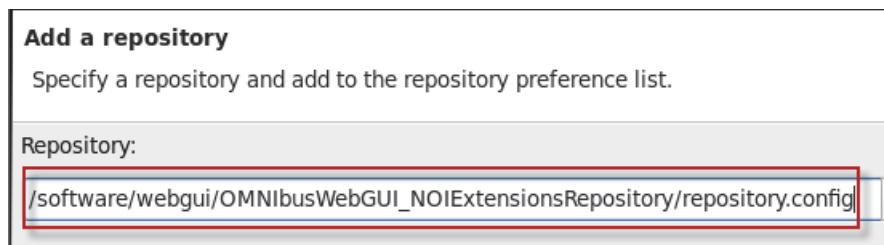
IBM Installation Manager opens.

3. Define the Web GUI repository.

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

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

/software/webgui/OMNibusWebGUI NOIExtensionsRepository/repository.config

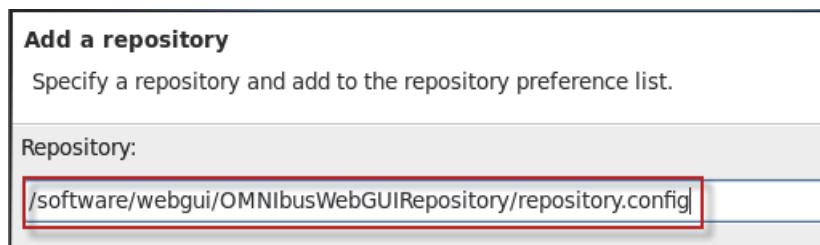


- e. Click **OK** to add the repository.

- f. Click **Add Repository**.

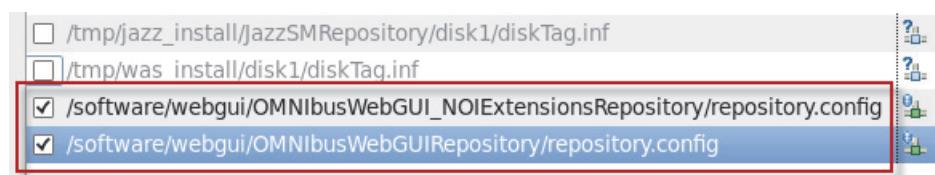
- g. Click **Browse** and select the following repository:

/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
IBM Tivoli Netcool/OMNibus Web GUI		
Version 8.1.0.16		Will be installed
Netcool Operations Insight Extensions for IBM Tivoli Netcool/OM		
Version 8.1.0.16		Will be installed

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

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

<input type="radio"/> Use the existing package group	<input checked="" type="radio"/> Create a new package group
Package Group Name	Installation Directory
IBM Netcool GUI Components	/opt/IBM/netcool/gui

Package Group Name: IBM Netcool GUI Components
 Installation Directory: /opt/IBM/netcool/gui

- e. Expand the list of features and select them all. Click **Next**.

Features
<ul style="list-style-type: none"> IBM Tivoli Netcool/OMNIbus Web GUI 8.1.0.16 <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Install base features <input checked="" type="checkbox"/> Install event search with IBM Operations Analytics - Log Analysis Netcool Operations Insight Extensions for IBM Tivoli Netcool/OMNIbus Web GUI 8.1.0.16 <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Install Event Analytics

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

Common Configurations
 WebSphere Application Server and Jazz for Service Management properties

Installation Directory Details

WebSphere Application Server	/opt/IBM/WebSphere/AppServer
Jazz for Service Management UI	/opt/IBM/JazzSM/ui

Profile Details

Server name	server1
User name	smadmin
Password	*****



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.csite.edu** for the host name.
- h. Enter **unityadmin** as the user name and password and click **Next**.

Configuration for IBM Tivoli Netcool/OMNibus Web GUI 8.1.0.16
Integrate with IBM Operations Analytics - Log Analysis

URL protocol type	https
URL host name	host1.csite.edu
URL port number	9987
URL context root	Unity
Data source name	omnibus
User name	unityadmin
Password	*****

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



Note: The installation process runs for approximately 25 minutes.

- j. 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 GUI Components
 - IBM Tivoli Netcool/OMNibus Web GUI 8.1.0.16
 - Netcool Operations Insight Extensions for IBM Tivoli Net

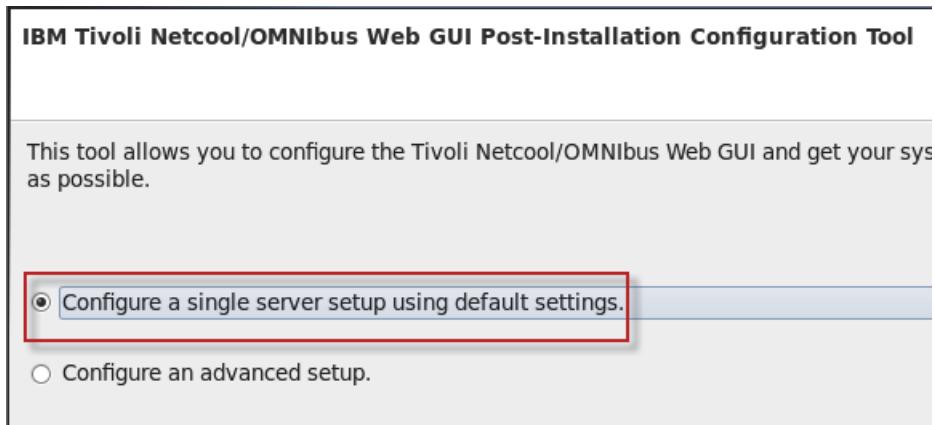
Which program do you want to start?

- Configure IBM Tivoli Netcool/OMNibus Web GUI
- Log on to IBM Tivoli Netcool/OMNibus Web GUI
- None

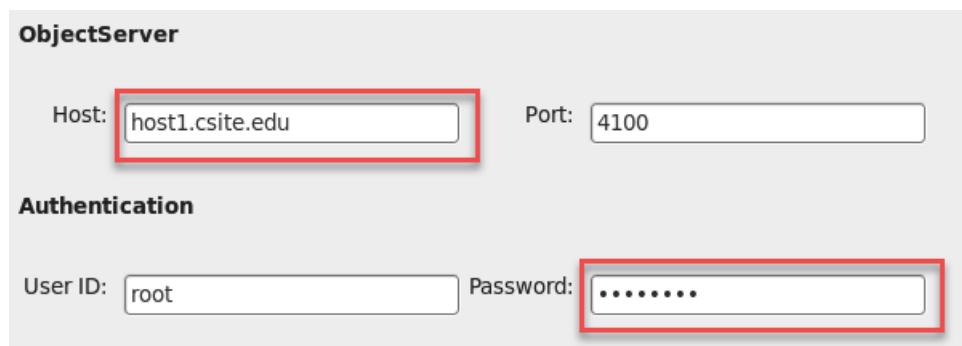
Web GUI postinstallation configuration

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

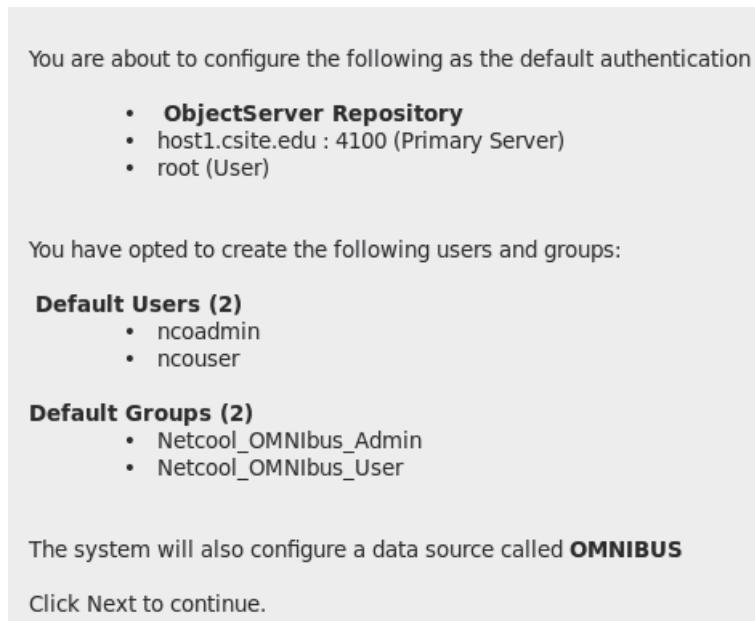
1. Leave the default setting and click **Next**.



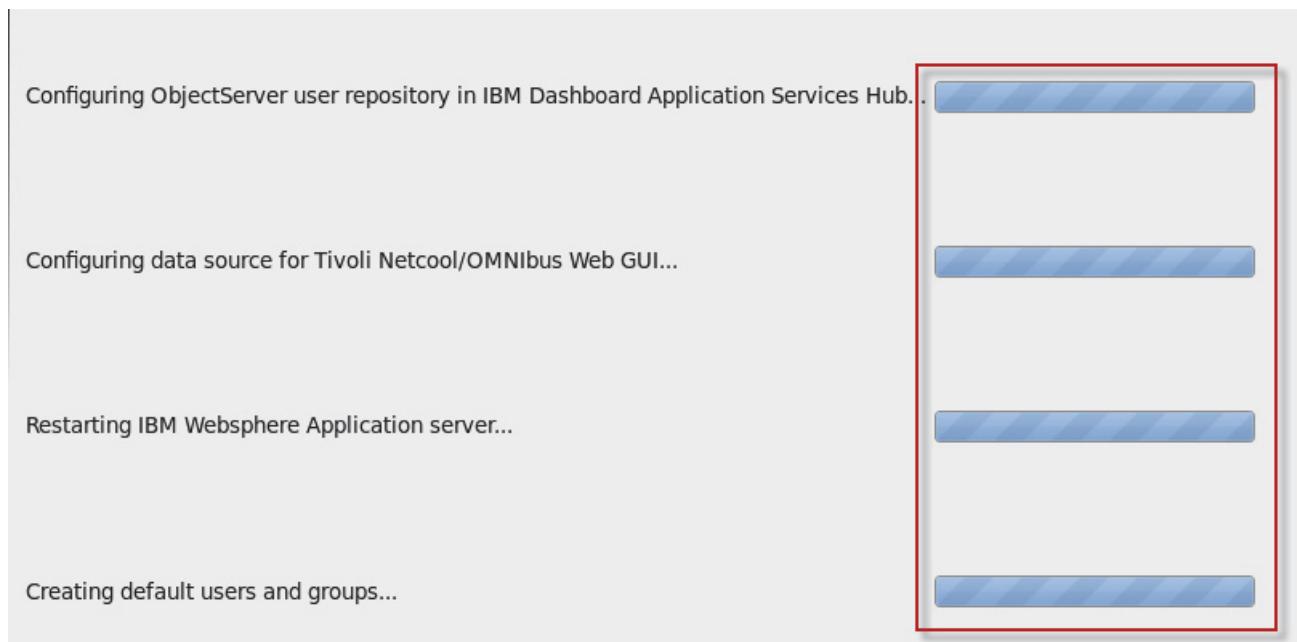
2. Change the Host to **host1.csuite.edu**, enter **object00** for the password, and click **Next**.



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 with the following commands:

```
cd /opt/IBM/netcool/gui/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 Jazz for Service Management 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 JazzSMPProfile 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 JazzSMPProfile 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 JazzSMPProfile 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.

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

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

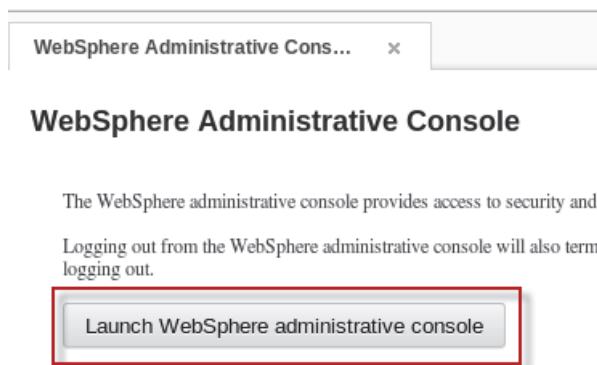


Hint: If you did not set the default home page previously, do so now.

- 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.

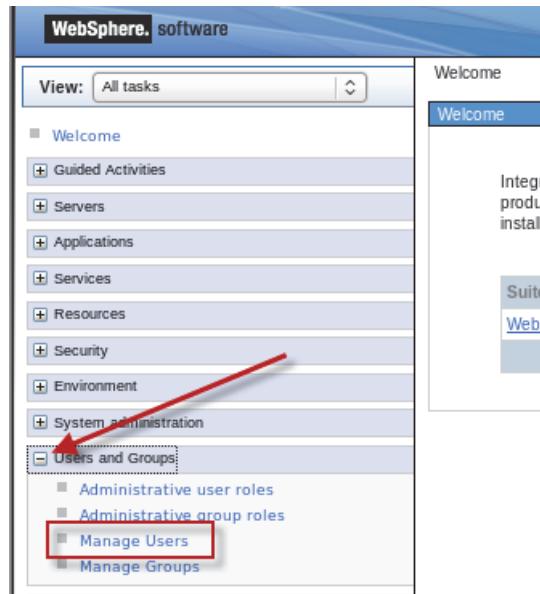
3. Remove the default users and groups.

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.

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



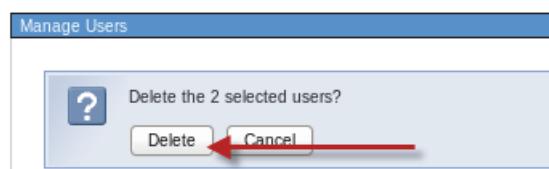
- b. Select the two users: **ncoadmin** and **ncouser**, then click **Delete**.

Select	User ID	First name	Last name	E-mail	Unique Name
<input checked="" type="checkbox"/>	ncoadmin	ncoadmin	tivoli		uid=ncoadmin,o=netcoolObjectServerRepository
<input checked="" type="checkbox"/>	ncouser	ncouser	tivoli		uid=ncouser,o=netcoolObjectServerRepository
<input type="checkbox"/>	nobody		Nobody		uid=nobody,o=netcoolObjectServerRepository

- c. Click **Delete**.

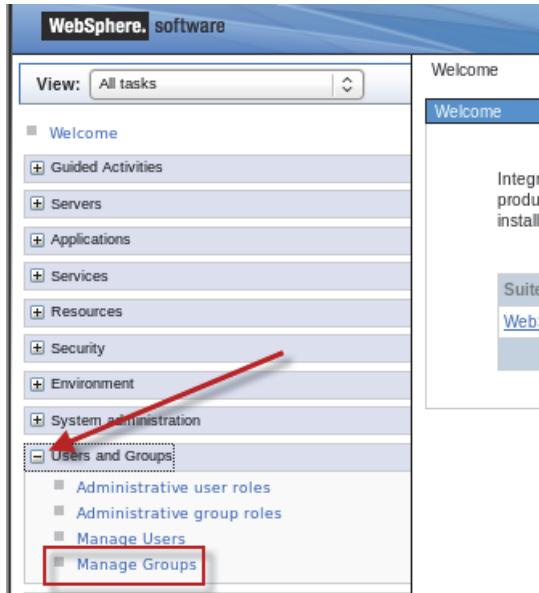


Important: Do not remove any of the other users.



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

d. Click **Manage Groups**.



e. Select the two groups: **Netcool_OMNIbus_Admin** and **Netcool_OMNIbus_User**, then click **Delete**.

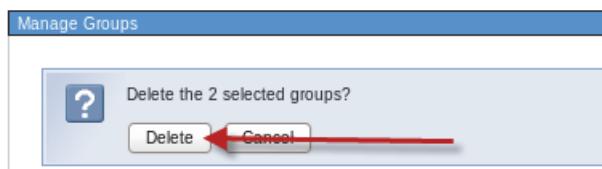
A screenshot of a table titled '10 groups matched the search criteria.' The table has columns for Select, Group name, Description, and a long URL. Two rows are selected: 'Netcool_OMNIbus Admin' and 'Netcool_OMNIbus User'. Both rows have checkboxes checked. A red box highlights the 'Select' button at the top of the table, and a red arrow points from the text above to this button. Another red box highlights the 'Delete' button at the top of the table.

Select	Group name	Description	
<input type="checkbox"/>	Administrator	Admin Group	cn=Administrator,o=netcoolObj
<input type="checkbox"/>	Gateway	Permissions required for a gateway user	cn=Gateway,o=netcoolObj
<input type="checkbox"/>	ISQL	Read only ISQL access	cn=ISQL,o=netcoolObj
<input type="checkbox"/>	ISQLWrite	Write ISQL access	cn=ISQLWrite,o=netcoolObj
<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=Normal,o=netcoolObj

f. Click **Delete**.



Important: Do not remove any of the other groups.



The **Netcool_OMNIbus_Admin** and **Netcool_OMNIbus_User** groups are deleted.

4. Remove the ObjectServer definition.
 - a. Expand **Security** and click **Global security**.



- b. 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

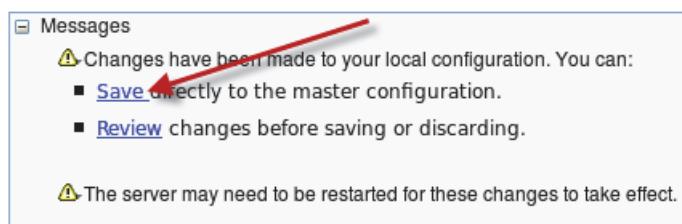
Available realm definitions:

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

- c. Scroll down on the page to *Repositories in the realm*, select the check box for the **o=netcoolObjectServerRepository** entry, 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"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File
<input checked="" type="checkbox"/>	o=netcoolObjectServerRepository	NetcoolObjectServer	Custom
Total 2			

- d. Click **Save**.



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

You can administer the following resources:			
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File
Total 1			

Related Items

- [Additional Properties](#)
- [Manage repositories](#) **(highlighted)**
- [Property extension repository](#)
- [Trusted authentication realms -](#)

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

Add ▾	Delete	
<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	
Select	Repository Identifier ▾	
You can administer the following resources:		
<input checked="" type="checkbox"/>	InternalFileRepository	File
<input checked="" type="checkbox"/>	NetcoolObjectServer	Custom

- g. Click **Save**.

Messages

⚠ Changes have been made to your local configuration. You can:

- [Save directly to the master configuration.](#) **(highlighted)**
- [Review changes before saving or discarding.](#)

- h. Log out of the administrative console.

Welcome smadmin Help | Logout IBM

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

- i. Log out of Dashboard Application Services Hub.

smadmin

- Credential Store
- Favorites
- My Startup Pages
- Change Password

Log out

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. Add 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**.

User account repository

Realm name
defaultWIMFileBasedRealm

Current realm definition
Federated repositories

Available realm definitions

Federated repositories Configure... Set as current

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

Repositories in the realm:

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

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

General Properties

* Repository
none defined

* Unique distinguished name
File repository

New Repository... **LDAP repository**

Distinguished name in the repository is different

- 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**.

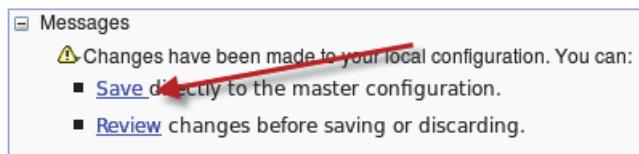
- k. Scroll to the bottom of the page and click **OK**.

The screenshot shows the 'Repository identifier' field set to 'TIVIDS'. Under the 'LDAP server' tab, 'Directory type' is 'IBM Tivoli Directory Server', 'Primary host name' is 'host1.csite.edu', and 'Port' is '389'. Under the 'Security' tab, 'Bind distinguished name' is 'cn=root', 'Bind password' is masked, and 'Federated repository properties for' is 'uid;cn'. A note at the bottom says 'Failover server used when primary is not available:'.

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

The screenshot shows the 'General Properties' dialog with 'Repository' set to 'TIVIDS'. In the 'Unique distinguished name of the base (or parent) entry in repositories' field, 'dc=ibm,dc=com' is entered and highlighted with a red box.

- 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 find values for each of the object classes. These definitions essentially define the LDAP subtree where the Netcool user information is located.

4. Define LDAP object class mappings.

- Scroll down on the page and click **TIVIDS**.

Repositories in the realm:

Add repositories (LDAP, custom, etc...) Use built-in repository	
Select	Base Entry
You can administer the following resources:	
<input type="checkbox"/>	dc=ibm,dc=com TIVIDS
<input type="checkbox"/>	o-defaultWIMFileBasedRealm InternalFileRepository

- 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.

- Click **Group**.

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

- 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**.

Messages

⚠ Changes have been made to your local configuration. You can:
 [Save directly to the master configuration.](#)
 [Review changes before saving or discarding.](#)

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.

a. 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.

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

Additional Properties		Related Items	
<ul style="list-style-type: none"> ■ Property extension repository ■ Entry mapping repository ■ Supported entity types ■ User repository attribute 	<ul style="list-style-type: none"> ■ 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:		
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	o=netcoolObjectServerRepository	o;ou;x
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.

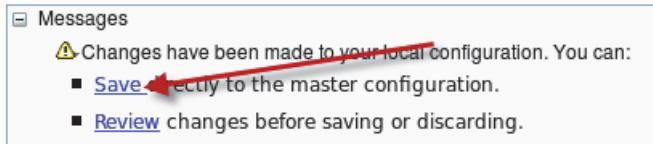
General Properties

- * Entity type: PersonAccount
- * Base entry for the default parent: `ou=tipusers,cn=tipRealm,DC=IBM,DC=COM`
- * Relative Distinguished Name properties: uid

- i. Verify that your entries look like the following example.

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

- j. 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
```

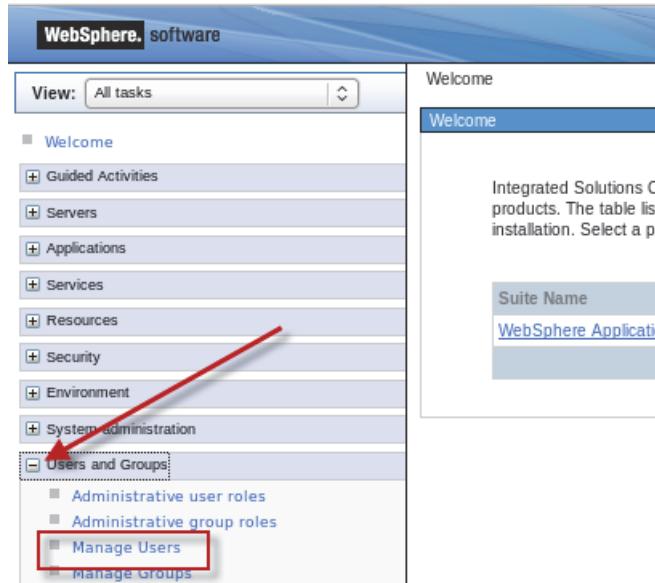
If the command finds a running process, wait a short time and check again.

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.

Manage Users

Search for Users

Search by * Search for * Maximum results

User ID	*	100
---------	---	-----

Search

27 users matched the search criteria.

Select an action...					
Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	abraman	Ariana Braman	Braman	abraman@ibm.com	cn=Ariana Braman,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	adurling	Adeline Durling	Durling	adurling@ibm.com	cn=Adeline Durling,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	bwinebarger	Bart Winebarger	Winebarger	bwinebarger@ibm.com	cn=Bart Winebarger,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	dselan	Dick Selan	Selan	dselan@ibm.com	cn=Dick Selan,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	eange	Earline Ange	Ange	eange@ibm.com	cn=Earline Ange,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	elotempio	Emelda Lotempio	Lotempio	elotempio@ibm.com	cn=Emelda Lotempio,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM

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.

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



2. 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**

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

Ignore case for authorization

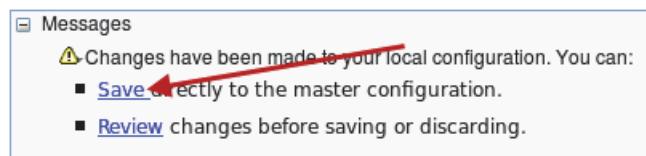
Allow operations if some of the repositories are down

Repositories in the realm:

Add repositories (LDAP, custom, etc...) Use built-in repos

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.

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]
```



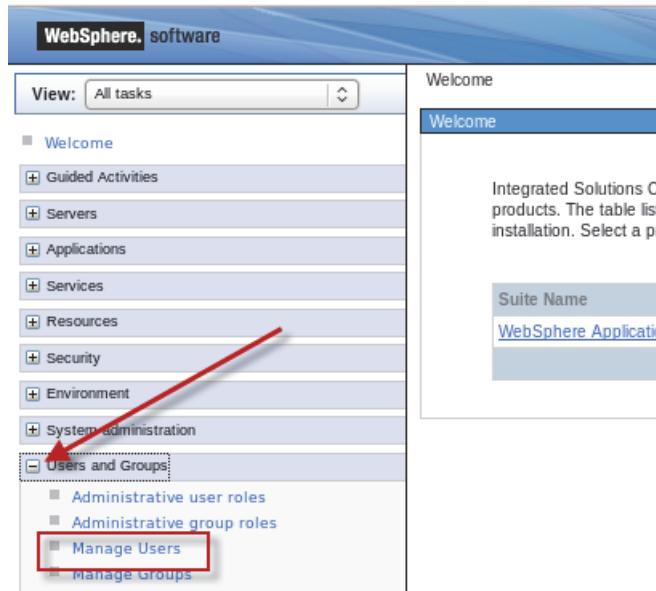
Important: Leave the terminal window as is. You return shortly and use it to restart the LDAP server.

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 was successful.

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			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 soon.

16. Restart the LDAP server.

- 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 fields:

- Search by: User ID
- * Search for: (empty)
- * Maximum results: 100

A red arrow points to the **Search** button. Below the search bar, a message says "27 users matched the search criteria." A red box highlights this message. The search results table has columns: Select, User ID, First name, Last name, E-mail, Unique Name. The results list 27 users, including abraman, adurling, bwinebarger, dselan, and eange.

All 27 users are again available.

18. Log out of the administrative console.

Configuring ObjectServer synchronization

1. Enable ObjectServer synchronization.

- 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. Find the following line:

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



Note: The line is at approximately line number 339 in the file.

- d. Change the property value to true:

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

- e. Save the file and close the gedit text editor.

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. Open the Web GUI initialization file in a text editor.

```
gedit ncwDataSourceDefinitions.xml
```

- h. Find the following line:

```
<config maxAge="3600"/>
```

- i. Change the property value to 600:

```
<config maxAge="600"/>
```

- j. Save the file and close the gedit text editor.

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:

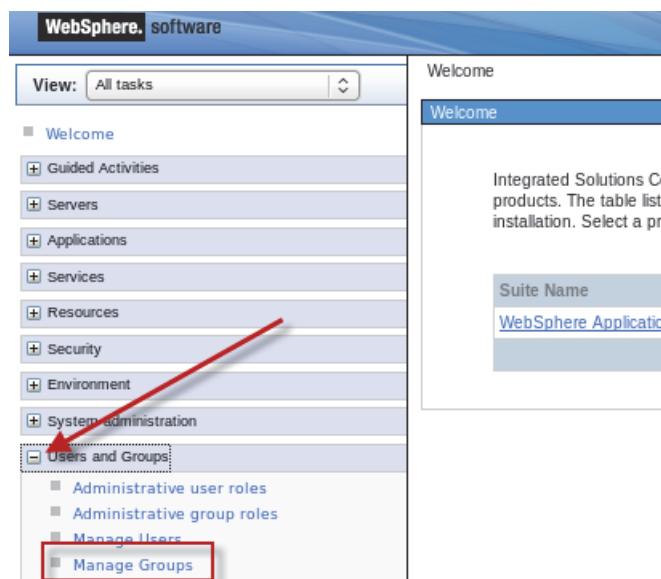
```
./startServer.sh server1
```

Configuring default users and groups

Now that the synchronization process is configured, you must recreate 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.

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



b. Click **Create**.

1 groups matched the search criteria.

Select	Group name	Description	Unique Name
<input type="checkbox"/>	WPAdministrators		cn=WPAdministrators,ou=tipgroups,cn=tipRealm,DC

c. Enter **Netcool_Admin** as the group name and click **Create**.

Create a Group

* Group name

Description

d. Click **Close**.



e. Repeat the previous steps and create the **Netcool_User** group.

When complete, the groups look like the following example.

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,c



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

4. Add the default users.

a. Click **Manage Users**.

- + Environment
- + System administration
- Users and Groups
 - Administrative user roles
 - Administrative group roles
 - Manage Users**
 - Manage Groups

b. Click **Create**.



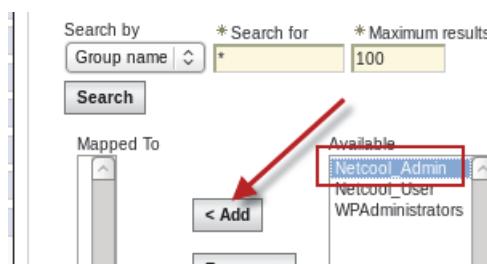
- c. Enter **ncoadmin** as the user ID.
d. Enter values for first and last names.
e. Enter **object00** for the password and click **Group Membership**.

A screenshot of the 'Create a User' form. It has fields for User ID ('ncoadmin'), First name ('Netcool'), Last name ('Admin'), E-mail ('ncoadmin'), Password ('object00'), and Confirm password ('object00'). A red arrow points from the 'User ID' field to a 'Group Membership' button.

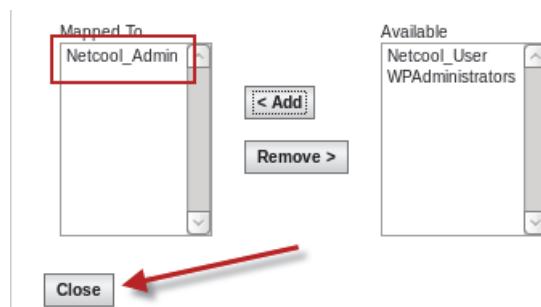
f. Click **Search**.



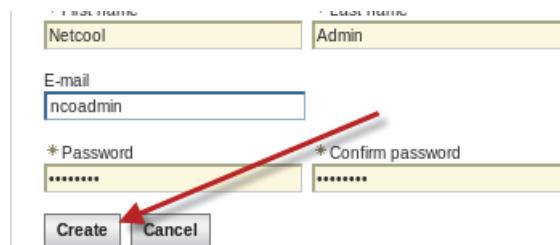
g. Click **Netcool_Admin** to select it and click **Add**.



h. Click **Close**.



- Click Create.



- Click Close.



- Repeat the previous steps to create the **ncouser** user and assign the user to the **Netcool_User** group.

When complete, the new user entries look like the following example.

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

- Close the Firefox tab.

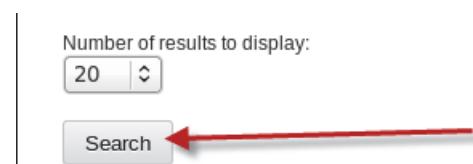
The users and groups are created in the LDAP directory and are now known to Dashboard Application Services Hub. However, no Dashboard Application Services Hub roles are assigned to either the users or the groups yet.

- Assign Dashboard Application Services Hub roles to the default groups.

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



- 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

<input checked="" type="checkbox"/>	iscadmins
<input type="checkbox"/>	monitor
<input checked="" type="checkbox"/>	ncw_admin
<input type="checkbox"/>	ncw_analytics_admin
<input checked="" type="checkbox"/>	ncw_dashboard_editor
<input checked="" type="checkbox"/>	ncw_gauges_editor



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**.

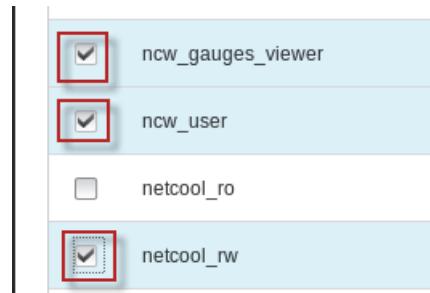
Group Name	Roles
Netcool_Admin	ncw_gauges_editor, ncw_admin, ncw_dashboard_editor, iscadmins, netcool_rw
Netcool_User	

- g. Scroll down and select the following roles:

ncw_gauges_viewer

ncw_user

netcool_rw

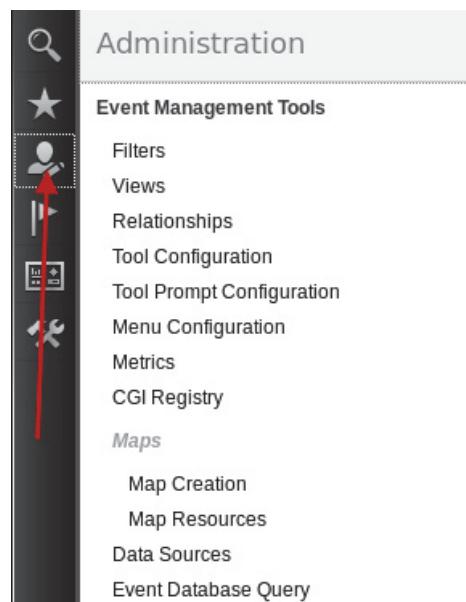


- h. Scroll to the bottom of the page and click **Save**.

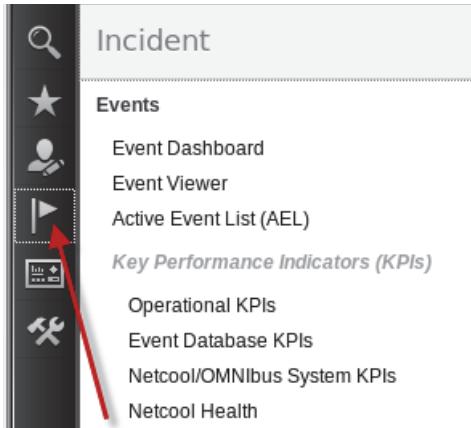
The role assignments now look like the following example.

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

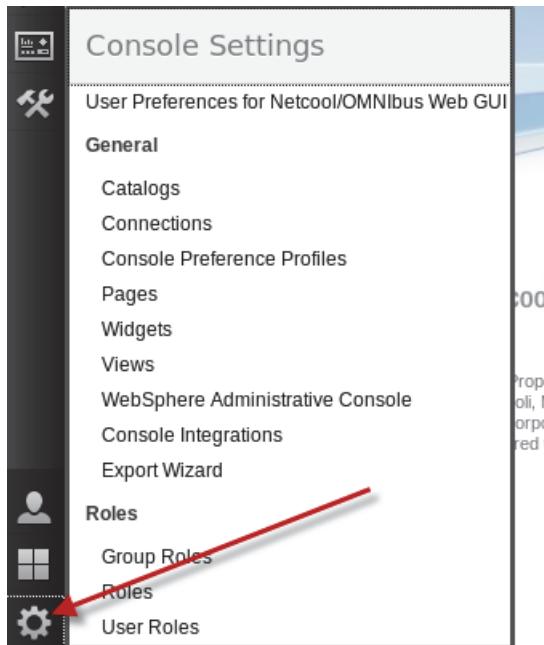
6. Log out of Dashboard Application Services Hub as the **smadmin** user.
7. Log in to Dashboard Application Services Hub as user **ncoadmin** with password **object00**.
8. Click the icon and verify access to Netcool administrative features.



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



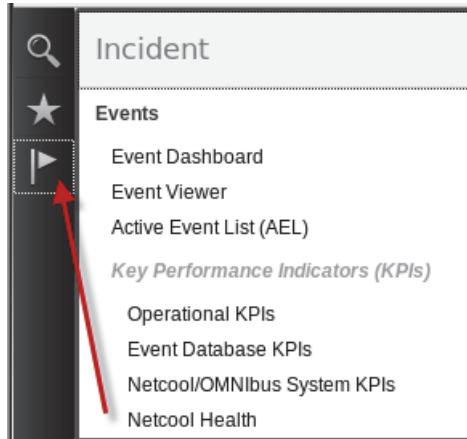
10. Click the icon and verify access to Dashboard Application Services Hub administrative features.



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**.

A screenshot of a search interface. At the top is a text input field labeled 'Group ID:' containing 'Netcool*'. To the right is a small 'Descr' button. Below is a dropdown for 'Number of results to display' set to '20'. At the bottom is a large red arrow pointing to a 'Search' button.

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

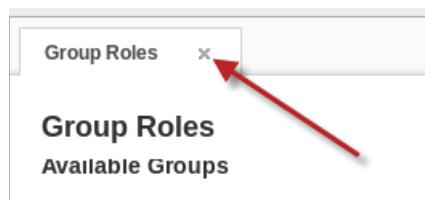
d. Scroll to the bottom of the page, select **tcrPortalOperator**, and click **Save**.



e. Repeat the previous steps to add **tcrPortalOperator** to the **Netcool_User** group.

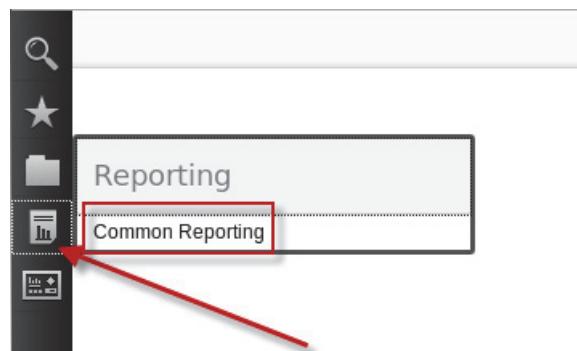
Group Name	Roles
Netcool_Admin	ncw_gauges_editor, ncw_admin, tcrPortalOperator, ncw_dashboard_editor, iscadmins, netcool_rw
Netcool_User	ncw_user, tcrPortalOperator, ncw_gauges_viewer, netcool_rw

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

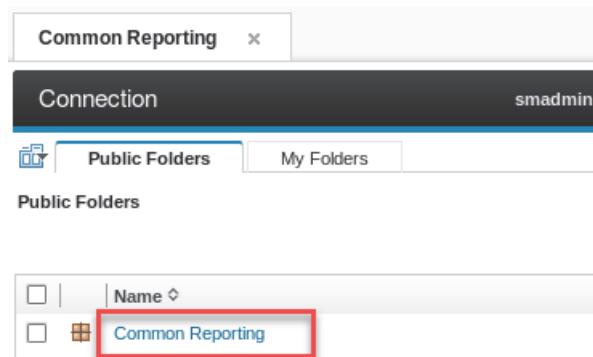


3. Verify basic Tivoli Common Reporting function.

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



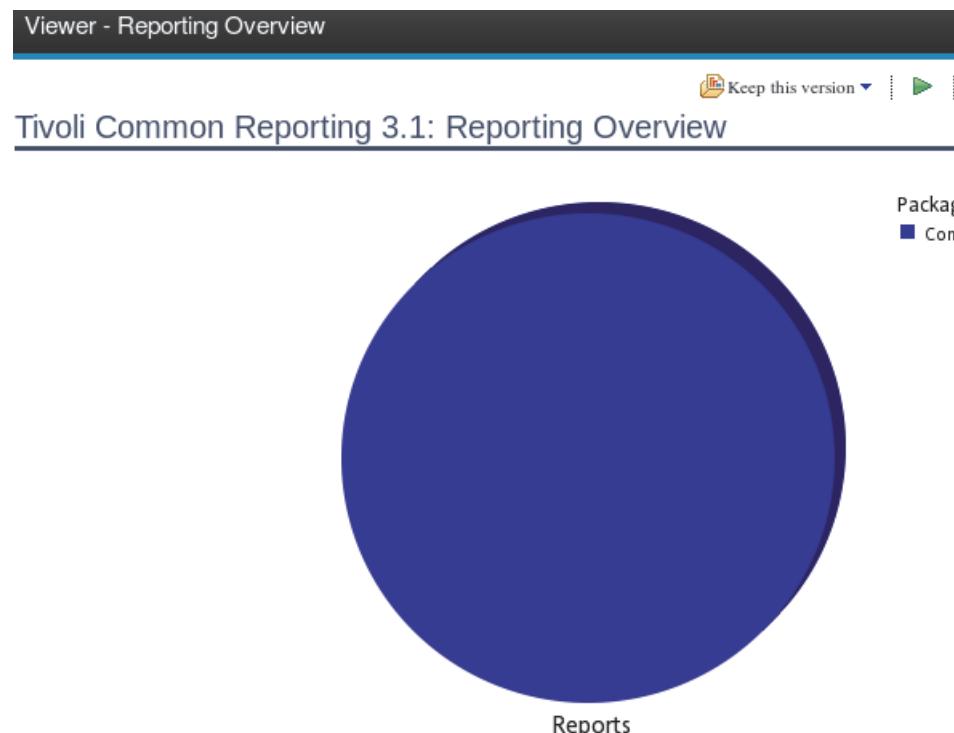
- b. Click the report package **Common Reporting**.



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

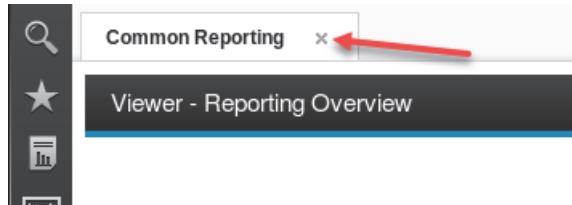


- d. Leave the default settings on the prompt page and click **Finish**.
The report opens.



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.

- Click the X to close the tab.



- 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 classroom 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.

- Open the *netcool* user environment file in a text editor.

```
cd /home/netcool
```

```
gedit .bashrc
```

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

```
#source /home/db2inst1/sqllib/db2profile
```

The modified line is shown as follows:

```
source /home/db2inst1/sqllib/db2profile
```

- Save the file and exit gedit.



Note: The file **/home/db2inst1/sqllib/db2profile** contains a definition for the **LD_LIBRARY_PATH** environment variable. This variable definition is what implements the required environment.

- Verify the environment change.

- Source the modified file.

```
source .bashrc
```

- Test the change.

```
which db2
```

```
/home/db2inst1/sqllib/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. Disable the IBM Cognos Application Firewall so other DASH applications can access the Cognos server.
 - a. Set the JAVA_HOME environment variable.

```
export JAVA_HOME=/opt/IBM/WebSphere/AppServer/java_1.7_64/jre/
```
 - b. Change to the target directory.

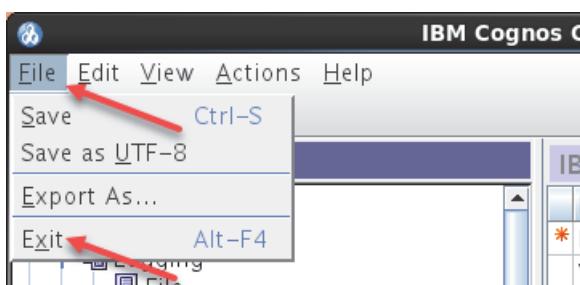
```
cd /opt/IBM/JazzSM/reporting/cognos/bin64
```
 - c. Start the Cognos Configuration tool.

```
./cogconfig.sh
```
 - d. Select **Local Configuration > Security > IBM Cognos Application Firewall**.
 - e. Set **Enable CAF validation** to **False**.
 - f. Set **third party XSS checking** to **False**.

Name	Value
* Enable CAF validation?	False
Valid domains or hosts	<click the edit button>
Is third party XSS checki...	False

Defines a group of properties to configure the IBM Cognos Firewall.

- g. Click **File > Exit**.



- h. Click **Yes** to confirm the changes.
 - i. Click **Close**.
10. 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.

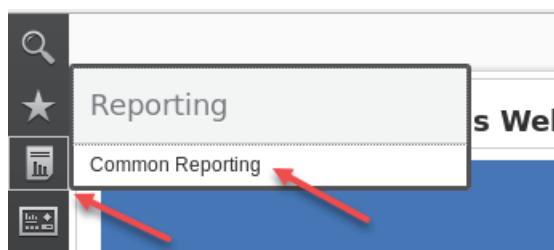
A set of Tivoli Common Reporting reports are bundled with Netcool/OMNibus. The report package must be imported into Tivoli Common Reporting.

11. Copy the report package.
- The report package file must be placed in a specific directory.
- a. Change to the source directory:

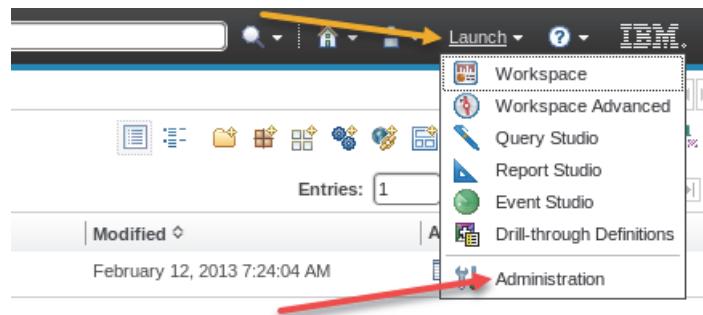
```
cd $OMNIHOME/extensions/tcr_event_reports
```
 - b. Copy the file to the target directory:

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

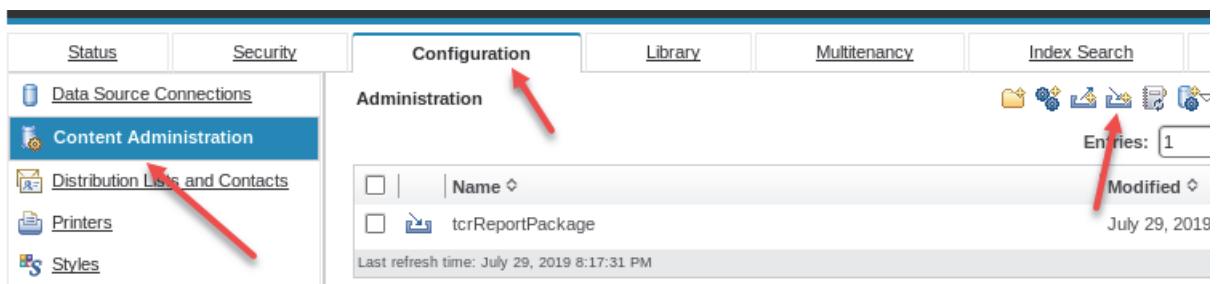
12. Import the package.
- a. Open a Firefox browser.
 - b. Log in to Dashboard Application Services Hub as user **smadmin** with password **object00**.
 - c. Click the icon and select Common Reporting.



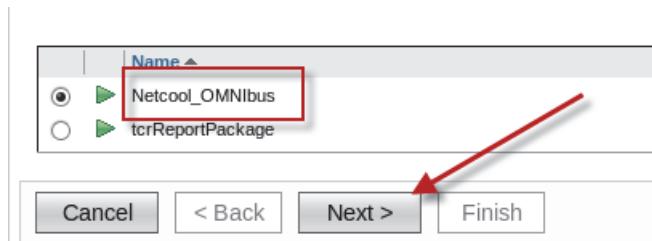
- d. Click **Launch** and select **Administration**.



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

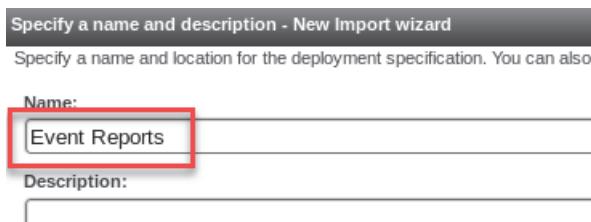


- h. Verify that the **Netcool_OMNIbus** package is selected and click **Next**.

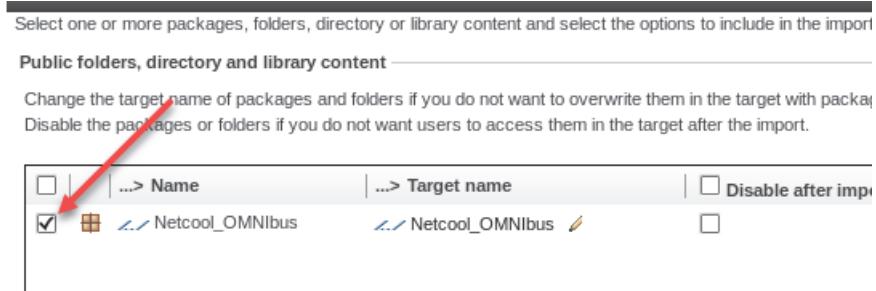


Important: If the Netcool_OMNIbus package is not listed, it means that it was not copied to the correct location.

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



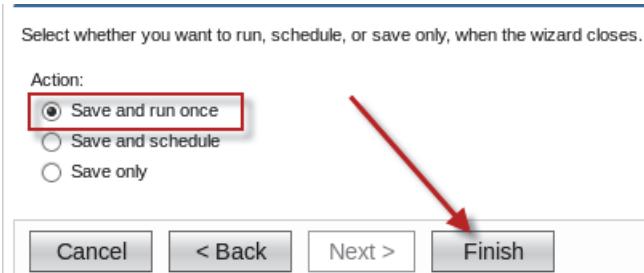
- j. Select the **Netcool_OMNIbus** package, scroll to the bottom of the page, and click **Next**.



- k. Scroll to the bottom of the general options page, and click **Next**.

- l. Scroll to the bottom of the summary review page, and click **Next**.

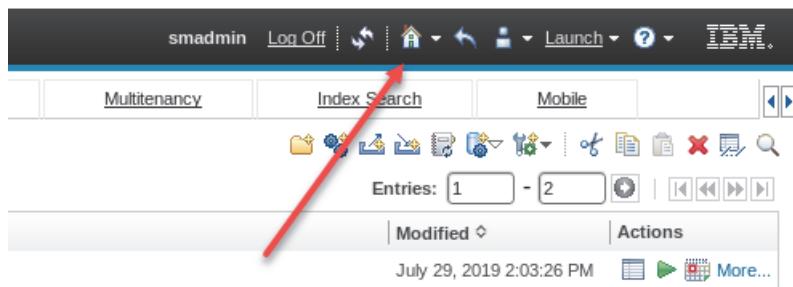
- m. Leave the option set as shown and click **Finish**.



- n. Scroll to the bottom of the page, and click **Run**.

- o. Click **OK**.

- p. Click the icon to return to the home page.



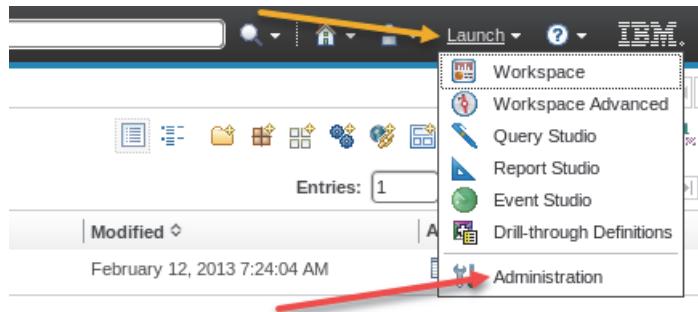
- q. Verify that the Netcool/OMNIbus report package is now available.



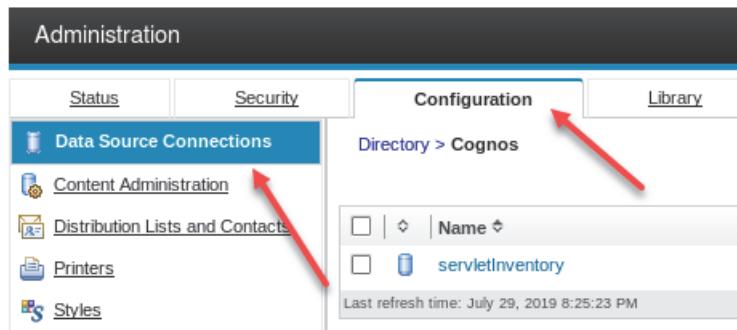
13. Create a data source.

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

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

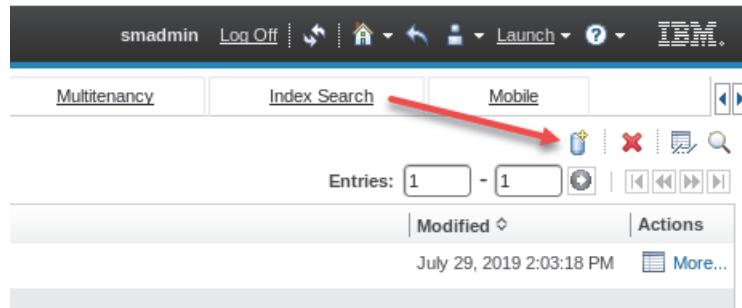


- Click the **Configuration** tab.
- Click **Data Source Connections**.



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.

- 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:

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 can be used to identify the connection in reports.

Type:

Isolation level: Use the default object gateway
 Specify a value:

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:

DB2 connect string:



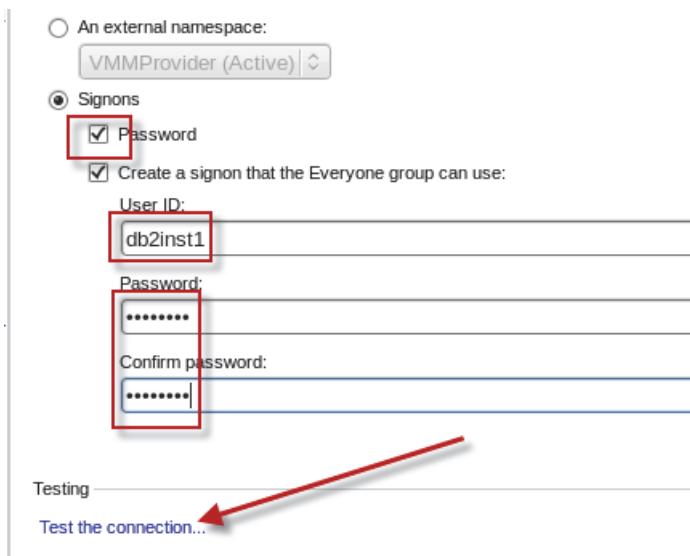
Important: This value must be REPORTER because it is the database name that is cataloged in DB2.

- i. Scroll down to the bottom of the page.

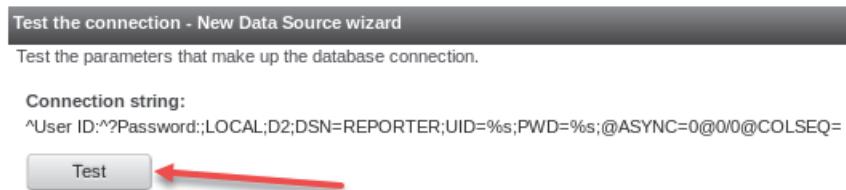
- j. Select the **Password** check box.

k. Enter **db2inst1** for the user ID and **object00** for the password.

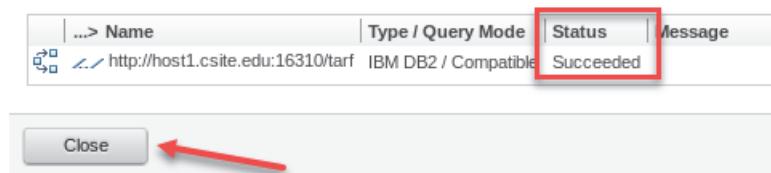
l. Click the line that is labeled **Test the connection**.



m. Click **Test**.



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

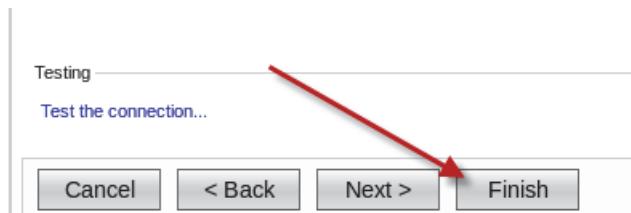


Important: If the test fails with QE-DEF-0285, it typically means that either the user ID or password is incorrect, or the **netcool** user environment variables are not correct.

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



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



- q. Verify that the **Reporter** data source is shown in the list of available data sources.
r. Click the icon to return to the report packages.

The screenshot shows the Cognos Configuration interface. The top navigation bar includes "smadmin", "Log Off", "Launch", and "IBM". Below the navigation bar, there are tabs for "Configuration", "Library", "Multitenancy", "Index Search", and "Mobile". The "Index Search" tab is active. In the center, there is a search bar and a table listing data sources. The table has columns for "Name", "Modified", and "Actions". Two entries are listed: "Reporter" (modified July 29, 2019 8:32:06 PM) and "servletInventory" (modified July 29, 2019 2:03:18 PM). A red box highlights the "Reporter" entry. An arrow points from the "Index Search" tab to the "Reporter" entry.

Name	Modified	Actions
Reporter	July 29, 2019 8:32:06 PM	
servletInventory	July 29, 2019 2:03:18 PM	

14. Verify the Netcool/OMNIbus reports.

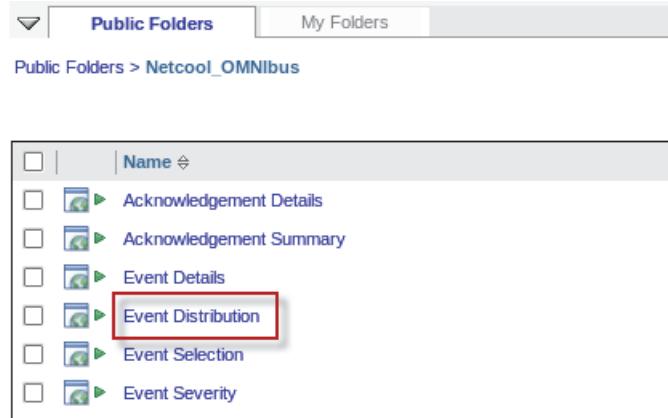
- a. Click **Netcool_OMNIbus** to view the report templates.

The screenshot shows the "Public Folders" interface. At the top, there are tabs for "Public Folders" and "My Folders", with "Public Folders" selected. Below the tabs, there is a search bar and a table listing report templates. The table has columns for "Name" and "Actions". One entry is listed: "Common Reporting" (under "Netcool_OMNIbus"). A red box highlights the "Netcool_OMNIbus" folder. An arrow points from the "Netcool_OMNIbus" folder to the "Netcool_OMNIbus" entry in the table.

Name	Actions
Common Reporting	

The list of reports opens.

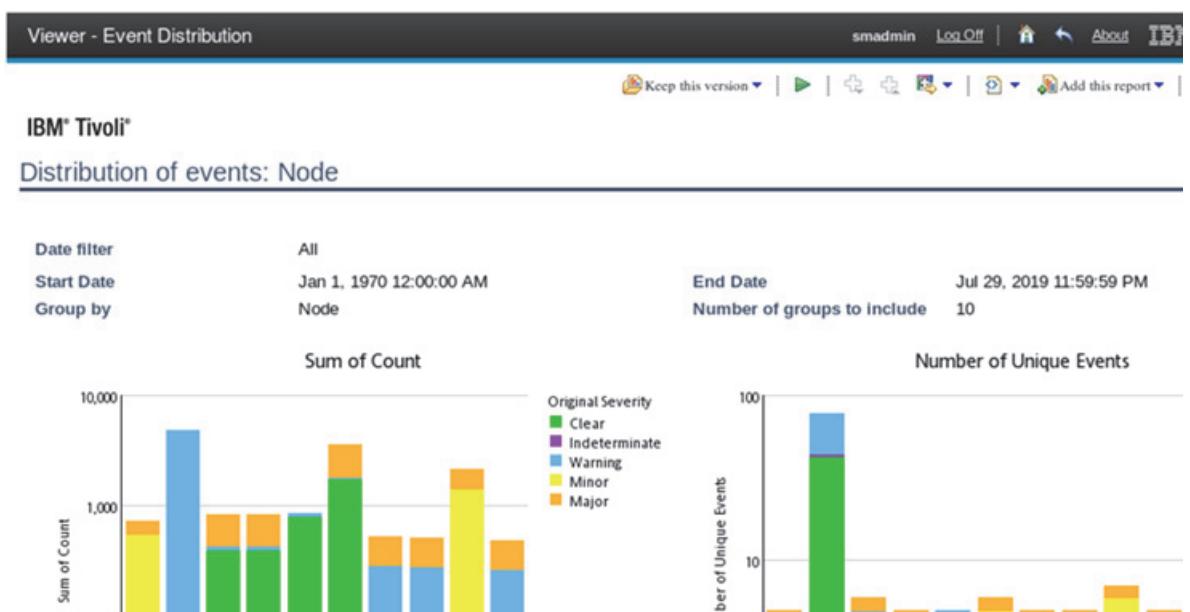
b. Click **Event Distribution**.



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

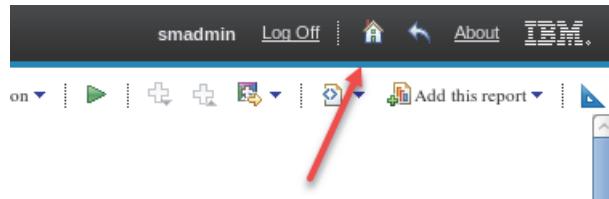
The screenshot shows the 'Grouping Criteria' dialog box. It has a 'Group by*' dropdown set to 'Node', a 'Number of groups to include' input field containing '10', and a 'Finish' button at the bottom right. A red arrow points to the 'Finish' button.

The report is generated and the event distribution report opens.

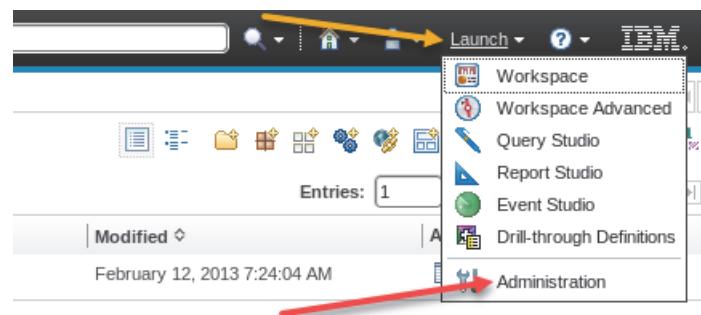


15. The smadmin user is configured with full access to Common Reporting features. Modify Common Reporting to allow access for all other users.

- Click the icon to return to the home page.

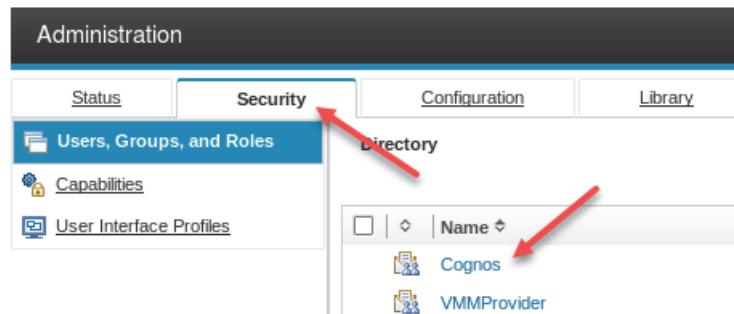


- Click **Launch** and select **Administration**.



- Click the **Security** tab.

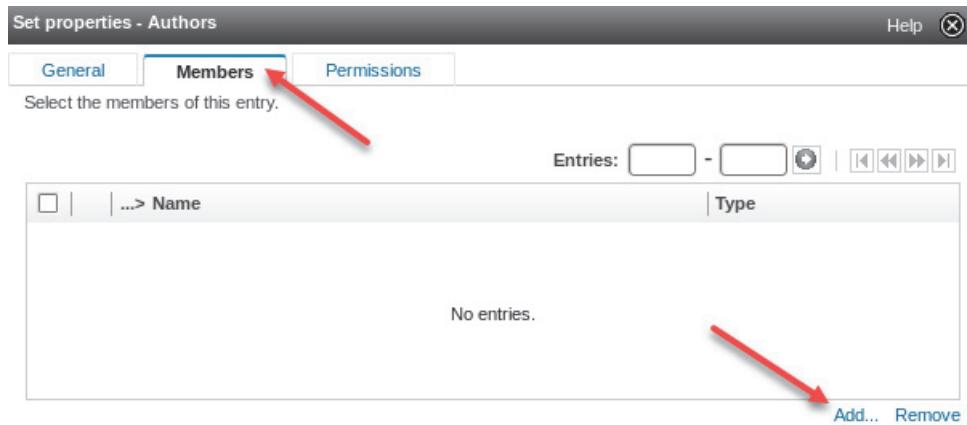
- Click **Cognos**.



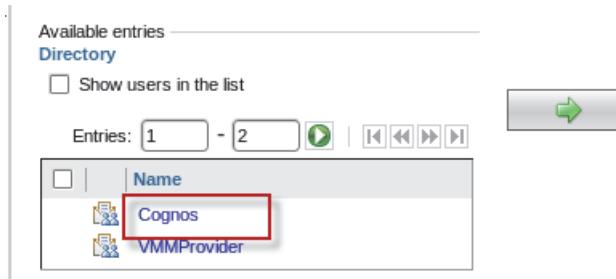
16. Select **Authors**, and click the icon to set properties.

	Name	Modified	Actions
<input type="checkbox"/>	Adaptive Analytics Administrators	July 29, 2019 2:00:51 PM	
<input type="checkbox"/>	Adaptive Analytics Users	July 29, 2019 2:02:40 PM	
<input type="checkbox"/>	All Authenticated Users	July 29, 2019 2:00:50 PM	
<input type="checkbox"/>	Analysis Users	July 29, 2019 2:02:40 PM	
<input type="checkbox"/>	Anonymous	July 29, 2019 2:00:56 PM	
<input checked="" type="checkbox"/>	Authors	July 29, 2019 2:02:39 PM	
<input type="checkbox"/>	Cognos Insight Users	July 29, 2019 2:02:40 PM	

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



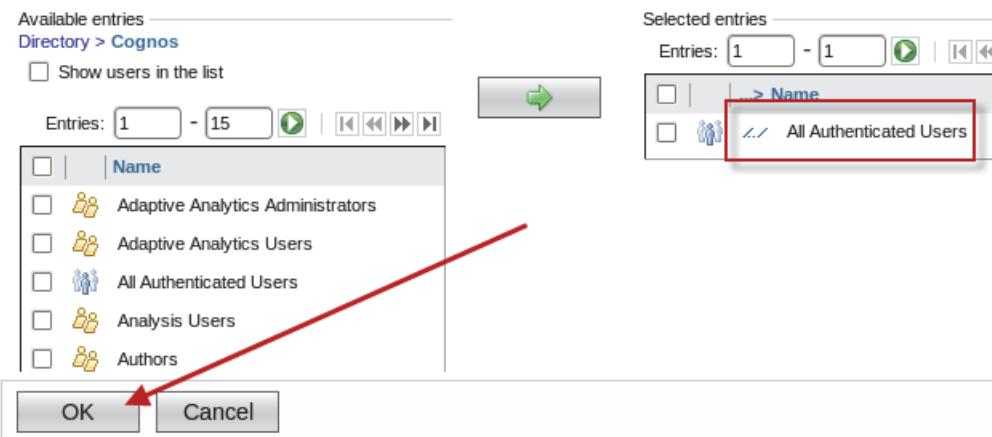
18. Click **Cognos**.

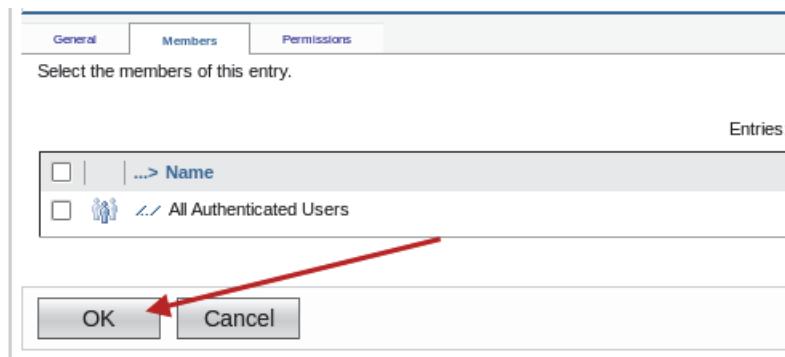


19. Select **All Authenticated Users**. Click the *green arrow* icon to add the entry.



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.

```
cd /software/impact
```

```
unzip TNIV7.1.0.16_LNX_EN.zip
```

2. Start IBM Installation Manager:

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

IBM Installation Manager opens.

3. Define the Impact repositories.

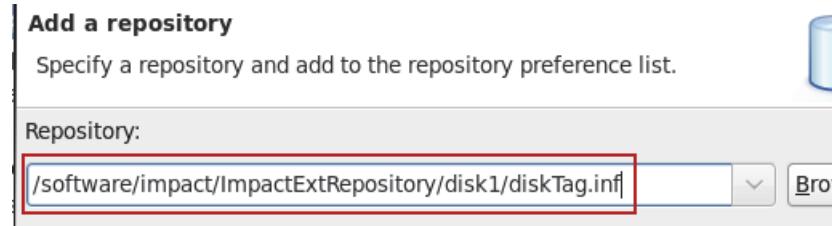
a. Click **File** and select **Preferences**.

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**.

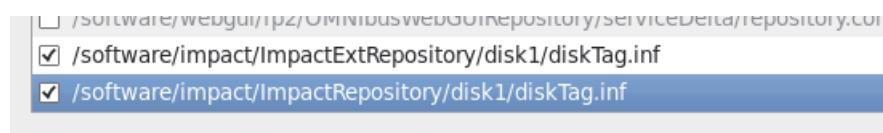
- g. Click **Browse** and select the following repository:

/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
BM Tivoli Netcool/Impact GUI Server Version 7.1.0.16	Will be installed	IBM
BM Tivoli Netcool/Impact Server Version 7.1.0.16	Will be installed	IBM
BM Tivoli Netcool/Impact Server Extensions for Netcool Operati Version 7.1.0.16	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**.



Package Group Name: IBM Tivoli Netcool Impact

Installation Directory: /opt/IBM/tivoli/impact

Architecture Selection: 32-bit 64-bit

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

Common Configurations

User Registry

Select the user registry to use for user management and authentication.

- ObjectServer
- ObjectServer with SSL
- LDAP
- LDAP with SSL
- Local File Based

- f. Click **OK**.



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

Provide an administrative user ID and password for Impact

Impact User ID

Impact Password (Minimum 6 characters)

Confirm Impact Password

- h. 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

Starting port number for Impact Server RMI (a 100 Port range will be used!)

ActiveMQBroker port number of GUI Server

Starting port number for GUI Server



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

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



Note: The installation runs for approximately 35 minutes.

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

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

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

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

6. Remove the installation files.

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

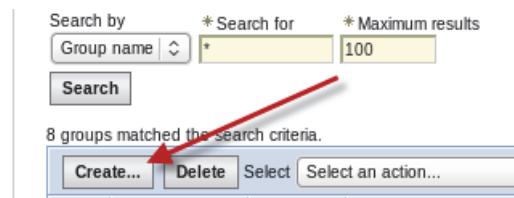
Configuring Netcool/Impact to use LDAP

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**.

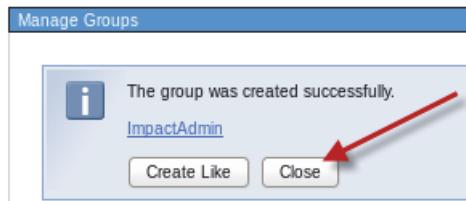


6. Enter **ImpactAdmin** for the Group name. Click **Create**.

The screenshot shows a 'Create a Group' dialog box. At the top is a title bar with the text 'Create a Group'. Below it is a form with a single input field labeled '* Group name' containing the value 'ImpactAdmin'. There is also a 'Description' field below it which is currently empty.

Important: The group name must be ImpactAdmin.

7. Click **Close**.



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

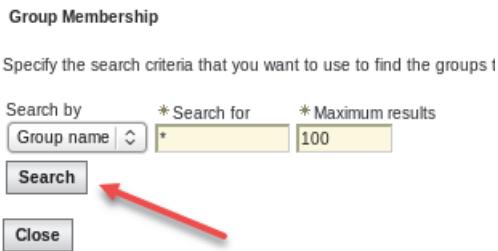
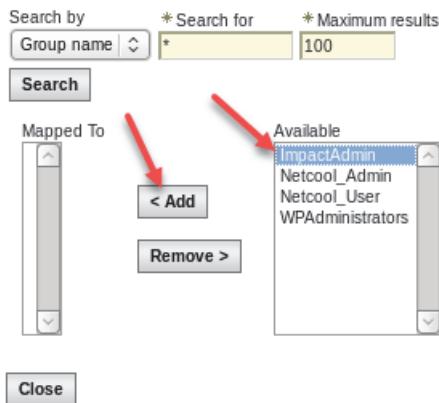


9. Click **Create**.



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

The screenshot shows a 'Create a User' dialog box. It includes fields for 'User ID' (containing 'impactadmin'), 'First name' (containing 'Impact'), 'Last name' (containing 'Admin'), 'E-mail' (containing 'impactadmin'), 'Password' (containing '*****'), 'Confirm password' (containing '*****'), and 'Group Membership'. Red arrows point to the 'User ID' field, the 'First name' and 'Last name' fields, and the 'Group Membership' button.

11. Click **Search**.12. Click **ImpactAdmin** to select it. Click **Add**.13. Click **Close**.

14. Click **Create**.

Create a User

* User ID: impactadmin Group Membership

* First name: Impact * Last name: Admin

E-mail:

* Password: ***** * Confirm password: *****

Create **Cancel**

15. Click **Close**.

16. Log out of WebSphere administrative console.

17. Close the Firefox tab.

18. Log out of Dashboard Application Services Hub.

19. Modify the property file.

- Change to the target directory:

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

- Save a copy of the original file:

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

- Modify the file:

```
gedit impactdap.properties
```

- Configure the following property values:

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

- Save the file and exit the gedit utility.

20. Run the configuration script.

- Run the following command to start the script.

```
./confAuth4LDAP.sh enable impactadmin object00 object00 object00
```

- Enter **object00** as the Bind DN password.

Enter LDAP Bind DN password: **object00**

- Look for messages that confirm the Impact servers have started and that the build is successful.

...

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: 4 minutes 45 seconds



Important: The build must be successful before you continue.

21. 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.

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

Verify that the user can access Netcool/Impact.

- Log out.

22. 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 course, you use LDAP as the common user repository.

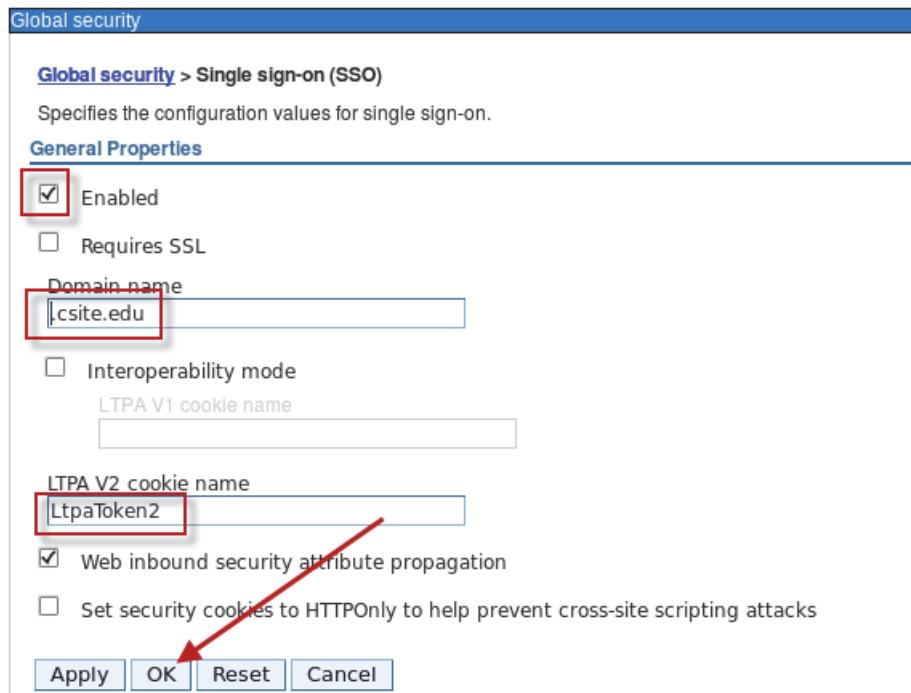
1. Open a Firefox browser.
2. Log in to Dashboard Application Services Hub as user **smadmin** with password **object00**.
3. Start WebSphere administrative console.
4. Enable single sign-on.
 - a. Expand **Security** and click **Global security**.



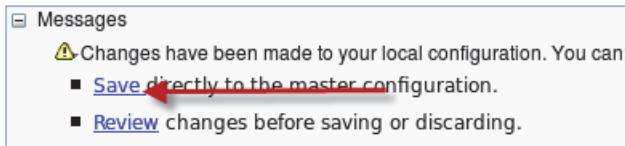
- b. On the right side of the page, expand **Web and SIP security**. Click **Single sign-on (SSO)**.

A screenshot of the 'Authentication' configuration page. It shows 'Authentication mechanisms and expiration' with 'LTPA' selected. Below that is 'Web and SIP security' with 'General settings' expanded. Under 'General settings', 'Single sign-on (SSO)' is highlighted with a red box and has a red arrow pointing to it from the left. Other options like 'Kerberos and LTPA' and 'SPNEGO web authentication' are also listed.

- 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, click the **Key stores and certificates** link.



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

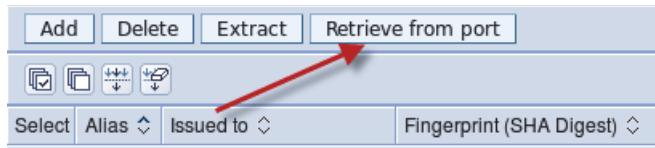
Select	Name ▾	Description ▾	Management Scope ▾
You can administer the following resources:			
<input type="checkbox"/>	NodeDefaultKeyStore	Default key store for JazzSMNode01	(cell):JazzSMNode01Cell:(node):JazzSMNode01
<input type="checkbox"/>	NodeDefaultTrustStore	Default trust store for JazzSMNode01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

- d. Under the *Additional Properties* section, select the **Signer certificates** link. The link is on the right side of the page.

The screenshot shows a sidebar titled "Additional Properties" with the following links:

- [Signer certificates](#) (highlighted with a red box)
- [Personal certificates](#)
- [Personal certificate requests](#)
- [Custom](#)

- 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

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

Retrieved signer information

Serial number
309156848

Issued to
CN=host1.csuite.edu, O=IBM, OU=ImpactUI, C=US

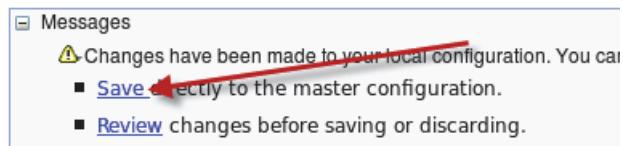
Issued by
CN=host1.csuite.edu, O=IBM, OU=ImpactUI, C=US

Fingerprint (SHA digest)
89:C8:F7:A9:0E:E6:3E:86:7A:BA:42:52:6E:2D:1A:8A:0F:8E:66:D4

Validity period
Nov 6, 2025

Apply OK Reset Cancel

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 pasting them into the key file, and click Export keys. Then, log on to the other cell, specify the same key file, and click Import keys.

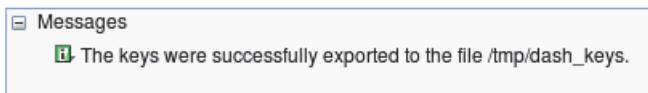
* Password

* Confirm password

Fully qualified key file name
/tmp/dash_keys

Import keys Export 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.csuite.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**.

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



4. Enter **impactadmin** and click **Search**.

User ID: impactadmin

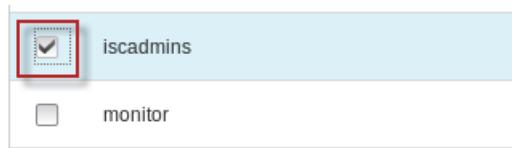
Number of results to display: 20

Search

5. Click **impactadmin**.

Select	User ID	Active	First
	impactadmin	Not Active	Impact

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



7. Logout as user **smadmin**.

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

9. 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.

* Required field

Console Integration ID:	
* Console Integration Name:	NetcoolImpact
* Console Integration URL:	https://host1.csuite.edu:17311/ibm/console/rest
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.

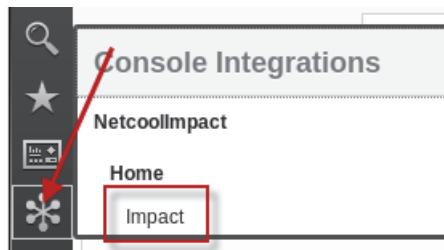
Select	Name	Status
<input checked="" type="radio"/>	NetcoolImpact	Connection Successful

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

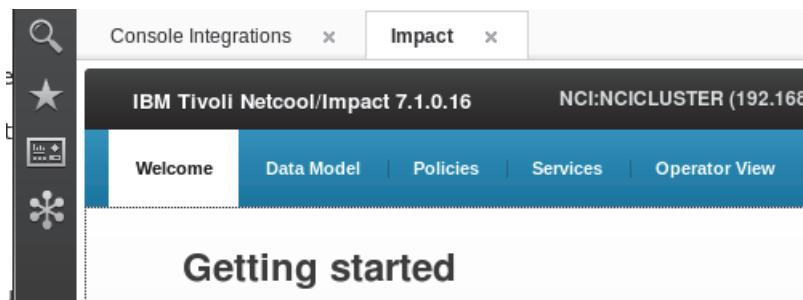


Important: The icon is visible for only users that are valid Netcool/Impact users.

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 this 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.

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

```
./mapRoles.sh -list -all
Roles:
ConsoleUser
ReadAdmin
WriteAdmin
impactAdminUser
impactFullAccessUser
impactMWMAdminUser
impactMWMUser
impactOSLCDDataProviderUser
impactOpViewUser
impactRBAUser
```

```
impactRestConfigurationRole  
impactSelectedOpViewUser  
impactUIDataProviderUser  
impactWebServiceUser
```

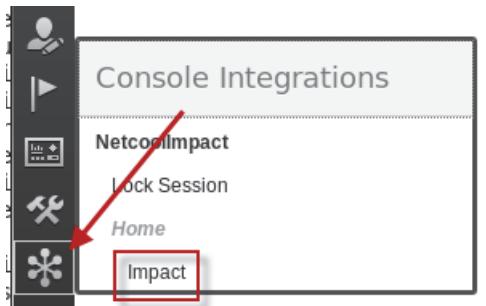
2. Add the impactAdminUser role to the Netcool_Admin group.

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

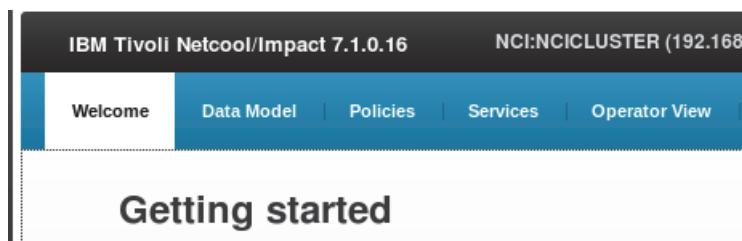
Adding group Netcool_Admin to role impactAdminUser

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:

- Change to the root user.

```
su -  
Password: object00
```

- Copy the supplied start script:

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

- Change the file permissions to allow execution:

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

- Create the logical links to enable the autostart feature:

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

2. Restart the Netcool/Impact components.

- Stop the NCI server component.

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

```
Stopping server NCI.  
Server NCI stopped.
```

- Stop the GUI server component.

```
/etc/init.d/impact_gui stop
```

```
Stopping server ImpactUI.  
Server ImpactUI stopped.
```

- 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
```

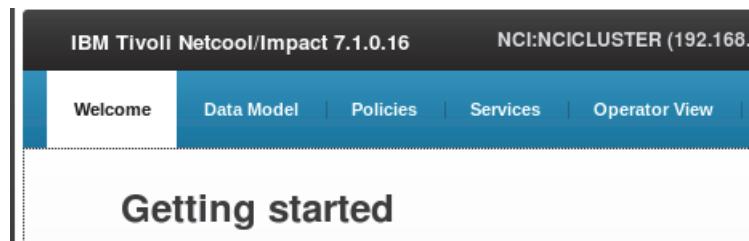
3. Open a Firefox browser.

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 starts.



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 Red Hat Enterprise Linux.

```
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 6 or 7.

4. Verify the 64-bit library requirement.

```
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 is disabled.

```
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 the Python version.

```
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 the server IP address and host name.

- a. To verify that the host name is configured correctly, enter the following command:

```
hostname
```

host1.csuite.edu

- b. To verify that the host name uses the fully qualified host name, enter the following command:

```
hostname -f
```

host1.csuite.edu

- c. 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.

```
ulimit -n
```

131073

10. Verify the virtual memory limit.

```
ulimit -v
```

unlimited

The suggested `ulimit -v` setting, which limits the virtual memory for processes, is **unlimited**.

11. Verify the locale setting.

```
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 archive file.

```
mkdir /software/la/lacore
```

```
cd /software/la/lacore
```

```
tar -zxvf ../../IOALAMDB1.3.5.3_LNX64BALLEDITEN.tar.gz
```

2. Start IBM Installation Manager:

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

IBM Installation Manager opens.

3. Define the Log Analysis repository.

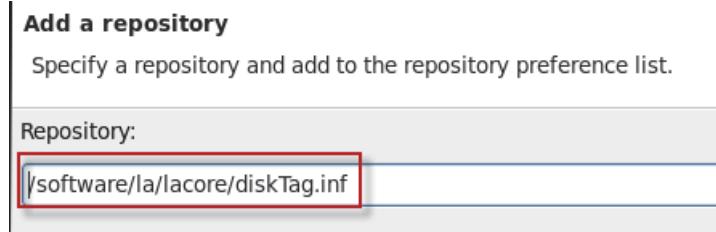
a. Click **File** and select **Preferences**.

b. Click **Repositories**.

c. Remove the check marks from the existing entries and click **Add Repository**.

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

```
/software/la/lacore/diskTag.inf
```



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

f. 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
▼	<input checked="" type="checkbox"/> IBM Operations Analytics - Log Analysis	
	<input checked="" type="checkbox"/> Version 1.3.5.3	Will be installed

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 1.3.5.3
	<input checked="" type="checkbox"/> IBM Operations Analytics - Log Analysis 1.3.5.3
	<input checked="" type="checkbox"/> Apache Solr 7.5.0
	<input checked="" type="checkbox"/> IBM Tivoli Log File Agent 06.30.02.00

- g. Accept the default port numbers and click **Next**.

Configuration for IBM Operations Analytics - Log Analysis 1.3.5.3

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 for approximately 15 minutes.

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



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

The following package was installed:

▼	IBM Operations Analytics - Log Analysis
	IBM Operations Analytics - Log Analysis 1.3.5.3

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.csuite.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 header bar with a search bar and various icons. Below it, the main navigation bar includes 'Administrative Settings', 'Learn More', and a dropdown for the user 'unityadmin'. A red arrow points from the top right towards the 'Logout' button in the user dropdown menu. The main content area has sections for 'New Search' and '+ Add Search'.

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**.

The screenshot shows a 'Create Group' dialog. It has a field labeled '* Group name' containing the value 'UnityAdmins'. There is also a 'Description' field below it.

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**.

A screenshot of the 'Create a User' interface. At the top, it says '30 users matched the search criteria.' Below that is a toolbar with 'Create...', 'Delete', 'Select', and 'Select an action...'. The 'Create...' button is highlighted with a red arrow. Below the toolbar is a search bar with fields for 'Select', 'User ID', 'First name', 'Last name', and 'E-mail'. The 'User ID' field contains 'unityadmin'.

11. Enter **unityadmin** for the User ID. Enter values for the first and last name fields. Enter **object00** for the password. Click **Group Membership**.

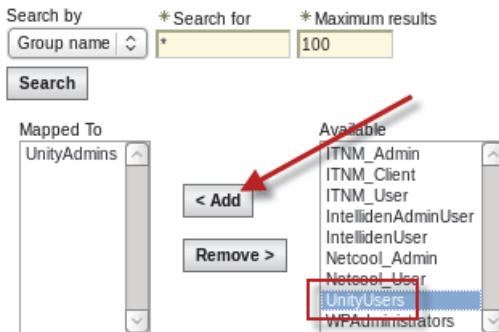
A screenshot of the 'Create a User' form. The 'User ID' field is highlighted with a red box and has an arrow pointing to the 'Group Membership' button. The 'First name' field is highlighted with a red box and has an arrow pointing to the 'Last name' field, which is also highlighted with a red box. The 'Password' and 'Confirm password' fields are both highlighted with red boxes.

12. Click **Search** to display the available groups.

13. Click **UnityAdmins** to select the entry. Click **Add**.

A screenshot of the 'Group Membership' search interface. It shows a search form with 'Search by' set to 'Group name', 'Search for' empty, and 'Maximum results' set to 100. A red arrow points to the 'Search' button. Below the search form are two lists: 'Mapped To' and 'Available'. The 'Available' list contains 'Netcool_Admin', 'Netcool_User', 'UnityAdmins' (which is highlighted with a red box), 'UnityUsers', and 'WPAdministrators'. There are '< Add' and 'Remove >' buttons between the lists.

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.

- 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. Find the following line. Remove the comment character (#) from the front of the line.

```
ldap_type_property=IBM Tivoli Directory Server
```

- e. Find the following lines and enter these values:

```
ldap_hostname_property=host1.csuite.edu
```

```
ldap_port_property=389
```

```
ldap_baseDN_property=DC=IBM,DC=COM
```

- f. Find the following lines and enter these values:

```
ldap_bindDN_property=cn=root
```

```
ldap_bindPassword_property=object00
```

```
ldap_realm_property=defaultWIMFileBasedRealm
```

- g. 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.
...
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.

- a. Run the following command to view the current user registry configuration.

```
more /opt/IBM/LogAnalysis/wlp/usr/servers/Unity/server.xml
```

- b. Verify that the line that references the `unityUserRegistry.xml` file is commented out.

Verify that the line that references the `ldapRegistry.xml` file is not commented out.

```
</application>
<httpEndpoint id="defaultHttpEndpoint" port="9988" httpsPort="9987">
  <tcpOptions soReusePort="true" />
</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 Unity configuration for war control and role mapping -->
<include optional="true" location="${server.config.dir}/unityConfig.xml"/>
<!-- Override updateTrigger for applicationMonitor -->
<applicationMonitor updateTrigger="10000" />
<!-- default keystore for certificates. located in <install home>/wlp/usr/servers/Unity/res
```

This line must be commented out

This line must NOT be commented out

25. Stop Log Analysis.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -stop
...
Stopped All Services...
```

26. Start Log Analysis.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -start
...
Started All Services...
```

27. Open a Firefox browser if necessary.

28. Connect to the following URL:

<https://host1.cssite.edu:9987/Unity/>

29. 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**.

30. Verify access and log out.

The screenshot shows a web browser window with the URL <https://host1.cssite.edu:9987/Unity/> in the address bar. The page title is "Log Analysis". The top navigation bar includes "Administrative Settings", "Learn More", and a dropdown menu for "unityadmin" which has options "Change Password" and "Logout". A red arrow points to the "unityadmin" dropdown, and a red box highlights the "Logout" button. Below the header, there is a search bar and a "Search" button. The main content area contains descriptive text about log analysis and links for "Logs" and "Dashboard".

31. 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 must 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 text string.

4. Modify the Log Analysis server.xml file.

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/wlp/usr/servers/Unity
```

- b. Save a copy of the file.

```
cp server.xml server.xml.orig
```

- c. Open the file in a text editor.

```
gedit server.xml
```

- d. Scroll to the bottom of the file. Add the two lines that are shown here in bold text. The value for `keysPassword` is the encoded password from the previous step. Add the lines between the `</oauthProvider>` and `</server>` lines.

```
</oauthProvider>  
<webAppSecurity ssoDomainNames="DashDomain" />  
<ltpa keysFileName="${server.output.dir}/resources/security/dash_keys"  
keysPassword="{xor}MD01Ojwrb28=" expiration="1440" />  
</server>
```

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

5. Stop Log Analysis.

```
/opt/IBM/LogAnalysis/utilities/unity.sh -stop  
...  
Stopped All Services...
```

6. Start Log Analysis.

```
/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.

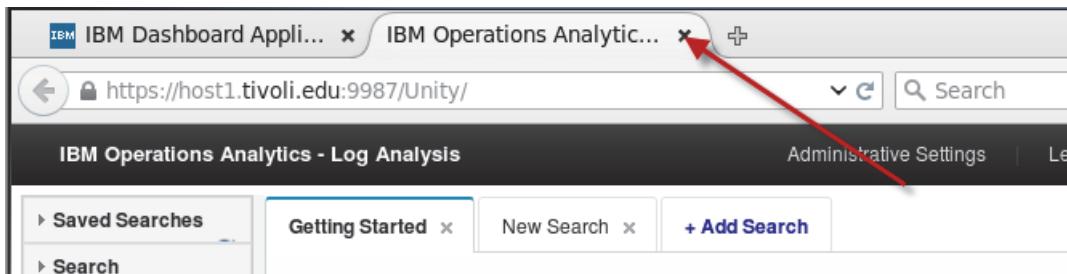


11. Connect to the following URL in the new tab:

<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.

```
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}FFAC4A5CBA0A3CC785330D7F5B1DEFF25
```



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 **unityuser**, you must update the password in the following files to match the updated password.

3. Modify the data collector file.

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/utilities/datacollector-client
```

- b. Save a copy of the file.

```
cp javaDatacollector.properties javaDatacollector.properties.orig
```

- c. Open the file in a text editor.

```
gedit javaDatacollector.properties
```

- d. Find 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 your encrypted password.

```
password = {aes}FFAC4A5CBA0A3CC785330D7F5B1DEFF25
```

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

4. Modify the `rest-api` file.

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/remote_install_tool/config
```

- b. Save a copy of the file.

```
cp rest-api.properties rest-api.properties.orig
```

- c. Open the file in a text editor.

```
gedit rest-api.properties
```

- d. Find 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.

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/UnityEIFReceiver/config
```

- b. Save a copy of the file.

```
cp unity.conf unity.conf.orig
```

- c. Open the file in a text editor.

```
gedit unity.conf
```

- d. Find 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.

- a. Change to the target directory:

```
cd /opt/IBM/LogAnalysis/solr_install_tool/scripts
```

- b. Save a copy of the file.

```
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 in a text editor.

```
gedit register_solr_instance.sh
```

- e. Find 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.

- a. Change to the target directory.

```
cd /opt/IBM/LogAnalysis/utilities
```

- b. Save a copy of the file.

```
cp pkg_mgmt.sh pkg_mgmt.sh.orig
```

- c. Change file permissions to allow modifications:

```
chmod +w pkg_mgmt.sh
```

- d. Open the file in a text editor.

```
gedit pkg_mgmt.sh
```

- e. Find 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
```

...

```
Started All Services...
```

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.

4. Exit the root user back to the **netcool** user.

```
exit
```

5. Open a Firefox browser.

6. Enter the following URL:

```
https://host1.csuite.edu:9987/Unity/
```

7. Log in with user **unityadmin** and password **object00**.

A successful login verifies that Log Analysis started when the server started.

8. Log out of Log Analysis.

9. 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 license key.

1. Change to the target directory.

```
cd /opt/IBM/LogAnalysis/utilities/
```

2. Run the following command to apply the license.

```
./unity_change_edition_util.sh -p /software/la/IOALA_ENABMT_KEY_STD_ED.swttag
```

3. Enter **y** when you are prompted.

You have ENTRY EDITION license. Would you like to upgrade to STANDARD MANAGED DEVICE BASED EDITION license (y/n)?:

y

4. Enter **q** to go to the end of the license agreement.

5. Enter **A** to accept the terms.

A

Upgraded license to STANDARD MANAGED DEVICE BASED EDITION. Restart IBM Operations Analytics - Log Analysis.

6. Run the following command to restart Log Analysis.

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

7. Look for a message like the following example. This message confirms that the license has been applied.

```
Starting IBM Operations Analytics - Log Analysis v1.3.5.3 STANDARD MANAGED DEVICE BASED EDITION
```

Configuring the Network Manager workaround

IBM Tivoli Network Manager v4.2 now uses the Apache ZooKeeper 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.

```
cp unity.sh unity.sh.orig
```

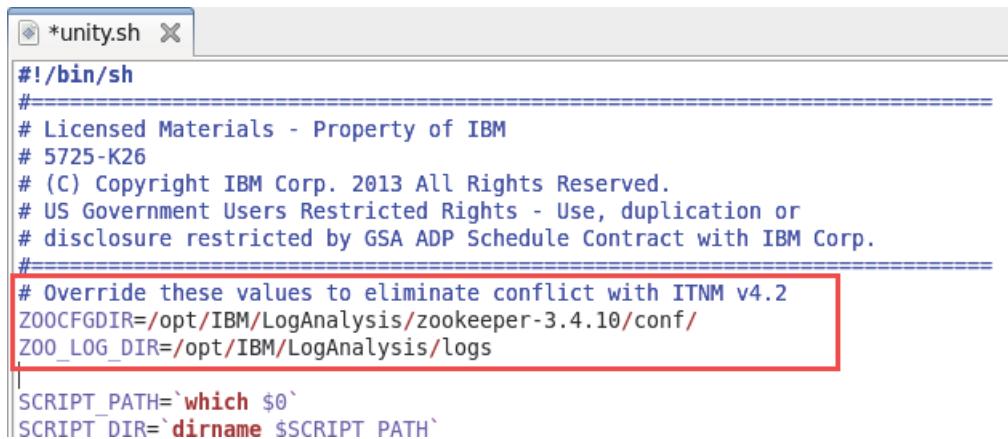
3. Modify the script.

a. Open the file in a text editor.

```
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-3.4.10/conf/
ZOO_LOG_DIR=/opt/IBM/LogAnalysis/logs
```



```
#!/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-3.4.10/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. Restart the Log Analysis components.

```
./unity.sh -restart
```

Wait for the components to start.

b. Verify the status of the Log Analysis components.

```
./unity.sh -status
```

IBM Operations Analytics - Log Analysis v1.3.5.3 STANDARD MANAGED DEVICE
BASED EDITION Application Services Status:

No.	Service	Status	Process ID
1	Derby Network Server	UP	32557
2	ZooKeeper	UP	32618
3	Websphere Liberty Profile	UP	607
4	EIF Receiver	UP	873
5	Log File Agent instance	UP	1187

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 started 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 OMNIbus 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
```

```
...
```

```
All Application Services are in Running State
```

```
Checking server initialization status: Server has initialized!
```

2. Create a directory for 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_v1.3.1.0.zip OMNIbus
```

4. Install the insight pack.

```
cd OMNIbus
```

 **Note:** Enter the following text as one line.

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

...

```
[packagemanager] 07/30/19 18:03:42:843 UTC [main] INFO - ContentPackManager :  
CTGLC0023I : Install of OMNIbusInsightPack_v1.3.1.0 completed successfully
```

BUILD SUCCESSFUL

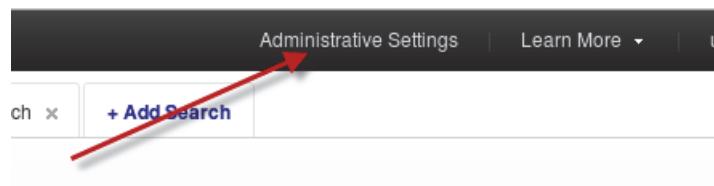
Total time: 5 seconds

 **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 (pkg_mgmt.sh) 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.csuite.edu:9987/Unity/>
3. Log in with user **unityadmin** and password **object00**.
4. Click **Administrative Settings**.

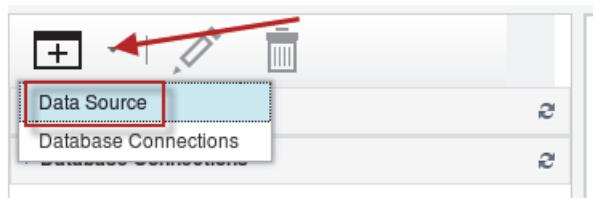


The administrative user interface opens in a new Firefox tab.

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.csuite.edu** as the host name. Click **Next**.

* **Select Location** * **Select Data** * **Set Attributes**

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

Local file
 Remote file
 Custom

* Host name:

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						
<hr/>								
Enter the location and type of data for this data source. The file path is not validated when you click Next.								
More...								
<table border="0"> <tr> <td style="padding-right: 20px;">* File path:</td> <td><input type="text" value="NOI_AGG_P"/></td> </tr> <tr> <td style="padding-right: 20px;">* Type:</td> <td> <input type="text" value="OMNIbus1100"/> → </td> </tr> <tr> <td style="padding-right: 20px;">Collection:</td> <td> <input type="text" value="OMNIbus1100-Collection"/> → </td> </tr> </table>			* File path:	<input type="text" value="NOI_AGG_P"/>	* Type:	<input type="text" value="OMNIbus1100"/> →	Collection:	<input type="text" value="OMNIbus1100-Collection"/> →
* File path:	<input type="text" value="NOI_AGG_P"/>							
* Type:	<input type="text" value="OMNIbus1100"/> →							
Collection:	<input type="text" value="OMNIbus1100-Collection"/> →							
<small>* Required</small>								

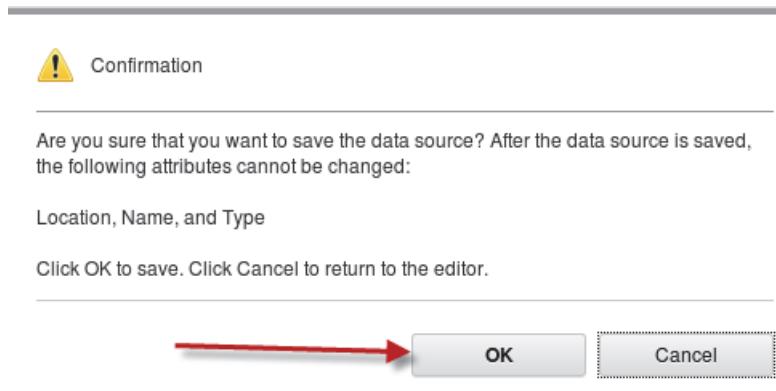
11. Enter **omnibus** for the **Name** field and click **Finish**.



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						
<hr/>								
Enter a name for the new data source. Optionally, set a description and assign the source to a group.								
<table border="0"> <tr> <td style="padding-right: 20px;">* Name:</td> <td><input type="text" value="omnibus"/></td> </tr> <tr> <td>Description:</td> <td><input type="text"/></td> </tr> <tr> <td>Group:</td> <td><input type="text"/></td> </tr> </table>			* Name:	<input type="text" value="omnibus"/>	Description:	<input type="text"/>	Group:	<input type="text"/>
* Name:	<input type="text" value="omnibus"/>							
Description:	<input type="text"/>							
Group:	<input type="text"/>							

12. Click **OK** to confirm the save.



13. Click **OK** to confirm.

14. Log out of the administration user interface.



15. Close the Firefox tab.

16. Log out of Log Analysis.

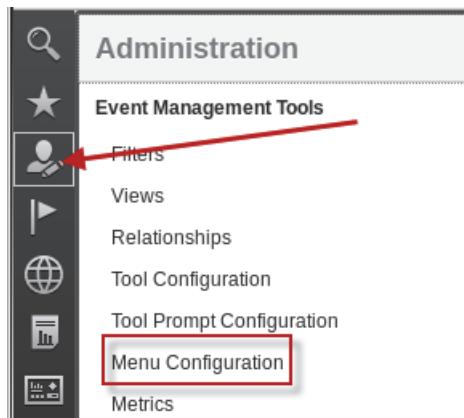


17. Close the Firefox browser.

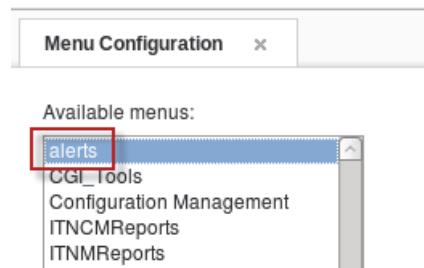
Configuring Web GUI

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**.

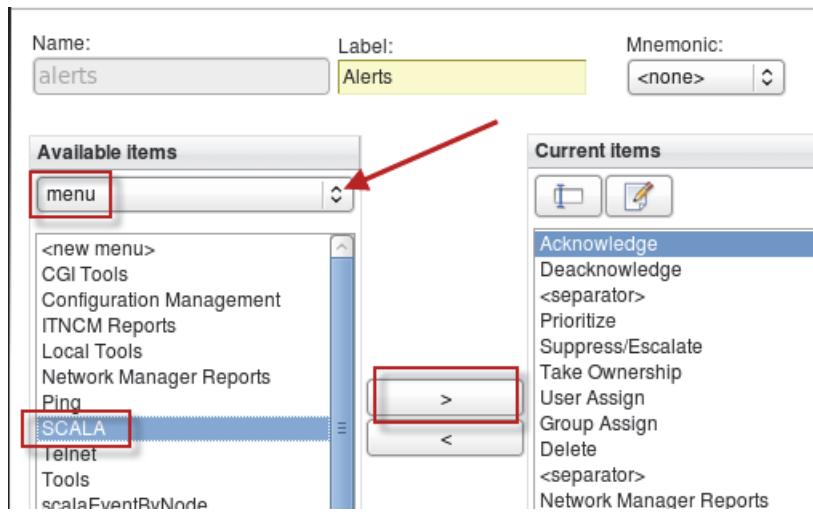


4. Click **alerts** to select it. Click **Modify**.



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 the menu up in the list.



8. Click **Save**.

9. Click **Ok**.

10. Log out of Dashboard Application Services Hub.

11. Close the **Firefox** browser.

Exercise 2 Message Bus Gateway

The event search 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_1.8.0/jre/bin/
```
 - c. Use the keytool utility to create a new keystore.



Note: Enter the following command 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")  
[no]: yes  
Enter key password for <host1key>:  
(RETURN if same as keystore password):
```

2. Check keystore contents.



Note: Enter the following command 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, Jul 30, 2019, keyEntry,  
Certificate fingerprint (SHA1):  
3D:13:94:06:CE:35:BE:B6:D0:EF:5F:73:5B:99:CF:8F:EC:39:AD:C7
```

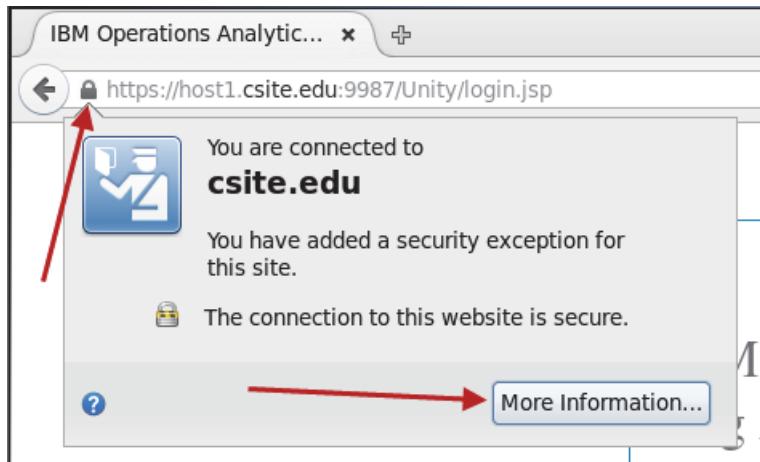
3. Export the server certificate from the host that runs IBM Operations Analytics Log Analysis with Firefox.

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

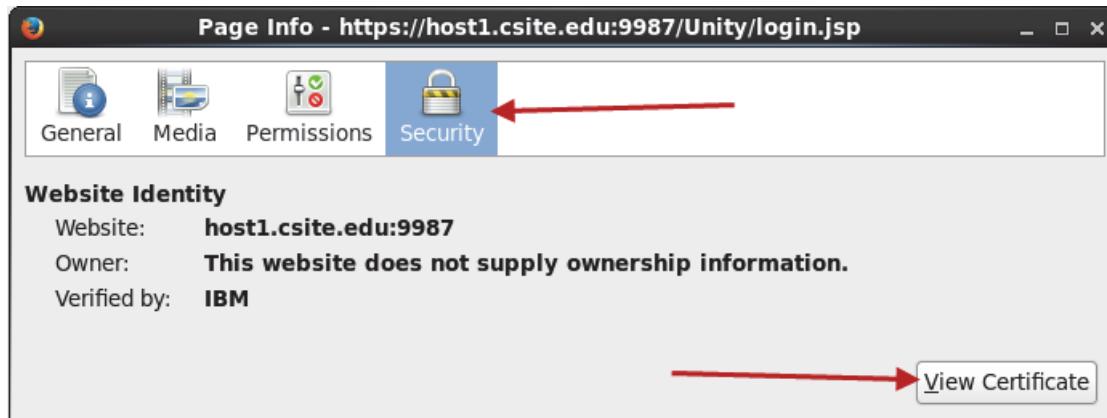
<https://host1.csite.edu:9987/Unity>

You see the IBM Operations Analytics Log Analysis login page. It is not necessary to log in with any user.

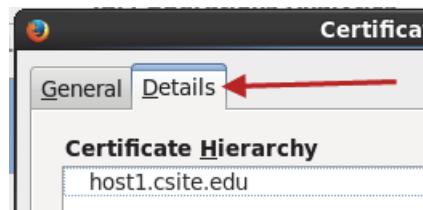
- b. Click the *padlock* icon and click **More Information**.



- c. Click **Security** and click **View Certificate**.



- d. Select the **Details** tab.

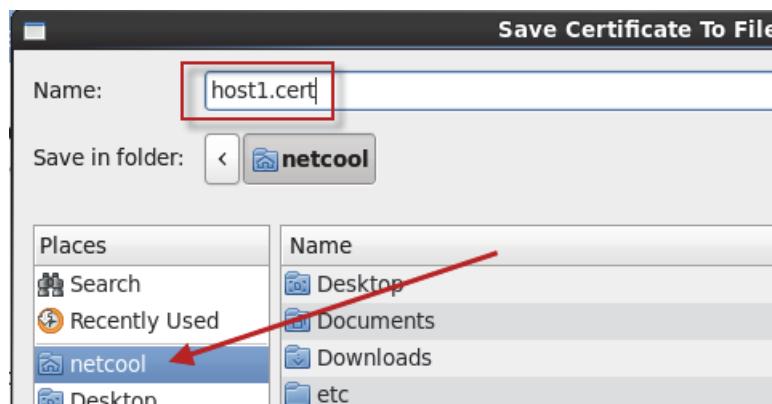


- e. Scroll to the bottom of the page and click **Export**.

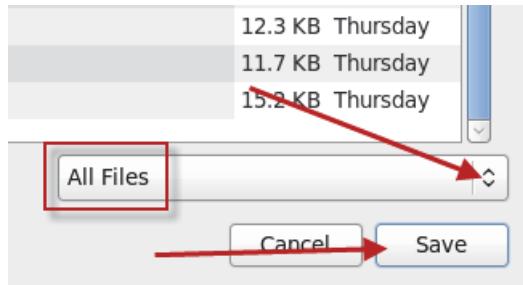


- f. Enter the following name for the file and click **netcool** to select the destination folder.

host1.cert

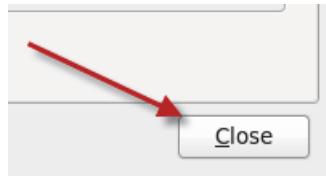


- g. Scroll down on the page. Select **All Files** for the output format. Click **Save** to export the file.



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_1.8.0/jre/bin
```



Note: Enter the following command as one line.

```
./keytool -import -keystore $OMNIHOME/java/security/cacerts.jks  
-file /home/netcool/host1.cert -alias loganalysis
```

Enter **object00** for the password when prompted.

```
Enter keystore password: object00  
Re-enter new password: object00
```

Enter **yes** to trust the certificate when prompted.

```
Trust this certificate? [no]: yes  
Certificate was added to keystore
```

Installing the gateway

The message bus gateway is installed with IBM Installation Manager.

1. Start IBM Installation Manager:

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

IBM Installation Manager opens.

2. Define the gateway repository.

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

- b. Select **Repositories**.

- c. Remove the check marks from all of the existing repository entries.

- d. Click **Add Repository**.

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

```
/software/msgbus/NCLOM_8P_GTY_FOR_MB_MPL_EN.zip
```



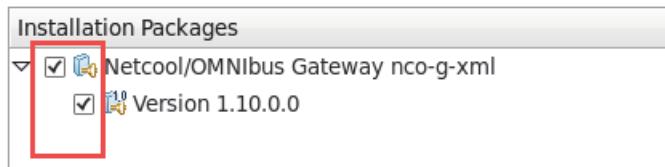
- f. Click **OK** to add the entry.

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

3. Start the installation.

- a. Click **Install**.

- b. Select the package and click **Next**.

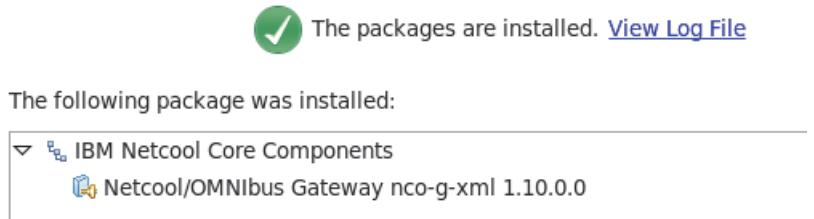


- c. Accept the license agreement and click **Next**.

- d. Leave the option set to use the existing package group and click **Next**.

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

- f. 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

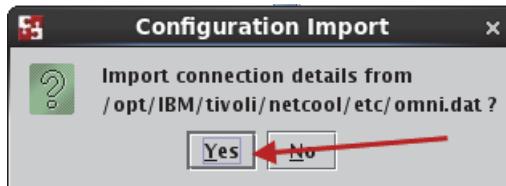
As provided with the product, the gateway replicates only new events to Log Analysis with standard IDUC. Event instances that deduplicate do not get sent to Log Analysis, because no configuration is in place to replicate these events without sending all updates.

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.

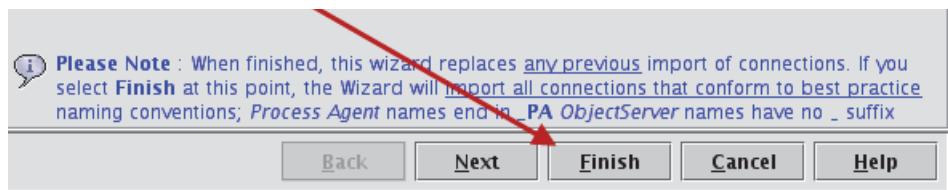
1. Start the Netcool/OMNIbus Administrator utility:

```
nco_config &
```

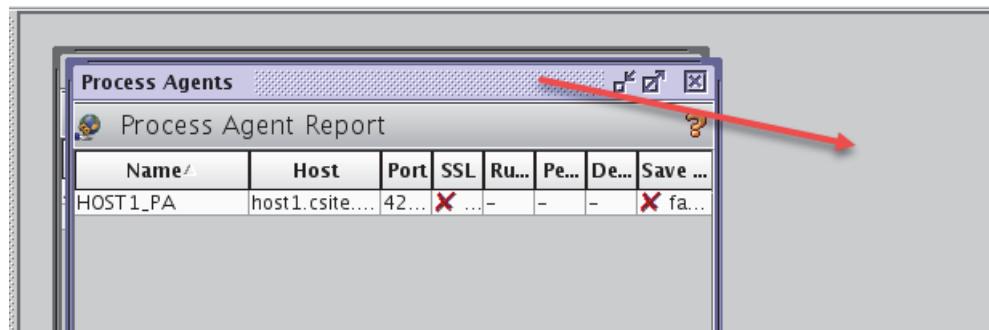
2. Click **Yes**.



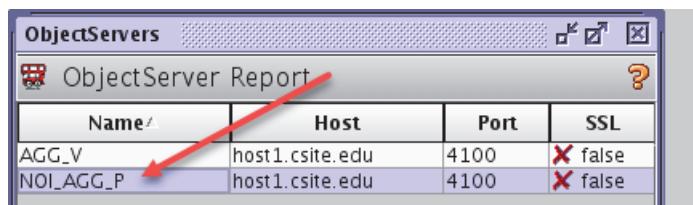
3. Click **Finish**.



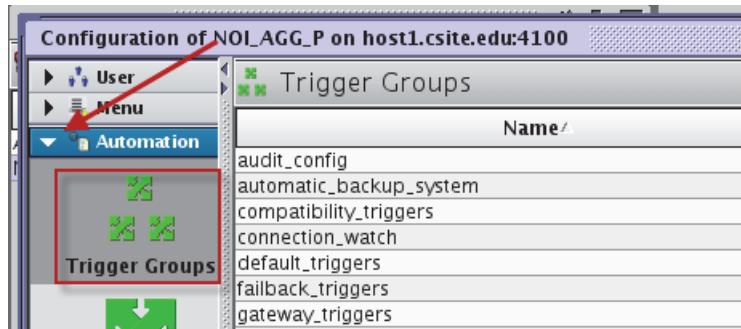
4. Drag the **Process Agents** window away to show the **ObjectServers** window.



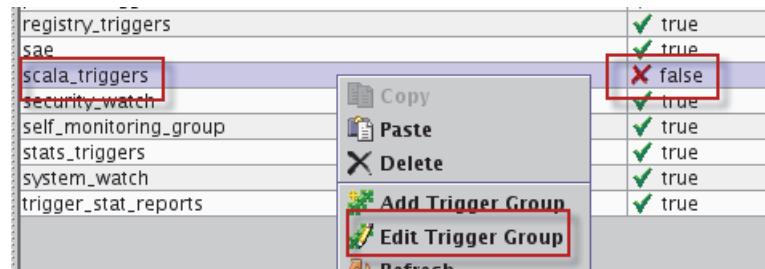
5. Double-click **NOI_AGG_P** in the list of ObjectServers.



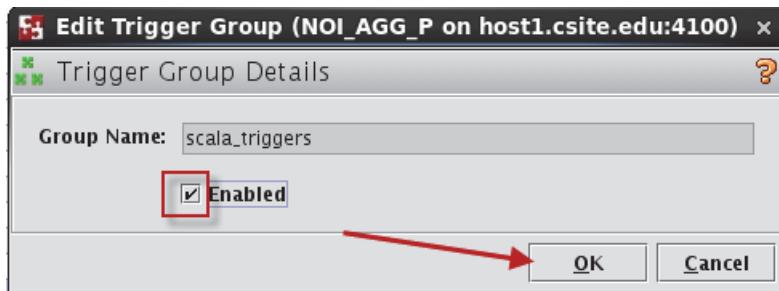
6. Connect to the **NOI_AGG_P** ObjectServer as the **root** user with password **object00**.
7. Expand **Automation** and select **Trigger Groups**.



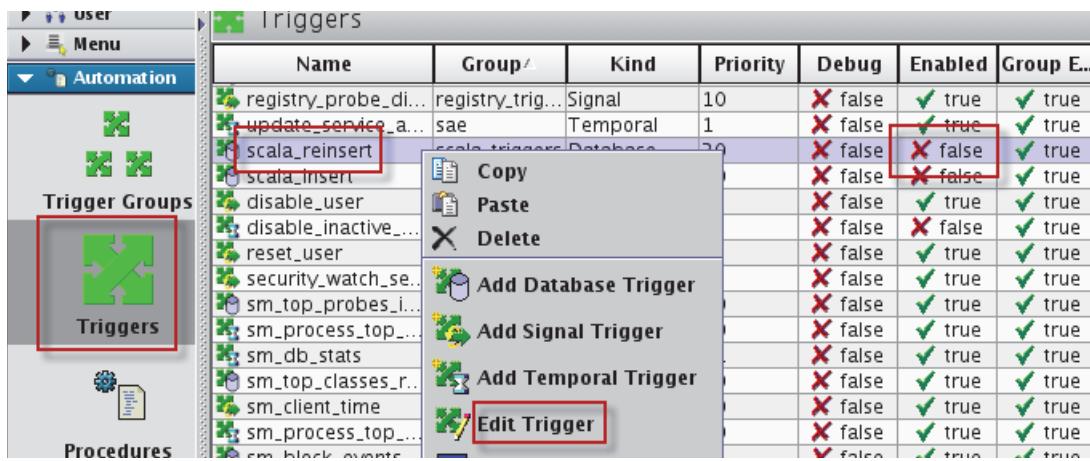
8. Right-click **scala-triggers** and select **Edit Trigger Group**.



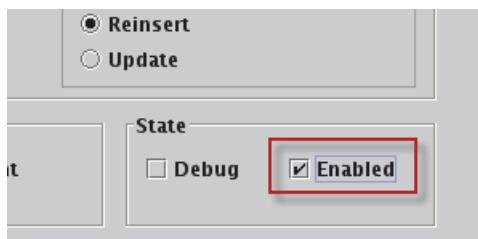
9. Select **Enabled** and click **OK**.



10. Select **Triggers**. Scroll down and find the two scala triggers. Right-click **scala_reinsert** and select **Edit Trigger**.



11. Select **Enabled** and click **OK**.



12. Repeat this step to enable the **scala_insert** trigger.

13. Verify that the triggers are both enabled.

Name	Group /	Kind	Priority	Debug	Enabled	Group E...
registry_probe_di...	registry_trig...	Signal	10	<input type="checkbox"/> false	<input checked="" type="checkbox"/> true	<input checked="" type="checkbox"/> true
update_service_a...	sae	Temporal	1	<input type="checkbox"/> false	<input checked="" type="checkbox"/> true	<input checked="" type="checkbox"/> true
scala_reinsert	scala_triggers	Database	20	<input type="checkbox"/> false	<input checked="" type="checkbox"/> true	<input checked="" type="checkbox"/> true
scala_insert	scala_triggers	Database	20	<input type="checkbox"/> false	<input checked="" type="checkbox"/> true	<input checked="" type="checkbox"/> true
disable user	security wa...	Signal	1	<input type="checkbox"/> false	<input checked="" type="checkbox"/> true	<input checked="" type="checkbox"/> true

14. Click **File** and select **Exit** to close the administrator utility.

15. Click **Yes** to confirm.

Configuring the gateway

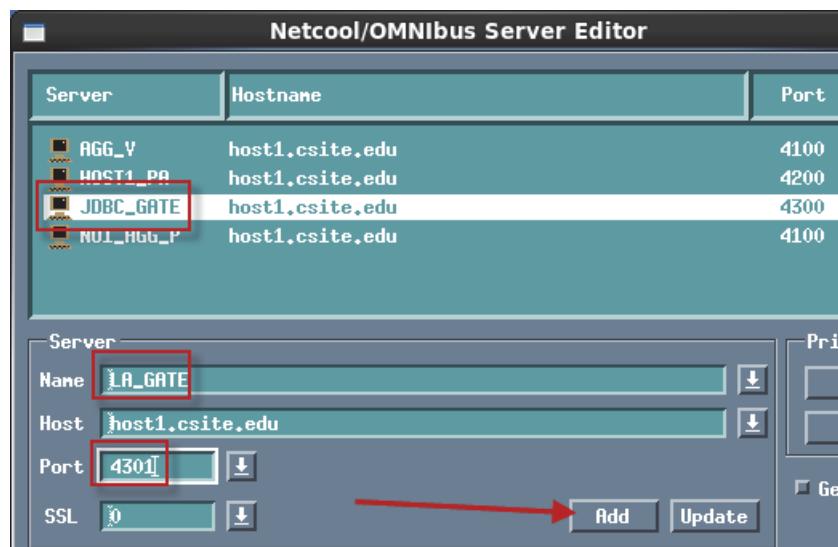
1. Add the gateway to the Netcool/OMNIbus communications file.

The gateway must have a name. For this exercise, use **LA_GATE**. The name must be added to the Netcool/OMNIbus communications file.

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

```
nco_xigen &
```

- b. Click the entry **JDBC_GATE** to select it.
- c. Change the Name to **LA_GATE**.
- d. 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. Verify that the entry for **LA_GATE** is listed.

Server	Hostname	Port
AGG_V	host1.csuite.edu	4100
HOST1_PA	host1.csuite.edu	4200
JDBC_GATE	host1.csuite.edu	4300
LA_GATE	host1.csuite.edu	4301
NOI_HUB_P	host1.csuite.edu	4100

- g. Click **Apply** and click **Close**.

2. Configure the gateway.

Some of the gateway configuration files are generic to the message bus gateway. Other gateway configuration files are used specifically for 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.

a. Open the file in a text editor.

```
gedit LA_GATE.props
```

b. Find the following lines near the top of the file:

```
MessageLog : '$OMNIHOME/log/G_SCALA.log'  
Name : 'G_SCALA'
```

c. Comment out these lines :

```
#MessageLog : '$OMNIHOME/log/G_SCALA.log'  
#Name : 'G_SCALA'
```

d. Find the following lines near the bottom of the file:

```
#####
# SCALA configuration
#####
```

- e. Add the following lines in bold text:

```
#####
# 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. Find the existing reader table replication definition:

```
Gate.Reader.TblReplicateDefFile :
'$OMNIHOME/gates/xml/scala/xml.reader.tblrep.def'
```

- g. Modify the property as shown here:

```
Gate.Reader.TblReplicateDefFile : '$OMNIHOME/etc/LA_GATE.reader.tblrep.def'
```

- h. Find the existing map file definition:

```
Gate.MapFile : '$OMNIHOME/gates/xml/scala/xml.map'
```

- i. Modify the property as shown here:

```
Gate.MapFile : '$OMNIHOME/etc/LA_GATE.1302.map'
```

- j. Find the existing startup file definition:

```
Gate.StartupCmdFile : '$OMNIHOME/gates/xml/scala/xml.startup.cmd'
```

- k. Modify the property 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. Find the following line:

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

- c. Change the line to match the following example:

```
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. Find the following text:

```
endpoint="https://localhost:9987/Unity/DataCollector"
```

c. Change the text to look like the following example:

```
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 another 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 another 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 similar to the following example:

```
2019-07-30T15:07:13: 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]
```

```
2019-07-30T15:07:13: 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:

```
07/30/19 15:07:22:862 UTC [Default Executor-thread-1545] ERROR - SolrUtil : CTGLA5556E :  
Error occurred while creating collection "UnityCollection_07_30_2019_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]
```

d. 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:

```
07/30/19 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  
07/30/19 15:13:45:533 UTC [Default Executor-thread-51] INFO -  
DataCollectorRestServlet : Batch of Size 200 processed and encountered 0  
failures  
07/30/19 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 Jul 30 15:13:45 UTC 2019].
```

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 timer. 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. Close both of the terminal windows that you used to view log files.

11. Stop the gateway.

a. Find the process ID 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
```

b. Stop the event gateway process:

```
kill -9 25406
```

12. 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 'LogAnalysisGateway'  
{  
    Command '$OMNIHOME/bin/nco_g_xml -name LA_GATE' run as 501  
    Host='host1.csuite.edu'  
    Managed=True  
    RestartMsg='${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, under the *ArchiveGateway* line.

```
process 'LogAnalysisGateway' 20
```

The *service* section now looks like the following example.

```
{  
    ServiceType=Master  
    ServiceStart=Auto  
    process 'MasterObjectServer' NONE  
    process 'ArchiveGateway' 20  
    process 'LogAnalysisGateway' 20  
}
```

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

13. 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.
```

14. Start process activity:

```
nco_pa_start -name HOST1_PA
```

15. Verify process status:

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

[netcool@host1 etc]\$ 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 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 existing Netcool/OMNIbus users to add access to Log Analysis. Users 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.

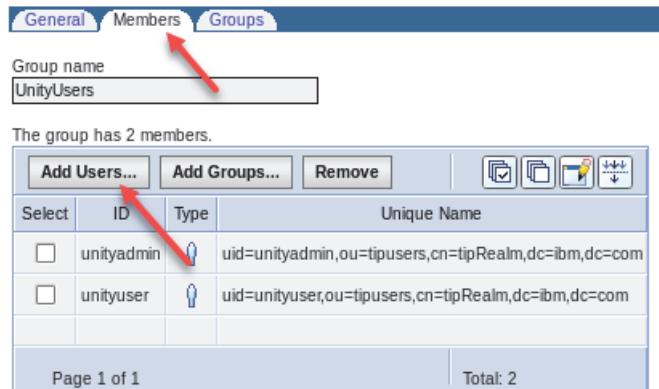
1. Log in to Dashboard Application Services Hub as the **smadmin** user with password **object00**.
2. Open WebSphere administrative console.
3. Expand **Users and Groups**. Select **Manage Groups**.



4. Click the **UnityUsers** group.

Select	Group name	Description	Unique Name
<input type="checkbox"/>	ImpactAdmin		cn=ImpactAdmin,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"/>	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"/>	WDAAdministrator		cn=WDAAdministrator,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM

5. Click the **Members** tab, then click **Add Users**.



6. Click **Search**.

7. Select two users: **ncoadmin** and **ncouser**.

8. Click **Add**.

Add Users to a Group

Group name
UnityUsers

Search for users that will be members of this group.

Search by * Search for * Maximum results
User ID * 100

Search

31 users matched the search criteria.

User ID	Name
mkumaranda	mkumaranda
ncoadmin	ncoadmin
ncouser	ncouser
tonuser1	tonuser1
tcruser2	tcruser2
tengbretson	tengbretson
tflowble	tflowble
tipuser1	tipuser1
tipuser2	tipuser2
unityadmin	unityadmin
unityuser	unityuser
whill	whill
ziverslie	ziverslie

Add Close

9. Click **Close**.

10. Verify that the two users are members of the **UnityUser** group.

The group has 4 members.

Select	ID	Type	Unique Name
<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

Page 1 of 1 Total: 4

11. Log out of WebSphere administrative console.

12. Close the Firefox tab.

13. Log out of Dashboard Application Services Hub as the **smadmin** user.

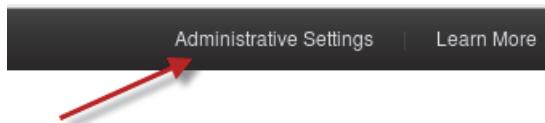
After you add the users to the UnityUsers group, they can now access Log Analysis features. However, Log Analysis limits access to log data by controlling access to each data source. In a previous exercise, you installed the Netcool/OMNIbus Event Insight pack, and created a Log Analysis data source for event records. You must configure Log Analysis to allow the users 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.

IBM Operations Analytics - Log Analysis

Getting Started | Data Types | Data Sources | Roles | **Users**

You can create and modify users to assign role-based access control to individual users or select an existing user and click the edit or delete icons. [Learn More...](#)

	User Name	Display Name
<input type="checkbox"/>	unityadmin	unityadmin

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.

* 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. Repeat this process to add the **ncoadmin** user.

21. 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 incidents. Click the **+** icon to add a new role, or select an existing role and click the **edit** or **delete** icons.

Role Name	Display Name
unityusers	unity users

22. 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	

23. Scroll down, and select **Assign Permission to Role**. Click the icon to add a permission.

Description									
<table border="1"> <tr> <td>Assign Users to Role</td> <td>Object Type</td> <td>Object Name</td> <td>Permission Type</td> </tr> <tr> <td>Assign Permissions to Role</td> <td></td> <td></td> <td></td> </tr> </table>		Assign Users to Role	Object Type	Object Name	Permission Type	Assign Permissions to Role			
Assign Users to Role	Object Type	Object Name	Permission Type						
Assign Permissions to Role									

24. Select the **omnibus** Data Source, and click **OK**.

Select permissions to be associated with this role [Clear All](#) [Select All](#)

Enter name to filter :

<input type="checkbox"/>	Object Type	Permission
<input type="checkbox"/>	Datasource	_alerts
<input checked="" type="checkbox"/>	Datasource	omnibus

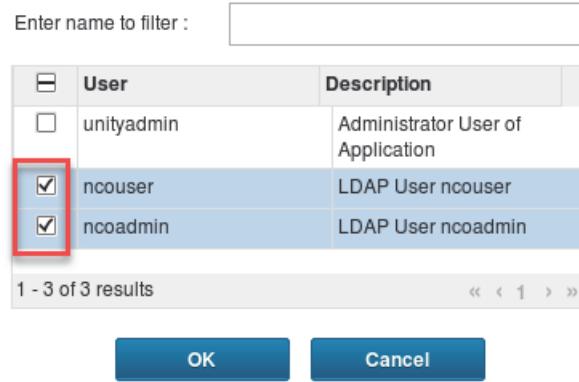
1 - 2 of 2 results « < 1 > »

OK **Cancel**

25. Select **Assign Users to Role**. Click the icon to add a user.

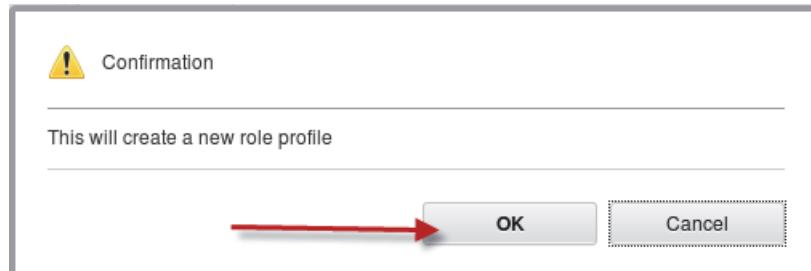
Description					
<table border="1"> <tr> <td>Assign Users to Role</td> <td></td> </tr> <tr> <td>Assign Permissions to Role</td> <td></td> </tr> </table>		Assign Users to Role		Assign Permissions to Role	
Assign Users to Role					
Assign Permissions to Role					

26. Select **ncouser** and **ncoadmin**. Click **OK**.

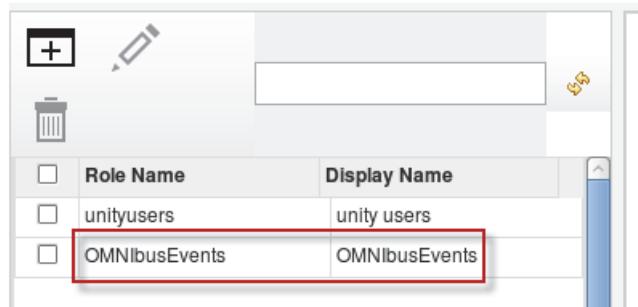


27. Scroll to the bottom of the page and click **OK** to create the role.

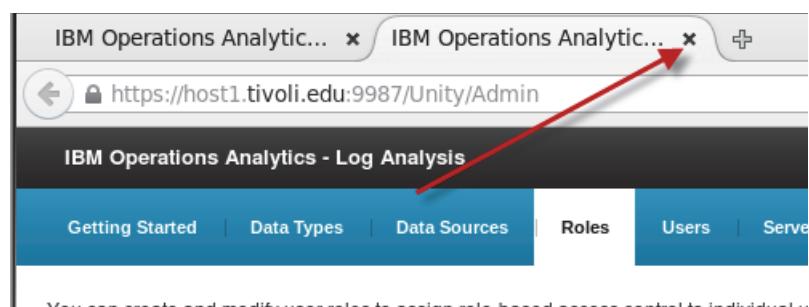
28. Click **OK** to confirm the new role.



The new role is available, and the users have access to the role.



29. Click the **X** to close the Administrative Settings tab.



30. Close the Firefox browser.

Verifying the Event Search feature

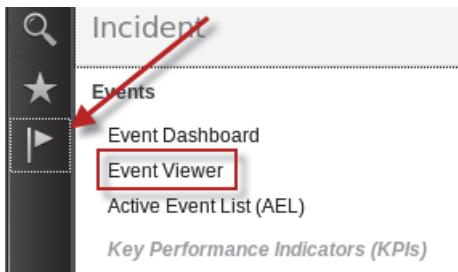
In a previous exercise, you configured the ncouser user for access to Log Analysis. In the following steps, you verify the event search feature.

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. Find an event where the First Occurrence date is today.
4. Right-click the event and select **Event Search > Search for events by node > 1 day before event**.

Node	Alert Group	Summary	First Occurrence	Last Occurrence
host1.csuite.edu	Acknowledge Ctrl+A	It limit: used 1 MB of capac	7/26/19, 4:25 PM	7/31/19, 4:12 PM
host1.csuite.edu	De-acknowledge Ctrl+D	DBC Gateway connected fr	7/31/19, 12:13 PM	7/31/19, 4:12 PM
host1.csuite.edu	Prioritize	lerts.status): 42	7/26/19, 4:29 PM	7/31/19, 4:08 PM
host1.csuite.edu	Suppress/Escalate	DBC Gateway connected fr	7/31/19, 12:13 PM	7/31/19, 4:12 PM
host1.csuite.edu	Take ownership	User Assign	7/26/19, 4:29 PM	15 minutes before event
host1.csuite.edu	User Assign	(alerts.journal): 0	7/26/19, 4:29 PM	1 hour before event
host1.csuite.edu	Group Assign			1 day before event
host1.csuite.edu	Delete	6 connections. Available co	7/26/19, 4:29 PM	
host1.csuite.edu	Ping	alerts.details): 0	7/26/19, 4:29 PM	1 week before event
host1.csuite.edu	Event Search	Show event dashboard by node		1 month before event
Rome	Information...	Shift+I		1 year before event
Rome	Journal...	Shift+J		Custom ...
Berlin	Copy	Ctrl+C		
Berlin	Quick Filter			

The screenshot shows a table of events. A context menu is open over an event for 'host1.csuite.edu'. The 'Event Search' option is highlighted with a red box. A sub-menu for 'Search for events by node' is also highlighted with a red box. The sub-menu items include 'Search for similar events', 'Search for events by node' (which is highlighted), and 'Show keywords and event count'. The 'Search for events by node' item has a submenu with options: '1 day before event' (highlighted with a red box), '1 week before event', '1 month before event', '1 year before event', and 'Custom ...'. The status bar at the bottom right shows '8 PM : 26 row(s) modified.'

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.

IBM Operations Analytics - Log Analysis

Getting Started x New Search x + Add Search

(Node:"host1.csuite.edu")

Log Events Granularity : Hour Time Range : 07/30/19, 12:13:03 - 07/31/19, 12:13:03

100
0

7/30/19, 12:00 07/30/19, 21:00

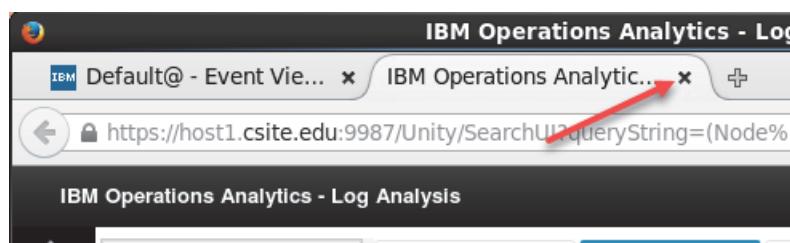
1 to 100 of 209 results >

[07/31/19 12:13:03:000 +0000]
_datasource:omnibus, Tally:1, ServerSerial:268, NodeAlias:host1.csuite.edu

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
5. As time allows, you can test the other options for event search launch from the Event Viewer.
 6. Close the Log Analysis tab.



7. Log out of Dashboard Application Services Hub.
8. Close the Firefox browser.

Exercise 3 Configuring Event Analytics

Configuring the Related Events feature

Netcool/Impact processes the analytics behind the related events feature. 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 file 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.



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)  
(0 rows affected)
```

3. Import the SQL update file.

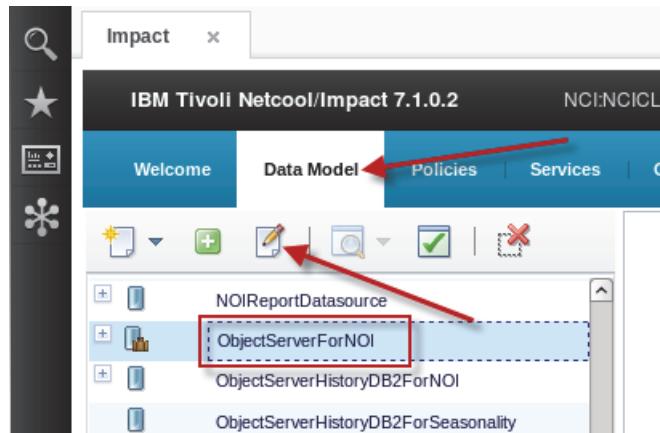
```
nco_sql -server NOI_AGG_P -user root -password object00 <  
relatedevents_objectserver_update_fp5.sql
```

```
(0 rows affected)  
(0 rows affected)  
(0 rows affected)  
(0 rows affected)  
(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.

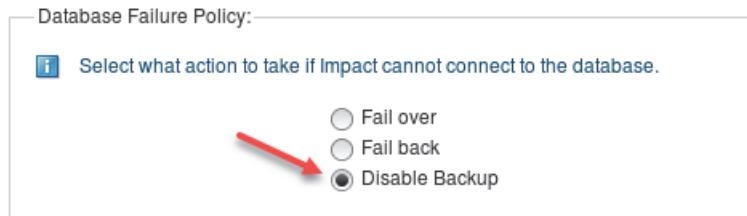
ObjectServer Data Source Editor

General Settings:

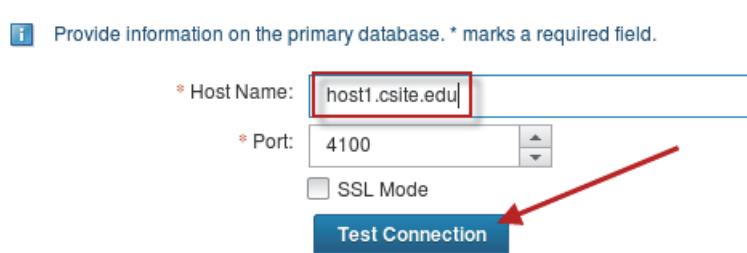
i Provide general information which describes the data source. An * indicates required fields.

* Data Source Name:	ObjectServerForNOI
* Username:	root
Password:	*****
Maximum SQL Connection:	30

6. Scroll down and click **Disable Backup**.



7. Scroll down and enter **host1.csuite.edu** for the host name. Click **Test Connection**.



8. Verify that the connection is successful and click **Close** to close the window.

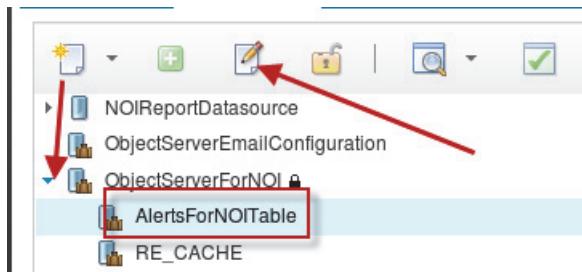


9. Click the icon to save the changes.

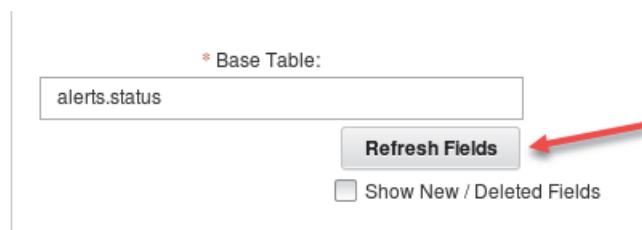


 Note: The data source page remains open after it is saved.

10. Expand **ObjectServerForNOI**. Click **AlertsForNOITable** to select it. Click the *pencil* icon to open the data type.

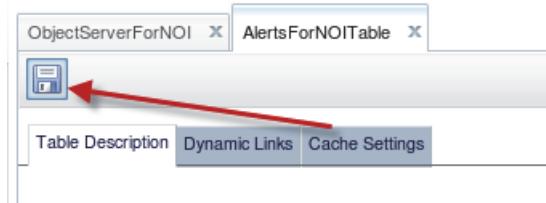


11. Scroll down and click **Refresh Fields**.

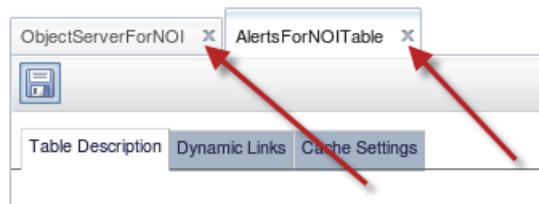


You added columns to the event record table in previous steps. When you click Refresh Fields, it causes Netcool/Impact to discover the table changes.

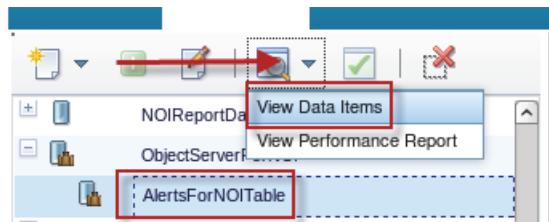
12. Click the icon to save the data type changes.



13. Click the **X** on each tab to close the data source page and the data type page.



14. Expand **ObjectServerForNOI**. Click **AlertsForNOITable** to select it. Click the *magnifying glass* icon and select **View Data Items**.



15. Verify that you are able to see event records.

The screenshot shows a software interface titled "Data Items: AlertsForNOITable". It displays a list of objects with checkboxes and identifiers. The objects listed are "TokyoMachineStats4Stats", "OMNIBus ObjectServer : Total SQL time for all clients NOI_...P:", and "NCI-Impact@host1.tiuli.educonnectedThu Apr 16 2013 07 2015". A red arrow points to the top right corner of the window, indicating where to click to close it.

Important: If you receive an error message, repeat the previous steps to refresh the list of event columns and save the data type.

16. Click the X on the tab to close the page.

The screenshot shows the same software interface as before, but with a red arrow pointing to the close button (an 'X') in the top right corner of the window.

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.

17. Click **ObjectServerHistoryDB2ForNOI** to select it. Click the *pencil* icon to open the data source definition.

The screenshot shows the "Data Model" tab of the software interface. A list of data sources is displayed, with "ObjectServerHistoryDB2ForNOI" highlighted by a red box. A red arrow points to the "pencil" icon in the toolbar above the list, indicating where to click to edit the data source.

18. Enter **db2inst1** for the user and **object00** for the password.

DB2 Data Source Editor

General Settings:

i Provide general information which describes the data source. An * indicates required fields.

* Data Source Name: ObjectServerHistoryDB2ForNOI

* Username: db2inst1

Password: *****

Maximum SQL Connection: 5

19. Scroll down and enter **host1.csite.edu** for the host name. Click **Test Connection**.

Primary Source:

i Provide information on the primary database. * marks a required field.

* Host Name:

* Port: 50000

* Database: REPORTER

Test Connection →

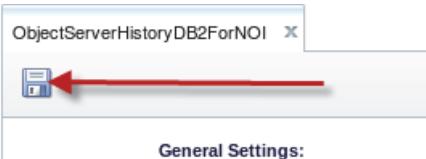
20. Verify that the connection is successful and click **Close** to close the window.

Testing

Connection OK i

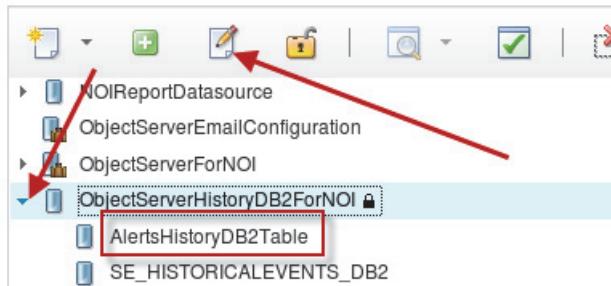
Close →

21. Click the icon to save the changes.



Note: The data source page remains open after it is saved.

22. Expand **ObjectServerHistoryDB2ForNOI**. Click **AlertsHistoryDB2Table** to select it. Click the *pencil* icon to open the data type.

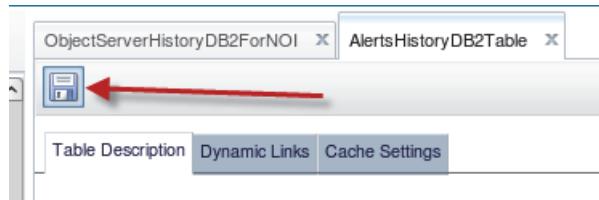


23. Scroll down and click **Refresh Fields**.

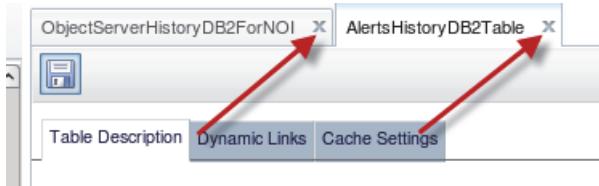


Note: The refresh is required only if you add columns to the event record table in the archive database. You do not add columns in this class, but it is typical in a production environment.

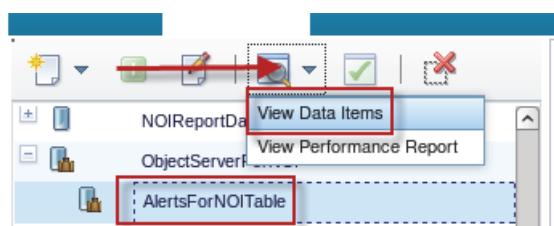
24. Click the icon to save the data type changes.



25. Click the X on each tab to close the data source page and the data type page.



26. Expand **ObjectServerHistoryDB2ForNOI**. Click **AlertsHistoryDB2Table** to select it. Click the magnifying glass icon and select **View Data Items**.



27. Verify that you are able to see records from the DB2 table.

The screenshot shows a table titled 'Data Type Name: AlertsHistoryDB2Table' with 270 objects. The columns are 'Select', 'View Links', 'Edit', 'CLASS', and 'IDENTI'. Two rows are visible:

Select	View Links	Edit	CLASS	IDENTI
<input type="checkbox"/>			3300	TokyoMachineStats4S
<input type="checkbox"/>			99999	OMNIbus ObjectServe all clients NOI_... F



Important: If you receive an error message, repeat the previous steps to refresh the list of event columns and save the data type.

28. Click the **X** on the tab to close the page.

A red arrow points to the close button ('X') in the top right corner of the browser tab.

The related events feature uses several Netcool/Impact services. Verify that the services are started.

29. Click the **Services** tab.

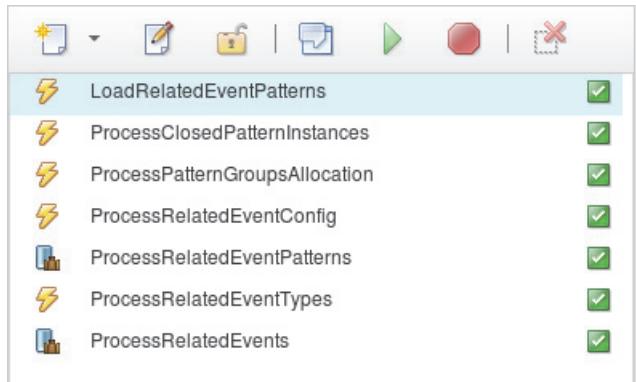
30. Click the arrow and select the **RelatedEvents** project.

A red arrow points to the 'RelatedEvents' project in the 'Select Project' list. Another red arrow points to the 'Manage Projects' dropdown menu, specifically the 'Delete Current Project' option.

31. Click **OK** to confirm the change.



32. Verify that all services are running. The green check marks indicate that the services are running.

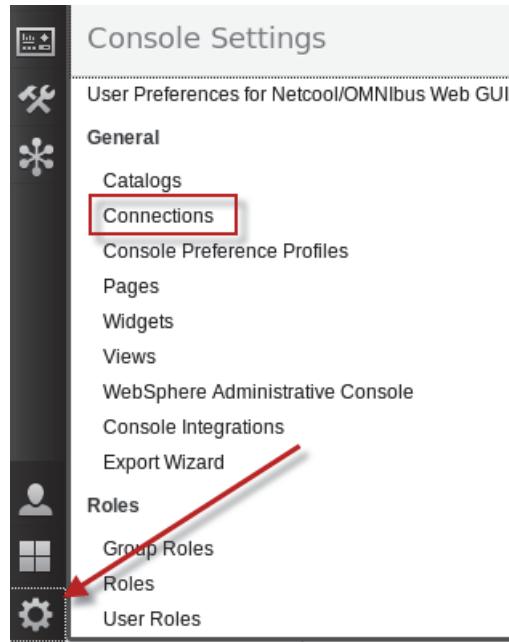


33. Click the X to close the Impact console page.

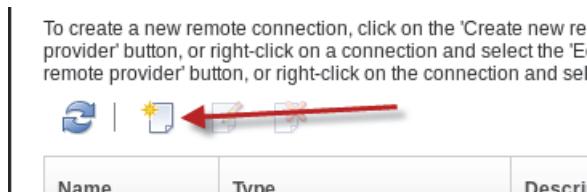


Dashboard Application Services Hub modifications

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**.
 - d. Enter **host1.csite.edu** for the host.
 - e. Enter **17310** for the port.
 - f. Enter **impactadmin** for the user and **object00** for the password.

g. Click Search.

Server information

* Protocol:	* Host name:	* Port:
HTTP	host1.csite.edu	17310
* Path:	/ibm/tivoli/rest	
<input type="checkbox"/> Connection goes through a firewall		
Firewall address	Firewall port	
Use the following credentials to query the remote data providers		
* Name:	* Password:	* Confirm password:
impactadmin	*****	*****

Search

If the access information is correct, the Netcool/Impact cluster is shown in the bottom of the window.

h. Select the cluster, scroll to the bottom of the page, and click **OK** to save the connection.

No filter applied

Name	Description
Impact_NCICLUSTER	

Total: 1 Selected: 1

Connection information

* Name:
Impact_NCICLUSTER

2. Verify that the connection is shown for Netcool/Impact.

Name	Type	Description
Impact_NCICLUSTER	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.

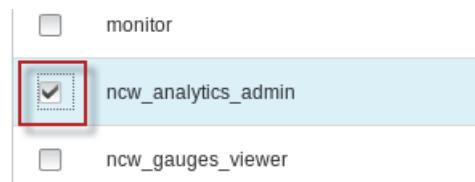
4. Click the icon and select **Group Roles**.



5. Click **Search** to display the available groups. Click **Netcool_Admin**.

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

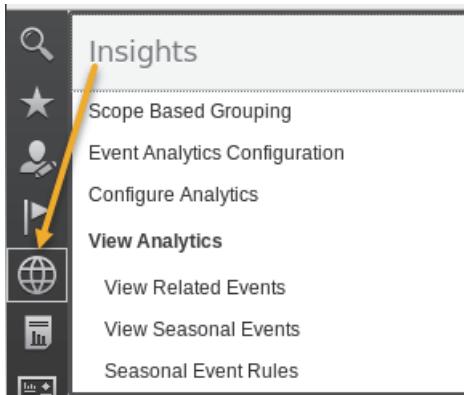
6. Scroll down and select **ncw_analytics_admin**. Click **Save**.



7. Log out of Dashboard Application Services Hub.

8. Log in to Dashboard Application Services Hub as **ncoadmin** with password **object00**.

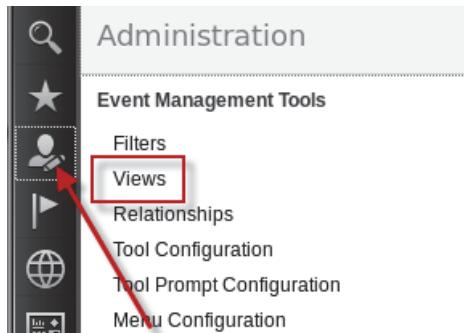
- Click the icon and observe the features.



Note: The `ncw_analytics_admin` role provides access to the related events user interface and seasonality.

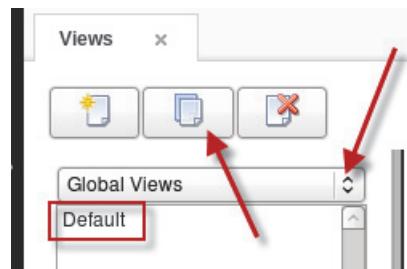
The next step is to create an event view and add the relationship definition.

- Click the icon and select **Views**.

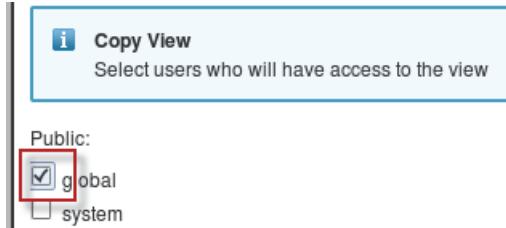


The View Builder opens.

- Click the arrow and select **Global Views**. Click **Default** to select it. Click the icon to copy the view.



12. Select **global** and click **Ok**.



13. Enter **RelatedEvents** for the name and click the **Relationships** tab.

Edit View: New View

* Name: **RelatedEvents**

Data Source: Click to show

Display Columns Sort Columns Group Columns Relationships

A red arrow points from the 'Relationships' tab to the 'Relationships' section below.

14. Click the arrow and select **IBM Related Events**.

Group Columns Relationships

How events are related to each other if a relationship exists in the event for this view. This setting does not affect other event lists such as the Act

Relationship:

Don't display event relationships for this view IBM Tivoli Network Manager Root Cause/Symptom

IBM Related Events

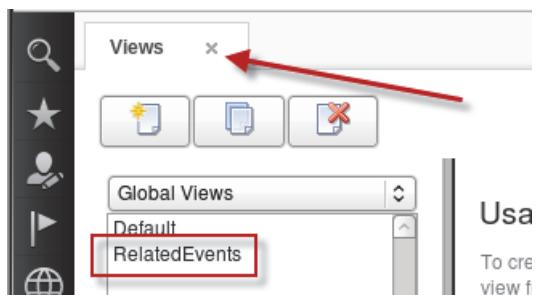
ot show any event relationships.

A red arrow points from the 'Relationships' tab to the dropdown menu, and another red arrow points to the 'IBM Related Events' option in the dropdown.

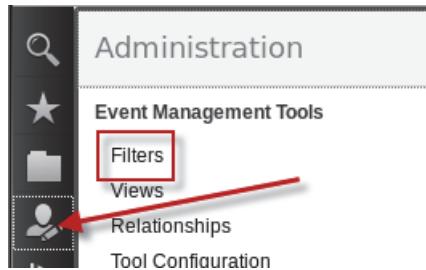
15. Click **Save and Close**.



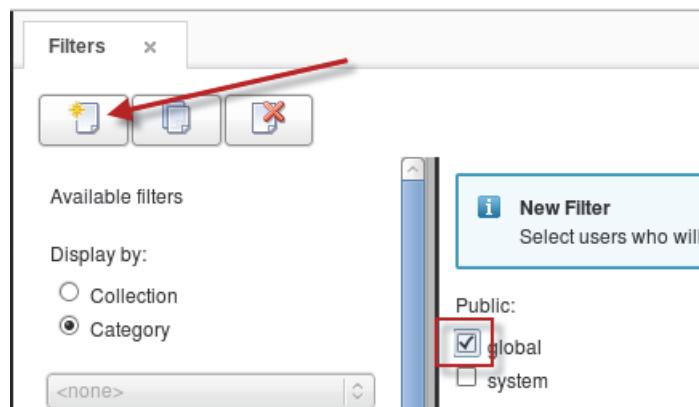
16. Click the **X** to close the Views page.



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. Scroll down. 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.

Filter Conditions

Basic	Advanced	Dependent	Metric
<input type="radio"/> All <input checked="" type="radio"/> Any			
Field	Comparator	Value	
AlertGroup	like	Parent	
<input type="button" value="Clear All"/>			

21. Click the arrow under **Field** and select **ParentIdentifier**. Click the arrow under **Comparator** and select **!=**. Leave Value empty.

Filter Conditions

Field	Comparator	Value
AlertGroup	like	Parent
ParentIdentifier	!=	

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 empty.

22. Click **Save and Close**.

23. Click the **X** to close the Filter page.



The configuration for related events is complete.

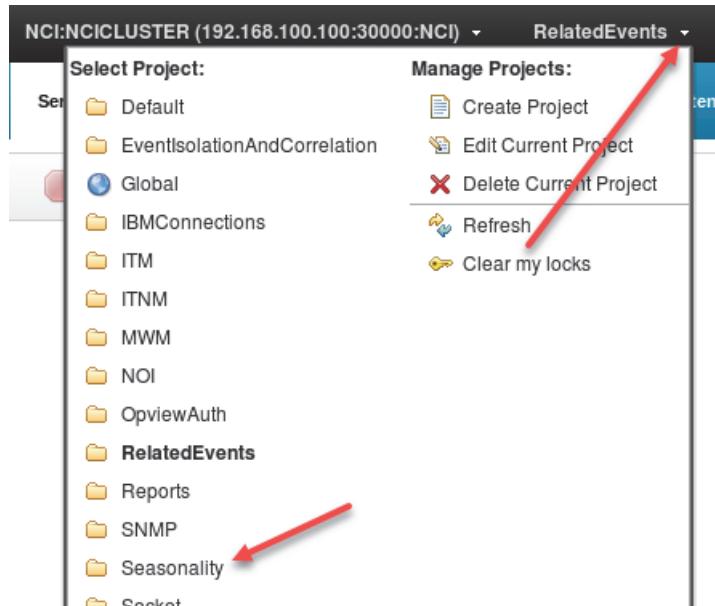
Configuring seasonality

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.

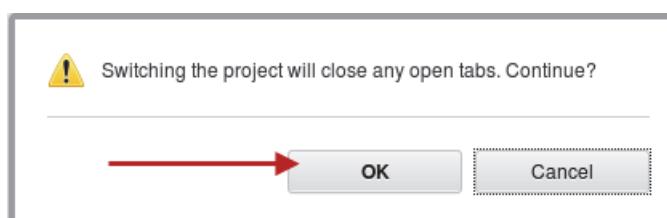


Note: You are currently logged in to Dashboard Application Services Hub as the **ncoadmin** user. You configured the ncoadmin user for access to Netcool/Impact in a previous exercise.

1. Click the **snowflake** icon and select **Impact** to open the Netcool/Impact console.
2. Change the project to **Seasonality**.

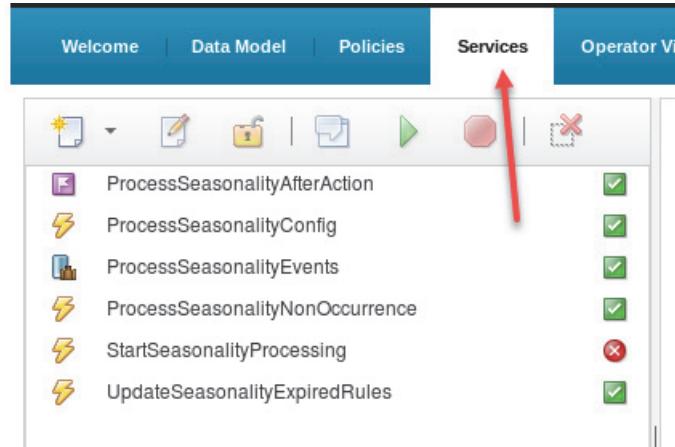


3. Click **OK** to confirm the change.



4. Click the **Services** tab.

5. Verify that all services except one are started. The green check marks indicate that the service is running.



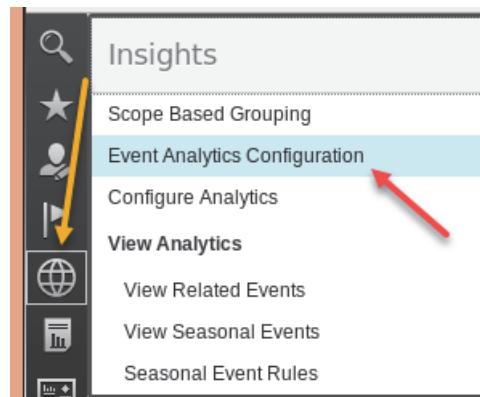
Note: The **StartSeasonalityProcessing** service is stopped, which is normal.

6. Click the X to close the Netcool/Impact console page.

Running the analytics wizard

To complete the configuration of event analytics, you must run the event analytics wizard.

1. Click the icon and click **Event Analytics Configuration**.



2. Click **Next** to start the wizard.
3. Enter **object00** as the password.

4. Click **Connect**.



5. Verify that the connection is successful.



6. Scroll down and click **Validate table**.

7. Verify that the table is valid. Click **Next**.



8. Click **Connect**. Verify that the connection to the ObjectServer is successful. Click **Next**.



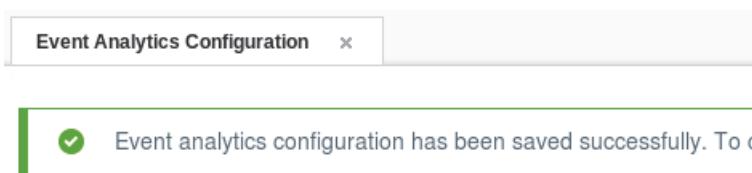
9. Click **Next** on the Configure report fields page.

10. Click **Next** on the Configure event patterns page.

11. Click **Next** on the Configure event suppression page.

12. Click **Save Configuration** on the summary page.

13. At the top of the page, verify that the configuration was saved.



14. Log out of Dashboard Application Services Hub.

15. Close the Firefox browser.

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 the ncouser for access to Log Analysis
- Verified the Event Search feature
- Configured the Related Events feature
- Configured Event Seasonality



4 IBM Tivoli Network Manager exercises

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

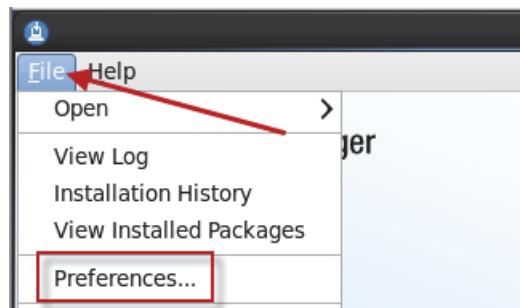
Exercise 1 Installing the SNMP probe

Tivoli Network Manager requires the SNMP probe and the Netcool Knowledge Library. The following steps demonstrate how to install those components.

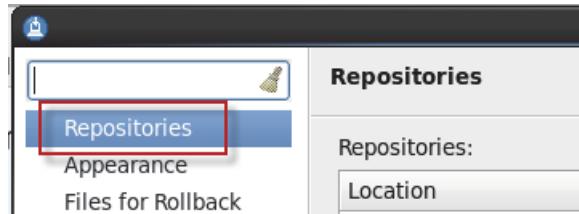
1. Open a terminal window if necessary.
2. Start IBM Installation Manager.

```
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/im-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/OMNIBusWebGUIRepository/repository.c	?

6. Click **Add Repository**.



7. Click **Browse** and find the following file:

/software/nckl/NcKL_4.8.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 find the following file:

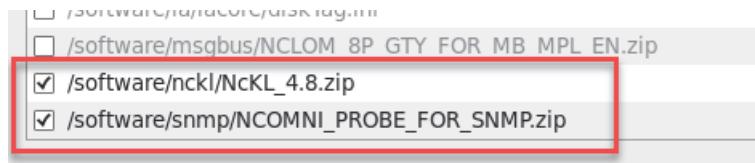
/software/snmp/NCOMNI_PROBE_FOR_SNMP.zip

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

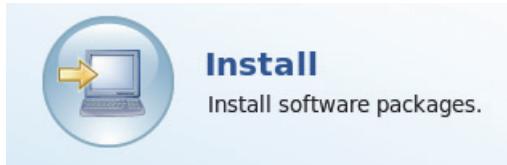
Repository:
 

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
Netcool/OMNIBus Knowledge Library	<input checked="" type="checkbox"/>	Will be installed
Version 4.8.7	<input checked="" type="checkbox"/>	
Netcool/OMNIBus Probe nco-p-mttrapd	<input checked="" type="checkbox"/>	Will be installed
Version 1.20.0.0	<input checked="" type="checkbox"/>	

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

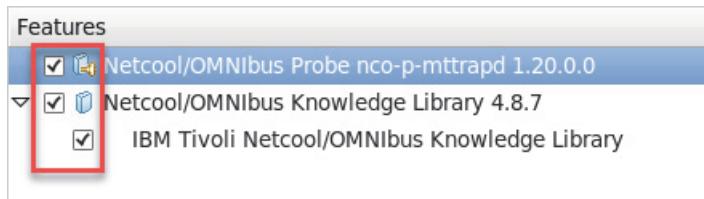
16. Change the installation directory for the Netcool Knowledge Library.

- Click the entry for **IBM Netcool Knowledge Library** to select it.
- Change the installation directory to **/opt/IBM/tivoli/NcKL**.
- 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	
IBM Netcool Knowledge Library	/opt/IBM/tivoli/NcKL
Netcool/OMNIBus Knowledge Library 4.8.7	

Package Group Name: IBM Netcool Knowledge Library
 Installation Directory:
 Architecture Selection: 32-bit 64-bit

17. Verify that all features are selected, and click **Next**.



18. Review the summary, and click **Install**.

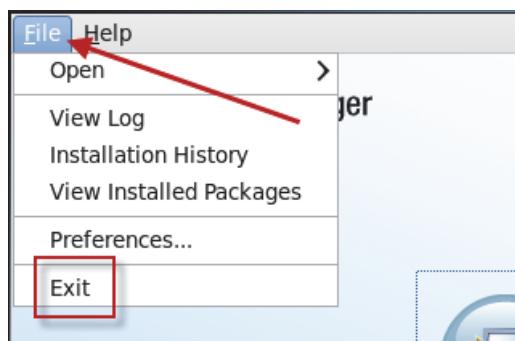
19. Verify that the installation is successful, and click **Finish**.

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

The following packages were installed:

▽ IBM Netcool Core Components
 Netcool/OMNIBus Probe nco-p-mttrapd 1.20.0.0
▽ IBM Netcool Knowledge Library
 Netcool/OMNIBus Knowledge Library 4.8.7

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)  

(0 rows affected)

```



Note: The error messages are normal and can be ignored.

23. Modify the SNMP probe property settings.

- a. Change to the location of the property file.

```
cd /opt/IBM/tivoli/netcool/omnibus/probes/linux2x86
```

- b. Open the property file in a text editor.

```
gedit mttrapd.props
```

- c. Add the following lines to the end of the file:

```
Server : 'NOI_AGG_P'  
RulesFile : '/opt/IBM/tivoli/NcKL/rules/snmptrap.rules'
```

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

24. Define the 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.

- a. Change to the root user.

```
su -  
Password: object00
```

- b. Change to the root user home directory.

```
cd /root
```

- c. Append the **netcool** user environment settings to the end of the root user file.

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

- d. Open the environment file in a text editor.

```
gedit .bashrc
```

```
*.bashrc X  
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
```

netcool user
variables

- e. Verify that the **netcool** user settings are listed in the file.

- f. Add the following lines to the end of the file:

```
# Required for Netcool Knowledge Library  
NC_RULES_HOME=/opt/IBM/tivoli/NcKL/rules  
export NC_RULES_HOME
```

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

- h. 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. Notice the process ID.

```
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 in a text editor.

```
gedit nco_pa.conf
```

- d. Add the following lines to the *nco_process* section.

```
nco_process 'SnmpProbe'  
{  
    Command '$OMNIHOME/probes/nco_p_mttrapd' run as 0  
    Host='host1.csuite.edu'  
    Managed=True  
    RestartMsg='${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 line to the *service* section, below the *LogAnalysisGateway* line.

```
process 'SnmpProbe' 20
```

- f. The *service* section now looks like the following example.

```
nco_service 'Core'  
{  
    ServiceType=Master  
    ServiceStart=Auto  
    process 'MasterObjectServer' NONE  
    process 'ArchiveGateway' 20  
    process 'LogAnalysisGateway' 20  
    process 'SnmpProbe' 20  
}
```

- g. 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 the processes. The probe and the gateways start after a 20-second delay.

```
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.csuite.edunetcool  RUNNING   18800  
                  ArchiveGateway     host1.csuite.edunetcool  RUNNING   18970  
                  LogAnalysisGateway host1.csuite.edunetcool  RUNNTNG  18971  
                  SnmpProbe        host1.csuite.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.

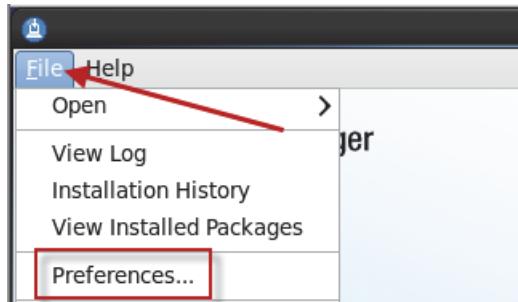
1. Expand the Network Manager installation file.

```
cd /software/itnm  
unzip ITNMIPEV4.2.0.7LNXML.zip
```

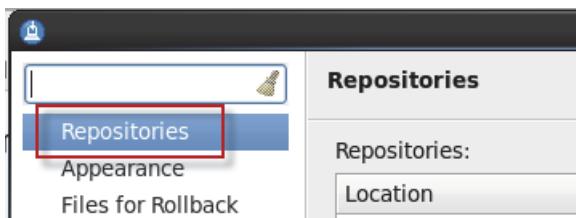
2. Start IBM Installation Manager.

```
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.

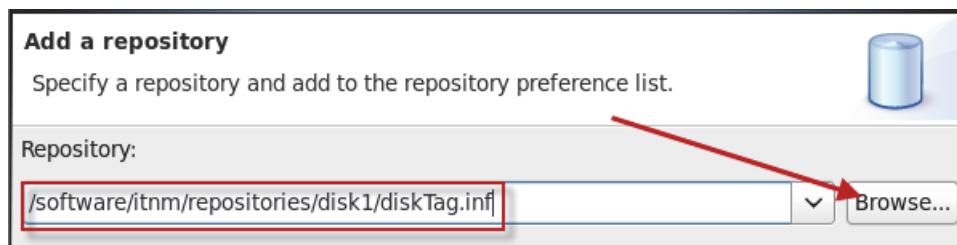
Repositories:	
Location	Connection
<input type="checkbox"/> /software/omnibus/OMNIbusRepository/repository.config	?
<input type="checkbox"/> /software/jdbc/im-nco-g-jdbc-rpt-scripts-1_0.zip	?
<input type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	?
<input type="checkbox"/> /tmp/jazz_install/repositories/disk1/diskTag.inf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

6. Click **Add Repository**.



7. Click **Browse** and find 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**.

The screenshot shows the 'Installation Packages' window. Under 'Network Manager Core Components', the 'Network Manager topology database creation scripts' package is selected (indicated by a checked checkbox) and highlighted in blue. Its version, 'Version 4.2.0.7', is also checked. Other packages like 'Network Manager GUI Components' and 'Network Health Dashboard' are listed but not selected.



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**.

The screenshot shows the 'Install Packages' screen. The 'Location' tab is selected. The 'Use the existing package group' radio button is selected and highlighted with a red box. Below it, 'Create a new package group' is an unselected option. In the package group list, 'IBM Netcool Core Components' is selected and highlighted in blue, with its installation directory set to '/opt/IBM/tivoli/netcool'. Another package group, 'Core services in Jazz for Service Management', is listed below it with its own directory.

14. Clear Oracle Database Server creation scripts, and click **Next**.

The screenshot shows the 'Features' screen. Under 'Network Manager topology database creation scripts 4.2.0.7', the 'Oracle Database Server creation scripts' checkbox is cleared (unchecked) and highlighted with a red box.



Note: You use DB2 for the class exercises.

15. Review the summary, and click **Install**.

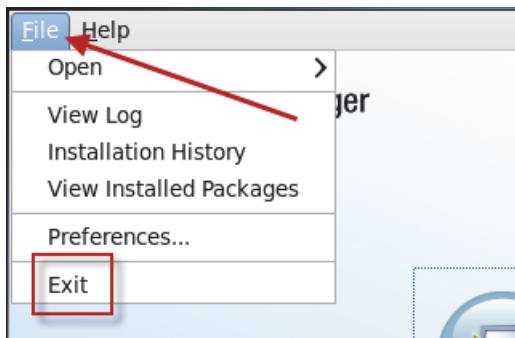
16. Verify that the package installation is successful, and click **Finish**.

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

The following package was installed:

- IBM Netcool Core Components
 - Network Manager topology database creation scripts 4.2.0.7

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.

```
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 in a text editor.

```
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 11.1.0  
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 11.1.0  
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**.

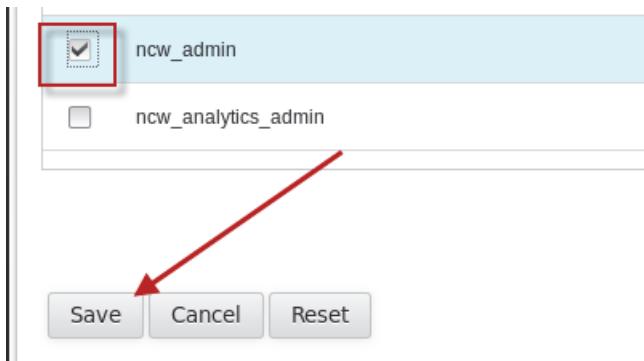
The image shows a search interface for users. It includes fields for 'First name:' and 'Last name:', 'User ID:' (which contains 'smadmin' and is highlighted with a red box), 'E-mail:', and 'Number of results to display:' (set to 20). A red arrow points from the 'User ID' field to the 'Search' button at the bottom.

5. Click **smadmin**.

A screenshot of a user search interface. At the top, there are icons for search and refresh, followed by a 'Logout' link. Below is a table header with columns: Select, User ID, Active, First Name, and Last Name. A red arrow points from the text 'smadmin' in the First Name column to the corresponding row in the table.

Select	User ID	Active	First Name	Last Name
	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 in IBM Installation Manager.

1. Start IBM Installation Manager.

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

2. Click **Install**.



3. Select **Network Manager Core Components** and click **Next**.

A screenshot of the 'Installation Packages' list in IBM Installation Manager. The table has columns: Installation Packages, Status, and Vendor. A red box highlights the first row, which contains the checked checkbox for 'Network Manager Core Components'. Another red box highlights the sub-row for 'Version 4.2.0.7', which is also checked and marked as 'Will be installed'.

Installation Packages	Status	Vendor
<input checked="" type="checkbox"/> Network Manager Core Components		
<input checked="" type="checkbox"/> Version 4.2.0.7	Will be installed	IBM
<input type="checkbox"/> Network Manager topology database creation scripts	Installed	
<input type="checkbox"/> Version 4.2.0.7	Installed	IBM
<input type="checkbox"/> Network Manager GUI Components		



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**.

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**.

Features
<input checked="" type="checkbox"/> Network Manager Core Components 4.2.0.7
<input checked="" type="checkbox"/> Core components
<input checked="" type="checkbox"/> Additional cryptographic routines

7. Enter the following values, and click **Next**.
 - a. Enter **NOI_AGG_P** for the ObjectServer name.
 - b. Enter **host1.csite.edu** for the host name.
 - c. Enter port number **4100**.
 - d. Enter **root** as the super user ID.

- e. Enter **object00** for the password.

ObjectServer Configuration

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

Name:	NOI_AGG_P
Host:	host1.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**.

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**.

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 server host.
- b. Enter **ncim** for the user name.

- c. Enter **object00** for the password.

Topology Database

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

Database server type

DB2 (default)
 Oracle

Database name: NCIM

Server host: host1.csuite.edu

Server port: 50000

User ID: ncim

Password: [REDACTED]

Create tables to hold topology data in selected database.

Skip database connection details verification.

The installation utility validates access to DB2.

11. Accept the default location for Python, and click **Next**.

12. Review the summary, and click **Install**.



Important: The installation runs for approximately 15 minutes.

13. Verify that the installation is successful, and click **Finish**.



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

To complete the Network Manager installation, you must run the script /opt/IBM/tivoli/netcool/precision/scripts/setup_run_as_setuid_root.sh as root. See the [Post installation tasks](#) in the installation documentation.

The following package was installed:

▽ IBM Netcool Core Components
 Network Manager Core Components 4.2.0.7

14. Leave IBM Installation Manager open.

Installing Network Manager GUI components

1. Click **Install**.



2. Select **Network Manager GUI Components** and click **Next**.

Installation Packages	Status
Network Manager Core Components	Installed
Version 4.2.0.7	Installed
Network Manager topology database creation scripts	Installed
Version 4.2.0.7	Installed
Network Manager GUI Components	Will be installed
Version 4.2.0.7	Will be installed
Network Health Dashboard	
Version 4.2.0.7	



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**.

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.
 - Enter port number **4100**.
 - Enter **root** as the super user ID.

- Enter **object00** as the password.

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.csite.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.

- Enter **object00** for the default users password, and click **Next**.

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:	*****

- Enter the following values, and click **Next**.

- Enter **host1.csite.edu** as the server host.
- Enter **ncim** for the user name.

- c. Enter **object00** for the password.

Topology Database

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

Database server type

- DB2 (default)
- Oracle

Database name: **NCIM**

Server host: **host1.csuite.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 for 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 4.2.0.7

12. Leave IBM Installation Manager open.

Installing Network Manager Reports

1. Click **Install**.



2. Select **Network Manager Reports** and click **Next**.

Installation Packages	Status
Network Manager Core Components	Installed
Version 4.2.0.7	Installed
Network Manager topology database creation scripts	Installed
Version 4.2.0.7	Installed
Network Manager GUI Components	Installed
Version 4.2.0.7	Installed
Network Health Dashboard	Installed
Version 4.2.0.7	Installed
Network Manager Reports	Will be installed
Version 4.2.0.7	Will be installed



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**.

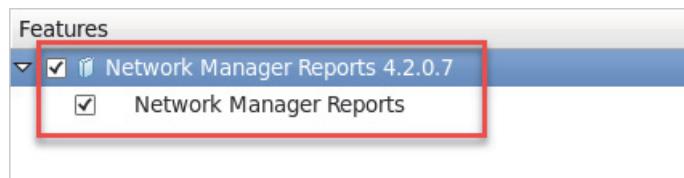
- Use the existing package group
- Create a new package group

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**.

Jazz for Service Management properties

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

Installation directory details

/opt/IBM/JazzSM

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

JazzSM user credentials

User name: smadmin

Password:

The installer validates access to Jazz for Service Management.

7. Enter **object00** for the password, and click **Next**.

Administrator Credentials

IBM Installation Manager needs the credentials of an OMNI (itnmadmin) to manage filters and views. The user must have Netcool WebGUI waapi command. Ensure that the user authenticates before continuing.

User ID: itnmadmin

Password:

8. Enter the following values, and click **Next**.

- a. Enter **host1.csite.edu** as the server host.
- b. Enter **ncim** for the user name.

- Enter **object00** for the password.

Topology Database

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

Database server type

DB2 (default)
 Oracle

Database name: NCIM

Server host: host1.csuite.edu

Server port: 50000

User ID: ncim

Password: *****

Skip database connection details verification.

The installation utility validates the access to DB2.

- Review the summary, and click **Install**.



Important: The installation runs for approximately 30 minutes.

- 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 4.2.0.7

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

Installing the Network Health Dashboard

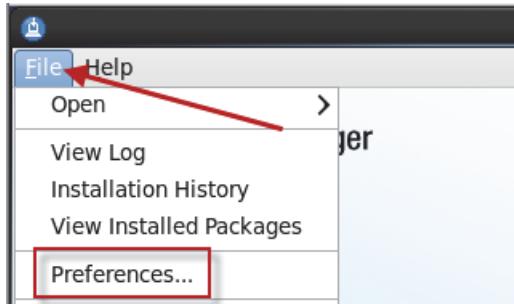
- Expand the dashboard installation file.

```
cd /software/itnm
mkdir dashboard
cd dashboard
unzip ../NETWORK_HEALTH_DASHBOARD_V4.2_LIN.zip
```

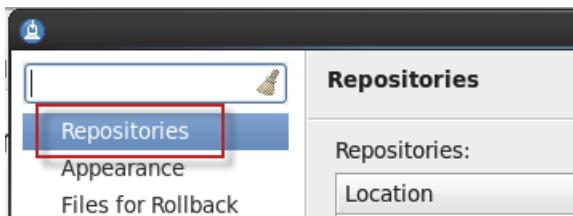
2. Start IBM Installation Manager.

```
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/im-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/OMNIBusWebGUIRepository/repository.c	

6. Click **Add Repository**.



7. Click **Browse** and find the following file:

```
/software/itnm/dashboard/repositories/disk1/diskTag.inf
```

A screenshot of the 'Add a repository' dialog box. It has a title 'Add a repository' and a subtitle 'Specify a repository and add to the repository preference list.' Below is a 'Repository:' field containing the path '/software/itnm/dashboard/repositories/disk1/diskTag.inf', which is highlighted with a red box.

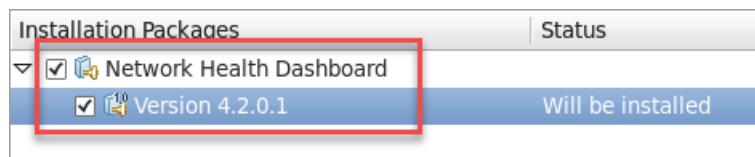
8. Click **OK** to add the repository.
9. Verify that the repository is selected, and click **OK**.



10. Click **Install**.



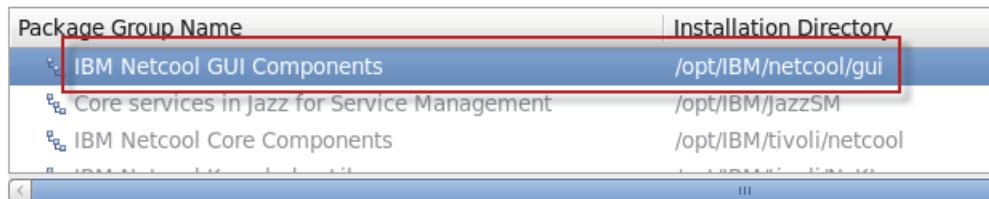
11. Select **Network Health Dashboard** and click **Next**.



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

13. Leave the default option to use the existing package group, and click **Next**.

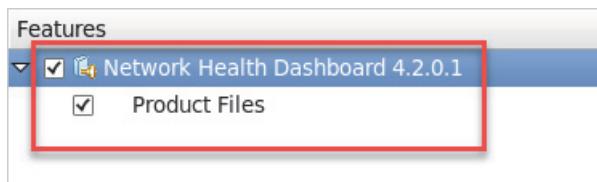
- Use the existing package group
 Create a new package group



Package Group Name: 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**.

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**.

Administrator Credentials

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

User ID: itnadmin

Password: *********

17. Review the summary, and click **Install**.



Important: The installation runs for approximately 20 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 4.2.0.1

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

Configuring the Network Health Dashboard

Users can launch to the Log Analysis UI from a Network View. These steps show you how to configure the tools and menus for the Log Analysis integration.

Modify the topoviz property settings.

1. Change to the target directory:

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

2. Open the property file in a text editor.

```
gedit topoviz.properties
```

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

```
topoviz.unity.customappsui=https://host1.csite.edu:9987/Unity/CustomAppsUI
```

4. Save the file and exit the gedit utility.



Exercise 4 Performing post-installation configuration

You must perform several post-installation 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 with the gedit utility.

```
gedit ModelNcimDb.NOI_AGG_P.cfg
```

4. Find 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', 'RttMonRttType', 'RttMonCodecType',
'rttMonCtrlOperStateToStdOperStatus', 'RowStatusToStdAdminStatus',
'NqaType', 'nqaAdminParaCodecType', 'nqaScheduleOperStatusToStdOperStatus')",
    500,
    "NOI_AGG_P"
);
create table dbModel.entityDetails
```

WebGUI data
source name

5. 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', 'RttMonRttType', 'RttMonCodecType',
'rttMonCtrlOperStateToStdOperStatus', 'RowStatusToStdAdminStatus',
'NqaType', 'nqaAdminParaCodecType', 'nqaScheduleOperStatusToStdOperStatus')",
    500,
    "OMNIBUS"
);
create table dbModel.entityDetails
```

6. Save the file and exit the gedit utility.

Configuring the core components to run as a non-root user

1. Switch to the root user.

```
su -
```

```
Password: object00
```

2. 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

Creating control script

/opt/IBM/tivoli/netcool/precision/custom/control/init.d/storm

4. 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 in a text editor.

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/itnm_status
```



Important: The command must return the correct path before you can proceed.

Adding MIB files

With this version of IBM Tivoli Network Manager, the Management Information Base (MIB) files are not installed. You must manually copy the MIB files into your IBM Tivoli Network Manager environment.

1. Create the required directory for the MIB files.

```
mkdir /opt/IBM/tivoli/netcool/precision/mibs
```

2. Change to the target directory.

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

3. Decompress the MIB archive file.

```
tar -xvf /workshop/itnm/MIBS/ITNM-MIBS.tar
```

4. Run the following command to compile the files into the NCMIB database.

```
ncp_mib
```

...

There are new modules on disk to add to database

Relational database requires updating.

This may take a few minutes. Processing...

Committed

```
ncp_mib: Terminating normally
```

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.

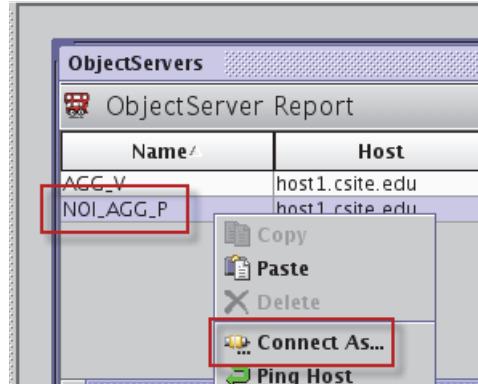
1. Open the Netcool/OMNIbus Administrator utility.

```
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**.

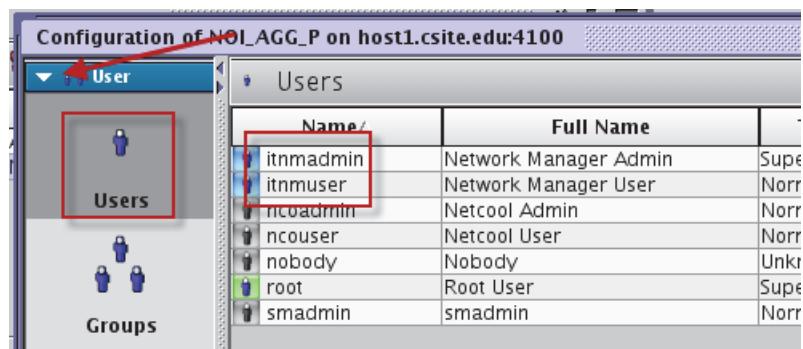


Hint: You might need to drag the Process Agents window away before you can see the ObjectServers window.

3. Enter **root** for the user and **object00** for the password. Click **OK**.



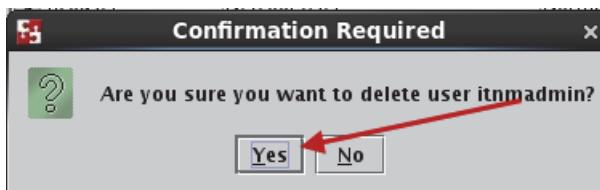
4. Expand **User**, and select **Users**.



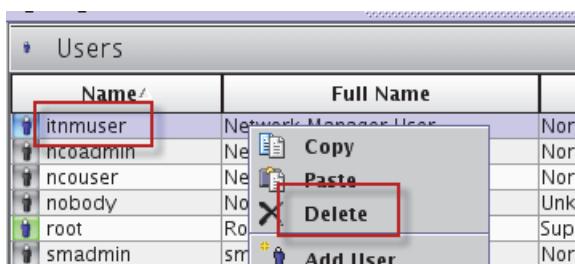
- Right-click **itnmadmin** and select **Delete**.



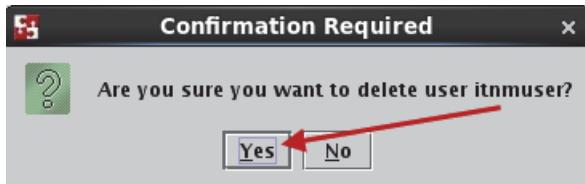
- Click **Yes** to confirm.



- Right-click **itnmuser** and select **Delete**.



- Click **Yes** to confirm.



- Click **File**, and select **Exit** to close the administrator utility.

- Click **Yes** to confirm.

Verifying the installation

In the following steps, you start the Network Manager processes and verify that the users have the necessary access authority.

- 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

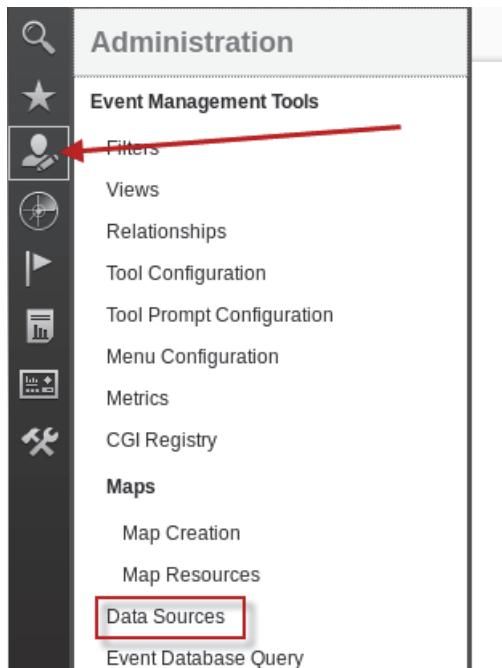
[netcool@host1 ~]\$ itnm_status			
Network Manager:			
Domain: NOI_AGG_P			
ncp_ctrl	RUNNING	PID=9138	NOI_AGG_P
ncp_store	RUNNING	PID=9248	NOI_AGG_P
ncp_class	RUNNING	PID=9249	NOI_AGG_P
ncp_model	RUNNING	PID=9452	NOI_AGG_P
ncp_disco	RUNNING	PID=9592	NOI_AGG_P
ncp_d_helpserv	RUNNING	PID=9250	NOI_AGG_P
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: 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.

The screenshot shows a table listing data sources. A red arrow points to the 'New' icon (a plus sign inside a box) in the toolbar above the table. The table has two columns: 'Name' and 'Enabled'. One entry, 'OMNIBUS', is listed with 'true' in the 'Enabled' column.

Name	Enabled
OMNIBUS	true



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.

Create New Data Source

General Failover Display Servers Self Monitoring Caching Connection Pools

* Name: NOI_AGG_P

Enabled

In Default Group

Primary ObjectServer

* Host: host1.csuite.edu

* Port: 4100

Use SSL ?

Test server connection

Authentication

i These authentication credentials apply to all servers defined in this data source (primary, backup and display servers).

* User ID: root

Password: *********

- f. Click **Test server connection**.

host1.csuite.edu

4100

Use SSL ?

Test server connection

- g. Verify that the ObjectServer is available, and click **Close**.



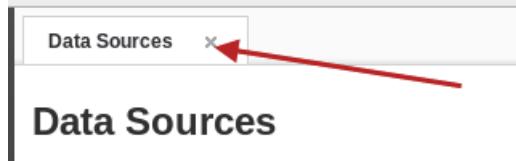
- h. Scroll to the bottom of the page and click **Save Datasource**.

Save Datasource **Reset Tab to Defaults** **Cancel**

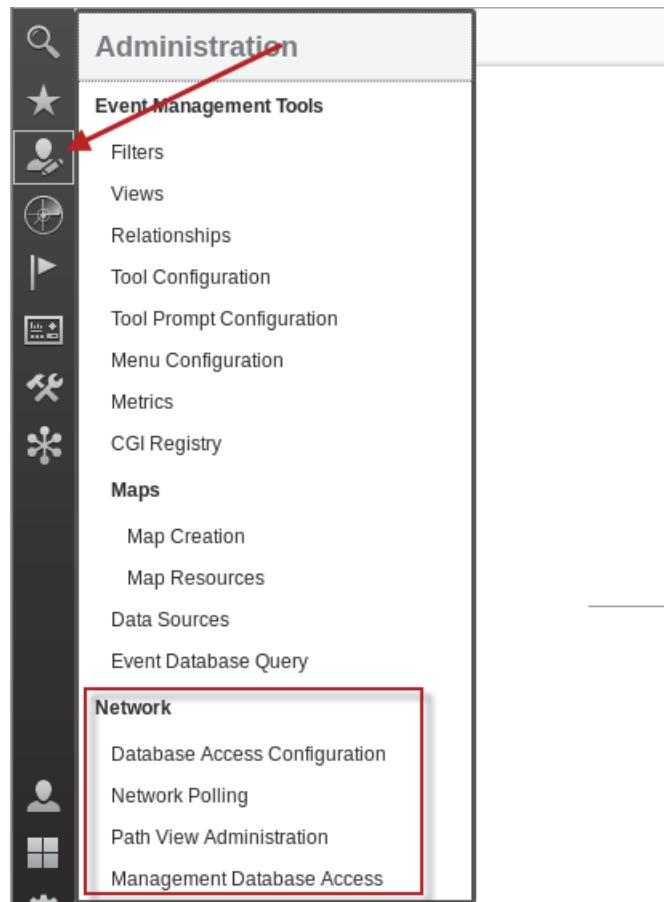
- i. Verify that the new data source is in the list.

Name	Enabled
OMNIBUS	true
NOI_AGG_P	true

- j. Click the X to close the tab.

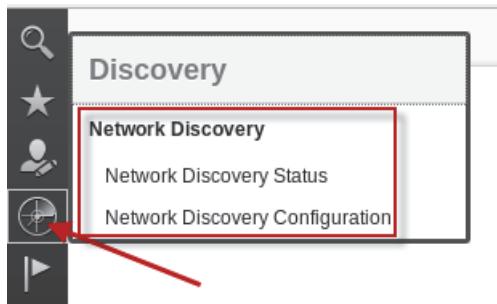


7. Click the icon and verify the items.



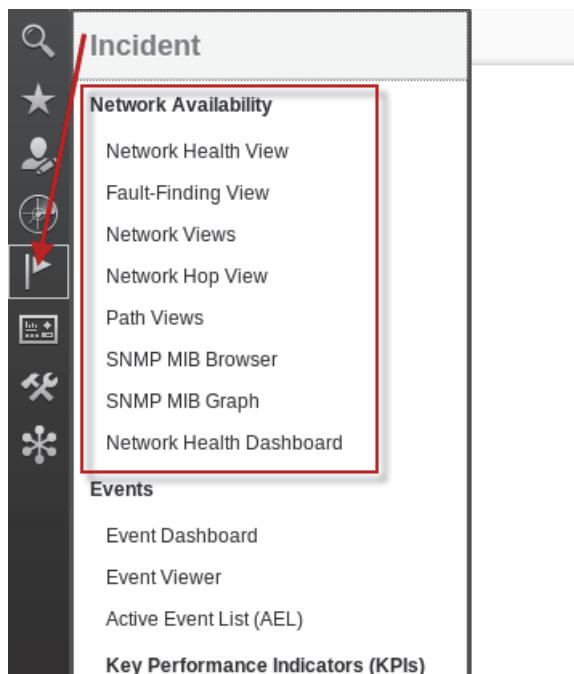
Verify that the user has access to the Network administration features.

8. Click the icon and verify the items.



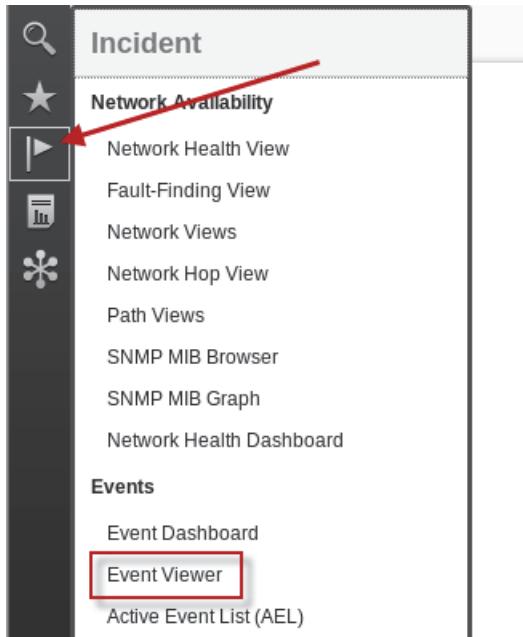
Verify that the user has access to the Network Discovery features.

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**.

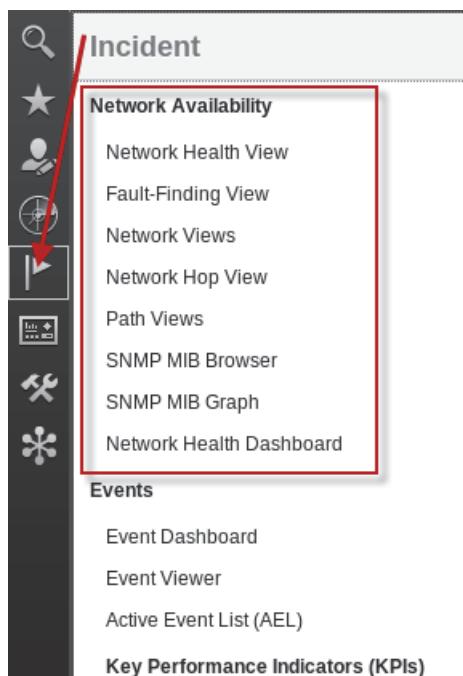


11. Right-click any event and examine the available tools.

The itnadmin 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 **itnadmin** user.

13. Log in to Dashboard Application Services Hub as user **itnmuser** with password **object00**.
14. Click the icon and verify the items.

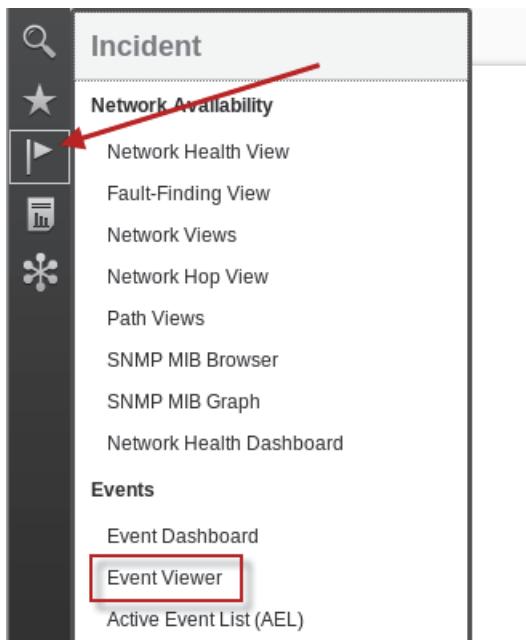


- Verify that the user has access to the Network Availability features.
15. Click the icon and verify the items.



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.

	No	chianti.tivlab.raleigh.ibm.com		: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Acknowledge Ctrl+A	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	De-acknowledge Ctrl+D	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Prioritize	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Suppress/Escalate	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Take ownership	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	User Assign	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Group Assign	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Delete	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Find In Hop View	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Find In Network View	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Find in Path View	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Trace IP Path	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Show Device Structure	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Open SNMP MIB Browser	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Open SNMP MIB Grapher	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Show Root Cause	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Show Suppressed Events	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Show SAE Related Events	: Linux_BP_SpaceUsedPct_Critical((C))
	No	chianti.tivlab.raleigh.ibm.com	Show SAE Related Services	: Linux_BP_SpaceUsedPct_Critical((C))

The **itnmuser** user is defined with the **netcool_rw** role. This role allows access to all tools, including the Network Manager 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
```

...

```
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_v1.3.5.0.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_v1.3.5.0.zip
```

...

```
[packagemanager] 08/01/19 16:31:13:698 UTC [main] INFO - ContentPackManager :  
CTGLC0023I : Install of NetworkManagerInsightPack_v1.3.5.0 completed  
successfully
```

BUILD SUCCESSFUL

Total time: 12 seconds



Important: The build must complete successfully before you proceed.

5. Remove the 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_v1.3.5.0/Ne  
twork_Topoogy_Search
```

- b. Open the file with the gedit utility:

```
gedit NM_EndToEndSearch.properties
```

- c. Modify the following properties.

ncp.dla.datasource.type	= db2
ncp.dla.datasource.driver	= com.ibm.db2.jcc.DB2Driver
ncp.dla.datasource.url	= jdbc:db2://host1.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.

- Check for the Cognos process.

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

Repeat this command until the process is not running.

- 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.

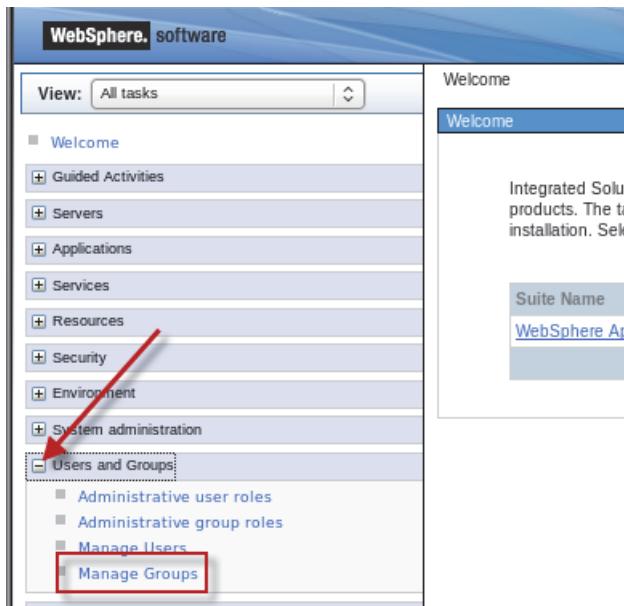
5. Open a Firefox browser if necessary.

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.

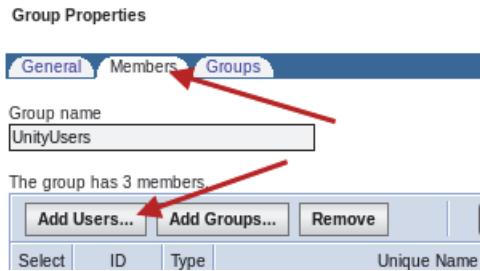
8. Expand **Users and Groups**. Click **Manage Groups**.



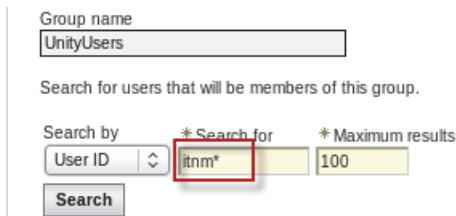
9. Click **UnityUsers**.

<input type="checkbox"/>	ITNM_User		cn=ITNM_User,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	Netcool_Admin		cn=Netcool_Admin,ou=tipgroups,cn=tipRealm,DC=IBM,DC=CO
<input type="checkbox"/>	Netcool_User		cn=Netcool_User,ou=tipgroups,cn=tipRealm,DC=IBM,DC=CO
<input type="checkbox"/>	UnityAdmins		cn=UnityAdmins,ou=tipgroups,cn=tipRealm,DC=IBM,DC=CO
<input type="checkbox"/>	UnityUsers		cn=UnityUsers,ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM

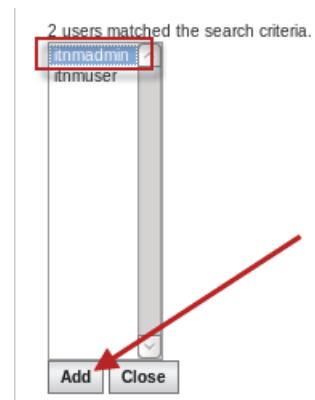
10. Select the **Members** tab and click **Add Users**.



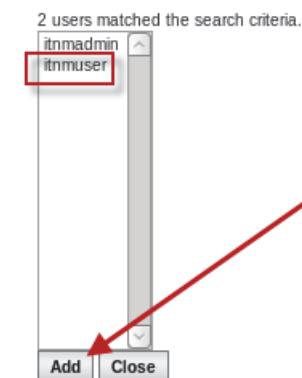
11. Enter **itnm*** and click **Search**.



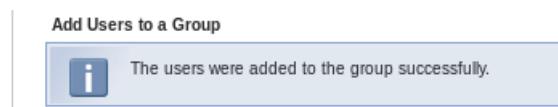
12. Select **itnadmin** and click **Add**.



13. Select **itnmuser** and click **Add**.



14. Click **Close**.



15. Verify that the users are listed and click the **General** tab.

Select	ID	Type	Unique Name
<input 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"/>	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.

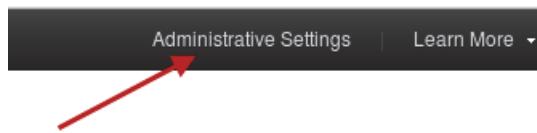
19. Log out of Dashboard Application Services Hub.

20. Connect to Log Analysis with the following URL:

<https://host1.csuite.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.

You can create and modify users to assign role-based access control to existing user and click the **edit** or **delete** icons. [Learn More...](#)

	User Name	Display Name
<input type="checkbox"/>	unityadmin	unityadmin
<input type="checkbox"/>

27. Enter **itnmuser** and click **OK**.

Configure LDAP User

A user profile is a distinct account with specific roles and permissions

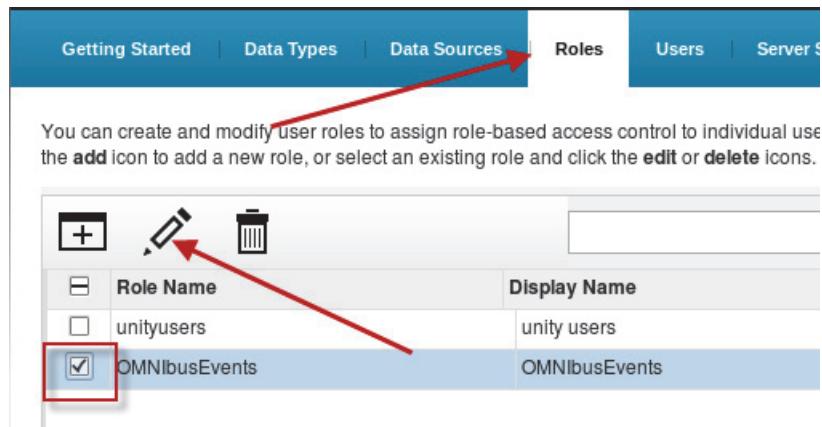
* User Name

itnmuser

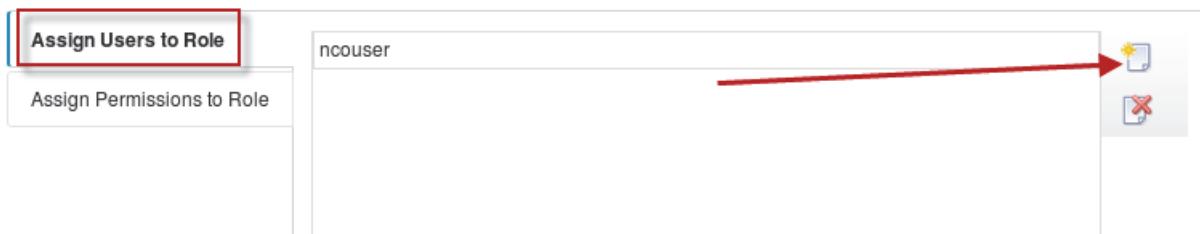
28. Click **OK** to confirm.



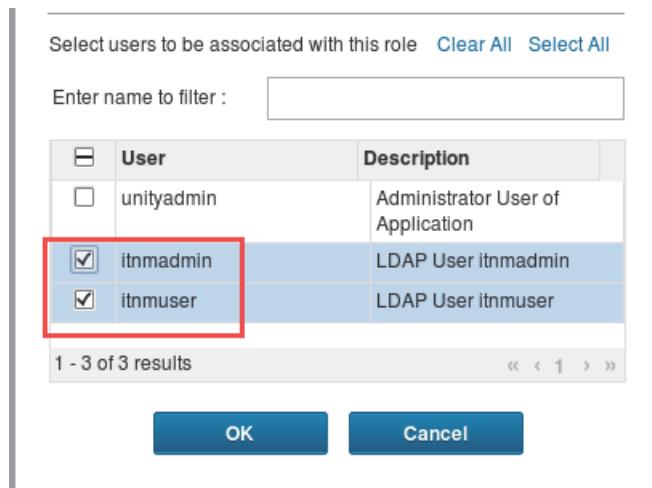
29. Click the **Roles** tab. Select **OMNIBusEvents**, and click the icon to edit the role.



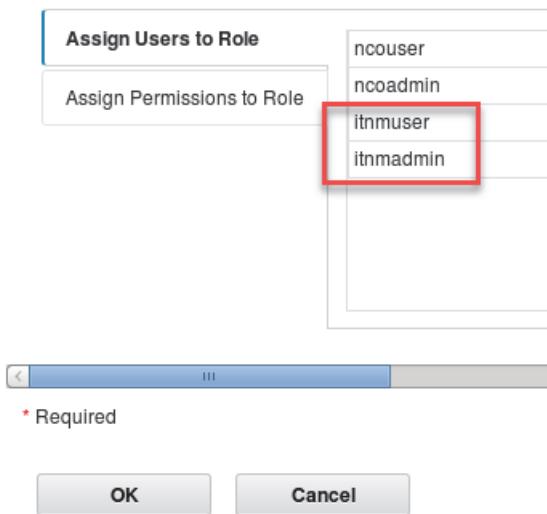
30. Select **Assign Users to Role**. Click the icon to add a user.



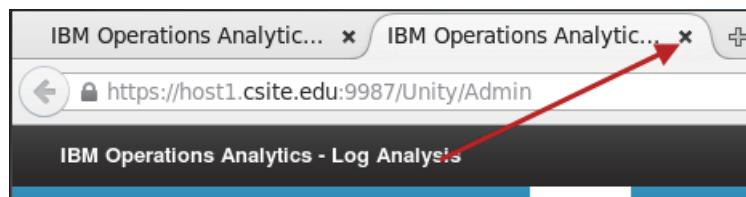
31. Select **itnmadmin** and **itnmuser**, then click **OK**.



32. Click **OK** to update the role.



33. Close the Firefox tab.



34. Log out of Log Analysis.

35. Close the Firefox browser.

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 target directory.

```
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 in a text editor.

```
gedit waapi.init
```

- c. Find the following lines:

```
waapi.user:root
```

```
waapi.password:
```

- d. Change the lines as follows:

```
waapi.user:ncoadmin
```

```
waapi.password:object00
```

- e. 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.

- a. Change to the WAPPI bin directory:

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

- b. Run the following command to install the tools:

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

```
*****
```

```
WAAPIClient: Request sent to server on  
http://localhost:16310/ibm/console/webtop/...  
Thu Aug 01 17:08:03 UTC 201  
*****
```

```
WAAPIClient: 3 methods were fully executed.
```

Configuring the tools in Network Manager

Users can launch to the Log Analysis UI from a Network View. These steps show you how to configure the tools and menus for the Log Analysis integrations.

1. 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 in a text editor.

```
gedit ncp_topoviz_device_menu.xml
```

- c. Add the following line as shown here:

```
<menu id="ncp_topo_e2esearch"/>
```

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

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

2. 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.

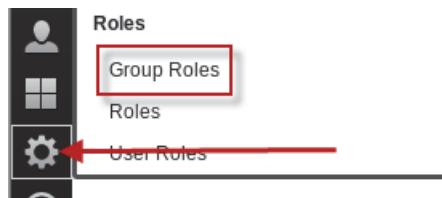
3. Add the required role.

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**.



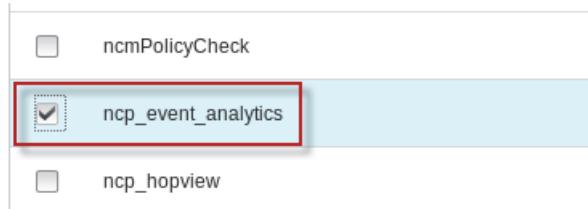
d. Enter **Network***, and click **Search**.

Group ID*	<input type="text" value="Network*"/>	Desc
Number of results to display:		
<input type="button" value="20"/>		
<input type="button" value="Search"/>		

e. Click **Network_Manager_IP_Admin**.

Group Name	Roles
Network_Manager_IP_Admin	ncp_oql_editor, ncp_networkview_admin_i...
Network_Manager_User	ncp_mibbrowser, ncp_webtools, ncp_mibg...

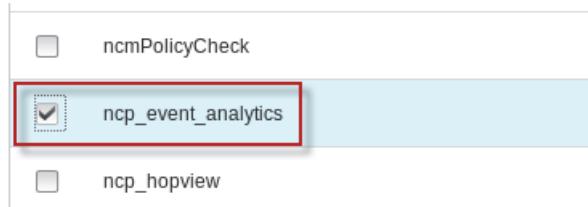
f. Scroll down and select **ncp_event_analytics**. Click **Save**.



g. Click **Network_Manager_User**.

Group Name	Roles
Network_Manager_IP_Admin	ncp_oql_editor, ncp_networkview_admin_ncp_mibrowser, ncp_webtools, ncp_mibg
Network_Manager_User	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. You install and run the application software as the netcool user. You must create new users to manage the database and to operate an FTP server. The next steps show you how to create and configure those users.

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.

```
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 in a text editor.

```
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..

```
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_BS6.4.2.8_LNX_EN.tar
```

2. Change file permissions on the directory and contents.

```
chmod -R a+r *
```

3. Switch to the **db2inst1** user.

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

4. Run the following command to create the database. The command runs for several minutes.

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

```
DB20000I The CREATE DATABASE command completed successfully.
```



Note: You can ignore any messages about libxml2.so.2 or libdb2.so.1.

5. Configure database user privileges.

a. Connect to the database.

```
db2 connect to itncm
```

Database Connection Information

```
Database server      = DB2/LINUXX8664 11.1.0
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_
CONNECT 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 itnmc 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 itnmc using logsecond 50
```

DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

```
db2 update db cfg for itnmc using LOCKLIST 8192
```

DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully.

- d. Commit the changes to the database.

```
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.

- 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/
```

- 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.

- Start IBM Installation Manager:

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

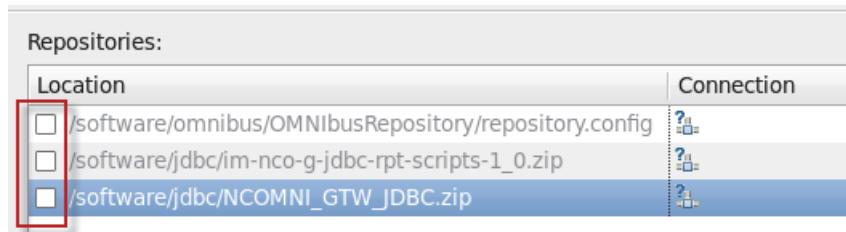
- Define the repositories.



Note: The installation files are still in **/tmp**, and the repository entries are still defined in IBM Installation Manager.

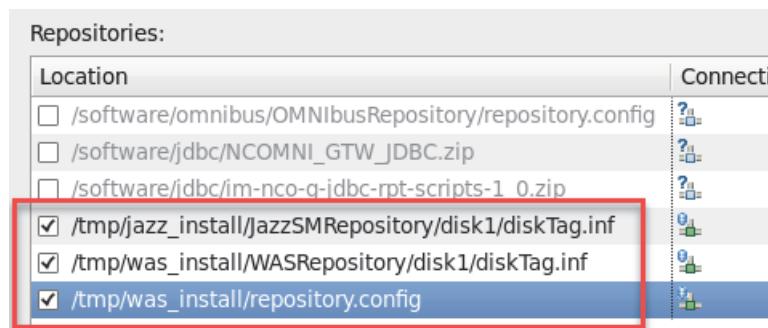
- Click **File** and select **Preferences**. Select **Repositories**.

- Remove the check marks from any existing entries.



Note: You added the Jazz and WebSphere repositories in a previous unit. You must locate the entries and select them.

- Select the Jazz repository entry. Select the WebSphere entries 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
IBM WebSphere Application Server	Installed
Version 8.5.5.15	Installed
IBM WebSphere SDK Java Technology Edition (Optional)	Installed
Version 7.0.9.30	Installed
Jazz for Service Management extension for IBM WebSphere 8.0	Installed
Version 1.1.0.2	Installed
Jazz for Service Management extension for IBM WebSphere 8.5	Installed
Version 1.1.2.1	Installed
IBM Dashboard Application Services Hub	Installed
Version 3.1.3.3	Installed
Reporting Services	Installed

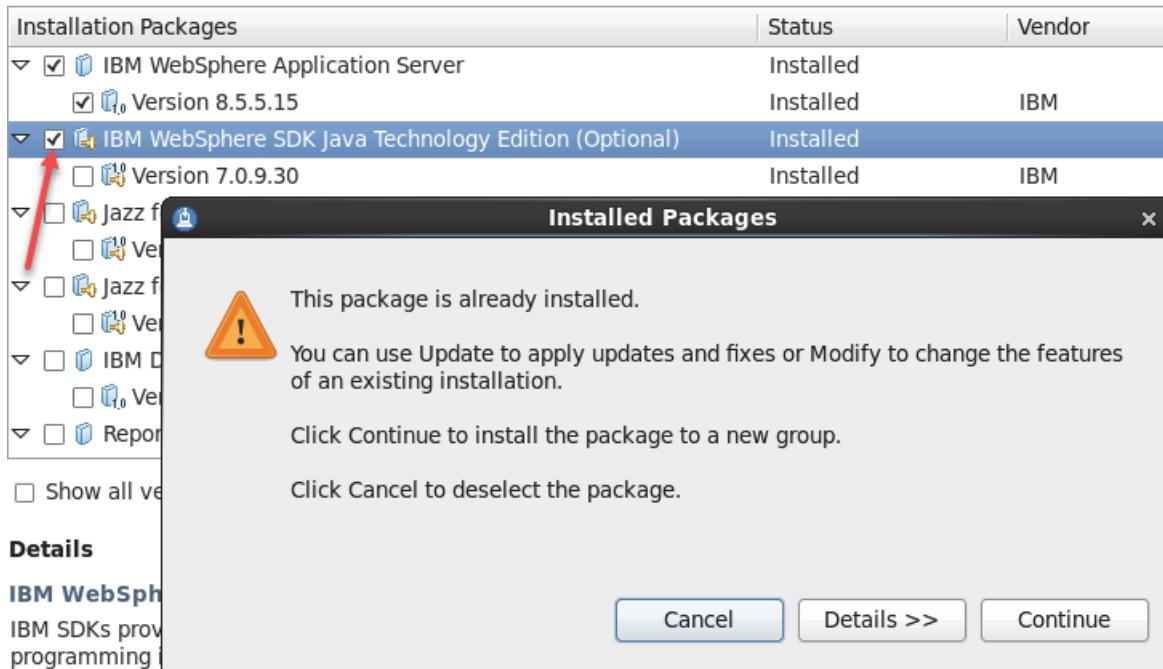
- b. Select **IBM WebSphere Application Server**, and click **Continue**.

The screenshot shows the 'Installation Packages' dialog. A red arrow points to the checkbox next to 'IBM WebSphere Application Server', which is checked. Another red arrow points to the 'Continue' button at the bottom right of a modal dialog titled 'Installed Packages'. The modal contains the following text:

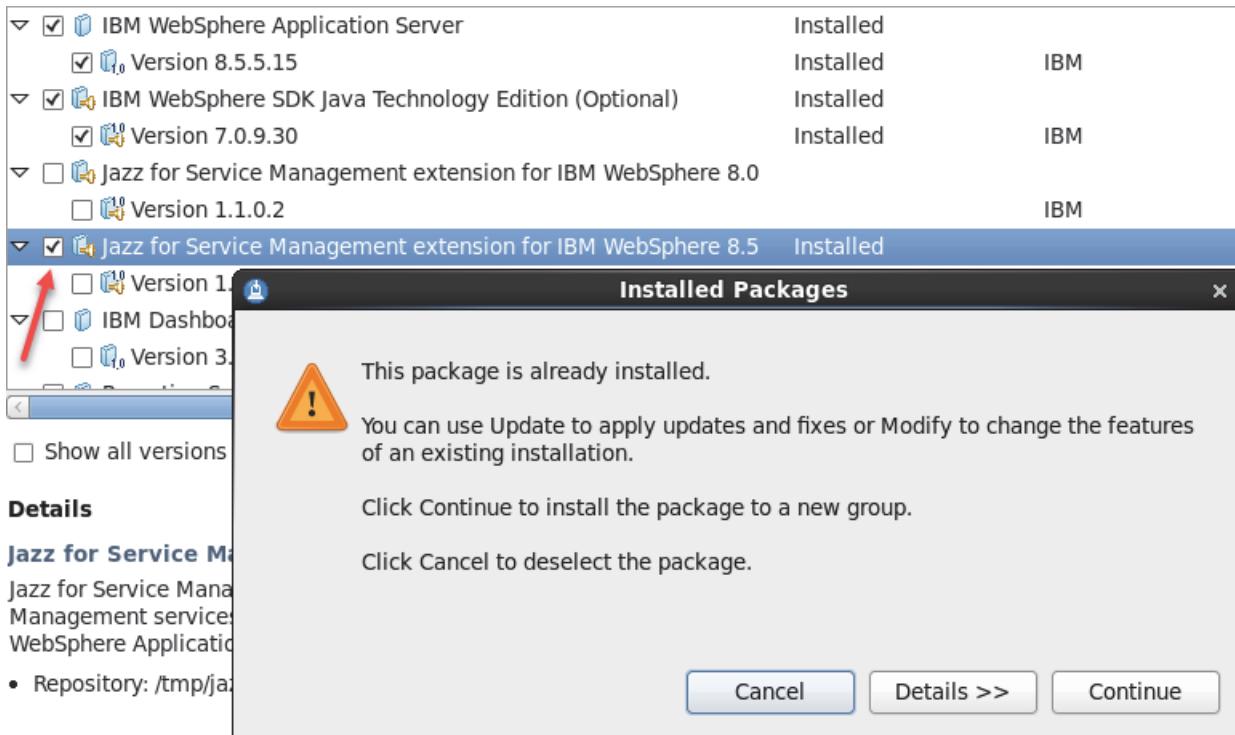
This package is already installed.
You can use Update to apply updates and fixes or Modify to change the features of an existing installation.
Click Continue to install the package to a new group.
Click Cancel to deselect the package.

At the bottom of the modal are three buttons: 'Cancel', 'Details >>', and 'Continue' (which is highlighted with a red arrow).

- 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**.

Installation Packages	Status	Vendor
<input checked="" type="checkbox"/> IBM WebSphere SDK Java Technology Edition (Optional)	Installed	
<input checked="" type="checkbox"/> Version 7.0.9.30	Installed	IBM
<input type="checkbox"/> Jazz for Service Management extension for IBM WebSphere 8.0		
<input type="checkbox"/> Version 1.1.0.2		IBM
<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	IBM
<input checked="" type="checkbox"/> IBM Dashboard Application Services Hub	Installed	

- f. Verify that you selected the required packages, and click **Next**.

Installation Packages	Status
<input checked="" type="checkbox"/> IBM WebSphere Application Server	Installed
<input checked="" type="checkbox"/> Version 8.5.5.15	Installed
<input checked="" type="checkbox"/> IBM WebSphere SDK Java Technology Edition (Optional)	Installed
<input checked="" type="checkbox"/> Version 7.0.9.30	Installed
<input type="checkbox"/> Jazz for Service Management extension for IBM WebSphere 8.0	
<input type="checkbox"/> Version 1.1.0.2	
<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 checked="" type="checkbox"/> IBM Dashboard Application Services Hub	Installed
<input checked="" type="checkbox"/> Version 3.1.3.3	Installed



Important: Do not select the **Reporting Services** package.

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

- h. Click the package named **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 8.5.5.15	
IBM WebSphere SDK Java Technology Edition (Optional)	
Jazz for Service Management extension for IBM WebS	
Core services in Jazz for Service Management_1	/home/netcool/IBM/JazzSM
IBM Dashboard Application Services Hub 3.1.3.3	

Package Group Name: IBM WebSphere Application Server V8.5_1

Installation Directory: **/opt/IBM/WebSphere/AppServer_ncm**

- 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_ncm
IBM WebSphere Application Server 8.5.5.15	
IBM WebSphere SDK Java Technology Edition (Optional)	
Jazz for Service Management extension for IBM Webs	
Core services in Jazz for Service Management_1	/opt/IBM/JazzSM_ncm
IBM Dashboard Application Services Hub 3.1.3.3	

Package Group Name: Core services in Jazz for Service Management_1

Installation Directory: **/opt/IBM/JazzSM_ncm**

- 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**.

Common Configurations
WebSphere Configuration

WebSphere installation location

Profile deployment type

Profile details

Profile location	/opt/IBM/JazzSM_ncm/profile
Profile name	JazzSMPProfile
Node name	JazzSMNode01
Server name	server1
User name	smadmin
Password	***** *****
Password confirmation	





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**.

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



Note: The installation process runs for 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 8.5.5.15
- ↳ IBM WebSphere SDK Java Technology Edition (Optional) 7
- ↳ Jazz for Service Management extension for IBM WebSphere
- ↳ Core services in Jazz for Service Management_1
- ↳ IBM Dashboard Application Services Hub 3.1.3.3

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 service
- None

4. Open a Firefox browser connect to IBM Dashboard Application Services Hub:
<https://host1.csuite.edu:15311/ibm/console/logon.jsp>
5. Expand **I Understand the Risks**, and click **Add Exception**.

▼ **I Understand the Risks**

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

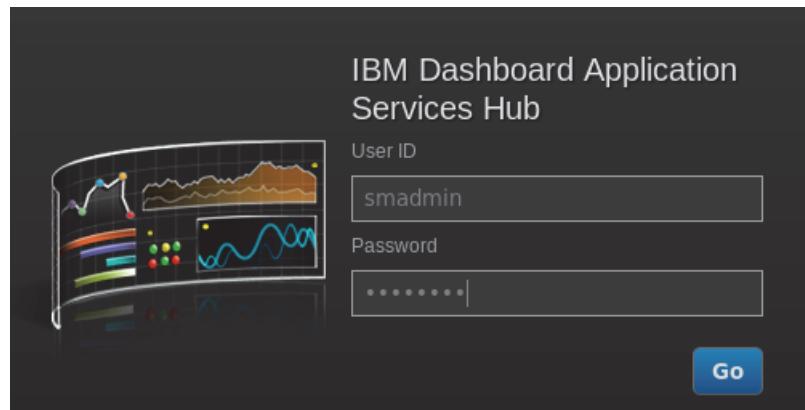
Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

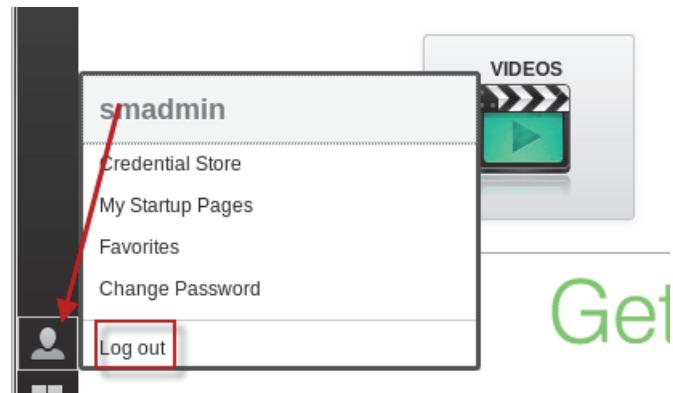
6. Click **Confirm Security Exception**.



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



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



9. Close the Firefox browser.
10. 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.

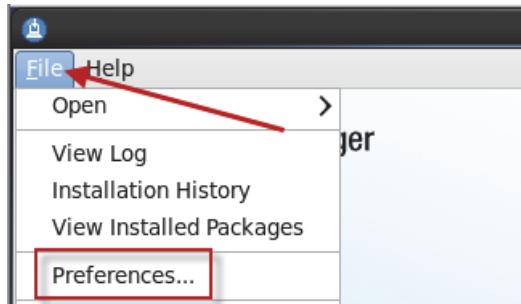
1. Start IBM Installation Manager.



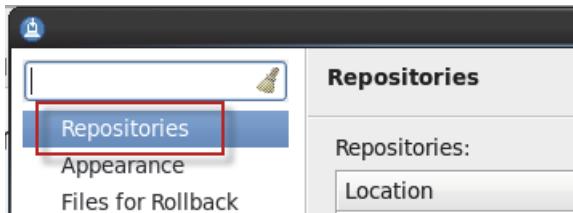
Note: IBM Installation Manager might still be open from the previous exercise.

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

2. Click **File** and select **Preferences**.



3. Select **Repositories**.



4. Remove all check marks from any existing repository entries.

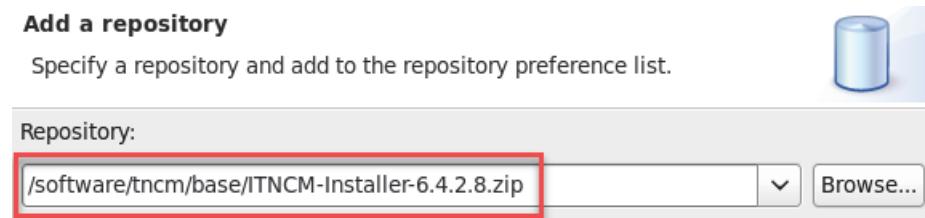
Repositories:	
Location	Connection
<input type="checkbox"/> /software/omnibus/OMNIBusRepository/repository.config	
<input type="checkbox"/> /software/jdbc/im-nco-g-jdbc-rpt-scripts-1_0.zip	
<input type="checkbox"/> /software/jdbc/NCOMNI_GTW_JDBC.zip	
<input type="checkbox"/> /tmp/jazz_install/repositories/disk1/diskTag.inf	
<input type="checkbox"/> /software/webgui/OMNIBusWebGUIRepository/repository.c	

5. Click **Add Repository**.



6. Click **Browse** and locate the following file:

/software/tncm/base/ITNCM-Installer-6.4.2.8.zip



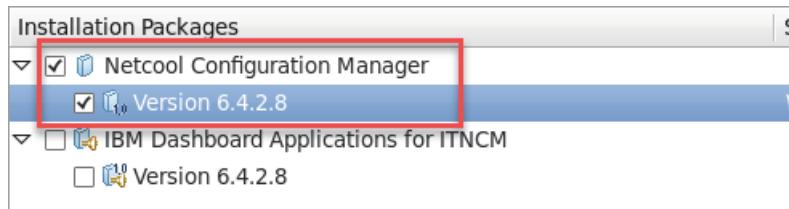
7. Click **OK** to add the repository.

8. Verify that the repository is selected, and click **OK**.

9. Click **Install**.



10. Select the **Netcool Configuration Manager** package. Click **Next**.



Important: Do not select IBM Dashboard Applications for ITNCM. You install this package later.

11. 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**.

- Use the existing package group
- Create a new package group

Package Group Name	Installation Directory
Netcool Configuration Manager	/opt/IBM/ncm

Package Group Name: Netcool Configuration Manager

Installation Directory: /opt/IBM/ncm

13. Accept the default list of features. Click **Next**.

14. Enter the db2 access information as follows, and click **Next**.

- a. Enter **host1.csite.edu** for the server host.
- b. Enter **50000** for the port number.
- c. 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 configu

Database server type

DB2 (default)
 Oracle 11
 Oracle 12

Database name:

Server host:

Server port:

User ID:

Password:

15. Click **OK** to accept the option to create the database tables.



16. Enter the following FTP access information, and scroll down.



Important: Make certain that you scroll down and complete the next step before you click **Next**.

- a. Enter **host1.csuite.edu** for the FTP server.
- 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. Scroll down.
- f. Select the option for integrated NCM - NM install.
- g. Enter **host1.csuite.edu** for the host name.
- h. Enter **16311** for the port number.
- i. Enter **itnadmin** for the user name.
- j. Enter **object00** for the password.
- k. Enter **ITNCM/NOI_AGG_P** for the realm.

l. Click **Next**.

Is This the main IDT Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
Select the type of install you require.	<input checked="" type="checkbox"/> Activate Configuration-Core <input checked="" type="checkbox"/> Activate Compliance-Core
<input checked="" type="checkbox"/> Is this an integrated NCM - NM Install?	
The NM Hostname	host1.csuite.edu
The port to connect to	16311
The NM User	itnadmin
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**.

Common Configurations
NCM JazzSM Details

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

Installation Directory Details
 (highlighted with a red box)

JazzSM user credentials

User name	smadmin
Password	***** (highlighted with a red box)
Password Confirmation	***** (highlighted with a red box)

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/IBMIMShared

Packages

Packages

Network Configuration Manager 6.4.2.0

ITNCM

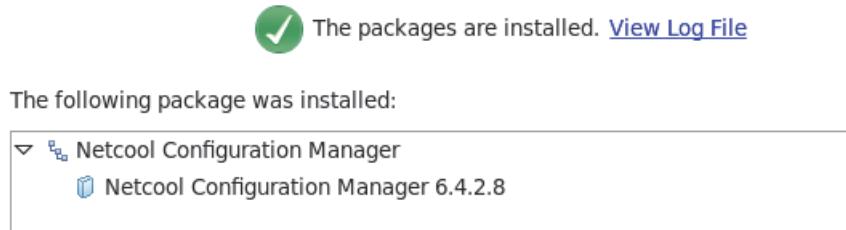
Server Installation Type

Presentation Server and Worker Server

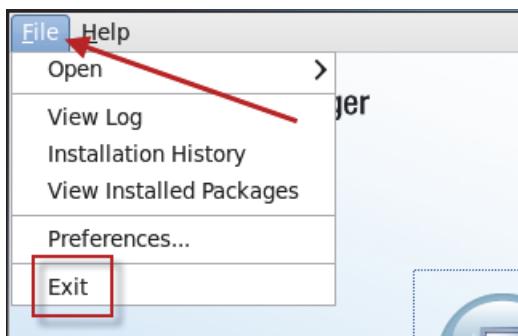


Note: The installation runs for approximately 25 minutes.

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
```

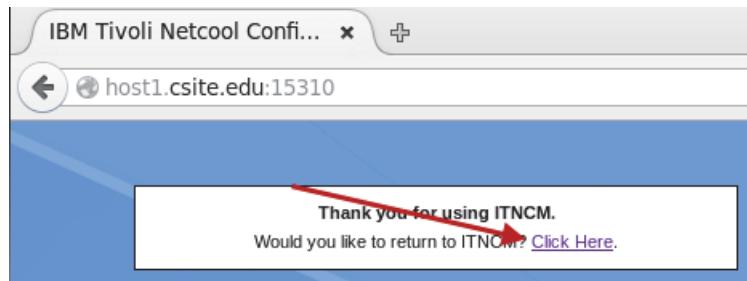
24. Log in as user **Intelliden** with password **object00**.



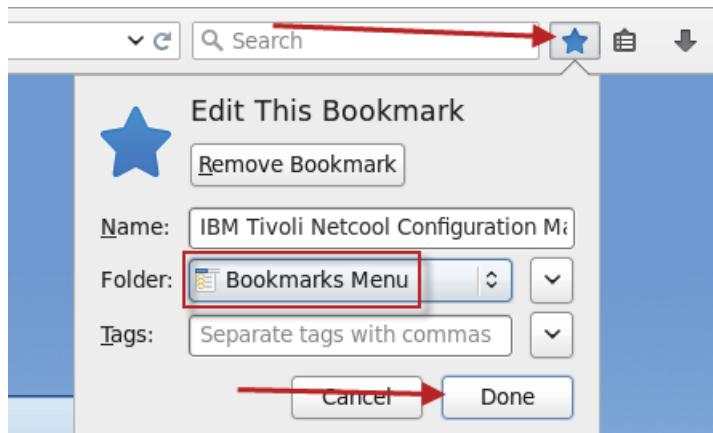
25. Verify access, and click **Logoff**.



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.

In a previous exercise, you expanded the installation file and defined the software repository.

1. Start IBM Installation Manager.

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

2. Click **Install**.3. Select **IBM Dashboard Applications for ITNCM**, and click **Next**.

Installation Packages	Status
Netcool Configuration Manager	Installed
Version 6.4.2.8	Installed
IBM Dashboard Applications for ITNCM	
Version 6.4.2.8	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**.

Features
IBM Dashboard Applications for ITNCM 6.4.2.8
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 **itnmadmin** 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, itnmadmin). The user must have the ncw_admin role and privileges to run the Netcool WebGUI waapi command. Ensure that the user authentication repository is accessible from this server before continuing.

User ID: **itnmadmin**

Password: *********

8. Enter the DB2 access information as shown here, and click **Next**.

- Enter **itncm** for the database schema.
- Enter **host1.csuite.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.csuite.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	<input type="text" value="https"/>	
ITNCM presentation server hostname	<input type="text" value="host1.csuite.edu"/>	
ITNCM presentation server web port	<input type="text" value="15311"/>	

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

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	<input type="text" value="https"/>	
ITNCM Reporting Server hostname	<input type="text" value="host1.csuite.edu"/>	
ITNCM Reporting Server web port	<input type="text" value="16311"/>	

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

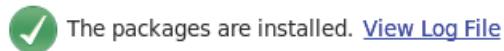
The installation process verifies access to the Common Reporting server.

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

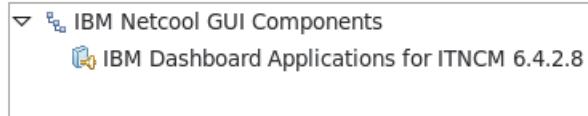


Important: The installation runs for approximately 20 minutes.

12. Verify that the installation is successful, and click **Finish**.



The following package was installed:



Leave IBM Installation Manager open.

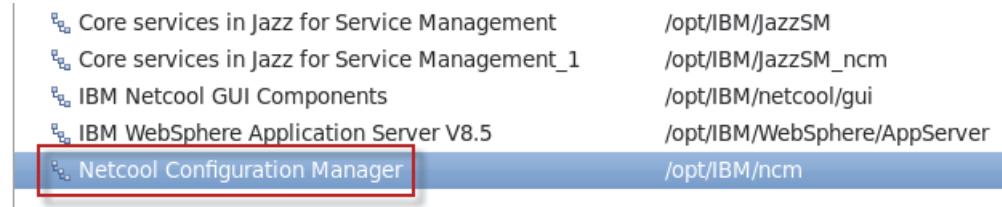
Installing Common Reporting reports

You expanded the installation file in a previous exercise.

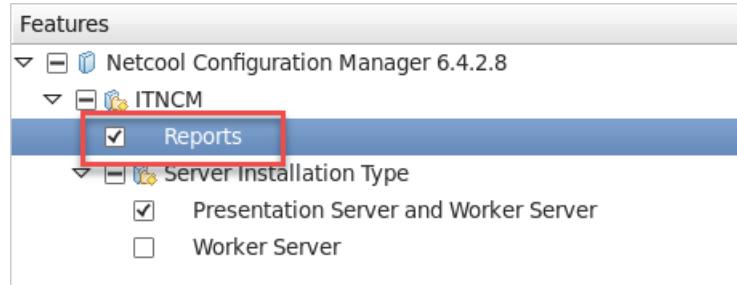
1. Click **Modify**.



2. Select the **Netcool Configuration Manager** package. Click **Next**.



3. Select **Reports**, and click **Next**.



4. Enter the db2 access information as follows, and click **Next**.

- a. Enter **host1.csite.edu** for the server host.
- b. Enter **50000** for the port number.
- c. 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.csuite.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: Netcool Configuration Manager
Installation Directory: /opt/IBM/ncm
Shared Resources Directory: /home/netcool/IBM/IBMIMShared

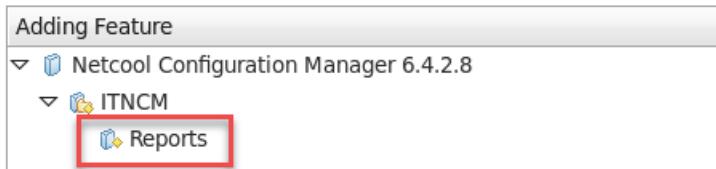
Features

Adding Feature

Netcool Configuration Manager 6.4.2.8

ITNCM

Reports



 **Note:** The process runs for approximately 10 minutes.

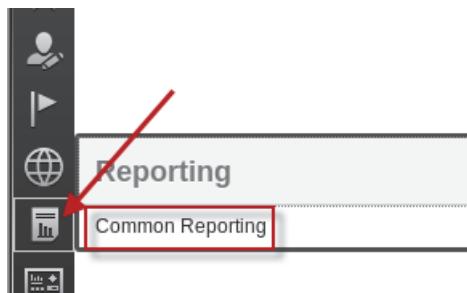
7. Verify that the modification is successful. Click **Finish**.

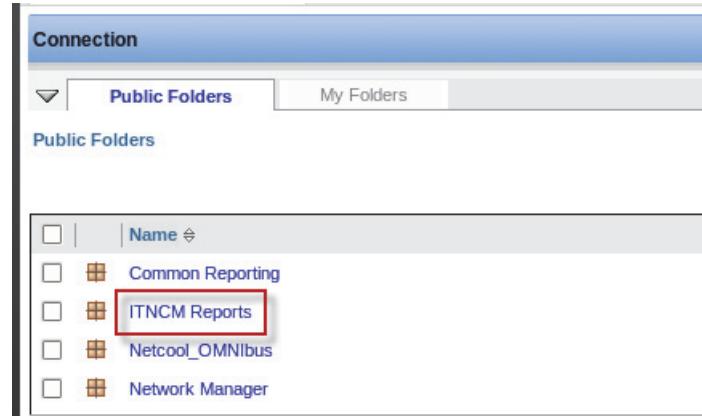
 The modification completed successfully. [View Log File](#)

The following package was modified:

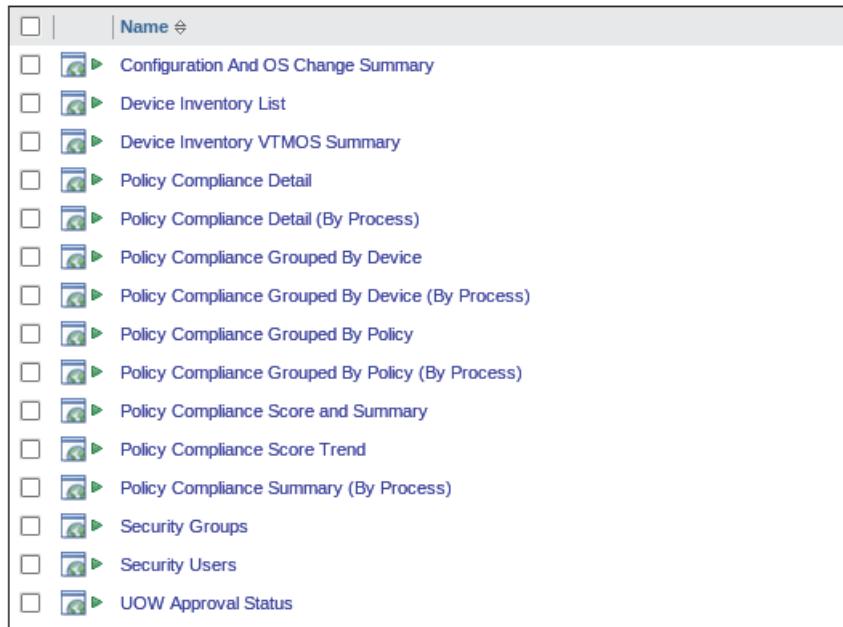
Netcool Configuration Manager

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.****15. Remove the Netcool Configuration Manager installation files to conserve disk space.**

```
rm -rf /software/tncm/ITNCM_BS6.4.2.8_LNX_EN.tar  
rm -rf /software/tncm/base/ITNCM-Installer-6.4.2.8.zip  
rm -rf /software/tncm/base/ibm_tivoli-jpa_db2.jar
```

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 installation 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 installation utility to run.

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

- c. Run the following command to start the installation utility.

```
./ITNCMDrivers.bin LAX_VM /opt/IBM/ncm/jre/bin/java -i console
```

- d. Press Enter when you are prompted.

PRESS <ENTER> TO CONTINUE:

- e. Enter 1 to accept the license agreement.

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

- f. Press Enter to accept the default installation folder.

Where would you like to install?

```
Default Install Folder: /opt/IBM/ncm
```

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT

:

- g. Press Enter when you are prompted.

Disk Space Information (for Installation Target):

Required: 104 MegaBytes

Available: 25,642 MegaBytes

PRESS <ENTER> TO CONTINUE:

- h. Press Enter when the installation is finished.

...

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  
  
rm -rf /software/tncm/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 installation utility to run.

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

- c. Run the following command to start the installation utility.

```
./ITNCMDrivers.bin
```

- d. Press Enter when you are prompted.

PRESS <ENTER> TO CONTINUE:

- e. Enter 1 to accept the license agreement.

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**

- f. Press Enter to accept the default installation folder.

Where would you like to install?

Default Install Folder: /opt/IBM/ncm

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT

- g. Enter 1 to install drivers for all devices.

```
=====
Choose Install Set
-----
```

Please choose the Install Set to be installed by this installer.

1- All Devices
2- ACME Devices
3- Actelis Devices

...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
: 1

- h. Press Enter when you are prompted.

...

Disk Space Information (for Installation Target):

Required: 13,738,673,199 Bytes
Available: 22,215,008,256 Bytes

PRESS <ENTER> TO CONTINUE:

- i. Press Enter when the installation is finished.

...

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 Netcool Configuration Manager.

```
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
```

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 the installation utility to run.

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

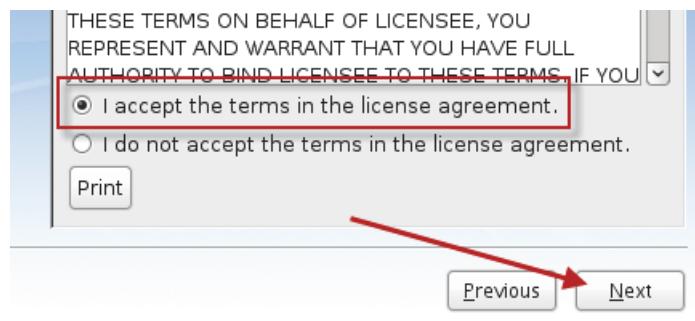
6. Run the installation utility.

```
./autodiscovery-aa85.bin LAX_VM /opt/IBM/ncm/jre/bin/java -i gui
```

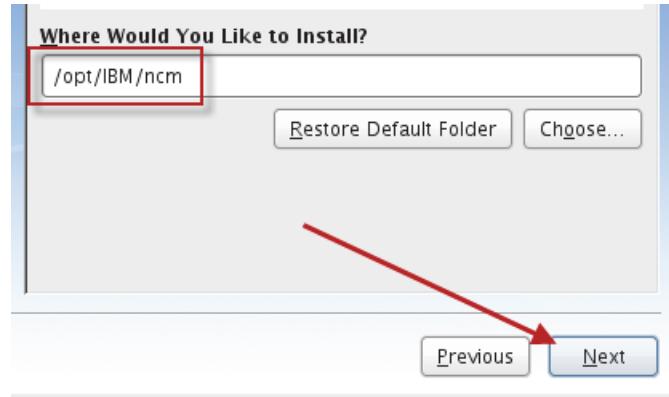
7. Click **Next**.



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



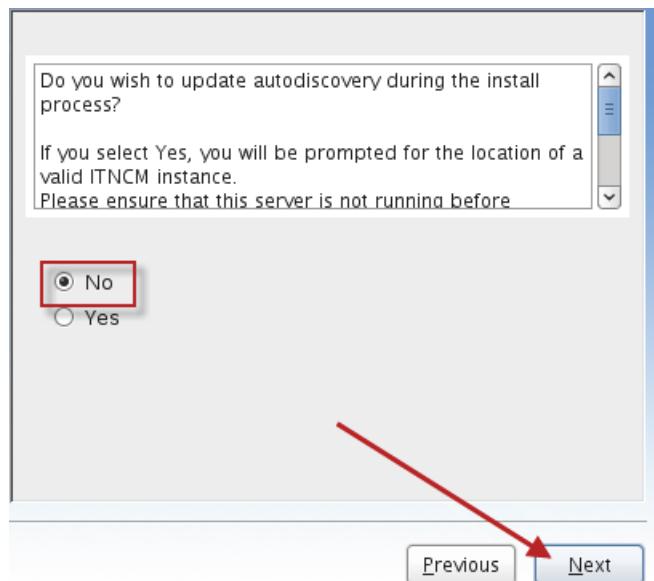
9. Accept the default folder, and click **Next**.



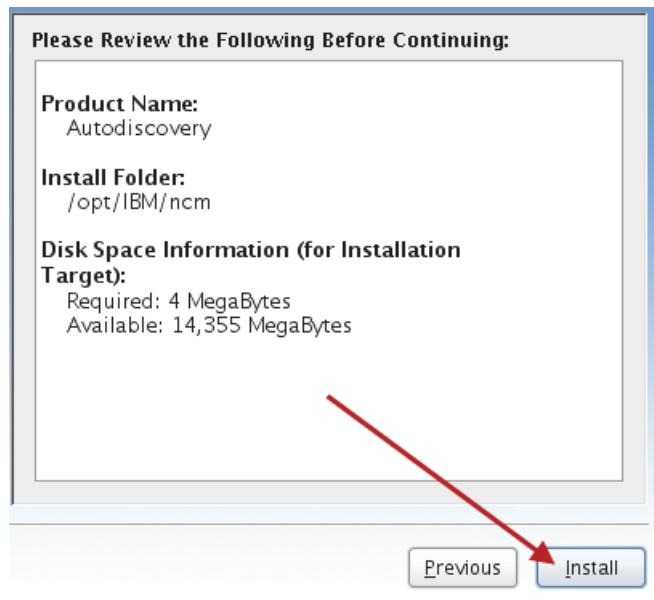
10. Ignore the warning message, and click **Continue**.



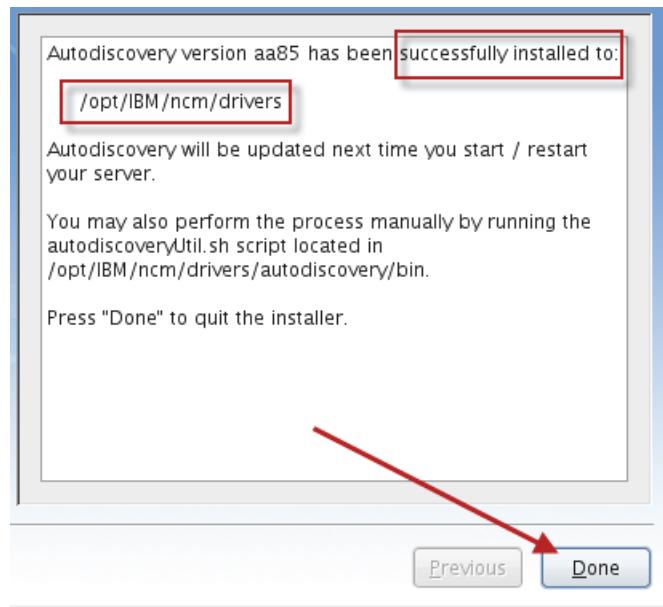
11. Accept the default update setting, and click **Next**.



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

Copying required Java files

1. Run the following commands to copy the key store file from the Network Manager GUI server into the Netcool Configuration Manager WebSphere instance.

```
cd /opt/IBM/WebSphere/AppServer_ncm/etc/  
cp /opt/IBM/WebSphere/AppServer/etc/vmm4ncos.jks .
```

- Run the following commands to copy the jar files from the Network Manager GUI server into the Netcool Configuration Manager WebSphere instance.

```
cd /opt/IBM/WebSphere/AppServer_ncm/lib/ext/  
cp /opt/IBM/WebSphere/AppServer/lib/ext/* .
```

- Verify that the key store file was copied to the Netcool Configuration Manager WebSphere instance.

```
ls /opt/IBM/WebSphere/AppServer_ncm/etc/
```

```
cea config digicert.jks tmx4jTransform.jar vmm4ncos.jks wim ws-security
```

- Verify that the jar files were copied to the Netcool Configuration Manager WebSphere instance.

```
ls /opt/IBM/WebSphere/AppServer_ncm/lib/ext/
```

```
com.ibm.tivoli.ncw.ncosvmm.jar jconn3.jar
```

Changing passwords

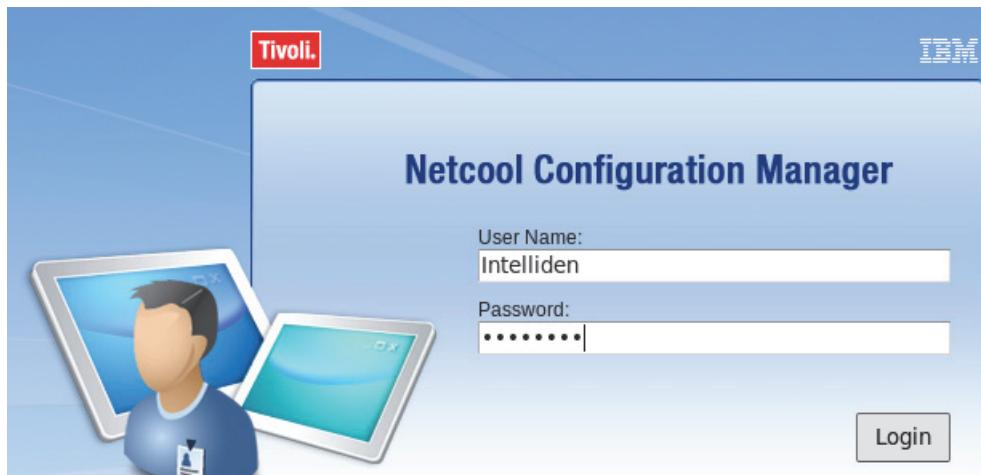
- Open a Firefox browser.
- Connect to the presentation server at the following URL.

<http://host1.csite.edu:15310/security/login.jsp>



Hint: Use the bookmark that you created previously to open the URL for the presentation server.

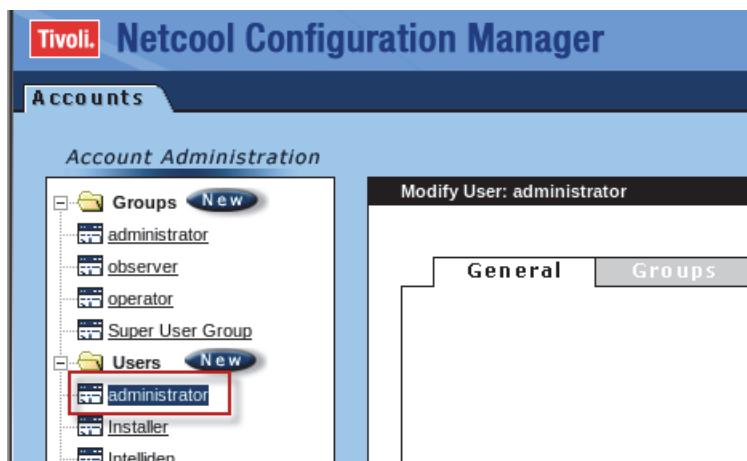
- Log in as user **Intelliden** with password **object00**.



4. Click **Account Management**.



5. Under Users, click **administrator**.



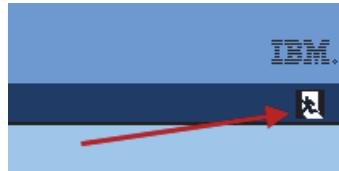
6. Change the password to **object00**, and click **Save**.

The screenshot shows the "Modify User: administrator" dialog box. The "Password" field contains "*****" and is highlighted with a red box. The "Validate Password" field also contains "*****". Below the fields are "First Name", "Middle Initial", "Last Name", "E-mail", "Telephone Number", and "Identification" fields, all containing "administrator". At the bottom right, there are "Save", "Remove", and "Cancel" buttons. A red arrow points from 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.

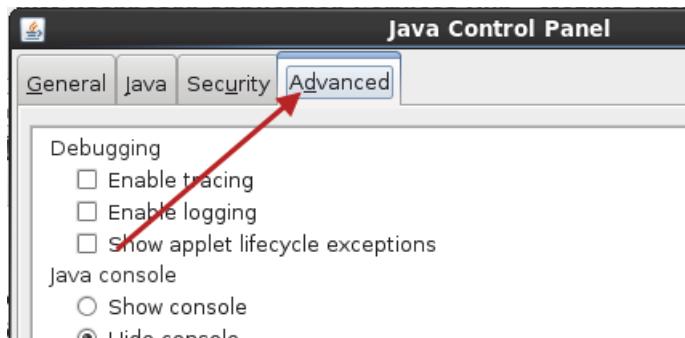
1. Change to the location of Java.

```
cd /opt/IBM/ncm/jre/bin
```

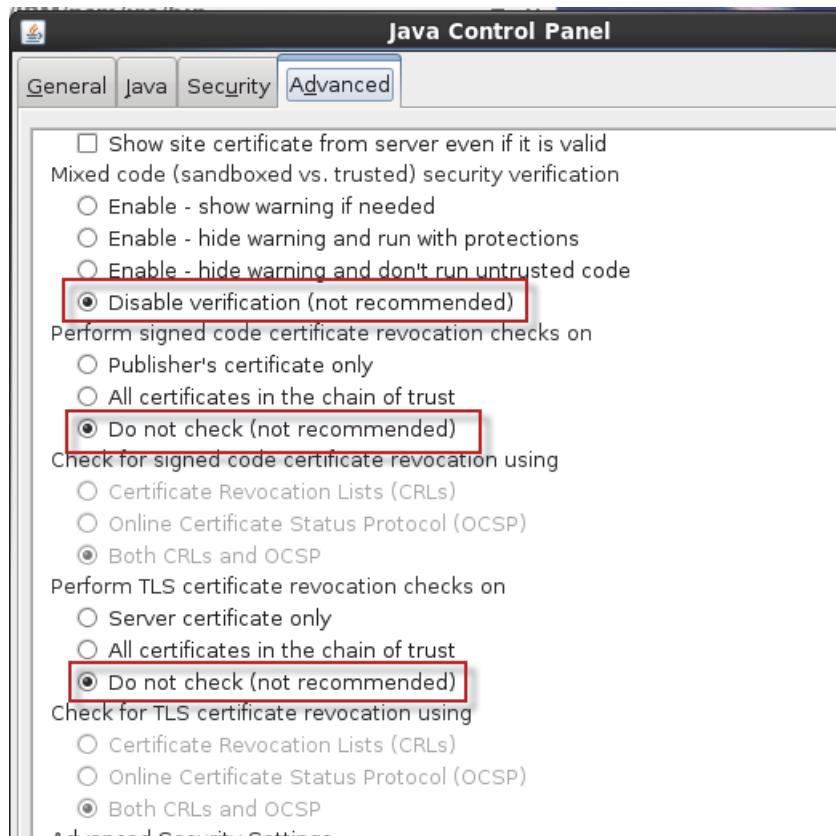
2. Open the Java control panel.

```
./ControlPanel
```

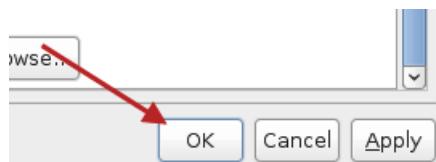
3. Click **Advanced**.



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 in a text editor.

```
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.

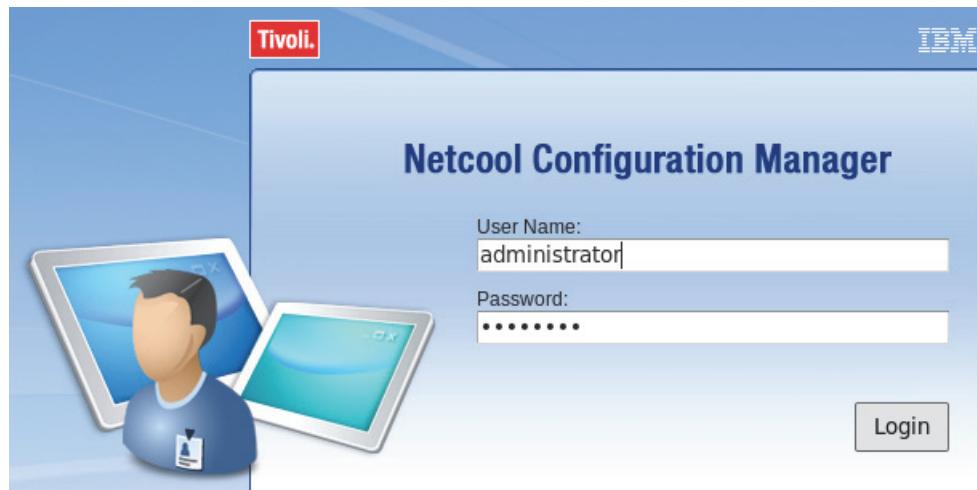
The following steps configure the Firefox browser to run the Java Webstart application.

10. Open a Firefox browser.

11. Connect to the following URL:

```
http://host1.csuite.edu:15310/security/login.jsp
```

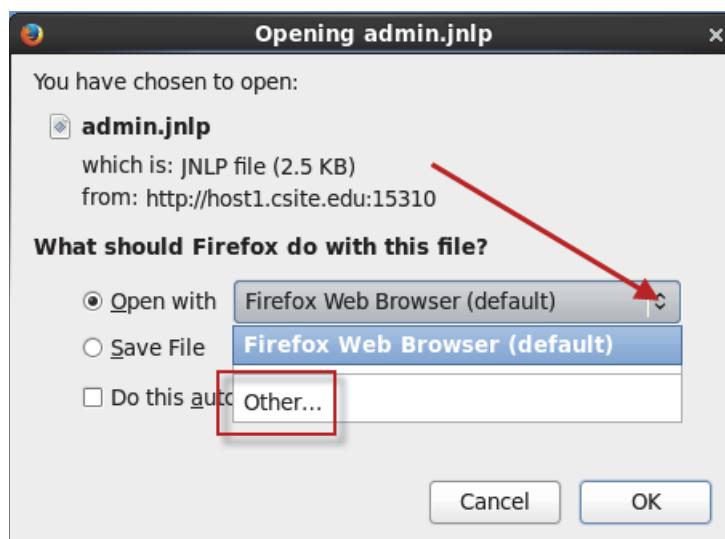
12. Log in as **administrator** with password **object00**.

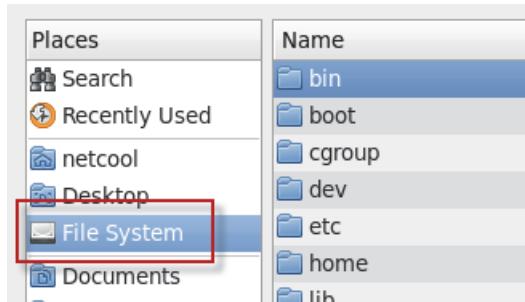
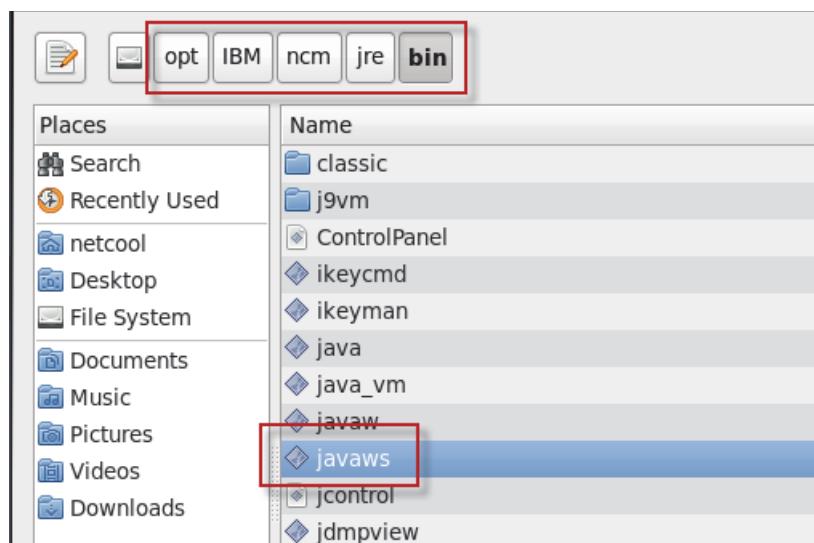
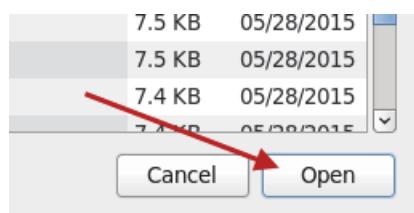


13. Select **ITNCM Webstart GUI**.

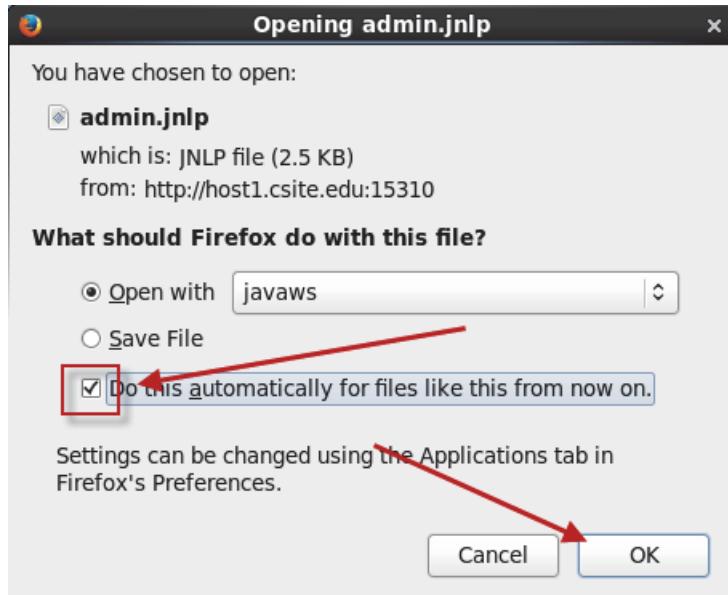


14. Click the arrow and select **Other**.



15. Click File System.**16. Navigate to /opt/IBM/ncm/jre/bin, and select javaws.****17. Click Open.**

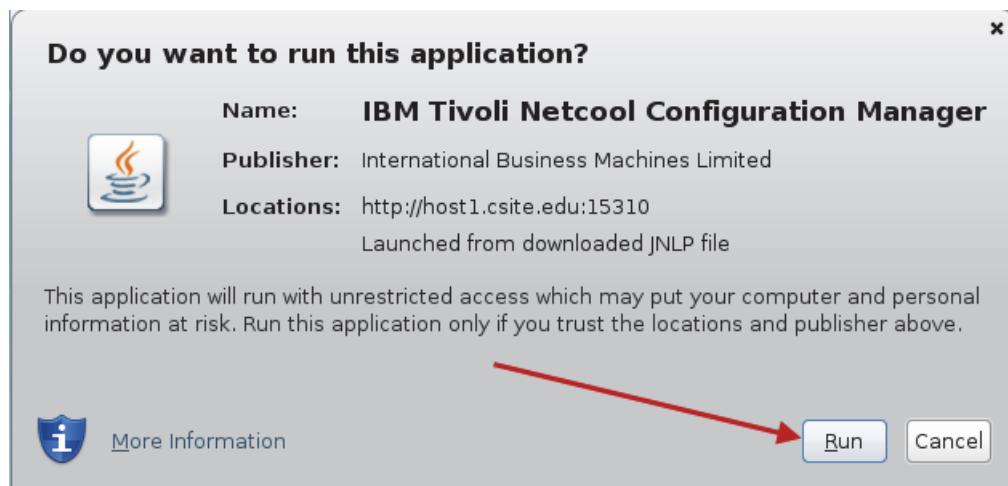
18. Select the option to do this automatically, and click **OK**.



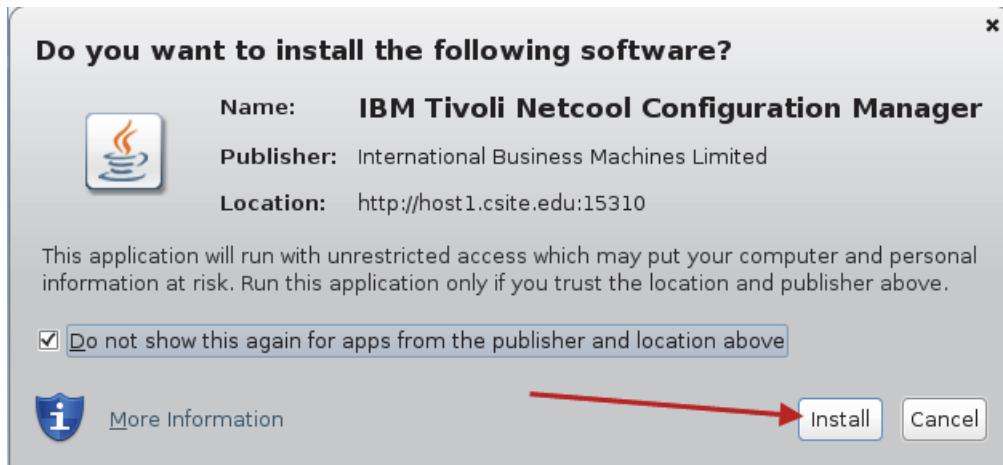
19. Select the option to not ask again, and click **Continue**.



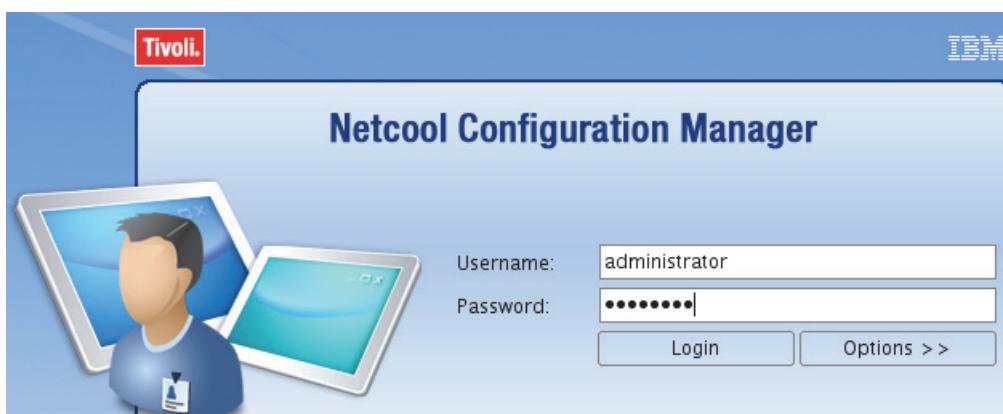
20. Click **Run**.



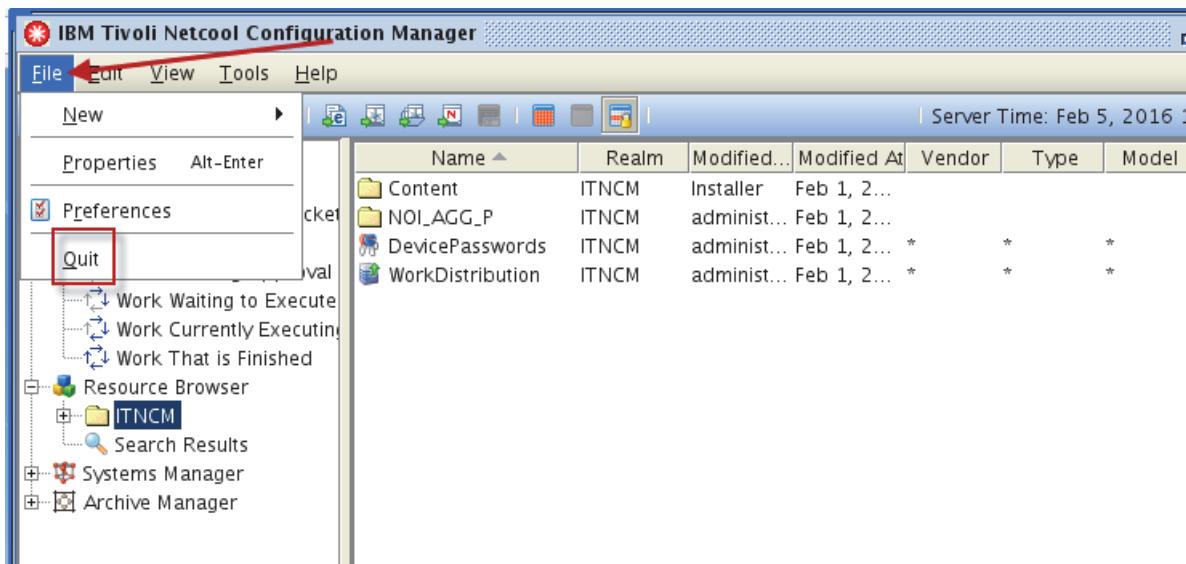
21. Select the option to not ask again, and click **Install**.



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.



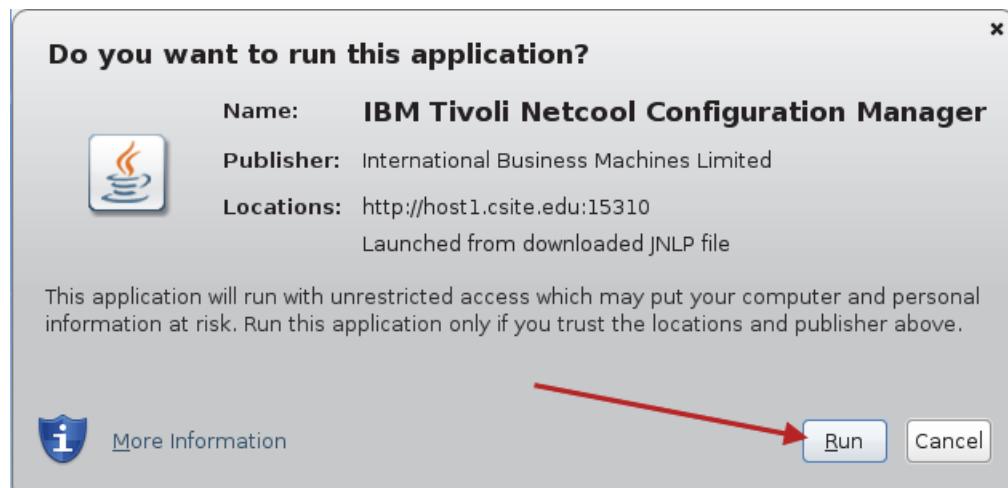
24. Click **OK** to confirm exit.



25. Click **ITNCM Compliance**.



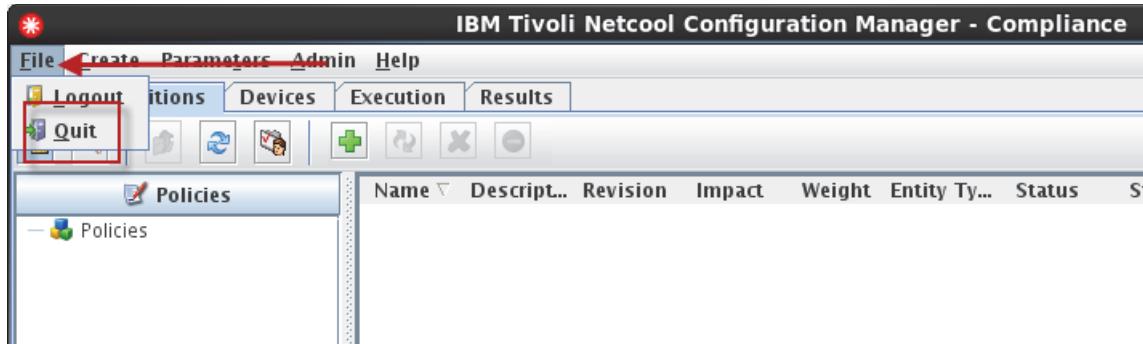
26. Click **Run**.



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.

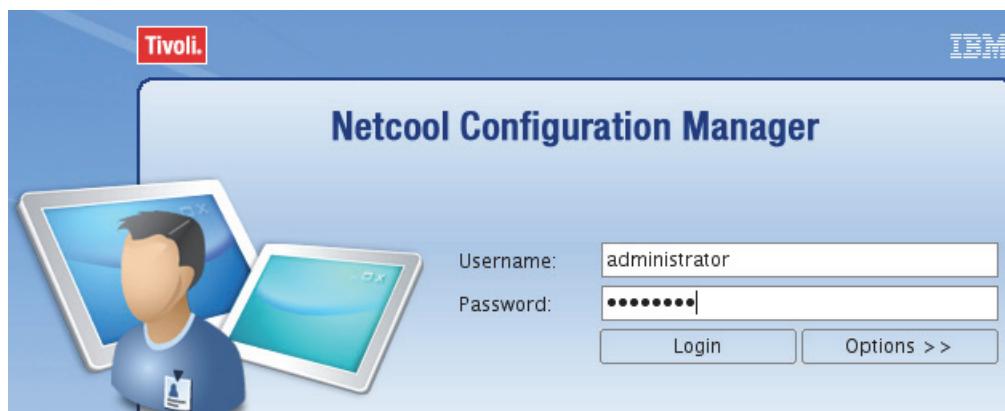


Configuring SNMP trap destination

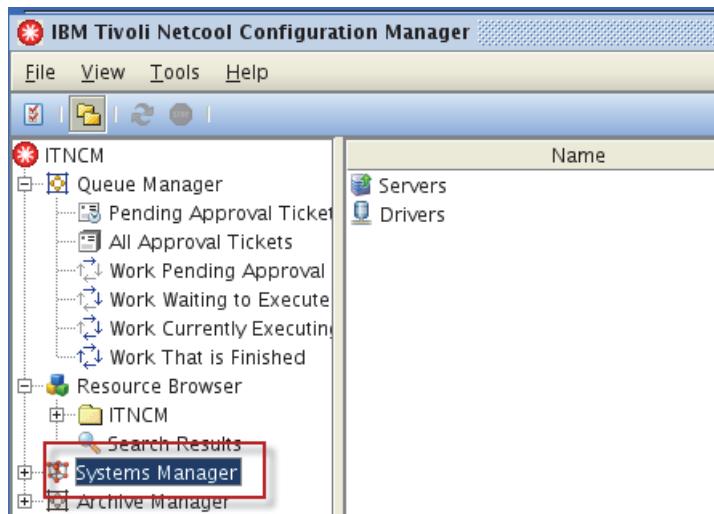
1. Click **ITNCM Webstart GUI**.



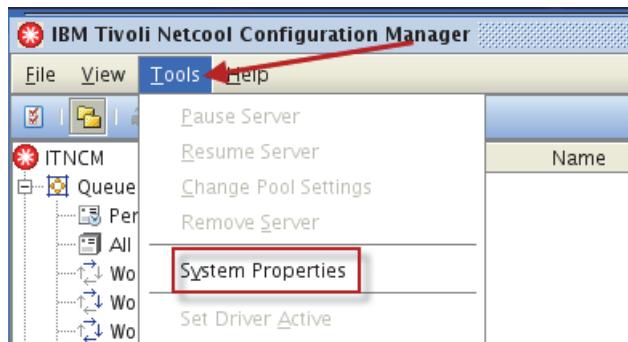
2. Enter **administrator** for the user name and **object00** for the password. Click **Login**.



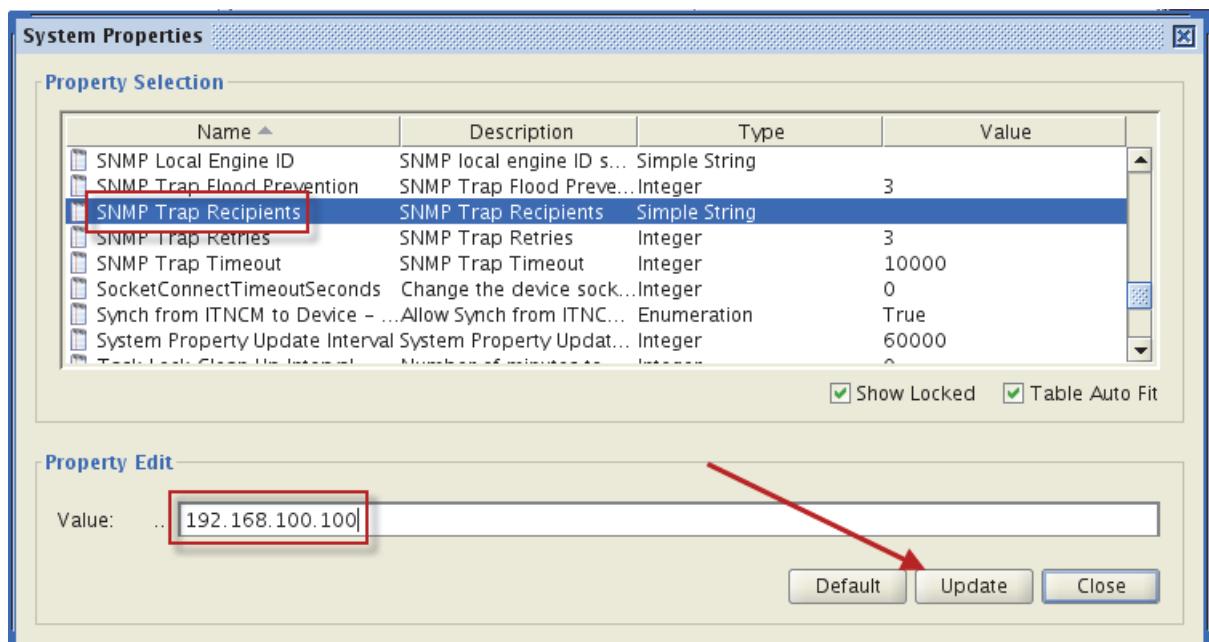
3. Click **Systems Manager** to select it.



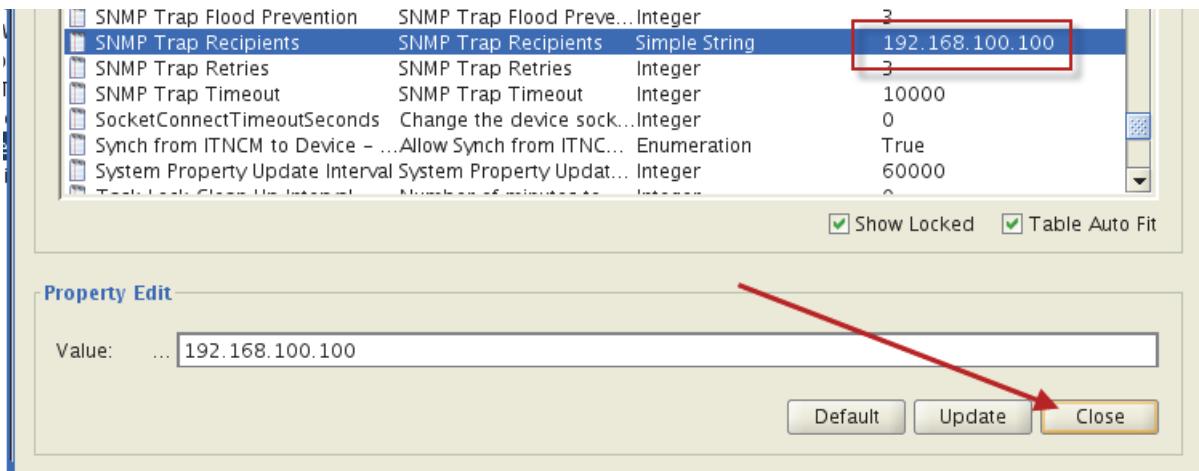
4. Click **Tools**, and select **System Properties**.



5. Click **SNMP Trap Recipients** to select it. Enter **192.168.100.100** for the value. Click **Update**.



- Verify that the value is correct. Click **Close**.



Updating the Work Distribution resource

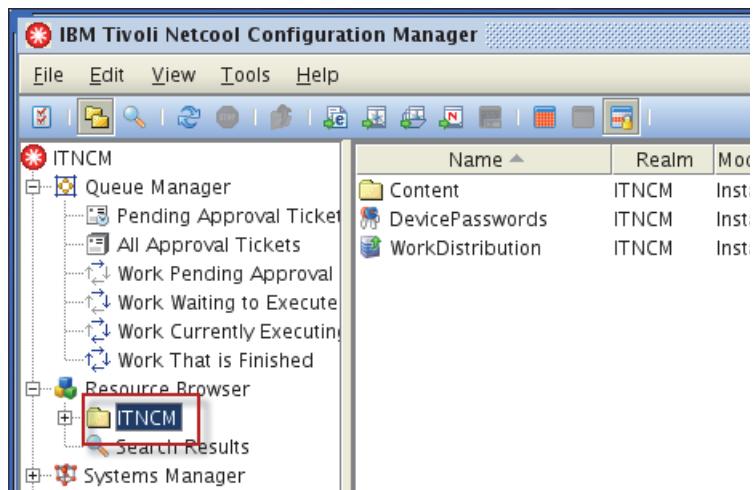
- Determine the value for the Server ID.

```
cat /opt/IBM/ncm/ITNCM.properties | grep ServerName
```

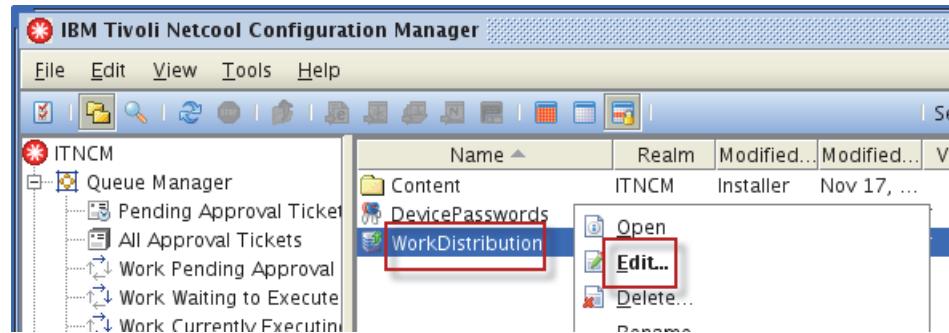
AdminManager/ServerName=**Worker1**

Note: The value for the Server ID is defined during installation of Netcool Configuration Manager.

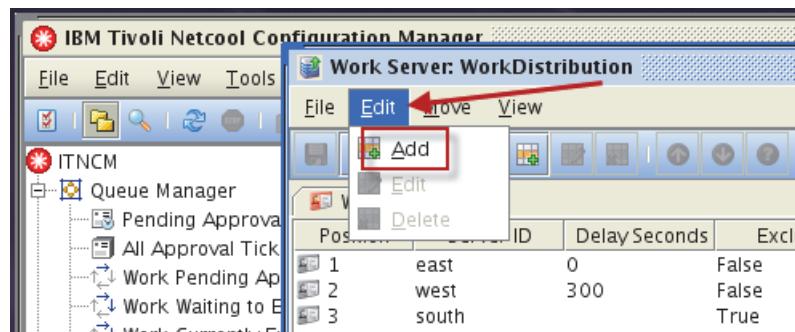
- Under **Resource Browser**, click **ITNCM** to select it.



3. Click **WorkDistribution** to select it, right-click and select **Edit**.

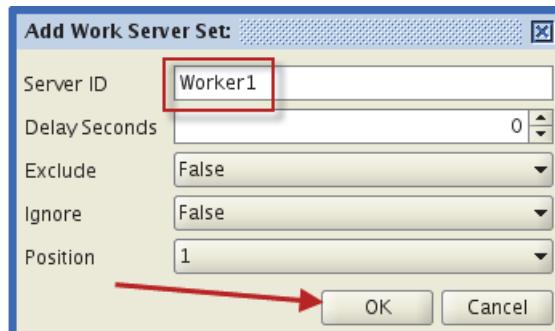


4. Click **Edit** and select **Add**.

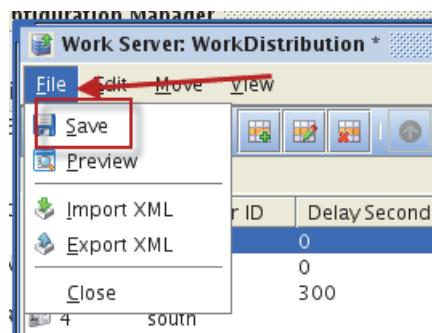


Note: None of the current entries are required. You can select one of the existing ones and modify it or create a new entry.

5. Enter **Worker1** and click **OK**.



6. Click **File** and select **Save**.

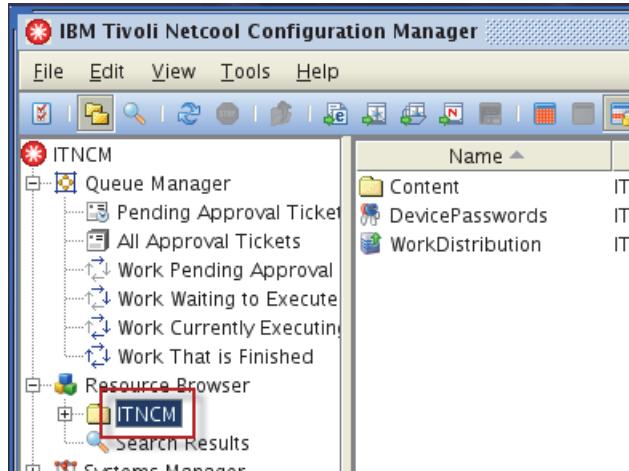


7. Click **File** and select **Close**.

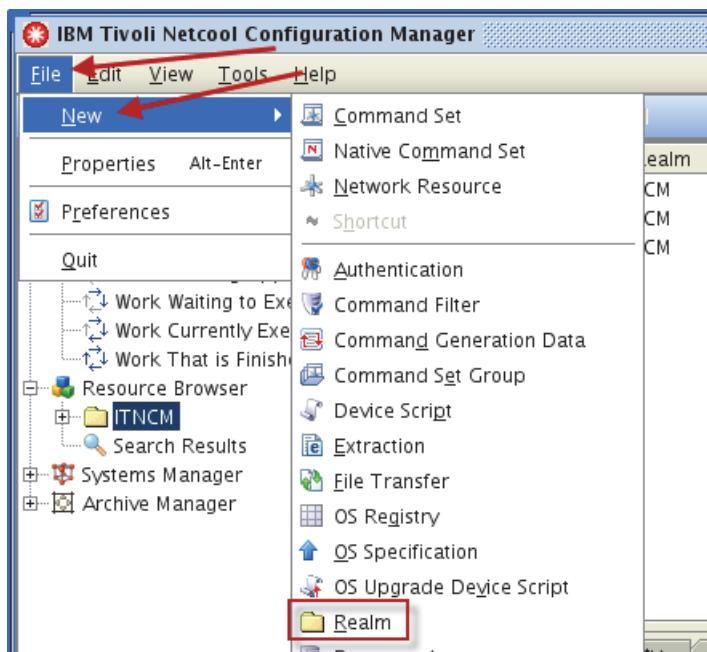
Creating resources to support device import

The following steps configure various Netcool Configuration Manager objects that are used for device import.

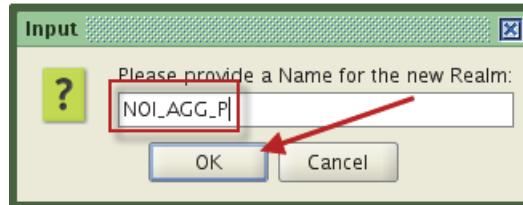
1. Under **Resource Browser**, click **ITNCM** to select it.



2. Click **File**, **New**, and select **Realm**.

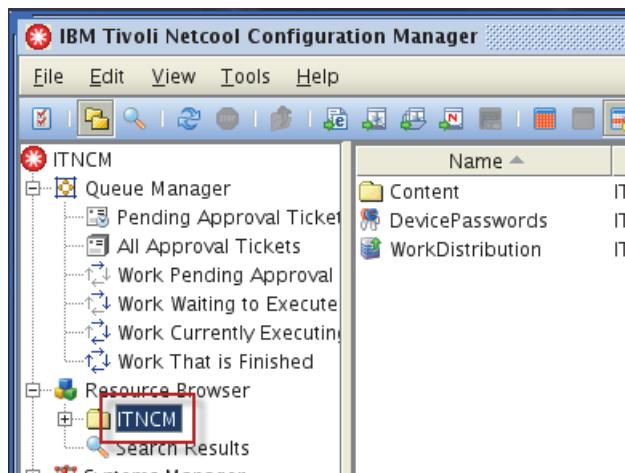


3. Enter NOI_AGG_P for the realm name and click OK.

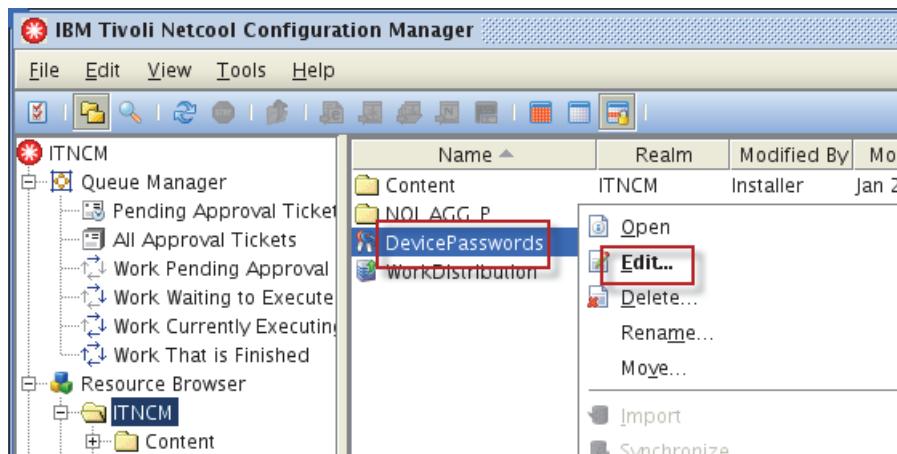


Hint: The realm name can be any valid value. If you use the same value as the Network Manager domain name, it can potentially avoid confusion.

4. Under Resource Browser, click ITNCM to select it.

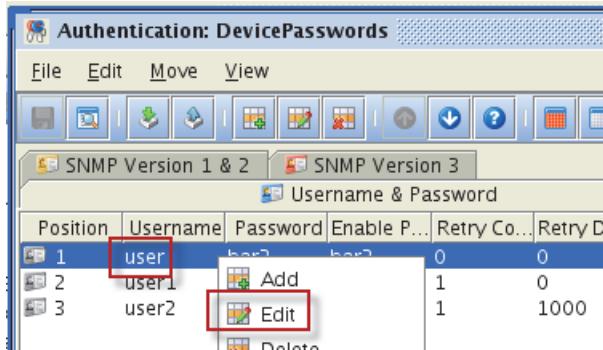


5. Click DevicePasswords to select it, right-click and select Edit.



Important: Later in this course, you discover devices in a simulated network. The following steps describe how to configure credentials that Netcool Configuration Manager uses to discover and access those simulated devices.

6. Click the entry for **user** to select it, right-click and select **Edit**.



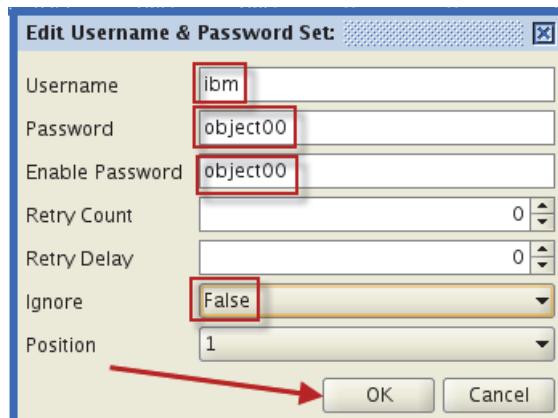
7. Enter the following values, and click **OK**.

Username: **ibm**

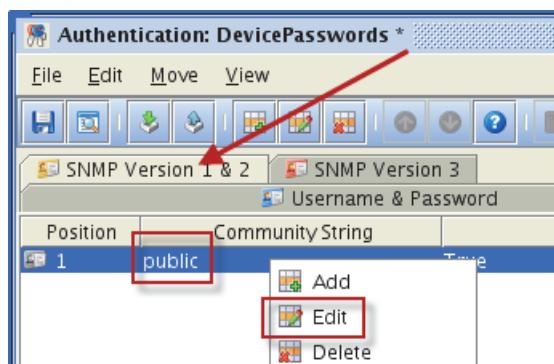
Password: **object00**

Enable Password: **object00**

Ignore: **False**



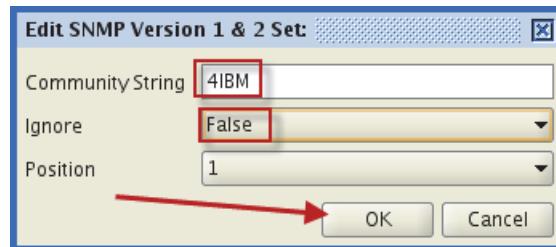
8. Click the SNMP Version 1 & 2 tab. Click the entry for **public** to select it. Right-click and select **Edit**.



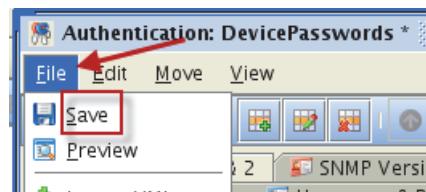
9. Enter the following values, and click **OK**.

Community String: **4IBM**

Ignore: **False**

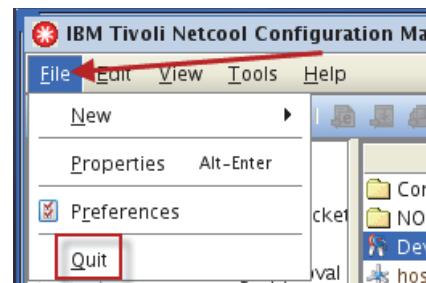


10. Click **File**, and select **Save**.



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.

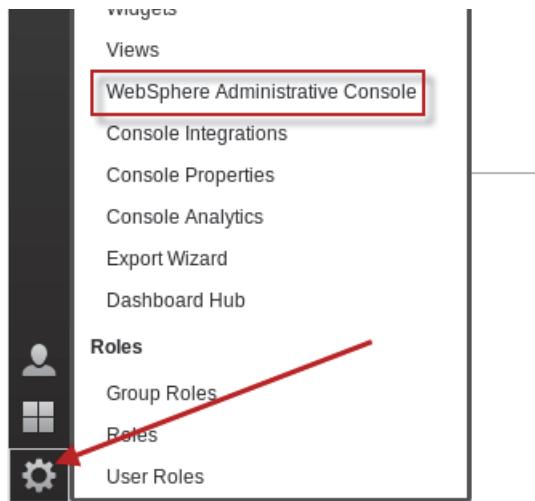
```
cd /opt/IBM/JazzSM_ncm/profile/config/cells/JazzSMNode01Cell/wim/config  
cp wimconfig.xml /home/netcool/wimconfig.xml_tncm
```



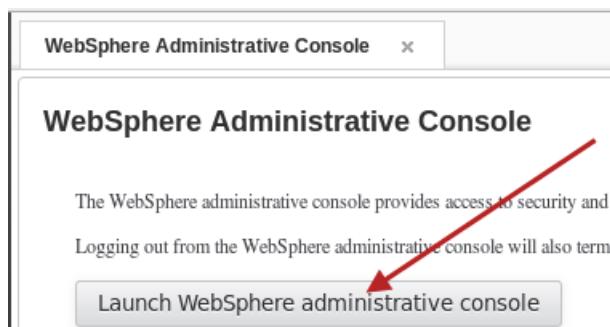
Important: If any of the following configuration steps fail, you can recover the original configurations by copying the saved files back to the original locations and restarting Dashboard Application Services Hub and the presentation server.

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**.



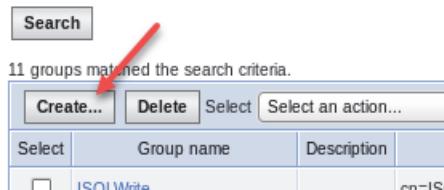
5. Click **Launch WebSphere administrative console**.



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 .

9. Click **Close**.



10. Click **Create**.



11. Enter **IntellidenUser** for the name, click **Create**.

* Group name

Description

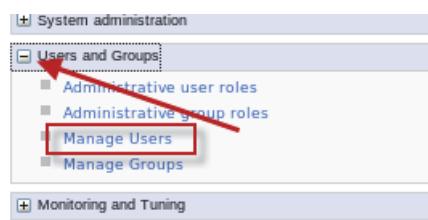


Important: Enter the group name exactly .

12. Click **Close**.



13. Expand **Users and Groups**. Select **Manage Users**.



14. Click **Create**.



15. Create a user.

- 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
Group name

* Search for *

* Maximum results
100

Search

17. Select **IntellidenAdminUser** and click **Add**.

Search by
Group name

* Search for *

* Maximum results
100

Search

Mapped To

< Add

Available

- ImpactAdmin
- IntellidenAdminUser**
- Netcool_Admin
- Netcool_User

18. Select **IntellidenUser** and click **Add**. Click **Close**.

Search by
Group name

* Search for *

* Maximum results
100

Search

Mapped To

IntellidenAdminUser

< Add

Available

- ImpactAdmin
- IntellidenUser**
- Netcool_Admin
- Netcool_User
- NetcoolAdmin

19. Click **Create**.

20. Click **Create Like**.



21. Create a user.

- 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, there are two buttons: "Create" and "Cancel". A red arrow points to the "Create" button.



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.

- 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**.

* User ID
observer
* First name
TNCM Observer
* Last name
User
E-mail
* Password

* Confirm password

25. Click **Search**.

Search by
Group name
* Search for
* Maximum results
100
Search

26. Select **IntellidenUser** and click **Add**. Click **Close**.

Search by
Group name
* Search for
* Maximum results
100
Search
Mapped To
< Add
Available
ImpactAdmin
IntellidenAdminUser
Netcool_Admin
Netcool_User

27. Click **Create**.

28. Click **Create Like**.



29. Create a user.

- 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**.

*User ID
operator

*First name
TNCM Oper

*Last name
User

E-mail

*Password

*Confirm password

Create → Cancel



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	

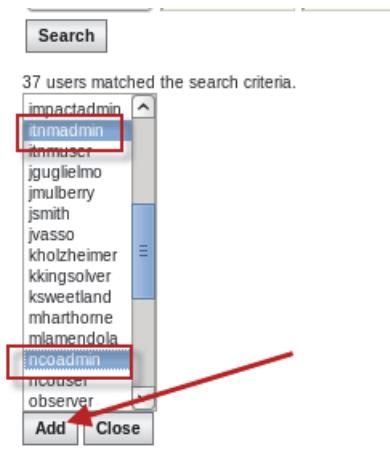
- Select the **Members** tab. Click **Add Users...**



- Click **Search**.

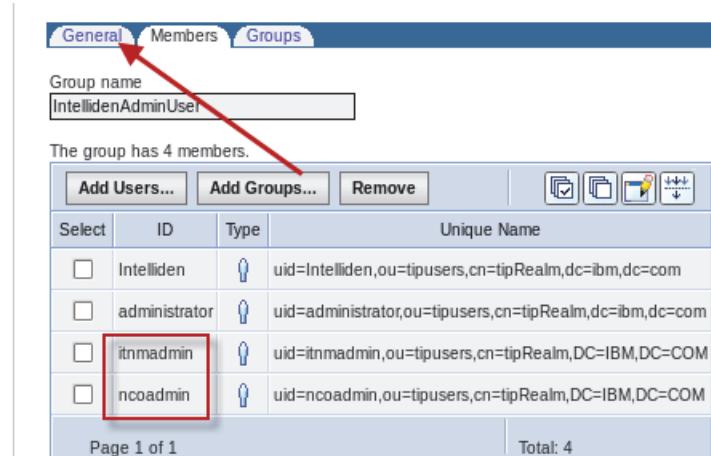


- Select **itnadmin**. Hold the Ctrl key and select **ncoadmin**, and click **Add**.



- Click **Close**.

- Verify that the user names appear, and click **General**.



- 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=tipgro
<input type="checkbox"/>	IntellidenAdminUser	cn=IntellidenAdminUser,ou
<input type="checkbox"/>	IntellidenUser	cn=IntellidenUser,ou=tipgrc

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. Use the Ctrl key to select these users, then click **Add**.

- itnmadmin
- itnmuser
- ncoadmin
- ncouser

37 users matched the search criteria.

impactadmin
itnmadmin
itnmuser
jguglielmo
jmulberry
jsmith
jvasso
kholzheimer
kkingsolver
ksweetland
mharthorne
mlamendola
ncoadmin
ncouser
observer

Add Close

13. Click **Close**.

14. Verify that the user names are shown, and click **General**.

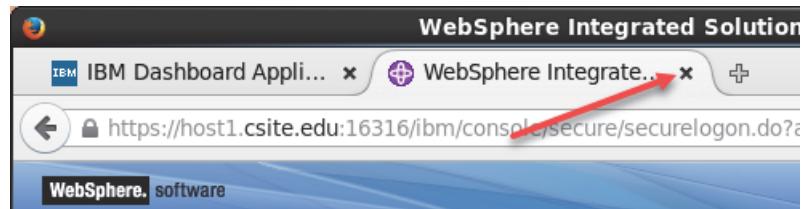
The group has 8 members.

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 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

Page 1 of 1 Total: 8

15. Click **OK** to save the group changes.

16. Close the WebSphere administrative console browser tab.



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**.

Group ID:
Intelliden*

Number of results to display:
20

Search

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
ncp_rest_api

6. Verify that the roles are present.

Group Name	Roles
IntellidenAdminUser	ncp_rest_api, IntellidenAdminUser, ncmConfigChange, ncmConfigEdit, nc

7. Select **IntellidenUser**.

IntellidenAdminUser	IntellidenAdminUser, ncmConfigChange ncmDashService, IntellidenUser, ncmlD ncmConfigViewing
IntellidenUser	

8. Select the following roles, and click **Save**.

IntellidenUser
ncmActivityViewing
ncmConfigViewing
ncmDashService
ncp_rest_api

9. Verify that the roles are present.



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. Add 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**.

User account repository

Realm name	getRealm
Current realm definition	Standalone custom registry
Available realm definitions	Federated repositories <input type="button" value="Configure..."/> <input type="button" value="Set as current"/>

- c. Click **Configure**.

User account repository

Realm name	getRealm
Current realm definition	Standalone custom registry
Available realm definitions	Federated repositories <input type="button" value="Configure..."/> <input type="button" value="Set as current"/>

- d. Change the user name to **Intelliden**.

General Properties

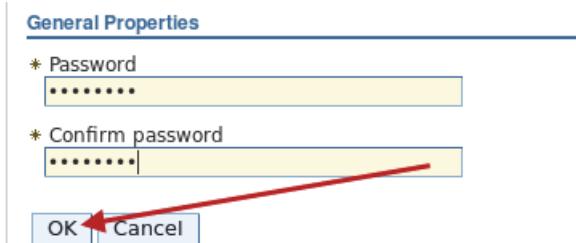
* Realm name	defaultWIMFileBasedRealm
* Primary administrative user name	Intelliden

Server user identity

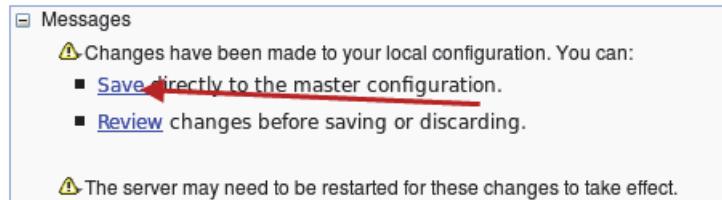
Automatically generated server identity

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

- f. Enter **object00** for the password, and click **OK**.



- g. Click **Save**.

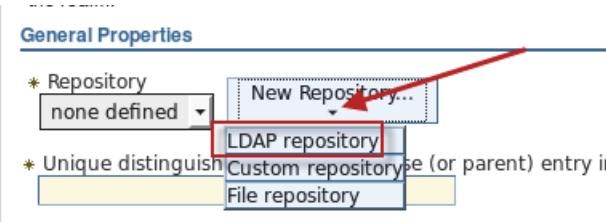


- h. Scroll down on the page to the *Repositories in the realm*, and click **Add repositories**.

Repositories in the realm:

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

- 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**.

General Properties

* 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.csuite.edu** Port **389**

Failover server used when primary is not available:

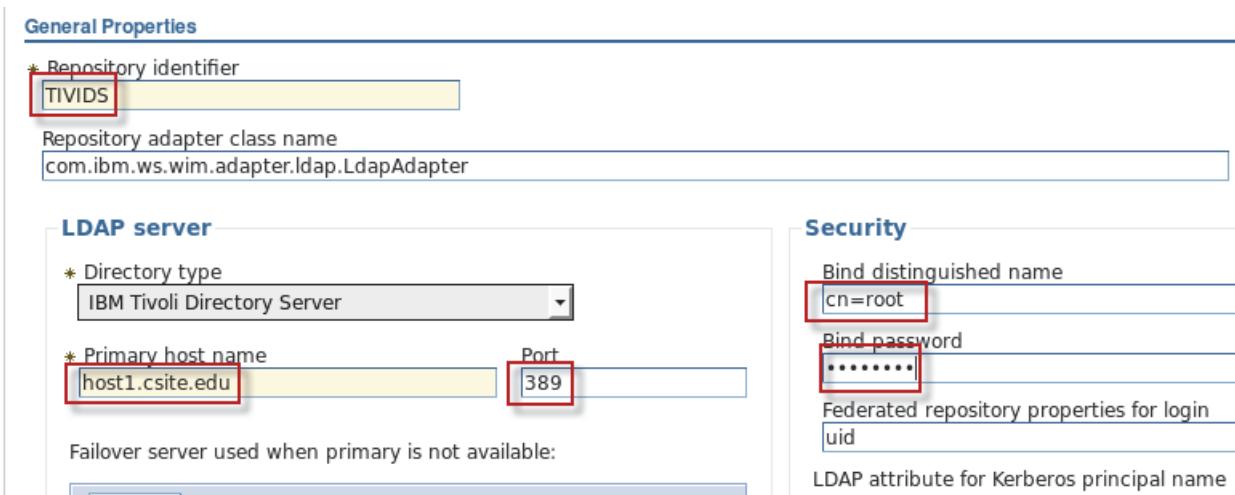
Security

Bind distinguished name **cn=root**

Bind password *********

Federated repository properties for login
uid

LDAP attribute for Kerberos principal name



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

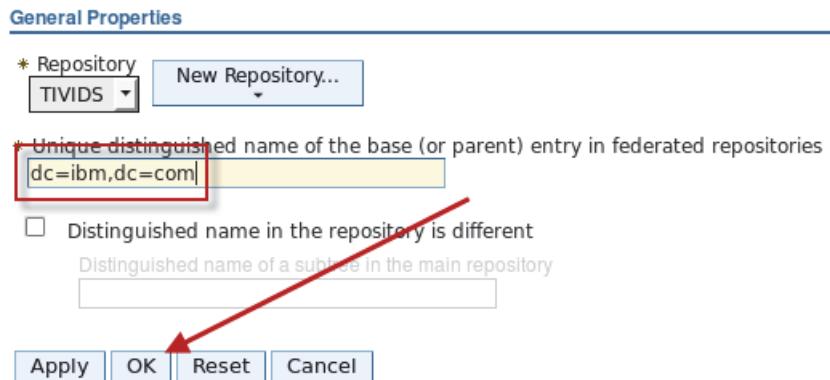
General Properties

* Repository **TIVIDS** New Repository...

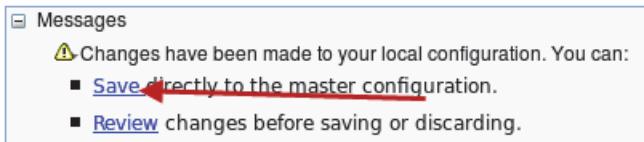
* Unique distinguished name of the base (or parent) entry in federated repositories **dc=ibm,dc=com**

Distinguished name in the repository is different
Distinguished name of a subtree in the main repository

Apply OK Reset Cancel



- 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. Define 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"/>	dc=ibm,dc=com	TIVIDS	LDAP:IDS
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	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"/>	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

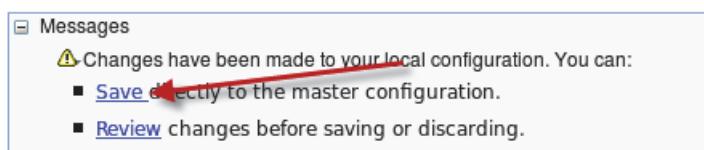
* Entity type

* 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 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:

- 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=defaultWIMFileBasedRealm	cn
OrgContainer	o=defaultWIMFileBasedRealm	o;ou;dc;cn
PersonAccount	o=defaultWIMFileBasedRealm	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.

- 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:		
Group	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn
OrgContainer	o=defaultWIMFileBasedRealm	o;oi
PersonAccount	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:		
Group	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn
OrgContainer	dc=ibm,dc=com	o;oi
PersonAccount	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

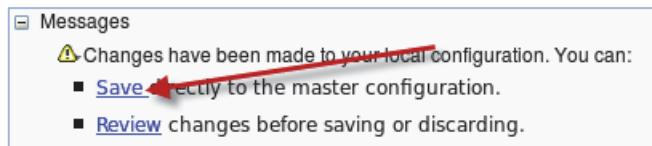
* Base entry for the default parent

* Relative Distinguished Name properties

- Verify that your environment looks like the following example.

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

- 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](#)

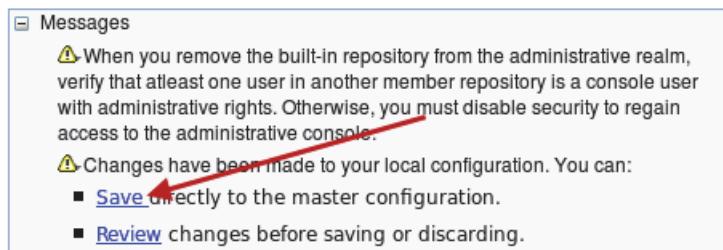
Entity Type ▾	Base Entry for the Default Parent ▾	Relative Distinguishing Name
You can administer the following resources:		
Group	ou=tipgroups,cn=tipRealm,DC=IBM,DC=COM	cn

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
<input type="checkbox"/>	dc=ibm,dc=com	TIVIDS	LDAP:IDS
<input checked="" type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

10. Click Save.



11. Click **Global security**.

The screenshot shows a blue header bar with the text "Global security". Below it is a section titled "Global security > Federated repositories". A red arrow points from the text "Click the arrow and select Federated repositories." to the "Federated repositories" link.

12. Click the arrow and select **Federated repositories**.

The screenshot shows a "User account repository" configuration page. In the "Available realm definitions" section, there is a dropdown menu with "Federated repositories" selected. A red arrow points from the text "Click the arrow and select Federated repositories." to the dropdown menu.

13. Click **Set as current**.

The screenshot shows the same "User account repository" configuration page. The "Available realm definitions" dropdown is still set to "Federated repositories". A red arrow points from the text "Click Set as current." to the "Set as current" button.

14. Click **Apply**.

15. Click **Save**.

The screenshot shows a "Messages" panel with several items:

- A warning message about restrict access to local resources.
- A note about saving changes.
- A note about changes to local configuration with options to save directly or review.
- A note about restarting the server.

A red arrow points from the text "Click Save." to the "Save" link in the second item.

16. Log out of the administrative console.

17. Close the Firefox browser.

18. Restart Netcool Configuration Manager.

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



Wait for the components to restart.

19. Open a Firefox browser and go to the following URL:

<https://host1.csite.edu:15316/ibm/console/logon.jsp>

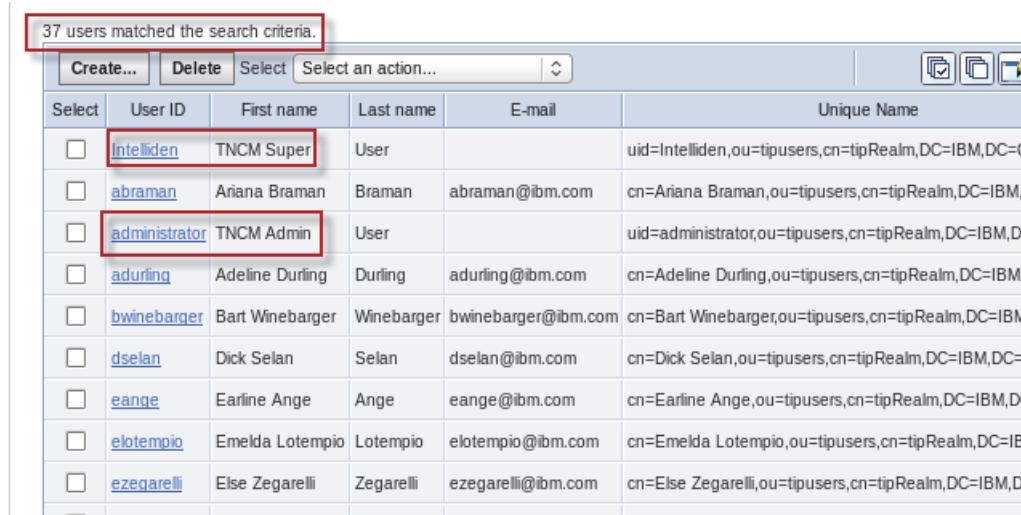
20. Log in as **Intelliden** with password **object00**.

21. Verify that the LDAP users are available within the presentation server.

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

A screenshot of the WebSphere Application Server administration console. The left sidebar shows a tree view with nodes like Welcome, Guided Activities, Servers, Applications, Services, Resources, Security, Environment, System Administration, Users and Groups, Administrative user roles, Administrative group roles, Manage Users, and Manage Groups. A red arrow points from the text above to the "Manage Users" link under the "Users and Groups" node. To the right, the main panel displays a "Welcome" message and a "Suite Name" section with "WebSphere Application".

b. Observe the list of users.



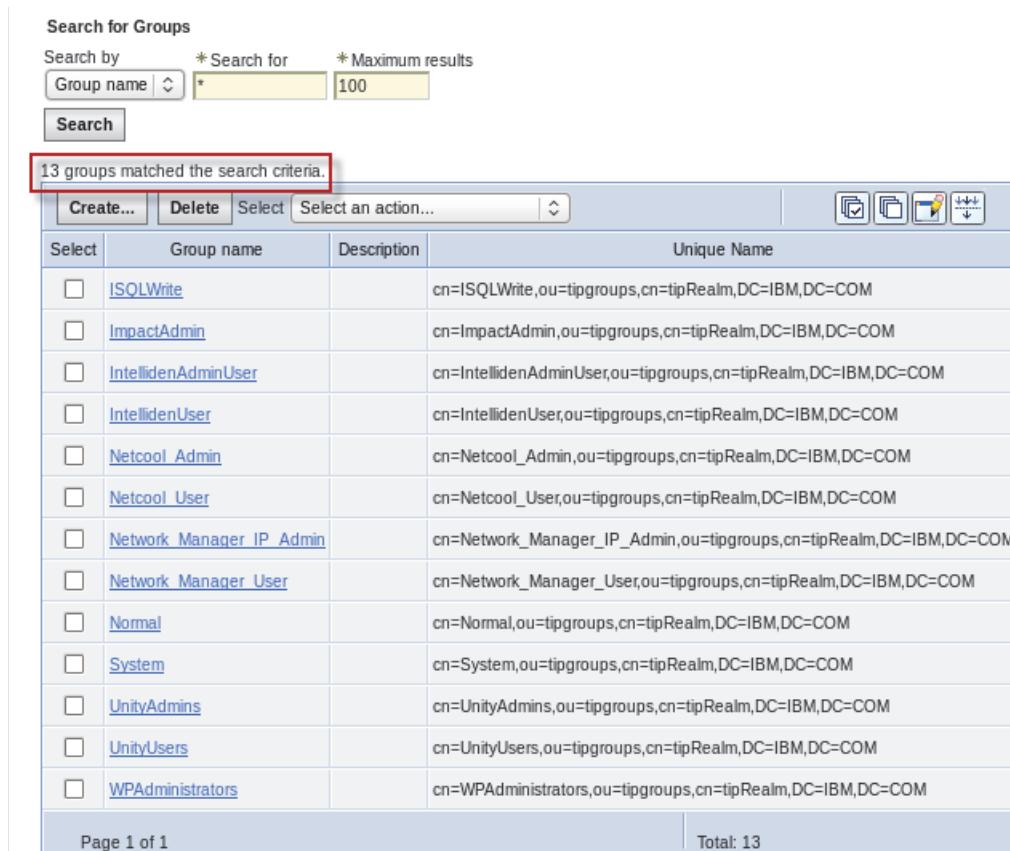
37 users matched the search criteria.

Select	User ID	First name	Last name	E-mail	Unique Name
<input type="checkbox"/>	Intelliden	TNCM Super	User		uid=Intelliden,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	abraman	Ariana Braman	Braman	abraman@ibm.com	cn=Ariana Braman,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	administrator	TNCM Admin	User		uid=administrator,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	adurling	Adeline Durling	Durling	adurling@ibm.com	cn=Adeline Durling,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	bwinebarger	Bart Winebarger	Winebarger	bwinebarger@ibm.com	cn=Bart Winebarger,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	dselan	Dick Selan	Selan	dselan@ibm.com	cn=Dick Selan,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	eange	Earline Ange	Ange	eange@ibm.com	cn=Earline Ange,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	elotempio	Emelda Lotempio	Lotempio	elotempio@ibm.com	cn=Emelda Lotempio,ou=tipusers,cn=tipRealm,DC=IBM,DC=COM
<input type="checkbox"/>	ezegarelli	Else Zegarelli	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.



Search for Groups

Search by * Search for * Maximum results
 Group name * 100

Search

13 groups matched the search criteria.

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

Page 1 of 1 Total: 13

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**.



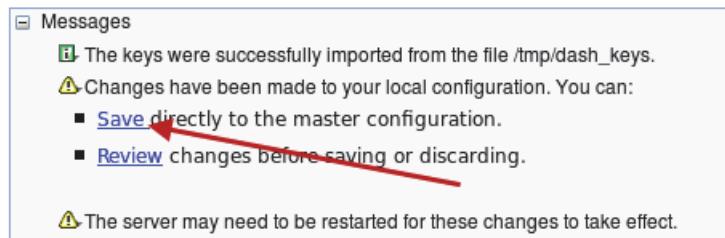
2. Click **LTPA**.

A screenshot of the 'Global security' configuration page. The 'Global security' tab is selected at the top. The 'Administrative security' section contains a checked checkbox for 'Enable administrative security' and three links: 'Administrative user roles', 'Administrative group roles', and 'Administrative authentication'. The 'Application security' section is partially visible. The 'Authentication' section on the right shows a radio button for 'LTPA' which is selected, indicated by a red arrow. Other options include 'Kerberos and LTPA' and 'Kerberos configuration'.

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'.

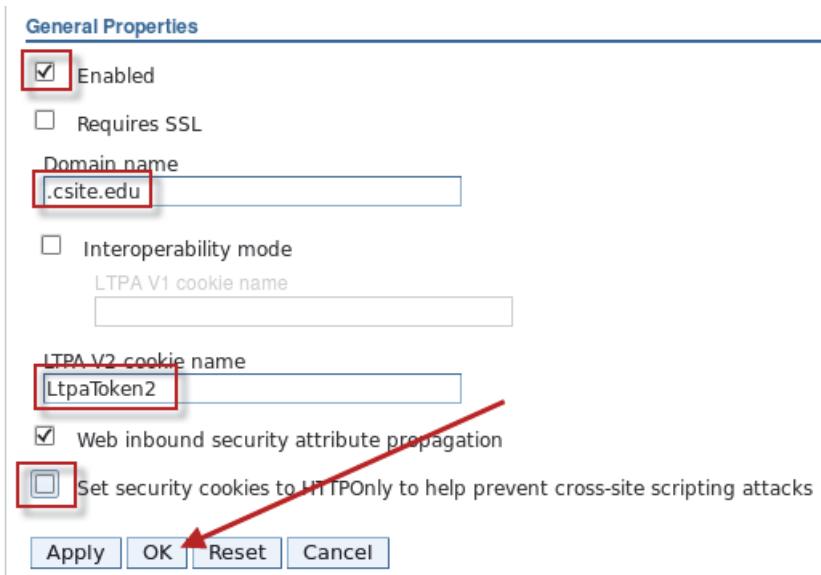
4. Click **Save**.



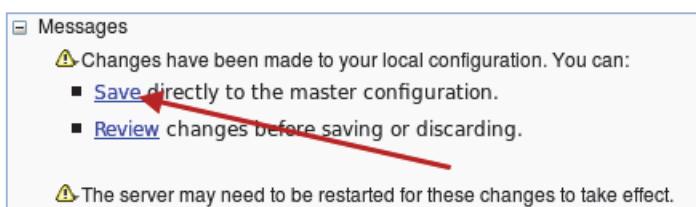
5. Expand **Web and SIP security**. Select **Single sign-on (SSO)**.



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**.

Related Items	
Applications between r establishing tablish secure ecified for the	<ul style="list-style-type: none"> SSL configurations Dynamic outbound endpoint SSL configurations Key stores and certificates 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"/>	NodeDefaultKeyStore	Default key store for JazzSMNode01	(0) (n)
<input type="checkbox"/>	NodeDefaultTrustStore	Default trust store for JazzSMNode01	(0) (n)

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

Additional Properties	
<ul style="list-style-type: none"> Signer certificates Personal certificates Personal certificate 	

e. Click **Retrieve from port**.



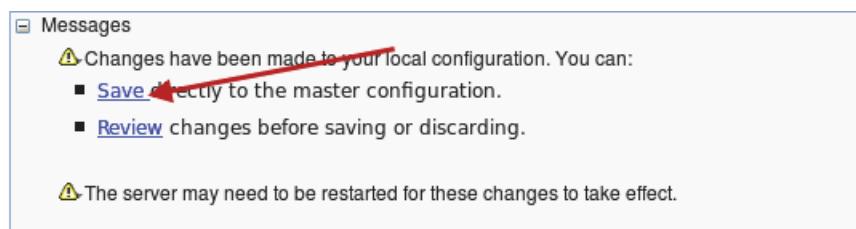
f. Enter **host1.csuite.edu** for the host. Enter **16311** for the port. Enter **DASH_SSL** for the alias.
Click **Retrieve signer information**.

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

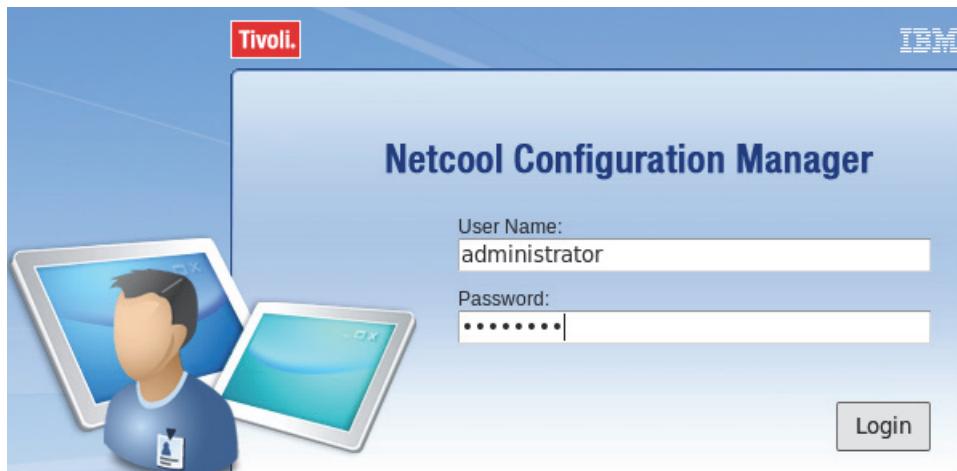
You added Netcool/OMNIbus and Network Manager users to Configuration Manager groups in a previous step. The group access grants access to certain Configuration Manager features. The following steps configure the user access rights within Configuration Manager.

1. Open a Firefox browser.

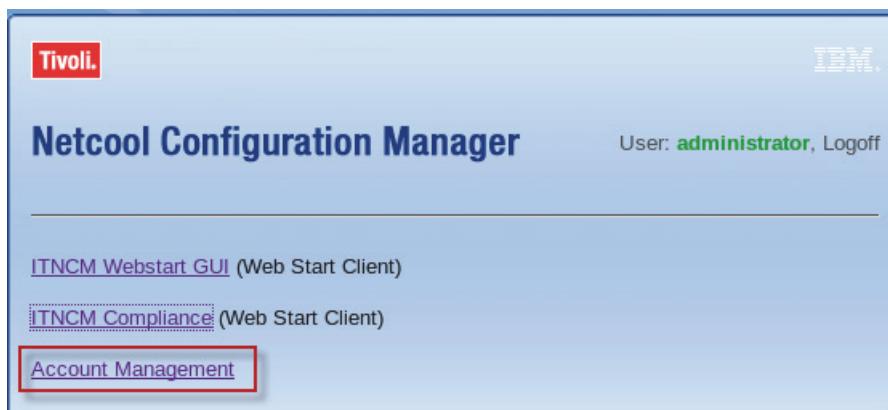
2. Connect to the following URL:

```
http://host1.csite.edu:15310/security/login.jsp
```

3. Log in as **administrator** with password **object00**.



4. Select **Account Management**.



Hint: If you do not see the Account Management link, log in and change the URL to:
<http://host1.csite.edu:15310/intelliden.jsp>.

5. Observe the list of users.



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.

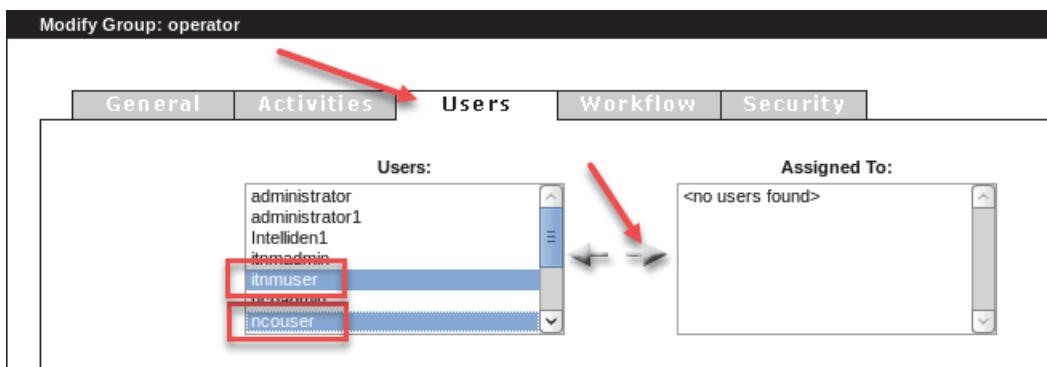


7. Select the **Security** tab.

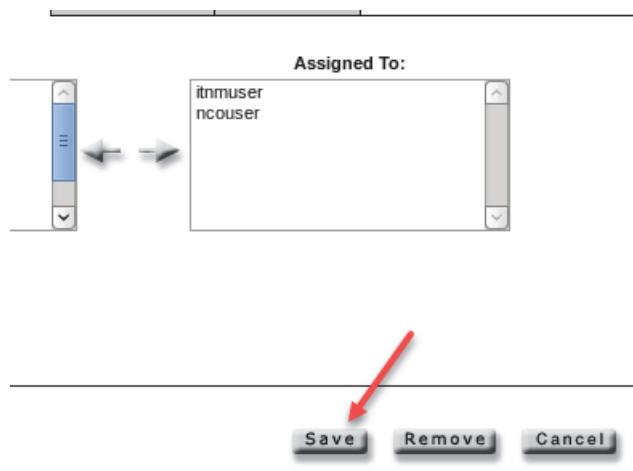
The screenshot shows the 'Modify Group: operator' dialog. At the top, there are tabs: General, Activities, Users, Workflow, and Security (which is highlighted with a red arrow). Below the tabs is a toolbar with buttons for Realm, Resource, and Content. The main area is a table titled 'Realm' with two rows: 'ITNCM' and 'ITNCM NOI AGG P'. Each row has five columns: View, Add, Modify, Delete, and All. Each column contains a checkbox, all of which are checked for both rows.

Users that belong to the operator group have full access rights to the ITNCM realm.

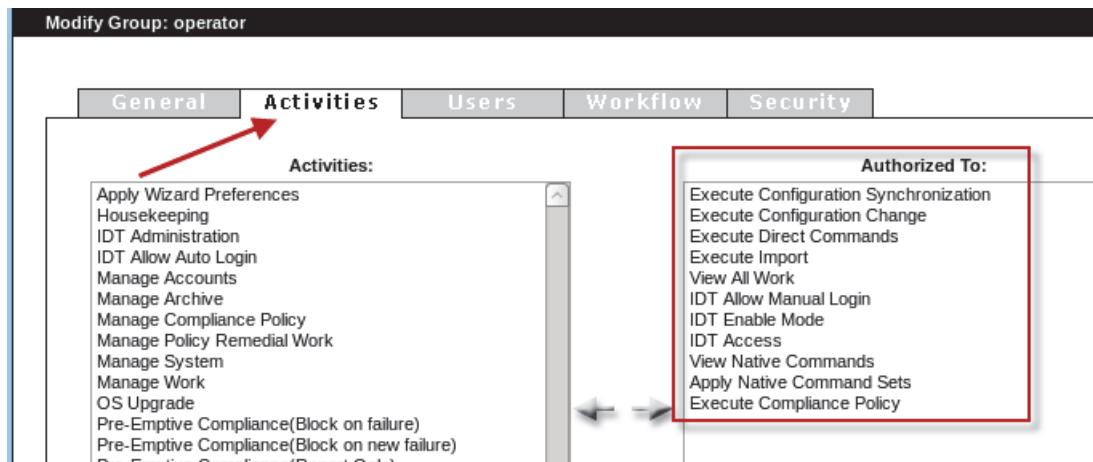
8. Select the **Users** tab.
9. Use the Ctrl key to select the **itnmuser** and **ncouser** users. Click the *right arrow* icon to add the users to the group.



10. Click **Save**.



11. Click the **Activities** tab.



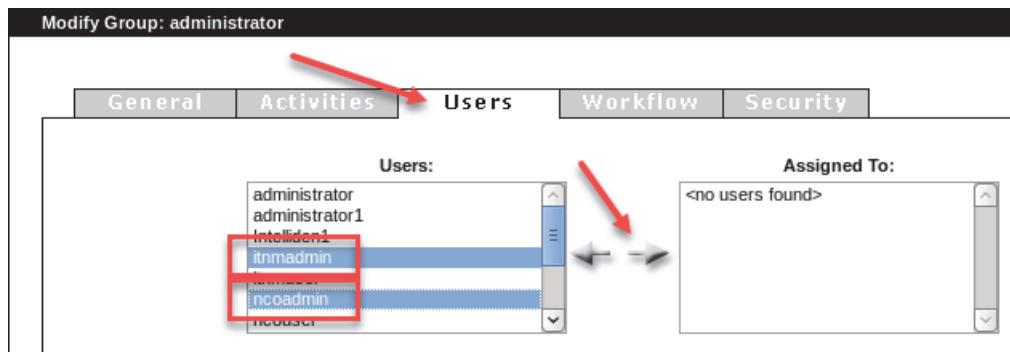
The members of the operator group are authorized to use these Configuration Management functions.

12. Click the **administrator** group.



13. Click the **Users** tab.

14. Use the Ctrl key to select the **itnmadmin** and **ncoadmin** users. Click the *right arrow* icon to add the users to the group.



15. Click **Save**.

16. Click the *running person* icon to log out.

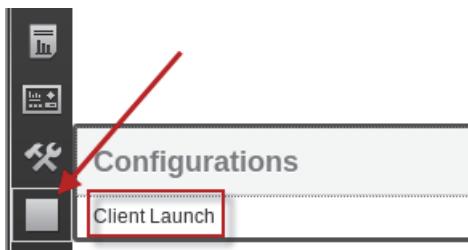


17. Close the Firefox browser.

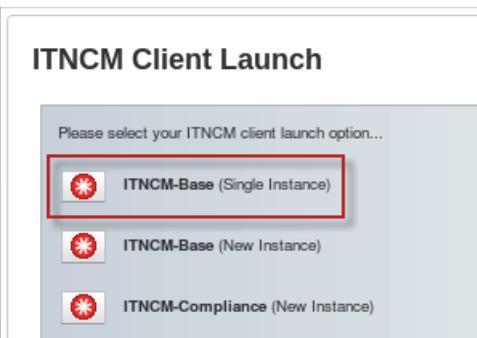
Verifying single sign-on

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

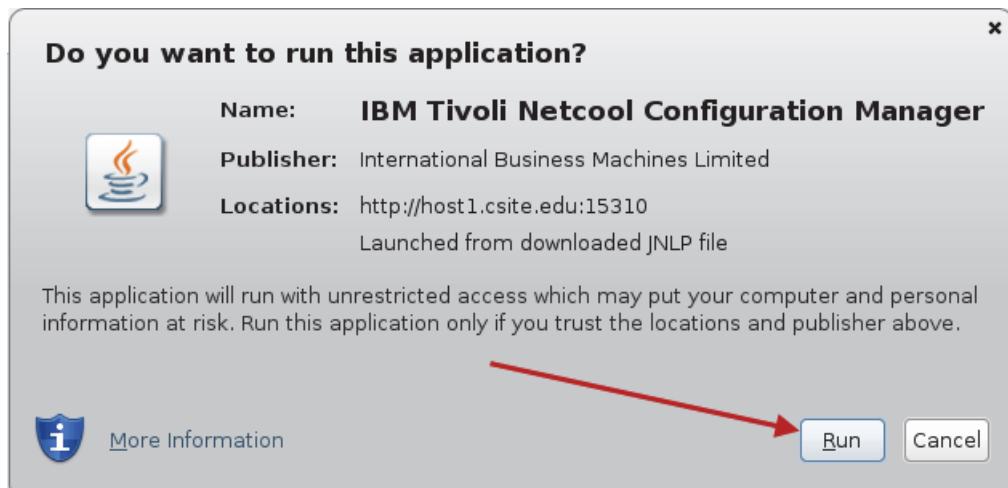
3. Click the indicated icon, and select Client Launch.



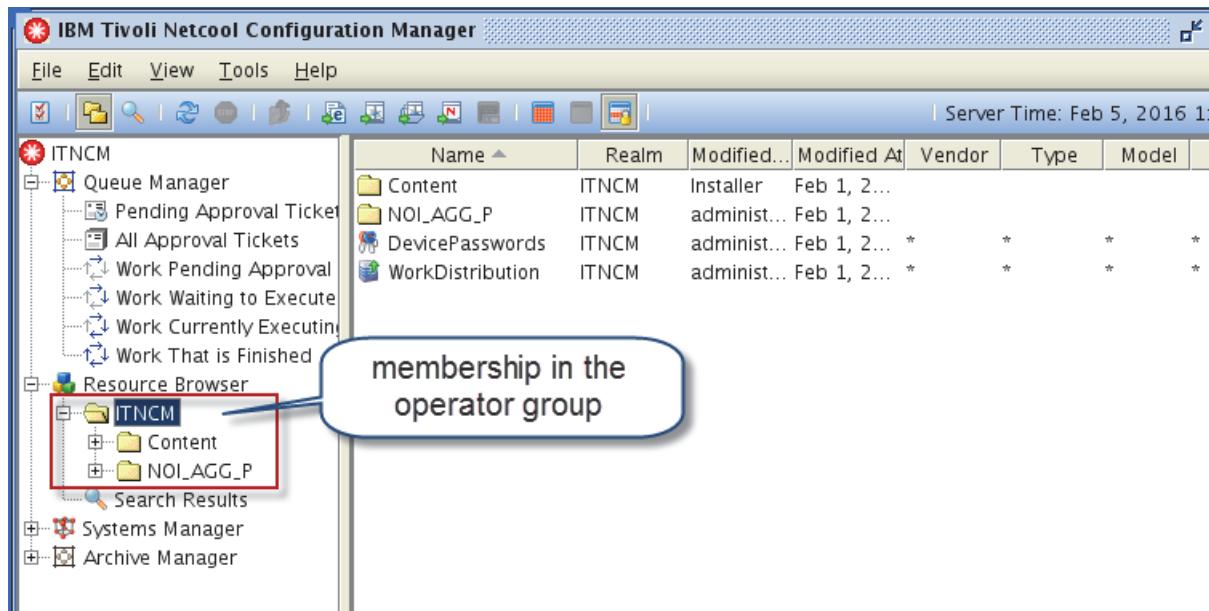
4. Click ITNCM-Base (Single Instance).



5. Click Run when prompted.

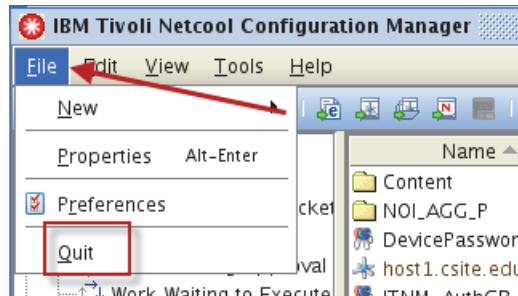


- Verify that the login is successful.

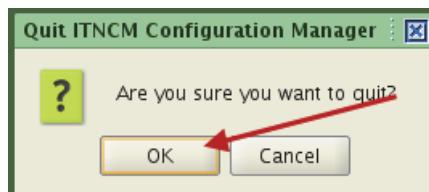


The ncoadmin user has access to the ITNCM realm because the user belongs to the operator group.

- Click **File** and select **Quit** to exit the client.



- Click **OK** to confirm.



- Log out of Dashboard Application Services Hub.

Installing sample policy packs

The following steps describe how to install a collection of pre-built compliance policies, and the 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.

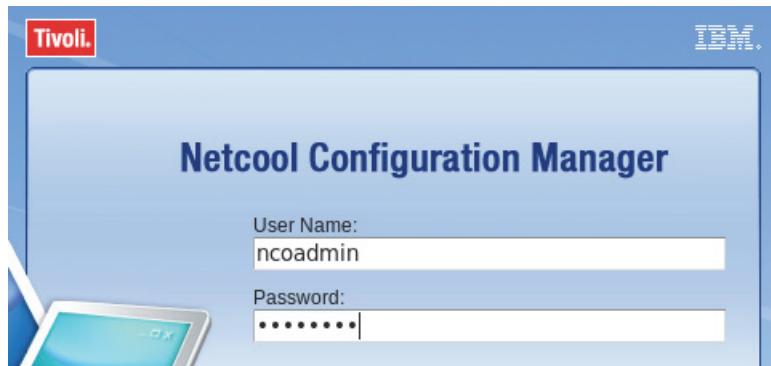
11. Grant access to the policies.

a. Open a Firefox browser.

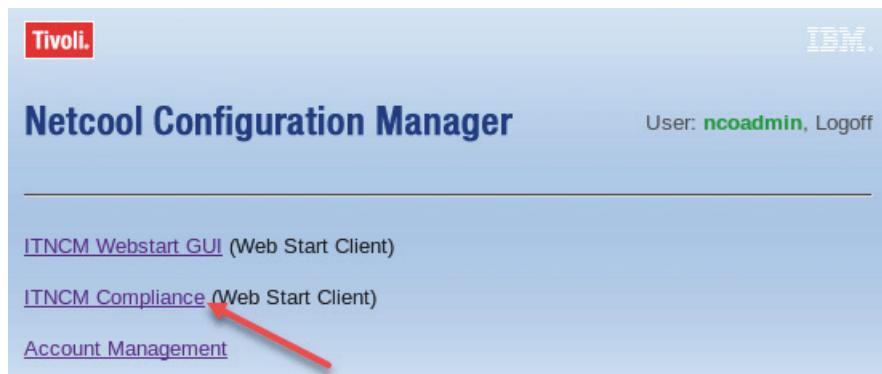
b. Connect to the following URL:

<http://host1.csite.edu:15310/security/login.jsp>

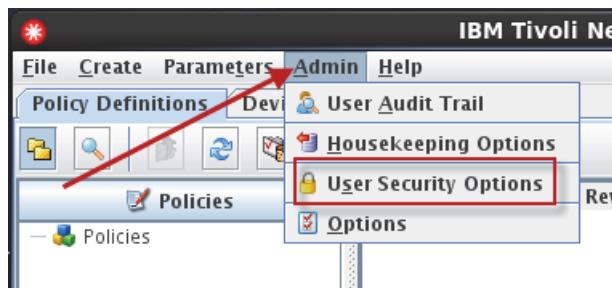
c. Log in as **ncoadmin** with password **object00**.



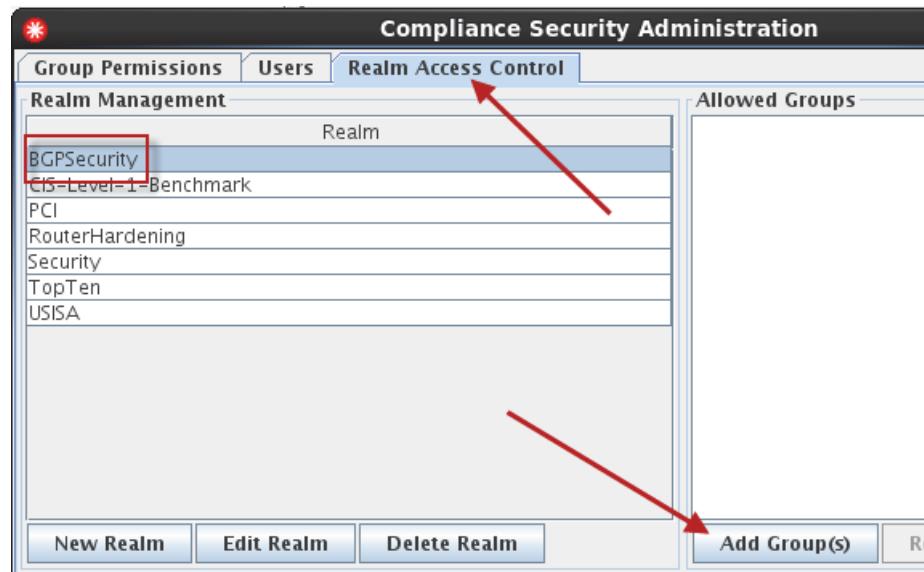
- d. Click **ITNCM Compliance**.



- e. Click **Run** when you are prompted.
f. Click **Admin**, and select **User Security Options**.

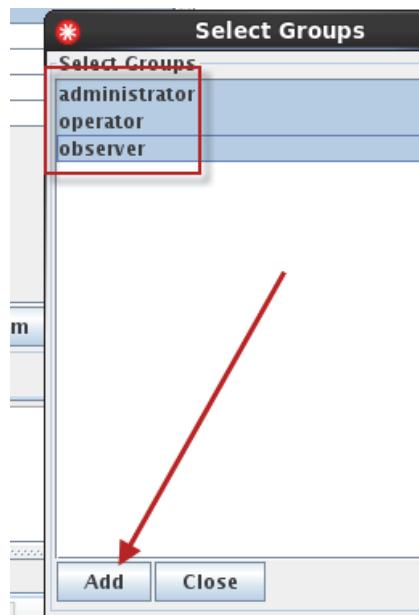


- g. Click the **Realm Access Control** tab.
h. Click **BGPSecurity** to select it.
i. Click **Add Group(s)**.



- j. Click **administrator** to select it.
k. Hold down the **Ctrl** key to select the **administrator**, **operator** and **observer** groups.

I. Click **Add**.



m. Verify that the three groups are added to the **BGPSecurity** realm.



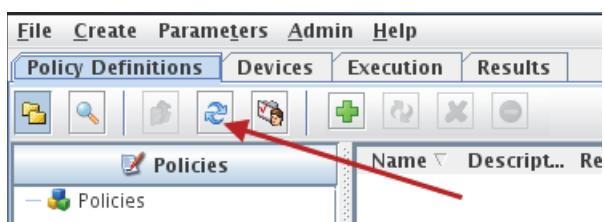
n. Repeat these steps to add the same groups to the other realms in the list.

o. Click **Close**.

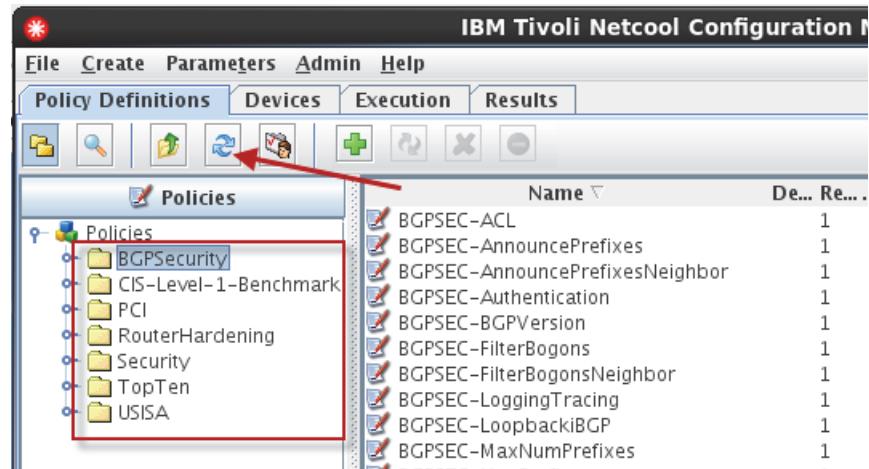


12. Verify access to the policies.

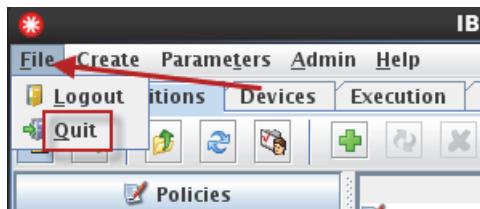
a. Click the icon with the *two blue arrows* to refresh the view.



The realms for the policy packs now appear in the list.



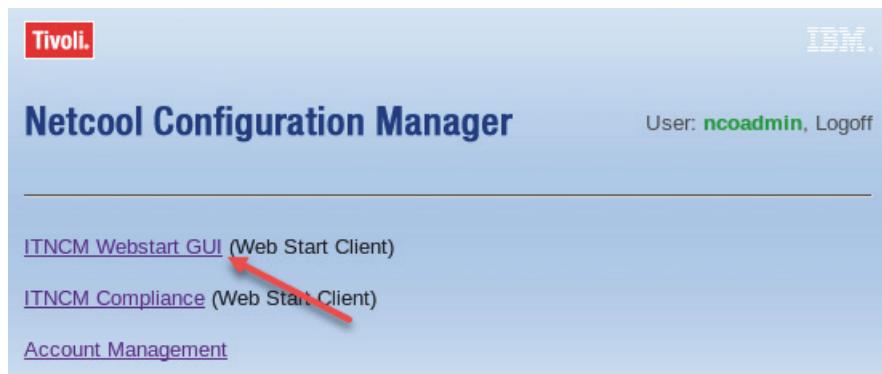
- b. Click **File** and select **Quit** to exit the compliance client.



Importing sample command sets

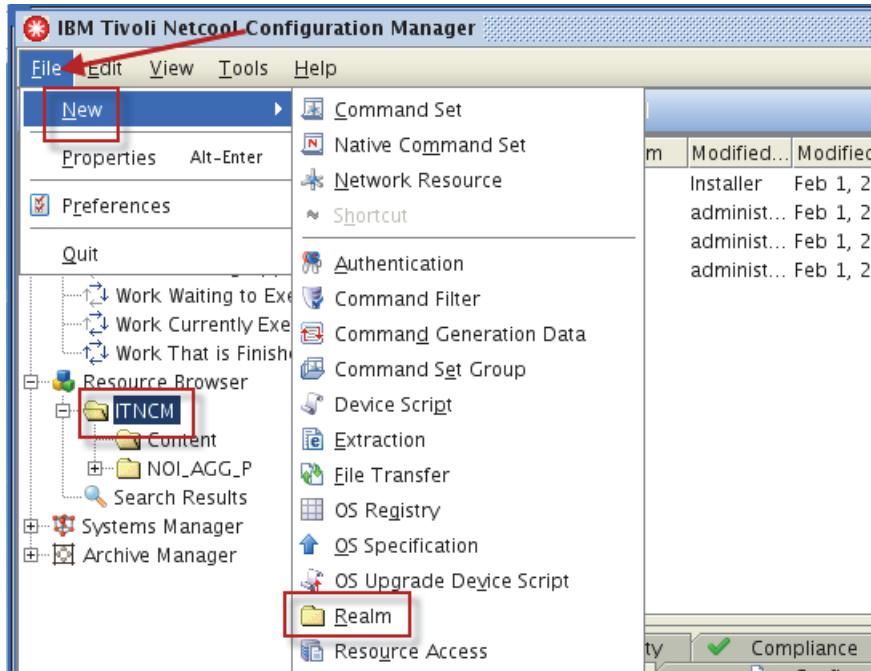
The workshop includes a small collection of sample command sets. The workshop compliance policies that you installed in the previous step reference these command sets.

1. Select **ITNCM Webstart GUI**.



2. Click **Run**.

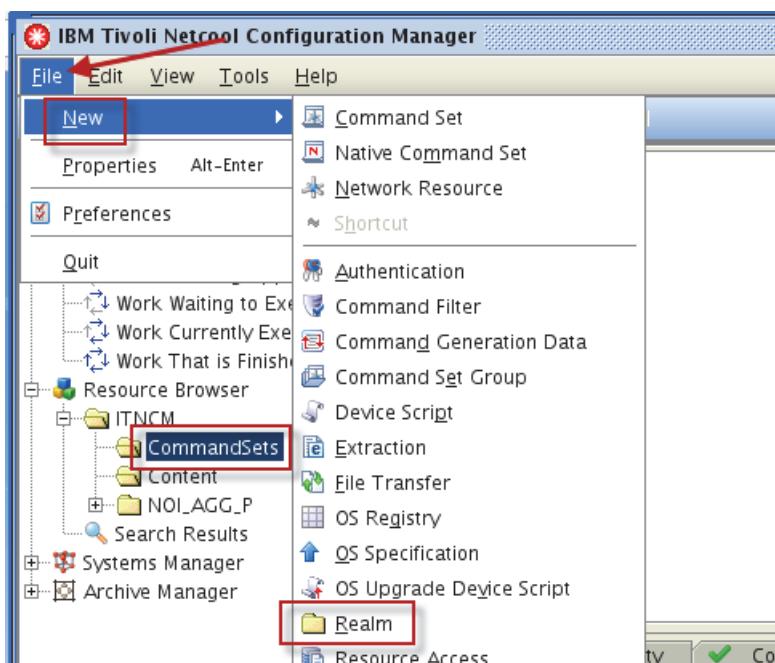
3. Under Resource Browser, click **ITNCM** to select it. Click **File**, and select **New > Realm**.



4. Enter **CommandSets** for the name, and click **OK**.



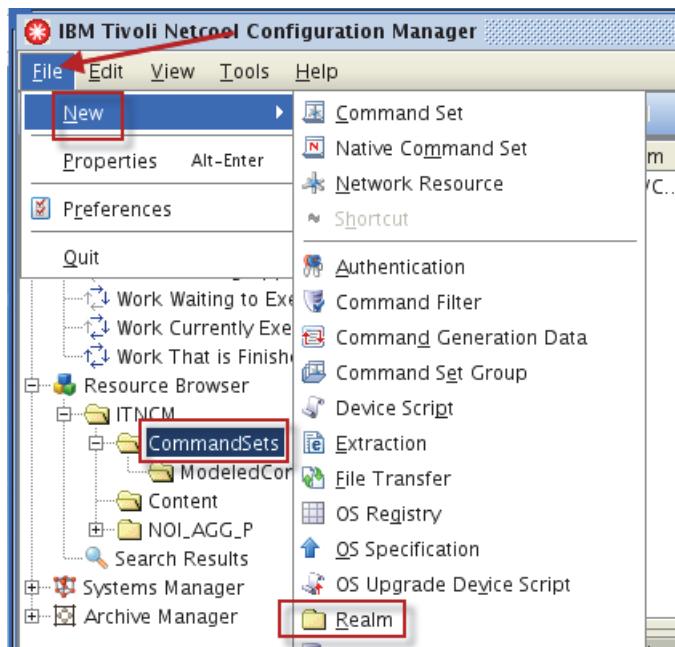
5. Under **ITNCM**, click **CommandSets** to select it. Click **File**, and select **New > Realm**.



6. Enter **ModeledCommands** for the name, and click **OK**.



7. Under ITNCM, click **CommandSets** to select it. Click **File**, and select **New > Realm**.

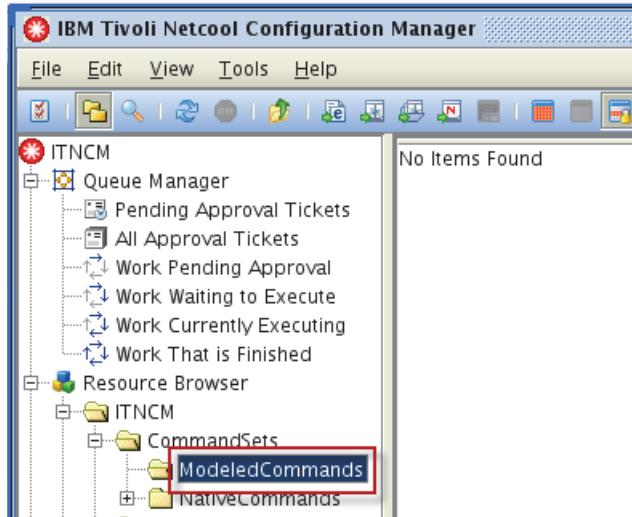


8. Enter **NativeCommands** for the name, and click **OK**.

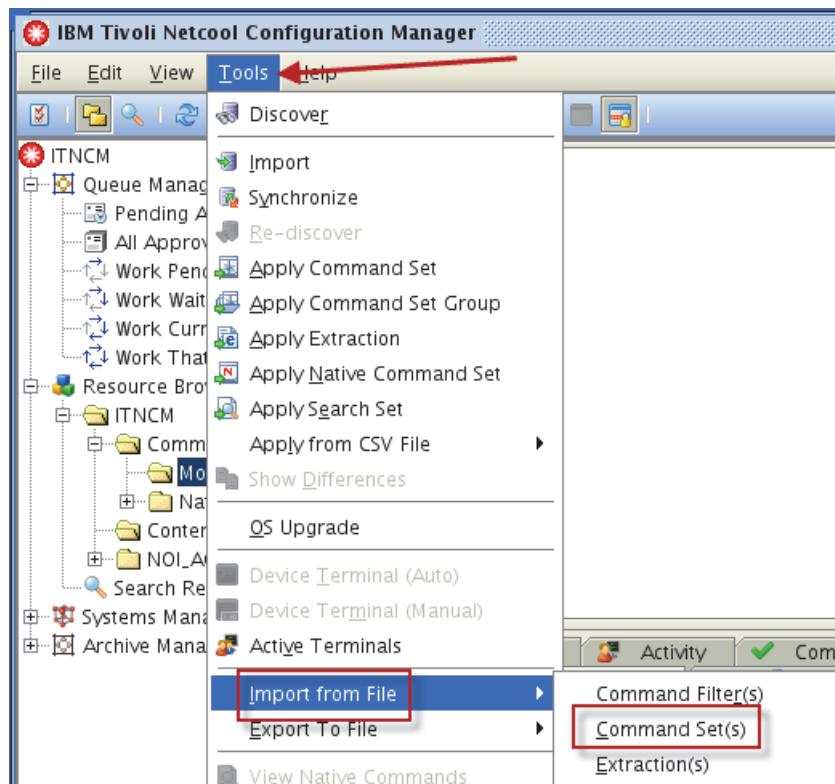


Note: The realm names are not significant. You create the realms to organize the command sets.

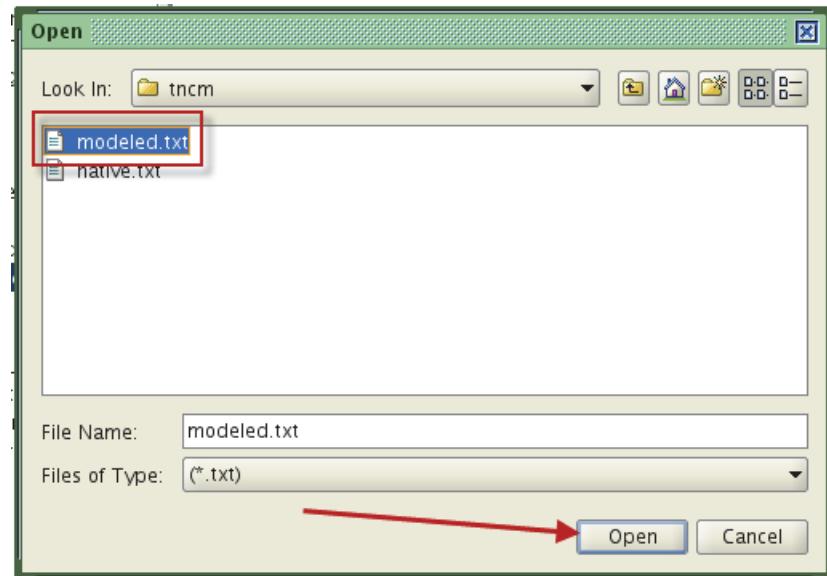
9. Under **CommandSets**, click **ModeledCommands** to select it.



10. Click **Tools**, and select **Import from File > Command Set(s)**.



11. Navigate to /workshop/tncm, and select **modeled.txt**. Click **Open**.

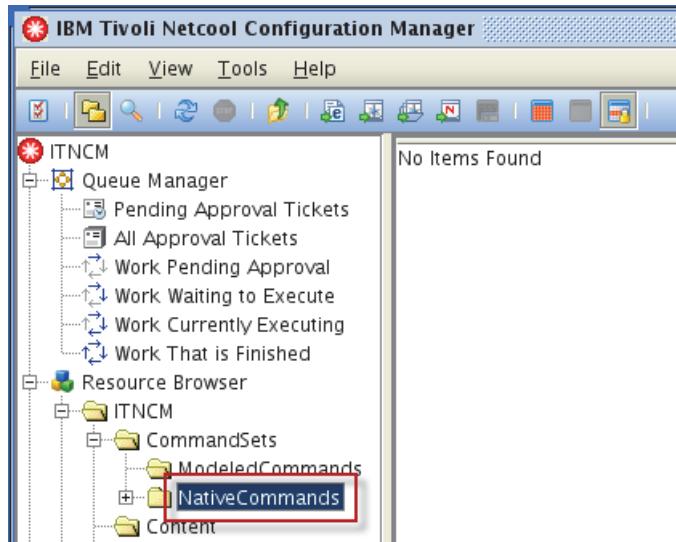


12. Wait a short time.

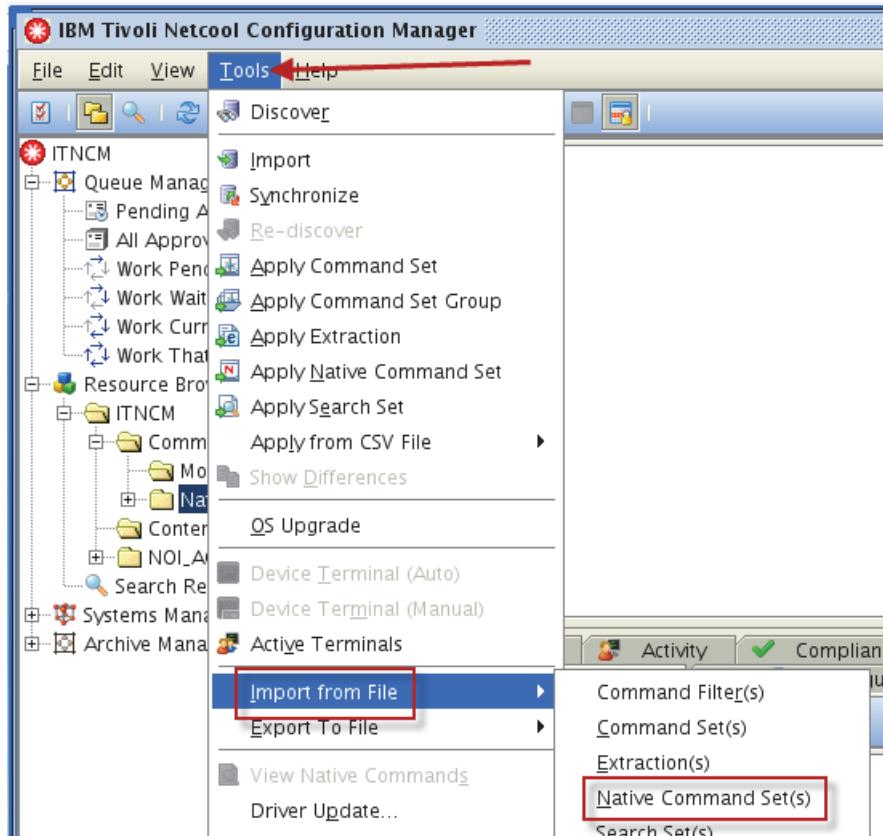
13. Verify that the command sets are present.

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*

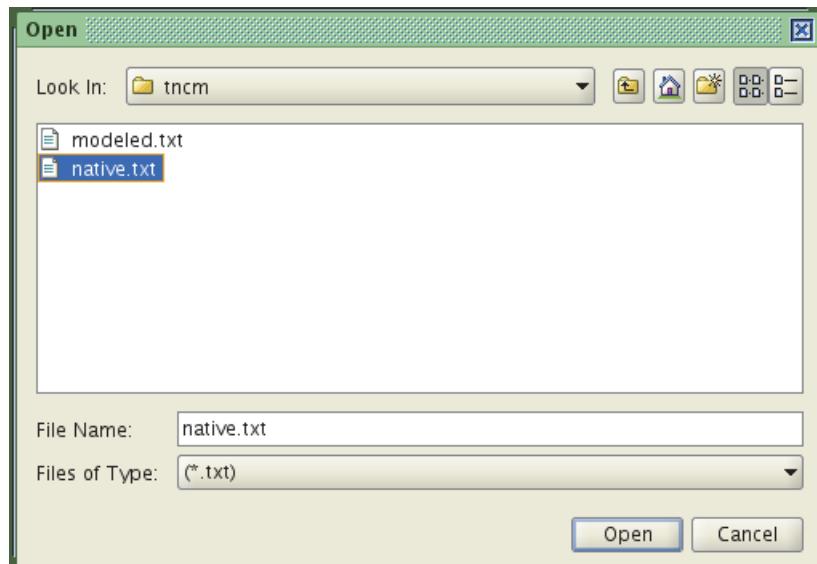
14. Under **CommandSets**, click **NativeCommands** to select it.



15. Click **Tools**, and select **Import from File > Native Command Set(s)**.

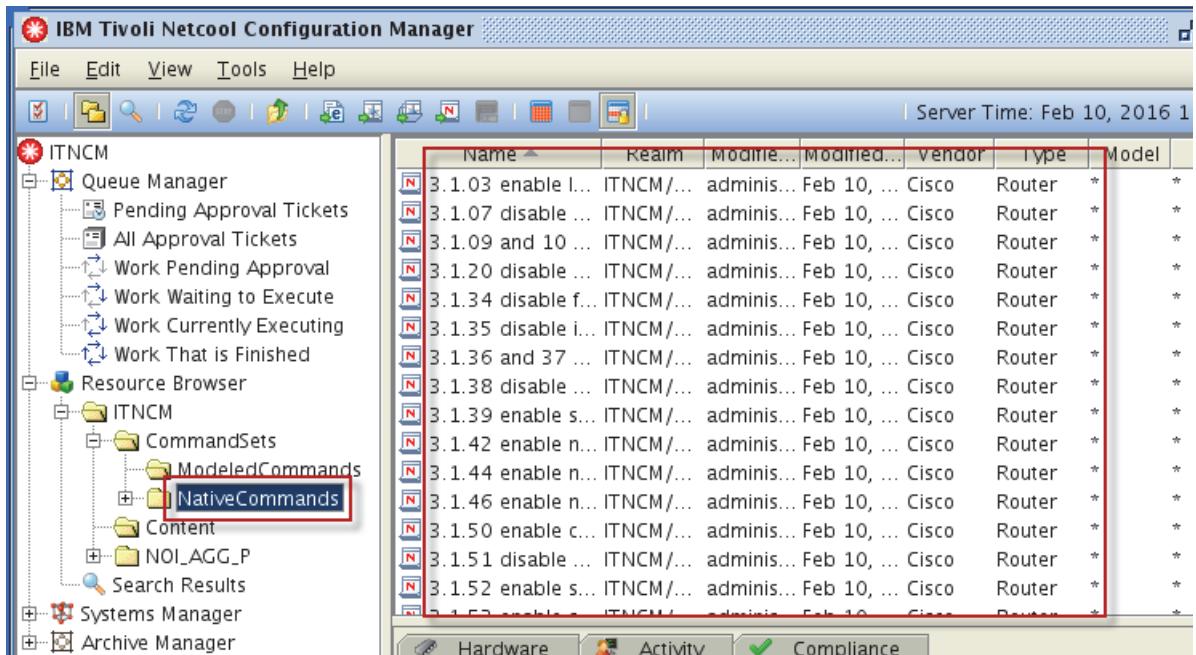


16. Navigate to **/workshop/tncm**, and select **native.txt**. Click **Open**.



17. Wait a short time.

18. Verify that the command sets are presents.



Name	Realm	Modified...	Vendor	Type	Model
N 3.1.03 enable I...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.07 disable ...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.09 and 10 ...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.20 disable ...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.34 disable f...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.35 disable i...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.36 and 37 ...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.38 disable ...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.39 enable s...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.42 enable n...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.44 enable n...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.46 enable n...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.50 enable c...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.51 disable ...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.52 enable s...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router
N 3.1.53 enable ...	ITNCM/...	adminis...	Feb 10, ...	Cisco	Router

19. Click **File** and select **Quit** to close the client.

20. Click **OK** to confirm.

21. Click **Logoff**.

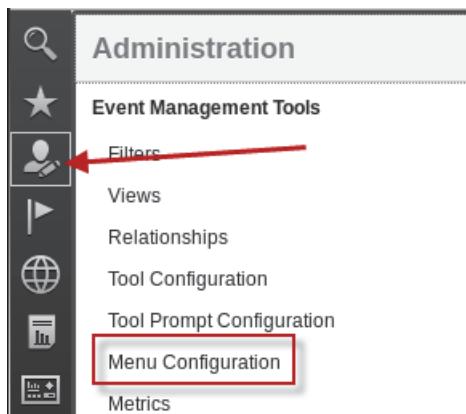


22. Close the Firefox browser.

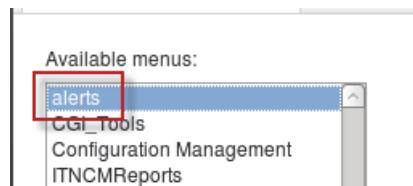
Configuring integration with Netcool/OMNibus

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.

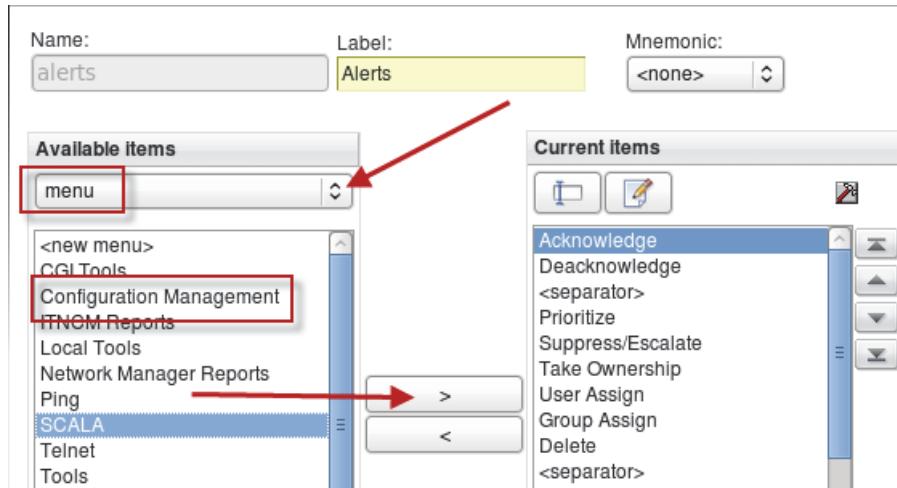
1. Add the Configuration Manager menu to the Web GUI alert menu.
 - a. Open a Firefox browser.
 - b. Log in to Dashboard Application Services Hub as **ncoadmin** with password **object00**.
 - c. Click the icon and select **Menu Configuration**.



- d. Click **alerts** to select it. Scroll to the bottom of the page and click **Modify**.

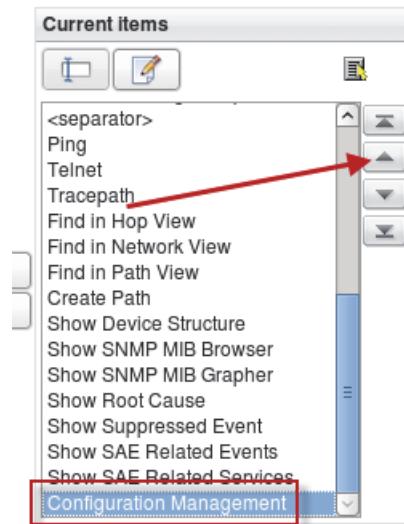


- e. Click the arrow and select **menu**. Click **Configuration Management** to select it. Click the **right arrow icon** to add the menu to the list.

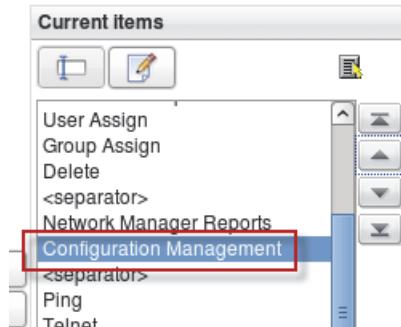


The Configuration Management menu is added to the bottom of the list.

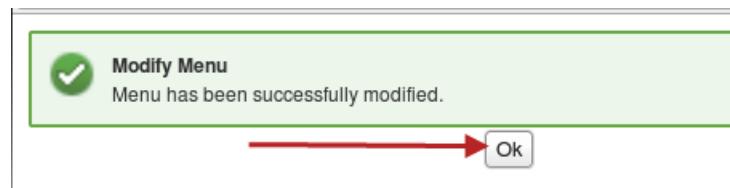
- f. Scroll to the bottom of the list and select **Configuration Management**. Click the **up arrow icon** several times.



- 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, along with other configuration changes.

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 in a text editor.

```
gedit rseries.properties
```

4. Find the following line:

```
NMEntityMappingComponent/ncmUser=administrator
```

5. Change the property value to **ncoadmin**.

```
NMEntityMappingComponent/ncmUser=ncoadmin
```

6. Find the following line:

```
NMEntityMappingComponent/period=1440
```

7. Change the property value to **5**.

```
NMEntityMappingComponent/period=5
```



Important: You change the NMEntityMappingComponent/period property to facilitate a subsequent workshop exercise. You do not typically change this value in a production environment.

8. Find the following line:

```
NMEntityMappingComponent/uri=
```

9. Add the following property value.
`NMEntityMappingComponent/uri=/ibm/console/nm_rest/topology/devices/domain/NOI_ AGG_P`
10. Save the file and exit the gedit utility.

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 in a text editor.
`gedit ncm.properties`
3. Find the following lines:
`ncm.server=localhost`
`ncm.port=16311`
4. Change the property values to match the following example.
`ncm.server=host1.csite.edu`
`ncm.port=15311`
5. Save the file and exit the gedit utility

Setting the compliance user

You can configure compliance policies to run command sets. These command sets must run as a user with the proper permissions. These steps show you how to set ncoadmin as the automated user.

1. Change to the target directory.
`cd /opt/IBM/ncm/compliance/bin/utils`
2. Run the following commands, one at a time, to set ncoadmin as the automated user.
`./intellidenRmUser.sh --set cmuser ncoadmin object00`
`./intellidenRmUser.sh --set rmuser ncoadmin object00`
`./intellidenRmUser.sh --set automateduser ncoadmin object00`

 **Note:** You restart Netcool Configuration Manager in a later step.

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
```

```
Aug 5 19:57:09 host1 netcool: this is a test
```

5. Install the OOBC software.

- a. Expand the installation file.

```
cd /opt
```

```
unzip /software/tncm/base/oobc_linux.zip
```

- b. Install the OOBC 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 ncoadmin

Enter clear text password:

Enter object00

Enter the worker user id ITNCM executes work as [intelliden]?

Enter ncoadmin

Enter the worker server address [intelliden]?

Enter host1.csuite.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.csuite.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/K870OBCDaemon_run1
/etc/rc.d/rc1.d/K870OBCDaemon_run1
/etc/rc.d/rc2.d/S130OBCDaemon_run1
/etc/rc.d/rc3.d/S130OBCDaemon_run1
/etc/rc.d/rc4.d/S130OBCDaemon_run1
/etc/rc.d/rc5.d/S130OBCDaemon_run1
/etc/rc.d/rc6.d/K870OBCDaemon_run1
BUILD SUCCESSFUL
Total time: 3 minutes 59 seconds
```

- c. Remove the 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 05 Aug 2019 20:12:00 Activating com.intelliden.oobc.OutOfBandChangeDaemon
INFO 05 Aug 2019 20:12:02 Recovered 0 PRE rolled-up Events (with 0 child events)
from last run.
INFO 05 Aug 2019 20:12:02 Recovered 0 POST rolled-up Events (with 0 child
events) from last run.
INFO 05 Aug 2019 20:12:02 Started com.intelliden.oobc.NotifierThread
INFO 05 Aug 2019 20:12:02 Started com.intelliden.oobc.RollupThread
INFO 05 Aug 2019 20:12:02 Started com.intelliden.oobc.ParserThread
WARN 05 Aug 2019 20:12:02 Starting log parsing with new marker file:
/opt/OutOfBandChange/run1/log.marker
WARN 05 Aug 2019 20:12:02 com.intelliden.oobc.OutOfBandChangeDaemon now Active.
INFO 05 Aug 2019 20:12:02
```

```
=====
ITNCM Host: host1.csuite.edu
ITNCM Port: 15310
ITNCM Protocol: iiop
ITNCM User: ncoadmin
Ignored host(Worker Server): host1.csuite.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: ncoadmin
3rd Party User: 3rdPartyUser
Number of Log pattern rules: 7
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 in a text editor.

```
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 look like the following example.

```
$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. Find both 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 to allow execute permissions.

```
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
```

```
-----  
6.4.2.8-27052019062220-01-f8a8c49b816
```

```
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.

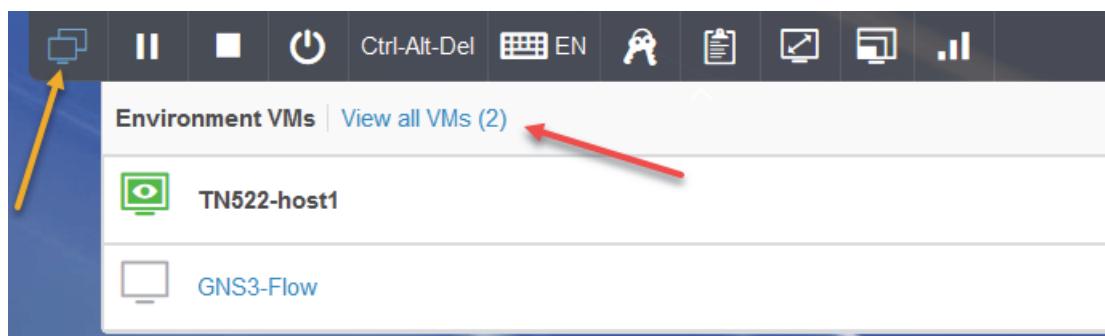
Exercise 1 Starting the network simulator

The verification steps use another VMware image. This image contains a network simulator.

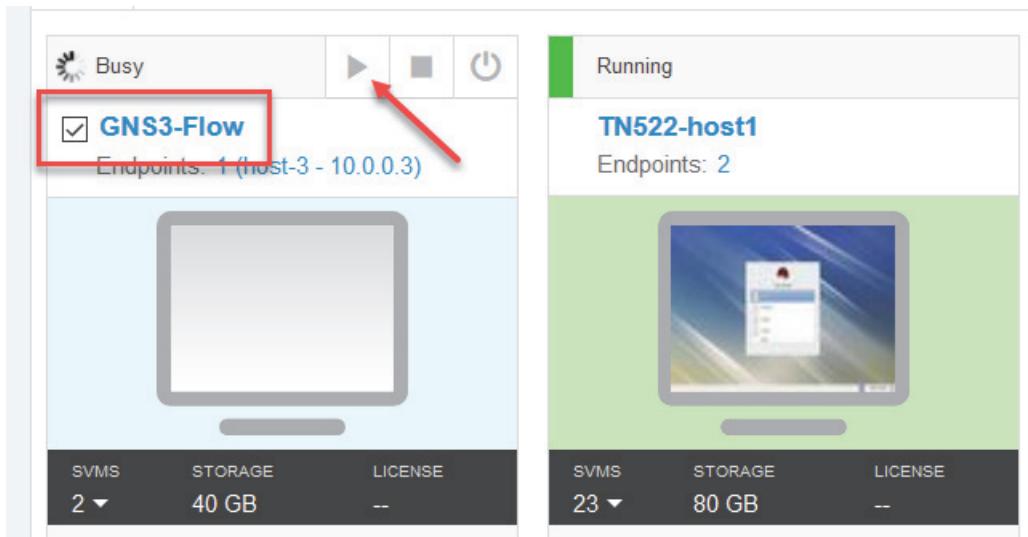
1. Switch to the GNS3-Flow virtual machine.
 - a. Click the tab at the top of the window to view the lab environment options.



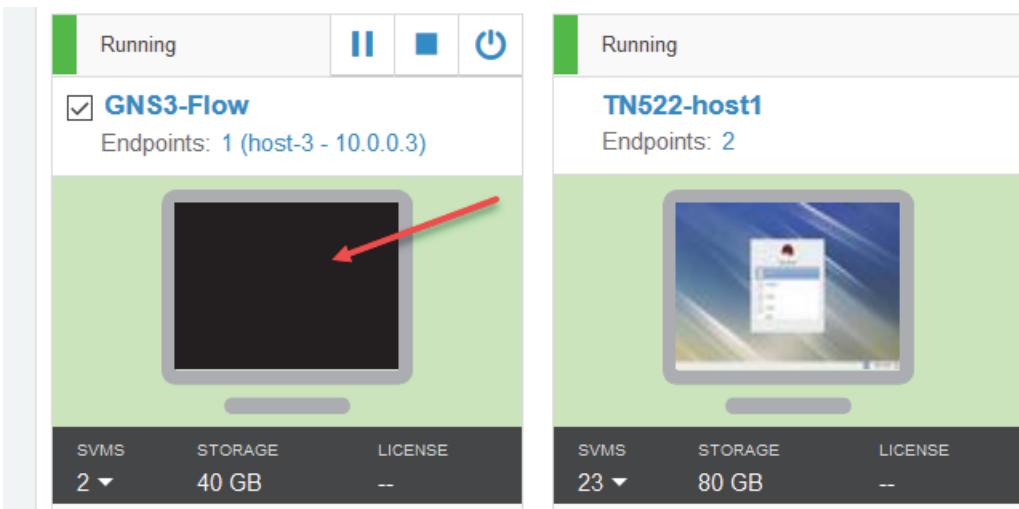
- b. Click the icon for environment VMs. Click **View all VMs**.



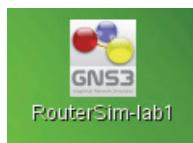
- c. Select the **GNS3-Flow** VM. Click the run button.



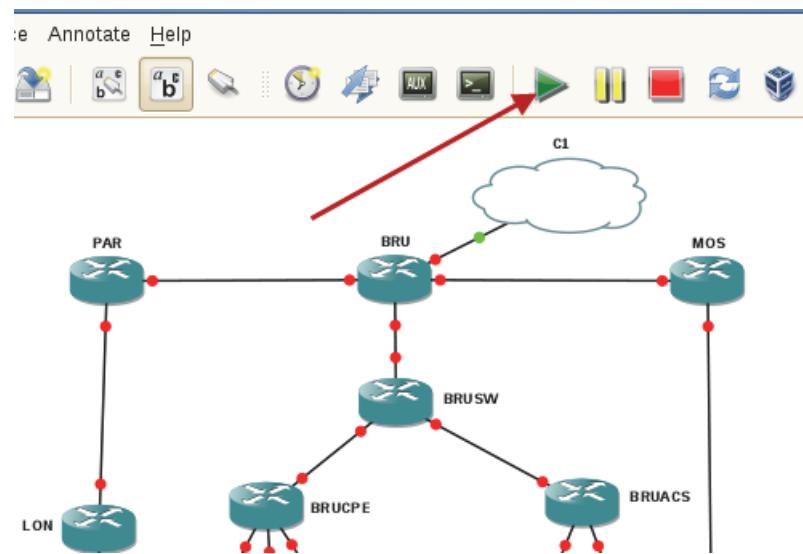
- d. The image takes several minutes to start. After a few moments, click the **GNS3-Flow** tile to connect to the console of the virtual machine.



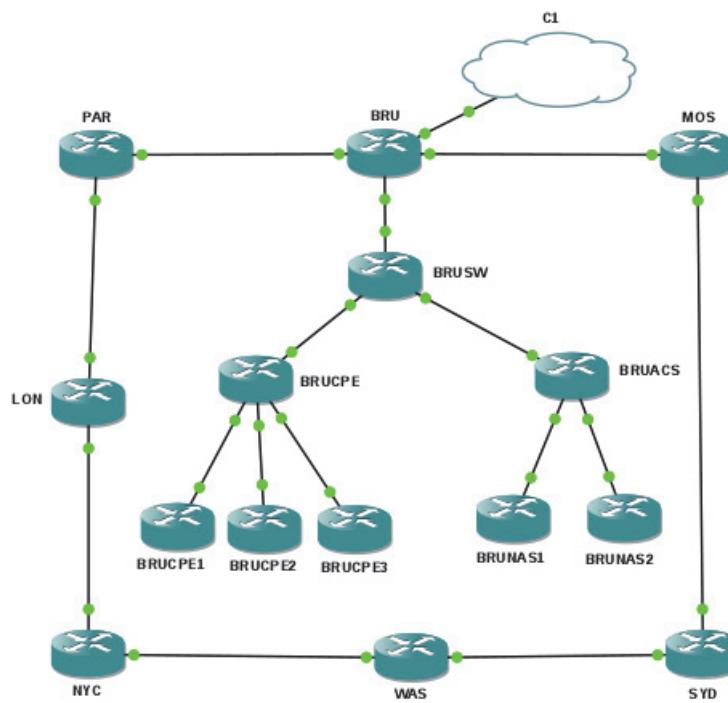
2. If prompted, log in as **root** with password **object00**.
3. Start the simulated devices.
 - a. Double-click the desktop icon labeled **RouterSim-lab1**.



- b. Click the green arrow icon to start the simulated devices.



- c. Wait until all of the dots turn green.



4. Return to the Netcool Operations Insight virtual machine.

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

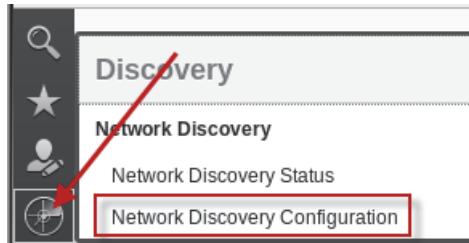
In this exercise, you verify many of the functions provided by the Networks for Operations Insight solution, including these items:

- 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

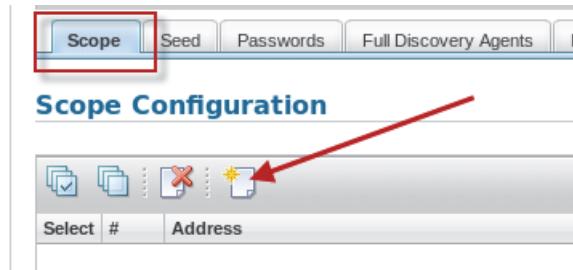
Discovering devices with Network Manager

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

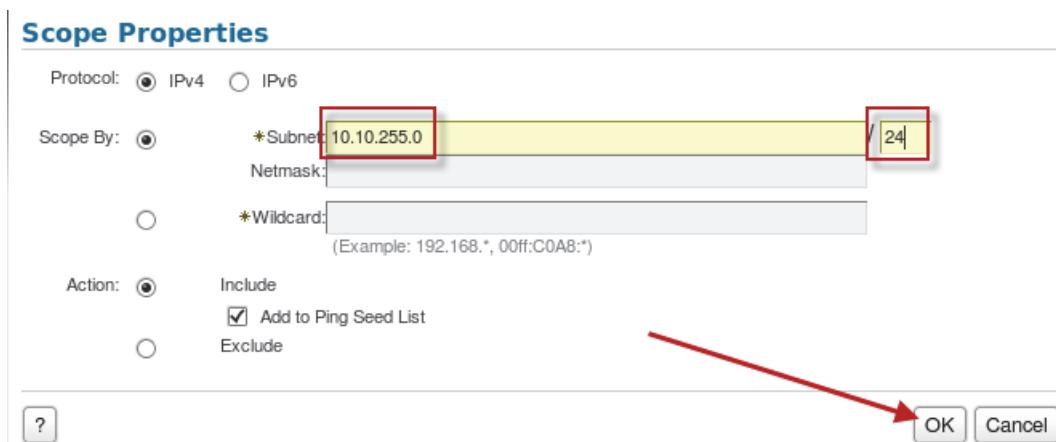
3. Click the icon and select Network Discovery Configuration.



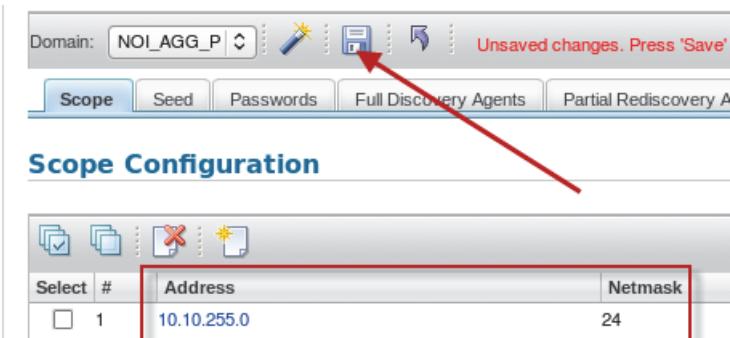
4. Click the icon to add a subnet.



5. Enter 10.10.255.0 / 24. Click OK.



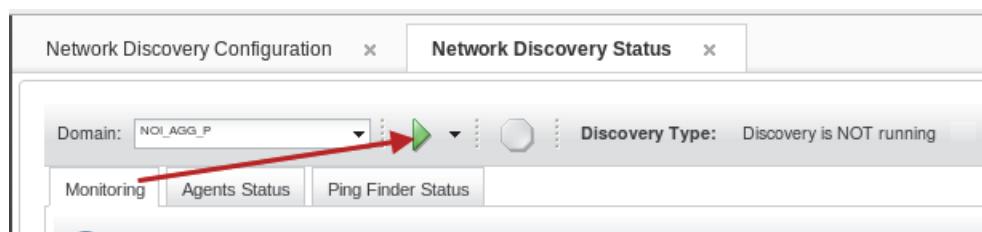
6. Click the icon to save the configuration.



7. Click the icon and select Network Discovery Status.



8. Click the green arrow icon to start the discovery.



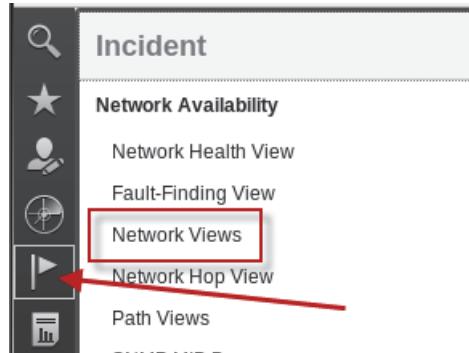
Note: The discovery runs for approximately 6 minutes.

9. Verify that discovery is complete.

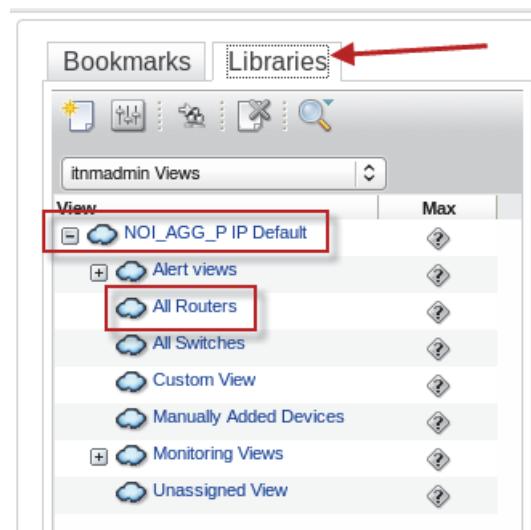
Phase	Status	Elapsed Time (H:MM:SS)	
		Current	Previous
Interrogating Devices	✓	0:02:34	-
Resolving Addresses	✓	0:00:08	-
Downloading Connections	✓	-	-
Correlating Connectivity	✓	0:00:03	-
Last status received: Discovery is NOT running			

10. Examine the devices.

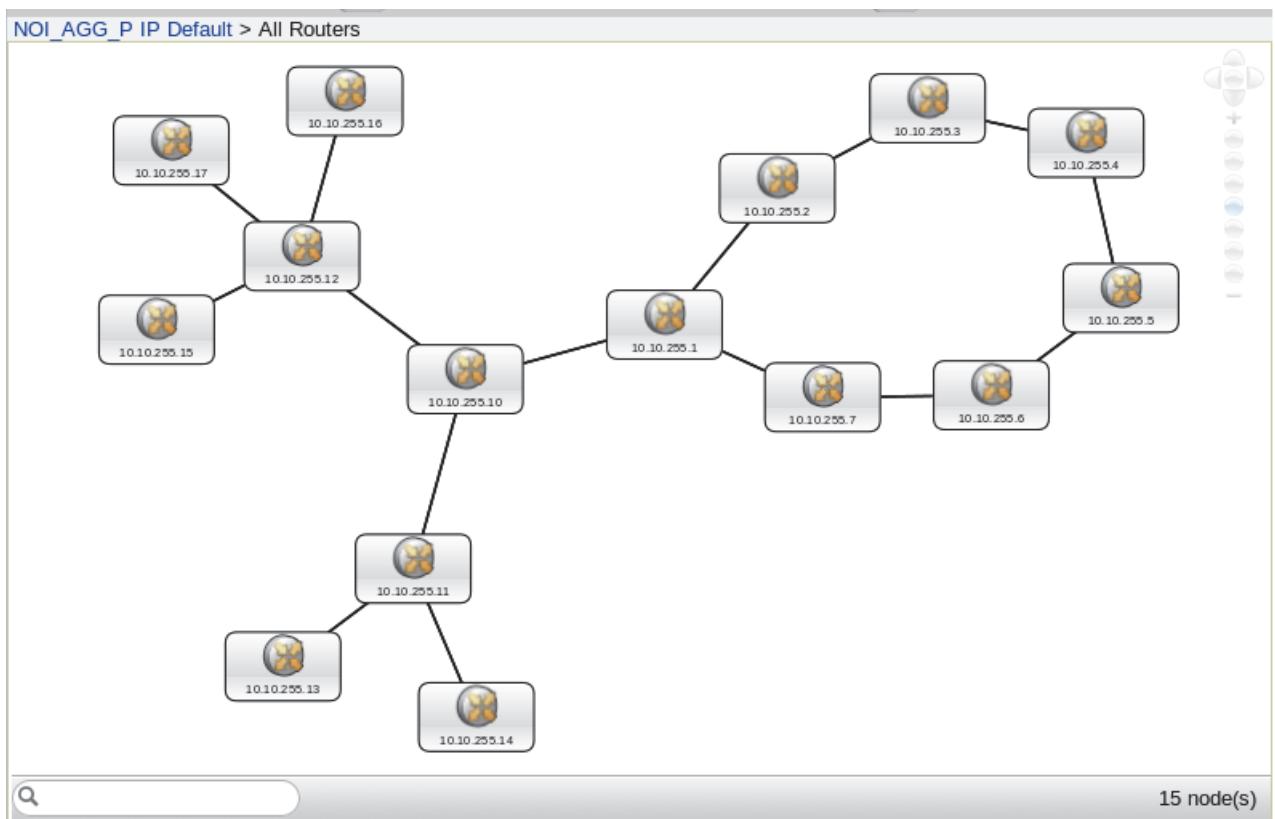
- a. Click the icon and select Network Views.



- 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 worker.log
```

...

```
2019.08.06 13:48:30 GMT+00:00 OperationRunner-004-Worker1 INFO WORKER
Worker1 com.intelliden.core.workflow.execute.OperationRunner :: Running
operation: AutoDiscovery
```

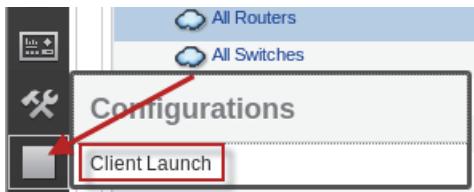
Messages like this verify that Netcool Configuration Manager is automatically discovering the devices that were discovered by Tivoli Network Manager.



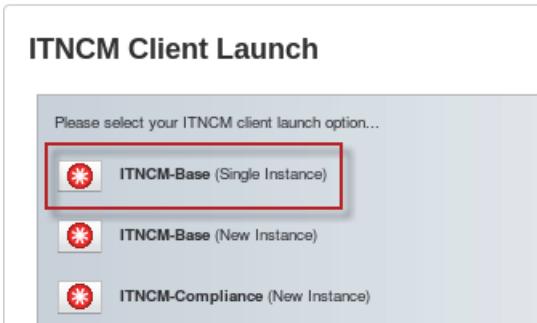
Important: You might need to repeat the tail command several times before the correct message appears.

2. Return to the Firefox browser.

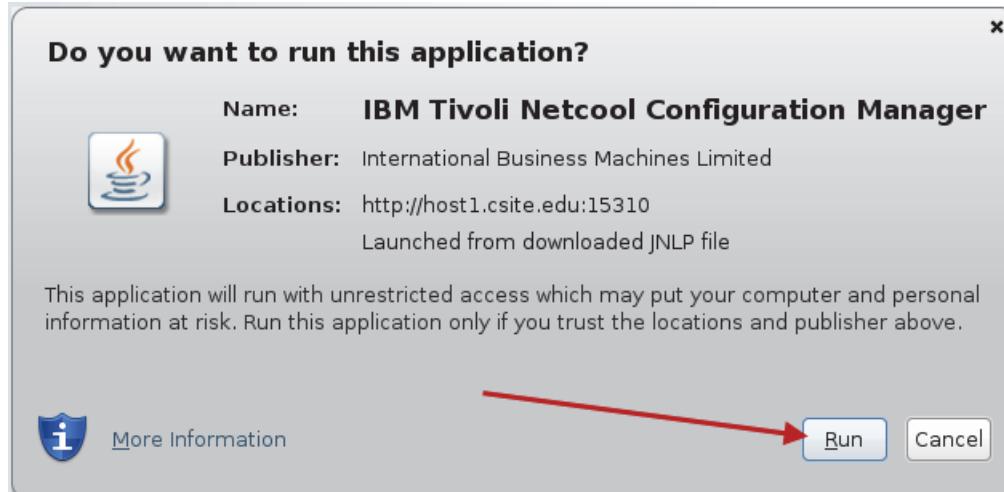
3. Click the icon and select **Client Launch**.



4. Click **ITNCM-Base (Single Instance)**.



5. Click Run.

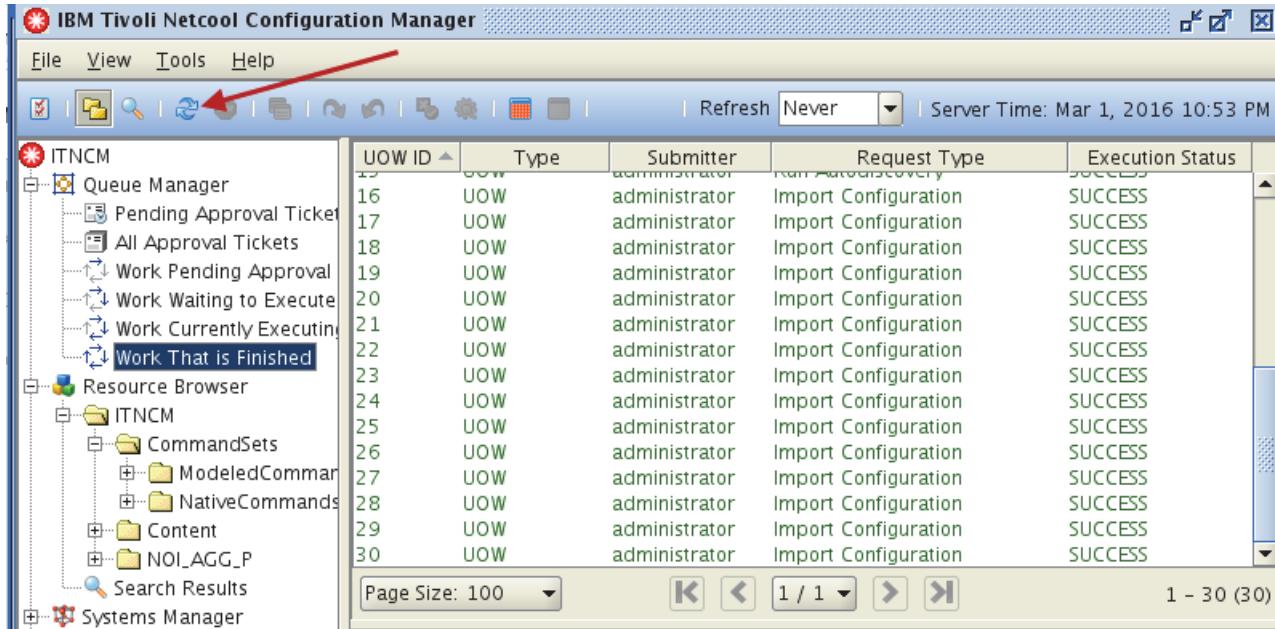


The Configuration Manager client opens, and you are logged in as the **itnadmin** user, which verifies that single sign-on works.

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

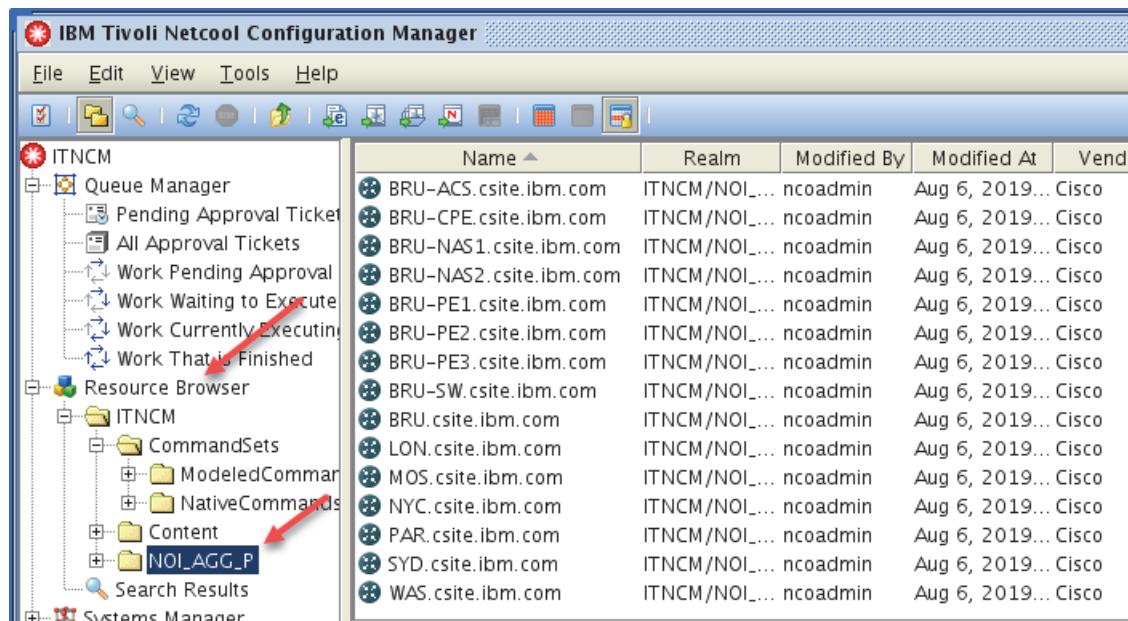
7. Verify that you have 30 *units of work* (UOW) under **Work That is Finished**.



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**.



9. Observe the entries for the imported routers.

10. Click any entry to select it. Click the **Configurations** tab.

Name	Realm	Modified By	Modified At	Vendor	Type
BRU-ACS.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router
BRU-CPE.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router
BRU-NAS1.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router
BRU-NAS2.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router
BRU-PE1.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router
BRU-PE2.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router
BRU-PE3.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router
BRU-SW.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router
BRU.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router
LON.csite.ibm.com	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router

Name	Realm	Modified By	Modified At	Vendor	Type	Model
Importe...	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco	Router	3640

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**.

Name	Realm	Modified At	Vendor	Type
BRU-ACS.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
BRU-CPE.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
BRU-NAS1.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
BRU-NAS2.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
BRU-PE1.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
BRU-PE2.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
BRU-PE3.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
BRU-SW.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
BRU.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
LON.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
MOS.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
NYC.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
PAR.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
SYD.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router
WAS.csite.ibm.com	ITNCM/NOI...	, 2019...	Cisco	Router

Name	Realm	Modified At	Vendor	Type	Model
Importe...	ITNCM/NOI...	Aug 6, 201...	Cisco	Router	3640

Open...

Edit...

Delete...

Rename...

Move...

Import

Synchronize

Re-discover

Trigger Config Backup

Trigger Config Restore

Apply Command Set

Apply Command Set Group

Apply Extraction

Apply Native Command Set

Apply Search Set

Show Differences

OS Upgrade

Device Terminal (Auto)

Device Terminal (Manual)

Active Terminals

View Native Commands

Driver Update...

12. Observe the actual device configuration. Close the window when you are finished.

Native Commands - Imported Configuration (10.10.255.1)

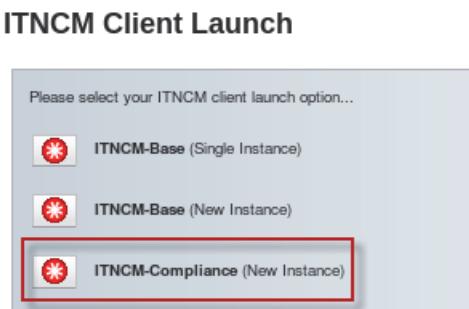
File Search Page 1: |

```
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: !
```

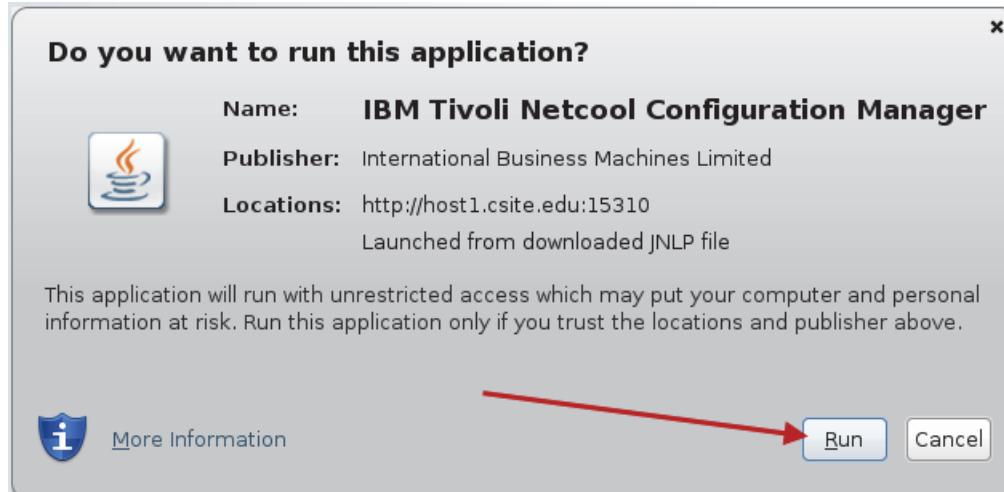
Leave the configuration client open. You use it again shortly.

Verifying Compliance Management

1. Return to the Firefox browser.
 2. Click **ITNCM-Compliance (New Instance)**.

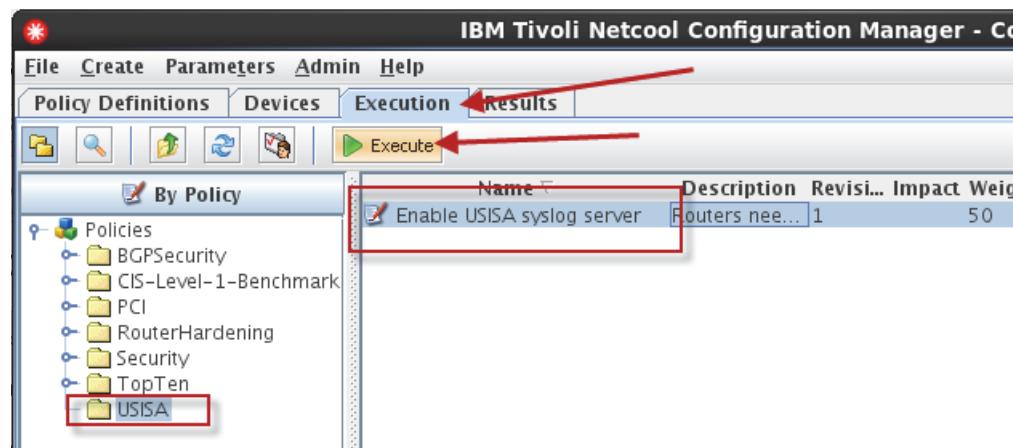


3. Click Run.



4. Evaluate the imported devices for compliance.

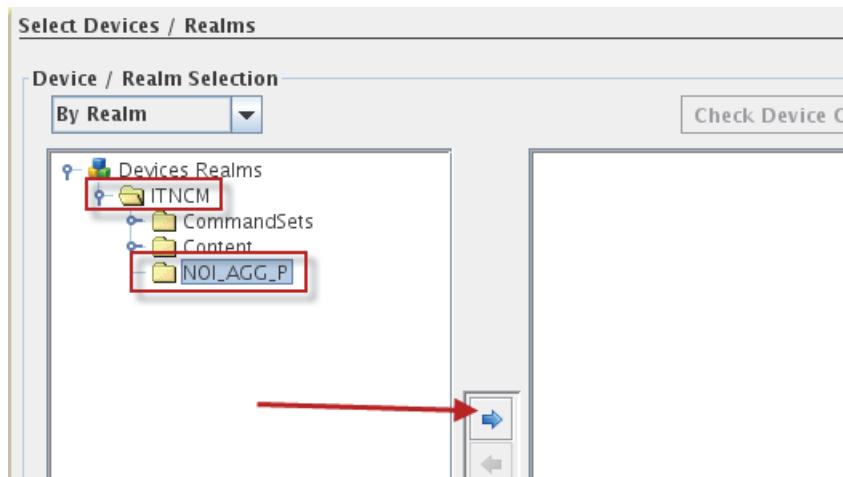
- Select the **Execution** tab.
- Under Policies, click **USISA**.
- Click **Enable USISA syslog server**.
- Click **Execute**.



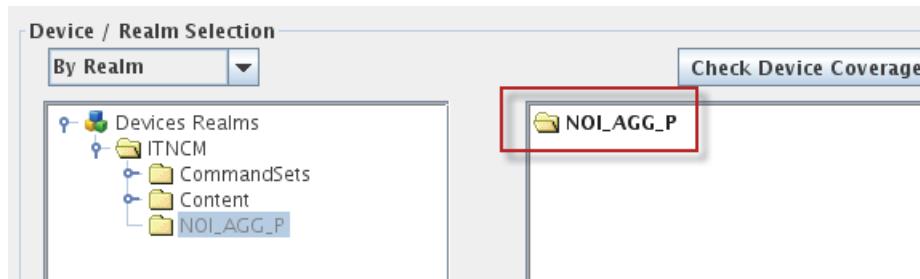
5. Enter a value for description, and click **Next**.

Name and Description	
Policy Execution Name & Description	
Name:	02-Mar-2016 10:19:25
Description:	Evaluate devices for syslog compliance

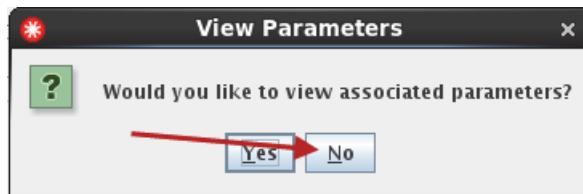
6. Expand the **ITNCM** realm. Click **NOI_AGG_P** to select it. Click the *right arrow* icon to select the devices in the realm.



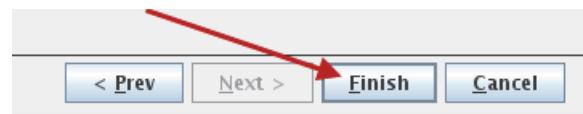
7. Click **Next**.



8. Click **No**.

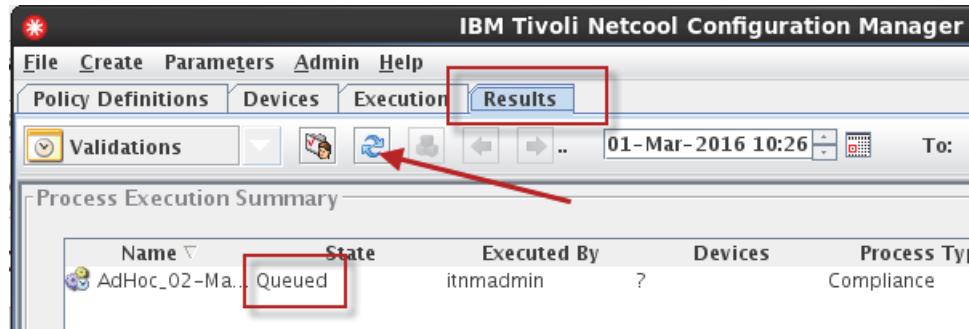


9. Click **Finish**.



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**.



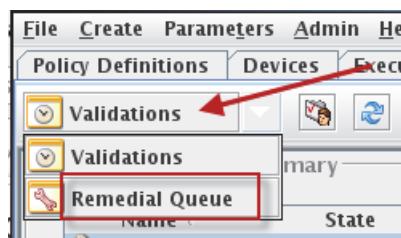
12. Click the entry to select it. Observe the results in the lower pane.

Name	State	Executed By	Devices	Process Type	Execution Type	Start Date
AdHoc_02-Ma...	Finished	itnmadmin	15	Compliance	AdHoc	02-Mar-

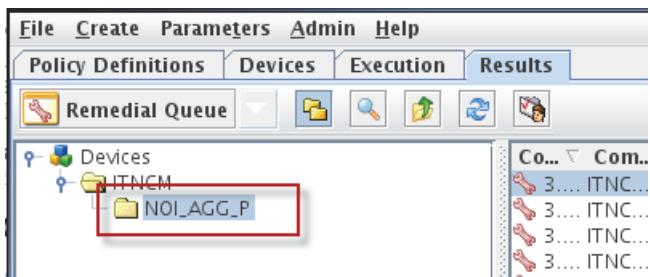
Policy Name	Severity	Revision	Date	Passed	Failed	Not As
Enable USISA s...	3	1	02-Mar-2016 12:00:00	0	15	0

The compliance policy evaluated 15 devices and they all failed.

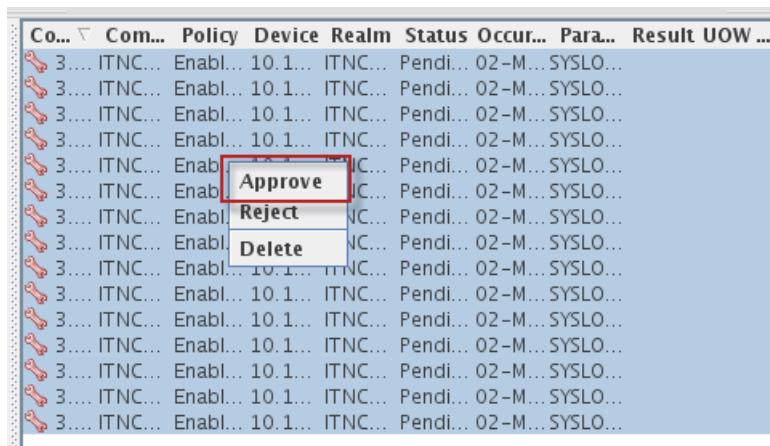
13. Click **Validations**, and select Remedial Queue.



14. Expand **ITNCM**, and click **NOI AGG P.**



15. Select all of the entries. Right-click the entries, and select **Approve**.

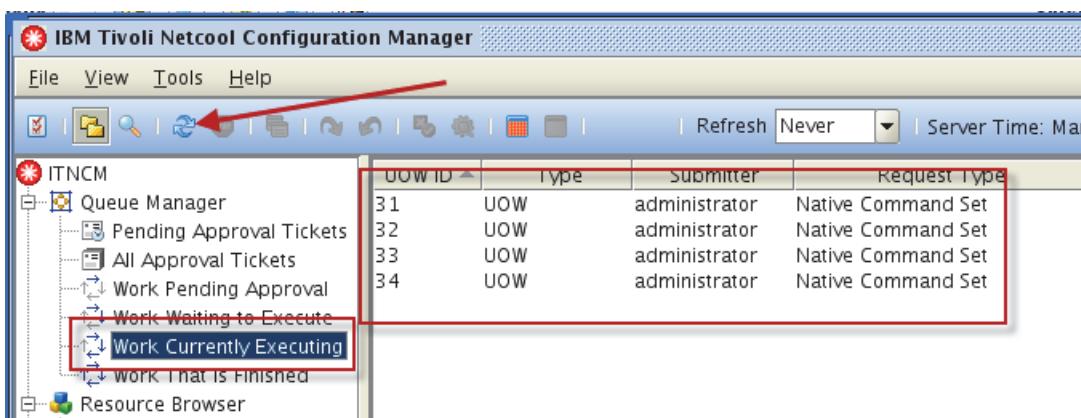


16. Click **Yes** to confirm the approval.



17. Return to the configuration manager client.

18. Under Queue Manager, click **Work Currently Executing**.

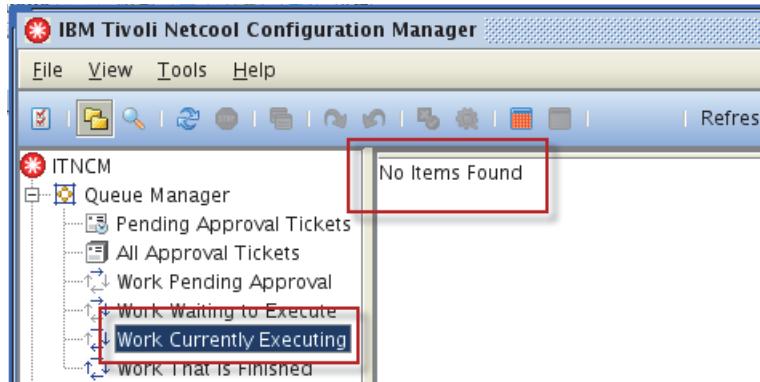


You see four *units of work*.



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.

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 Netcool Operations Insight interface. On the left, the Resource Browser tree view has the 'NOI_AGG_P' folder selected. On the right, the main workspace displays the 'Configurations' tab of the 'Work' section. Two configuration files are listed:

Name	Realm	Modified By	Modified At	Vendor
Importe...	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Cisco
Native c...	ITNCM/NOI...	ncoadmin	Aug 6, 201...	Router

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**.

The screenshot shows the Compliance Manager client interface. The top navigation bar includes 'File', 'Create', 'Parameters', 'Admin', and 'Help'. Below the bar, there are tabs: 'Policy Definitions', 'Devices', 'Execution' (which is highlighted with a red arrow), and 'Results'. The 'Execution' tab is active, showing a toolbar with icons for 'New', 'Search', 'Import', 'Export', and 'Execute' (also highlighted with a red arrow). The main workspace is divided into two panes: 'By Policy' on the left and a table on the right. The 'By Policy' pane shows a tree structure with 'Policies' expanded, listing 'BGPSecurity', 'CIS-Level-1-Benchmark', 'PCI', 'RouterHardening', 'Security', 'TopTen', and 'USISA'. The table on the right lists policy details:

Name	Description	Revised	Impact	Weight	Enabled
En...	Route...	1	50	P	

24. Enter a value for description, and click **Next**.

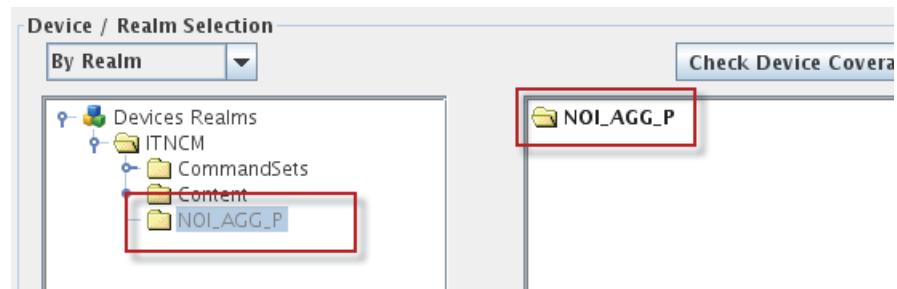
Name and Description

Policy Execution Name & Description

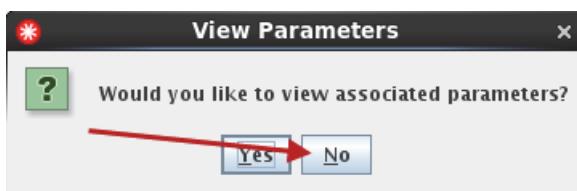
Name: 02-Mar-2016 13:03:22

Description: Re-check syslog compliance.

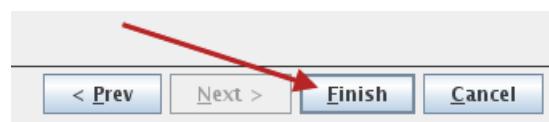
25. Select the **NOI_AGG_P** realm, and click **Next**.



26. Click **No**.

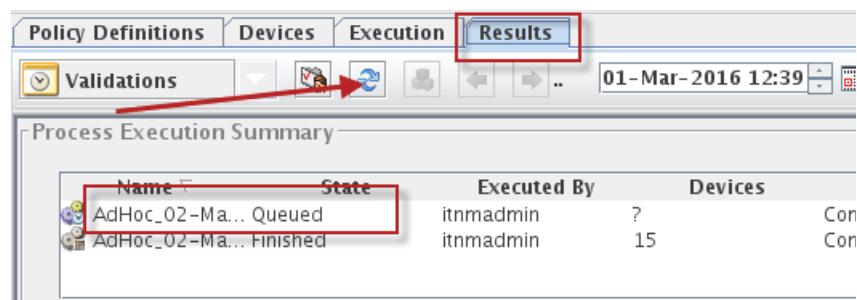


27. Click **Finish**.



The results view opens automatically. You see a second entry.

28. Click the *blue arrows* icon to refresh the display.

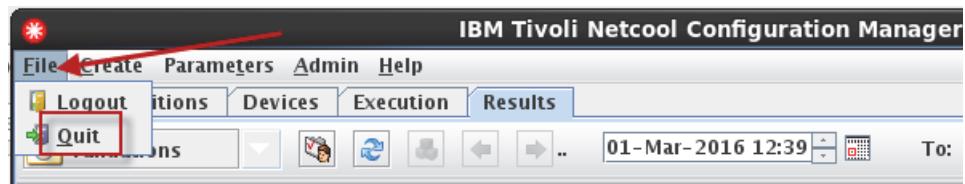


29. After the entry completes, click the entry to select it, and observe the results.

The screenshot shows two windows side-by-side. The top window is titled 'Process Execution Summary' and lists two entries: 'AdHoc_02-Ma...' (State: Finished, Executed By: itnmadmin, Devices: 15, Process Type: Compliance, Execution Type: AdHoc, Status: 02-Mar) and another identical entry. The bottom window is titled 'Policy Validation Summary' and shows a single policy named 'Enable USISA s... 3' with a severity of 1, revision 1, and a date of 02-Mar-2016 13:15. It indicates 15 devices passed, 0 failed, and 0 not applicable.

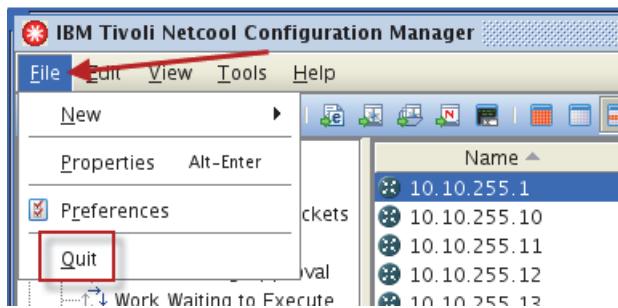
All 15 devices are compliant.

30. Click **File**, and select **Quit** to close the compliance manager client.



31. Click **Yes** to confirm the exit.

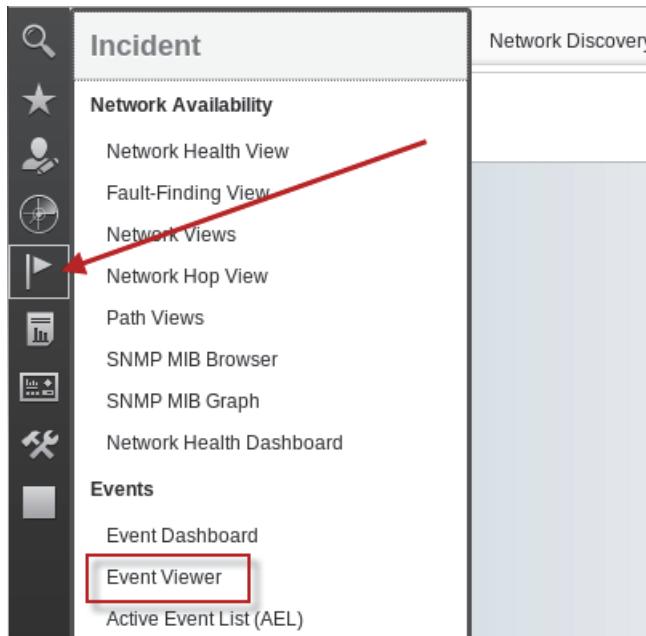
32. Click **File**, and select **Quit** to close the configuration manager client.



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.

Sev	Ack	Node	Alert Group	Summary
⚠	No	WAS.csite.ibm.com	Policy Trap	WAS.csite.ibm.com is in violation of policy
⚠	No	BRU.csite.ibm.com	Policy Trap	BRU.csite.ibm.com is in violation of policy
⚠	No	BRU-PE2.csite.ibm.com	Policy Trap	BRU-PE2.csite.ibm.com is in violation of policy
⚠	No	BRU-ACS.csite.ibm.com	Policy Trap	BRU-ACS.csite.ibm.com is in violation of policy
⚠	No	BRU-PE3.csite.ibm.com	Policy Trap	BRU-PE3.csite.ibm.com is in violation of policy
⚠	No	BRU-CPE.csite.ibm.com	Policy Trap	BRU-CPE.csite.ibm.com is in violation of policy
⚠	No	BRU-SW.csite.ibm.com	Policy Trap	BRU-SW.csite.ibm.com is in violation of policy

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.

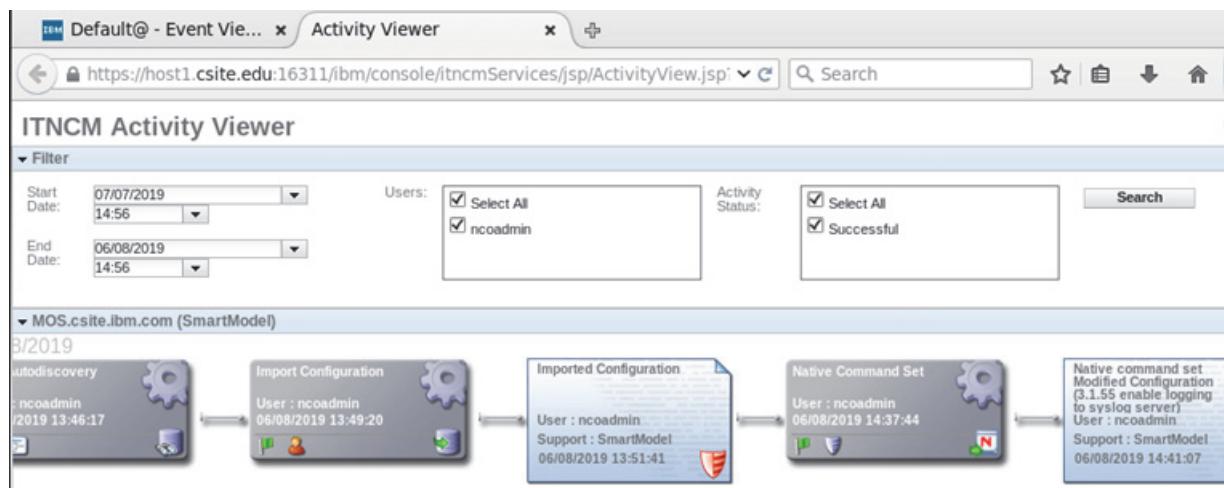
4. Scroll down within the event list until you find a **UOW trap**.

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.csuite.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, 12:32:55.6

5. Click any UOW trap event to select it. Right-click and select **Configuration Management > Device Activity Sequence**.

Ack	Node	Alert Group	Summary
No	192.168.100.100	UOW trap	Apply Native Commandset UOW '35' submitted by administrator is executing (531658018)
No	192.168.100.100	UOW trap	Apply Native Commandset UOW '37' submitted by administrator is executing (531658023)
No	192.168.100.100	UOW trap	Apply Native Commandset UOW '41' submitted by administrator is executing (531669050)
No	host1.csuite.edu	DBStatus	Last 5 mins alerts.details (inserts): 0
No	192.168.100.100	UOW trap	Import UOW '17 submitted by administrator is executing (531557597) 61 days, 12:32:55.6
No	192.168.100.100	UOW trap	Import UOW '31' submitted by administrator is executing (531557597) 61 days, 12:32:55.6
No	192.168.100.100	UOW trap	Import UOW '31' submitted by administrator is executing (531557597) 61 days, 12:32:55.6
No	192.168.100.100	UOW trap	Import UOW '31' submitted by administrator is executing (531557597) 61 days, 12:32:55.6
No	192.168.100.100	UOW trap	Import UOW '31' submitted by administrator is executing (531557597) 61 days, 12:32:55.6
No	192.168.100.100	UOW trap	Import UOW '31' submitted by administrator is executing (531557597) 61 days, 12:32:55.6

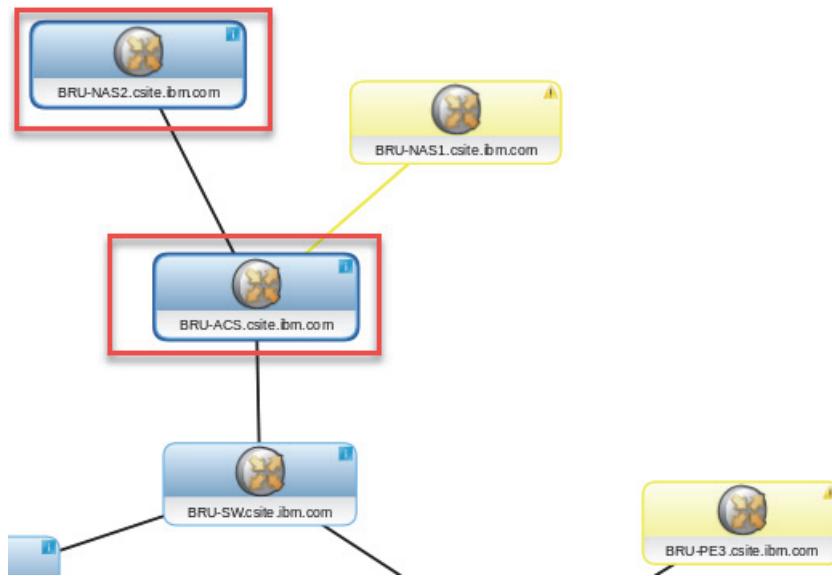
The Activity Viewer opens in a new tab.



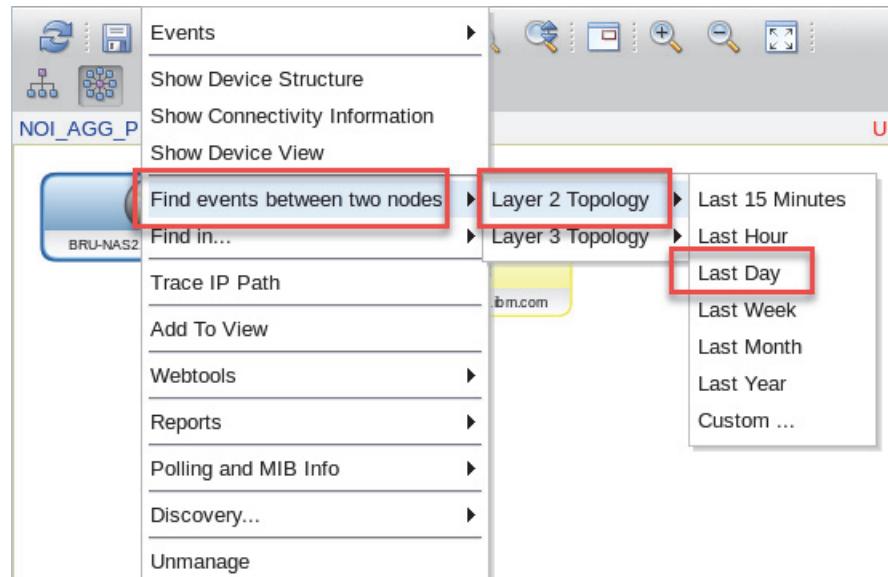
Each box represents a separate Configuration Manager action.

6. Click the X to close the **Activity Viewer** tab.

7. Return to the Network Views page.
8. Click a device icon to select it. Hold the Ctrl key, and click a second device icon to select it.



9. Right-click either device icon, and select **Find events between two nodes > Layer 2 Topology > Last Day**.

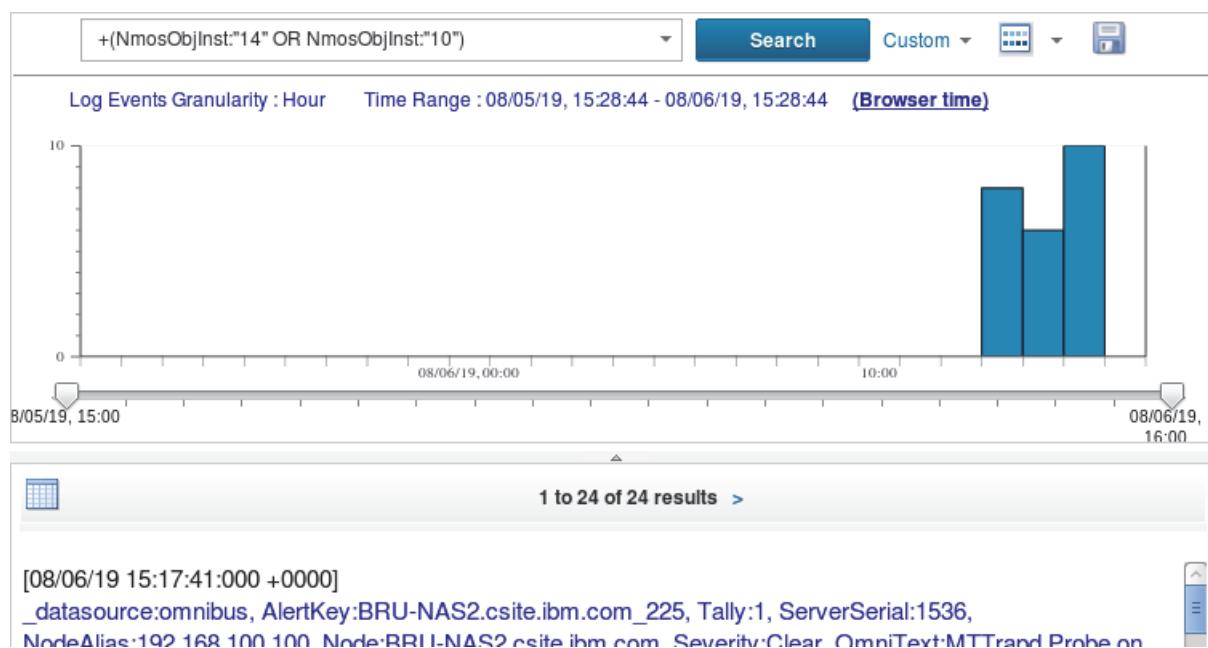


The Log Analysis user interface opens in a new Firefox tab. The topology search runs, and the event summary is displayed.

- Click the Route 1 entry.



The event details are displayed.



- Close the Log Analysis tab.

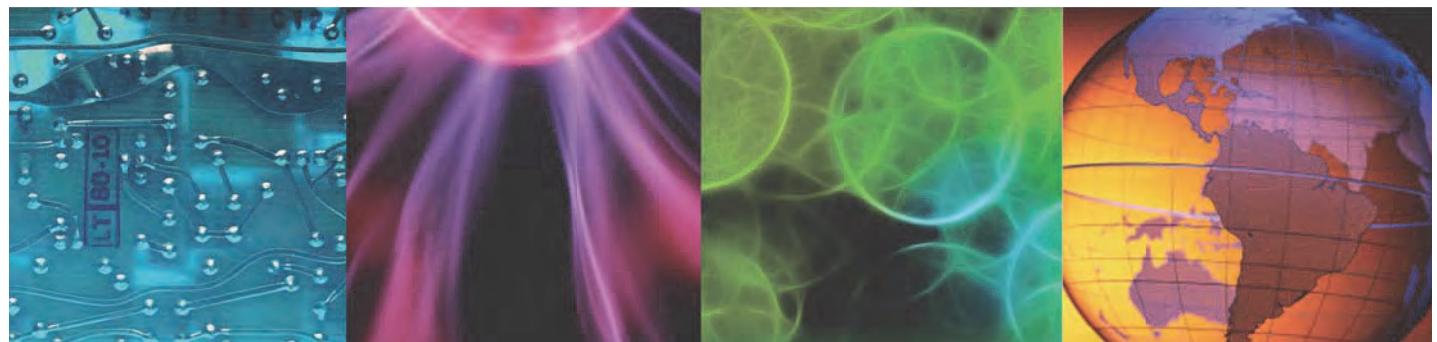
- Log out of Dashboard Application Services Hub.

- 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

TN522 1.0



ibm.com/training

Authorized
IBM | Training