

Course Exercises

# IBM Network Performance Insight 1.3.1

## Installation and Configuration

Course code: TN530 ERC 1.0



## March 2020 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](http://www.ibm.com/legal/copytrade.shtml).

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

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

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

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

ITIL is a Registered Trade Mark of AXELOS Limited.

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

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

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

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

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

**© Copyright International Business Machines Corporation 2016.**

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

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

---

# Contents

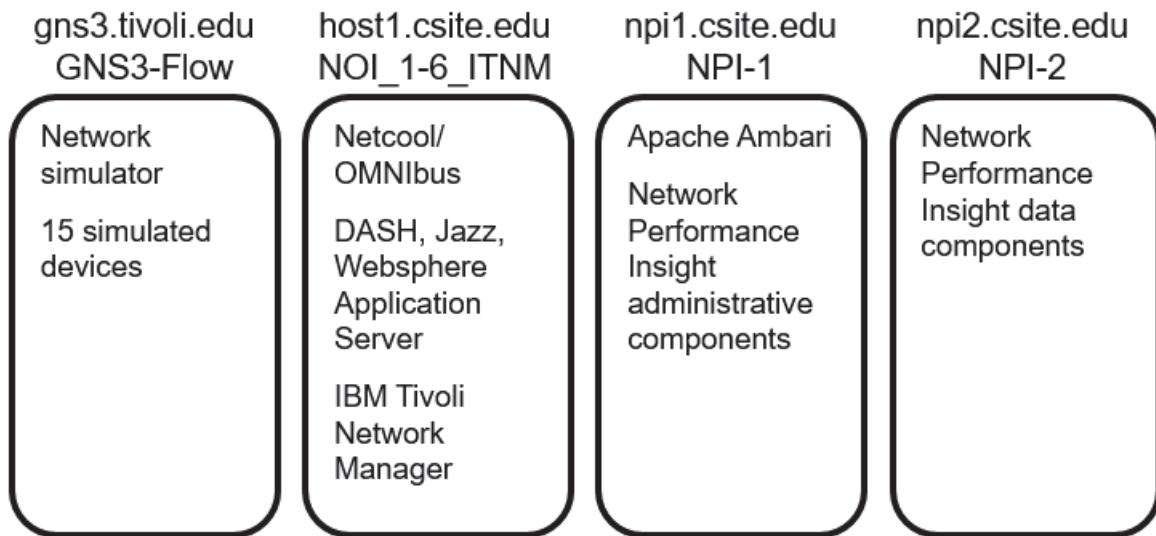
<b>About these exercises .....</b>	<b>1</b>
User IDs and passwords .....	0-2
Commonly used URLs .....	0-2
<b>Unit 1 Overview and installation .....</b>	<b>1-1</b>
Exercise 1 Getting started .....	1-1
Exercise 2 Pre-installation tasks .....	1-10
Exercise 3 Installing Network Performance Insight .....	1-20
<b>Unit 2 Integration.....</b>	<b>2-1</b>
Exercise 1 Integration with IBM Tivoli Network Manager .....	2-1
Exercise 2 Integration with Netcool/OMNibus .....	2-7
Exercise 3 Integration with Dashboard Application Services Hub .....	2-11
<b>Unit 3 Post-installation configuration .....</b>	<b>3-1</b>
Exercise 1 Installing technology packs .....	3-1
Exercise 2 Installing the Device Dashboard .....	3-3
Exercise 3 Installing an interim fix .....	3-17
Exercise 4 Setting the resource scope .....	3-32
<b>Unit 4 Solution verification.....</b>	<b>4-1</b>



# About these exercises

In the exercises for this course, you install Network Performance Insight on two hosts. You also integrate Network Performance Insight with Netcool Operations Insight.

This course includes four virtual images. The following diagram shows the function of each virtual machine.



The host named gns3.tivoli.edu runs a network simulator. After your installation is finished, you monitor the simulated devices with Network Performance Insight.

The host named host1.csuite.edu runs Netcool Operations Insight. Throughout these exercises, you integrate Network Performance Insight with the following Netcool Operations Insight components:

- IBM Tivoli Network Manager, to obtain discovery data and performance metrics
- Dashboard Application Services Hub, to show the Network Performance Insight user interface and dashboards
- Netcool/OMNIbus, to notify operators when a performance metric has violated a threshold

Initially, the host named npi1.csuite.edu is not running any IBM software. You install the Network Performance Insight administrative components on this host, such as Apache Ambari, HDFS, and Zookeeper.

The host named npi2.csuite.edu is not running any IBM software at the start of the lab either. You install the Network Performance Insight services on this host, including the SNMP collector, the flow collector, and the Network Manager collector.

# User IDs and passwords

The user IDs and passwords for this lab are listed in the following table. You create other user IDs and passwords as you complete the lab exercises.

Type	User ID	Password	Usage
Linux	root	object00	Linux super user
Linux	netcool	object00	Linux user who owns all IBM products
Jazz for Service Management and DASH	smadmin	object00	WebSphere, Jazz, and DASH super user

# Commonly used URLs

Dashboard Application Services Hub, which is the common user interface for IBM Netcool Operations Insight software:

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

Ambari Manager, which you use to manage IBM Network Performance Insight:

<http://npi1.csite.edu:8080>

# Unit 1 Overview and installation

In the exercises for this unit, you prepare the hosts, install Ambari, install Hortonworks Data Platform, and install Network Performance Insight

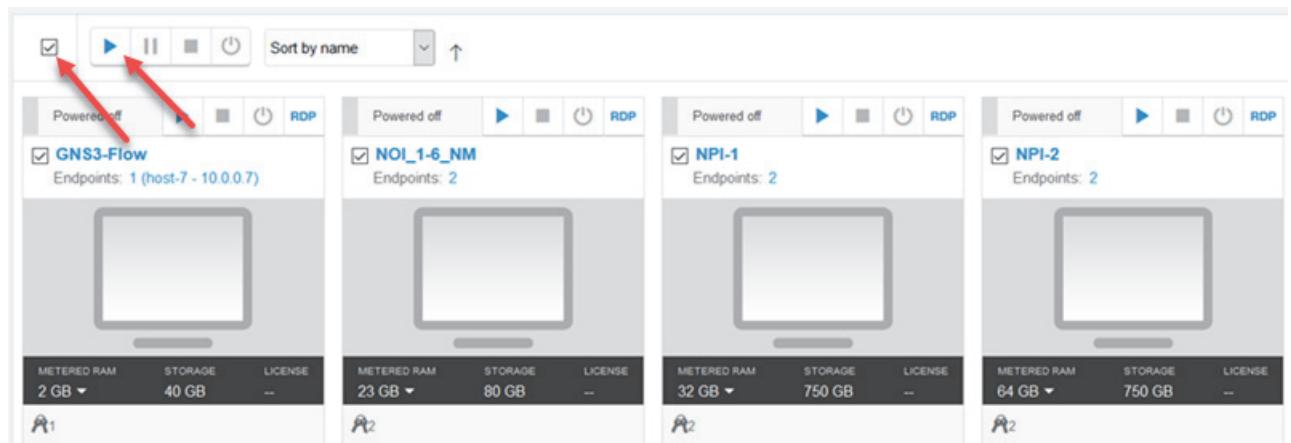
## Exercise 1 Getting started

In this exercise, you start your lab servers and discover a simulated network.

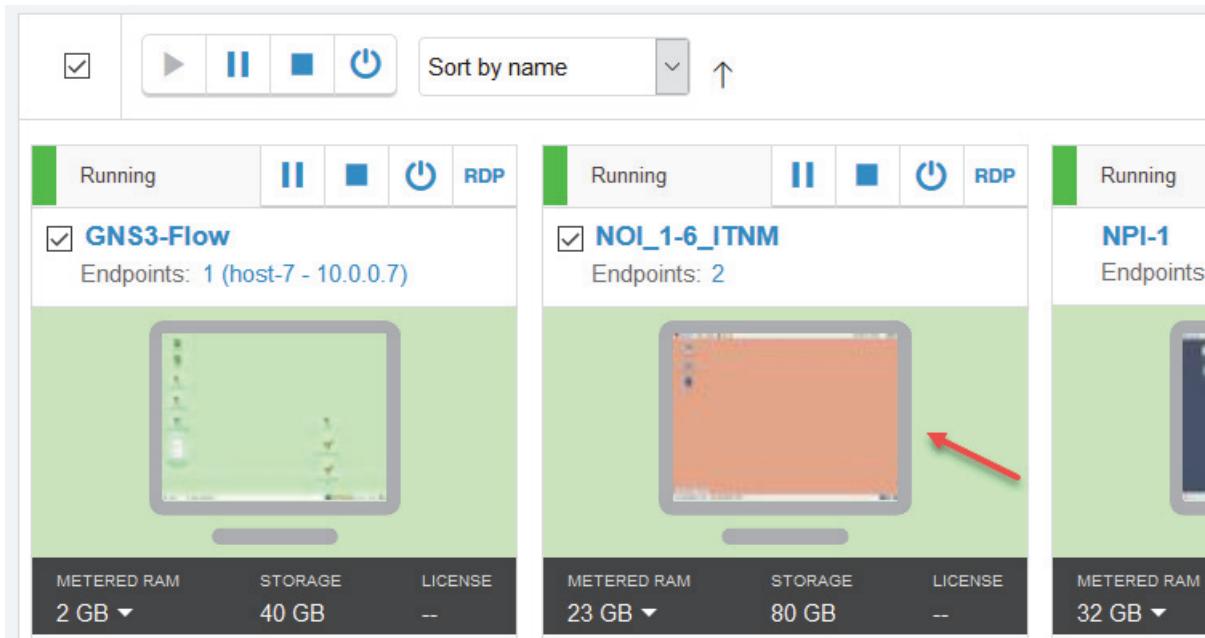
### Starting your lab

In this section, you start your lab servers and verify that they are running.

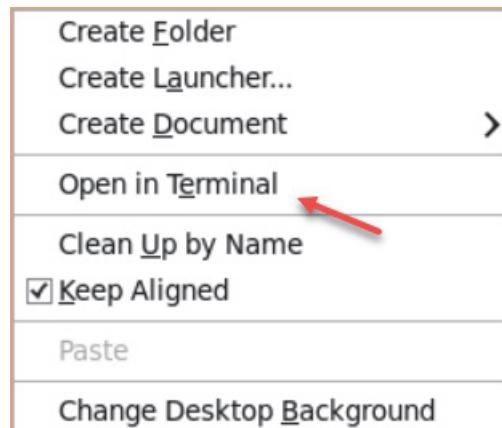
1. Depending on how this course is delivered, your lab servers might already be running. If they are not running, start them now.
  - a. Click the check box at the top left to select all four virtual servers.
  - b. Click the **Run** button to start all four servers. The lab servers take about 10 minutes to completely start.



2. Verify that Netcool/OMNIbus and IBM Tivoli Network Manager are running.
  - a. Click the desktop of the virtual server labeled: **NOI\_1-6\_ITNM**.



- b. Right-click the desktop of the Netcool Operations Insight server and click **Open in Terminal**.



- c. Run the following command to verify that Netcool/OMNIbus is running.  
`nco_ping NOI_AGG_P`

NCO\_PING: Server available.

- d. Run the following command to verify that IBM Tivoli Network Manager is running. All processes should be in the RUNNING state.

```
itnm_status
```

Network Manager:

Domain: NOI_AGG_P			
ncp_ctrl	RUNNING	PID=9726	NOI_AGG_P
ncp_store	RUNNING	PID=10108	NOI_AGG_P
ncp_class	RUNNING	PID=10109	NOI_AGG_P
ncp_model	RUNNING	PID=10634	NOI_AGG_P
ncp_disco	RUNNING	PID=11367	NOI_AGG_P
ncp_d_helpserv	RUNNING	PID=10110	NOI_AGG_P
ncp_config	RUNNING	PID=10111	NOI_AGG_P
ncp_poller_default	RUNNING	PID=12026	NOI_AGG_P
ncp_poller_admin	RUNNING	PID=12027	NOI_AGG_P
nco_p_ncpmonitor	RUNNING	PID=10112	NOI_AGG_P
ncp_g_event	RUNNING	PID=11712	NOI_AGG_P
ncp_webtool	RUNNING	PID=10113	NOI_AGG_P
ncp_virtualdomain	RUNNING	PID=12513	NOI_AGG_P

Apache Storm:

supervisord	RUNNING	PID=5318
storm_nimbus	RUNNING	PID=5329
storm_supervisor	RUNNING	PID=5334
zookeeper	RUNNING	PID=5327

- e. If you receive an error about Apache Storm, run the following commands to remove the lock file and start Apache Storm.

```
rm -rf /opt/IBM/tivoli/netcool/var/precision/storm/sup.skt
```

```
itnm_start storm
```

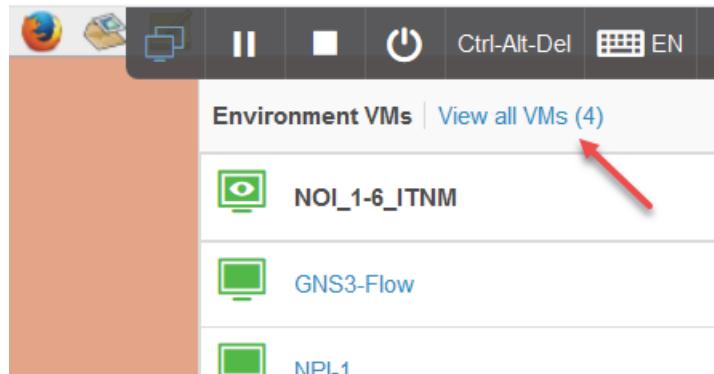
- f. Run the following command again to confirm that all the IBM Tivoli Network Manager processes are running.

```
itnm_status
```

- g. Click the tab at the top of the window to view the lab environment options.

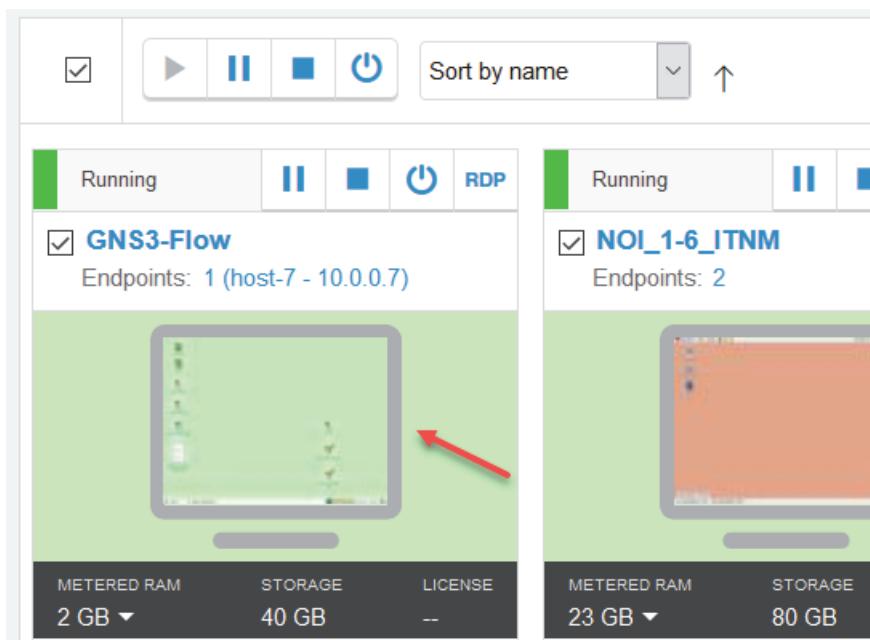


- h. Click the icon for environment VMs. Click **View all VMs**.



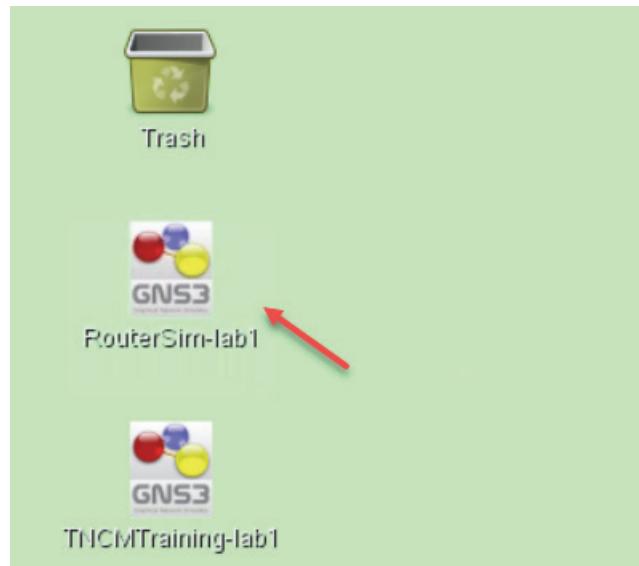
3. Start the network simulator.

- a. Click the desktop of the virtual server labeled: **GNS3-Flow**.

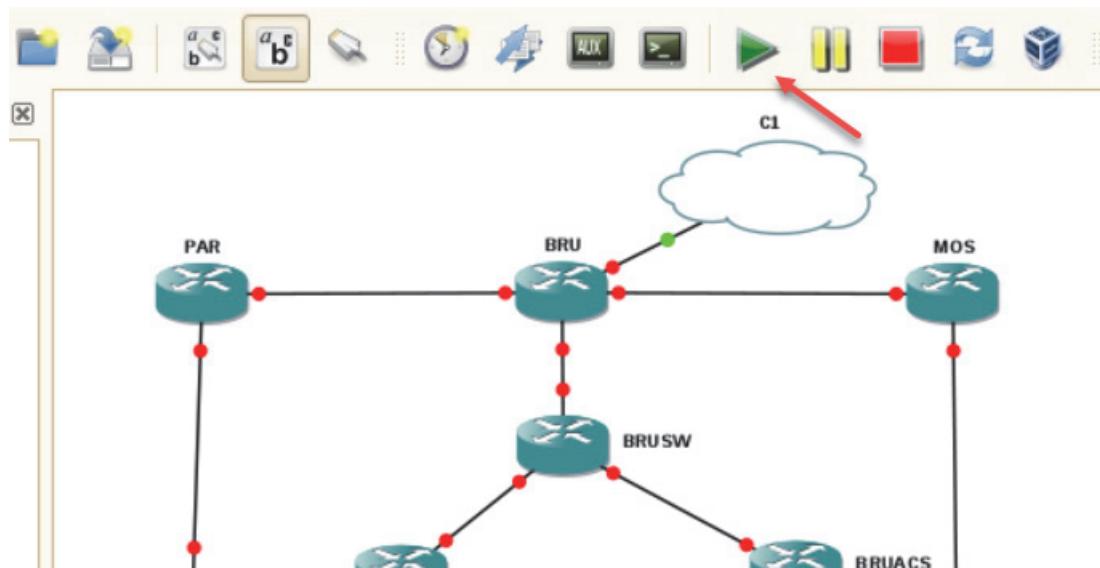


- b. Log in to the host with the user name **root** and the password **object00**.

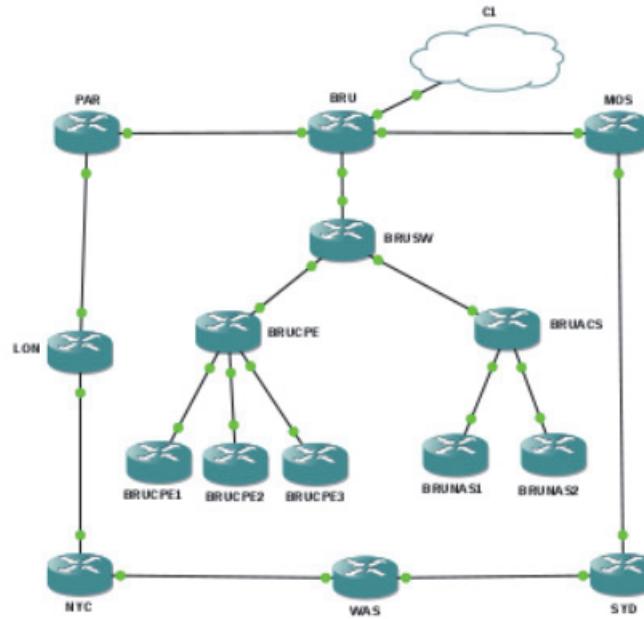
- c. Right-click the **RouterSim-lab1** icon and click **Open**.



- d. After the network diagram loads, click the green start button.



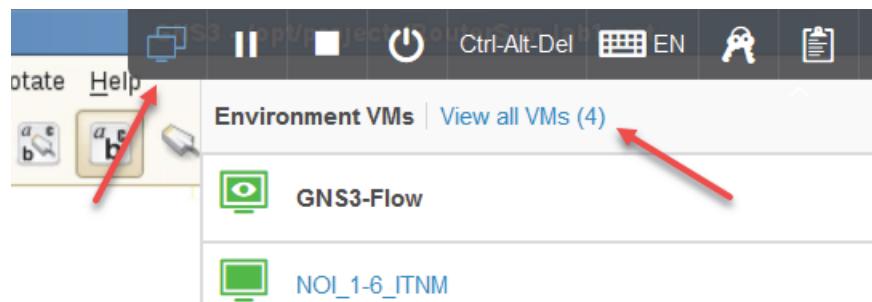
- e. Wait until all of the red dots turn green.



- f. Click the tab at the top of the window to view the lab environment options.



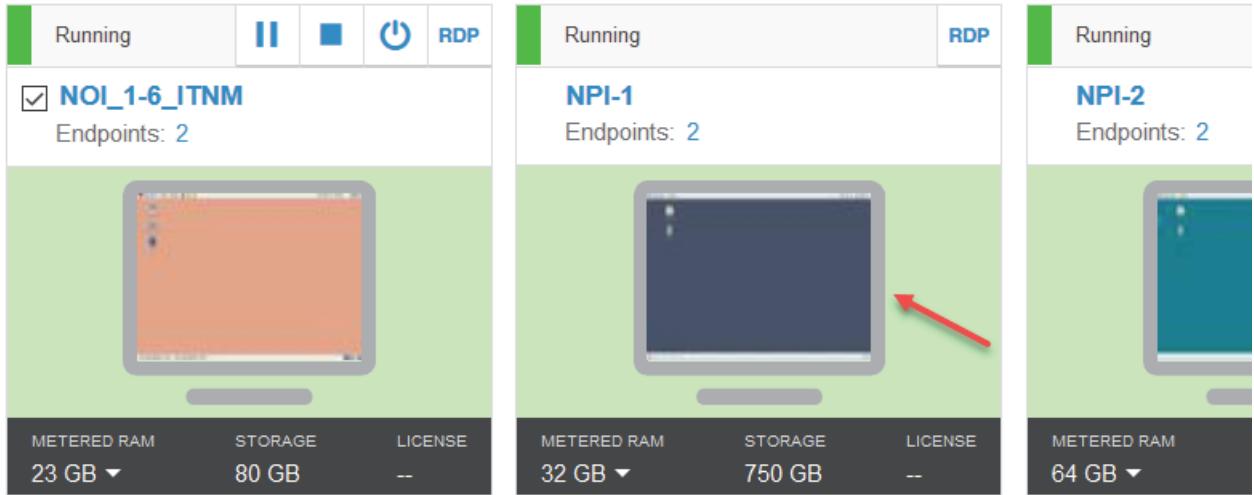
- g. Click the icon for environment VMs. Click **View all VMs**.



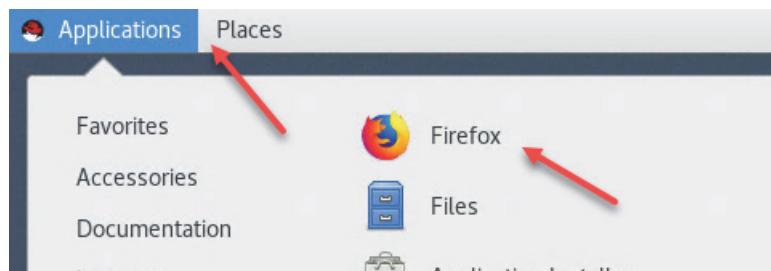
## Discovering the network

In this section, you use IBM Tivoli Network Manager (ITNM) to discover a network of simulated devices.

1. Connect to the first NPI server. Click the desktop of the virtual server labeled: **NPI-1**.

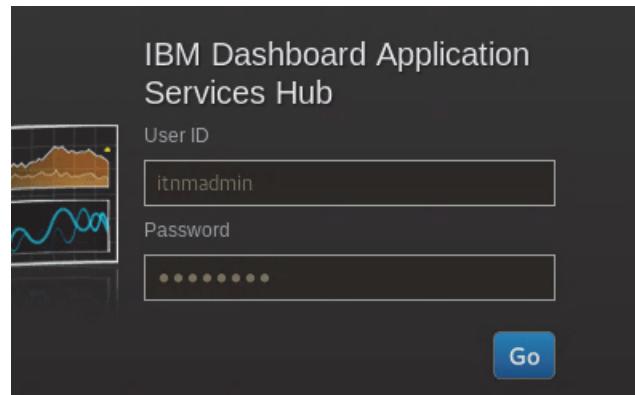


2. Discover the simulated network.
  - a. Open a browser window and login to Dashboard Application Services Hub (DASH) as the **itnmadmin** user.
  - b. Click **Applications > Firefox** at the top left of the desktop.

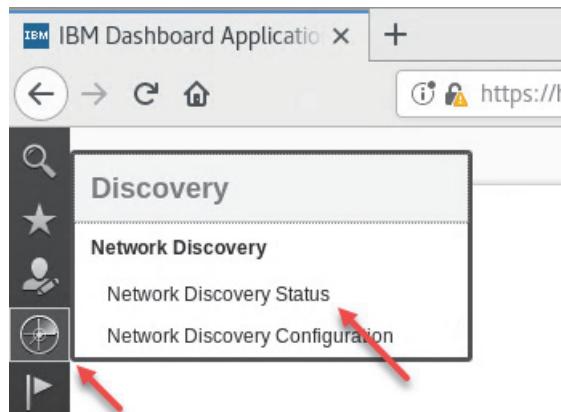


- c. Go to the following URL:  
<https://host1.csite.edu:16311/ibm/console/logon.jsp>

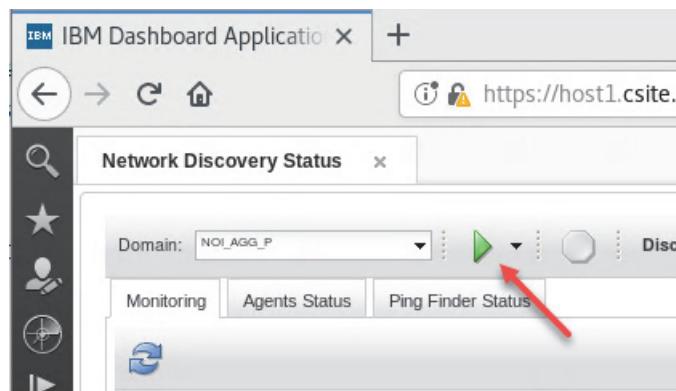
- d. Log in with the user name **itnmadmin** and the password **object00**.



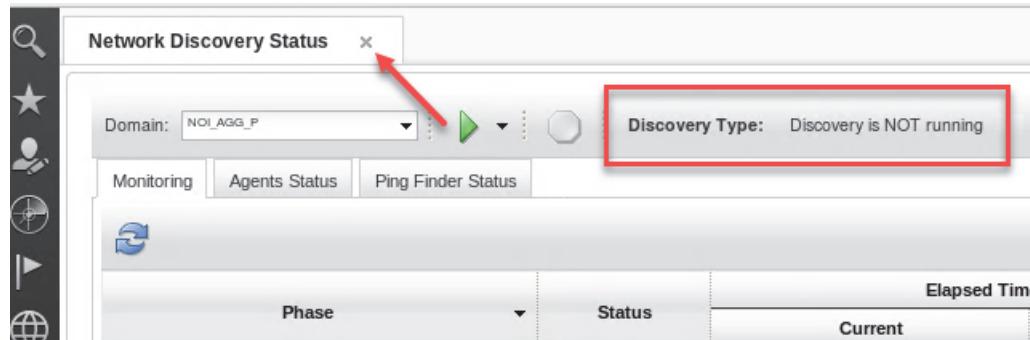
- e. Click **Discovery > Network Discovery Status**.



- f. Click the green start button. Look for the messages: Discovery Starting, or Full Discovery. The discovery process takes about six minutes.



- g. Discovery is finished when you see the message: Discovery is NOT running. Close the Network Discovery Status tab.



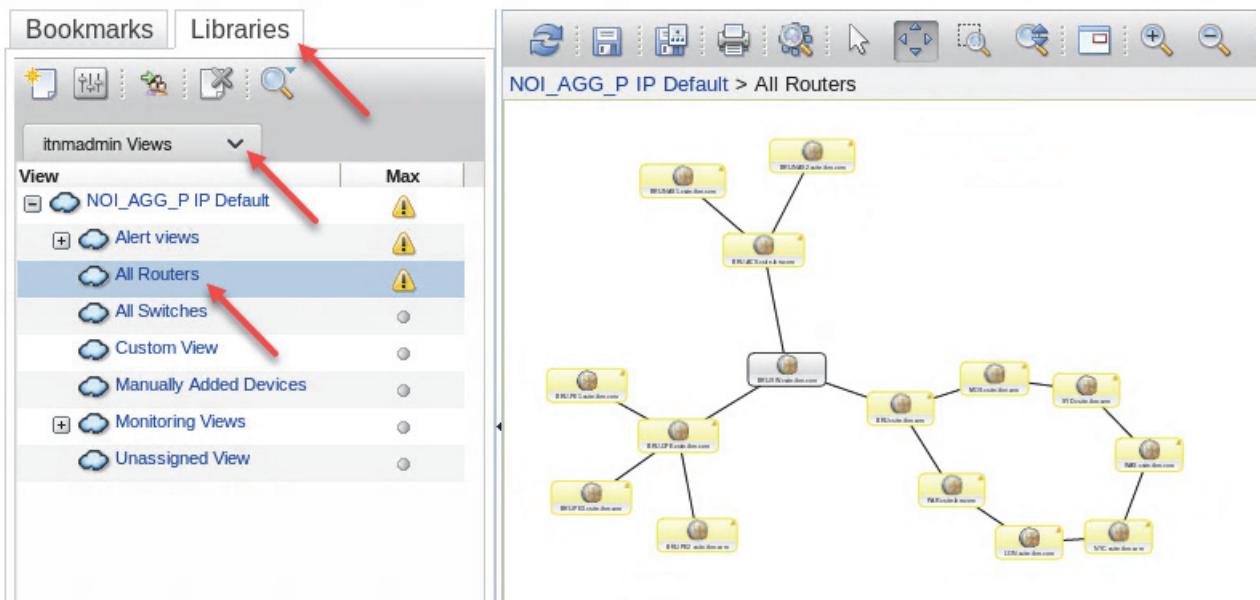
3. Verify that the simulated devices have been discovered.

- a. Click **Incident > Network Views**.

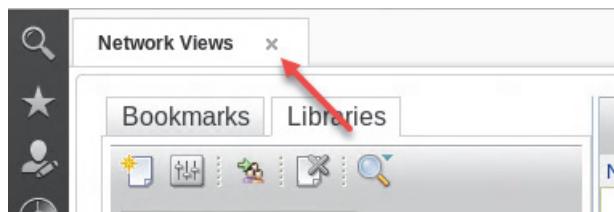


- b. Click the **Libraries** tab.  
c. Select **itnadmin Views**.  
d. Expand **NOI\_AGG\_P IP Default** and click **All Routers**.

- e. Verify that the topology map shows 15 devices.



- f. Close the Network Views tab.



- g. Close the browser window.

- h. Stay connected to the virtual server labeled: **NPI-1**. You use this sever in the next exercise.

## Exercise 2 Pre-installation tasks

You are going to install IBM Network Performance Insight on two hosts: npi1.csuite.edu and npi2.csuite.edu. In this exercise, you prepare the operating system of these two hosts for installation.

1. Decompress the IBM Network Performance Insight installation media.
  - a. Right-click the desktop of npi1.csuite.edu and click **Open Terminal**. The npi1.csuite.edu host is labeled **NPI-1** in your virtual lab environment.
  - b. Run the following commands to change to the correct directory and decompress the installation media.

```
cd /software/NPI/
```

```
tar -zxvf NOIPM_1.3.1_LNX_ML.tgz
```

- c. Run the following commands to change to the CC29WML sub-directory and decompress the installation media.

```
cd /software/NPI/CC29WML/
```

```
tar -zxvf NPI-1.3.1.0.tgz
```

2. Move the Hortonworks Data Platform (HDP) installation packages to the new directory.

- a. Run the following commands to move the installation packages into the CC29WML sub-directory.

```
cd /software/NPI/CC29WML/
```

```
mv /software/HDP/* .
```

- b. Run the following command to verify that the four installation packages are in the correct directory. Verify that the output of the command matches the following example.

```
ls /software/NPI/CC29WML/
```

<b>ambari-2.6.2.2-centos7.tar.gz</b>	<b>HDP-UTILS-1.1.0.22-centos7.tar.gz</b>
<b>HDP-2.6.4.0-centos7-rpm.tar.gz</b>	<b>NPI-1.3.1.0</b>
<b>HDP-GPL-2.6.4.0-centos7-rpm.tar.gz</b>	<b>NPI-1.3.1.0.tgz</b>

3. You are going to install Apache Ambari on npi1.csuite.edu. Apache Ambari requires passwordless SSH authentication to all hosts in the Ambari cluster, including its own host and the host where IBM Netcool Operations Insight is running.

- a. Run the following command to change to the root user. The password is **object00**.

```
su - root
```

Password: **object00**

- b. Run the following utility to configure passwordless SSH authentication to the following three hosts as the root user.

- ◆ npi1.csuite.edu (this is the host where you will install Apache Ambari and Hortonworks Data Platform)
- ◆ npi2.csuite.edu (this is the host where you will install the Network Performance Insight components)
- ◆ host1.csuite.edu (This is the host where Netcool Operations Insight is running)

```
/software/NPI/CC29WML/NPI-1.3.1.0/bin/setup_cluster_ssh.sh
```

- c. Enter **y** when you are prompted to set up remote hosts.

```
Continue to setup remote hosts[Y/n] ? y
```

- d. Enter **npi1.csuite.edu** when you are prompted for the remote host name.

```
Enter remote hostname (FQDN) : npi1.csuite.edu
```

- e. Enter **yes** when you are prompted to continue.

Are you sure you want to continue connecting (yes/no) ? **yes**

- f. Enter **object00** when you are prompted for the password. You will be prompted twice.

root@npi1.csite.edu's password: **object00**

- g. Enter **y** to setup the next remote host.

Continue to setup next remote hosts[Y/n] ? **y**

- h. Enter **npi2.csite.edu** when you are prompted for the remote host name.

Enter remote hostname (FQN) : **npi2.csite.edu**

- i. Enter **yes** when you are prompted to continue.

Are you sure you want to continue connecting (yes/no) ? **yes**

- j. Enter **object00** when you are prompted for the password. You will be prompted twice.

root@npi2.csite.edu's password: **object00**

- k. Enter **y** to setup the next remote host.

Continue to setup next remote hosts[Y/n] ? **y**

- l. Enter **host1.csite.edu** when you are prompted for the remote host name.

Enter remote hostname (FQN) : **host1.csite.edu**

- m. Enter **yes** when you are prompted to continue.

Are you sure you want to continue connecting (yes/no) ? **yes**

- n. Enter **object00** when you are prompted for the password. You will be prompted twice.

root@host1.csite.edu's password: **object00**

- o. Enter **n** when you are prompted to setup the next host. This action exits the setup utility.

Continue to setup next remote hosts[Y/n] ? **n**

4. Verify that passwordless SSH authentication is configured for the root user on npi1.csite.edu.

Run the following commands and confirm that you are not prompted for a password.

ssh npi1.csite.edu

Last login: Mon Oct 28 13:16:59 2019

exit

Connection to npi1.csite.edu closed.

5. Verify that passwordless SSH authentication is configured for the root user on npi2.csite.edu. Run the following commands and confirm that you are not prompted for a password.

```
ssh npi2.csite.edu
Last login: Mon Oct 21 13:34:23 2019
```

```
exit
```

```
Connection to npi2.csite.edu closed.
```

6. Verify that passwordless SSH authentication is configured for the root user on host1.csite.edu. Run the following commands and confirm that you are not prompted for a password.

```
ssh host1.csite.edu
```

```
exit
```

```
Connection to host1.csite.edu closed.
```

7. Netcool Operations Insight is installed on host1.csite.edu and runs as the netcool user. Setup passwordless SSH from npi1.csite.edu as the root user to host1.csite.edu as the netcool user.
  - a. Run the following command to change to the correct directory.

```
cd /root/.ssh
```

- b. Run the following command to copy the public keys to host1.csite.edu. Enter **object00** as the password.

```
ssh-copy-id -i id_rsa.pub netcool@host1.csite.edu
```

```
/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "id_rsa.pub"
/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out
any that are already installed
/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted
now it is to install the new keys
```

```
netcool@host1.csite.edu's password: object00
```

- c. Verify that passwordless ssh authentication is configured for root from npi1.csite.edu to host1.csite.edu as the netcool user. Run the following commands and confirm that you are not prompted for a password.

```
ssh netcool@host1.csite.edu
```

```
exit
```

```
Connection to host1.csite.edu closed
```

8. Setup passwordless SSH from np1.csite.edu as the netcool user to host1.csite.edu as the netcool user.
  - a. Open a new terminal window. Run the following command to verify that you are the netcool user.

```
whoami
```

```
netcool
```

- b. Run the following command to generate the public key. Press Enter to accept all of the default settings.

```
ssh-keygen
```

- c. Run the following command to copy the public keys to host1.csite.edu. Enter **yes** to continue. Enter **object00** as the password.

```
ssh-copy-id -i ~/.ssh/id_rsa.pub host1.csite.edu
```

- d. Verify that passwordless ssh authentication is configured for netcool from np1.csite.edu to host1.csite.edu as the netcool user. Run the following commands and confirm that you are not prompted for a password.

```
ssh host1.csite.edu
```

```
exit
```

```
Connection to host1.csite.edu closed.
```

- e. Close the terminal window where you are the netcool user.

9. Configure system settings on the np1.csite.edu host.

- a. Return to the terminal window where you are the root user. Open the /etc/sysctl.conf in a text editor.

```
vi /etc/sysctl.conf
```

- b. Add the following lines to the bottom of the file. Save and close the file when you are finished.

```
net.core.rmem_default = 33554432  
net.core.rmem_max = 33554432  
net.core.netdev_max_backlog = 10000
```

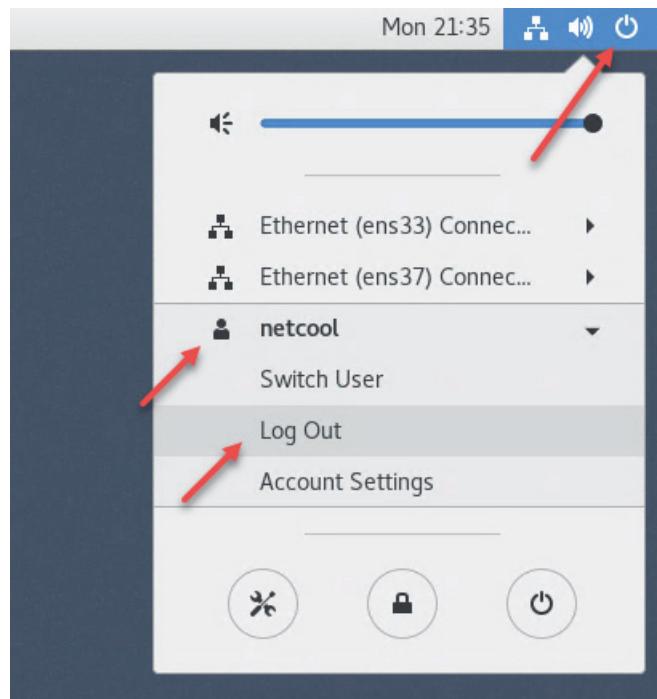
- c. Run the following command to refresh the host with the new configuration.

```
sysctl -p
```

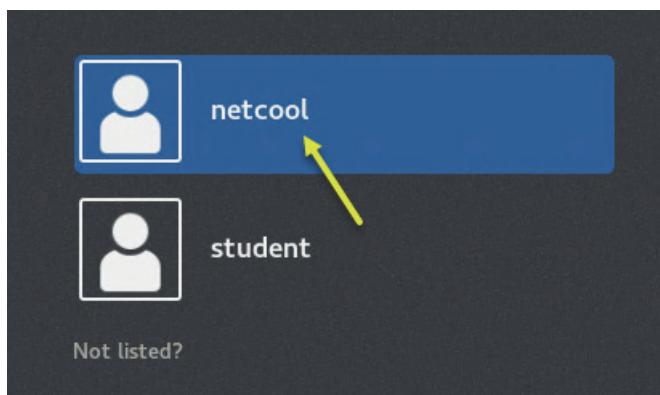
- d. Increase the number of processes and open files permitted for all users. Run the following command to create and open a configuration drop-in file.

```
vi /etc/security/limits.d/30-nproc.conf
```

- e. Add the following lines to the file. Save and close the file when you are finished.  
\* -nofile 65536  
\* -nproc 65536
- f. Type **exit** to close the terminal session as the root user.
- g. Type **exit** again to close the terminal window.
- h. Click the power icon at the top right of the desktop.
- i. Expand the **netcool** user.
- j. Click **Log Out**. You must log out and log back in to apply the changes.



- k. Click **Log Out** to confirm.
- l. Click the **netcool** user to log back in. Enter **object00** as the password.



- m. Right-click the desktop and click **Open Terminal**.
- n. Run the following commands to verify that the resource limits have been changed for the netcool user.

```
ulimit -n  
65536
```

```
ulimit -u  
65536
```

- o. Change to the root user. Use **object00** as the password.

```
su - root  
Password: object00
```

- p. Run the following commands to verify that the resource limits have been changed for the root user.

```
ulimit -n  
65536
```

```
ulimit -u  
65536
```

## 10. Configure system settings on the npi2.csite.edu host.

- a. Connect to the npi2.csite.edu host.

```
ssh npi2.csite.edu
```

- b. Verify that you are logged in as the root user.

```
whoami
```

```
root
```

- c. Open the /etc/sysctl.conf file in a text editor.

```
vi /etc/sysctl.conf
```

- d. Add the following lines to the bottom of the file. Save and close the file when you are finished.

```
net.core.rmem_default = 33554432  
net.core.rmem_max = 33554432  
net.core.netdev_max_backlog = 10000
```

- e. Run the following command to refresh the host with the new configuration.

```
sysctl -p
```

- f. Open the existing configuration drop-in file with a text editor.

```
vi /etc/security/limits.d/20-nproc.conf
```

- g. Add the comment character (#) in front of the following two lines. Save and close the file when you are finished.

```
#*          soft      nproc      4096
#root      soft      nproc      unlimited
```

- h. Increase the number of processes and open files permitted for all users. Run the following command to create and open a configuration drop-in file.

```
vi /etc/security/limits.d/30-nproc.conf
```

- i. Add the following lines to the file. Save and close the file when you are finished.

```
* - nofile 65536
* - nproc 65536
```

- j. Type **exit** to close the connection to npi2.csite.edu. You must log out and log back in to apply the changes.

```
exit
```

- k. Connect to npi2.csite.edu again.

```
ssh npi2.csite.edu
```

- l. Run the following commands to verify that the resource limits have been changed for the root user.

```
ulimit -n
65536
```

```
ulimit -u
65536
```

- m. Run the following command to change to the netcool user.

```
su - netcool
```

- n. Run the following commands to verify that the resource limits have been changed for the netcool user.

```
ulimit -n
65536
```

```
ulimit -u
65536
```

- o. Type **exit** to end the session as the netcool user.

- p. Type **exit** again to close the connection to npi2.csite.edu.

11. Configure npi1.csite.edu and npi2.csite.edu so that users do not need a controlling terminal to run commands.

- a. Run the following command to edit the sudoers file.

```
visudo
```

- b. Add the following line to the bottom of the file. Save and close the file when you are finished.

```
Defaults !requiretty
```

- c. Connect to the npi2.csite.edu host.

```
ssh npi2.csite.edu
```

- d. Run the following command to edit the sudoers file.

```
visudo
```

- e. Add the following line to the bottom of the file. Save and close the file when you are finished.

```
Defaults !requiretty
```

- f. Type **exit** to close the connection to npi2.csite.edu.

12. Run the following **rpm -qa** commands to verify that the required operating system packages are installed on npi1.csite.edu.

```
rpm -qa libtirpc-devel  
libtirpc-devel-0.2.4-0.16.el7.x86_64
```

```
rpm -qa redhat-lsb  
redhat-lsb-4.1-27.el7.x86_64
```

```
rpm -qa python-devel  
python-devel-2.7.5-86.el7.x86_64
```

```
rpm -qa gcc  
gcc-4.8.5-39.el7.x86_64
```

13. Run the following commands to verify that the required operating system packages are installed on npi2.csite.edu.

```
ssh npi2.csite.edu rpm -qa libtirpc-devel  
libtirpc-devel-0.2.4-0.16.el7.x86_64
```

```
ssh npi2.csite.edu rpm -qa redhat-lsb  
redhat-lsb-4.1-27.el7.x86_64
```

```
ssh npi2.csite.edu rpm -qa python-devel  
python-devel-2.7.5-86.el7.x86_64
```

```
ssh npi2.csite.edu rpm -qa gcc  
gcc-4.8.5-39.el7.x86_64
```

14. Disable the python security certificate verification on npi1.csite.edu and npi2.csite.edu.

- a. Open the cert-verification.cfg file in a text editor.

```
vi /etc/python/cert-verification.cfg
```

- b. Edit the following option and change the **verify** setting to **disabled**. Save and close the file when you are finished.

```
verify=disable
```

- c. Connect to the npi2.csite.edu host.

```
ssh npi2.csite.edu
```

- d. Open the cert-verification.cfg file in a text editor.

```
vi /etc/python/cert-verification.cfg
```

- e. Edit the following option and change the **verify** setting to **disabled**. Save and close the file when you are finished.

```
verify=disable
```

- f. Type **exit** to close the connection to npi2.csite.edu.

15. Stop and disable the firewalld service on npi1.csite.edu and npi2.csite.edu.

- a. Run the following commands to stop and disable the service on npi1.csite.edu.

```
systemctl stop firewalld.service
```

```
systemctl disable firewalld.service
```

- b. Run the following command to verify that the service is disabled on npi1.csite.edu.

```
systemctl status firewalld.service
```

```
firewalld.service - firewalld - dynamic firewall daemon
```

```
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor
   preset: enabled)
```

```
     Active: inactive (dead)
```

```
       Docs: man:firewalld(1)
```

- c. Run the following commands to stop and disable the service on npi2.csite.edu.

```
ssh npi2.csite.edu systemctl stop firewalld.service
```

```
ssh npi2.csite.edu systemctl disable firewalld.service
```

- d. Run the following command to verify that the service is disabled on npi2.csite.edu.

```
ssh npi2.csite.edu systemctl status firewalld.service
```

```
firewalld.service - firewalld - dynamic firewall daemon
```

```
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor
   preset: enabled)
```

```
     Active: inactive (dead)
```

```
       Docs: man:firewalld(1)
```

16. Run the following commands to remove the existing yum cache on npi1.csite.edu and npi2.csite.edu.

```
rm -rf /var/cache/yum
```

```
ssh npi2.csite.edu rm -rf /var/cache/yum
```

## Exercise 3 Installing Network Performance Insight

In this exercise, you install Apache Ambari, Hortonworks Data Platform (HDP), and Network Performance Insight.

### ***Installing Ambari and Hortonworks Data Platform (HDP)***

1. Verify your environment.

- a. Verify that you are connected to the host npi1.csite.edu and you are working as the root user.

- b. Change to the installer directory.

```
cd /software/NPI/CC29WML/NPI-1.3.1.0/bin/
```

2. Configure and run the package installer.

- a. Run the following command to start the package installer. The directory in the command is the location of the Network Performance Insight and Hortonworks Data Platform installation media.

```
./install.sh /software/NPI/CC29WML
```

```
Validating HDP packages completed
```

```
INFO: Verifying NPI relevant packages started...
```

- b. Enter **2** as the number of hosts in the cluster.

```
Enter the number of hosts that will be a part of cluster including ambari host
```

```
2
```

- c. Enter **npi1.csite.edu** as the first host name.

```
Enter the hostname that will be part of cluster
```

```
npi1.csite.edu
```

- d. If you are prompted to continue after warnings in the log file, enter **y**.

Please check the WARNINGS before proceeding. The log file is at  
npi1.csuite.edu:/tmp

Do you want to continue(y/n)

**y**

- e. Enter **npi2.csuite.edu** as the next host name.

Enter the hostname that will be part of cluster

**npi2.csuite.edu**

- f. If you are prompted to continue after warnings in the log file, enter **y**.

Please check the WARNINGS before proceeding. The log file is at  
npi2.csuite.edu:/tmp

Do you want to continue(y/n)

**y**

- g. After 5-10 minutes, the installer finishes. Verify that the installation is complete before you continue.

Complete!

INFO: Install NPI packages completed

## **Setting up and deploying your Network Performance Insight cluster**

1. Start the installation wizard.

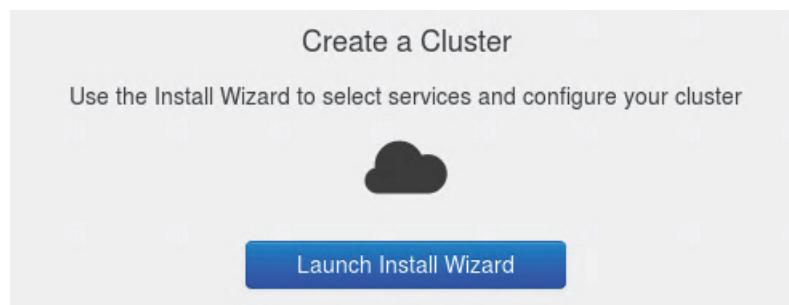
- a. Run the following command to start Firefox as the root user.

firefox &

- b. Browse to the following URL. Log in with the user name **admin** and the password **admin**.

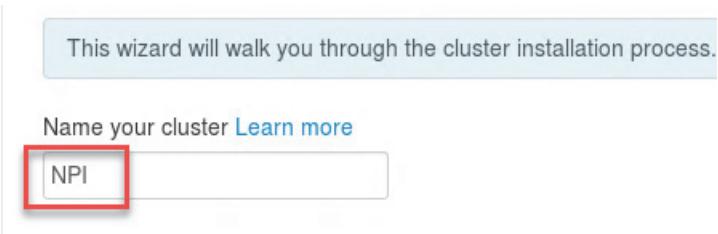
<http://npi1.csuite.edu:8080>

- c. Click **Launch Install Wizard**.



2. Register your target hosts.

- a. Enter **NPI** as the name of the cluster and click **Next**.



- b. Verify that **HDP-2.6.NPI** is the selected version.

- c. Verify that the **Use Public Repository** is selected.

- d. Click **Next**.

HDP-2.6.NPI

HDP-2.6

HDP-2.5

HDP-2.4

Use Public Repository

Use Local Repository

Component	Count
Ambari Metrics	0
Cassandra	3
HDFS	2
Kafka	0
NPI	1
NPI Spark Client Scala 2.11	2
YARN	2

- e. Enter the following host names, one per line, into the **Target Hosts** field.

npi1.csuite.edu

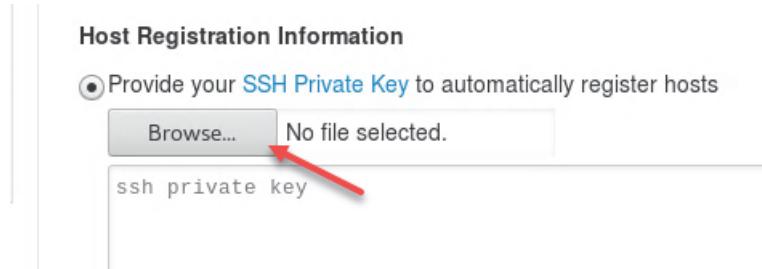
npi2.csuite.edu

**Target Hosts**

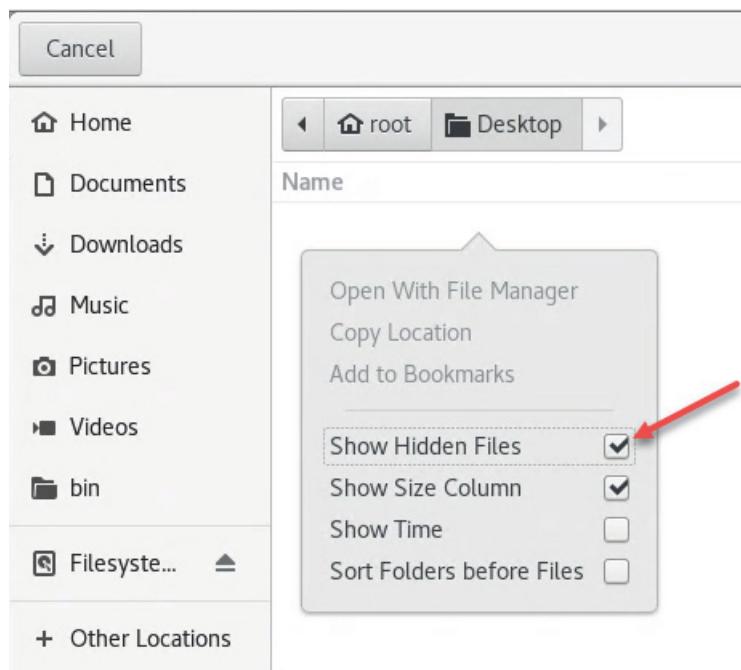
Enter a list of hosts using the Fully Qualified Domain Name

npi1.csuite.edu  
npi2.csuite.edu

- f. Click **Browse** in the Host Registration Information field.

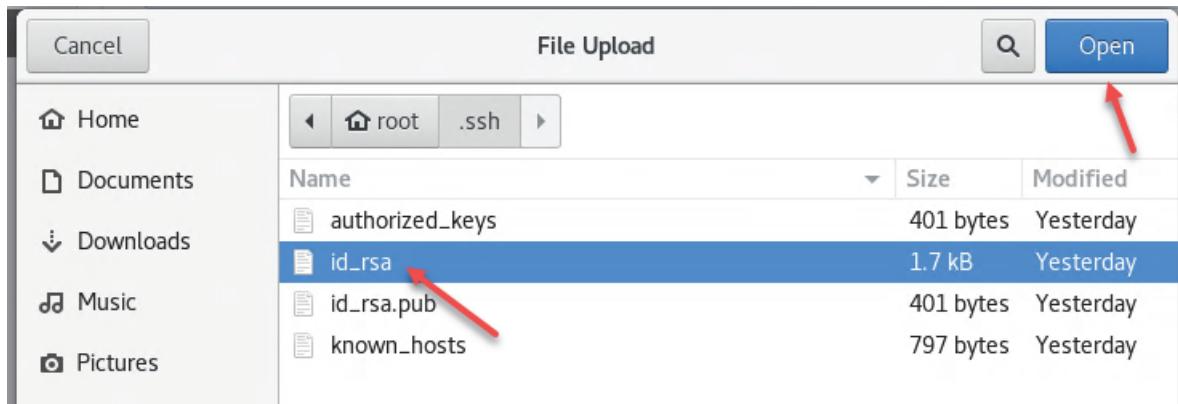


- g. Right-click the file window, then select **Show Hidden Files**.

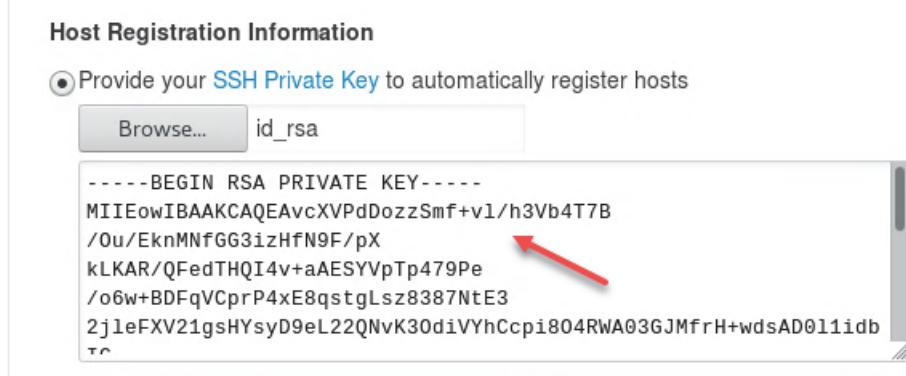


- h. Browse to the **/root/.ssh** directory.

- i. Select the **id\_rsa** file, then click **Open**.



- j. Confirm that the private key is in the **Host Registration Information** field, then click **Register and Confirm**.



- k. The Confirm Hosts page shows the status of your hosts as **Installing**, then as **Registering**. After a few moments, the status changes to **Failed**. This is expected.

## Confirm Hosts

Registering your hosts.  
Please confirm the host list and remove any hosts that you do not want to include in the cluster.

		<input type="button" value="Remove Selected"/>	<input type="button" value="Retry Failed"/>	Show:	All (2)	<a href="#">Installing (0)</a>	<a href="#">Registering (0)</a>	<input type="button" value=""/>
	Host	Progress	Status	A				
<input type="checkbox"/>	npi1.csuite.edu	<div style="width: 20%; background-color: #f08080;"></div>	Failed	<input type="button" value=""/>				
<input type="checkbox"/>	npi2.csuite.edu	<div style="width: 20%; background-color: #f08080;"></div>	Failed	<input type="button" value=""/>				



**Hint:** You must change the Ambari agent TLS version to 1.2 on npi1.csuite.edu and npi2.csuite.edu.

- l. Return to the terminal window where you are the root user. Run the following command to open the Ambari agent configuration file.

```
vi /etc/ambari-agent/conf/ambari-agent.ini
```

- m. Find the [security] section of the file. Add the following line below the [security] line. Save and close the file when you are finished.

```
[security]
force_https_protocol=PROTOCOL_TLSv1_2
```

- n. Run the following command to connect to npi2.csuite.edu.

```
ssh npi2.csuite.edu
```

- o. Run the following command to open the Ambari agent configuration file.

```
vi /etc/ambari-agent/conf/ambari-agent.ini
```

- p. Find the [security] section of the file. Add the following line below the [security] line.  
Save and close the file when you are finished.

```
[security]  
force_https_protocol=PROTOCOL_TLSv1_2
```

- q. Type **exit** to close the connection to npi2.csuite.edu.  
r. Return to the Firefox browser where the installation wizard is running.  
s. Click **Retry Failed**.

## Confirm Hosts

Registering your hosts.  
Please confirm the host list and remove any hosts that you do not want to include in the cluster.

		<input type="button" value="Remove Selected"/>	<input type="button" value="C Retry Failed"/>	Show:	All (2)   <a href="#">Installing (0)</a>   <a href="#">Registering (0)</a>   <a href="#">A</a>
	Host	Progress	Status	A	
<input type="checkbox"/>	npi1.csuite.edu	<div style="width: 0%; background-color: red;"></div>	Failed	<input type="button" value="Edit"/>	
<input type="checkbox"/>	npi2.csuite.edu	<div style="width: 0%; background-color: red;"></div>	Failed	<input type="button" value="Edit"/>	

- t. Confirm that the status of both hosts is **Success**, then click **Next**.

Host	Progress	Status	Action
npi1.csuite.edu	<div style="width: 100%; background-color: green;"></div>	Success	<input type="button" value="Edit"/>
npi2.csuite.edu	<div style="width: 100%; background-color: green;"></div>	Success	<input type="button" value="Edit"/>

3. Configure and deploy your Network Performance Insight cluster.
- Leave all of the default options selected on the Choose Services page, then click **Next**.
  - Leave all of the default options selected on the Assign Masters page, then click **Next**.

- c. De-select **Cacti Collector** and **Timeseries Exporter** on the Assign Slaves and Clients page, then click **Next**.

The screenshot shows a table with two rows of checkboxes. The first row has columns for 'Dashboard' and 'Cacti Collector' (unchecked), 'DNS' (unchecked), 'Event' (unchecked), 'Timeseries Exporter' (unchecked), 'Flow Analytics' (unchecked), and 'Filebeat' (unchecked). The second row has columns for 'Dashboard' and 'Cacti Collector' (unchecked), 'DNS' (checked), 'Event' (checked), 'Timeseries Exporter' (unchecked), 'Flow Analytics' (checked), and 'Filebeat' (checked). Red boxes highlight the 'Cacti Collector' and 'Timeseries Exporter' checkboxes in both rows. Below the table is a pagination bar with 'Show: 25' and '1 - 2 of 2'. At the bottom right is a green 'Next →' button.



**Note:** Network Performance Insight can use metric data from Cacti, which is a monitoring tool. You do not have Cacti in your classroom environment, so you do not need to install the Cacti Collector. The Timeseries Exporter component sends metric data from Network Performance Insight to an external software interface. You will not be exporting any metric data in this course, so you do not need to install the Timeseries Exporter.

- d. Click the **Ambari Metrics** tab on the Customize Services page.

## Customize Services

We have come up with recommended configurations for the services you selected.

HDFS YARN MapReduce2 ZooKeeper Ambari Metrics 1 Kafka  
NPI Spark Client Scala 2.11 Misc

- e. Enter **admin** as the Grafana admin password. Enter **admin** again to confirm.

The screenshot shows a form for Grafana Admin configuration. It has fields for 'Grafana Admin Username' (containing 'admin') and 'Grafana Admin Password' (containing two input fields: 'Type password' and 'Retype Password', both highlighted with a red box). Below the form is a section titled 'Metric Collector' with a dropdown arrow.

- f. Click the **Cassandra** tab. Expand **Advanced cassandra-site**.

The screenshot shows the Ambari interface with the 'Cassandra' tab selected. Below the tabs, there is a 'Manage Config Groups' section with a dropdown set to 'Default (2)'. Underneath, there are three configuration groups: 'Advanced cassandra-env', 'Advanced cassandra-site' (which has a red circle with '1' indicating changes), and 'Custom cassandra-env'. The 'Advanced cassandra-site' group is expanded, showing its contents.

- g. Scroll down and enter "npi2.csuite.edu" in the **seed\_provider\_parameters\_seeds** field. Be sure to include the double-quotes before and after the host name.

A screenshot of the 'Advanced cassandra-site' configuration page. It shows three fields: 'seed\_provider\_class\_name' (set to 'org.apache.cassandra.locator.SimpleSeedProvider'), 'seed\_provider\_parameters\_seeds' (containing the value '"npi2.csuite.edu"'), and 'server\_encryption\_level' (set to 'none'). The 'seed\_provider\_parameters\_seeds' field is highlighted with a red box.

- h. Click the **NPI** tab. Click the **NPI settings** tab.

The screenshot shows the Ambari interface with the 'NPI' tab selected. Below the tabs, there is a 'Manage Config Groups' section with a dropdown set to 'Default (2)'. Underneath, there are three tabs: 'NOI Core Settings', 'NPI Settings' (which has a red arrow pointing to it), and 'Advanced'. The 'NPI Settings' tab is selected.

- i. Scroll down and enter **npi2.csite.edu:13081** in the **storage.jdbc-service** field.

NPI Common

storage.jdbc-service

npi2.csite.edu:13081

kafka.zk-connect

{{{zookeeper.connect}}}

- j. Scroll down and enter **admin** in the **manager.ambari.user** field. Enter **admin** again in the **manager.ambari.password** fields.

NPI Manager

manager.ambari.user

admin

manager.ambari.password

.....

Retype Password

- k. Scroll to the bottom of the page and click **Next**.
- l. Click **Proceed Anyway** on the warning about the value of the mapreduce.reduce.memory.mb property.
- m. Click **Deploy** at the bottom of the Review page. The deployment process runs for about 35 minutes.

- n. Verify that the deployment is successful on both hosts, then click **Next**.

Show: All (2)   In Progress (0)   Warning (0)   Success (2)   Fail (0)		
Host	Status	Message
npi1.csuite.edu	100%	Success
npi2.csuite.edu	100%	Success
2 of 2 hosts showing - Show All		
Show: 25   1 - 2 of 2   < >		

Successfully installed and started the services.

[Next →](#)

- o. Click **Complete** on the Summary page.  
 p. In the menu on the left of the page, click NPI. Scroll down and verify that all NPI services are running. Look for green numbers indicating that each expected instance is running, for example, 1/1.

Summary			Configs																																																			
<b>Summary</b>																																																						
<table border="1"> <tbody> <tr> <td><a href="#">Manager</a></td> <td>Started</td> <td>No alerts</td> </tr> <tr> <td><a href="#">Manager</a></td> <td>Started</td> <td>No alerts</td> </tr> <tr> <td><a href="#">Dashboard</a></td> <td>1/1</td> <td>Dashboard Live</td> </tr> <tr> <td><a href="#">Cacti Collector</a></td> <td>0/0</td> <td>Cacti Collector Live</td> </tr> <tr> <td><a href="#">DNS</a></td> <td>1/1</td> <td>DNS Live</td> </tr> <tr> <td><a href="#">Event</a></td> <td>1/1</td> <td>Event Live</td> </tr> <tr> <td><a href="#">Timeseries Exporter</a></td> <td>0/0</td> <td>Timeseries Exporter Live</td> </tr> <tr> <td><a href="#">Flow Analytics</a></td> <td>1/1</td> <td>Flow Analytics Live</td> </tr> <tr> <td><a href="#">Flow Collector</a></td> <td>1/1</td> <td>Flow Collector Live</td> </tr> <tr> <td><a href="#">Formula Service</a></td> <td>1/1</td> <td>Formula Service Live</td> </tr> <tr> <td><a href="#">Inventory</a></td> <td>1/1</td> <td>Inventory Live</td> </tr> <tr> <td><a href="#">NM Collector</a></td> <td>1/1</td> <td>NM Collector Live</td> </tr> <tr> <td><a href="#">SNMP Collector</a></td> <td>1/1</td> <td>SNMP Collector Live</td> </tr> <tr> <td><a href="#">Storage</a></td> <td>1/1</td> <td>Storage Live</td> </tr> <tr> <td><a href="#">Threshold</a></td> <td>1/1</td> <td>Threshold Live</td> </tr> <tr> <td><a href="#">Timeseries</a></td> <td>1/1</td> <td>Timeseries Live</td> </tr> <tr> <td><a href="#">UI</a></td> <td>1/1</td> <td>UI Live</td> </tr> </tbody> </table>				<a href="#">Manager</a>	Started	No alerts	<a href="#">Manager</a>	Started	No alerts	<a href="#">Dashboard</a>	1/1	Dashboard Live	<a href="#">Cacti Collector</a>	0/0	Cacti Collector Live	<a href="#">DNS</a>	1/1	DNS Live	<a href="#">Event</a>	1/1	Event Live	<a href="#">Timeseries Exporter</a>	0/0	Timeseries Exporter Live	<a href="#">Flow Analytics</a>	1/1	Flow Analytics Live	<a href="#">Flow Collector</a>	1/1	Flow Collector Live	<a href="#">Formula Service</a>	1/1	Formula Service Live	<a href="#">Inventory</a>	1/1	Inventory Live	<a href="#">NM Collector</a>	1/1	NM Collector Live	<a href="#">SNMP Collector</a>	1/1	SNMP Collector Live	<a href="#">Storage</a>	1/1	Storage Live	<a href="#">Threshold</a>	1/1	Threshold Live	<a href="#">Timeseries</a>	1/1	Timeseries Live	<a href="#">UI</a>	1/1	UI Live
<a href="#">Manager</a>	Started	No alerts																																																				
<a href="#">Manager</a>	Started	No alerts																																																				
<a href="#">Dashboard</a>	1/1	Dashboard Live																																																				
<a href="#">Cacti Collector</a>	0/0	Cacti Collector Live																																																				
<a href="#">DNS</a>	1/1	DNS Live																																																				
<a href="#">Event</a>	1/1	Event Live																																																				
<a href="#">Timeseries Exporter</a>	0/0	Timeseries Exporter Live																																																				
<a href="#">Flow Analytics</a>	1/1	Flow Analytics Live																																																				
<a href="#">Flow Collector</a>	1/1	Flow Collector Live																																																				
<a href="#">Formula Service</a>	1/1	Formula Service Live																																																				
<a href="#">Inventory</a>	1/1	Inventory Live																																																				
<a href="#">NM Collector</a>	1/1	NM Collector Live																																																				
<a href="#">SNMP Collector</a>	1/1	SNMP Collector Live																																																				
<a href="#">Storage</a>	1/1	Storage Live																																																				
<a href="#">Threshold</a>	1/1	Threshold Live																																																				
<a href="#">Timeseries</a>	1/1	Timeseries Live																																																				
<a href="#">UI</a>	1/1	UI Live																																																				

4. The installation of your cluster is complete. Leave the Ambari manager page in the Firefox browser open. Leave the terminal window where you are the root user open. You use these two tools in the exercises for the next unit.

---

# **Unit 2 Integration**

In the exercises for this unit, you integrate Network Performance Insight with IBM Tivoli Network Manager, Netcool/OMNIbus, and Dashboard Application Services Hub (DASH).

## **Exercise 1 Integration with IBM Tivoli Network Manager**

Network Performance Insight uses IBM Tivoli Network Manager to obtain an inventory of resources to monitor. Network Performance Insight can also reuse SNMP metrics that are polled and stored by Network Performance Insight. Use these steps to integrate Network Performance Insight with IBM Tivoli Network Manager.

1. Open the Ambari manager page, if you do not already have it open.

- a. Run the following command to start Firefox as the root user.

```
firefox &
```

- b. Browse to the following URL. Log in with the user name **admin** and the password **admin**.

```
http://npi1.csite.edu:8080
```

2. Configure Network Performance Insight with the details of your IBM Tivoli Network Manager environment.
  - a. In the menu on the left of the page, click NPI.
  - b. Click the **Configs** tab.

The screenshot shows the Ambari interface for the Network Performance Insight (NPI) service. The top navigation bar includes the Ambari logo, the NPI service name, and status indicators for 0 ops and 1 alert. The left sidebar lists various components: HDFS, YARN, MapReduce2, ZooKeeper, Ambari Metrics, Kafka, Cassandra, and NPI. The NPI entry is highlighted with a red arrow. The main panel has tabs for 'Summary' (which is selected, indicated by a blue background) and 'Configs'. Below these tabs, there's a group dropdown set to 'Default (1)'. A configuration card is displayed, showing version V5, a timestamp of 'about a month ago', and the cluster name 'HDP-2.6.NP'. At the bottom of the main panel, there are buttons for 'Actions', 'NPI Core Settings', and 'NPI Settings'. A section titled 'NOI Components' lists 'NOI SNMP Collector'.

- c. Choose **DB2** as the platform.
- d. Enter **host1.csite.edu** as the value for itnm.host.
- e. Enter **50000** as the port.
- f. Enter **db2inst1** as the user name.

- g. Enter **object00** as the password. Enter **object00** again to confirm.

NOI Components

NOI SNMP Collector

itnm.platform

DB2 

itnm.host 

itnm.port 

itnm.username 

itnm.password 

- h. Scroll down and enter **NCIM** as the value for itnm.database.

- i. Enter the following URL in the itnm.kafka.connect.rest.url field:

<http://npi1.csuite.edu:8083/connectors>

itnm.database 

itnm.probe.import.interval 

itnm.kafka.connect.rest.url 

- j. Click the **Advanced** tab.
- k. Expand **Advanced npi-env**.
- l. Add the following two lines to the **content** field.

```
collector.itnm.entity.discovery-content-path =  
"/opt/IBM/npi/npi-itnm-collector/discovery/content"  
collector.itnm.entity.import-interval = 1h
```

The screenshot shows the 'NPI Settings' tab selected. Under the 'Advanced' tab, there is a section titled 'Advanced npi-env'. The 'content' field contains the following configuration:

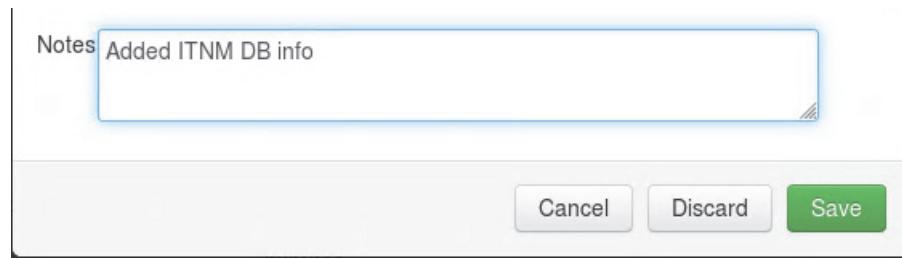
```
#NPI conf HOCON style config.  
# Deploy to all microservices  
collector.itnm.entity.discovery-content-path = "/opt/IBM/npi/npi-itnm-collector/discovery/content"  
collector.itnm.entity.import-interval = 1h
```

**Note:** The **collector.itnm.entity.import-interval** setting controls how often Network Performance Insight obtains a full list of devices from Tivoli Network Manager. You set this interval to one hour to accelerate inventory reconciliation in your lab environment. In a production environment this interval would typically be longer, for example one day.

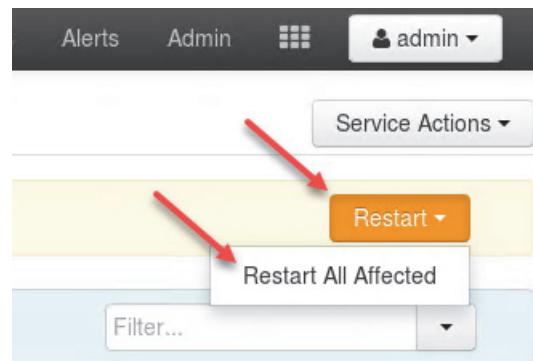
- m. Click **Save** near the top of the page.

The screenshot shows the 'NPI Settings' tab selected. At the bottom of the page, there are two buttons: 'Discard' and 'Save'. A red arrow points to the 'Save' button.

- n. Enter a reason for the configuration change, and click **Save**.



- o. Click **OK** to confirm.
- p. Some components must be restarted after the configuration change. At the top of the page, click **Restart > Restart All Affected**.



- q. Click **Confirm Restart All**.
- r. After a few minutes, the components restart. Click **OK** to close the operations window.
3. Copy the encryption key file from IBM Tivoli Network Manager to Network Performance Insight. This key is used to obtain SNMP community strings from IBM Tivoli Network Manager.
- Return to the terminal window where you are the root user.
  - Connect to npi2.csuite.edu.  
ssh npi2.csuite.edu
  - Change to the correct directory.  
cd /opt/IBM/npi/npi-itnm-collector/
  - Create the resources/itnm/security/keys sub-directory.  
mkdir -p resources/itnm/security/keys
  - Run the following command to copy the conf.key file to the correct directory on npi2.csuite.edu. Run the entire command on one line.  
scp netcool@host1.csuite.edu:/opt/IBM/tivoli/netcool/etc/security/keys/conf.key /opt/IBM/npi/npi-itnm-collector/resources/itnm/security/keys
  - Enter **yes** when you are prompted to continue.

- g. Enter **object00** as the password.
  - h. Run the following command to verify that the conf.key file is now in the correct directory.  

```
ls /opt/IBM/npi/npi-itnm-collector/resources/itnm/security/keys
```

  
conf.key
  - i. Type **exit** to close the connection to npi2.csite.edu.
4. Copy the kafka.properties file to the correct location and edit it to include the Network Performance Insight Kafka servers. Complete this step on host1.csite.edu, where IBM Tivoli Network Manager is installed.
- a. Connect to host1.csite.edu.  

```
ssh netcool@host1.csite.edu
```
  - b. Change to the target directory.  

```
cd /opt/IBM/tivoli/netcool/precision/storm/conf
```
  - c. Copy the kafka.properties file to the correct location.  

```
cp default/kafka.properties .
```
  - d. Open the kafka.properties file in a text editor.  

```
vi kafka.properties
```
  - e. Find the following two lines near the top of the file. Edit these lines to look like the following example. Save and close the file when you are finished.  

```
kafka.consumer.bootstrap.servers=npi1.csite.edu:6667
kafka.producer.bootstrap.servers=npi1.csite.edu:6667
```
  - f. You must restart IBM Tivoli Network Manager to apply the configuration change. Run the following command to stop IBM Tivoli Network Manager.  

```
itnm_stop
```

```
Stopping Network Manager domain NOI_AGG_P
```

- g. Run the following command to start IBM Tivoli Network Manager.

```
itnm_start
```

- h. Check the status of IBM Tivoli Network Manager. Repeat the command until you see all processes in the **RUNNING** or **ACTIVE** state.

```
itnm_status
```

Network Manager:

Domain:	NOI_AGG_P
ncp_ctrl	RUNNING PID=1742 NOI_AGG_P
ncp_store	RUNNING PID=2241 NOI_AGG_P
ncp_class	RUNNING PID=2242 NOI_AGG_P
ncp_model	RUNNING PID=2813 NOI_AGG_P
ncp_disco	RUNNING PID=3072 NOI_AGG_P
ncp_d_helpserv	RUNNING PID=2243 NOI_AGG_P
ncp_config	RUNNING PID=2244 NOI_AGG_P
ncp_poller_default	RUNNING PID=3825 NOI_AGG_P
ncp_poller_admin	RUNNING PID=3826 NOI_AGG_P
nco_p_ncpmonitor	RUNNING PID=2245 NOI_AGG_P
ncp_g_event	RUNNING PID=3325 NOI_AGG_P
ncp_webtool	RUNNING PID=2246 NOI_AGG_P
ncp_virtualdomain	RUNNING PID=4222 NOI_AGG_P

Apache Storm:

supervisord	RUNNING PID=1965
storm_nimbus	RUNNING PID=1968
storm_supervisor	RUNNING PID=1969
zookeeper	RUNNING PID=1967

Storm topologies:

NMStormTopology	ACTIVE
-----------------	--------

- i. Type **exit** to close the connection to host1.csuite.edu.

## Exercise 2 Integration with Netcool/OMNIbus

Network Performance Insight monitors performance metrics for threshold violations. When a violation occurs, Network Performance Insight uses the Netcool/OMNIbus Standard Input Probe to send an event to the ObjectServer. The same probe is used to send a clearing event when the threshold is no longer violated. In this exercise, you configure the Standard Input Probe that is installed with Network Performance Insight.

1. Add the alias `omnithost` for the host where Netcool/OMNIbus is running. Do this in the hosts file for `npi1.csuite.edu` and `npi2.csuite.edu`.
  - a. Return to the terminal window where you are the root user.
  - b. Open the hosts file in a text editor.  
`vi /etc/hosts`

- c. Find the following line. Add `omnihost` to the end of the line, as in the following example.  
Save and close the file when you are finished.

```
192.168.100.100 host1.csite.edu host1 omnihost
```

- d. Run the following command to test the change. Verify that the pings are successful.  
`ping -c3 omnihost`

...

```
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
```

- e. Connect to `npi2.csite.edu`.

```
ssh npi2.csite.edu
```

- f. Open the hosts file in a text editor.

```
vi /etc/hosts
```

- g. Find the following line. Add `omnihost` to the end of the line, as in the following example.  
Save and close the file when you are finished.

```
192.168.100.100 host1.csite.edu host1 omnihost
```

- h. Run the following command to test the change. Verify that the pings are successful.

```
ping -c3 omnihost
```

...

```
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
```

- i. Stay connected to `npi2.csite.edu`. You use the connection in the next step.

2. Configure the Standard Input Probe to use the name of your ObjectServer, which is `NOI_AGG_P`.

- a. Use SSH to connect to `npi2.csite.edu`, if you are not already connected.

- b. Change to the target directory.

```
cd /opt/IBM/npi/npi-event/stdin-probe/omnibus/probes/linux2x86
```

- c. Open the probe properties file with a text editor.

```
vi npi-flow-stdin.props
```

- d. Add the following line to the bottom of the file. Save and close the file when you are finished.

```
Server : 'NOI_AGG_P'
```

3. Edit the OMNibus interfaces file so that the probe can connect to the ObjectServer.

- a. Change to the target directory.

```
cd /opt/IBM/npi/npi-event/stdin-probe/etc
```

- b. Open the interfaces file with a text editor.

```
vi interfaces.linux2x86
```

- c. Find the following line. Add the comment character (#) to the start of the line, as in the following example.

#NCOMS

- d. Add the following line below the line you edited in the preceding step.

NOI\_AGG\_P

- e. After your changes, this section of your interfaces file should look like the following example. Save and close the file when you are finished.

```
# NCMS => omnihost 4100
#NCOMS
NOI_AGG_P
    master tcp sun-ether omnihost 4100
    query tcp sun-ether omnihost 4
```

- f. Stay connected to npi2.csite.edu. You use the connection later in this exercise.

4. Restart the Event service.

- a. Return to the Ambari manager page. If you need to open the manager page, open a Firefox browser as root and use the following URL with the user name **admin** and the password **admin**.

<http://npi1.csite.edu:8080>

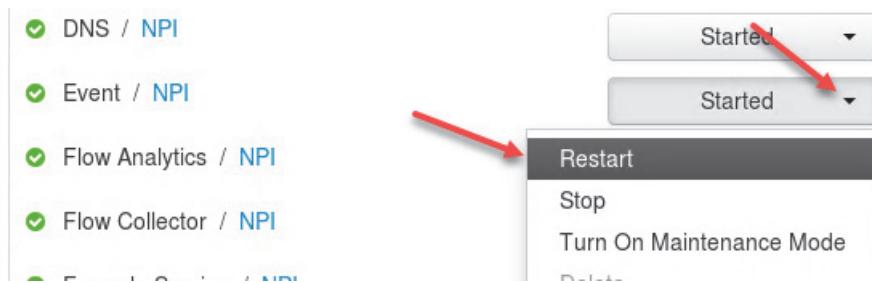
- b. Click the **Hosts** tab close to the top of the page.



- c. Click **npi2.csite.edu**.

Filter by host and component attributes or search by key	
Name	IP Address
<input type="checkbox"/> npi1.csite.edu	192.168.100.100
<input type="checkbox"/> npi2.csite.edu	192.168.100.101

- d. Scroll down and find the Event service. Click the Started button, then click **Restart**.



- e. Click **OK** to confirm.  
f. In a short time, the restart operation is 100% complete. Click **OK** to confirm.

Operations	Start Time	Duration	Show:
✓ Restart Event	Today 16:56	11.19 secs	<div style="width: 100%;">100%</div>

5. Verify that the probe is running.
- Return to the terminal window where you are connected to npi2.csite.edu.
  - Run the following command to verify that the probe is running. Look for the process named **nco\_p\_stdin**.

```
ps -ef | grep nco_p_stdin
```

```
netcool 12261 10716 0 17:09 ? 00:00:00
/opt/IBM/npi/npi-event/.stdin-probe/omnibus/probes/linux2x86/nco_p_stdin
-propsfile
/opt/IBM/npi/npi-event/.stdin-probe/omnibus/probes/linux2x86/npi-flow-stdin.pr
ops -rulesfile
/opt/IBM/npi/npi-event/.stdin-probe/omnibus/probes/linux2x86/npi-flow-stdin.ru
les -messagelog /opt/IBM/npi/npi-event/.var/stdin-probe/stdin.probe.log
```

- Run the following command to view the probe log file. If no new messages are present in the log file, the probe is running correctly.

```
cat /opt/IBM/npi/npi-event/var/stdin-probe/stdin.probe.log
```

- Type **exit** to close the connection to npi2.csite.edu.

# Exercise 3 Integration with Dashboard Application Services Hub

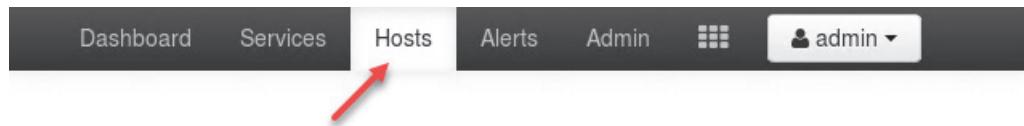
In this exercise, you integrate the Network Performance Insight user interface with Dashboard Application Services Hub (DASH).

1. Ensure that the Network Performance Insight Dashboard service is running. If it is not running, start it.

- a. Return to the Ambari manager page. If you need to open the manager page, open a Firefox browser as root and use the following URL with the user name **admin** and the password **admin**.

<http://npi1.csite.edu:8080>

- b. Click the **Hosts** tab close to the top of the page.



- c. Click **npi2.csite.edu**.

Filter by host and component attributes or search by	
Name	IP Address
<input type="checkbox"/> npi1.csite.edu	192.168.
<input type="checkbox"/> npi2.csite.edu	192.168.

- a. Scroll down and find the Dashboard service. If it is not running, click the **Stopped** button, then click **Start**.



- b. Click **OK** to confirm.

- c. In a short time, the start operation is 100% complete. Click **OK** to confirm.

- d. Verify that the Dashboard service is started before you continue.

✓ NodeManager / YARN	Started ▾
✓ Dashboard / NPI	Started ▾
✓ DNS / NPI	Started ▾
✓ Event / NPI	Started ▾

- e. Keep the Ambari manager page open. You use it again soon.
2. Configure the details of the Network Performance Insight SSL certificate by editing the custom.cfg file.
- Change to the target directory.  
cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
  - Open the custom.cfg file in a text editor.  
vi custom.cfg
  - Find the following three properties and change their values to match the following example.  
Do not change any other property.

```
...
DASH_CONNECTION=netcool@host1.csuite.edu
...
DOMAIN_NAME=*.csuite.edu
...
NPI_UI_HOST=npi2.csuite.edu
...
```

- d. Verify that your custom.cfg file looks like the following example. Save and close the file when you are finished.

```
#####
# CUSTOMIZE THE FOLLOWING BASED ON YOUR REQUIREMENT #
#####

--- Ambari Server Port, default 8080--#
AMBARI_SERVER_PORT=8080

# Directory where npi-installer-tools are installed.
NPI_INSTALLER_TOOLS_DIR=/opt/IBM/basecamp/basecamp-installer-tools

DASH_ENABLE_OPTION=TRUE
DASH_CONNECTION=netcool@host1.csite.edu
DASH_SSH_PORT=22
WEBSPHERE_APP_SERVER_PATH=/opt/IBM/WebSphere/AppServer/
JAZZSM_PATH=/opt/IBM/JazzSM
DASH_USERNAME=smadmin
KEYSTORE_OPTION=USE_DEFAULT_KEY
EXIST_KEYSTORE_FILEPATH=/tmp/security.keystore
EXIST_CA_FILEPATH=/tmp/ca.crt
ALIAS=npi
DOMAIN_NAME=*.csite.edu
ORG_NAME=PSL
LOCALITY=UT
STATE=SL
COUNTRY=MY
WAS_PROFILE_NAME=JazzSMProfile
WAS_NODE=JazzSMNode01
WAS_SERVER_NAME=server1
WAS_PROFILE_PATH=/opt/IBM/JazzSM/profile/
NPI_UI_HOST=npi2.csuite.edu
```

3. Generate the SSL certificate and keystore files, then verify that they were created successfully.
- Run the following command to generate the SSL certificate and keystore files. Run the entire command on one line.

```
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/securityKeyTool.sh
--default=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.cfg
--custom=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/custom.cfg
--keyStorePassword=changeit -keyPassword=changeit
```



**Important:** You must use **changeit** as the key store password and the key password.

- b. Run the following command to check the ambari\_npi\_key\_startup.log file. Verify that there are no warnings or errors in the log file.

```
cat /tmp/ambari_npi_key_startup.log
```

- c. Run the following command to check the securityKeyTool.<timestamp>.log file. Use the actual timestamp in your environment, not the timestamp in the following example. Verify that there are no warnings or errors in the log file.

```
cat /tmp/securityKeyTool.202001162000.log
```

- d. Run the following command to check the genSecurityKey.log file. Verify that there are no warnings or errors in the log file.

```
cat /tmp/genSecurityKey.log
```

4. Enable the integration with Jazz for Service Management and DASH.

- a. Run the following command to verify that the Netcool/OMNIbus ObjectServer is running.

```
ssh host1.csite.edu nco_ping NOI_AGG_P
```

NCO\_PING: Server available.

- b. Run the following command to enable the integration. Run the entire command on one line.

```
/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/npiDashIntegration.sh  
-default=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/default.cfg  
-custom=/opt/IBM/basecamp/basecamp-installer-tools/dash-integration/custom.cfg  
-dashPassword=object00 -npiUserPassword=object00
```

- c. Run the following command to check the npiDashIntegration.log file. Verify that there are no warnings or errors in the log file.

```
cat /tmp/npiDashIntegration.log
```

- d. Run the following command to check the enableDash.log file on the host where DASH is running. Verify that there are no warnings or errors in the log file.

```
ssh host1.csite.edu cat /tmp/enableDash.log
```

5. Configure the details of your DASH environment in Ambari manager.
  - a. Return to the browser where the Ambari manager page is open. You might need to log in again with the user name **admin** and the password **admin**.
  - b. Click **Ambari** at the top left, then click **NPI > Configs > NOI Core Settings**.

The screenshot shows the Ambari Manager interface. At the top, there's a navigation bar with the Ambari logo, the text "NPI", "0 ops", and "1 alert". Below the navigation bar is a sidebar on the left containing a list of services: HDFS, YARN, MapReduce2, ZooKeeper, Ambari Metrics, Kafka, Cassandra, and NPI (which is highlighted). To the right of the sidebar is the main content area. It has tabs for "Summary" and "Configs", with "Configs" being the active tab. Under the "Configs" tab, there are buttons for "Group", "Default (2)", and "Manage Config Groups". Below these are two configuration versions: V2 (selected) and V1. Both versions show the author as "admin" and were updated "2 days ago". A message below the versions says "admin authored on Wed, Jan 15, 2020 16:42:12". At the bottom of the main content area, there are three tabs: "NOI Core Settings" (selected), "NPI Settings", and "Advanced".

- c. Select **DASH** as the value for web.auth.
- d. Enter **object00** as the DASH password. Enter **object00** again to confirm.

The screenshot shows the "NOI Services" configuration page under the "Authentication" section. It has a "web.auth" dropdown menu set to "DASH", indicated by a red arrow. Below it is a "security.dash.username" field containing "smadmin". At the bottom, there are two "security.dash.password" fields, each containing "\*\*\*\*\*", enclosed in a red box.

- e. Scroll down. Enter `/opt/IBM/basecamp/basecamp-ui/conf/security/security.keystore` as the value of `https.keystore.file`.

- f. Enter **changeit** as the keystore password. Enter **changeit** again to confirm.
- g. Enter **changeit** as the key password. Enter **changeit** again to confirm.

https.keystore.file  
np/basecamp-ui/conf/security/security.keystore

https.keystore.password  
.....  
.....

https.key.password  
.....  
.....

- h. Click the **Advanced** tab. Expand **Advanced np-auth**.
- i. Enter **host1.csuite.edu** as the DASH host name.

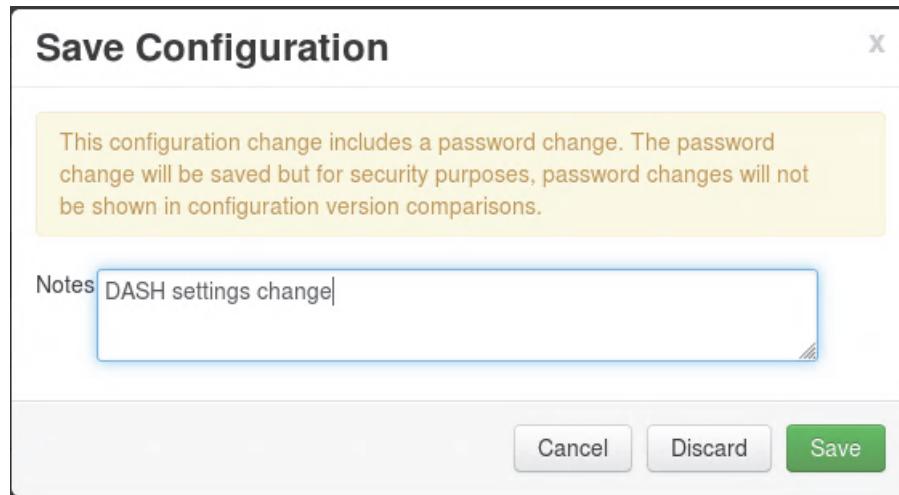
NOI Core Settings NPI Settings Advanced

Advanced np-auth

security.dash.hostnames	host1.csuite.edu
security.dash.port	16311

- j. Click **Save** near the top of the page.

- k. Enter a reason for the configuration change, and click **Save**.



- l. Click **OK** to proceed if you are prompted about recommended changes to security.dash.hostnames.
- m. Click **OK** to confirm.
6. Restart the **Network Performance Insight** services.
- Click the **Services** tab at the top of the page.
  - Click **NPI** in the menu on the left of the page.
  - Click **Service Actions > Restart All**.

The screenshot shows the Ambari interface. The top navigation bar includes 'Ambari', 'NPI', 'Dashboard', 'Services', 'Hosts', 'Alerts', 'Admin', and a user dropdown. The 'Services' tab is active. On the left, a sidebar lists services: HDFS, YARN, MapReduce 2, ZooKeeper, Ambari Metrics, Kafka, Cassandra, and NPI. The NPI service is selected, indicated by a red arrow pointing to its icon. The main content area shows a summary of 15 components on 2 hosts, with a message: 'Restart Required: 15 Components on 2 Hosts'. Below this is a detailed summary of components: Manager (2/2 Started, No alerts), Manager (2/2 Started, No alerts), Dashboard (1/1 Dashboard Live), Cacti Collector (0/0 Cacti Collector Live), and DNS (1/1 DNS Live). To the right, a 'Service Actions' dropdown menu is open, with 'Restart All' highlighted in red, indicated by a red arrow. Other options in the menu include Start, Stop, and other restart options for various services like Dashboards, DNSs, Events, Flow Analyticss, Flow Collectors, Formula Services, Inventorys, and NM Collectore.

- d. Click **Confirm Restart All**.
- e. When the services are finished restarting, click **OK**.

- f. Start the Dashboard service manually. Click the **Hosts** tab close to the top of the page.



- g. Click **npi2.csite.edu**.

Filter by host and component attributes or search by	
Name	IP Address
<input type="checkbox"/> npi1.csite.edu	192.168.
<input checked="" type="checkbox"/> npi2.csite.edu	192.168.

- a. Scroll down and find the Dashboard service. If it is not running, click the **Stopped** button, then click **Start**.

A screenshot of a service status list. On the left, services are listed with their status: NodeManager / YARN (green checkmark), Dashboard / NPI (red warning triangle), DNS / NPI (green checkmark), and Event / NPI (green checkmark). On the right, there are two dropdown menus for the Dashboard service. The top menu shows 'Started' and 'Stopped'. The bottom menu shows 'Start', 'Turn On Maintenance Mode', and 'Delete'. A red arrow points from the 'Stopped' button to the 'Start' option in the dropdown menu.

- b. Click **OK** to confirm.

- c. In a short time, the start operation is 100% complete. Click **OK** to confirm.

- d. Verify that the Dashboard service is started before you continue.

A screenshot of the same service status list. The 'Dashboard / NPI' service is now highlighted with a red box and has a green checkmark next to its name. Its status dropdown menu also has a red box around it and shows 'Started' as the selected option. The other services (NodeManager / YARN, DNS / NPI, Event / NPI) are also shown as started.

7. Confirm that the security.keystore file was created.

- a. Run the following command to connect to npi2.csite.edu.

```
ssh npi2.csite.edu
```

- b. Run the following command to verify that the security.keystore file exists and is in the correct directory.

```
ls -al /opt/IBM/basecamp/basecamp-ui/conf/security
```

```
-rwxr-xr-x 1 root      root    3437 Jan 17 16:39 security.keystore
```

- c. Stay connected to npi2.csuite.edu. You use the connection in the next step.

8. On npi2.csuite.edu, compare the following two certificate fingerprints to verify that they match:

- ◆ **WebSphereCACert**, in the cacerts file
- ◆ **npi\_ca**, in the key store file

- a. Run the following command to show the details of the WebSphereCACert certificate. Run the entire command on one line. Note the certificate fingerprint in the output of the command. The fingerprint in your environment will be different than the following example.

```
keytool -keystore /opt/IBM/basecamp/basecamp-jre/java-1.8.0-openjdk.x86_64/jre/lib/security/cacerts -storepass changeit -list -alias WebSphereCACert
```

```
WebSphereCACert, Jan 17, 2020, trustedCertEntry,  
Certificate fingerprint (SHA1):
```

```
83:31:0C:87:E5:66:66:57:FD:B3:E4:5D:D7:0A:E5:8B:94:F1:87:BA
```

- b. Run the following command to show the details of the npi\_ca certificate. Run the entire command on one line. Notice the npi\_ca certificate fingerprint in the output of the command. The fingerprint in your environment will be different than the following example. Verify that this matches the WebSphereCACert fingerprint you found in the preceding step.

```
keytool -keystore /opt/IBM/basecamp/basecamp-ui/conf/security/security.keystore -storepass changeit -list
```

```
Keystore type: jks  
Keystore provider: SUN
```

```
Your keystore contains 2 entries
```

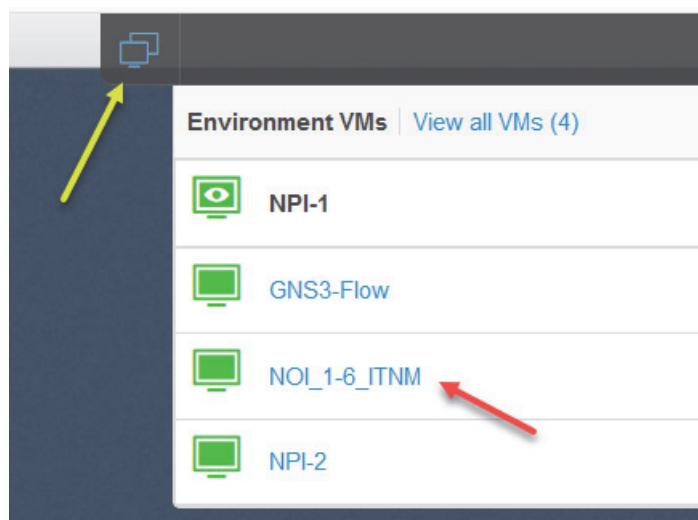
```
npi_ca, Jan 16, 2020, trustedCertEntry,  
Certificate fingerprint (SHA1):  
83:31:0C:87:E5:66:66:57:FD:B3:E4:5D:D7:0A:E5:8B:94:F1:87:BA  
npi, Jan 16, 2020, PrivateKeyEntry,  
Certificate fingerprint (SHA1):  
25:3C:83:B6:DA:F3:D4:9E:5D:4E:F7:8B:C2:72:DE:A0:18:84:7C:B7
```

- c. Type **exit** to close the connection to npi2.csuite.edu.

9. Configure SSL in WebSphere Application Server.
  - a. Perform the next steps on the host where WebSphere Application Server is running. Change your lab environment to the desktop of host1.csite.edu, which is labeled **NOI\_1-6\_ITNM**. Click the tab at the top of the window to view the lab environment options.



- b. Click the icon for environment VMs. Click **NOI\_1-6\_ITNM**.

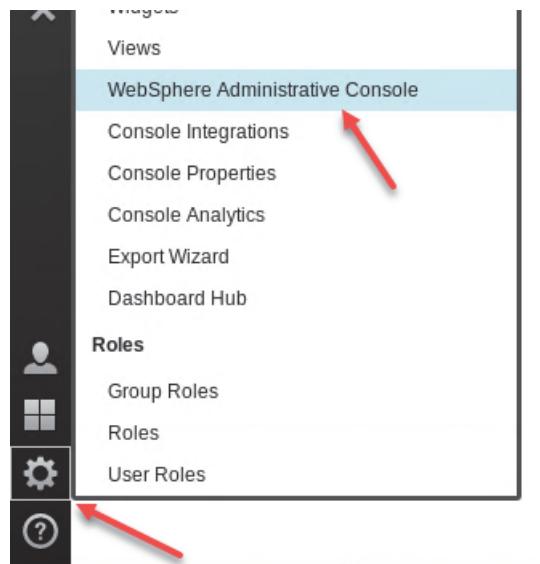


- c. Open a Firefox browser.

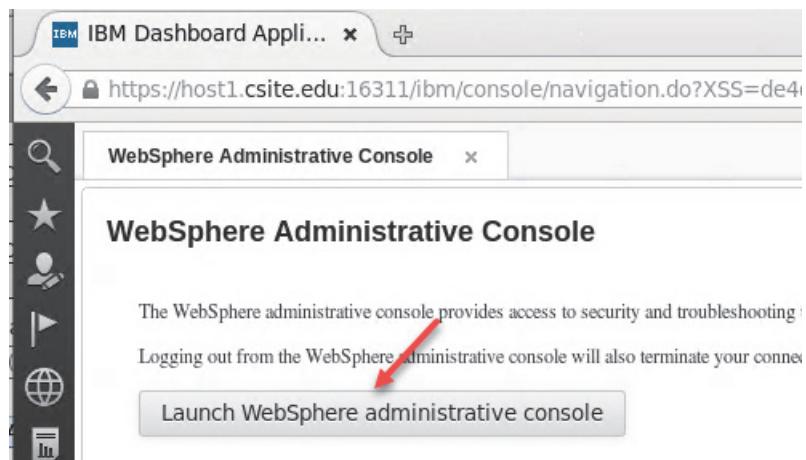


- d. Go to the following URL:  
<https://host1.csite.edu:16311.ibm/console/logon.jsp>
  - e. Log in with the user name **smadmin** and the password **object00**.

f. Click **Console Settings > WebSphere Administrative Console**.



g. Click the **Launch WebSphere administrative console** button.



h. Expand **Security**. Click **SSL certificate and key management**.



- i. Click **SSL configurations** at the right of the page.

The screenshot shows a sidebar with the following text:  
 s between  
 listing  
 secure  
 for the  
 ↳ each  
 single  
 ↳ enables you  
 ↳ established  
 ↳ established

**Related Items**

- [SSL configurations](#)
- [Dynamic outbound endpoint SSL configurations](#)
- [Key stores and certificates](#)
- [Key sets](#)
- [Key set groups](#)

- j. Click **NodeDefaultSSLSettings**.

The screenshot shows a list of resources with the following interface:  
 New... Delete  
 Select Name ▾  
 You can administer the following resources:  
 Total 1

<input type="checkbox"/>	<a href="#">NodeDefaultSSLSettings</a>
--------------------------	--

- k. Select **netcool** as the Default server certificate alias.  
 l. Select **netcool** as the Default client certificate alias.  
 m. Click **OK**.

**General Properties**

\* Name

Trust store name

Keystore name

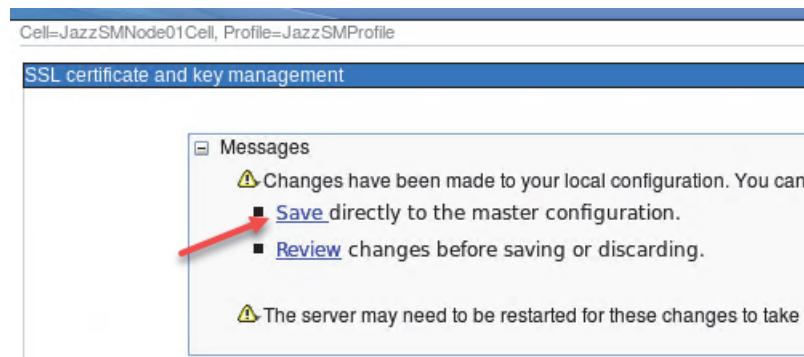
Default server certificate alias  
 ▼

Default client certificate alias  
 ▼

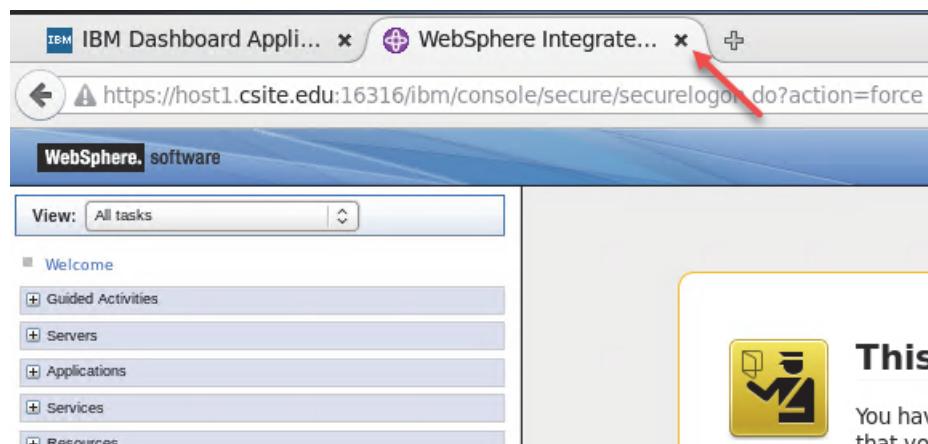
Management scope

**Buttons:**

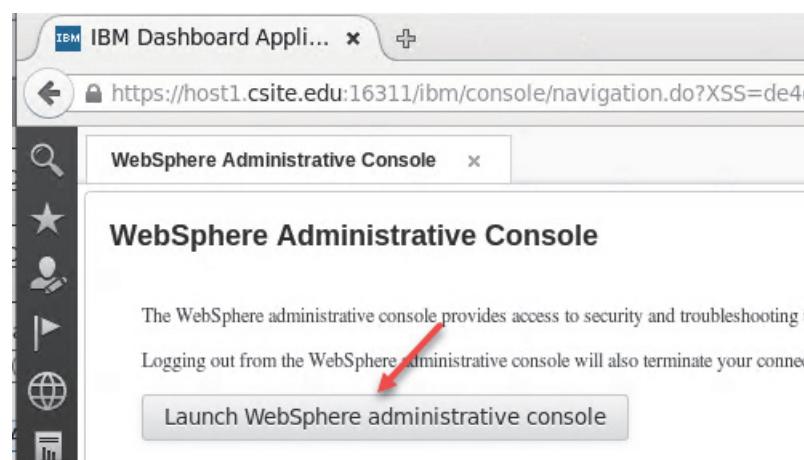
- n. Click **Save** at the top of the page.



- o. At this point, you might see warnings about an invalid certificate. Close the WebSphere Integrated Console tab.



- p. Click the **Launch WebSphere administrative console** button.



- q. Expand **I Understand the Risks**. Click **Add Exception**.

The screenshot shows a Firefox security warning dialog. At the top is a yellow icon of a person holding a shield. The main title is "This Connection is Untrusted". Below it, a message says: "You have asked Firefox to connect securely to **host1.cs**, so Firefox has checked that your connection is secure." A note follows: "Normally, when you try to connect securely, sites will check that you are going to the right place. However, this site..." A section titled "What Should I Do?" contains a button labeled "Get me out of here!". Below this are two expandable sections: "Technical Details" and "I Understand the Risks". Red arrows point from the question text to both the "I Understand the Risks" section and the "Add Exception..." button at the bottom.

**This Connection is Untrusted**

You have asked Firefox to connect securely to **host1.cs**, so Firefox has checked that your connection is secure.

Normally, when you try to connect securely, sites will check that you are going to the right place. However, this site...

**What Should I Do?**

If you usually connect to this site without problems, this means the site is trying to impersonate the site, and you shouldn't continue.

**Get me out of here!**

► **Technical Details**

▼ **I Understand the Risks**

If you understand what's going on, you can tell Firefox to trust this site. Even if you trust the site, this error could be caused by someone tampering with your connection.

Don't add an exception unless you know there's a good reason. Firefox can't tell if this site is really who it claims to be.

**Add Exception...**

- r. Click **Confirm Security Exception**.



10. Verify that the new certificates are available.  
a. Expand **Security**. Click **SSL certificate and key management**.



- b. Click **Key stores and certificates** on the right side of the page.

Applications between establishing and establishing secure connections for the

Configure each endpoint to define a single capability enables you to can be established SL configuration.

In migration utilities, the various ke advantage of the

**Related Items**

- [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. Click **NodeDefaultKeyStore**.

Key stores and certificates				
<a href="#">New...</a> <a href="#">Delete</a> <a href="#">Change password...</a> <a href="#">Exchange signers...</a>				
		Select Name  Description		Management
You can administer the following resources:				
<input type="checkbox"/>	<a href="#">NodeDefaultKeyStore</a>	Default key store for JazzSMNode01	(cell):JazzSMNode01 (node):JazzSMNode01	
<input type="checkbox"/>	<a href="#">NodeDefaultTrustStore</a>	Default trust store for JazzSMNode01	(cell):JazzSMNode01 (node):JazzSMNode01	
Total 2				

- d. Click **Personal certificates** on the right side of the page.

**Additional Properties**

- [Signer certificates](#)
- **[Personal certificates](#)**
- [Personal certificate requests](#)
- [Custom properties](#)

- e. Verify that the **netcool** certificate is present.

You can administer the following resources:					
<input type="checkbox"/>		<a href="#">default</a>	CN=host1.csuite.edu, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US	CN=host1.csuite.edu, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US	16
<input type="checkbox"/>			CN=host1.csuite.edu, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US	CN=host1.csuite.edu, OU=Root Certificate, OU=JazzSMNode01Cell, OU=JazzSMNode01, O=IBM, C=US	16
<input type="checkbox"/>		<a href="#">netcool</a>	CN=*.csuite.edu, O=DEMO, L=DEMO_LOCALITY, ST=DEMO_STATE, C=MY	CN=*.csuite.edu, O=DEMO, L=DEMO_LOCALITY, ST=DEMO_STATE, C=MY	12

- f. Click the **Key stores and certificates** link at the top of the page.

SSL certificate and key management

SSL certificate and key management > [Key stores and certificates](#) > [NodeDefaultKeyStore](#) > Personal certificates

Manages personal certificates.

[Preferences](#)

[Create](#) [Delete](#) [Receive from a certificate authority...](#) [Replace...](#) [Extract...](#) [Import...](#) [Export](#)

- g. Click **NodeDefaultTrustStore**.

Select	Name	Description	Manager
You can administer the following resources:			
<input type="checkbox"/>	<a href="#">NodeDefaultKeyStore</a>	Default key store for JazzSMNode01	(cell):Jaz:node):Ja
<input type="checkbox"/>	<a href="#">NodeDefaultTrustStore</a>	Default trust store for JazzSMNode01	(cell):Jaz:node):Ja

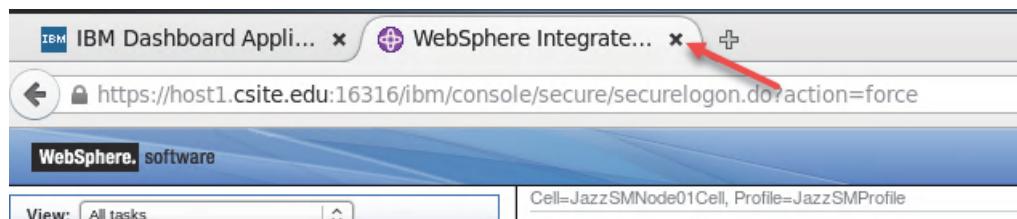
h. Click **Signer certificates**.



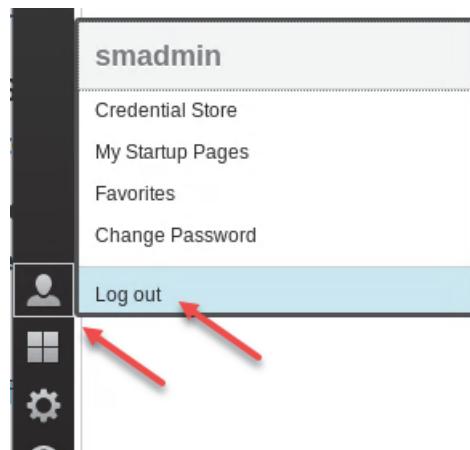
i. Verify that the **npi\_ca** certificate is present.

You can administer the following resources.			
<input type="checkbox"/>	<a href="#">impact_ssl</a>	CN=host1.csuite.edu, O=IBM, OU=ImpactUI, C=US	EF:4B:F4:61:85:A5:F7:1C:7C:08:E1
<input type="checkbox"/>	<a href="#">npi_ca</a>	CN=*.csuite.edu, O=DEMO, L=DEMO_LOCALITY, ST=DEMO_STATE, C=MY	83:31:0C:87:E5:66:66:57:FD:B3:E4
<input type="checkbox"/>	<a href="#">root</a>	CN=host1.csuite.edu, OU=Root Certificate, OU=JazzSMNode01Cell.	6C:11:66:8E:A5:23:E7:D8:CB:C0:6

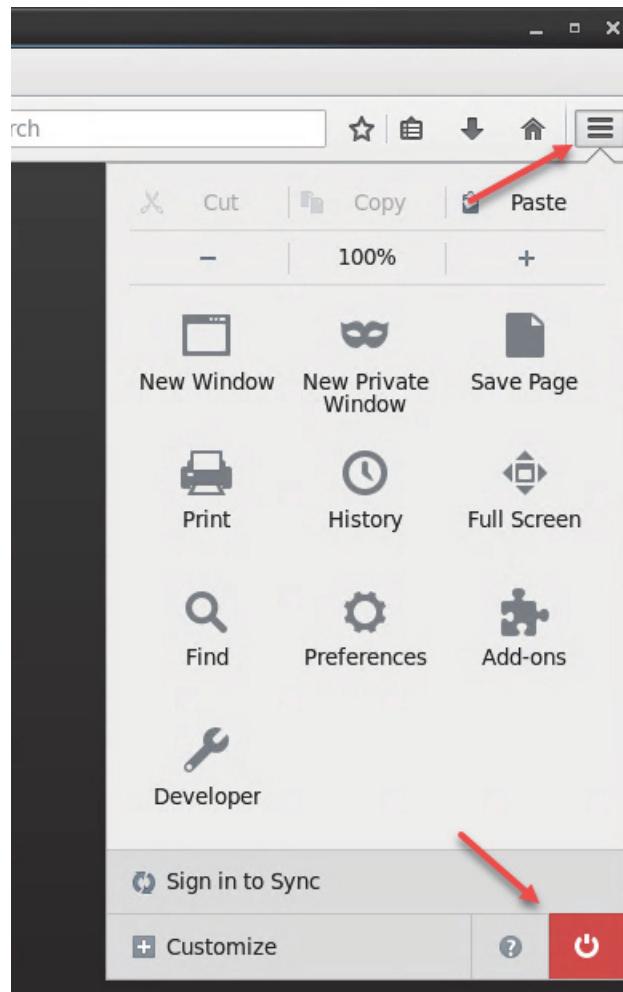
j. Close the WebSphere Integrated Console tab.



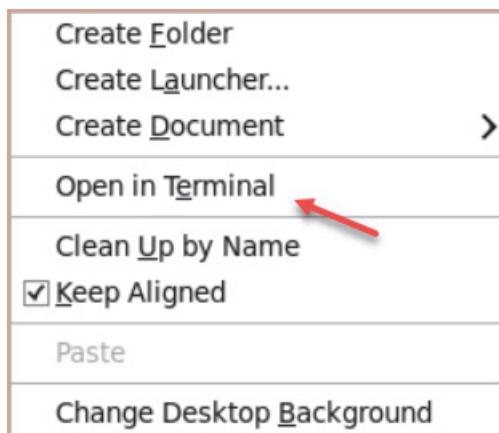
- k. Click the user icon, then click **Log out**.



- l. Click the Firefox menu button, then click the quit icon.



11. Restart WebSphere Application Server, Jazz for Service Management, and DASH.
  - a. Right-click the desktop of the Netcool Operations Insight server and click **Open in Terminal**.



- b. Run the following command to change to the root user. The password is **object00**.

```
su - root
```

Password: **object00**

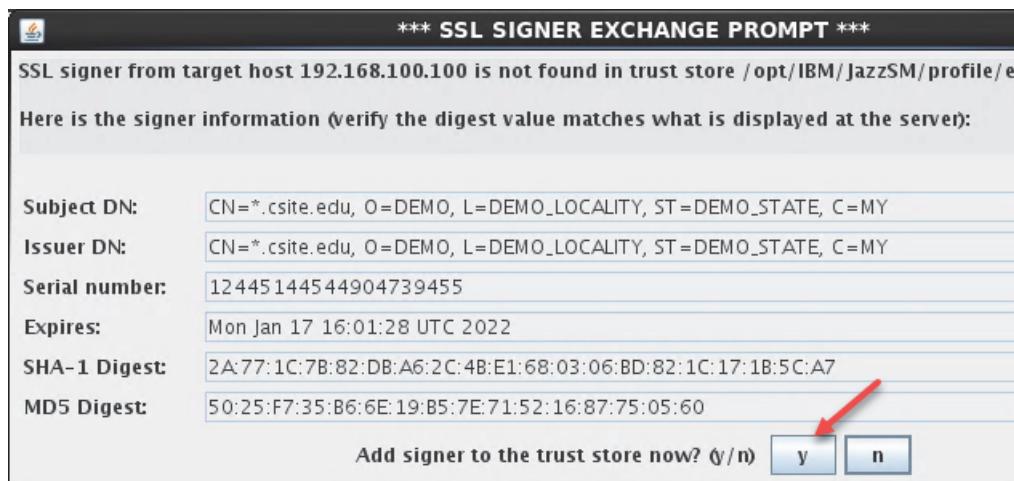
- c. Change to the target directory.

```
cd /etc/init.d/
```

- d. Run the following command to stop WebSphere Application Server, Jazz for Service Management, and DASH.

```
./jazz stop
```

- e. Click **y** when you are prompted to add the SSL signer.



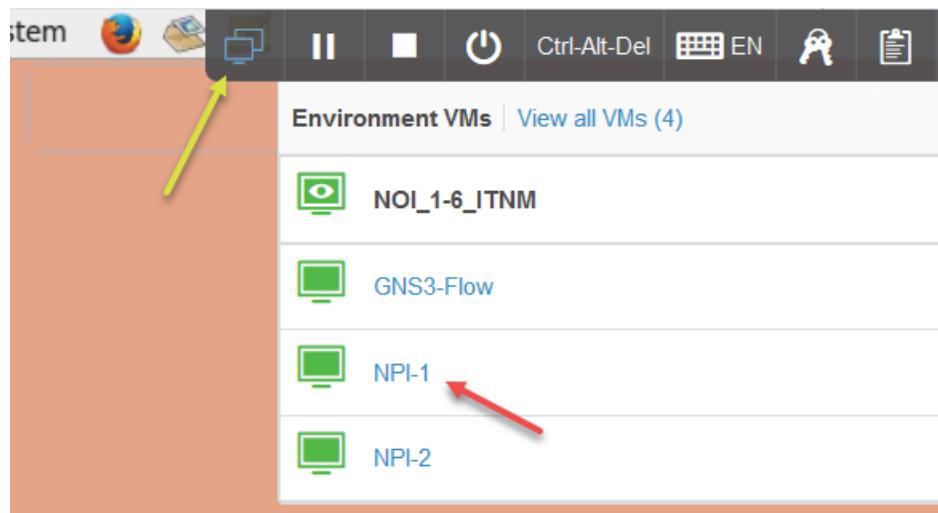
- f. Wait until the service is stopped. Run the following command to start WebSphere Application Server, Jazz for Service Management, and DASH.

```
./jazz start
```

12. Return your lab environment to the desktop of np1.csite.edu, which is labeled NPI-1.
- Click the tab at the top of the window to view the lab environment options.



- Click the icon for environment VMs. Click **NPI-1**.



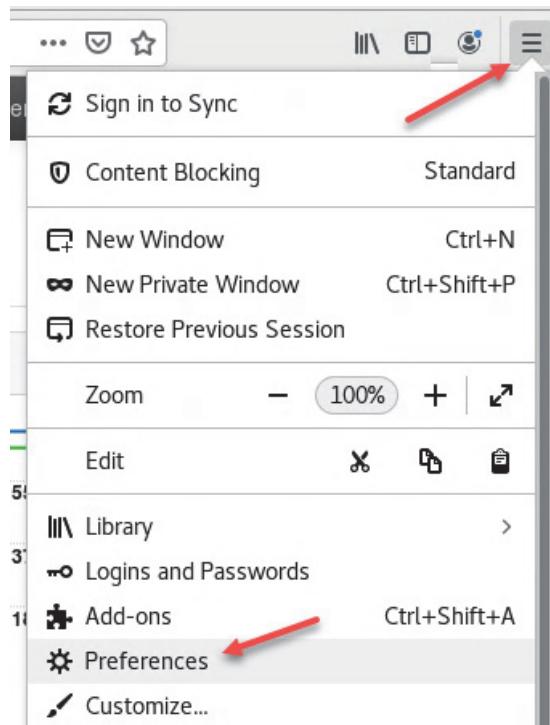
13. Import the ca.crt file from WebSphere Application Server into your browser.



**Note:** In a production environment, you must import the ca.crt file into all computers and browsers that will access Network Performance Insight.

- Return to the terminal window on np1.csite.edu where you are the root user.
- Run the following command to change to the target directory.  
`cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration`
- Run the following command to copy the ca.crt file to a directory that the netcool user can access.  
`cp ca.crt /home/netcool/`
- Open a Firefox browser if you do not already have one open.

- e. Click the Firefox menu button, then click **Preferences**.



- f. Click **Privacy and Security**.  
g. Scroll down and click **View Certificates**.

A screenshot of the Firefox Preferences window. On the left, there is a sidebar with icons for General, Home, Search, Privacy & Security (which has a red arrow pointing to it), and Sync. The main pane shows the 'Security' section under 'Deceptive Content and Dangerous Software Protection'. It includes options like 'Block dangerous and deceptive content' (checked) and 'Block dangerous downloads' (checked). Below that is the 'Certificates' section, which asks when a server requests a personal certificate ('Select one automatically' or 'Ask you every time') and includes an option to 'Query OCSP responder servers to confirm the current validity of certificates' (checked). At the bottom right of this section are two buttons: 'View Certificates...' (highlighted with a red arrow) and 'Security Devices...'.

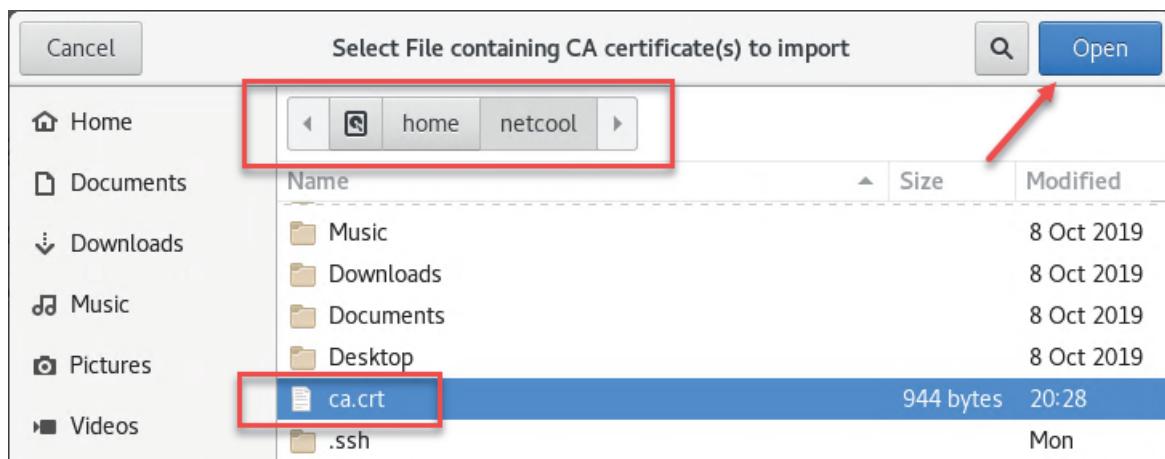
- h. Click **Authorities > Import.**

The screenshot shows the 'Authorities' tab selected in a navigation bar. Below it, a message says 'You have certificates on file that identify these certificate authorities'. A list of certificates is shown, each with a 'View...', 'Edit Trust...', 'Import...', 'Export...', and 'Delete...' button. A red arrow points to the 'Import...' button for the 'ACCV' entry.

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Default Trust
Global Chambersign Root - 2008	Default Trust
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce ...	Default Trust
Camerfirma Global Chambersign Root	Default Trust
ACCV	
ACCVRAIZ1	Default Trust

View... Edit Trust... Import... Export... Delete...

- i. Browse to the **/home/netcool** directory.  
j. Select the ca.crt file.  
k. Click **Open**.



- I. Select all trust options and click **OK**.



- m. Click **OK** to close the Certificate Manager window.



**Important:** If you ran Firefox as the root user, then the ca.crt file was imported only for the root user. Open Firefox as the netcool user and import the ca.crt file again if you want to access the user interface from a browser run by netcool.

# Unit 3 Post-installation configuration

In the exercises for this unit, you complete the following tasks:

- Install technology packs
- Install and configure the Device Dashboard
- Configure Dashboard Application Services Hub (DASH) roles
- Install an interim fix
- Set the resource scope

## Exercise 1 Installing technology packs

In this exercise, you install the technology packs that are suitable for the simulated network devices in your lab environment.

1. Connect to the desktop of npi1.csite.edu if you are not already connected. The npi1.csite.edu host is labeled NPI-1.
2. Open a terminal window and switch to the root user.
3. Install the Network Health technology pack.
  - a. Change to the target directory.

```
cd /opt/IBM/basecamp/basecamp-installer-tools/pack-installer
```

b. Run the following command to install the Network Health technology pack.

```
./pack-install.sh install ../ootb-packs/network-health-1.2.0.jar
```

c. Enter **npiadmin** when you are prompted for the user name.

```
NPI Username: npiadmin
```

d. Enter **netcool** when you are prompted for the password.

```
NPI Password: netcool
```

e. Press Enter to accept the default port number.

```
NPI Port[9443]:
```

4. Install the Generic Health technology pack.

a. Run the following command to install the Generic Health technology pack.

```
./pack-install.sh install ../ootb-packs/network-health-generic-1.2.0.jar
```

- b. Enter **npiadmin** when you are prompted for the user name.

NPI Username: npiadmin

- c. Enter **netcool** when you are prompted for the password.

NPI Password: **netcool**

- d. Press Enter to accept the default port number.

NPI Port[9443] :

5. Install the Cisco Health technology pack.

- a. Run the following command to install the Cisco Health technology pack.

```
./pack-install.sh install ../ootb-packs/network-health-cisco-1.1.0.jar
```

- b. Enter **npiadmin** when you are prompted for the user name.

NPI Username: npiadmin

- c. Enter **netcool** when you are prompted for the password.

NPI Password: **netcool**

- d. Press Enter to accept the default port number.

NPI Port[9443] :

6. Install the Cisco Probe technology pack.

- a. Run the following command to install the Cisco Probe technology pack.

```
./pack-install.sh install ../ootb-packs/network-probe-cisco-1.0.0.jar
```

- b. Enter **npiadmin** when you are prompted for the user name.

NPI Username: npiadmin

- c. Enter **netcool** when you are prompted for the password.

NPI Password: **netcool**

- d. Press Enter to accept the default port number.

NPI Port[9443] :

7. Run the following command to verify that the technology packs were successfully installed.

Confirm that you see four technology packs in the output of the command.

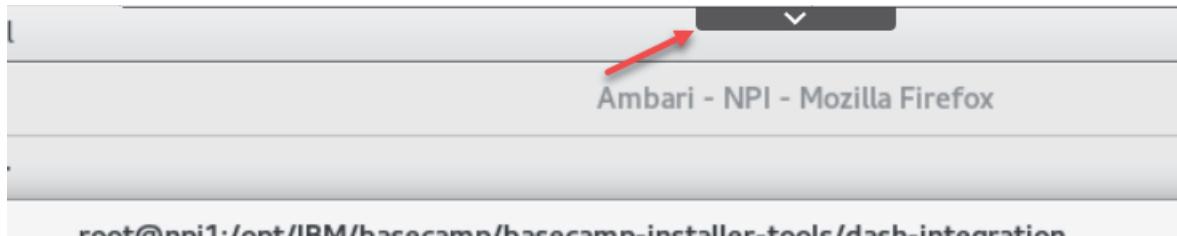
```
./status.sh
```

npil.csuite.edu	network-health-generic	1.2.0
	network-health	1.2.0
	network-health-cisco	1.1.0
	network-probe-cisco	1.0.0

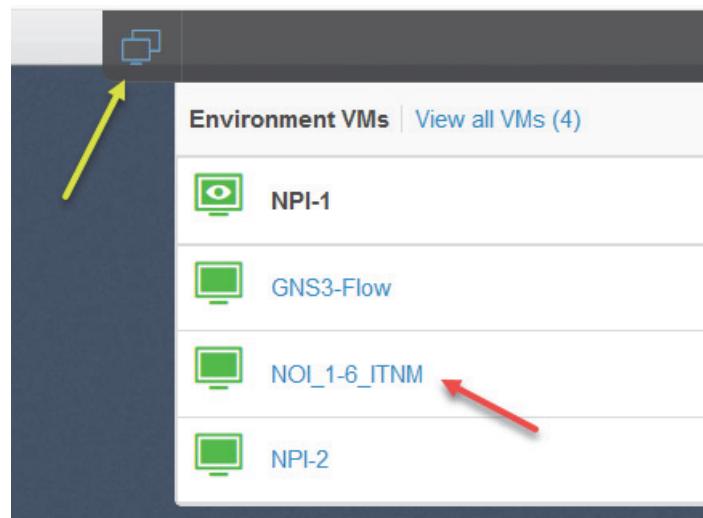
# Exercise 2 Installing the Device Dashboard

In this exercise, you install and configure the Network Performance Insight Device Dashboard. You also add DASH roles to the Network Performance Insight users.

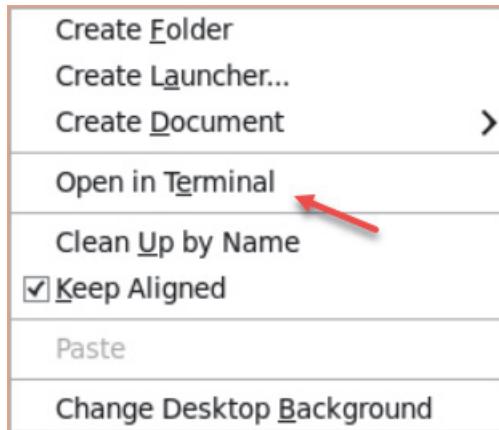
1. Perform the next steps on the host where Netcool Operations Insight is running. Change your lab environment to the desktop of host1.csite.edu, which is labeled **NOI\_1-6\_ITNM**.
  - a. Click the tab at the top of the window to view the lab environment options.



- b. Click the icon for environment VMs. Click **NOI\_1-6\_ITNM**.



2. Open a terminal window. Right-click the desktop of the Netcool Operations Insight host and click **Open in Terminal**.



3. Decompress the Device Dashboard installation files.

- a. Change to the target directory.

```
cd /software/DeviceDashboard
```

- b. Run the following command to decompress the installation media.

```
tar -xvf DEVICE_DASHBOARD_V1.1.0.2_LINUX.tar
```

4. Start Installation Manager.

- a. Change to the target directory.

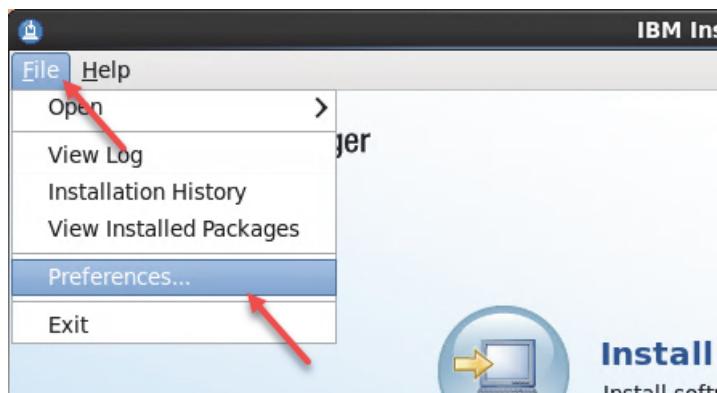
```
cd ~/IBM/InstallationManager/eclipse/
```

- b. Run the following command to start Installation Manager.

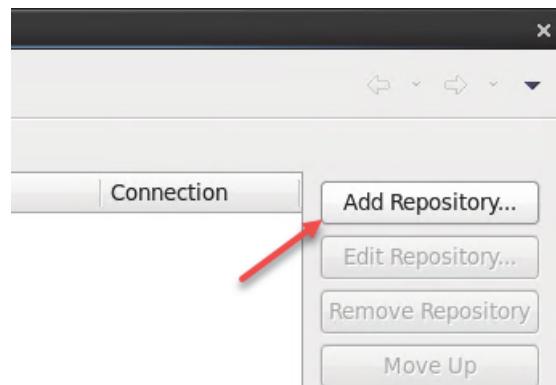
```
./IBMMIM
```

5. Add the Device Dashboard installation media as a repository.

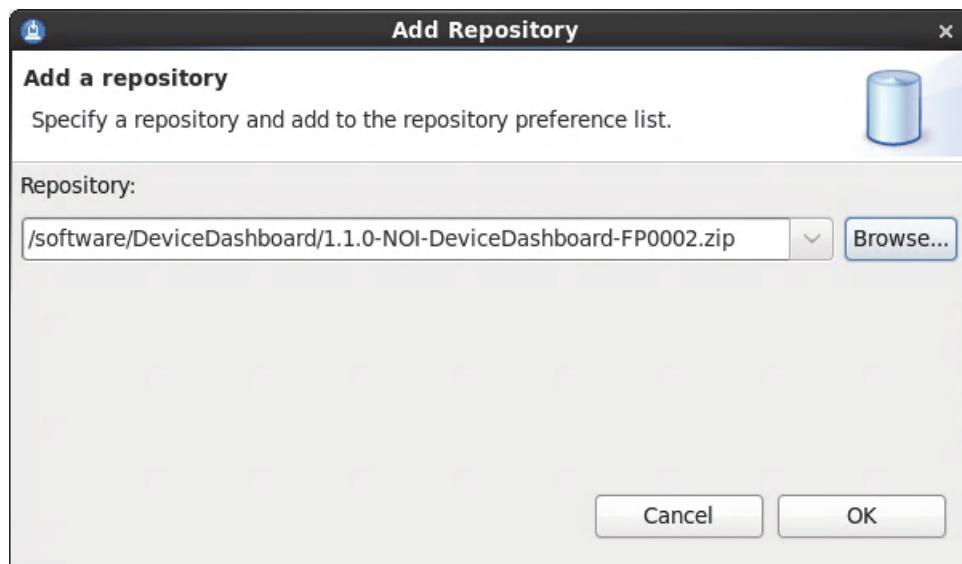
- a. Click **File > Preferences**.



- b. Click **Add Repository**.



- c. Browse to the **/software/DeviceDashboard/1.1.0-NOI-DeviceDashboard-FP0002.zip** file, then click **OK**.

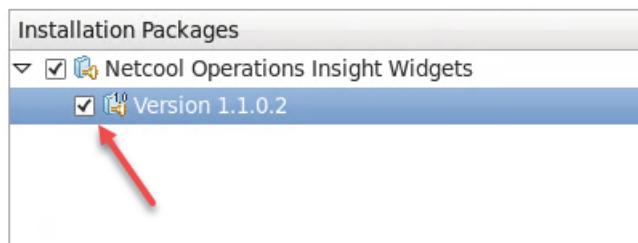


- d. Click **OK** to close the preferences window.

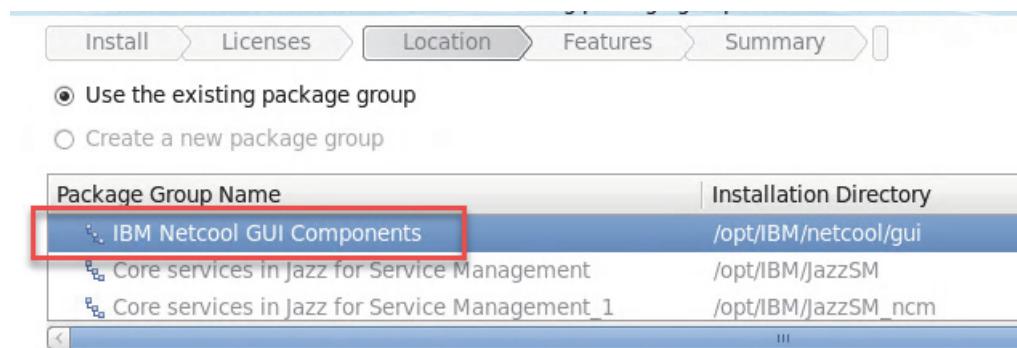
6. Install the Device Dashboard.
  - a. Click **Install** to start the installation wizard.



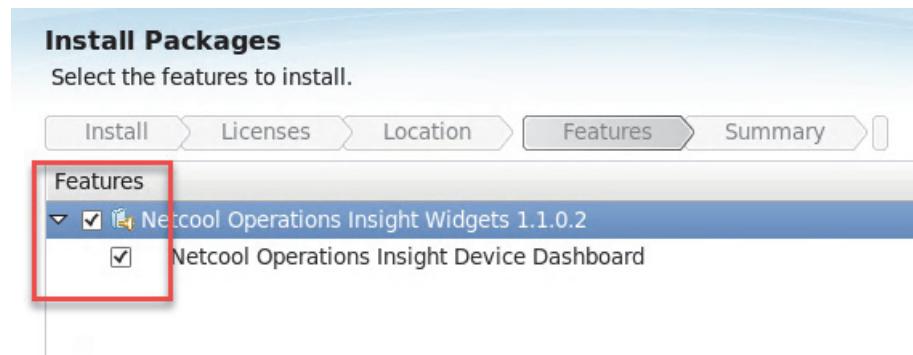
- b. Select the version 1.1.0.2 package and click **Next**.



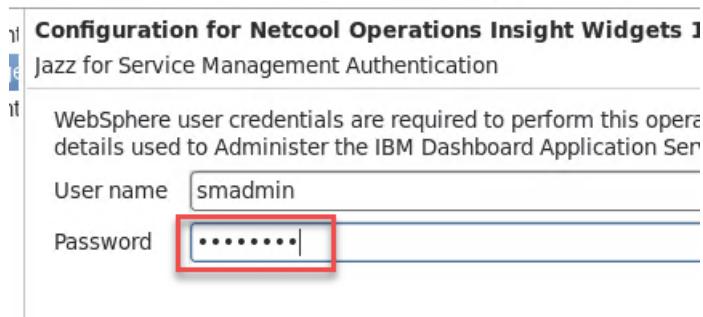
- c. Accept the license agreement and click **Next**.
  - d. Confirm that IBM Netcool GUI Components is selected as the package group and click **Next**.



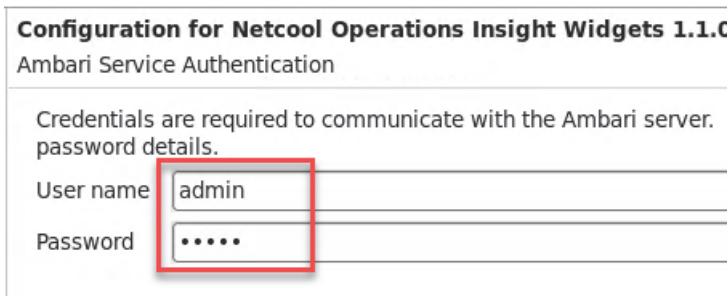
- e. Verify that both features are selected and click **Next**.



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



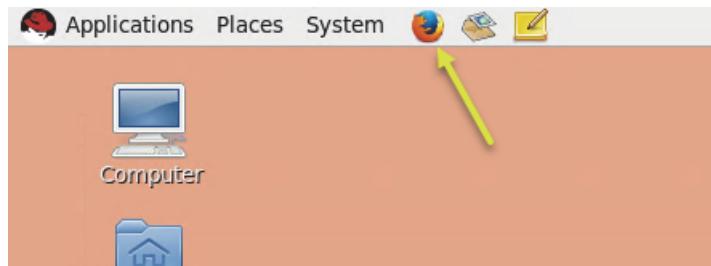
- g. Enter **admin** as the Ambari user name and password, then click **Next**.



- h. Click **Install** at the summary page. The installation takes about 20 minutes.
- i. Click **Finish** to close the installation wizard.
- j. Click **File > Exit** to close Installation Manager.
- k. Stay connected to the desktop of the Netcool Operations Insight host (host1.csite.edu). You will use this host in the next steps.

7. Add DASH roles to the Network Performance Insight users.

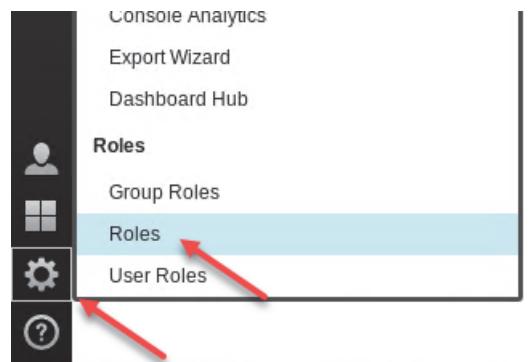
- a. Open a Firefox browser.



- b. Browse to the following URL. Log in with the user name **smadmin** and the password **object00**.

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

- c. Click **Console Settings > Roles**.



- d. Enter **npi** in the filter field.

- e. Click the **noi\_npi** role.

Role Management				
	New...	Delete	Filter:	
#	Role Name	Type	Users	Actions
1	noi_npi	System	0	
2	noi_npi_admin	System	0	

- f. Expand **Users and Groups**.

- g. Click the icon to add users.

Type of role: System

**Users and Groups:**

This section lists the users and groups using this role. To add user or group, select the cor from the list and click Remove.

**Users**

Select	User ID	First Name	Last Name
<input type="checkbox"/>			

**Add** | **Filter**

- h. Enter **npi\*** as the user id, then click **Search**.

- i. Select the **npiadmin** and **npiuser** users, then click **Add**.

**Roles**

First name: \_\_\_\_\_ Last name: \_\_\_\_\_

User ID: **npi\*** E-mail: \_\_\_\_\_

Number of results to display: 20

**Search**

Select	User ID	First Name
<input checked="" type="checkbox"/>	npiadmin	npiadmin
<input checked="" type="checkbox"/>	npiuser	npiuser

**Add** **Cancel**

- j. Verify that the users are listed and click **Save**.

The screenshot shows a table titled 'Users' with columns: Select, User ID, First Name, and Last Name. There are two rows: one for 'npiadmin' and one for 'npiuser'. The 'npiadmin' row is highlighted with a red box. Below the table, it says 'Total: 2 Selected: 0'. At the bottom are 'Save' and 'Cancel' buttons.

► Access to Views: 0  
► Access to Pages: 1

Save Cancel

- k. Click the **noi\_npi\_admin** role.

The screenshot shows a table titled 'Roles' with columns: Select and Role Name. There are two rows: 'noi\_npi' and 'noi\_npi\_admin'. The 'noi\_npi\_admin' row is highlighted with a red arrow pointing to it.

- l. Expand **Users and Groups**.

- m. Click the icon to add users.

\* Role name: noi\_npi\_admin  
Type of role: System

**▼ Users and Groups:**

This section lists the users and groups using this role. To add user or group from the list and click Remove.

Users

Save Cancel

- n. Enter **npi\*** as the user id, then click **Search**.

- o. Select the **npiadmin** user, then click **Add**.

**Roles**

First name: \_\_\_\_\_ Last name: \_\_\_\_\_

User ID: \_\_\_\_\_ E-mail: \_\_\_\_\_

User ID: npi\*

Number of results to display: 20

Search

|

Select	User ID	First Name
<input checked="" type="checkbox"/>	npiadmin	npiadmin
<input type="checkbox"/>	npiuser	npiuser

Add Cancel

Select	User ID	First Name
<input checked="" type="checkbox"/>	npiadmin	npiadmin
<input type="checkbox"/>	npiuser	npiuser

- p. Verify that the user is present and click **Save**.

**Roles**

\* Role name: noi\_npi\_admin

Type of role: System

▼ **Users and Groups:**

This section lists the users and groups using this role. To add a user or group, click the + icon.

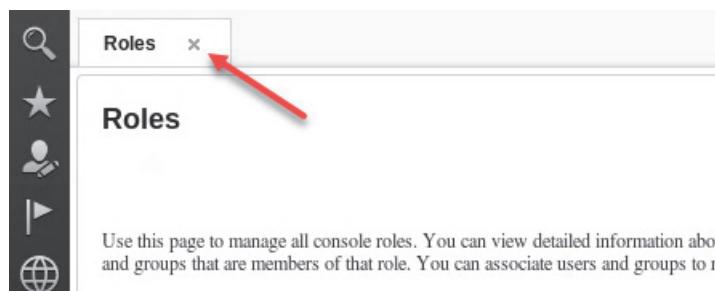
**Users**

Select	User ID	First Name
<input type="checkbox"/>	npiadmin	npiadmin

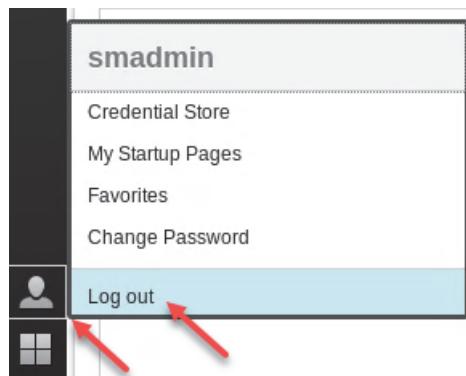
► Access to Views: 0  
► Access to Pages: 1

**Save** **Cancel**

- q. Close the **Roles** tab.

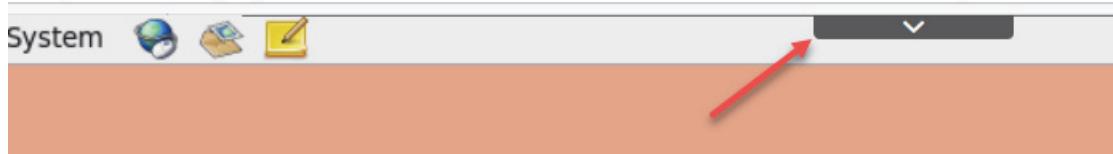


- r. Log out of DASH.

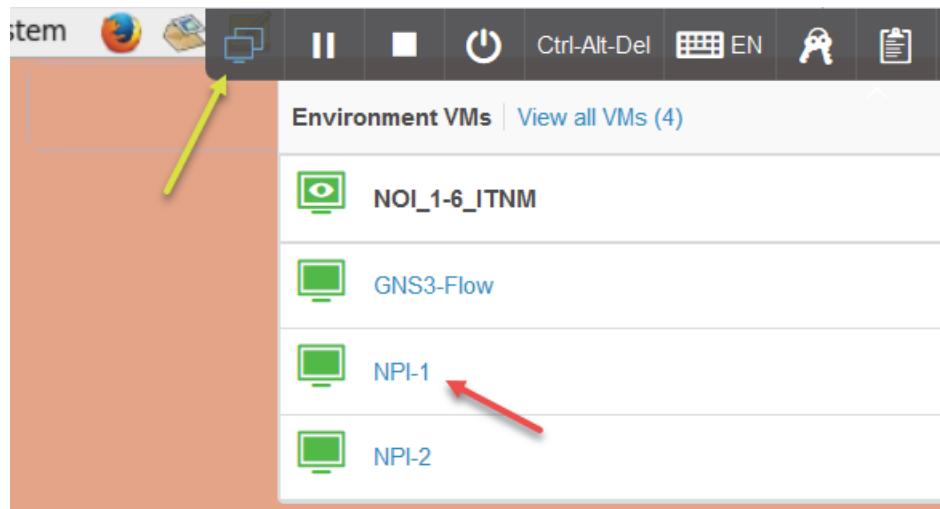


- s. Close the Firefox browser.
8. Configure IBM Tivoli Network Manager to access flow data from Network Performance Insight.
- Return to the terminal window. Verify that you are the netcool user.
  - Open the tnm.properties file in a text editor.  
`vi /opt/IBM/netcool/gui/precision_gui/profile/etc/tnm/tnm.properties`
  - Add the following line to the bottom of the file. Save and close the file when you are finished.  
`tnm.npi.host.name=https://npi2.csuite.edu:9443`
9. Configure IBM Tivoli Network Manager with the Network Performance Insight version.
- Open the npi.properties file in a text editor.  
`vi /opt/IBM/netcool/gui/precision_gui/profile/etc/tnm/npi.properties`
  - Add the following line to the bottom of the file. Save and close the file when you are finished.  
`npi.server.version=1.3.1`
10. Restart WebSphere Application Server, Jazz for Service Management, and DASH.
- Run the following command to change to the root user. The password is **object00**.  
`su - root`
  - Change to the target directory.  
`cd /etc/init.d/`
  - Run the following command to stop WebSphere Application Server, Jazz for Service Management, and DASH  
`./jazz stop`
  - Wait until the service is stopped. Run the following command to start WebSphere Application Server, Jazz for Service Management, and DASH.  
`./jazz start`

- e. After the service is started, press Enter a few times to show the command prompt. Type **exit** to log out as the root user.
11. Return your lab environment to the desktop of npi1.csite.edu, which is labeled NPI-1.
  - a. Click the tab at the top of the window to view the lab environment options.

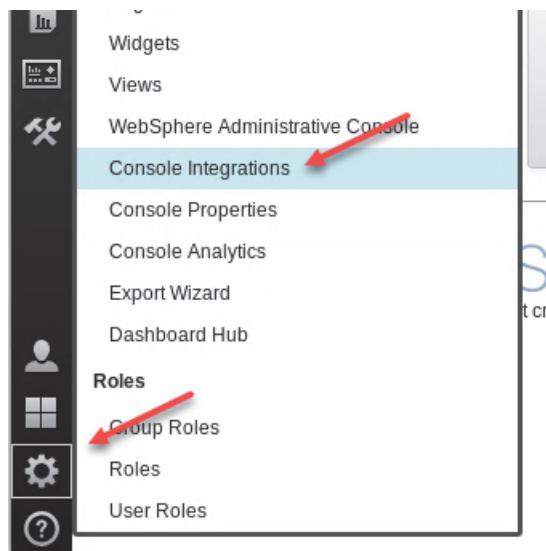


- b. Click the icon for environment VMs. Click **NPI-1**.



12. Verify that the Network Performance Insight Console Integration is working.
  - a. Open a Firefox browser and go to the following URL. Log in with the user name **npiadmin** and the password **object00**.  
<https://host1.csite.edu:16311/ibm/console/logon.jsp>
  - b. If you are prompted with a warning about an insecure or non-private connection click **advanced**, add a security exception to your browser, and proceed to the web page.

c. Click **Console Settings > Console Integrations.**



d. Click **NPI.**

Console Integration is used to integrate tasks from other supported consoles into the current console. This page shows the Console Integrations currently in the console.

Select	Name	Status
<input type="radio"/>	NPI	Unable to connect to the remote console. Please check the console URL externally.
<input type="radio"/>	Netcool Impact	Connection Successful

e. Click **Save.**

\* Console Integration Name:  \*

\* Console Integration URL:  \*

Integration Location:

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

- f. Close the Console Integrations tab.

The screenshot shows the 'Console Integrations' page. On the left is a vertical toolbar with icons for search, star, user, network, play, globe, and a bar chart. The main area has a title 'Console Integrations' with a close button. Below it is a sub-header 'Console Integration is used to integrate tasks from other supported consoles i shows the Console Integrations currently in the console.' A table lists two entries:

Select	Name	Status
<input type="radio"/>	NPI	Connection Successful
<input type="radio"/>	Netcool Impact	Connection Successful

A red arrow points to the close button in the title bar, and another red box highlights the 'Connection Successful' status for the NPI entry.

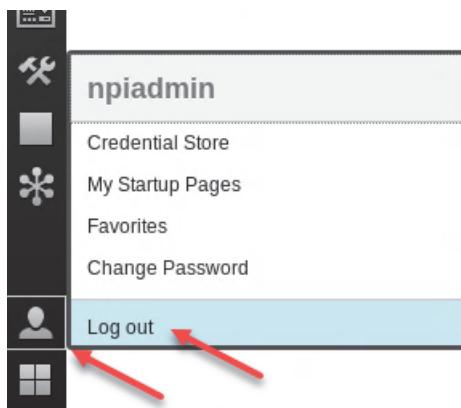
- g. Click the snowflake icon. Verify that you see the Network Performance Insight menu options, such as Autonomous Systems, Cacti Servers, Domain Names, and so on.

The screenshot shows the 'NPI' menu. On the left is a vertical toolbar with icons for search, star, user, network, play, globe, and a bar chart. The main area has a title 'Console Integrations' with a close button. Below it is a sub-header 'NPI'. A list of menu options is shown:

- System Configuration
  - Autonomous System
  - Cacti Servers
  - Domain Names
  - Entity Thresholds
  - Flow Aggregation
  - Flow Devices
  - Flow Interfaces
  - Flow IP Grouping
  - Flow Thresholds
  - NBAR
  - Pack Details
  - Polling Configuration
  - Resource Type

A red arrow points to the snowflake icon in the toolbar.

- h. Log out of DASH.



## Exercise 3 Installing an interim fix

In this exercise, you install interim fix pack 2.

1. Stop the Network Performance Insight services.
  - a. Open a Firefox browser if you do not already have one open.
  - b. Browse to the following URL. Log in with the user name **admin** and the password **admin**.  
<http://npi1.csite.edu:8080>
  - c. Click the **Services** tab.
  - d. Select the **NPI** service at the left of the page.
  - e. Click **Service Actions > Stop**.

A screenshot of the Ambari NPI Services page. The top navigation bar shows 'Ambari', 'NPI', '0 ops', '1 alert', 'Dashboard', 'Services' (which is the active tab), 'Hosts', 'Alerts', 'Admin', and a user dropdown for 'admin'. The sidebar on the left lists services: HDFS, YARN, MapReduce 2, ZooKeeper, Ambari Metrics, Kafka, Cassandra, and NPI (which is selected and highlighted in grey). The main panel shows a 'Summary' table with various service status and alert counts. To the right of the summary table is a 'Service Actions' dropdown menu with options: Start, Stop (which is highlighted in dark grey), Restart All, Restart Dashboards, Restart DNSs, Restart Events, Restart Flow Analytics, Restart Flow Collectors, Restart Formula Services, Restart Inventorys, and Restart NM Collectors. Red arrows point from the sidebar's NPI selection to the 'NPI' in the summary table, and from the 'Stop' button in the dropdown to the 'Stop' button in the summary table.

- f. Click **Confirm Stop**.
- g. Click **OK** when the Stop NPI operation is finished.

- h. Leave the Ambari manager page open. You use it again soon.
2. Decompress the interim fix files.
  - a. Return to the terminal window where you are the root user.
  - b. Change to the target directory.

```
cd /software/IF2
```
  - c. Run the following command to decompress the interim fix pack.

```
tar -zxvf 1.3.1.0-TIV-NPI-IF0002.tgz
```
3. Back up the existing Network Performance Insight users.
  - a. Change to the target directory.

```
cd 1.3.1.0-TIV-NPI-IF0002/bin
```
  - b. Run the following utility to back up your existing users.

```
./dashboard_user_backup.sh
```

  
...  

```
INFO: User backup done on npi2.csite.edu
```
4. Run the following command to install the interim fix. The installation takes about 10 minutes.

```
./fix_update.sh
```

  
...  

```
DB configs consistency check: no errors and warnings were found.
INFO: NPI 1.3.1.0 IF0002 Interim Fix update is completed.
```
5. Restart the Network Performance Insight Storage Service and UI Service.
  - a. Return to the Firefox browser where the Ambari Manager page is open. Log in with the user name and password: **admin**.
  - b. Click the **Services** tab.
  - c. Select the **NPI** service at the left of the page.

d. Click **Service Actions > Restart Storages.**

The screenshot shows the Ambari Services page. On the left, a sidebar lists various services: HDFS, YARN, MapReduce 2, ZooKeeper, Ambari Metrics, Kafka, Cassandra, and NPI. The NPI service is selected, indicated by a red arrow pointing to its 'Actions' dropdown menu. The main panel displays a summary of services, including Manager, Dashboard, Cacti Collector, DNS, Event, Timeseries Exporter, Flow Analytics, and Flow Collector. A message at the top states 'Restart Required: 15 Components on 2 Hosts'. On the right, a 'Service Actions' dropdown menu is open, with a red arrow pointing to the 'Restart Storages' option, which is highlighted in grey.

e. Click **Trigger Rolling Restart.**

f. Click **OK** when the operation is finished.

g. Click **Service Actions > Restart UIs.**

The screenshot shows the 'Service Actions' dropdown menu. A red arrow points to the 'Service Actions' button at the top. The menu lists several options: Start, Stop, Restart All, Restart Dashboards, Restart DNSs, Restart Events, Restart Flow Analytics, Restart Flow Collectors, Restart Formula Services, Restart Inventory, Restart NM Collectors, Restart SNMP Collectors, Restart Storages, Restart Thresholds, Restart Timeseries, and Restart UIs. The 'Restart UIs' option is highlighted in grey, indicating it is selected.

h. Click **Trigger Rolling Restart.**

- i. Click **OK** when the operation is finished.
6. Update the technology packs.
    - a. Return to the terminal window where you are the root user.
    - b. Run the following command to start the update utility.  
`./packs-update.sh`
    - c. Enter **npiadmin** as the user name.  
 NPI Username: npiadmin
    - d. Enter **object00** as the password. The update operation takes about 5 minutes.  
 NPI Password: object00

...

Running sync of pack resource types with config UI  
Script completed

---

HOST	PACK NAME	VERSION
npi1.csuite.edu	network-health-huawei	1.1.0
	network-health-generic	1.2.0
...		

7. Start all Network Performance Insight services that are not running.
  - a. Return to the Firefox browser where the Ambari Manager page is open.
  - b. Click the **Services** tab.
  - c. Select the **NPI** service at the left of the page.
  - d. Click **Service Actions > Start**.

The screenshot shows the Ambari Manager interface. The top navigation bar includes tabs for Dashboard, Services (which is the active tab), Hosts, Alerts, Admin, and a user dropdown for 'admin'. Below the navigation is a summary bar indicating 'Restart Required: 13 Components on 2 Hosts'. On the left, a sidebar lists various services: HDFS, YARN, MapReduce, ZooKeeper, Ambari Metrics, Kafka, Cassandra, and NPI. The NPI service is currently selected, indicated by a red arrow pointing to its icon. The main content area displays a 'Summary' table with components like Manager, Dashboard, Cacti Collector, DNS, and Event, each with their current status (e.g., Stopped) and live counts. To the right of the summary is a 'Service Actions' dropdown menu, also highlighted with a red arrow. This menu lists options such as Start, Stop, Restart All, and several other restart and stop actions for various services.

- e. Click **Confirm Start**.
  - f. Click **OK** when the operation is finished.
8. Restore the Network Performance Insight users that you previously backed up.
- a. Return to the Ambari manager page.
  - b. Stop the Network Performance Insight Dashboard service. Click the **Hosts** tab and click **npi2.csite.edu**.

Name	IP Address	Rack	Cores	RAM	Disk Usage	Load Avg
npi1.csite.edu	192.168.100.195/default-		8 (8)	31.26GB		0.34
<b>npi2.csite.edu</b>	192.168.100.196/default-		16 (16)	62.76GB		2.19

- c. Scroll down and find the Dashboard service. Click the **Started** button then click **Stop**.

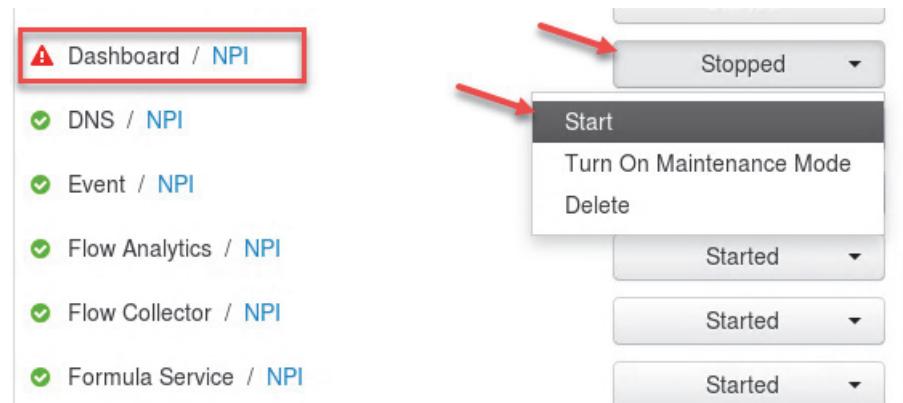
- d. Click **OK** to confirm.
- e. Click **OK** when the operation is finished.
- f. Return to the terminal window where you are the root user.
- g. Run the following command to restore the users.

```
./dashboard_user_restore.sh
```

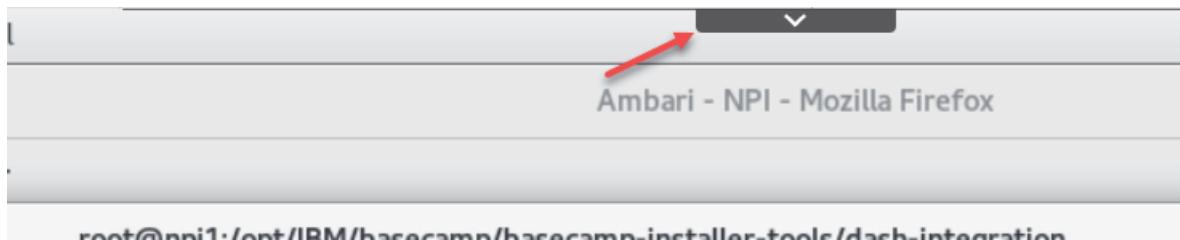
...

INFO: User restore done on npi2.csite.edu

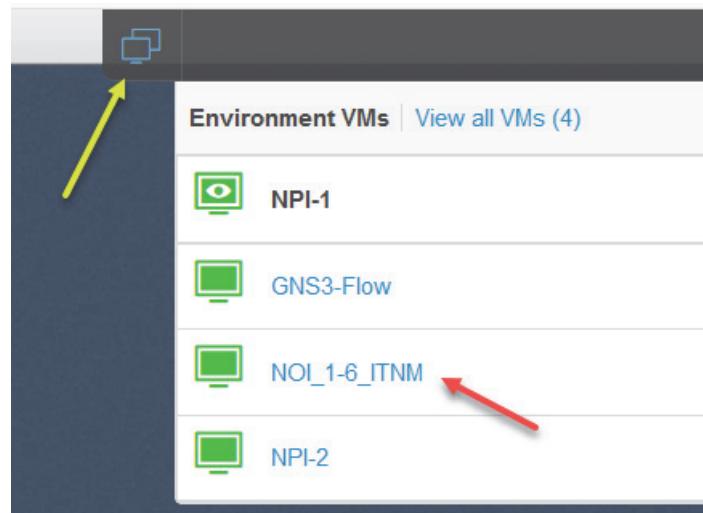
- h. Return to the Ambari manager page.
- i. Find the Dashboard service. Click the **Stopped** button and click **Start**.



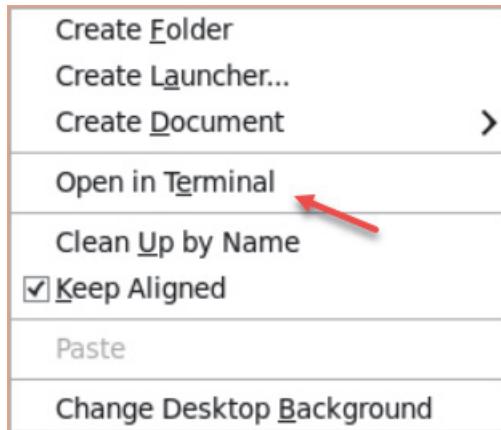
- j. Click **OK** to confirm.
- k. Click **OK** when the operation is finished.
9. Uninstall the Device Dashboard. You perform this task on the Netcool Operations Insight server.
  - a. Change your lab environment to the desktop of host1.csite.edu, which is labeled **NOI\_1-6\_ITNM**.
  - b. Click the tab at the top of the window to view the lab environment options.



- c. Click the icon for environment VMs. Click **NOI\_1-6\_ITNM**.



- d. Open a terminal window. Right-click the desktop of the Netcool Operations Insight host and click **Open in Terminal**.



- e. Use Installation Manager to uninstall the Device Dashboard. Change to the Installation Manager directory.

```
cd ~/IBM/InstallationManager/eclipse/
```

- f. Run the following command to start Installation Manager.

```
./IBMMIM
```

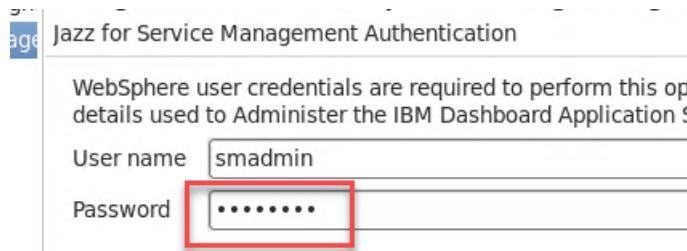
- g. Click **Uninstall**.



- h. Select Netcool Operations Insight Widgets 1.1.0.2 as the package to uninstall. Click **Next**.

Installation Packages	Version	Vendor
IBM Netcool GUI Components		
IBM Tivoli Netcool/OMNIBUS Web GUI	8.1.0.16	IBM
Netcool Operations Insight Extensions for 8.1.0.16		IBM
Netcool Operations Insight Widgets	1.1.0.2	IBM
Network Manager GUI Components	4.2.0.7	IBM
Network Health Dashboard	4.2.0.1	IBM
Network Manager Reports	4.2.0.7	IBM
Core services in Jazz for Service Management		
IBM Dashboard Application Services Hub	3.1.3.3	IBM
Reporting Services	2.1.2.0	IBM

- i. Enter **object00** as the password for smadmin and click **Next**.



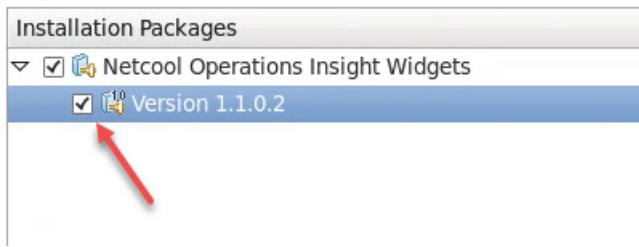
- j. Click **Uninstall** on the summary page. The operation to uninstall the Device Dashboard takes about 5 minutes.
- k. Click **Finish** to close the wizard. Leave Installation Manager open.

10. Install the Device Dashboard again.

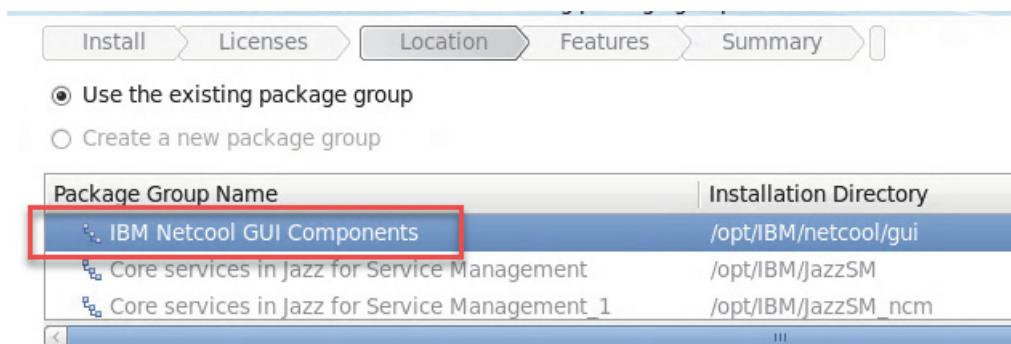
- a. Click **Install** to start the installation wizard.



- b. Select the version 1.1.0.2 package and click **Next**.



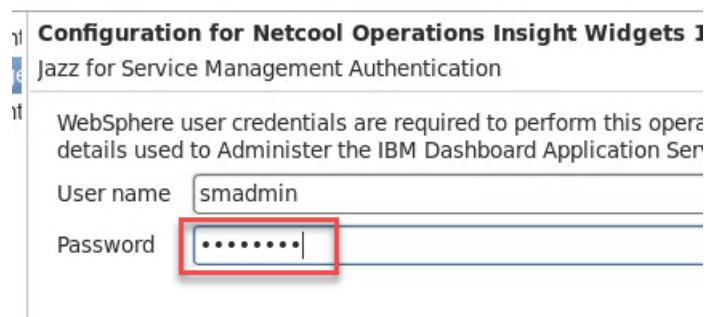
- c. Accept the license agreement and click **Next**.
- d. Confirm that IBM Netcool GUI Components is selected as the package group and click **Next**.



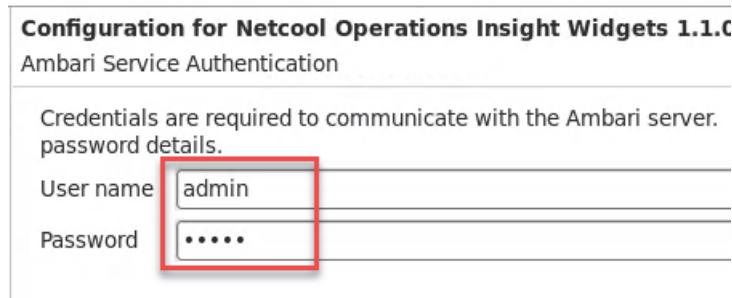
- e. Verify that both features are selected and click **Next**.



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



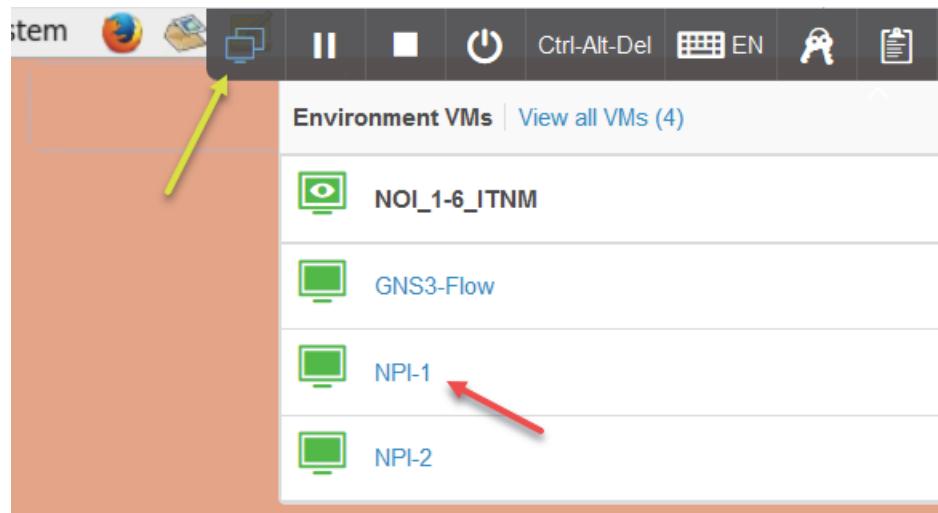
- g. Enter **admin** as the Ambari user name and password, then click **Next**.



- h. Click **Install** at the summary page. The installation takes about 20 minutes.  
i. Click **Finish** to close the installation wizard.  
j. Click **File > Exit** to close Installation Manager.
11. Return your lab environment to the desktop of npi1.csite.edu, which is labeled NPI-1.
- a. Click the tab at the top of the window to view the lab environment options.

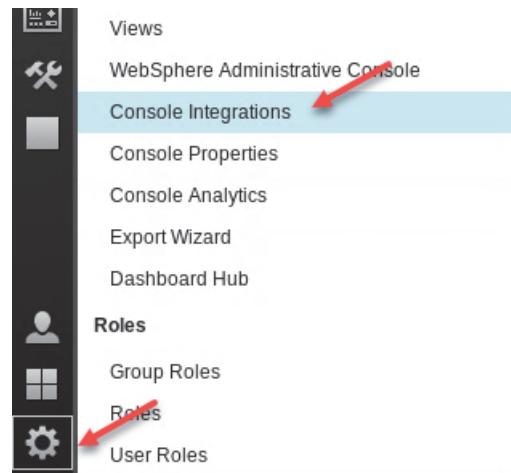


- b. Click the icon for environment VMs. Click **NPI-1**.



12. Configure the DASH Console Integration for Network Performance Insight.
- a. Open a Firefox browser. Go to the following URL. Log in with the user name **npiadmin** and the password **object00**.
- <https://host1.csite.edu:16311/ibm/console/logon.jsp>

- b. Click **Console Settings > Console Integrations.**



- c. Click **NPI.**



- d. Click **Test.** You can ignore the status message.

- e. Click **Save.**

\* Required field

Console Integration ID:

\* Console Integration Name:

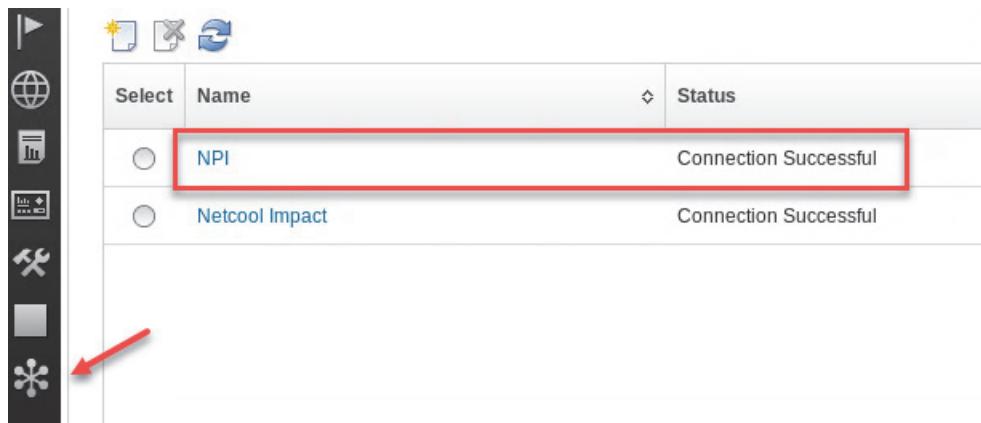
\* Console Integration URL:

Integration Location:

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

Status: **Unable to connect to the remote console. Please check the console URL externally to ensure it works.**

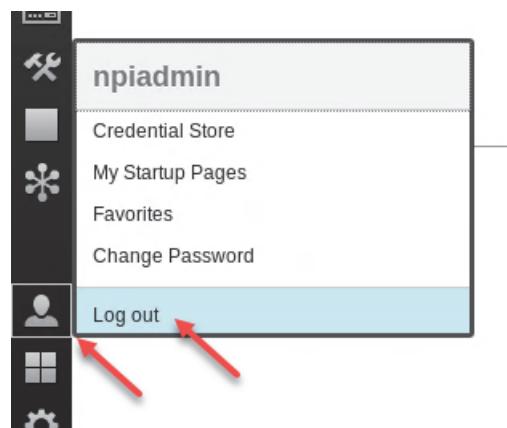
- f. Verify that the connection is successful for the NPI Console Integration. Verify that you see a snowflake icon in the menu on the left.



- g. Close the Console Integrations tab.



- h. Log out of DASH.



## Installing a hot fix

In this section, you install a hot fix to resolve collection and inventory issues.

1. Return to the terminal window where you are the root user.
2. Connect to the npi2.csite.edu host.

```
ssh npi2.csite.edu
```

3. Change to the directory where the hot fix is saved.

```
cd /software/Hotfix
```

4. Decompress the hot fix files.

```
tar -xvf TS003350386_HotFix.tgz
```

5. Change to the correct directory.

```
cd TS003350386_HotFix
```

6. Run the following command to apply the hot fix.

```
./apply_hotfix.sh
```

```
INFO:Updating UI dependency: basecamp-ui
```

```
INFO:Updating UI dependency is done successfully.
```

```
INFO:Updating npi-itnm-collector dependency: npi-itnm-collector
```

```
INFO:Updating npi-itnm-collector dependency is done successfully.
```

```
INFO:Please restart UI, npi-itnm-collector services from ambari portal.
```

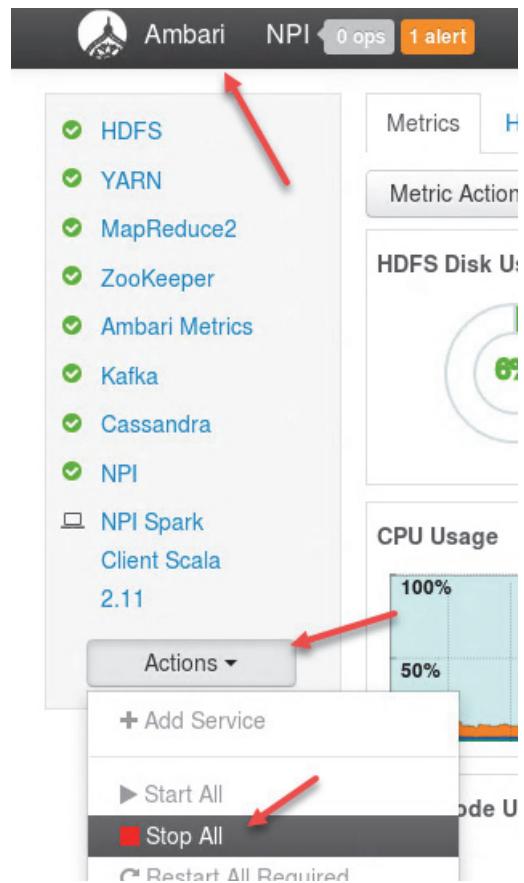
7. Type **exit** to close the connection to npi2.csite.edu.

8. Restart all services.

- a. Return to the Ambari manager page.

- b. Click **Ambari** at the top right of the page.

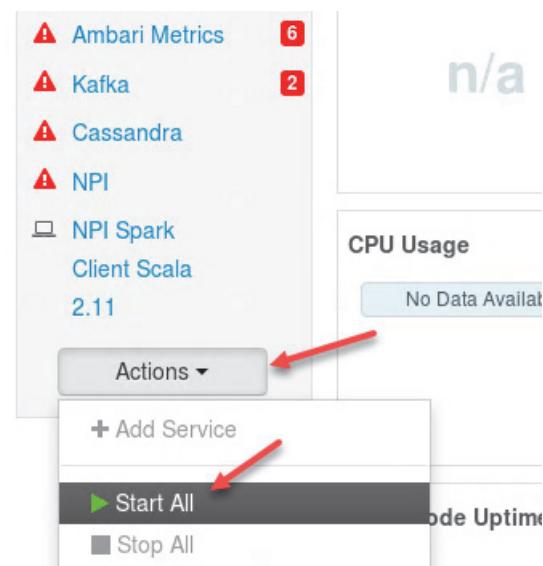
- c. Click **Actions > Stop All.**



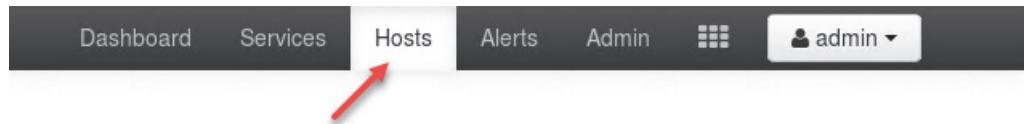
- d. Click **Confirm Stop.**

- e. After a few minutes, the components stop. Click **OK** to close the operations window.

- f. In the same menu, click **Actions > Start All.**



- g. Click **Confirm Start**.
- h. After a few minutes, the components start. Click **OK** to close the operations window.
9. If the Dashboard service is not running, start it manually.
  - a. Click the **Hosts** tab close to the top of the page.



- b. Click **npi2.csite.edu**.

Filter by host and component attributes or search by		
	Name	IP Address
<input type="checkbox"/>	npi1.csite.edu	192.168.
<input checked="" type="checkbox"/>	npi2.csite.edu	192.168.

- a. Scroll down and find the Dashboard service. If it is not running, click the **Stopped** button, then click **Start**.



- b. Click **OK** to confirm.
- c. In a short time, the start operation is 100% complete. Click **OK** to confirm.
- d. Verify that the Dashboard service is started before you continue.



# Exercise 4 Setting the resource scope

By default, Network Performance Insight does not collect SNMP data. To enable SNMP collection, you must set the resource scope to start polling SNMP data for a device or a range of devices. In this exercise, you set the resource scope to include all of the simulated devices.

1. Set the resource scope for SNMP metric collection.

- a. Return to the terminal window where you are the root user.

- b. Change to the target directory.

```
cd /opt/IBM/basecamp/basecamp-installer-tools/snmp
```

- c. Run the following command to set the resource scope to include all of the simulated devices. Run the entire command on one line.

```
./snmp-scoping.sh set npi2.csuite.edu "range(resource.agentIp, '10.10.255.1', '10.10.255.254')"
```

- d. Run the following command to enable SNMP collection for npi2.csuite.edu, which is the host where the SNMP collector is running.

```
./snmp-scoping.sh set npi2.csuite.edu true
```

- e. Run the following command to verify that the scope is enabled.

```
./snmp-scoping.sh list
```

```
npi-npi2.csuite.edu : { "formula.entity-scope" : "true" }
```

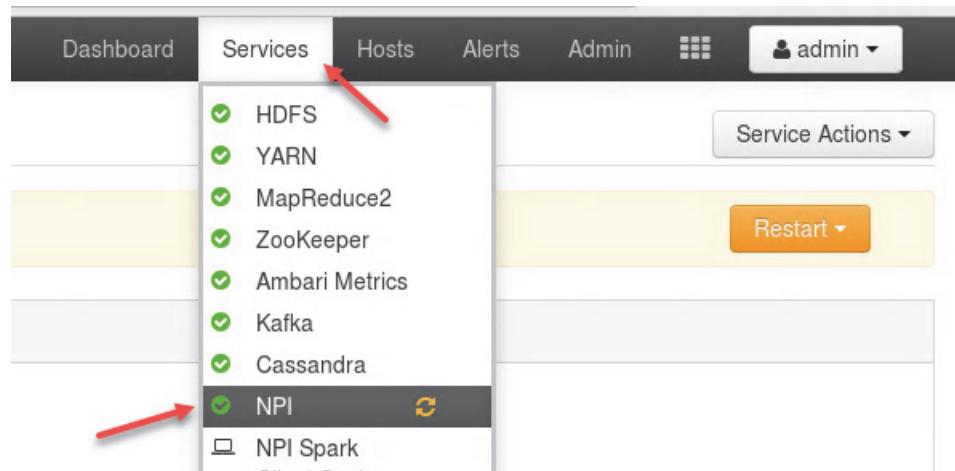
- f. Run the following command to test your scope. Run the entire command on one line.

```
./snmp-scoping.sh test npi2.csuite.edu "range(resource.agentIp, '10.10.255.1', '10.10.255.254')"
```

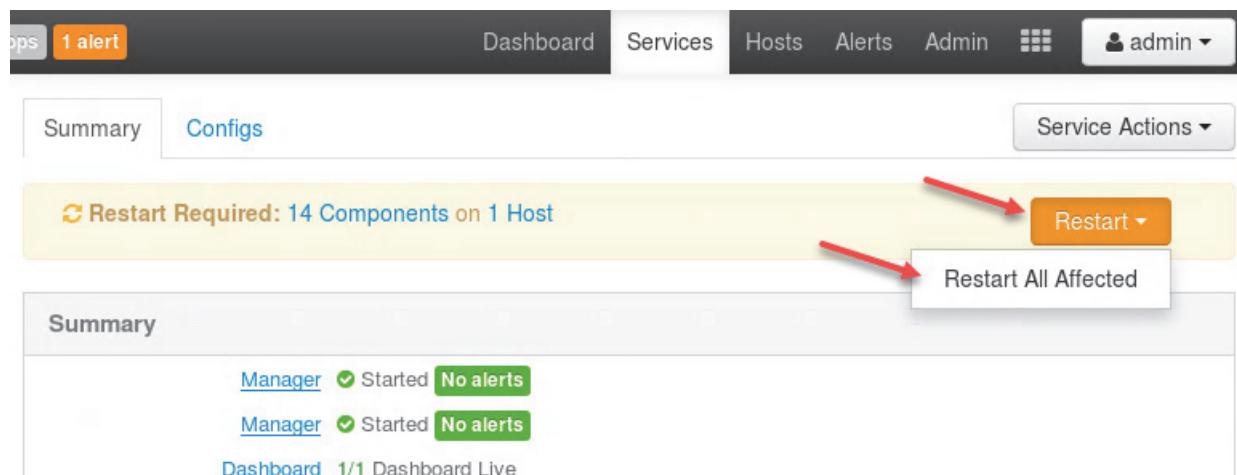
```
[{"entityName": "10.10.255.5"}, {"entityName": "10.10.255.7"}, {"entityName": "10.10.255.10"}, {"entityName": "10.10.255.12"}, {"entityName": "10.10.255.11"}, {"entityName": "10.10.255.2"}, {"entityName": "10.10.255.15"}, {"entityName": "10.10.255.14"}]
```

```
...
```

2. Restart all affected Network Performance Insight services.
  - a. Return to the Ambari manager page.
  - b. Click the **Services** tab and select **NPI**.



- c. Click **Restart > Restart All Affected**.



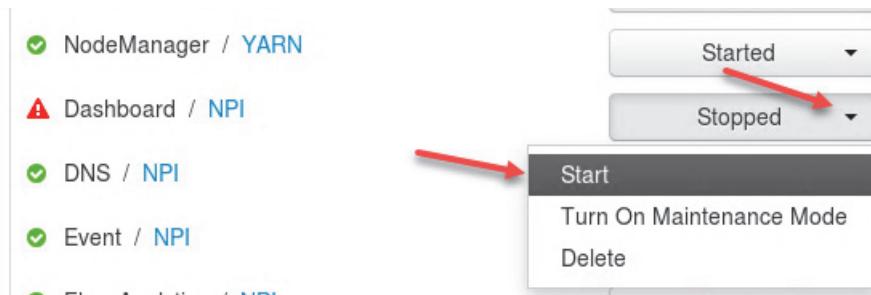
- d. Click **Confirm Restart All**.
- e. Click **OK** when the operation is finished.
- f. Start the Dashboard service manually. Click the **Hosts** tab close to the top of the page.



- g. Click **npi2.csuite.edu**.

Filter by host and component attributes or search by	
Name	IP Address
<input type="checkbox"/> npi1.csuite.edu	192.168.
<input checked="" type="checkbox"/> npi2.csuite.edu	192.168.

- h. Scroll down and find the Dashboard service. If it is not running, click the **Stopped** button, then click **Start**.



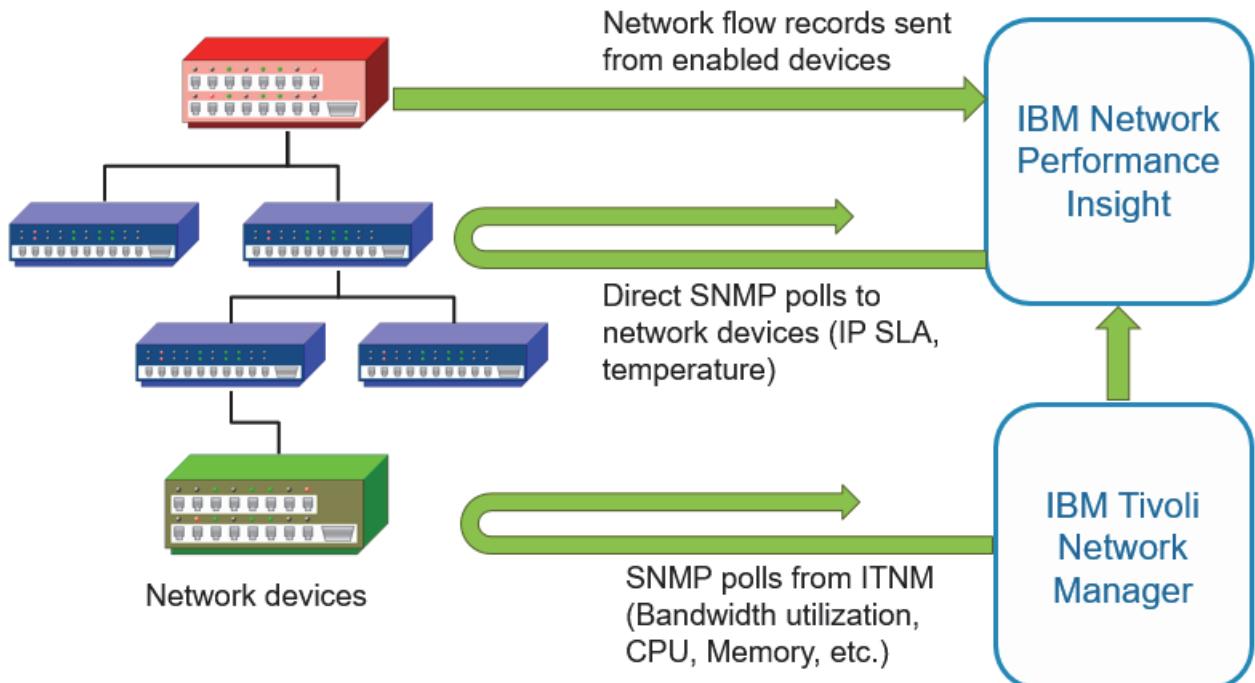
- i. Click **OK** to confirm.  
j. In a short time, the start operation is 100% complete. Click **OK** to confirm.  
k. Verify that the Dashboard service is started before you continue.



# Unit 4 Solution verification

In your lab environment, IBM Network Performance Insight obtains performance data using the following three methods:

- **From network flow records:** A network flow record is data that is generated by a network device, such as a router or switch. The data in a network flow record describes the traffic that has passed through a network interface of the device. The devices export these flow records to IBM Network Performance Insight.
- **From SNMP polls:** Network devices can expose performance measurements about themselves using SNMP agents. IBM Network Performance Insight can directly poll these SNMP-enabled devices to obtain the current value of these measurements. In your lab environment, IBM Network Performance Insight is directly polling the simulated network devices for IP SLA metrics.
- **From IBM Tivoli Network Manager:** IBM Tivoli Network Manager can also poll devices for SNMP data. IBM Network Performance Insight can obtain the metrics that are generated by IBM Tivoli Network Manager and use them in reports and dashboards. In your environment, IBM Network Performance Insight is reusing IBM Tivoli Network Manager metrics such as bandwidth utilization, CPU utilization, memory utilization, and others.



In these exercises, you verify that IBM Network Performance Insight is successfully collecting, aggregating, and reporting performance data from these three data sources. You also learn how to navigate the IBM Network Performance Insight user interface and set thresholds on flow data.

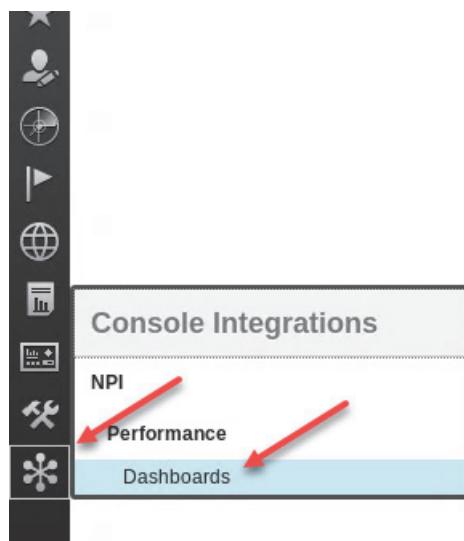
1. One of the devices in your simulated network is exporting flow records. Verify that IBM Network Performance Insight is processing network flow records.

- a. Browse to Dashboard Application Service Hub (DASH). Go to the following URL:

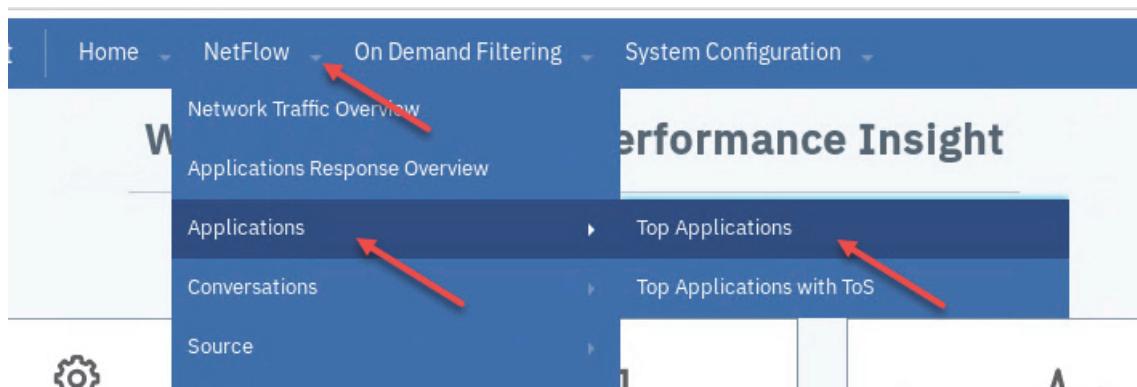
<https://host1.csite.edu:16311/ibm/console/logon.js>

- b. Log in with the user name **npiadmin** and the password **object00**.

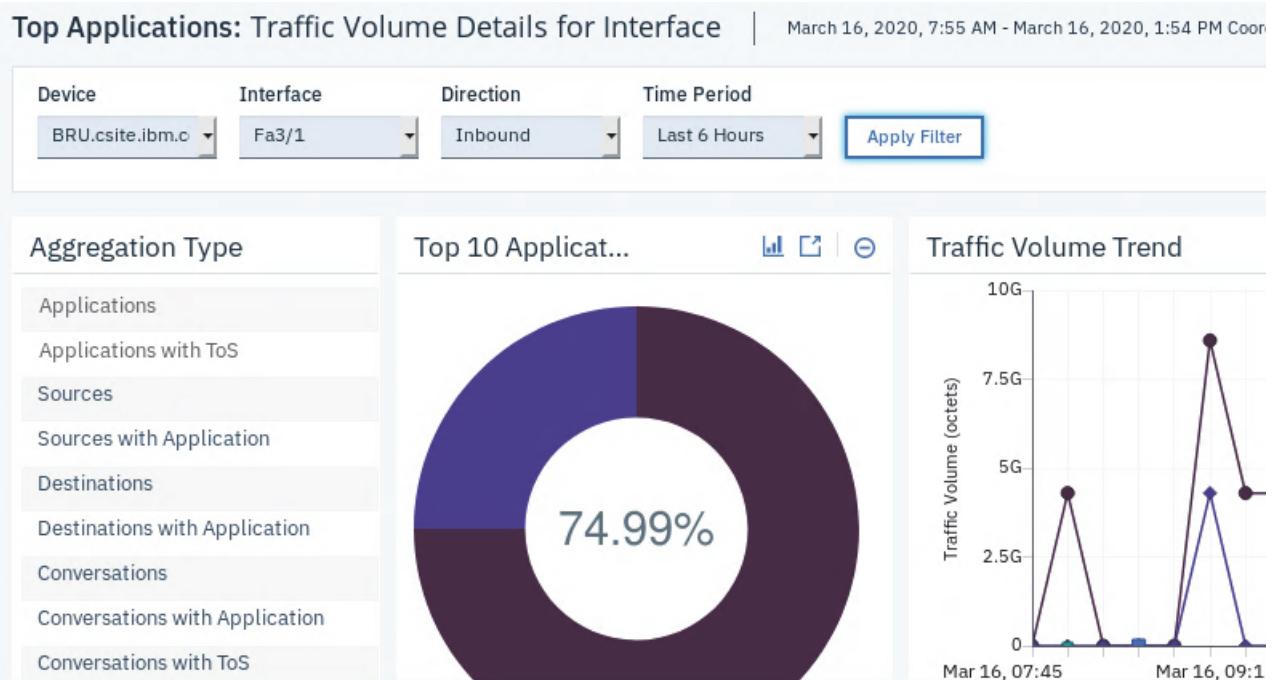
- c. Click **Console Integrations > Dashboards**.



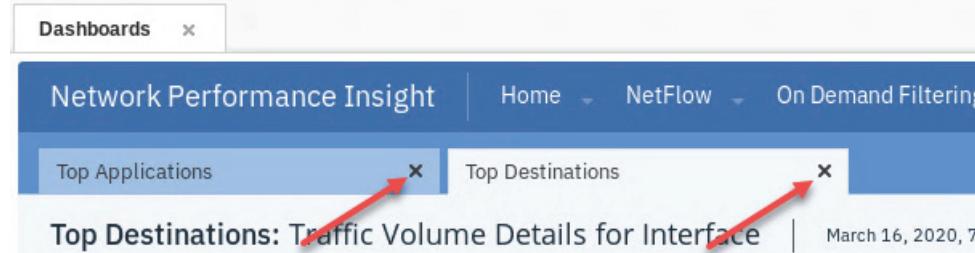
- d. Click **NetFlow > Applications > Top Applications**.



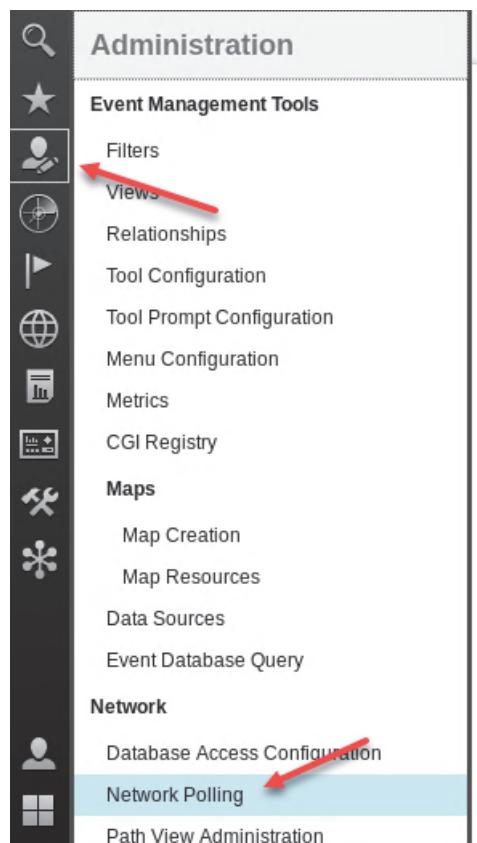
- e. This dashboard shows the top applications that are flowing through the device. Notice the following features of this page:
- ◆ At the top of the dashboard, you can change the network interface, traffic direction, and reporting time period.
  - ◆ If you scroll down, you see additional data about each network application.
  - ◆ On the left of the page, you can change the dashboard to show other aspects of network traffic, such as traffic categorized by source, destination, and conversations between two end points.



- f. Spend a few moments interacting with this dashboard. Change the aggregation type on the left of the page to explore all of the aspects of network traffic that are derived from network flow records.
- g. Close the **Top Applications** tab and any other NetFlow dashboards you have opened.



2. Some metrics are collected by IBM Tivoli Network Manager and reused by IBM Network Performance Insight. Verify that these metrics are present in IBM Network Performance Insight reports and dashboards.
  - a. IBM Tivoli Network Manager is polling devices for several metrics. Look at the specific metrics that IBM Tivoli Network Manager is collecting.
  - b. Click **Administration > Network Polling**.



- c. Scroll down through the list of poll definitions and view the metrics that are enabled. These metrics are polled by IBM Tivoli Network Manager and reused by IBM Network Performance Insight. Notice that IP SLA metrics are not in this list, meaning they are not collected by IBM Tivoli Network Manager.

- d. Close the Network Polling tab when you are finished.

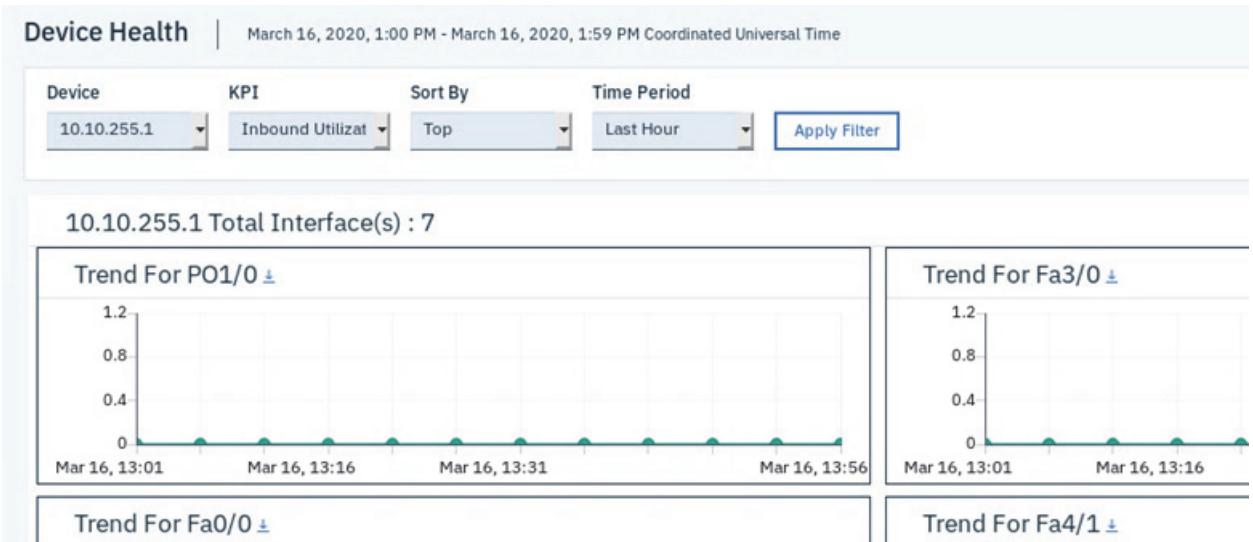
The screenshot shows a table titled "Network Polling" with a domain set to "NOI\_AGG\_P". The table has columns for "Enabled" (checkboxes), "Status" (checkboxes), and "Name". All metrics listed are enabled and have a green checkmark in the status column. The names of the metrics are: ciscoEnvMonTemperatureState, ciscoMemoryPctgUsage, ciscoMemoryPool, ConfirmDeviceDown, and ConfirmHighDiscardRate.

Enabled	Status	Name
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscoEnvMonTemperatureState
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscoMemoryPctgUsage
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscoMemoryPool
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ConfirmDeviceDown
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ConfirmHighDiscardRate

- e. View the corresponding metrics in IBM Network Performance Insight. Return to the **Dashboards** tab.  
f. Click **On Demand Filtering > Device Health**.

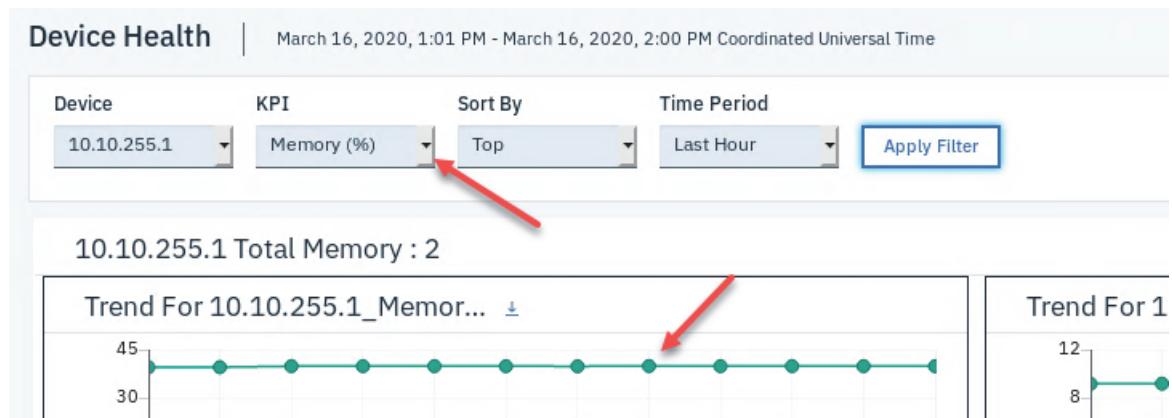
The screenshot shows the IBM Network Performance Insight dashboard. The top navigation bar includes tabs for "Dashboards", "Home", "NetFlow", "On Demand Filtering", and "System Configuration". The "On Demand Filtering" tab is currently active and its dropdown menu is open, showing options: Device Health, IP SLA, Flow, HTTP Operations, and Timeseries Data. The main dashboard area displays a "Welcome" message and some network-related icons.

- g. Look at the Device Health Dashboard. At the top of the page, you can change the device, the KPI, and the reporting time period. In this example, the metric is inbound utilization. Remember that IBM Tivoli Network Manager is collecting this metric.



3. Open a historical trend dashboard.

- a. Select a KPI at the top of the page. In your lab environment, memory utilization is likely to change over time. Click a data point in one of the charts.



- b. The historical trend dashboard opens. This shows the metric over time along with minimum, maximum, and average values.



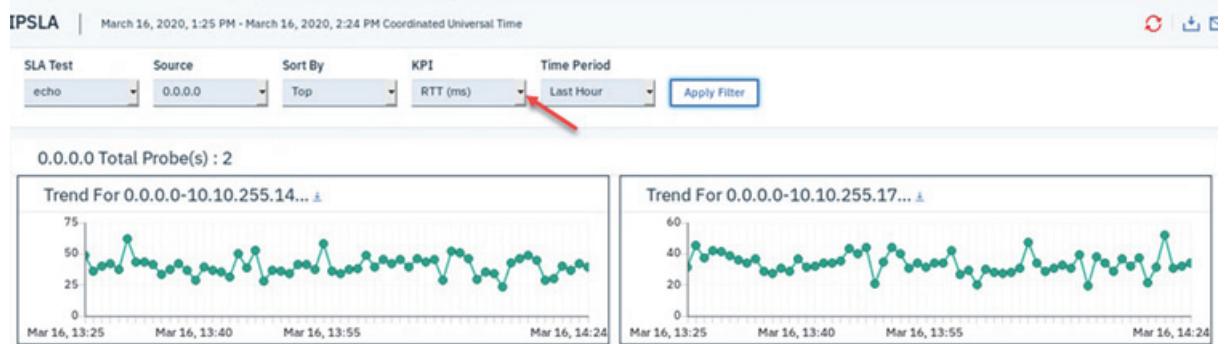
- c. Close any Device Health dashboards you have opened.

The screenshot shows the 'Network Performance Insight' dashboard interface. At the top, there's a navigation bar with 'Dashboards' and other options. Below it, a blue header bar contains the title 'Network Performance Insight' and several dropdown menus like 'Home', 'NetFlow', 'On Demand Filtering', etc. Two tabs are visible: 'Device Health' and 'Device Health History'. The 'Device Health History' tab is currently active, displaying a timestamp from March 16, 2020, 1:05 PM to March 16, 2020, 2:04 PM. Below the tabs are four filter buttons: 'Device', 'KPI', 'Resource', and 'Time Period'. Red arrows point to the close (X) icons on both the 'Device Health' and 'Device Health History' tabs.

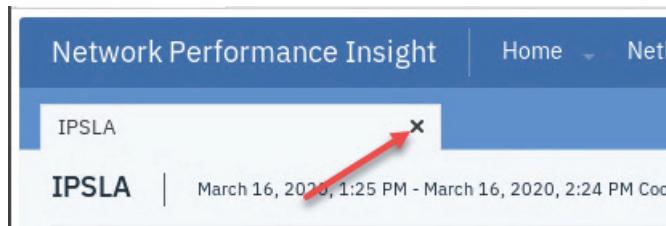
4. Recall that IBM Tivoli Network Manager is not polling for IP SLA data. View IP SLA data in reports and dashboards to confirm that IBM Network Performance Insight is directly polling for IP SLA statistics.
- Click **On Demand Filtering > IPSLA**.

The screenshot shows the 'Network Performance Insight' dashboard with the 'On Demand Filtering' menu open. The menu items include 'Device Health', 'IPSLA' (which is highlighted), 'Flow', and 'HTTP Operations'. A red arrow points to the 'IPSLA' option. The background shows a 'Welcome' message and some dashboard cards.

- Change the KPI to **RTT (ms)**. This metric shows round-trip times for ICMP echoes across network segments.

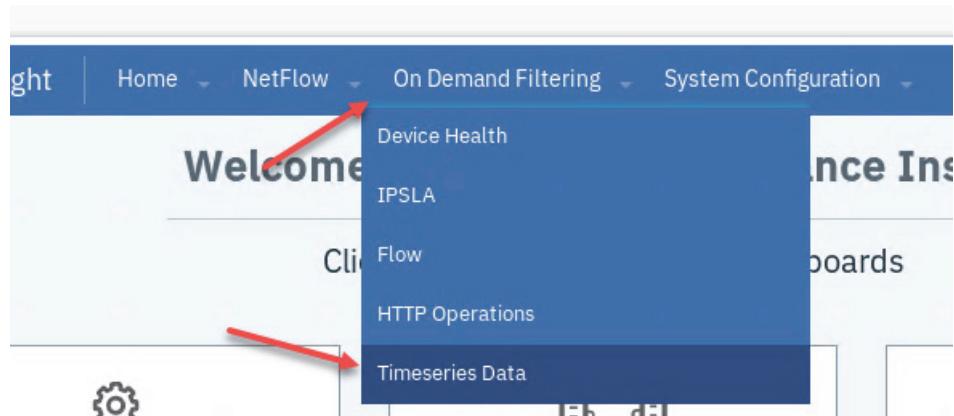


c. Close the IPSLA dashboard.



5. Test the time series reports.

a. Click **On Demand Filtering > Timeseries data**.



b. In the list of KPIs on the left, scroll down and select **Network.Inbound.Utilization.Percent** and **Network.Outbound.Utilization.Percent**.

c. Right-click one of the selected metrics and click **KPI(s) Trend**.

Device	Resource Type	Resource Name	Time Period
10.10.255.1	interface	10.10.255.1-PO	Last Hour

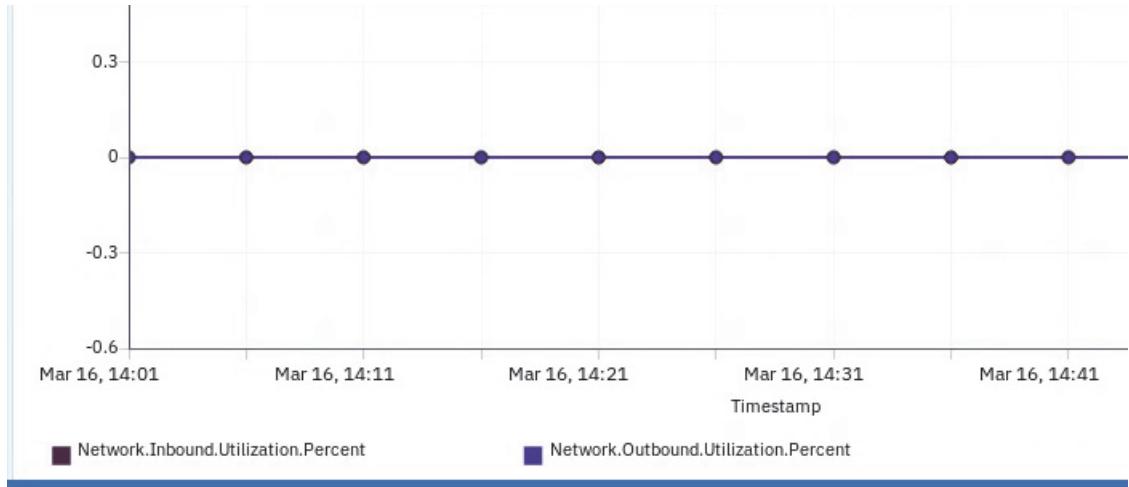
  

List of KPI	
<input type="checkbox"/>	KPI Name
<input type="checkbox"/>	Network.Inbound.Frame.Count
<input type="checkbox"/>	Network.Unknown.Protocols.Dropped.C
<input type="checkbox"/>	Network.Outbound.Packets.Count
<input checked="" type="checkbox"/>	Network.Inbound.Utilization.Percent
<input type="checkbox"/>	Network.Inbound.Broad

**KPI(s) Trend**

KPI(s) Trend - Network.Inbound.Ignored.	

- d. The selected metrics are plotted on a chart. In this example, inbound and outbound utilization are close to zero because minimal traffic is flowing through the simulated network.

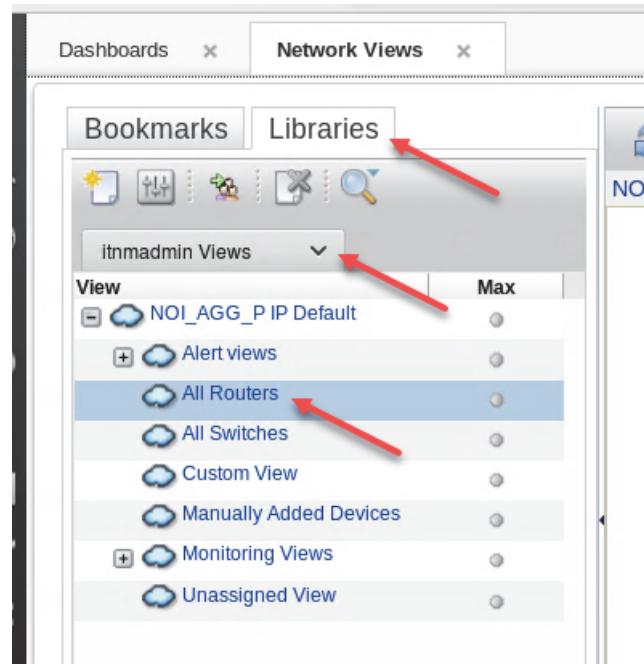


- e. Close the **Timeseries Data** tab.

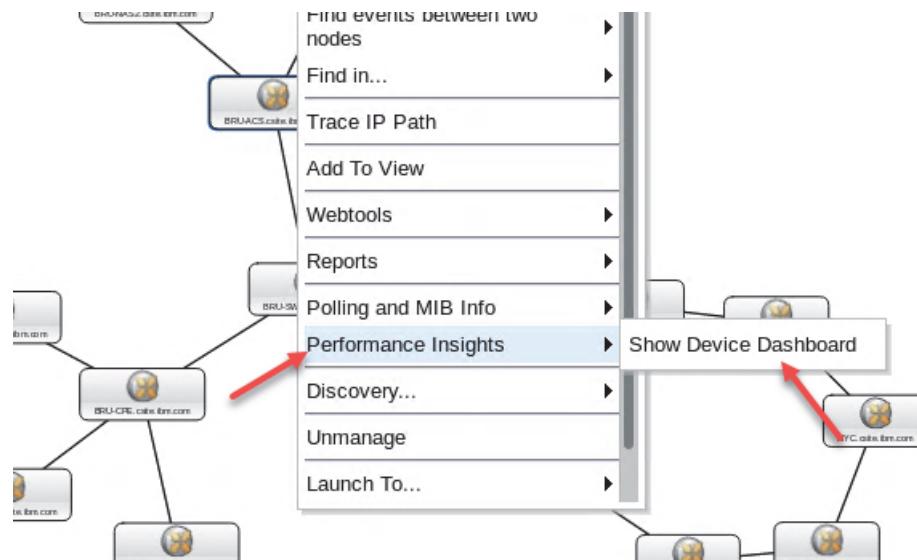
6. Confirm that the Device Dashboard shows IBM Network Performance Insight data. You access the Device Dashboard from an IBM Tivoli Network Manager network view.
- Open a network view. Click **Incident > Network Views**.

- Click the **Libraries** tab.
- Select **itnmadmin Views**.

d. Expand **NOI\_AGG\_P IP Default** and click **All Routers**.



e. Right-click any device and click **Performance Insights > Show Device Dashboard**.



- f. Note the list of metrics at the top right of the dashboard. These metrics are coming from Network Performance Insight.

The screenshot shows two panels side-by-side. The left panel is titled 'Topology' and displays a network diagram with four nodes and various connections. The right panel is titled 'Metrics' and lists three metrics: 'Controller APIs.Connected', 'CPU.Utilization.Percent', and 'ICMP.Message.Received'. The 'CPU.Utilization.Percent' row is highlighted with a red box.

- g. Click the **Interfaces** tab.  
h. Select Network.Inbound.Utilization.Percent as the metric. Scroll down and view the utilization for each interface for the last 30 minutes.

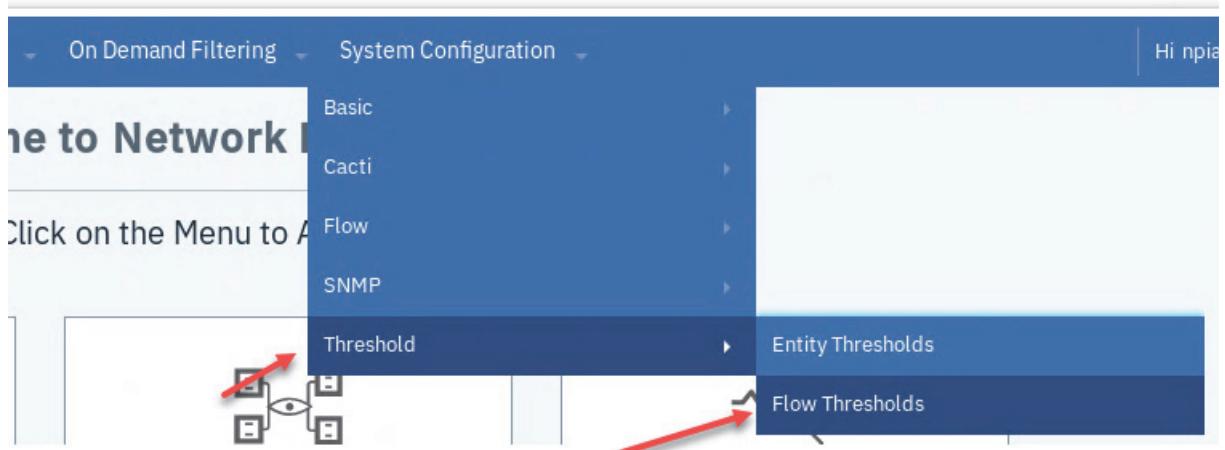
The screenshot shows the 'Interfaces (24)' tab selected. A red arrow points to the tab title. Another red arrow points to the 'Metric' dropdown menu, which is set to 'Network.Inbound.Utilization.'. Below the table, a red arrow points to the 'Last 30 mins' column header. The table lists two interfaces: Fa0/0 and Fa1/0, both showing 0 utilization.

Metric	Network.Inbound.Utilization.	Number Polled (4)	Filter	
Sev.	Interface	Metric Thresholds	Value	Last 30 mins
[Green]	Fa0/0	No metric thresholds set	0	
[Green]	Fa1/0	No metric thresholds set	0	

- i. Close the **Network Views** and **Device Dashboard** tabs.

The screenshot shows the top navigation bar with three tabs: 'Dashboards', 'Network Views', and 'Network Performance Insight Device Dashboard'. Red arrows point to the 'Network Views' and 'Network Performance Insight Device Dashboard' tabs, indicating they are being closed.

7. Set a traffic volume threshold for one of the interfaces where network flow is enabled.
  - a. Return to the IBM Network Performance Insight user interface.
  - b. Click **System Configuration > Threshold > Flow Thresholds**.



- c. Find the **BRU.csuite.ibm.com-Fa3/0** egress interface.
- d. Click **Edit**.

Flow Thresholds								
Configure flow thresholds for each interface								
Enabled	Interface	Speed	Direction	Limit Type	Upper Limit	Lower Limit	Number of Events	Actions
No	BRU.csuite.ibm.com-Fa3/0	100000000	Egress	Over	3.00 KB	2.25 KB	2	<a href="#">Edit   Enable</a>
No	BRU.csuite.ibm.com-Fa3/0	100000000	Ingress	Over	3.00 KB	2.25 KB	2	<a href="#">Edit   Enable</a>
No	BRU.csuite.ibm.	100000000	Egress	Over	6.60 KB	4.95 KB	2	<a href="#">Edit  </a>

- e. Select **Enabled**.
- f. Enter **40** as the upper limit.
- g. Enter **35** as the lower limit.

h. Click **OK**.

**Edit Flow Threshold**  
Configure the selected flow threshold

Enabled

Limit Type: Over

Upper Limit: 40 KB / Minute

Lower Limit: 35 KB / Minute

Number of Events: 2

Ok Cancel

i. Find the **BRU.csite.ibm.com-Fa3/0** ingress interface.

j. Click **Edit**.

**Flow Thresholds**

Configure flow thresholds for each interface

Enabled	Interface	Speed	Direction	Limit Type	Upper Limit	Lower Limit	Number of Events	Actions
No	BRU.csite.ibm.com-Fa3/0	100000000	Egress	Over	3.00 KB	2.25 KB	2	<a href="#">Edit   Enable</a>
No	BRU.csite.ibm.com-Fa3/0	100000000	Ingress	Over	3.00 KB	2.25 KB	2	<a href="#">Edit   Enable</a>
No	BRU.csite.ibm.	100000000	Egress	Over	6.60 KB	4.95 KB	2	<a href="#">Edit  </a>

k. Select **Enabled**.

l. Enter **40** as the upper limit.

m. Enter **35** as the lower limit.

n. Click **OK**.

**Edit Flow Threshold**  
Configure the selected flow threshold

Enabled

Limit Type: Over

Upper Limit:	40	/ KB	/ Minute
Lower Limit:	35	/ KB	/ Minute
Number of Events:	2		

Ok Cancel

o. Verify that both thresholds are enabled.

**Flow Thresholds**  
Configure flow thresholds for each interface

Enabled    Interface    Speed    Direction

Enabled	Interface	Speed	Direction
Yes	BRU.csuite.ibm.com-Fa3/0	100000000	Egress
Yes	BRU.csuite.ibm.com-Fa3/0	100000000	Ingress
No	BRU.csuite.ibm.com-Fa3/0	100000000	Egress

8. Generate a burst of HTTP traffic through the simulated network. This burst will cause the thresholds to be violated.

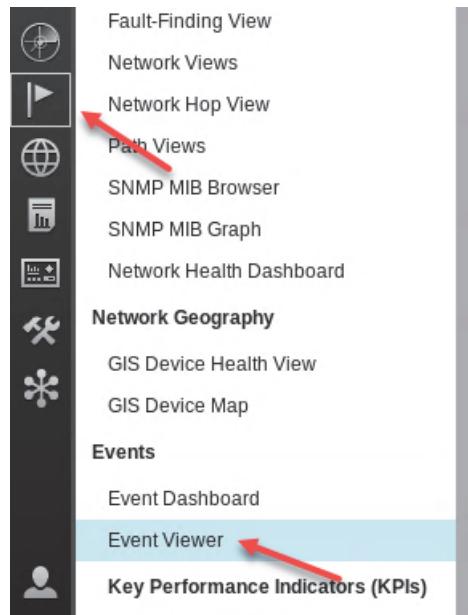
a. Change to the target directory.

/home/netcool/traffic\_scripts

b. Run the following script to generate traffic.

./http\_generate.sh

9. When a threshold is violated, IBM Network Performance Insight sends notification to Netcool/OMNibus. Look at the threshold violation event and investigate the violation with the Traffic Details page.
- Open the Netcool/OMNibus event viewer. Click **Incident > Event Viewer**.



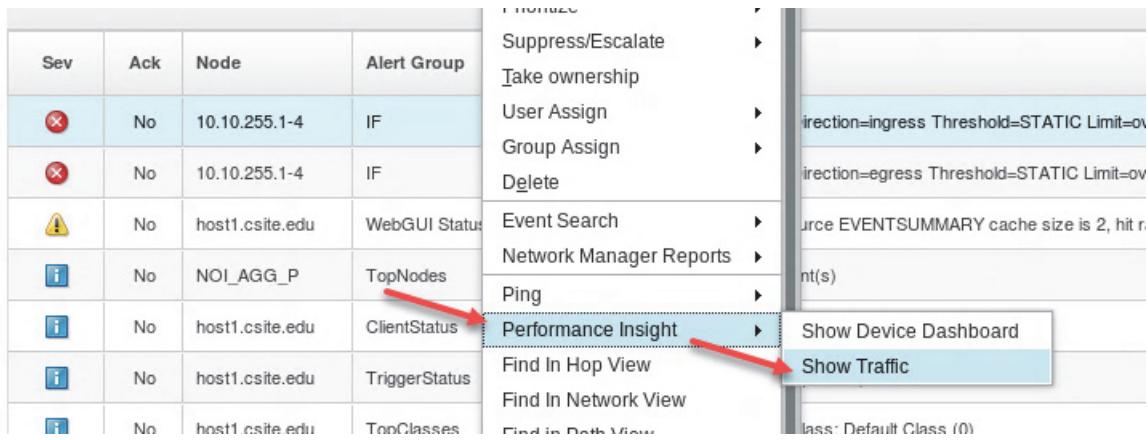
- After a short time, you see events like the following example. The node in the events is **10.10.255.1-4**. You might see events for the ingress interface, the egress interface, or both.

The screenshot shows the 'Event Viewer' window. The title bar says 'Event Viewer'. The main area displays a table of events:

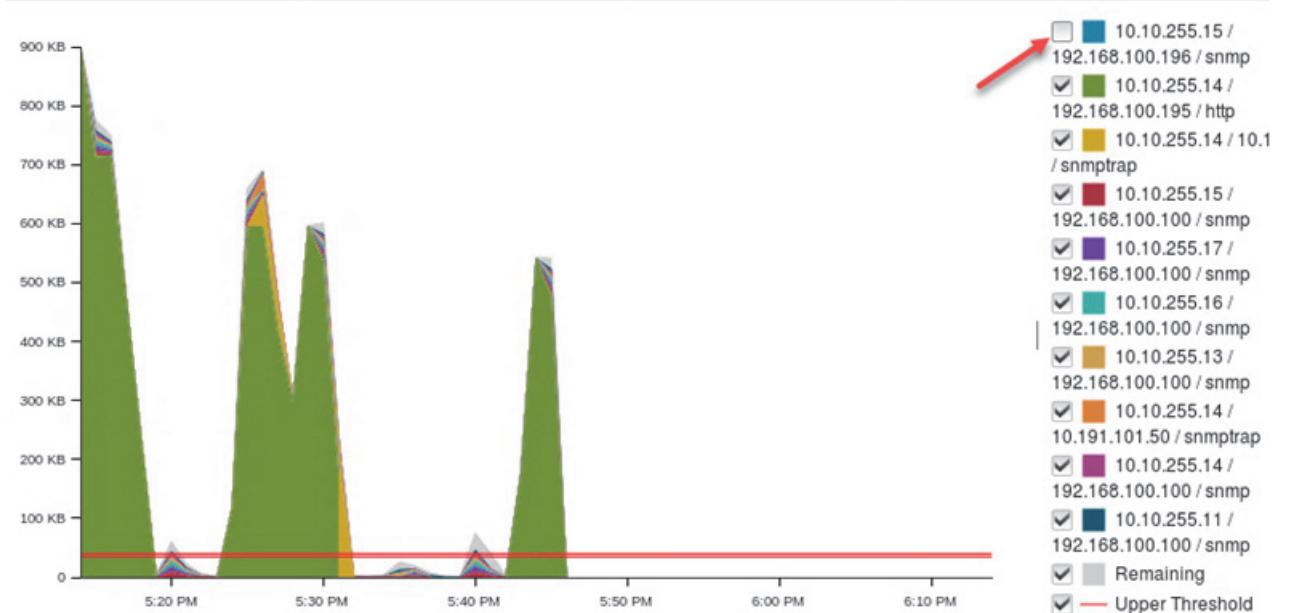
Sev	Ack	Node	Alert Group	Summary
✗	No	10.10.255.1-4	IF	IpAddress=10.10.255.1 Interface=4 Direction=egress Threshold=STATIC Limit=over Upper=
✗	No	10.10.255.1-4	IF	IpAddress=10.10.255.1 Interface=4 Direction=ingress Threshold=STATIC Limit=over Upper=
⚠	No	host1.csite.edu	WebGUI Status	ALERT: Web GUI OMNIBUS data source EVENTSUMMARY cache size is 2, hit rate: 16%

The first two rows, corresponding to the node 10.10.255.1-4, are highlighted with a red border.

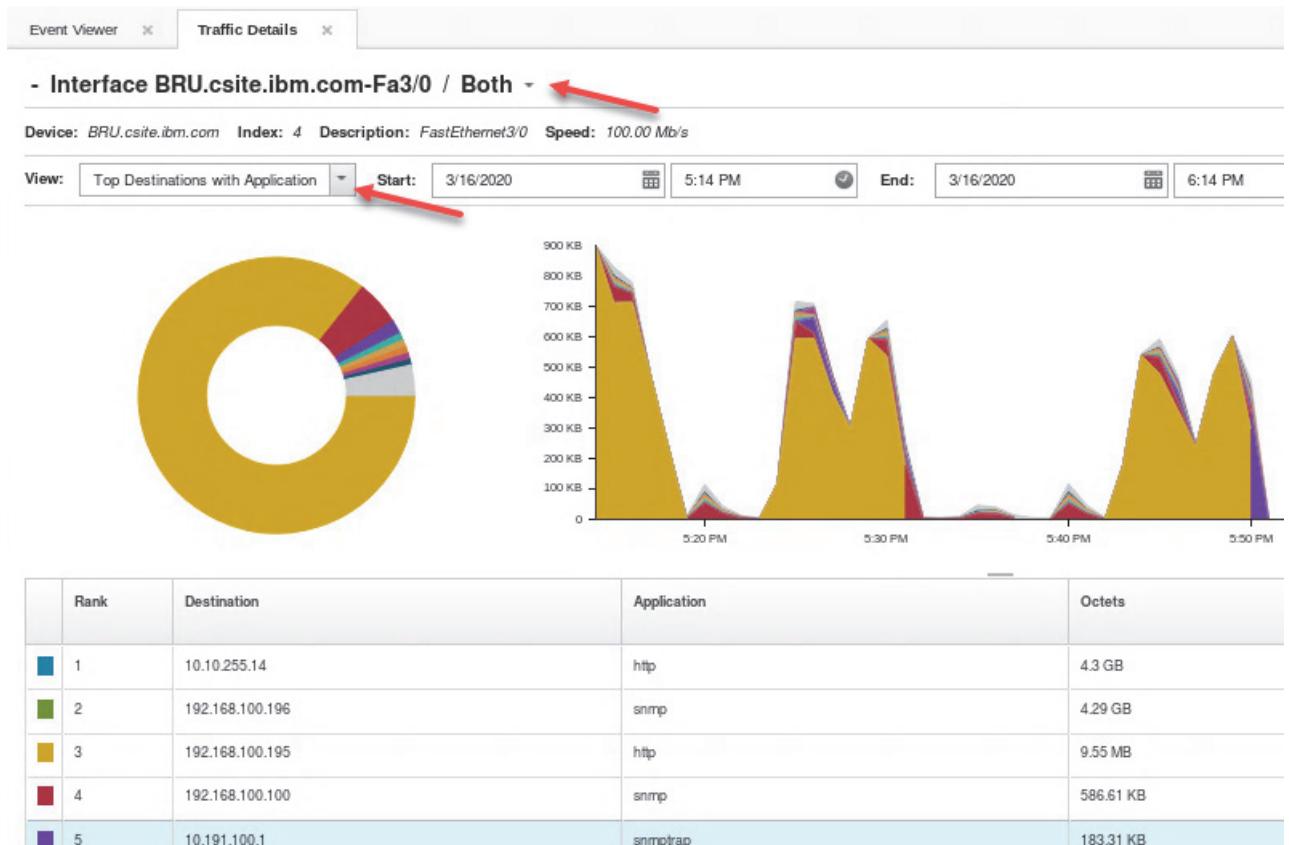
- c. Right-click one of the events and click **Performance Insight > Show Traffic**.



- d. The Traffic Details page is displayed, along with the threshold levels. On the right, you can select and deselect different traffic flows and applications for display. This helps you to identify the following attributes of the threshold violation:
- ◆ The network application, for example HTTP
  - ◆ The source of the traffic
  - ◆ The destination of the traffic



- e. Take some time to explore the traffic details page. Notice that you can change the traffic direction to ingress, egress, or both. You can also change the report view to show these traffic aspects and more:
- ◆ Top Sources
  - ◆ Top Sources with Application
  - ◆ Top Applications
  - ◆ Top Applications with Source
  - ◆ Top Applications with Destination
  - ◆ Top Applications with Conversation
  - ◆ Top Protocols
  - ◆ Top Protocols with Source
  - ◆ Top Protocols with Application
  - ◆ Top Protocols with Destination
  - ◆ Top Conversations
  - ◆ Top Conversations with Application
  - ◆ Top Destinations
  - ◆ Top Destinations with Application







IBM Training



© Copyright IBM Corporation 2020. All Rights Reserved.