Course Exercises

IBM Network Performance Insight 1.3.1 Installation and Configuration

Course code: TN530 ERC 1.0

IBM Training

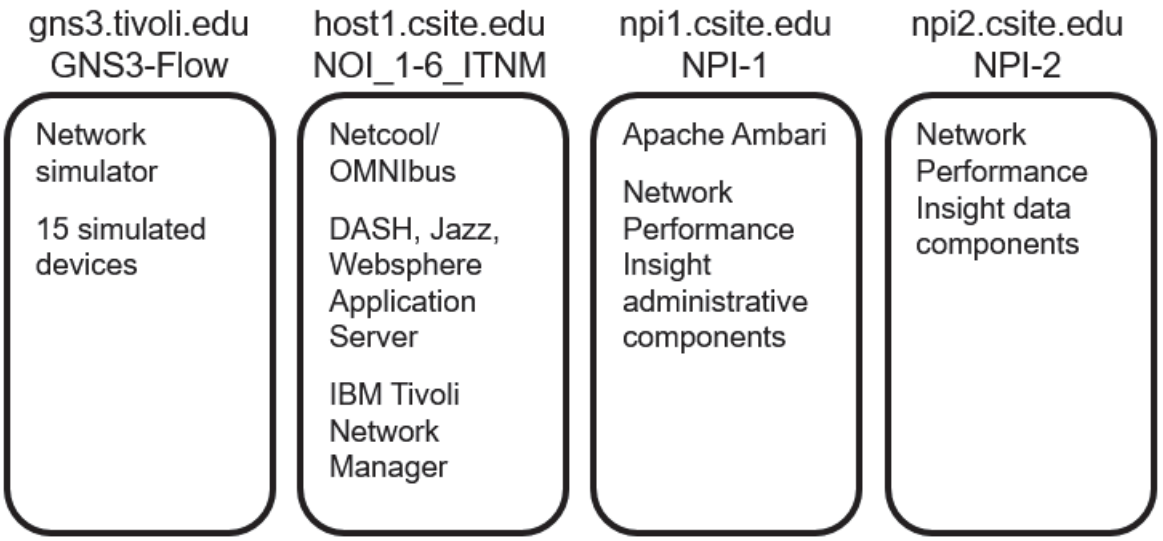
March 2020 edition

Contents

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.csite.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.csite.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.csite.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

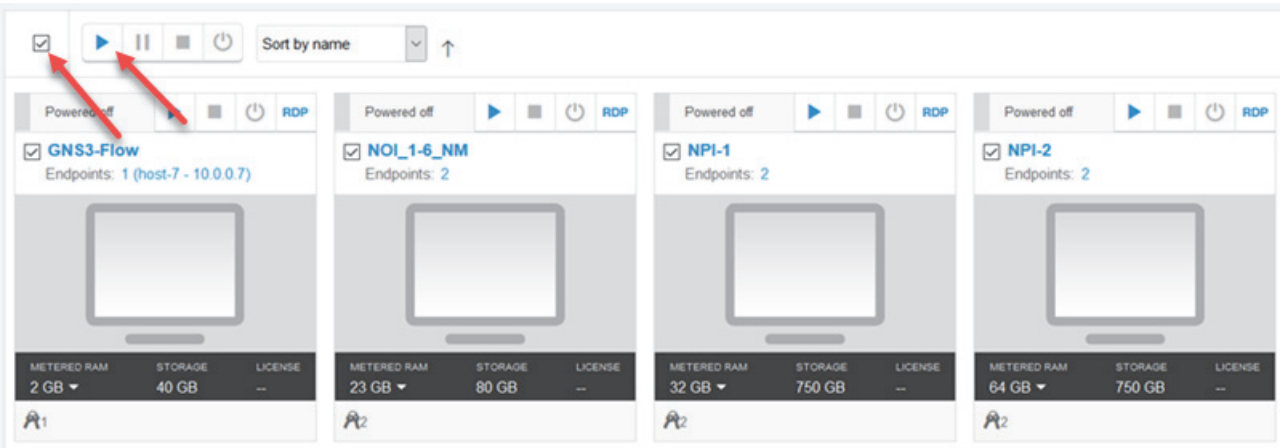
Exercise 1 Getting started

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

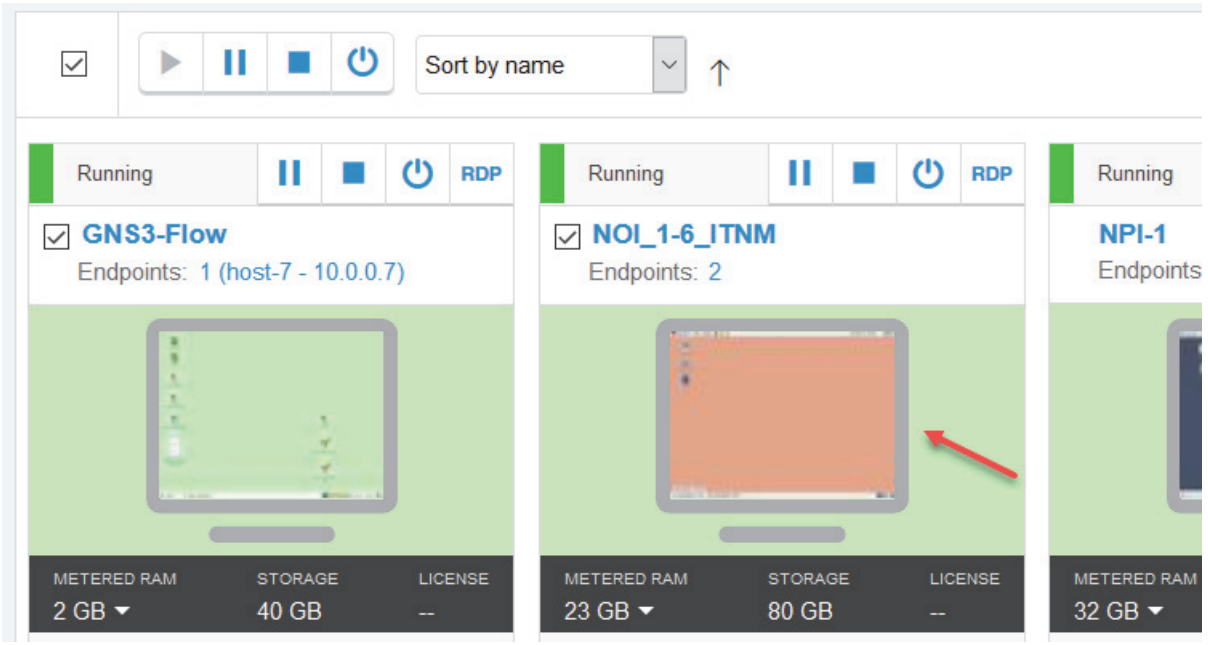
Starting your lab

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

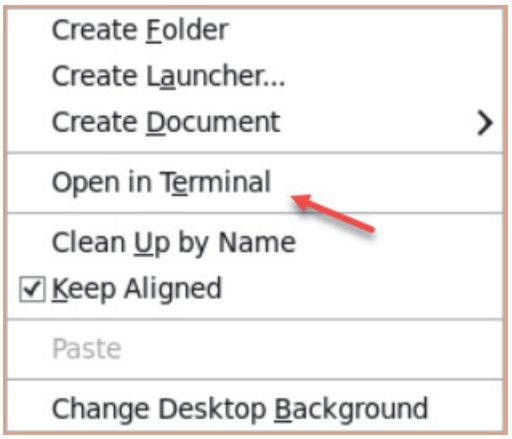
1. Depending on how this course is delivered, your lab servers might already be running. If they are not running, start them now.
   a. Click the check box at the top left to select all four virtual servers.
   b. Click the **Run** button to start all four servers. The lab servers take about 10 minutes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

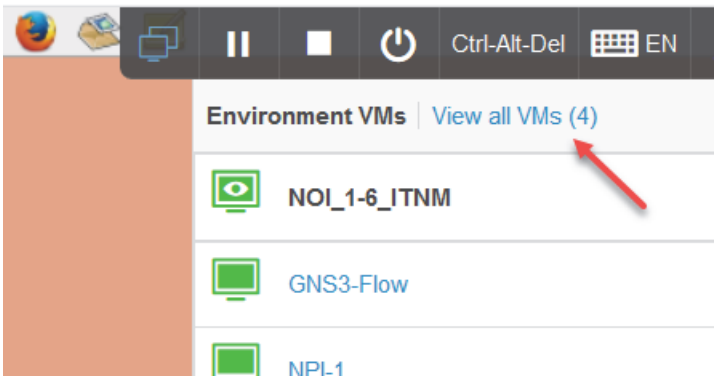
```
rm -rf /opt/IBM/tivoli/netcool/var/precision/storm/sup.skt

itnm_start storm
```

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

```
intm_status
```

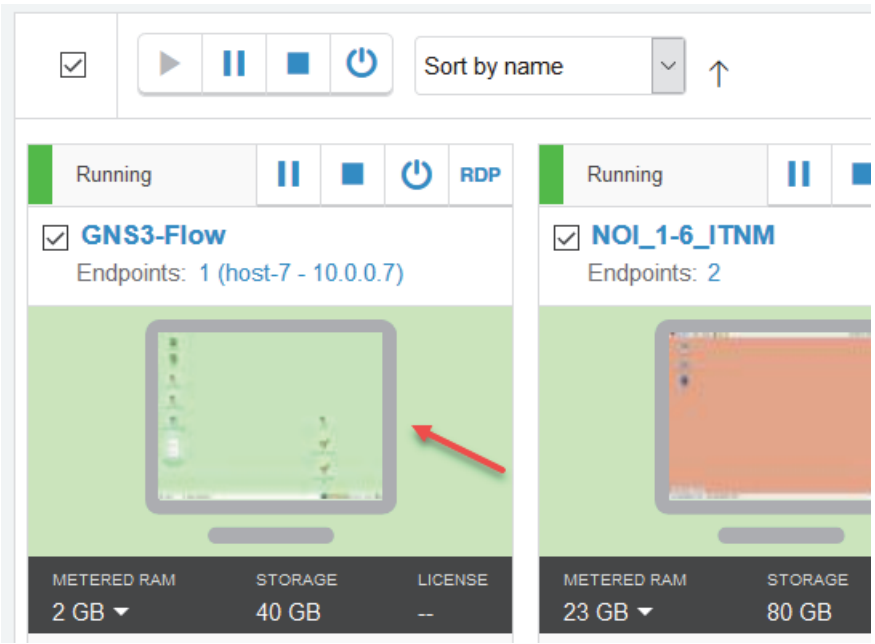
g. Click the tab at the top of the window to view the lab environment options.

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



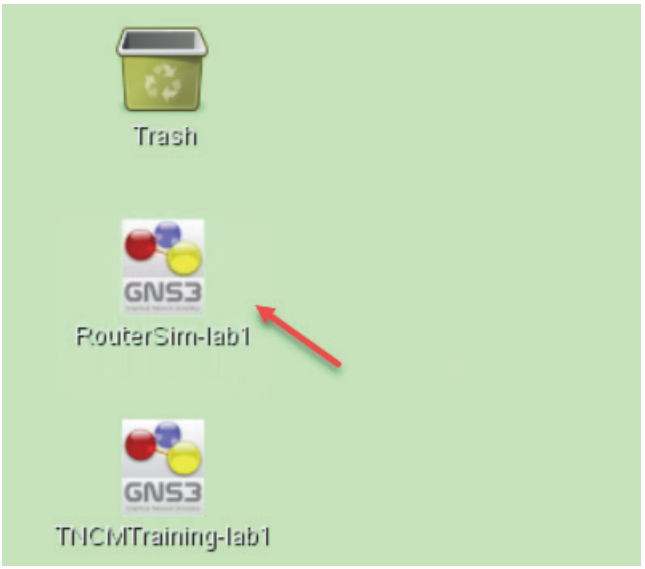
3. Start the network simulator.

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

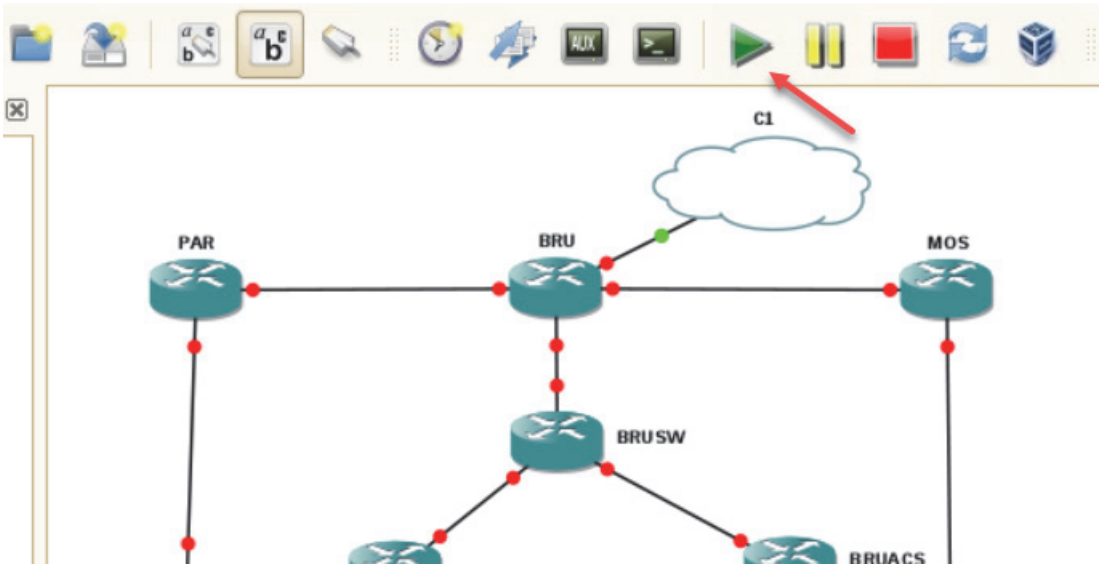


b. Log in to the host with the user name **root** and the password **object00**.

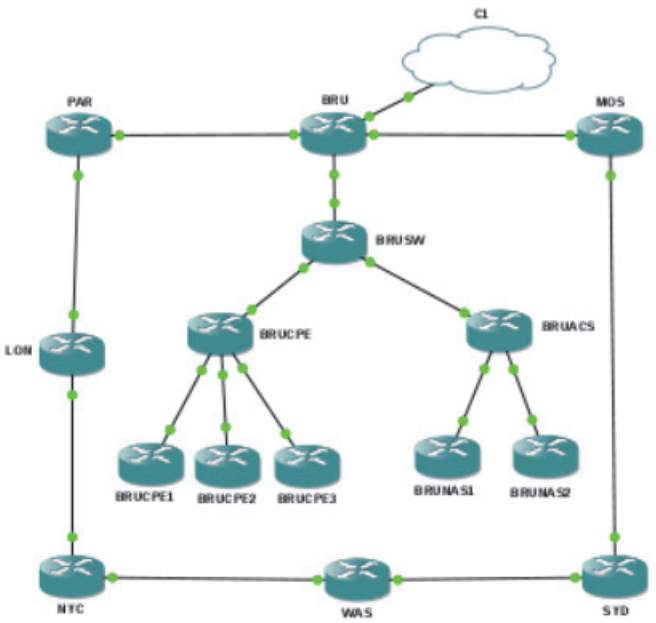
c. Right-click the **RouterSim-lab1** icon and click **Open**.



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

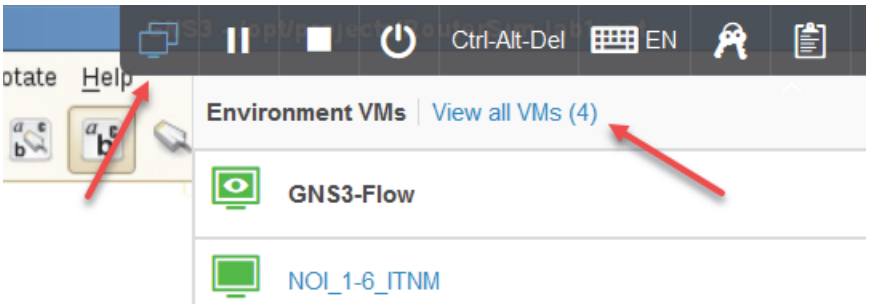


e. Wait until all of the red dots turn green.



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

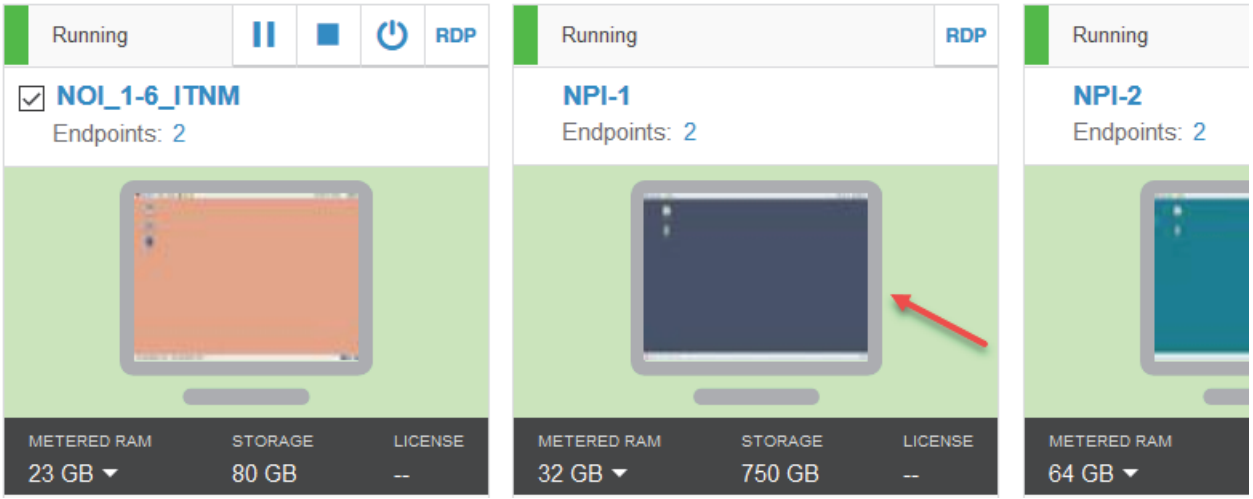
g. Click the icon for environment VMs. Click **View all VMs**.



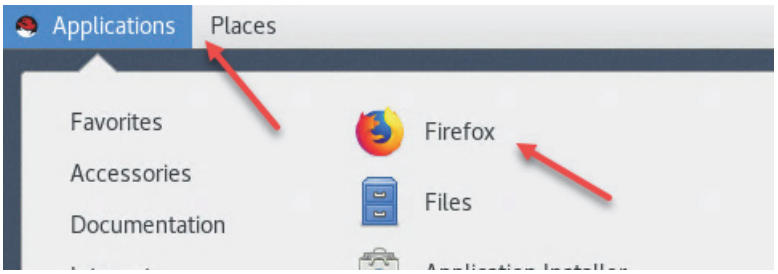
Discovering the network

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**.



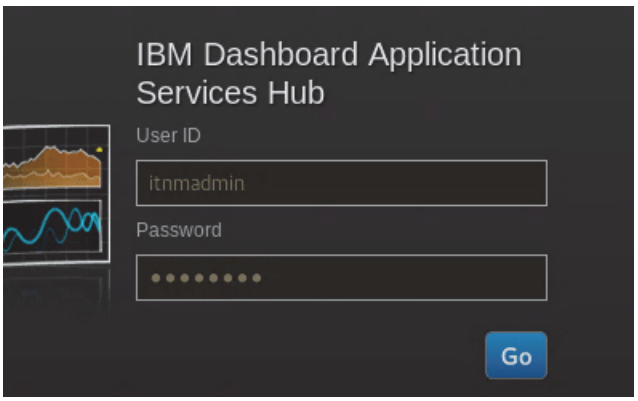
2. Discover the simulated network.
   a. Open a browser window and login to Dashboard Application Services Hub (DASH) as the **itnmadmin** user.
   b. Click **Applications > Firefox** at the top left of the desktop.



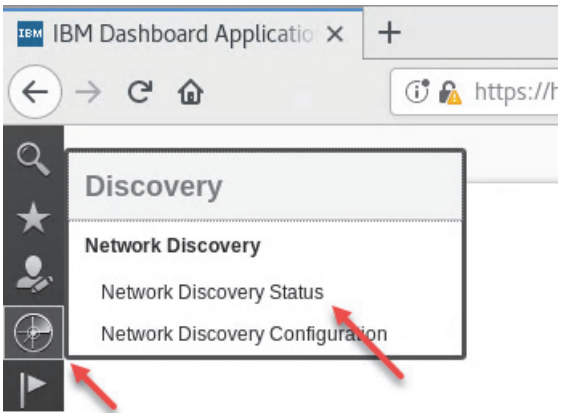
   c. Go to the following URL:

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

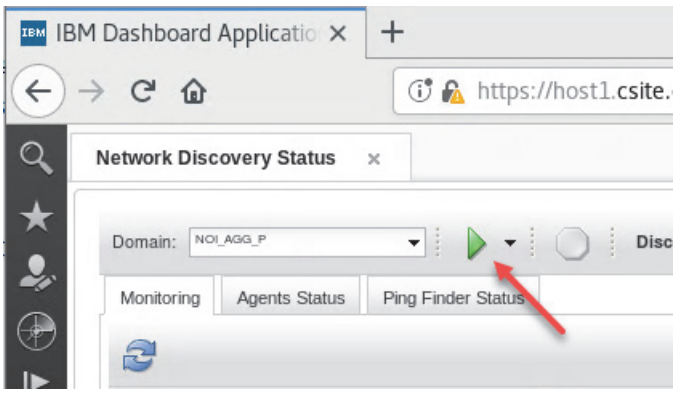
d. Log in with the user name **itnmadmin** and the password **object00**.



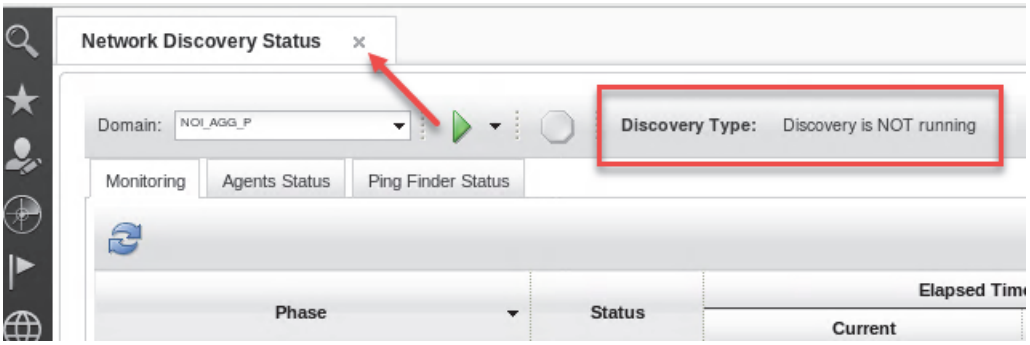
e. Click **Discovery > Network Discovery Status**.



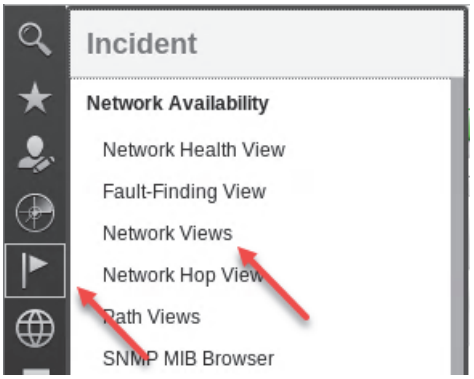
f. Click the green start button. Look for the messages: `Discovery Starting`, or `Full Discovery`. The discovery process takes about six minutes.



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

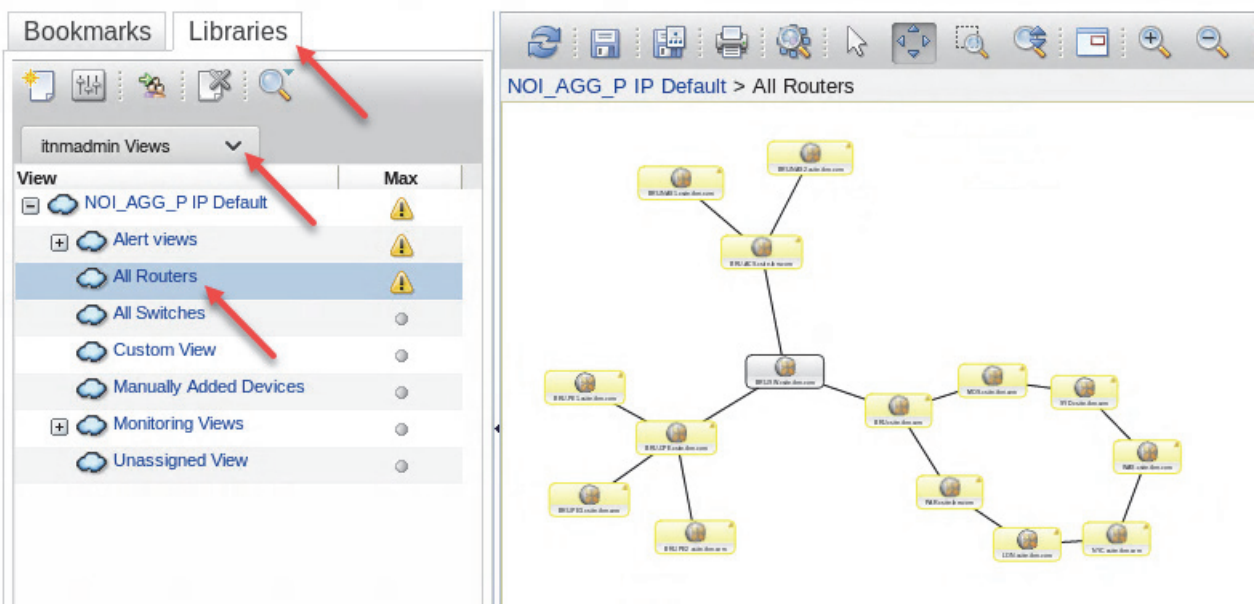


3. Verify that the simulated devices have been discovered.
   a. Click **Incident > Network Views**.

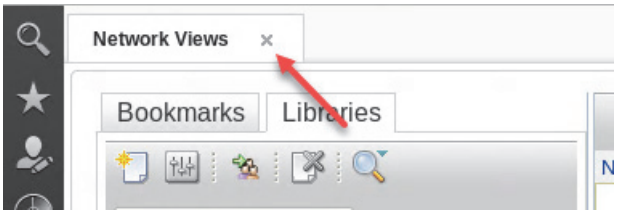


   b. Click the **Libraries** tab.
   c. Select **itnmadmin Views**.
   d. Expand **NOI_AGG_P IP Default** and click **All Routers**.

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.csite.edu and npi2.csite.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.csite.edu and click **Open Terminal**. The npi1.csite.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/
```

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

3. You are going to install Apache Ambari on npi1.csite.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.csite.edu (this is the host where you will install Apache Ambari and Hortonworks Data Platform)
- npi2.csite.edu (this is the host where you will install the Network Performance Insight components)
- host1.csite.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.csite.edu** when you are prompted for the remote host name.

```
Enter remote hostname (FQN): npi1.csite.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 npi1.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 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 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 npi1.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
```

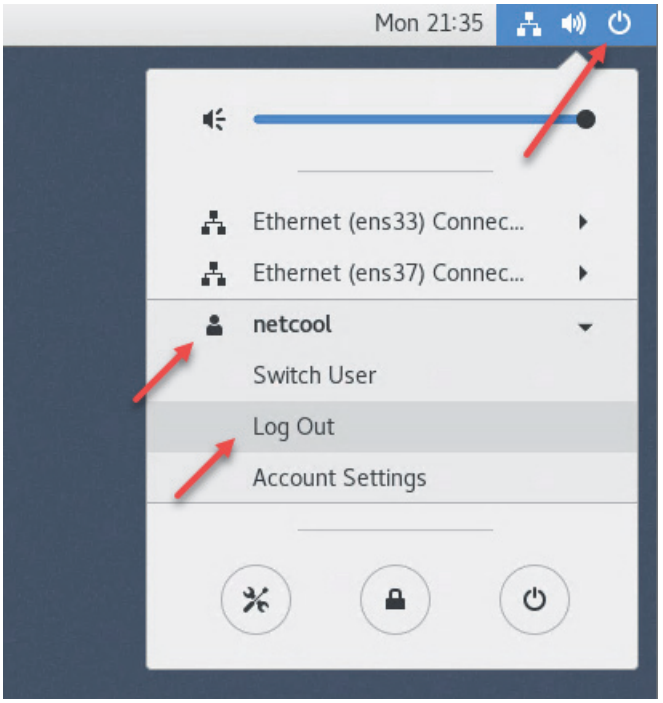
f. Type **exit** to close the terminal session as the root user.

g. Type **exit** again to close the terminal window.

h. Click the power icon at the top right of the desktop.

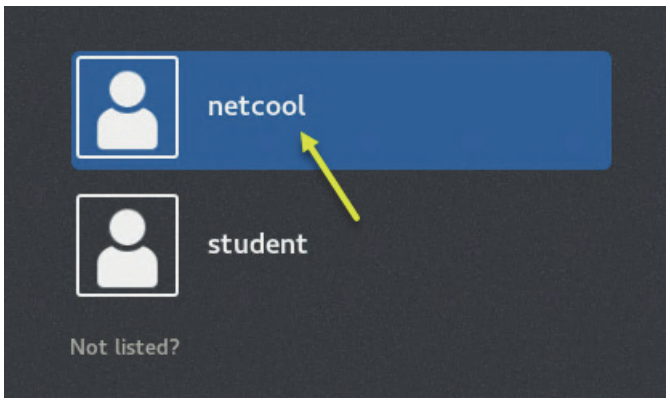
i. Expand the **netcool** user.

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 **disable**. 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 **disable**. 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.csite.edu:/tmp
Do you want to continue(y/n)
```

y

e. Enter **npi2.csite.edu** as the next host name.

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

npi2.csite.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.csite.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

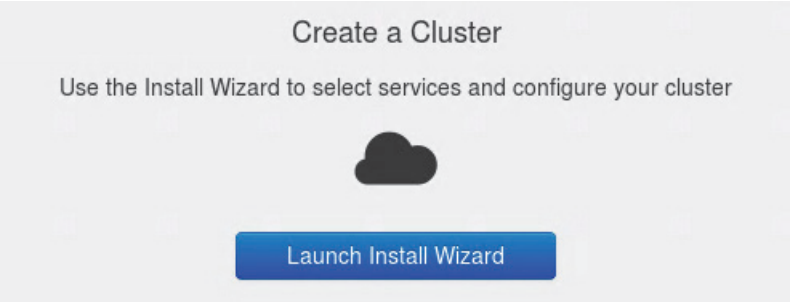
1. Start the installation wizard.
   a. Run the following command to start Firefox as the root user.

```
firefox &
```

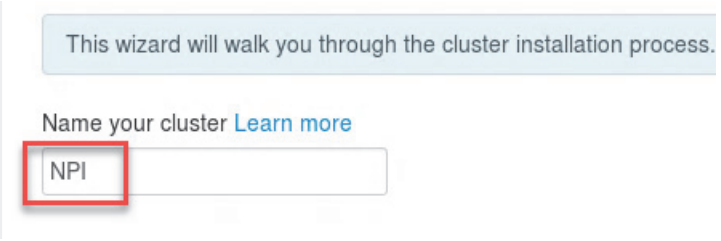
   b. Browse to the following URL. Log in with the user name **admin** and the password **admin**.

      http://npi1.csite.edu:8080

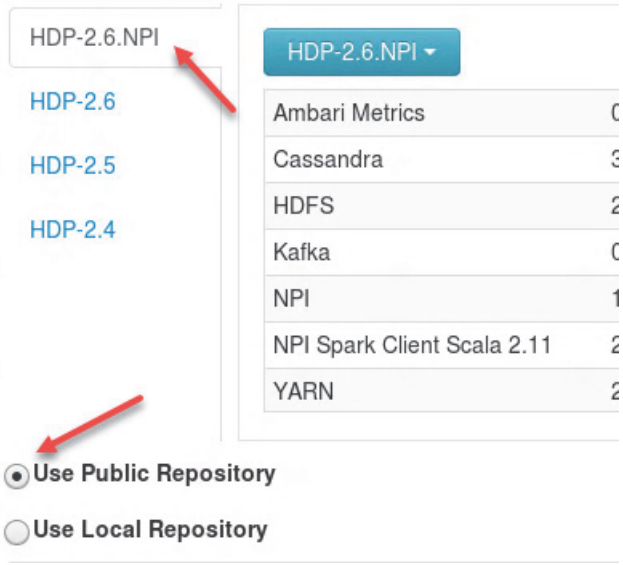
   c. Click **Launch Install Wizard**.



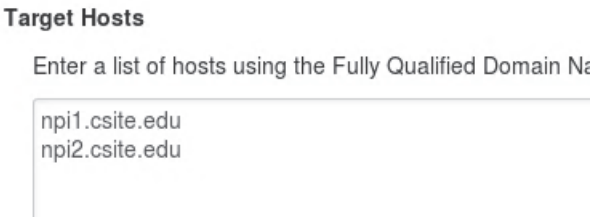
2. Register your target hosts.
   a. Enter **NPI** as the name of the cluster and click **Next**.



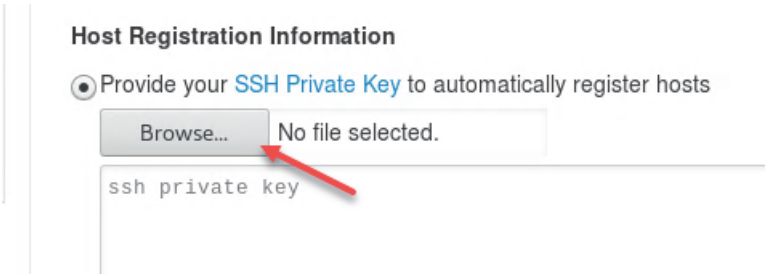
   b. Verify that **HDP-2.6.NPI** is the selected version.
   c. Verify that the **Use Public Repository** is selected.
   d. Click **Next**.



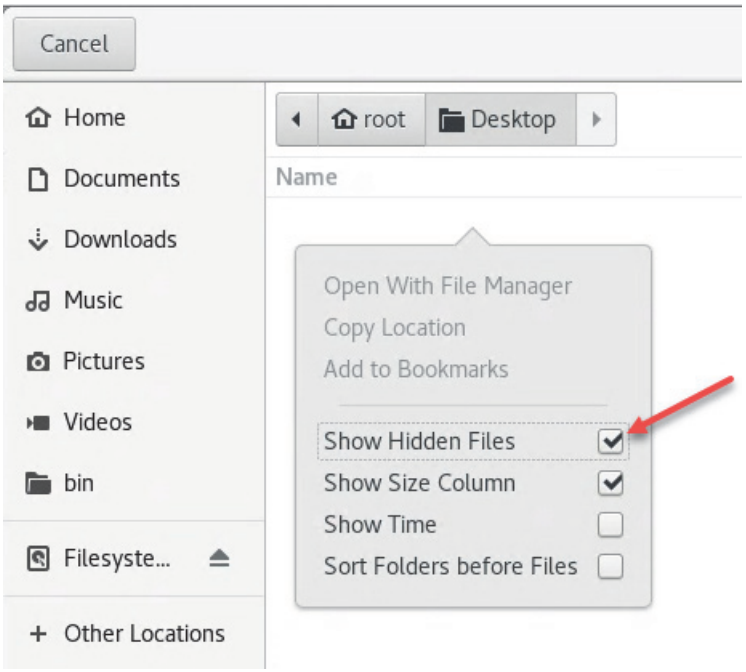
   e. Enter the following host names, one per line, into the **Target Hosts** field.
   npi1.csite.edu
   npi2.csite.edu



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

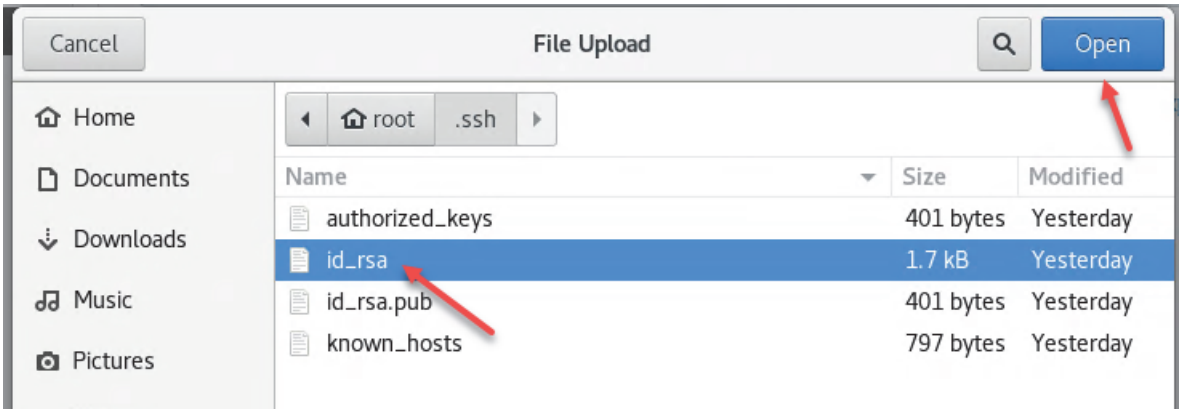


g. Right-click the file window, then select **Show Hidden Files**.

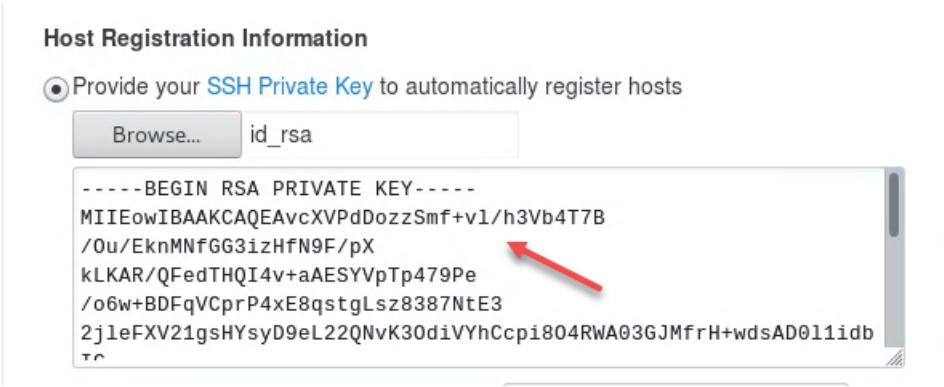


h. Browse to the **/root/.ssh** directory.

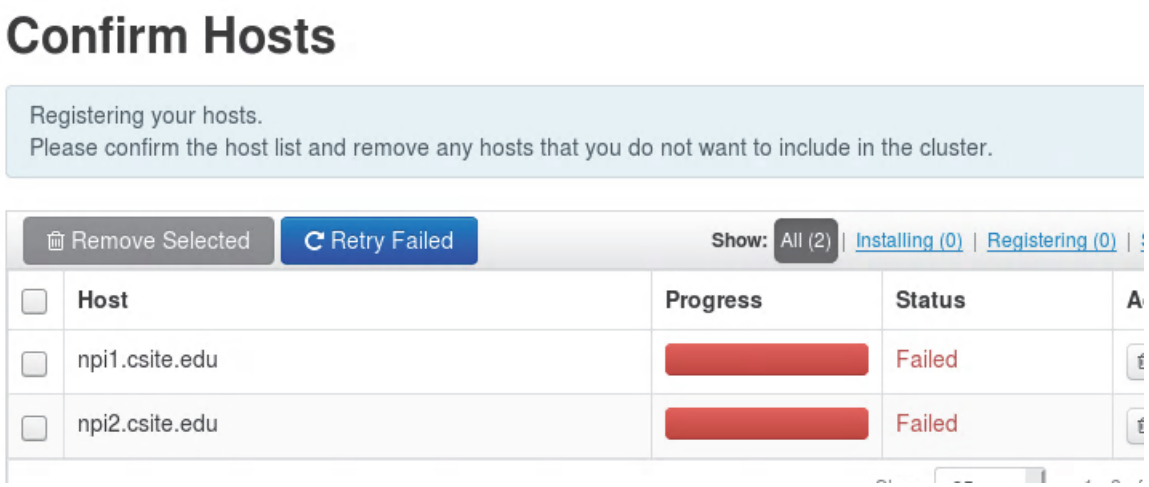
i. Select the **id_rsa** file, then click **Open**.



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.



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

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

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

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

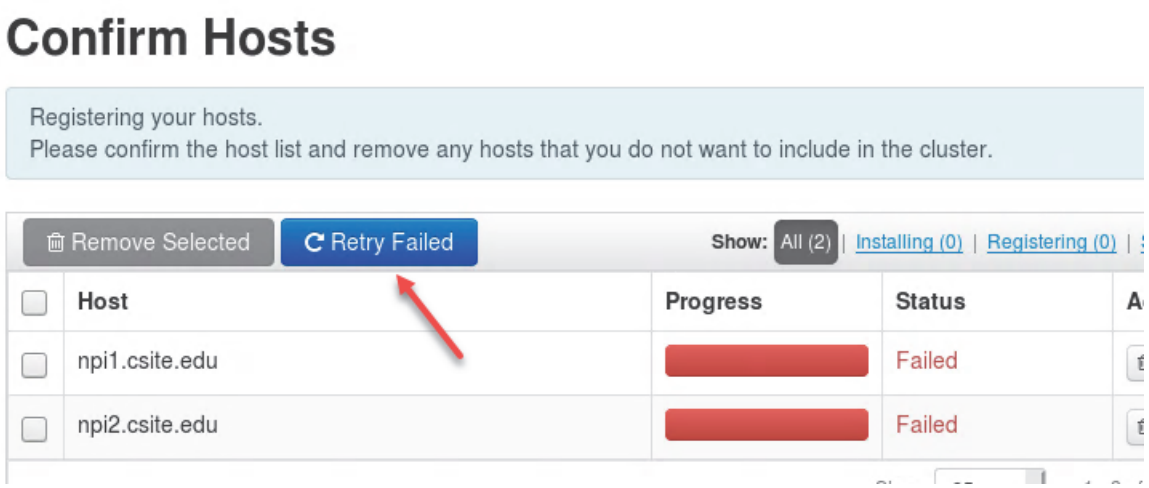
p. Find the `[security]` section of the file. Add the following line below the `[security]` line. Save and close the file when you are finished.

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

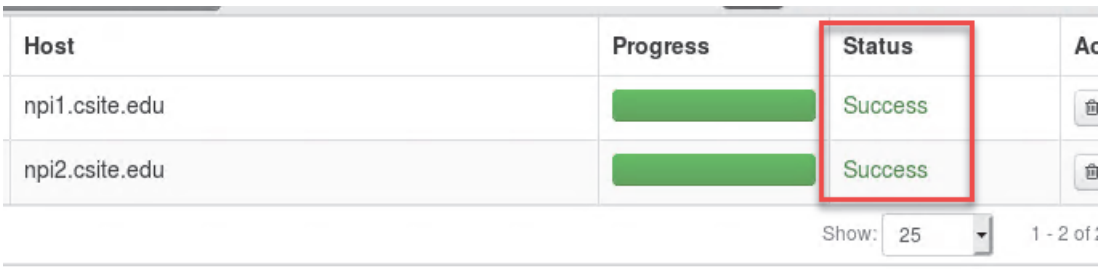
q. Type **exit** to close the connection to npi2.csite.edu.

r. Return to the Firefox browser where the installation wizard is running.

s. Click **Retry Failed**.



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

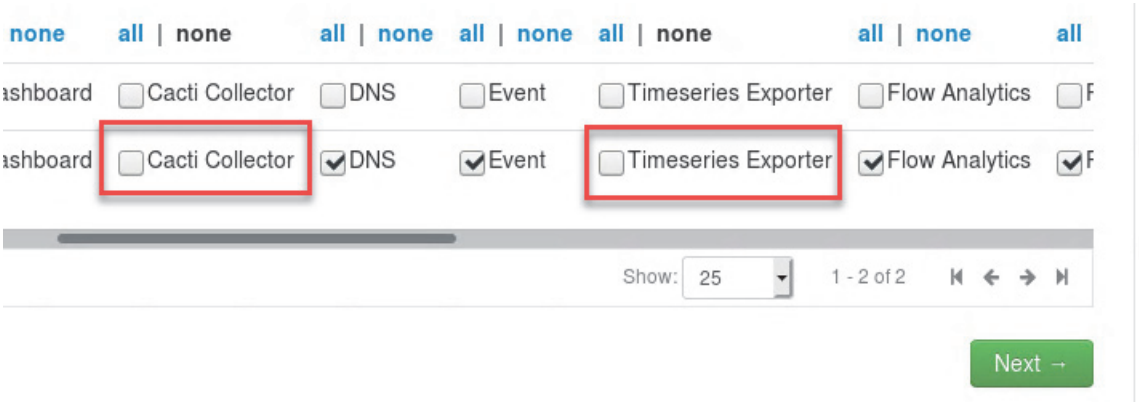


3. Configure and deploy your Network Performance Insight cluster.

a. Leave all of the default options selected on the Choose Services page, then click **Next**.

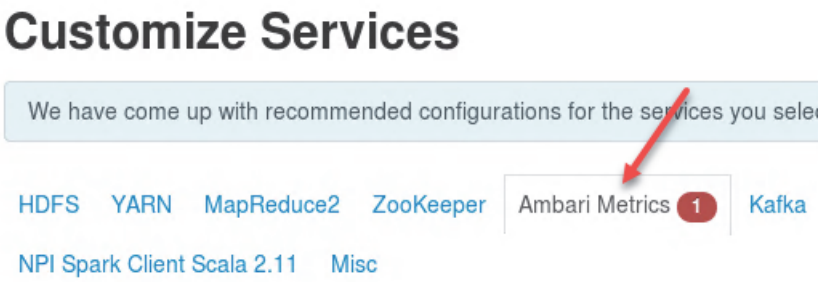
b. Leave all of the default options selected on the Assign Masters page, then click **Next**.

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

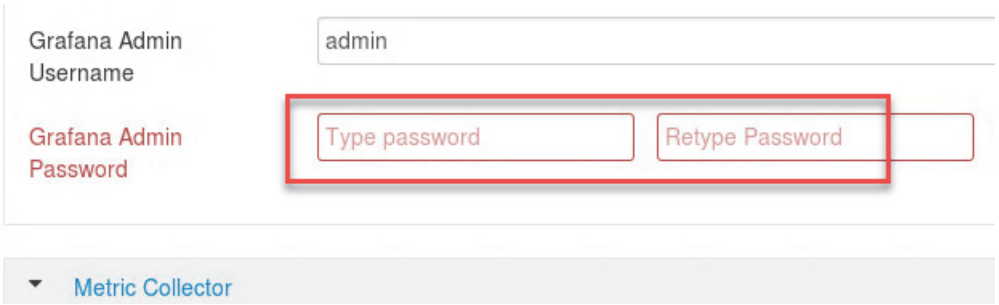


Note: Network Performance Insight can use metric data from Cacti, which is a monitoring tool. You do not have Cacti in your classroom environment, so you do not need to install the Cacti Collector. The Timeseries Exporter component sends metric data from Network Performance Insight to an external software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

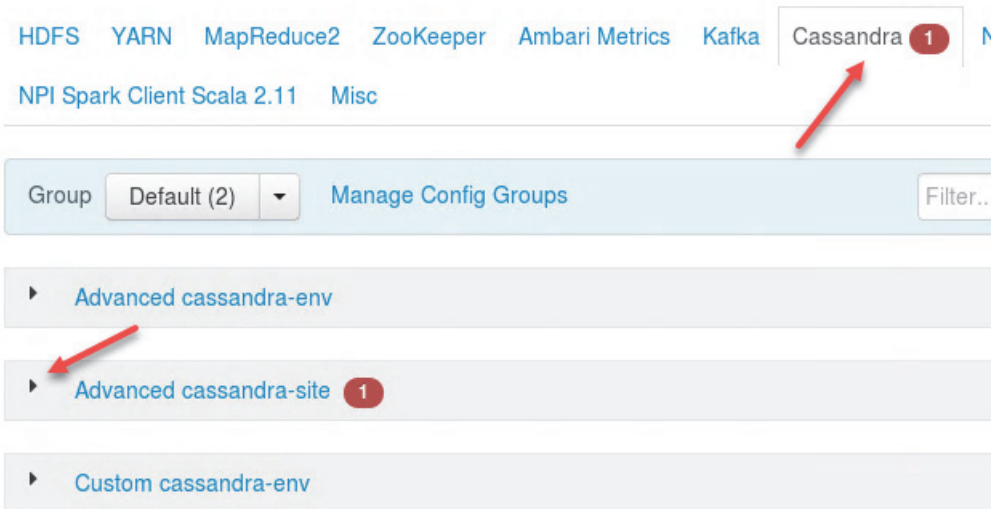
d. Click the **Ambari Metrics** tab on the Customize Services page.



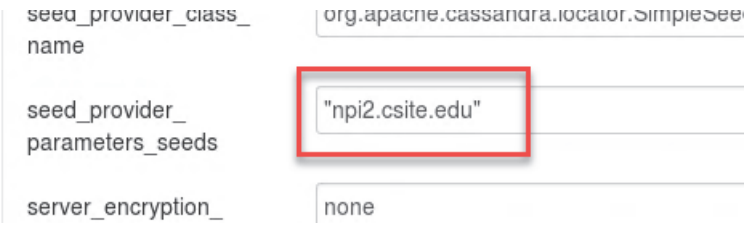
e. Enter **admin** as the Grafana admin password. Enter **admin** again to confirm.



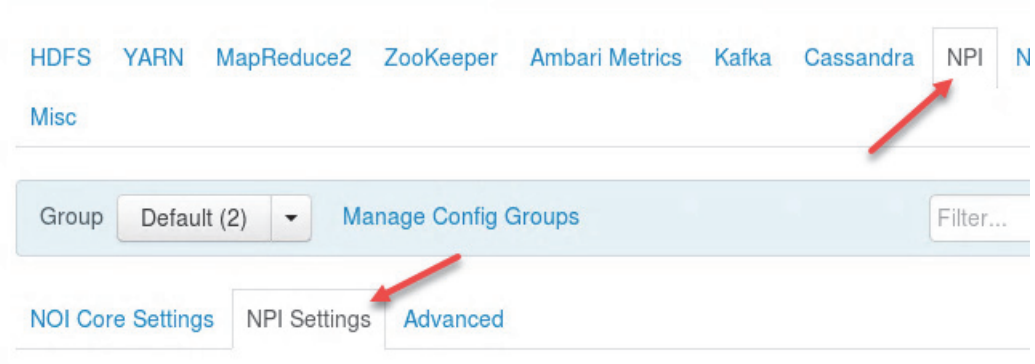
f. Click the **Cassandra** tab. Expand **Advanced cassandra-site**.



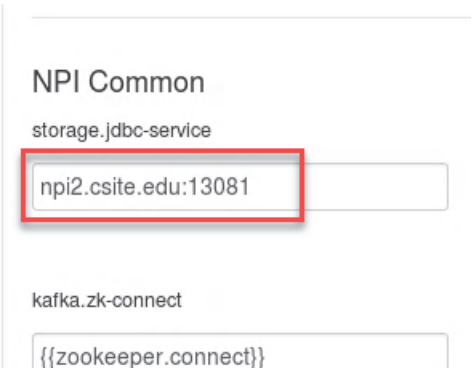
g. Scroll down and enter "`npi2.csite.edu`" in the **seed_provider_parameters_seeds** field. Be sure to include the double-quotes before and after the host name.



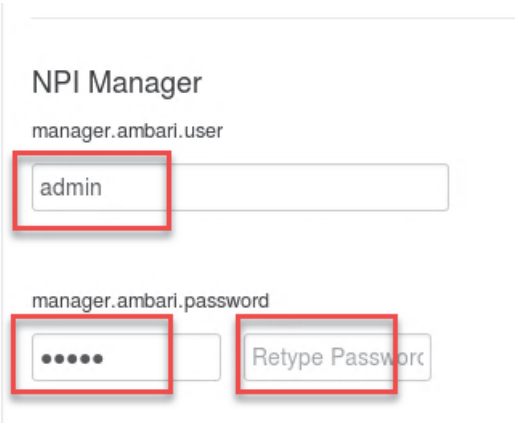
h. Click the **NPI** tab. Click the **NPI settings** tab.



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



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

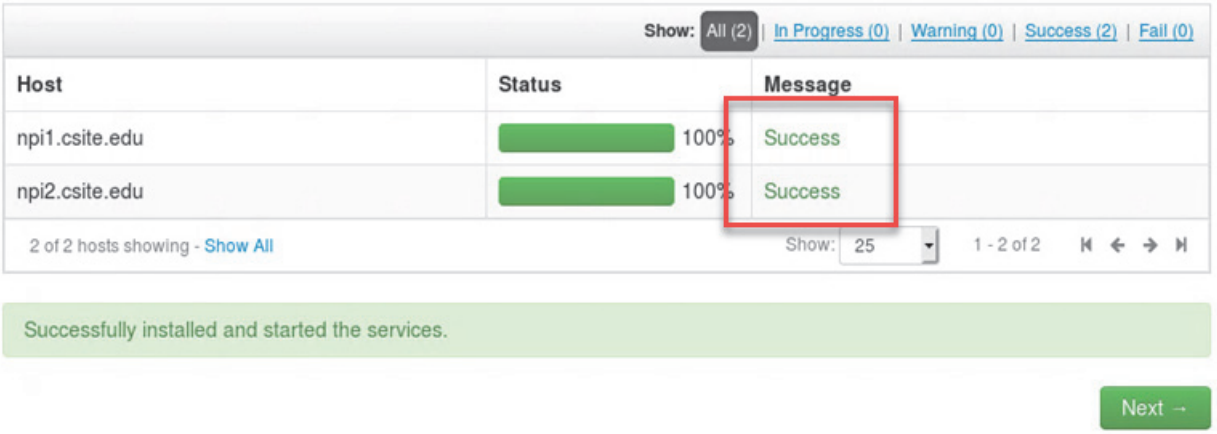


k. Scroll to the bottom of the page and click **Next**.

l. Click **Proceed Anyway** on the warning about the value of the mapreduce.reduce.memory.mb property.

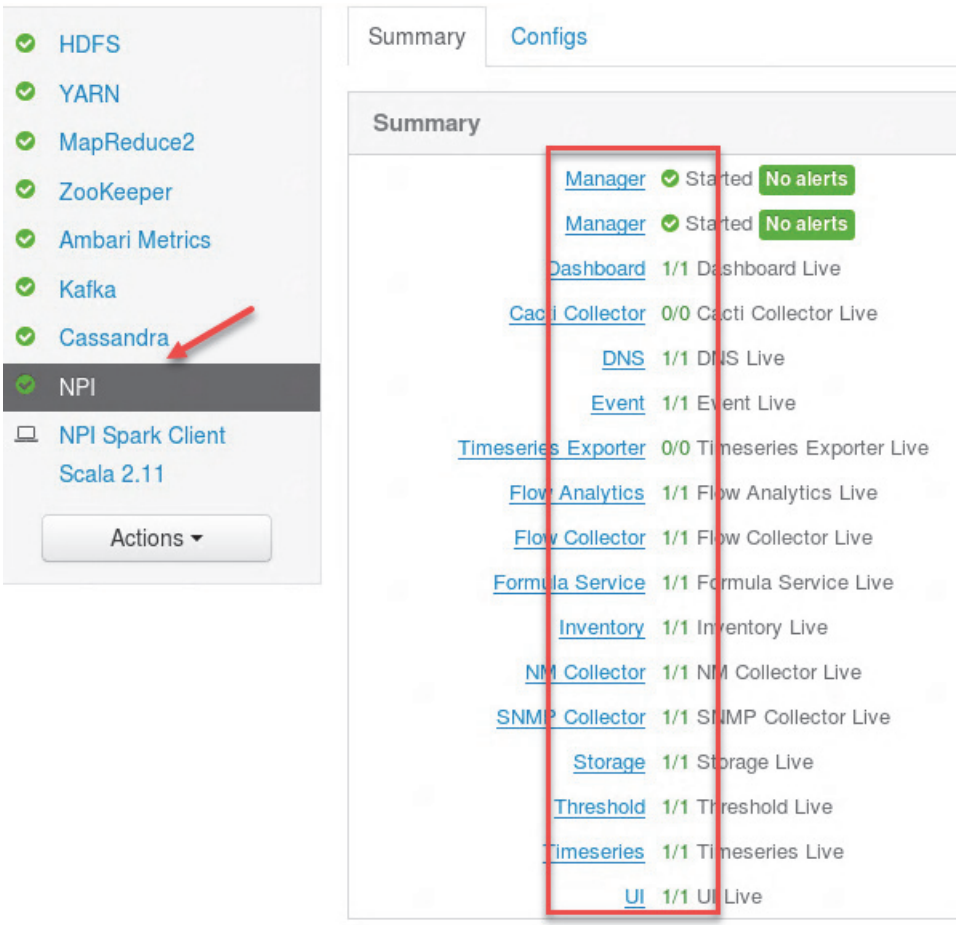
m. Click **Deploy** at the bottom of the Review page. The deployment process runs for about 35 minutes.

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



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**.



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.

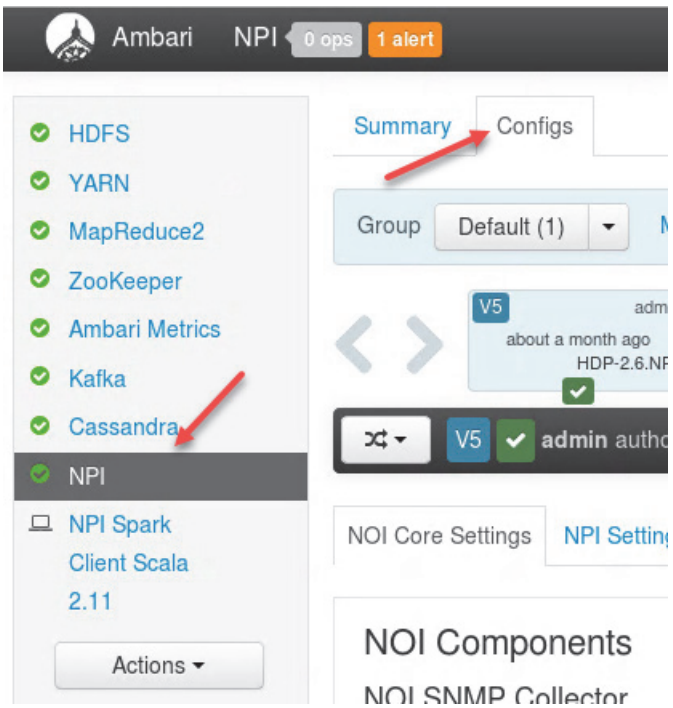
1. Open the Ambari manager page, if you do not already have it open.
   a. Run the following command to start Firefox as the root user.

   ```
   firefox &
   ```

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

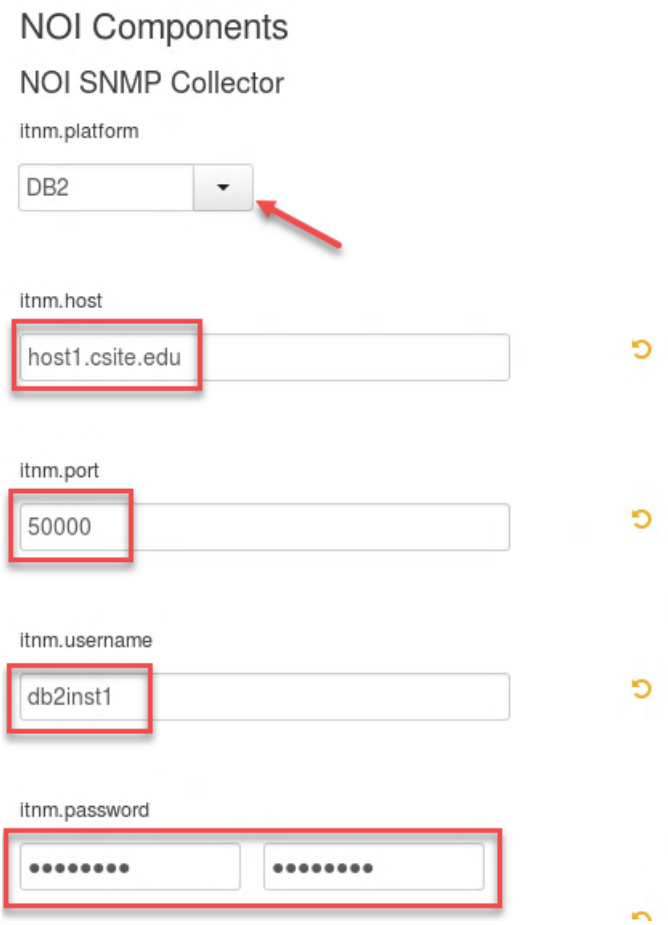
      http://npi1.csite.edu:8080

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.



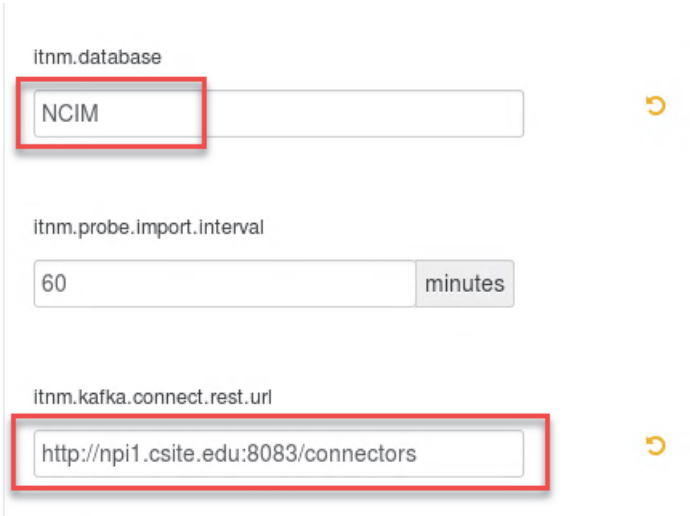
   c. Choose **DB2** as the platform.
   d. Enter **host1.csite.edu** as the value for itnm.host.
   e. Enter **50000** as the port.
   f. Enter **db2inst1** as the user name.

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



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.csite.edu:8083/connectors

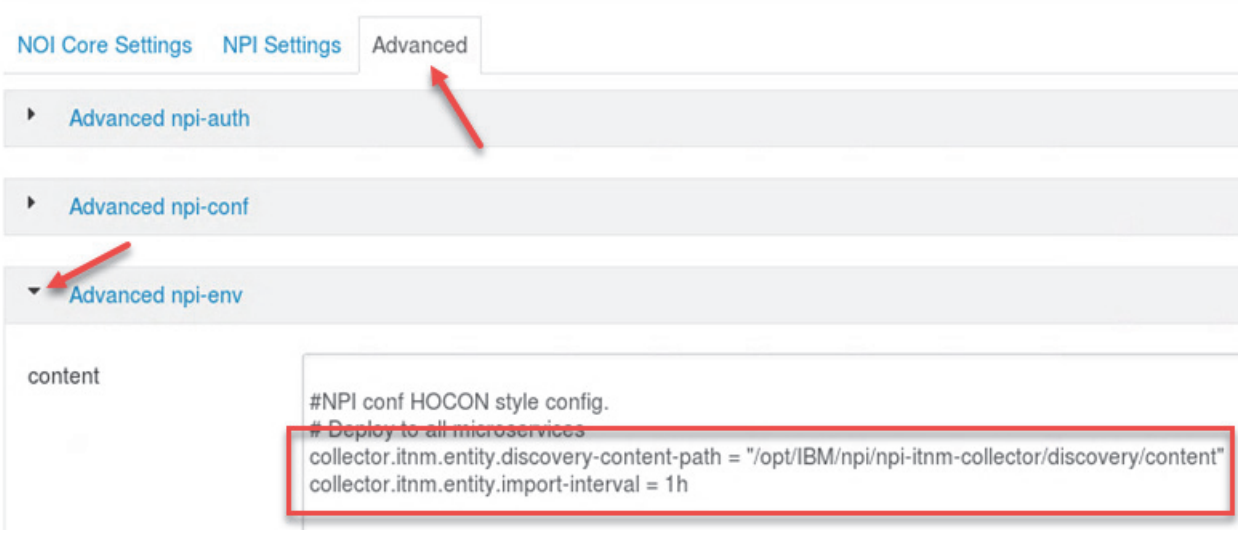


j. Click the **Advanced** tab.

k. Expand **Advanced npi-env**.

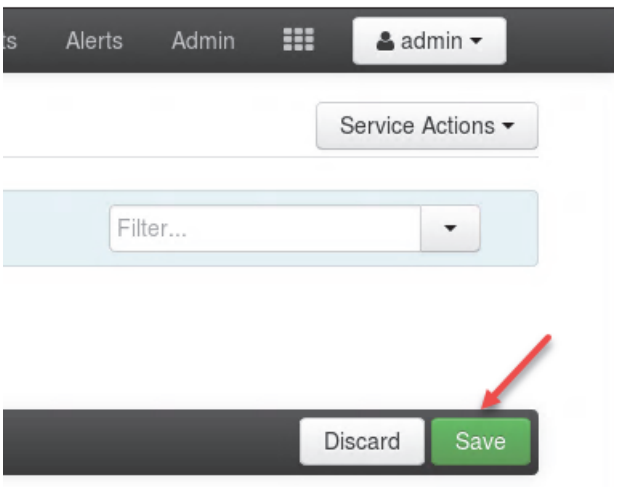
l. Add the following two lines to the **content** field.

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

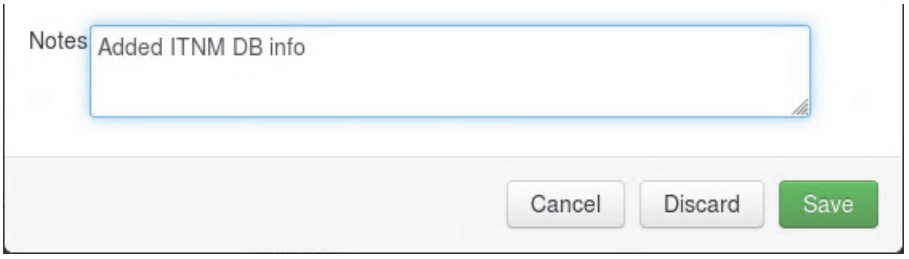


Note: The **collector.itnm.entity.import-interval** setting controls how often Network Performance Insight obtains a full list of devices from Tivoli Network Manager. You set this interval to one hour to accelerate inventory reconciliation in your lab environment. In a production environment this interval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

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

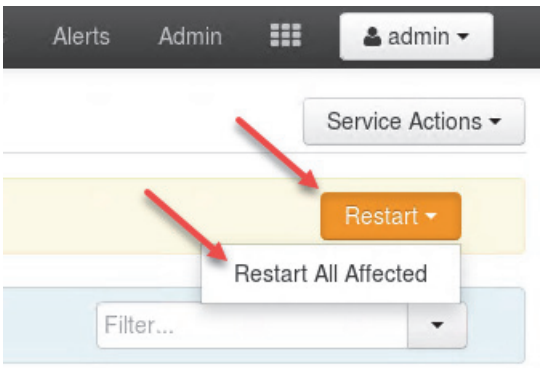


n. Enter a reason for the configuration change, and click **Save**.



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.

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

b. Connect to npi2.csite.edu.

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

c. Change to the correct directory.

```
cd /opt/IBM/npi/npi-itnm-collector/
```

d. Create the resources/itnm/security/keys sub-directory.

```
mkdir -p resources/itnm/security/keys
```

e. Run the following command to copy the conf.key file to the correct directory on npi2.csite.edu. Run the entire command on one line.

```
scp netcool@host1.csite.edu:/opt/IBM/tivoli/netcool/etc/security/keys/conf.key
/opt/IBM/npi/npi-itnm-collector/resources/itnm/security/keys
```

f. 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.csite.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 not longer violated. In this exercise, you configure the Standard Input Probe that is installed with Network Performance Insight.

1. Add the alias `omnihost` for the host where Netcool/OMNIbus is running. Do this in the hosts file for npi1.csite.edu and npi2.csite.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.

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

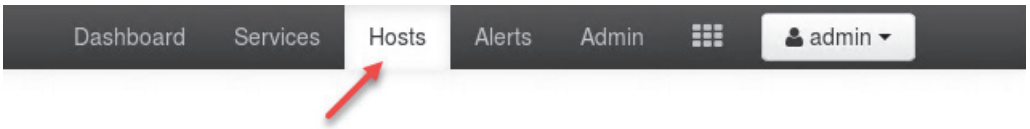
f. Stay connected to npi2.csite.edu. You use the connection later in this exercise.

4. Restart the Event service.

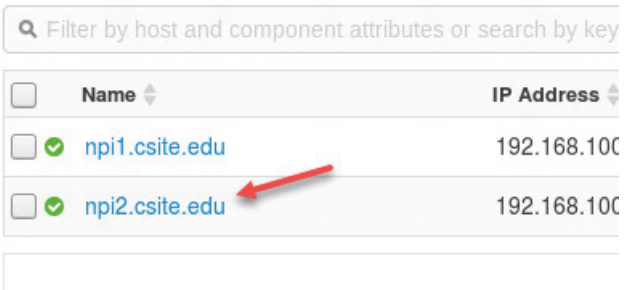
a. Return to the Ambari manager page. If you need to open the manager page, open a Firefox browser as root and use the following URL with the user name **admin** and the password **admin**.

http://npi1.csite.edu:8080

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



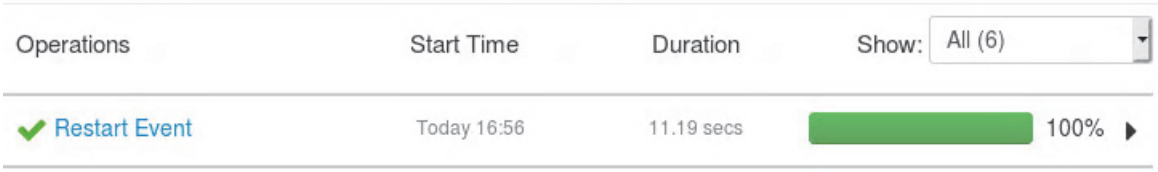
c. Click **npi2.csite.edu**.



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.



5. Verify that the probe is running.

a. Return to the terminal window where you are connected to npi2.csite.edu.

b. 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
```

c. 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
```

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

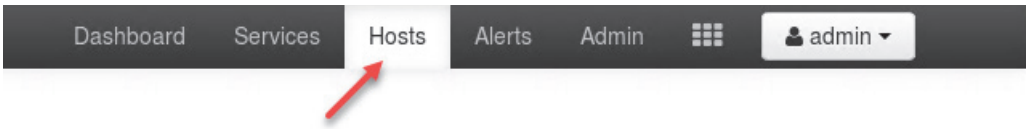
Exercise 3 Integration with Dashboard Application Services Hub

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

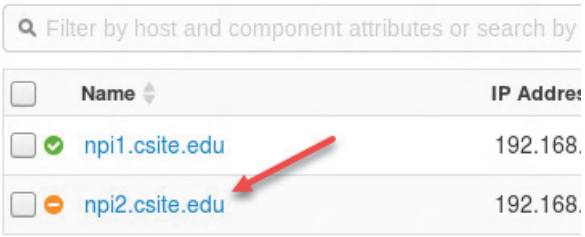
1. Ensure that the Network Performance Insight Dashboard service is running. If it is not running, start it.
   a. Return to the Ambari manager page. If you need to open the manager page, open a Firefox browser as root and use the following URL with the user name **admin** and the password **admin**.

      http://npi1.csite.edu:8080

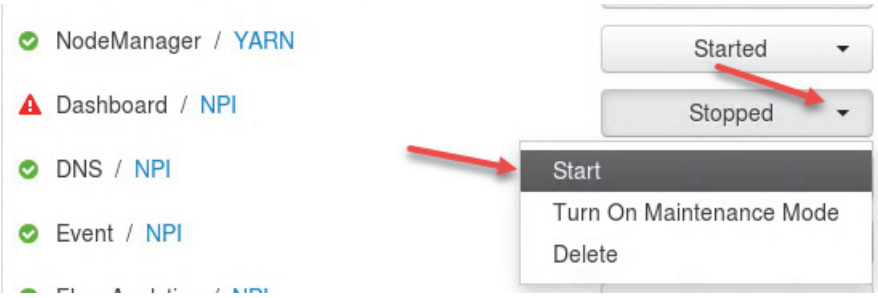
   b. Click the **Hosts** tab close to the top of the page.



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



   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.

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.

   a. Change to the target directory.

   ```
   cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
   ```

   b. Open the custom.cfg file in a text editor.

   ```
   vi custom.cfg
   ```

   c. Find the following three properties and change their values to match the following example. Do not change any other property.

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

3. Generate the SSL certificate and keystore files, then verify that they were created successfully.
   a. 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
```

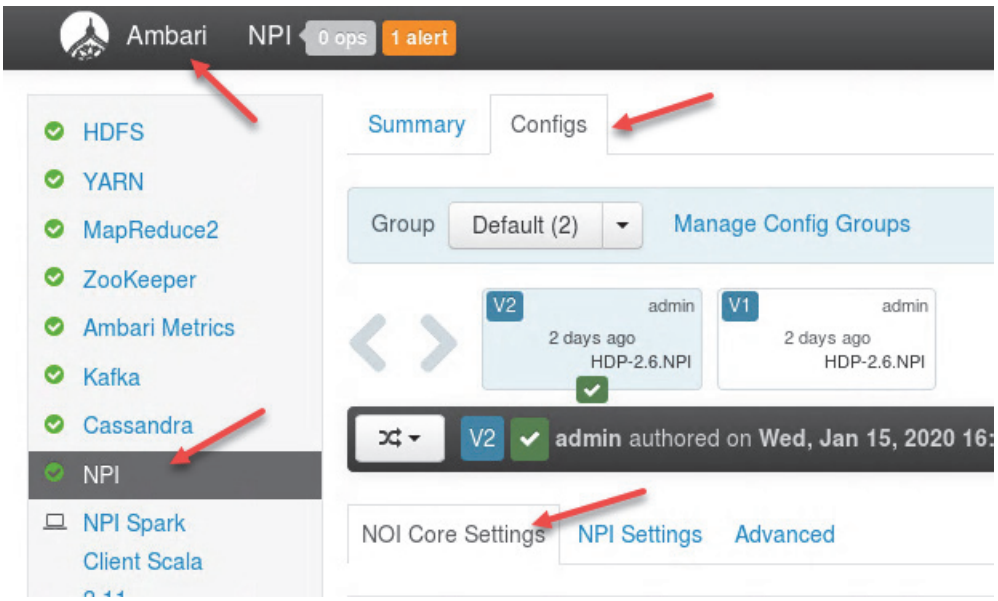
c. Run the following command to check the npiDashIntegration.log file. Verify that there are no warnings or errors in the log file.

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

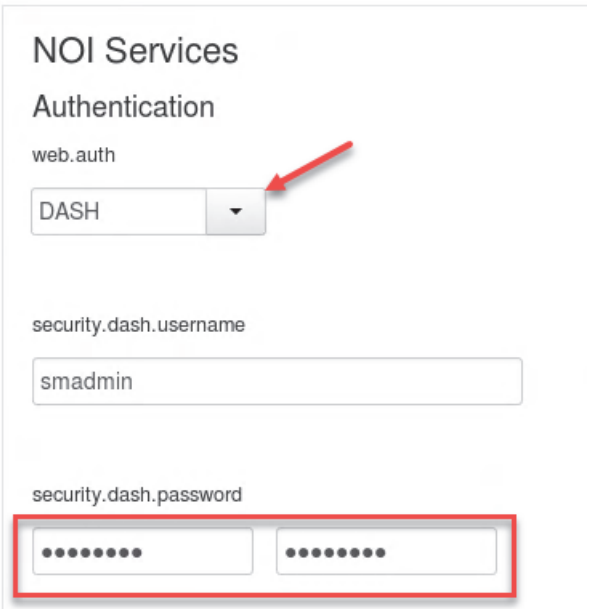
d. Run the following command to check the enableDash.log file on the host where DASH is running. Verify that there are no warnings or errors in the log file.

```
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**.



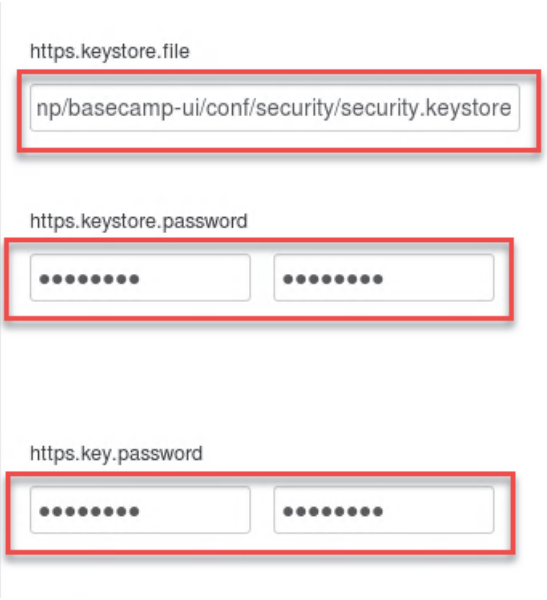
   c. Select **DASH** as the value for web.auth.
   d. Enter **object00** as the DASH password. Enter **object00** again to confirm.



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

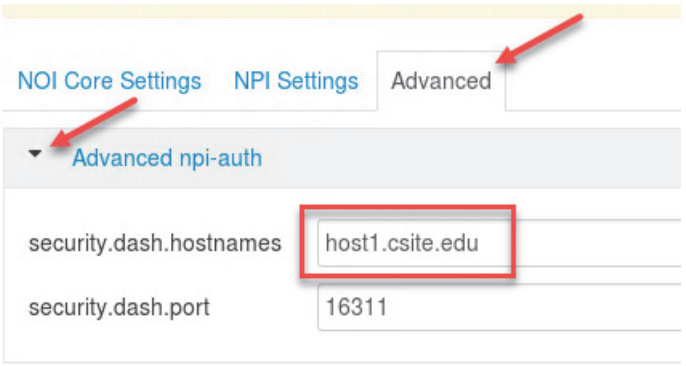
f. Enter **changeit** as the keystore password. Enter **changeit** again to confirm.

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



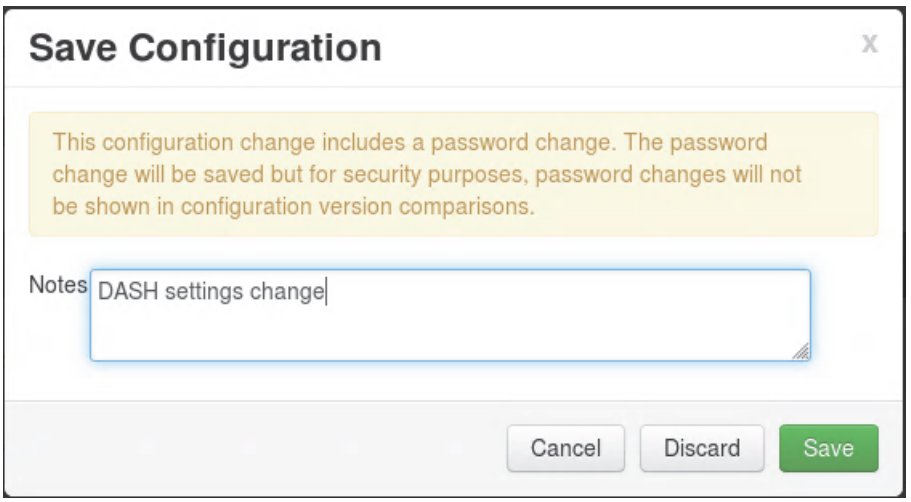
h. Click the **Advanced** tab. Expand **Advanced npi-auth**.

i. Enter **host1.csite.edu** as the DASH host name.



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.

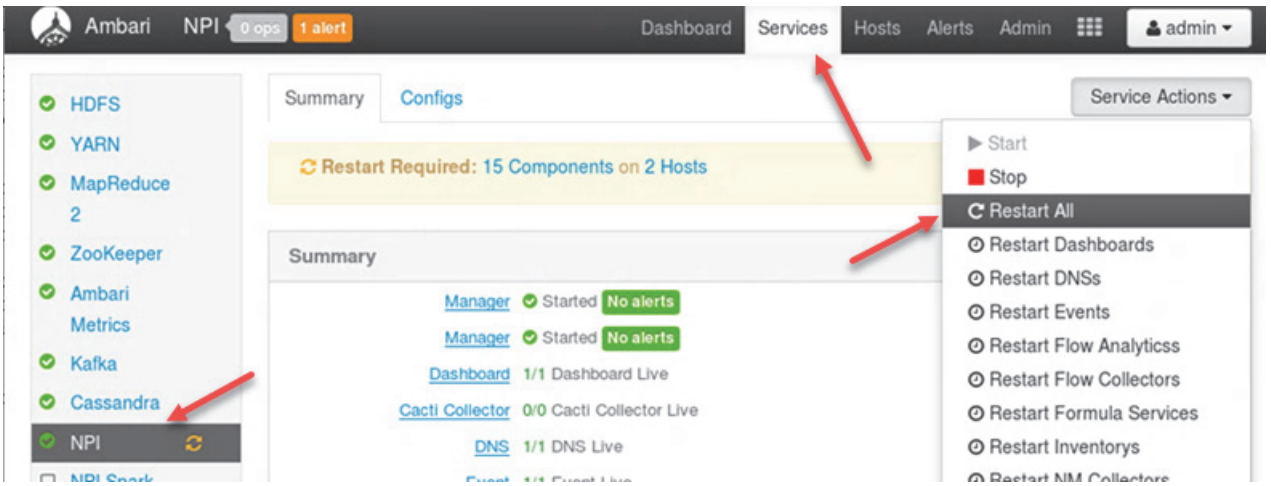
m. Click **OK** to confirm.

6. Restart the **Network Performance Insight** services.

a. Click the **Services** tab at the top of the page.

b. Click **NPI** in the menu on the left of the page.

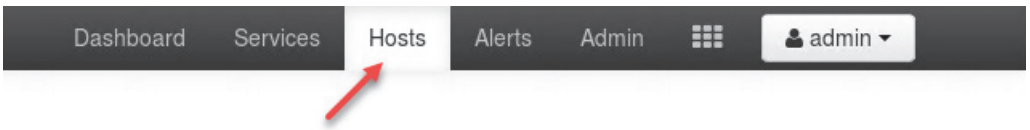
c. Click **Service Actions > Restart All**.



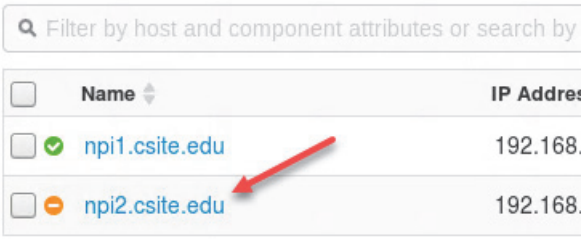
d. Click **Confirm Restart All**.

e. When the services are finished restarting, click **OK**.

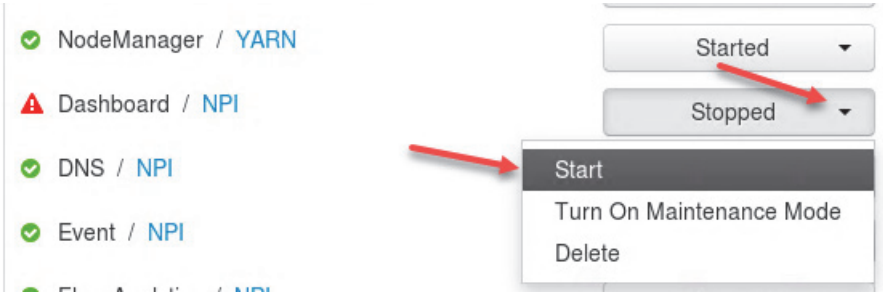
f. Start the Dashboard service manually. Click the **Hosts** tab close to the top of the page.



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



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.

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.csite.edu. You use the connection in the next step.

8. On npi2.csite.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.

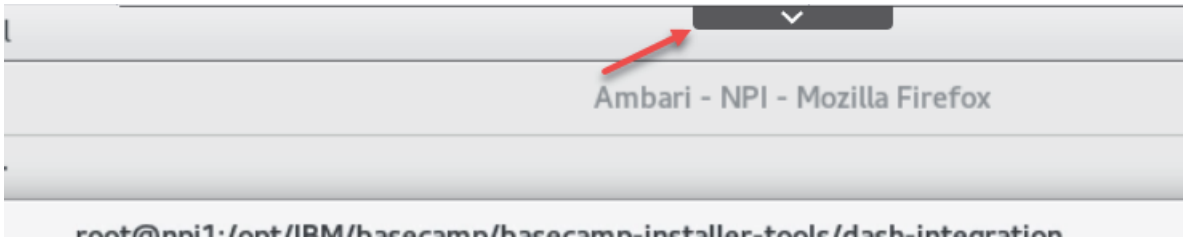
```
keytool -keystore
/opt/IBM/basecamp/basecamp-jre/java-1.8.0-openjdk.x86_64/jre/lib/security/cacer
ts -storepass changeit -list -alias WebSphereCACert

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.

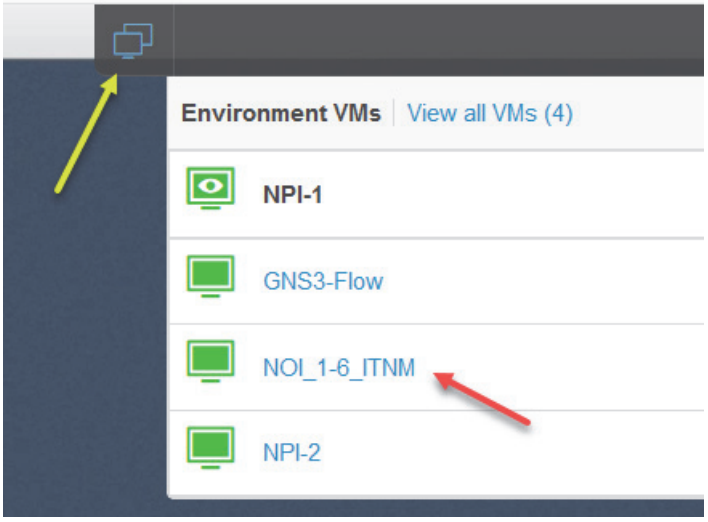
```
keytool -keystore /opt/IBM/basecamp/basecamp-ui/conf/security/security.keystore
-storepass changeit -list

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.csite.edu.

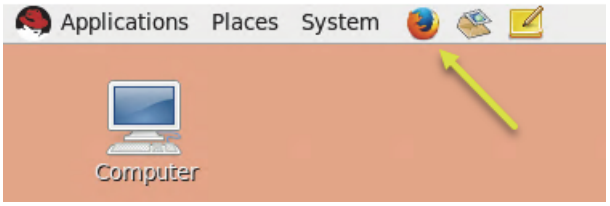
9. Configure SSL in WebSphere Application Server.
   a. Perform the next steps on the host where WebSphere Application Server is running. Change your lab environment to the desktop of host1.csite.edu, which is labeled **NOI_1-6_ITNM.** Click the tab at the top of the window to view the lab environment options.



   b. Click the icon for environment VMs. Click **NOI_1-6_ITNM**.



   c. Open a Firefox browser.

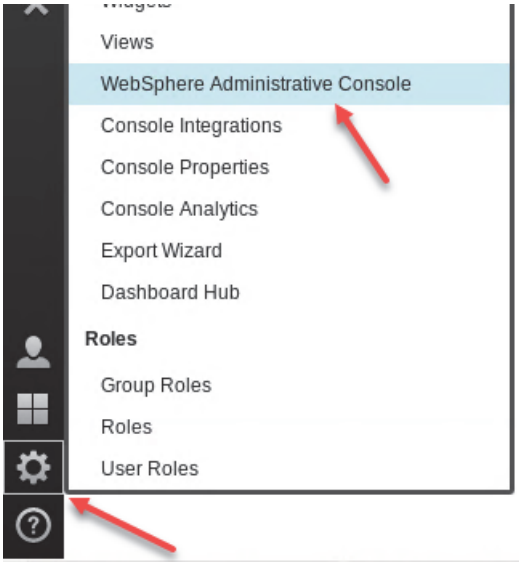


   d. Go to the following URL:

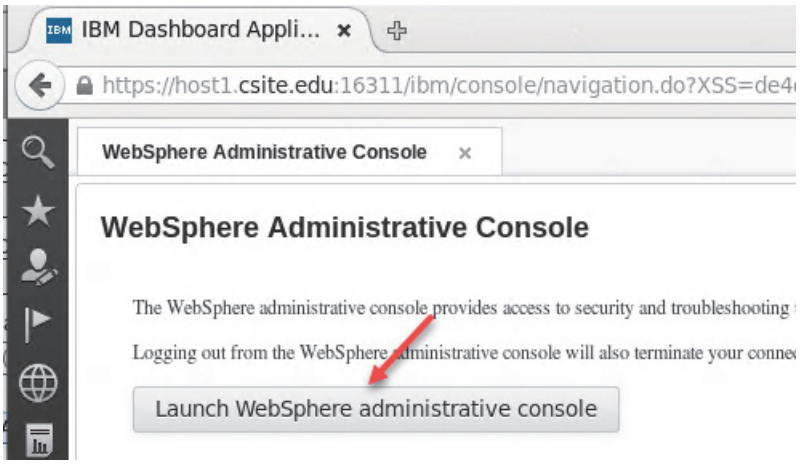
      https://host1.csite.edu:16311/ibm/console/logon.jsp

   e. Log in with the user name **smadmin** and the password **object00**.

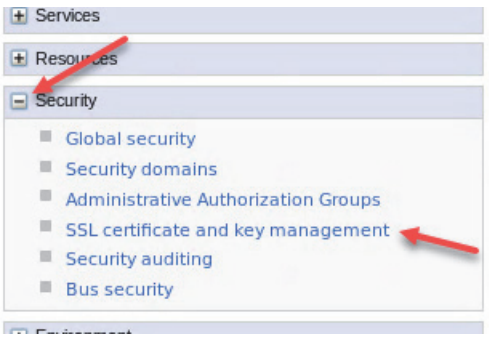
f. Click **Console Settings > WebSphere Administrative Console**.



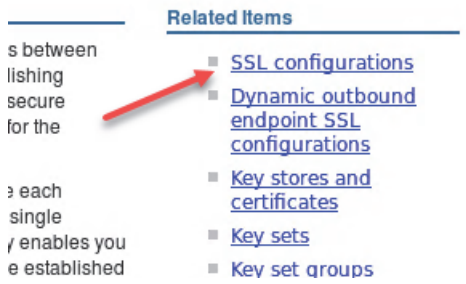
g. Click the **Launch WebSphere administrative console** button.



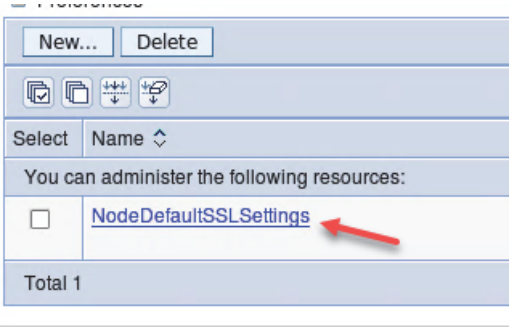
h. Expand **Security**. Click **SSL certificate and key management**.



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



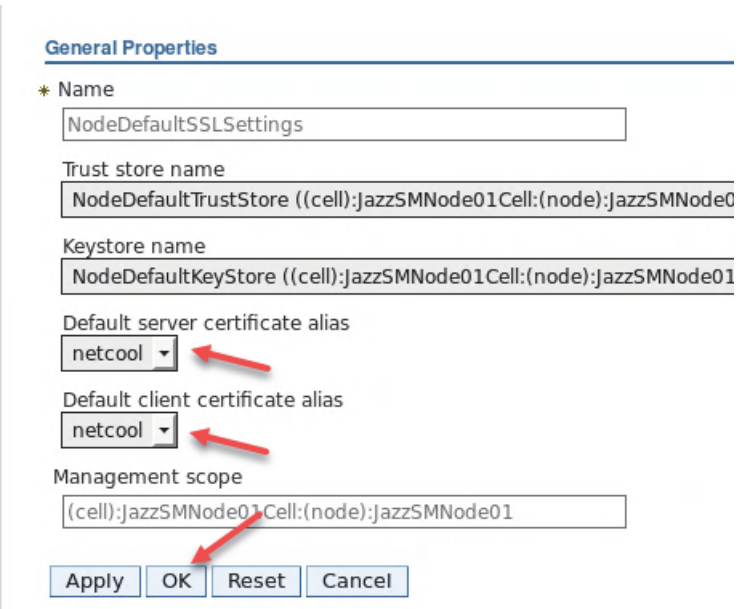
j. Click **NodeDefaultSSLSettings**.



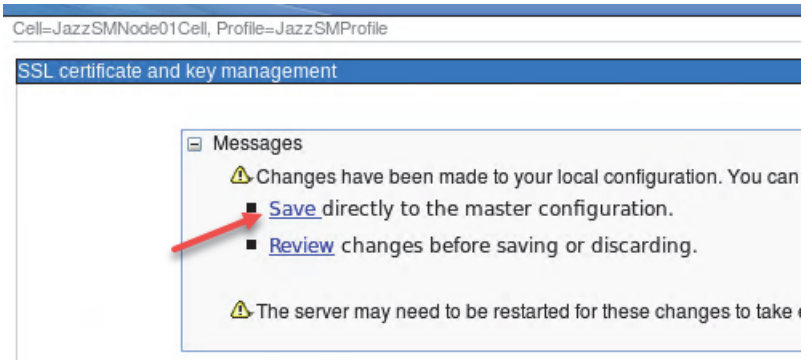
k. Select **netcool** as the Default server certificate alias.

l. Select **netcool** as the Default client certificate alias.

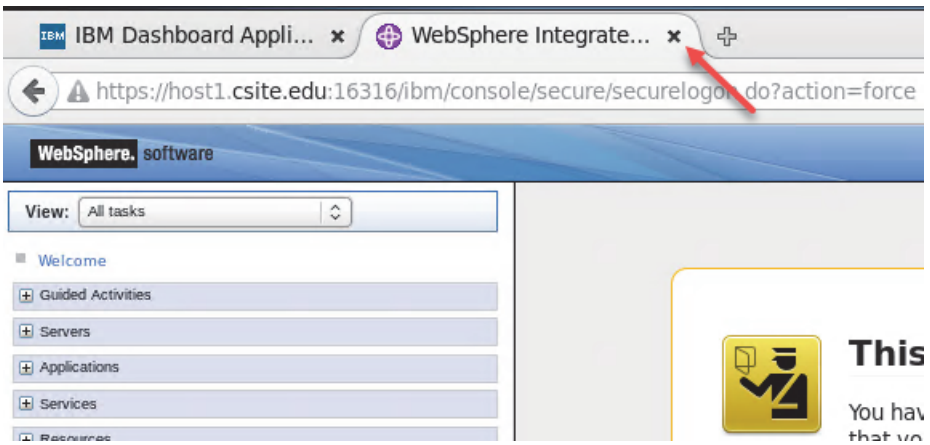
m. Click **OK**.



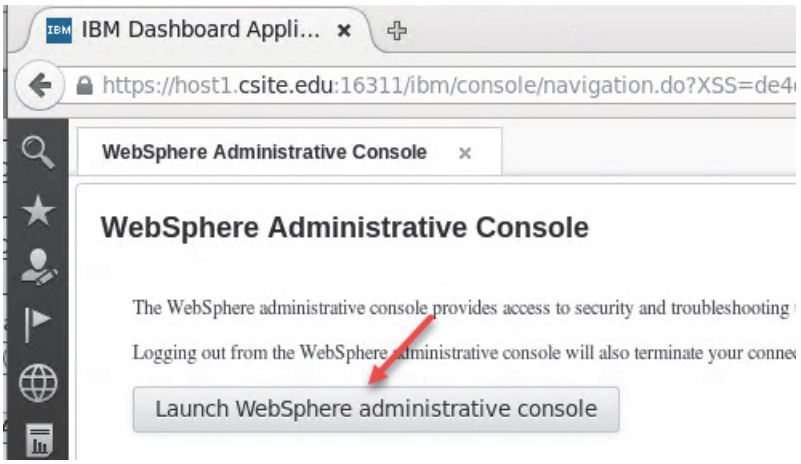
n. Click **Save** at the top of the page.



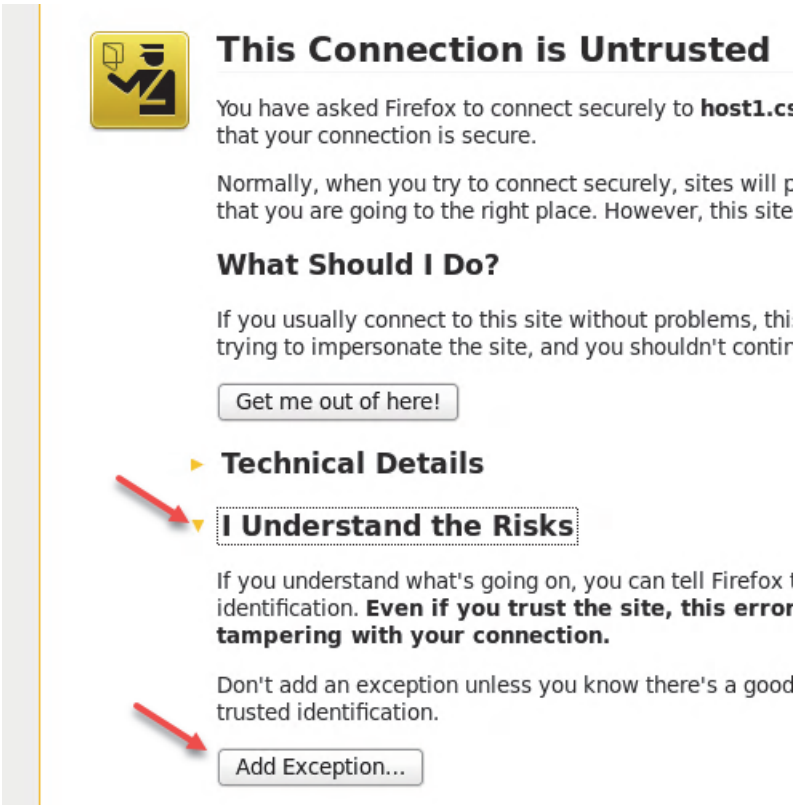
o. At this point, you might see warnings about an invalid certificate. Close the WebSphere Integrated Console tab.



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

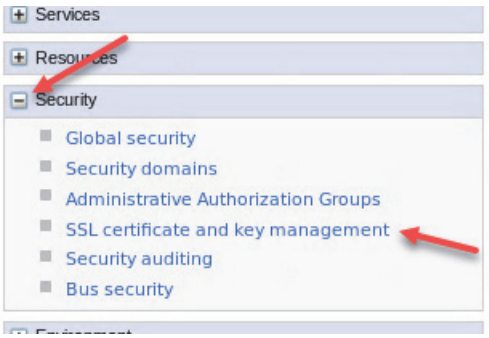


q. Expand **I Understand the Risks**. Click **Add Exception**.

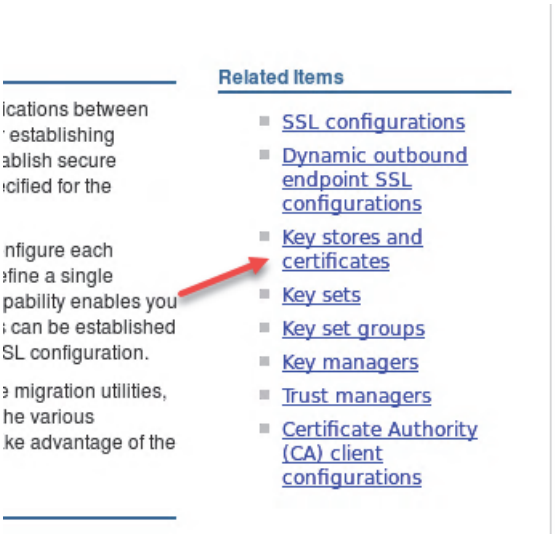


r. Click **Confirm Security Exception**.

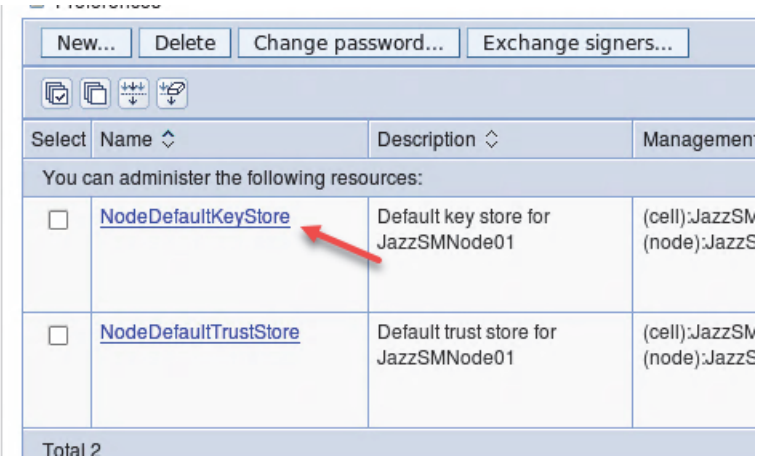
10. Verify that the new certificates are available.
    a. Expand **Security**. Click **SSL certificate and key management**.



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

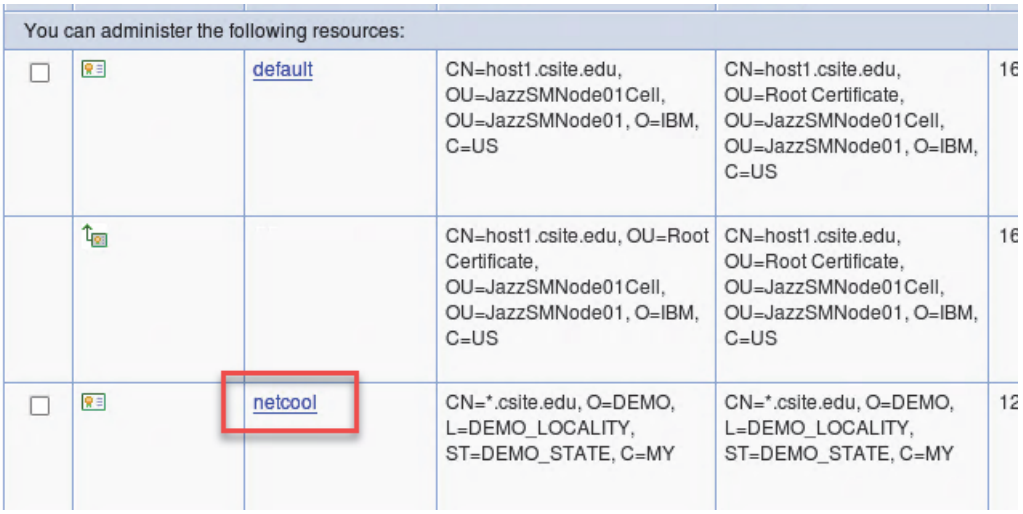


c. Click **NodeDefaultKeyStore**.



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

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

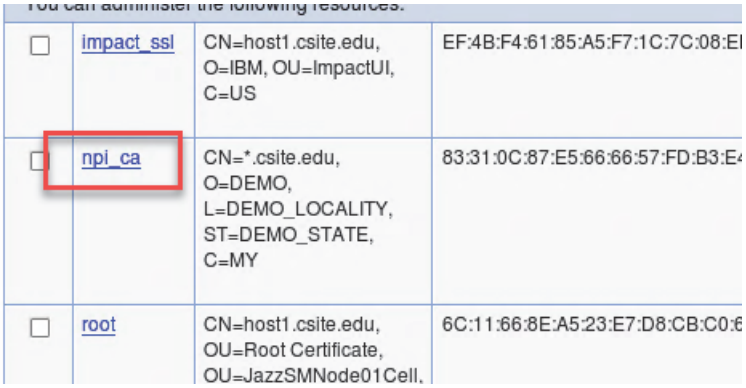


f. Click the **Key stores and certificates** link at the top of the page.

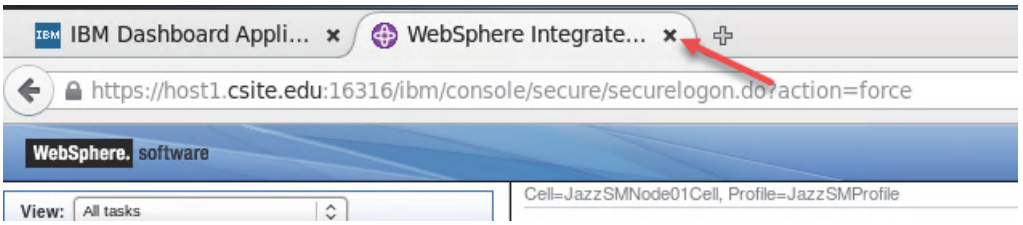
g. Click **NodeDefaultTrustStore**.

h. Click **Signer certificates**.

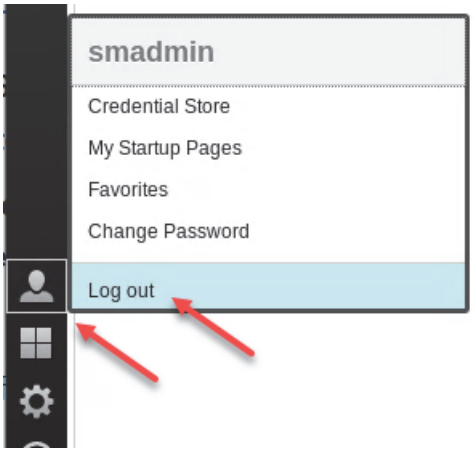
i. Verify that the **npi_ca** certificate is present.



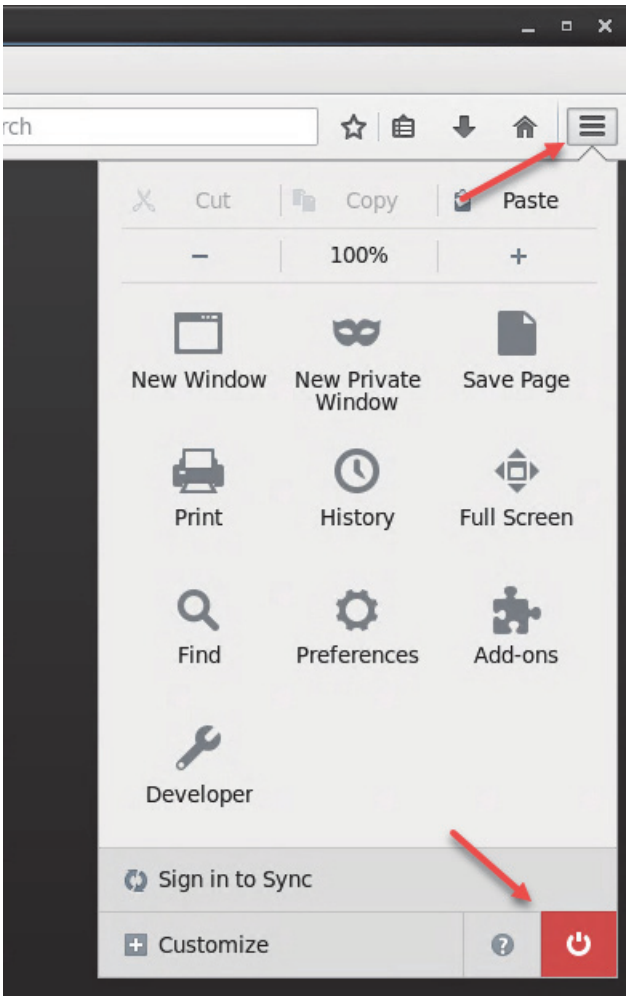
j. Close the WebSphere Integrated Console tab.



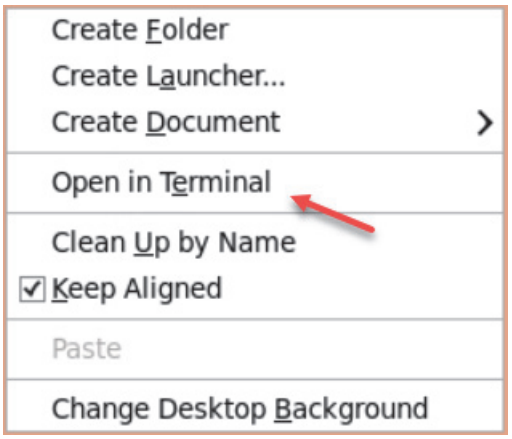
k. Click the user icon, then click **Log out**.



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
```

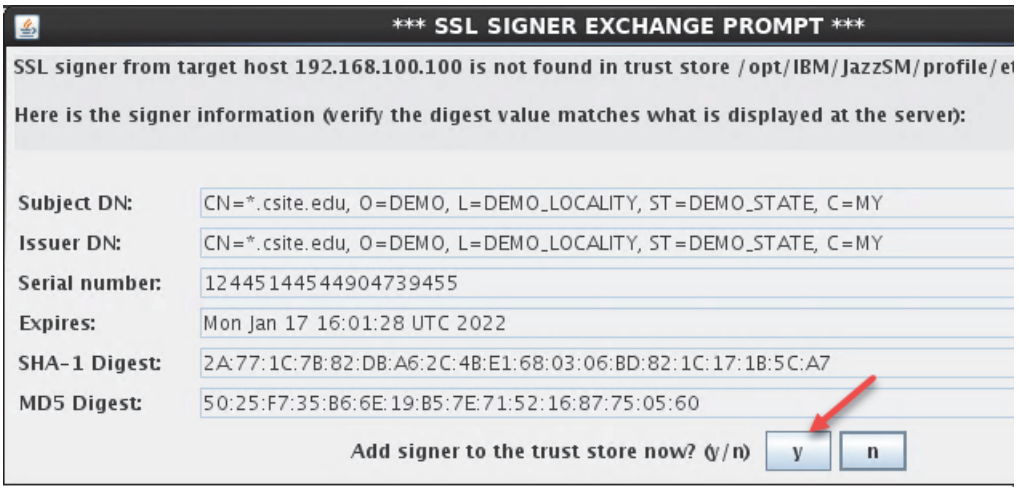
    c. Change to the target directory.

```
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.

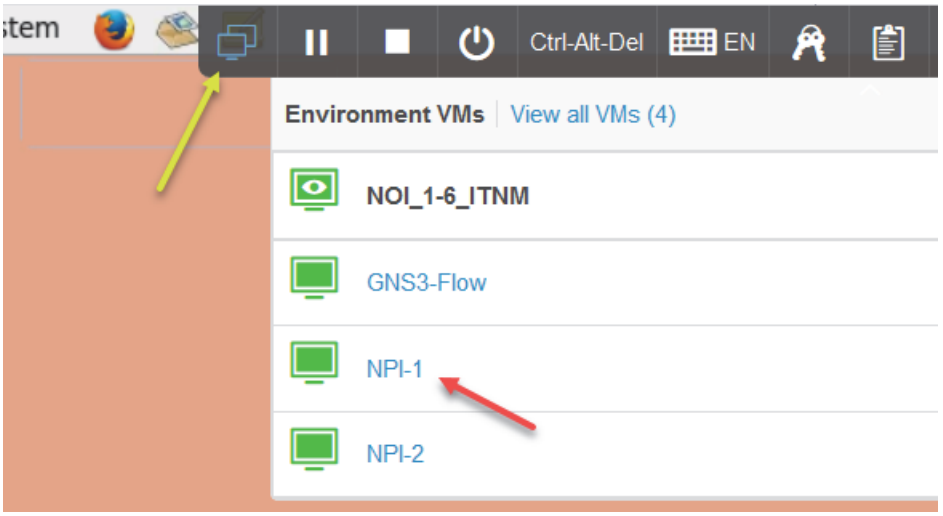


    f. Wait until the service is stopped. Run the following command to start WebSphere Application Server, Jazz for Service Management, and DASH.

```
./jazz start
```

12. Return your lab environment to the desktop of 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**.



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.

    a. Return to the terminal window on npi1.csite.edu where you are the root user.
    b. Run the following command to change to the target directory.

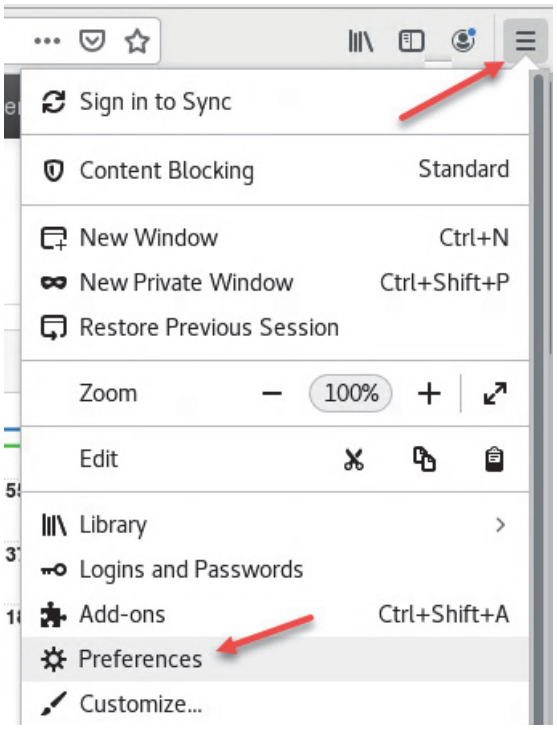
```
cd /opt/IBM/basecamp/basecamp-installer-tools/dash-integration
```

    c. Run the following command to copy the ca.crt file to a directory that the netcool user can access.

```
cp ca.crt /home/netcool/
```

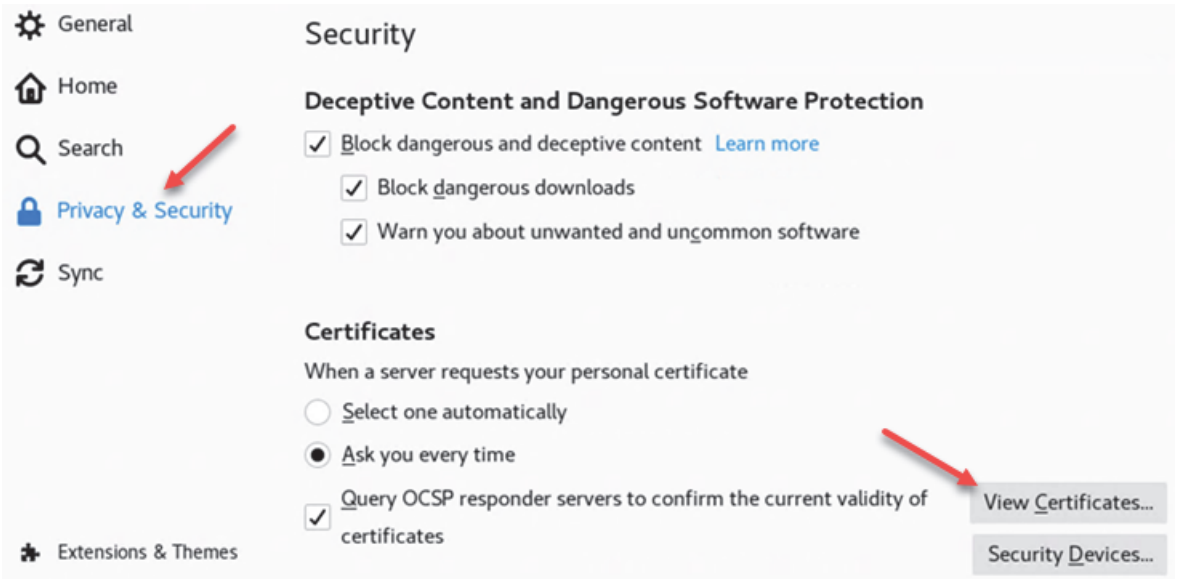
    d. Open a Firefox browser if you do not already have one open.

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

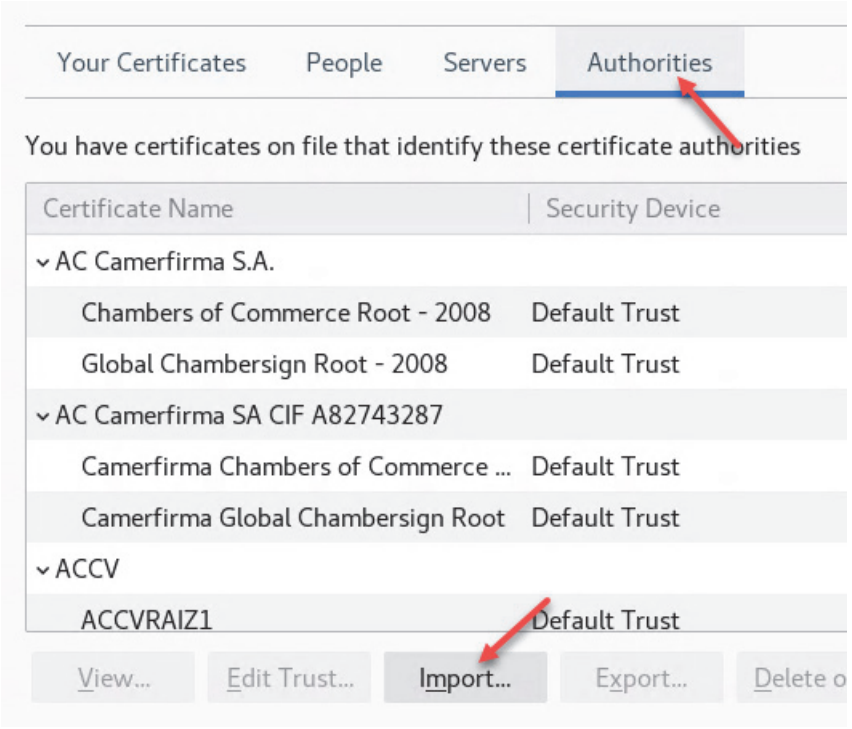


f. Click **Privacy and Security**.

g. Scroll down and click **View Certificates**.



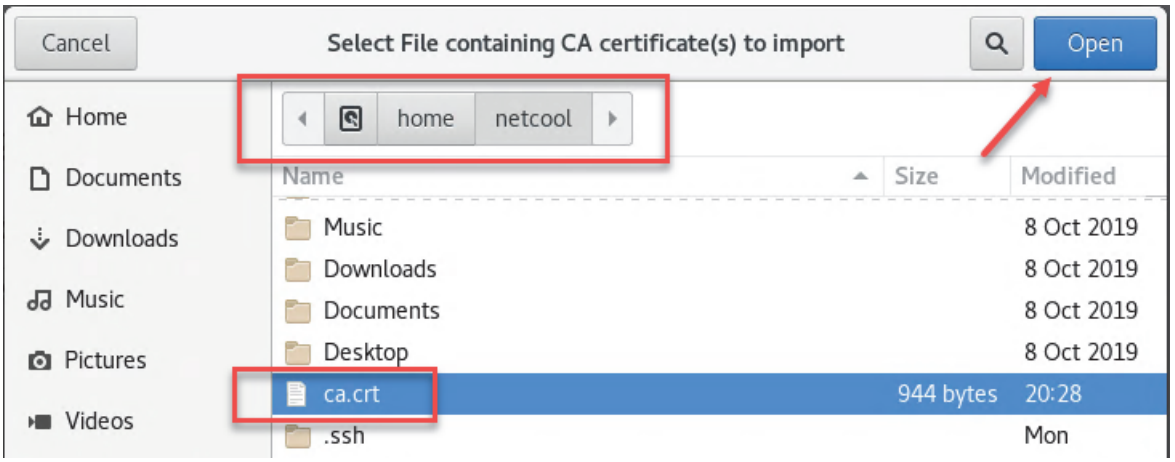
h. Click **Authorities > Import**.



i. Browse to the **/home/netcool** directory.

j. Select the ca.crt file.

k. Click **Open**.



l. 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.

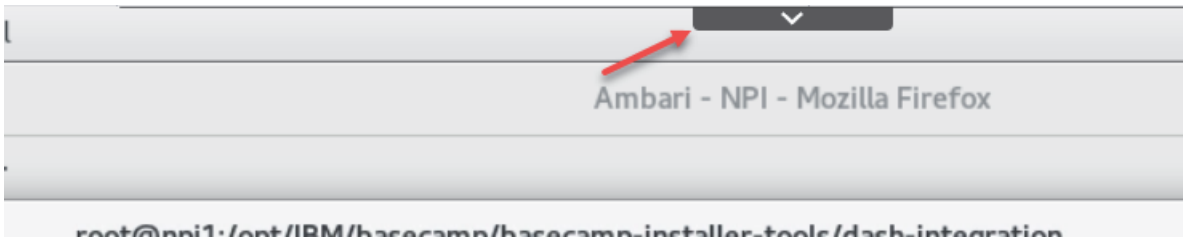
```
./status.sh
```

```
npi1.csite.edu                  network-health-generic      1.2.0
                                network-health              1.2.0
                                network-health-cisco        1.1.0
                                network-probe-cisco         1.0.0
```

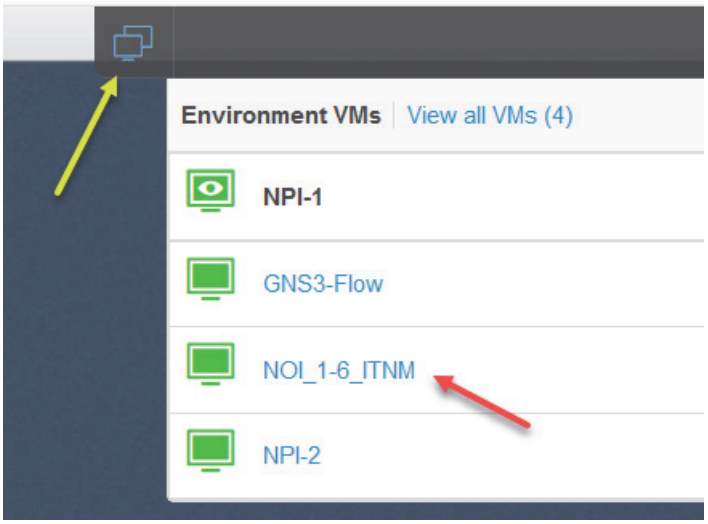
Exercise 2 Installing the Device Dashboard

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

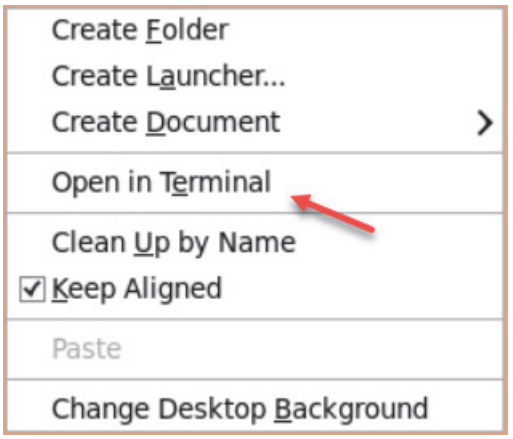
1. Perform the next steps on the host where Netcool Operations Insight is running. Change your lab environment to the desktop of host1.csite.edu, which is labeled **NOI_1-6_ITNM.**
   a. Click the tab at the top of the window to view the lab environment options.



   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
```

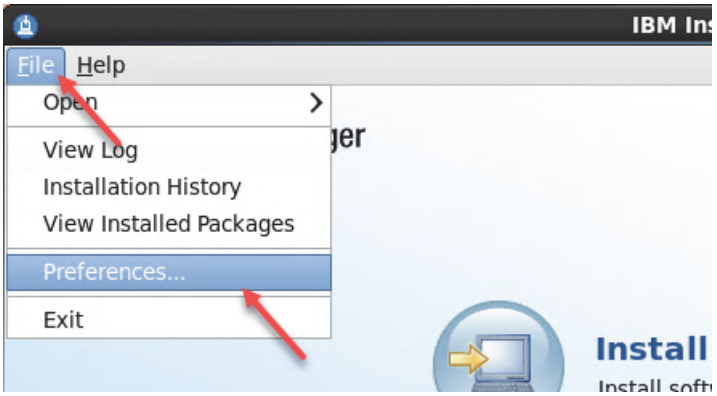
4. Start Installation Manager.
   a. Change to the target directory.

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

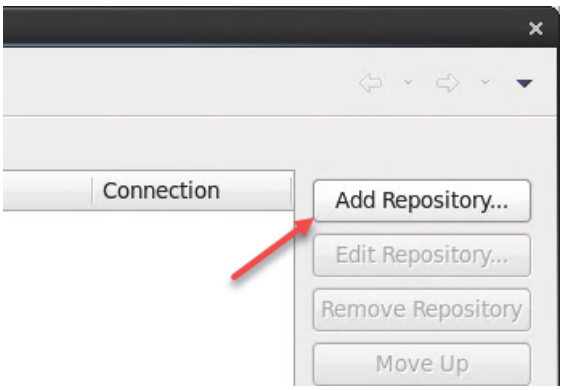
   b. Run the following command to start Installation Manager.

```
./IBMIM
```

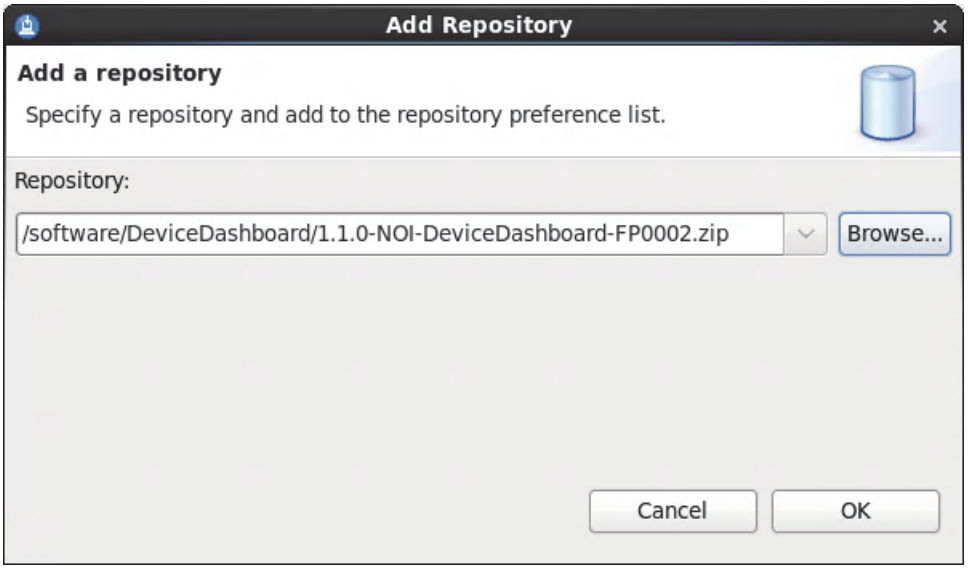
5. Add the Device Dashboard installation media as a repository.
   a. Click **File > Preferences**.



b. Click **Add Repository**.



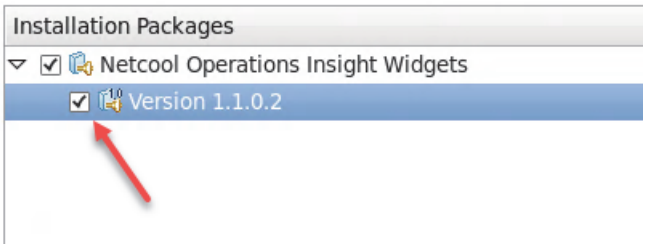
c. Browse to the **/software/DeviceDashboard/1.1.0-NOI-DeviceDashboard-FP0002.zip** file, then click **OK**.



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

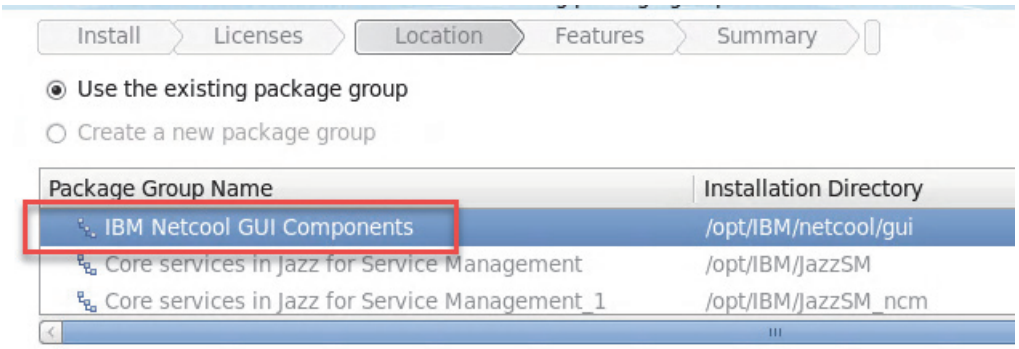
6. Install the Device Dashboard.
   a. Click **Install** to start the installation wizard.

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

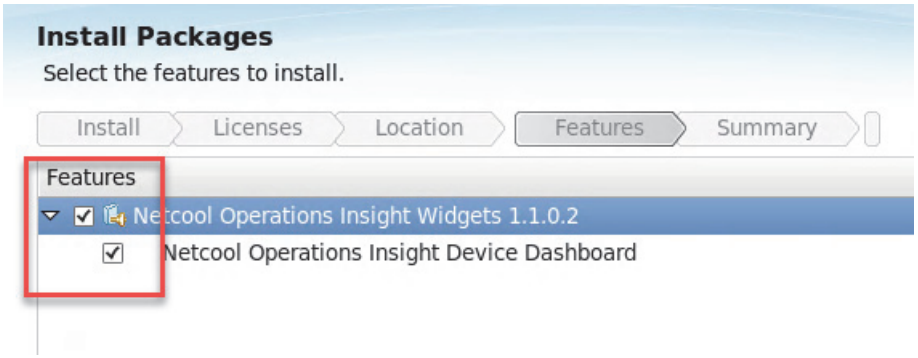


   c. Accept the license agreement and click **Next**.

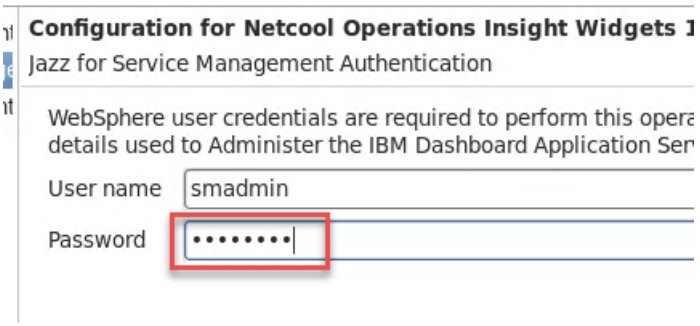
   d. Confirm that IBM Netcool GUI Components is selected as the package group and click **Next**.



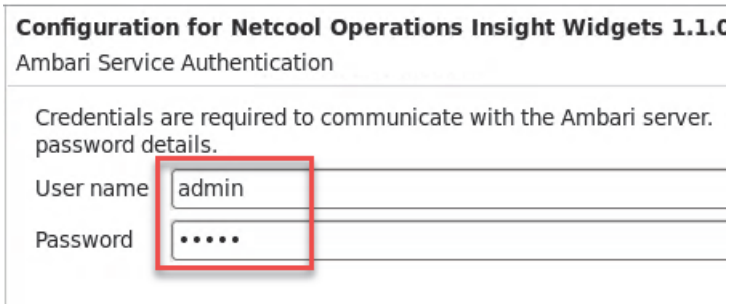
e. Verify that both features are selected and click **Next**.



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



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



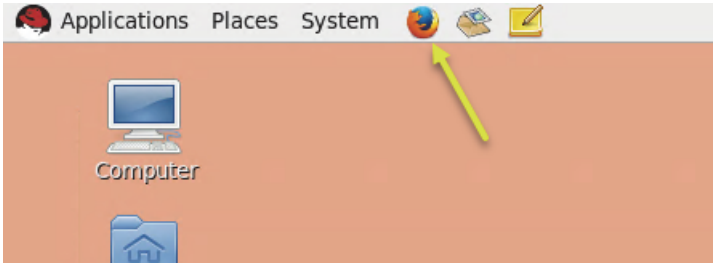
h. Click **Install** at the summary page. The installation takes about 20 minutes.

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 use this host in the next steps.

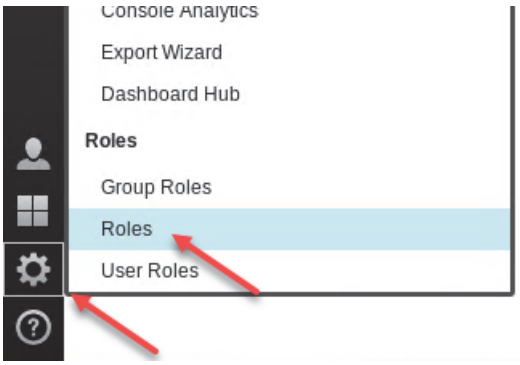
7. Add DASH roles to the Network Performance Insight users.
   a. Open a Firefox browser.



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

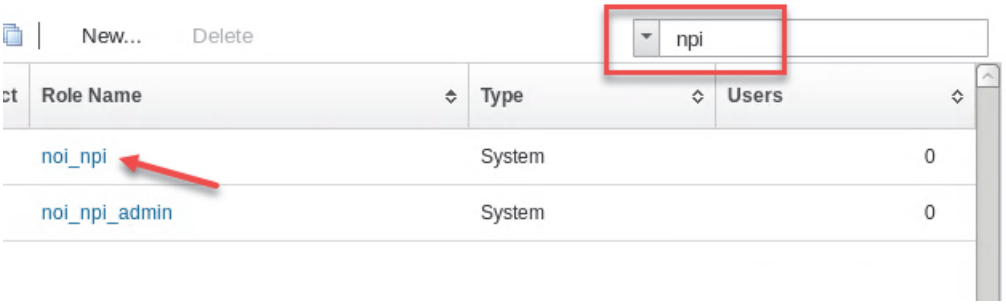
      https://host1.csite.edu:16311/ibm/console/logon.jsp

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



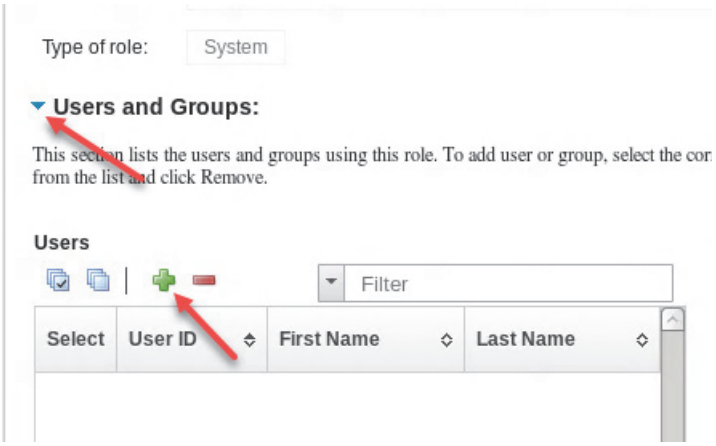
   d. Enter **npi** in the filter field.

   e. Click the **noi_npi** role.



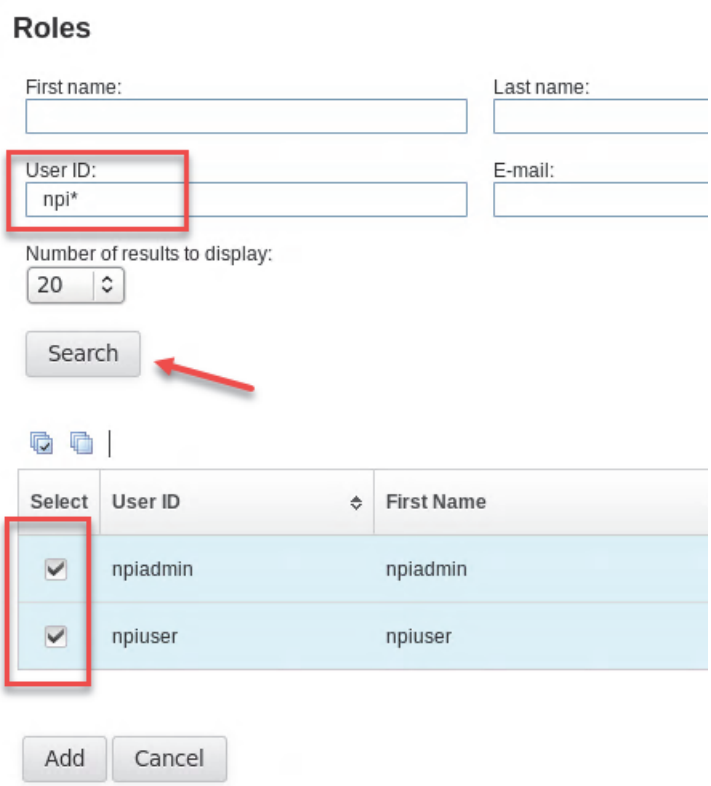
   f. Expand **Users and Groups**.

g. Click the icon to add users.

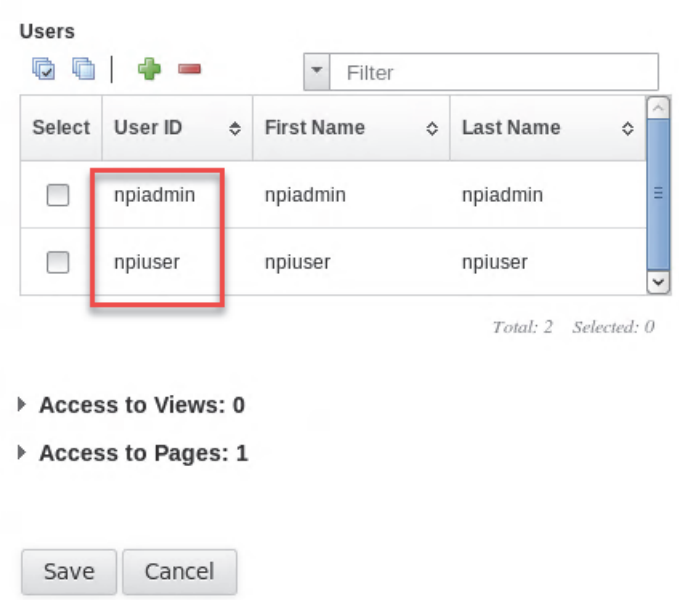


h. Enter **npi*** as the user id, then click **Search**.

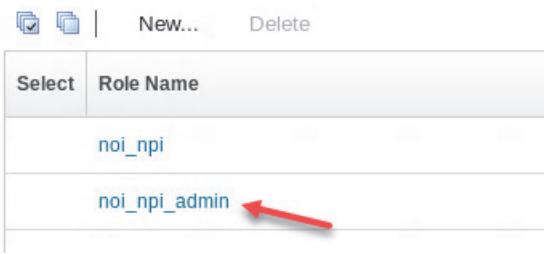
i. Select the **npiadmin** and **npiuser** users, then click **Add**.



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

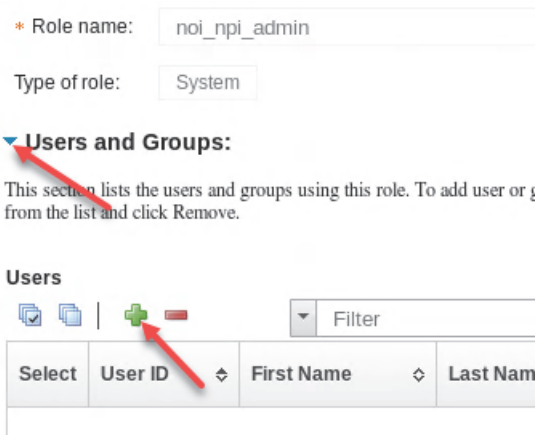


k. Click the **noi_npi_admin** role.



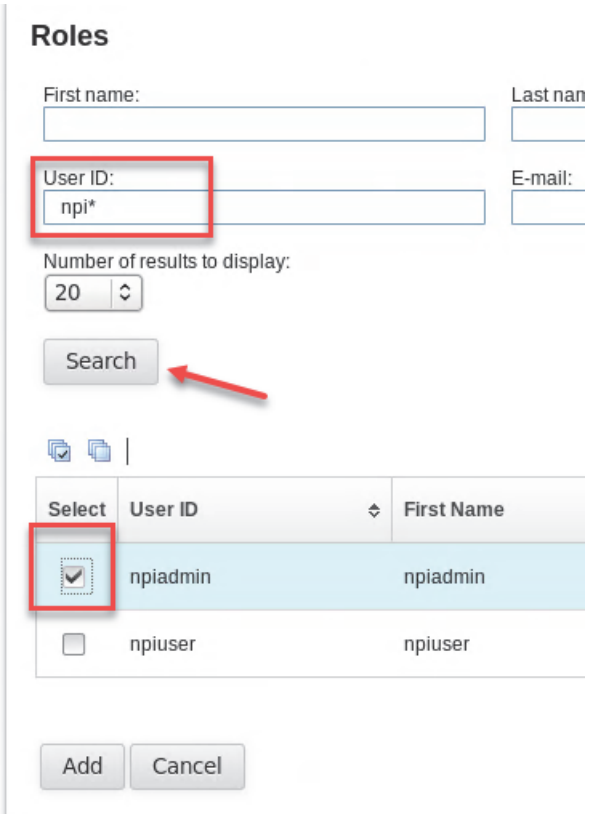
l. Expand **Users and Groups**.

m. Click the icon to add users.

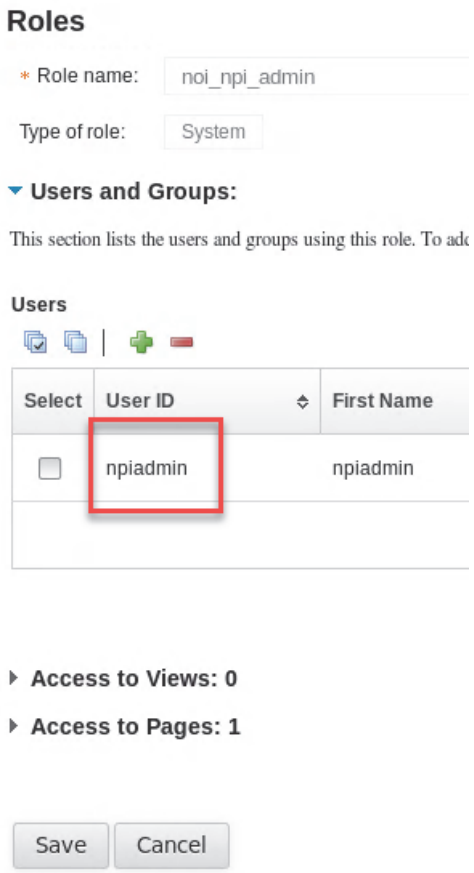


n. Enter **npi*** as the user id, then click **Search**.

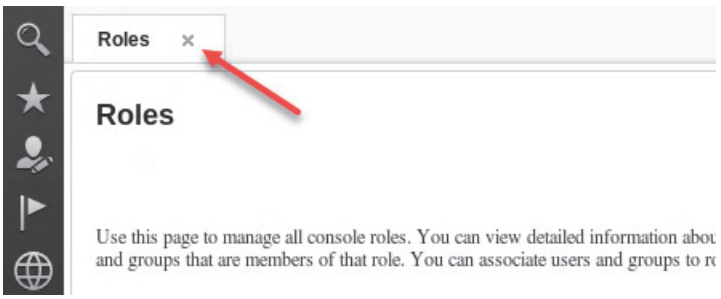
o. Select the **npiadmin** user, then click **Add**.



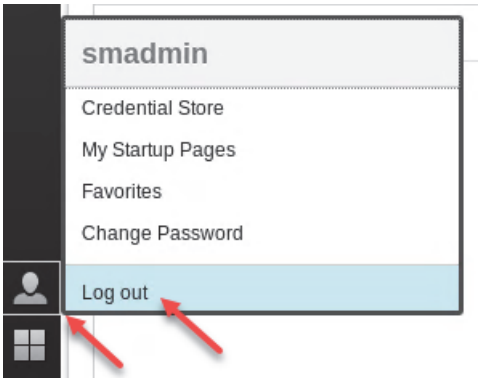
p. Verify that the user is present and click **Save**.



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.
   a. Return to the terminal window. Verify that you are the netcool user.
   b. Open the tnm.properties file in a text editor.

```
vi /opt/IBM/netcool/gui/precision_gui/profile/etc/tnm/tnm.properties
```

   c. 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.csite.edu:9443
```

9. Configure IBM Tivoli Network Manager with the Network Performance Insight version.
   a. Open the npi.properties file in a text editor.

```
vi /opt/IBM/netcool/gui/precision_gui/profile/etc/tnm/npi.properties
```

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

```
su - root

Password: object00
```

    b. Change to the target directory.

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

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

```
./jazz stop
```

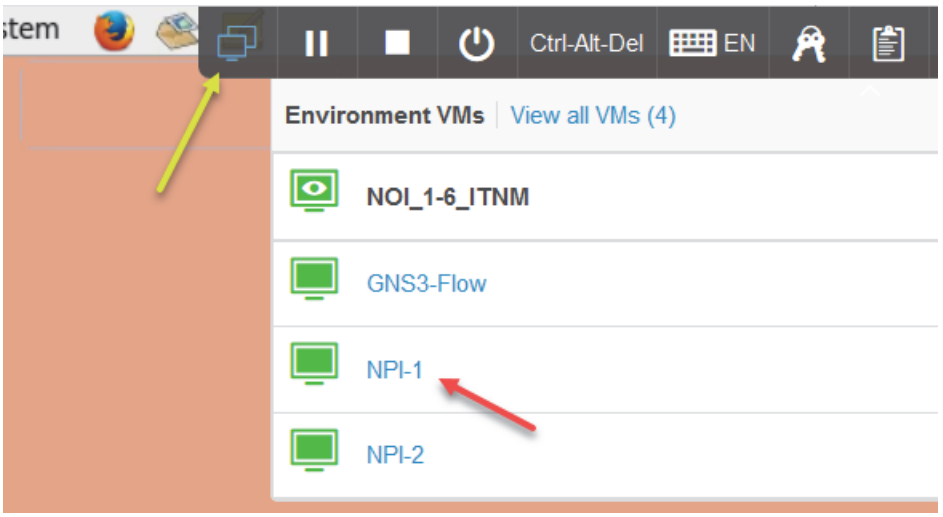
    d. Wait until the service is stopped. Run the following command to start WebSphere Application Server, Jazz for Service Management, and DASH.

```
./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**.

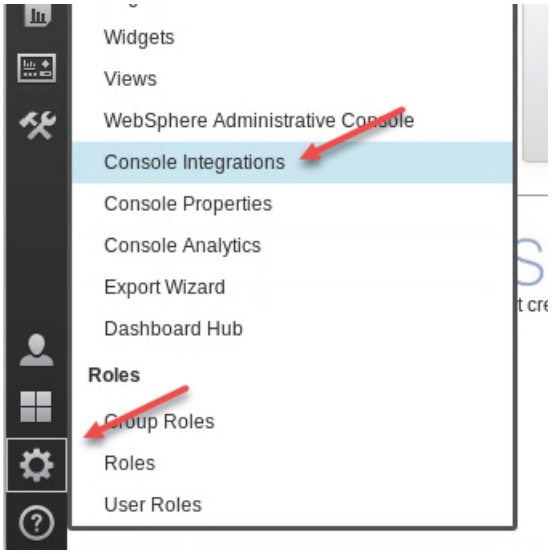


12. Verify that the Network Performance Insight Console Integration is working.
    a. Open a Filefox browser and go to the following URL. Log in with the user name **npiadmin** and the password **object00**.

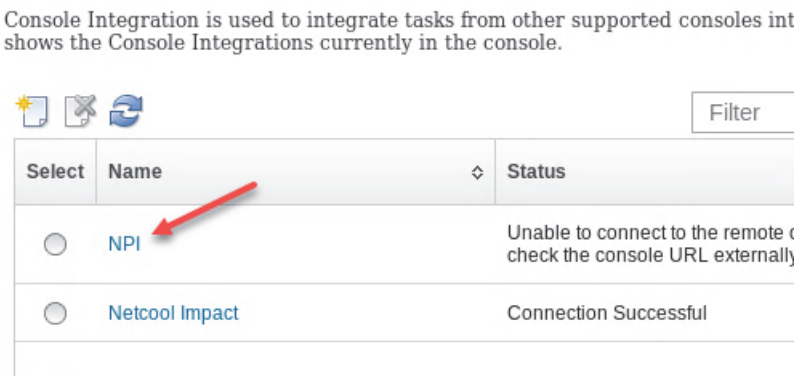
       https://host1.csite.edu:16311/ibm/console/logon.jsp

    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.

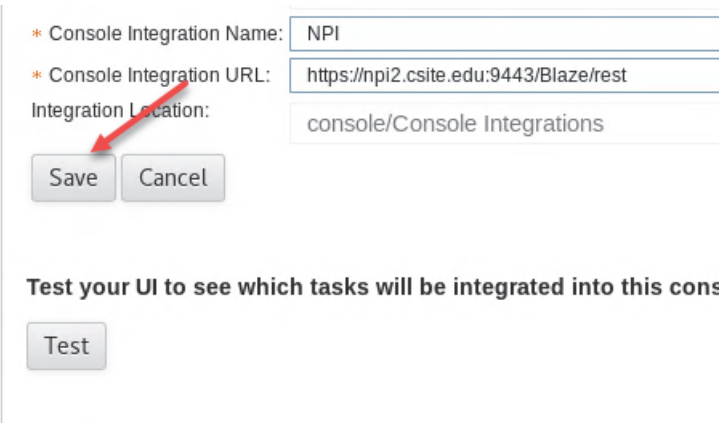
c. Click **Console Settings > Console Integrations**.



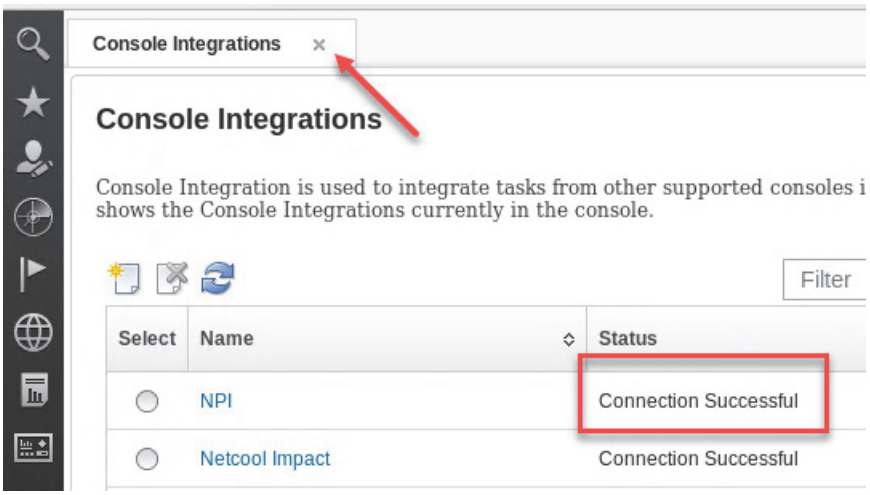
d. Click **NPI**.



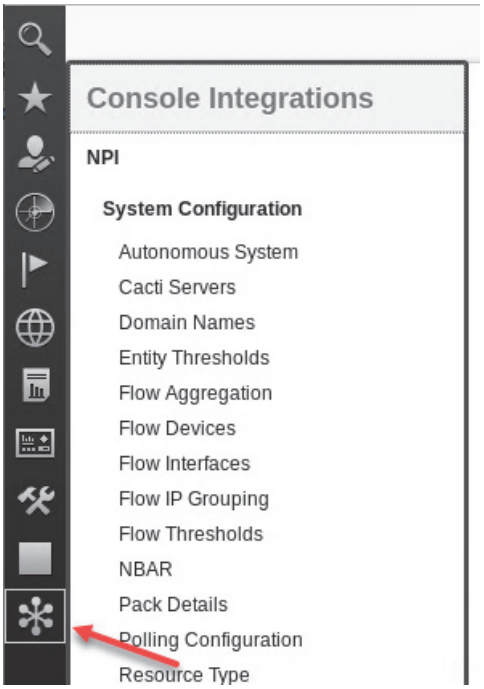
e. Click **Save**.



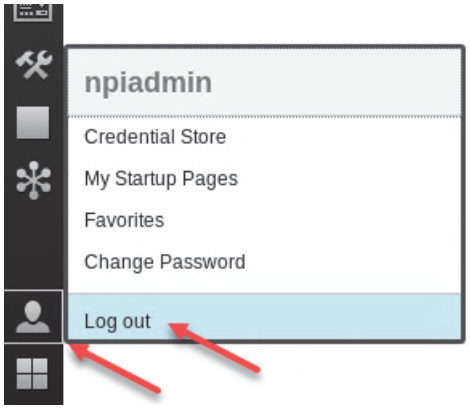
f. Close the Console Integrations tab.



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.



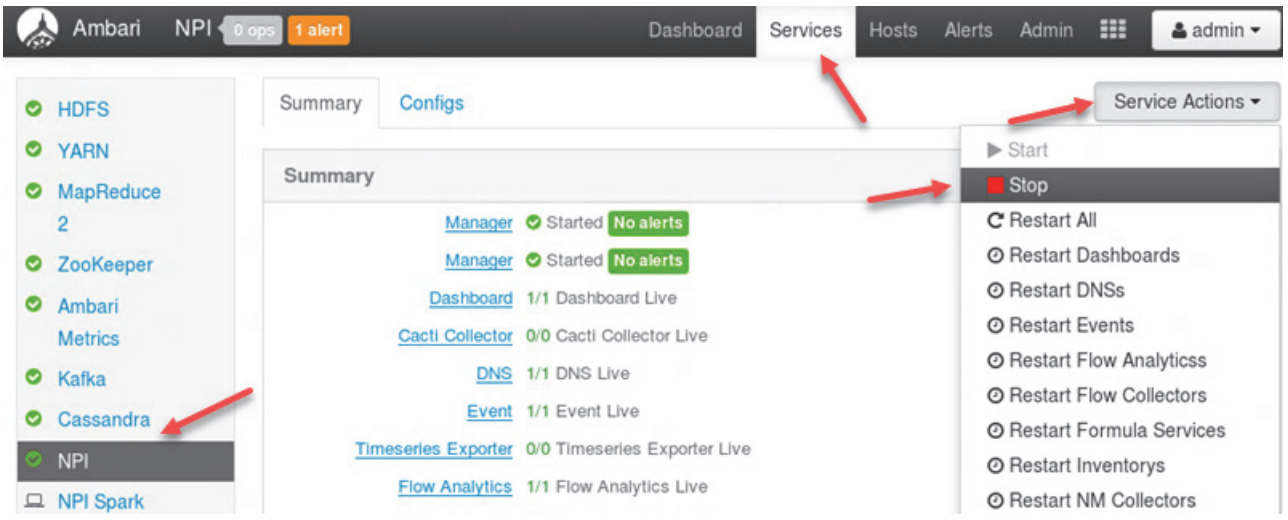
h. Log out of DASH.



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**.



   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.

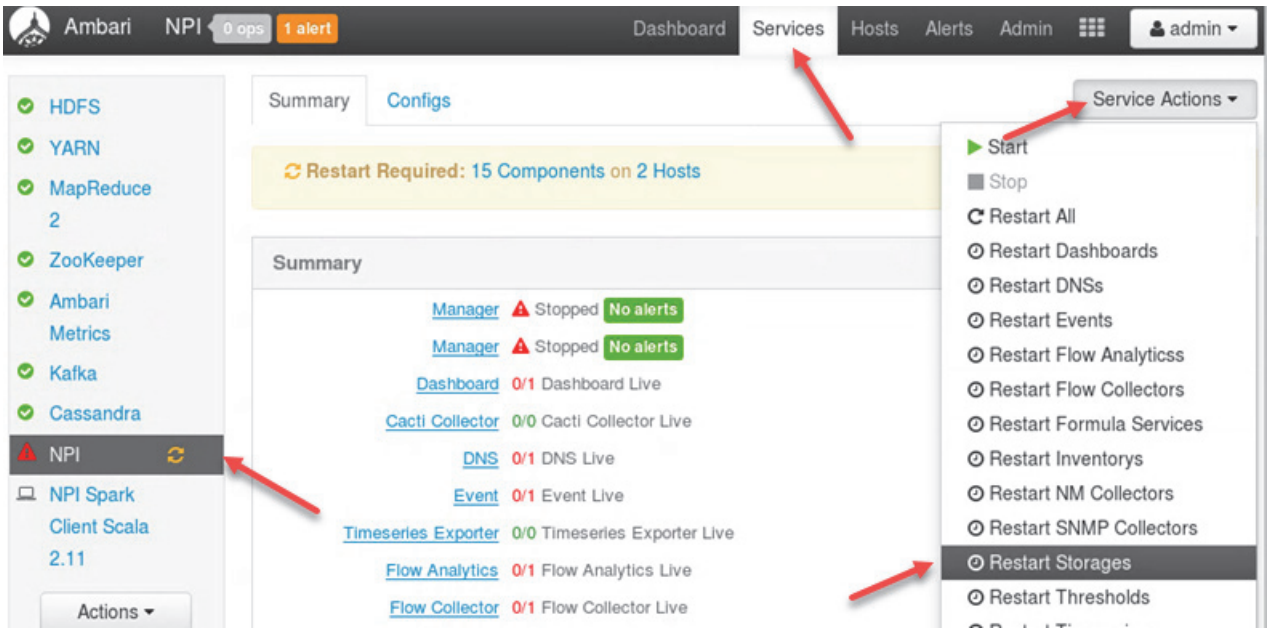
```
./dashboard_user_backup.sh

...
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.

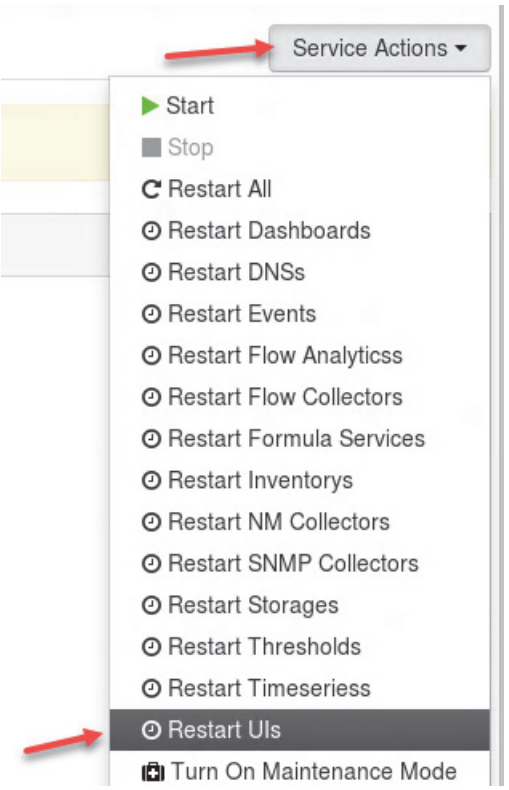
d. Click **Service Actions > Restart Storages**.



e. Click **Trigger Rolling Restart**.

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

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



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
```

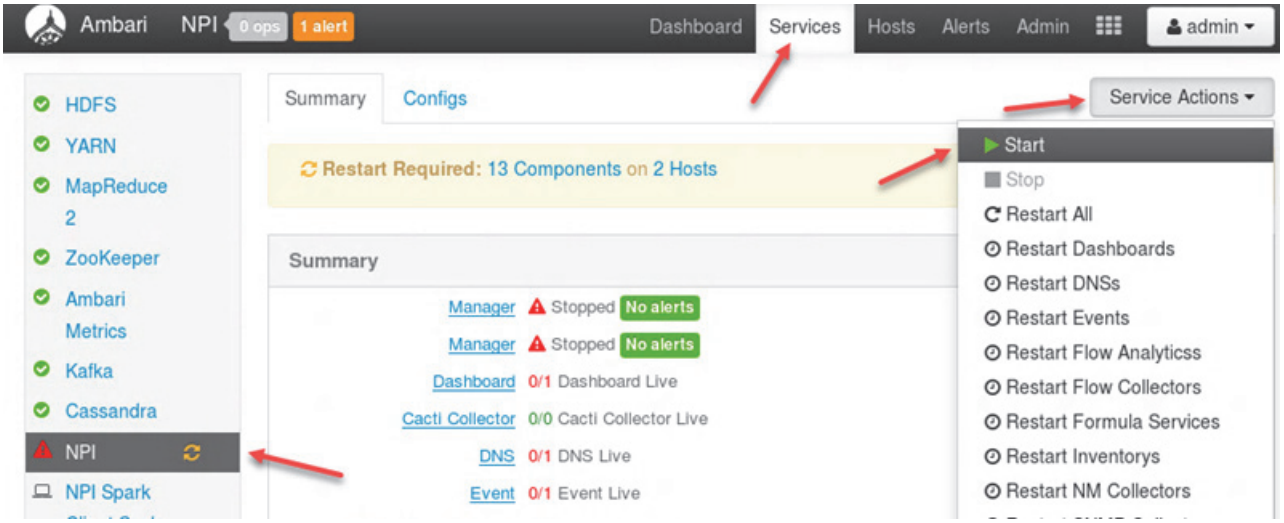
   c. Enter **npiadmin** as the user name.

```
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.csite.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**.



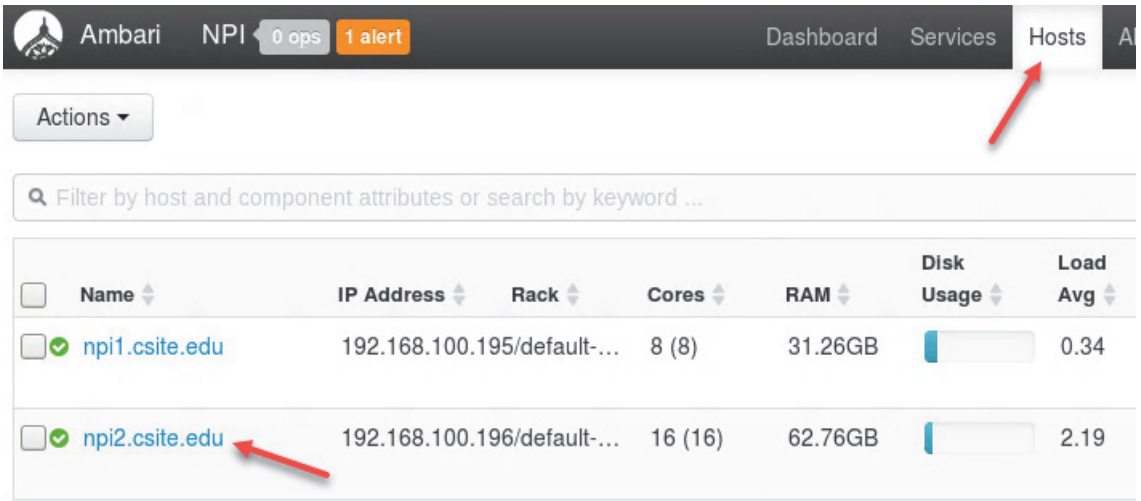
e. Click **Confirm Start**.

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

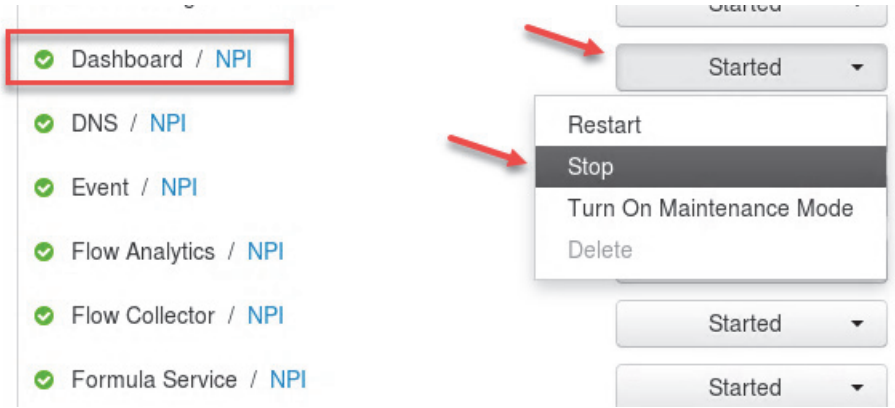
8. Restore the Network Performance Insight users that you previously backed up.

a. Return to the Ambari manager page.

b. Stop the Network Performance Insight Dashboard service. Click the **Hosts** tab and click **npi2.csite.edu**.



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.

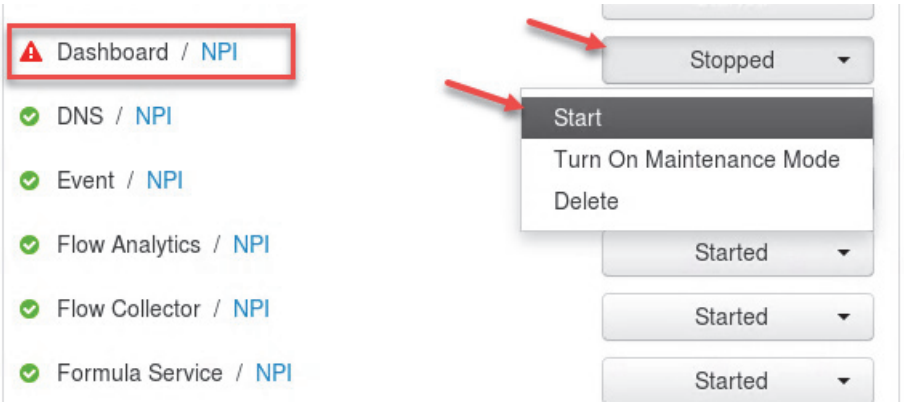
f. Return to the terminal window where you are the root user.

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**.



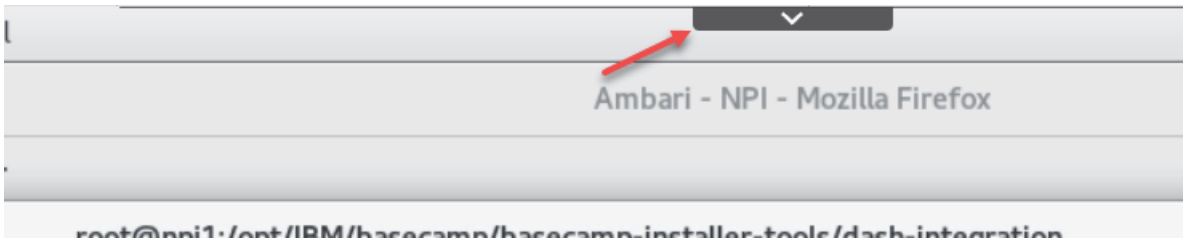
j. Click **OK** to confirm.

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

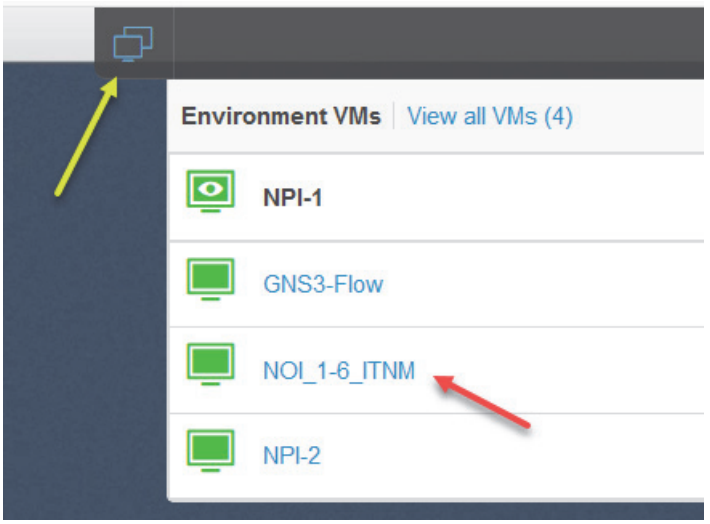
9. Uninstall the Device Dashboard. You perform this task on the Netcool Operations Insight server.

a. Change your lab environment to the desktop of host1.csite.edu, which is labeled **NOI_1-6_ITNM.**

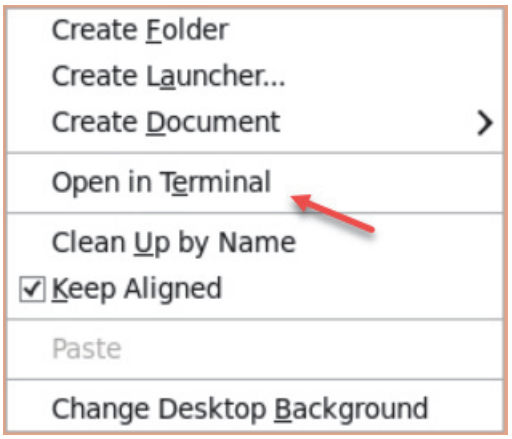
b. Click the tab at the top of the window to view the lab environment options.



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**.



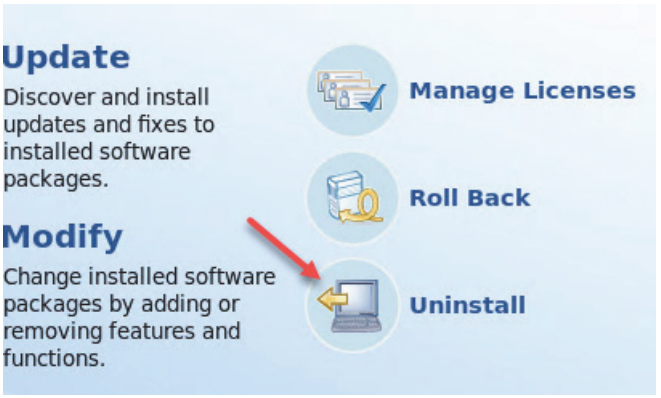
e. Use Installation Manager to uninstall the Device Dashboard. Change to the Installation Manager directory.

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

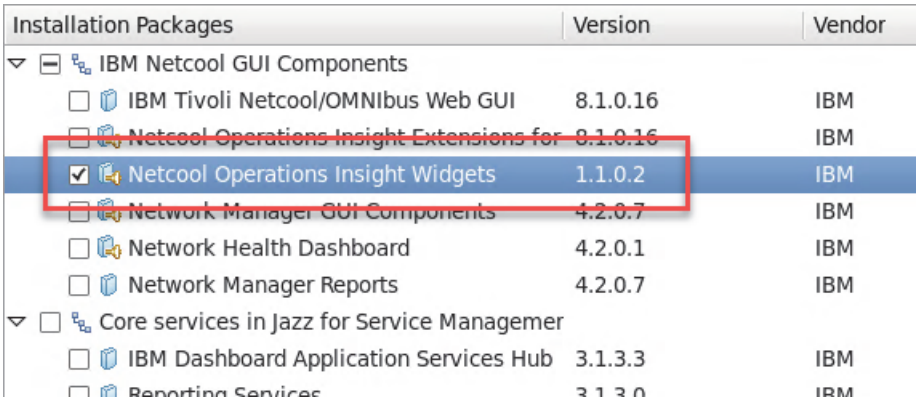
f. Run the following command to start Installation Manager.

```
./IBMIM
```

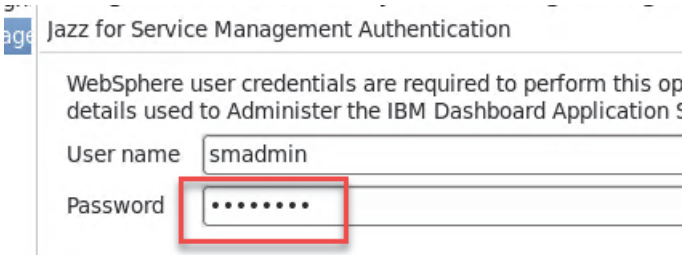
g. Click **Uninstall**.



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



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



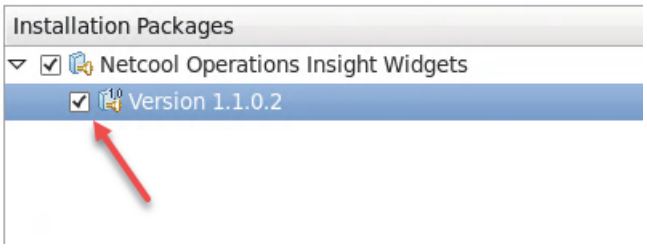
j. Click **Uninstall** on the summary page. The operation to uninstall the Device Dashboard takes about 5 minutes.

k. Click **Finish** to close the wizard. Leave Installation Manager open.

10. Install the Device Dashboard again.

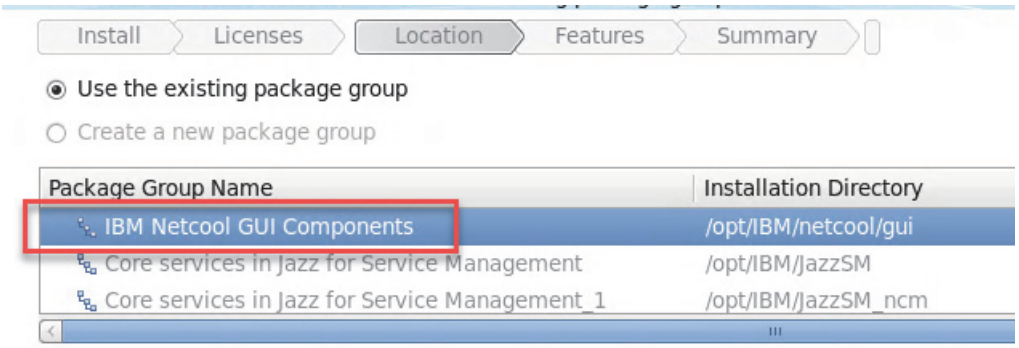
a. Click **Install** to start the installation wizard.

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

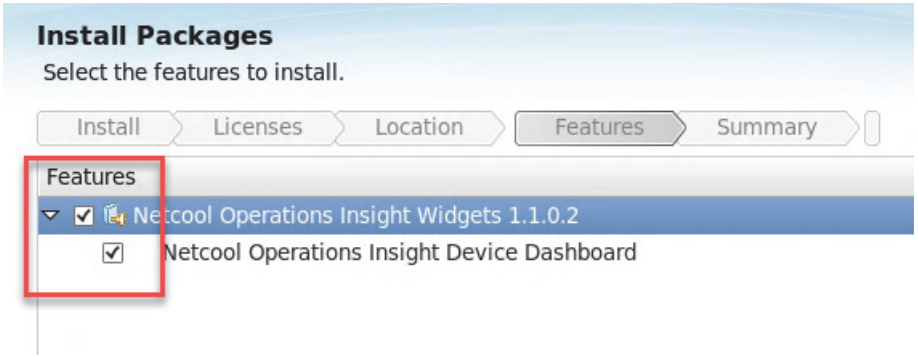


c. Accept the license agreement and click **Next**.

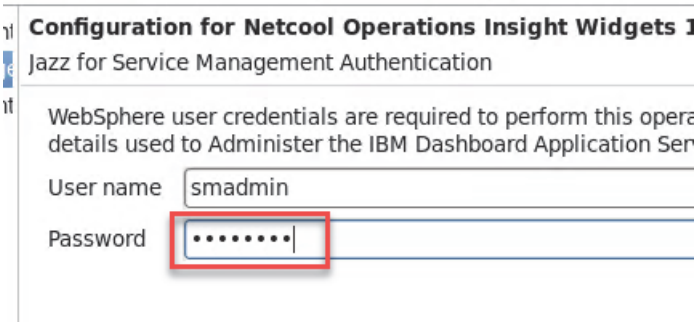
d. Confirm that IBM Netcool GUI Components is selected as the package group and click **Next**.



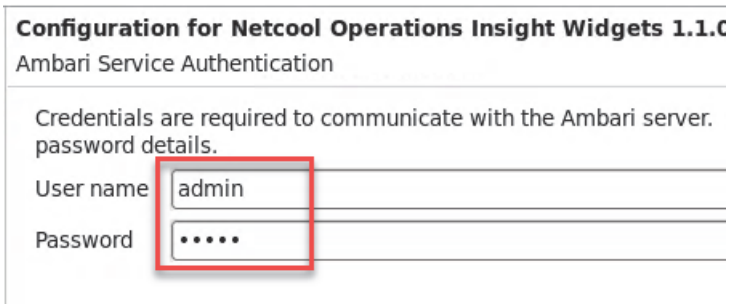
e. Verify that both features are selected and click **Next**.



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.

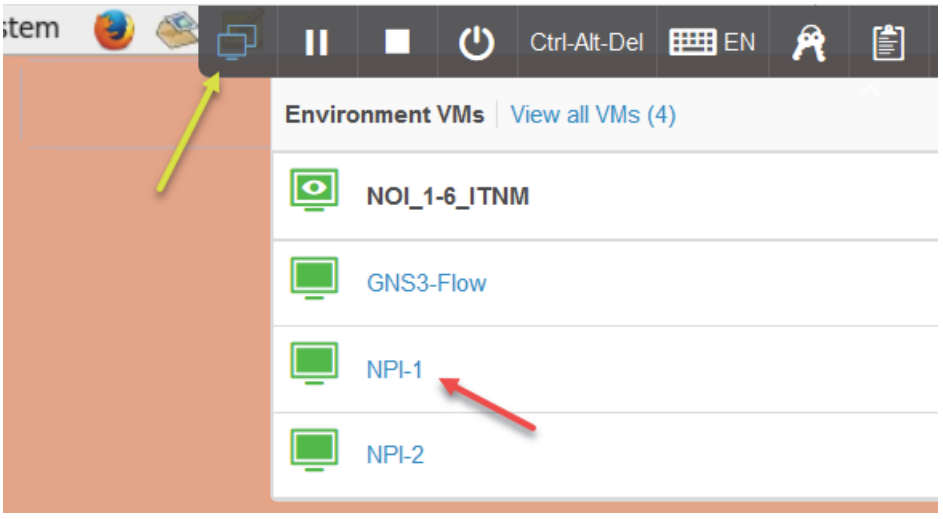
i. Click **Finish** to close the installation wizard.

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**.

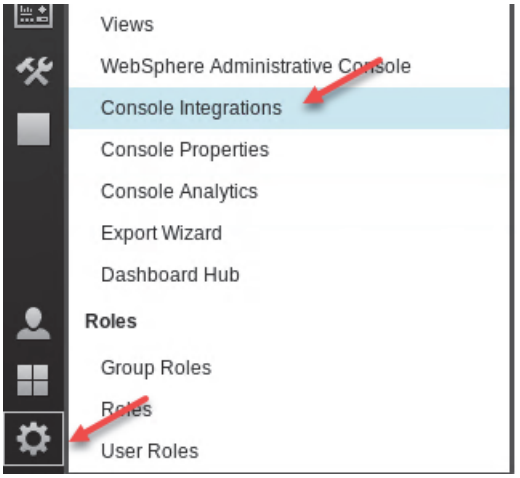


12. Configure the DASH Console Integration for Network Performance Insight.

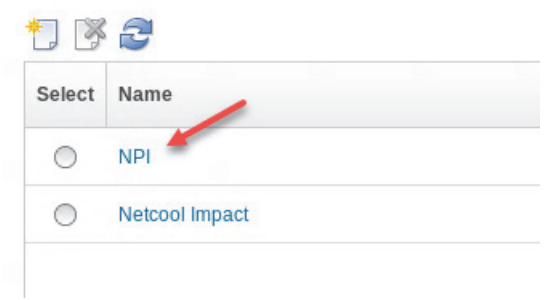
a. Open a Firefox browser. Go to the following URL. Log in with the user name **npiadmin** and the password **object00**.

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

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

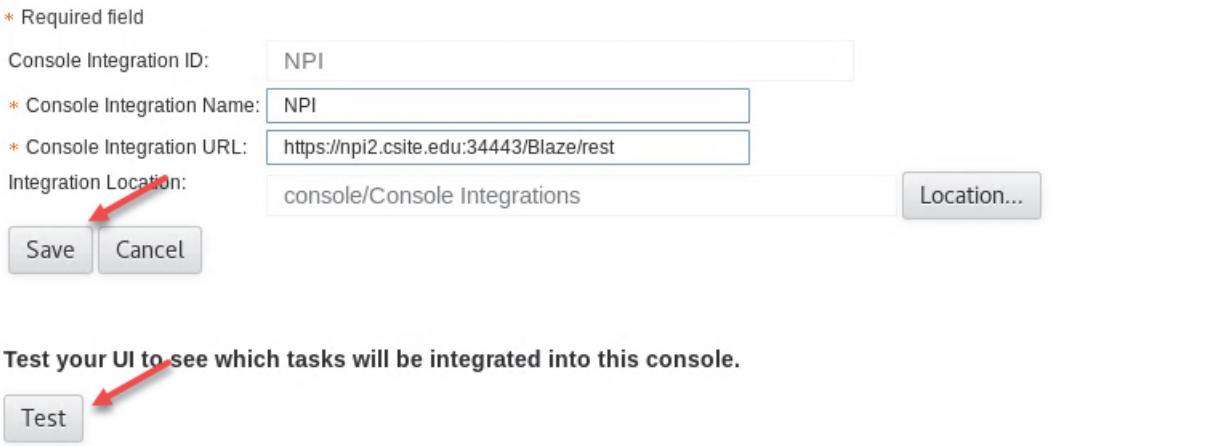


c. Click **NPI**.

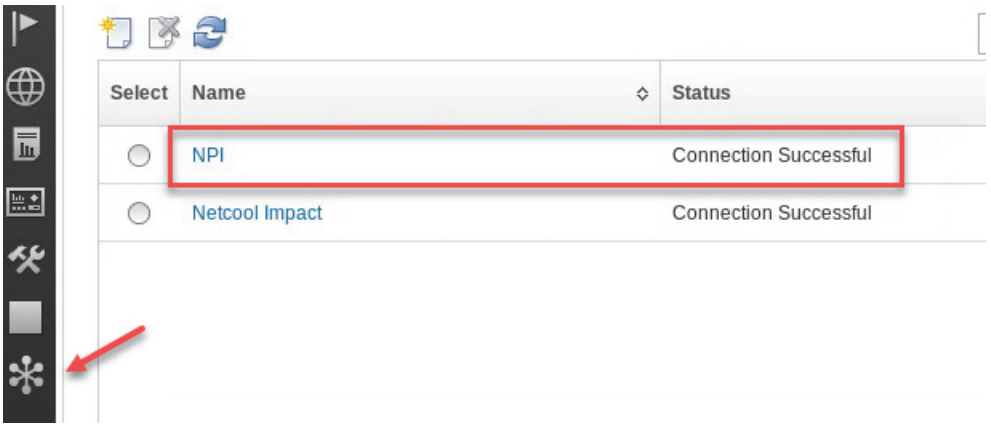


d. Click **Test**. You can ignore the status message.

e. Click **Save**.

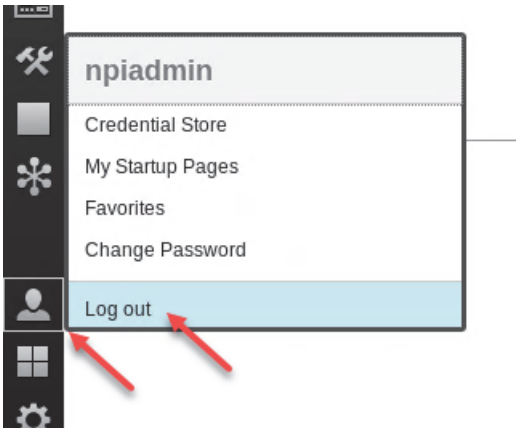


f. Verify that the connection is successful for the NPI Console Integration. Verify that you see a snowflake icon in the menu on the left.



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.

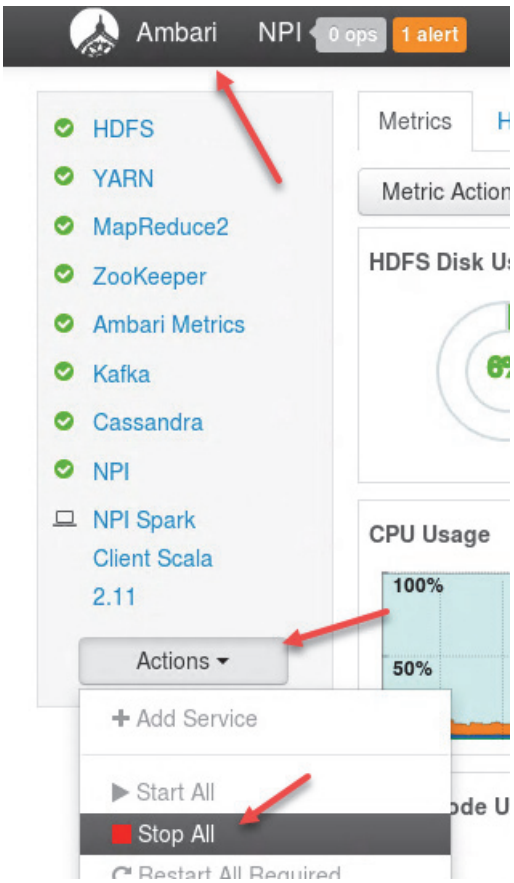
   ```
   ./apply_hotfix.sh

   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.

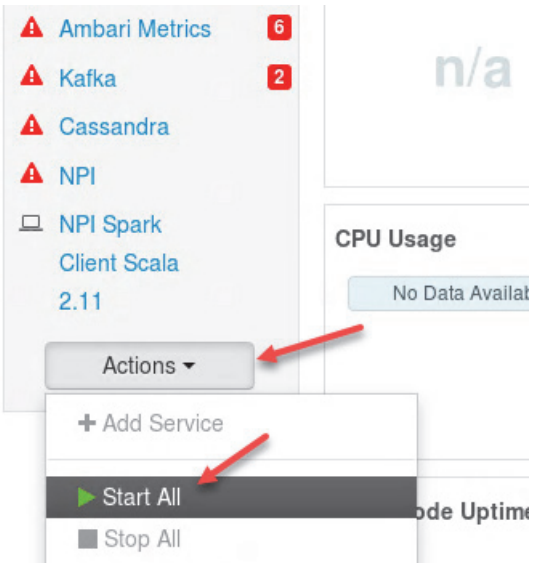
c. Click **Actions > Stop All**.



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**.

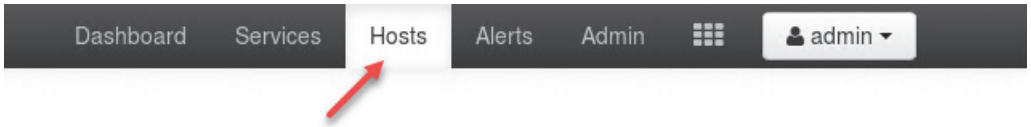


g. Click **Confirm Start**.

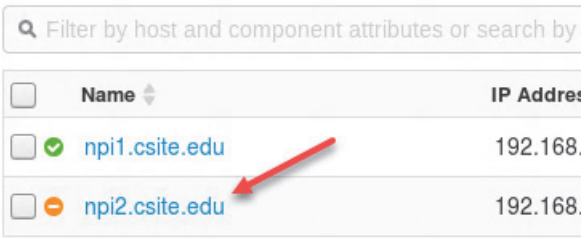
h. After a few minutes, the components start. Click **OK** to close the operations window.

9. If the Dashboard service is not running, start it manually.

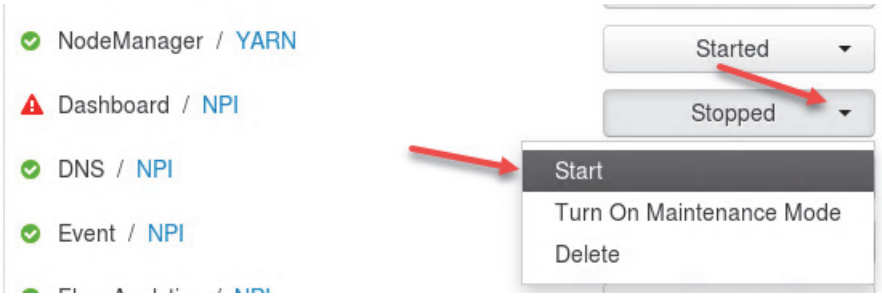
a. Click the **Hosts** tab close to the top of the page.



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



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.csite.edu "range(resource.agentIp, '10.10.255.1',
'10.10.255.254')"
```

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

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

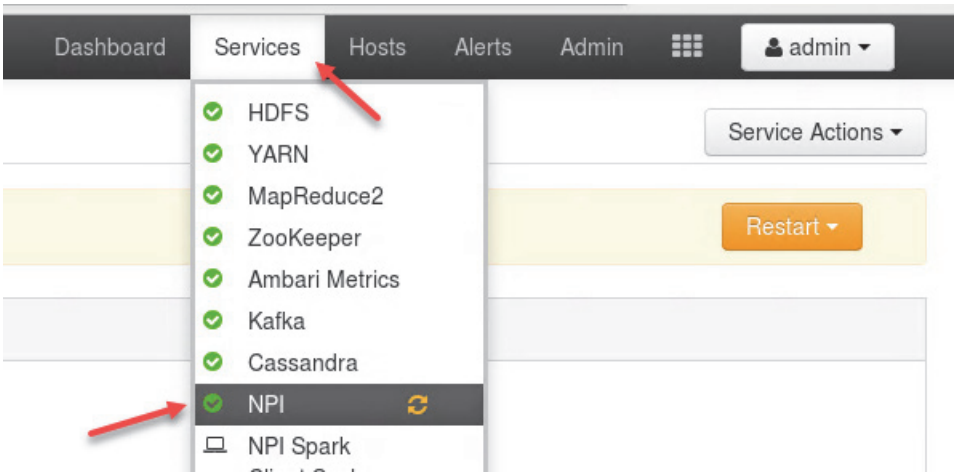
   e. Run the following command to verify that the scope is enabled.

```
./snmp-scoping.sh list

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

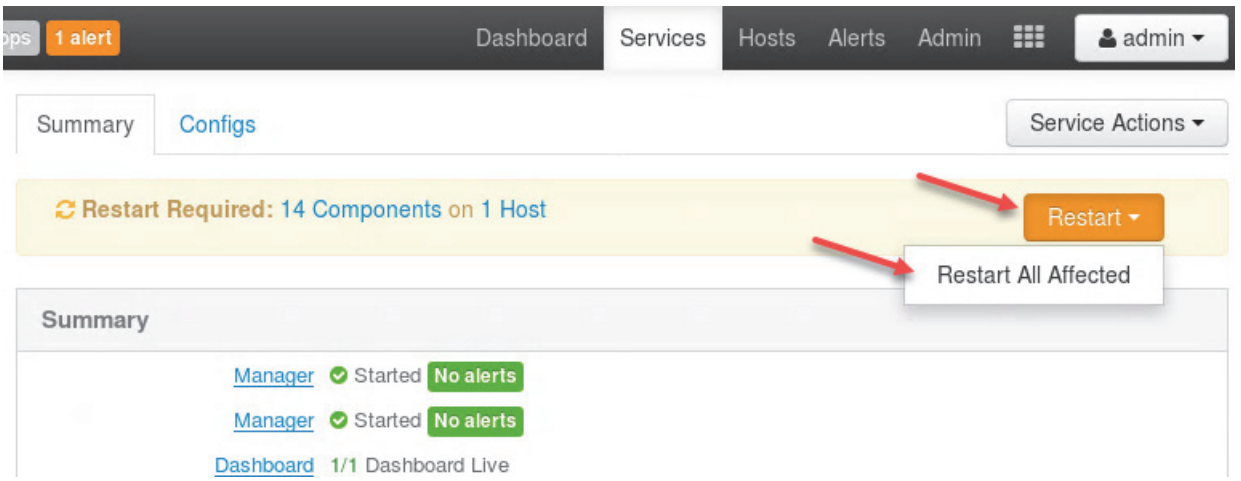
   f. Run the following command to test your scope. Run the entire command on one line.

```
./snmp-scoping.sh test npi2.csite.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"},{"entityN
ame":"10.10.255.2"},{"entityName":"10.10.255.15"},{"entityName":"10.10.255.14"}
...
```

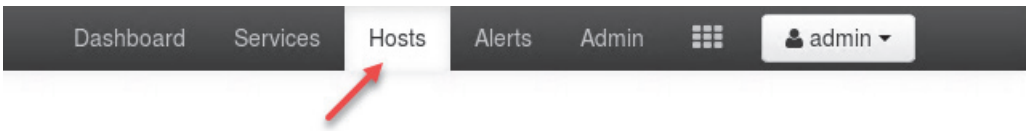
2. Restart all affected Network Performance Insight services.
   a. Return to the Ambari manager page.
   b. Click the **Services** tab and select **NPI**.



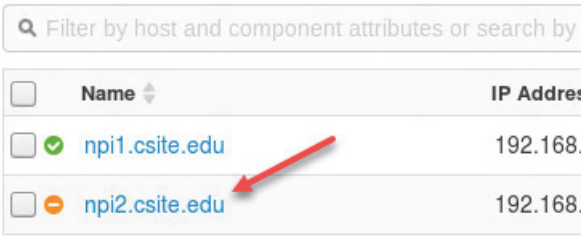
   c. Click **Restart > Restart All Affected**.



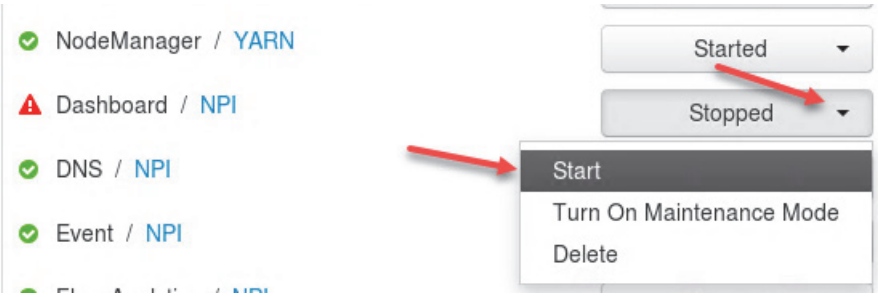
   d. Click **Confirm Restart All**.
   e. Click **OK** when the operation is finished.
   f. Start the Dashboard service manually. Click the **Hosts** tab close to the top of the page.



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



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.

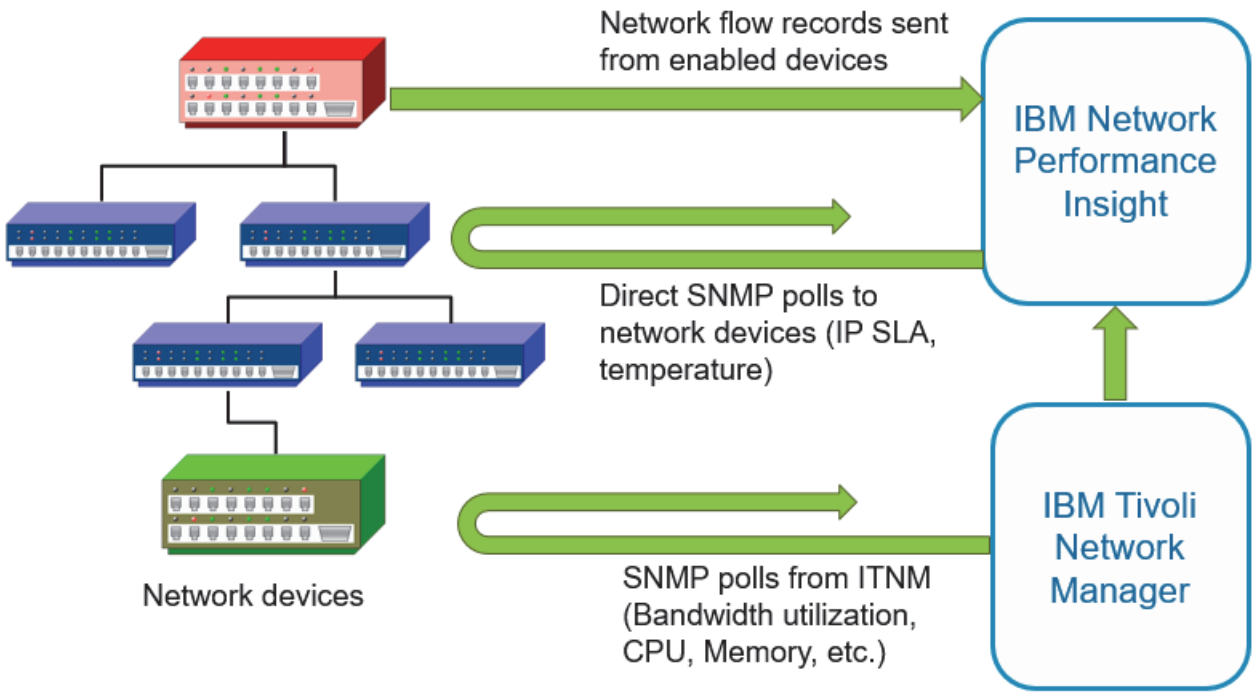
j. In a short time, the start operation is 100% complete. Click **OK** to confirm.

k. Verify that the Dashboard service is started before you continue.

Unit 4 Solution verification

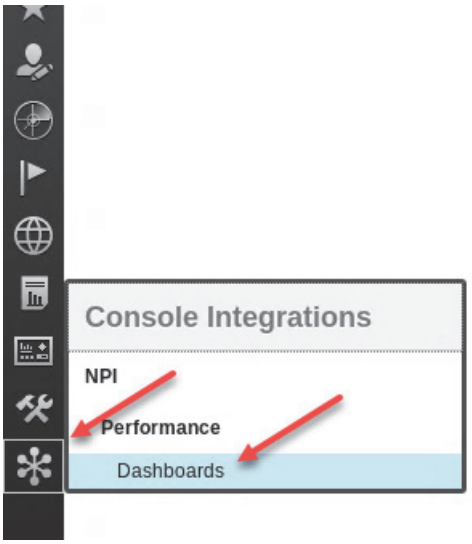
In your lab environment, IBM Network Performance Insight obtains performance data using the following three methods:

- **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.

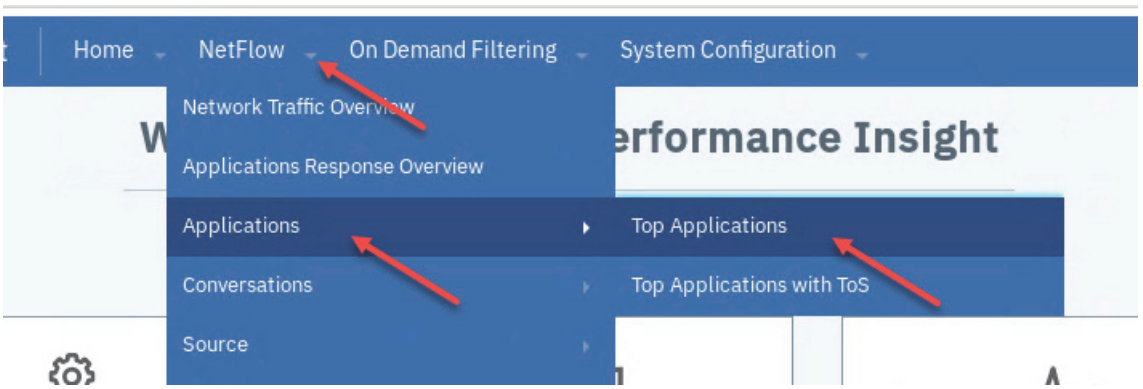


In these exercises, you verify that IBM Network Performance Insight is successfully collecting, aggregating, and reporting performance data from these three data sources. You also learn how to navigate the IBM Network Performance Insight user interface and set thresholds on flow data.

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**.

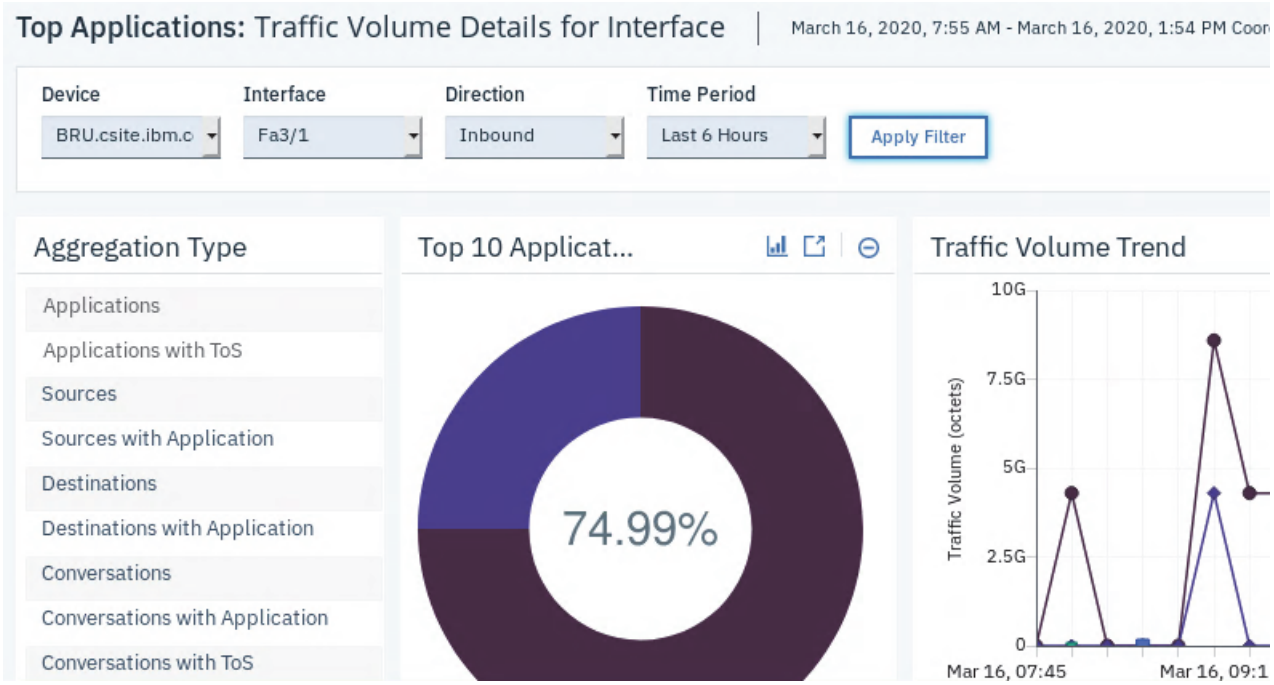


   d. Click **NetFlow > Applications > Top Applications**.



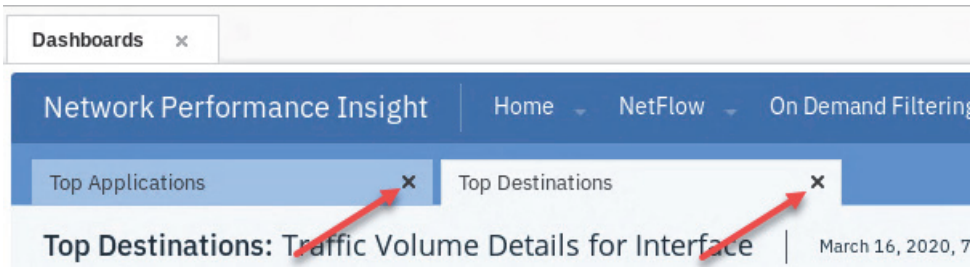
e. This dashboard shows the top applications that are flowing through the device. Notice the following features of this page:

- 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.

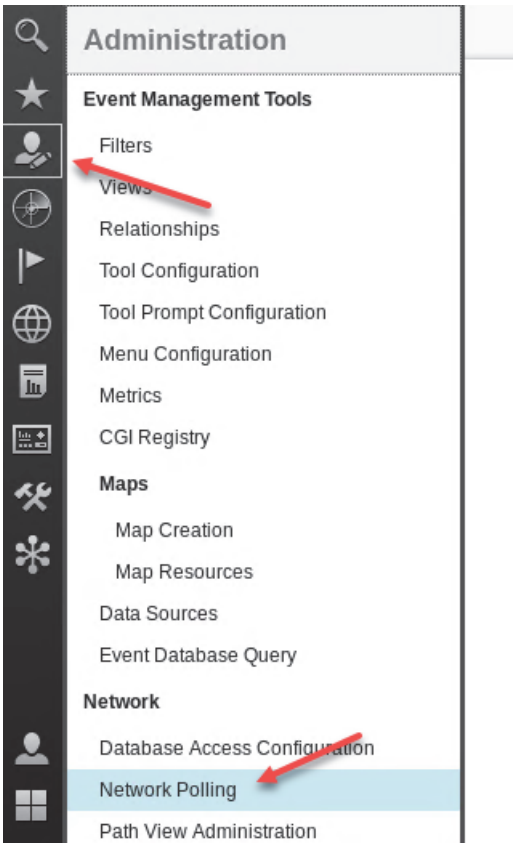


f. Spend a few moments interacting with this dashboard. Change the aggregation type on the left of the page to explore all of the aspects of network traffic that are derived from network flow records.

g. Close the **Top Applications** tab and any other NetFlow dashboards you have opened.

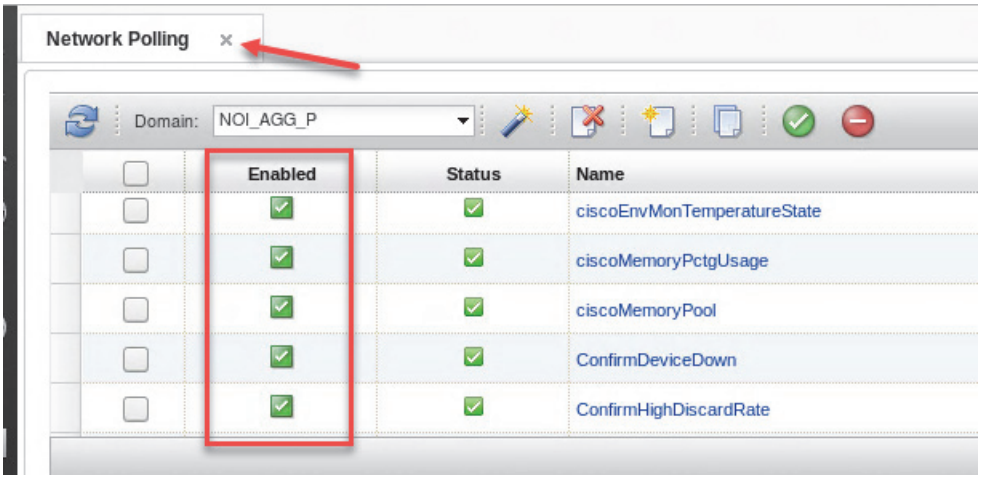


2. Some metrics are collected by IBM Tivoli Network Manager and reused by IBM Network Performance Insight. Verify that these metrics are present in IBM Network Performance Insight reports and dashboards.
   a. IBM Tivoli Network Manager is polling devices for several metrics. Look at the specific metrics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



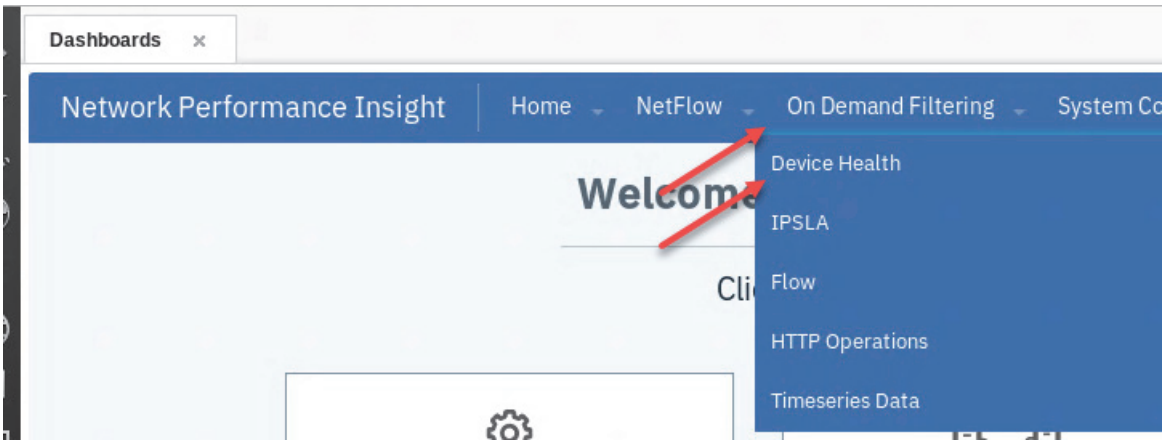
   c. Scroll down through the list of poll definitions and view the metrics that are enabled. These metrics are polled by IBM Tivoli Network Manager and reused by IBM Network Performance Insight. Notice that IP SLA metrics are not in this list, meaning they are not collected by IBM Tivoli Network Manager.

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

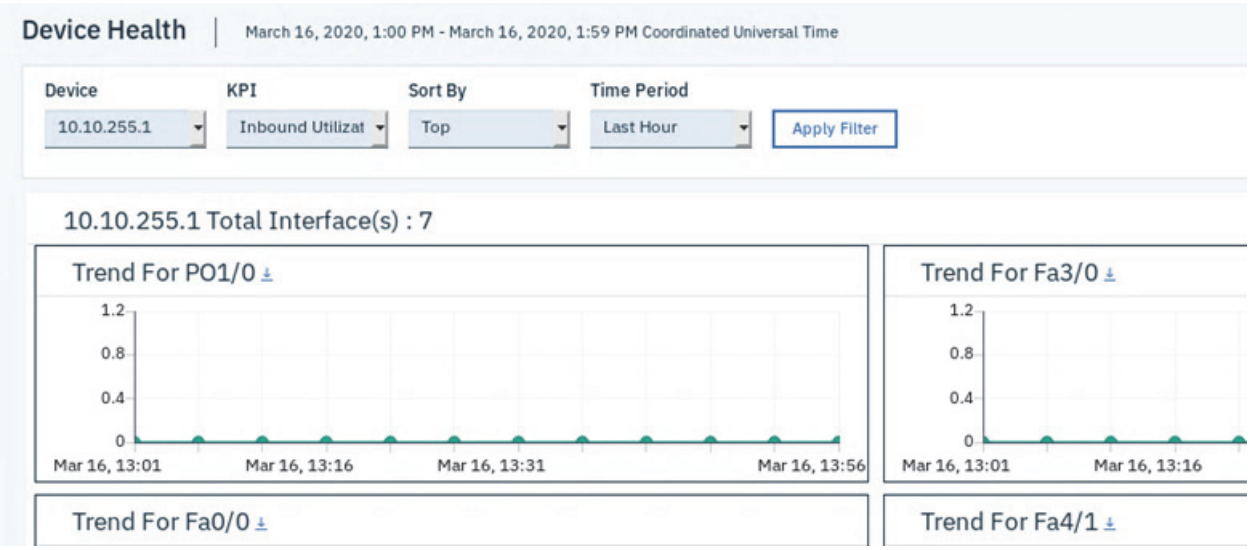


e. View the corresponding metrics in IBM Network Performance Insight. Return to the **Dashboards** tab.

f. Click **On Demand Filtering > Device Health**.

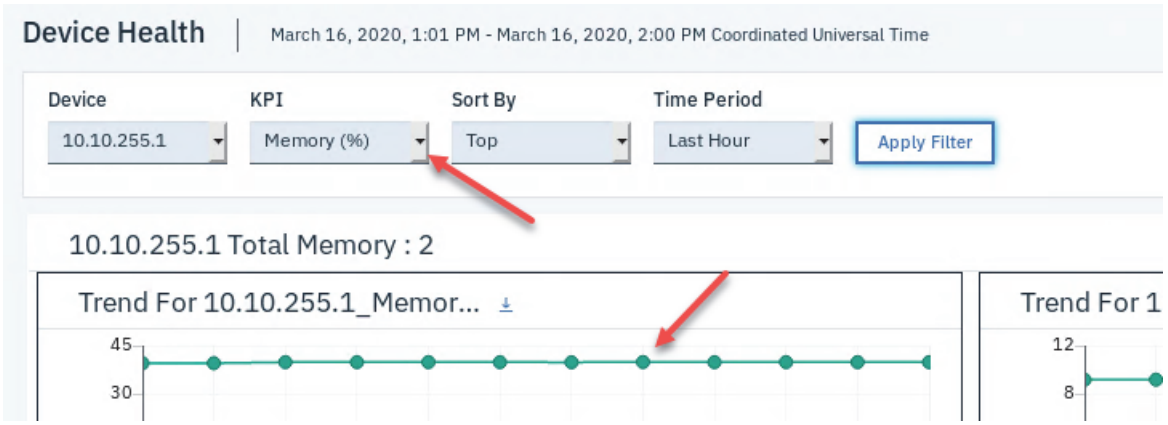


g. Look at the Device Health Dashboard. At the top of the page, you can change the device, the KPI, and the reporting time period. In this example, the metric is inbound utilization. Remember that IBM Tivoli Network Manager is collecting this metric.



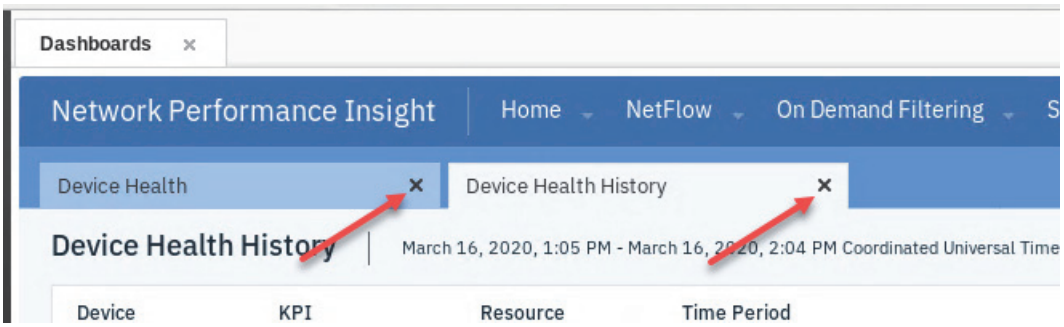
3. Open a historical trend dashboard.

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.



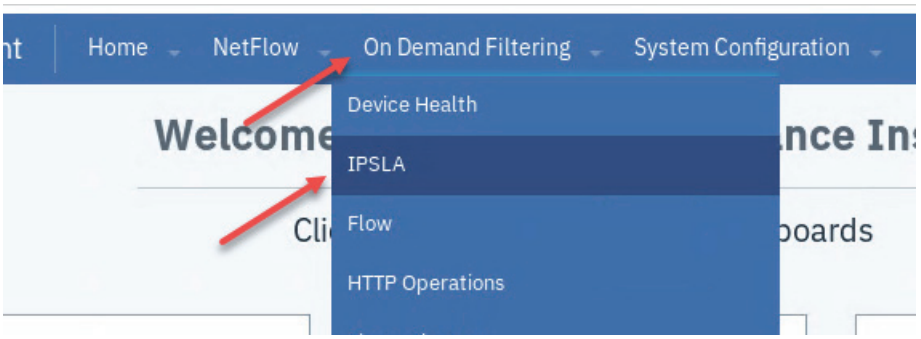
b. The historical trend dashboard opens. This shows the metric over time along with minimum, maximum, and average values.

c. Close any Device Health dashboards you have opened.

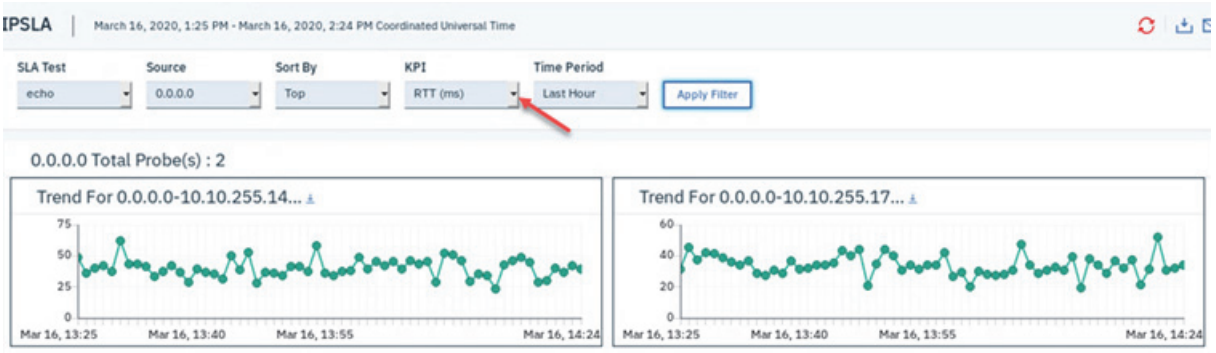


4. Recall that IBM Tivoli Network Manager is not polling for IP SLA data. View IP SLA data in reports and dashboards to confirm that IBM Network Performance Insight is directly polling for IP SLA statistics.

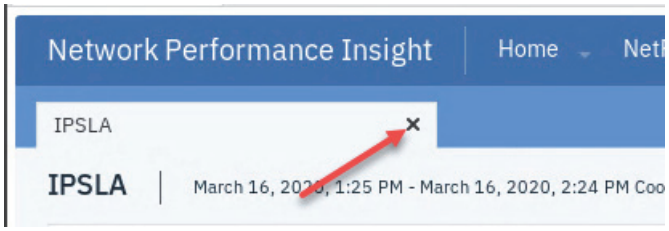
a. Click **On Demand Filtering > IPSLA**.



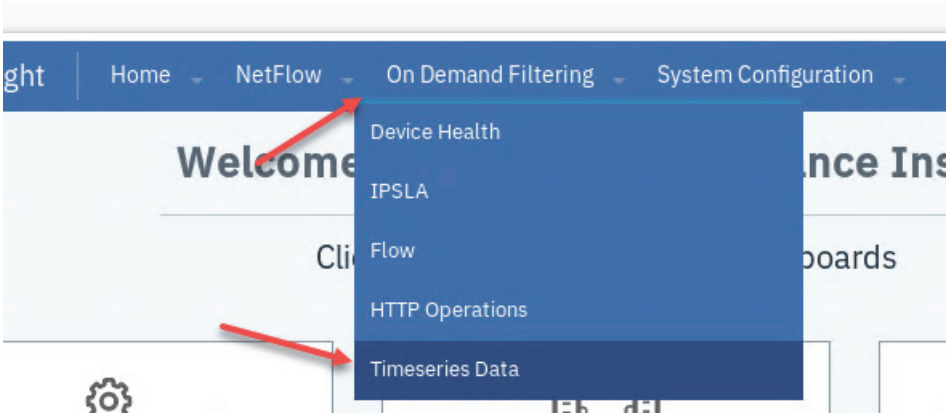
b. Change the KPI to **RTT (ms)**. This metric shows round-trip times for ICMP echoes across network segments.



c. Close the IPSLA dashboard.

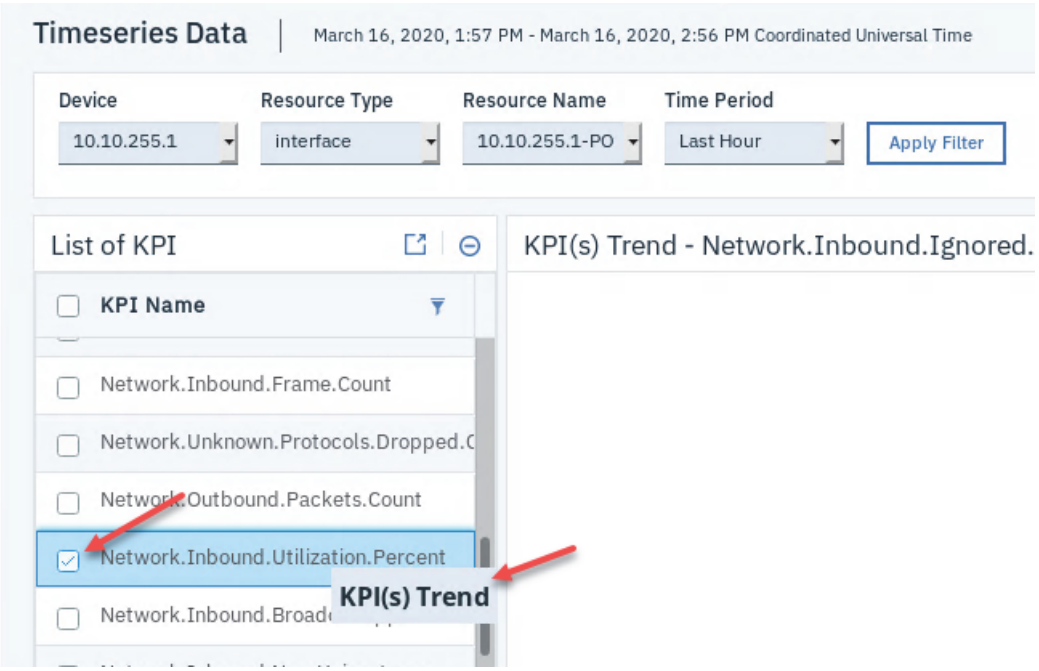


5. Test the time series reports.
   a. Click **On Demand Filtering > Timeseries data**.

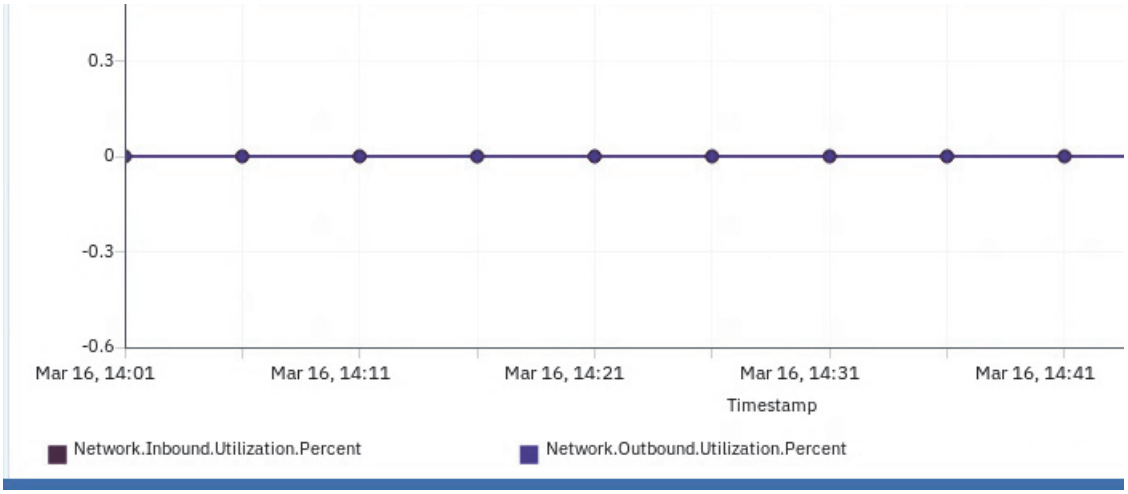


   b. In the list of KPIs on the left, scroll down and select **Network.Inbound.Utilization.Percent** and **Network.Outbound.Utilization.Percent**.

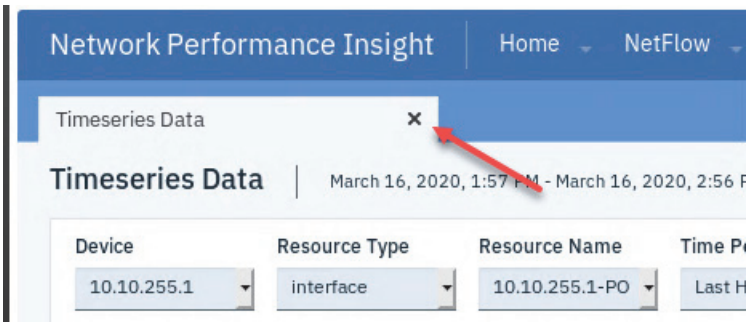
   c. Right-click one of the selected metrics and click **KPI(s) Trend**.



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.

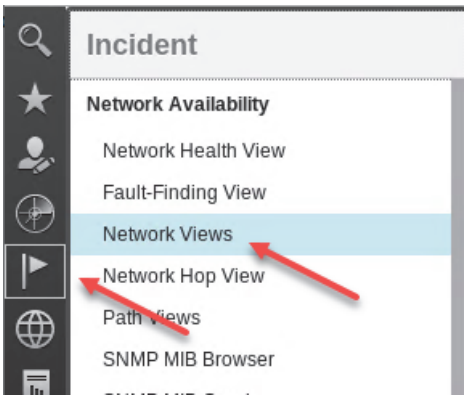


e. Close the **Timeseries Data** tab.



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.

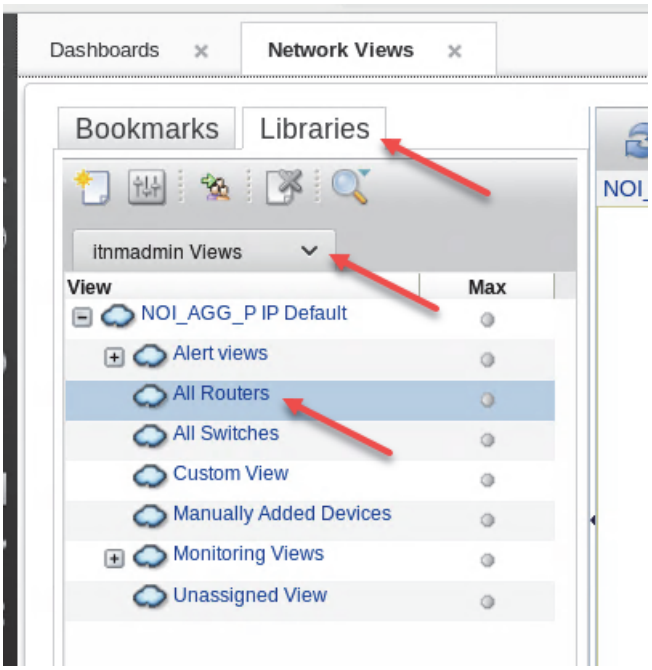
a. Open a network view. Click **Incident > Network Views**.



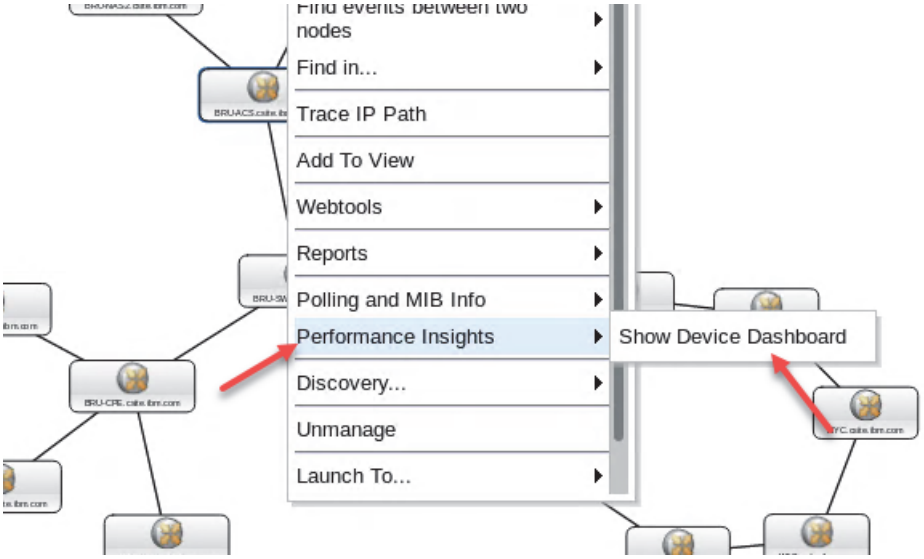
b. Click the **Libraries** tab.

c. Select **itnmadmin Views**.

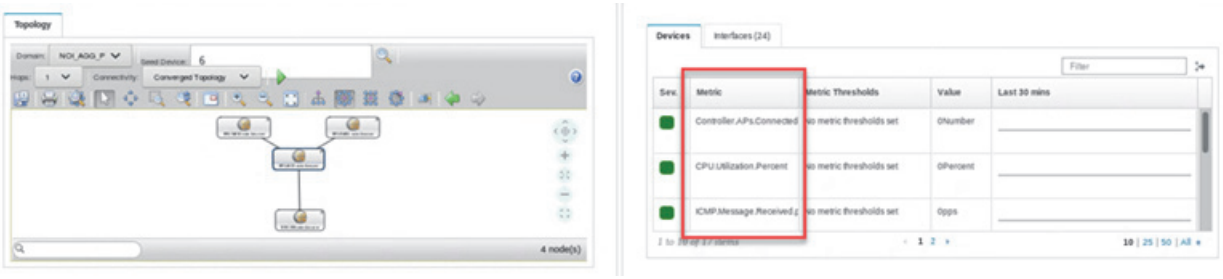
d. Expand **NOI_AGG_P IP Default** and click **All Routers**.



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

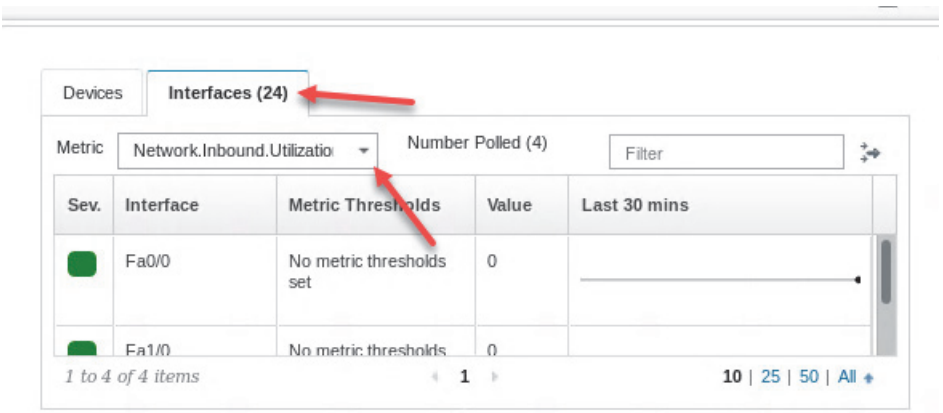


f. Note the list of metrics at the top right of the dashboard. These metrics are coming from Network Performance Insight.

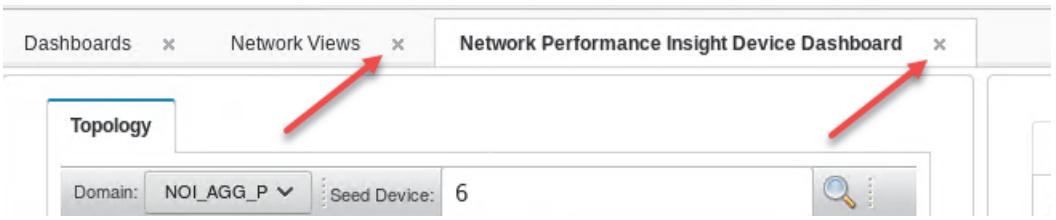


g. Click the **Interfaces** tab.

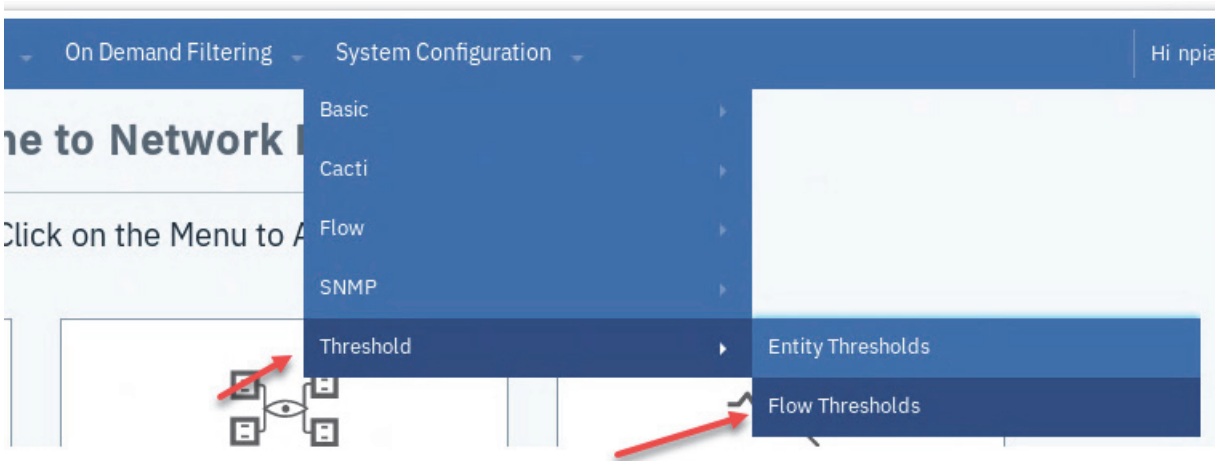
h. Select Network.Inbound.Utilization.Percent as the metric. Scroll down and view the utilization for each interface for the last 30 minutes.



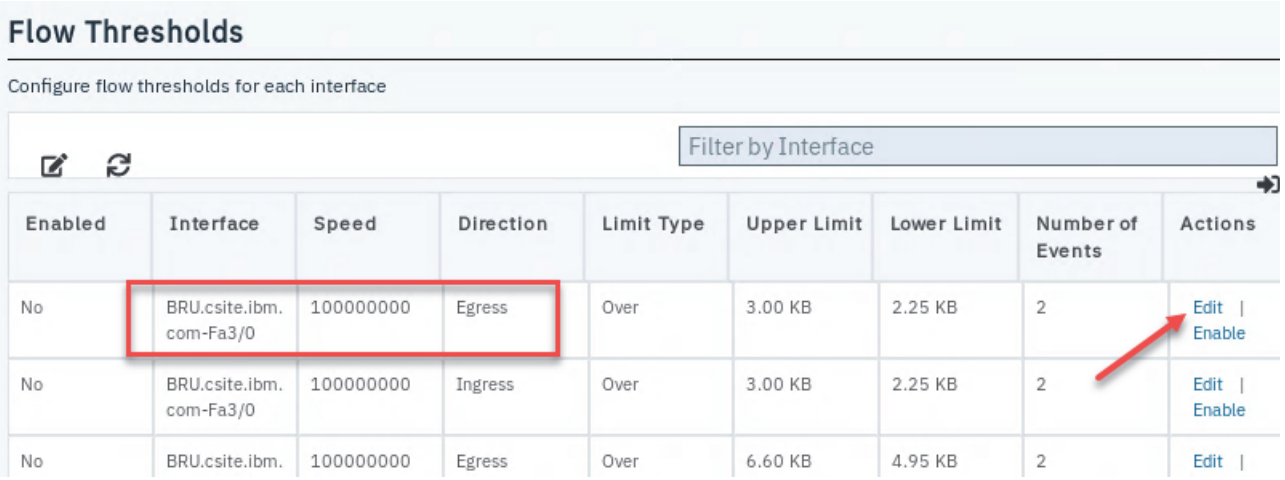
i. Close the **Network Views** and **Device Dashboard** tabs.



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**.

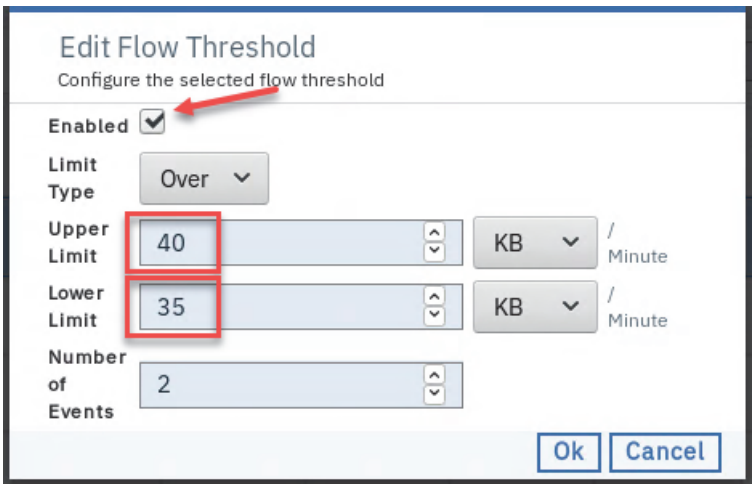


   c. Find the **BRU.csite.ibm.com-Fa3/0** egress interface.
   d. Click **Edit**.



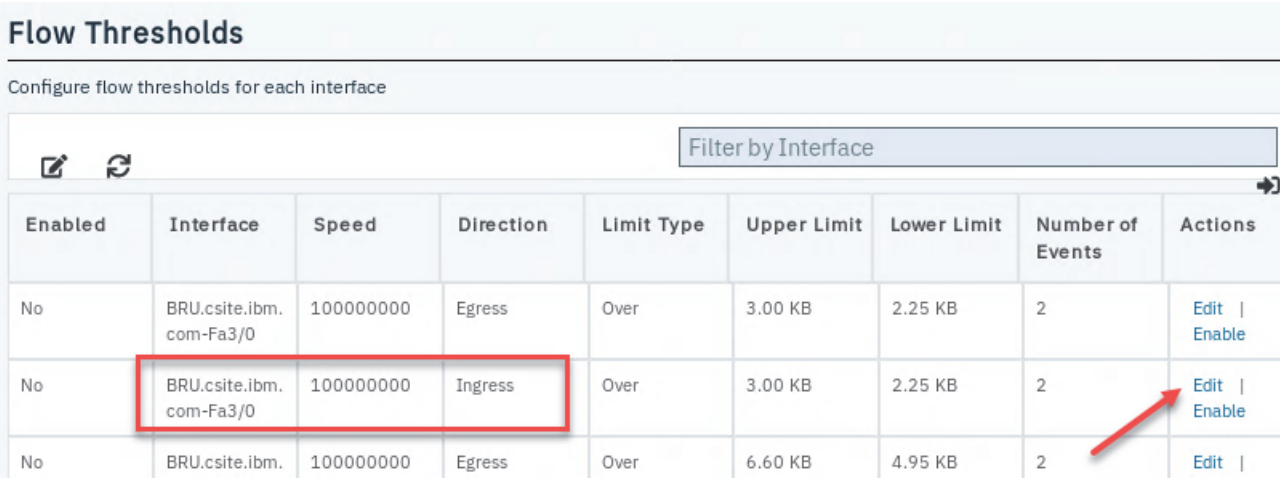
   e. Select **Enabled**.
   f. Enter **40** as the upper limit.
   g. Enter **35** as the lower limit.

h. Click **OK**.



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

j. Click **Edit**.

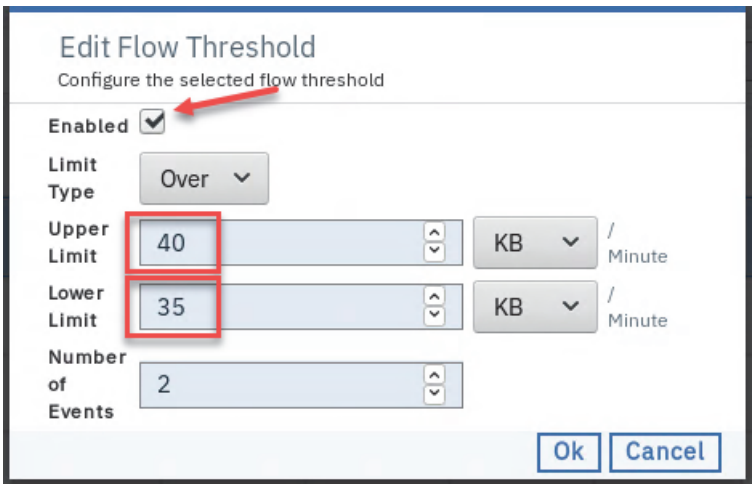


k. Select **Enabled**.

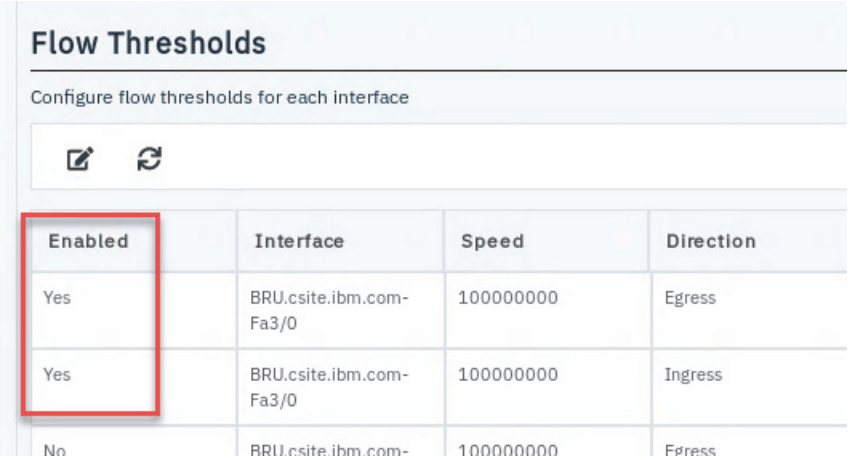
l. Enter **40** as the upper limit.

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

n. Click **OK**.



o. Verify that both thresholds are enabled.



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

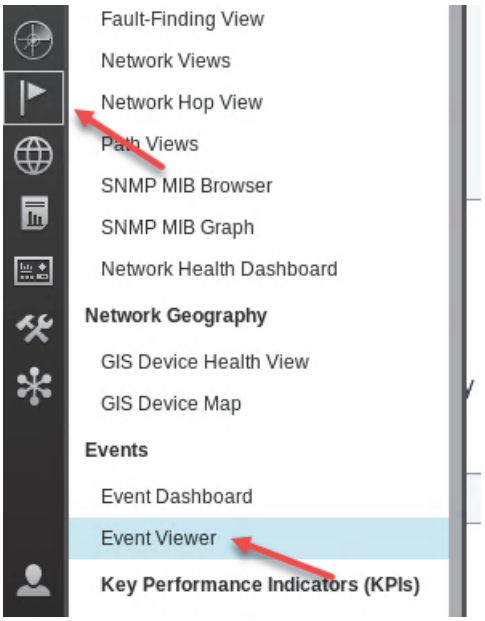
   a. Change to the target directory.

   ```
   /home/netcool/traffic_scripts
   ```

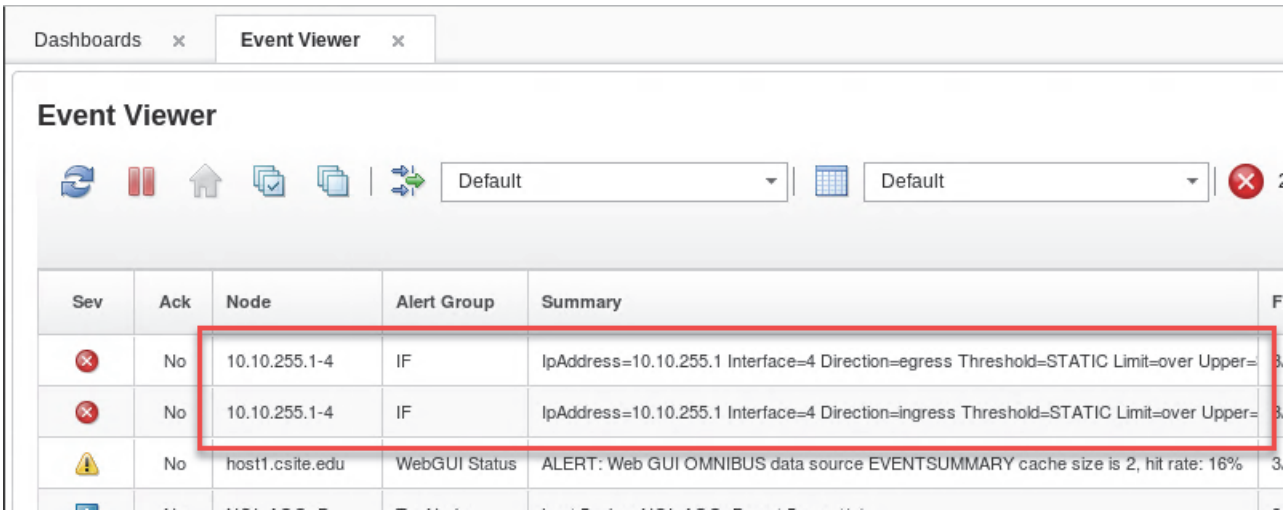
   b. Run the following script to generate traffic.

   ```
   ./http_generate.sh
   ```

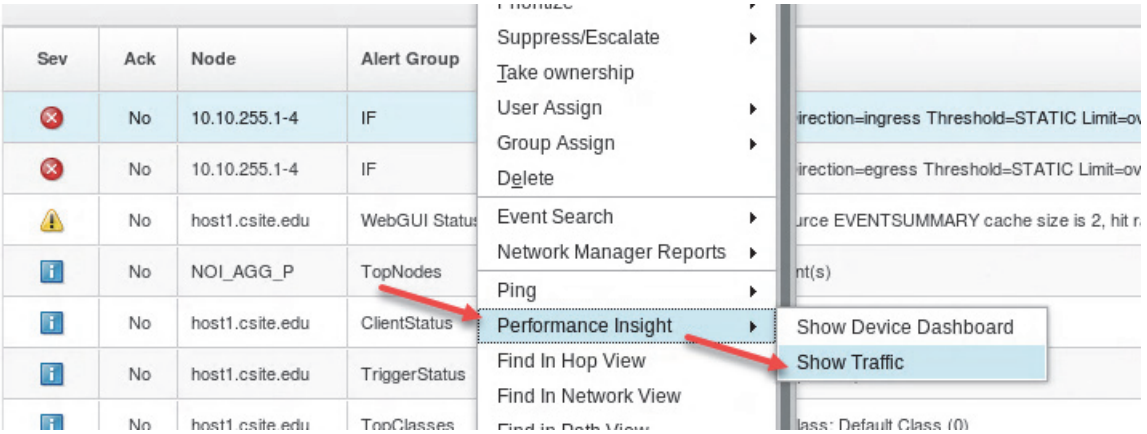
9. When a threshold is violated, IBM Network Performance Insight sends notification to Netcool/OMNIbus. Look at the threshold violation event and investigate the violation with the Traffic Details page.
   a. Open the Netcool/OMNIbus event viewer. Click **Incident > Event Viewer**.



   b. 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.

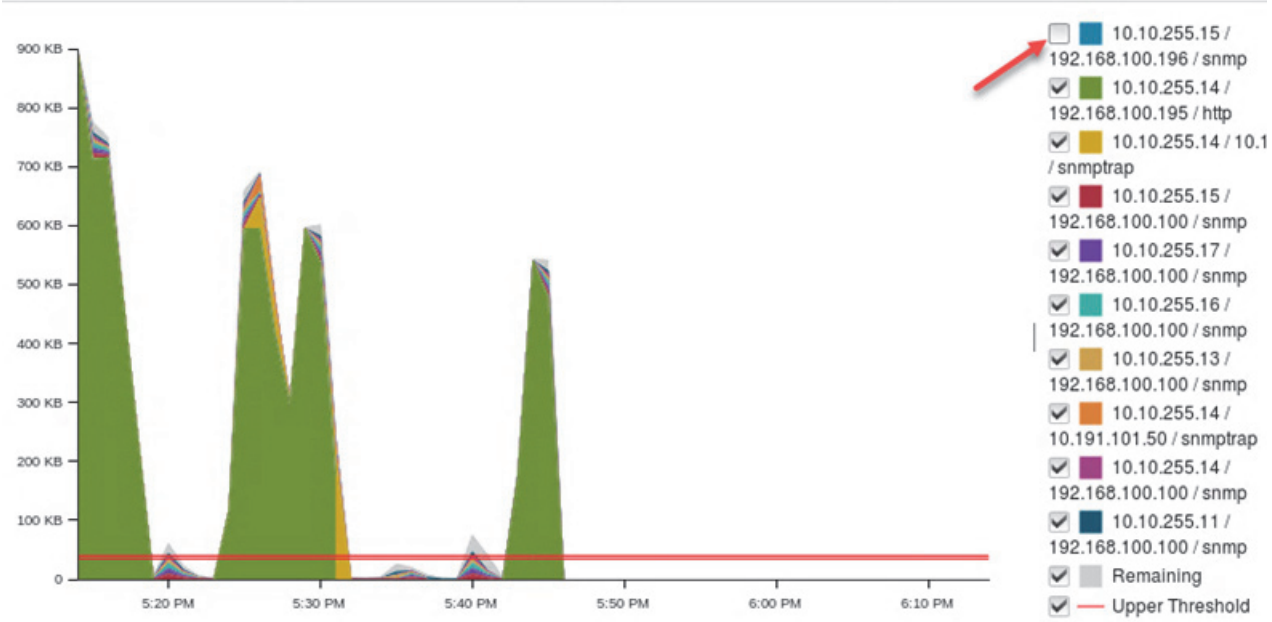


c. Right-click one of the events and click **Performance Insight > Show Traffic**.



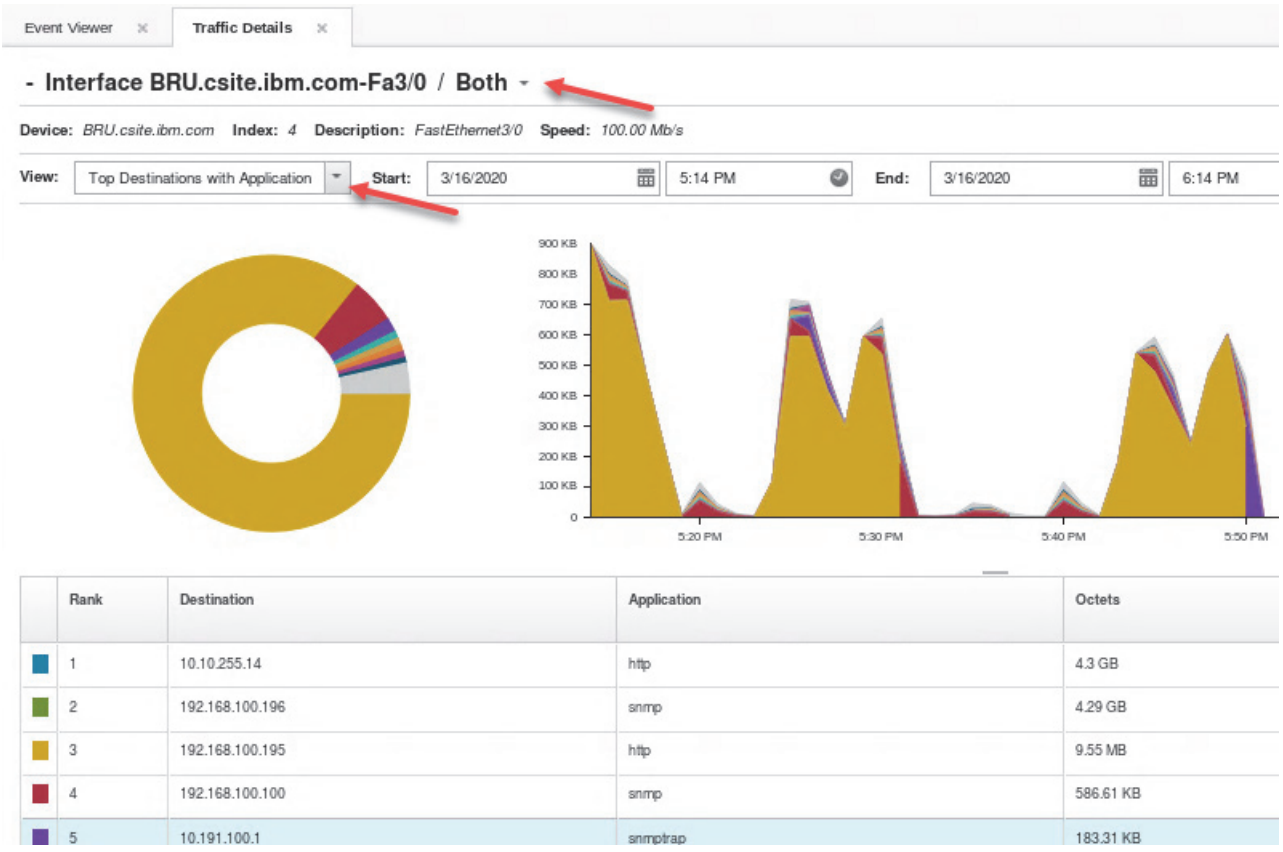
d. The Traffic Details page is displayed, along with the threshold levels. On the right, you can select and deselect different traffic flows and applications for display. This helps you to identify the following attributes of the threshold violation:

- 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