ASSIGNMENT 1
Agent and Management Station

Changtong Zhou (008621223)
Shweta More (009701601)

End-to-End Flow Description

To beginning this assignment, we started off by installing VirtualBox and Ubuntu. This was done by downloading and installing the two software from the websites. Next we installed Net-SNMP on Ubuntu. This was done by adding the `.tar.gz` on the virtual machine under Controller IDE. Next step was to install the management system (OpenNMS), which was done with three quick steps found on the opennms.org website through the virtual machine's terminal.

Agent Configuration

Community (for version 1) – How is it configured?

- Install SNMP and Net-SNMP
  ```
  sudo apt-get install snmpd
  ```

- Backup the default `snmpd.conf` file
  ```
  sudo mv /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak
  ```

- Create a blank `/etc/snmp/snmpd.conf` file with the following information
  ```
  rocommunity public
  ```

- Modify `/etc/default/snmpd`

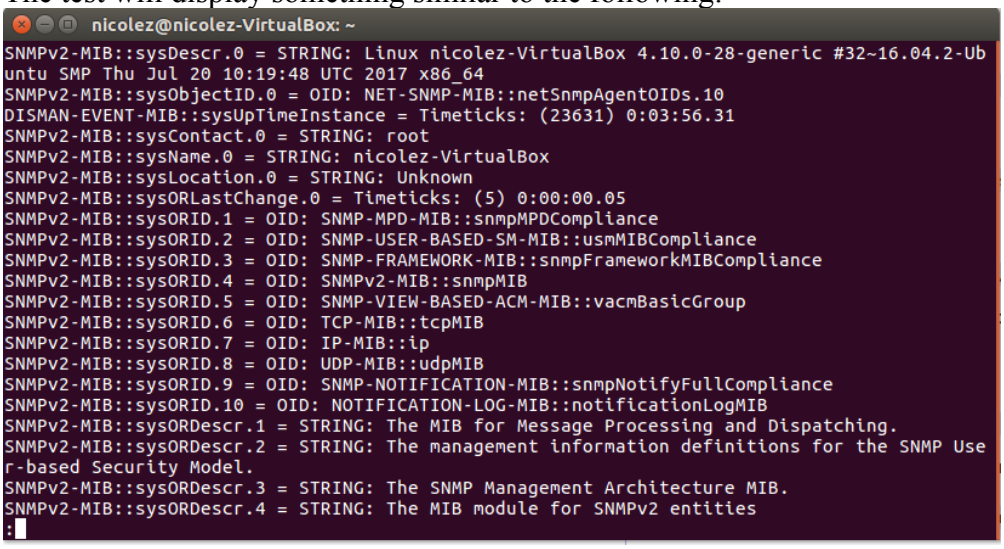
  Change from (or something similar):
  ```
  SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p
  /var/run/snmpd/pid 127.0.01'
  ```

  To:
  ```
  SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p
  /var/run/snmpd/pid 127.0.01'
  SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p
  /var/run/snmpd/pid -c /etc/snmp/snmpd.conf'
  ```

- Restart the SNMP daemon
  ```
  sudo /etc/init.d/snmpd restart
  ```

- Test it out using
  ```
  snmpwalk -c public -v1 localhost | less
  ```

The test will display something similar to the following:



Management Station Configuration

Community (for version 1) – How is it configured?

- After installing OpenNMS, we had to make sure the firewall enables port 8980, which is the default port that OpenNMS runs on. This was done using the following commands:
  `sudo ufw enable`
  `sudo ufw allow 8980`
  `sudo ufw status`

- Do the following to find your localhost address:
  `sudo nano /etc/hosts` (127.0.0.1 was ours)

- Then go to the browser, and http://127.0.0.1:8980/opennms, here you will login using:
  Username: admin
  Password: admin
  (given in the terminal)

Connect OpenNMS to SNMP agent

- On http://127.0.0.1:8980/opennms page:

  Add IP address:
  Admin Configure Discovery Specific IP addresses Add new Type your IP address (e.g. 127.0.0.1), then click Add click Save and Restart Discovery

  Link SNMP (Management Station Community Config):
  Admin Configure SNMP Community Names by IP address First IP address: type your IP address (e.g. 127.0.0.1) Click Save

Display SNMP information:
On Navigation bar click Node List click your saved IP address/Node It will display the information about your SNMP

Polling Rate – How is it configured?

Polling in OpenNMS is controlled by the poller-configuration.xml file, the following snippet shows the look of such file:

```
<poller-configuration threads="30" serviceUnresponsiveEnabled="false" pathOutageEnabled="false">
        <node-outage status="on"
                     pollAllIfNoCriticalServiceDefined="true">
                <critical-service name="ICMP"/>
        </node-outage>
```

The main idea for polling is to check whether the resource is responding properly. Monitors connect to a network resource and perform simples tests to check this. If they fail these tests, events are generated as alerts.

An SNMP counter is used to calculate this rate. SNMP counters can be found in the MIB that is used to measure traffic on a network interface. The MIB will display a total number of octets (bytes) that have travelled in and out of the interface. For instance, if you poll the MIB and see that it sent out 100 octets, then poll it again in 10 minutes and see that it sent out 10,000 octets, you can calculate that within 10 minutes, it sent out 9000 octets.

This can be calculated further through the following:
((9000 * 8) / (10 * 6)) = 120. Therefore, 9,000 octets —> 120 bps

On average, people poll this status every 15 minutes, and poll critical connections every 1-2 minutes.

Data Handling

Storing the data – What tool performs it?

Storing the data on OpenNMS is done using RRDTool, Jrobin or Newts. Data is stored in time series.

Currently data can be collected by: SNMP-collection, NSClinet (the Nagios Agent), JMX, and HTTP.

Visualizing the data – What tool performs it?

For RRD files:

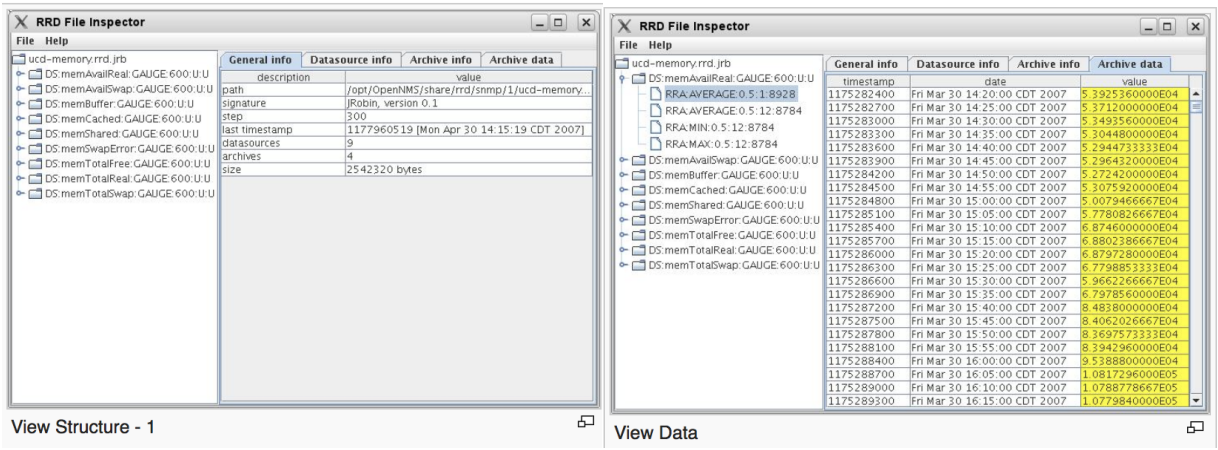
- The stored data will be stored in .rrd and .jrb files.
- To access these files, you will need rrdtool, nodeid
- Go to `/var/opennms/rrd/snmp/nodeid` directory
- Here you will see files ending in .rrd
- To get all the collected files do the following:

```
rrdtool dump RRDfilename
```

For jrobin files:

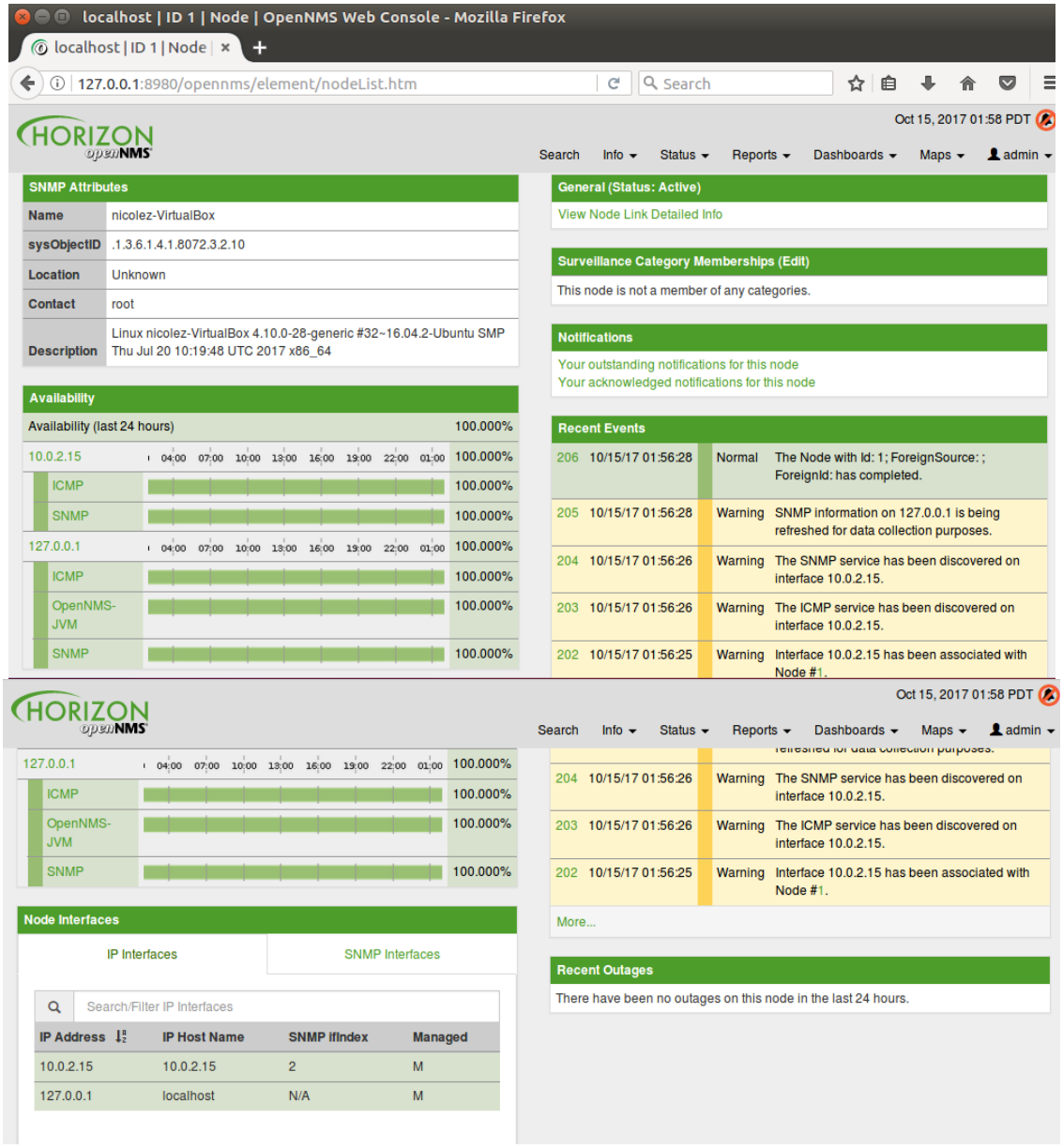
- First dump the collected data by doing the following:
  `echo -e dump multiicmp.jrb\\n . | java -jar $OPENNMS_HOME/lib/jrobin-x.y.z.jar`

- Then run jrobin inspector, which is a gui interface that lets you look at data stored in jrobin files, by doing the following:
  `$OPENNMS_HOME/bin/jrobin-inspector`
  `jrobin-inspector &` (export the display)

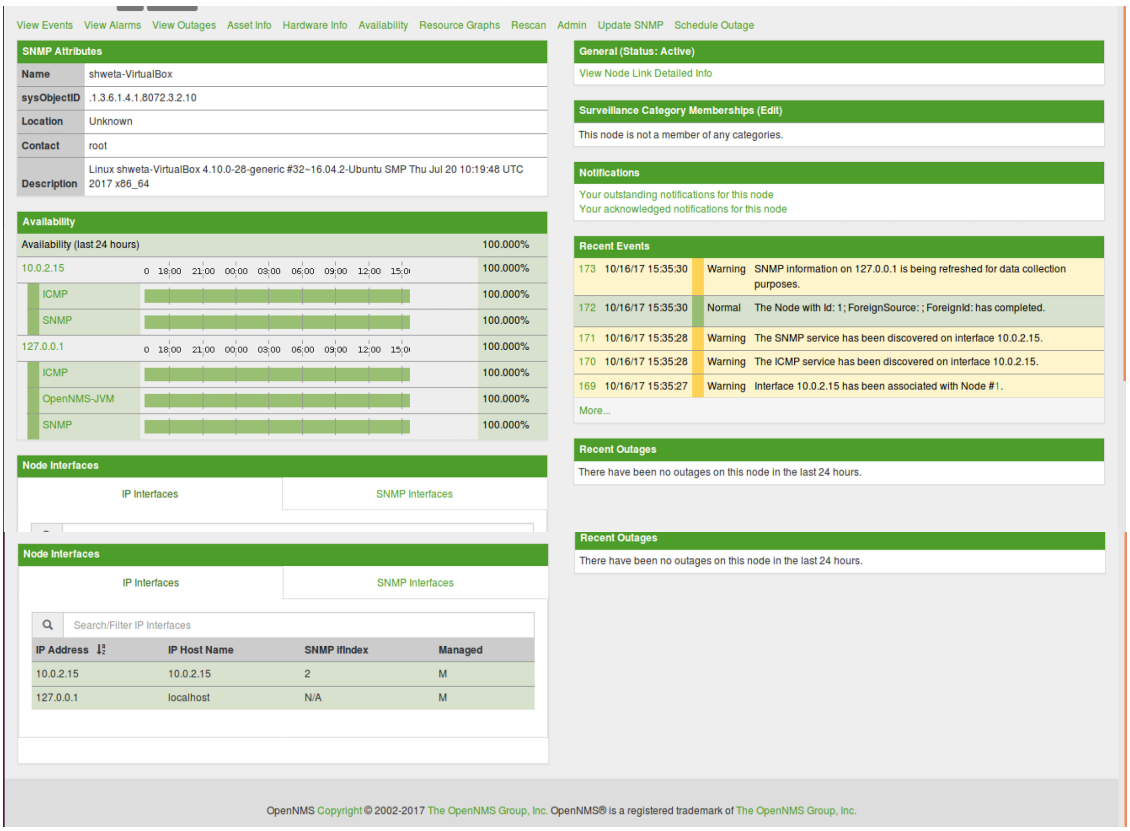


RRD Inspector that displays JRobin RRD Files

Snapshots from Management Station



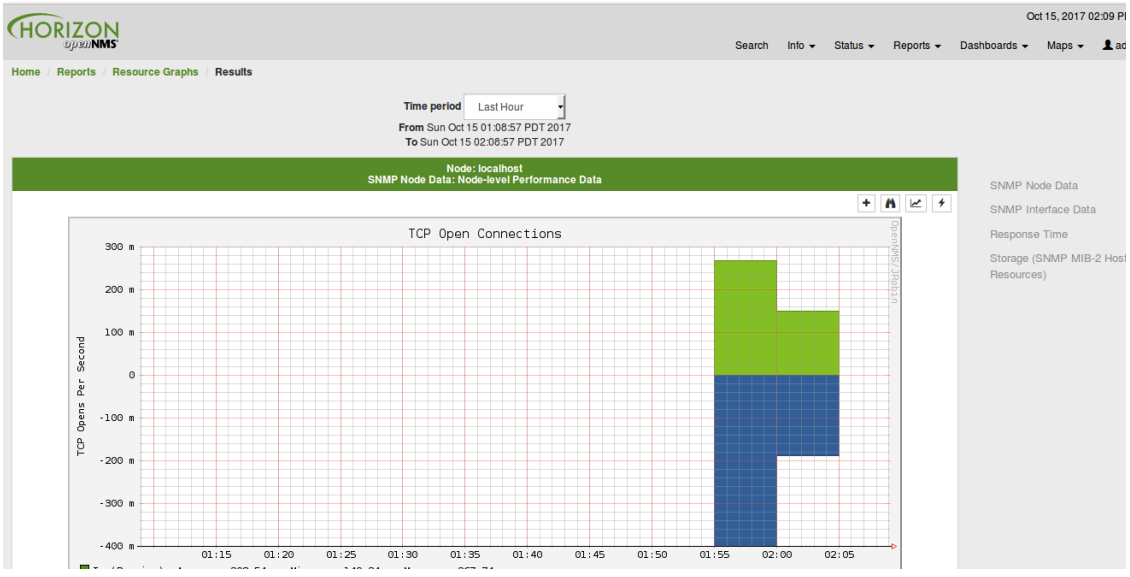
Changtong Zhou (Nicole)'s Management Station

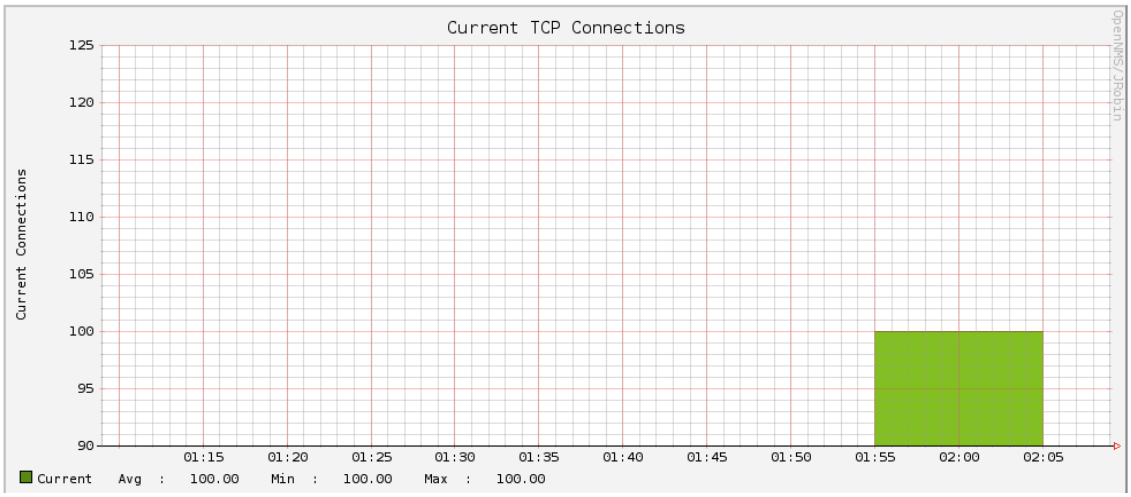


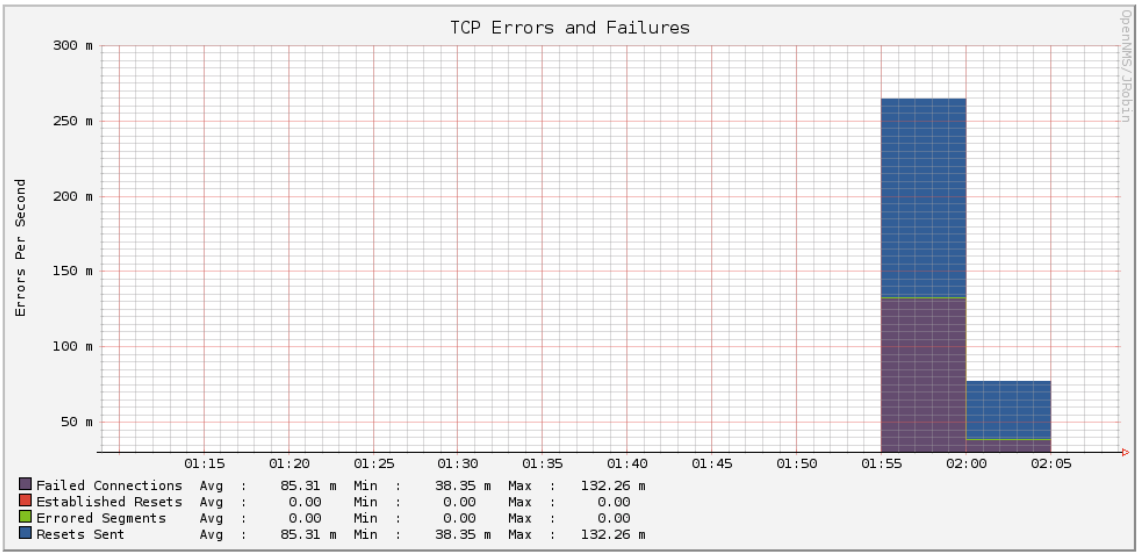
Shweta's Management Station

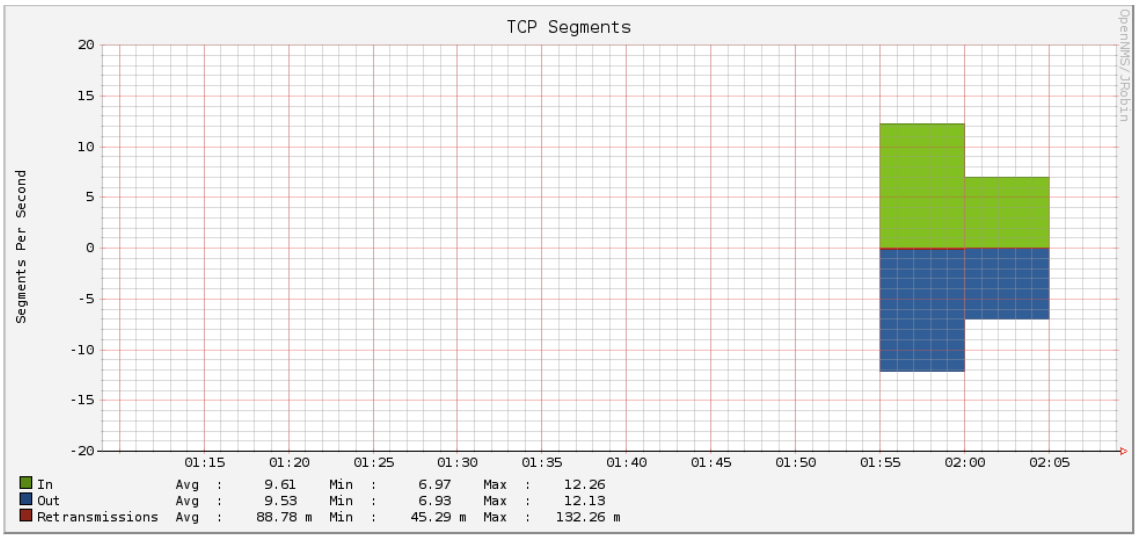
Show Graphic Performances:

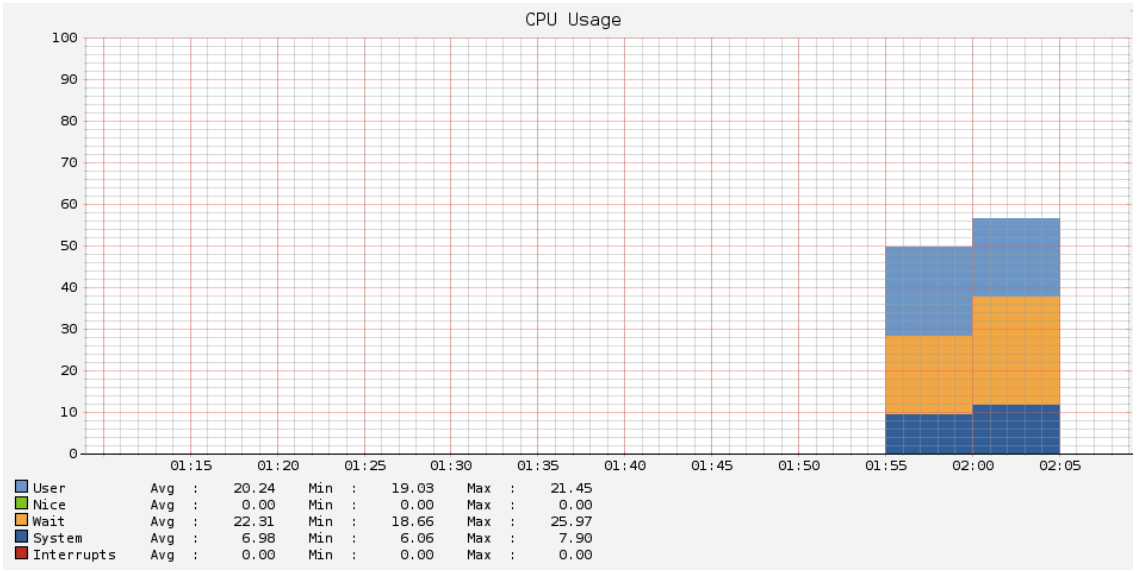
Click Resource Graphics → Graph All

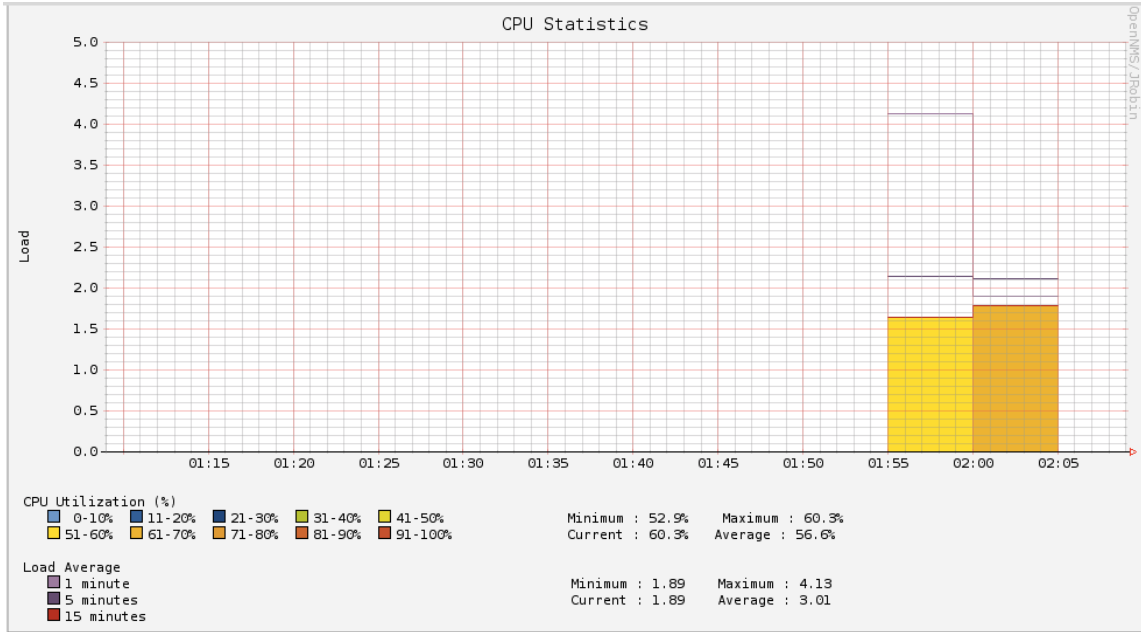



Current TCP Connections
Current Connections
125
120
115
110
105
100
95
90
01:15
01:20
01:25
01:30
01:35
01:40
01:45
01:50
01:55
02:00
02:05
OpenNMS/JRobin
Current Avg : 100.00 Min : 100.00 Max : 100.00


TCP Errors and Failures
Errors Per Second
300 m
250 m
200 m
150 m
100 m
50 m
01:15
01:20
01:25
01:30
01:35
01:40
01:45
01:50
01:55
02:00
02:05
OpenNMS/JRobin
Failed Connections Avg : 85.31 m Min : 38.35 m Max : 132.26 m
Established Resets Avg : 0.00 Min : 0.00 Max : 0.00
Errored Segments Avg : 0.00 Min : 0.00 Max : 0.00
Resets Sent Avg : 85.31 m Min : 38.35 m Max : 132.26 m


TCP Segments
Segments Per Second
20
15
10
5
0
-5
-10
-15
-20
01:15
01:20
01:25
01:30
01:35
01:40
01:45
01:50
01:55
02:00
02:05
OpenNMS/JRobin
In Avg : 9.61 Min : 6.97 Max : 12.26
Out Avg : 9.53 Min : 6.93 Max : 12.13
Retransmissions Avg : 88.78 m Min : 45.29 m Max : 132.26 m


CPU Usage
100
90
80
70
60
50
40
30
20
10
0
01:15
01:20
01:25
01:30
01:35
01:40
01:45
01:50
01:55
02:00
02:05
User Avg : 20.24 Min : 19.03 Max : 21.45
Nice Avg : 0.00 Min : 0.00 Max : 0.00
Wait Avg : 22.31 Min : 18.66 Max : 25.97
System Avg : 6.98 Min : 6.06 Max : 7.90
Interrupts Avg : 0.00 Min : 0.00 Max : 0.00


CPU Statistics
OpenNMS/JRobin
Load
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
01:15
01:20
01:25
01:30
01:35
01:40
01:45
01:50
01:55
02:00
02:05
CPU Utilization (%)
0-10% 11-20% 21-30% 31-40% 41-50%
51-60% 61-70% 71-80% 81-90% 91-100%
Minimum : 52.9% Maximum : 60.3%
Current : 60.3% Average : 56.6%
Load Average
1 minute
5 minutes
15 minutes
Minimum : 1.89 Maximum : 4.13
Current : 1.89 Average : 3.01

Resources

Data handling:
https://wiki.opennms.org/wiki/View_collected_data

Polling rate understanding:
https://thwack.solarwinds.com/community/solarwinds-community/geek-speak_tht/blog/2008/05/20/understanding-snmp-polling-and-counters

Viewing collected data:
https://wiki.opennms.org/wiki/View_collected_data

Net-SNMP:
http://net-snmp.sourceforge.net/wiki/index.php/Net-Snmp_on_Ubuntu
https://sourceforge.net/projects/net-snmp/files/net-snmp/

OpenNMS:
https://www.opennms.org/en/install-debian
https://www.howtoforge.com/tutorial/how-to-install-and-configure-opennms-on-ubuntu-1604

Configuration of SNMP Agent:
http://www.bauer-power.net/2012/10/how-to-configure-snmp-for-ubuntu-in-5.html#.WeKpMxNSxTY

Linking SNMP and MS:
https://www.youtube.com/watch?v=AfWZvDClvNk