

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 127.0.0.1'
```

To:

```
SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p  
/var/run/snmpd/pid 127.0.0.1'  
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:

```
nicolez@nicolez-VirtualBox: ~
SNMPv2-MIB::sysDescr.0 = STRING: Linux nicolez-VirtualBox 4.10.0-28-generic #32~16.04.2-Ub
untu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (23631) 0:03:56.31
SNMPv2-MIB::sysContact.0 = STRING: root
SNMPv2-MIB::sysName.0 = STRING: nicolez-VirtualBox
SNMPv2-MIB::sysLocation.0 = STRING: Unknown
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (5) 0:00:00.05
SNMPv2-MIB::sysORID.1 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORID.6 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.7 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.8 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.9 = OID: SNMP-NOTIFICATION-MIB::snmpNotifyFullCompliance
SNMPv2-MIB::sysORID.10 = OID: NOTIFICATION-LOG-MIB::notificationLogMIB
SNMPv2-MIB::sysORDescr.1 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.2 = STRING: The management information definitions for the SNMP Use
r-based Security Model.
SNMPv2-MIB::sysORDescr.3 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
:
```

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>
</poller-configuration>
```

The main idea for polling is to check whether the resource is responding properly. Monitors connect to a network resource and perform simple 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:

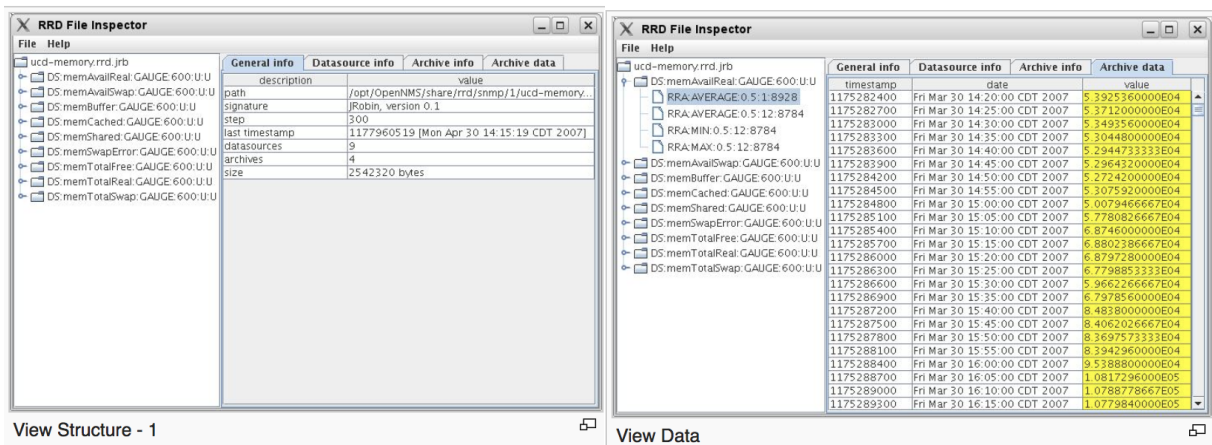
```
rrdtool dump RRDfilename
```

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

The screenshot displays the OpenNMS Horizon web console in a Mozilla Firefox browser. The page shows the configuration and status of a node named 'nicolez-VirtualBox' (ID 1). The interface is divided into several sections:

- SNMP Attributes:** A table listing node details.

Attribute	Value
Name	nicolez-VirtualBox
sysObjectID	.1.3.6.1.4.1.8072.3.2.10
Location	Unknown
Contact	root
Description	Linux nicolez-VirtualBox 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64
- Availability:** A chart showing 100.000% availability for the last 24 hours. Below the chart, a table shows the status of various services for two IP addresses.

IP Address	Service	Status	Availability
10.0.2.15	ICMP	Active	100.000%
	SNMP	Active	100.000%
	OpenNMS-JVM	Active	100.000%
	SNMP	Active	100.000%
127.0.0.1	ICMP	Active	100.000%
	OpenNMS-JVM	Active	100.000%
	SNMP	Active	100.000%
	SNMP	Active	100.000%
- General (Status: Active):** A section with a link to 'View Node Link Detailed Info'.
- Surveillance Category Memberships (Edit):** A message stating 'This node is not a member of any categories.'
- Notifications:** A section for outstanding and acknowledged notifications.
- Recent Events:** A list of events with timestamps and descriptions.

ID	Time	Severity	Message
206	10/15/17 01:56:28	Normal	The Node with id: 1; ForeignSource: ; ForeignId: has completed.
205	10/15/17 01:56:28	Warning	SNMP information on 127.0.0.1 is being refreshed for data collection purposes.
204	10/15/17 01:56:26	Warning	The SNMP service has been discovered on interface 10.0.2.15.
203	10/15/17 01:56:26	Warning	The ICMP service has been discovered on interface 10.0.2.15.
202	10/15/17 01:56:25	Warning	Interface 10.0.2.15 has been associated with Node #1.
- Node Interfaces:** A section with tabs for 'IP Interfaces' and 'SNMP Interfaces'. The 'IP Interfaces' tab is active, showing a table of interfaces.

IP Address	IP Host Name	SNMP ifIndex	Managed
10.0.2.15	10.0.2.15	2	M
127.0.0.1	localhost	N/A	M
- Recent Outages:** A message stating 'There have been no outages on this node in the last 24 hours.'

Changtong Zhou (Nicole)'s Management Station

View Events View Alarms View Outages Asset Info Hardware Info Availability Resource Graphs Rescan Admin Update SNMP Schedule Outage

SNMP Attributes

Name	shweta-VirtualBox
sysObjectID	.1.3.6.1.4.1.8072.3.2.10
Location	Unknown
Contact	root
Description	Linux shweta-VirtualBox 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64

Availability

Availability (last 24 hours) 100.000%

IP Address	ICMP	SNMP	Availability (last 24 hours)
10.0.2.15	100.000%	100.000%	100.000%
127.0.0.1	100.000%	100.000%	100.000%

Node Interfaces

IP Interfaces SNMP Interfaces

Node Interfaces

IP Interfaces SNMP Interfaces

Search/Filter IP Interfaces

IP Address	IP Host Name	SNMP ifIndex	Managed
10.0.2.15	10.0.2.15	2	M
127.0.0.1	localhost	N/A	M

General (Status: Active)

View Node Link Detailed Info

Surveillance Category Memberships (Edit)

This node is not a member of any categories.

Notifications

Your outstanding notifications for this node
Your acknowledged notifications for this node

Recent Events

ID	Time	Severity	Message
173	10/16/17 15:35:30	Warning	SNMP information on 127.0.0.1 is being refreshed for data collection purposes.
172	10/16/17 15:35:30	Normal	The Node with Id: 1; ForeignSource:; ForeignId: has completed.
171	10/16/17 15:35:28	Warning	The SNMP service has been discovered on interface 10.0.2.15.
170	10/16/17 15:35:28	Warning	The ICMP service has been discovered on interface 10.0.2.15.
169	10/16/17 15:35:27	Warning	Interface 10.0.2.15 has been associated with Node #1.

More...

Recent Outages

There have been no outages on this node in the last 24 hours.

Recent Outages

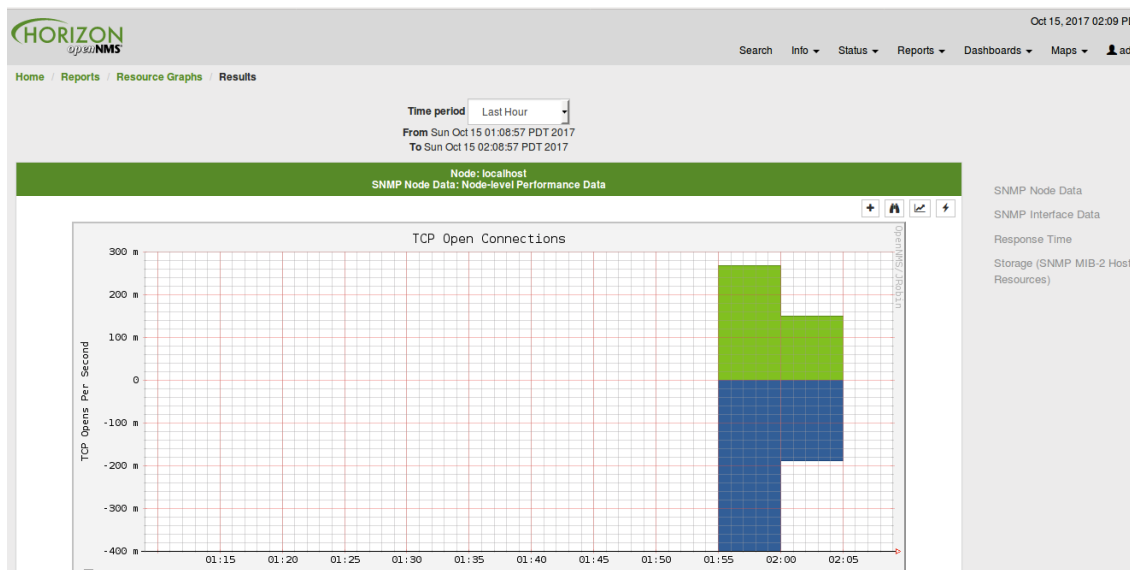
There have been no outages on this node in the last 24 hours.

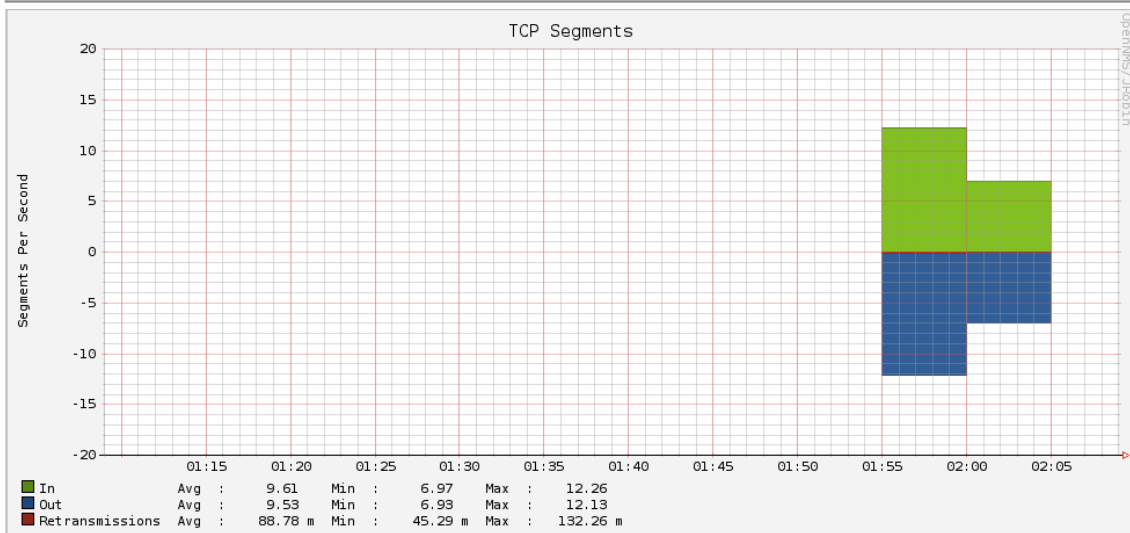
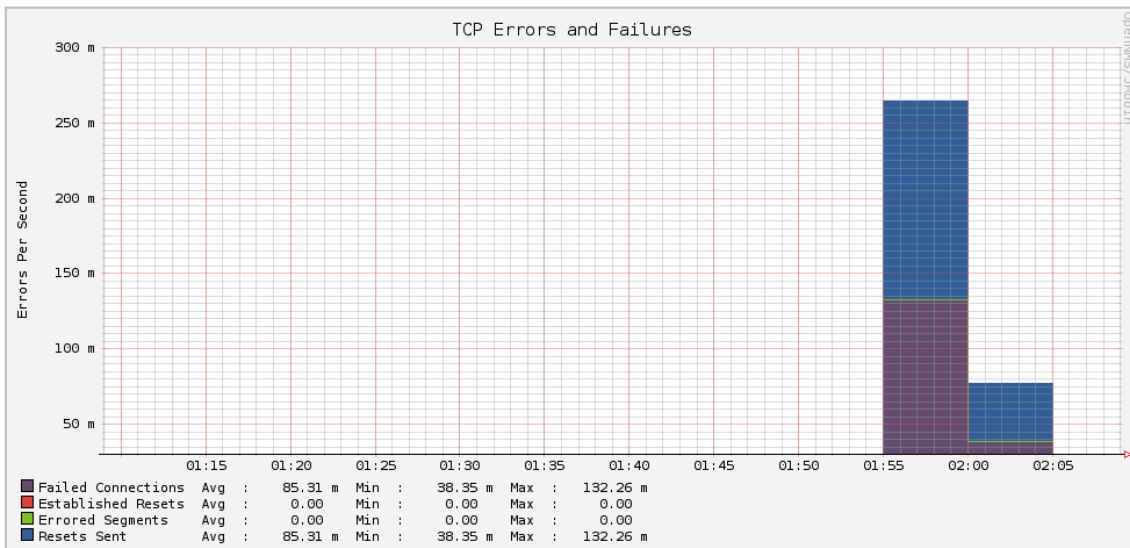
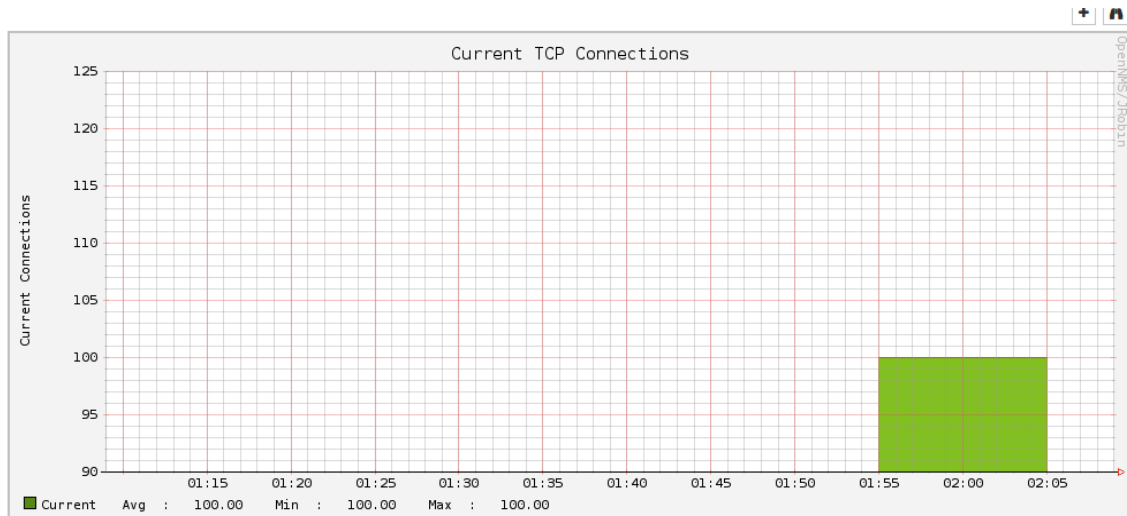
OpenNMS Copyright © 2002-2017 The OpenNMS Group, Inc. OpenNMS® is a registered trademark of The OpenNMS Group, Inc.

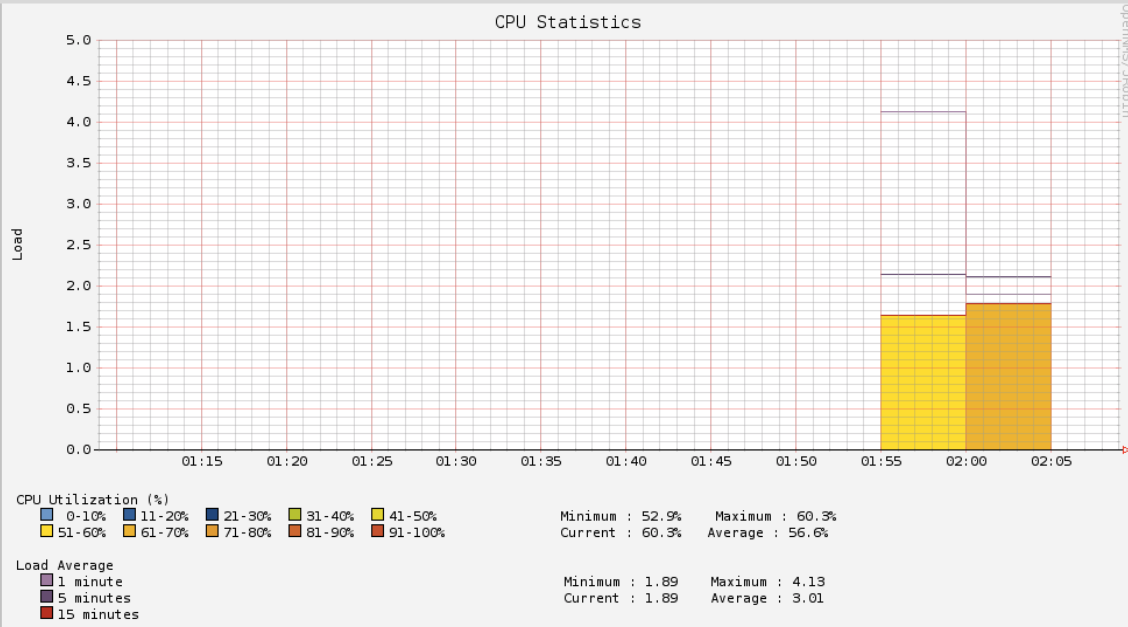
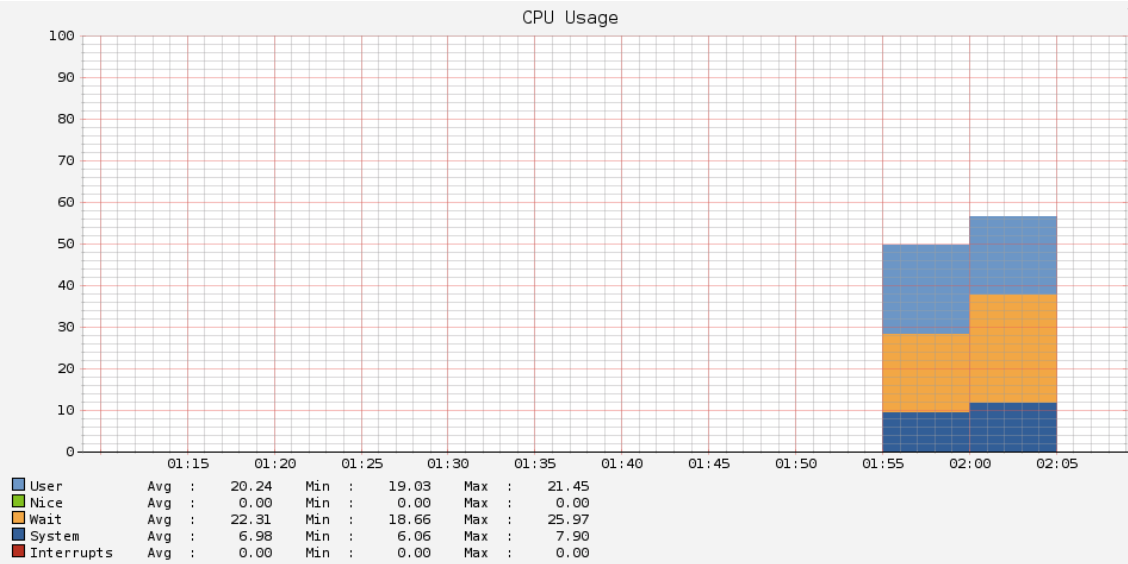
Shweta's Management Station

Show Graphic Performances:

Click Resource Graphics → Graph All







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=AfWZvDCIvNk>