NAGIOS
CS307 - ASSIGNMENT 2

TEAM NUMBER 11

Abhishek Tiwari, B15238
Mamta Bhagia, B15117
Gurmeet Singh, B15114
Deepanshu Tyagi, B15311

NAGIOS OVERVIEW

Nagios is an open source software application, designed for Linux, that monitors systems, networks and infrastructure. Nagios offers monitoring and alerting services for servers, switches, applications and services. It provides monitoring of network services, host resources and hardware which have the ability to send data via a network.
Nagios has various useful plugins like, PnP4Nagios, a data graphing plugin and NRPE, a plugin for monitoring via remotely run scripts.

SNMP

Simple Network Management Protocol is an application-layer protocol used to manage and monitor network devices and their functions. SNMP provides a common language for network devices to relay management information. It is supported on a large range of hardware – from routers, switches to printers scanners and IoT devices.
Components of an SNMP-managed network:
1.SNMP agent: This program runs on the hardware or service being monitored, collecting data about various metrics like bandwidth use or disk space.
2. SNMP-managed devices and resources: These are the nodes on which an agent runs.
3. SNMP manager : This software platform is where all the agents feed their information. The manager requests agents to send data updates at regular intervals. The manager monitors and records the data from the agents.
4. Management information base (MIB): This database is a text file (.mib) that itemizes and describes all objects used by a particular device that can be monitored using SNMP. This database is used to identify and monitor the status of the device's properties. MIB uses a tree

structure to store different objects, and each node(objects) is assigned its object identifier (OID) according to the nodes it has to go through to get to this particular object.

In the assignment, we were to monitor 4 services on 4 hosts.

HOSTS:

- Insite : insite.iitmandi.ac.in : 10.8.1.4
- Students: students.iitmandi.ac.in : 10.8.1.3
- Network: network.iitmandi.ac.in : 10.8.1.5
- Web-Opac: webopac.iitmandi.ac.in : 10.8.1.14

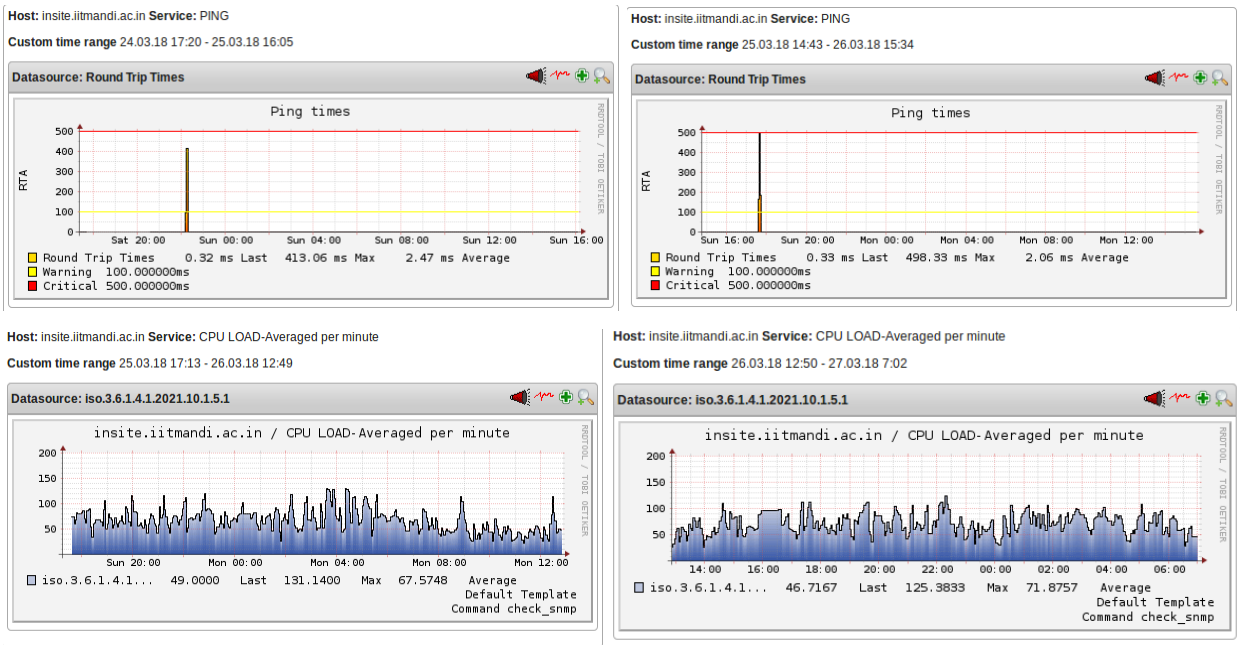
SERVICES:

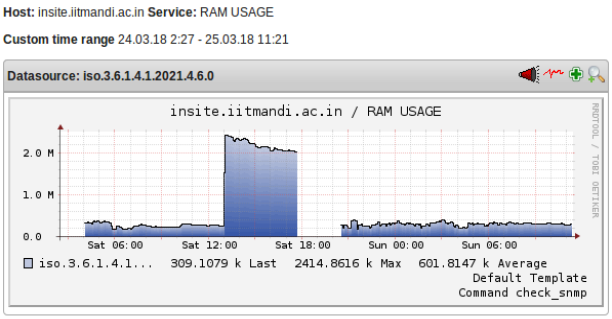
- PING (Round Trip Average time in milliseconds)
  command for ping is predefined in SNMP – check_ping.
- RAM Usage (in kB)
  OID : 1.3.6.1.4.1.2021.4.6.0
- User Load (number of total processes on server)
  OID : 1.3.6.1.2.1.25.1.6.0
- CPU Load (fractional usage)
  OID : 1.3.6.1.4.1.2021.10.1.5.1

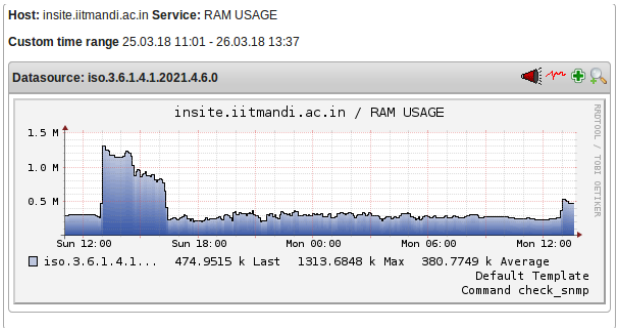
PERFORMANCE DATA GRAPHS:

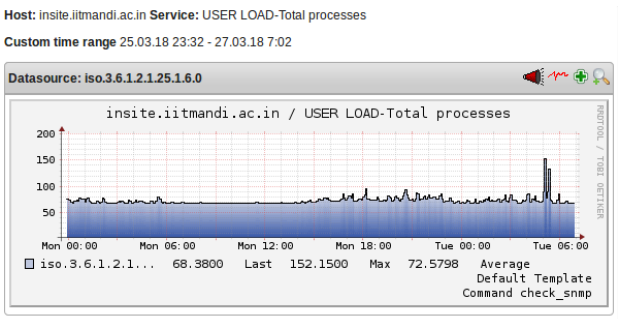
NOTE: The local laptop time in our Nagios server machine is 5 hour and 30 minutes ahead.

INSITE:





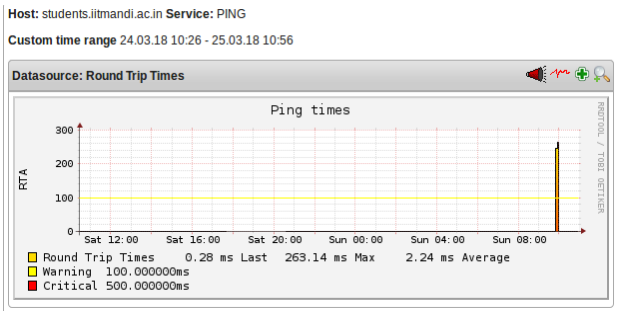


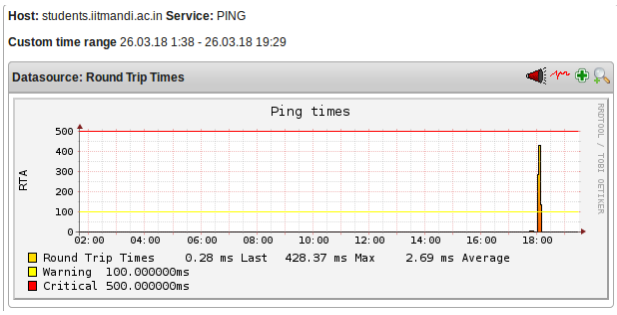


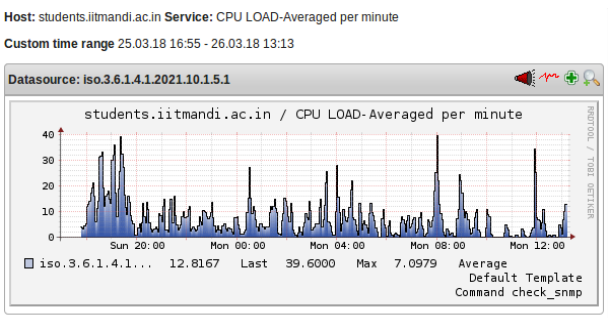
OBSERVATIONS:

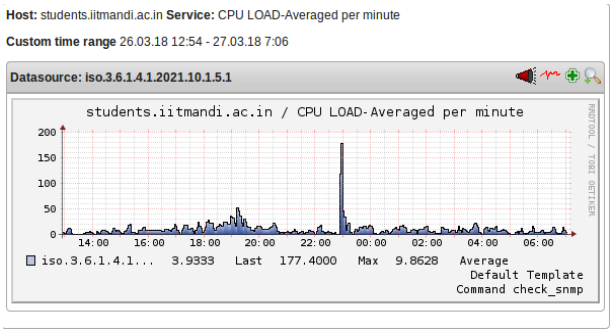
- 0.32 ms is the average round trip ping time, while it shoots up to 413ms on Saturday evening and again shoots up to 498ms on Sunday afternoon, around 3:30pm. This could simply be because of some Wifi problems at those times. Since we are monitoring insite, it has to be a problem within the intra network, not the actual Internet issue.
- The CPU Load averages to 60-70 percent on both days, but we can see a certain drop from 3:30am to 8:30pm, presumably because most students were asleep. Interestingly, the CPU load percentages cross 100 a few times too, which means that the extra load is put in queue, waiting to be run. This could happen due to network congestion.
- RAM usage increases on all days, from 6:30am to 10:30am, which could be some scheduled tasks or checks that have to be run daily. Notice, the break after 12:30pm on Saturday, where usage decreases to zero. This was during a power cut in campus. The same cut can be seen in Ping graphs, on zooming in.
- User Load mostly stays constants with some spikes on Monday night 11:30pm-12:00. This could be attributed to some assignment submissions at 12:00am, making the total number of processes increasing.

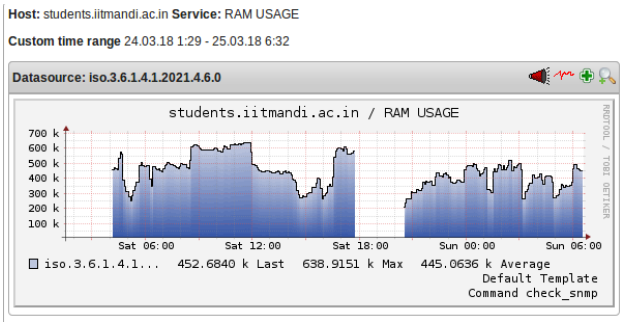
STUDENTS:

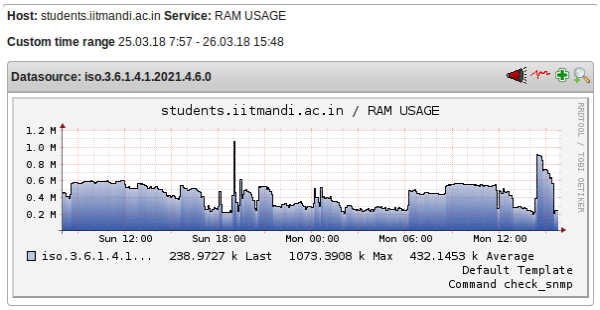


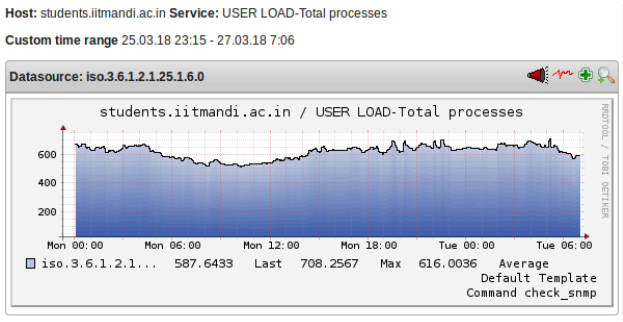










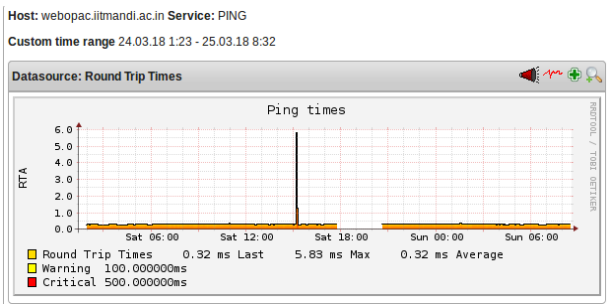


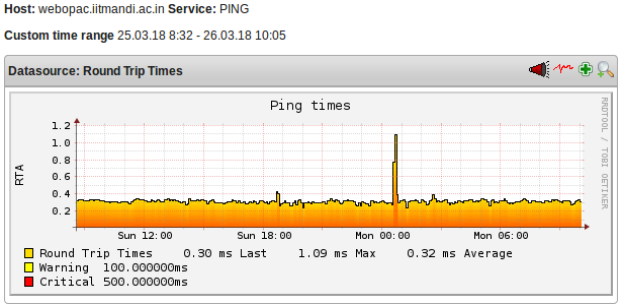
OBSERVATIONS:

- On Monday evening, there was a sudden spike in the CPU Load to 170%, while it varied between 0-40% rest of the time.
- Ping-time increases suddenly on Sunday 4:00am, and 12:30pm on Monday. Generally the ping RTA is about 0.28ms, which is surprisingly lesser than insite's ping RTA.

- RAM Usage is around 600 MB, but it becomes zero(or more appropriately, we get zero results) at 12:30pm on Saturday for a few hours, due to the power cut. This same cut is seen in all server's graphs.
- User Load stays around 500. Since we have monitored user load by monitoring total number of processes, we consider the minimum of the graph to be the total number of system processes. The variations above it are user processes. As expected normally, the user processes, i.e. user load decreases during the night and stays constant during the day.

WEB-OPAC:





OBSERVATIONS:

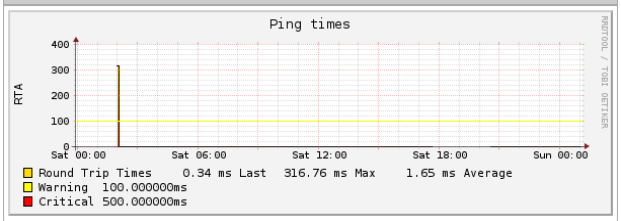
- SNMP is not installed on Web-Opac. Therefore, we get no results for the rest of our monitoring requests, except Ping.
- The ping time graph shows the same break on Saturday at 12:30pm, which was due to the power cut. It also shows two peaks, one on 11:30am on Saturday and one on Sunday 6:30pm.

NETWORK:

Host: network.iitmandi.ac.in **Service:** PING

Custom time range 23.03.18 23:53 - 25.03.18 1:05

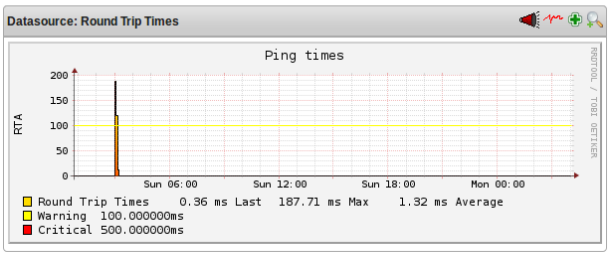
Datasource: Round Trip Times



Host: network.iitmandi.ac.in **Service:** PING

Custom time range 25.03.18 0:45 - 26.03.18 4:03

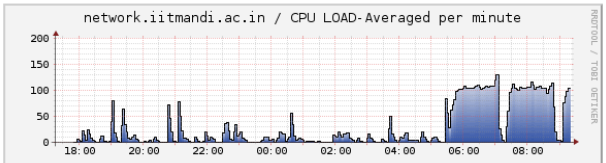
Datasource: Round Trip Times



Host: network.iitmandi.ac.in **Service:** CPU LOAD-Averaged per minute

Custom time range 25.03.18 17:15 - 26.03.18 9:21

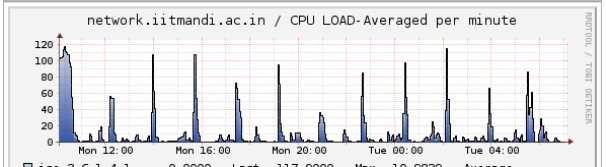
Datasource: iso.3.6.1.4.1.2021.10.1.5.1



Host: network.iitmandi.ac.in **Service:** CPU LOAD-Averaged per minute

Custom time range 26.03.18 10:04 - 27.03.18 7:04

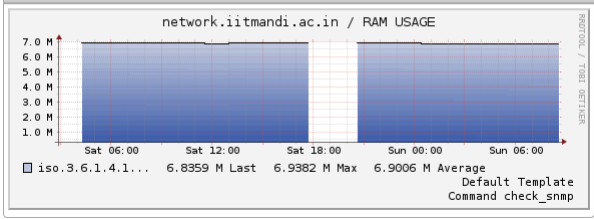
Datasource: iso.3.6.1.4.1.2021.10.1.5.1



Host: network.iitmandi.ac.in **Service:** RAM USAGE

Custom time range 24.03.18 2:50 - 25.03.18 8:35

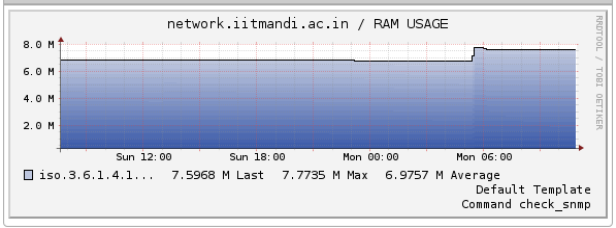
Datasource: iso.3.6.1.4.1.2021.4.6.0



Host: network.iitmandi.ac.in **Service:** RAM USAGE

Custom time range 25.03.18 7:35 - 26.03.18 10:53

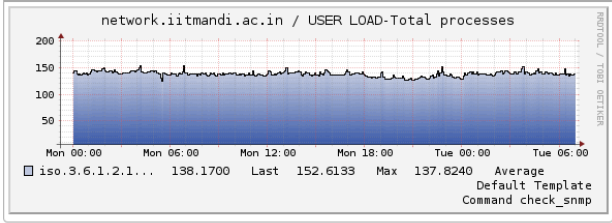
Datasource: iso.3.6.1.4.1.2021.4.6.0



Host: network.iitmandi.ac.in **Service:** USER LOAD-Total processes

Custom time range 25.03.18 23:13 - 27.03.18 7:04

Datasource: iso.3.6.1.2.1.25.1.6.0



OBSERVATIONS:

- Ping again gives on peak per day, around 2-3:00am in the night. Rest of the time, the RTA is around 0.34ms.

- CPU Load averages to 5% but there is a peak on Sunday night, from 12:00am to 5:00am approximately, which could be weekly checks/tasks that run on IIT Mandi's Nagios.
- RAM Usage doesn't show much changes, except for the break on Saturday afternoon, around 12:30pm due to the power cut. RAM Usage averages to 6GB, which is, and should be much more than the RAM Usage of any of the other servers, since Nagios IIT Mandi runs various queries repeatedly and stores this frequent data in RAM.
- Total processes graph shows a constant curve, which means, there are only system processes, and not much of user processes. Or, the user processes are also running consistently, so we are unable to separate the two.

NRPE IMPLEMENTATIONS:

SNMP and NRPE are two different approaches for network monitoring each having their specific purpose where one is preferred over other.

How to monitor services using NRPE:

On Remote Host:

1.Install NRPE plugin

2.In the remote host edit the file /etc/xinetd.d/nrpe and add the ip-address of monitoring server:

only_from = 127.0.0.1 localhost 10.8.18.55

3.In the /etc/services specify port 5666 for NRPE

nrpe 5666/tcp

4.Add iptable rule (if you have a restricted network) for accepting packets with destination port 5666

sudo iptables -I INPUT -p tcp --dport 5666 -j ACCEPT

5.Restart xinetd service

sudo service xinetd restart

On Monitoring Server:

1.Install NRPE plugin

2.Execute /usr/local/nagios/libexec/check_nrpe to monitor various services

./check_nrpe -H 10.8.8.7 -c check_users

REFERENCES:

- http://www.linux-admins.net/2012/02/linux-snmp-oids-for-cpumemory-and-disk.html
- http://www.debianadmin.com/linux-snmp-oids-for-cpumemory-and-disk-statistics.html
- https://www.naemon.org/documentation/usersguide/addon-pnp-quickstart.html
- https://docs.pnp4nagios.org/pnp-0.6/config
- https://www.tecmint.com/how-to-add-linux-host-to-nagios-monitoring-server/