Vivekanand Education Society's

Institute of Technology

An Autonomous Institute Affiliated to University of Mumbai,, Approved by AICTE & Recognized by Govt. of Maharashtra

Hashu Advani Memorial Complex, Collector Colony, Chembur East, Mumbai - 400074.

Department of Information Technology

A.Y. 2024-25

Advance DevOps Lab
Experiment 10

Aim: To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

Roll No.	42
Name	NAIKWADI YASH SHIVDAS
Class	D15B
Subject	Advance DevOps Lab
LO Mapped	LO1: To understand the fundamentals of Cloud Computing and be fully proficient with Cloud based DevOps solution deployment options to meet your business requirements. LO5: To use Continuous Monitoring Tools to resolve any system errors (low memory, unreachable server etc.) before they have any negative impact on the business productivity.
Grade:	

AIM : To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

THEORY :

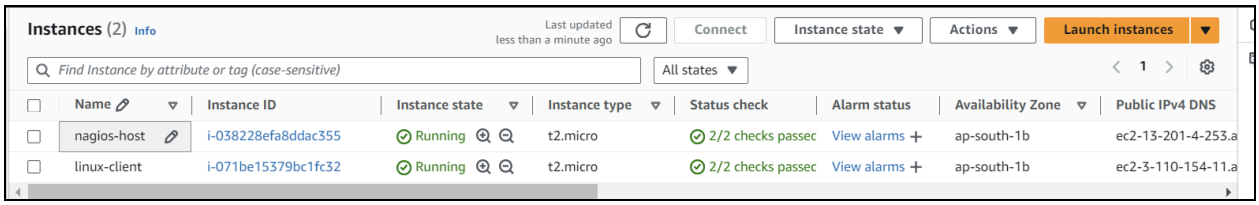
Port and Service Monitoring:
Port and service monitoring is essential in maintaining the performance and security of a network. Ports are communication endpoints for various services running on a machine, and monitoring them ensures that critical services like SSH, HTTP, and others are active and functioning properly. Service monitoring tracks the status and availability of different services to ensure uninterrupted operations.

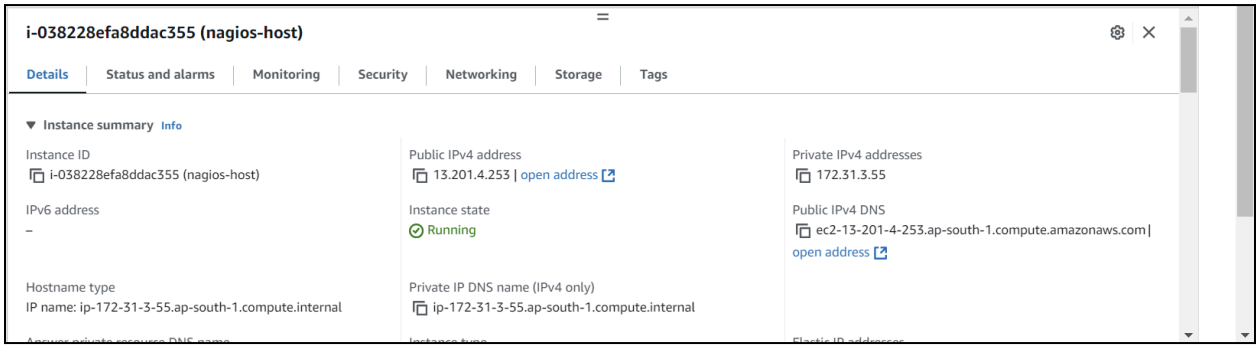
Nagios and NRPE:
Nagios is an open-source tool used for monitoring servers, networks, and infrastructure. It can detect system failures and performance issues, making it vital for real-time monitoring. NRPE (Nagios Remote Plugin Executor) extends Nagios' capabilities by enabling monitoring of remote Linux/Windows servers. It allows the Nagios server to execute monitoring scripts (plugins) on remote machines to gather data about system health, services, and ports.

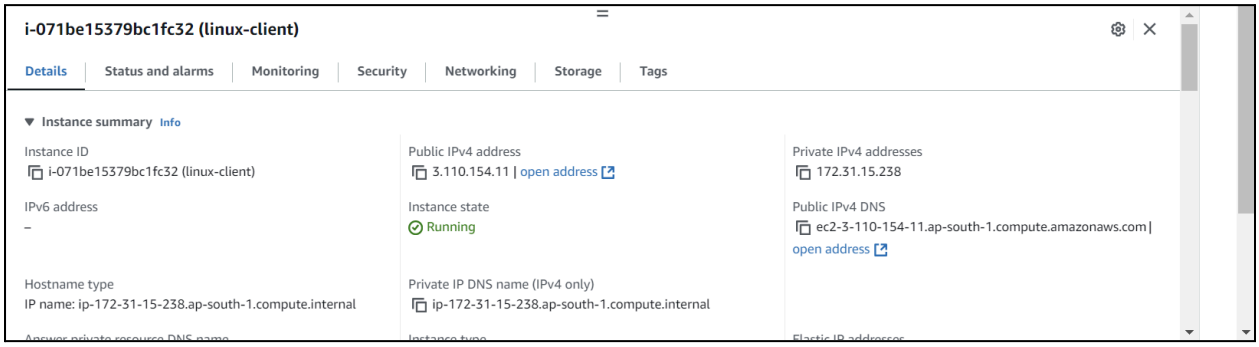
Windows and Linux Server Monitoring:
Monitoring Windows and Linux servers is crucial in both large and small IT environments. Each server's health, including CPU usage, memory, disk space, and running services, must be constantly tracked to prevent downtimes. Nagios can be set up to monitor servers across platforms, offering insights into specific system parameters such as swap usage, active processes, and running ports, helping to avoid system overload or failures.

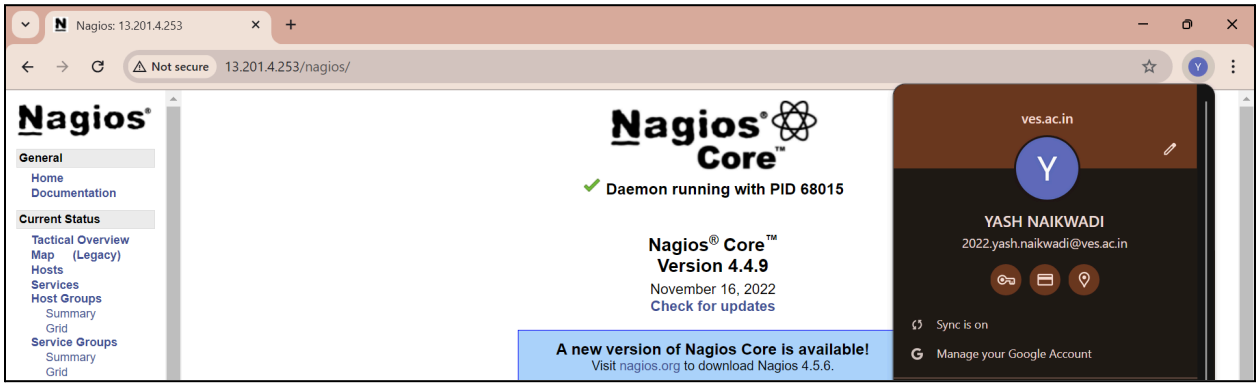
Ports and Services Monitored:
- SSH (Port 22): Monitored for secure remote access to the server.
- HTTP (Port 80): Monitored to check the availability of web servers and their services.
- Services Monitoring: Apart from ports, Nagios helps monitor key server services like user status, system load, total processes, and the state of critical system partitions (e.g., root partition).

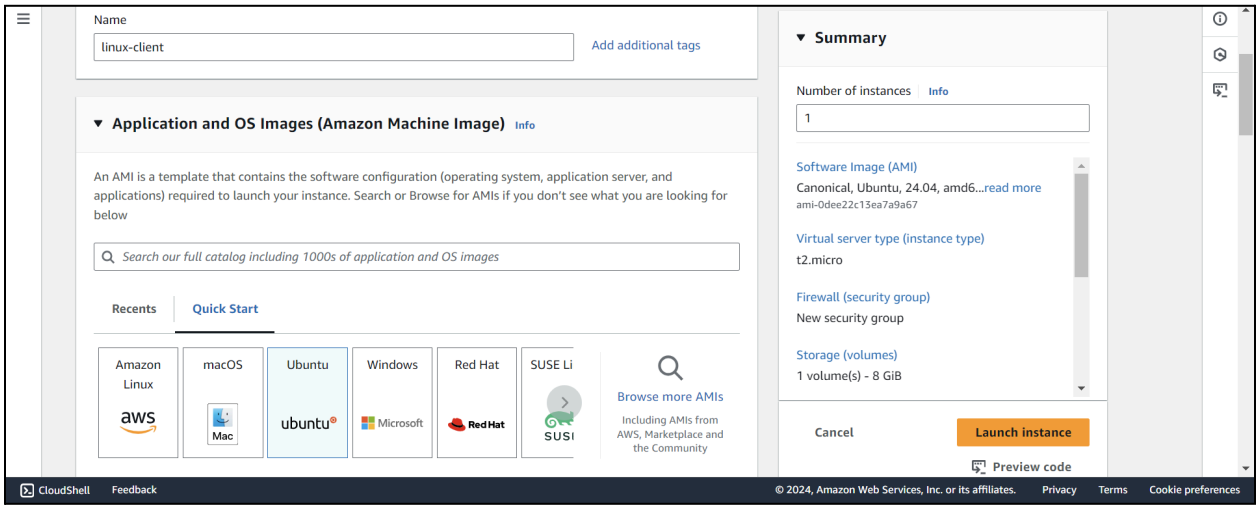
Alerts and Notifications:
Nagios, along with NRPE, continuously monitors these parameters and sends alerts to administrators when thresholds are breached or if a service is down. This proactive approach enables quick resolution before an issue escalates, minimizing system downtime and performance degradation.

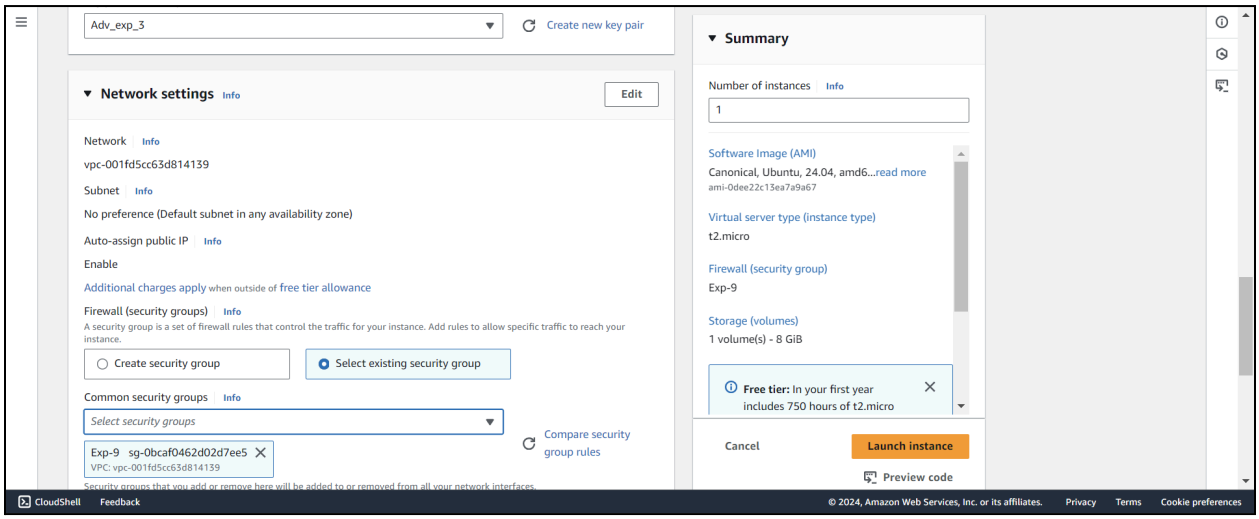

Instances (2) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
nagios-host
i-038228efa8ddac355
Running
t2.micro
2/2 checks passed
View alarms
ap-south-1b
ec2-13-201-4-253.a
linux-client
i-071be15379bc1fc32
Running
t2.micro
2/2 checks passed
View alarms
ap-south-1b
ec2-3-110-154-11.a


i-038228efa8ddac355 (nagios-host)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-038228efa8ddac355 (nagios-host)
Public IPv4 address
13.201.4.253 | open address
Private IPv4 addresses
172.31.3.55
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-13-201-4-253.ap-south-1.compute.amazonaws.com | open address
Hostname type
IP name: ip-172-31-3-55.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-172-31-3-55.ap-south-1.compute.internal


i-071be15379bc1fc32 (linux-client)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-071be15379bc1fc32 (linux-client)
Public IPv4 address
3.110.154.11 | open address
Private IPv4 addresses
172.31.15.238
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-3-110-154-11.ap-south-1.compute.amazonaws.com | open address
Hostname type
IP name: ip-172-31-15-238.ap-south-1.compute.internal
Private IP DNS name (IPv4 only)
ip-172-31-15-238.ap-south-1.compute.internal


Nagios: 13.201.4.253
Not secure
13.201.4.253/nagios/
Nagios
General
Home
Documentation
Current Status
Tactical Overview
Map (Legacy)
Hosts
Services
Host Groups
Summary
Grid
Service Groups
Summary
Grid
Nagios Core
Daemon running with PID 68015
Nagios® Core™
Version 4.4.9
November 16, 2022
Check for updates
A new version of Nagios Core is available!
Visit nagios.org to download Nagios 4.5.6.
ves.ac.in
YASH NAIKWADI
2022.yash.naikwadi@ves.ac.in
Sync is on
Manage your Google Account





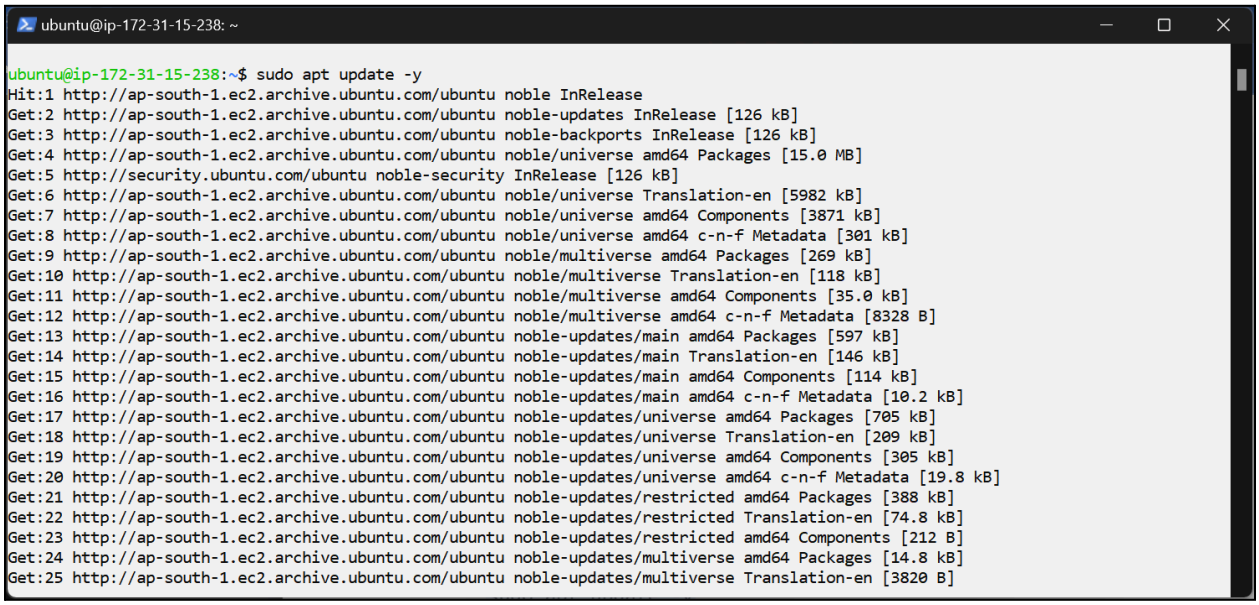
On host:

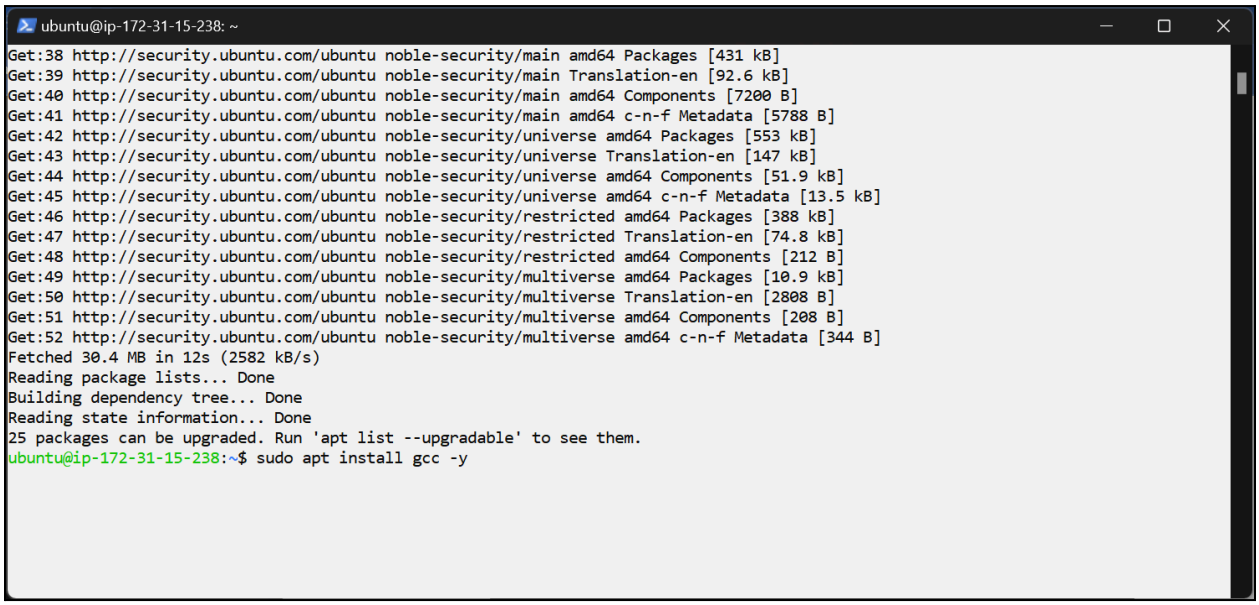
```
Last login: Fri Oct 18 05:18:43 2024 from 171.48.85.204
[ec2-user@ip-172-31-3-55 ~]$  sudo systemctl status nagios
● nagios.service - Nagios Core 4.4.9
     Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Fri 2024-10-18 04:58:29 UTC; 35min ago
       Docs: https://www.nagios.org/documentation
    Process: 68013 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
    Process: 68014 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
   Main PID: 68015 (nagios)
      Tasks: 6 (limit: 1112)
     Memory: 6.9M
        CPU: 742ms
     CGroup: /system.slice/nagios.service
             ├─68015 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─68016 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─68017 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─68018 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─68019 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─68020 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 18 05:03:21 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: SERVICE ALERT: localhost;HTTP;WARNING;HARD;4;HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in >
Oct 18 05:03:51 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: SERVICE ALERT: localhost;Swap Usage;CRITICAL;SOFT;2;SWAP CRITICAL - 0% free (0 MB out of 0 MB) - >
Oct 18 05:04:51 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: SERVICE ALERT: localhost;Swap Usage;CRITICAL;SOFT;3;SWAP CRITICAL - 0% free (0 MB out of 0 MB) - >
Oct 18 05:05:51 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: SERVICE NOTIFICATION: nagiosadmin;localhost;Swap Usage;CRITICAL;notify-service-by-email;SWAP CRIT>
Oct 18 05:05:51 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: SERVICE ALERT: localhost;Swap Usage;CRITICAL;HARD;4;SWAP CRITICAL - 0% free (0 MB out of 0 MB) - >
Oct 18 05:05:51 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: wproc: NOTIFY job 4 from worker Core Worker 68016 is a non-check helper but exited with return co>
Oct 18 05:05:51 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: wproc:   host=localhost; service=Swap Usage; contact=nagiosadmin
Oct 18 05:05:51 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: wproc:   early_timeout=0; exited_ok=1; wait_status=32512; error_code=0;
Oct 18 05:05:51 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: wproc:   stderr line 01: /bin/sh: line 1: /bin/mail: No such file or directory
Oct 18 05:05:51 ip-172-31-3-55.ap-south-1.compute.internal nagios[68015]: wproc:   stderr line 02: /usr/bin/printf: write error: Broken pipe
lines 1-28/28 (END)
[ec2-user@ip-172-31-3-55 ~]$
```

```
[ec2-user@ip-172-31-3-55 nagios-plugins-2.0.3]$ ps -ef | grep nagios
nagios     68015       1  0 04:58 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     68016   68015  0 04:58 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68017   68015  0 04:58 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68018   68015  0 04:58 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68019   68015  0 04:58 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68020   68015  0 04:58 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user   70472   70117  0 05:39 pts/2    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-3-55 nagios-plugins-2.0.3]$ _
```

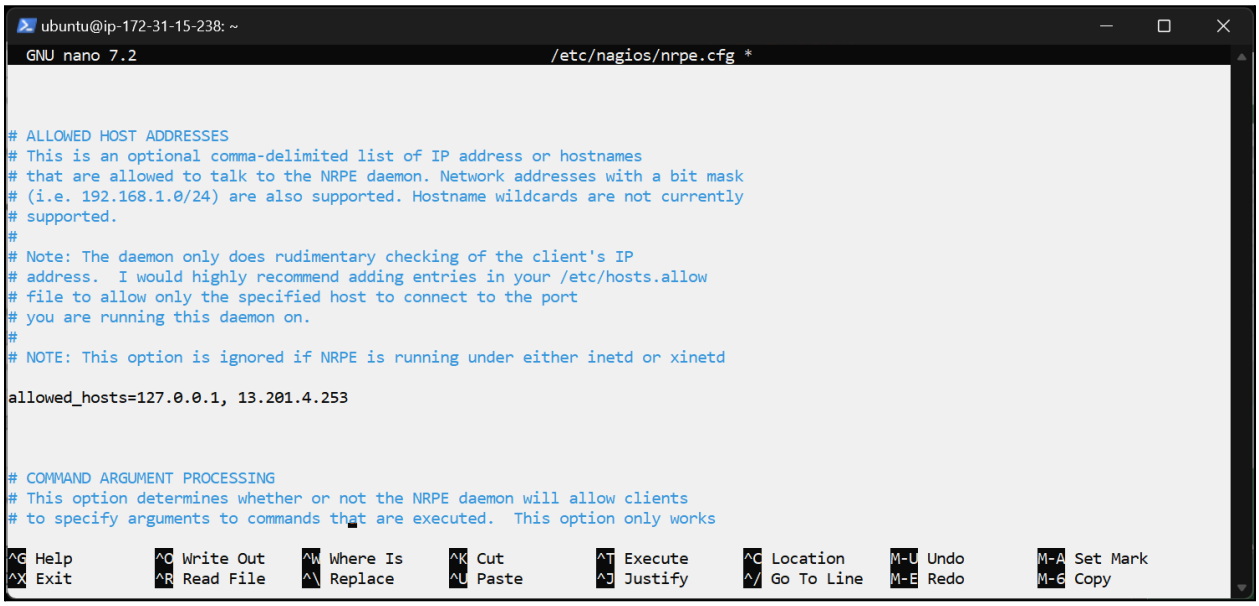
On client:

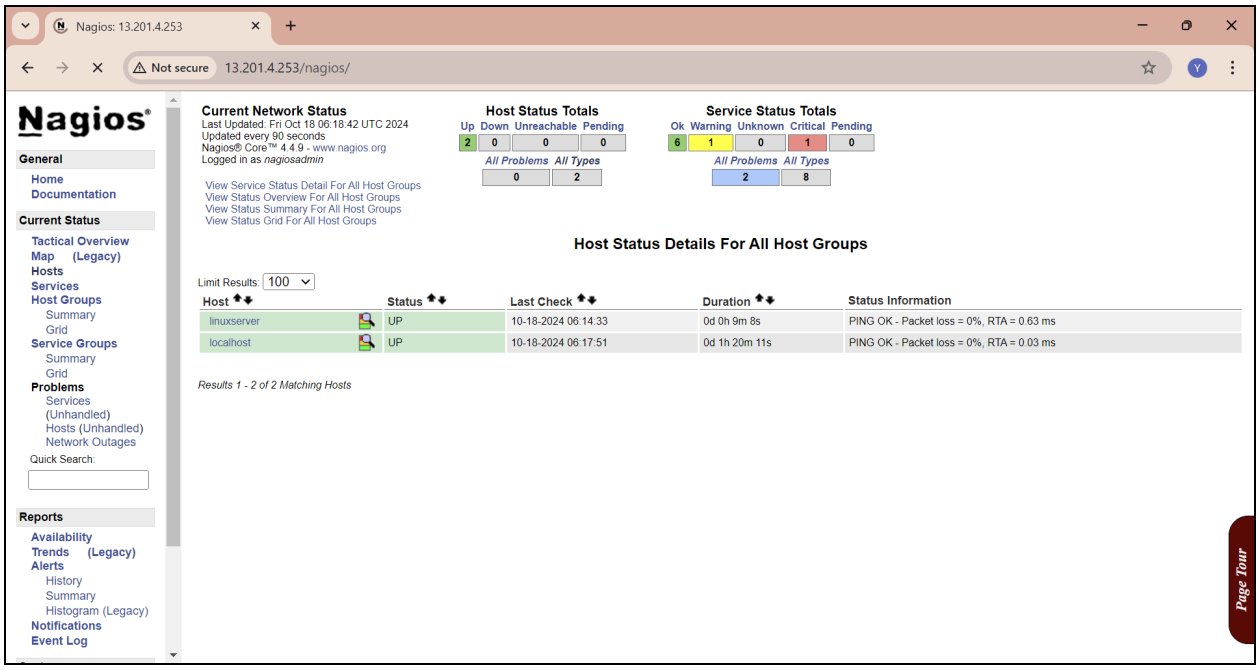

ubuntu@ip-172-31-15-238: ~
ubuntu@ip-172-31-15-238:~$ sudo apt update -y
Hit:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:8 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:9 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:10 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:11 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:12 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:13 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [597 kB]
Get:14 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [146 kB]
Get:15 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [114 kB]
Get:16 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [10.2 kB]
Get:17 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [705 kB]
Get:18 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [209 kB]
Get:19 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [305 kB]
Get:20 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [19.8 kB]
Get:21 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [388 kB]
Get:22 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [74.8 kB]
Get:23 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Get:24 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [14.8 kB]
Get:25 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [3820 B]

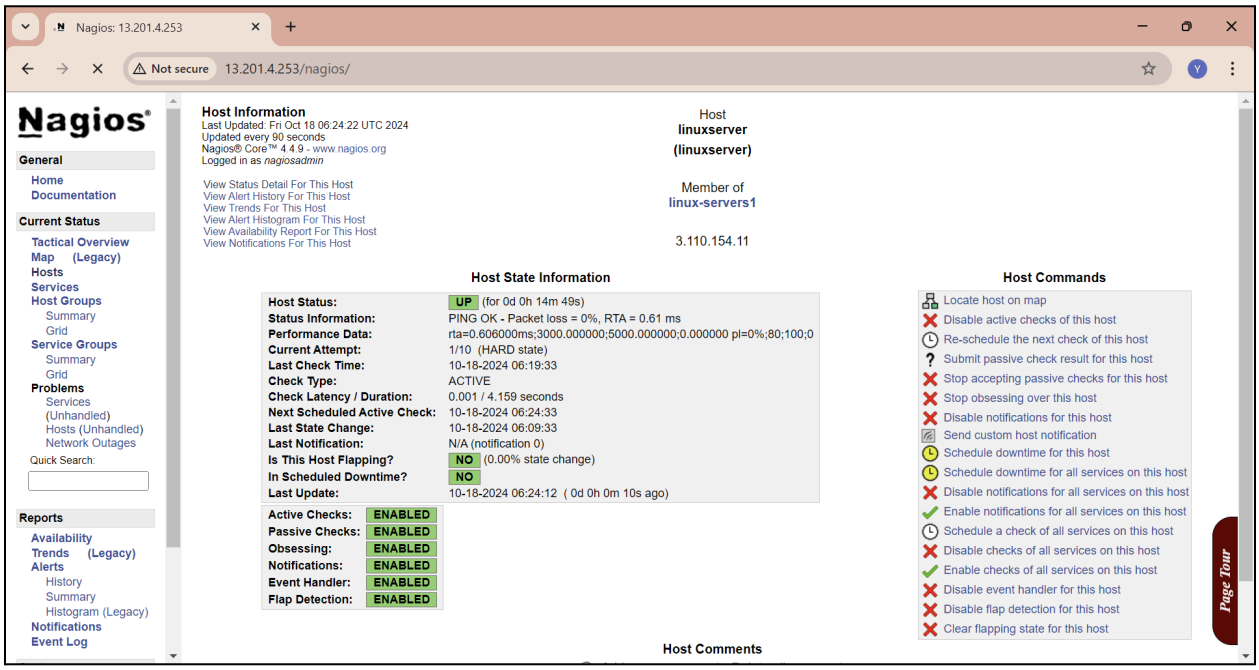

ubuntu@ip-172-31-15-238: ~
Get:38 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [431 kB]
Get:39 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [92.6 kB]
Get:40 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [7200 B]
Get:41 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [5788 B]
Get:42 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [553 kB]
Get:43 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [147 kB]
Get:44 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51.9 kB]
Get:45 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [13.5 kB]
Get:46 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [388 kB]
Get:47 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [74.8 kB]
Get:48 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:49 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [10.9 kB]
Get:50 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [2808 B]
Get:51 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:52 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 c-n-f Metadata [344 B]
Fetched 30.4 MB in 12s (2582 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
25 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-172-31-15-238:~$ sudo apt install gcc -y


ubuntu@ip-172-31-15-238: ~
ubuntu@ip-172-31-15-238:~$ sudo apt install -y nagios-nrpe-server nagios-plugins
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
The following additional packages will be installed:
libavahi-client3 libavahi-common-data libavahi-common3 libcups2t64 libdbi1t64 libldb2 libmysqlclient21 libnet-snmp-perl libpq5
libradcli4 libsmbclient0 libsnmp-base libsnmp40t64 libtalloc2 libtdb1 libtevent0t64 liburiparser1 libwbclient0
monitoring-plugins-basic monitoring-plugins-common monitoring-plugins-standard mysql-common python3-gpg python3-ldb
python3-markdown python3-samba python3-talloc python3-tdb rpcbind samba-common samba-common-bin samba-dsdb-modules samba-libs
smbclient snmp
Suggested packages:
cups-common libcrypt-des-perl libdigest-hmac-perl libio-socket-inet6-perl snmp-mibs-downloader icinga2 nagios-plugins-contrib
fping postfix | sendmail-bin | exim4-daemon-heavy | exim4-daemon-light qstat xinetd | inetd python-markdown-doc heimdal-clients
python3-dnspython cifs-utils
The following NEW packages will be installed:
libavahi-client3 libavahi-common-data libavahi-common3 libcups2t64 libdbi1t64 libldb2 libmysqlclient21 libnet-snmp-perl libpq5
libradcli4 libsmbclient0 libsnmp-base libsnmp40t64 libtalloc2 libtdb1 libtevent0t64 liburiparser1 libwbclient0 monitoring-plugins
monitoring-plugins-basic monitoring-plugins-common monitoring-plugins-standard mysql-common nagios-nrpe-server python3-gpg
python3-ldb python3-markdown python3-samba python3-talloc python3-tdb rpcbind samba-common samba-common-bin samba-dsdb-modules
samba-libs smbclient snmp
0 upgraded, 37 newly installed, 0 to remove and 21 not upgraded.
Need to get 16.1 MB of archives.
After this operation, 72.0 MB of additional disk space will be used.
Get:1 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 nagios-nrpe-server amd64 4.1.0-1ubuntu3 [356 kB]
Get:2 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 rpcbind amd64 1.2.6-7ubuntu2 [46.5 kB]
Get:3 http://ap-south-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libavahi-common-data amd64 0.8-13ubuntu6 [29.7 kB]

```
ubuntu@ip-172-31-15-238:~$ sudo nano /etc/nagios/nrpe.cfg
```







CONCLUSION :

Thus, we learned about port and service monitoring using Nagios and successfully monitored a Linux server. Using Nagios and NRPE, we were able to track server performance and monitor key services and ports effectively.