V.E.S.
Since 1962

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.

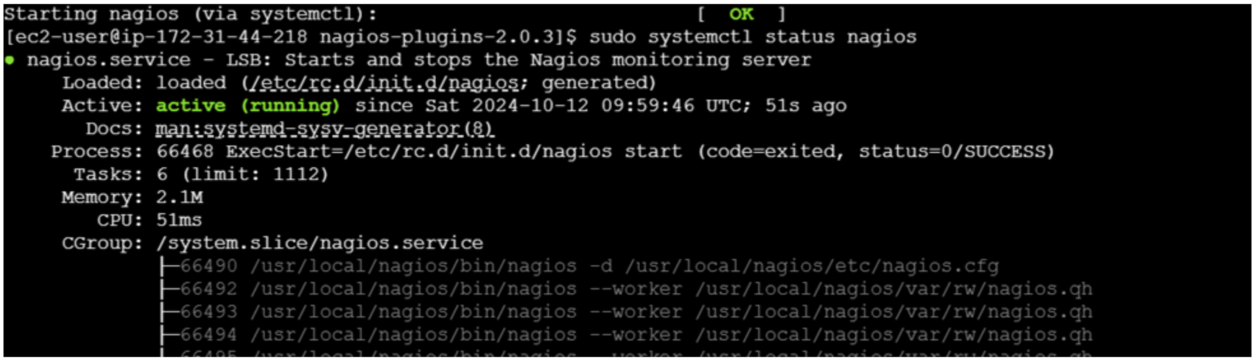
Roll No.	22
Name	Sarthak Harade
Class	D15B
Subject	Advance DevOps Lab
LO Mapped	LO1: To understand the fundamentals of Cloud Computing and be fully proficient with Cloud based DevOps solution deployment options to meet your business requirements. LO5: To use Continuous Monitoring Tools to resolve any 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.

Steps:

Prerequisites: AWS Free Tier, Nagios Server running on Amazon Linux Machine.

1. To Confirm that Nagios is running **on the server side**, run this *sudo systemctl status nagios* on the “NAGIOS HOST”.



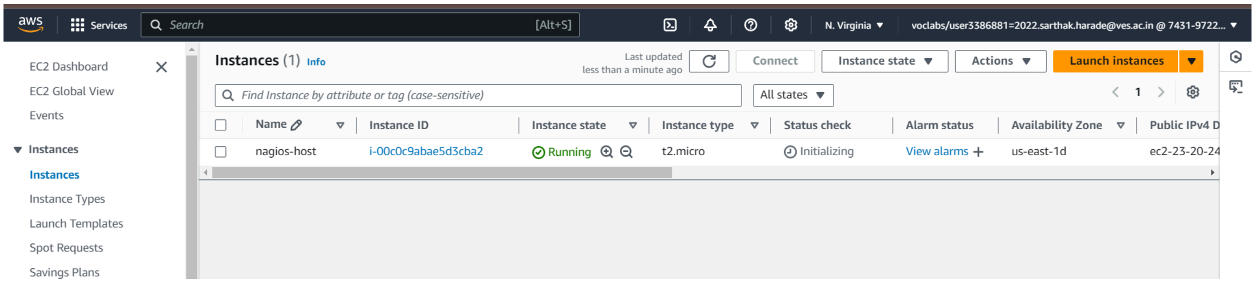
```
Starting nagios (via systemctl):                           [  OK  ]
[ec2-user@ip-172-31-44-218 nagios-plugins-2.0.3]$ sudo systemctl status nagios
● nagios.service - LSB: Starts and stops the Nagios monitoring server
     Loaded: loaded (/etc/rc.d/init.d/nagios; generated)
     Active: active (running) since Sat 2024-10-12 09:59:46 UTC; 51s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 66468 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
      Tasks: 6 (limit: 1112)
     Memory: 2.1M
        CPU: 51ms
     CGroup: /system.slice/nagios.service
             ├─66490 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─66492 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─66493 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─66494 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
```

You can proceed if you get this message.

2. Before we begin,

To monitor a Linux machine, create an Ubuntu 20.04 server EC2 Instance in AWS.

Provide it with the same security group as the Nagios Host and name it ‘linux-client’ alongside the host.



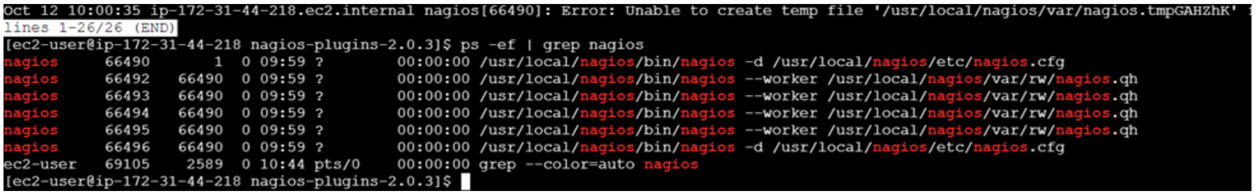
Instances (1) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
□	nagios-host	i-00c0c9abae5d3cba2	Running	t2.micro	Initializing	View alarms +	us-east-1d	ec2-23-20-24

For now, leave this machine as is, and go back to your nagios HOST machine.

3. On the server, run this command

ps -ef | grep nagios



```
Oct 12 10:00:35 ip-172-31-44-218.ec2.internal nagios[66490]: Error: Unable to create temp file '/usr/local/nagios/var/nagios.tmpGAHZhK'
lines 1-26/26 (END)
[ec2-user@ip-172-31-44-218 nagios-plugins-2.0.3]$ ps -ef | grep nagios
nagios     66490       1  0 09:59 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     66492   66490  0 09:59 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     66493   66490  0 09:59 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     66494   66490  0 09:59 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     66495   66490  0 09:59 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     66496   66490  0 09:59 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user   69105    2589  0 10:44 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-44-218 nagios-plugins-2.0.3]$ 
```

4. Become a root user and create 2 folders

```
sudo su
mkdir /usr/local/nagios/etc/objects/monitorhosts
mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
```

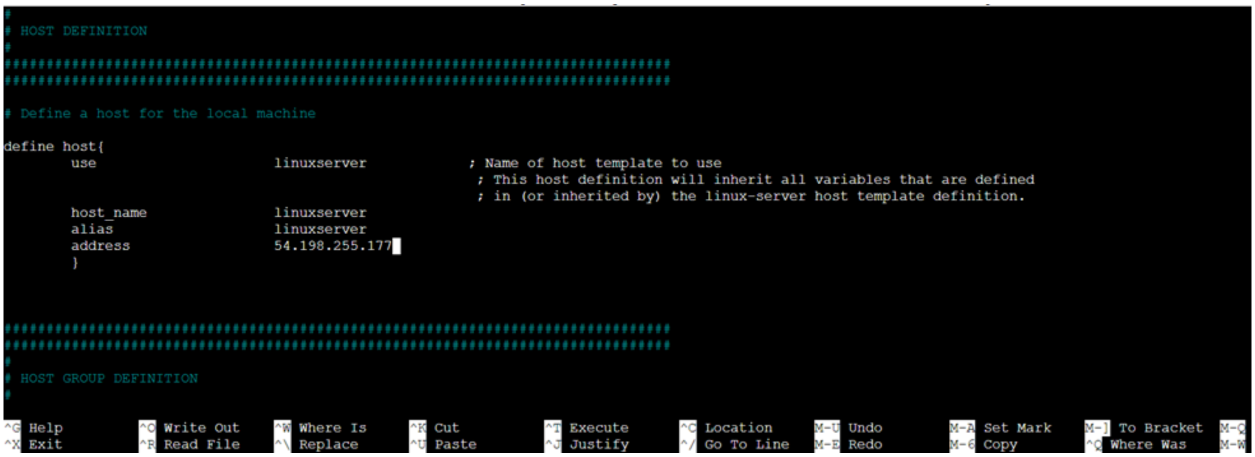
5. Copy the sample localhost.cfg file to linuxhost folder

```
cp /usr/local/nagios/etc/objects/localhost.cfg
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

6. Open linuxserver.cfg using nano and make the following changes

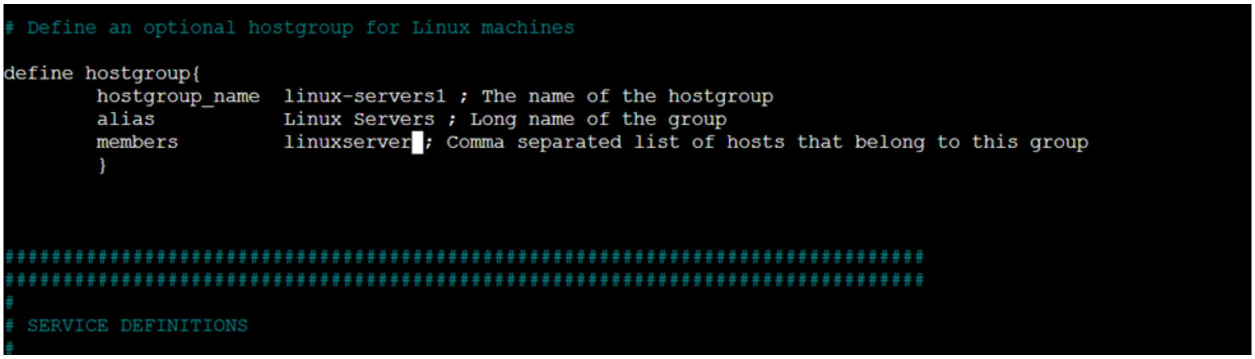
```
nano
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

Change the hostname to linuxserver (EVERYWHERE ON THE FILE)
Change address to the public IP address of your LINUX CLIENT.



```
#
# HOST DEFINITION
#
################################################################################
################################################################################

# Define a host for the local machine

define host{
        use                     linuxserver             ; Name of host template to use
                                                         ; This host definition will inherit all variables that are defined
                                                         ; in (or inherited by) the linux-server host template definition.

        host_name               linuxserver
        alias                   linuxserver
        address                 54.198.255.177
        }


################################################################################
################################################################################
#
# HOST GROUP DEFINITION
#
```

Change hostgroup_name under hostgroup to linux-servers1



```
# Define an optional hostgroup for Linux machines

define hostgroup{
        hostgroup_name  linux-servers1 ; The name of the hostgroup
        alias           Linux Servers ; Long name of the group
        members         linuxserver ; Comma separated list of hosts that belong to this group
        }


################################################################################
################################################################################
#
# SERVICE DEFINITIONS
#
```

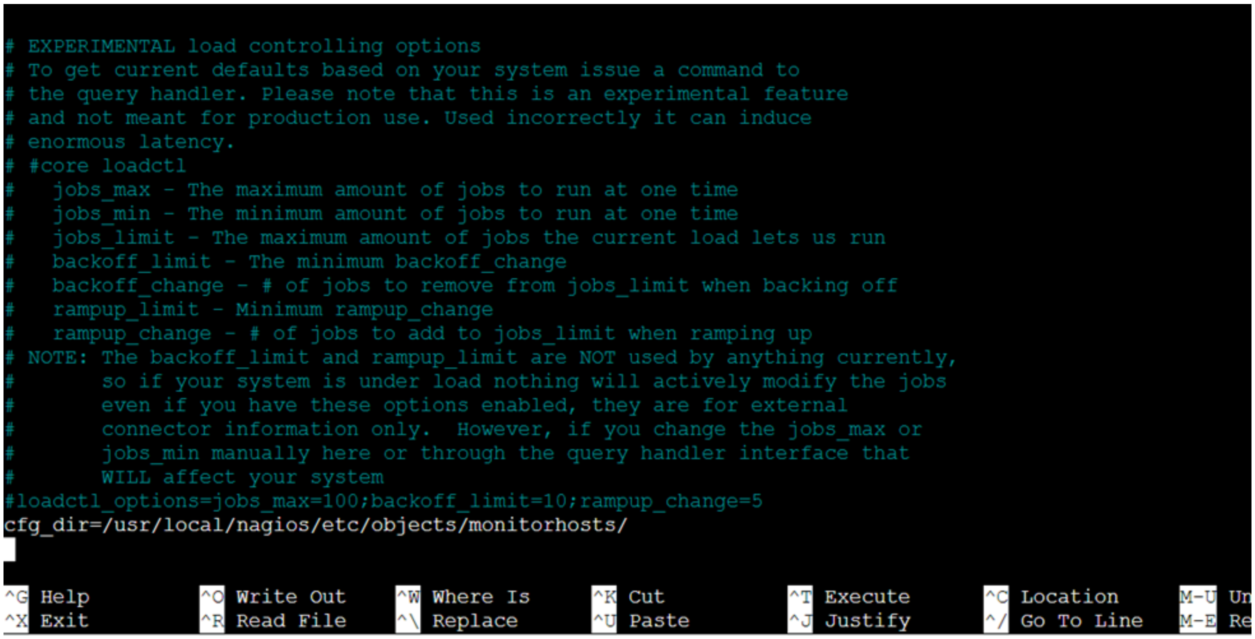
Everywhere else on the file, change the hostname to linuxserver instead of localhost.

7. Open the Nagios Config file and add the following line

nano /usr/local/nagios/etc/nagios.cfg

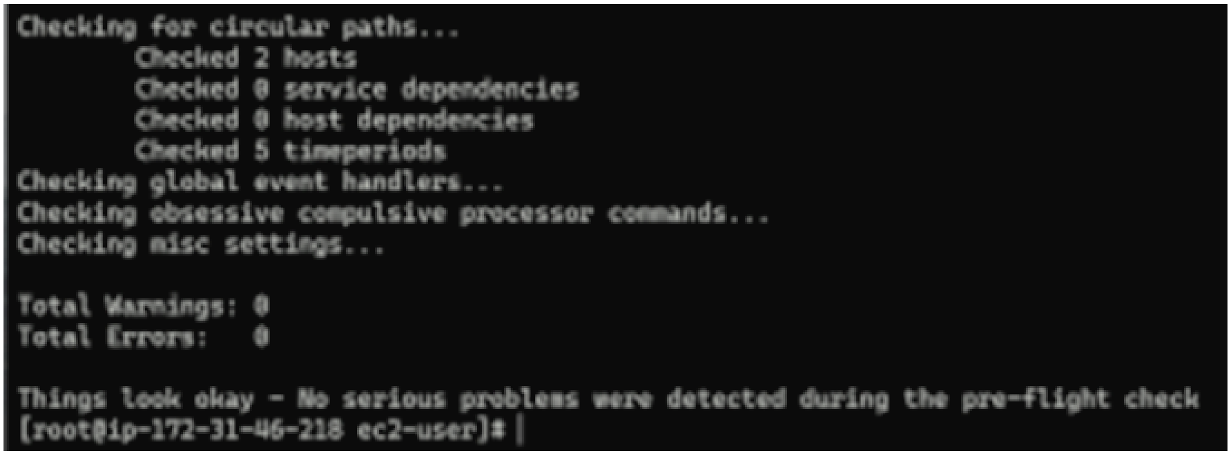
##Add this line

cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/



```
# EXPERIMENTAL load controlling options
# To get current defaults based on your system issue a command to
# the query handler. Please note that this is an experimental feature
# and not meant for production use. Used incorrectly it can induce
# enormous latency.
# #core loadctl
#   jobs_max - The maximum amount of jobs to run at one time
#   jobs_min - The minimum amount of jobs to run at one time
#   jobs_limit - The maximum amount of jobs the current load lets us run
#   backoff_limit - The minimum backoff_change
#   backoff_change - # of jobs to remove from jobs_limit when backing off
#   rampup_limit - Minimum rampup_change
#   rampup_change - # of jobs to add to jobs_limit when ramping up
# NOTE: The backoff_limit and rampup_limit are NOT used by anything currently,
#       so if your system is under load nothing will actively modify the jobs
#       even if you have these options enabled, they are for external
#       connector information only.  However, if you change the jobs_max or
#       jobs_min manually here or through the query handler interface that
#       WILL affect your system
#loadctl_options=jobs_max=100;backoff_limit=10;rampup_change=5
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/
```

8. Verify the configuration files

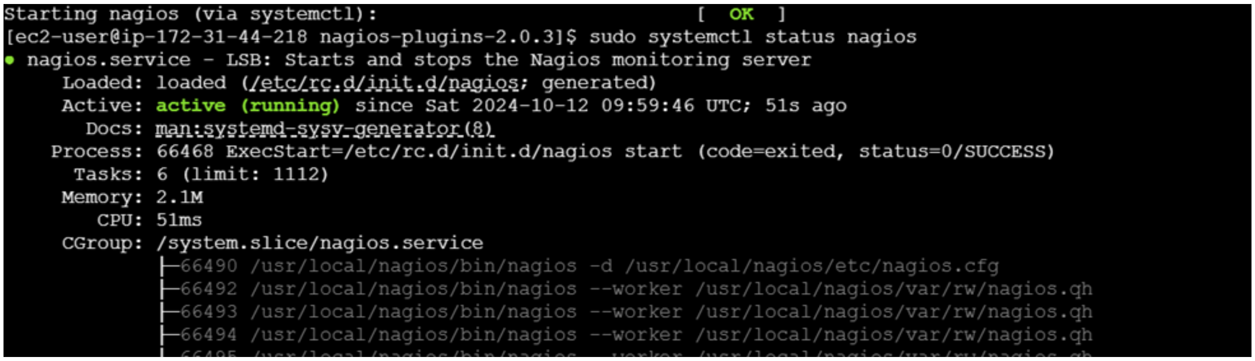


```
Checking for circular paths...
        Checked 2 hosts
        Checked 0 service dependencies
        Checked 0 host dependencies
        Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
[root@ip-172-31-46-218 ec2-user]# 
```

You are good to go if there are no errors.

9. Restart the nagios service

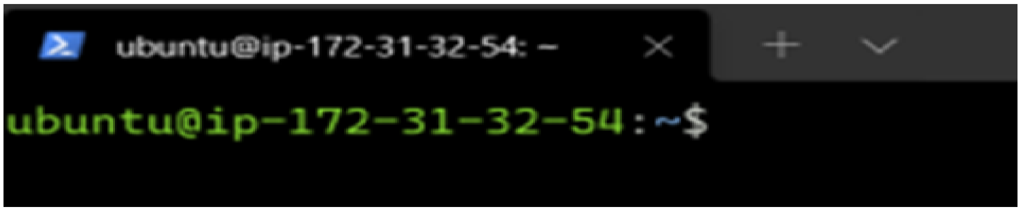
service nagios restart



```
Starting nagios (via systemctl):                           [  OK  ]
[ec2-user@ip-172-31-44-218 nagios-plugins-2.0.3]$ sudo systemctl status nagios
● nagios.service - LSB: Starts and stops the Nagios monitoring server
     Loaded: loaded (/etc/rc.d/init.d/nagios; generated)
     Active: active (running) since Sat 2024-10-12 09:59:46 UTC; 51s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 66468 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status=0/SUCCESS)
      Tasks: 6 (limit: 1112)
     Memory: 2.1M
        CPU: 51ms
     CGroup: /system.slice/nagios.service
             ├─66490 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─66492 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─66493 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─66494 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─66495 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
```

Now it is time to switch to the client machine.

10. SSH into the machine or simply use the EC2 Instance Connect



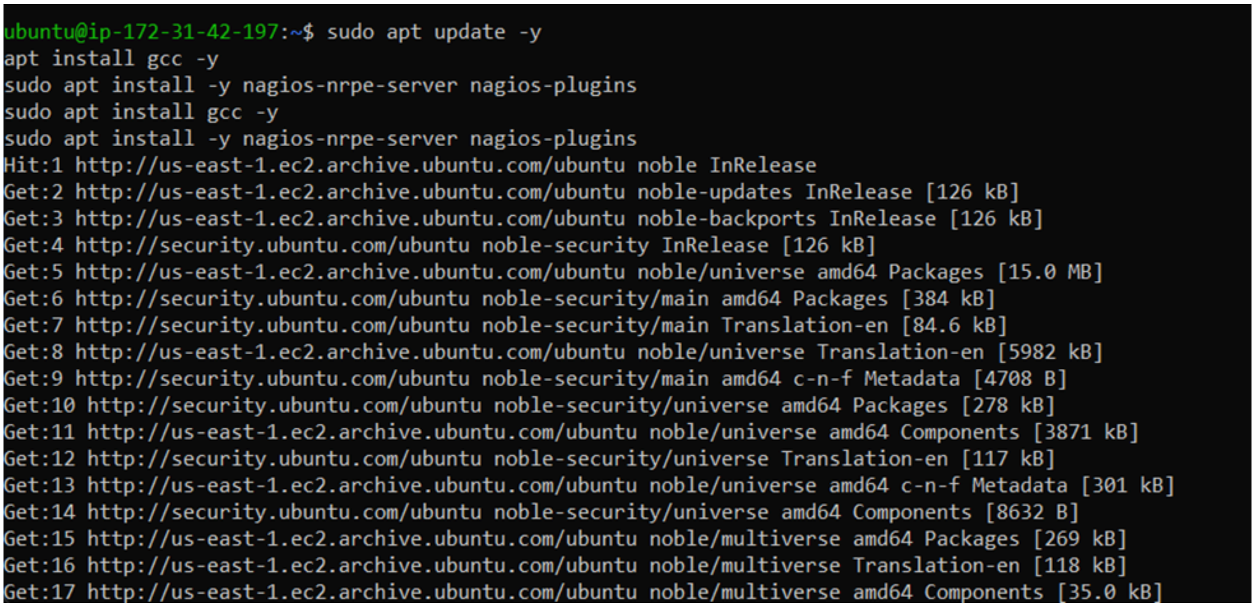
```
ubuntu@ip-172-31-32-54:~$
```

11. Make a package index update and install gcc, nagios-nrpe-server and the plugins.

sudo apt update -y

sudo apt install gcc -y

sudo apt install -y nagios-nrpe-server nagios-plugins

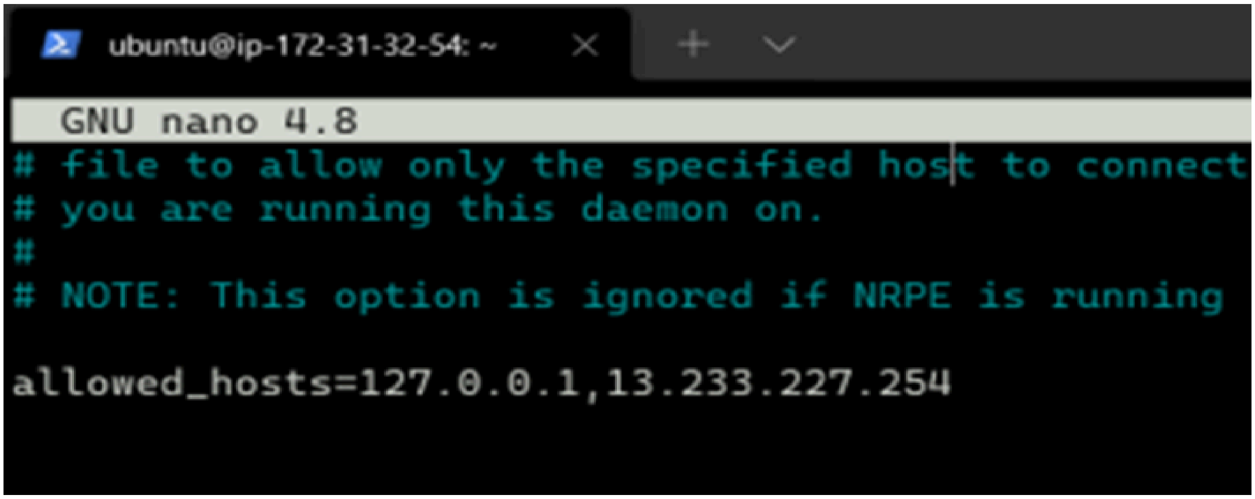


```
ubuntu@ip-172-31-42-197:~$ sudo apt update -y
apt install gcc -y
sudo apt install -y nagios-nrpe-server nagios-plugins
sudo apt install gcc -y
sudo apt install -y nagios-nrpe-server nagios-plugins
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [384 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [84.6 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4708 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [278 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [117 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [8632 B]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
```

12. Open nrpe.cfg file to make changes.

sudo nano /etc/nagios/nrpe.cfg

Under allowed_hosts, add your nagios host IP address like so



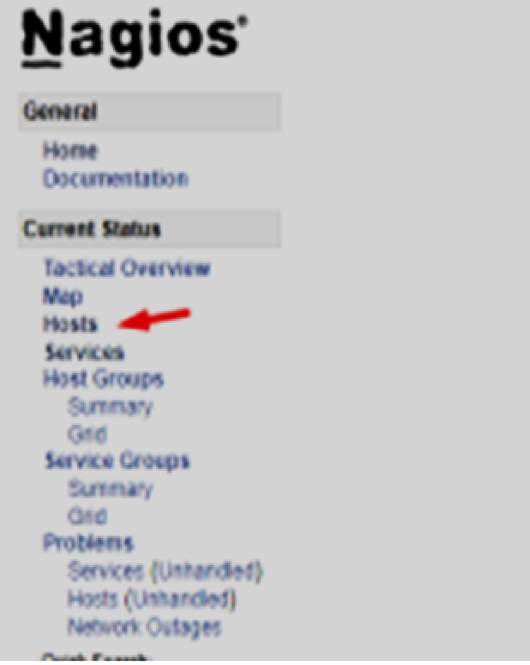
```
 GNU nano 4.8
# file to allow only the specified host to connect
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running

allowed_hosts=127.0.0.1,13.233.227.254
```

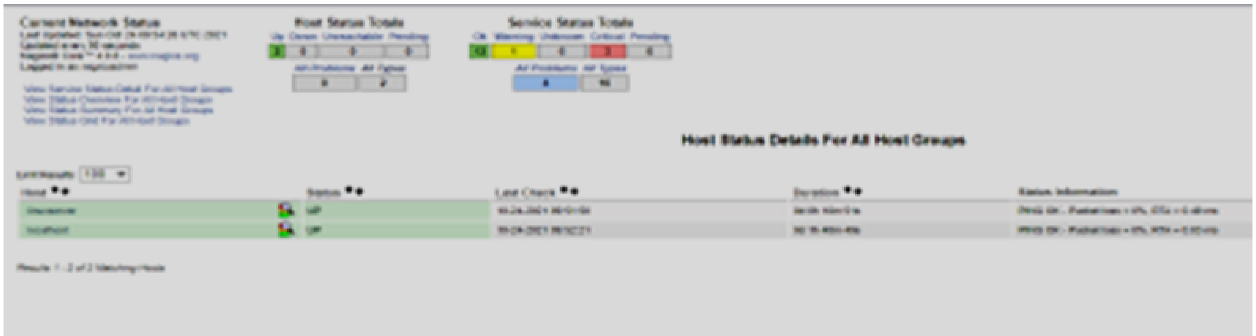
13. Restart the NRPE server

sudo systemctl restart nagios-nrpe-server

14. Now, check your nagios dashboard and you'll see a new host being added.

Click on Hosts.





Current Network Status
Last Updated: Sun Oct 24 [illegible] UTC 2021
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as nagiosadmin

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals			
Up	Down	Unreachable	Pending
2	0	0	0
All Problems	All Types		
0	2		

Service Status Totals				
Ok	Warning	Unknown	Critical	Pending
12	1	0	3	0
All Problems	All Types			
4	16			

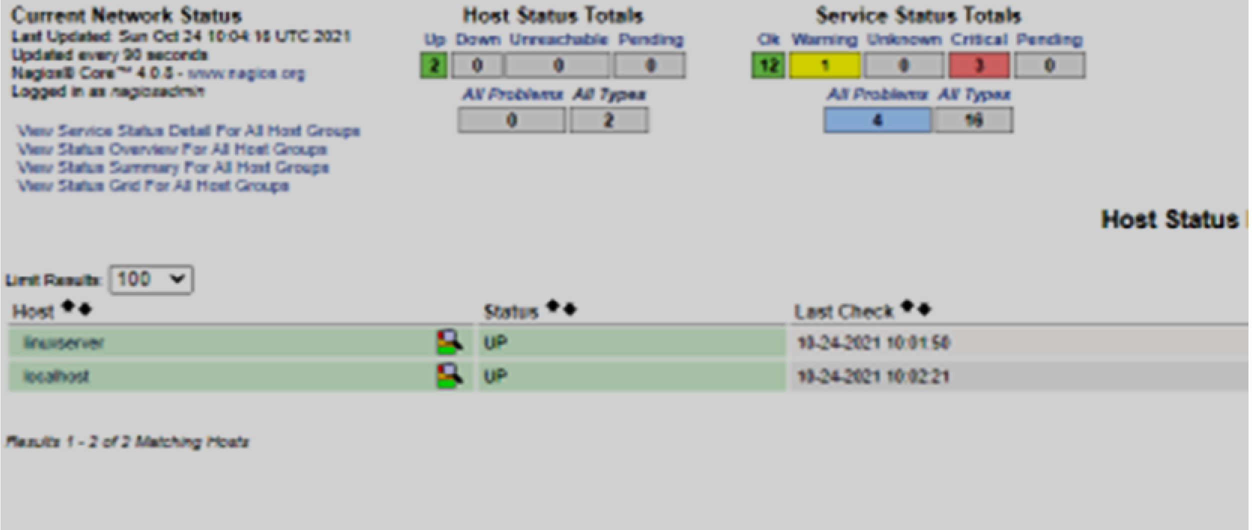
Host Status Details For All Host Groups

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
linuxserver	UP	10-24-2021 10:01:58	[illegible]	PING OK - Packet loss = 0%, RTA = [illegible]
localhost	UP	10-24-2021 10:02:21	[illegible]	PING OK - Packet loss = 0%, RTA = [illegible]

Results 1 - 2 of 2 Matching Hosts

Click on linuxserver to see the host details



Current Network Status
Last Updated: Sun Oct 24 10:04:16 UTC 2021
Updated every 90 seconds
Nagios® Core™ 4.0.8 - www.nagios.org
Logged in as nagiosadmin

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

Host Status Totals			
Up	Down	Unreachable	Pending
2	0	0	0
All Problems	All Types		
0	2		

Service Status Totals				
Ok	Warning	Unknown	Critical	Pending
12	1	0	3	0
All Problems	All Types			
4	16			

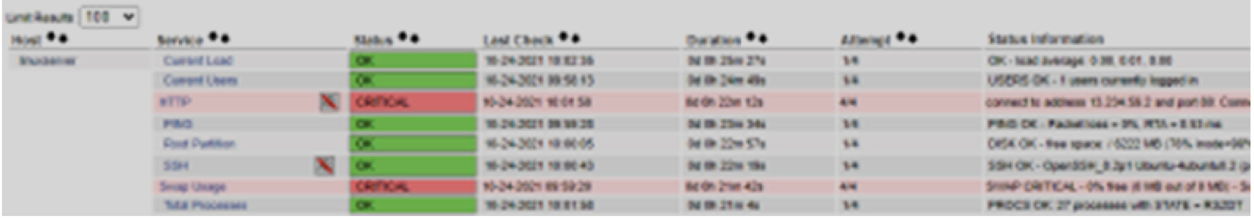
Host Status

Limit Results: 100

Host	Status	Last Check
linuxserver	UP	10-24-2021 10:01:58
localhost	UP	10-24-2021 10:02:21

Results 1 - 2 of 2 Matching Hosts

You can click Services to see all services and ports being monitored.



Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
linuxserver	Current Load	OK	10-24-2021 10:02:36	0d 0h 25m 27s	1/4	OK - load average: 0.00, 0.01, 0.00
	Current Users	OK	10-24-2021 09:58:13	0d 0h 24m 49s	1/4	USERS OK - 1 users currently logged in
	HTTP	CRITICAL	10-24-2021 10:01:58	0d 0h 22m 12s	4/4	connect to address 13.234.58.2 and port 80: Conn
	PING	OK	10-24-2021 09:59:28	0d 0h 23m 34s	1/4	PING OK - Packet loss = 0%, RTA = 0.53 ms
	Root Partition	OK	10-24-2021 10:00:05	0d 0h 22m 57s	1/4	DISK OK - free space: / 6222 MB (70% inode=98%
	SSH	OK	10-24-2021 10:00:43	0d 0h 22m 19s	1/4	SSH OK - OpenSSH_8.2p1 Ubuntu-4ubuntu0.2 (p
	Swap Usage	CRITICAL	10-24-2021 09:59:29	0d 0h 21m 42s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - S
	Total Processes	OK	10-24-2021 10:01:38	0d 0h 21m 4s	1/4	PROCS OK: 27 processes with STATE = RSZDT

As you can see, we have our linuxserver up and running. It is showing critical status on HTTP due to permission errors and swap because there is no partition created.

In this case, we have monitored -

Servers: 1 linux server

Services: swap

Ports: 22, 80 (ssh, http)

Processes: User status, Current load, total processes, root partition, etc.

Recommended Cleanup

- Terminate both of your EC-2 instances to avoid charges.
- Delete the security group if you created a new one (it won’t affect your bill, you may avoid it)

- **Conclusion:**

Thus, we learned about service monitoring using Nagios and successfully monitored a Linux Server and monitored its different ports and services using Nagios and NRPE.