Advanced DevOps
Lab Experiment 10

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

Nagios. **Steps:**

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

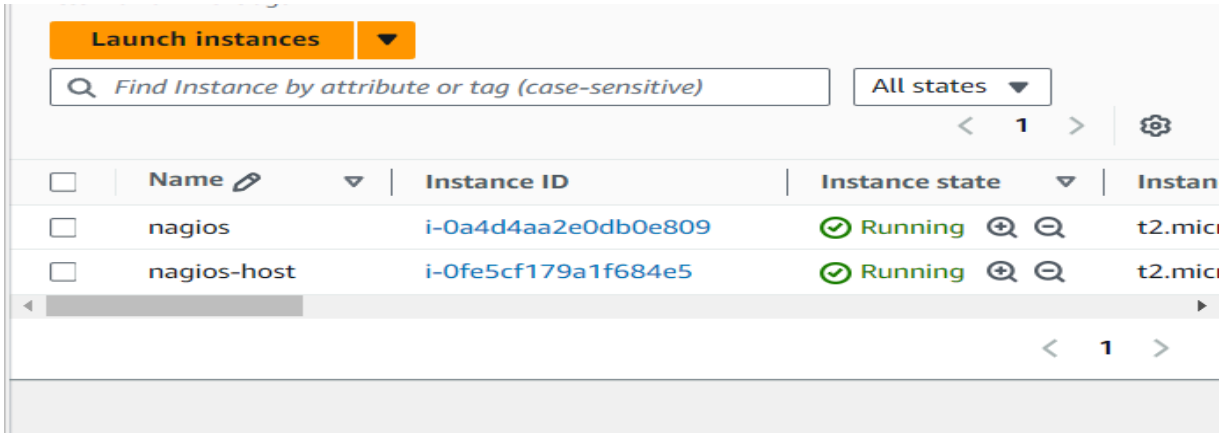
1. To Confirm that Nagios is running **on the server side**, run this *sudo systemctl status nagios* on the "NAGIOS HOST".

```
● nagios.service - Nagios Core 4.4.6
     Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Sun 2024-10-06 11:51:46 UTC; 12min ago
       Docs: https://www.nagios.org/documentation
   Main PID: 89956 (nagios)
      Tasks: 6 (limit: 1112)
     Memory: 3.2M
        CPU: 221ms
     CGroup: /system.slice/nagios.service
             ├─89956 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─89957 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─89958 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─89959 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─89960 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─89961 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
```

   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.



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
```

```
[ec2-user@ip-172-31-38-150 nagios-plugins-2.4.11]$ ps -ef | grep nagios
nagios     89956       1  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/et
/nagios.cfg
nagios     89957   89956  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nag
os/var/rw/nagios.qh
nagios     89958   89956  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nag
os/var/rw/nagios.qh
nagios     89959   89956  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nag
os/var/rw/nagios.qh
nagios     89960   89956  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nag
os/var/rw/nagios.qh
nagios     89961   89956  0 11:51 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/et
/nagios.cfg
ec2-user   91366    2723  0 12:12 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-38-150 nagios-plugins-2.4.11]$
```

4. Become a root user and create 2 folders

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

```
/nagios.cfg
ec2-user   91366    2723  0 12:12 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-38-150 nagios-plugins-2.4.11]$ sudo su
[root@ip-172-31-38-150 nagios-plugins-2.4.11]# mkdir /usr/local/nagios/etc/objects/monitorhosts
mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-38-150 nagios-plugins-2.4.11]#
```

`/usr/local/nagios/etc/objects/monitorhosts/linuxhosts` 5. Copy

```
[root@ip-172-31-38-150 nagios-plugins-2.4.11]# cp /usr/local/nacp /usr/local/nagios/etc/objects/localhos
.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserve
[root@ip-172-31-38-150 nagios-plugins-2.4.11]# nano
[root@ip-172-31-38-150 nagios-plugins-2.4.11]#
```

the sample localhost.cfg file to linuxhost folder

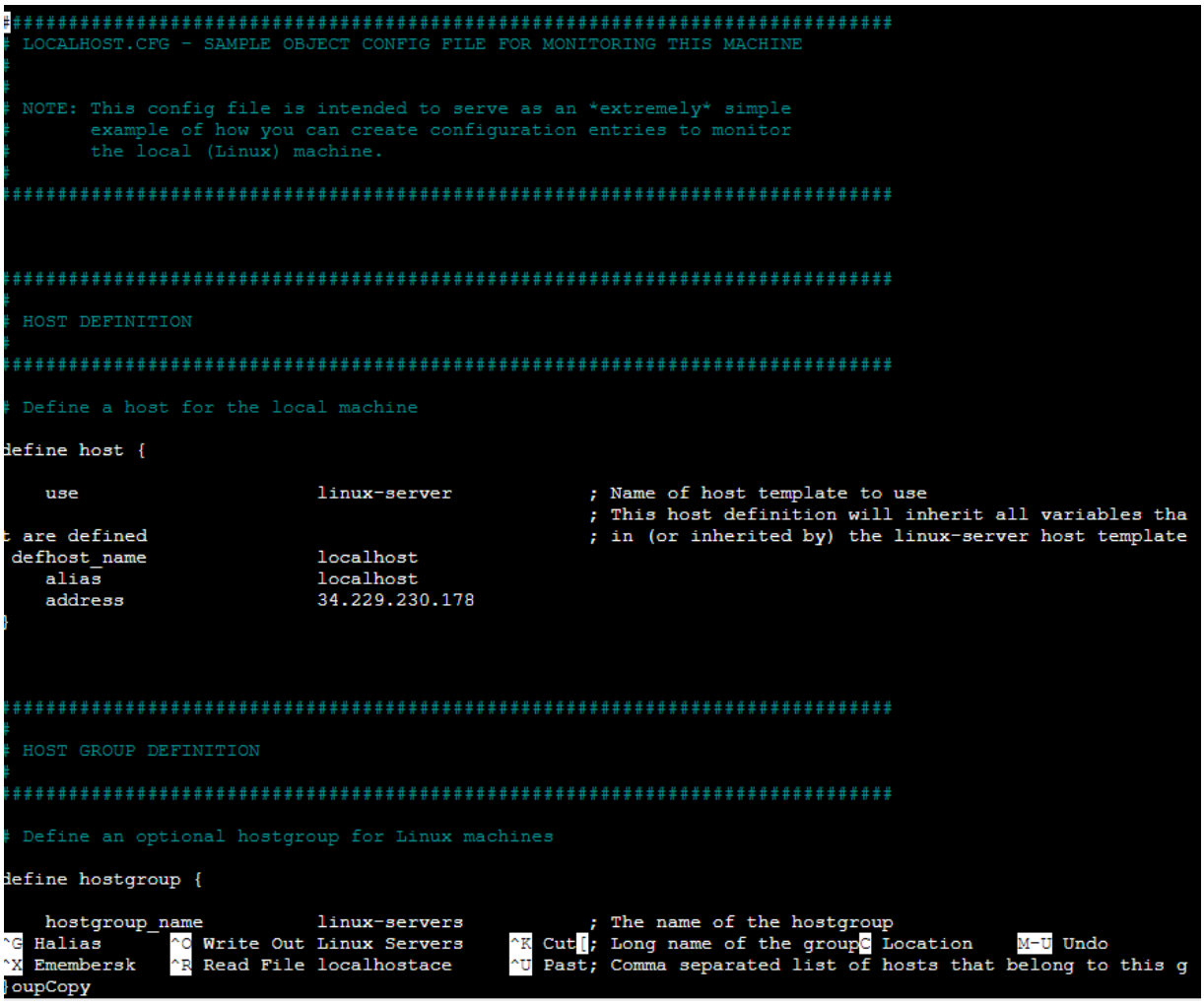
```
cp /usr/local/nagios/etc/objects/localhost.cfg
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cf
```

g 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.



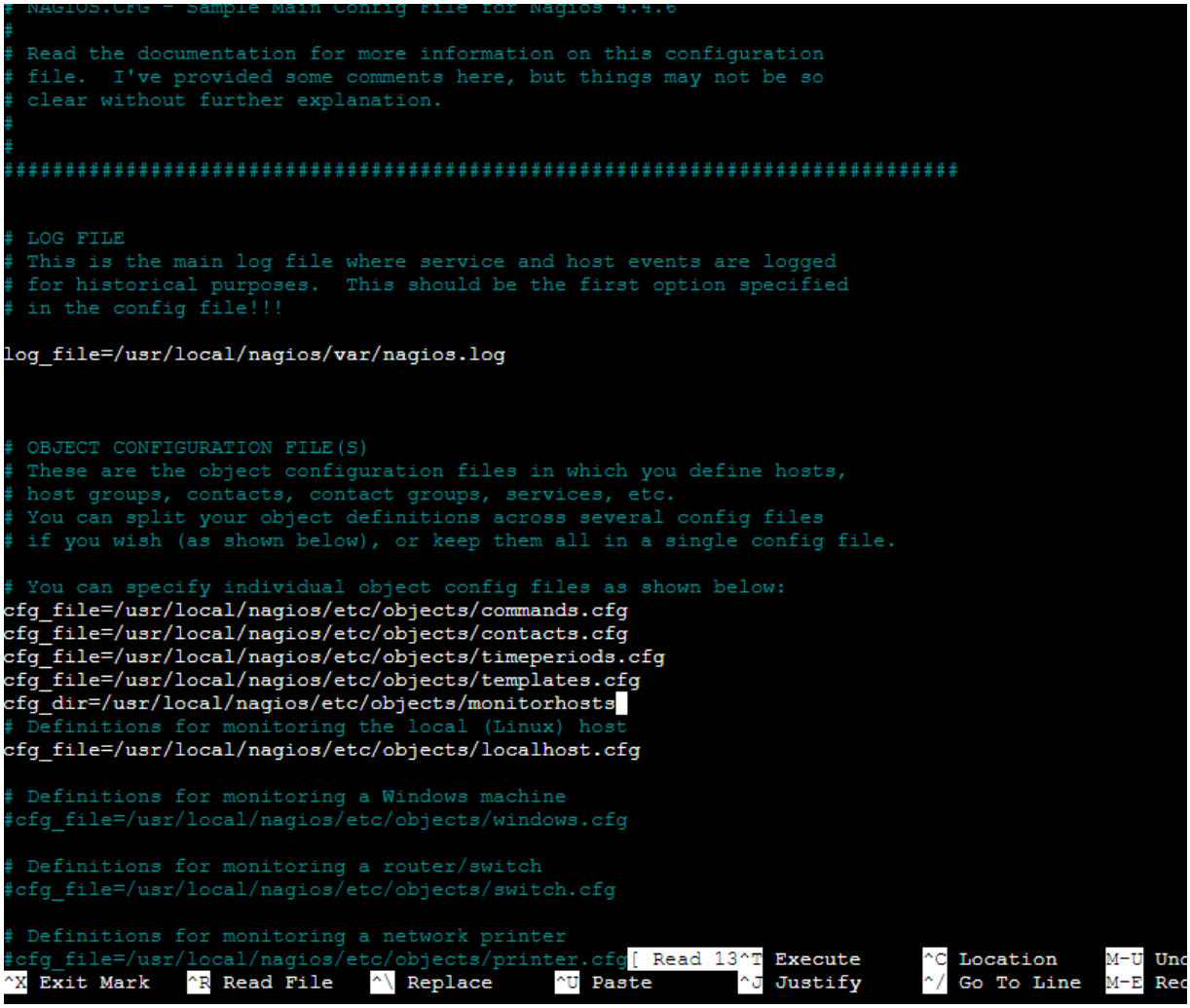
Change hostgroup_name under hostgroup to linux-servers1

```
# Define a service to "ping" the local machine

define service {

    use                     local-service           ; Name of service template to use
    host_name               localhost
    service_description     PING
    check_command           check_ping!100.0,20%!500.0,60%
}



# Define a service to check the disk space of the root partition

# < 10% free space on partition. if < 20% free, critical if


define service {
    use                     local-service           ; Name of service template to use
    host_name               localhost
    service_description     Root Partition
    check_command           check_local_disk!20%!10%!/
}



# Define a service to check the number of currently logged in
# users on the local machine.  Warning if > 20 users, critical
# if > 50 users.

define service {

    use                     local-service           ; Name of service template to use
    host_name               localhost
    service_description     Current Users
    check_command           check_local_users!20!50
}



# Define a service to check the number of currently running procs
# on the local machine.  Warning if > 250 processes, critical if
```

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/
```



8. Verify the configuration files

```
Running pre-flight check on configuration data...

Checking objects...
        Checked 8 services.
        Checked 2 hosts.
        Checked 2 host groups.
        Checked 0 service groups.
        Checked 1 contacts.
        Checked 1 contact groups.
        Checked 24 commands.
        Checked 5 time periods.
        Checked 0 host escalations.
        Checked 0 service escalations.
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
```

You are good to go if there are no errors.

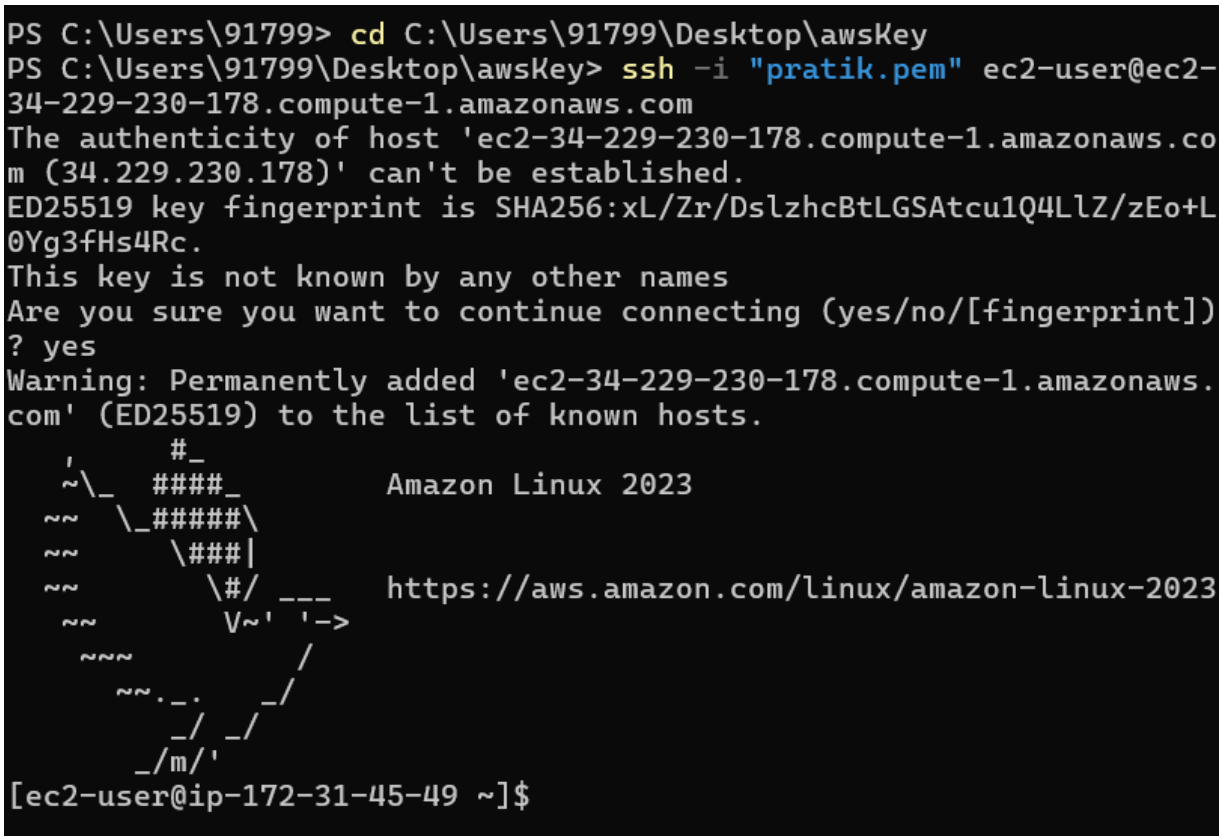
9. Restart the nagios service

```
service nagios restart
```

```
Redirecting to /bin/systemctl restart nagios.service
[root@ip-172-31-38-150 ec2-user]# sudo systemctl status nagios
● nagios.service - Nagios Core 4.4.6
     Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Sun 2024-10-06 12:55:30 UTC; 32s ago
       Docs: https://www.nagios.org/documentation
    Process: 94331 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
code=exited, status=0/>
    Process: 94332 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (co
e=exited, status=0/SUC>
   Main PID: 94333 (nagios)
      Tasks: 6 (limit: 1112)
     Memory: 1.8M
        CPU: 18ms
     CGroup: /system.slice/nagios.service
             ├─94333 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─94334 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─94335 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─94336 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─94337 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─94338 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 06 12:55:30 ip-172-31-38-150.ec2.internal nagios[94333]: wproc: Registry request: name=Core W
rker 94334;pid=94334
Oct 06 12:55:30 ip-172-31-38-150.ec2.internal nagios[94333]: Warning: Duplicate definition found
or service 'HTTP' on h>
Oct 06 12:55:30 ip-172-31-38-150.ec2.internal nagios[94333]: Warning: Duplicate definition found
or service 'SSH' on ho>
Oct 06 12:55:30 ip-172-31-38-150.ec2.internal nagios[94333]: Warning: Duplicate definition found
or service 'Swap Usage>
Oct 06 12:55:30 ip-172-31-38-150.ec2.internal nagios[94333]: Warning: Duplicate definition found
```

Now it is time to switch to the client machine.

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



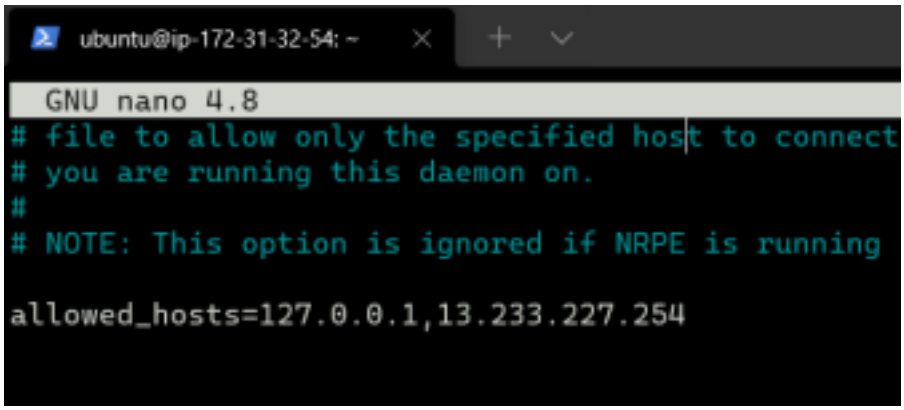
11. Make a package index update and install gcc, nagios-nrpe-server and the plugins.

```
sudo apt update -y
sudo apt install gcc -y
sudo apt install -y nagios-nrpe-server nagios-plugins
```

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



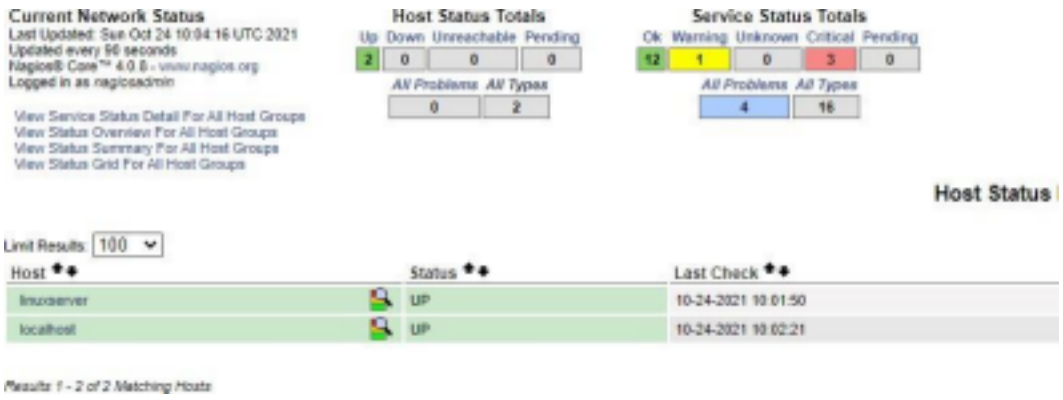
13. Restart the NRPE server

```
sudo systemctl restart nagios-nrpe-server
```

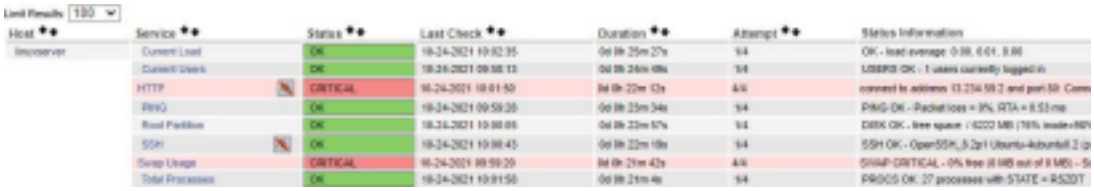
14. Now, check your nagios dashboard and you'll see a new host being added.

    Click on Hosts.

    Click on linuxserver to see the host details



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



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:

Nagios is a widely used open-source monitoring tool designed to monitor systems, networks, and infrastructure. It can alert administrators when things go wrong and notify them of recovery. The monitoring includes various aspects, such as services, system performance, port status, and network health.