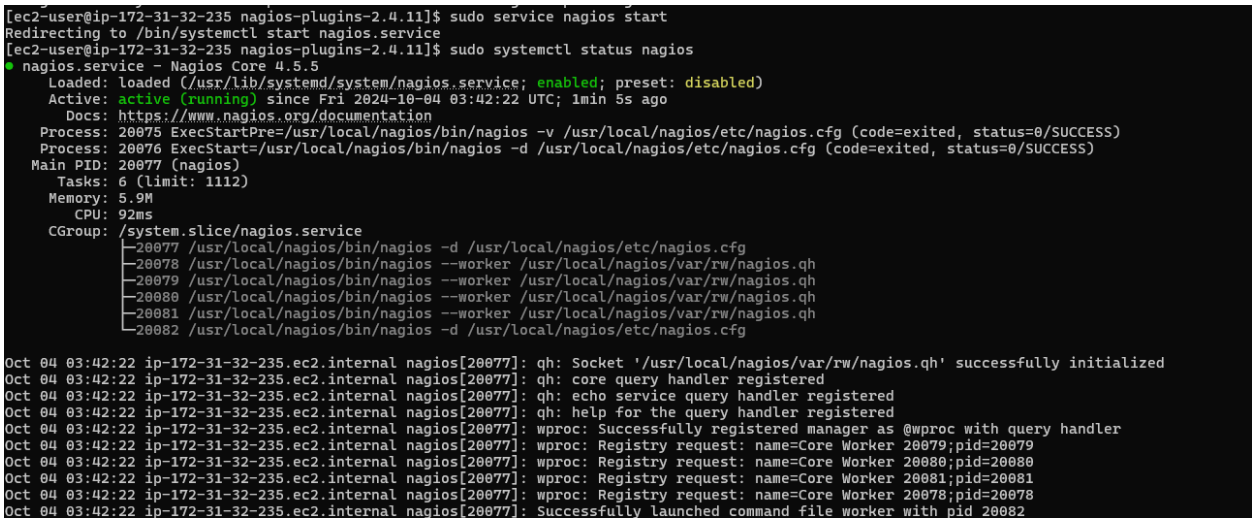
**Aim**: To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

**Prerequisites:**
Nagios Server running on Amazon Linux Machine.

STEPS:

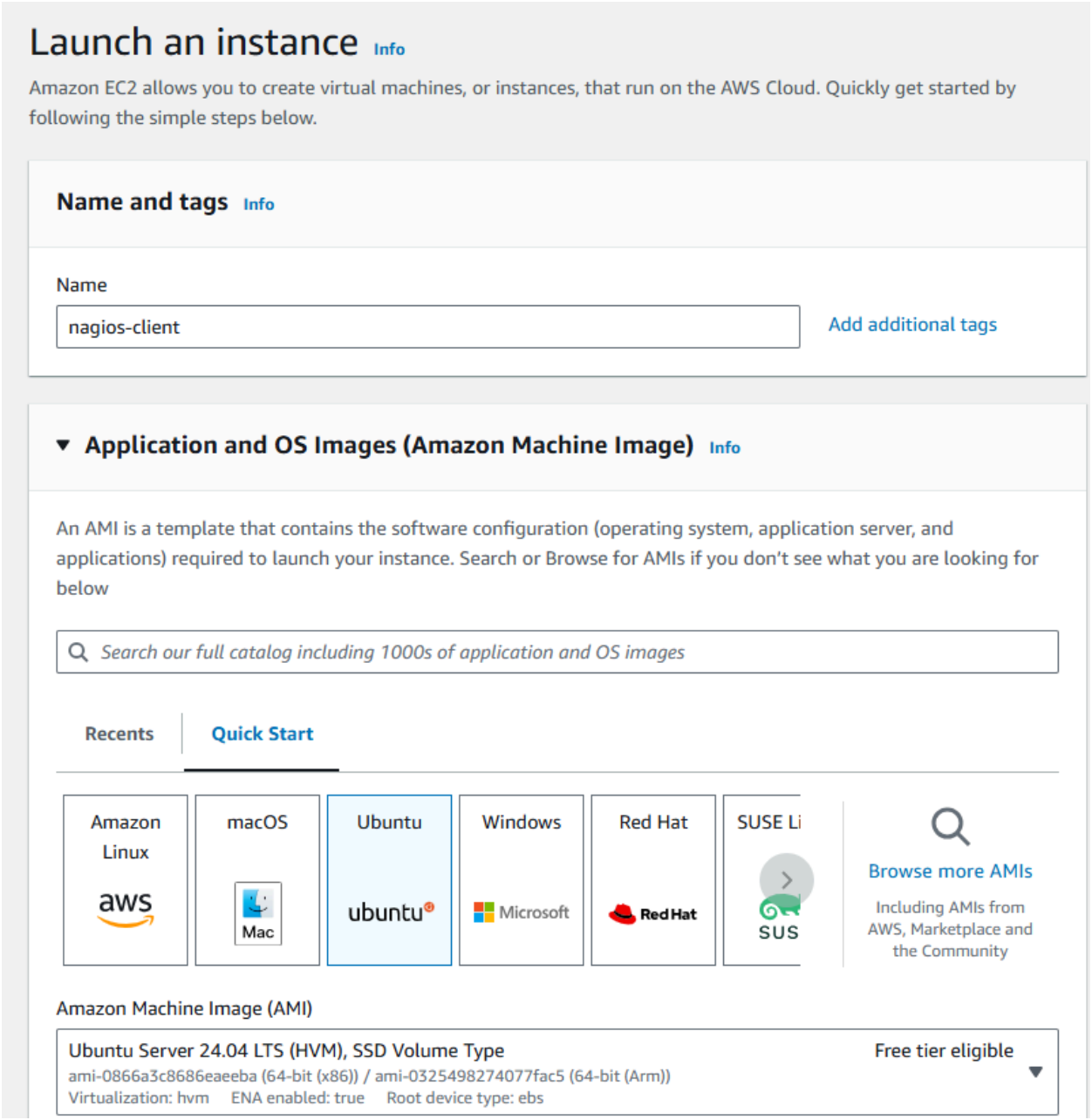
1. To Confirm Nagios is running on the server side Perform the following command on your Amazon Linux Machine (Nagios-host).

   **sudo systemctl status nagios**

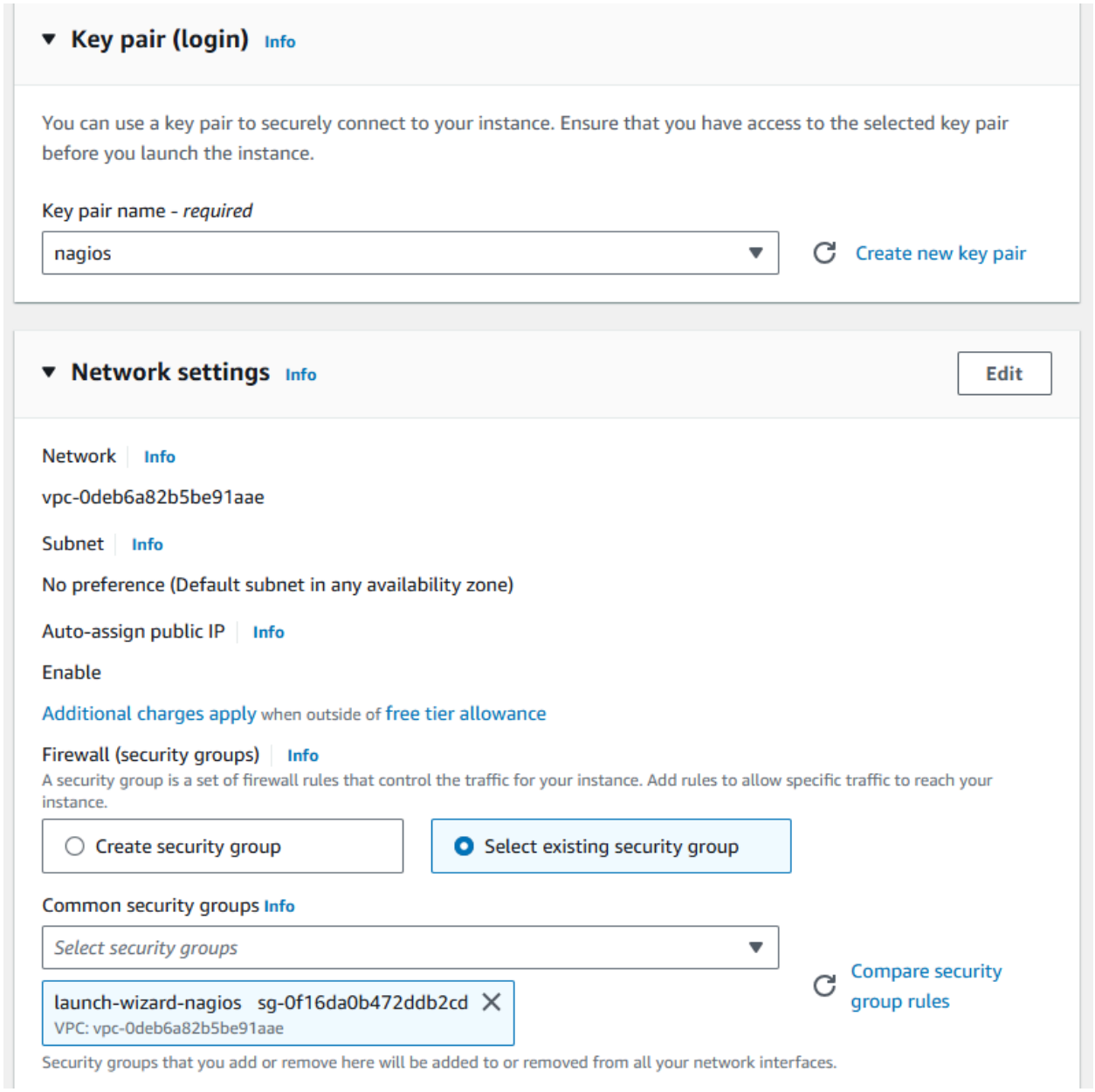



   As nagios service on main machine is running, we can proceed further

2. Now Create a new EC2 instance. Name: Nagios-client, AMI: Ubuntu Instance Type: t2.micro.

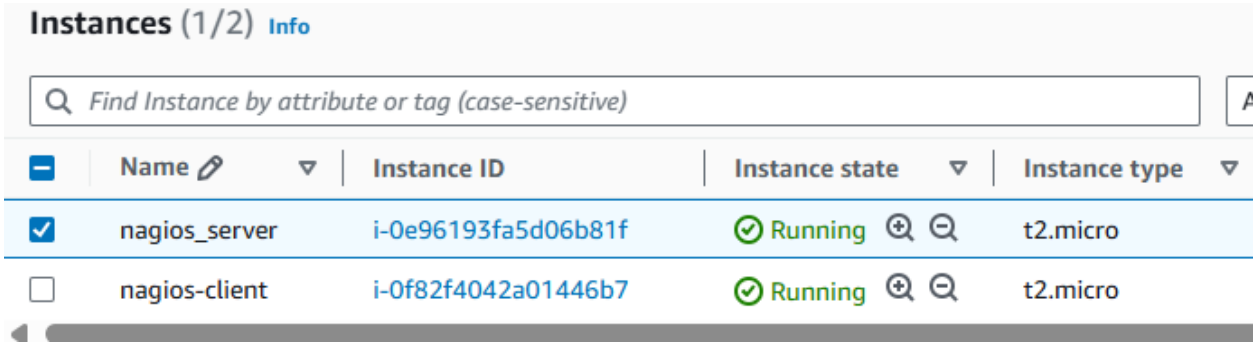



Select the existing security group and choose the one configured in Experiment 9, or the same security group used for the Nagios server (Nagios-host).




Launched successfully message appears:


You can see both the instances required for this experiment




After creating the EC2 instance, click on "Connect," copy the SSH command from the SSH Client section, open the terminal in the folder containing your RSA key (.pem), and paste the command.

```
PS C:\Users\Avan\Downloads> ssh -i "nagios.pem" ubuntu@ec2-18-206-185-207.compute-1.amazonaws.com
The authenticity of host 'ec2-18-206-185-207.compute-1.amazonaws.com (18.206.185.207)' can't be established.
ED25519 key fingerprint is SHA256:HGCTF4Wul1HL3RyrMxyq6ea/z7UeVTLxcXAi0rcw50Q.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-18-206-185-207.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri Oct  4 04:09:51 UTC 2024

  System load:  0.31              Processes:             107
  Usage of /:   22.9% of 6.71GB   Users logged in:       0
  Memory usage: 22%               IPv4 address for enX0: 172.31.36.170
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

***Now perform all the commands on the Nagios-host till step 10***

**4**. Now on the server Nagios-host run the following command.

**ps -ef | grep nagios**

```
[ec2-user@ip-172-31-32-235 ~]$ ps -ef | grep nagios
ec2-user    2860    2353  0 03:31 pts/0    00:00:00 journalctl -xeu nagios.service
nagios     20077       1  0 03:42 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     20078   20077  0 03:42 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     20079   20077  0 03:42 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     20080   20077  0 03:42 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     20081   20077  0 03:42 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     20082   20077  0 03:42 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user   21798    2353  0 04:12 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-32-235 ~]$
```

**5**. Now Become root user and create root directories.
**sudo su**
**mkdir /usr/local/nagios/etc/objects/monitorhosts**
**mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts**

```
[ec2-user@ip-172-31-32-235 ~]$ sudo su
[root@ip-172-31-32-235 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts
[root@ip-172-31-32-235 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
```

**6**. Copy the sample localhost.cfg to linuxhost.cfg by running the following command.(Below command should come in one line see screenshot below)

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

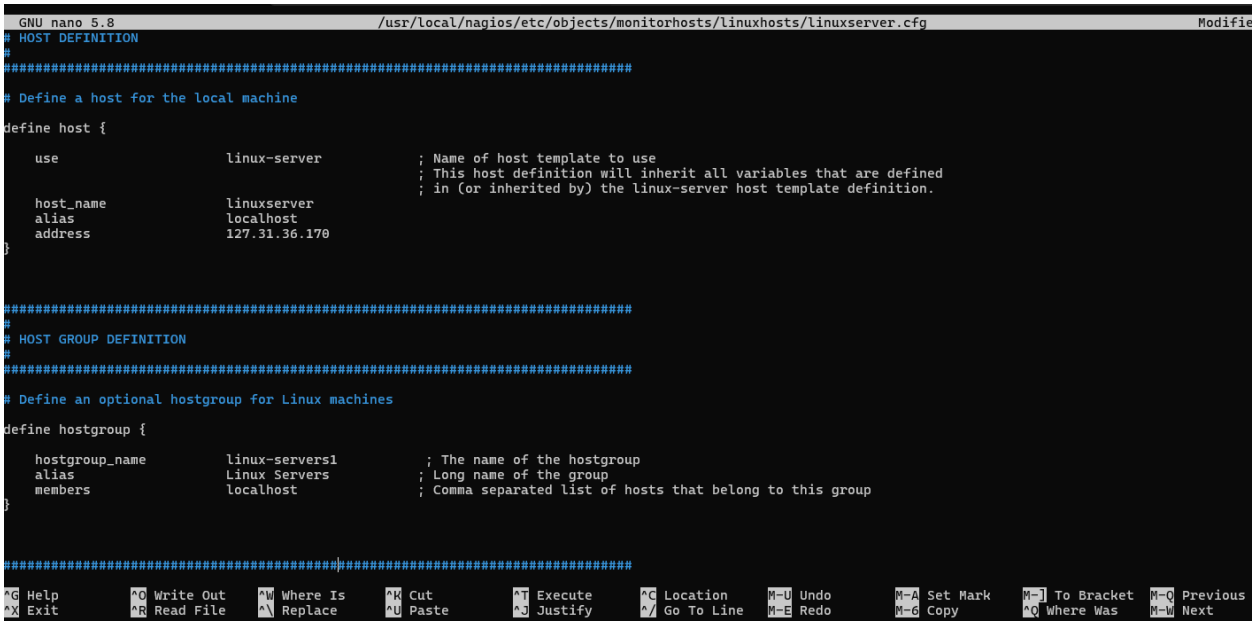
```
[root@ip-172-31-32-235 ec2-user]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxho
sts/linuxserver.cfg
[root@ip-172-31-32-235 ec2-user]#
```

**7**. Open linuxserver.cfg using nano and make the following changes in all Positions everywhere in file

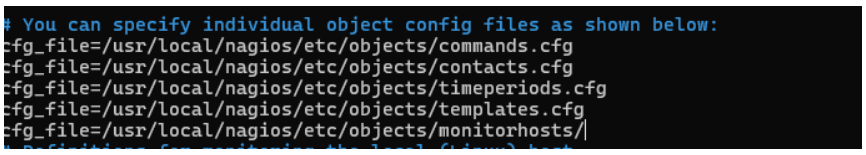
**nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg**

```
# LOG FILE
# This is the main log file where service and host events are logged
# for historical purposes.  This should be the first option specified
# in the config file!!!

log_file=/usr/local/nagios/var/nagios.log



# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg
cfg_file=/usr/local/nagios/etc/objects/monitorhosts/
# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# Definitions for monitoring a Windows machine
#cfg_file=/usr/local/nagios/etc/objects/windows.cfg

^G Help        ^O Write Out    ^W Where Is     ^K Cut          ^T Execute
^X Exit        ^R Read File    ^\ Replace      ^U Paste        ^J Justify
```

Change hostname to **linuxserver.**
Change address to the **public IP of your Linux client**.
Set hostgroup_name to **linux-servers1**.




**8**. Now update the Nagios config file .Add the following line in the file. Line to add :
**cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/**
**nano /usr/local/nagios/etc/nagios.cfg**




**9.** Now Verify the configuration files by running the following commands.
**/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg**

```
[root@ip-172-31-32-235 ec2-user]# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.5.5
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2024-09-17
License: GPL

Website: https://www.nagios.org
Reading configuration data...
   Read main config file okay...
Warning: Duplicate definition found for service 'HTTP' on host 'localhost' (config file '/usr/local/na
Warning: Duplicate definition found for service 'SSH' on host 'localhost' (config file '/usr/local/nag
Warning: Duplicate definition found for service 'Swap Usage' on host 'localhost' (config file '/usr/lo
Warning: Duplicate definition found for service 'Current Load' on host 'localhost' (config file '/usr/
Warning: Duplicate definition found for service 'Total Processes' on host 'localhost' (config file '/u
Warning: Duplicate definition found for service 'Current Users' on host 'localhost' (config file '/usr
Warning: Duplicate definition found for service 'Root Partition' on host 'localhost' (config file '/us
Warning: Duplicate definition found for service 'PING' on host 'localhost' (config file '/usr/local/na
   Read object config files okay...

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
```

We got no errors and warnings for current configuration

**10**. Now restart the services of nagios by running the following command.
**service nagios restart**

```
[root@ip-172-31-32-235 ec2-user]# service nagios restart
Redirecting to /bin/systemctl restart nagios.service
[root@ip-172-31-32-235 ec2-user]#
```

**11.** Now Go to the Nagios-client ssh terminal and update and install the packages by running the following command.

**sudo apt update -y**
**sudo apt install gcc -y**

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

```
ubuntu@ip-172-31-36-170:~$ sudo apt update -y
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://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [382 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 c-n-f Metadata [301 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Packages [269 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse Translation-en [118 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 c-n-f Metadata [8328 B]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [537 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [132 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 c-n-f Metadata [8860 B]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [384 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [159 kB]
Get:19 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [83.9 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 c-n-f Metadata [14.9 kB]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [14.4 kB]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [3608 B]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [212 B]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 c-n-f Metadata [532 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-backports/main amd64 c-n-f Metadata [112 B]
```

```
Creating config file /etc/nagios-plugins/config/nt.cfg with new version

Creating config file /etc/nagios-plugins/config/pgsql.cfg with new version

Creating config file /etc/nagios-plugins/config/radius.cfg with new version

Creating config file /etc/nagios-plugins/config/rpc-nfs.cfg with new version

Creating config file /etc/nagios-plugins/config/snmp.cfg with new version
Setting up monitoring-plugins (2.3.5-1ubuntu3) ...
Setting up libldb2:amd64 (2:2.8.0+samba4.19.5+dfsg-4ubuntu9) ...
Setting up libavahi-client3:amd64 (0.8-13ubuntu6) ...
Setting up samba-libs:amd64 (2:4.19.5+dfsg-4ubuntu9) ...
Setting up python3-ldb (2:2.8.0+samba4.19.5+dfsg-4ubuntu9) ...
Setting up samba-dsdb-modules:amd64 (2:4.19.5+dfsg-4ubuntu9) ...
Setting up libsmbclient0:amd64 (2:4.19.5+dfsg-4ubuntu9) ...
Setting up libcups2t64:amd64 (2.4.7-1.2ubuntu7.3) ...
Setting up python3-samba (2:4.19.5+dfsg-4ubuntu9) ...
Setting up smbclient (2:4.19.5+dfsg-4ubuntu9) ...
Setting up samba-common-bin (2:4.19.5+dfsg-4ubuntu9) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-36-170:~$
```

12. Now restart the NRPE server by this command.
**sudo systemctl restart nagios-nrpe-server**

```
[ec2-user@ip-172-31-32-235 ~]$ sudo nano /etc/nagios/nrpe.cfg

[ec2-user@ip-172-31-32-235 ~]$ sudo systemctl restart nagios-nrpe-server
```

**13.** Now again check the status of Nagios by running this command on Nagios-host and also check httpd is active and run the command to active it.

**sudo systemctl status nagios**

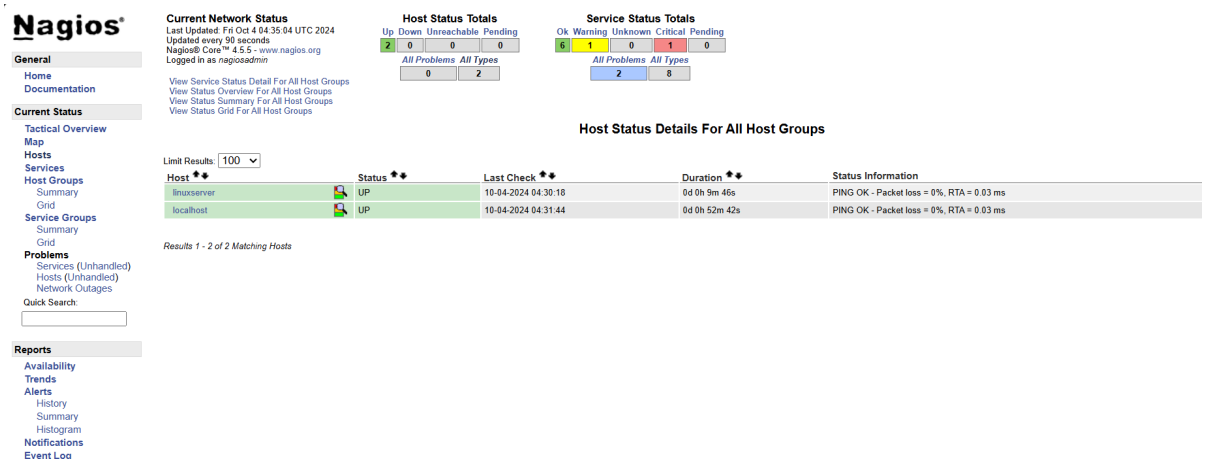
**sudo systemctl status httpd**

```
[root@ip-172-31-32-235 ec2-user]# sudo systemctl status httpd
sudo systemctl start httpd
sudo systemctl enable httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
    Drop-In: /usr/lib/systemd/system/httpd.service.d
             └─php-fpm.conf
     Active: active (running) since Fri 2024-10-04 03:39:13 UTC; 55min ago
       Docs: man:httpd.service(8)
   Main PID: 5507 (httpd)
     Status: "Total requests: 51; Idle/Busy workers 100/0;Requests/sec: 0.0154; Bytes served/sec:  58 B/sec"
      Tasks: 177 (limit: 1112)
     Memory: 19.1M
        CPU: 1.983s
     CGroup: /system.slice/httpd.service
             ├─5507 /usr/sbin/httpd -DFOREGROUND
             ├─5509 /usr/sbin/httpd -DFOREGROUND
             ├─5510 /usr/sbin/httpd -DFOREGROUND
             ├─5511 /usr/sbin/httpd -DFOREGROUND
             └─5512 /usr/sbin/httpd -DFOREGROUND

Oct 04 03:39:12 ip-172-31-32-235.ec2.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Oct 04 03:39:13 ip-172-31-32-235.ec2.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Oct 04 03:39:13 ip-172-31-32-235.ec2.internal httpd[5507]: Server configured, listening on: port 80
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[root@ip-172-31-32-235 ec2-user]# Z
```

**Both nagios and httpd service is running fine on host system**

**14.** Now to check Nagios dashboard go to http://<nagios host ip>/nagios
Or you can go to the instance id and click on the Public Ip <-link-> and Nagios server gets loaded
**Enter username as nagiosadmin and password which you set in Exp 9 if prompted.**


Now Click on Hosts from left side panel




Our nagios client is showing up on nagios host dashboard

Host status :

**Host Information**
Last Updated: Fri Oct 4 04:35:25 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.5.5 - www.nagios.org
Logged in as *nagiosadmin*

View Status Detail For This Host
View Alert History For This Host
View Trends For This Host
View Alert Histogram For This Host
View Availability Report For This Host
View Notifications For This Host

Host
**localhost**
**(linuxserver)**

Member of
**No hostgroups**

127.31.36.170

**Host State Information**

| | |
|---|---|
| **Host Status:** | UP (for 0d 0h 10m 7s) |
| **Status Information:** | PING OK - Packet loss = 0%, RTA = 0.03 ms |
| **Performance Data:** | rta=0.034000ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0 |
| **Current Attempt:** | 1/10 (HARD state) |
| **Last Check Time:** | 10-04-2024 04:30:18 |
| **Check Type:** | ACTIVE |
| **Check Latency / Duration:** | 0.000 / 4.159 seconds |
| **Next Scheduled Active Check:** | 10-04-2024 04:35:18 |
| **Last State Change:** | 10-04-2024 04:25:18 |
| **Last Notification:** | N/A (notification 0) |
| **Is This Host Flapping?** | NO (0.00% state change) |
| **In Scheduled Downtime?** | NO |
| **Last Update:** | 10-04-2024 04:35:17 ( 0d 0h 0m 8s ago) |

| | |
|---|---|
| **Active Checks:** | ENABLED |
| **Passive Checks:** | ENABLED |
| **Obsessing:** | ENABLED |
| **Notifications:** | ENABLED |
| **Event Handler:** | ENABLED |
| **Flap Detection:** | ENABLED |

**Host Comments**

Add a new comment  Delete all comments

| Entry Time | Author | Comment | Comment ID | Persistent | Type | Expires | Actions |
|---|---|---|---|---|---|---|---|
| This host has no comments associated with it | | | | | | | |

Service Status Details for Host localhost:

**Current Network Status**
Last Updated: Fri Oct 4 04:37:03 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.5.5 - www.nagios.org
Logged in as *nagiosadmin*

View History For This Host
View Notifications For This Host
View Service Status Detail For All Hosts

**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 |
|---|---|---|---|---|
| 6 | 1 | 0 | 1 | 0 |

| All Problems | All Types |
|---|---|
| 2 | 8 |

**Service Status Details For Host 'localhost'**

Limit Results: 100

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---|---|---|---|---|---|---|
| localhost | Current Load | OK | 10-04-2024 04:32:59 | 0d 0h 54m 4s | 1/4 | OK - load average: 0.00, 0.02, 0.00 |
| | Current Users | OK | 10-04-2024 04:33:37 | 0d 0h 53m 26s | 1/4 | USERS OK - 2 users currently logged in |
| | HTTP | WARNING | 10-04-2024 04:32:14 | 0d 0h 49m 49s | 4/4 | HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.000 second response time |
| | PING | OK | 10-04-2024 04:34:52 | 0d 0h 52m 11s | 1/4 | PING OK - Packet loss = 0%, RTA = 0.04 ms |
| | Root Partition | OK | 10-04-2024 04:35:29 | 0d 0h 51m 34s | 1/4 | DISK OK - free space: / 5584 MiB (68.81% inode=98%): |
| | SSH | OK | 10-04-2024 04:36:07 | 0d 0h 50m 56s | 1/4 | SSH OK - OpenSSH_8.7 (protocol 2.0) |
| | Swap Usage | CRITICAL | 10-04-2024 04:34:44 | 0d 0h 47m 19s | 4/4 | SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size. |
| | Total Processes | OK | 10-04-2024 04:32:22 | 0d 0h 49m 41s | 1/4 | PROCS OK: 39 processes with STATE = RSZDT |

*Results 1 - 8 of 8 Matching Services*

Here these details indicate that the client machine is running with :

**Current Load**: OK (load average is low).
**Current Users**: OK (2 users are logged in).
**HTTP**: Warning (HTTP 403 Forbidden, indicating a potential access permission issue).

**PING**: OK (no packet loss, response time is very low).
**Swap Usage**: Critical (swap is either 0 or disabled).
**Total Processes**: OK (39 processes are running as expected).

**Conclusion:**

In this experiment, we focused on monitoring ports, services, and a Linux server using Nagios. By following a structured approach, we successfully configured Nagios to monitor critical network services on the Linux server. Through the setup of both the Nagios host and client, we effectively tracked system performance, ensured service availability, and monitored key metrics such as CPU and memory usage.Additionally, the configuration of Nagios files, particularly defining the host name and correctly setting the IP address of the server, played a crucial role. This ensures proper identification and communication between the Nagios host and the monitored server, allowing accurate monitoring of services. Properly configuring these details is essential for the efficient operation and management of network resources.