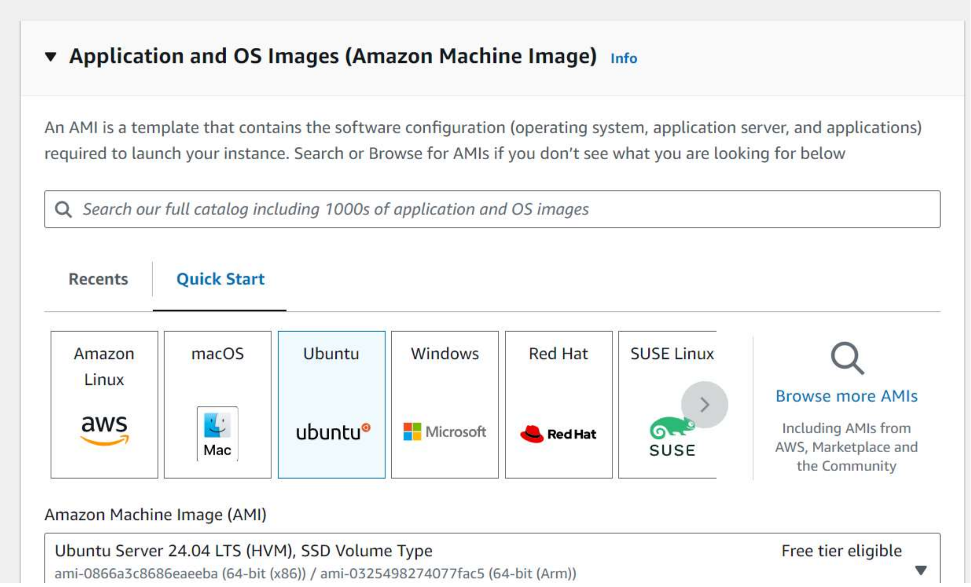
Aim: To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

Prerequisites: An EC2 instance(nagios-host) with a nagios server already setup. (We can use the instance created in the previous experiment).

1. Go to EC2 on your AWS academy lab. Click on Launch instance and. Give an appropriate name and select Ubuntu as the instance type. Use the same key pair and the security group which was used in previous experiment. Confirm the configurations and click on create instance.



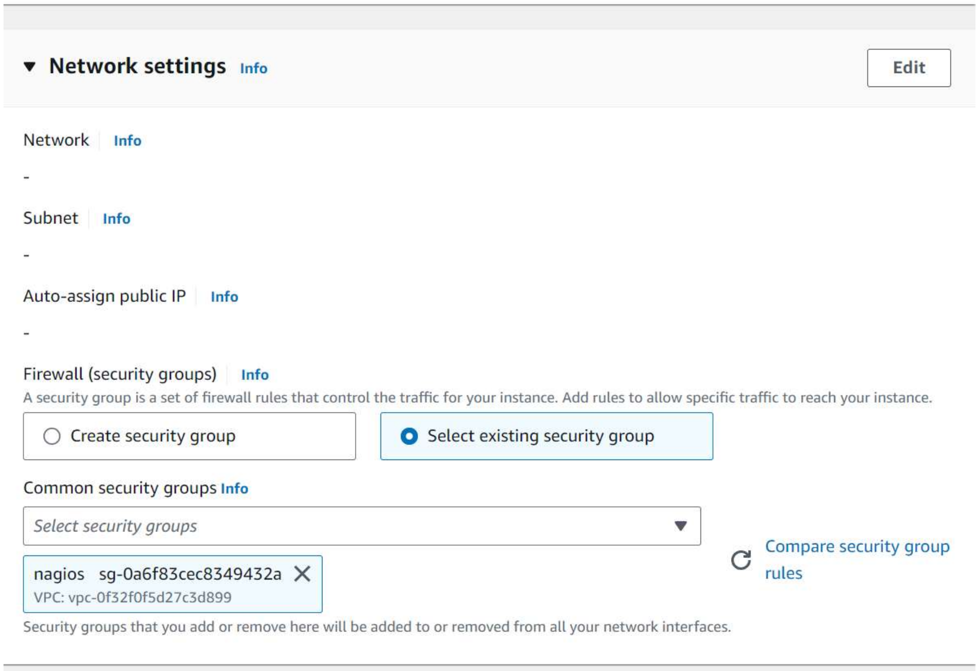
▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type Free tier eligible
ami-0866a3c8686eaeeba (64-bit (x86)) / ami-0325498274077fac5 (64-bit (Arm))



▼ Network settings Info

Network Info
-

Subnet Info
-

Auto-assign public IP Info
-

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

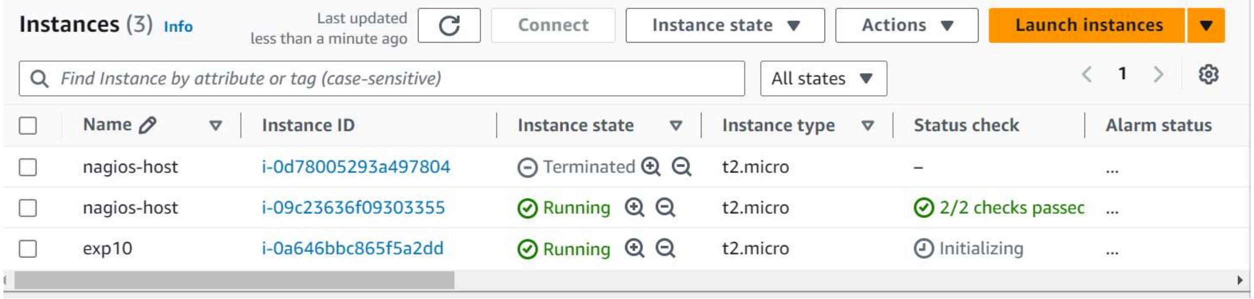
○ Create security group ● Select existing security group

Common security groups Info

Select security groups

nagios sg-0a6f83cec8349432a
VPC: vpc-0f32f0f5d27c3d899

Security groups that you add or remove here will be added to or removed from all your network interfaces.

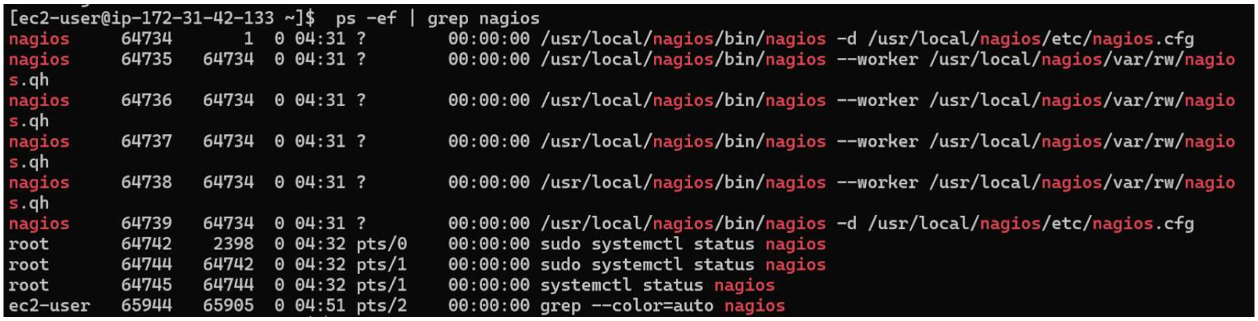

Instances (3) Info
Last updated less than a minute ago
Connect
Instance state ▼
Actions ▼
Launch instances ▼
Find Instance by attribute or tag (case-sensitive)
All states ▼
< 1 >

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status
□	nagios-host	i-0d78005293a497804	Terminated	t2.micro	–	...
□	nagios-host	i-09c23636f09303355	Running	t2.micro	2/2 checks passec	...
□	exp10	i-0a646bbc865f5a2dd	Running	t2.micro	Initializing	...

You should have both the host instance and the newly created instance.

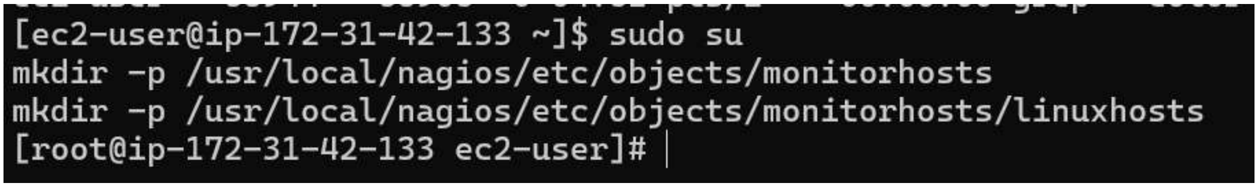
2. Now click on the instance id for the newly created instance, click on connect. Go to the ssh tab and copy the example command. Open the folder where .pem file for key pair was installed in your terminal and run the copied command. This will connect your terminal to the ec2 instance. Do this for the host instance as well.

3. To verify whether the nagios service is running or not, run the following command
 ps -ef | grep nagios
Perform the following commands in the host instance until specified to do otherwise.



```
[ec2-user@ip-172-31-42-133 ~]$  ps -ef | grep nagios
nagios     64734       1  0 04:31 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     64735   64734  0 04:31 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagio
s.qh
nagios     64736   64734  0 04:31 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagio
s.qh
nagios     64737   64734  0 04:31 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagio
s.qh
nagios     64738   64734  0 04:31 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagio
s.qh
nagios     64739   64734  0 04:31 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
root       64742    2398  0 04:32 pts/0    00:00:00 sudo systemctl status nagios
root       64744   64742  0 04:32 pts/1    00:00:00 sudo systemctl status nagios
root       64745   64744  0 04:32 pts/1    00:00:00 systemctl status nagios
ec2-user   65944   65905  0 04:51 pts/2    00:00:00 grep --color=auto nagios
```

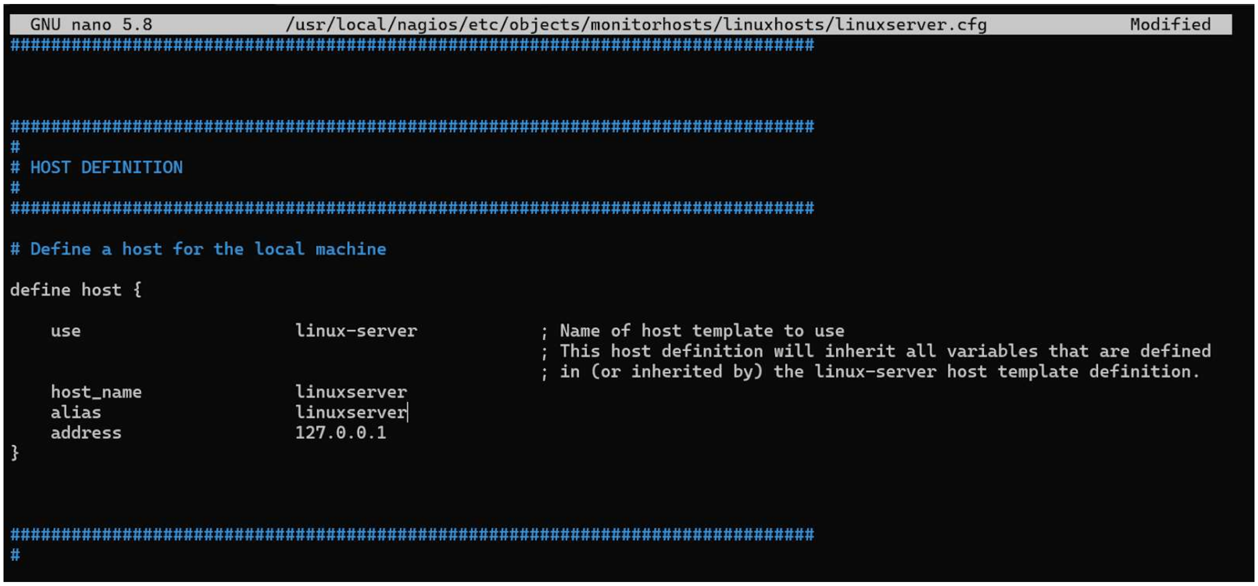
4. sudo su
mkdir -p /usr/local/nagios/etc/objects/monitorhosts
mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
This makes you the root user and creates two folders with the above paths.



```
[ec2-user@ip-172-31-42-133 ~]$ sudo su
mkdir -p /usr/local/nagios/etc/objects/monitorhosts
mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-42-133 ec2-user]# 
```

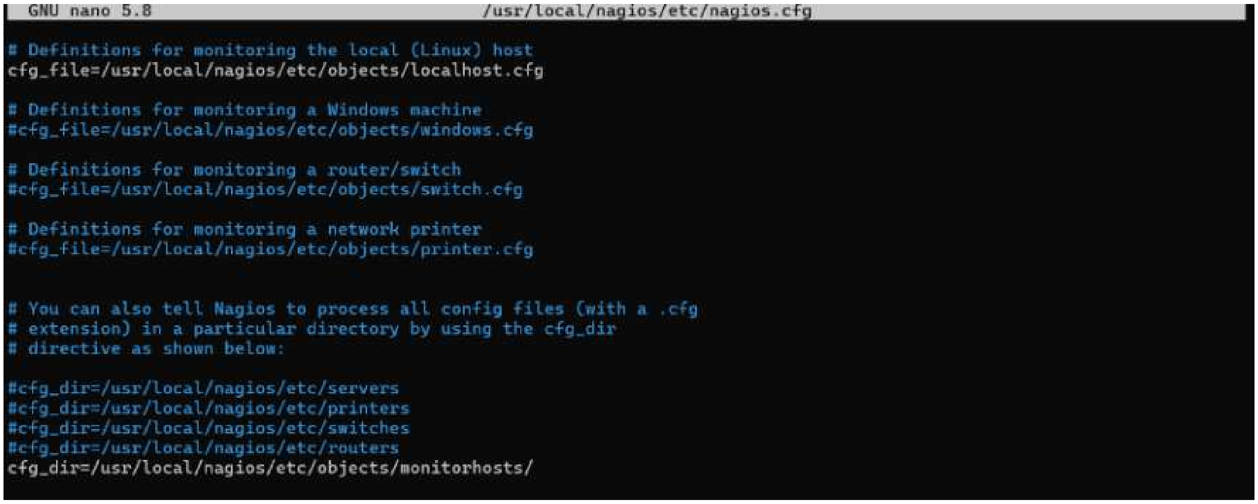
5. Open the config file using the nano editor as we need to make some changes in the configuration.
nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

Change hostname and alias from ‘hostname’ to ‘linuxserver’.
Change address to the public ip address of the ubuntu-client instance.
Change hostgroup_name to ‘linux-servers1’.
Change all the subsequent occurrences of hostname in the file from ‘localhost’ to linuxserver’.



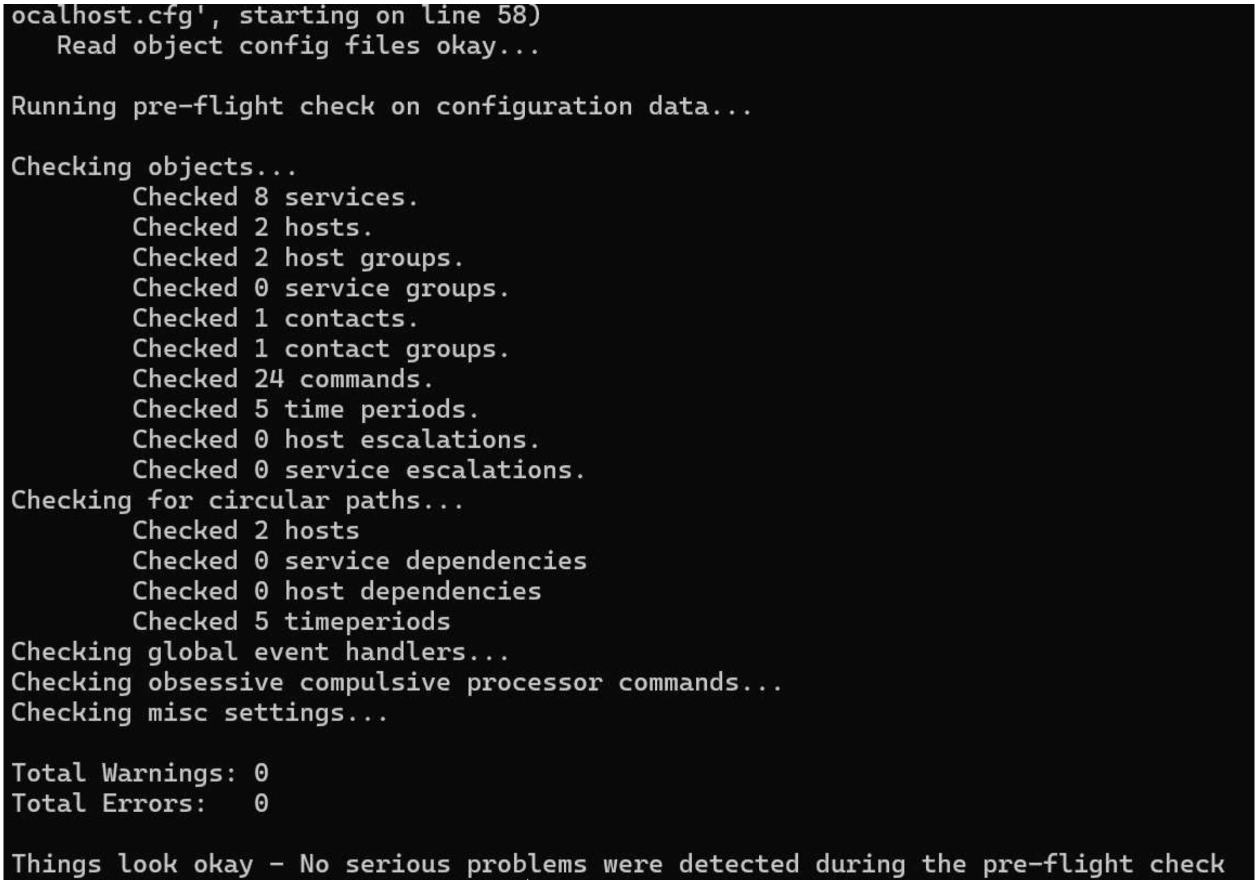
```
  GNU nano 5.8             /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg             Modified
################################################################################



################################################################################
#
# HOST DEFINITION
#
################################################################################

# Define a host for the local machine

define host {

    use                     linux-server            ; 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                 127.0.0.1
}



################################################################################
#
```

6. Open the Nagios config file using the following command:
nano /usr/local/nagios/etc/nagios.cfg
Then, add the following line to the config file:
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/



```
  GNU nano 5.8                                        /usr/local/nagios/etc/nagios.cfg

# 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

# Definitions for monitoring a router/switch
#cfg_file=/usr/local/nagios/etc/objects/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/usr/local/nagios/etc/objects/printer.cfg


# You can also tell Nagios to process all config files (with a .cfg
# extension) in a particular directory by using the cfg_dir
# directive as shown below:

#cfg_dir=/usr/local/nagios/etc/servers
#cfg_dir=/usr/local/nagios/etc/printers
#cfg_dir=/usr/local/nagios/etc/switches
#cfg_dir=/usr/local/nagios/etc/routers
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/
```

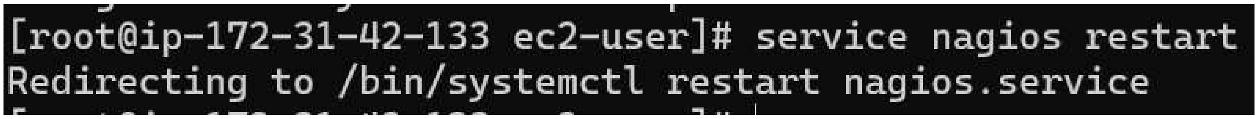
7. To check and verify if the configurations are correct or not run the following command:
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg



```
ocalhost.cfg', starting on line 58)
   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

Things look okay - No serious problems were detected during the pre-flight check
```

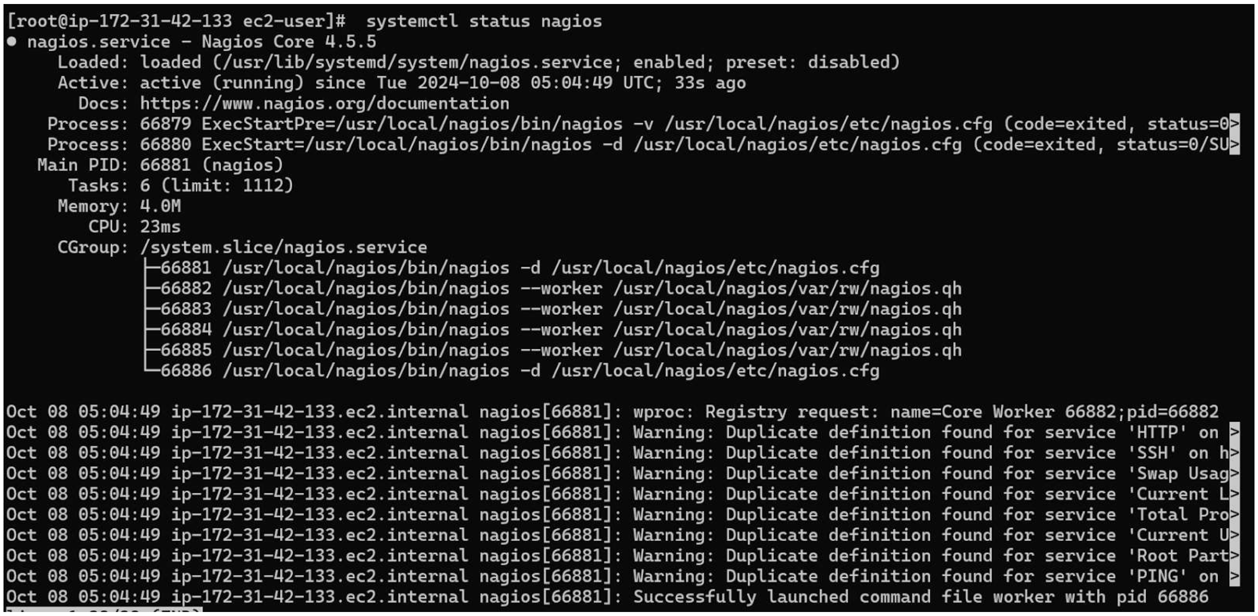
In the end you will see “Total warning” and “total error” as 0, this confirms that the configurations is correct.

8. Now we will restart the nagios server to implement the above made changes.
   service nagios restart



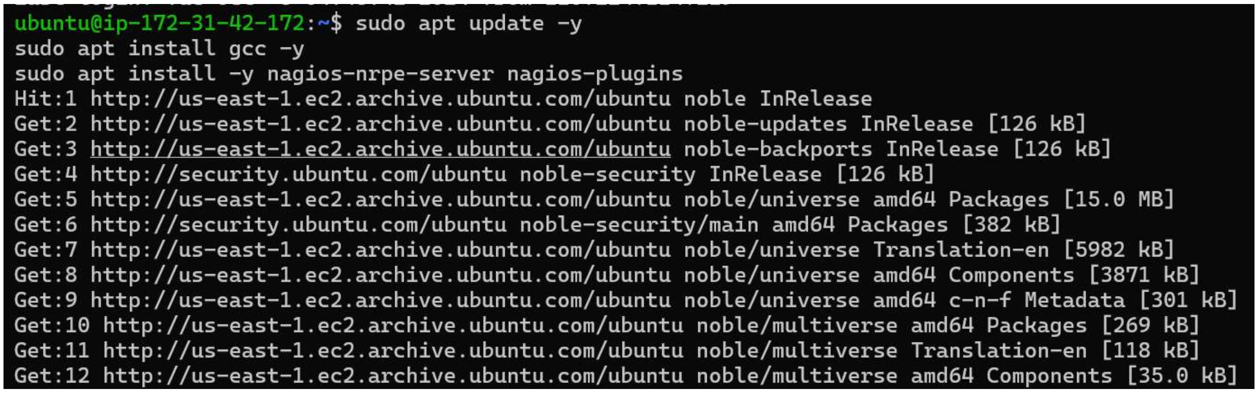
```
[root@ip-172-31-42-133 ec2-user]# service nagios restart
Redirecting to /bin/systemctl restart nagios.service
```

9. systemctl status nagios
   Using the above command, we check the status of the nagios server and ensure that it is active (running).



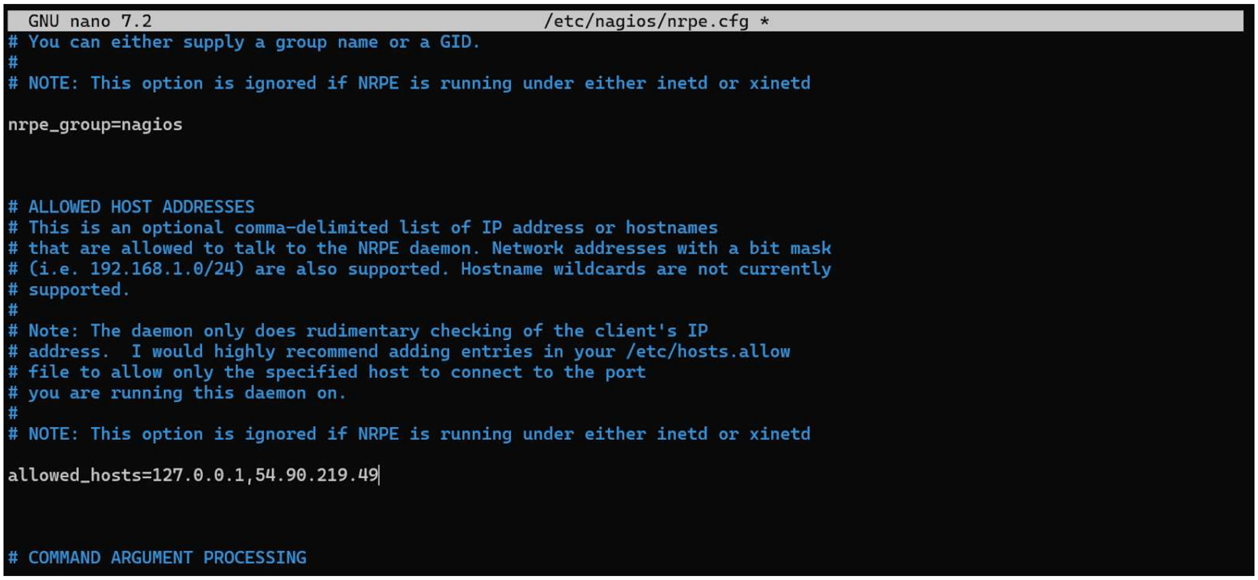
```
[root@ip-172-31-42-133 ec2-user]#  systemctl status nagios
● nagios.service - Nagios Core 4.5.5
     Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Tue 2024-10-08 05:04:49 UTC; 33s ago
       Docs: https://www.nagios.org/documentation
    Process: 66879 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0>
    Process: 66880 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SU>
   Main PID: 66881 (nagios)
      Tasks: 6 (limit: 1112)
     Memory: 4.0M
        CPU: 23ms
     CGroup: /system.slice/nagios.service
             ├─66881 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─66882 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─66883 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─66884 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─66885 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─66886 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: wproc: Registry request: name=Core Worker 66882;pid=66882
Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: Warning: Duplicate definition found for service 'HTTP' on >
Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: Warning: Duplicate definition found for service 'SSH' on h>
Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: Warning: Duplicate definition found for service 'Swap Usag>
Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: Warning: Duplicate definition found for service 'Current L>
Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: Warning: Duplicate definition found for service 'Total Pro>
Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: Warning: Duplicate definition found for service 'Current U>
Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: Warning: Duplicate definition found for service 'Root Part>
Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: Warning: Duplicate definition found for service 'PING' on >
Oct 08 05:04:49 ip-172-31-42-133.ec2.internal nagios[66881]: Successfully launched command file worker with pid 66886
```

10. Now open the terminal which is connected to the ubuntu instance. If not connect, follow the 2nd step in similar fashion to connect to the instance, run the following command in ubuntu instance.
    sudo apt update -y
    sudo apt install gcc -y
    sudo apt install -y nagios-nrpe-server nagios-plugins



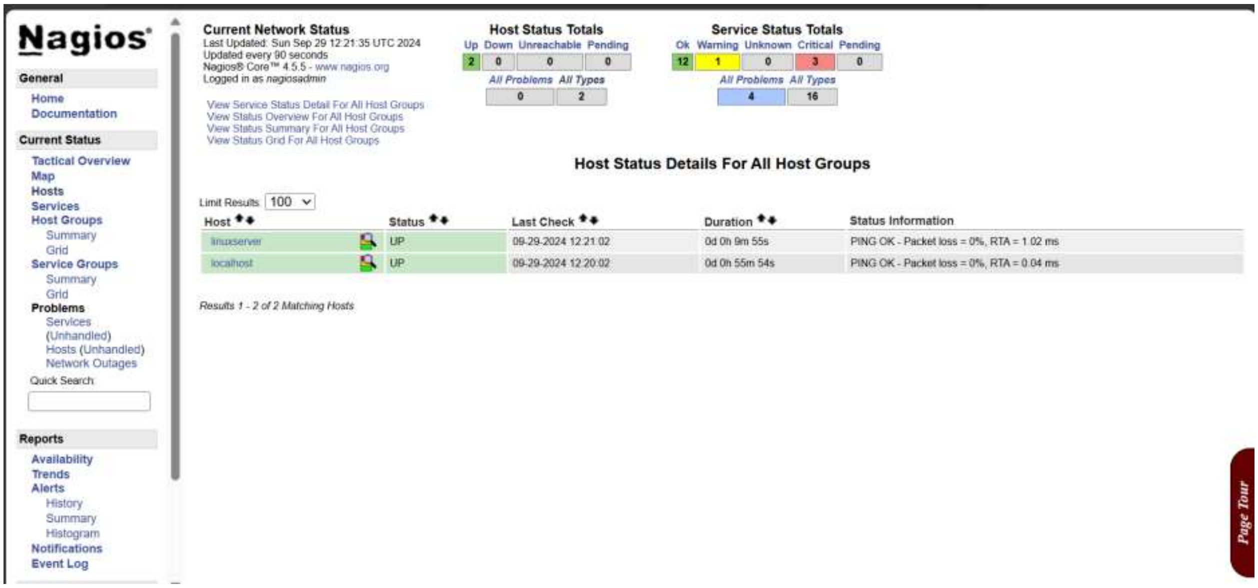
```
ubuntu@ip-172-31-42-172:~$ sudo apt update -y
sudo apt install gcc -y
sudo apt install -y nagios-nrpe-server nagios-plugins
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu 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://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [382 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 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]
```

11. Run the following command:
    sudo nano /etc/nagios/nrpe.cfg
    The above command opens the NRPE config file. Here, we need to add the public IP address of our host nagios-host instance to the NRPE configuration file. Under allowed_hosts, add the nagios-host public IPv4 address. The public ip address can be seen by click on the instance id of the instance in EC2 dashboard.



```
  GNU nano 7.2                                    /etc/nagios/nrpe.cfg *
# You can either supply a group name or a GID.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

nrpe_group=nagios



# ALLOWED HOST ADDRESSES
# This is an optional comma-delimited list of IP address or hostnames
# that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
# (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
# supported.
#
# Note: The daemon only does rudimentary checking of the client's IP
# address.  I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

allowed_hosts=127.0.0.1,54.90.219.49



# COMMAND ARGUMENT PROCESSING
```

12. Once everything is completed, open the nagios dashboard in browser with url http://<publicipaddress>/nagiso. Click on the hosts and we will see that linuxserver has been added as a host



Current Network Status
Last Updated: Sun Sep 29 12:21:35 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.5.5 - www.nagios.org
Logged in as *nagiosadmin*

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

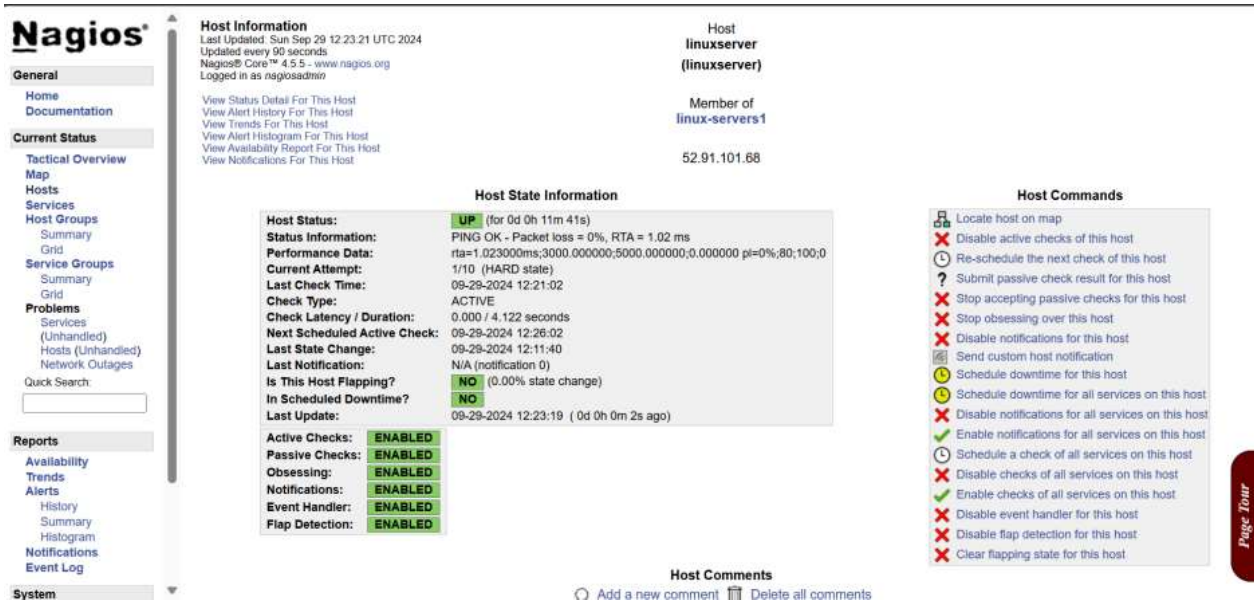
All Problems	*All Types*
4	16

Host Status Details For All Host Groups

Host	Status	Last Check	Duration	Status Information
linuxserver	UP	09-29-2024 12:21:02	0d 0h 9m 55s	PING OK - Packet loss = 0%, RTA = 1.02 ms
localhost	UP	09-29-2024 12:20:02	0d 0h 55m 54s	PING OK - Packet loss = 0%, RTA = 0.04 ms

Results 1 - 2 of 2 Matching Hosts

Click on 'linuxserver'. Here, we can access all information about the 'linuxserver' host.



Host Information
Last Updated: Sun Sep 29 12:23:21 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
linuxserver
(linuxserver)

Member of
linux-servers1

52.91.101.68

Host State Information

Host Status:	UP (for 0d 0h 11m 41s)
Status Information:	PING OK - Packet loss = 0%, RTA = 1.02 ms
Performance Data:	rta=1.023000ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0
Current Attempt:	1/10 (HARD state)
Last Check Time:	09-29-2024 12:21:02
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 4.122 seconds
Next Scheduled Active Check:	09-29-2024 12:26:02
Last State Change:	09-29-2024 12:11:40
Last Notification:	N/A (notification 0)
Is This Host Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	09-29-2024 12:23:19 (0d 0h 0m 2s ago)

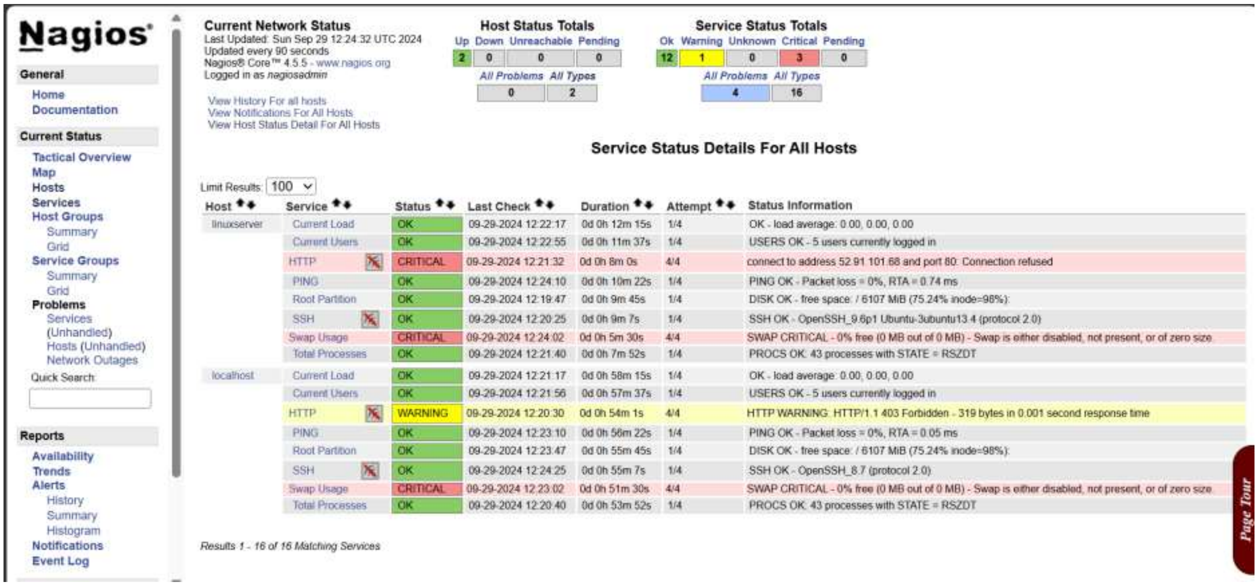
Active Checks:	ENABLED
Passive Checks:	ENABLED
Obsessing:	ENABLED
Notifications:	ENABLED
Event Handler:	ENABLED
Flap Detection:	ENABLED

Host Commands

Locate host on map
✗ Disable active checks of this host
Re-schedule the next check of this host
? Submit passive check result for this host
✗ Stop accepting passive checks for this host
✗ Stop obsessing over this host
✗ Disable notifications for this host
Send custom host notification
Schedule downtime for this host
Schedule downtime for all services on this host
✗ Disable notifications for all services on this host
✓ Enable notifications for all services on this host
Schedule a check of all services on this host
✗ Disable checks of all services on this host
✓ Enable checks of all services on this host
✗ Disable event handler for this host
✗ Disable flap detection for this host
✗ Clear flapping state for this host

Host Comments

Click on ‘Services’. Here, we can see all the services that are being monitored by ‘linuxserver’.



Current Network Status
Last Updated: Sun Sep 29 12:24:32 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.5.5 - www.nagios.org
Logged in as *nagiosadmin*

View History For all hosts
View Notifications For All Hosts
View Host 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
12	1	0	3	0

All Problems	*All Types*
4	16

Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
linuxserver	Current Load	OK	09-29-2024 12:22:17	0d 0h 12m 15s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	09-29-2024 12:22:55	0d 0h 11m 37s	1/4	USERS OK - 5 users currently logged in
	HTTP	CRITICAL	09-29-2024 12:21:32	0d 0h 8m 0s	4/4	connect to address 52.91.101.68 and port 80: Connection refused
	PING	OK	09-29-2024 12:24:10	0d 0h 10m 22s	1/4	PING OK - Packet loss = 0%, RTA = 0.74 ms
	Root Partition	OK	09-29-2024 12:19:47	0d 0h 9m 45s	1/4	DISK OK - free space: / 6107 MiB (75.24% inode=98%):
	SSH	OK	09-29-2024 12:20:25	0d 0h 9m 7s	1/4	SSH OK - OpenSSH_9.6p1 Ubuntu-3ubuntu13.4 (protocol 2.0)
	Swap Usage	CRITICAL	09-29-2024 12:24:02	0d 0h 5m 30s	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	09-29-2024 12:21:40	0d 0h 7m 52s	1/4	PROCS OK: 43 processes with STATE = RSZDT
localhost	Current Load	OK	09-29-2024 12:21:17	0d 0h 58m 15s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	09-29-2024 12:21:56	0d 0h 57m 37s	1/4	USERS OK - 5 users currently logged in
	HTTP	WARNING	09-29-2024 12:20:30	0d 0h 54m 1s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.001 second response time
	PING	OK	09-29-2024 12:23:10	0d 0h 56m 22s	1/4	PING OK - Packet loss = 0%, RTA = 0.05 ms
	Root Partition	OK	09-29-2024 12:23:47	0d 0h 55m 45s	1/4	DISK OK - free space: / 6107 MiB (75.24% inode=98%):
	SSH	OK	09-29-2024 12:24:25	0d 0h 55m 7s	1/4	SSH OK - OpenSSH_8.7 (protocol 2.0)
	Swap Usage	CRITICAL	09-29-2024 12:23:02	0d 0h 51m 30s	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	09-29-2024 12:20:40	0d 0h 53m 52s	1/4	PROCS OK: 43 processes with STATE = RSZDT

Results 1 - 16 of 16 Matching Services

Conclusion:

In this experiment, we successfully performed port, service, and Linux server monitoring using Nagios. After setting up a new Ubuntu EC2 instance, we configured it as a monitored client by creating appropriate Nagios configuration files and modifying the host instance's settings. We installed the Nagios NRPE server and plugins on the Ubuntu instance, added the public IP of the Nagios host to the NRPE config file, and verified the changes in the Nagios dashboard.