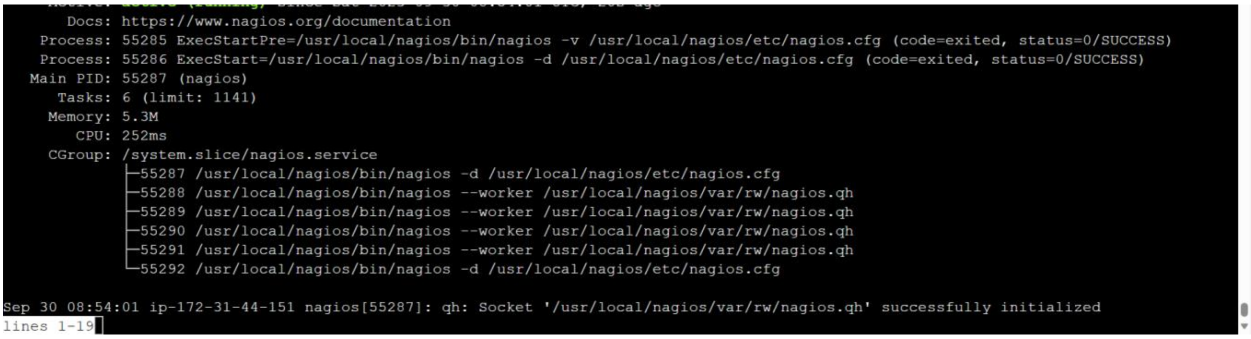
# Experiment 10

**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”.



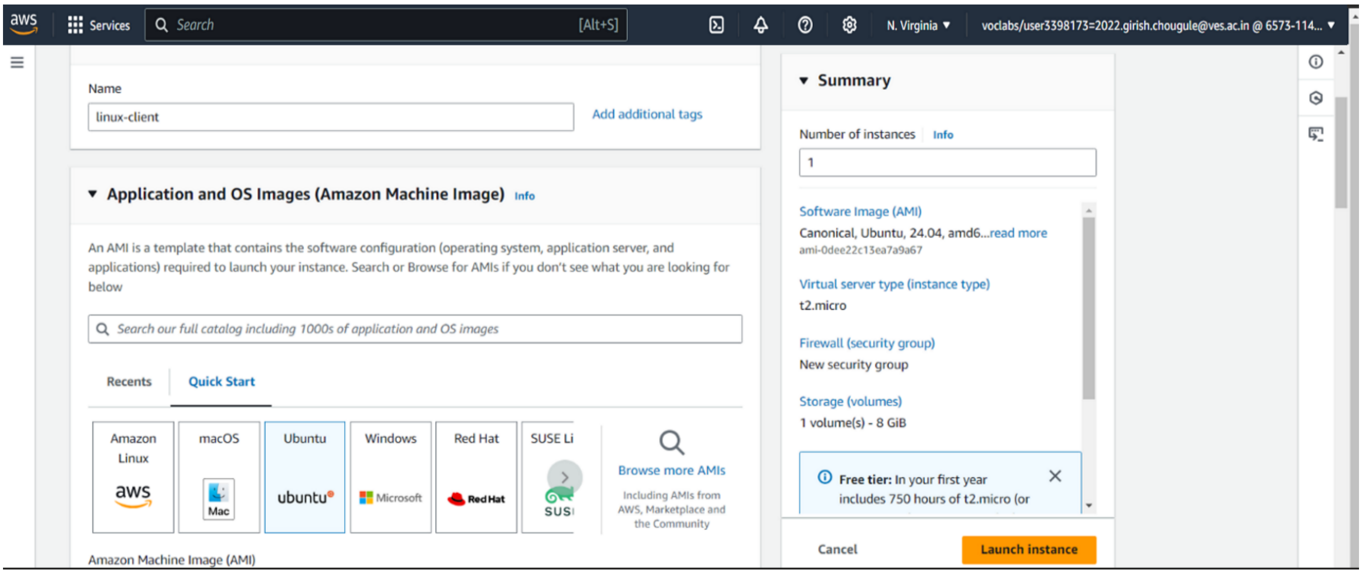
```
     Docs: https://www.nagios.org/documentation
  Process: 55285 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
  Process: 55286 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Main PID: 55287 (nagios)
    Tasks: 6 (limit: 1141)
   Memory: 5.3M
      CPU: 252ms
   CGroup: /system.slice/nagios.service
           ├─55287 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
           ├─55288 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─55289 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─55290 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           ├─55291 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
           └─55292 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 08:54:01 ip-172-31-44-151 nagios[55287]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
lines 1-19
```

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.



aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3398173=2022.girish.chougule@ves.ac.in @ 6573-114...

Name: linux-client

**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 Li
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)

**Summary**

Number of instances: 1

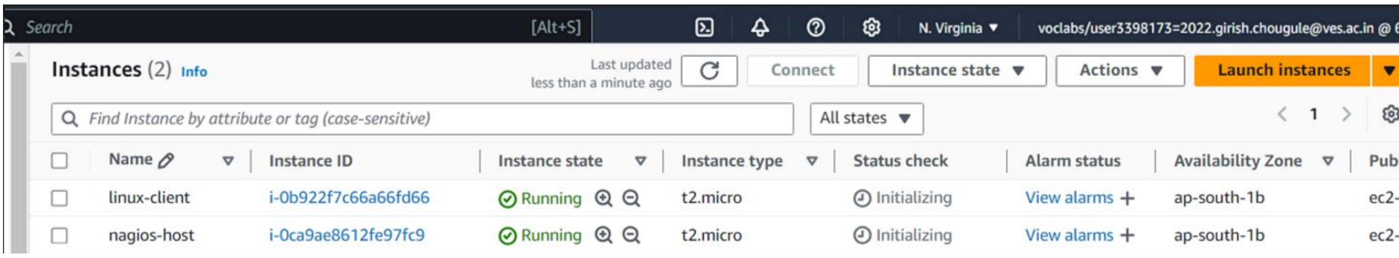
Software Image (AMI): Canonical, Ubuntu, 24.04, amd6...read more ami-0dee22c13ea7a9a67

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or


Search [Alt+S]
N. Virginia
voclabs/user3398173=2022.girish.chougule@ves.ac.in @
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
1

| | Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Pub |
|---|---|---|---|---|---|---|---|---|
| □ | linux-client | i-0b922f7c66a66fd66 | Running | t2.micro | Initializing | View alarms + | ap-south-1b | ec2- |
| □ | nagios-host | i-0ca9ae8612fe97fc9 | Running | t2.micro | Initializing | View alarms + | ap-south-1b | ec2- |

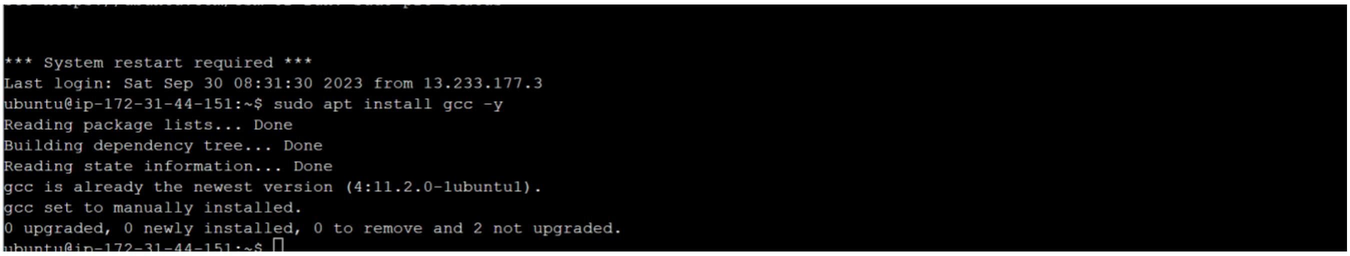
**For now, leave this machine as is, and go back to your nagios HOST machine**.

**Step 3:** On client side make a package index update and install gcc, nagios-nrpe-server and the plugins.

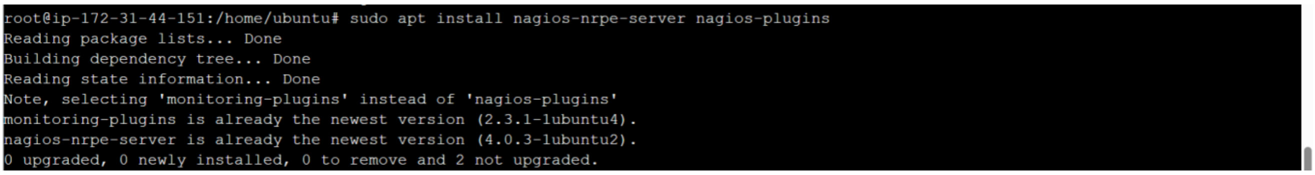
sudo apt update -y

sudo apt install gcc -y

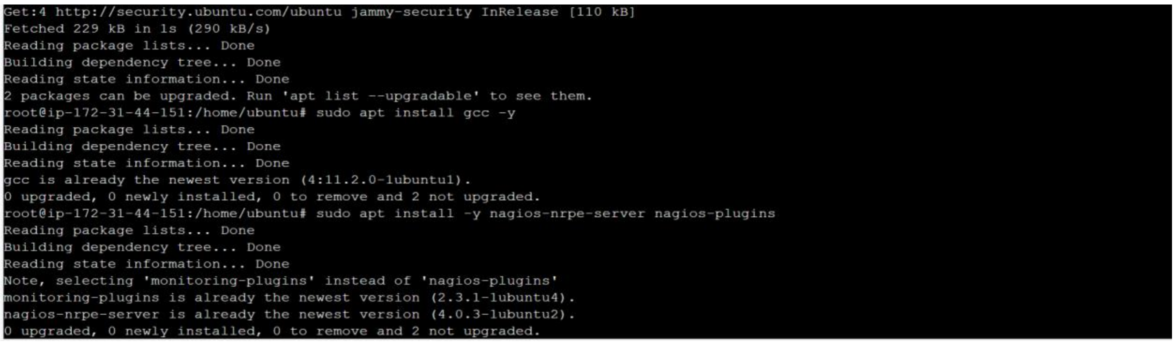
sudo apt install -y nagios-nrpe-server nagios-plugins



```
*** System restart required ***
Last login: Sat Sep 30 08:31:30 2023 from 13.233.177.3
ubuntu@ip-172-31-44-151:~$ sudo apt install gcc -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gcc is already the newest version (4:11.2.0-1ubuntu1).
gcc set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
ubuntu@ip-172-31-44-151:~$ 
```



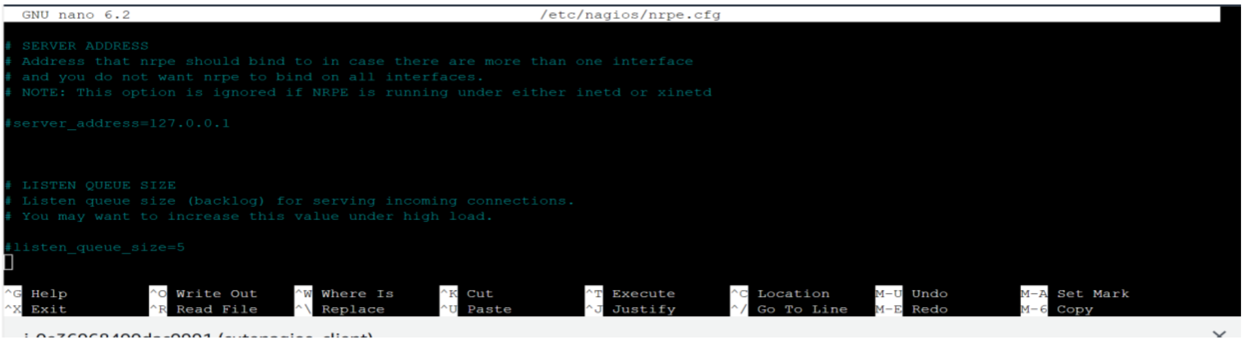
```
root@ip-172-31-44-151:/home/ubuntu# sudo apt install nagios-nrpe-server nagios-plugins
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
monitoring-plugins is already the newest version (2.3.1-1ubuntu4).
nagios-nrpe-server is already the newest version (4.0.3-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
```



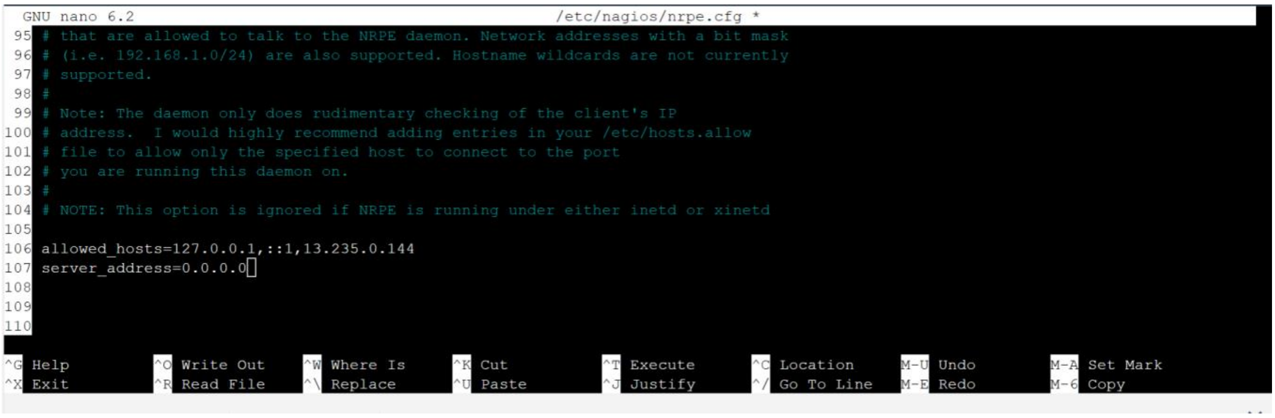
```
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 229 kB in 1s (290 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ip-172-31-44-151:/home/ubuntu# sudo apt install gcc -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gcc is already the newest version (4:11.2.0-1ubuntu1).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
root@ip-172-31-44-151:/home/ubuntu# 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'
monitoring-plugins is already the newest version (2.3.1-1ubuntu4).
nagios-nrpe-server is already the newest version (4.0.3-1ubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
```

**Step 4:** Open nrpe.cfg file to make changes.

sudo nano /etc/nagios/nrpe.cfg



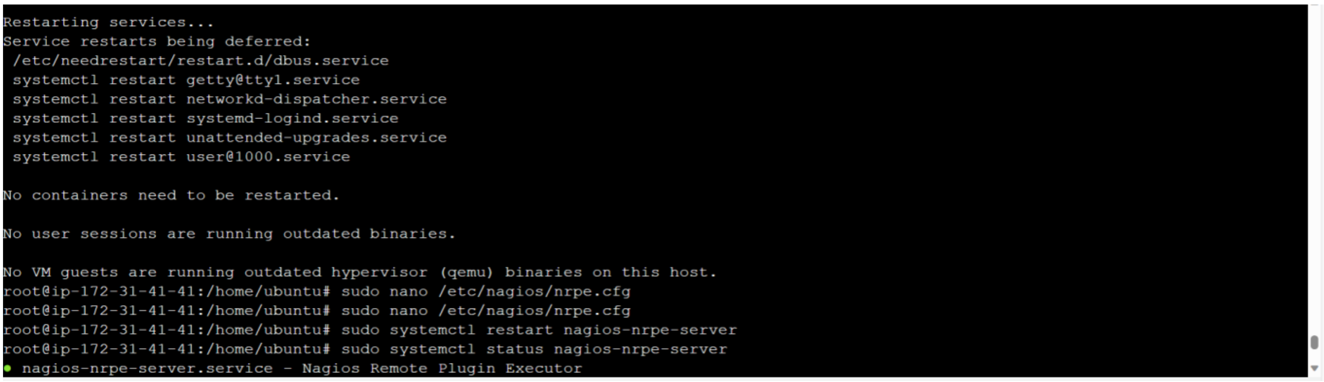
```
GNU nano 6.2                                   /etc/nagios/nrpe.cfg

# SERVER ADDRESS
# Address that nrpe should bind to in case there are more than one interface
# and you do not want nrpe to bind on all interfaces.
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

#server_address=127.0.0.1


# LISTEN QUEUE SIZE
# Listen queue size (backlog) for serving incoming connections.
# You may want to increase this value under high load.

#listen_queue_size=5

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy
```



```
GNU nano 6.2                                   /etc/nagios/nrpe.cfg *
# 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,::1,13.235.0.144
server_address=0.0.0.0




^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy
```

**Step 5:** Restart the NRPE server

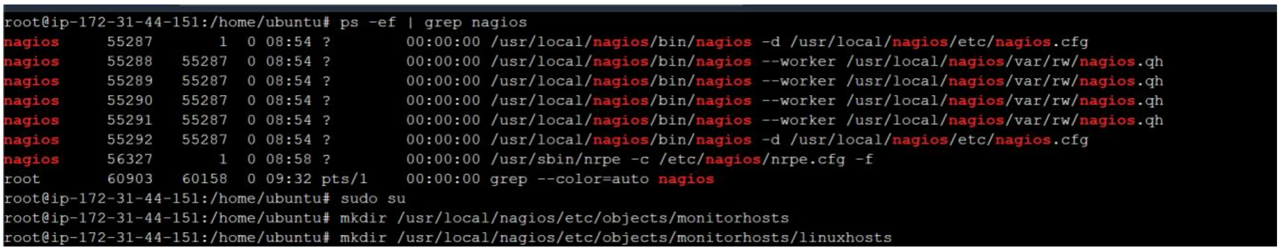
sudo systemctl restart nagios-nrpe-server



```
Restarting services...
Service restarts being deferred:
 /etc/needrestart/restart.d/dbus.service
 systemctl restart getty@tty1.service
 systemctl restart networkd-dispatcher.service
 systemctl restart systemd-logind.service
 systemctl restart unattended-upgrades.service
 systemctl restart user@1000.service

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.
root@ip-172-31-41-41:/home/ubuntu# sudo nano /etc/nagios/nrpe.cfg
root@ip-172-31-41-41:/home/ubuntu# sudo nano /etc/nagios/nrpe.cfg
root@ip-172-31-41-41:/home/ubuntu# sudo systemctl restart nagios-nrpe-server
root@ip-172-31-41-41:/home/ubuntu# sudo systemctl status nagios-nrpe-server
● nagios-nrpe-server.service - Nagios Remote Plugin Executor
```

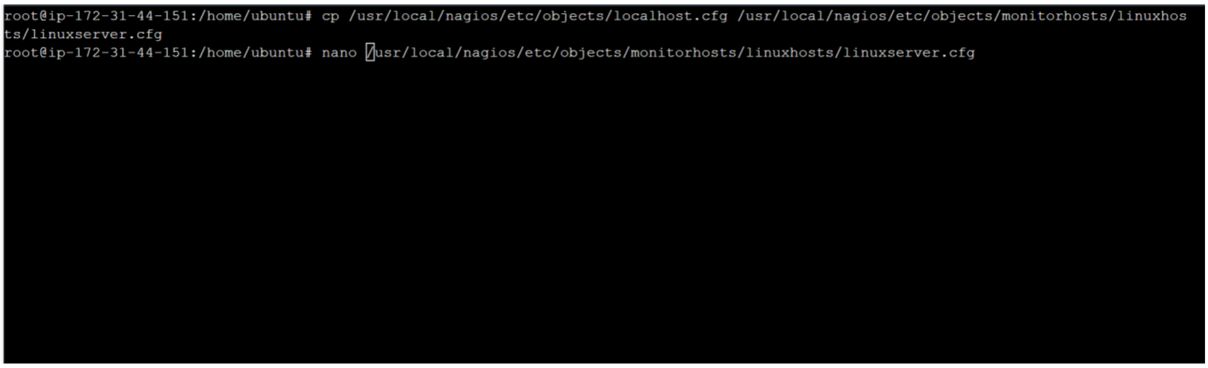
**Step 6:** On the server run this command

ps -ef | grep nagios



```
root@ip-172-31-44-151:/home/ubuntu# ps -ef | grep nagios
nagios     55287       1  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     55288   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     55289   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     55290   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     55291   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     55292   55287  0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     56327       1  0 08:58 ?        00:00:00 /usr/sbin/nrpe -c /etc/nagios/nrpe.cfg -f
root       60903   60158  0 09:32 pts/1    00:00:00 grep --color=auto nagios
root@ip-172-31-44-151:/home/ubuntu# sudo su
root@ip-172-31-44-151:/home/ubuntu# mkdir /usr/local/nagios/etc/objects/monitorhosts
root@ip-172-31-44-151:/home/ubuntu# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
```

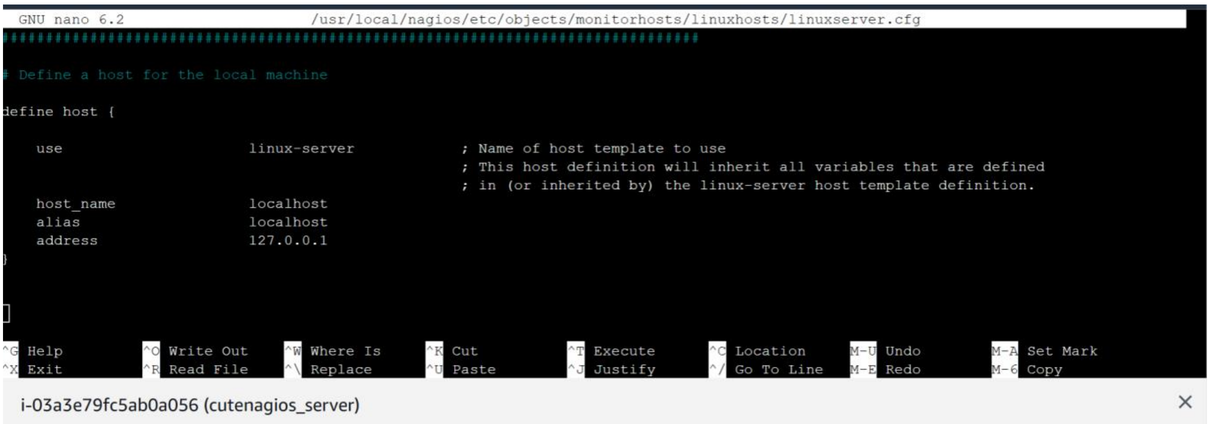
**Step 7:** Become a root user and create 2 folders 1.sudo su 2.mkdir /usr/local/nagios/etc/objects/monitorhosts 3.mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts Copy the sample localhost.cfg file to linuxhost folder 4.cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg



```
root@ip-172-31-44-151:/home/ubuntu# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhos
ts/linuxserver.cfg
root@ip-172-31-44-151:/home/ubuntu# nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

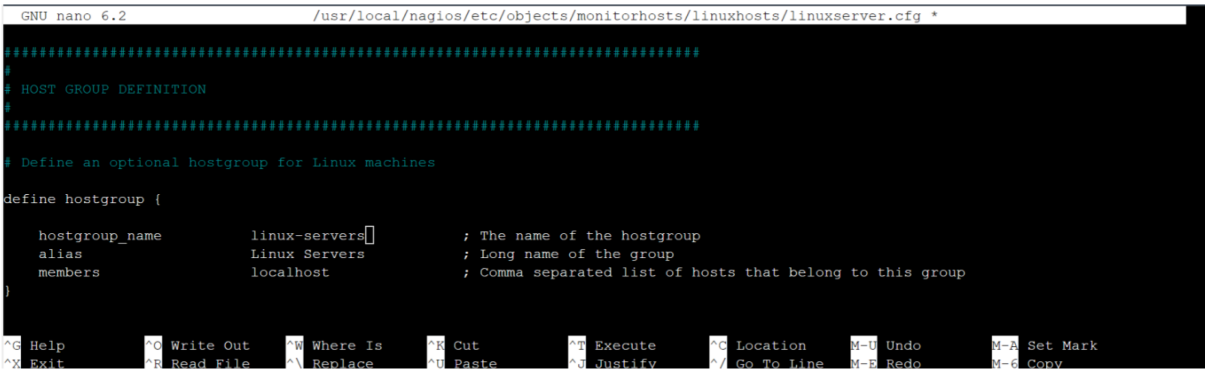
**Step 8:** Open linuxserver.cfg using nano and make the following changes

nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg Change the hostname to linux server (EVERYWHERE ON THE FILE) Change address to the public IP address of your LINUX CLIENT.



```
 GNU nano 6.2                    /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
###############################################################################

# 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               localhost
    alias                   localhost
    address                 127.0.0.1
}


^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

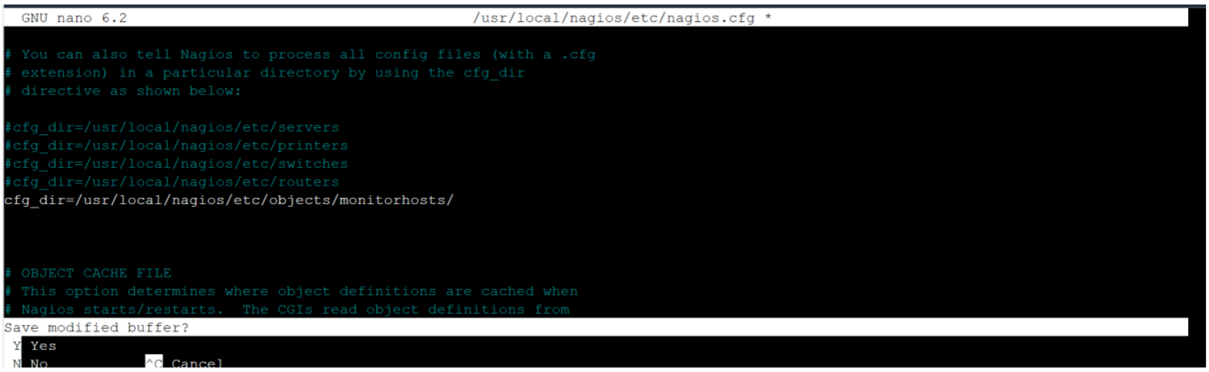
i-03a3e79fc5ab0a056 (cutenagios_server) ×



```
 GNU nano 6.2                    /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg *

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

# Define an optional hostgroup for Linux machines

define hostgroup {

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

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy
```

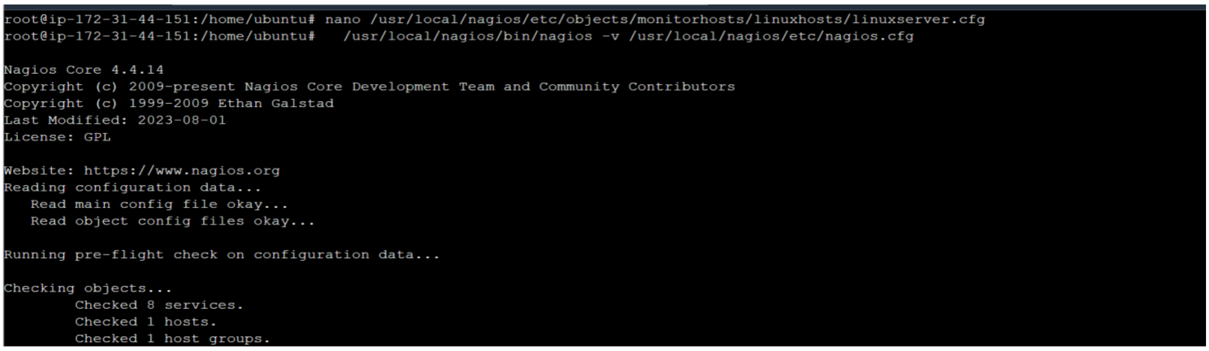
Change hostgroup_name under hostgroup to linux-servers1

**Step 9:** 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/

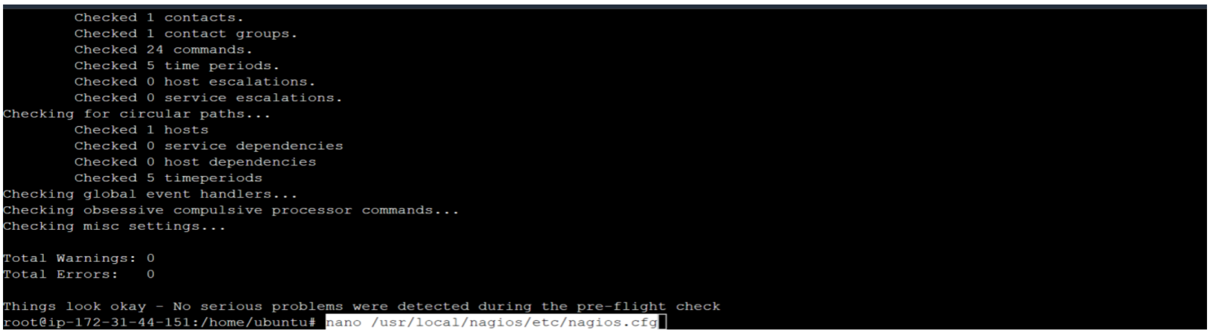


```
  GNU nano 6.2                                       /usr/local/nagios/etc/nagios.cfg *

# 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/



# OBJECT CACHE FILE
# This option determines where object definitions are cached when
# Nagios starts/restarts.  The CGIs read object definitions from
Save modified buffer?
 Y Yes
 N No             ^C Cancel
```

**Step 10:** Verify the configuration files.



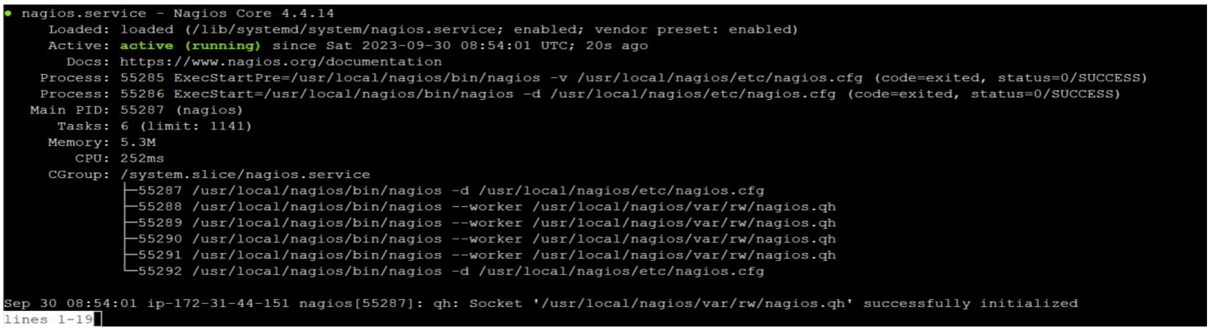
```
root@ip-172-31-44-151:/home/ubuntu# nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
root@ip-172-31-44-151:/home/ubuntu#   /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.4.14
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2023-08-01
License: GPL

Website: https://www.nagios.org
Reading configuration data...
   Read main config file okay...
   Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
        Checked 8 services.
        Checked 1 hosts.
        Checked 1 host 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 1 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-172-31-44-151:/home/ubuntu# nano /usr/local/nagios/etc/nagios.cfg
```

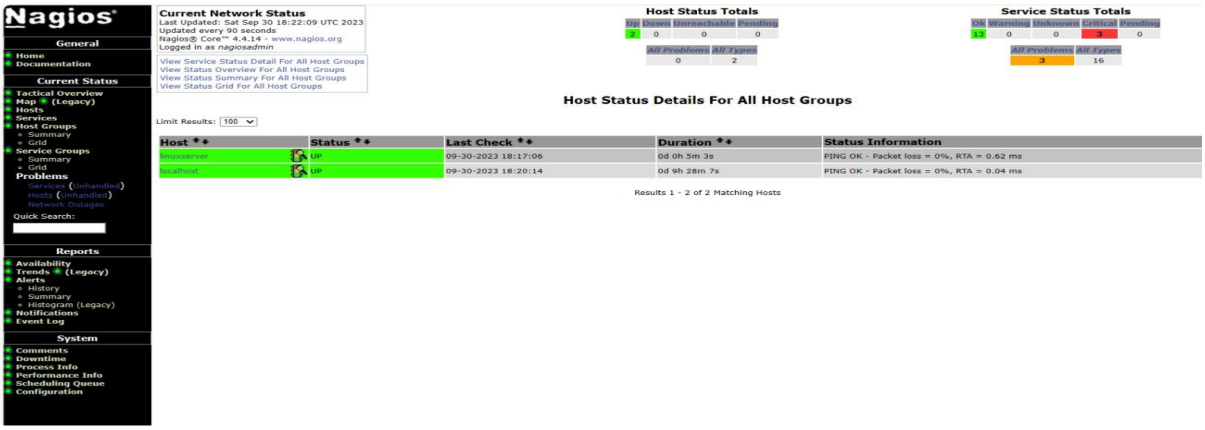
**Step 11:** Restart the nagios service service nagios restart

Sudo systemctl status nagios



```
● nagios.service - Nagios Core 4.4.14
     Loaded: loaded (/lib/systemd/system/nagios.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-09-30 08:54:01 UTC; 20s ago
       Docs: https://www.nagios.org/documentation
    Process: 55285 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
    Process: 55286 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
   Main PID: 55287 (nagios)
      Tasks: 6 (limit: 1141)
     Memory: 5.3M
        CPU: 252ms
     CGroup: /system.slice/nagios.service
             ├─55287 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─55288 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─55289 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─55290 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─55291 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─55292 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 08:54:01 ip-172-31-44-151 nagios[55287]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
lines 1-19
```

**Step 12:** Now, check your nagios dashboard and you'll see a new host being added.



Current Network Status
Last Updated: Sat Sep 30 18:22:09 UTC 2023
Updated every 90 seconds
Nagios® Core™ 4.4.14 - 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 |
|---|---|---|---|---|
| 13 | 0 | 0 | 3 | 0 |

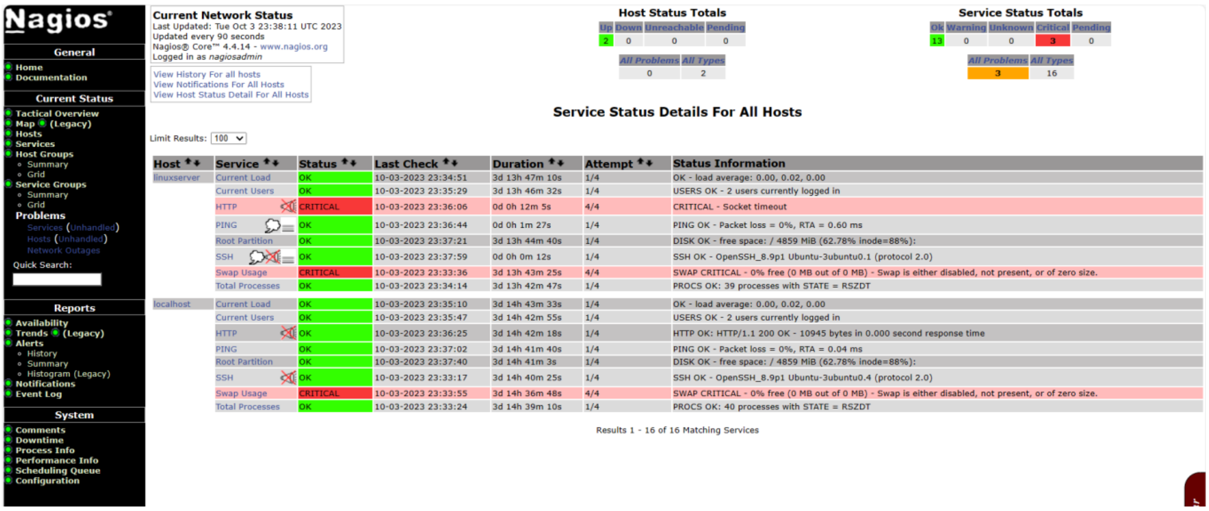
| All Problems | All Types |
|---|---|
| 3 | 16 |

Host Status Details For All Host Groups

Limit Results: 100

| Host | Status | Last Check | Duration | Status Information |
|---|---|---|---|---|
| linuxserver | UP | 09-30-2023 18:17:06 | 0d 0h 5m 3s | PING OK - Packet loss = 0%, RTA = 0.62 ms |
| localhost | UP | 09-30-2023 18:20:14 | 0d 9h 28m 7s | PING OK - Packet loss = 0%, RTA = 0.04 ms |

Results 1 - 2 of 2 Matching Hosts



Current Network Status
Last Updated: Tue Oct 3 23:38:11 UTC 2023
Updated every 90 seconds
Nagios® Core™ 4.4.14 - 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 |
|---|---|---|---|---|
| 13 | 0 | 0 | 3 | 0 |

| All Problems | All Types |
|---|---|
| 3 | 16 |

Service Status Details For All Hosts

Limit Results: 100

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---|---|---|---|---|---|---|
| linuxserver | Current Load | OK | 10-03-2023 23:34:51 | 3d 13h 47m 10s | 1/4 | OK - load average: 0.00, 0.02, 0.00 |
| | Current Users | OK | 10-03-2023 23:35:29 | 3d 13h 46m 32s | 1/4 | USERS OK - 2 users currently logged in |
| | HTTP | CRITICAL | 10-03-2023 23:36:06 | 0d 0h 12m 5s | 4/4 | CRITICAL - Socket timeout |
| | PING | OK | 10-03-2023 23:36:44 | 0d 0h 1m 27s | 1/4 | PING OK - Packet loss = 0%, RTA = 0.60 ms |
| | Root Partition | OK | 10-03-2023 23:37:21 | 3d 13h 44m 40s | 1/4 | DISK OK - free space: / 4859 MiB (62.78% inode=88%): |
| | SSH | OK | 10-03-2023 23:37:59 | 0d 0h 0m 12s | 1/4 | SSH OK - OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 (protocol 2.0) |
| | Swap Usage | CRITICAL | 10-03-2023 23:33:36 | 3d 13h 43m 25s | 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 | 10-03-2023 23:34:14 | 3d 13h 42m 47s | 1/4 | PROCS OK: 39 processes with STATE = RSZDT |
| localhost | Current Load | OK | 10-03-2023 23:35:10 | 3d 14h 43m 33s | 1/4 | OK - load average: 0.00, 0.02, 0.00 |
| | Current Users | OK | 10-03-2023 23:35:47 | 3d 14h 42m 55s | 1/4 | USERS OK - 2 users currently logged in |
| | HTTP | OK | 10-03-2023 23:36:25 | 3d 14h 42m 18s | 1/4 | HTTP OK: HTTP/1.1 200 OK - 10945 bytes in 0.000 second response time |
| | PING | OK | 10-03-2023 23:37:02 | 3d 14h 41m 40s | 1/4 | PING OK - Packet loss = 0%, RTA = 0.04 ms |
| | Root Partition | OK | 10-03-2023 23:37:40 | 3d 14h 41m 3s | 1/4 | DISK OK - free space: / 4859 MiB (62.78% inode=88%): |
| | SSH | OK | 10-03-2023 23:33:17 | 3d 14h 40m 25s | 1/4 | SSH OK - OpenSSH_8.9p1 Ubuntu-3ubuntu0.4 (protocol 2.0) |
| | Swap Usage | CRITICAL | 10-03-2023 23:33:55 | 3d 14h 36m 48s | 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 | 10-03-2023 23:33:24 | 3d 14h 39m 10s | 1/4 | PROCS OK: 40 processes with STATE = RSZDT |

Results 1 - 16 of 16 Matching Services

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.