Snehal Patil   D15A   39

Advanced DevOps Lab

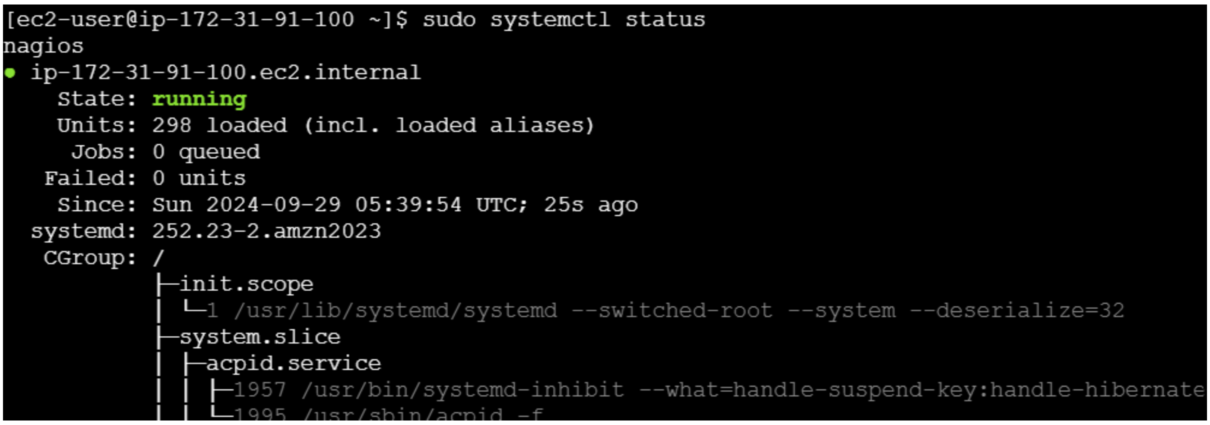
Experiment No: 10

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".

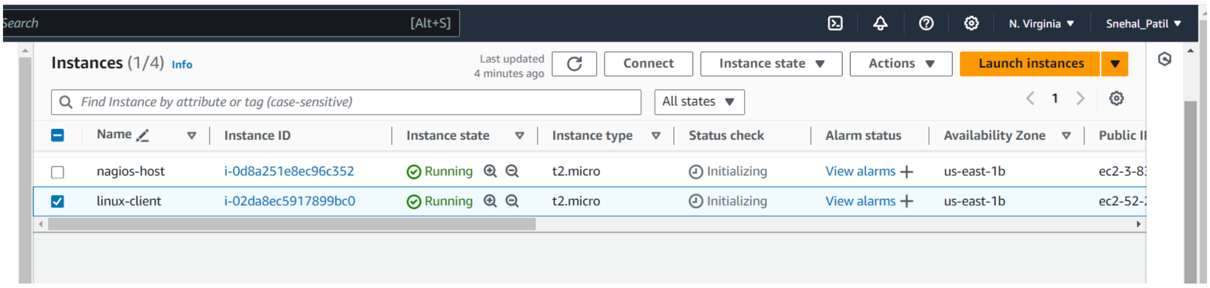


```
[ec2-user@ip-172-31-91-100 ~]$ sudo systemctl status
nagios
● ip-172-31-91-100.ec2.internal
    State: running
    Units: 298 loaded (incl. loaded aliases)
     Jobs: 0 queued
   Failed: 0 units
    Since: Sun 2024-09-29 05:39:54 UTC; 25s ago
  systemd: 252.23-2.amzn2023
   CGroup: /
           ├─init.scope
           │ └─1 /usr/lib/systemd/systemd --switched-root --system --deserialize=32
           ├─system.slice
           │ ├─acpid.service
           │ │ ├─1957 /usr/bin/systemd-inhibit --what=handle-suspend-key:handle-hibernate
           │ │ └─1995 /usr/sbin/acpid -f
```

You can proceed if you get this message.

Before we begin,

2. 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.



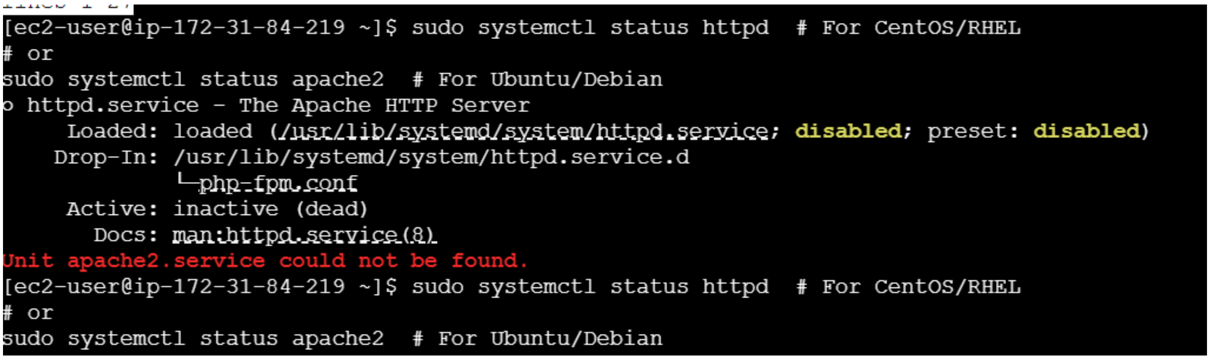
☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public I
☐	nagios-host	i-0d8a251e8ec96c352	Running	t2.micro	Initializing	View alarms +	us-east-1b	ec2-3-8
☑	linux-client	i-02da8ec5917899bc0	Running	t2.micro	Initializing	View alarms +	us-east-1b	ec2-52-

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

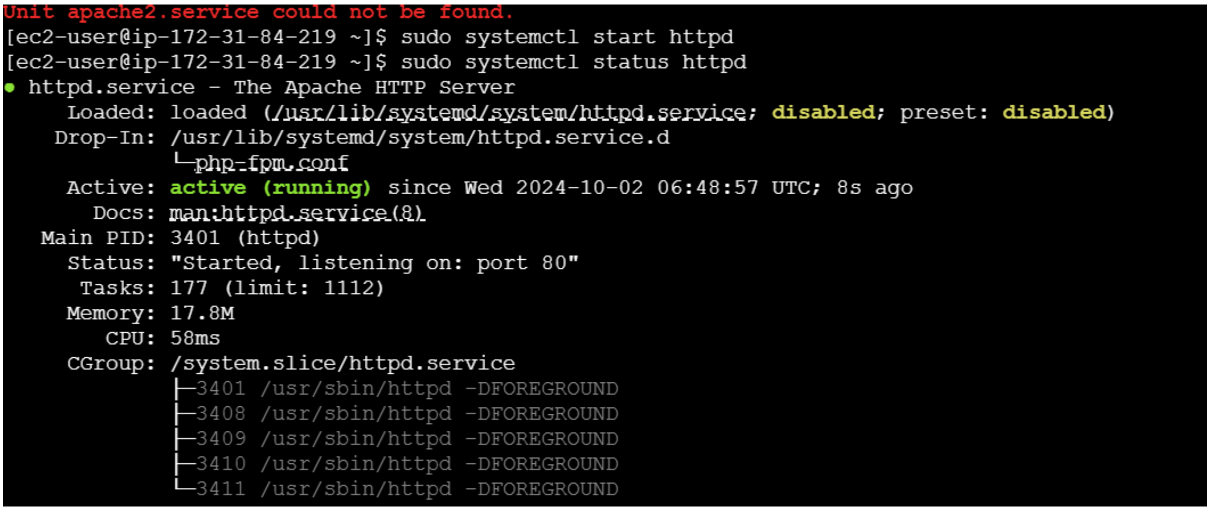
Extra:

Apache Server was Not Running

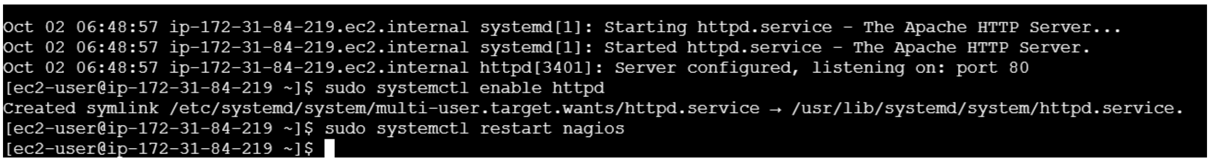
Problem: Unable to access the Nagios web interface due to the Apache HTTP server not running.



```
[ec2-user@ip-172-31-84-219 ~]$ sudo systemctl status httpd  # For CentOS/RHEL
# or
sudo systemctl status apache2  # For Ubuntu/Debian
○ 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: inactive (dead)
       Docs: man:httpd.service(8)
Unit apache2.service could not be found.
[ec2-user@ip-172-31-84-219 ~]$ sudo systemctl status httpd  # For CentOS/RHEL
# or
sudo systemctl status apache2  # For Ubuntu/Debian
```



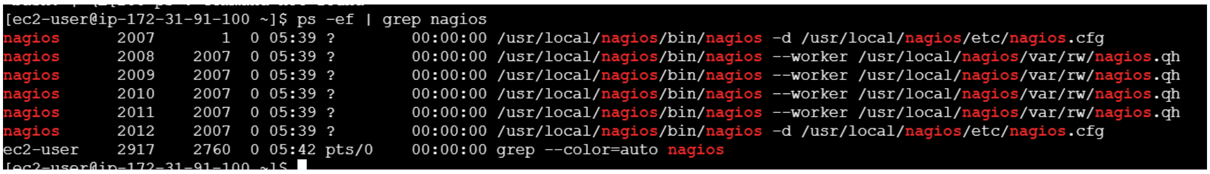
```
Unit apache2.service could not be found.
[ec2-user@ip-172-31-84-219 ~]$ sudo systemctl start httpd
[ec2-user@ip-172-31-84-219 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
    Drop-In: /usr/lib/systemd/system/httpd.service.d
             └─php-fpm.conf
     Active: active (running) since Wed 2024-10-02 06:48:57 UTC; 8s ago
       Docs: man:httpd.service(8)
   Main PID: 3401 (httpd)
     Status: "Started, listening on: port 80"
      Tasks: 177 (limit: 1112)
     Memory: 17.8M
        CPU: 58ms
     CGroup: /system.slice/httpd.service
             ├─3401 /usr/sbin/httpd -DFOREGROUND
             ├─3408 /usr/sbin/httpd -DFOREGROUND
             ├─3409 /usr/sbin/httpd -DFOREGROUND
             ├─3410 /usr/sbin/httpd -DFOREGROUND
             └─3411 /usr/sbin/httpd -DFOREGROUND
```



```
Oct 02 06:48:57 ip-172-31-84-219.ec2.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Oct 02 06:48:57 ip-172-31-84-219.ec2.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Oct 02 06:48:57 ip-172-31-84-219.ec2.internal httpd[3401]: Server configured, listening on: port 80
[ec2-user@ip-172-31-84-219 ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-172-31-84-219 ~]$ sudo systemctl restart nagios
[ec2-user@ip-172-31-84-219 ~]$ 
```

3. On the server, run this command

ps -ef | grep nagios



```
[ec2-user@ip-172-31-91-100 ~]$ ps -ef | grep nagios
nagios      2007      1  0 05:39 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios      2008   2007  0 05:39 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      2009   2007  0 05:39 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      2010   2007  0 05:39 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      2011   2007  0 05:39 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      2012   2007  0 05:39 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user    2917   2760  0 05:42 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-91-100 ~]$ 
```

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.

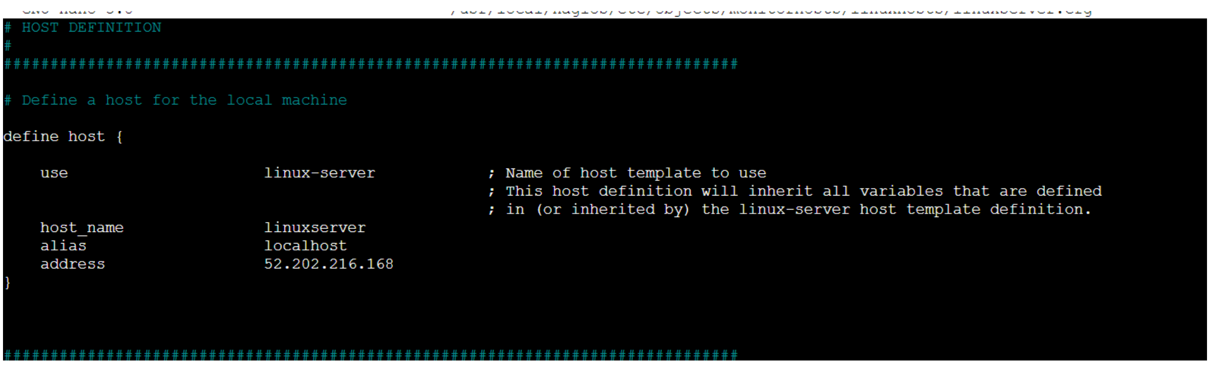
```
cp /usr/local/nagios/etc/objects/localhost.cfg
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

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

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

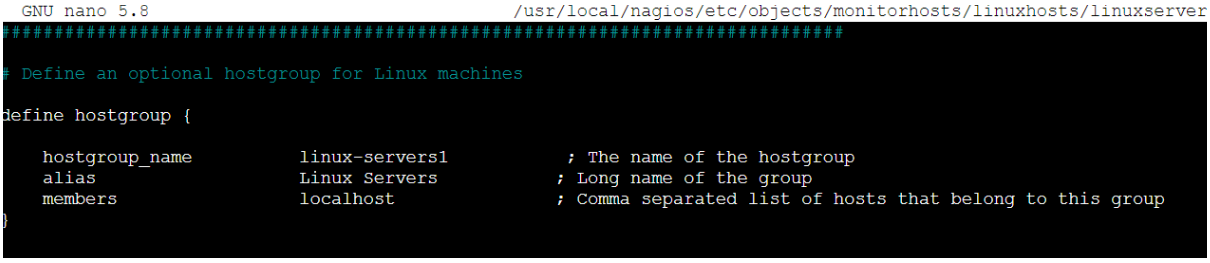
Change the hostname to linuxserver (EVERYWHERE ON THE FILE)

Change address to the public IP address of your LINUX CLIENT.



```
  GNU nano 5.8                    /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
# 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                   localhost
    address                 52.202.216.168
}


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

Change hostgroup_name under hostgroup to linux-servers1



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

# 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                 localhost               ; Comma separated list of hosts that belong to this group
}
```

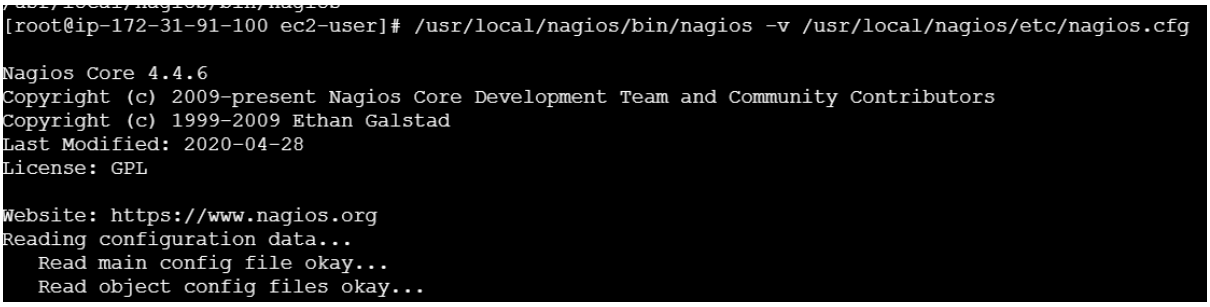
7. Open the Nagios Config file and add the following line

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

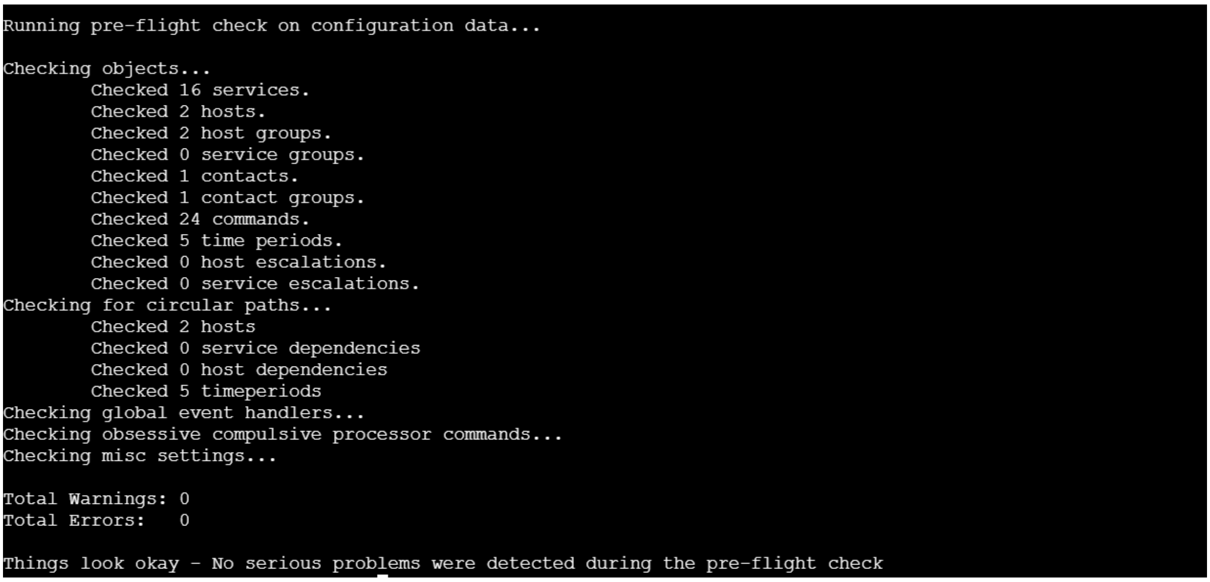
##Add this line

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

8. Verify the configuration files



```
/usr/local/nagios/bin/nagios
[root@ip-172-31-91-100 ec2-user]# /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.4.6
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2020-04-28
License: GPL

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



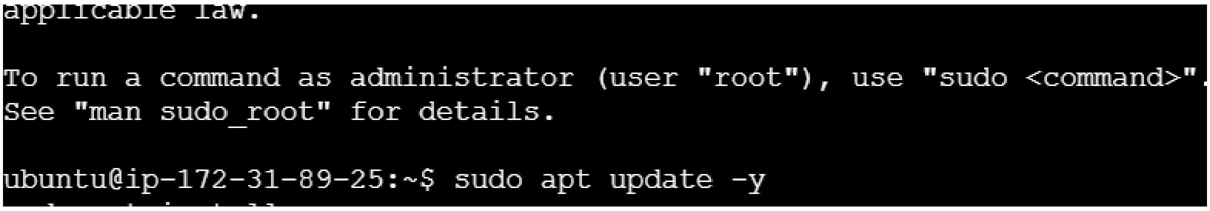
```
Running pre-flight check on configuration data...

Checking objects...
        Checked 16 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
```

You are good to go if there are no errors.

9. Restart the nagios service

service nagios restart

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



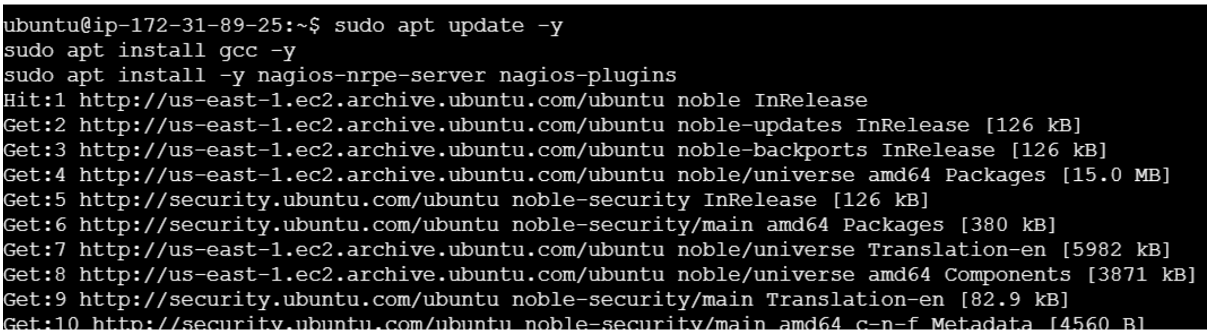
```
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-89-25:~$ sudo apt update -y
```

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-172-31-89-25:~$ 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://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]
Get:5 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [380 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://security.ubuntu.com/ubuntu noble-security/main Translation-en [82.9 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4560 B]
```

12. Open nrpe.cfg file to make changes.

sudo nano /etc/nagios/nrpe.cfg

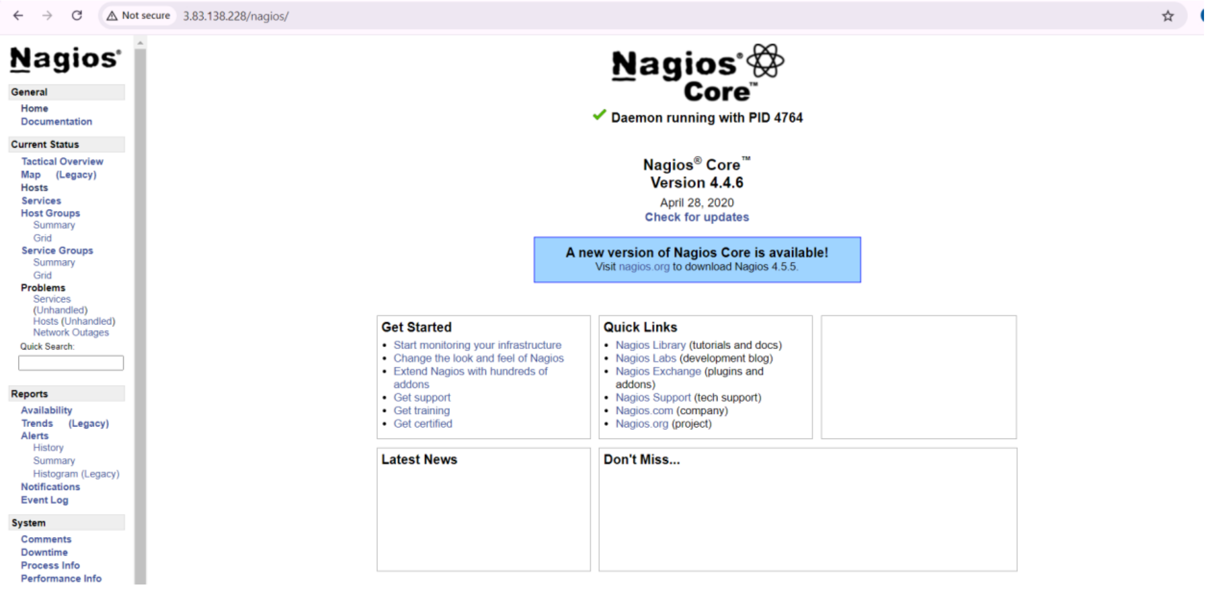
Under allowed_hosts, add your nagios host IP address like so

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.



✓ Daemon running with PID 4764

Nagios® Core™
Version 4.4.6
April 28, 2020
Check for updates

A new version of Nagios Core is available!
Visit nagios.org to download Nagios 4.5.5.

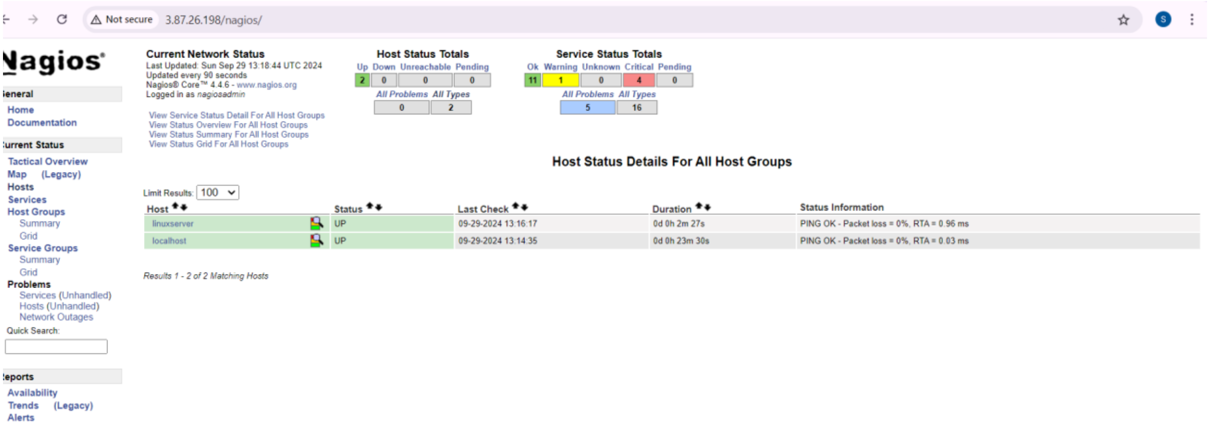
Get Started
- Start monitoring your infrastructure
- Change the look and feel of Nagios
- Extend Nagios with hundreds of addons
- Get support
- Get training
- Get certified

Quick Links
- Nagios Library (tutorials and docs)
- Nagios Labs (development blog)
- Nagios Exchange (plugins and addons)
- Nagios Support (tech support)
- Nagios.com (company)
- Nagios.org (project)

Latest News

Don't Miss...

Now here we can see there is a host added



Current Network Status
Last Updated: Sun Sep 29 13:18:44 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - 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
11	1	0	4	0

All Problems	All Types
5	16

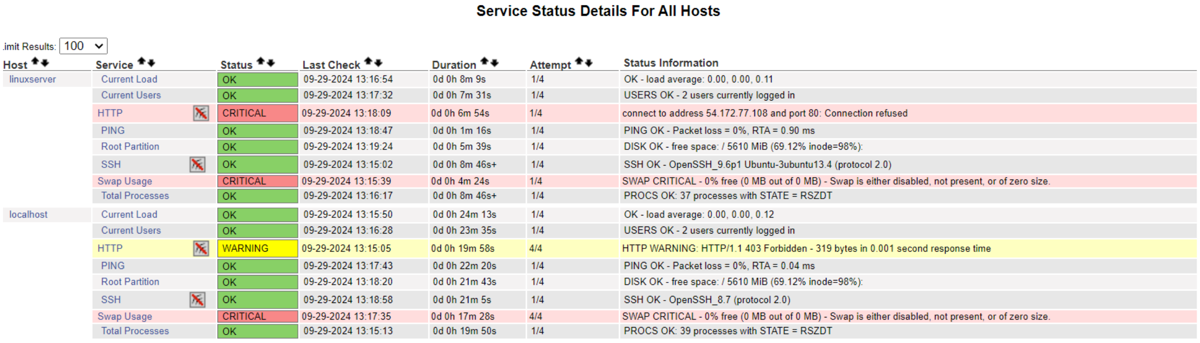
Host Status Details For All Host Groups

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
linuxserver	UP	09-29-2024 13:16:17	0d 0h 2m 27s	PING OK - Packet loss = 0%, RTA = 0.96 ms
localhost	UP	09-29-2024 13:14:35	0d 0h 23m 30s	PING OK - Packet loss = 0%, RTA = 0.03 ms

Results 1 - 2 of 2 Matching Hosts

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



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 13:16:54	0d 0h 8m 9s	1/4	OK - load average: 0.00, 0.00, 0.11
	Current Users	OK	09-29-2024 13:17:32	0d 0h 7m 31s	1/4	USERS OK - 2 users currently logged in
	HTTP	CRITICAL	09-29-2024 13:18:09	0d 0h 6m 54s	1/4	connect to address 54.172.77.108 and port 80: Connection refused
	PING	OK	09-29-2024 13:18:47	0d 0h 1m 16s	1/4	PING OK - Packet loss = 0%, RTA = 0.90 ms
	Root Partition	OK	09-29-2024 13:19:24	0d 0h 5m 39s	1/4	DISK OK - free space: / 5610 MiB (69.12% inode=98%):
	SSH	OK	09-29-2024 13:15:02	0d 0h 8m 46s+	1/4	SSH OK - OpenSSH_9.6p1 Ubuntu-3ubuntu13.4 (protocol 2.0)
	Swap Usage	CRITICAL	09-29-2024 13:15:39	0d 0h 4m 24s	1/4	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 13:16:17	0d 0h 8m 46s+	1/4	PROCS OK: 37 processes with STATE = RSZDT
localhost	Current Load	OK	09-29-2024 13:15:50	0d 0h 24m 13s	1/4	OK - load average: 0.00, 0.00, 0.12
	Current Users	OK	09-29-2024 13:16:28	0d 0h 23m 35s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	09-29-2024 13:15:05	0d 0h 19m 58s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.001 second response time
	PING	OK	09-29-2024 13:17:43	0d 0h 22m 20s	1/4	PING OK - Packet loss = 0%, RTA = 0.04 ms
	Root Partition	OK	09-29-2024 13:18:20	0d 0h 21m 43s	1/4	DISK OK - free space: / 5610 MiB (69.12% inode=98%):
	SSH	OK	09-29-2024 13:18:58	0d 0h 21m 5s	1/4	SSH OK - OpenSSH_8.7 (protocol 2.0)
	Swap Usage	CRITICAL	09-29-2024 13:17:35	0d 0h 17m 28s	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 13:15:13	0d 0h 19m 50s	1/4	PROCS OK: 39 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:

In this experiment, I successfully implemented Nagios for comprehensive port and service monitoring across both Windows and Linux servers. The setup allowed us to effectively track the status of critical services and ports, ensuring optimal performance and availability of server resources.