Anushka Shahane D15A 55

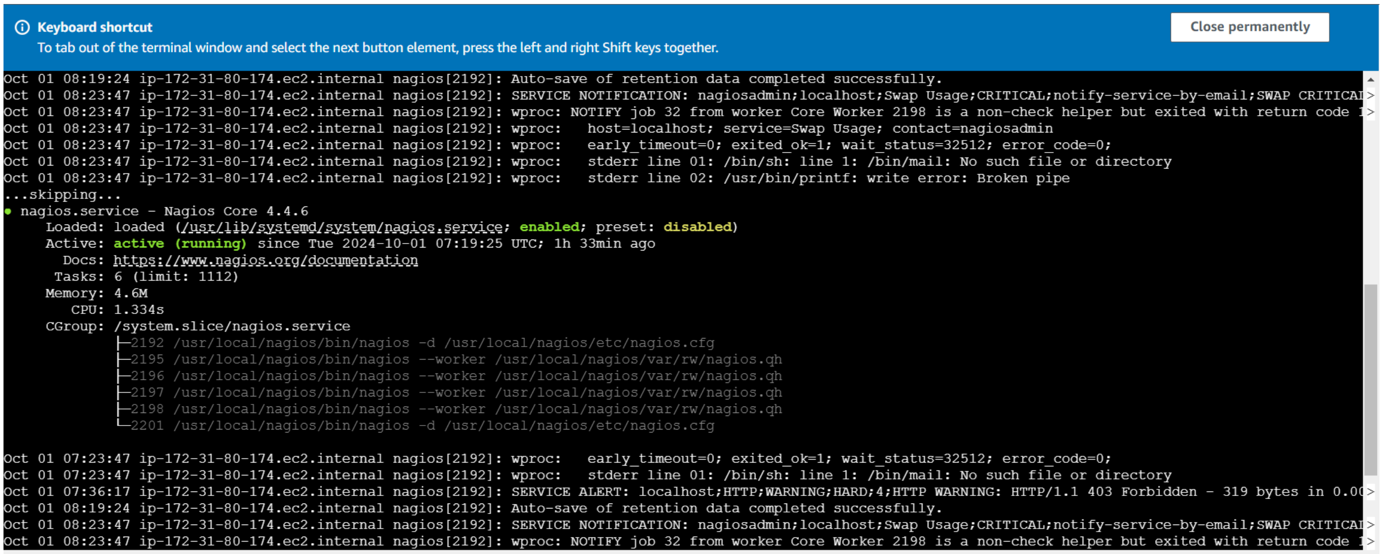
ADVANCE DEVOPS EXPERIMENT 10

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"



Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.
Close permanently

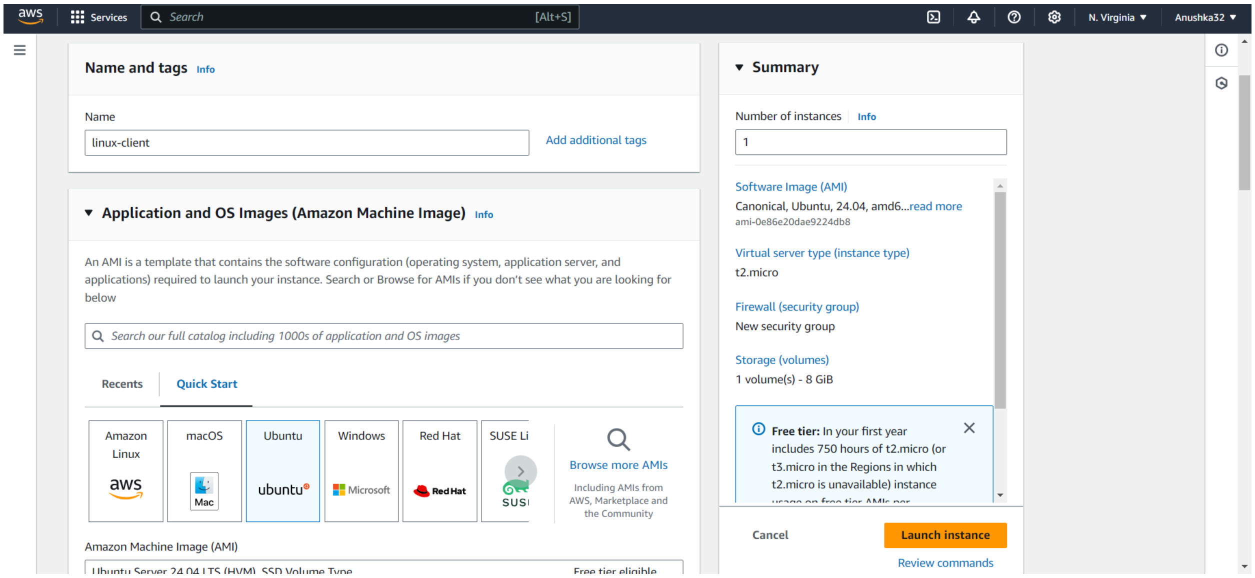
```
Oct 01 08:19:24 ip-172-31-80-174.ec2.internal nagios[2192]: Auto-save of retention data completed successfully.
Oct 01 08:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: SERVICE NOTIFICATION: nagiosadmin;localhost;Swap Usage;CRITICAL;notify-service-by-email;SWAP CRITICAL>
Oct 01 08:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: wproc: NOTIFY job 32 from worker Core Worker 2198 is a non-check helper but exited with return code 1>
Oct 01 08:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: wproc:   host=localhost; service=Swap Usage; contact=nagiosadmin
Oct 01 08:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: wproc:   early_timeout=0; exited_ok=1; wait_status=32512; error_code=0;
Oct 01 08:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: wproc:   stderr line 01: /bin/sh: line 1: /bin/mail: No such file or directory
Oct 01 08:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: wproc:   stderr line 02: /usr/bin/printf: write error: Broken pipe
...skipping...
● nagios.service - Nagios Core 4.4.6
     Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
     Active: active (running) since Tue 2024-10-01 07:19:25 UTC; 1h 33min ago
       Docs: https://www.nagios.org/documentation
      Tasks: 6 (limit: 1112)
     Memory: 4.6M
        CPU: 1.334s
     CGroup: /system.slice/nagios.service
             ├─2192 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
             ├─2195 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─2196 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─2197 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             ├─2198 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
             └─2201 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Oct 01 07:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: wproc:   early_timeout=0; exited_ok=1; wait_status=32512; error_code=0;
Oct 01 07:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: wproc:   stderr line 01: /bin/sh: line 1: /bin/mail: No such file or directory
Oct 01 07:36:17 ip-172-31-80-174.ec2.internal nagios[2192]: SERVICE ALERT: localhost;HTTP;WARNING;HARD;4;HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.00>
Oct 01 08:19:24 ip-172-31-80-174.ec2.internal nagios[2192]: Auto-save of retention data completed successfully.
Oct 01 08:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: SERVICE NOTIFICATION: nagiosadmin;localhost;Swap Usage;CRITICAL;notify-service-by-email;SWAP CRITICAL>
Oct 01 08:23:47 ip-172-31-80-174.ec2.internal nagios[2192]: wproc: NOTIFY job 32 from worker Core Worker 2198 is a non-check helper but exited with return code 1>
```

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.

Anushka Shahane D15A 55



Name and tags Info

Name: linux-client

Add additional tags

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)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible

Summary

Number of instances Info: 1

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-0e86e20dae9224db8

Virtual server type (instance type)
t2.micro

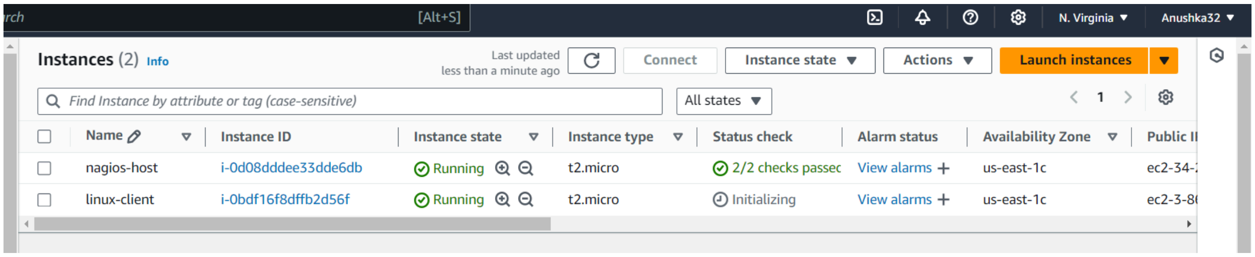
Firewall (security group)
New security group

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

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per

Cancel | Launch instance

Review commands



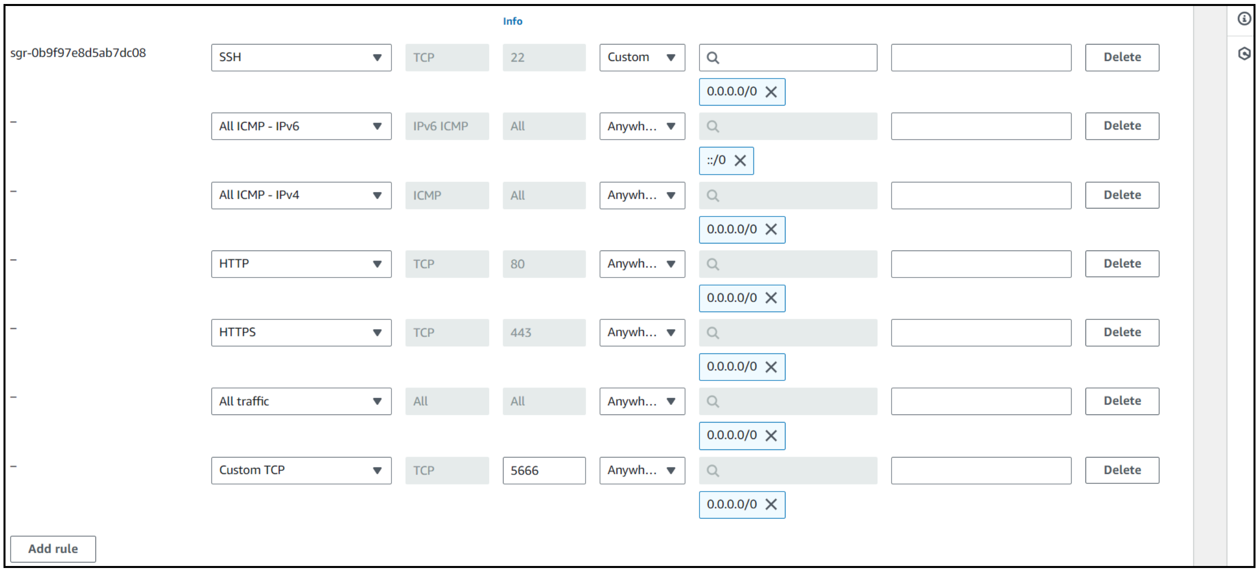
Instances (2) Info

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	Public II
□	nagios-host	i-0d08dddee33dde6db	✓ Running	t2.micro	✓ 2/2 checks passec	View alarms +	us-east-1c	ec2-34-:
□	linux-client	i-0bdf16f8dffb2d56f	✓ Running	t2.micro	Initializing	View alarms +	us-east-1c	ec2-3-8(



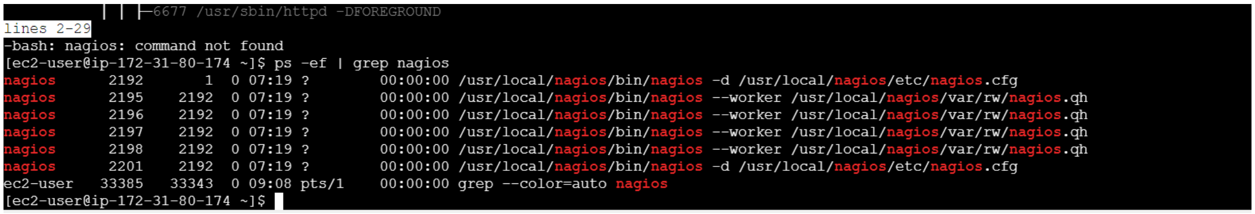
Info

sgr-0b9f97e8d5ab7dc08	SSH	TCP	22	Custom	0.0.0.0/0		Delete
–	All ICMP - IPv6	IPv6 ICMP	All	Anywh...	::/0		Delete
–	All ICMP - IPv4	ICMP	All	Anywh...	0.0.0.0/0		Delete
–	HTTP	TCP	80	Anywh...	0.0.0.0/0		Delete
–	HTTPS	TCP	443	Anywh...	0.0.0.0/0		Delete
–	All traffic	All	All	Anywh...	0.0.0.0/0		Delete
–	Custom TCP	TCP	5666	Anywh...	0.0.0.0/0		Delete

Add rule

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

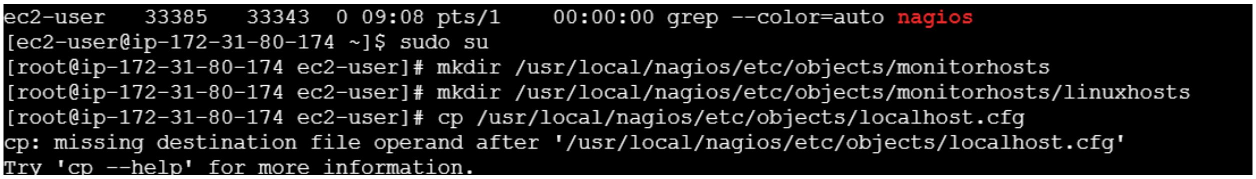
3. On the server, run this command
ps -ef | grep nagios



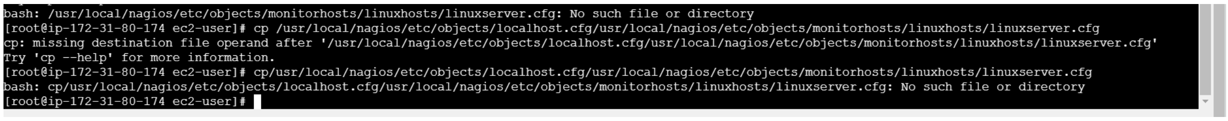
```
           | | ├─6677 /usr/sbin/httpd -DFOREGROUND
lines 2-29
-bash: nagios: command not found
[ec2-user@ip-172-31-80-174 ~]$ ps -ef | grep nagios
nagios      2192       1  0 07:19 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios      2195    2192  0 07:19 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      2196    2192  0 07:19 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      2197    2192  0 07:19 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      2198    2192  0 07:19 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios      2201    2192  0 07:19 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user   33385   33343  0 09:08 pts/1    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-80-174 ~]$
```

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. Copy the sample localhost.cfg file to linuxhost folder
cp /usr/local/nagios/etc/objects/localhost.cfg
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg



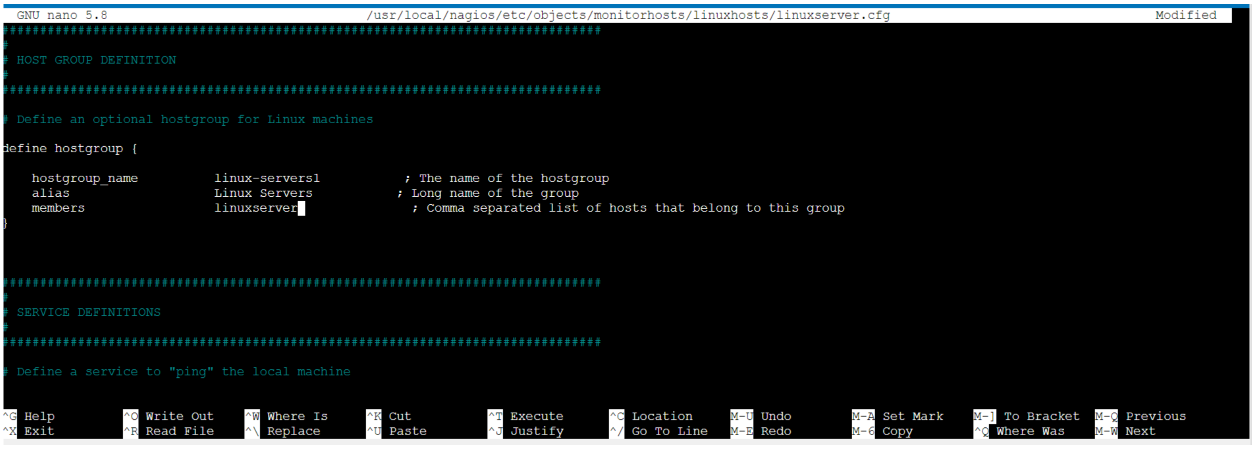
```
ec2-user   33385   33343  0 09:08 pts/1    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-80-174 ~]$ sudo su
[root@ip-172-31-80-174 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts
[root@ip-172-31-80-174 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-80-174 ec2-user]# cp /usr/local/nagios/etc/objects/localhost.cfg
cp: missing destination file operand after '/usr/local/nagios/etc/objects/localhost.cfg'
Try 'cp --help' for more information.
```



```
bash: /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg: No such file or directory
[root@ip-172-31-80-174 ec2-user]# cp /usr/local/nagios/etc/objects/localhost.cfg/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
cp: missing destination file operand after '/usr/local/nagios/etc/objects/localhost.cfg/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg'
Try 'cp --help' for more information.
[root@ip-172-31-80-174 ec2-user]# cp/usr/local/nagios/etc/objects/localhost.cfg/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
bash: cp/usr/local/nagios/etc/objects/localhost.cfg/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg: No such file or directory
[root@ip-172-31-80-174 ec2-user]#
```

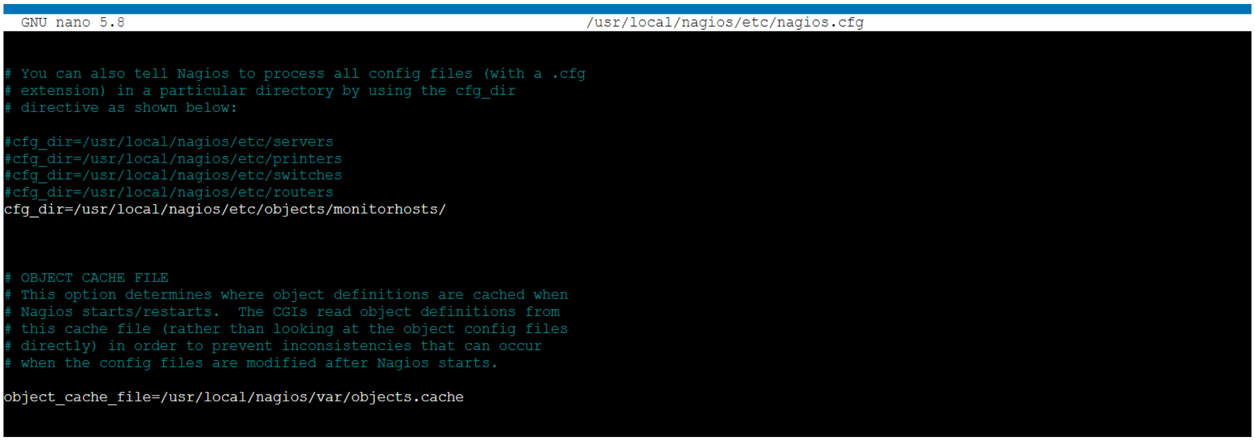
6. Open linuxserver.cfg using nano and make the following changes
nano
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
Change the hostname to linuxserver (EVERYWHERE ON THE FILE)
Change address to the public IP address of your LINUX CLIENT.

Change hostgroup_name under hostgroup to linux-servers1



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

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



###############################################################################
#
# SERVICE DEFINITIONS
#
###############################################################################

# Define a service to "ping" the local machine


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

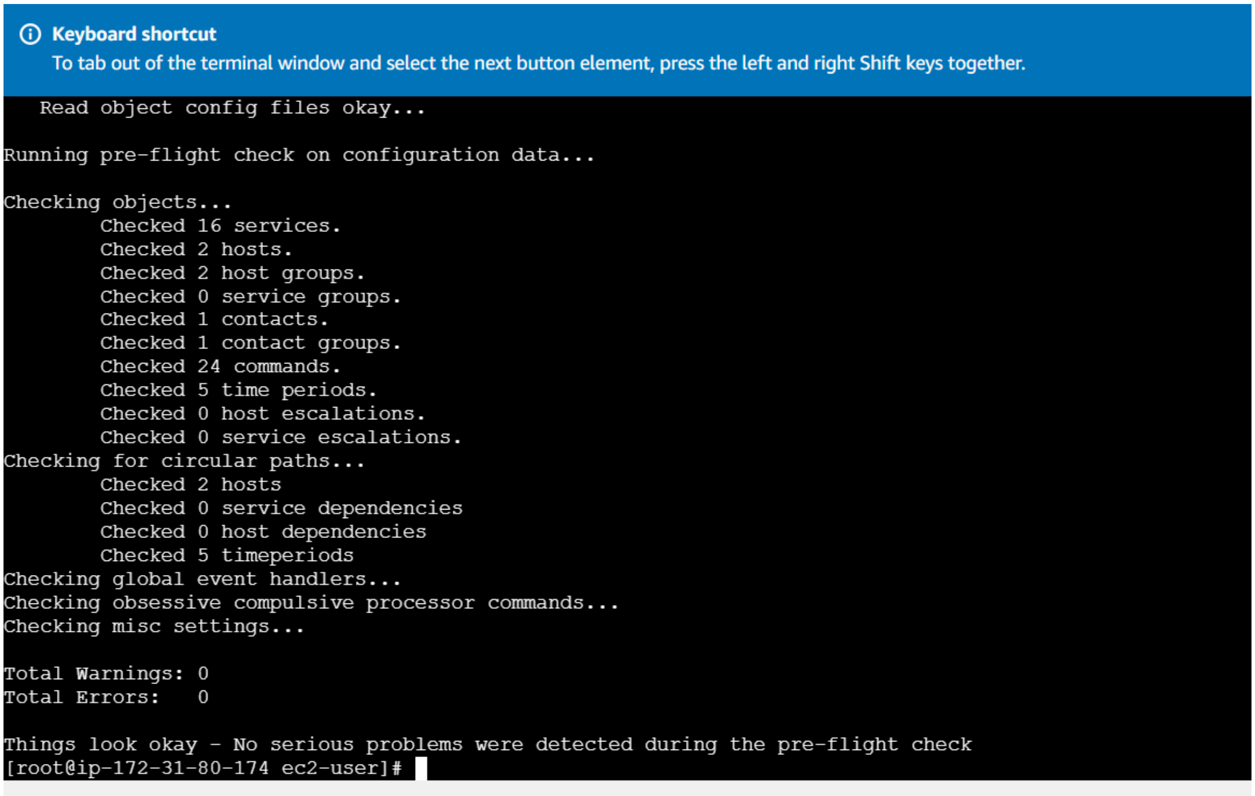
Everywhere else on the file, change the hostname to linuxserver instead of localhost.
7. Open the Nagios Config file and add the following line
nano /usr/local/nagios/etc/nagios.cfg
##Add this line
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/



```
  GNU nano 5.8                                        /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
# this cache file (rather than looking at the object config files
# directly) in order to prevent inconsistencies that can occur
# when the config files are modified after Nagios starts.

object_cache_file=/usr/local/nagios/var/objects.cache
```

8. Verify the configuration files

You are good to go if there are no errors.



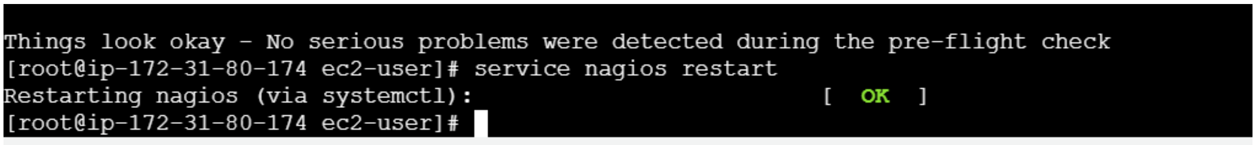
Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.

```
   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
[root@ip-172-31-80-174 ec2-user]#
```

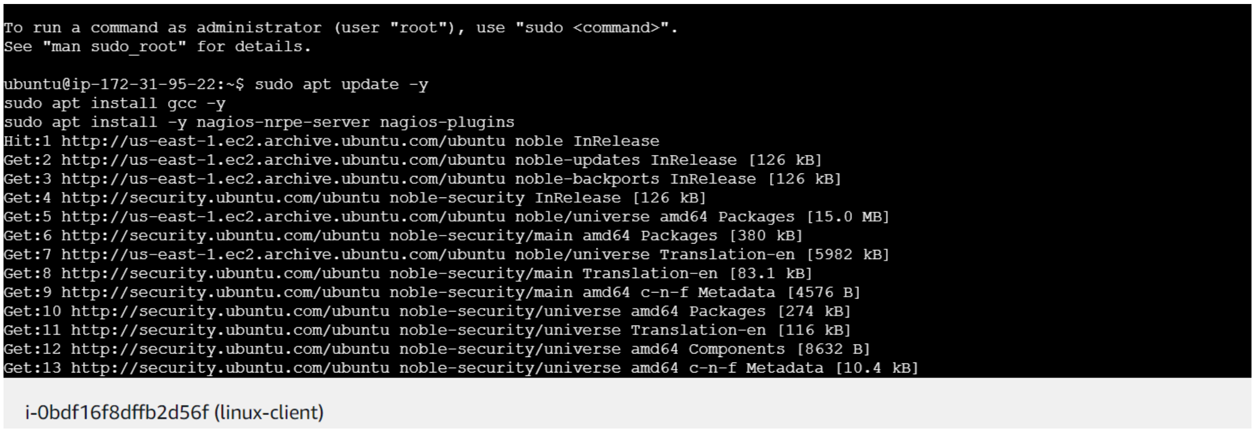
9. Restart the nagios service
service nagios restart

Now it is time to switch to the client machine.

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



```
Things look okay - No serious problems were detected during the pre-flight check
[root@ip-172-31-80-174 ec2-user]# service nagios restart
Restarting nagios (via systemctl):                         [  OK  ]
[root@ip-172-31-80-174 ec2-user]#
```



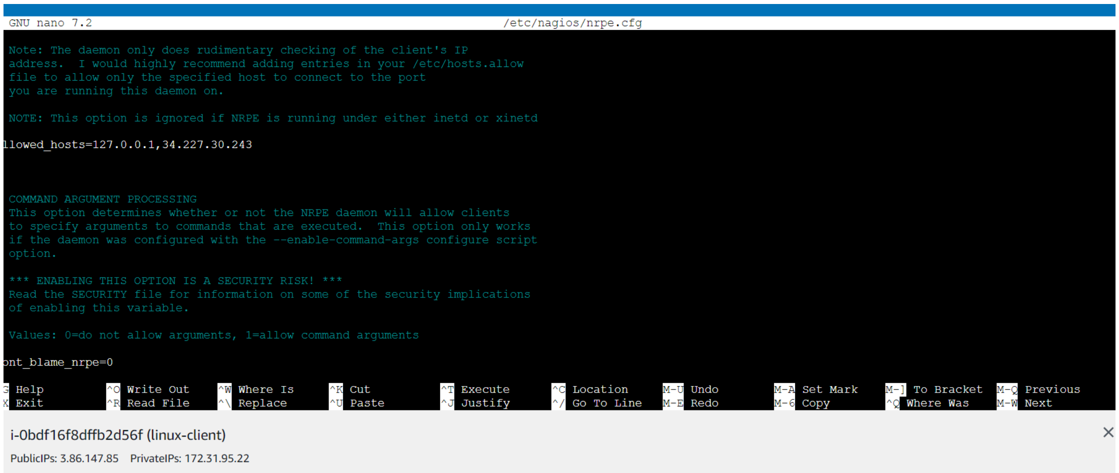
```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-95-22:~$ 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 [380 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Translation-en [5982 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [83.1 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4576 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [274 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [116 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [8632 B]
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [10.4 kB]
```

i-0bdf16f8dffb2d56f (linux-client)

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

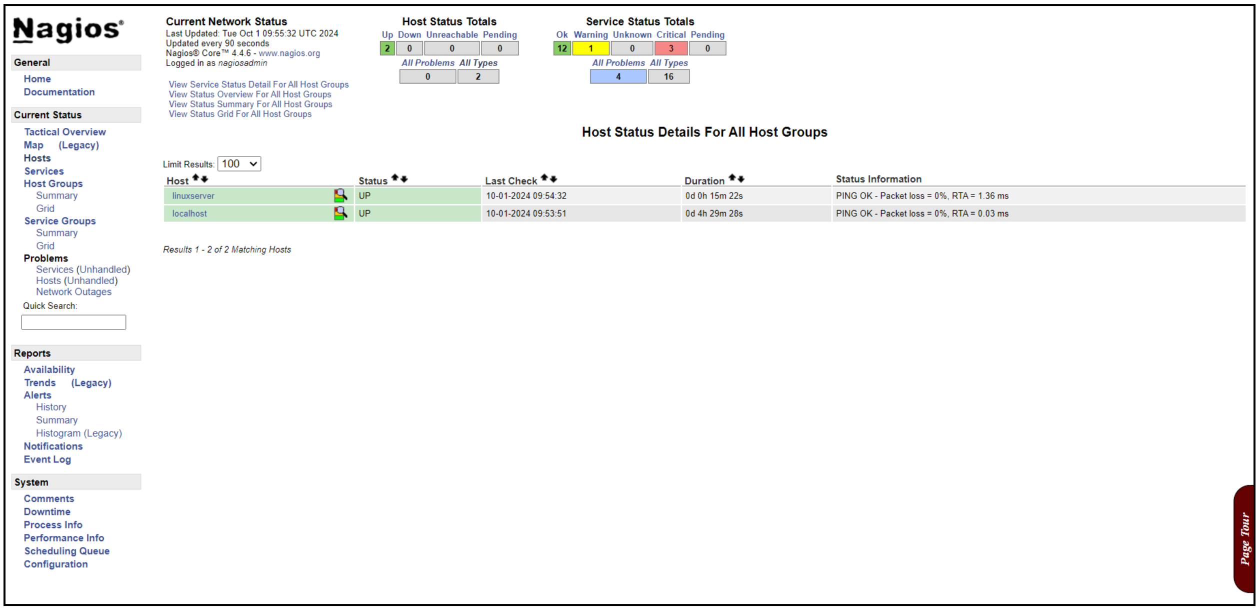


```
 GNU nano 7.2                                              /etc/nagios/nrpe.cfg

 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

llowed_hosts=127.0.0.1,34.227.30.243



 COMMAND ARGUMENT PROCESSING
 This option determines whether or not the NRPE daemon will allow clients
 to specify arguments to commands that are executed.  This option only works
 if the daemon was configured with the --enable-command-args configure script
 option.

 *** ENABLING THIS OPTION IS A SECURITY RISK! ***
 Read the SECURITY file for information on some of the security implications
 of enabling this variable.

 Values: 0=do not allow arguments, 1=allow command arguments

ont_blame_nrpe=0

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

i-0bdf16f8dffb2d56f (linux-client)

PublicIPs: 3.86.147.85   PrivateIPs: 172.31.95.22

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



Current Network Status
Last Updated: Tue Oct 1 09:55:32 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - www.nagios.org
Logged in as *nagiosadmin*

View Service Status Detail For All Host Groups
View Status Overview For All Host Groups
View Status Summary For All Host Groups
View Status Grid For All Host Groups

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

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
linuxserver	UP	10-01-2024 09:54:32	0d 0h 15m 22s	PING OK - Packet loss = 0%, RTA = 1.36 ms
localhost	UP	10-01-2024 09:53:51	0d 4h 29m 28s	PING OK - Packet loss = 0%, RTA = 0.03 ms

Results 1 - 2 of 2 Matching Hosts