Advanced DevOps Lab

Experiment 10

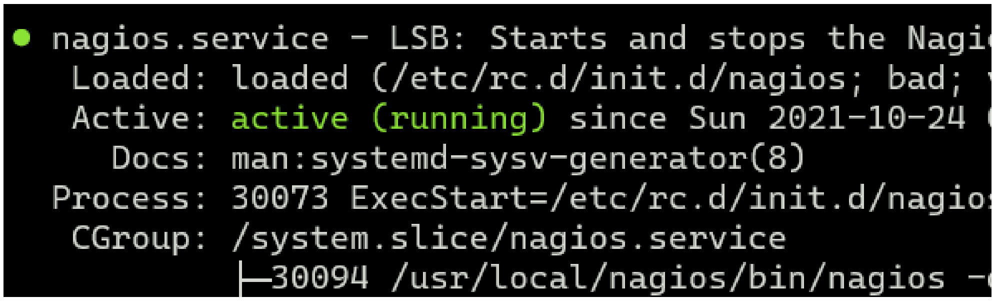
Roll No.	24
Name	Iyer Sreekesh Subramanian
Class	D15-A
Subject	Advanced DevOps Lab

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

<u>Steps:</u>

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”.

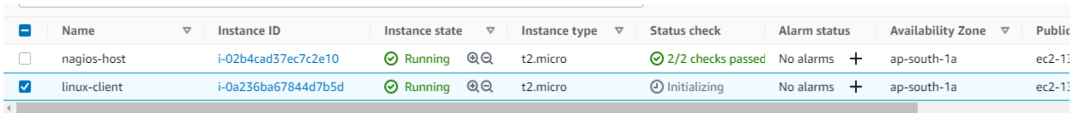


```
● nagios.service - LSB: Starts and stops the Nagi
   Loaded: loaded (/etc/rc.d/init.d/nagios; bad; 
   Active: active (running) since Sun 2021-10-24 
     Docs: man:systemd-sysv-generator(8)
  Process: 30073 ExecStart=/etc/rc.d/init.d/nagio
   CGroup: /system.slice/nagios.service
           ├─30094 /usr/local/nagios/bin/nagios -
```

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.

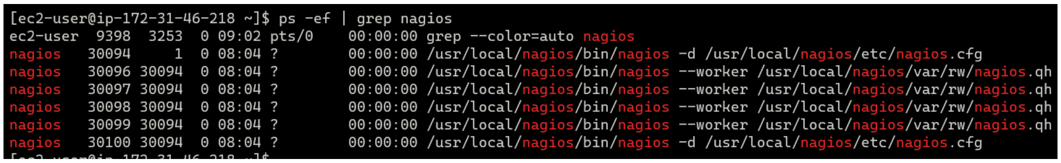


☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
☐	nagios-host	i-02b4cad37ec7c2e10	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms +	ap-south-1a	ec2-1
☑	linux-client	i-0a236ba67844d7b5d	✓ Running	t2.micro	Initializing	No alarms +	ap-south-1a	ec2-1

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
```



```
[ec2-user@ip-172-31-46-218 ~]$ ps -ef | grep nagios
ec2-user  9398  3253  0 09:02 pts/0    00:00:00 grep --color=auto nagios
nagios   30094     1  0 08:04 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios   30096 30094  0 08:04 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios   30097 30094  0 08:04 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios   30098 30094  0 08:04 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios   30099 30094  0 08:04 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios   30100 30094  0 08:04 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
[ec2-user@ip-172-31-46-218 ~]$
```

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
```

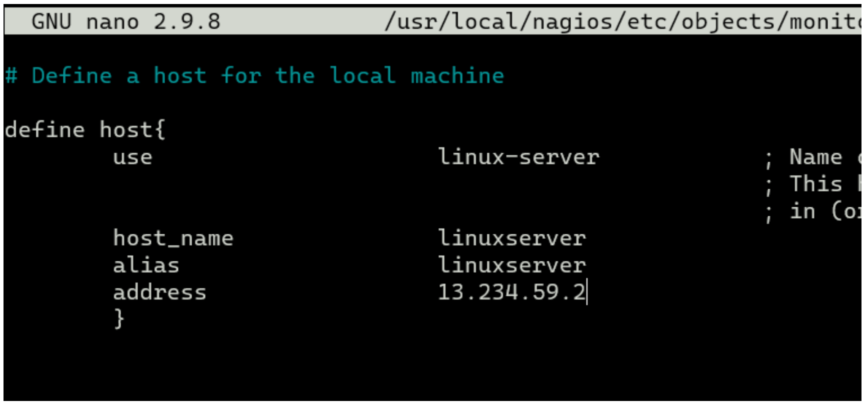
5. Copy the sample localhost.cfg file to linuxhost folder

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

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

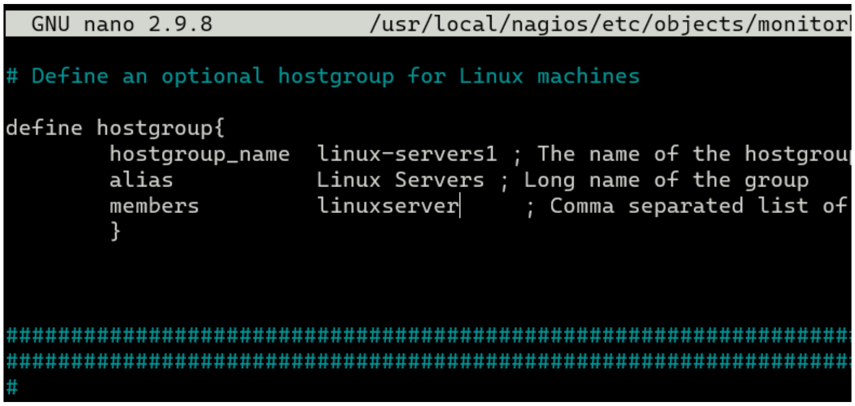
```
nano
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

Change the hostname to linuxserver (EVERYWHERE ON THE FILE)
Change address to the public IP address of your **LINUX CLIENT**.



```
  GNU nano 2.9.8            /usr/local/nagios/etc/objects/monit

# Define a host for the local machine

define host{
        use                     linux-server            ; Name
                                                        ; This
                                                        ; in (o

        host_name               linuxserver
        alias                   linuxserver
        address                 13.234.59.2
        }
```

Change hostgroup_name under hostgroup to linux-servers1

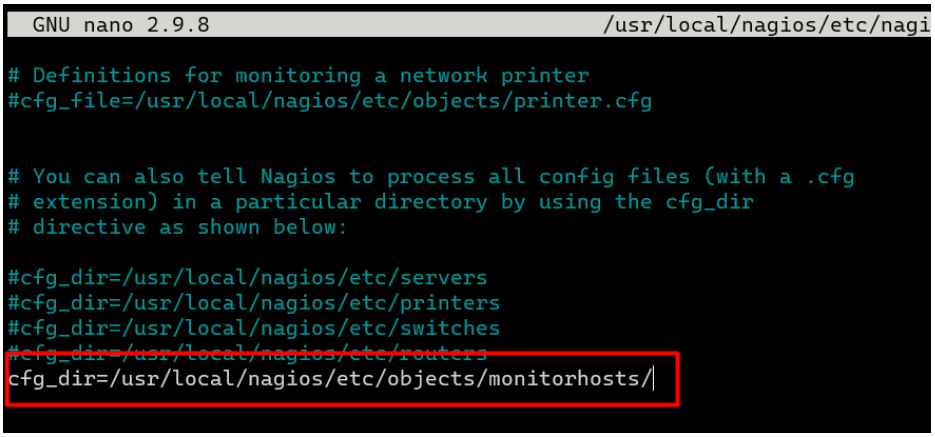


```
  GNU nano 2.9.8              /usr/local/nagios/etc/objects/monitor

# Define an optional hostgroup for Linux machines

define hostgroup{
        hostgroup_name  linux-servers1 ; The name of the hostgrou
        alias           Linux Servers ; Long name of the group
        members         linuxserver     ; Comma separated list of
        }



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

Everywhere else on the file, change the hostname to linuxserver instead of localhost.

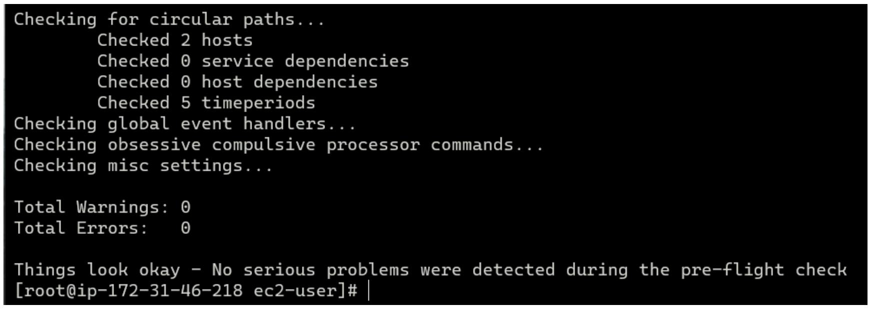
7. Open the Nagios Config file and add the following line

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

##Add this line
cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/
```



```
  GNU nano 2.9.8                                    /usr/local/nagios/etc/nagi

# 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/
```

8. Verify the configuration files

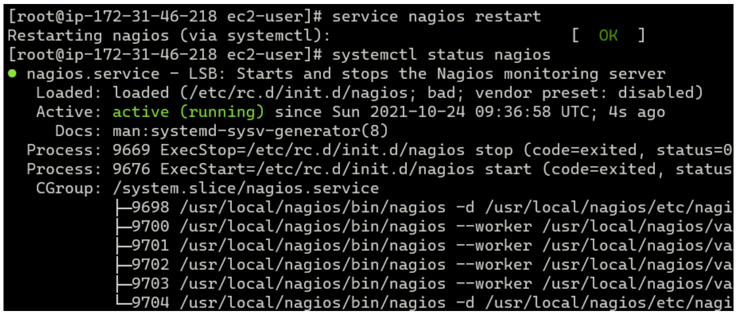


```
Checking for circular paths...
        Checked 2 hosts
        Checked 0 service dependencies
        Checked 0 host dependencies
        Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
[root@ip-172-31-46-218 ec2-user]# 
```

You are good to go if there are no errors.

9. Restart the nagios service

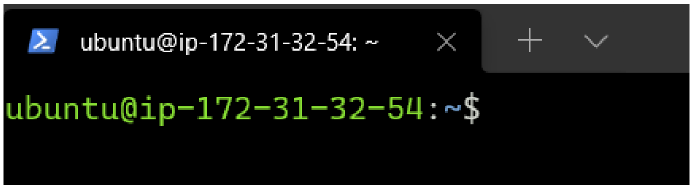
```
service nagios restart
```



```
[root@ip-172-31-46-218 ec2-user]# service nagios restart
Restarting nagios (via systemctl):                         [  OK  ]
[root@ip-172-31-46-218 ec2-user]# systemctl status nagios
● nagios.service - LSB: Starts and stops the Nagios monitoring server
   Loaded: loaded (/etc/rc.d/init.d/nagios; bad; vendor preset: disabled)
   Active: active (running) since Sun 2021-10-24 09:36:58 UTC; 4s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 9669 ExecStop=/etc/rc.d/init.d/nagios stop (code=exited, status=0
  Process: 9676 ExecStart=/etc/rc.d/init.d/nagios start (code=exited, status
   CGroup: /system.slice/nagios.service
           ├─9698 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagi
           ├─9700 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/va
           ├─9701 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/va
           ├─9702 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/va
           ├─9703 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/va
           └─9704 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagi
```

Now it is time to switch to the client machine.

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



```
ubuntu@ip-172-31-32-54:~$
```

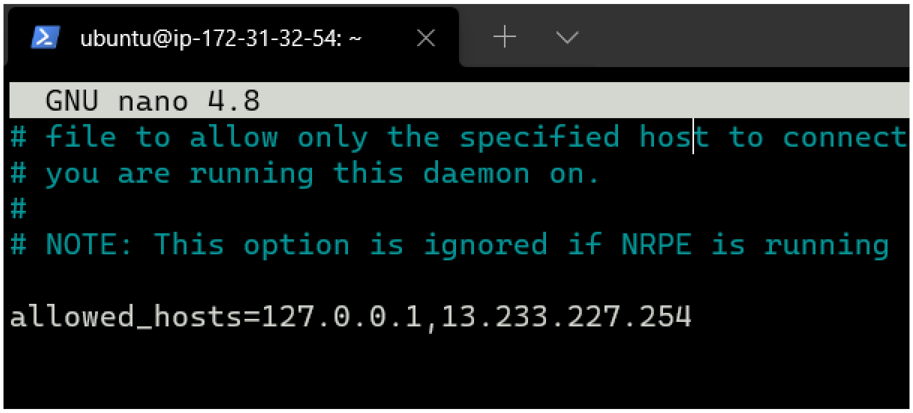
11. Make a package index update and install gcc, nagios-nrpe-server and the plugins.

```
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



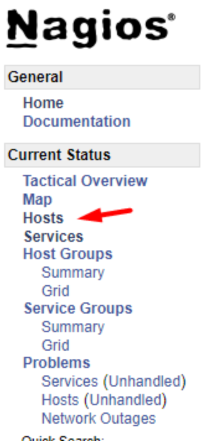
```
 GNU nano 4.8
# file to allow only the specified host to connect
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running

allowed_hosts=127.0.0.1,13.233.227.254
```

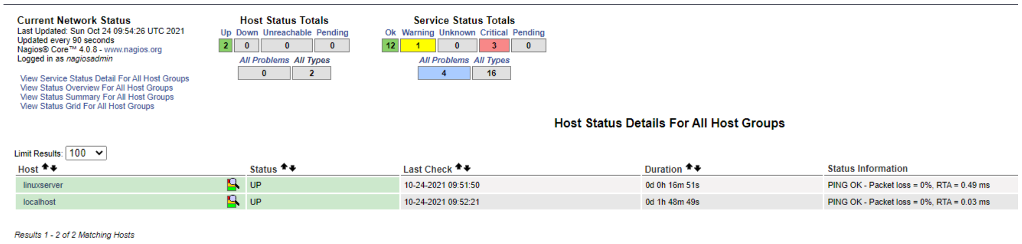
13. Restart the NRPE server

```
sudo systemctl restart nagios-nrpe-server
```

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

Click on Hosts.





Current Network Status
Last Updated: Sun Oct 24 09:54:26 UTC 2021
Updated every 90 seconds
Nagios® Core™ 4.0.8 - 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

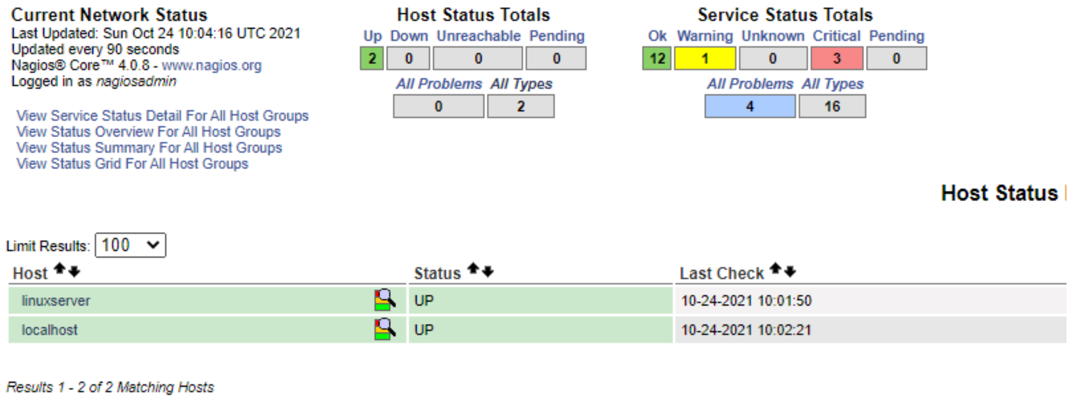
Host Status Details For All Host Groups

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
linuxserver	UP	10-24-2021 09:51:50	0d 0h 16m 51s	PING OK - Packet loss = 0%, RTA = 0.49 ms
localhost	UP	10-24-2021 09:52:21	0d 1h 48m 49s	PING OK - Packet loss = 0%, RTA = 0.03 ms

Results 1 - 2 of 2 Matching Hosts

Click on linuxserver to see the host details



Current Network Status
Last Updated: Sun Oct 24 10:04:16 UTC 2021
Updated every 90 seconds
Nagios® Core™ 4.0.8 - 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

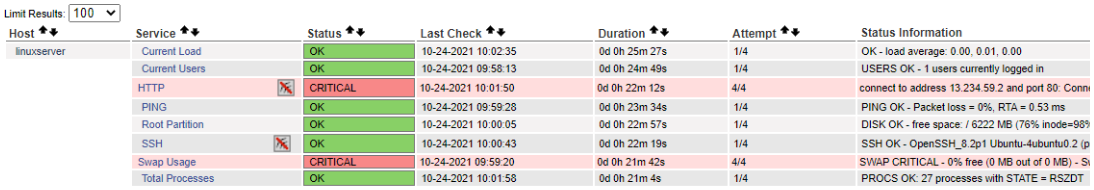
Host Status

Limit Results: 100

Host	Status	Last Check
linuxserver	UP	10-24-2021 10:01:50
localhost	UP	10-24-2021 10:02:21

Results 1 - 2 of 2 Matching Hosts

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



Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
linuxserver	Current Load	OK	10-24-2021 10:02:35	0d 0h 25m 27s	1/4	OK - load average: 0.00, 0.01, 0.00
	Current Users	OK	10-24-2021 09:58:13	0d 0h 24m 49s	1/4	USERS OK - 1 users currently logged in
	HTTP	CRITICAL	10-24-2021 10:01:50	0d 0h 22m 12s	4/4	connect to address 13.234.59.2 and port 80: Conn
	PING	OK	10-24-2021 09:59:28	0d 0h 23m 34s	1/4	PING OK - Packet loss = 0%, RTA = 0.53 ms
	Root Partition	OK	10-24-2021 10:00:05	0d 0h 22m 57s	1/4	DISK OK - free space: / 6222 MB (76% inode=98%
	SSH	OK	10-24-2021 10:00:43	0d 0h 22m 19s	1/4	SSH OK - OpenSSH_8.2p1 Ubuntu-4ubuntu0.2 (p
	Swap Usage	CRITICAL	10-24-2021 09:59:20	0d 0h 21m 42s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - S
	Total Processes	OK	10-24-2021 10:01:58	0d 0h 21m 4s	1/4	PROCS OK: 27 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)

<u>Conclusion:</u>

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.