Name:Sahil Ramrakhyani Div:D15C RollNo:42

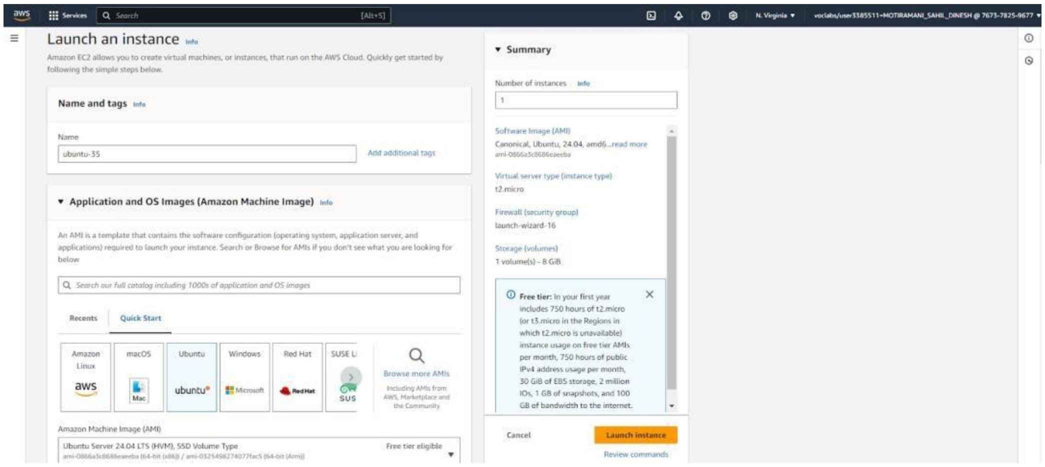
Aim: To perform Port, Service monitoring, Windows/Linux server monitoring using Nagios.

Prerequisites:

1) An Amazon Linux instance with nagios already set up.

Step 1: Set up ubuntu instance

1) Login to your AWS account. Search for EC2 on services. Open the interface and click on Create Instance.



Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: ubuntu-35

Application and OS Images (Amazon Machine Image)

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

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))

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04, amd6...read more
ami-0866a3c8686eaeeba

Virtual server type (instance type): t2.micro

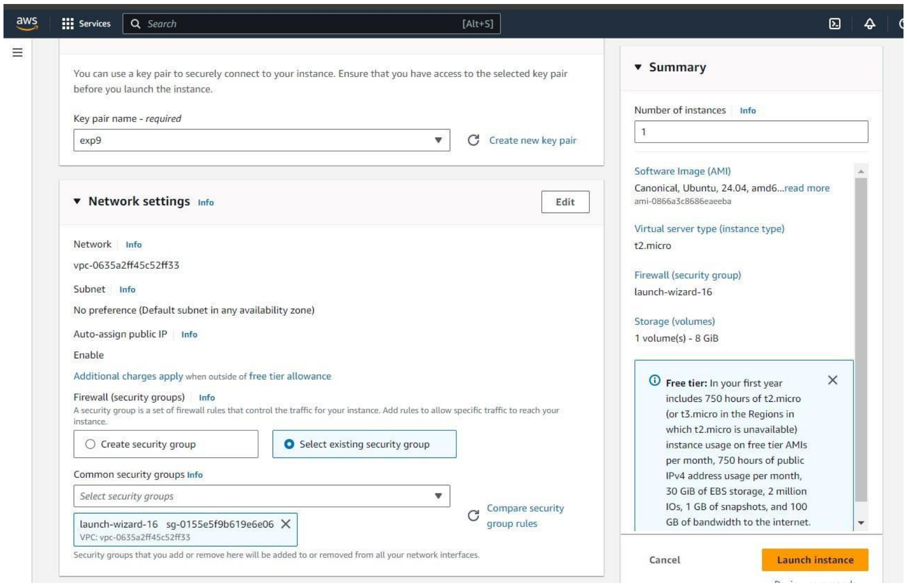
Firewall (security group): launch-wizard-16

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 month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Select The OS Image as Ubuntu.

2) Make sure to select the same private key that you created for the Amazon Linux instance. Also select the same security group as you created for the Linux instance.



You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: exp9

Network settings

Network: vpc-0635a2ff45c52ff33

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)
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: launch-wizard-16 sg-0155e5f9b619e6e06
VPC: vpc-0635a2ff45c52ff33

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

Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04, amd6...read more
ami-0866a3c8686eaeeba

Virtual server type (instance type): t2.micro

Firewall (security group): launch-wizard-16

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

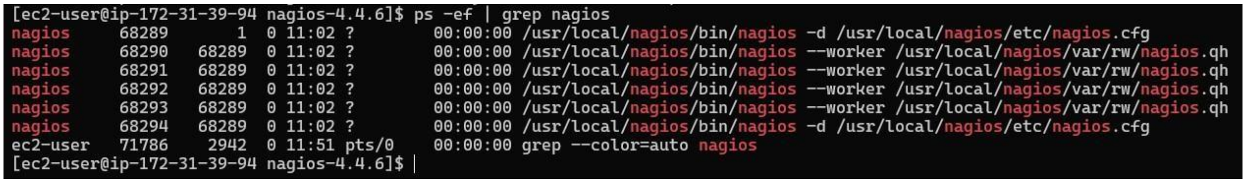
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Name:Sahil Ramrakhyani Div:D15C RollNo:42

3) Now come back to the instances screen. Click on the instance ID of your instance. Then click on Connect. Click on SSH client. Copy the example command. Now, we have to connect our local OS terminal to the instance using SSH. For this, open terminal wher the private key file is located (.pem). Paste the copied SSH command and run it.

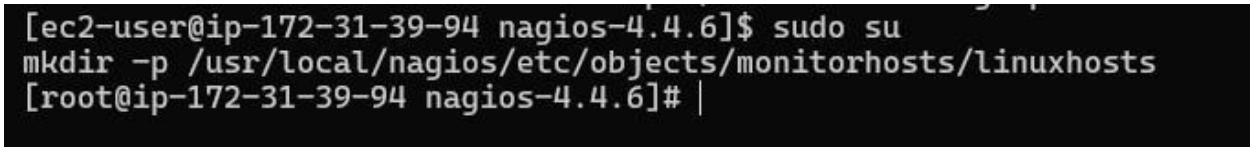
Step 2: Execute the following on Nagios Host machine (Linux)

1) We need to verify whether the nagios service is running or not. Fo that, run this command.
   ps -ef | grep nagios



```
[ec2-user@ip-172-31-39-94 nagios-4.4.6]$ ps -ef | grep nagios
nagios     68289       1  0 11:02 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     68290   68289  0 11:02 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68291   68289  0 11:02 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68292   68289  0 11:02 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68293   68289  0 11:02 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     68294   68289  0 11:02 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
ec2-user   71786    2942  0 11:51 pts/0    00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-39-94 nagios-4.4.6]$ |
```

2) Now, make yourself as the root user, and create a folder with the path '/usr/local/nagios/etc/objects/monitorhosts/linuxhosts'
   sudo su
   mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts

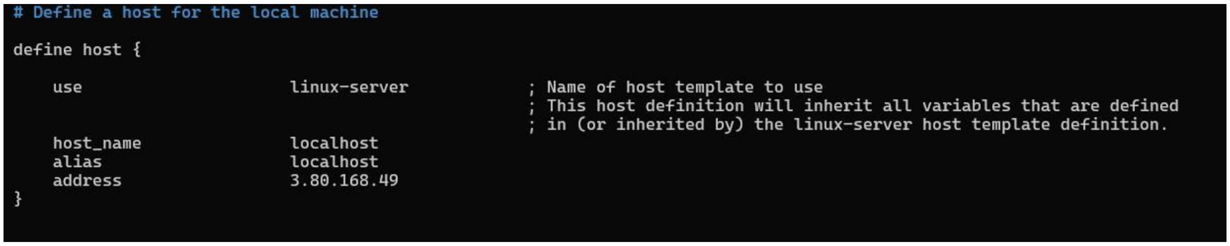


```
[ec2-user@ip-172-31-39-94 nagios-4.4.6]$ sudo su
mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-39-94 nagios-4.4.6]# |
```

3) We need to create a config file in this folder. So, copy the contents of the existing localhost config to the new file 'linuxserver.cfg'. **cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg**

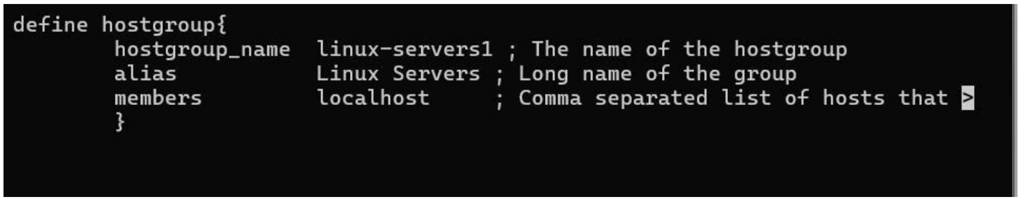
4) We need to make some changes in this config file. Open it using nano editor.
   nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

   Change **hostname** and **alias** to **linuxserver**
   Change address to **public ip address of client instance** (Ubuntu instance)



```
# 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                 3.80.168.49
}
```

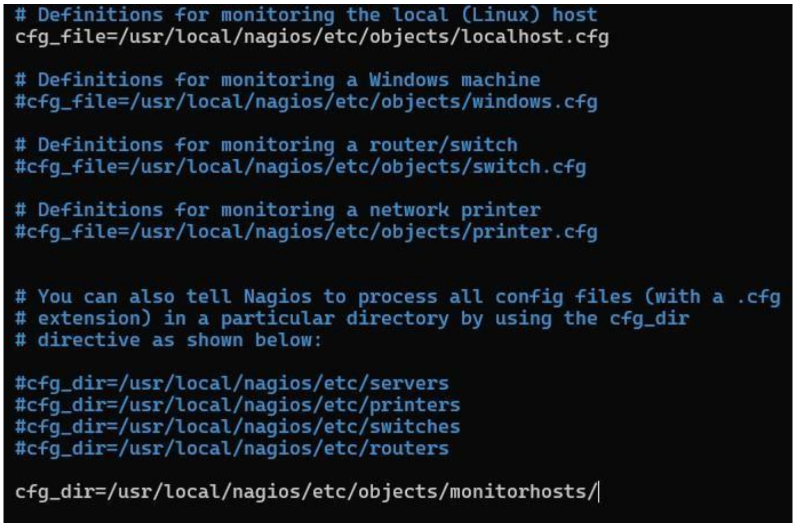
Change hostgroup_name to **linux-servers1**



```
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 >
        }
```

Change the **occurrences of hostname** further in the document from **localhost** to **linuxserver**

5) Now, we need to edit the nagios configuration file to add this directory.
   nano /usr/local/nagios/etc/nagios.cfg Run this command and add the following line
   cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/

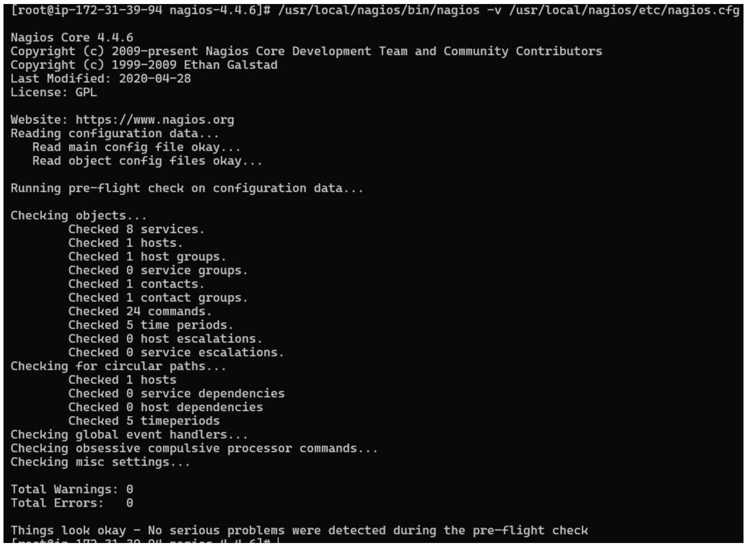


```
# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg

# 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/
```

6) Now we verify the configuration files.

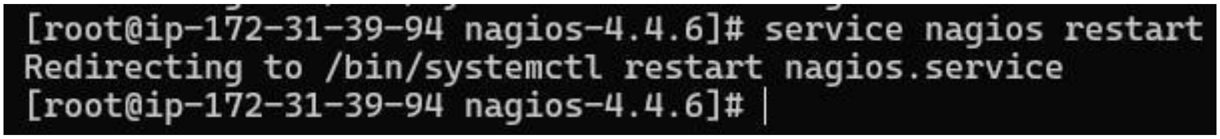
Name:Sahil Ramrakhyani Div:D15C RollNo:42

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg



```
[root@ip-172-31-39-94 nagios-4.4.6]# /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 8 services.
        Checked 1 hosts.
        Checked 1 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 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-172-31-39-94 nagios-4.4.6]# |
```

7) Once the files are verified, we need to restart the server.
   service nagios restart



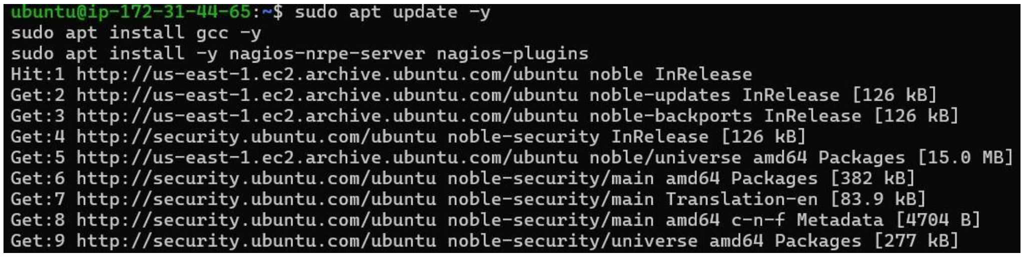
```
[root@ip-172-31-39-94 nagios-4.4.6]# service nagios restart
Redirecting to /bin/systemctl restart nagios.service
[root@ip-172-31-39-94 nagios-4.4.6]# |
```

Step 3: Execute the following on Nagios Client machine (Ubuntu)

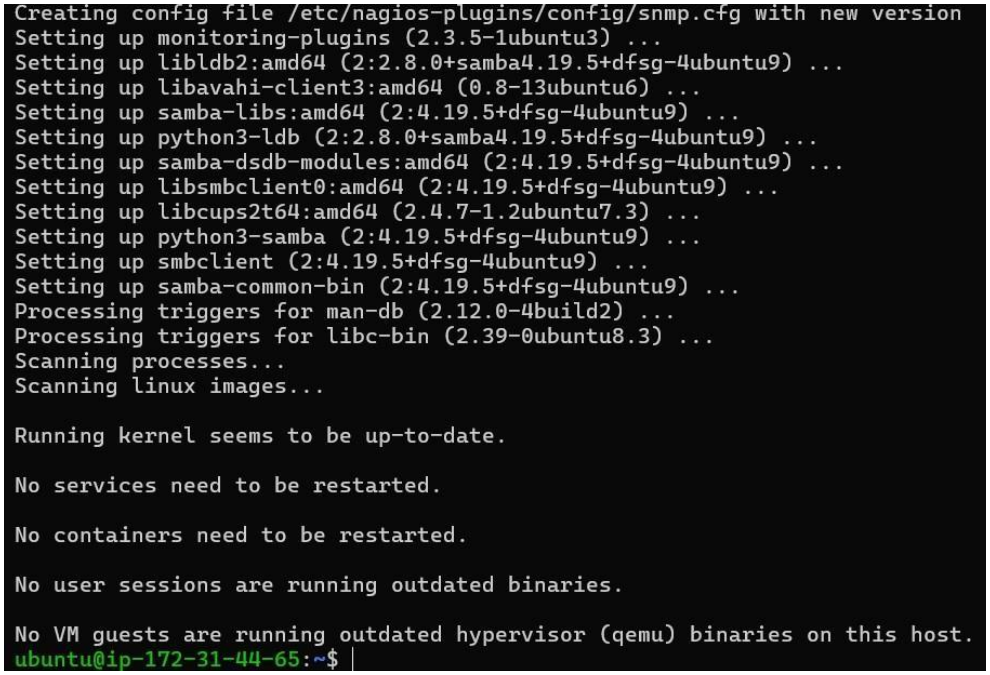
1) First, we check for any new updates, then we install gcc, nagios nrpe server and nagios plugins.

Name:Sahil Ramrakhyani Div:D15C RollNo:42

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



```
ubuntu@ip-172-31-44-65:~$ 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://security.ubuntu.com/ubuntu noble-security/main Translation-en [83.9 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [4704 B]
Get:9 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [277 kB]
```



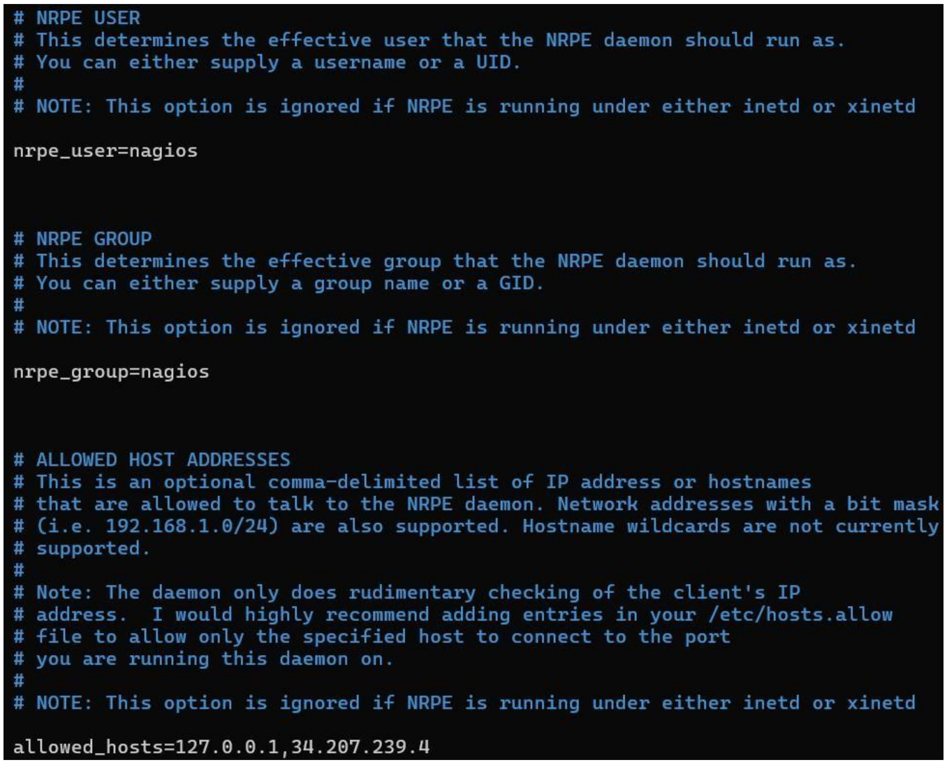
```
Creating config file /etc/nagios-plugins/config/snmp.cfg with new version
Setting up monitoring-plugins (2.3.5-1ubuntu3) ...
Setting up libldb2:amd64 (2:2.8.0+samba4.19.5+dfsg-4ubuntu9) ...
Setting up libavahi-client3:amd64 (0.8-13ubuntu6) ...
Setting up samba-libs:amd64 (2:4.19.5+dfsg-4ubuntu9) ...
Setting up python3-ldb (2:2.8.0+samba4.19.5+dfsg-4ubuntu9) ...
Setting up samba-dsdb-modules:amd64 (2:4.19.5+dfsg-4ubuntu9) ...
Setting up libsmbclient0:amd64 (2:4.19.5+dfsg-4ubuntu9) ...
Setting up libcups2t64:amd64 (2.4.7-1.2ubuntu7.3) ...
Setting up python3-samba (2:4.19.5+dfsg-4ubuntu9) ...
Setting up smbclient (2:4.19.5+dfsg-4ubuntu9) ...
Setting up samba-common-bin (2:4.19.5+dfsg-4ubuntu9) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

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.
ubuntu@ip-172-31-44-65:~$
```

2) We need to add the public IP address of our host Nagios machine (Linux) to the nrpe configuration file.

sudo nano /etc/nagios/nrpe.cfg

Under allowed_hosts, add the nagios host ip address (public)

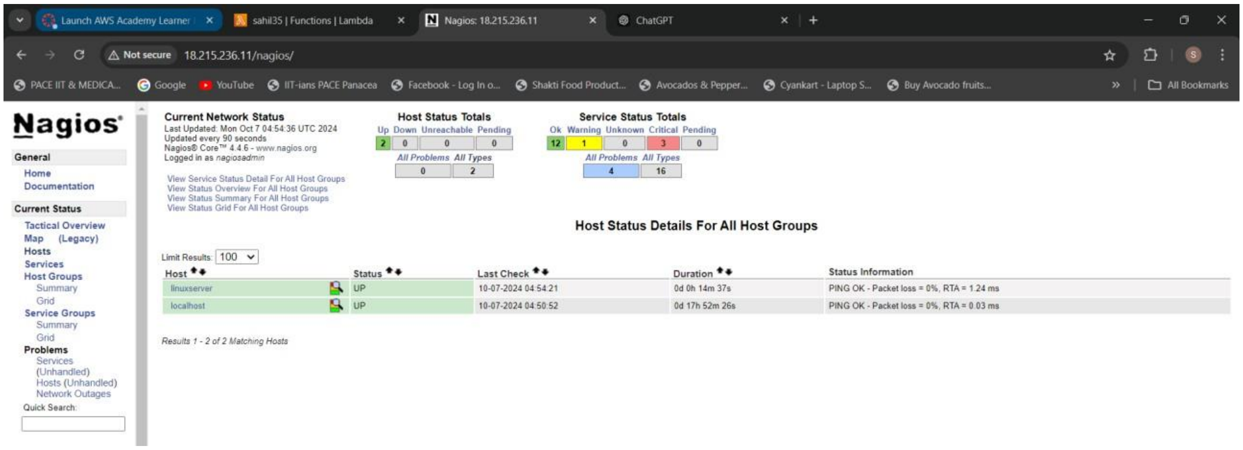
Name:Sahil Ramrakhyani Div:D15C RollNo:42



```
# NRPE USER
# This determines the effective user that the NRPE daemon should run as.
# You can either supply a username or a UID.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

nrpe_user=nagios



# NRPE GROUP
# This determines the effective group that the NRPE daemon should run as.
# 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=127.0.0.1,34.207.239.4
```

Step 4: Check the Nagios Dashboard

1) Go to Nagios dashboard, click on hosts.
   Here, we can see that the linuxserver is also added as a host.



Current Network Status
Last Updated: Mon Oct 7 04:54:36 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
12	1	0	3	0

All Problems	*All Types*
4	16

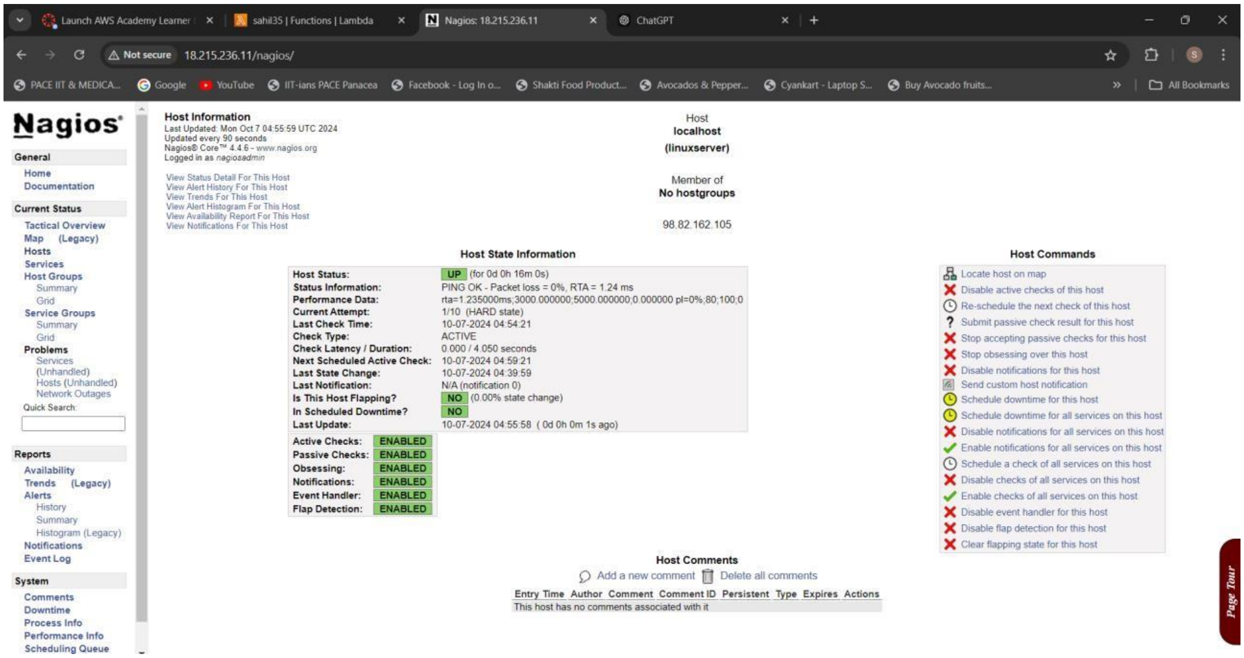
Host Status Details For All Host Groups

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
linuxserver	UP	10-07-2024 04:54:21	0d 0h 14m 37s	PING OK - Packet loss = 0%, RTA = 1.24 ms
localhost	UP	10-07-2024 04:50:52	0d 17h 52m 26s	PING OK - Packet loss = 0%, RTA = 0.03 ms

Results 1 - 2 of 2 Matching Hosts

2) Click on linuxserver. Here, we can check all the information about linuxserver host.



Host Information
Last Updated: Mon Oct 7 04:55:59 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - 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
localhost
(linuxserver)

Member of
No hostgroups

98.82.162.105

Host State Information

Host Status:	UP (for 0d 0h 16m 0s)
Status Information:	PING OK - Packet loss = 0%, RTA = 1.24 ms
Performance Data:	rta=1.235000ms;3000.000000;5000.000000;0.000000 pl=0%;80;100;0
Current Attempt:	1/10 (HARD state)
Last Check Time:	10-07-2024 04:54:21
Check Type:	ACTIVE
Check Latency / Duration:	0.000 / 4.050 seconds
Next Scheduled Active Check:	10-07-2024 04:59:21
Last State Change:	10-07-2024 04:39:59
Last Notification:	N/A (notification 0)
Is This Host Flapping?	NO (0.00% state change)
In Scheduled Downtime?	NO
Last Update:	10-07-2024 04:55:58 (0d 0h 0m 1s ago)

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

Host Commands

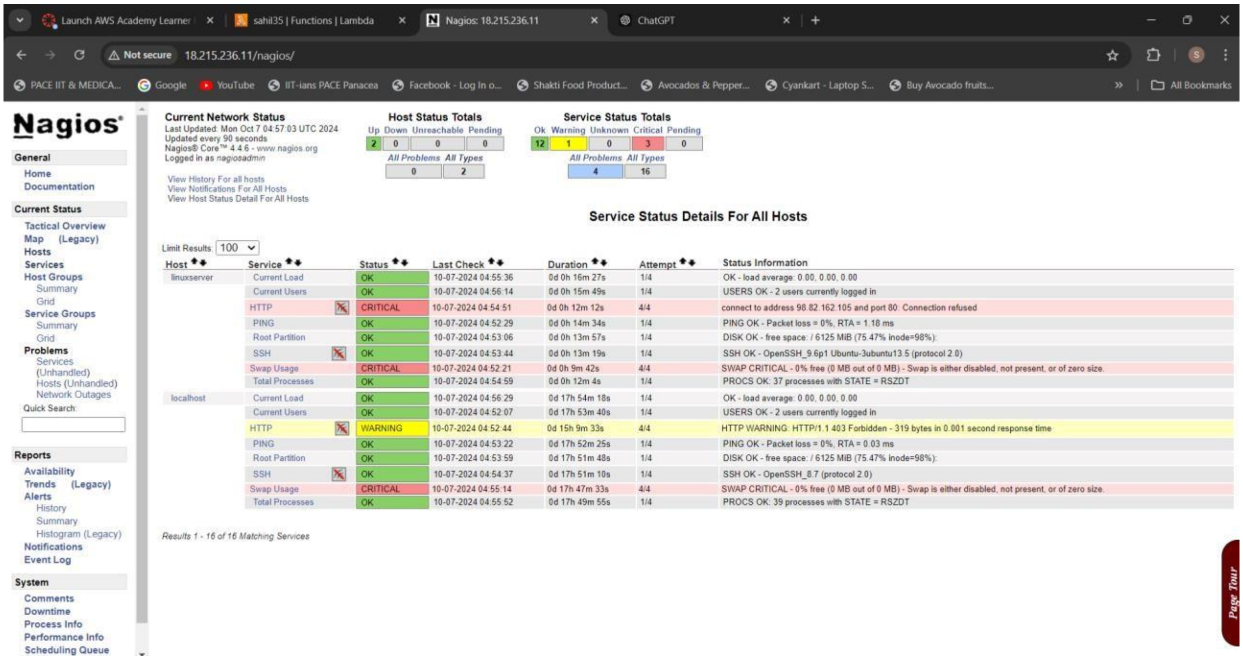
- Locate host on map
- ✗ Disable active checks of this host
- Re-schedule the next check of this host
- ? Submit passive check result for this host
- ✗ Stop accepting passive checks for this host
- ✗ Stop obsessing over this host
- ✗ Disable notifications for this host
- Send custom host notification
- 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

Add a new comment   Delete all comments

Entry Time	Author	Comment	Comment ID	Persistent	Type	Expires	Actions
This host has no comments associated with it							

3) Click on services. Here we an see all the services that are being monitored by linuxserver.



Current Network Status
Last Updated: Mon Oct 7 04:57:03 UTC 2024
Updated every 90 seconds
Nagios® Core™ 4.4.6 - 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	10-07-2024 04:55:36	0d 0h 16m 27s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	10-07-2024 04:56:14	0d 0h 15m 49s	1/4	USERS OK - 2 users currently logged in
	HTTP	CRITICAL	10-07-2024 04:54:51	0d 0h 12m 12s	4/4	connect to address 98.82.162.105 and port 80: Connection refused
	PING	OK	10-07-2024 04:52:29	0d 0h 14m 34s	1/4	PING OK - Packet loss = 0%, RTA = 1.18 ms
	Root Partition	OK	10-07-2024 04:53:06	0d 0h 13m 57s	1/4	DISK OK - free space: / 6125 MiB (75.47% inode=98%):
	SSH	OK	10-07-2024 04:53:44	0d 0h 13m 19s	1/4	SSH OK - OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 (protocol 2.0)
	Swap Usage	CRITICAL	10-07-2024 04:52:21	0d 0h 9m 42s	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	10-07-2024 04:54:59	0d 0h 12m 4s	1/4	PROCS OK: 37 processes with STATE = RSZDT
localhost	Current Load	OK	10-07-2024 04:56:29	0d 17h 54m 18s	1/4	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	10-07-2024 04:52:07	0d 17h 53m 40s	1/4	USERS OK - 2 users currently logged in
	HTTP	WARNING	10-07-2024 04:52:44	0d 15h 9m 33s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 319 bytes in 0.001 second response time
	PING	OK	10-07-2024 04:53:22	0d 17h 52m 25s	1/4	PING OK - Packet loss = 0%, RTA = 0.03 ms
	Root Partition	OK	10-07-2024 04:53:59	0d 17h 51m 48s	1/4	DISK OK - free space: / 6125 MiB (75.47% inode=98%):
	SSH	OK	10-07-2024 04:54:37	0d 17h 51m 10s	1/4	SSH OK - OpenSSH_8.7 (protocol 2.0)
	Swap Usage	CRITICAL	10-07-2024 04:55:14	0d 17h 47m 33s	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	10-07-2024 04:55:52	0d 17h 49m 55s	1/4	PROCS OK: 39 processes with STATE = RSZDT

Results 1 - 16 of 16 Matching Services

Name:Sahil Ramrakhyani Div:D15C RollNo:42

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.

Conclusion:

In this experiment, we set up port and server monitoring using Nagios.

1. Linux Instance: Hosts the Nagios dashboard and server.
2. Ubuntu Instance : Acts as the second monitored host.
3. Configuration:
   - Add the Ubuntu instance’s IP to the Nagios server’s configuration.
   - On the Ubuntu instance, configure the NRPE server and allow the Nagios server's IP.
4. Restart NRPE: After configuration, restart the NRPE service on Ubuntu.
5. Monitor: The Ubuntu instance will appear as "linuxserver" on the Nagios dashboard for monitoring.