Experiment 10

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

Nagios. Steps:

1. Firstly, we will check whether nagios is running on the server side by using the command "sudo systemctl status nagios" on the host machine (host machine is the instance connected to the terminal in experiment 9, ensure that you have started the instance created for exp9, also check status of apache).

```
[ec2-user@ip-172-31-87-75 ~]$ sudo systemctl status
nagios
• ip-172-31-87-75.ec2.internal
    State: running
    Units: 295 loaded (incl. loaded aliases)
        Jobs: 1 queued
    Failed: 0 units
        Since: Wed 2024-10-02 06:17:29 UTC; 2min 42s ago
systemd: 252.23-2.amzn2023
```

```
[ec2-user@ip-172-31-87-75 ~]$ sudo service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[ec2-user@ip-172-31-87-75 ~]$ sudo systemctl status httpd
• httpd.service - The Apache HTTP Server

Loaded: loaded (/usr/lib/systemd/system/httpd.service;
Drop-In: /usr/lib/systemd/system/httpd.service.d

_php-fpm.conf

Active: active (running) since Wed 2024-10-02 06:26:51

Docs: man:httpd.service(8)

Main PID: 3242 (httpd)

Status: "Started, listening on: port 80"

Tasks: 177 (limit: 1112)

Memory: 13.1M

CPU: 47ms

CGroup: /system.slice/httpd.service

-3242 /usr/sbin/httpd -DFOREGROUND

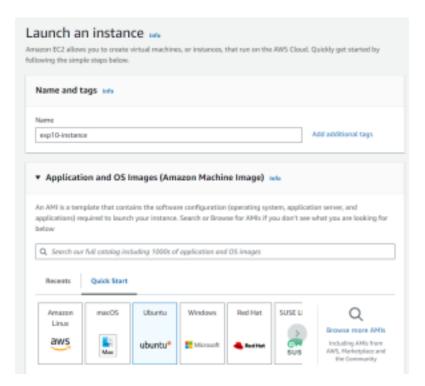
-3243 /usr/sbin/httpd -DFOREGROUND

-3244 /usr/sbin/httpd -DFOREGROUND

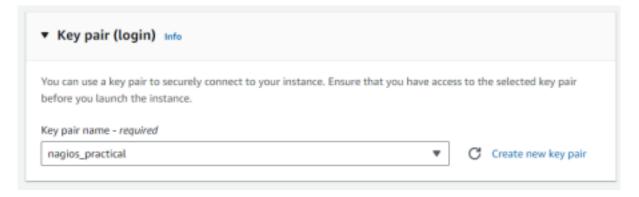
-3245 /usr/sbin/httpd -DFOREGROUND

-3246 /usr/sbin/httpd -DFOREGROUND
```

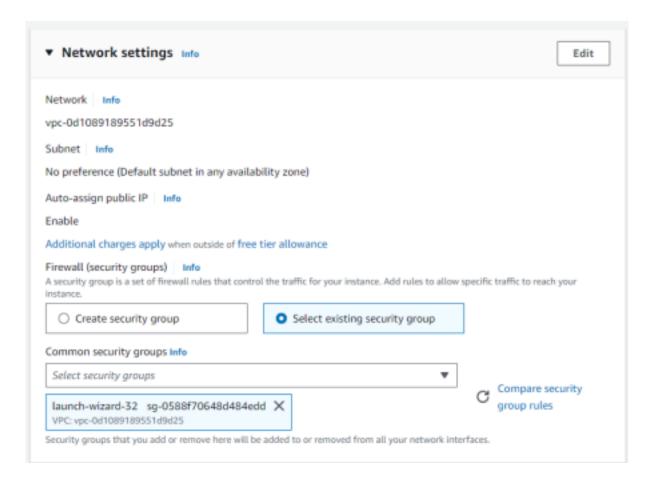
2. Now we will launch a new instance. Select ubuntu for the OS.



3. Select the key pair which was created and used in the exp 9.



4. Select existing security group and from the list of options select the security group created for exp 9. Previously it was launch wizard 32 and so here I have selected the same.



5. Open a new terminal to connect to the client machine. Copy the SSH command provided in the SSH client section during connection of instance. When pasting the command into your terminal, ensure you specify the full path to your .pem file instead of just the file name.

6. Now go back to your host machine and run the following command ps -ef | grep nagios

```
[ec2-user@ip-172-31-87-75 -]$ ps -ef | grep nagios nagios 2002 1 0 86:17 ? 00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg nagios 2003 2002 8 86:17 ? 00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh nagios 2004 2002 8 86:17 ? 00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh nagios 2006 2002 8 86:17 ? 00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh nagios 2007 2002 8 06:17 ? 00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh nagios 2007 2002 8 06:17 ? 00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg 00:00:00 grep --colormauto nagios (ec2-user@ip-172-31-87-75 -]$
```

7. Now perform these commands on the host terminal sudo su mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts

```
[root@ip-172-31-87-75 ec2-user]# mkdir -p /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-87-75 ec2-user]# |
```

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

```
[root@ip-172-31-87-75 ec2-user]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhosts/linuxhost
```

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

The above given command will open the nano text editor wherein you have to do the following changes:

i. Change the hostgroup name to linux-servers1

ii. Change host name and alias from localhost to linuxserver everywhere in the file

iii. Change the address to the public IPv4 address of the ubuntu instance (You will find the ip address when you select the instance on the ec2 instances dashboard)

8. Open the Nagios Config file by using this command: nano /usr/local/nagios/etc/nagios.cfg nano text editor will get opened

```
NAGIOS.CFG - Sample Main Config File for Nagios 4.5.5
# file. I've provided some comments here, but things may not be so
  clear without further explanation.
# LOG FILE
# This is the main log file where service and host events are logged
# for historical purposes. This should be the first option specified
# in the config file!!!
log_file=/usr/local/nagios/var/nagios.log
# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.
# You can specify individual object config files as shown below: cfg_file=/usr/local/nagios/etc/objects/commands.cfg
cfg_file=/usr/local/nagios/etc/objects/contacts.cfg
cfg_file=/usr/local/nagios/etc/objects/timeperiods.cfg
cfg_file=/usr/local/nagios/etc/objects/templates.cfg
# Definitions for monitoring the local (Linux) host
cfg_file=/usr/local/nagios/etc/objects/localhost.cfg
# Definitions for monitoring a Windows machine
```

9. In the text editor add "cfg_dir=/usr/local/nagios/etc/objects/monitorhosts/" this line

```
# 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/
```

10. Now we will verify the configuration files

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

```
Nagios Core 4.5.5
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2024-09-17
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 θ 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:
Things look okay - No serious problems were detected during the pre-flight check
[root@ip-172-31-87-75 ec2-user]# |
```

If there are no errors we can proceed further

11. We will now restart the nagios service service nagios restart

```
[root@ip-172-31-87-75 ec2-user]# service nagios restart Redirecting to /bin/systemctl restart nagios.service [root@ip-172-31-87-75 ec2-user]# |
```

12. Now on the client machine (The ubuntu machine we created for this experiment) run the following command:

sudo apt update -y

```
ubuntu@ip-172-31-40-130:-$ sudo apt update -y

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-backports InRelease [126 kB]

Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [15.0 MB]

Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Packages [18.0 MB]

Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]

Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe amd64 Components [3871 kB]

Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [3871 kB]

Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]

Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]

Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/multiverse amd64 Components [35.0 kB]

Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-multiverse amd64 Components [35.0 kB]

Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [535 kB]

Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [380 kB]

Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [380 kB]

Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]

Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]

Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [45.0 kB]

Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [212 B]

Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/multivers
```

sudo apt install gcc -y

```
t be installed:
utils-x86-64-linux-gnu cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linux-gnu fontconfig-config fonts-dejavu-core
gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu libaom3 libasan8 libatomic1 libbinutis libc-dev-bin libc-devtools
dev libtef-nobfd0 libctf0 libde250-0 libdeflate0 libfontconfig1 libgcc-13-dev libgd3 libgenp1 libgprofig0
f-plugin-aomenc libheif-plugin-libde265 libheif1 libhwasan0 libisl23 libitm1 libjbig0 libjpeg-turbo8 libjpeg8 liblerc4
0 libsframe1 libsharpyuv0 libitff6 libtsan2 libubsan1 libwebp7 libxpm4 linux-libc-dev manpages-dev rpcsvc-proto
0 to remove and 6 not upgraded.
```

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

```
sudo apt install -y nagios-nrpe-server nagios-plugins
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
The following additional packages will be installed:
libavahi-client3 libavahi-common-data libavahi-common3 libcups2t64 libdbi1t64 libldb2 libmysqlclient21 libnet-snmp-perl libpq5 libradcli4 libsmbclient0
libsnmp-base libsnmp40t64 libtalloc2 libtdb1 libtevent0t64 liburiparser1 libmbclient0 monitoring-plugins-basic monitoring-plugins-common
monitoring-plugins-standard mysql-common python3-gpg python3-ldb python3-markdown python3-samba python3-talloc python3-tdb rpcbind samba-common
samba-common-bin samba-dsdb-modules samba-libs smbclient snmp
                              Amba-common-bin samba-dsdb-modules samba-libs smbclient snmp

pested packages:

pested packages will be installed:

blowing NEW packages will be installed:

blowahi-cinent3 libavahi-common-data libavahi-common3 libcups2t64 libdbi1t64 libldb2 libmysqlclient21 libnet-snmp-perl libpq5 libradcli4 libsmbclient8

blowahi-cinent3 libavahi-common-data libavahi-common3 libcups2t64 libdbi1t64 libldb2 libmysqlclient21 libnet-snmp-perl libpq5 libradcli4 libsmbclient8

blosnmp-base libsnmp40t64 libtalloc2 libtdb1 libtevent0t64 liburiparser1 libmbclient0 monitoring-plugins monitoring-plugins-basic

printoring-plugins-common monitoring-plugins-standard mysql-common nagios-nrpe-server python3-gpg python3-ldb python3-markdown python3-samba

pyraded, 37 newly installed, 0 to remove and 6 not upgraded.

I to get 16.1 MB of archives.

Per this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation, 72.0 MB of additional disk space will be used.

Pet this operation of the this operation of the transfer of
```

13. Open nrpe.cfg file to make changes.

sudo nano /etc/nagios/nrpe.cfg

Under allowed hosts, add your nagios host public IPv4 address:

```
# 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=127.0.0.1,54.163.184.143

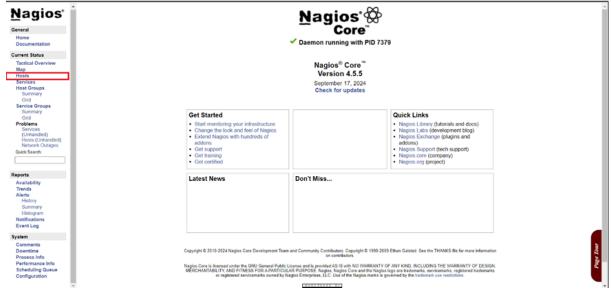
# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed. This option only works
# if the daemon was configured with the --enable-command-args configure script
# option.
#
# *** ENABLING THIS OPTION IS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

14. Now restart the NRPE server

sudo systemctl restart nagios-nrpe-server

```
ubuntu@ip-172-31-40-130:~$ sudo systemctl restart nagios-nrpe-server ubuntu@ip-172-31-40-130:~$
```

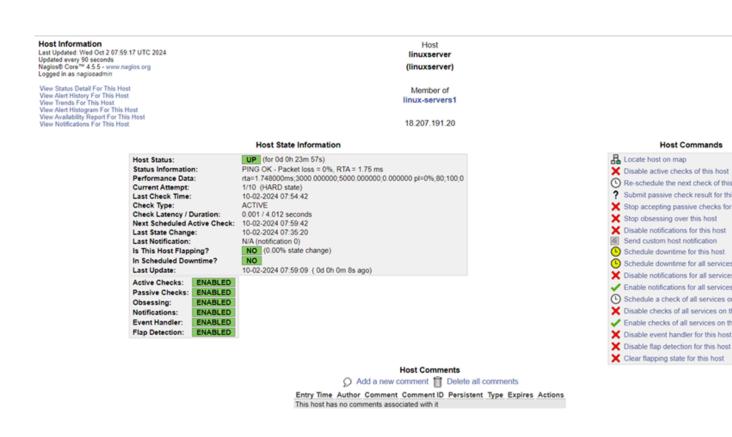
15. Go to the nagios dashboard and click on hosts



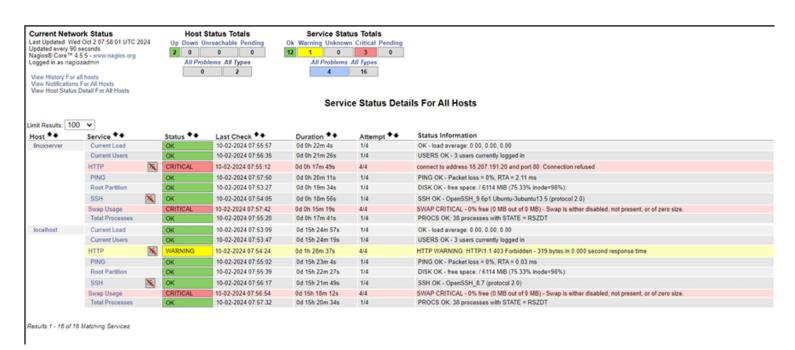
Click on linux server



We can see the host state information:



If you want to see all the services and ports being monitored then select the services option and you will see the page as shown below:



Conclusion: To conduct this experiment, it's necessary to start the instance from the previous experiment, as it will serve as the host, while the instance created in this experiment will act as the client machine. When I attempted to run the command to verify the Nagios configuration file, I encountered errors. To resolve these errors, I reinstalled the Nagios plugins and restarted the Nagios service, which fixed the issues.