

Experiment No 10

Mayur Jaiswal
D15B 26
Batch B

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

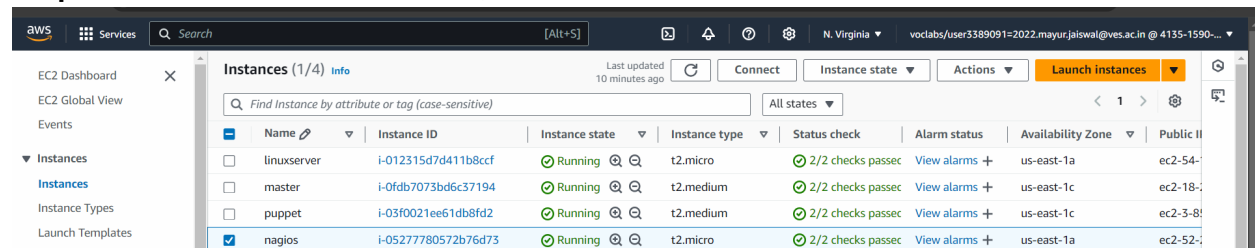
Output-

Step 1: To Confirm that Nagios is running on the server side, run this `sudo systemctl status nagios` on the "NAGIOS HOST".

```
● nagios.service - Nagios Core 4.4.14
   Loaded: loaded (/lib/systemd/system/nagios.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2023-09-30 08:54:01 UTC; 20s ago
     Docs: https://www.nagios.org/documentation
  Process: 55285 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
  Process: 55286 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
 Main PID: 55287 (nagios)
    Tasks: 6 (limit: 1141)
   Memory: 5.3M
      CPU: 252ms
  CGroup: /system.slice/nagios.service
          └─55287 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
            └─55288 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
              └─55289 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                └─55290 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                  └─55291 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
                    └─55292 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg

Sep 30 08:54:01 ip-172-31-44-151 nagios[55287]: qh: Socket '/usr/local/nagios/var/rw/nagios.qh' successfully initialized
lines 1-19
```

Step 2: To monitor a Linux machine, create an Ubuntu 20.04 server EC2 Instance in AWS.



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
linuxserver	i-012315d7d411b8cfc	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-54-
master	i-0fdb7073bd6c37194	Running	t2.medium	2/2 checks passed	View alarms	us-east-1c	ec2-18-
puppet	i-03f0021ee61db8fd2	Running	t2.medium	2/2 checks passed	View alarms	us-east-1c	ec2-3-8-
nagios	i-05277780572b76d73	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-52-

Step 3: On client side Step-03 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
```

```
[root@ip-172-31-40-105 ec2-user]# sudo yum update -y # For CentOS/RHEL
sudo dnf update -y # For Fedora
Last metadata expiration check: 1:55:22 ago on Tue Oct 15 16:43:59 2024.
Dependencies resolved.
Nothing to do.
Complete!
Last metadata expiration check: 1:55:23 ago on Tue Oct 15 16:43:59 2024.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-172-31-40-105 ec2-user]#
```

```
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'monitoring-plugins' instead of 'nagios-plugins'
monitoring-plugins is already the newest version (2.3.1-lubuntu4).
nagios-nrpe-server is already the newest version (4.0.3-lubuntu2).
0 upgraded, 0 newly installed, 0 to remove and 2 not upgraded.
```

```
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?addressfamily=ipv4&connType=standard&instanceId=i-05277780572b76d73&osUser=ec2-user&region=us-east-1&sshPort=22#
AWS Services Search [Alt+S] N. Virginia voclabs/user3389091=2022.mayur.jaiswal@ves.ac.in @ 4135-1590-...

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

/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/contacts.cfg /usr/local/nagios/etc/objects/contacts.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/timeperiods.cfg /usr/local/nagios/etc/objects/timeperiods.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/localhost.cfg /usr/local/nagios/etc/objects/localhost.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/windows.cfg /usr/local/nagios/etc/objects/windows.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/printer.cfg /usr/local/nagios/etc/objects/printer.cfg
/usr/bin/install -c -b -m 664 -o nagios -g nagios sample-config/template-object/switch.cfg /usr/local/nagios/etc/objects/switch.cfg

*** Config files installed ***

Remember, these are *SAMPLE* config files. You'll need to read
the documentation for more information on how to actually define
services, hosts, etc. to fit your particular needs.

/usr/bin/install -c -m 775 -o nagios -g nagios -d /usr/local/nagios/var/rw
chmod g+s /usr/local/nagios/var/rw

*** External command directory configured ***

/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf
if [ 0 -eq 1 ]; then \
    ln -s /etc/httpd/conf.d/nagios.conf /etc/apache2/sites-enabled/nagios.conf; \
fi

*** Nagios/Apache conf file installed ***

[root@ip-172-31-40-105 nagios-4.4.6]# sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.conf
sudo systemctl start nagios
```

```
AWS Services Search [Alt+S] N. Virginia voclabs/user3389091=2022.mayur.jaiswal@ves.ac.in @ 4135-1590-...

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

Nagios user: nagios
Nagios group: nagios

Review the options above for accuracy. If they look okay,
type 'make all' to compile the NRPE daemon and client
or type 'make' to get a list of make options.

cd ./src/; make
make[1]: Entering directory '/tmp/nrpe-nrpe-4.0.3/src'
gcc -g -O2 -DHAVE_CONFIG_H -I ../include -I ../include -o nrpe ./nrpe.c ./utils.c ./acl.c
gcc -g -O2 -DHAVE_CONFIG_H -I ../include -I ../include -o check_nrpe ./check_nrpe.c ./utils.c
make[1]: Leaving directory '/tmp/nrpe-nrpe-4.0.3/src'

*** Compile finished ***

You can now continue with the installation or upgrade process.

Read the PDF documentation (docs/NRPE.pdf) for information on the next
steps you should take to complete the installation or upgrade.

groupadd -r nagios
useradd -r -g nagios nagios
[root@ip-172-31-38-178 nrpe-nrpe-4.0.3]# sudo make install
sudo make install-config
sudo nano /etc/services
nrpe 5666/tcp
```

```
GNU nano 6.2 /etc/nagios/nrpe.cfg *
95 # that are allowed to talk to the NRPE daemon. Network addresses with a bit mask
96 # (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
97 # supported.
98 #
99 # Note: The daemon only does rudimentary checking of the client's IP
100 # address. I would highly recommend adding entries in your /etc/hosts.allow
101 # file to allow only the specified host to connect to the port
102 # you are running this daemon on.
103 #
104 # NOTE: This option is ignored if NRPE is running under either inetd or xinetd
105
106 allowed_hosts=127.0.0.1,::1,13.235.0.144
107 server_address=0.0.0.0
108
109
110

^G Help ^O Write Out ^W Where Is ^K Cut ^_ Execute ^C Location ^U Undo ^M-A Set Mark
^X Exit ^R Read File ^N Replace ^V Paste ^J Justify ^_ Go To Line ^M-B Redo ^M-C Copy
```

Step 5: Restart the NRPE server

sudo systemctl restart nagios-nrpe-server

```
Restarting services...
Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart getty@tty1.service
systemctl restart networkd-dispatcher.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service
systemctl restart user@1000.service

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.
root@ip-172-31-41-41:/home/ubuntu# sudo nano /etc/nagios/nrpe.cfg
root@ip-172-31-41-41:/home/ubuntu# sudo nano /etc/nagios/nrpe.cfg
root@ip-172-31-41-41:/home/ubuntu# sudo systemctl restart nagios-nrpe-server
root@ip-172-31-41-41:/home/ubuntu# sudo systemctl status nagios-nrpe-server
● nagios-nrpe-server.service - Nagios Remote Plugin Executor
```

Step 6:

```
root@ip-172-31-44-151:/home/ubuntu# ps -ef | grep nagios
nagios    55287      1    0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios    55288    55287    0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios    55289    55287    0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios    55290    55287    0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios    55291    55287    0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios    55292    55287    0 08:54 ?        00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios    56327      1    0 08:58 ?        00:00:00 /usr/sbin/nrpe -c /etc/nagios/nrpe.cfg -f
root      60903    60158    0 09:32 pts/1    00:00:00 grep --color=auto nagios
root@ip-172-31-44-151:/home/ubuntu# sudo su
root@ip-172-31-44-151:/home/ubuntu# mkdir /usr/local/nagios/etc/objects/monitorhosts
root@ip-172-31-44-151:/home/ubuntu# mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
```

Step 7: /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

```
root@ip-172-31-44-151:/home/ubuntu# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
root@ip-172-31-44-151:/home/ubuntu# nano /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
```

```
GNU nano 6.2 /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg
#####
# 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            127.0.0.1
}

[

^G Help      ^C Write Out  ^W Where Is   ^R Cut        ^T Execute    ^L Location   ^U Undo       ^M Set Mark
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_/ Go To Line ^_B Redo      ^_C Copy

i-03a3e79fc5ab0a056 (cutenagios_server)
```

```
GNU nano 6.2 /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg *

#####
#
# HOST GROUP DEFINITION
#
#####

# Define an optional hostgroup for Linux machines

define hostgroup {

    hostgroup_name    linux-servers    ; 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
}

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark
^X Exit      ^R Read File  ^N Replace    ^U Paste      ^J Justify    ^_/ Go To Line  M-E Redo      M-G Copy
```

Change hostgroup_name under hostgroup to linuxserver

```
GNU nano 6.2 /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
Save modified buffer?
Y Yes
N No      ^G Cancel
```

Step 10: Verify the configuration files.

```
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-172-31-44-151:/home/ubuntu# nano /usr/local/nagios/etc/nagios.cfg
```

Step 12: Now, check your nagios dashboard and you'll see a new host being added.

Not secure | 3.111.245.110/nagios/

Nagios

General

Home

Documentation

Current Status

Tactical Overview

Map (Legacy)

Hosts

Services

Host Groups

Summary

Grid

Service Groups

Summary

Grid

Problems

Services (Unhandled)

Hosts (Unhandled)

Network Outages

Quick Search:

Reports

Availability

Trends (Legacy)

Alerts

History

Summary

Histogram (Legacy)

Notifications

Event Log

System

Comments

Downtime

Process Info

Performance Info

Scheduling Queue

Configuration

Current Network Status
Last Updated: Sat Sep 30 18:22:09 UTC 2023
Updated every 90 seconds
Nagios® Core™ 4.4.14 - 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

No Down	Unreachable	Pending
0	0	0

All Problems

All Types

0	2
---	---

Service Status Totals

No Warning	Unknown	Critical	Pending
0	0	3	0

All Problems

All Types

3	16
---	----

Host Status Details For All Host Groups

Limit Results: 100

Host **	Status **	Last Check **	Duration **	Status Information
linuxserver	UP	09-30-2023 18:17:06	0d 0h 5m 3s	PING OK - Packet loss = 0%, RTA = 0.62 ms
localhost	UP	09-30-2023 18:20:14	0d 0h 28m 7s	PING OK - Packet loss = 0%, RTA = 0.04 ms

Results 1 - 2 of 2 Matching Hosts

General

Home

Documentation

Current Status

Tactical Overview

Map (Legacy)

Hosts

Services

Host Groups

Summary

Grid

Service Groups

Summary

Grid

Problems

Services (Unhandled)

Hosts (Unhandled)

Network Outages

Quick Search:

Reports

Availability

Trends (Legacy)

Alerts

History

Summary

Histogram (Legacy)

Notifications

Event Log

System

Comments

Downtime

Process Info

Performance Info

Scheduling Queue

Configuration

Current Network Status
Last Updated: Tue Oct 3 23:38:11 UTC 2023
Updated every 90 seconds
Nagios® Core™ 4.4.14 - 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

No Down	Unreachable	Pending
2	0	0

All Problems

All Types

0	2
---	---

Service Status Totals

No Warning	Unknown	Critical	Pending
0	0	3	0

All Problems

All Types

3	16
---	----

Conclusion: In this experiment, a new host was added to the Nagios monitoring system. The process involved configuring the host's definition in Nagios, applying changes by restarting the Nagios service, and verifying the host's visibility on the web interface. Proper configuration and connectivity were key to successfully monitoring the new host