Adv DevOps Practical 10

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

Theory:

Port and Service Monitoring

Port and service monitoring in Nagios involves checking the availability and responsiveness of network services running on specific ports. This ensures that critical services (like HTTP, FTP, or SSH) are operational. Nagios uses plugins to ping the ports and verify whether services are up and responding as expected, allowing administrators to be alerted in case of outages.

Windows/Linux Server Monitoring

Windows/Linux server monitoring with Nagios entails tracking the performance and health of servers running these operating systems. It includes monitoring metrics such as CPU usage, memory consumption, disk space, and system logs. Nagios employs various plugins to gather data, enabling administrators to ensure optimal performance, identify potential issues, and maintain uptime across their server infrastructure.

Prerequisites:

AWS Academy or Personal account.

Nagios Server running on Amazon Linux Machine. (Refer Experiment No 9)

Monitoring Using Nagios:

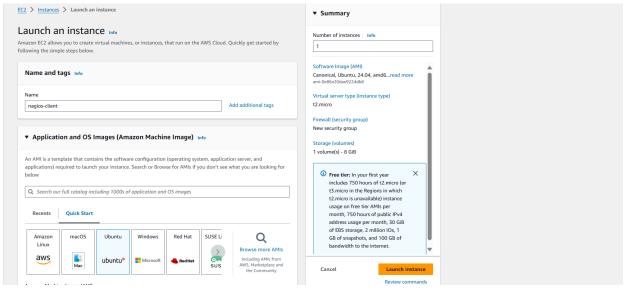
Step 1: To Confirm Nagios is running on the server side Perform the following command on your Amazon Linux Machine (Nagios-host).

sudo systemctl status nagios

```
coaueu (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
active (running) since Sun 2024-09-29 16:18:08 UTC; 21min ago
https://www.nagios.org/documentation
1942 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
1944 ExecStart=/usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
1946 (nagios)
8 (limit: 1112)
7.7M
387ms
//system.slice/
```

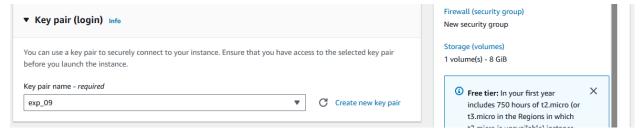
You can now proceed if you get the above message/output.

Step 2: Now Create a new EC2 instance. Name: Nagios-client, AMI: Ubuntu Instance Type: t2.micro.



For Key pair : Click on create key and make key of type RSA with extension .pem . Key will be downloaded to your local machine.

Now select that key in key pair if you already have key with type RSA and extension .pem no need to create new key but you must have that key downloaded.



Select the Existing Security Group and select the Security Group that we have created in Experiment no 9 or the same one you have used for the Nagios server (Nagios-host).

▼ Network settings Info	Number of instances Info Edit 1
Network Info vpc-0d4c0d8f48c2e4508 Subnet Info No preference (Default subnet in any availability zone)	Software Image (AMI) Canonical, Ubuntu, 24.04, amd6read more ami-0e86e20dae9224db8 Virtual server type (instance type)
Auto-assign public IP Info	t2.micro Firewall (security group) launch-wizard-3
Additional charges apply when outside of free tier allowance Firewall (security groups) Info A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach you instance.	Storage (volumes) 1 volume(s) - 8 GiB
Create security groups Common security groups info Select security groups Taunch-wizard-3 sg-09d51590eb1851b46 X VPC: vpc-0d4c0d8f48c2e4508 Security groups that you add or remove here will be added to or removed from all your network interfaces.	Tree 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 10s, 1

Step 4: Now on the server Nagios-host run the following command.

ps -ef | grep nagios

```
[ec2-user@ip-172-3i-91-91 ~]$ ps -ef | grep nagios
nagios 1946 1 0 16:18 ? 00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios 1947 1946 0 16:18 ? 00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios 1948 1946 0 16:18 ? 00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios 1949 1946 0 16:18 ? 00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios 1950 1946 0 16:18 ? 00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios 1956 1946 0 16:18 ? 00:00:00 /usr/local/nagios/bin/nagios -d /usr/local/nagios/var/rw/nagios.qh
root 3090 3055 0 16:40 pts/0 00:00:00 sudo systemctl status nagios
root 3092 3090 0 16:40 pts/1 00:00:00 sudo systemctl status nagios
root 3093 3092 0 16:40 pts/1 00:00:00 sudo systemctl status nagios
ec2-user 3014 3890 0 16:59 pts/2 00:00:00 grep --color=auto nagios
[ec2-user@ip-172-31-91-91 -]$
```

Step 5: Now Become root user and create root directories.

sudo su

mkdir /usr/local/nagios/etc/objects/monitorhosts

mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts

```
[ec2-user@ip-172-31-91-91 ~]$ sudo su
[root@ip-172-31-91-91 ec2-user]# mkdir /usr/local/nagios/etc/objects/monitorhosts mkdir /usr/local/nagios/etc/objects/monitorhosts/linuxhosts
[root@ip-172-31-91-91 ec2-user]# |
```

Step 6: Copy the sample localhost.cfg to linuxhost.cfg by running the following command.(Below command should come in one line see screenshot below)

cp /usr/local/nagios/etc/objects/localhost.cfg

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

[root@ip-172-31-91-91 ec2-user]# cp /usr/local/nagios/etc/objects/localhost.cfg /usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg [root@ip-172-31-91-91 ec2-user]# |

Step 7:Open linuxserver.cfg using nano and make the following changes in all positions?everywhere in file.

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

Change hostname to linuxserver.

Change address to the public IP of your Linux client.

Set hostgroup name to linux-servers1.

Step 8: Now update the Nagios config file .Add the following line in the file. Line to add : > nano /usr/local/nagios/etc/nagios.cfg

cfg dir=/usr/local/nagios/etc/objects/monitorhosts/

Step 9: Now Verify the configuration files by running the following commands. /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

```
Inings took okay - No serious problems were detected during the pre-+tight check
[root@ip-172-31-91-91 ec2-user]# /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
```

```
Running pre-flight check on configuration data...

Checked 8 services.
Checked 2 hosts.
Checked 2 hosts groups.
Checked 0 service groups.
Checked 1 contacts.
Checked 1 contacts.
Checked 1 contacts groups.
Checked 2 commands.
Checked 2 time periods.
Checked 5 time periods.
Checked 6 host escalations.
Checked 6 host escalations.
Checked 8 service escalations.
Checked 9 service escalations.
Checked 9 hosts
Checked 1 contacts
Checked 1 contacts
Checked 2 hosts
Checked 3 host escalations.
Checked 3 host escalations.
Checked 4 host service dependencies
Checked 6 host dependencies
Checked 8 host dependencies
Checked 9 host dependencies
Checking global event handlers...
Checking misc settings...

Total Warnings: 0
Total Warnings: 0
Total Errors: 0
```

Step 10: Now restart the services of nagios by running the following command.

service nagios restart

```
[root@ip=172-31-91-91 ec2-user]# service nagios restart

[root@ip=172-31-91-91 ec2-user]# service nagios restart

[ OK ]

[root@ip=172-31-91-91 ec2-user]# |
```

Step 11: Now Go to the Nagios-client ssh terminal and update and install the packages by running the following command.

sudo apt update -y sudo apt install gcc -y

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

```
ubuntu@ip-172-31-92-146:-$ sudo apt update -y
sudo apt install gcc -y
sudo apt install gcc -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-packports 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://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/universe Tanslation-en [5982 kB]
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Tanslation-en [82.9 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main Tanslation-en [82.9 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main Tanslation-en [82.9 kB]
Get:10 http://security.ubuntu.com/ubuntu noble-security/main Tanslation-en [82.7 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [3871 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [272 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [272 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [3622 B]
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [3623 B]
Get:16 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [18 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [333 kB]
Get:18 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [68:1 kB]
Get:19 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [68:1 kB]
Get:19 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:19 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Get:20 http://security.ubuntu.co
```

```
Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart getty@tty1.service
systemctl restart networkd-dispatcher.service
systemctl restart serial-getty@tty50.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service
No containers need to be restarted.

User sessions running outdated binaries:
ubuntu @ session #2: sshd[992,1102]
ubuntu @ session #7: sshd[1190,1248]
ubuntu @ session #7: sshd[1190,1248]
```

Step 12: Open nrpe.cfg file to make changes. Under allowed hosts, add your nagios host IP address.

51

sudo nano /etc/nagios/nrpe.cfg

```
# This determines the effective group that the NRPE daemon should run as.
# You can either supply a group name or a GID.
nrpe_group=nagios
# 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.
allowed_hosts=127.0.0.1,::1,34.207.68.187
# 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.
```

Step 13: Now restart the NRPE server by this command.

sudo systemctl restart nagios-nrpe-server

```
0 upgraded, 0 newly installed, 0 to remove and 139 not upgraded.
ubuntu@ip-172-31-92-146:~$ sudo nano /etc/nagios/nrpe.cfg
ubuntu@ip-172-31-92-146:~$ sudo systemctl restart nagios-nrpe-server
ubuntu@ip-172-31-92-146:~$
```

Step 14: Now again check the status of Nagios by running this command on Nagios-host and also check httpd is active and run the command to active it.

sudo systemctl status nagios

```
C2-user@ip-172-31-91-91 ~| sudo systemctl status nagios
nagios.service - Nagios Core 4.5.5
Loaded: loaded (/usr/lib/systemd/system/nagios.service; enabled; preset: disabled)
Active: active (running) since Sun 2024-09-29 17:20:07 UTC; 12min ago
Docs: https://www.nagios.org/documentation
Process: 4761 ExecStartPre=/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
Process: 4762 ExecStartPs_usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg (code=exited, status=0/SUCCESS)
Main PID: 4763 (nagios)
Tasks: 6 (limit: 1112)
Memory: 4.1M
CPU: 234ms
CGroup: /system.slice/nagios.service
-4763 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
-4764 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
-4765 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
-4766 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
-4767 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
-4768 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
-4768 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/etc/nagios.cfg
Sep 29 17:20:07 ip-172-31-91-91.ec2.internal nagios[4763]: Warning: Duplicate definition found for service 'Current Users' on host 'localhost' (config file Sep 29 17:20:07 ip-172-31-91-91.ec2.internal nagios[4763]: Warning: Duplicate definition found for service 'Root Partition' on host 'localhost' (config file Sep 29 17:20:07 ip-172-31-91-91.ec2.internal nagios[4763]: Warning: Duplicate definition found for service 'PING' on host 'localhost' (config file '/usr/Co Sep 29 17:20:07 ip-172-31-91-91.ec2.internal nagios[4763]: SCRUCE NOILFICATION: nagiosadmin; localhost; Swap Usage; CRITCAL; notify-service-by-email; SWAP CRI Sep 29 17:22:30 ip-172-31-91-91.ec2.internal nagios[4763]: wproc: stderr line 02: /usr/bin/sh: line 1: /bin/shi: Nail nail: No such file or directory stderr line 02: /usr/bin/printf: write error: Broken pipe
```

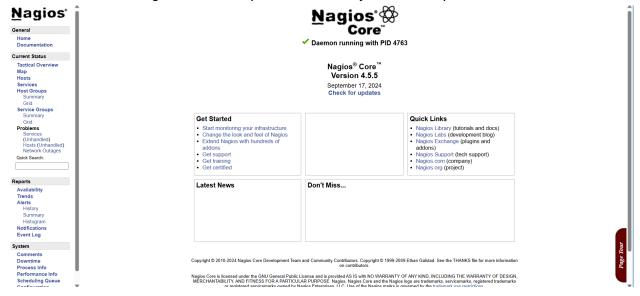
sudo systemctl status httpd

sudo systemctl start httpd sudo systemctl enable httpd

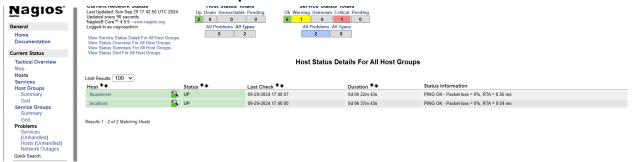
```
[ec2-user@ip-172-31-91-91 ~]$ sudo systemctl start httpd
[ec2-user@ip-172-31-91-91 ~]$ sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-172-31-91-91 ~]$ |
```

Step 15: Now to check Nagios dashboard go to http://<nagios host ip>/nagios Eg. http://34.207.68.187/nagios

Enter username as nagiosadmin and password which you set in Exp 9.



Now Click on Hosts from left side panel



Conclusion:

In this exercise, we established a Nagios host and client to oversee service and server performance across both Linux and Windows environments. We configured Nagios on an Amazon Linux instance to track essential services such as HTTP, SSH, and system resources, guaranteeing their availability and health. By provisioning a new EC2 instance as the Nagios client, we facilitated effective communication between the client and host, enabling streamlined service monitoring. This configuration enhances uptime and allows for swift identification of any issues within the infrastructure.