**Experiment Number 10**

Name:Aarya Gandhi

Roll No 15

Class:D15B

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

Theory:

**Introduction to Nagios**

Nagios is a powerful, open-source monitoring system designed to oversee the health and performance of IT infrastructure components, including servers, networks, applications, and services. It provides real-time monitoring, alerting, and reporting, enabling administrators to detect and address issues proactively before they impact business operations. Nagios is highly extensible through a modular architecture that supports a wide range of plugins and add-ons, making it adaptable to diverse monitoring needs.

**Key Features of Nagios:**

* **Comprehensive Monitoring:** Monitors network services (HTTP, SMTP, SSH), host resources (processor load, disk usage), and more.
* **Alerting Mechanism:** Sends notifications via email, SMS, or other channels when issues are detected or resolved.
* **Extensibility:** Supports custom plugins and scripts to monitor virtually any aspect of an IT environment.
* **Scalability:** Capable of monitoring large and complex infrastructures.
* **Web Interface:** Provides a user-friendly dashboard for visualizing the status of monitored components.

**Port Monitoring with Nagios**

**Port monitoring** involves checking the availability and responsiveness of specific network ports on servers and devices. Ports are essential for facilitating communication between different services and applications. Monitoring these ports ensures that services are reachable and functioning correctly.

**Objectives of Port Monitoring:**

* **Availability Check:** Ensure that a particular port is open and accepting connections.
* **Performance Assessment:** Measure response times and latency associated with port communication.
* **Security Oversight:** Detect unauthorized or unexpected services running on ports, which could indicate security breaches.

**Service Monitoring with Nagios**

**Service monitoring** focuses on overseeing the operational status and performance of specific services running on servers or network devices. This encompasses applications like web servers, databases, mail servers, and more, ensuring they are running smoothly and efficiently.

**Objectives of Service Monitoring:**

* **Operational Status:** Confirm that services are active and functioning as expected.
* **Performance Metrics:** Track service-specific metrics such as response times, throughput, and error rates.
* **Dependency Management:** Understand and monitor dependencies between different services to identify cascading failures.

**Steps:**

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

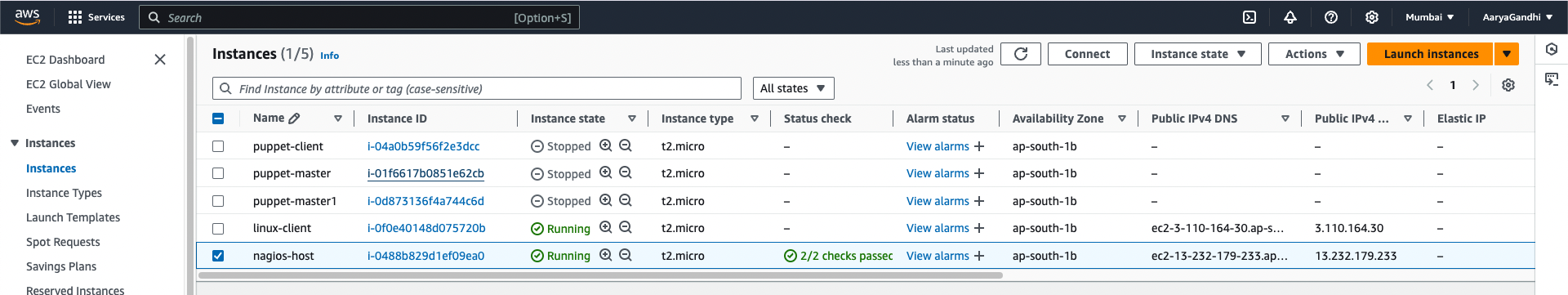
nagios on the “NAGIOS HOST”.

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’

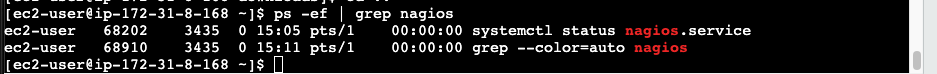
alongside the host.



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



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

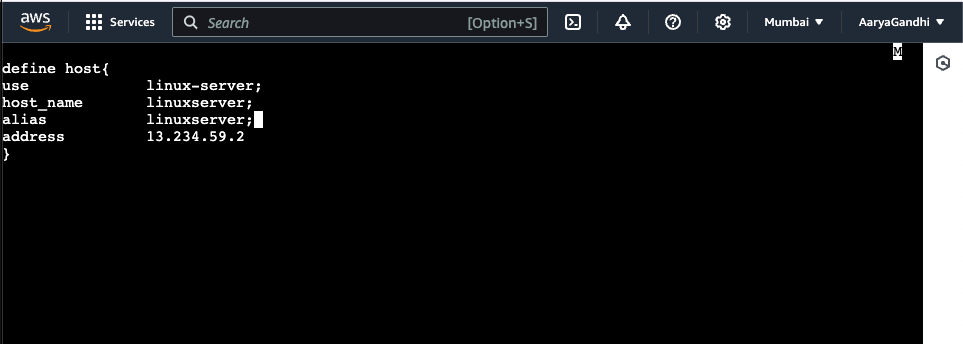
cp /usr/local/nagios/etc/objects/localhost.cfg

/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

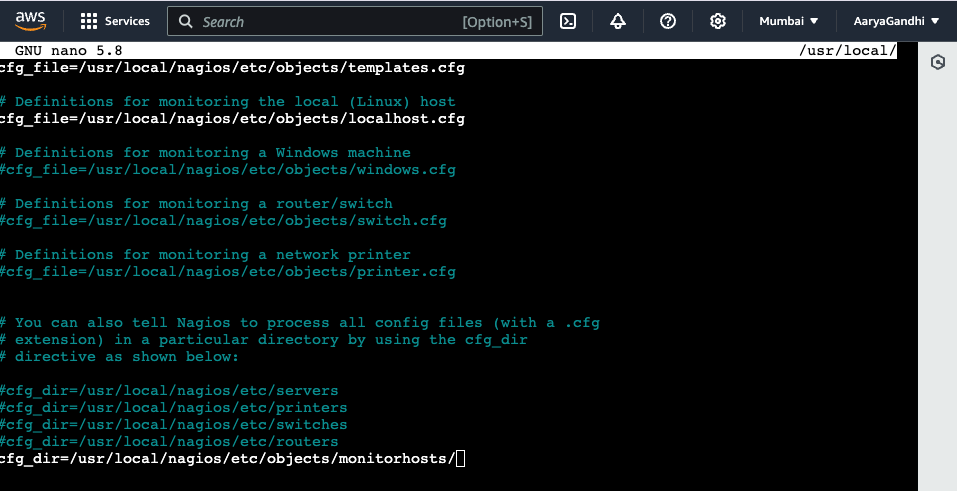


7. Open the Nagios Config file and add the following line

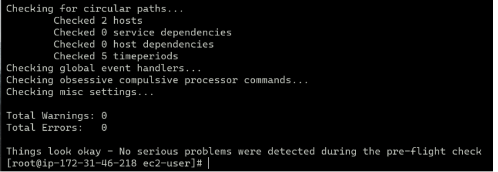
nano /usr/local/nagios/etc/nagios.cfg

##Add this line

cfg\_dir=/usr/local/nagios/etc/objects/monitorhosts/



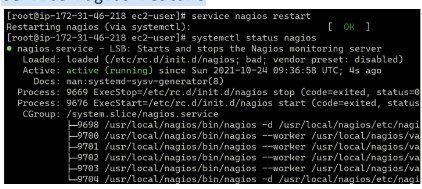
8. Verify the configuration files



You are good to go if there are no errors.

9. Restart the nagios service

service nagios restart



Now it is time to switch to the client machine.

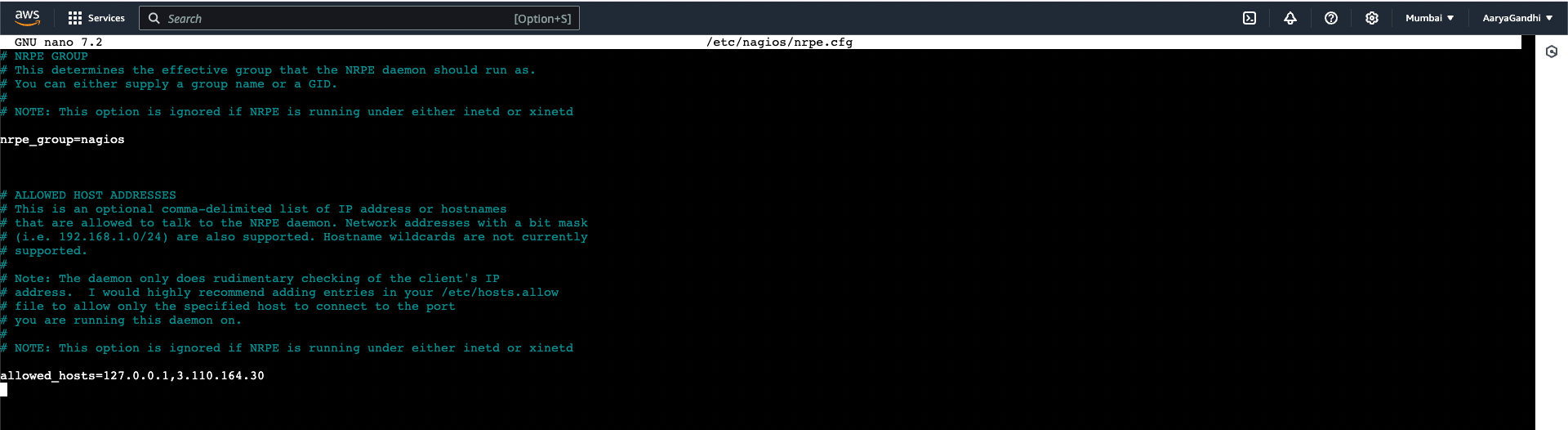
10. SSH into the machine or simply use the EC2 Instance Connect feature.

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

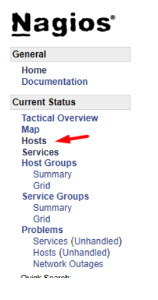


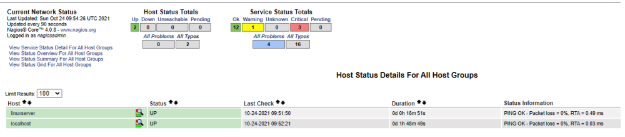
13. Restart the NRPE server

sudo systemctl restart nagios-nrpe-server

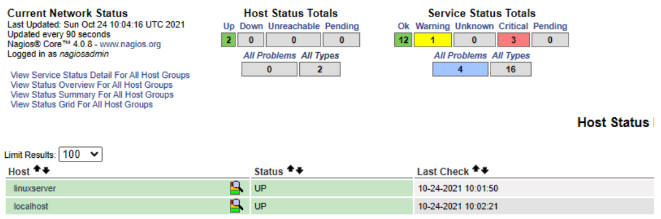
14. Now, check your nagios dashboard and you’ll see a new host being added.

Click on Hosts.

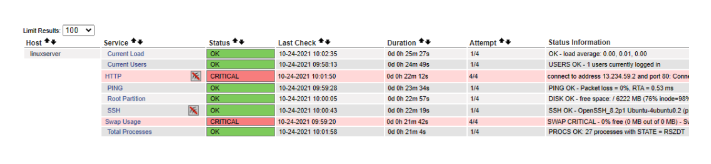




Click on linuxserver to see the host details



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



**Conclusion:**

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.