Name: Roma Shirodkar

Div: D15B

Roll No: 58

Experiment 10

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

Theory:

Nagios is an open-source monitoring system designed to monitor network services, host resources, and server metrics. It provides a comprehensive view of system and service status and alerts administrators about potential issues before they become critical. Here’s an overview of how to perform port and service monitoring, as well as Windows/Linux server monitoring using Nagios.

### **1. Overview of Nagios**

* **Architecture**: Nagios has a client-server architecture. The Nagios server monitors the services and hosts, while Nagios agents (or plugins) on the clients collect data.
* **Components**:
  + **Core**: The main monitoring engine.
  + **Plugins**: Executable scripts that check the status of services and system metrics.
  + **Web Interface**: A graphical interface for accessing monitoring data.

Service and port monitoring is a crucial aspect of IT infrastructure management, ensuring that network services and applications are running smoothly and securely. Here’s a detailed explanation of both concepts, their importance, methods, and tools commonly used in service and port monitoring.

### **2. Service Monitoring**

**Definition**:  
Service monitoring involves tracking the health and performance of various applications and services running on a server or network. This includes monitoring web servers, databases, file servers, email services, and more.

**Importance**:

* **Availability**: Ensures that critical services are operational and accessible to users.
* **Performance**: Helps identify performance bottlenecks and resource utilization issues.
* **Error Detection**: Alerts administrators to service failures or unexpected behaviors.
* **Proactive Maintenance**: Enables IT teams to address issues before they impact users or business operations.

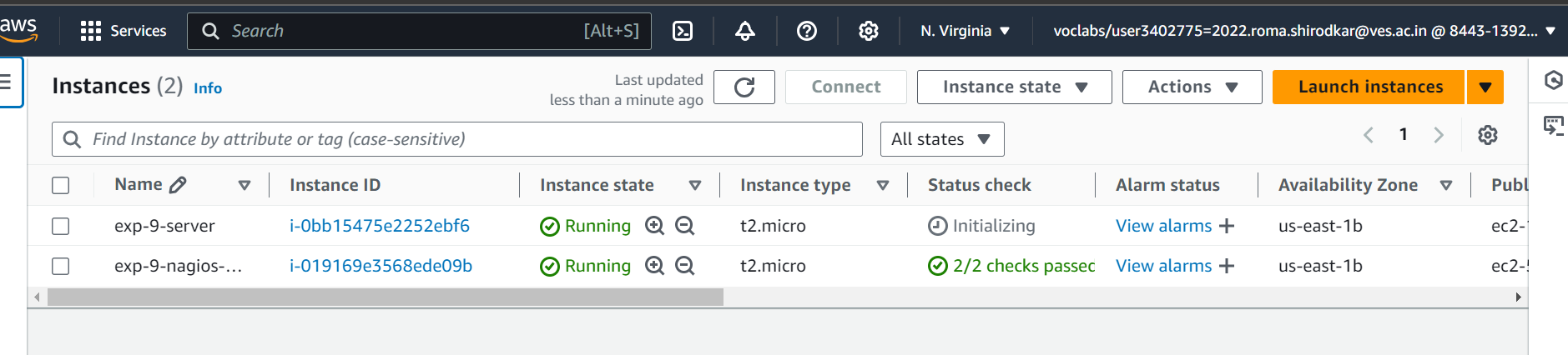
### **3. Port Monitoring**

**Definition**:  
Port monitoring focuses on tracking the status of network ports on a server or device to determine whether they are open, closed, or filtered. It checks whether specific services are listening on designated ports.

**Importance**:

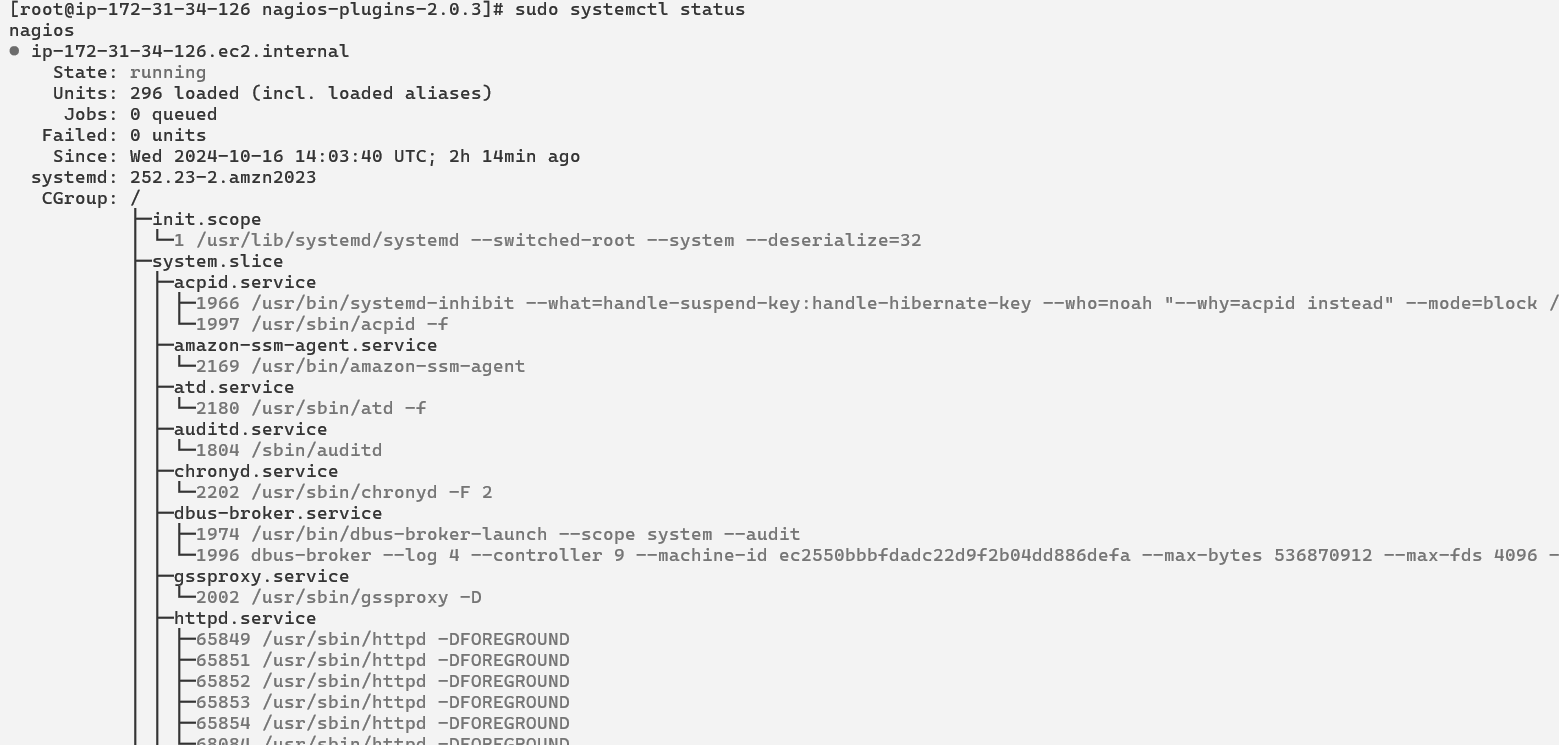
* **Security**: Identifies unauthorized access or potential vulnerabilities by monitoring open ports.
* **Service Accessibility**: Ensures that applications and services are accessible on the required ports.
* **Network Performance**: Helps in troubleshooting connectivity issues and ensuring optimal performance.

Create an ubuntu ec2 instance which will act as linux server



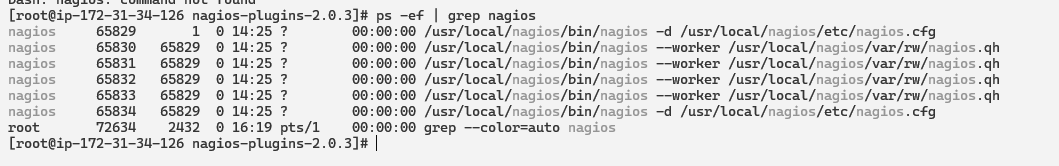
To Confirm that Nagios is running on the server side, run this sudo systemctl status

nagios on the “NAGIOS HOST”.



On the server, run this command

ps -ef | grep nagios

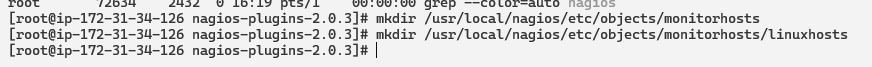


Become a root user and create 2 folders

sudo su

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

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



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



Open linuxserver.cfg using nano and make the following changes

nano

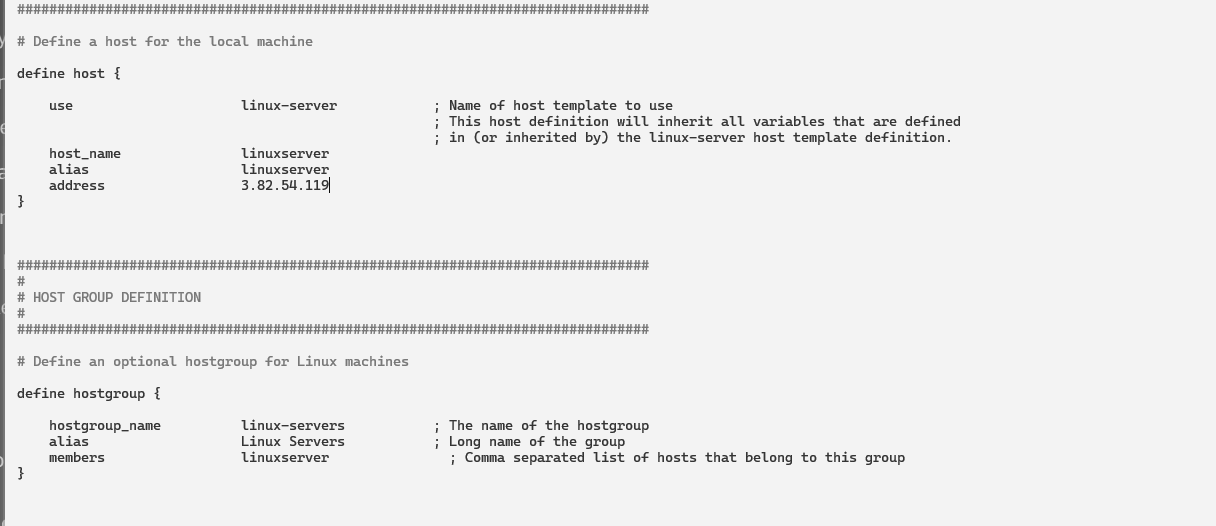
/usr/local/nagios/etc/objects/monitorhosts/linuxhosts/linuxserver.cfg

Change the hostname to linuxserver (EVERYWHERE ON THE FILE)

Change address to the public IP address of your LINUX CLIENT.

Change hostgroup\_name under hostgroup to linux-servers1

Everywhere else on the file, change the hostname to linuxserver instead of localhost.



Open the Nagios Config file and add the following line

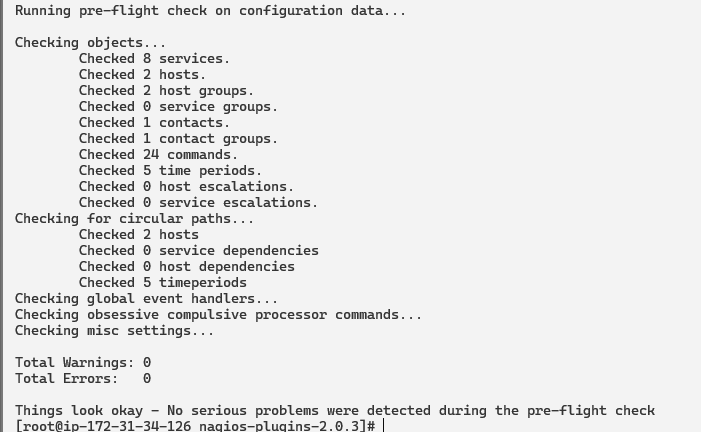
nano /usr/local/nagios/etc/nagios.cfg

##Add this line

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



Verify the configuration files

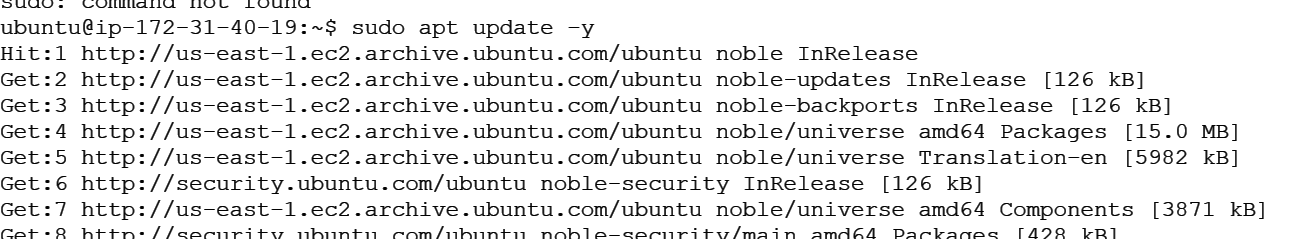


Restart the nagios service

service nagios restart

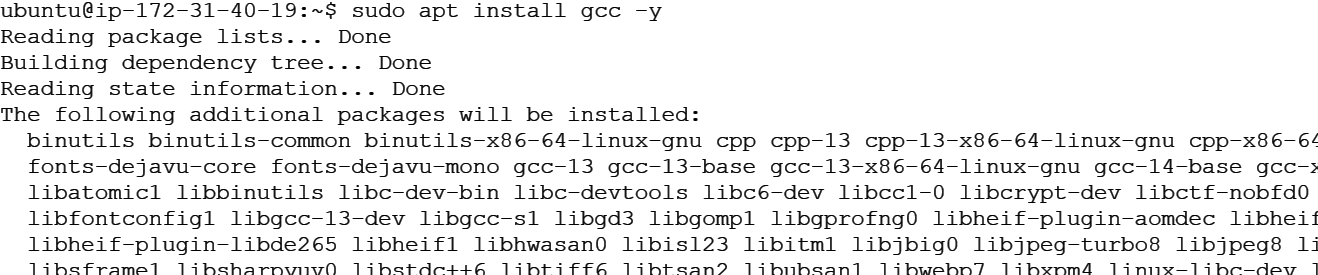
Check status





Now it is time to switch to the client machine.

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

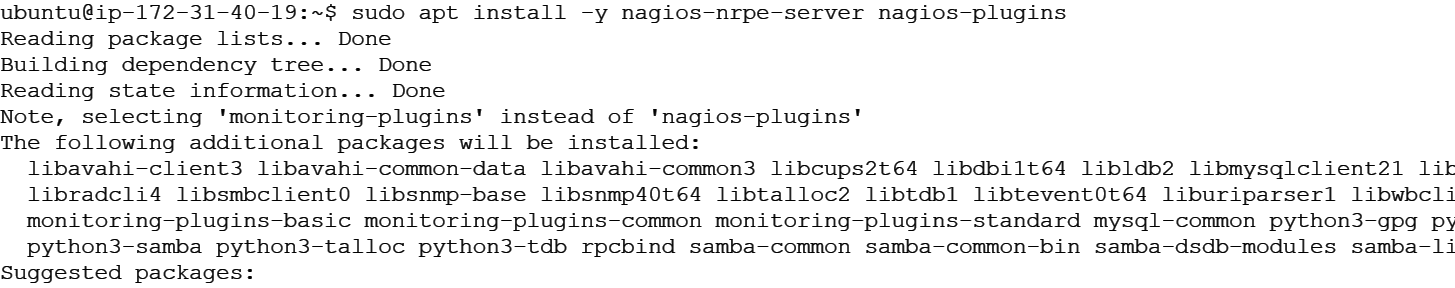


Make a package index update and install gcc, nagios-nrpe-server and the plugins.

sudo apt update -y

sudo apt install gcc -y

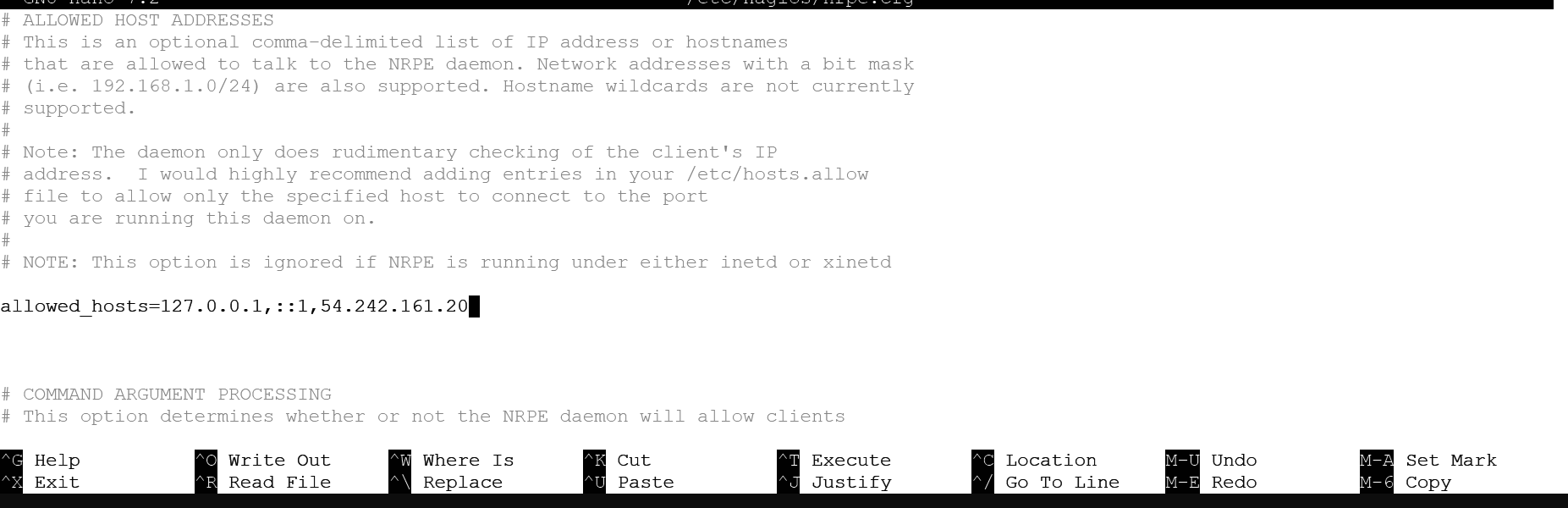
sudo apt install -y nagios-nrpe-server nagios-plugins



Open nrpe.cfg file to make changes.

sudo nano /etc/nagios/nrpe.cfg

Under allowed\_hosts, add your nagios host IP address like so

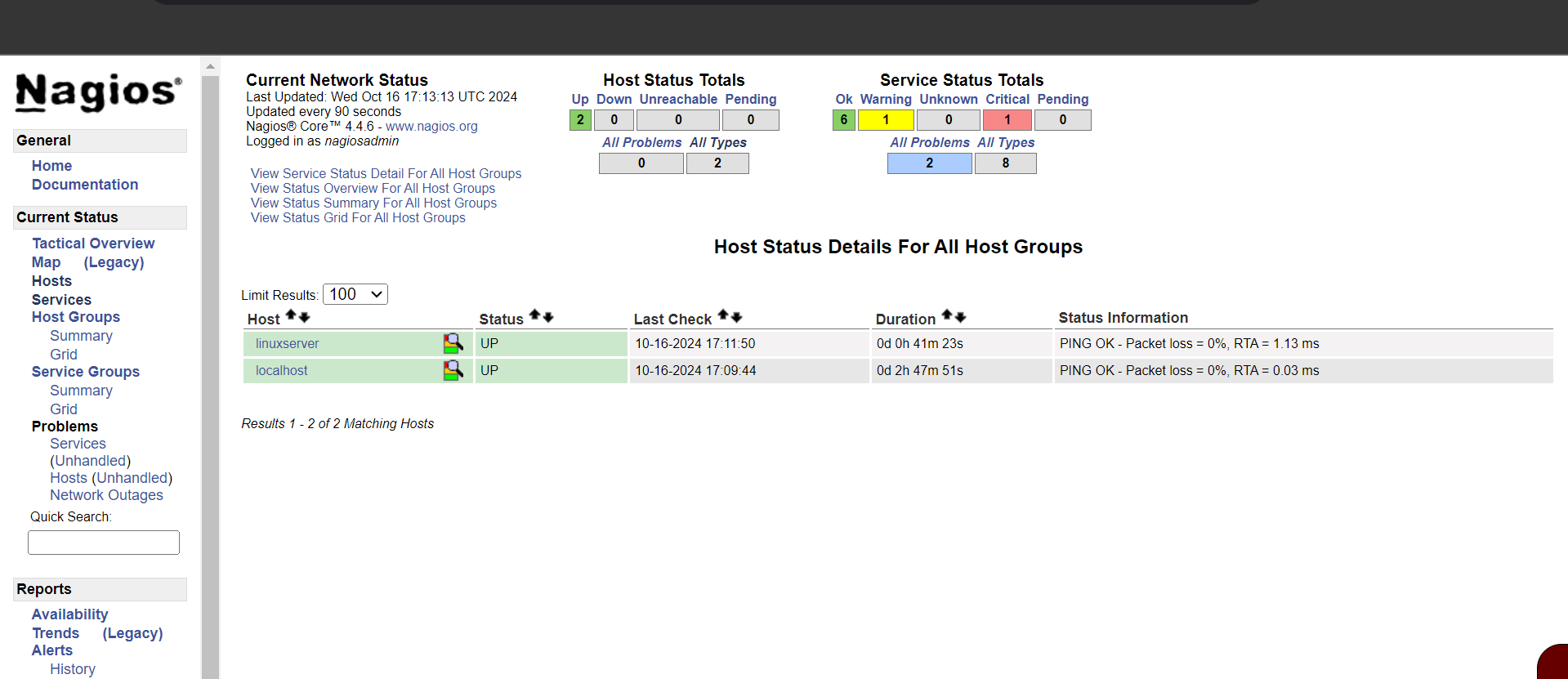


Restart the NRPE server

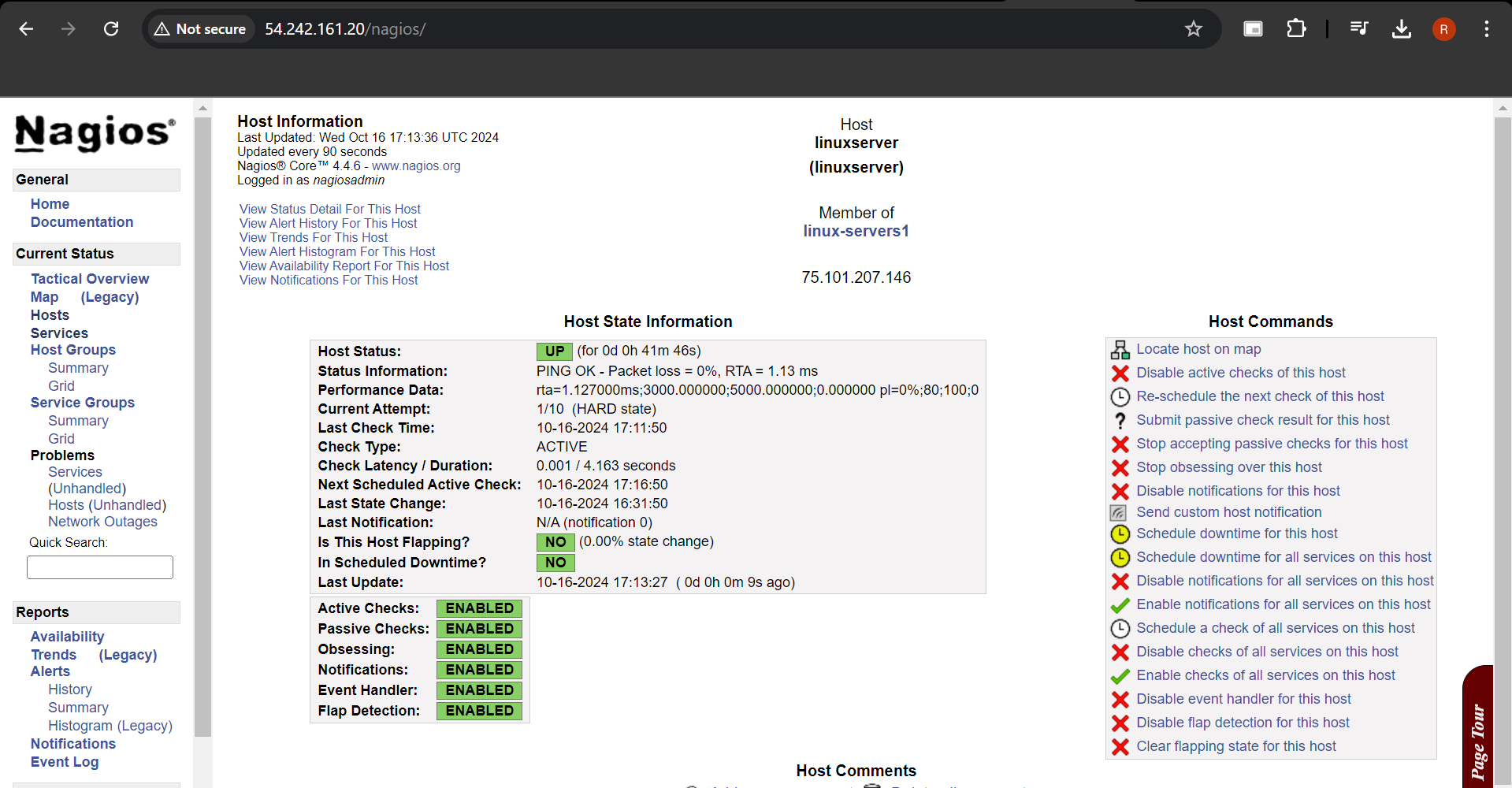
sudo systemctl restart nagios-nrpe-server

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



Conclusion: Service and port monitoring are essential for maintaining the health and security of IT infrastructure. By actively monitoring services and ports, organizations can ensure service availability, improve performance, and proactively identify and mitigate security risks. Utilizing effective monitoring tools and strategies enables IT teams to maintain operational efficiency and enhance the overall user experience.