**MONITORING WITH NAGIOS**

P.Sai Pradeep 20A91A05H6

G.Vamshidhar 20A91A0580

K.D.P.N.Jyothi 20A91A05F5

Ch.Sai Poojitha 20A91A05E2

**MONITORING WITH NAGIOS**

**Nagios:** Nagios is an open source continuous monitoring tool which monitors network, applications and servers. It can find and repair problems detected in the infrastructure, and stop future issues before they affect the end users. It gives the complete status of your IT infrastructure and its performance.

**Why Nagios?**

* It can monitor Database servers such as SQL Server, Oracle, Mysql, Postgresql
* It gives application level information (Apache, Postfix, etc.).
* Provides active development.
* Has excellent support form huge active community.
* Nagios runs on any operating system.

**Benefits of Nagios**

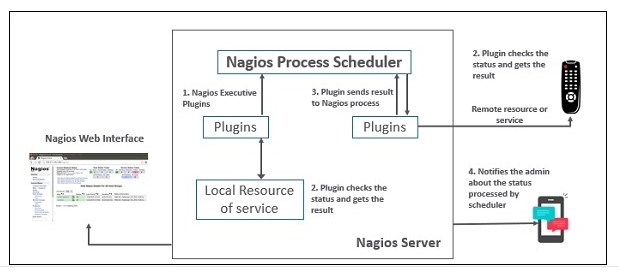
Nagios offers the following benefits for the users −

* It helps in getting rid of periodic testing.
* It reduces maintenance cost without sacrificing performance.
* It provides timely notification to the management of control and breakdown.

## Nagios Architecture

The following points are worth notable about Nagios architecture −

* Nagios has server-agent architecture.
* Nagios server is installed on the host and plugins are installed on the remote hosts/servers which are to be monitored.
* Nagios sends a signal through a process scheduler to run the plugins on the local/remote hosts/servers.
* Plugins collect the data (CPU usage, memory usage etc.) and sends it back to the scheduler.
* Then the process schedules send the notifications to the admin/s and updates Nagios GUI.



## Nagios Core (one of the nagios product which is absolutely free)

It is the core on monitoring IT infrastructure. Nagios XI product is also fundamentally based on Nagios core. Whenever there is any issue of failure in the infrastructure, it sends an alert/notification to the admin who can take the action quickly to resolve the issue. This tool is absolutely free.

*Nagios XI , Nagios Log Server , Nagios Fusion , Nagios Network Analyser are also nagios products that are paid.*

## Nagios Plugins

Plugins helps to monitor databases, operating systems, applications, network equipment, protocols with Nagios. Plugins are compiled executables or script (Perl or non-Perl) that extends Nagios functionality to monitor servers and hosts. Nagios will execute a Plugin to check the status of a service or host. Nagios can be compiled with support for an embedded Perl interpreter to execute Perl plugins. Without it, Nagios executes Perl and non-Perl plugins by forking and executing the plugins as an external command.

## Types of Nagios Plugins

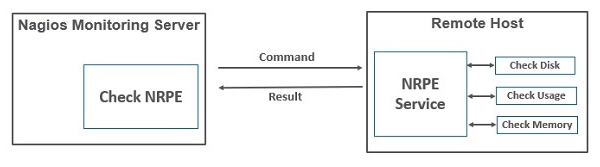
Nagios has the following plugins available in it −

**Official Nagios Plugins −** There are 50 official Nagios Plugins. Official Nagios plugins are developed and maintained by the official Nagios Plugins Team.

**Community Plugins** − There are over 3,000 third party Nagios plugins that have been developed by hundreds of Nagios community members.

**Custom Plugins** − You can also write your own Custom Plugins. There are certain guidelines that must be followed to write Custom Plugins.

**Nagios-NRPE**

The Nagios daemon which run checks on remote machines in NRPE (Nagios Remote Plugin Executor). It allows you to run Nagios plugins on other machines remotely. You can monitor remote machine metrics such as disk usage, CPU load etc. It can also check metrics of remote windows machines through some windows agent addons. 

**Hosts and services:**

Nagios is the most popular tool which is used to monitor hosts and services running in our IT infrastructure. Hosts and service configurations are the building blocks of Nagios Core.

* Host is just like a computer; it can be a physical device or virtual.
* Services are those which are used by Nagios to check something about a host.

## Features:

* Nagios Core is open source, hence free to use.
* Powerful monitoring engine which can scale and manage 1000s of hosts and servers.
* Fast alerting system, sends alerts to admins immediately after any issue is identified.
* Multiple plugins available to support Nagios, custom coded plugins can also be used with Nagios.
* It has good log and database system storing everything happening on the network with ease.

**Applications:**

* Monitor host resources such as disk space, system logs etc.
* Monitor network resources – http, ftp, smtp, ssh etc.
* Monitor windows/linux/unix/web applications and its state.
* Send alerts/notifications.
* via email, sms, pager of any issue on infrastructure.
* Recommending when to upgrade the IT infrastructure.

**Installation of Nagios**

Step By Step method for installing Nagios in Amazon Linux

Step 1: Install Prerequisite Software

Step 2: Create Account Information

Step 3: Download Nagios Core and the Plugins

Step 4: Compile and Install Nagios

Step 5: Customize Configuration

Step 6: Configure the Web Interface

Step 7: Compile and Install the Nagios Plugins

Step 8: Start Nagios

Step 9: Update AWS Security Group

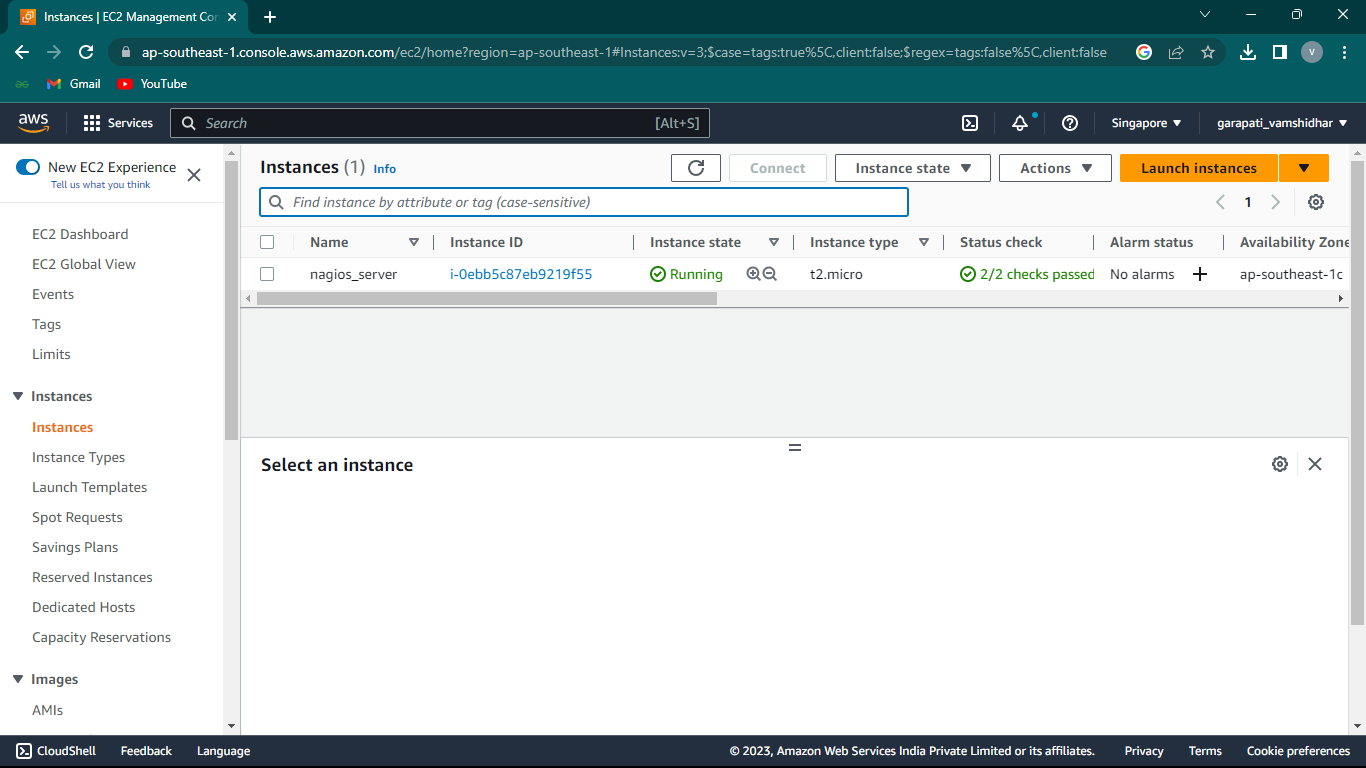
Step 10: Log in to the Web Interfac

\*To Start Nagios Core Installation you must have your EC2 instance up and running and have already configured SSH access to the instance.

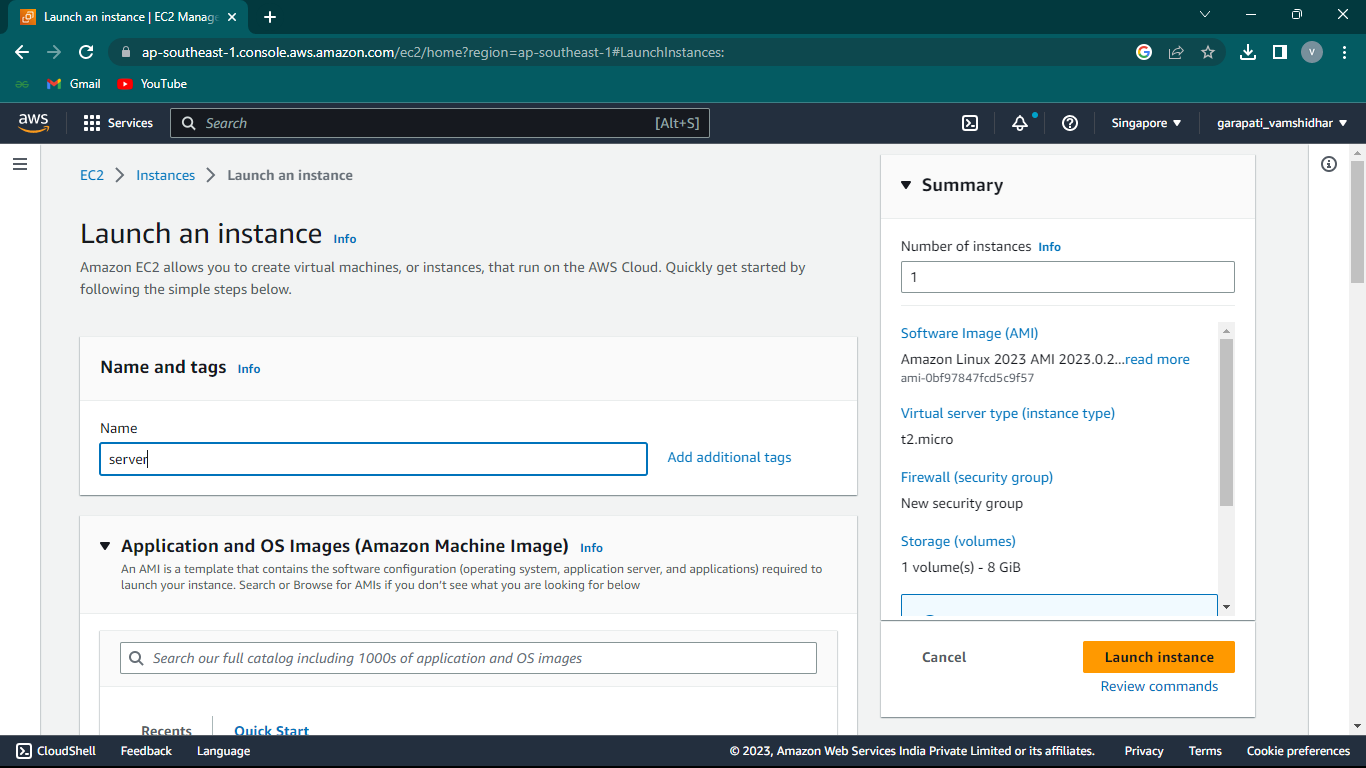
For this we have to launch EC2 instance.

1.First Login to AWS console page

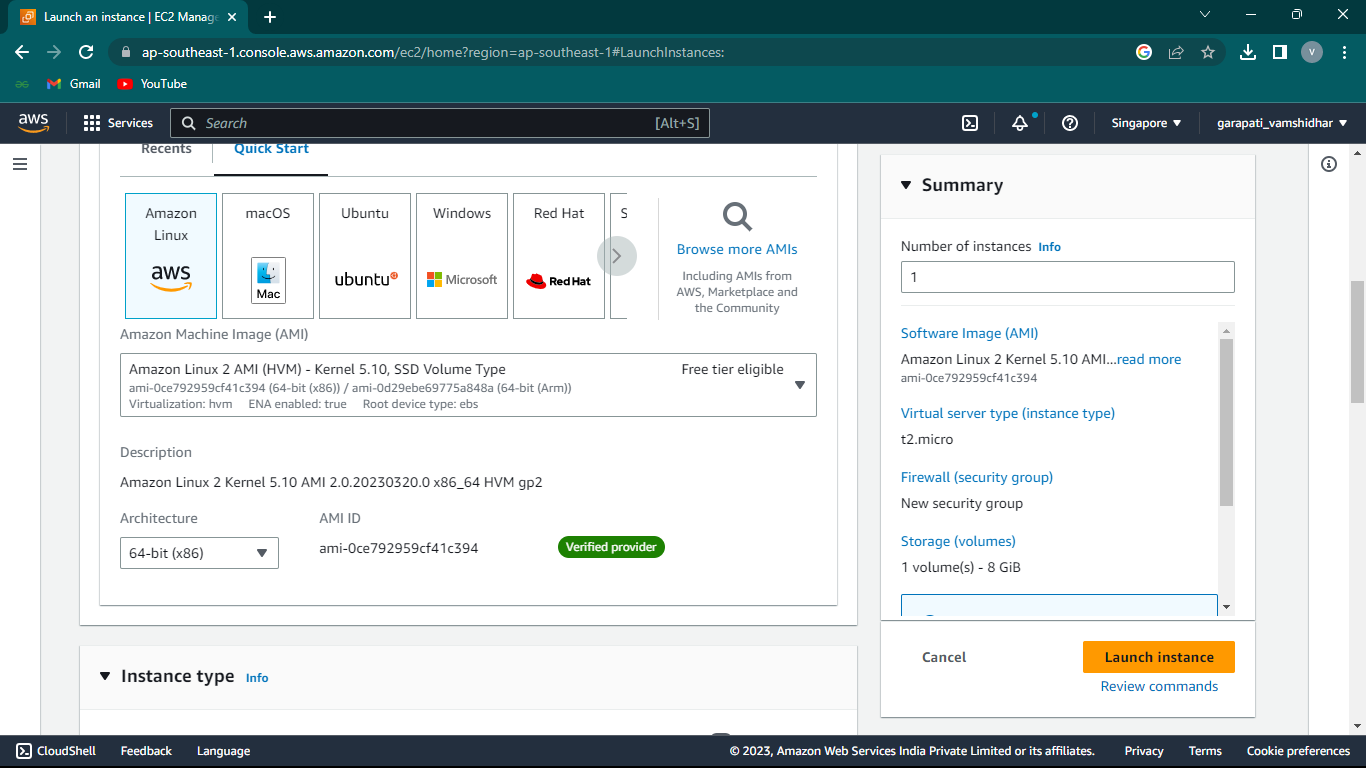


2.Click on Launch instances to launch instance

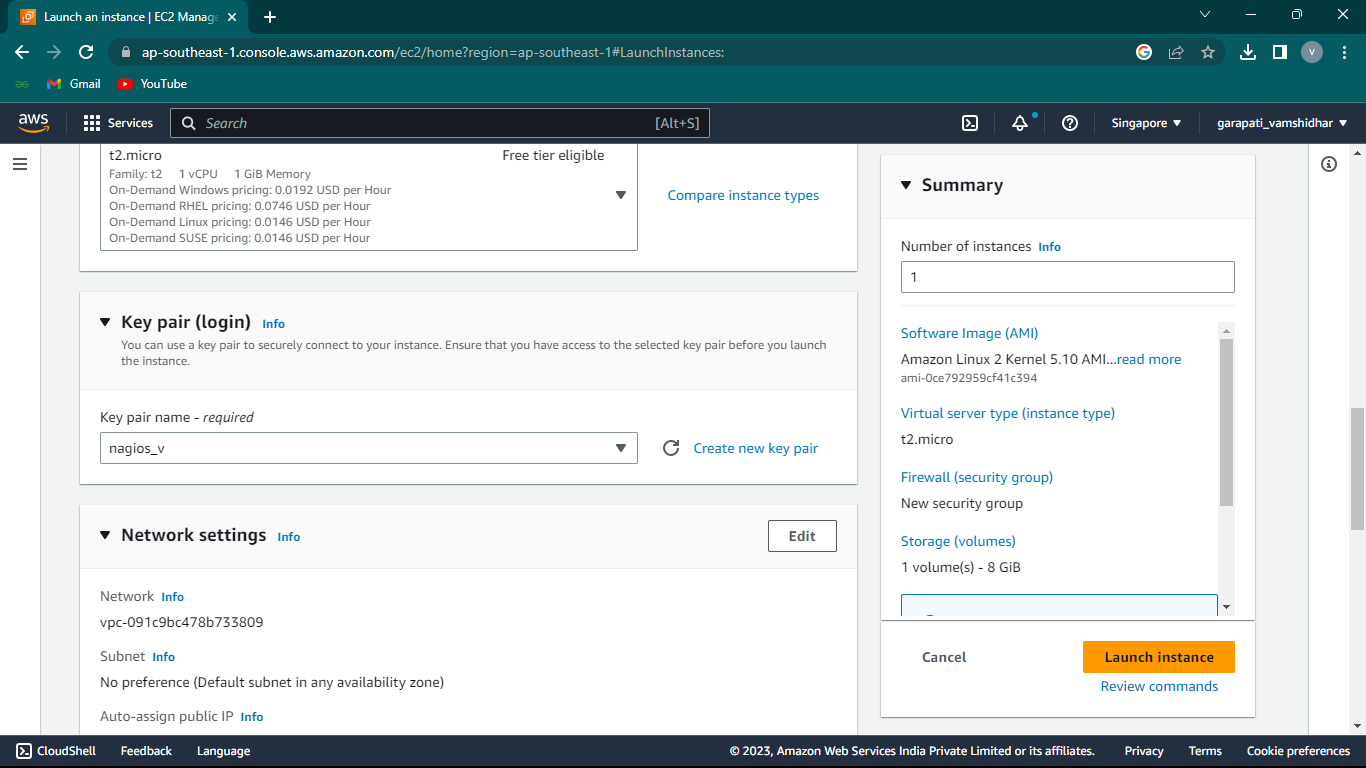
3.Give name to your instance



4.Select Amazon linux as Amazon Machine Image



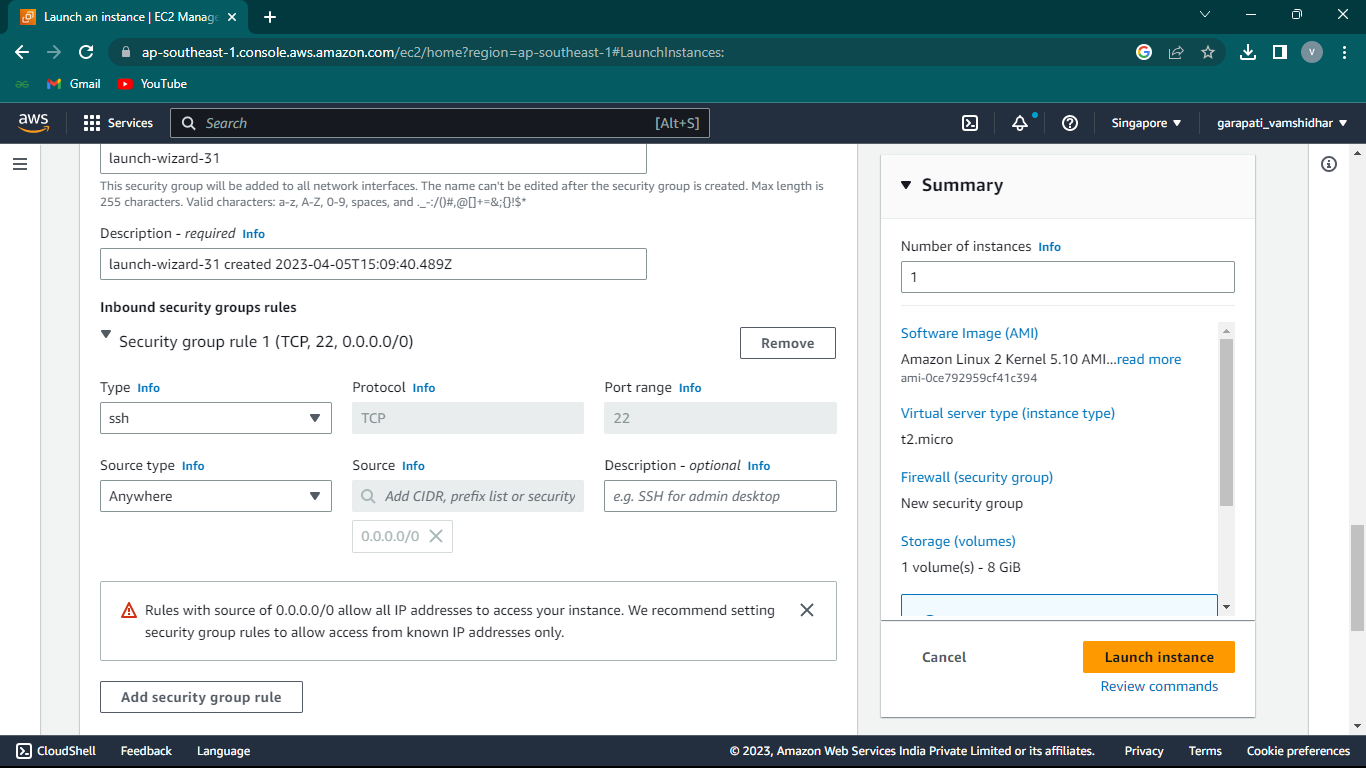
5.Create new key pair in ppk format



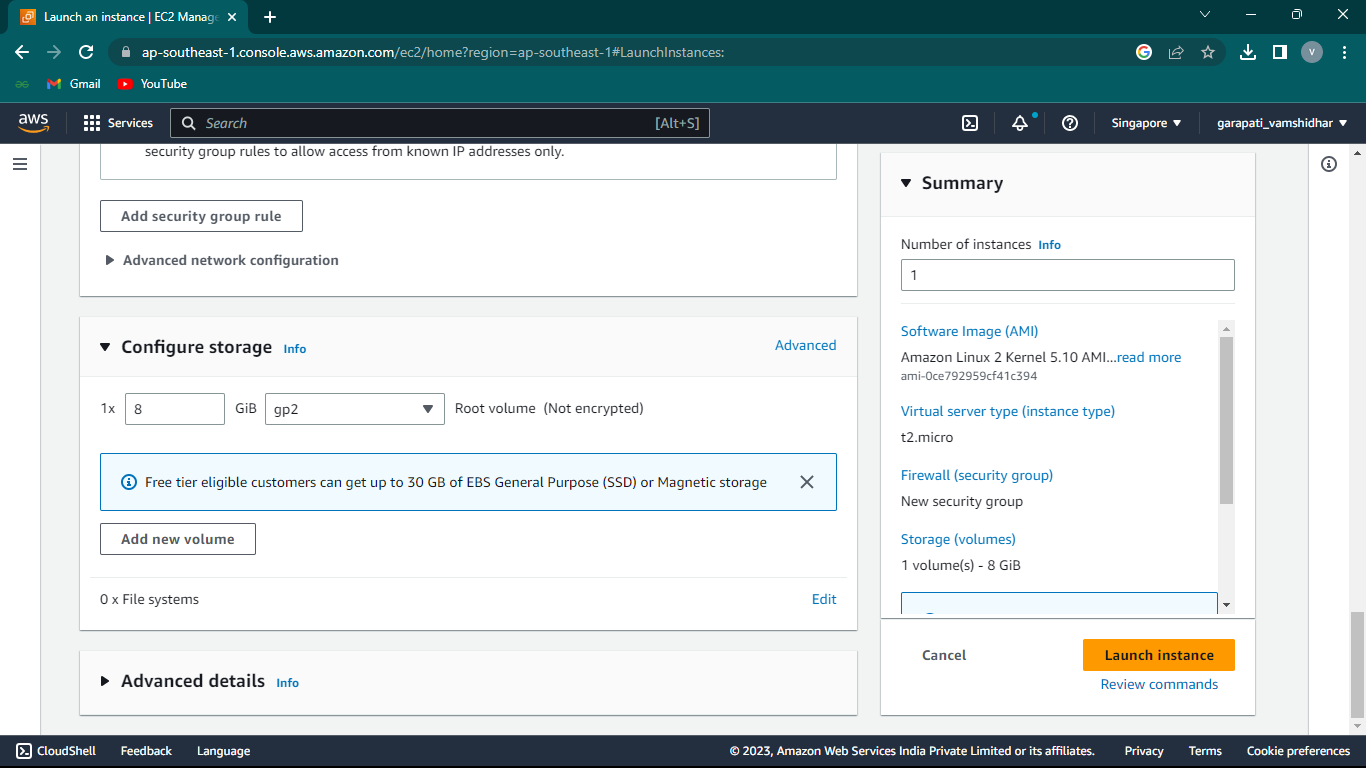
6.In network settings use default VPC and default subnet



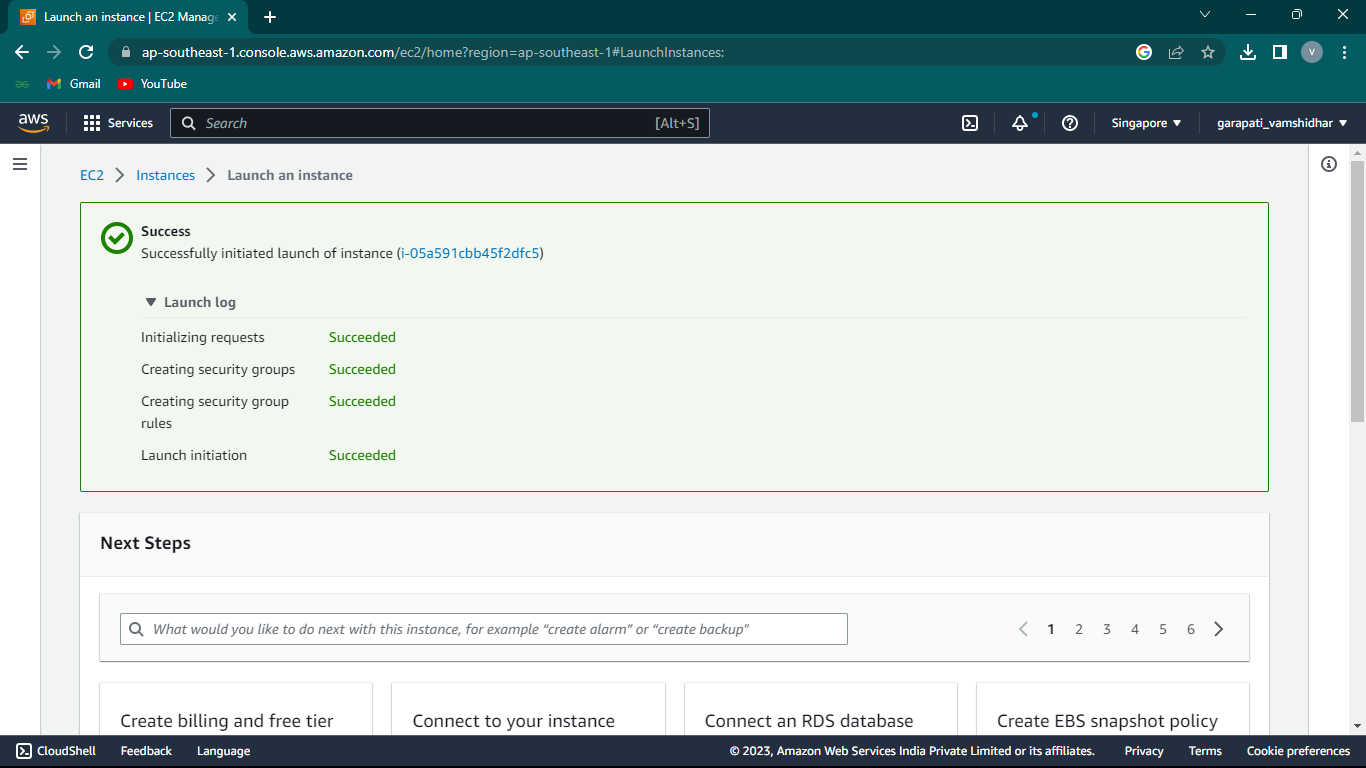
7.Create new security group and edit inbound rules as ssh type with source type as anywhere



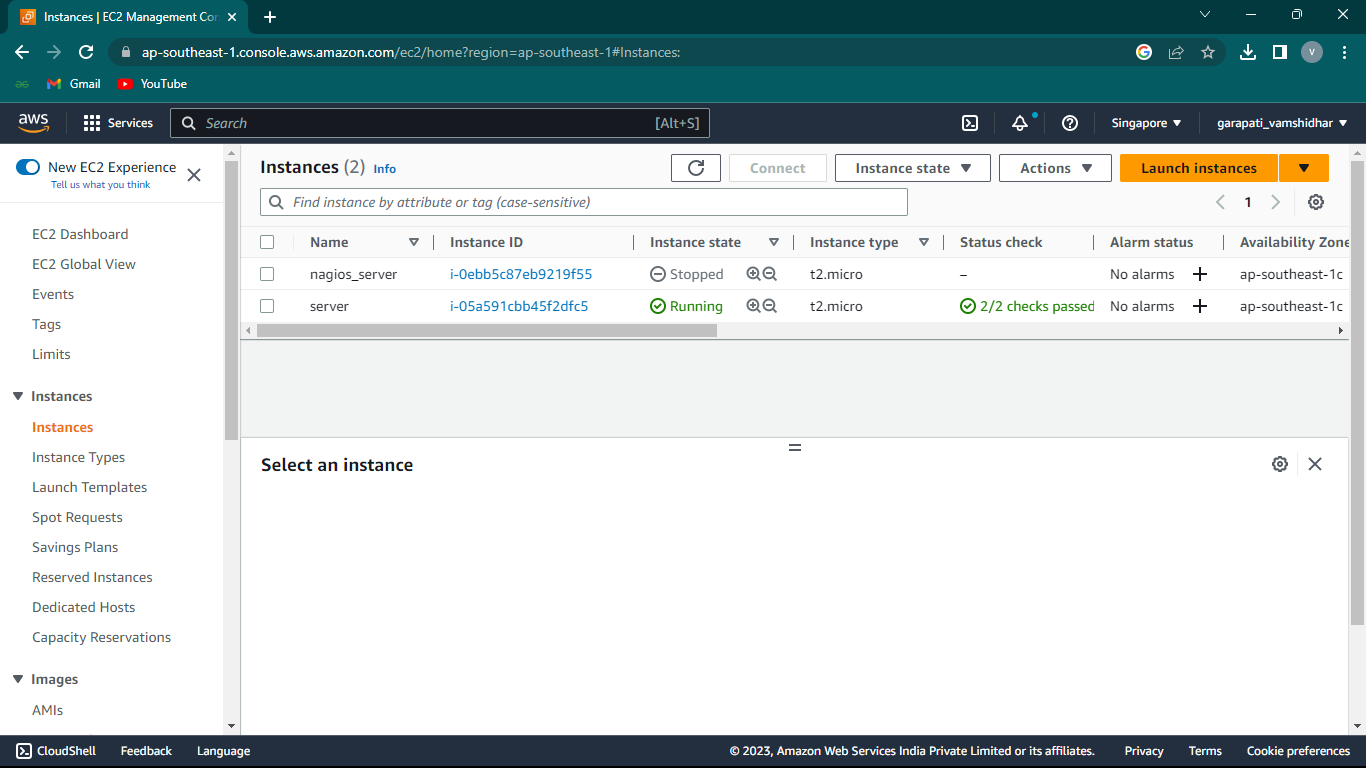
8.Click on launch instance to launch the instance



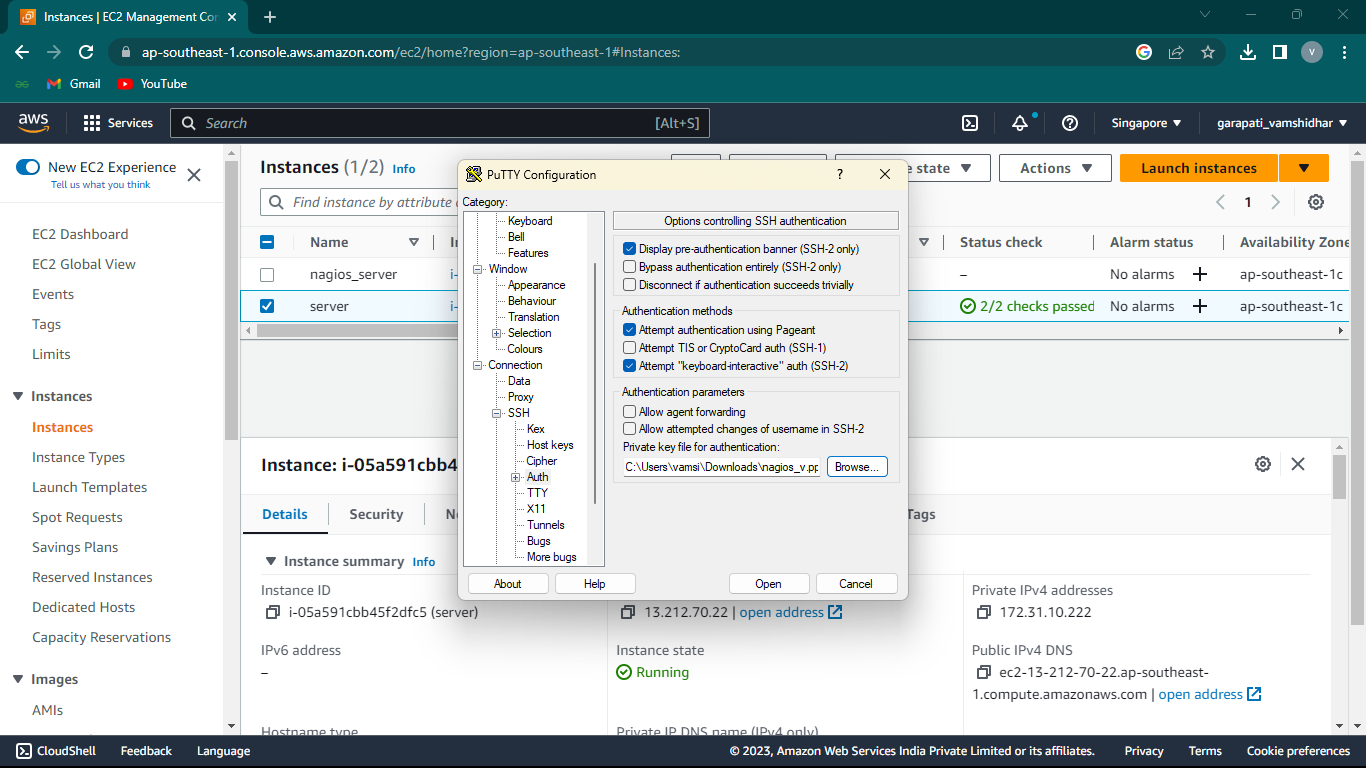
9.Instance is launched successfully



10.The instance is in running state



11.Connect to EC2 instance using putty



**Installation steps(putty):**

**Step 1: Install Prerequisite Software**

Nagios requires the following packages are installed on your server prior to installing Nagios:

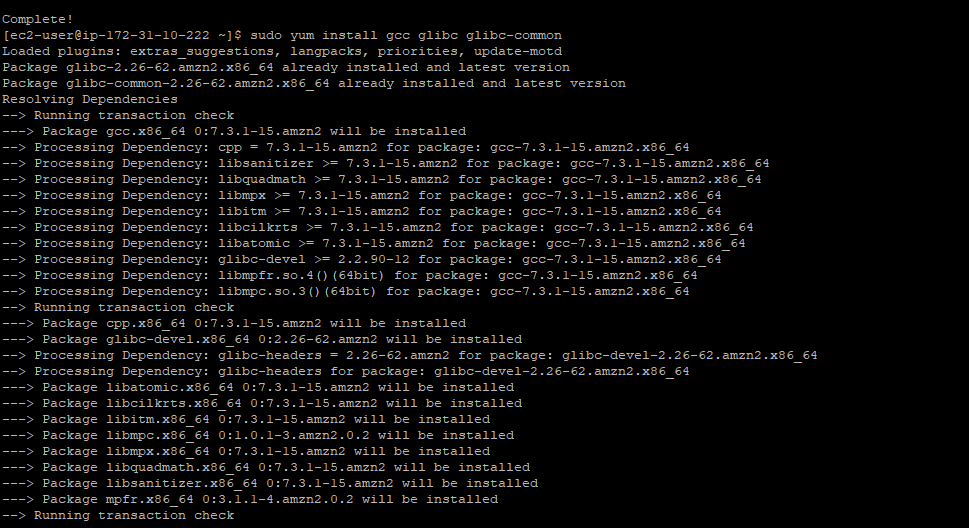
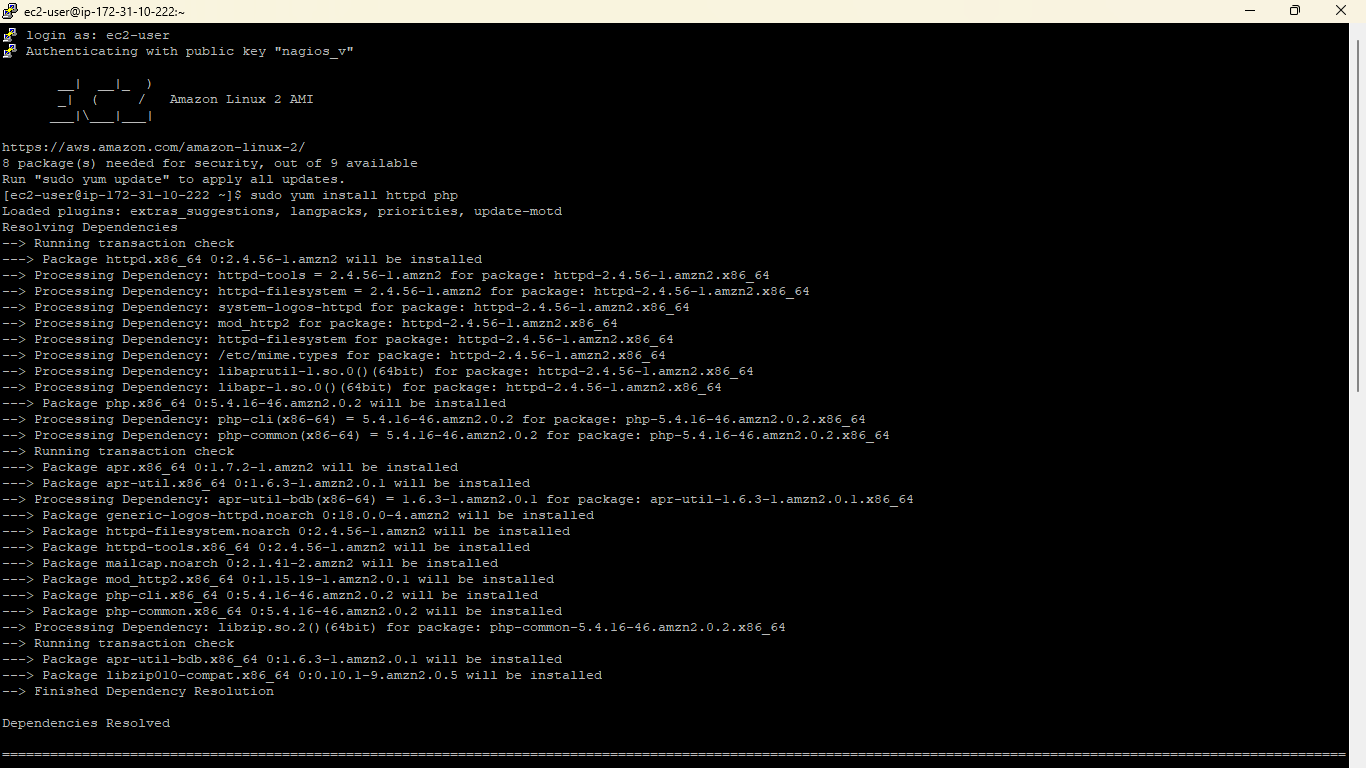
\* Apache  
\* PHP  
\* GCC compiler  
\* GD development libraries

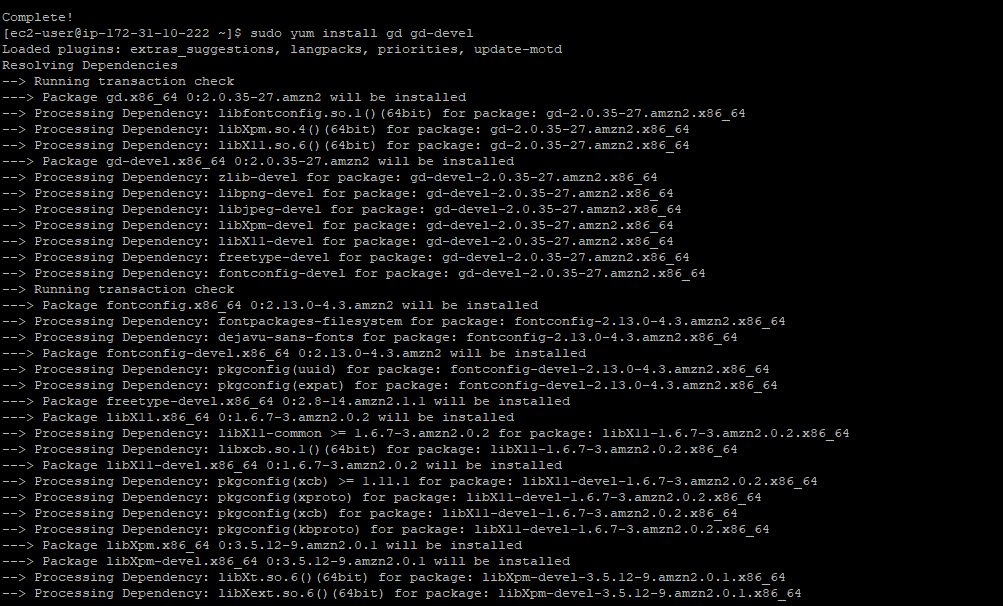
You can use yum to install these packages by running the following commands (as ec2-user):

**$sudo yum install httpd php**

**$sudo yum install gcc glibc glibc-common**

**$sudo yum install gd gd-devel**





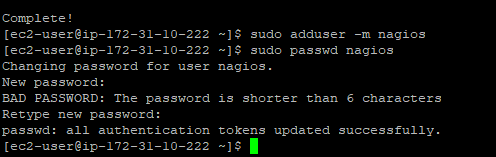
**Step 2: Create Account Information**

You need to set up a Nagios user. Run the following commands:

**$sudo adduser -m nagios**

**$sudo passwd nagios**

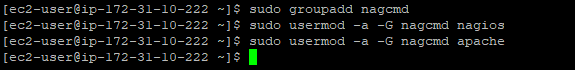
Type the new password twice.



**$sudo groupadd nagcmd**

**$sudo usermod -a -G nagcmd nagios**

**$sudo usermod -a -G nagcmd apache**



**Step 3: Download Nagios Core and the Plugins**

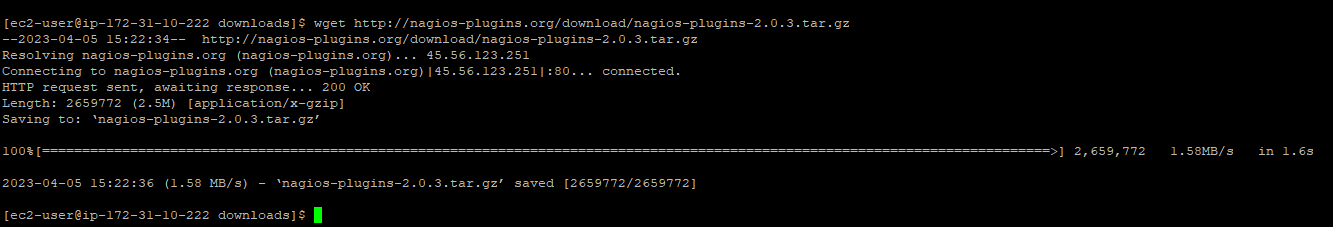
Create a directory for storing the downloads.

**$mkdir ~/downloads**

**$cd ~/downloads**

**$wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz**

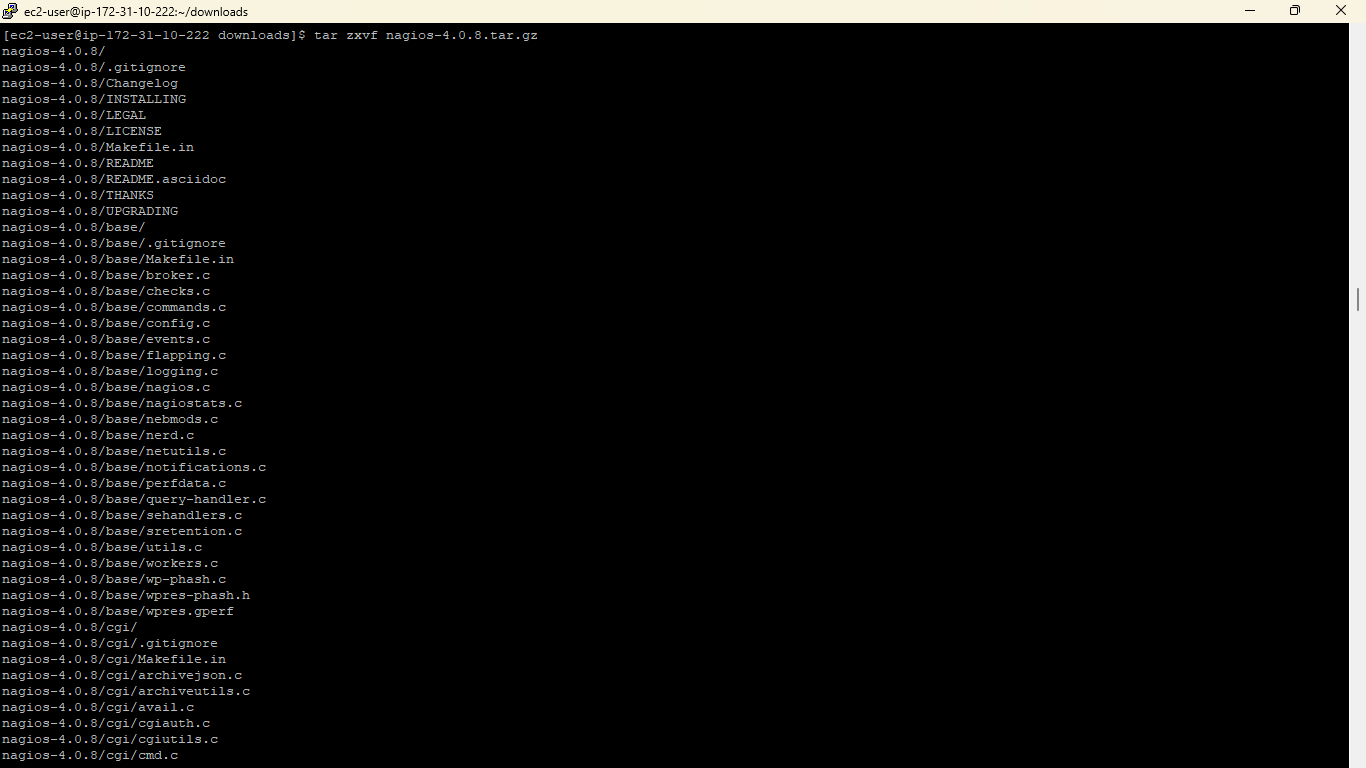
**$wget http://nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz**



**Step 4: Compile and Install Nagios**

Extract the Nagios source code tarball.

**$tar zxvf nagios-4.0.8.tar.gz**

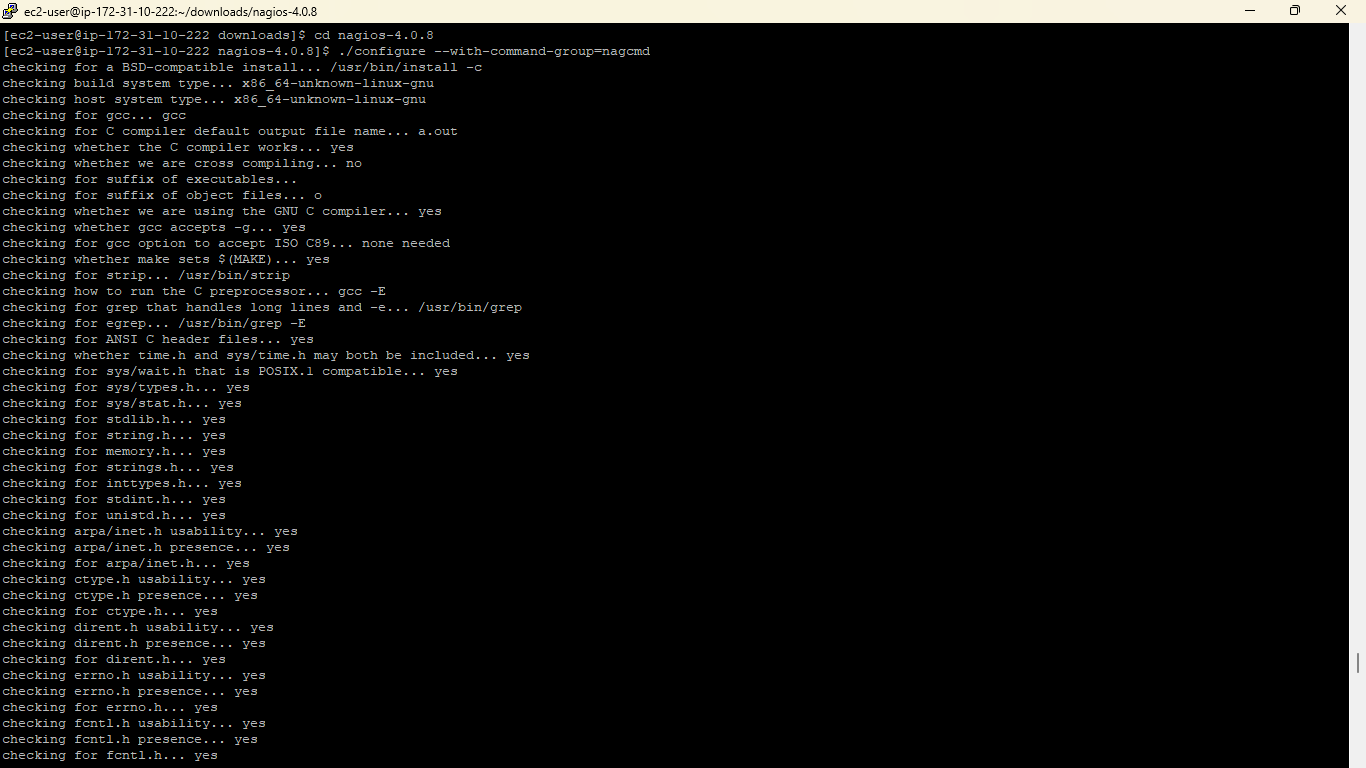


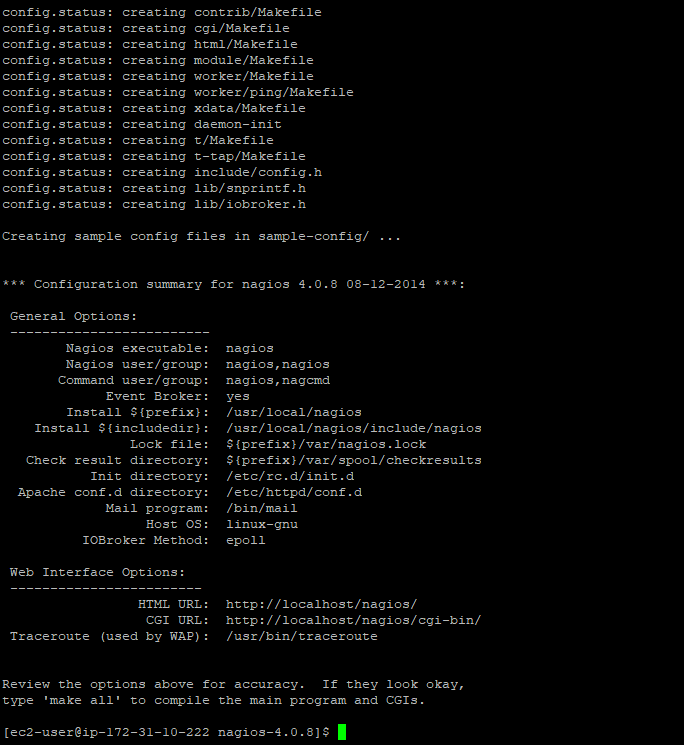
Change the directory to nagios-4.0.8 by using cd command

**$cd nagios-4.0.8**

Run the configuration script with the name of the group which you have created in the above step.

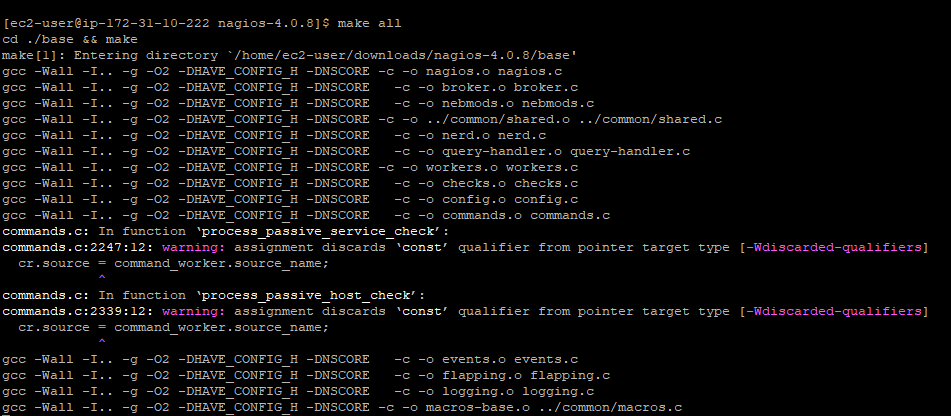
**$./configure --with-command-group=nagcmd**





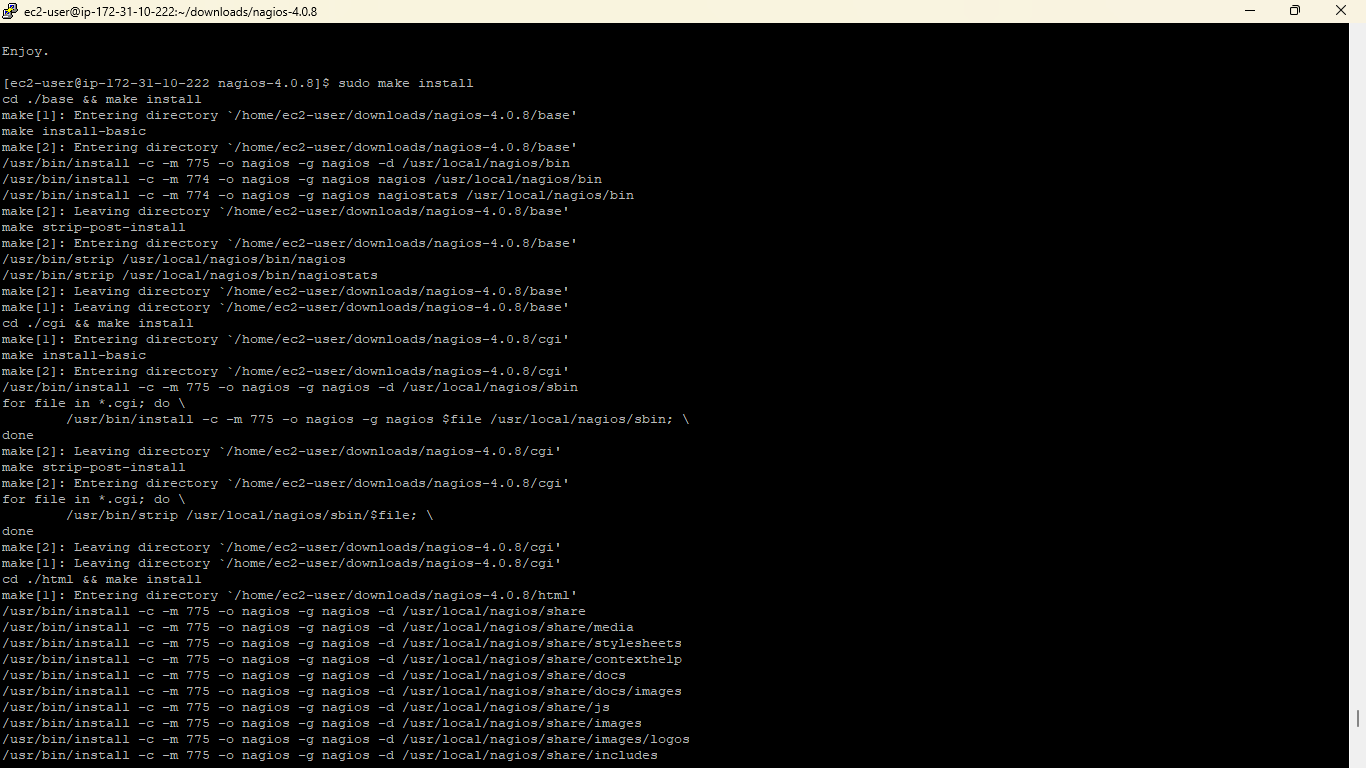
Compile the Nagios source code.

**$make all**

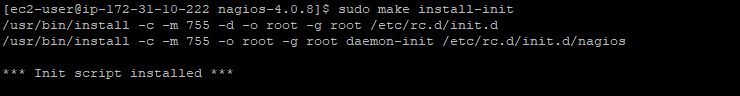


Install binaries, init script, sample config files and set permissions on the external command directory.

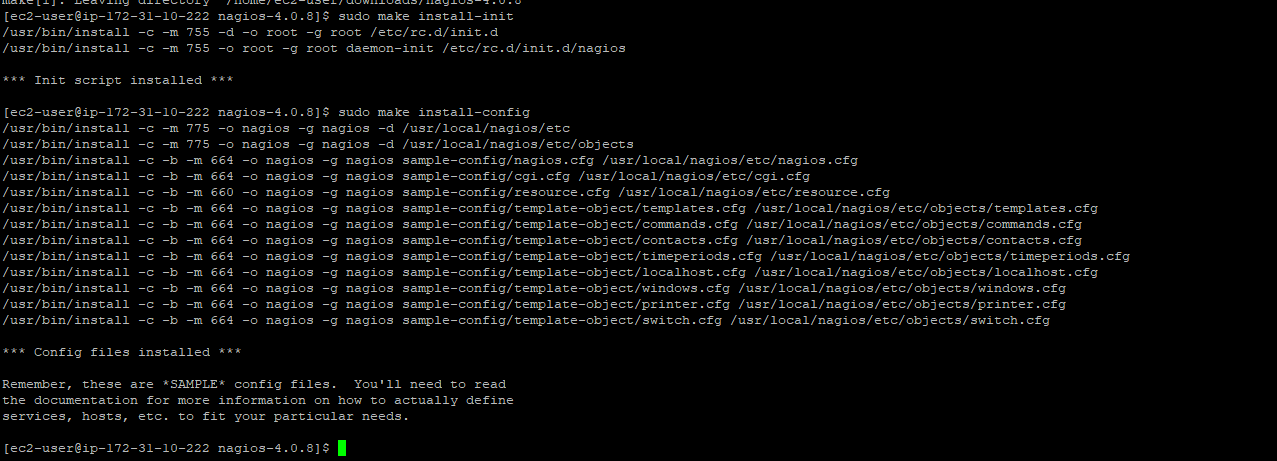
**$sudo make install**



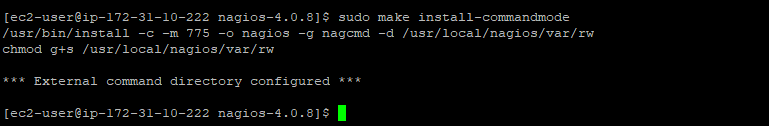
**$sudo make install-init**



**$sudo make install-config**



**$sudo make install-commandmode**

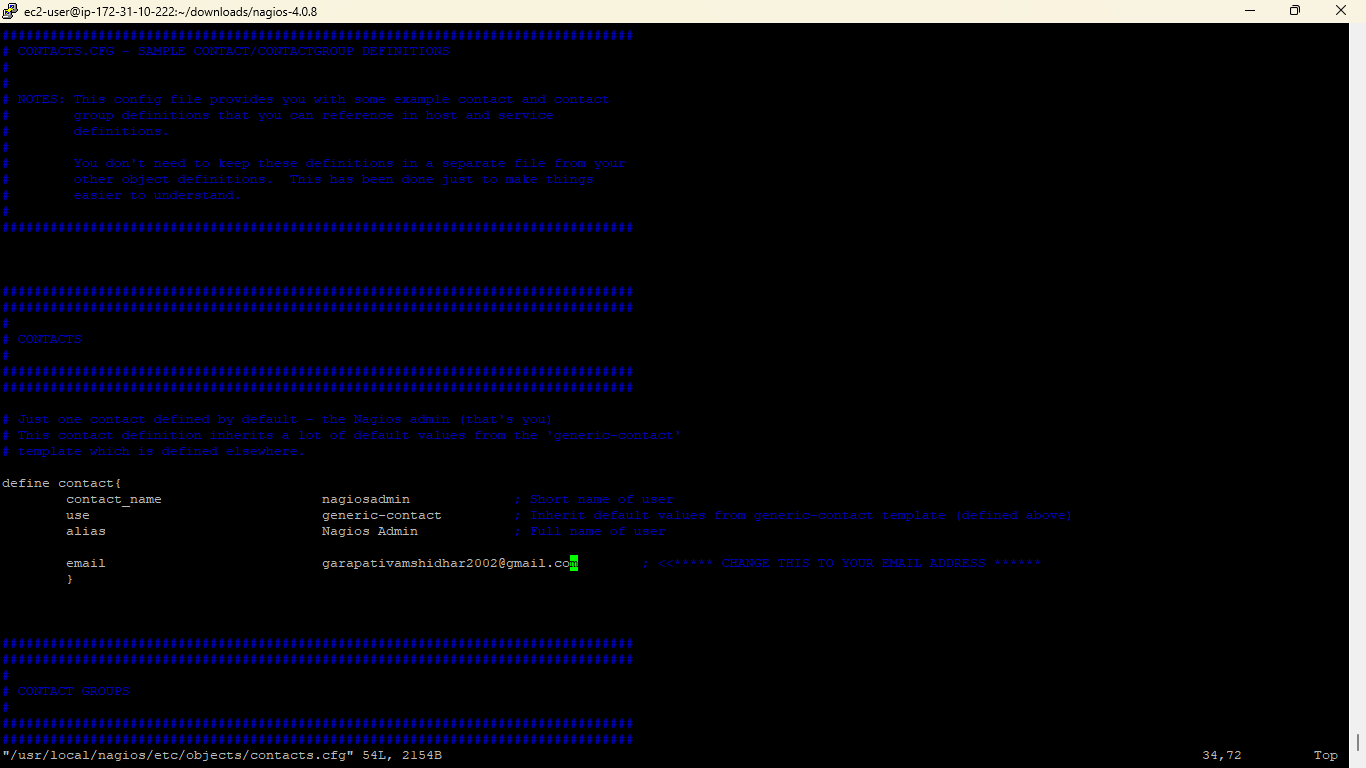


**Step 5: Customize Configuration**

**$sudo vim /usr/local/nagios/etc/objects/contacts.cfg**

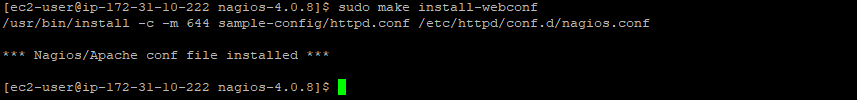


Change E-Mail address with nagiosadmin contact definition you’d like to use for receiving Nagios alerts.



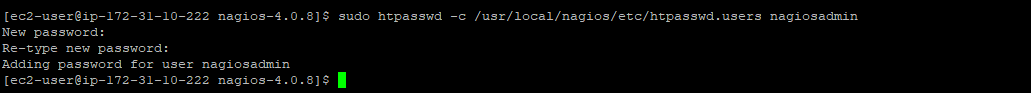
**Step 6: Configure the Web Interface**

**$sudo make install-webconf**



Create a nagiosadmin account for logging into the Nagios web interface. Note the password you need it while login to Nagios web console.

**$sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin**

****

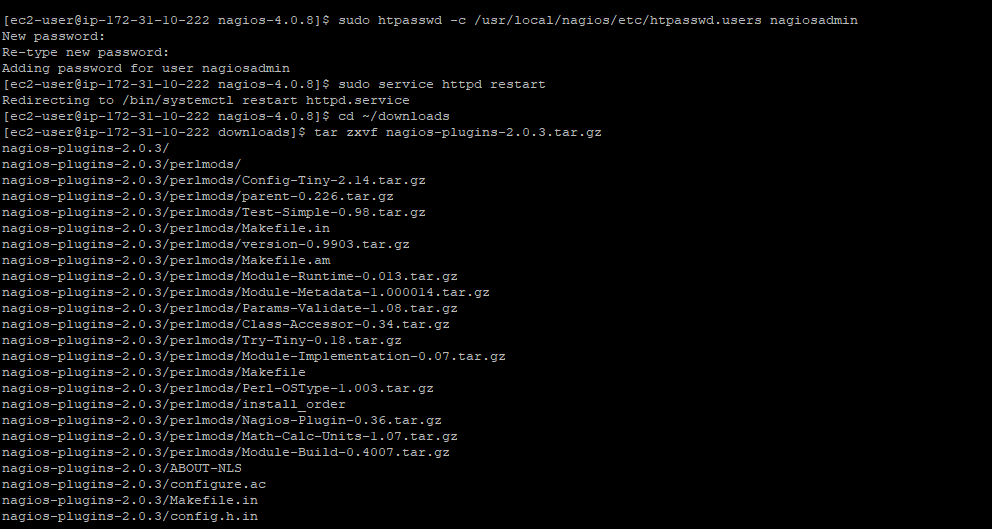
**$sudo service httpd restart**

**Step 7: Compile and Install the Nagios Plugins**

Extract the Nagios plugins source code tarball.

**$cd ~/downloads**

**$tar zxvf nagios-plugins-2.0.3.tar.gz**

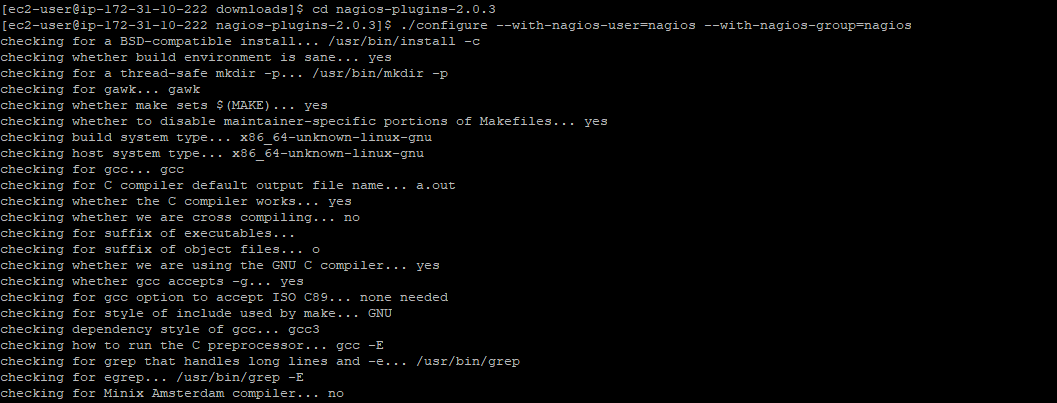


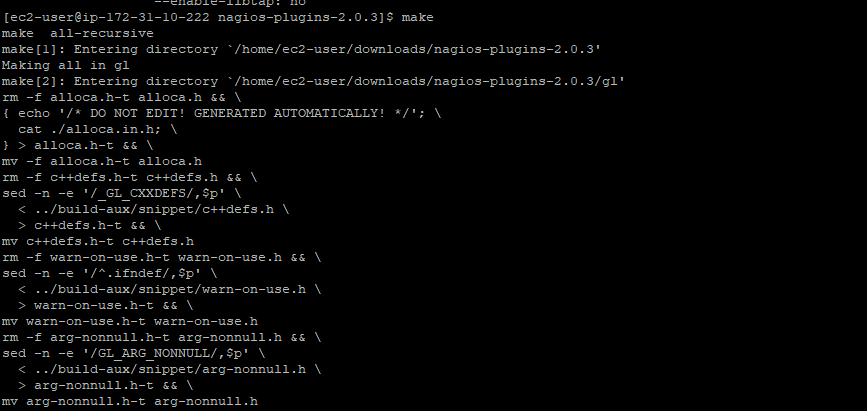
**$cd nagios-plugins-2.0.3**

Compile and install the plugins.

**$./configure --with-nagios-user=nagios --with-nagios-group=nagios**

**$ make**





**$sudo make install**

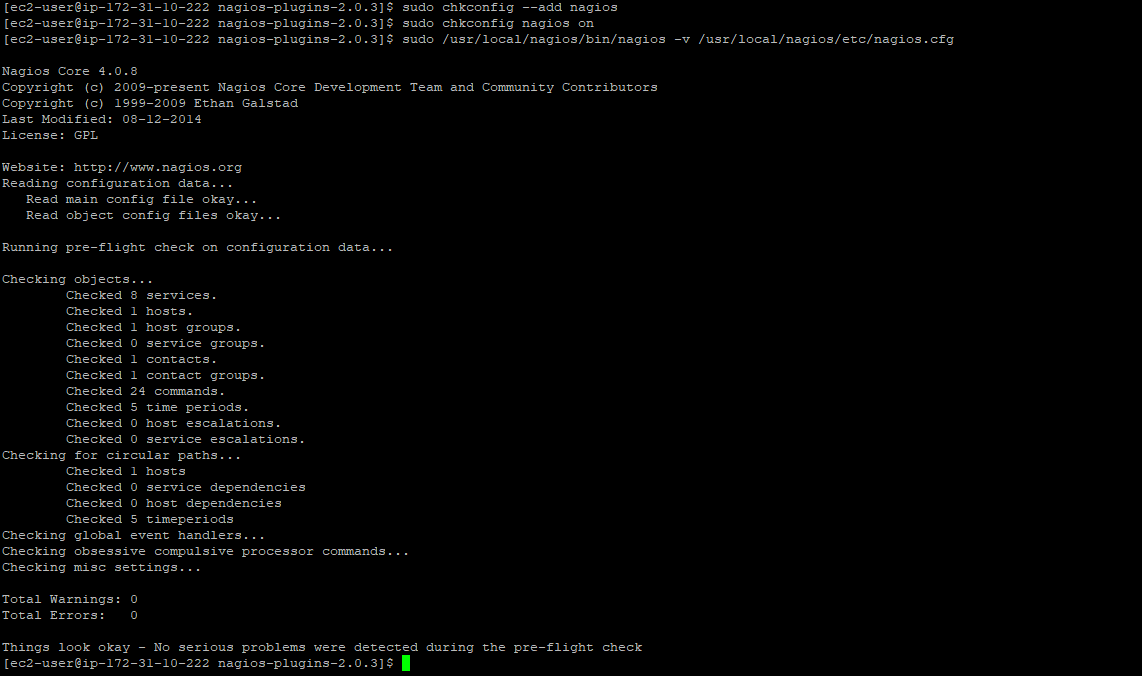


**Step 8: Start Nagios**

Add Nagios to the list of system services and have it automatically start when the system boots.

**$sudo chkconfig --add nagios**

**$sudo chkconfig nagios on**



If there are no errors, start Nagios.

**$sudo service nagios start**

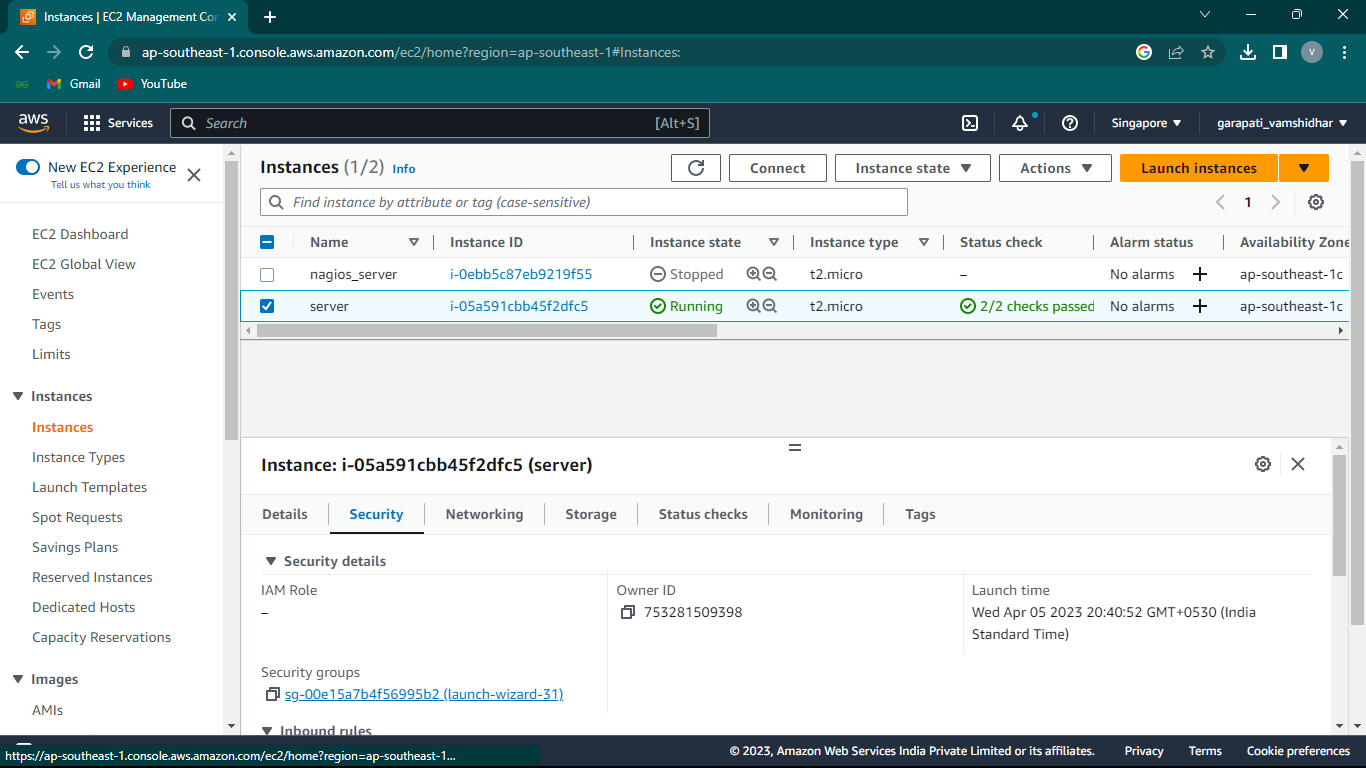


**Step 9: Update AWS Security Group**

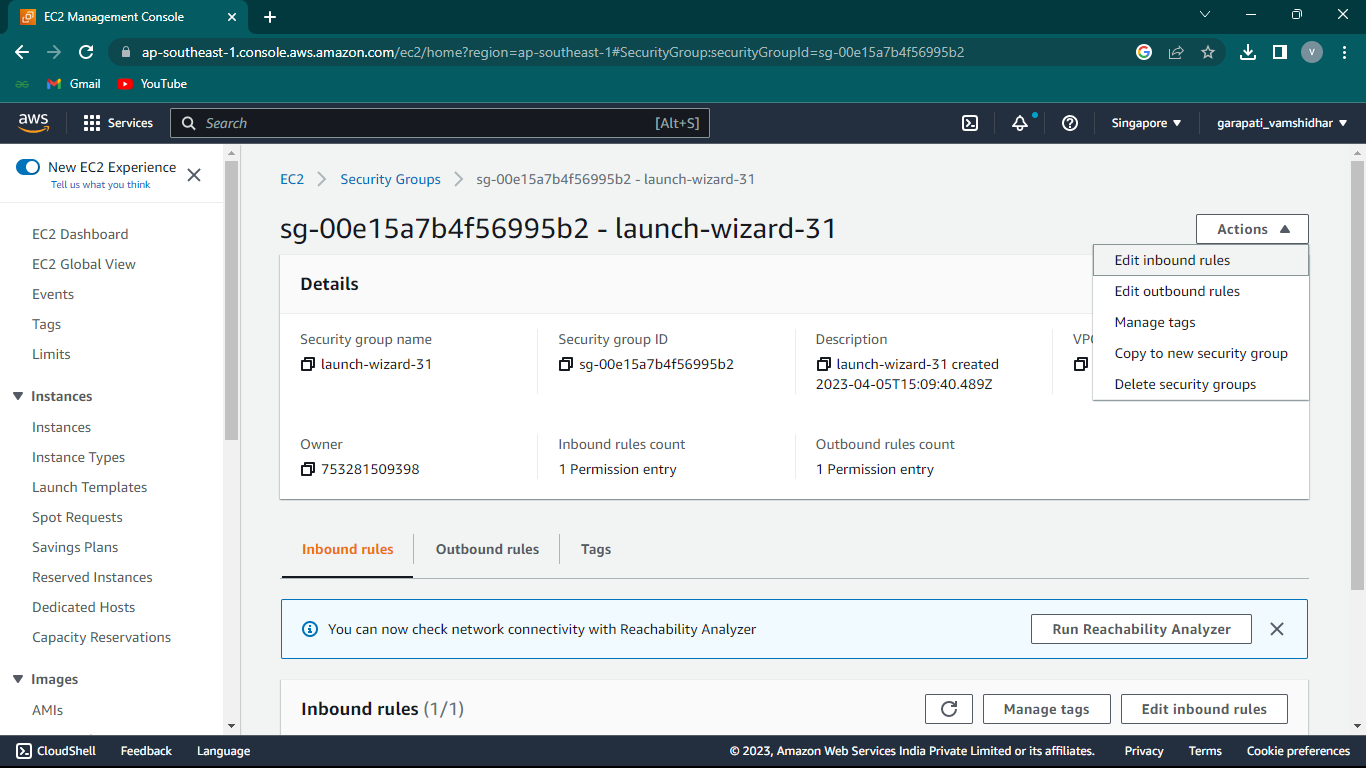
you need to open port 80 on the new AWS EC2 server to incoming traffic so you can connect to the new Nagios webpage.

\* From the EC2 console select Security Groups from the left navigation pane.  
\* Select the Security Group applicable for the instance that Nagios was installed on and open the Inbound tab  
\* If there is no rule to allow HTTP traffic on port 80 then click edit in the Inbound tab to add a new rule  
\* Click on New Rule button  
\* Scroll down to select HTTP from the list of Type  
\* If you want to be able to access Nagios from anywhere then select Save, otherwise enter the IP address or range of IP address you want to be able to access it from then select Save.

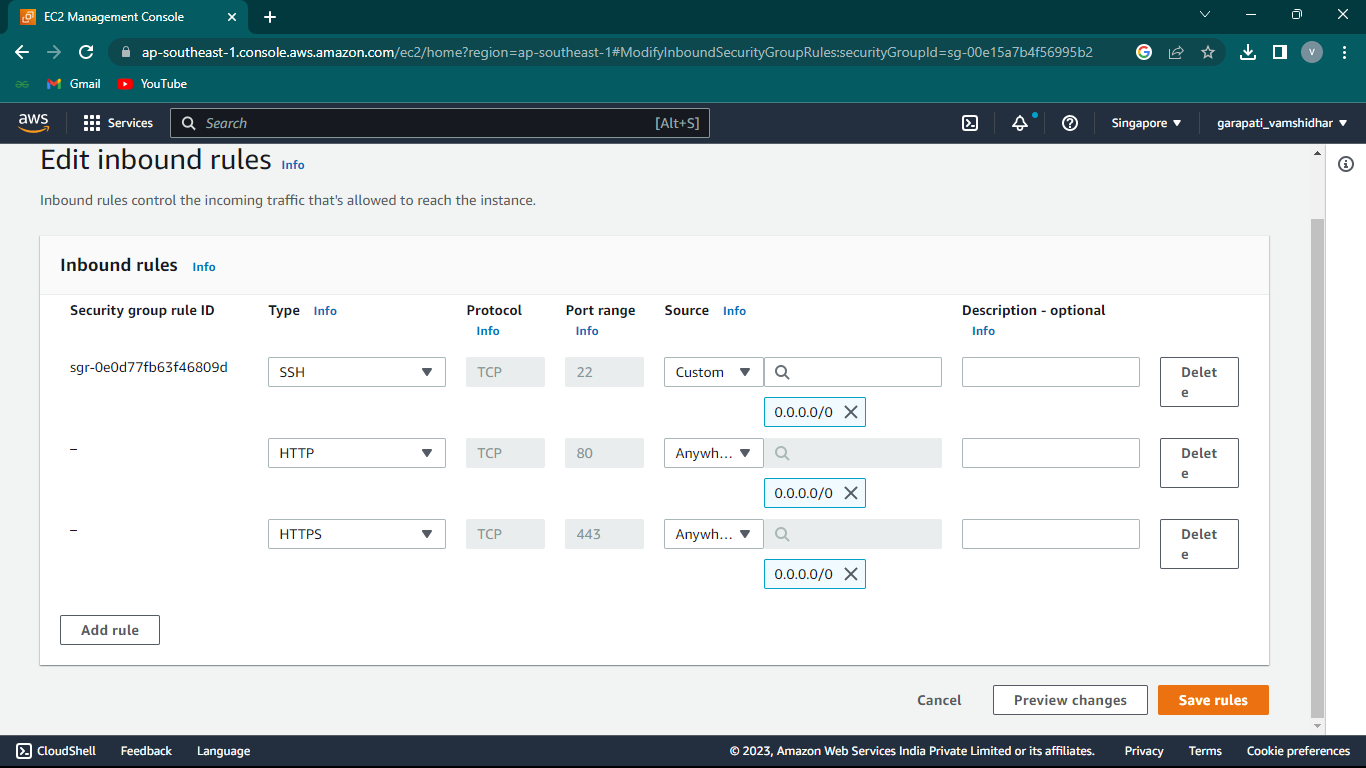
* Now go to EC2 instance



* Go to security



* Now edit the inbound rules



**Step 10: Log in to the Web Interface**

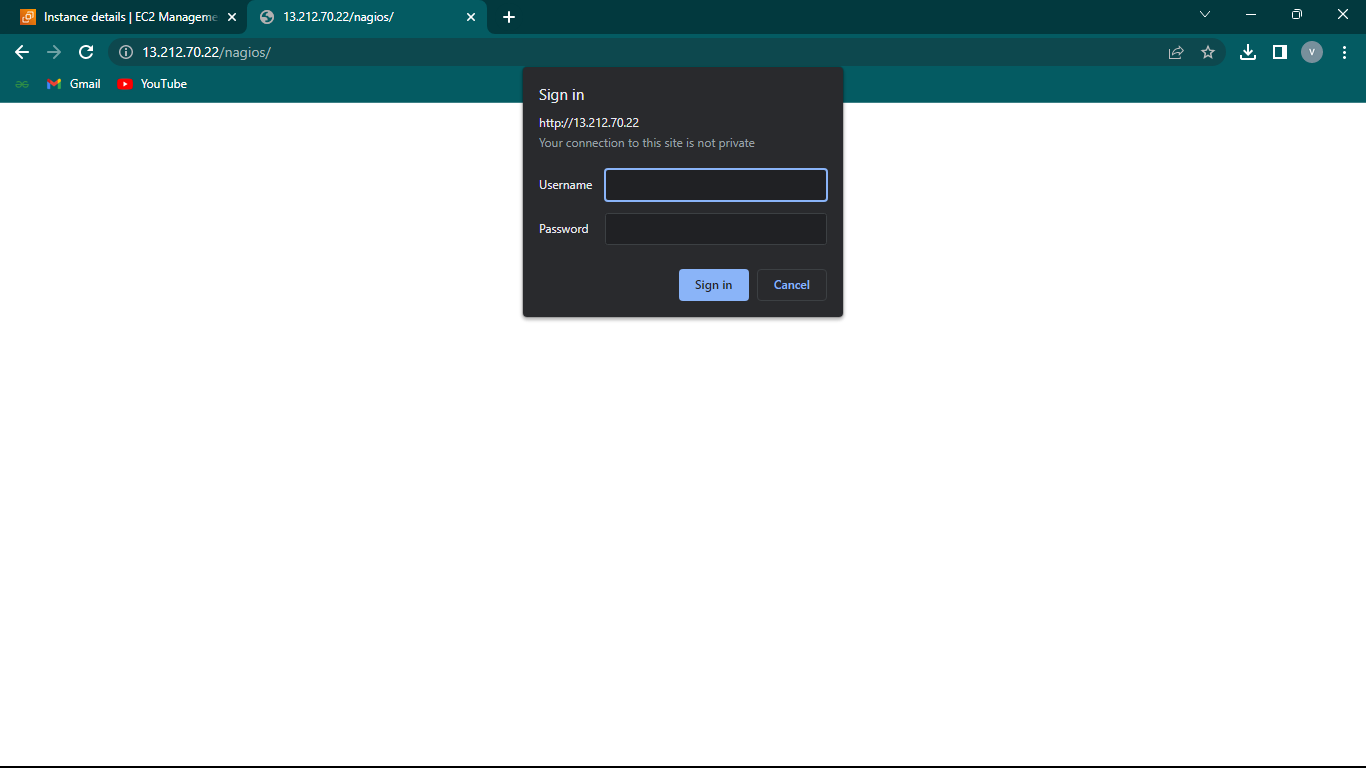
access the Nagios web interface to do this you will need to know the Public DNS or IP for your instance, you can get this from the Instance section of the EC2 Console if you do not already know it. You’ll be prompted for the username (nagiosadmin) and password you specified earlier.

Eg:Ipaddress/nagios

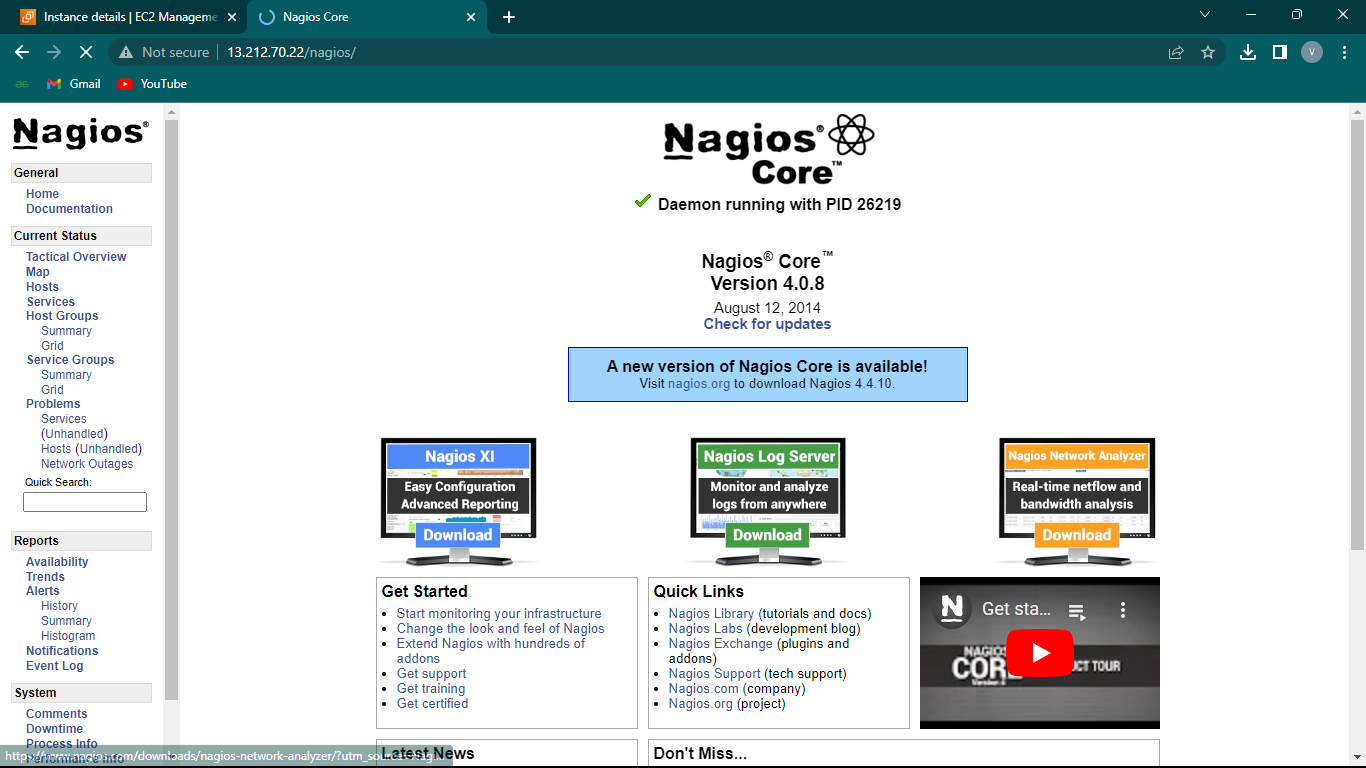
Sign in to the Nagios by using username and password.

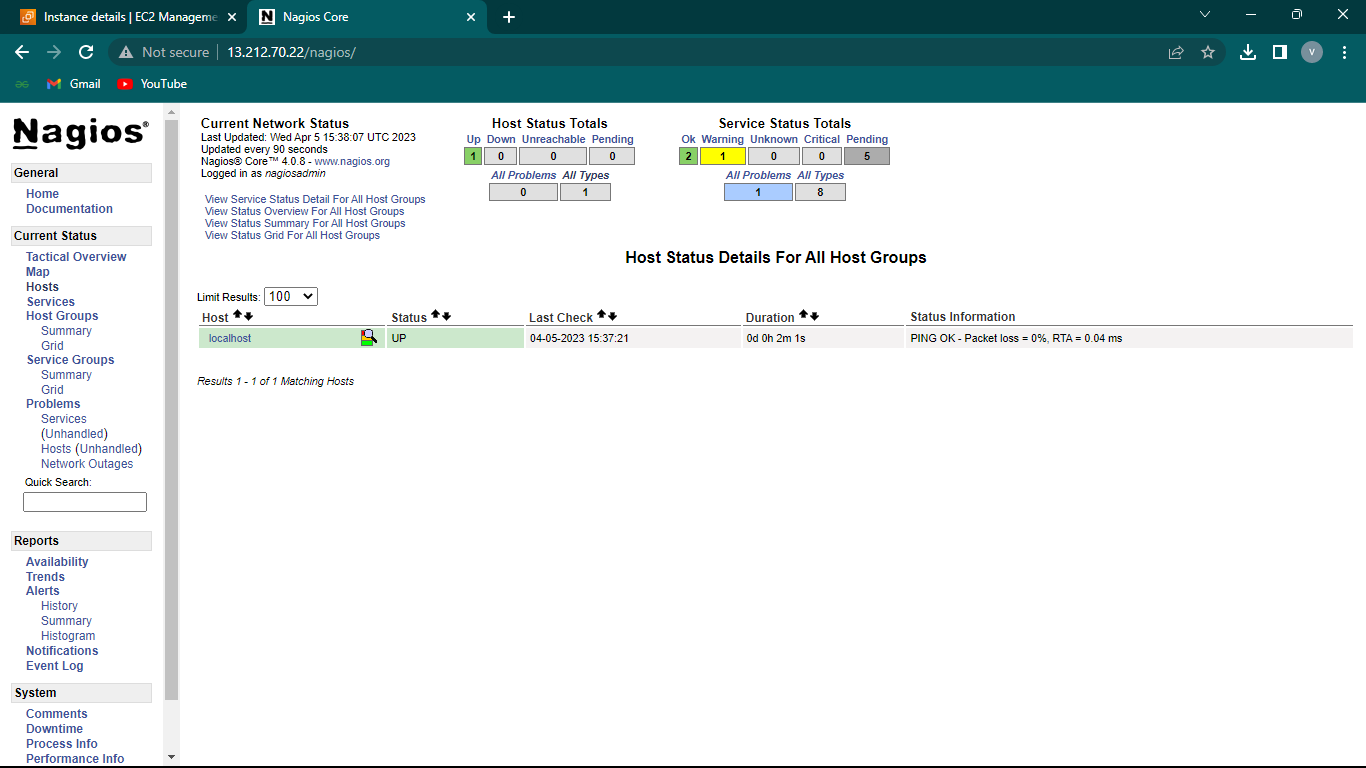
**Username: nagiosadmin**

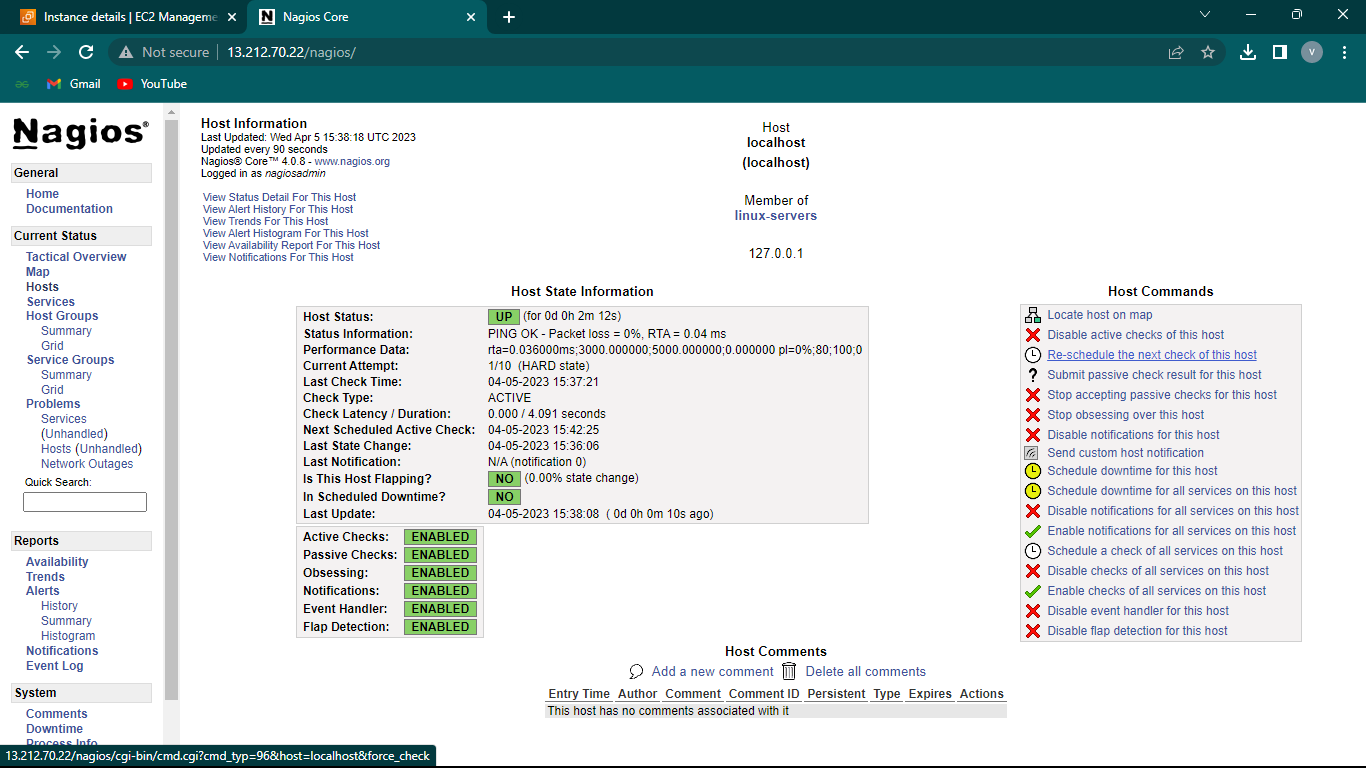
**Password: sai@1**



* This is the Interface of the Nagios Core





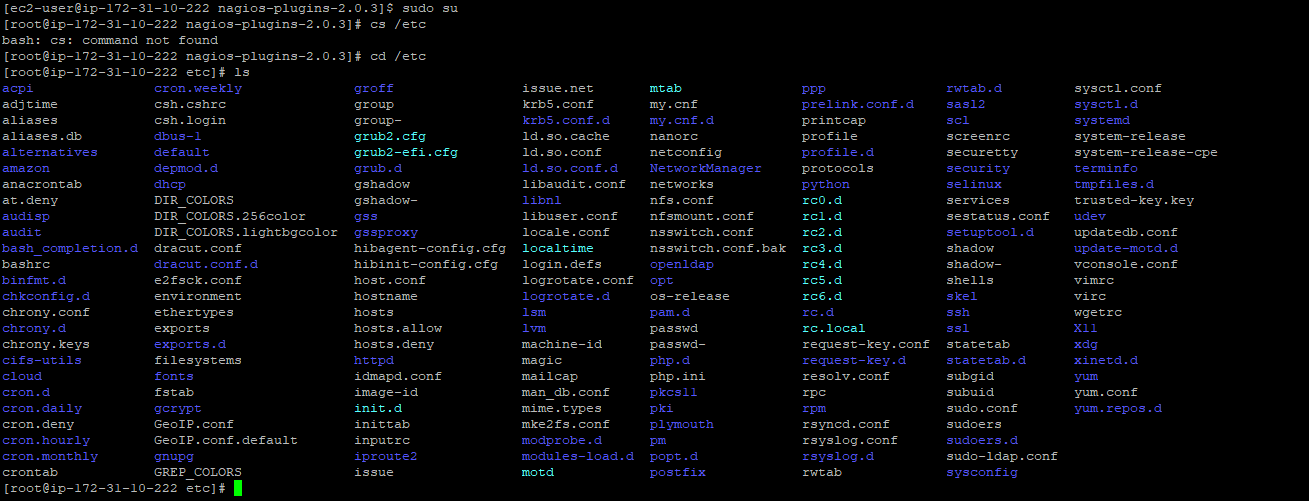


**Monitoring with different ip’s**

1.In the first step connect to the root user and switch to the /etc directory and also check the list of files available in that directory.

**$sudo su**

**$cd /etc**



2. Now switch to ssh directory and change the authentication and password rules for the access of root user.

**$cd ssh**

**$ls**

**$nano sshd\_config**

Change the rules:

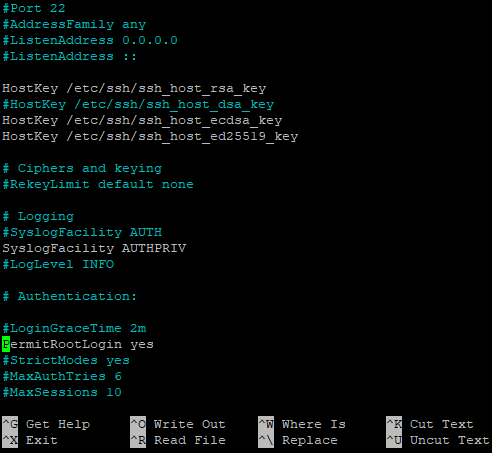
**#PermitRootLogin Yes ---> PermitRootLogin Yes**

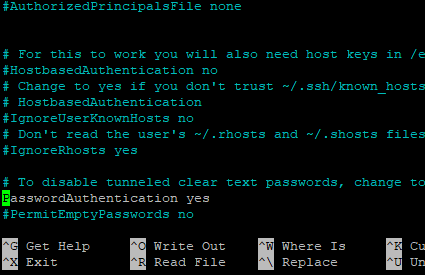
**#PasswordAuthentication Yes---> PasswordAuthentication Yes**

Now save the changes.





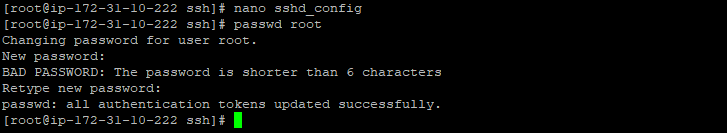




3.Generate the password for the login and restart sshd.

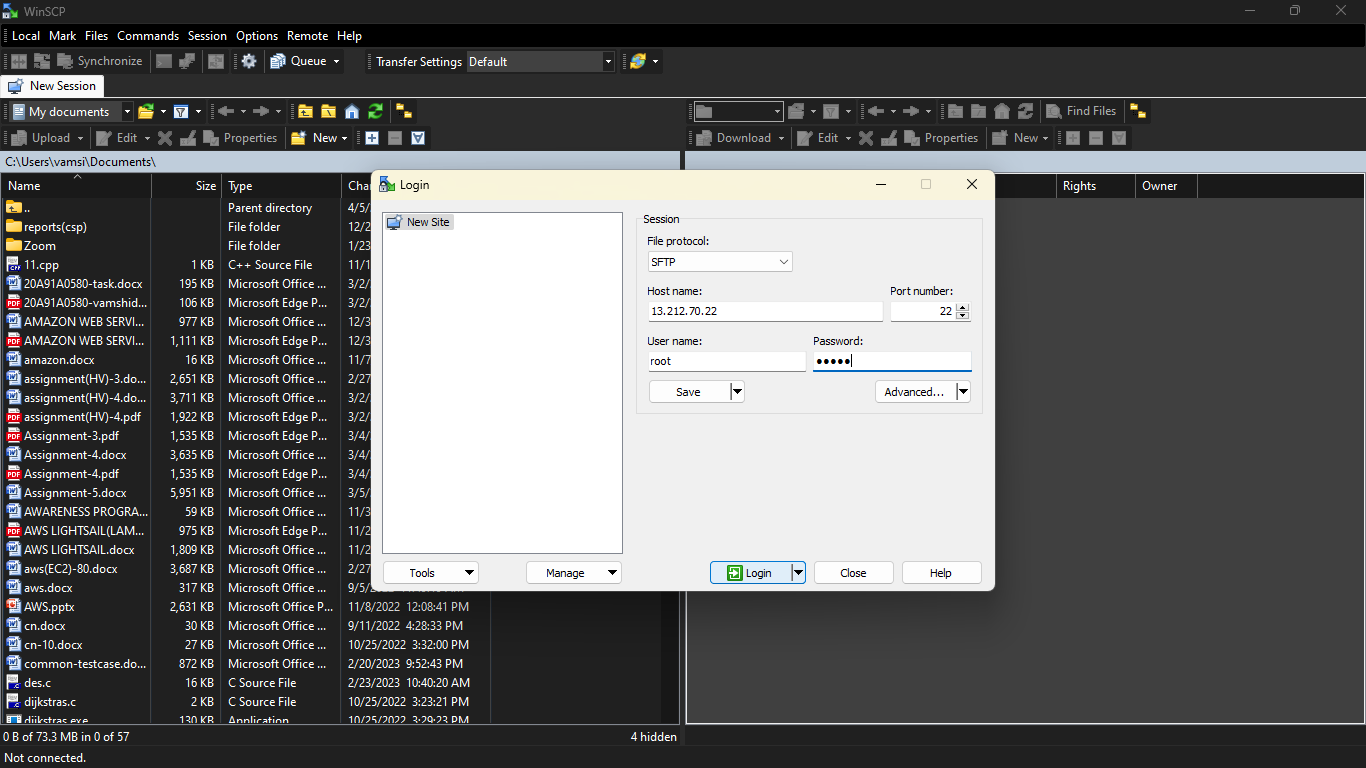
**$passwd root**

**$systemctl restart sshd**



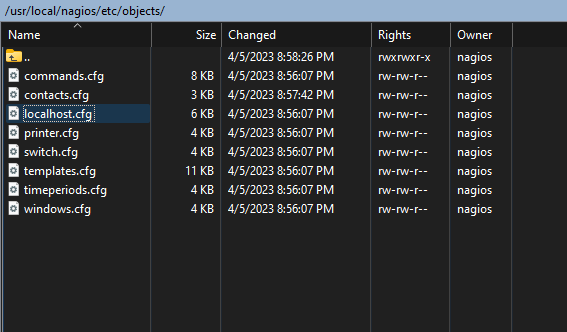
4.Install WinSCP tool for generating and modifying the configuration files instead of using command line interface(CLI).

5.After the installation give the host name(public Ip),username(root) and password.



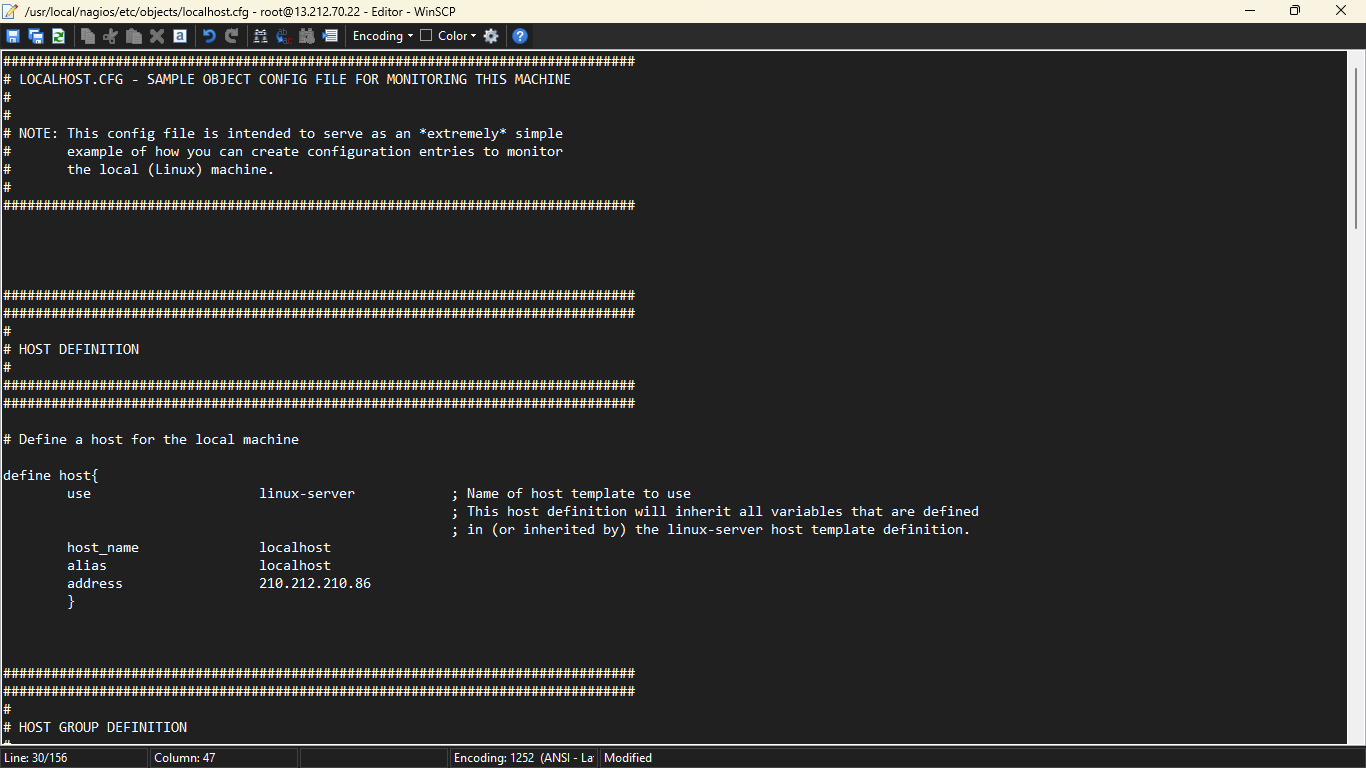
6.Now switch to the localhost.cfg using the below path

Path: **/usr/local/nagios/etc/objects/**



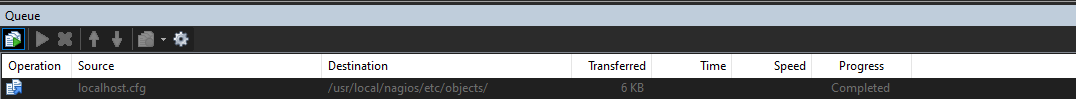
7.In the host definition modify the ip address which is to be monitored. Here we are using codemind

Monitoring code mind IP(**210.212.210.86**)

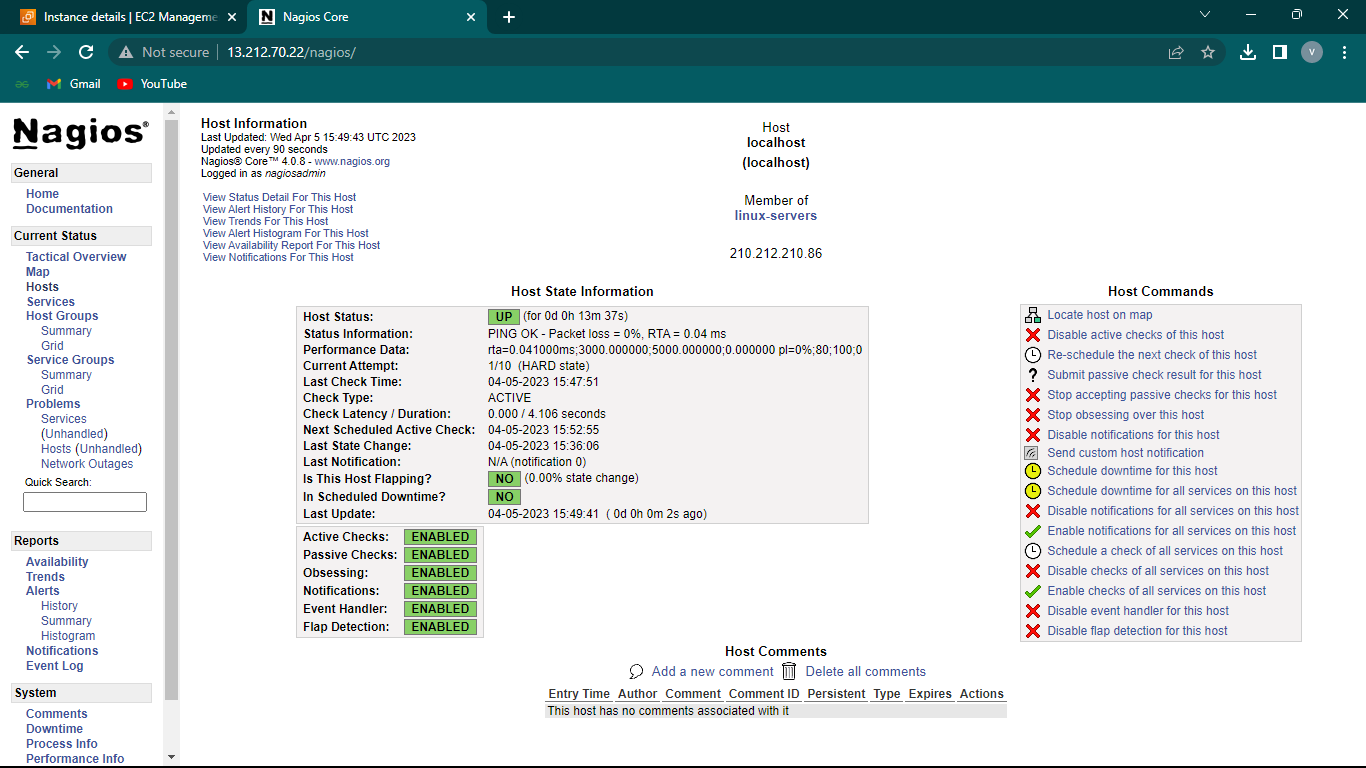


8.After modifying the localhost.cfg file save the file and restart the nagios.

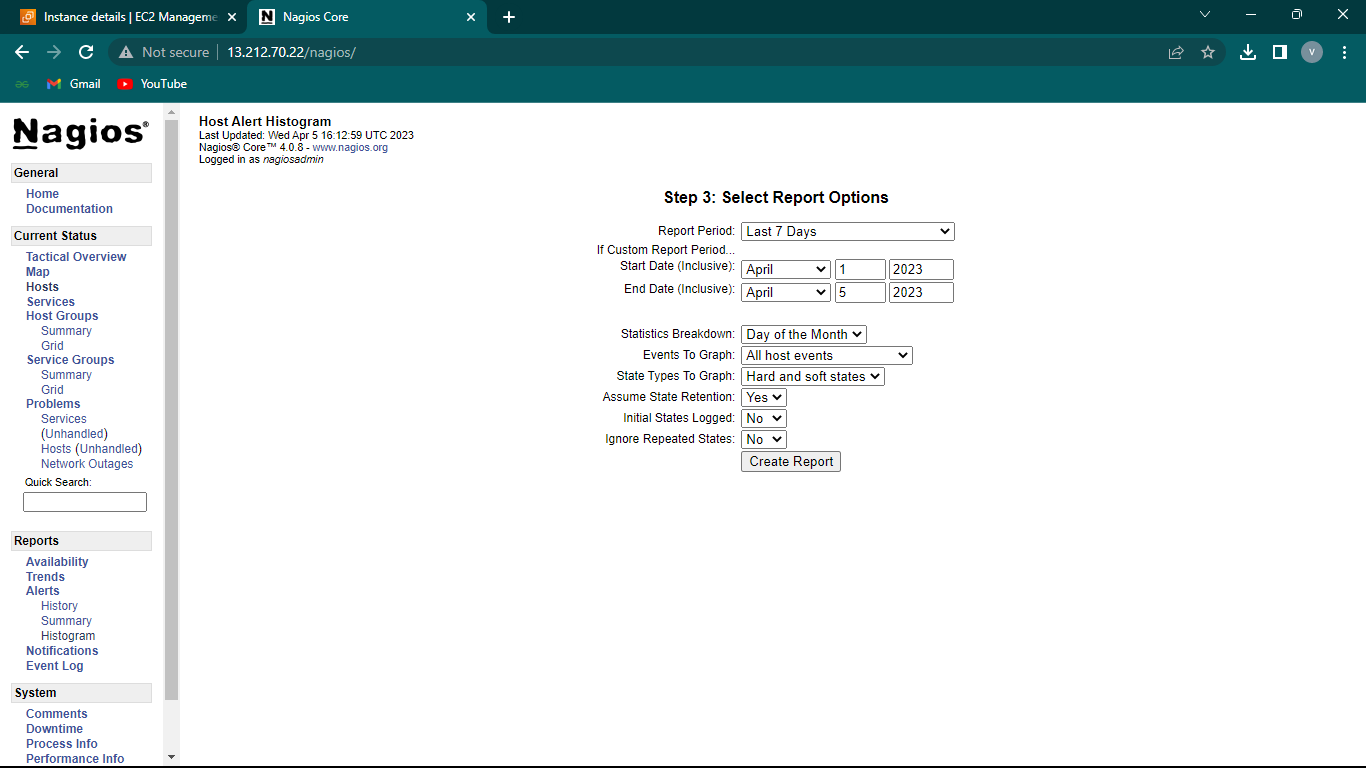
**$systemctl restart nagios**

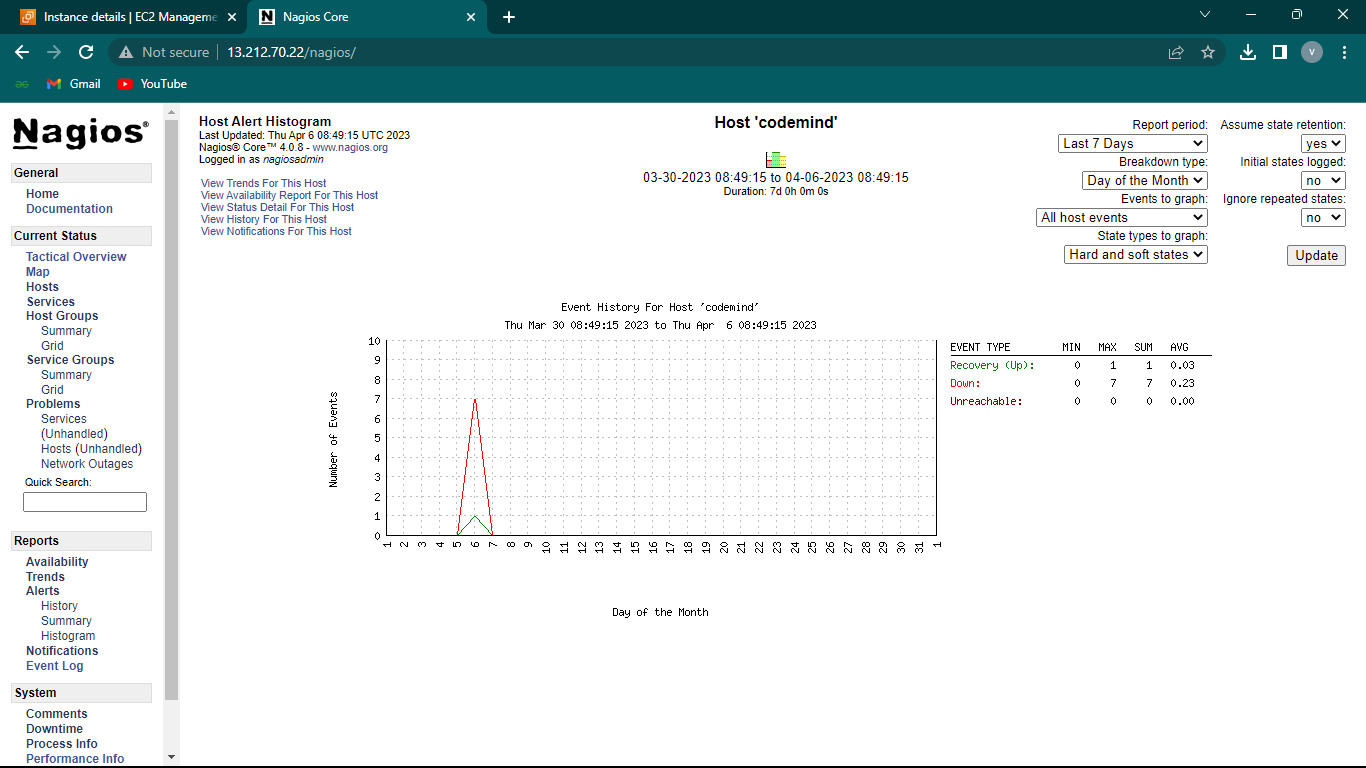






9.In the histogram we can find the graph which is easy to understand.





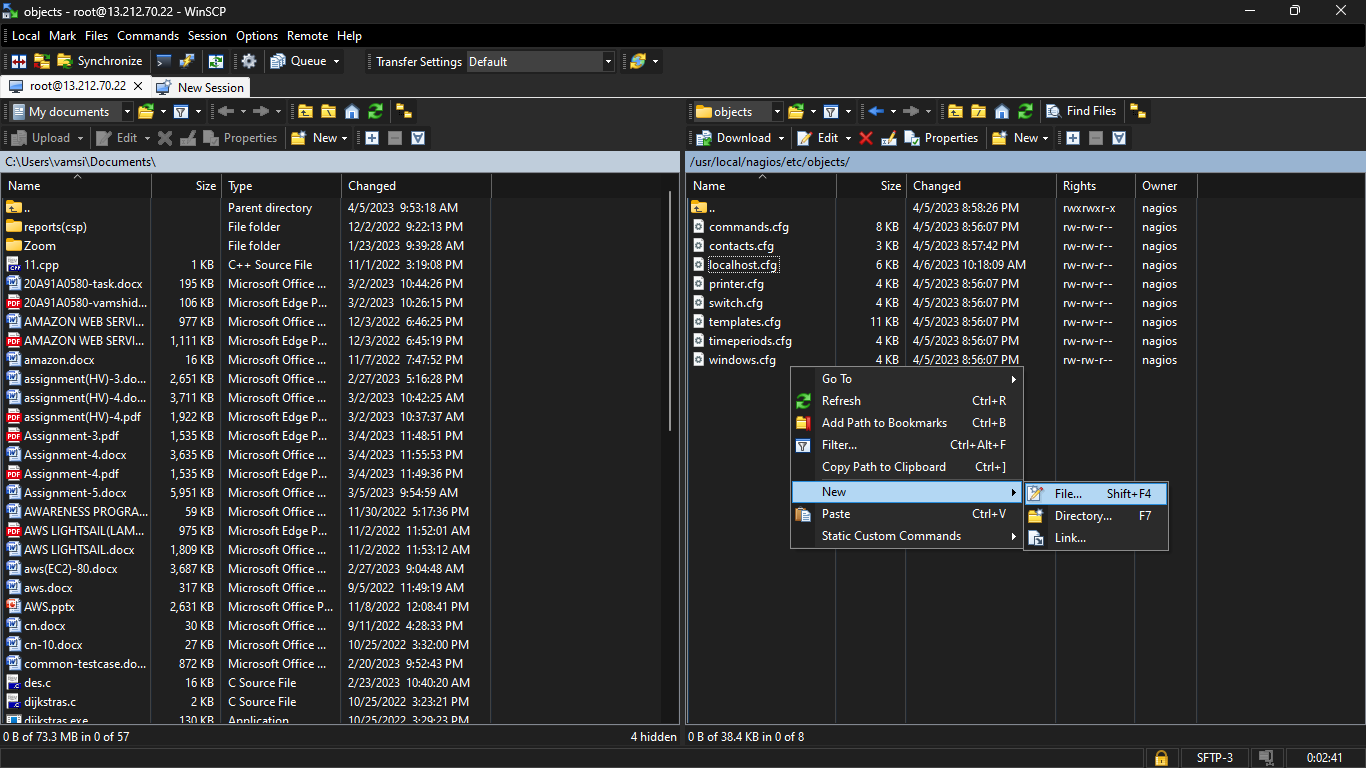
**Adding hosts and monitoring:**

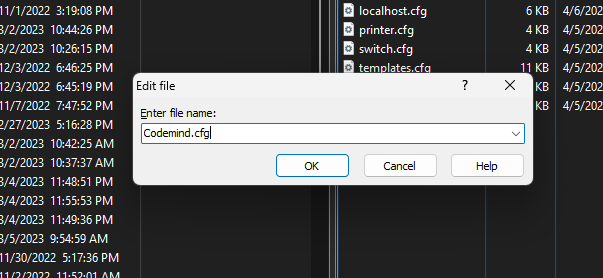
1.Switch to the path below:

Path: **/usr/local/nagios/etc/objects/**

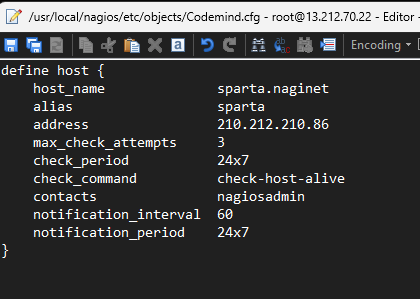
**2.create a new file with .cgf extention.**

**Eg:Codemind.cfg**



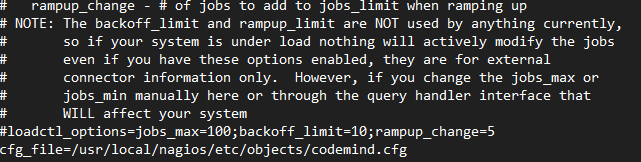


3.Enter the below code with the required ip and save it.



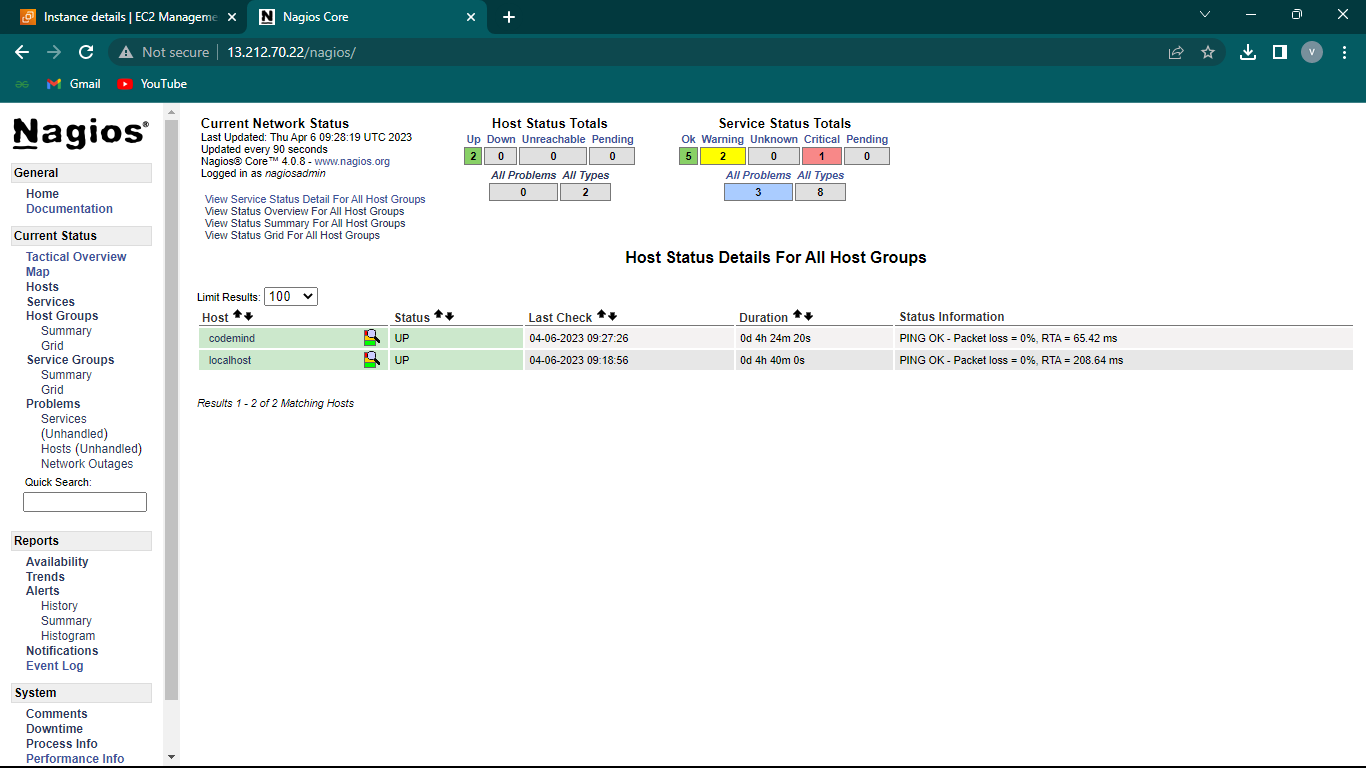
4.Switch to the path below and add the mentioned line in nagios.cfg file. Restart the nagios.

Path: **/usr/local/nagios/etc/objects/codemind.cfg**

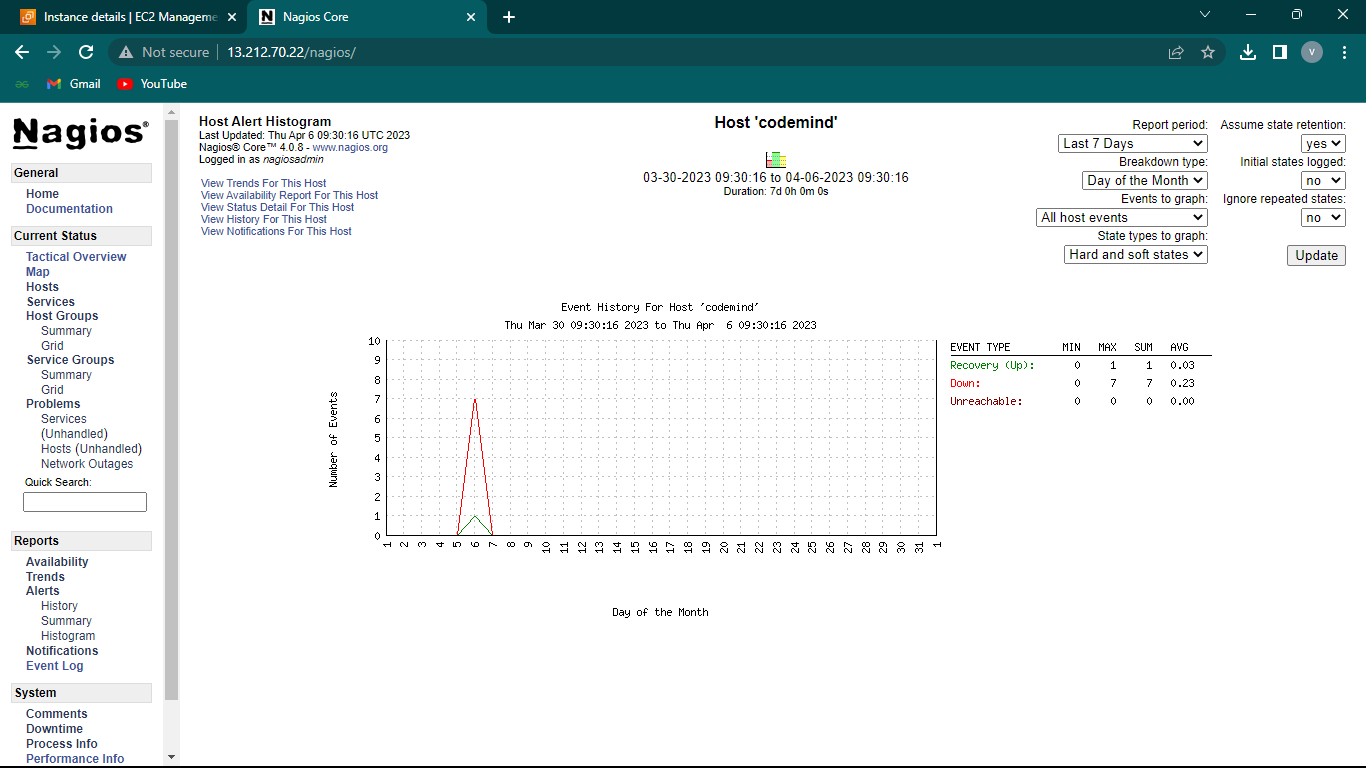




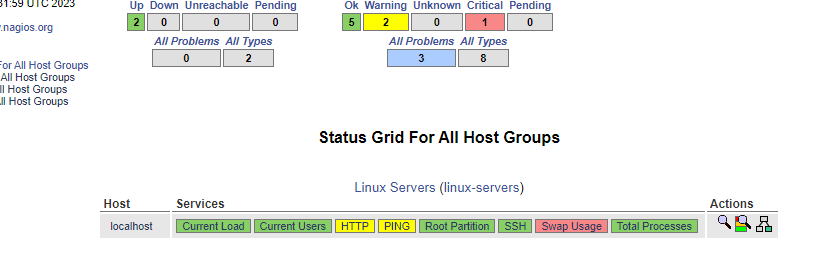
5.In the url ip/nagios we can file the host that was added.



6.In the histograms we can observe the graph.

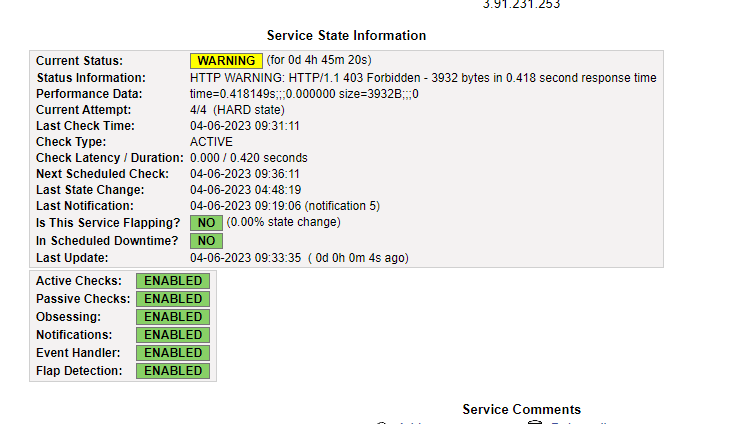


7.In the grid we can find many options like SSH,HTTP,PING etc.

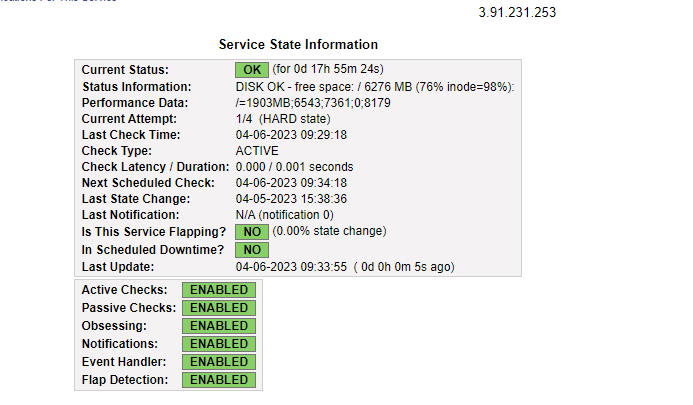


8.Selecting the options we can observe HTTP, SSH, storage used, ping status ,etc.

HTTP status:



DISK status:



USERS status:

