### **Nagios:**

##### **Prerequisites:**

Before installing nagios make sure httpd and php are installed on your server

And also implement gcc compiler

*yum install gd gd-devel gcc glibc glibc-common wget*

##### **Installation:**

Create a new nagios user account and give it a password:

*useradd -m nagios*

*passwd nagios*

Create a new nagcmd group for allowing external commands to be submitted through the web interface. Add both the nagios user and the apache user to the group.

groupadd nagcmd

usermod -a -G nagcmd nagios

usermod -a -G nagcmd apache

##### **Download nagios and nagios-plugins:**

Goto nagios download page and install any version of nagios.

Here I am installing nagios 4.0.3 version

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

And download nagios plugins too.

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

##### **Install nagios:**

Go to the folder where you’ve downloaded nagios, and extract it using command:

*tar xzf nagios-4.0.8.tar.gz*

Change to the nagios directory, and run the following commands to compile and install nagios.

*cd nagios-4.0.8*

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

*make all*

*make install*

*make install-init*

*make install-config*

Install nagios command mode using

*make install-commandmode*

Install nagios web interface using

*make install-webconf*

Create a nagiosadmin account for logging into the Nagios web interface.

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

##### **Install nagios plugins:**

Go to the directory where you downloaded the nagios plugins, and extract it.

*tar xzf nagios-plugins-2.0.3.tar.gz*

*cd nagios-plugins-2.0.3*

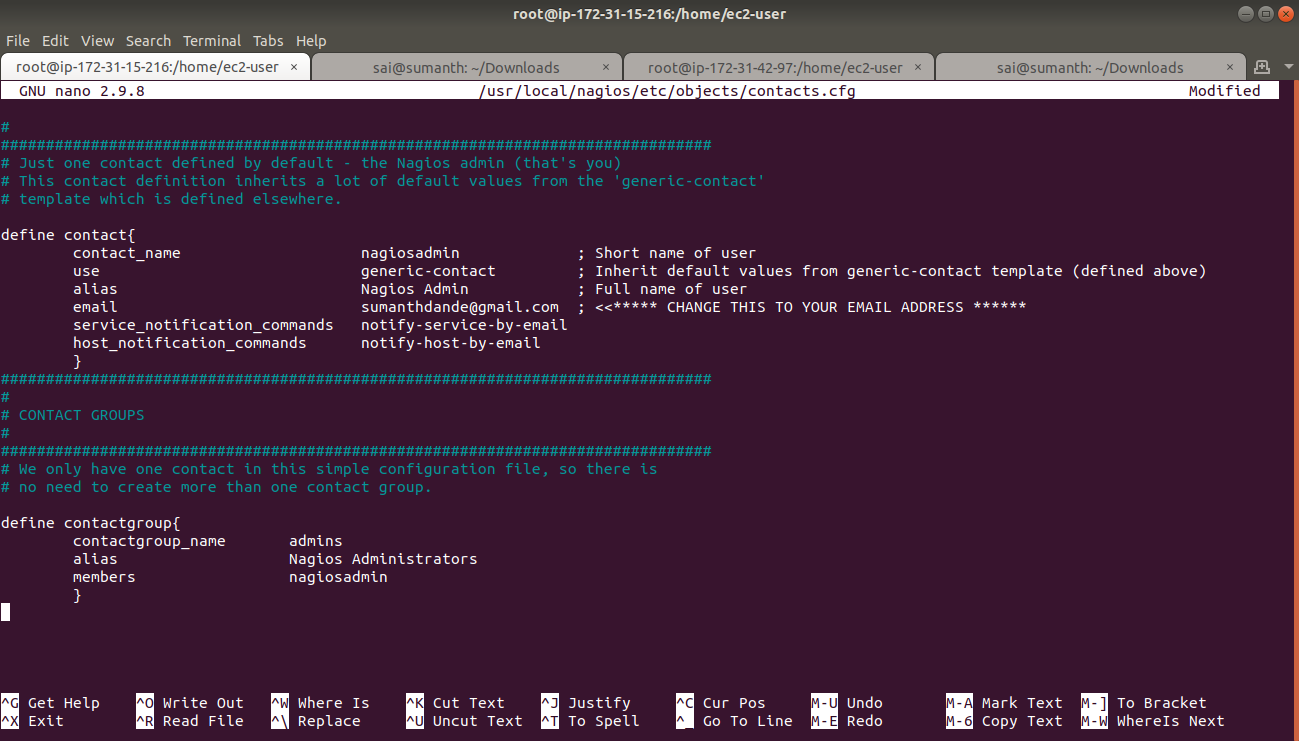
*./configure --with-nagios-user=nagios --with-nagios-group=nagios*

*Make*

*make install*

##### **Configure Nagios:**

Edit the configuration file in the location /usr/local/nagios/etc/objects/contacts.cfg



Now, check for any configuration errors using command:

*/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg*

If there are no errors, start nagios service and make it to start automatically on every boot.

*systemctl start nagios*

*chkconfig --add nagios*

*chkconfig nagios on*

By default, SELinux will be in enforcing mode, and it throws “Internal Server Error” messages when you attempt to access the Nagios CGIs.

To rectify this error, edit file /etc/selinux/config:

And, set SELinux to permissive mode.



##### **Access Nagios Web Interface:**

Open nagios administrator console with URL http://nagios-server-ip/nagios and enter the username as nagiosadmin and its password which we created in the earlier steps.

This is how Nagios administrative console looks:



Click on the “Hosts” section in the left pane of the console. You will see there the no of hosts to be monitored by Nagios server.

##### **Add Monitoring targets to Nagios server:**

Open remote servers and install following services on remote server

Add EPEL repository in your CentOS 7 clients to install nrpe package.

*yum install epel-release*

Install “nrpe” and “nagios-plugins” packages in client systems:

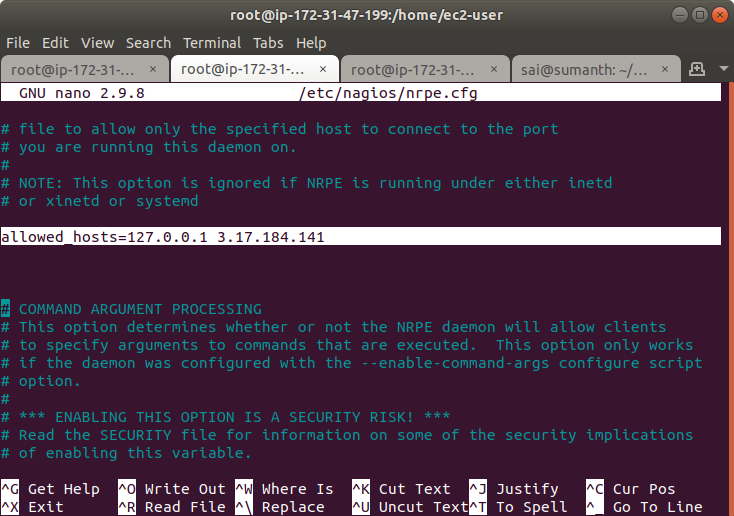
yum install nrpe nagios-plugins-all openssl

Configure monitoring targets

Edit /etc/nagios/nrpe.cfg

Add allowed\_hosts

Add your Nagios server ip address:



Start nrpe service

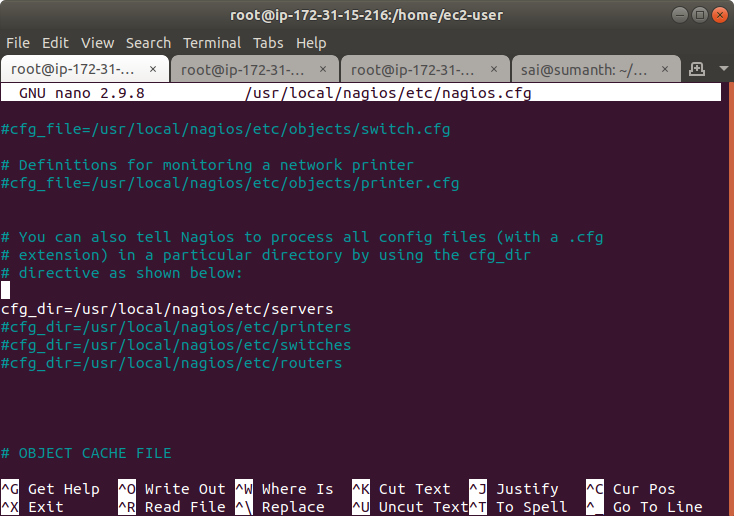
*service nrpe start*

Now go back to nagios server and add the clients in configuration file

To do that edit /usr/local/nagios/etc/nagios.cfg file

Find and uncomment the following line

*cfg\_dir=/usr/local/nagios/etc/servers*



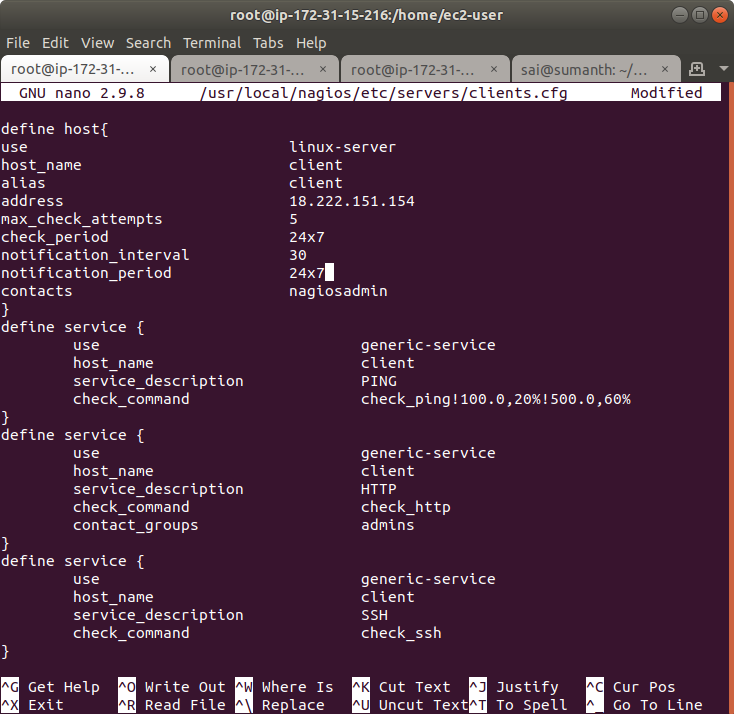
Create a directory called “servers” under “/usr/local/nagios/etc/”.

mkdir /usr/local/nagios/etc/servers

Create config file to the client to be monitored:

*nano /usr/local/nagios/etc/servers/clients.cfg*

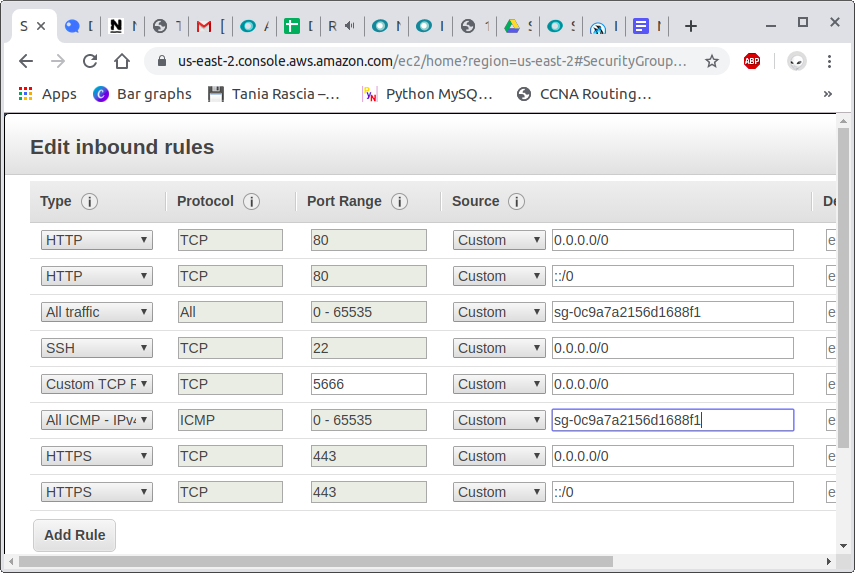
Add remote-server and services in the configuration file



Here 18.222.151.154 is my remote server ip address and restart nagios service

*service nagios restart*

In the security group of remote server allow all traffic from nagios server

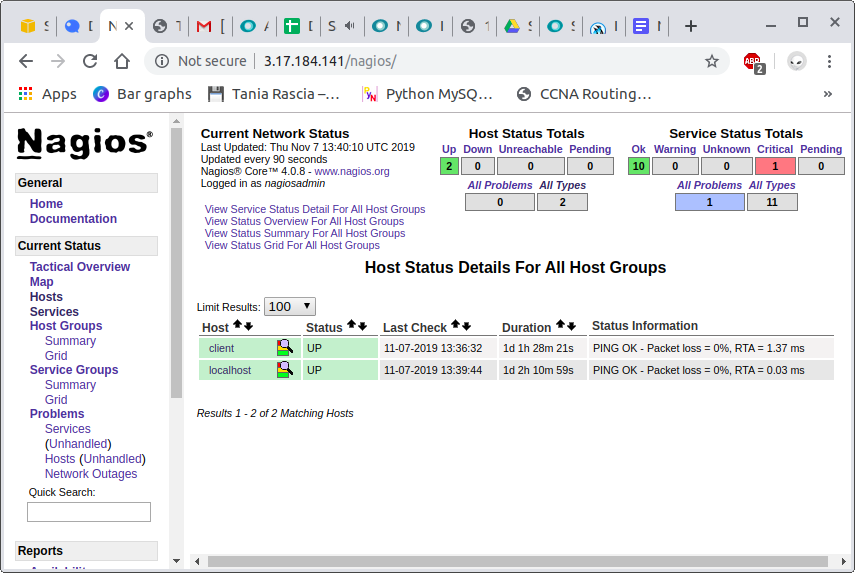


Here the security group mentioned is the security group of the nagios server

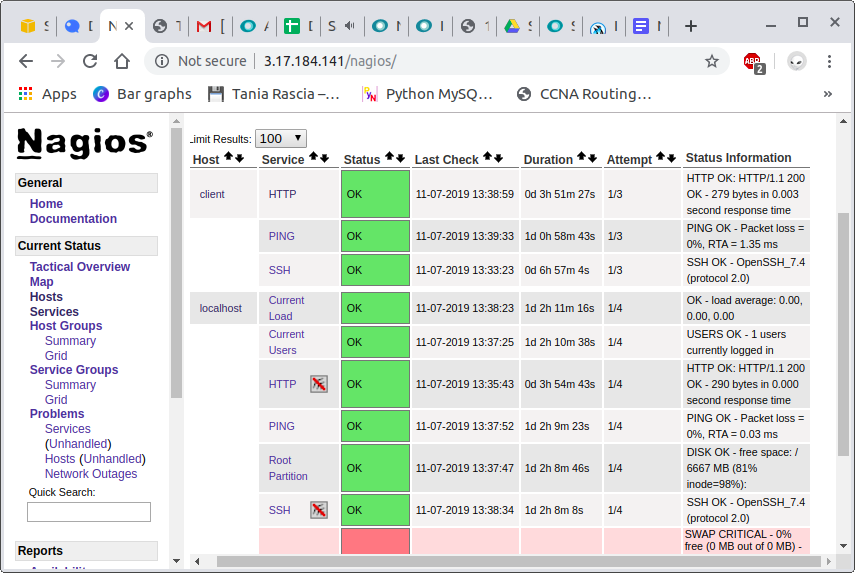
Add 5666/tcp in /etc/services in remote-server if you are facing any errors.

And open the nagios-server-ip/nagios and you can see the remote-host added on the left side

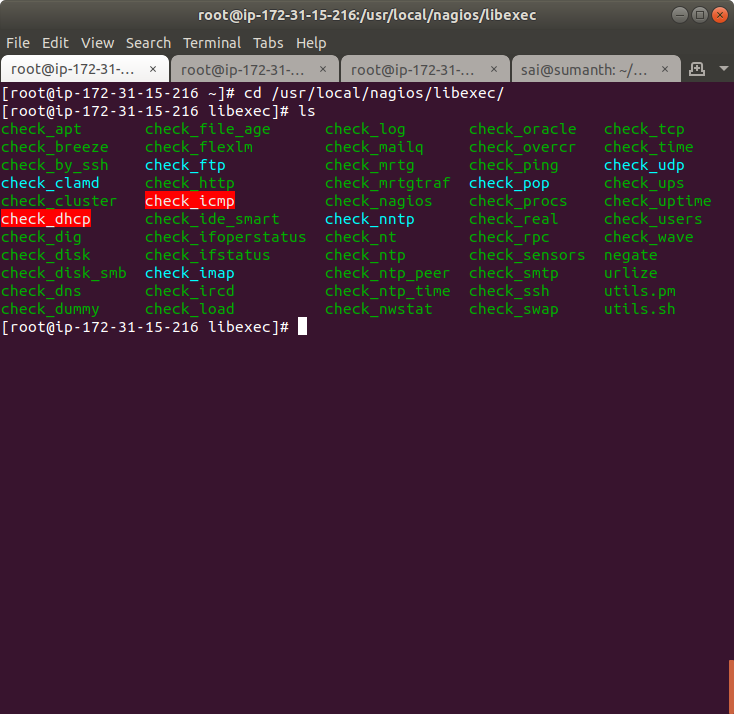
Here we can see that remote-server is added



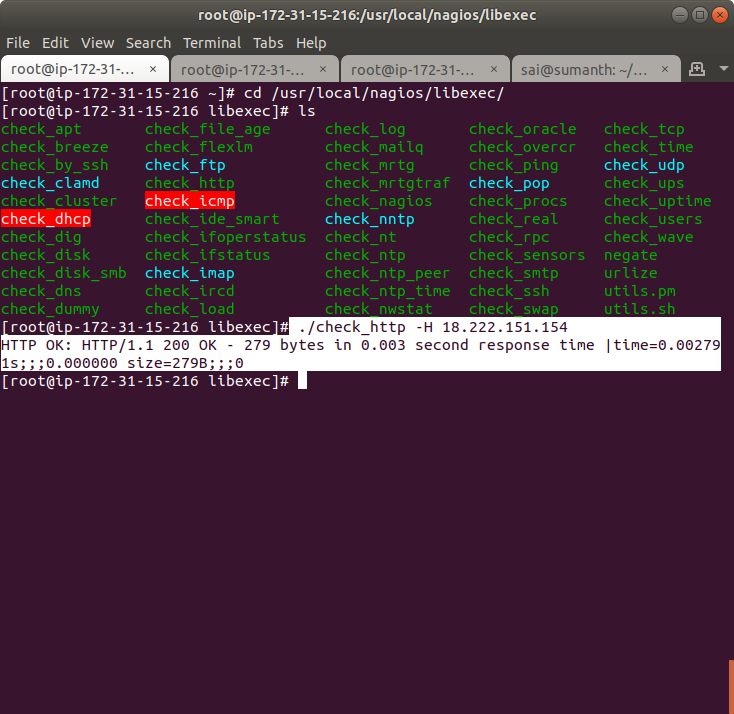
And we can monitor the services of remote-server



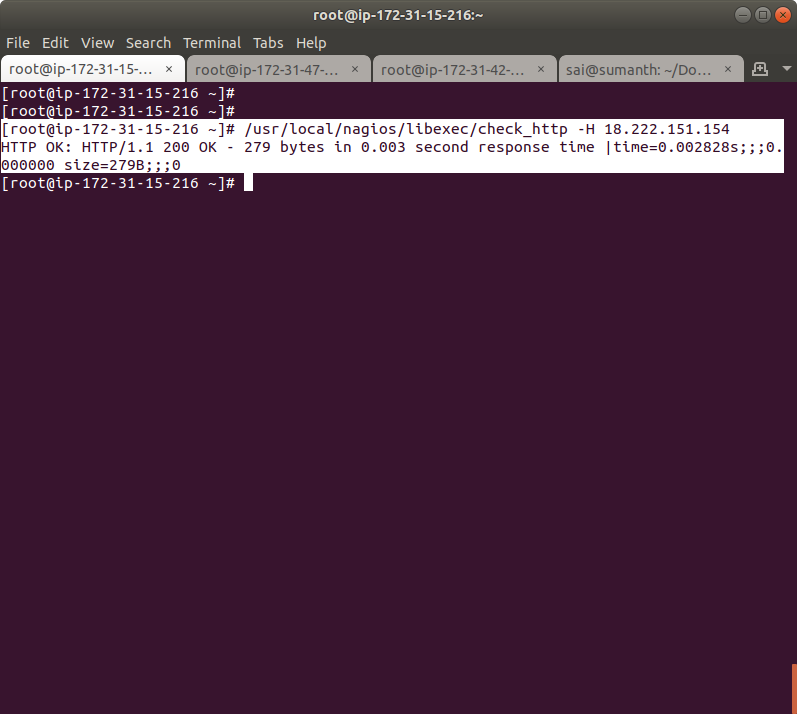
To see all the plugins available go to location /usr/local/nagios/libexec/ and ls



To execute any of the plugin use the following command



Or you can execute the plugins from anywhere using the location



### **New Relic:**

First install node js in server using

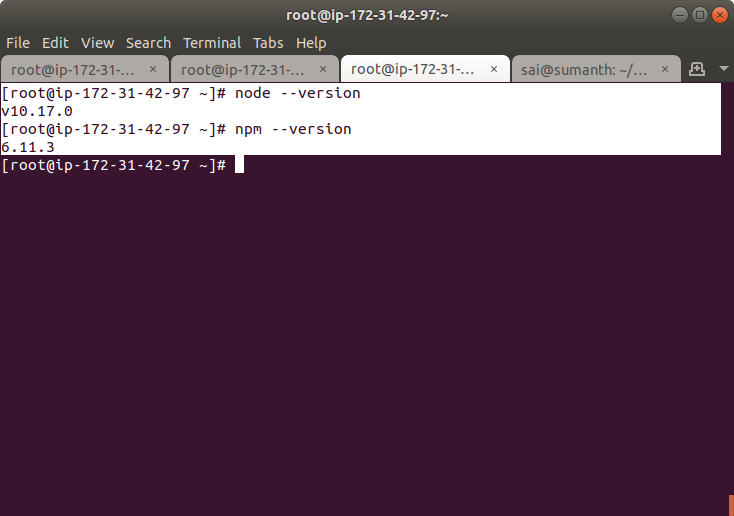
*curl -sL https://rpm.nodesource.com/setup\_10.x | sudo bash -*

*sudo yum install nodejs*

Verify node js and npm installation using

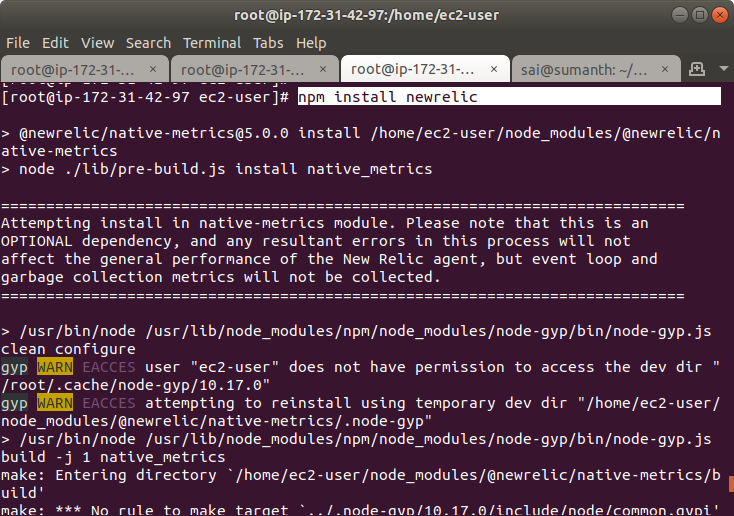
*node --version*

*npm --version*



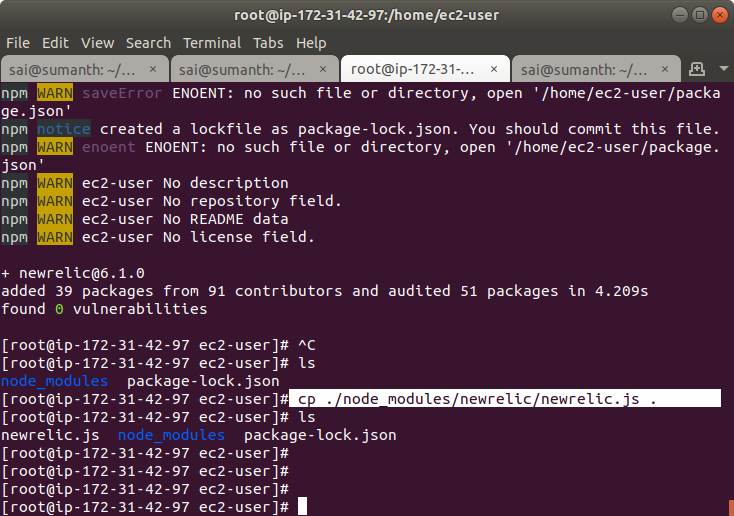
Install the New Relic Node.js agent

*npm install newrelic*

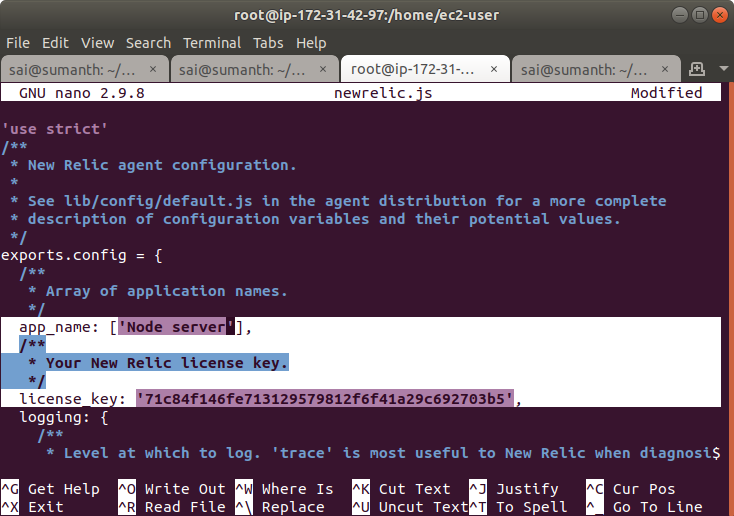


Copy the newrelic.js from node\_modules/newrelic to root directory of application

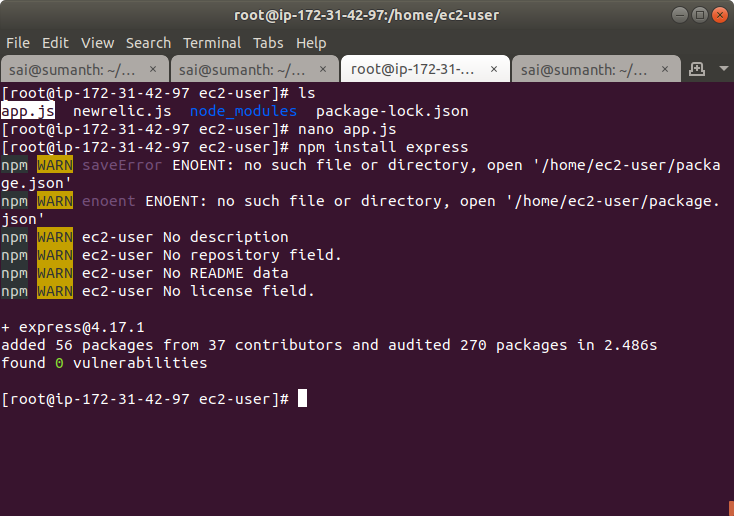
*cp ./node\_modules/newrelic/newrelic.js .*



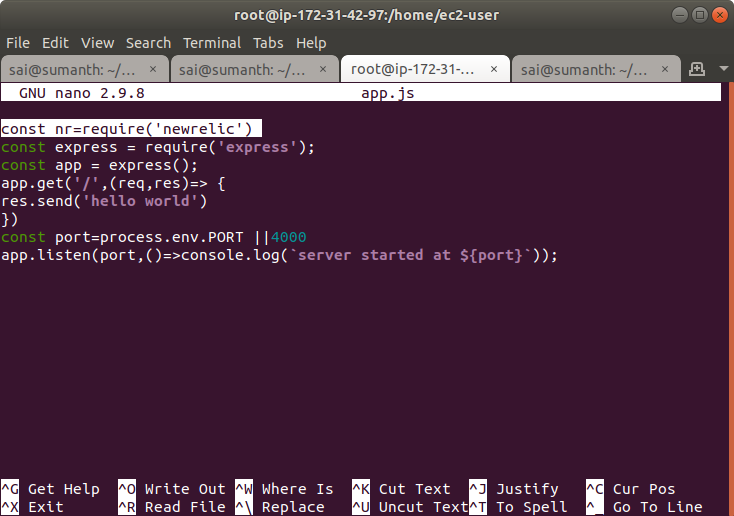
Open the newrelic.js file and add the license\_key and app\_name



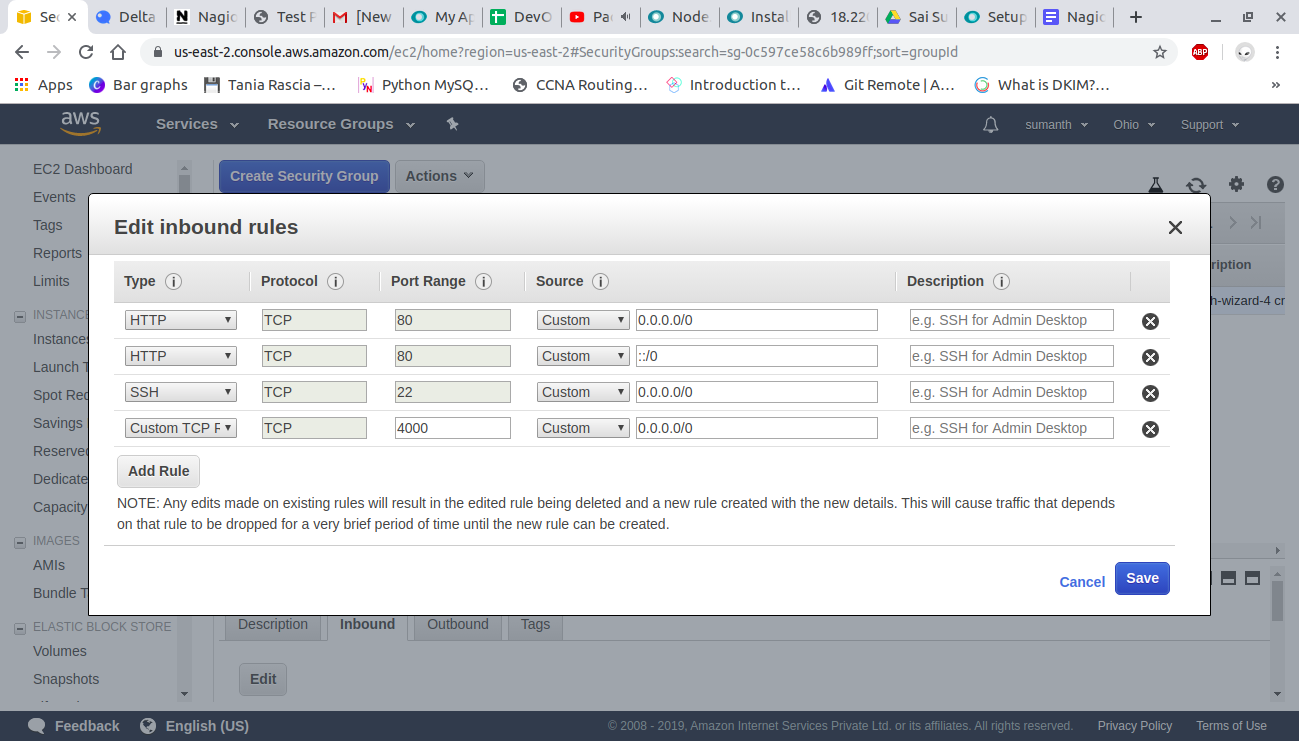
Create an app.js and execute it



Include new relic in your application

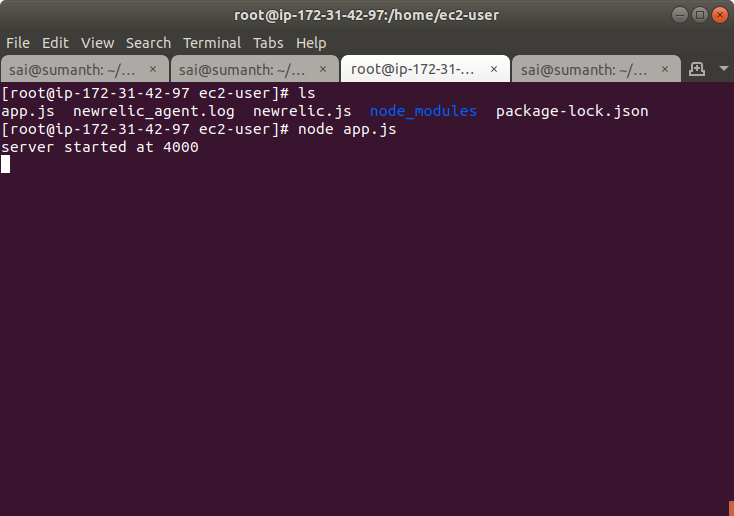


Open the 4000 port in the security group for the server because here we are running our application on port number 4000

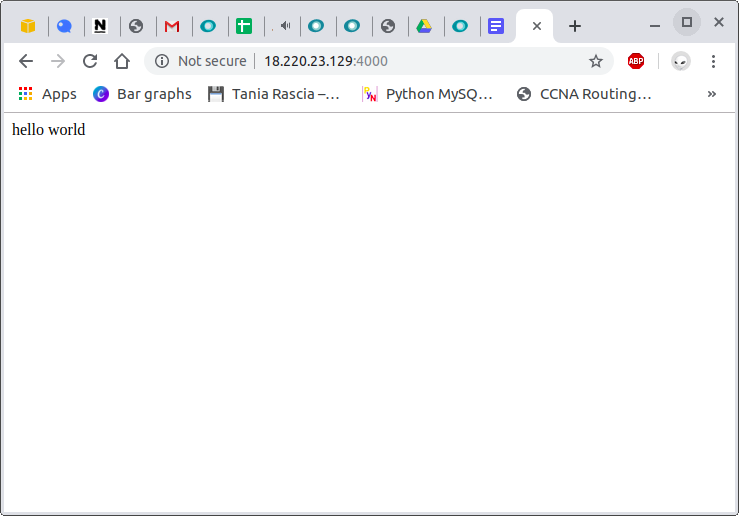


Execute your application using node

node app.js



You can see the service is running on port 4000



Now your application will be automatically detected in new relic

