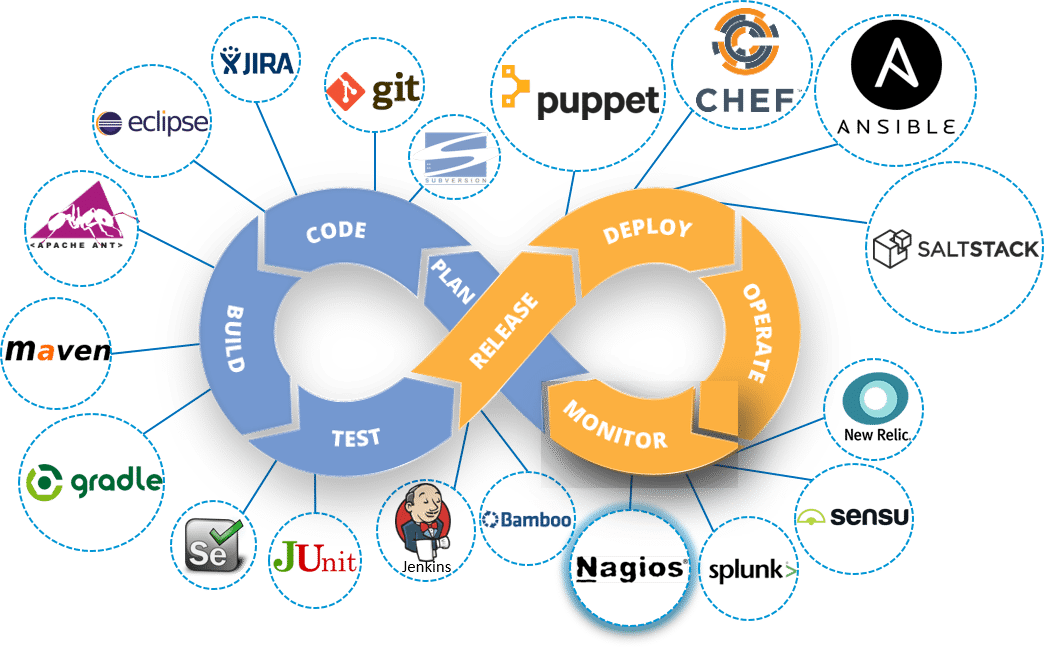
**Assignment-1                                              Marks: 25**

Explain the role of continuous monitoring in DevOps and demonstrate the use of Nagios as a continuous monitoring tool by configuring a host machine with Nagios server.

**Solution :**

## ****Continuous Monitoring:****

Let me first tell you where Continuous Monitoring lies in the DevOps life-cycle, consider the diagram below:



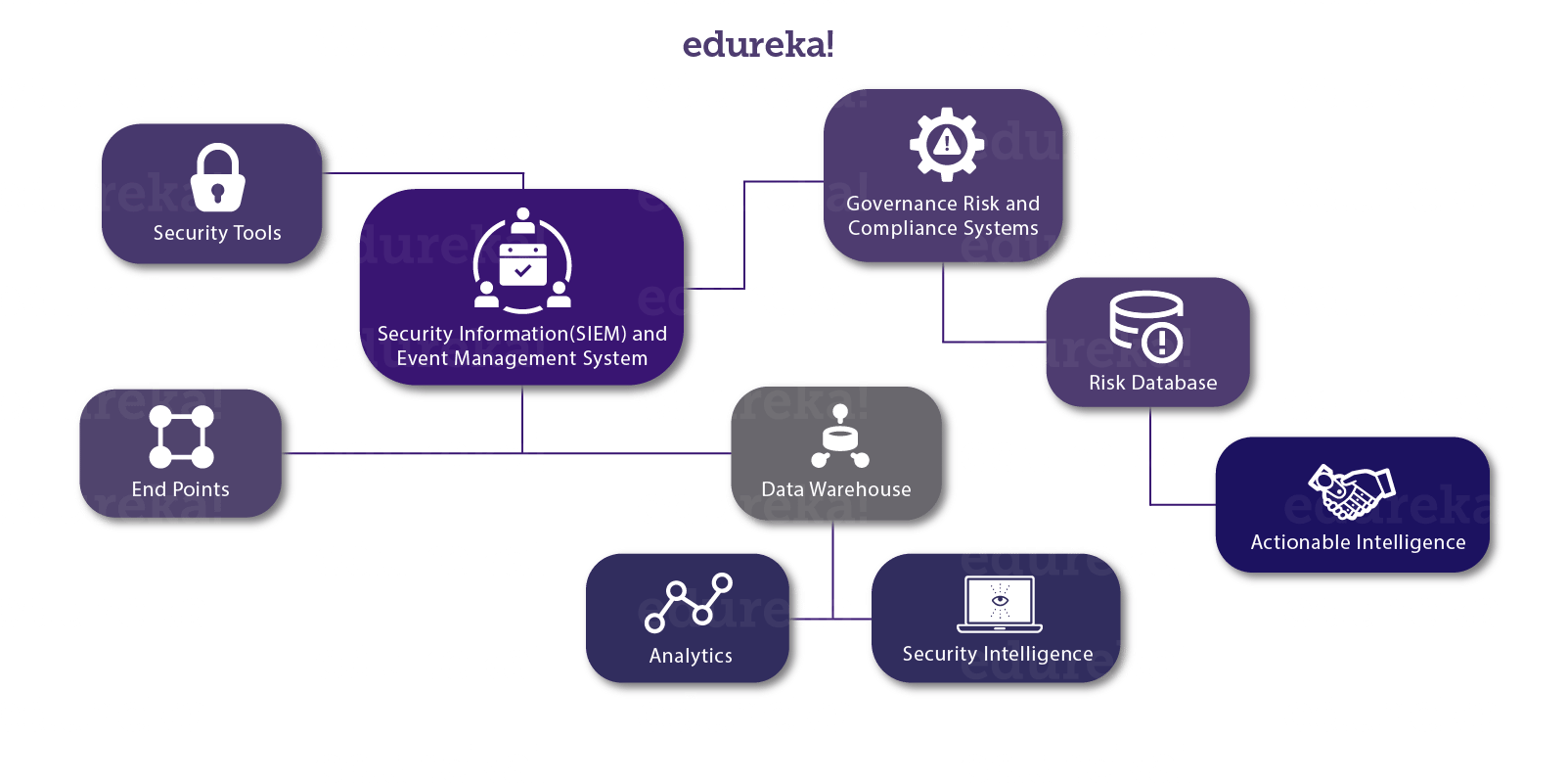
Looking at the diagram you must be thinking this is the last stage in the DevOps lifecycle, but this is not the case. There is no end to a DevOps life cycle, and that is the reason for the infinity symbol. Continuous Monitoring comes into the picture, once the application is deployed on the production servers.

Continuous Monitoring is all about the ability of an organization to detect, report, respond, contain and mitigate the attacks that occur, in its infrastructure.

Continuous Monitoring is actually not new, it’s been around for some time. For years our security professionals are performing static analysis from – system log, firewall logs, IDS logs, IPS logs etc. But, it did not provide proper analysis and response. Today’s Continuous Monitoring approache gives us the ability to aggregate all of the events that I discussed above, co-relate them, compare them and then estimate the organization’s risk posture.

If we take all these pieces and ensure the interlinking between them. This is the crux of Continuous Monitoring.

Let me explain this with a use-case. Consider the diagram below:

Now, let me explain you the above diagram:

1. We have various security tools, like Firewall, IDS, End Point Protection etc. they are connected with a ‘Security Information and Event Management system.
2. In order to achieve Continuous Monitoring, we need to have all the parts talking to each other, let me explain that to you.
3. So we have security tools and series of ‘End Points’,  this can include client and servers, routers, switches, mobile devices and so on.
4. These two groups can then talk to a Security Information and Event Management system (SIEM), through a common language and in more automated fashion.
5. Connected to this SIEM there are two important components, first one is a Data Warehouse. Now to this Data Warehouse, we will connect ‘Analytics’ and ‘Security Intelligence’.
6. Security intelligence (SI) is the information relevant to protecting an organization from external and insider threats as well as the processes, policies and tools designed to gather and analyze that information.
7. This SIEM is also connected to a ‘Governance Risk and Compliance System’ it basically provides dashboarding.
8. To this ‘Governance Risk and Compliance System’  we attach a risk database. This gives us ‘Actionable Intelligence’.
9. Actionable Intelligence is nothing but information that can be acted upon, with the further implication that actions *should*be taken.

So here, we are Monitoring the events on the on going basis and determining what level of risk we are experiencing. With this, we can correlate the events at the SIEM. We can perform Network Behavior and Anomaly Detection at the ‘Analytics Engine’. This is what Continuous Monitoring is all about:

*The integration of an organization security tools, the aggregation, normalization and correlation of the data that is produced by the security tools. The analysis of that data, based on the organization’s risk goals and threat knowledge, and near real-time response to the risks identified.*

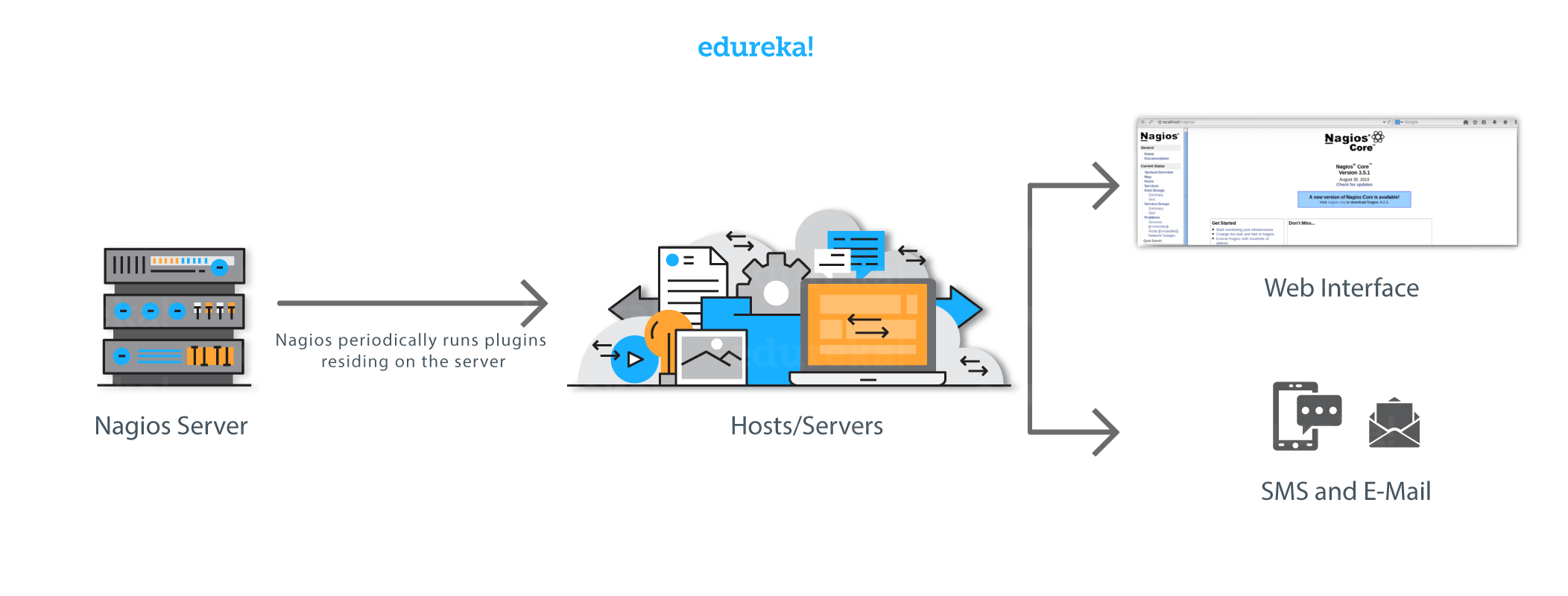
‘If you can’t measure it you can’t manage it’. I hope you know what I am talking about.

Next up in this Nagios tutorial, I will be introducing you to one of the most famous monitoring tool ‘Nagios’.

**What is Nagios?**

Nagios is used for Continuous monitoring of systems, applications, services, and business processes etc in a DevOps culture. In the event of a failure, Nagios can alert technical staff of the problem, allowing them to begin remediation processes before outages affect business processes, end-users, or customers. With Nagios, you don’t have to explain why an unseen infrastructure outage affect your organization’s bottom line.

Let me explain to you how Nagios works. Consider the diagram below:

Nagios runs on a server, usually as a daemon or a service.

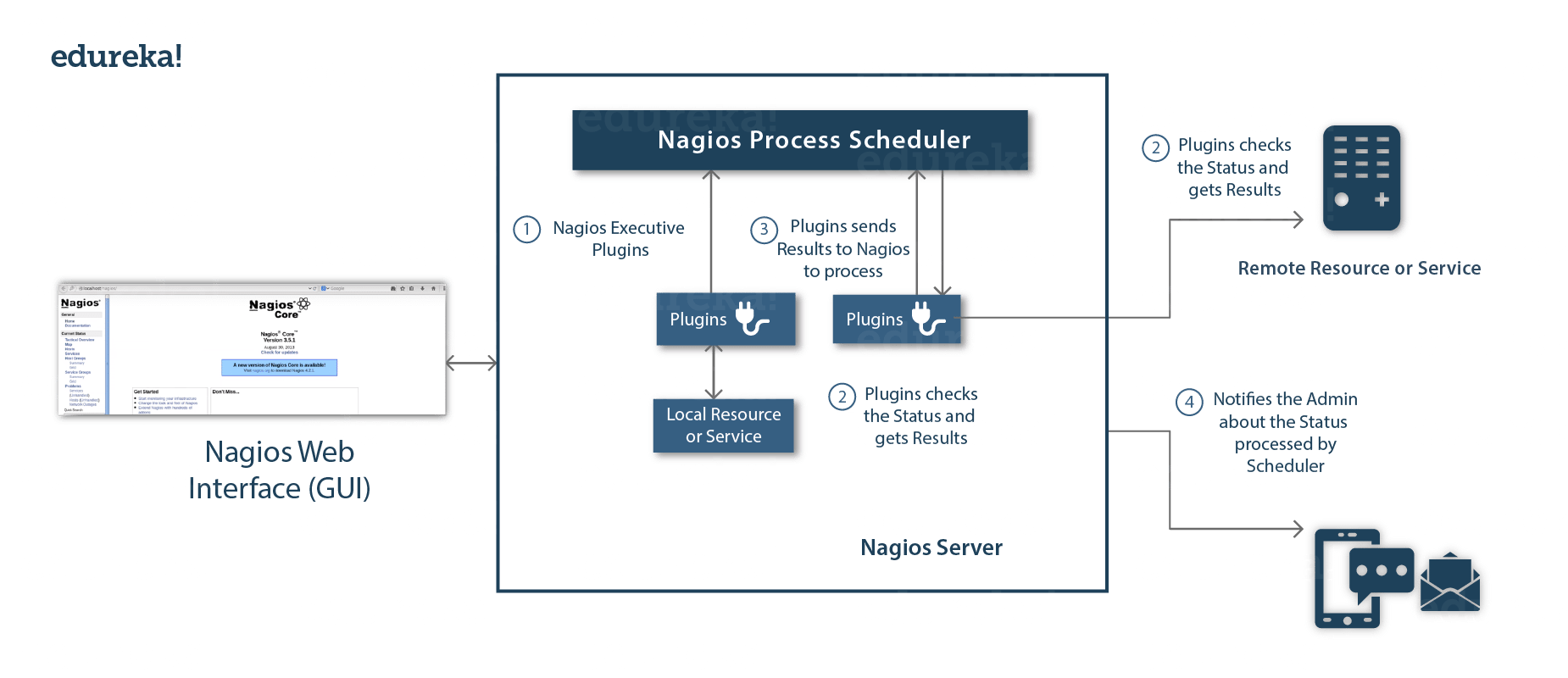
It periodically runs plugins residing on the same server, they contact hosts or servers on your network or on the internet. One can view the status information using the web interface. You can also receive email or SMS notifications if something happens.  
The Nagios daemon behaves like a scheduler that runs certain scripts at certain moments. It stores the results of those scripts and will run other scripts if these results change.

*Plugins:*These are compiled executables or scripts (Perl scripts, shell scripts, etc.) that can be run from a command line to check the status or a host or service. Nagios uses the results from the plugins to determine the current status of the hosts and services on your network.

Let’s now discuss it’s architecture.

**Nagios Architecture:**

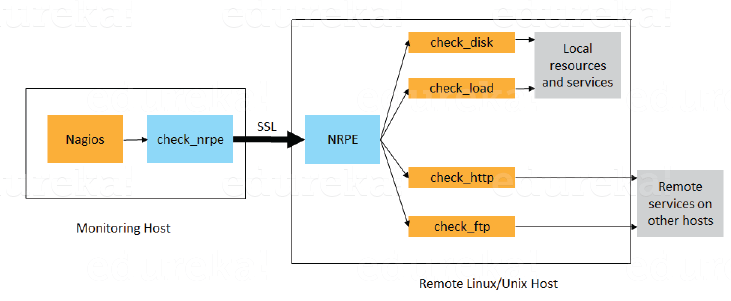
* Nagios is built on a server/agents architecture.
* Usually, on a network, a Nagios server is running on a host, and Plugins interact with local and all the remote hosts that need to be monitored.
* These plugins will send information to the Scheduler, which displays that in a GUI.



I also need to explain you NRPE (Nagios Remote Plugin Executor).

The NRPE addon is designed to allow you to execute Nagios plugins on remote Linux/Unix machines. The main reason for doing this is to allow Nagios to monitor “local” resources (like CPU load, memory usage, etc.) on remote machines. Since these public resources are not usually exposed to external machines, an agent like NRPE must be installed on the remote Linux/Unix machines.

Consider the diagram below:



* The check\_nrpe plugin, resides on the local monitoring machine.
* The NRPE daemon, runs on the remote Linux/Unix machine.
* There is a SSL (Secure Socket Layer) connection between monitoring host and remote host as shown in the diagram above.

Now in this Nagios tutorial, it is time for some **Hands-on**.

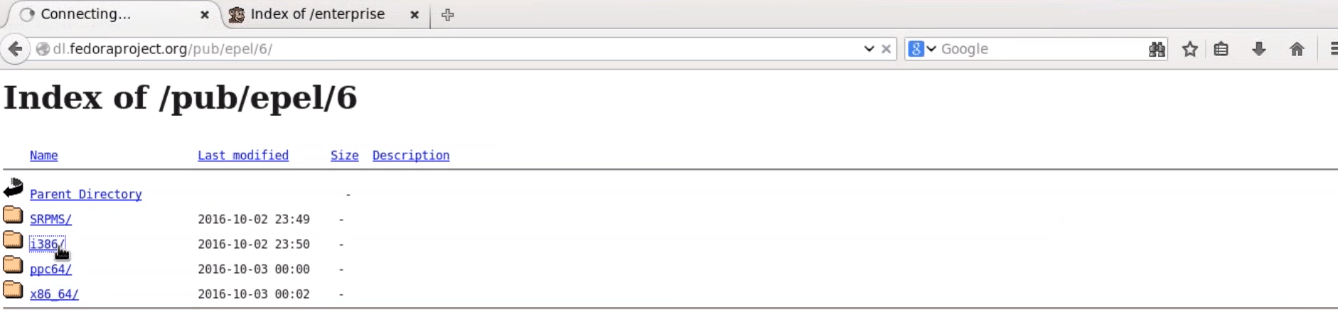
Let’s start by installing Nagios Core

**Install Nagios Core:**

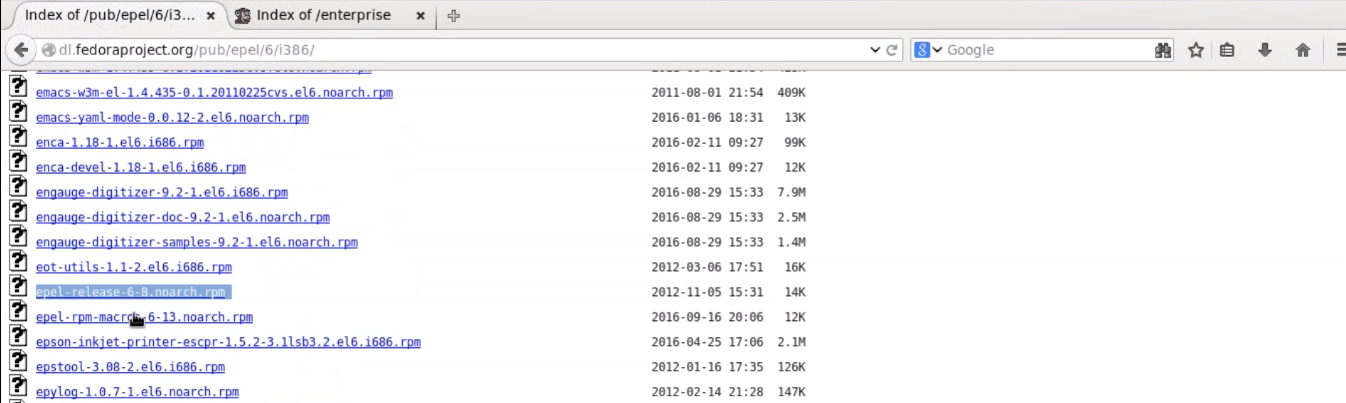
The complete process to install Nagios can be summarized in four steps:

1. Install Required Packages In The Monitoring Server
2. Install Nagios Core, Nagios Plugins And NRPE (Nagios Remote Plugin Executor)
3. Set Nagios Password To Access The Web Interface
4. Install NRPE In Client

**Step – 1: Install Required Packages On The Monitoring Server:**



Click on i386, and then you will be redirected to a page.



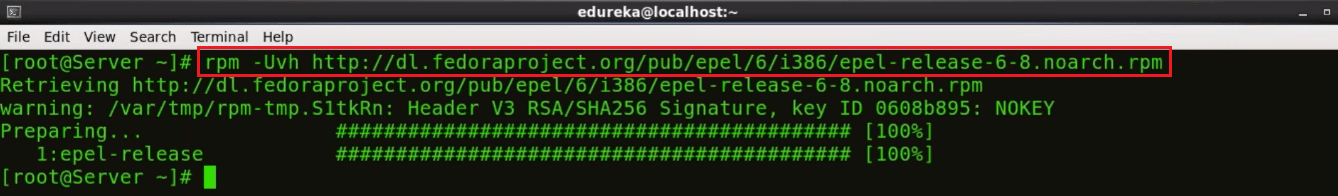
Since I am using CentOS 6, so I will right click and copy the link location of ‘*epel-release-6-8.noarch.rpm*‘, as shown in the above screenshot.

[[](https://www.edureka.co/devops-certification-training)](https://www.edureka.co/devops-certification-training" \t "_blank)

**[DevOps Certification Training Course](https://www.edureka.co/devops-certification-training" \t "_blank)**

[Explore Curriculum](https://www.edureka.co/devops-certification-training" \t "_blank)

Open the terminal and use *rpm -Uvh*command and paste the link.

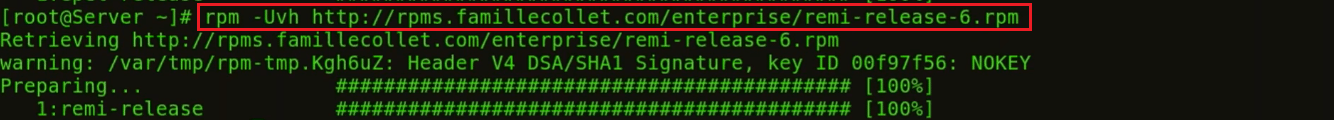


We need to download one more repository, for that visit the website ‘<http://rpms.famillecollet.com/enterprise/>‘



Right-click and copy the link location for ‘*remi-release-6.rpm*‘

Again open the terminal and use *rpm -Uvh* command and paste the link.



Fine, so we are done with the pre-requisites. Let’s proceed to the next step.

**Step – 2: Install Nagios Core, Nagios Plugins And NRPE (Nagios Remote Plugin Executor):**

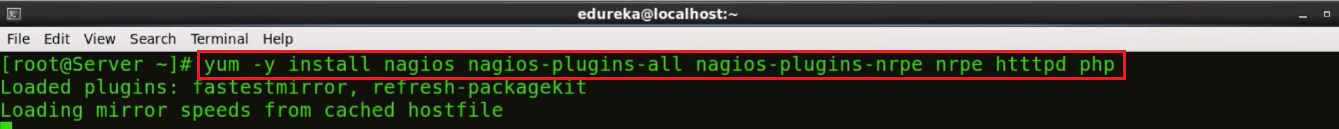
Execute the below command in the terminal:

yum -y install nagios nagios-plugins-all nagios-plugins-nrpe nrpe httpd php

This will install Nagios, Nagios Plugins, Plugins for NRPE, NRPE, Apache and PHP

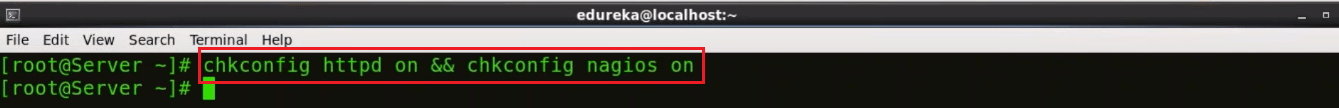
Apache web server is required to monitor the current web server status.

Php is used to process dynamic content of the site date.



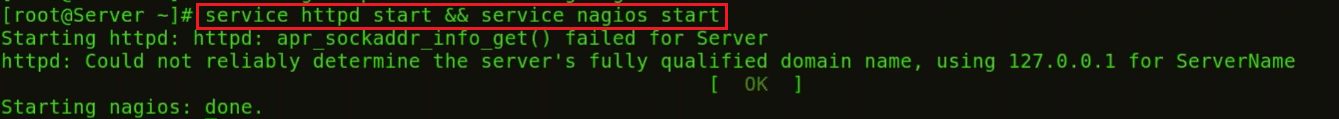
Next, we need to enable Apache and Nagios service:

chkconfig httpd on && chkconfig nagios on



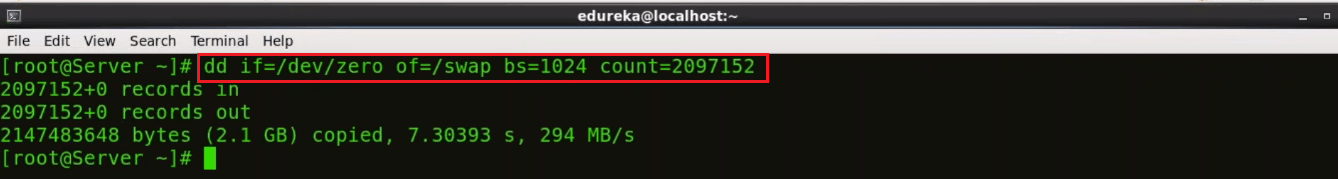
Our next step is to start Nagios and Apache:

service httpd start && service nagios start



Now, I will enable swap memory of at least 1GB. It’s time to create the swap file itself using the dd command:

dd if=/dev/zero of=/swap bs=1024 count=2097152

Swap is basically used to free some, not so frequently accessed information from RAM, and move it to a specific partition on our hard drive.

Now that you have created the swap partition, use the command *mkswap* to setup the swap partition. This is going to prepare the swap file by creating a linux swap area.

mkswap /swap

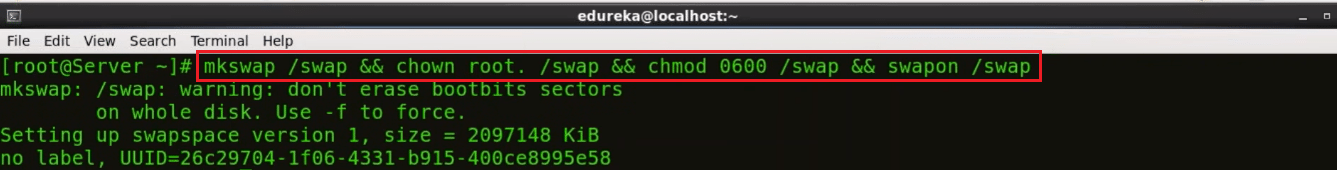
To prevent the file from being world-readable, you should set up the correct permissions on the swap file:

chown root. /swap

chmod 0600 /swap

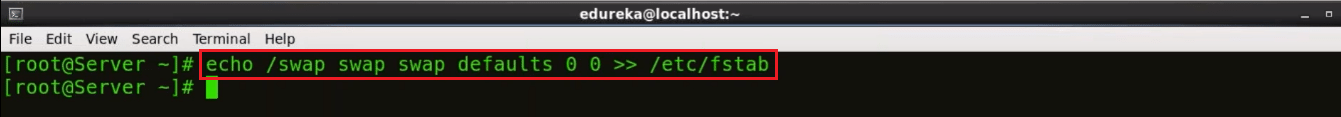
If you see no errors, your swap space is ready to use. To activate it immediately, type:

swapon /swap



This file will last on the virtual private server until the machine reboots. You can ensure that the swap is permanent by adding it to the fstab file.

echo /swap swap swap defaults 0 0 >> /etc/fstab



The operating system kernel can adjust how often it relies on swap through a configuration parameter known as **swappiness**.

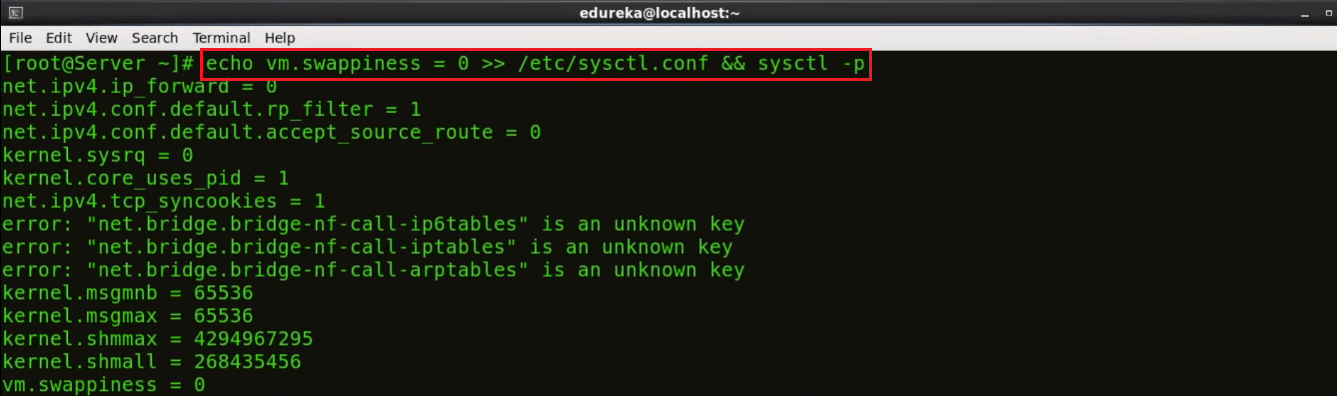
To find the current swappiness settings, type:

cat /proc/sys/vm/swappiness

Swapiness can be a value from 0 to 100. Swappiness near 100 means that the operating system will swap often and usually, too soon. Although swap provides extra resources, RAM is much faster than swap space. Anytime something is moved from RAM to swap, it slows down.

A swappiness value of 0 means that the operating will only rely on swap when it absolutely needs to. We can adjust the swappiness with the sysctl command. To make your VPS automatically apply this setting every time it boots up, you can add the setting to the /etc/sysctl.conf file:

echo vm.swappiness = 0 >> /etc/sysctl.conf && sysctl -p



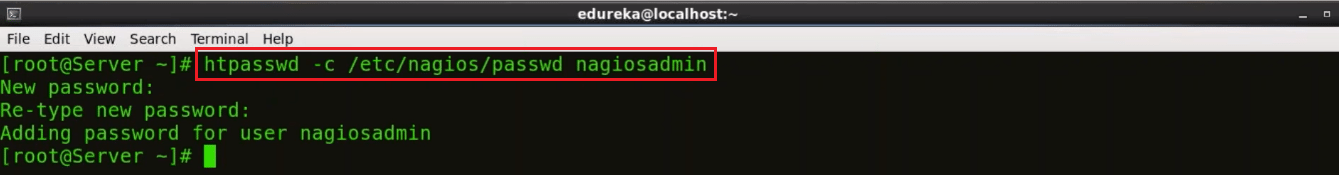
Finally, we are done with the second step.

Let’s proceed further and set Nagios password to access the web interface.

**Step – 3: Set Nagios Password To Access The Web Interface:**

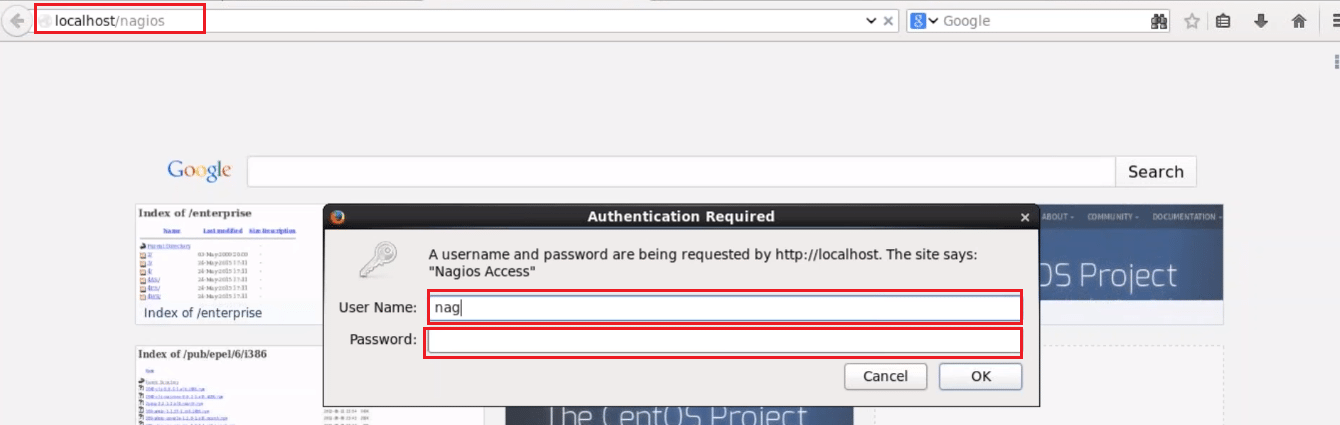
Set the password to access the web interface, use the below command:

htpasswd -c /etc/nagios/passwd nagiosadmin



Type the password and confirm it by retyping it.

Now, open the browser. Here, type your public IP or hostname/nagios. Consider the example below:



Here, give the user name and password. By default, the user name is *nagiosadmin,*and password is what you have set in the previous step. Finally, press OK.

After this, you will directed to Nagios Core dashboard.

**Assignment-3                                                                Marks: 25**

Explain the role of Terraform as Infrastructure as Code and provisioning tool and demonstrate the process to perform the basic operations of Terraform to provision EC2 instance in AWS.

**Solution :**

**Introduction to Terraform:**

Terraform is an infrastructure as code (IaC) tool that allows you to build, change, and version infrastructure safely and efficiently. This includes low-level components such as compute instances, storage, and networking, as well as high-level components such as DNS entries, SaaS features, etc. Terraform can manage both existing service providers and custom in-house solutions.

**Key Features :**

**Infrastructure as Code**:

You describe your infrastructure using Terraform's high-level [configuration language](https://www.terraform.io/docs/language/index.html) in human-readable, declarative configuration files. This allows you to create a blueprint that you can version, share, and reuse.

### [»](https://www.terraform.io/intro/index.html" \l "execution-plans)Execution Plans:

Terraform generates an execution plan describing what it will do and asks for your approval before making any infrastructure changes. This allows you to review changes before Terraform creates, updates, or destroys infrastructure.

### [»](https://www.terraform.io/intro/index.html" \l "resource-graph)Resource Graph:

Terraform builds a resource graph and creates or modifies non-dependent resources in parallel. This allows Terraform to build resources as efficiently as possible and gives you greater insight into your infrastructure.

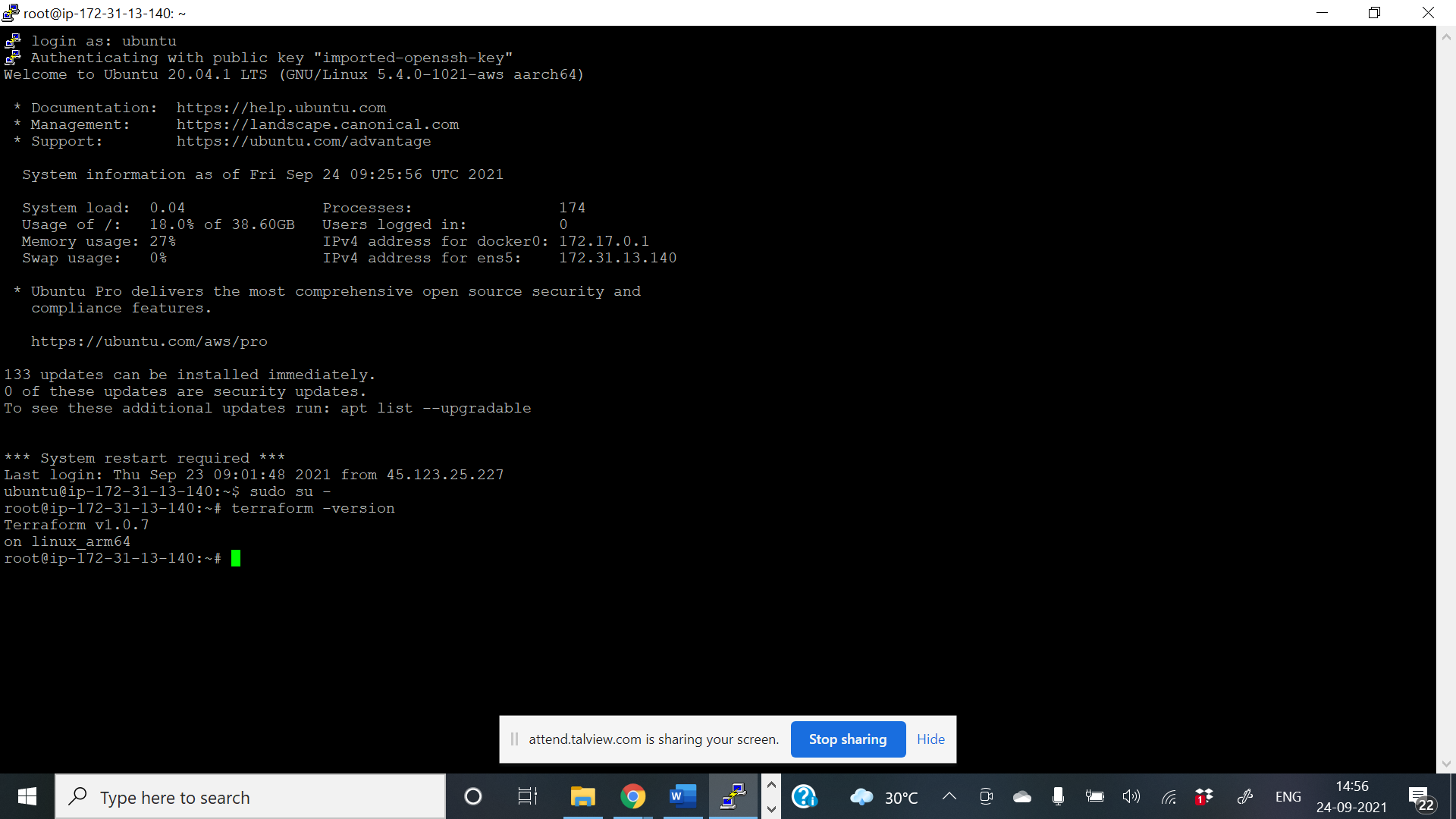
### [»](https://www.terraform.io/intro/index.html" \l "change-automation)Change Automation:

Terraform can apply complex changesets to your infrastructure with minimal human interaction. When you update configuration files, Terraform determines what changed and creates incremental execution plans that respect dependencies.

*Demonstrate the process to perform the basic operations of Terraform to provision EC2 instance in AWS*

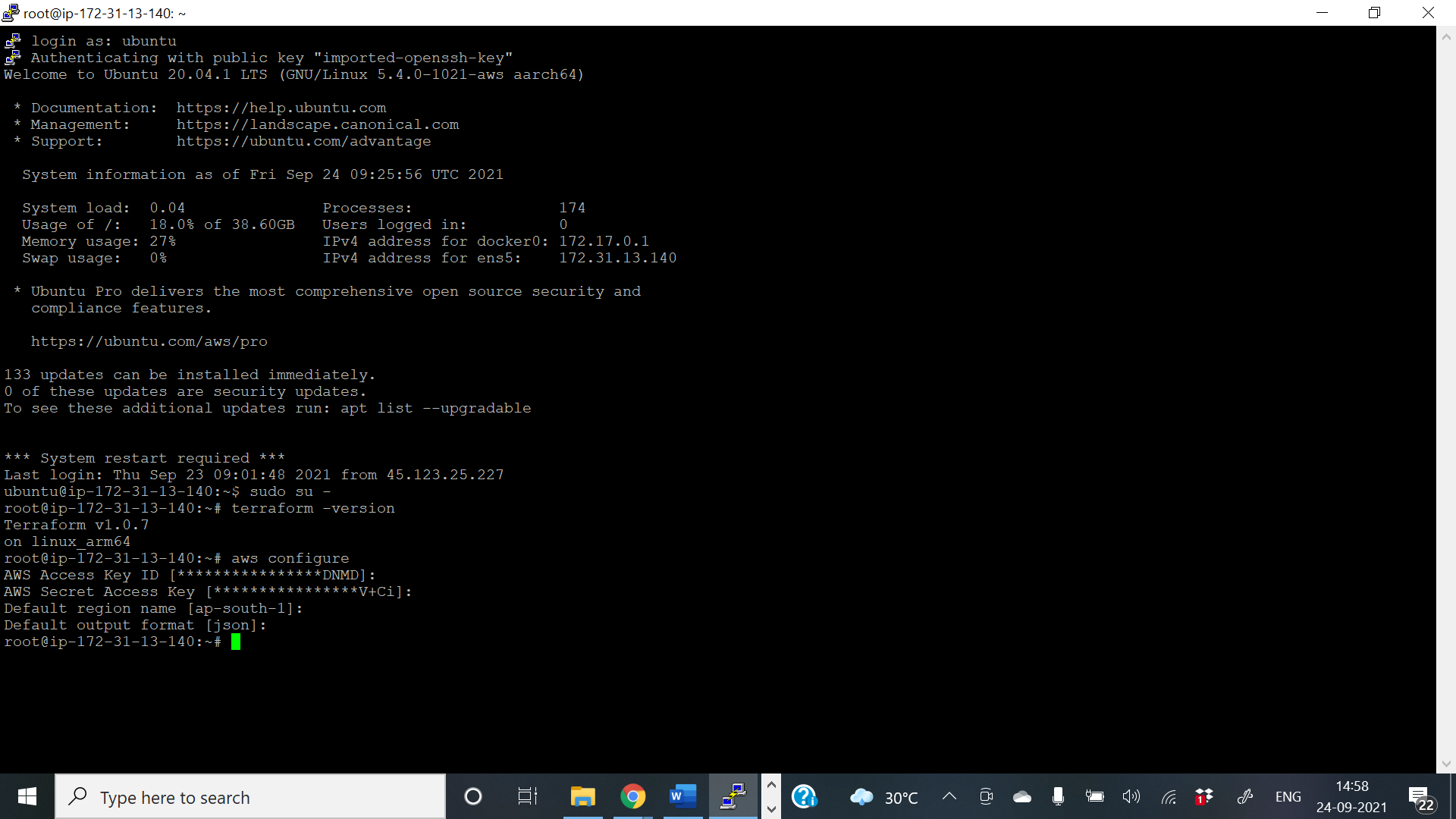
Commands to in install Terraform:

**sudo apt-get update && sudo apt-get install terraform**



**Build Infrastucre :**

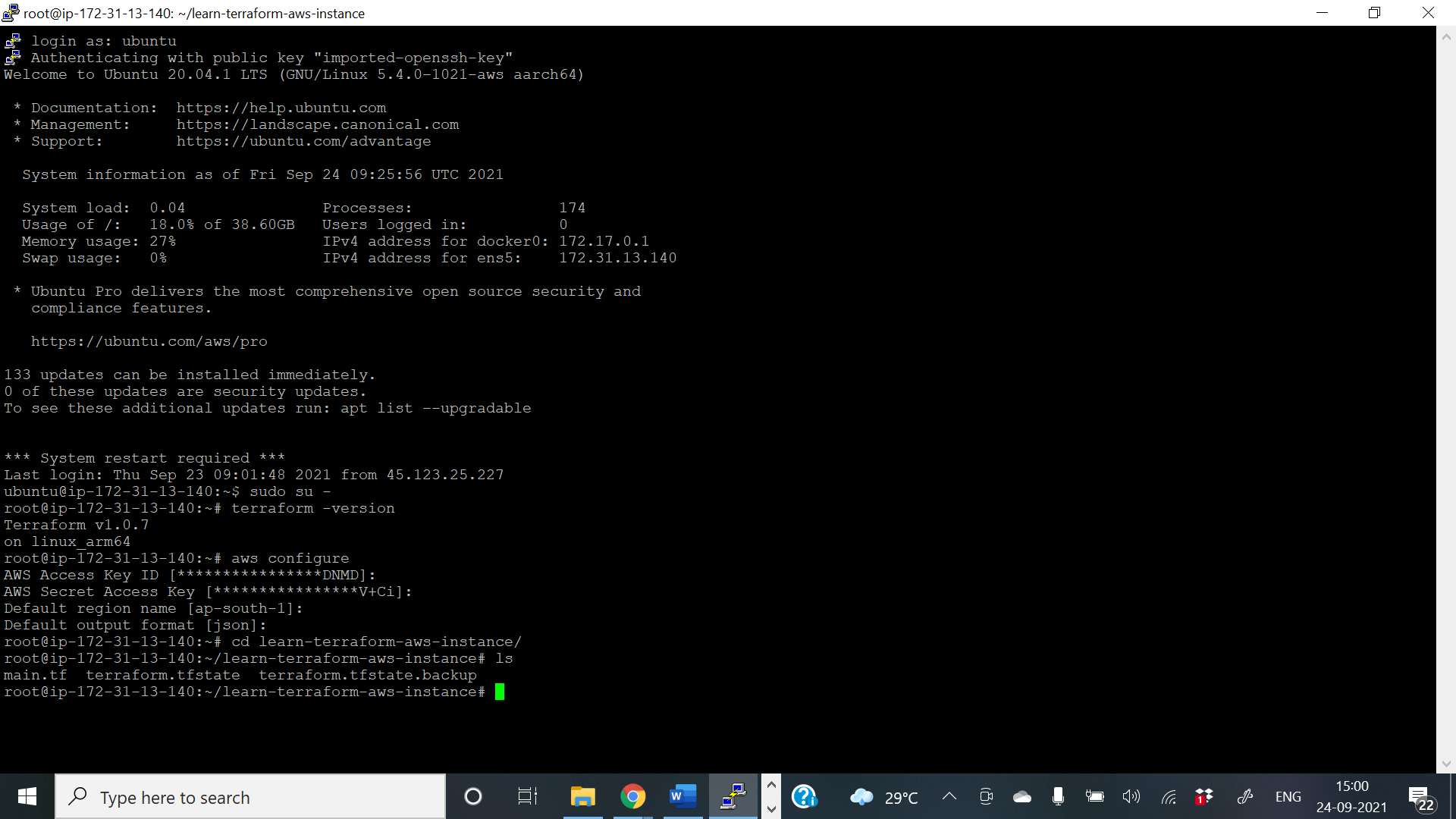
* **aws configure**

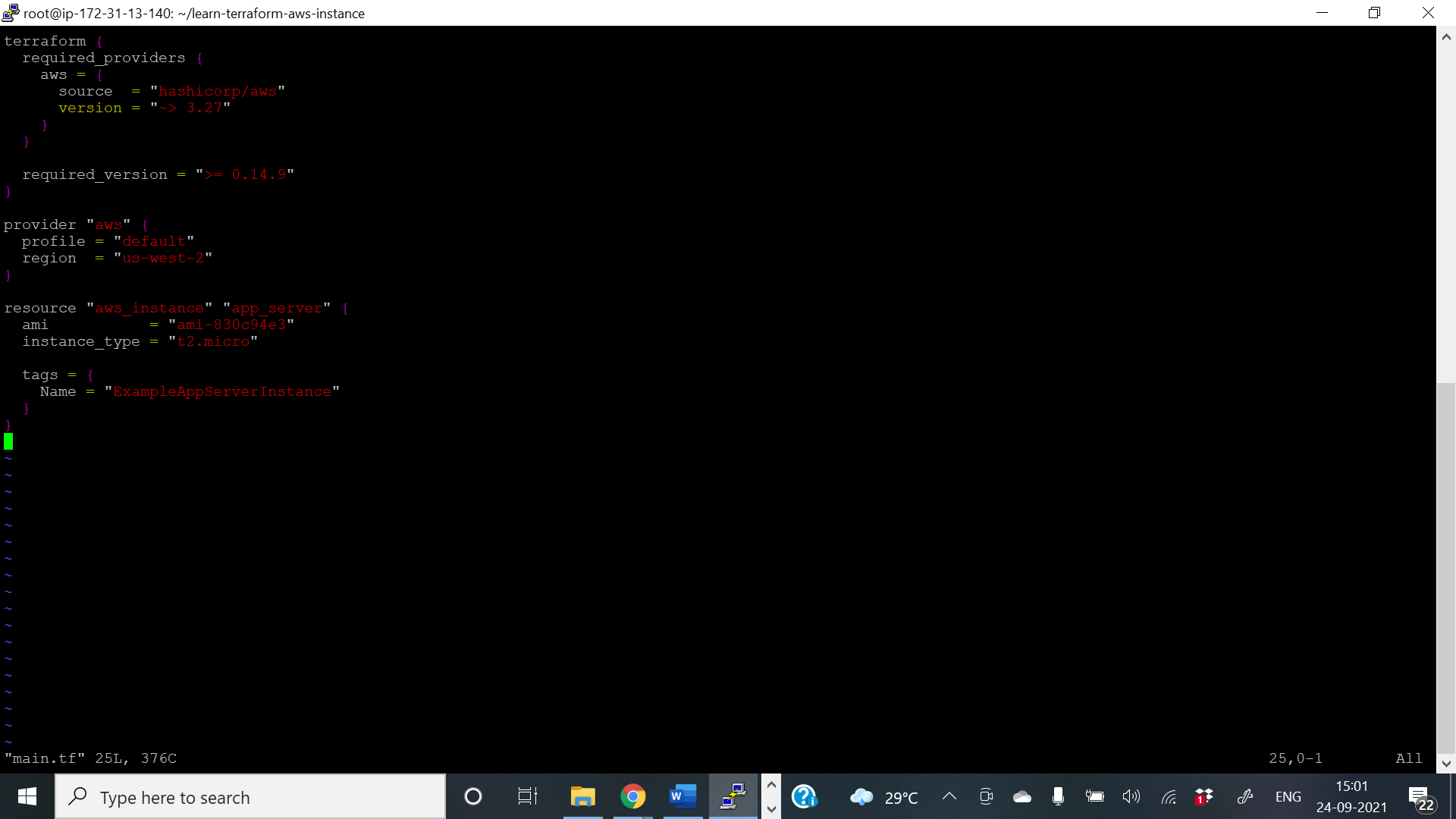


**mkdir learn-terraform-aws-instance**

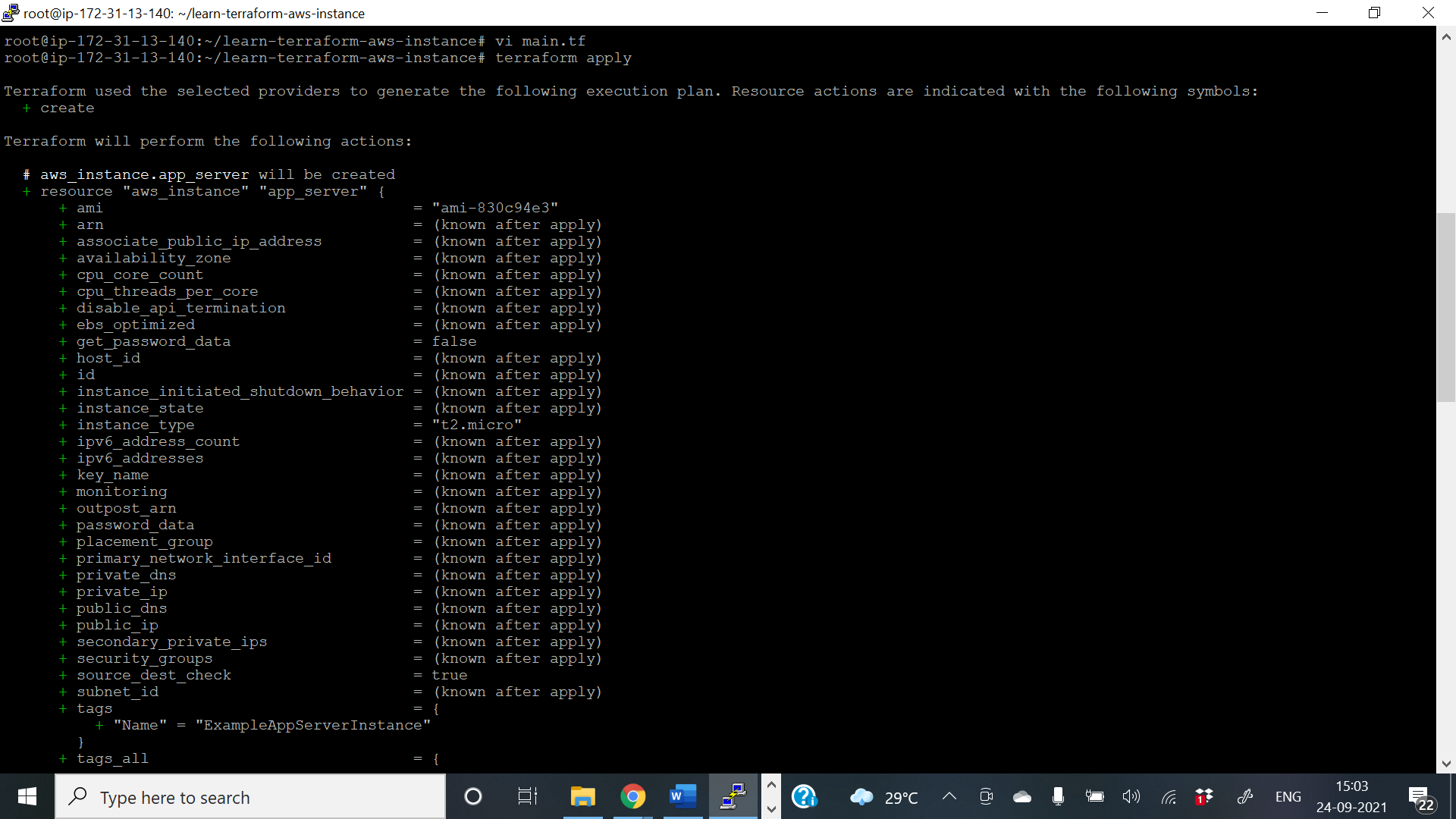
**cd learn-terraform-aws-instance**

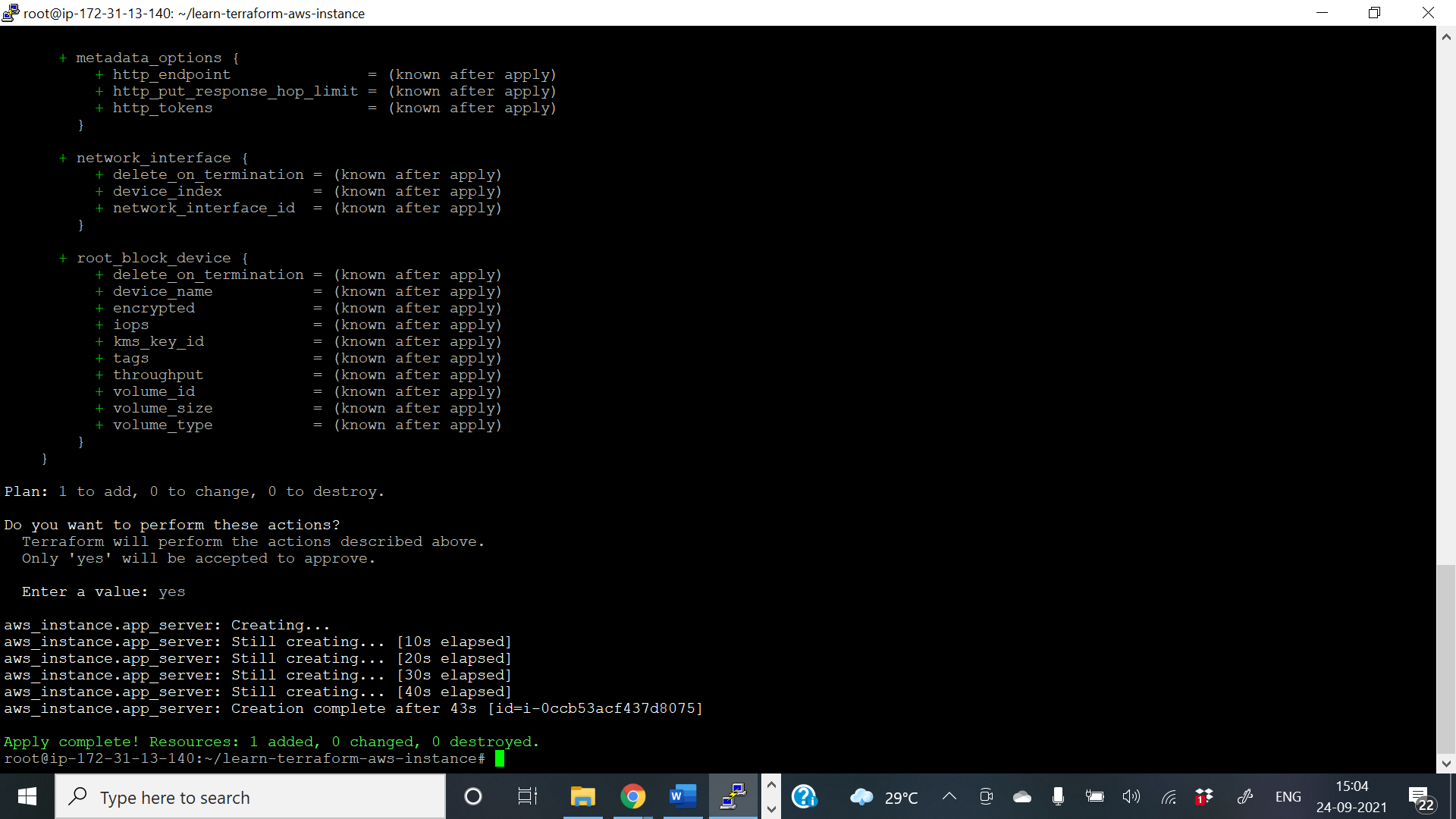
**touch main.tf**

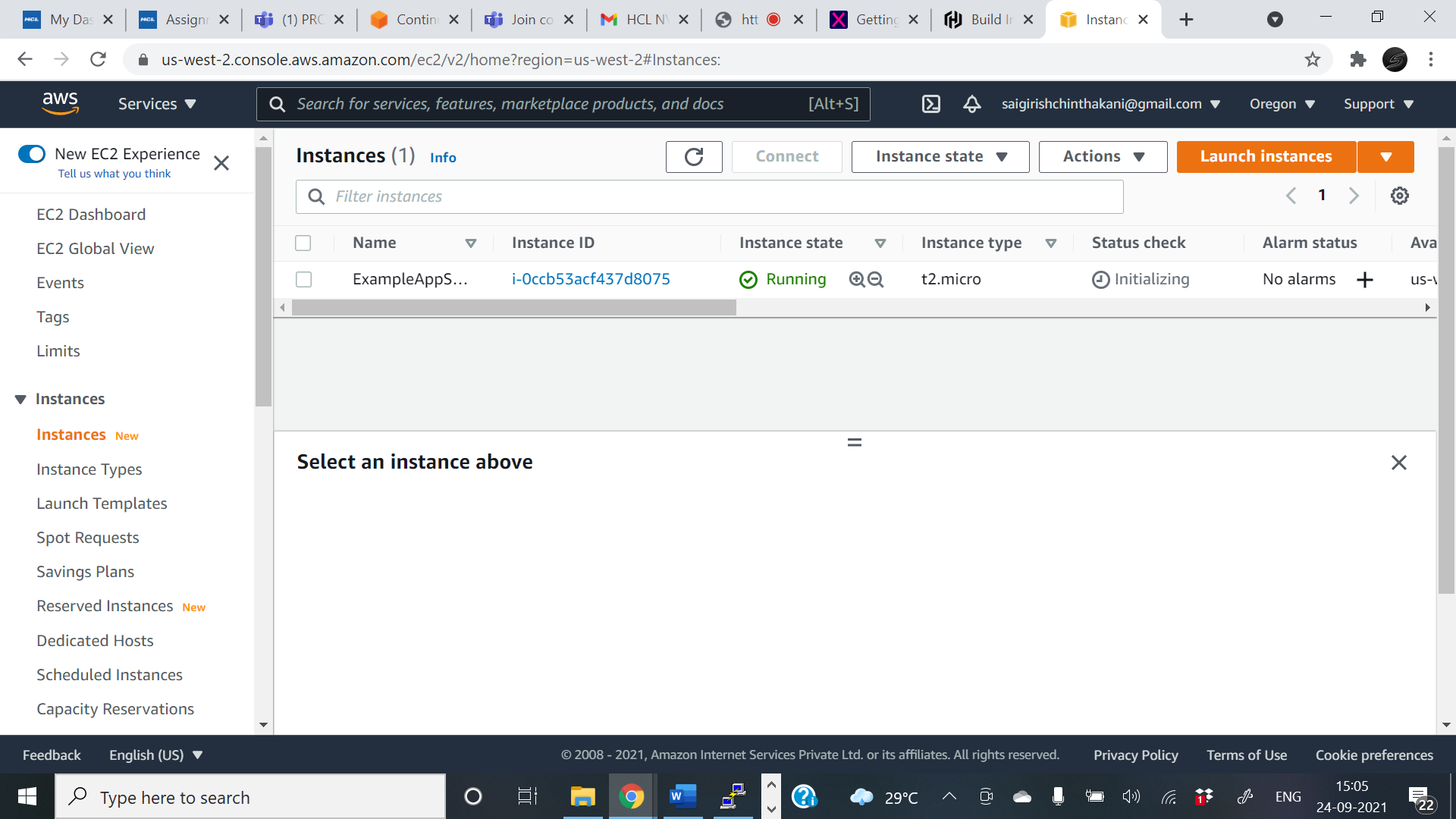




**terraform apply**







**terraform destroy**

