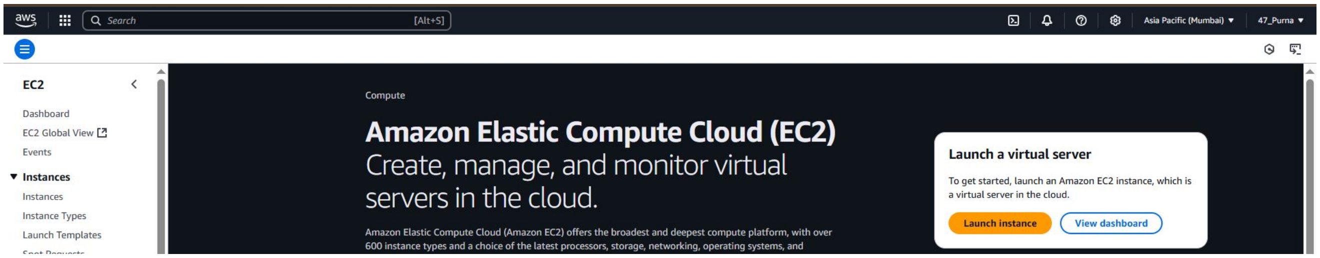
ASSIGNMENT NO :- 12: Deploy and run the project in AWS without using the port.

STEP 1 :- Go to the EC2 site and click on Launch instance.



Compute

Amazon Elastic Compute Cloud (EC2)

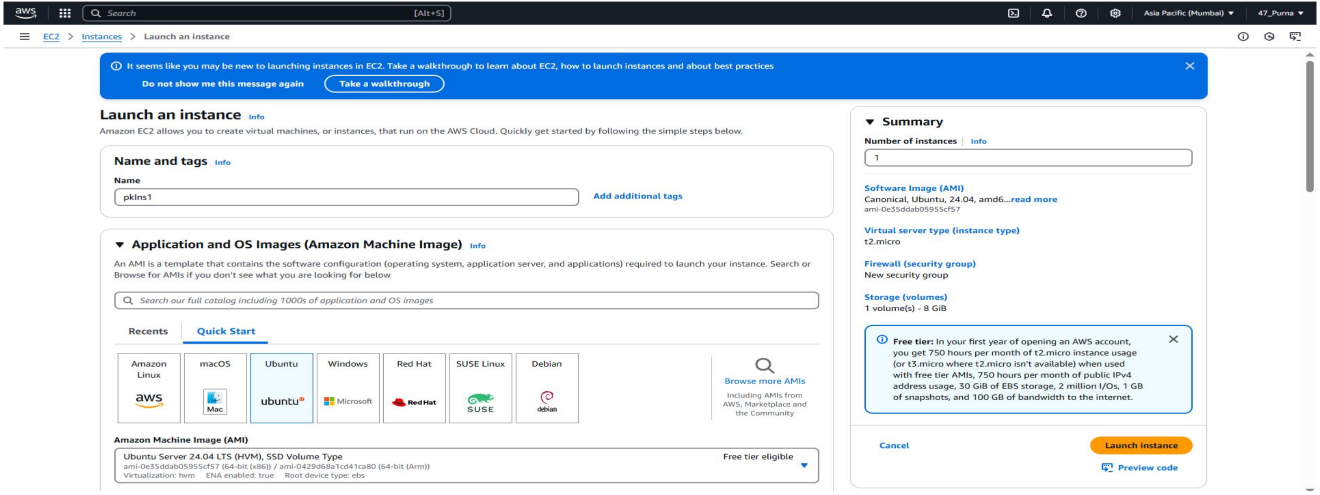
Create, manage, and monitor virtual servers in the cloud.

Amazon Elastic Compute Cloud (Amazon EC2) offers the broadest and deepest compute platform, with over 600 instance types and a choice of the latest processors, storage, networking, operating systems, and

Launch a virtual server

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

STEP 2 :- Give your instance a name and then select Ubuntu.



It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name: pkIns1

▼ Application and OS Images (Amazon Machine Image)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-0e35ddab05955cf57 (64-bit (x86)) / ami-0429d68a1cd41ca80 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

▼ Summary

Number of instances: 1

Software Image (AMI): Canonical, Ubuntu, 24.04, amd6...read more
ami-0e35ddab05955cf57

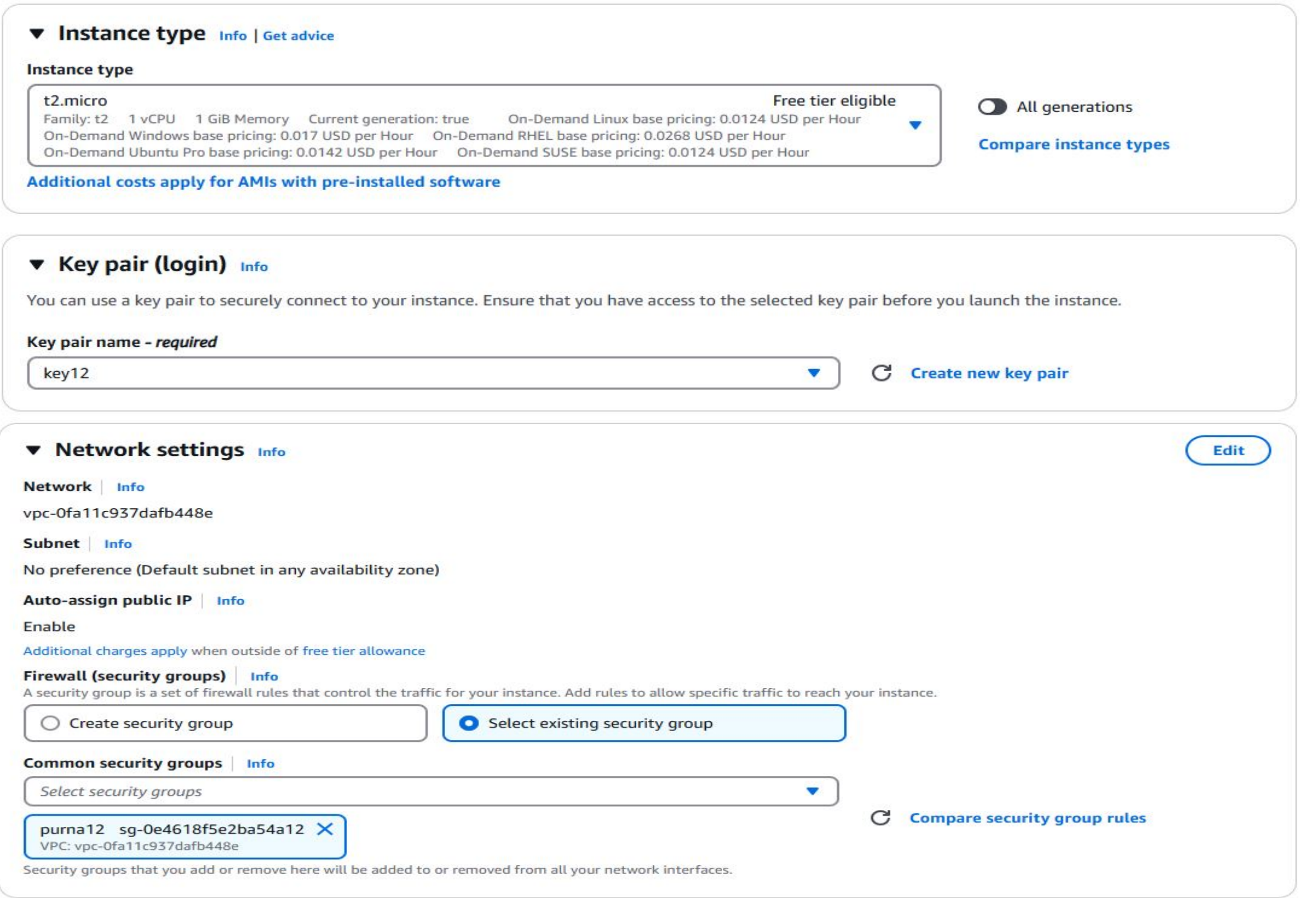
Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

STEP 3 :- Create or Select a key pair Then select Select existing security group and then choose your security group.



▼ Instance type

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Windows base pricing: 0.017 USD per Hour On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour On-Demand SUSE base pricing: 0.0124 USD per Hour

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*: key12

▼ Network settings

Network: vpc-0fa11c937dafb448e

Subnet: No preference (Default subnet in any availability zone)

Auto-assign public IP: Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

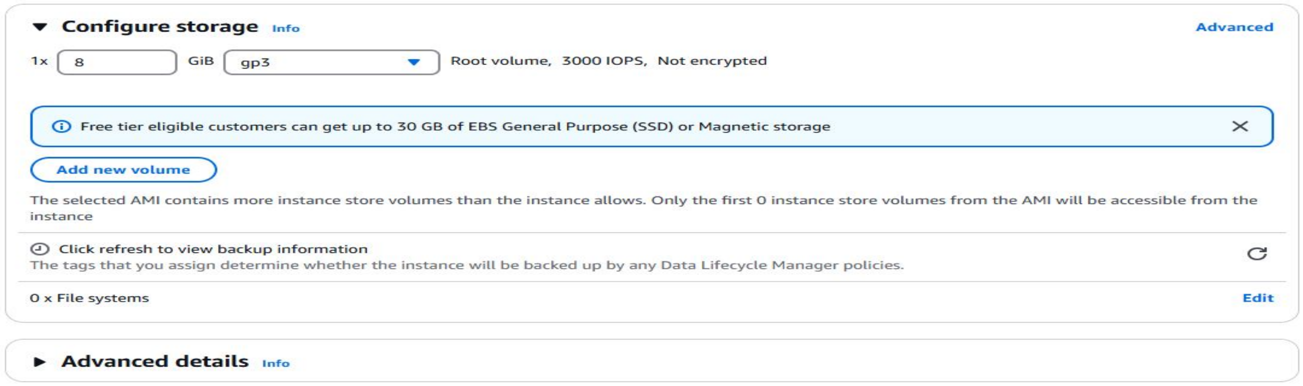
Common security groups: Select security groups

purna12 sg-0e4618f5e2ba54a12 ✕
VPC: vpc-0fa11c937dafb448e

Security groups that you add or remove here will be added to or removed from all your network interfaces.

STEP 4 :- Then click on Advanced options and then go to User data and then Write the following commands given below in User data and click on Launch Instance in Right hand bottom of page.

>> Give your Github Repository where you have stored the index.js file



▼ Configure storage Info

Advanced

1x 8 GiB gp3 ▼ Root volume, 3000 IOPS, Not encrypted

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage ✕

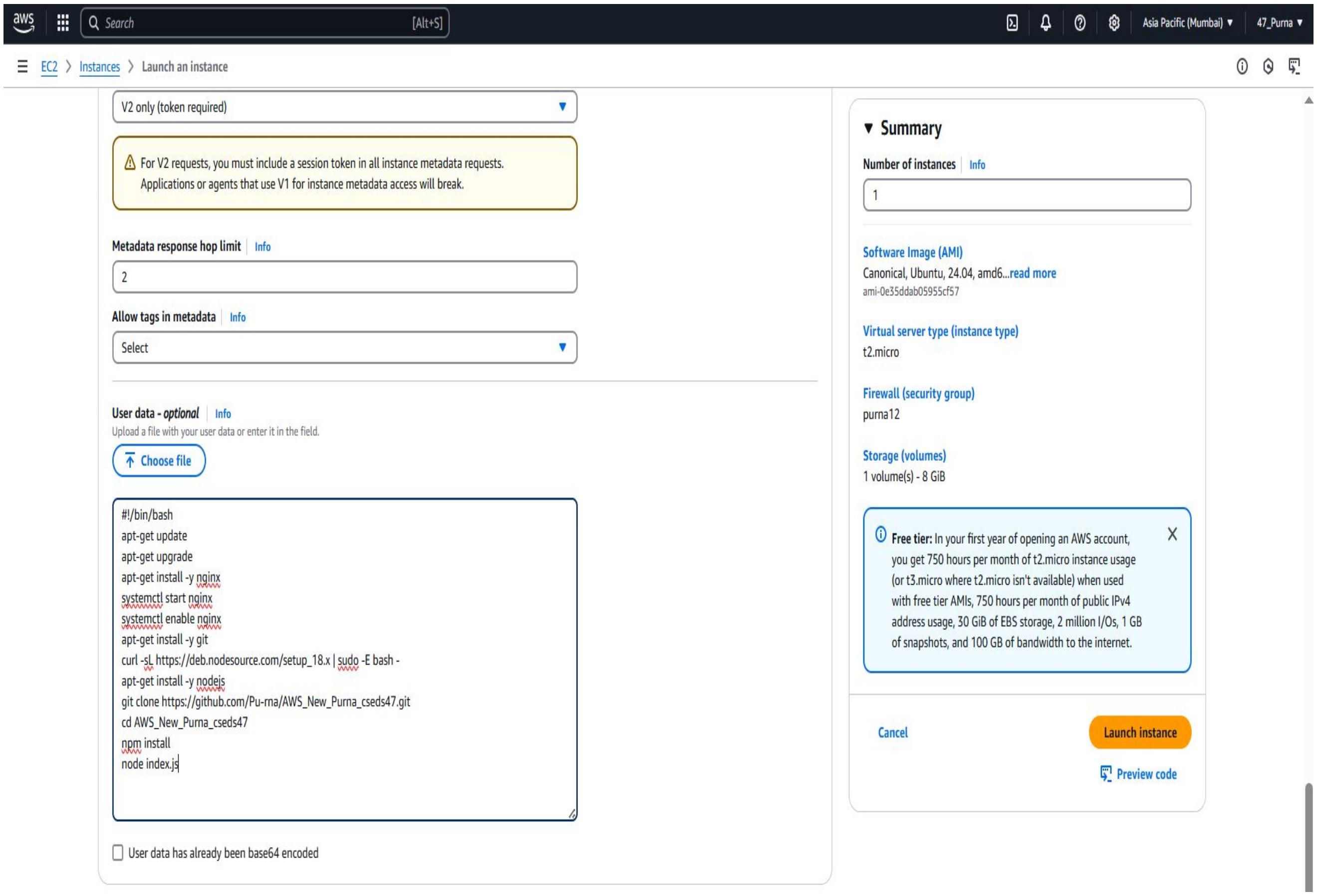
Add new volume

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

► Advanced details Info



V2 only (token required) ▼

⚠ For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.

Metadata response hop limit | Info
2

Allow tags in metadata | Info
Select ▼

User data - *optional* | Info
Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
apt-get update
apt-get upgrade
apt-get install -y nginx
systemctl start nginx
systemctl enable nginx
apt-get install -y git
curl -sL https://deb.nodesource.com/setup_18.x | sudo -E bash -
apt-get install -y nodejs
git clone https://github.com/Pu-rna/AWS_New_Purna_cseds47.git
cd AWS_New_Purna_cseds47
npm install
node index.js
```

□ User data has already been base64 encoded

▼ Summary

Number of instances | Info
1

Software Image (AMI)
Canonical, Ubuntu, 24.04, amd6...read more
ami-0e35ddab05955cf57

Virtual server type (instance type)
t2.micro

Firewall (security group)
purna12

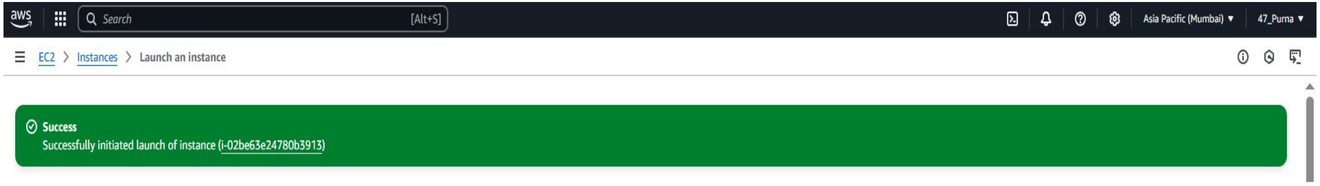
Storage (volumes)
1 volume(s) - 8 GiB

ⓘ **Free tier:** In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. X

Cancel Launch instance

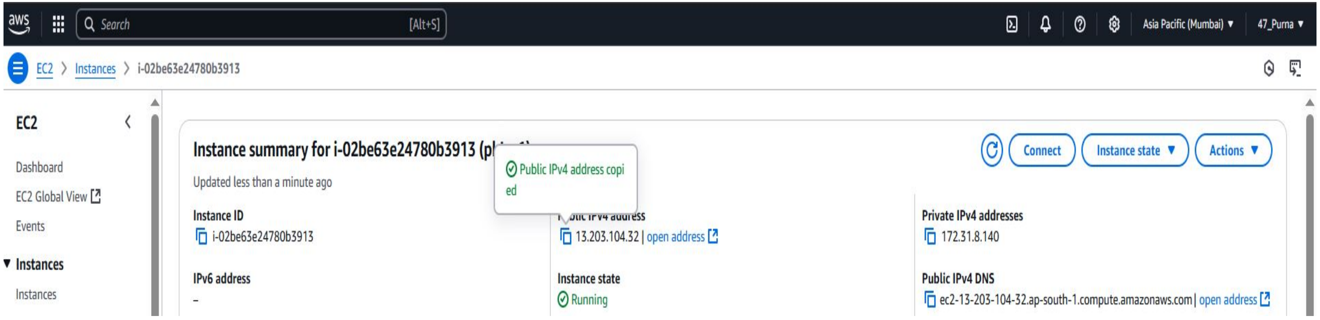
Preview code

>> And your Instance is Successfully Launched.



Success
Successfully initiated launch of instance (i-02be63e24780b3913)

STEP 5 :- Click on the Instance ID and copy the Public IPV4 Address.



Instance summary for i-02be63e24780b3913 (pl

✓ Public IPv4 address copied

Updated less than a minute ago

Instance ID
i-02be63e24780b3913

Public IPv4 address
13.203.104.32 | open address

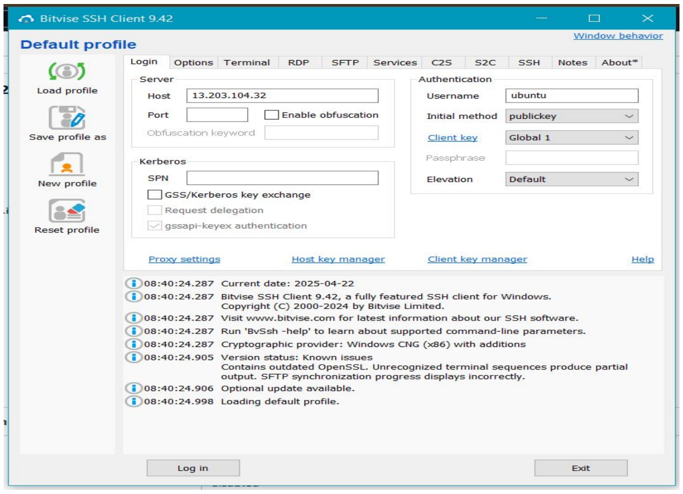
Private IPv4 addresses
172.31.8.140

IPv6 address
–

Instance state
✓ Running

Public IPv4 DNS
ec2-13-203-104-32.ap-south-1.compute.amazonaws.com | open address

STEP 6 :- Open the Bitvise SSH Client Server and paste the Public IPV4 Address in the Host then import your Key from Client key manager and all other features will same.

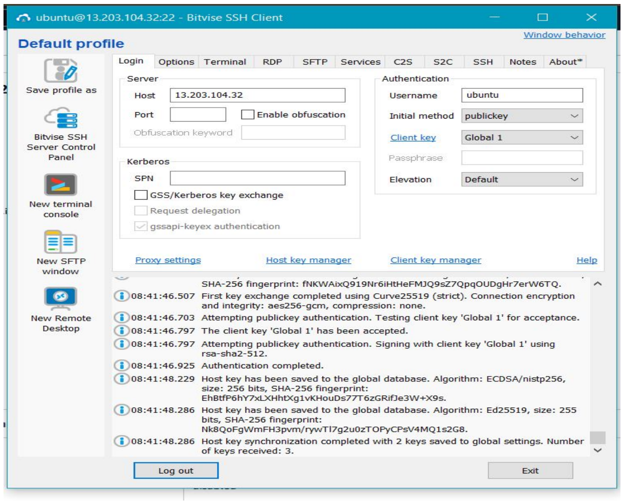


Server
Host: 13.203.104.32
Port:
□ Enable obfuscation
Obfuscation keyword:

Kerberos
SPN:
□ GSS/Kerberos key exchange
□ Request delegation
☑ gssapi-keyex authentication

Authentication
Username: ubuntu
Initial method: publickey
Client key: Global 1
Passphrase:
Elevation: Default

```
08:40:24.287 Current date: 2025-04-22
08:40:24.287 Bitvise SSH Client 9.42, a fully featured SSH client for Windows.
             Copyright (C) 2000-2024 by Bitvise Limited.
08:40:24.287 Visit www.bitvise.com for latest information about our SSH software.
08:40:24.287 Run 'BvSsh -help' to learn about supported command-line parameters.
08:40:24.287 Cryptographic provider: Windows CNG (x86) with additions
08:40:24.905 Version status: Known issues
             Contains outdated OpenSSL. Unrecognized terminal sequences produce partial
             output. SFTP synchronization progress displays incorrectly.
08:40:24.906 Optional update available.
08:40:24.998 Loading default profile.
```



Server
Host: 13.203.104.32
Port:
□ Enable obfuscation
Obfuscation keyword:

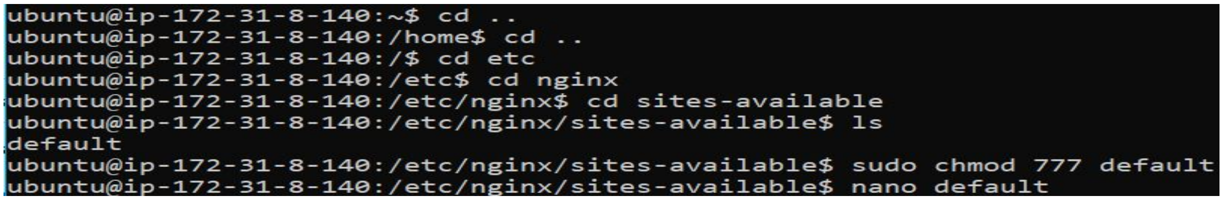
Kerberos
SPN:
□ GSS/Kerberos key exchange
□ Request delegation
☑ gssapi-keyex authentication

Authentication
Username: ubuntu
Initial method: publickey
Client key: Global 1
Passphrase:
Elevation: Default

```
             SHA-256 fingerprint: fNKWAixQ919Nr6iHtHeFMJQ9sZ7QpqOUDgHr7erW6TQ.
08:41:46.507 First key exchange completed using Curve25519 (strict). Connection encryption
             and integrity: aes256-gcm, compression: none.
08:41:46.703 Attempting publickey authentication. Testing client key 'Global 1' for acceptance.
08:41:46.797 The client key 'Global 1' has been accepted.
08:41:46.797 Attempting publickey authentication. Signing with client key 'Global 1' using
             rsa-sha2-512.
08:41:46.925 Authentication completed.
08:41:48.229 Host key has been saved to the global database. Algorithm: ECDSA/nistp256,
             size: 256 bits, SHA-256 fingerprint:
             EhBtfP6hY7xLXHhtXg1vKHouDs77T6zGRifJe3W+X9s.
08:41:48.286 Host key has been saved to the global database. Algorithm: Ed25519, size: 255
             bits, SHA-256 fingerprint:
             Nk8QoFgWmFH3pvm/rywTl7g2u0zTOPyCPsV4MQ1s2G8.
08:41:48.286 Host key synchronization completed with 2 keys saved to global settings. Number
             of keys received: 3.
```

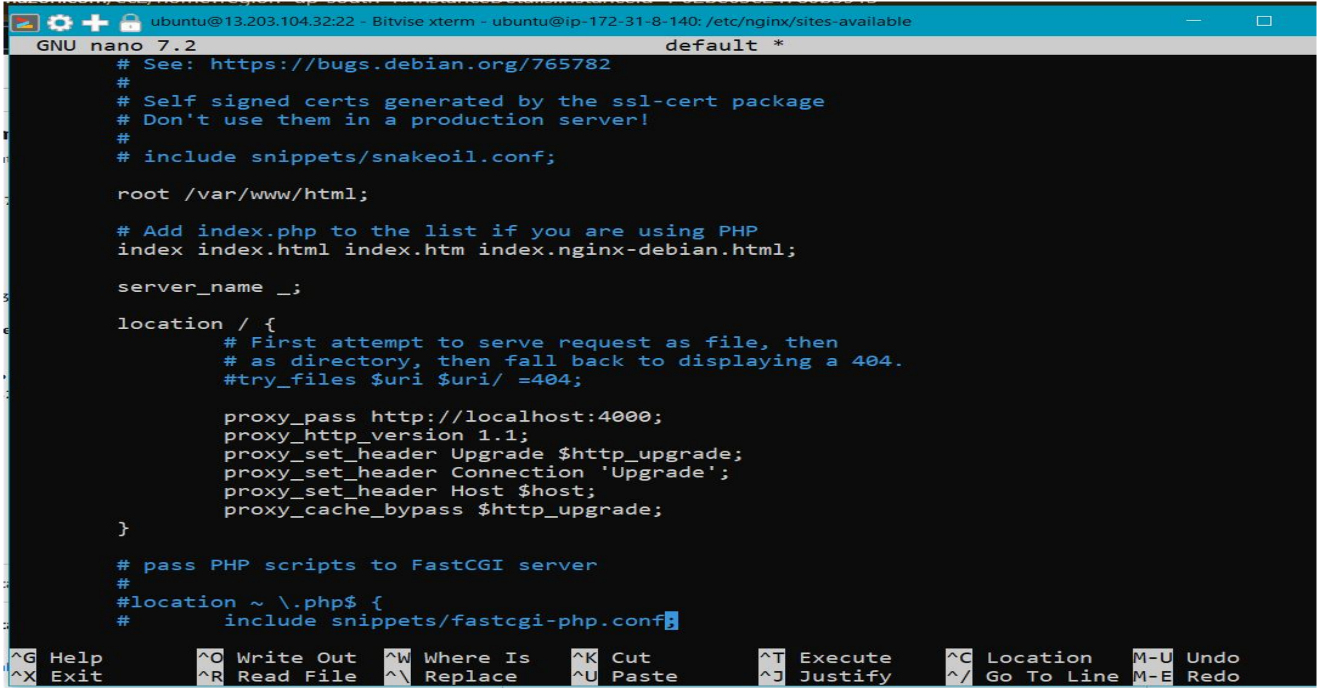
STEP 7 :- Then write the following command in the terminal :

- Go to the root terminal
- Move to folder etc
- Then move to nginx
- Then go to sites-available
- Change the mode of the default file to writable
- Edit the default file



```
ubuntu@ip-172-31-8-140:~$ cd ..
ubuntu@ip-172-31-8-140:/home$ cd ..
ubuntu@ip-172-31-8-140:/$ cd etc
ubuntu@ip-172-31-8-140:/etc$ cd nginx
ubuntu@ip-172-31-8-140:/etc/nginx$ cd sites-available
ubuntu@ip-172-31-8-140:/etc/nginx/sites-available$ ls
default
ubuntu@ip-172-31-8-140:/etc/nginx/sites-available$ sudo chmod 777 default
ubuntu@ip-172-31-8-140:/etc/nginx/sites-available$ nano default
```

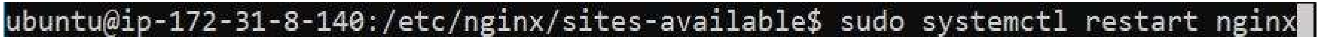
STEP 8 :- Then write the following code in the default file under server_name_ location/ and save the file :



ubuntu@13.203.104.32:22 - Bitvise xterm - ubuntu@ip-172-31-8-140: /etc/nginx/sites-available

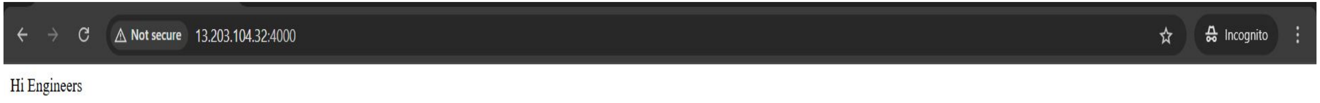
```
  GNU nano 7.2                                    default *
        # See: https://bugs.debian.org/765782
        #
        # Self signed certs generated by the ssl-cert package
        # Don't use them in a production server!
        #
        # include snippets/snakeoil.conf;

        root /var/www/html;

        # Add index.php to the list if you are using PHP
        index index.html index.htm index.nginx-debian.html;

        server_name _;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.
                #try_files $uri $uri/ =404;

                proxy_pass http://localhost:4000;
                proxy_http_version 1.1;
                proxy_set_header Upgrade $http_upgrade;
                proxy_set_header Connection 'Upgrade';
                proxy_set_header Host $host;
                proxy_cache_bypass $http_upgrade;
        }

        # pass PHP scripts to FastCGI server
        #
        #location ~ \.php$ {
        #       include snippets/fastcgi-php.conf;

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo
```

STEP 9 :- Then go back to the terminal and run the file as sudosystemctl restart nginx.



```
ubuntu@ip-172-31-8-140:/etc/nginx/sites-available$ sudo systemctl restart nginx
```

STEP 10:- Again copy the instance IPV4 Address and run in incognito website and you can see your Webpage.



Hi Engineers