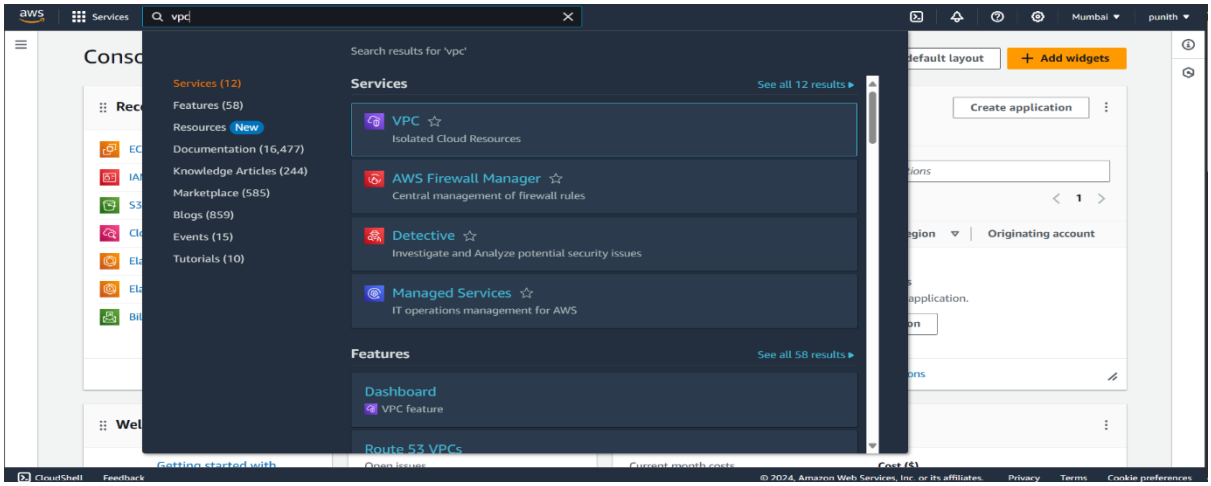
VPC(Virtual Private Cloud)

- VPC stands for Virtual Private Cloud and it is a private cloud that can be created inside a public cloud. It can be used in our own data centres and availability zones.By default, AWS provides a default VPC for every user.
- VPC contains components like IP Addresses, Subnets, Route-Table, Security Groups, NACL, Internet Gateways, NAT etc..
  Each component have been explained in detail below:

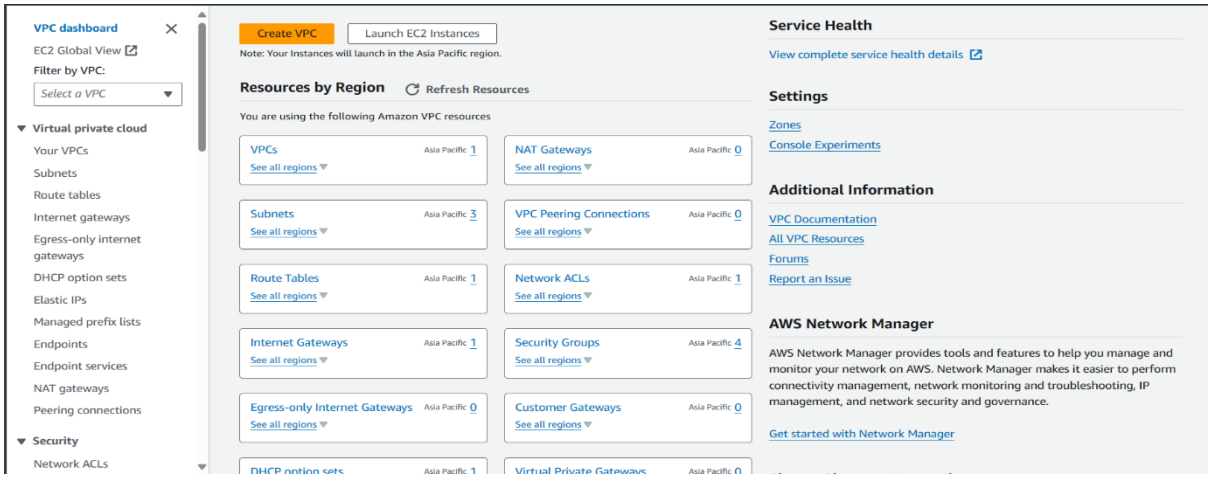
- IP Address: IP Address allows users to connect to internet or server.AWS provides IPV4 and IPV6 addresses that are CIDR.
- Subnet: The subnets defines the range of ip address of each ec2.Here, We have public subnets and private subnets.
- Route-Table: Route Tables helps to direct the network traffic from subnets, gateways.
- Security Groups: These security groups helps to control the traffic at an ec2 from inbound and outbound rules.
- NACL: NACL stands for Network Access Control List and they allows or denies specific traffic at the subnet level.
- NAT: NAT stands for Network Address Translation and NAT helps to connect and access the resources and services like ec2 from outside the VPC with private subnet.
- Internet Gateways: Allows communication between the VPC and Internet.

- Now, We see how to create a custom VPC and attach to EC2 and deploy the EC2 on server with photos attached below:

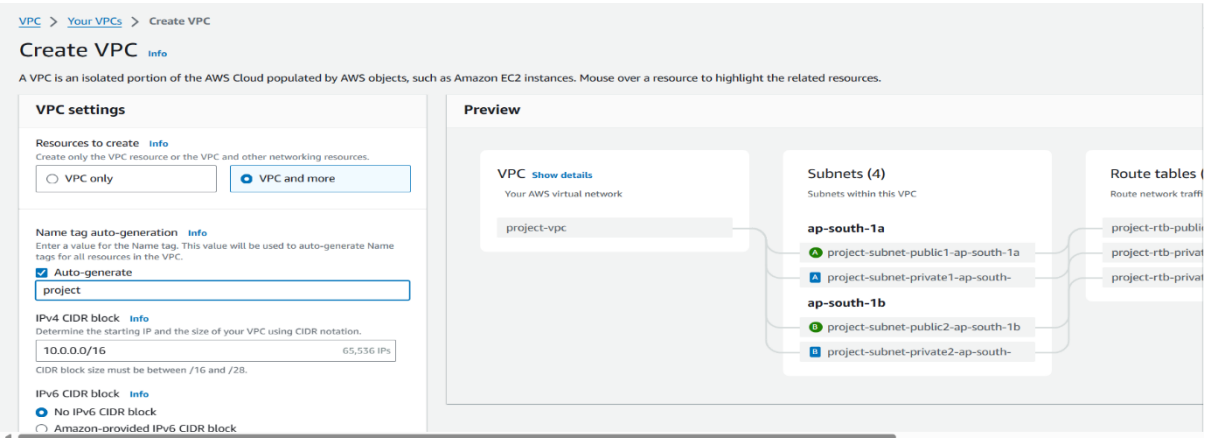
Login to AWS console and search for VPC.



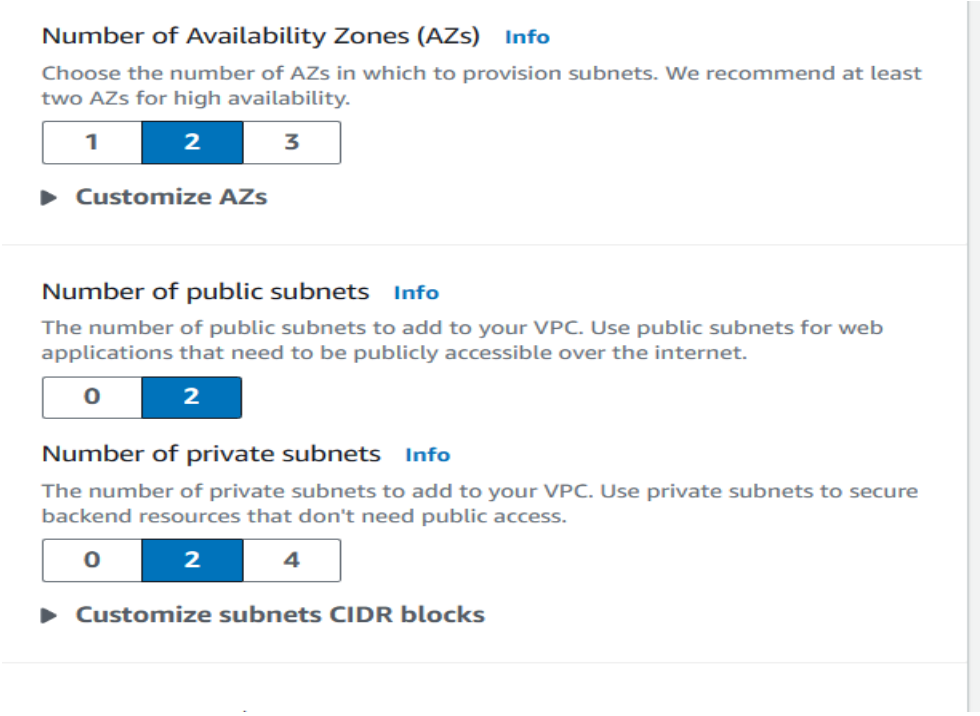
This is how VPC dashboard looks like. Choose create VPC.



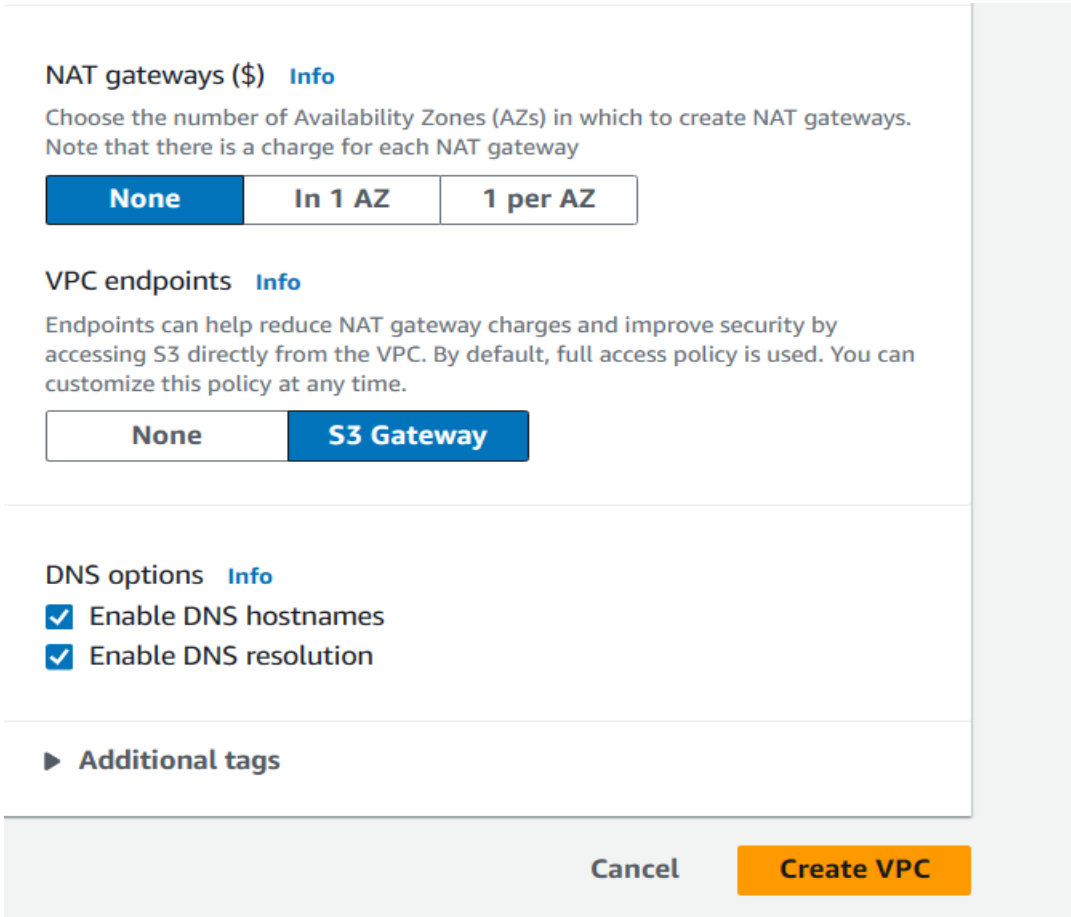
Choose VPC and more and name the VPC.



Select the no.of availability zones,Public and Private subnets to be created.

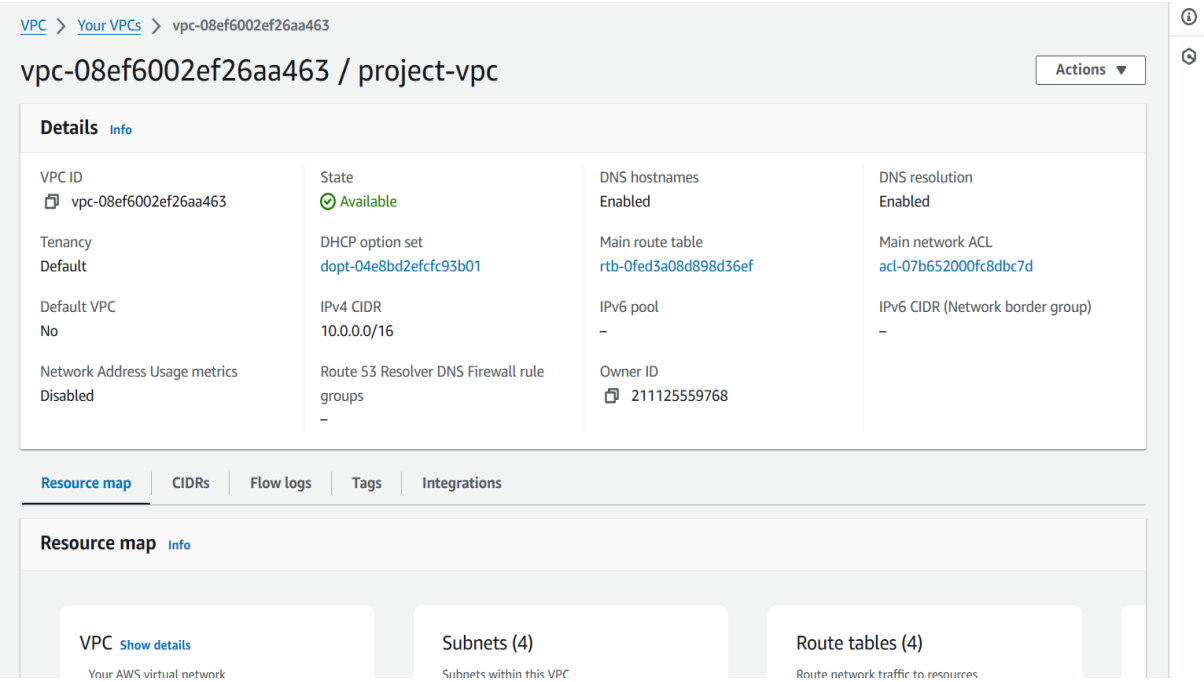


Choose the default settings and enable the DNS options.Choose create VPC.

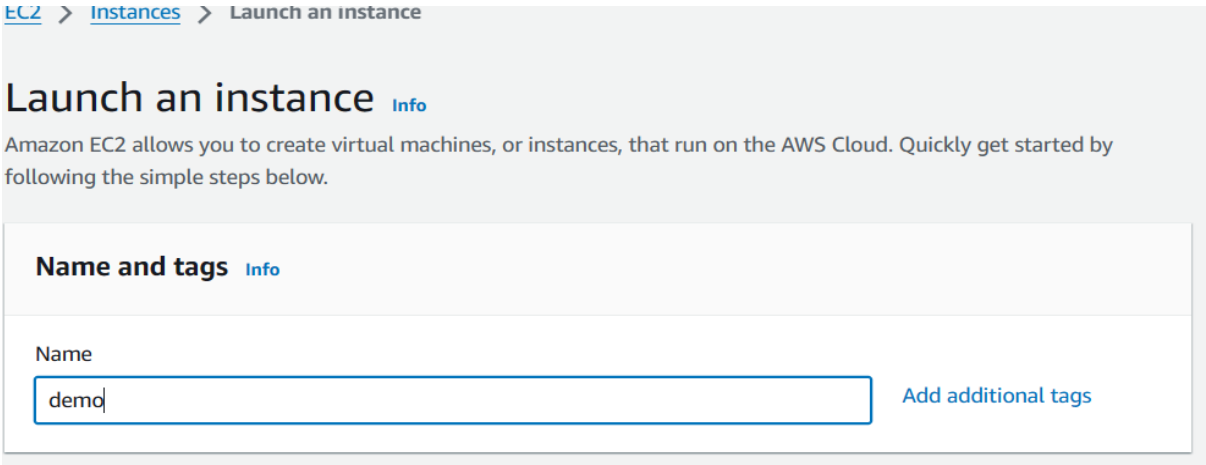


One by one, the VPC configuration gets created. Choose view VPC.

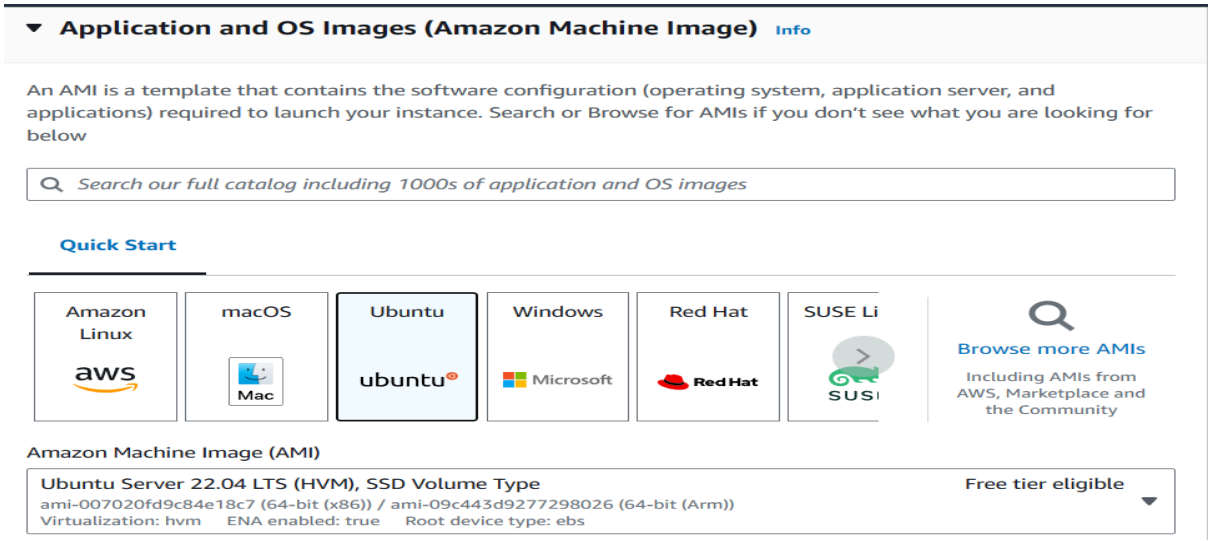
You can see the overview of the VPC created.



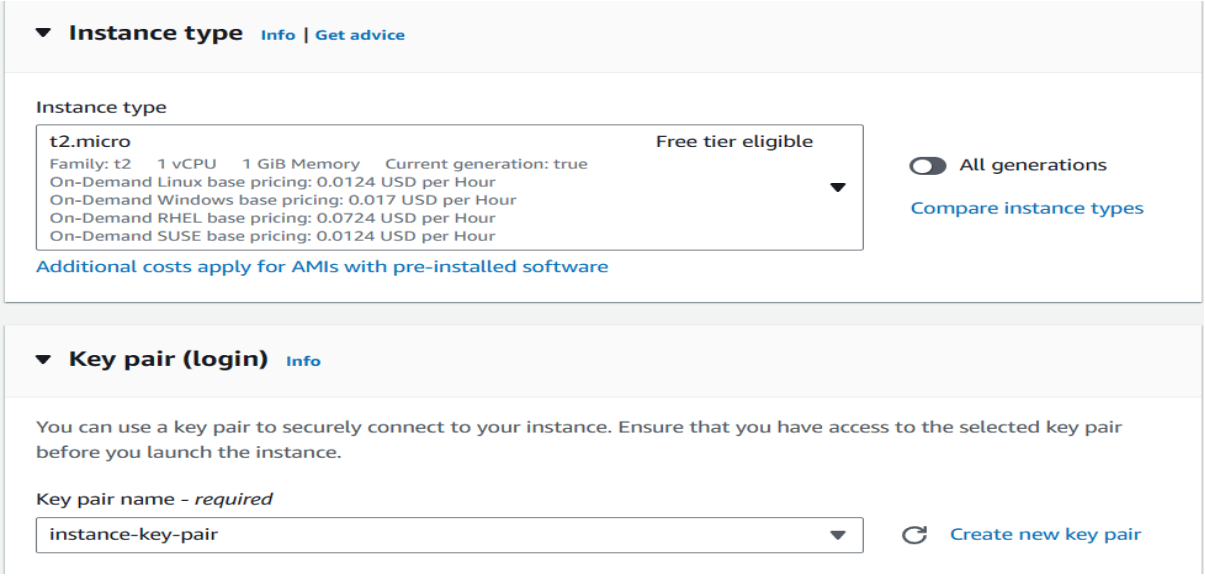
Comeback to EC2 and Launch an instance.



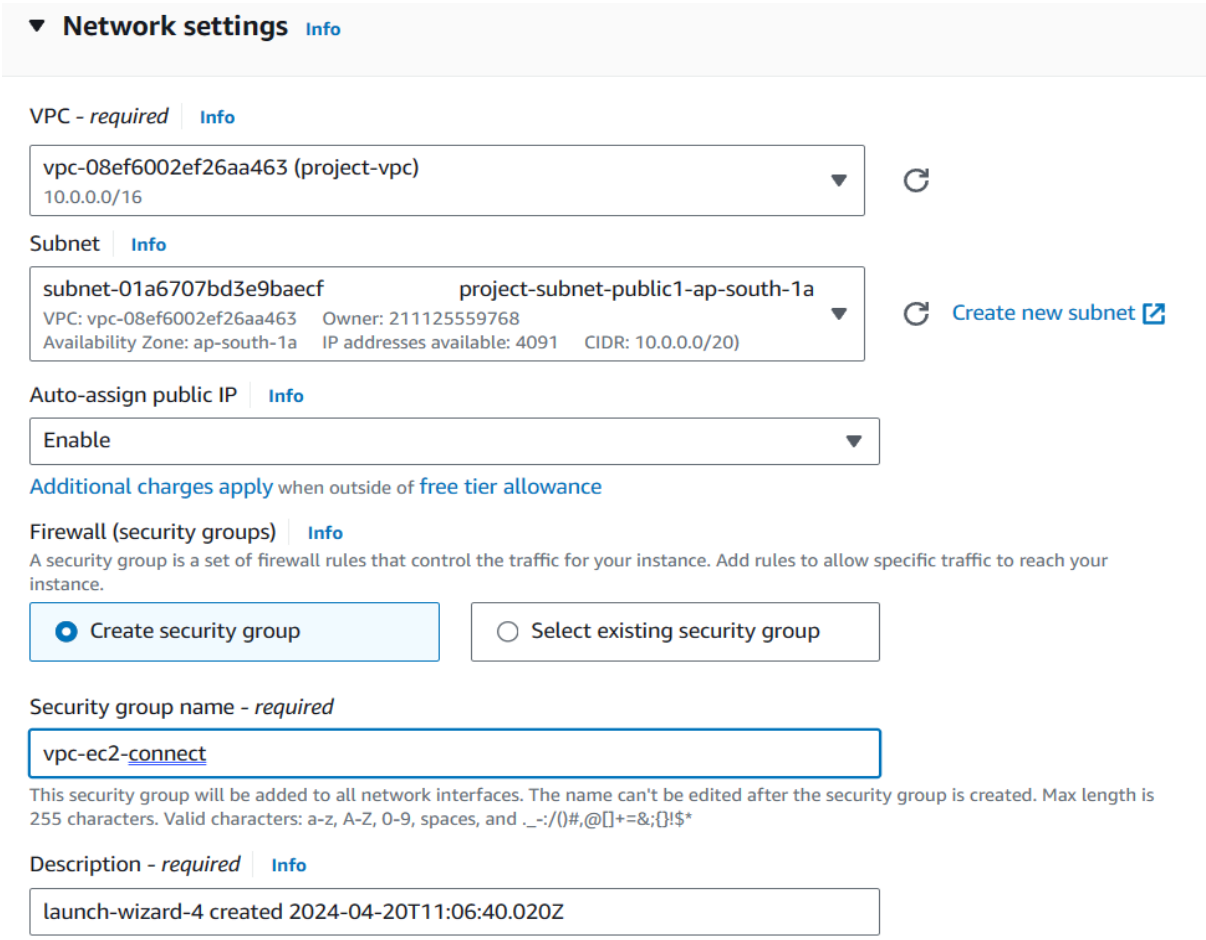
Choose ubuntu and it's version.



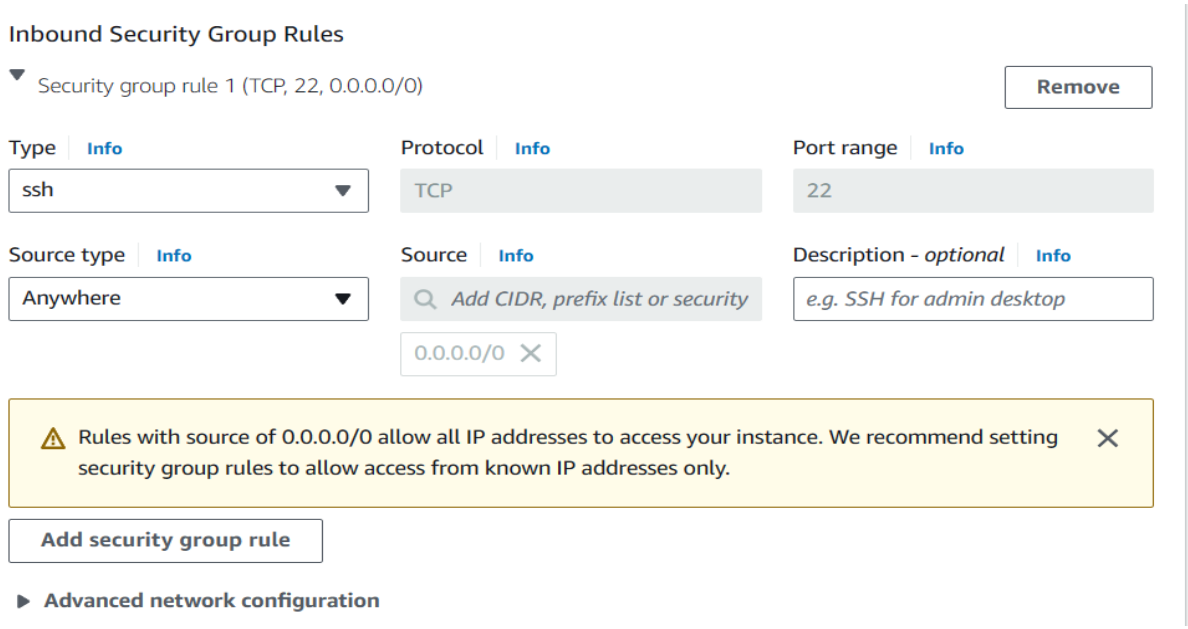
Choose instance type and the key-pair.



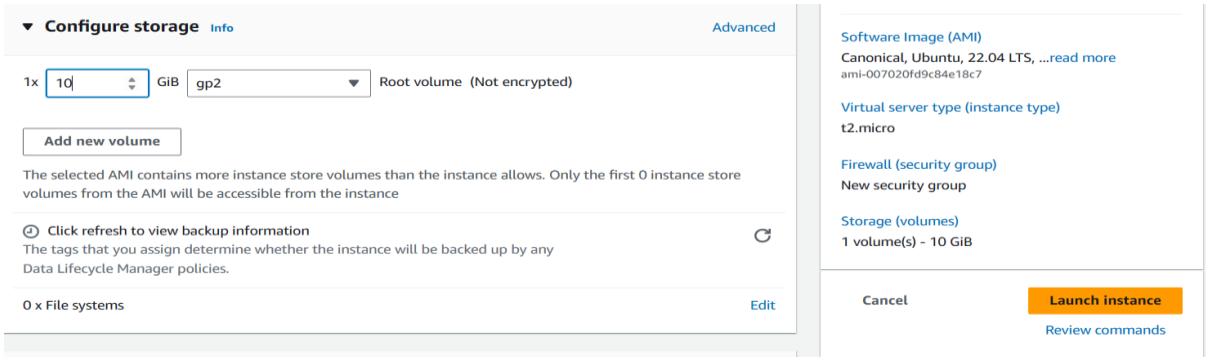
Here, We have choose our VPC created,public subnet and enable auto-assign public IP. Choose to create a new security group and name it.



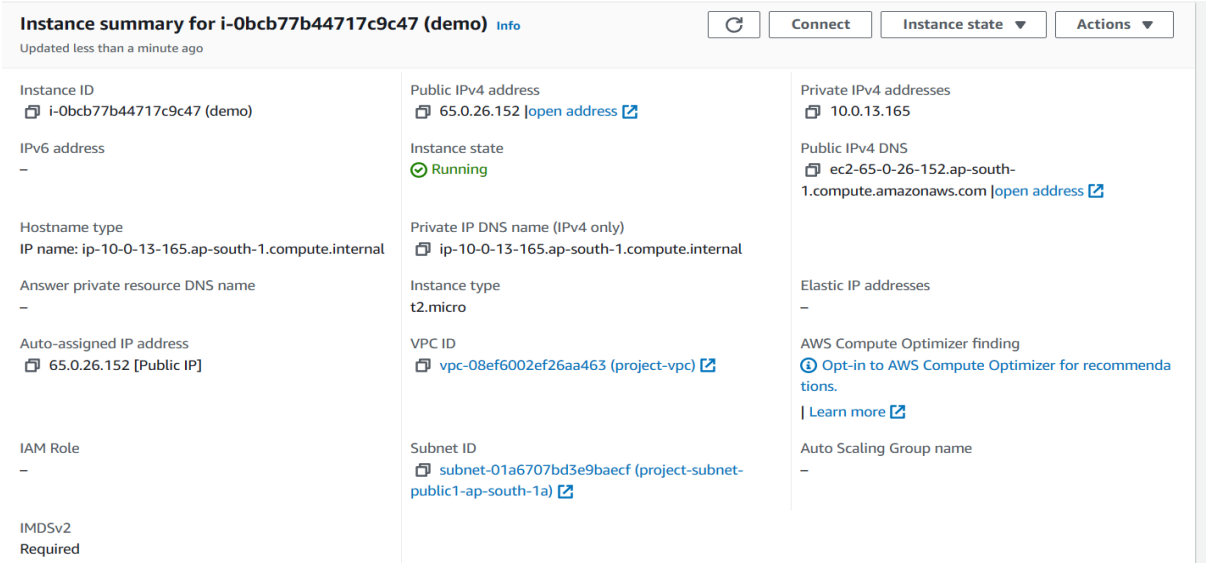
Keep it default and we will see in deep in upcoming images.



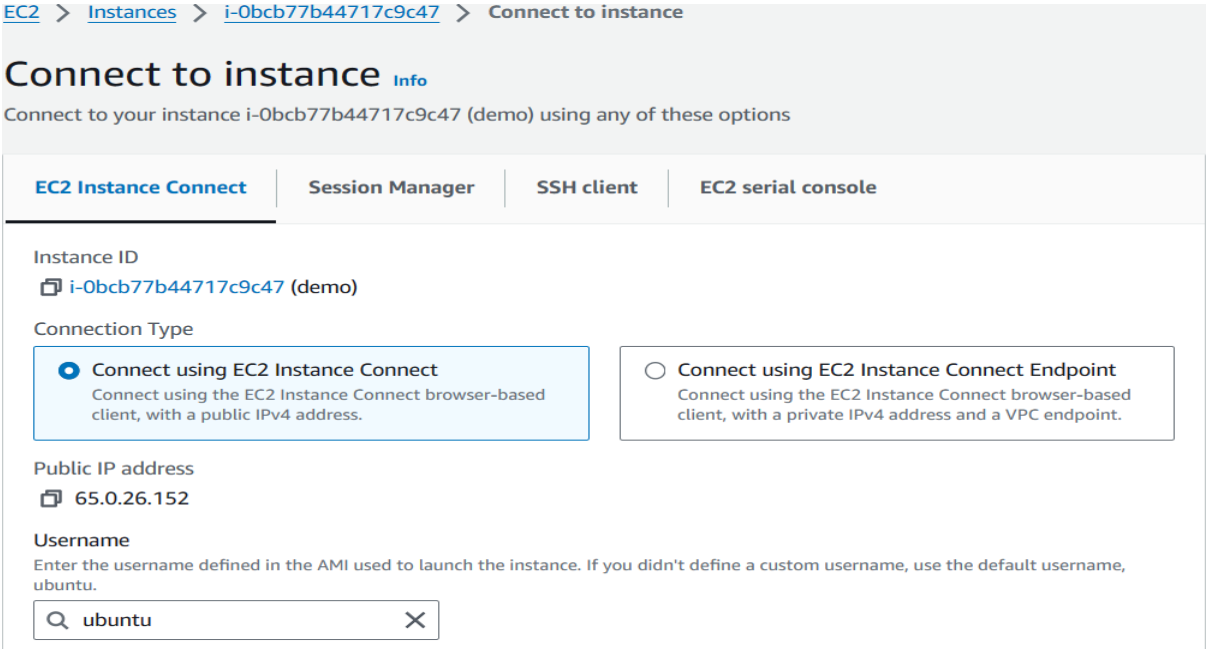
Choose the storage size and launch instance.



Here, We can see the VPC that we have attached to the instance.



Connect the instance to browser.



Go to root and update the packages.

```
ubuntu@ip-10-0-13-165:~$ sudo su -
root@ip-10-0-13-165:~# apt update
```

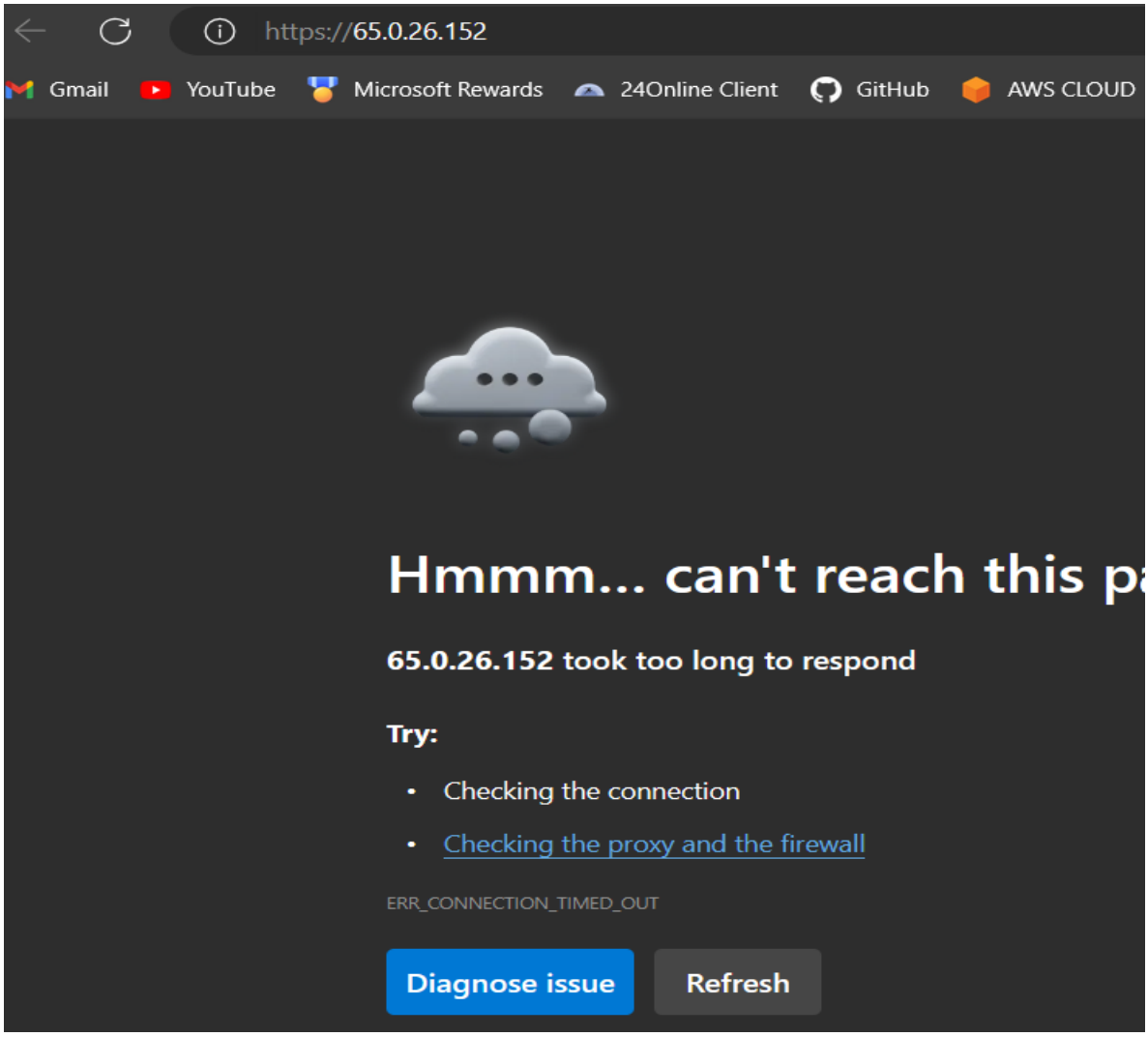
Install apache2 http server on instance.It helps the instance to connect on http server using port 80.

```
root@ip-10-0-13-165:~# apt install apache2
```

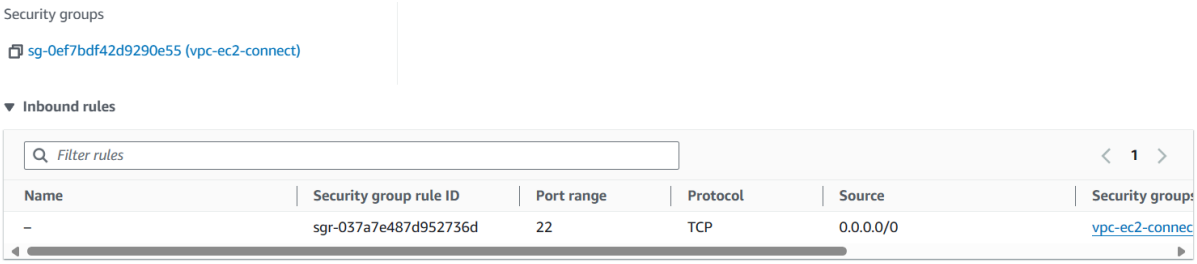
Check the status of the apache2 server.

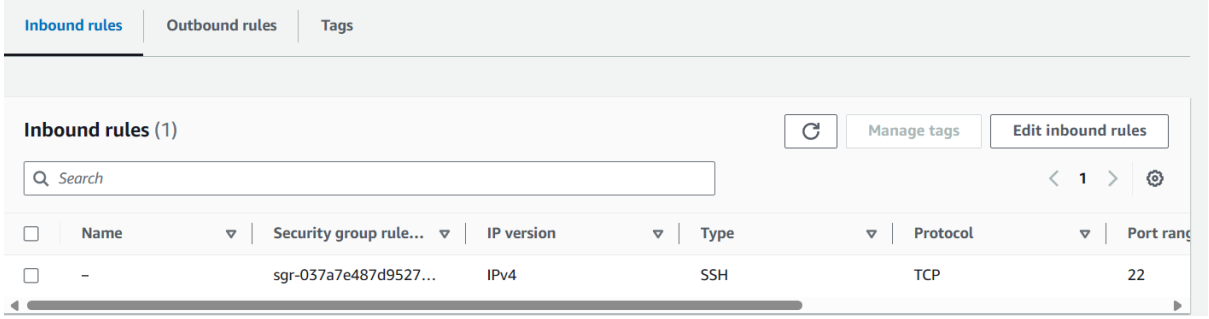
```
root@ip-10-0-13-165:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2024-04-20 11:17:11 UTC; 17s ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 2652 (apache2)
      Tasks: 55 (limit: 1121)
     Memory: 4.9M
        CPU: 33ms
     CGroup: /system.slice/apache2.service
             ├─2652 /usr/sbin/apache2 -k start
             ├─2654 /usr/sbin/apache2 -k start
             └─2655 /usr/sbin/apache2 -k start

Apr 20 11:17:10 ip-10-0-13-165 systemd[1]: Starting The Apache HTTP Server...
Apr 20 11:17:11 ip-10-0-13-165 systemd[1]: Started The Apache HTTP Server.
root@ip-10-0-13-165:~#
```

Go the brower and check if the http server working successfully.It won't work because, we haven't configured the http and the port in security group in inboundrules.

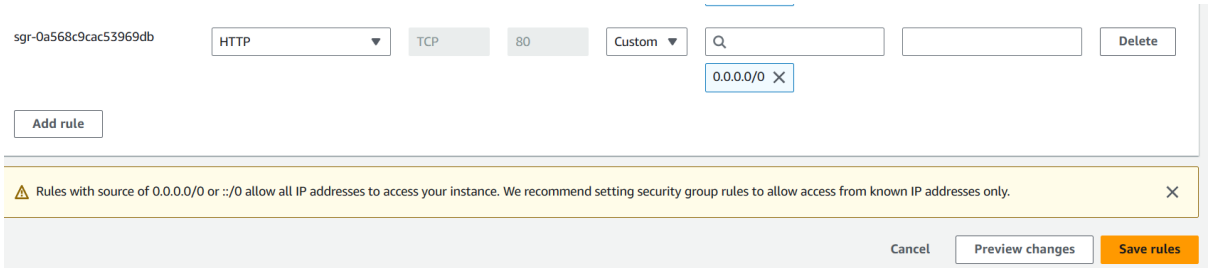


Comeback to instance and go to security groups. Choose the security group. Click on edit inbound rules to add the protocol and port.

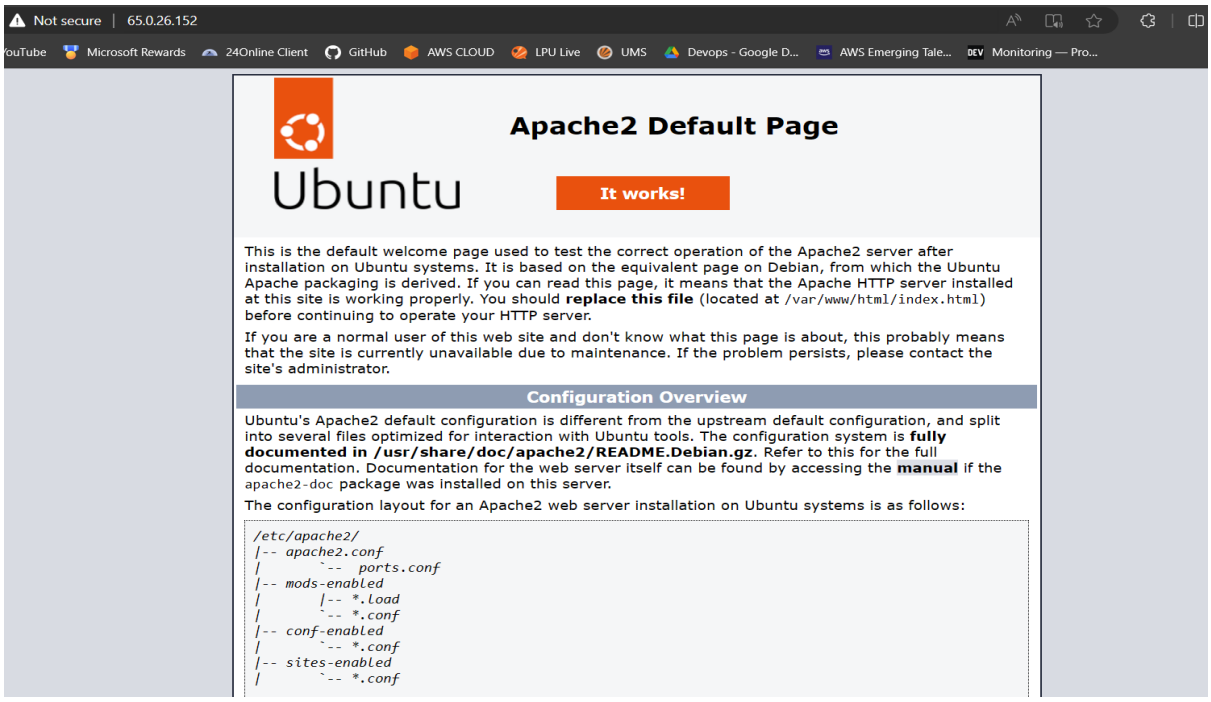




Add HTTP protocol and save the rules.



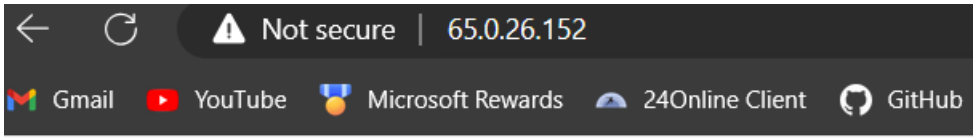
Enter the IP of instance again and we can see the http server running.



Here, We can customize the server settings and enter the command shown below.

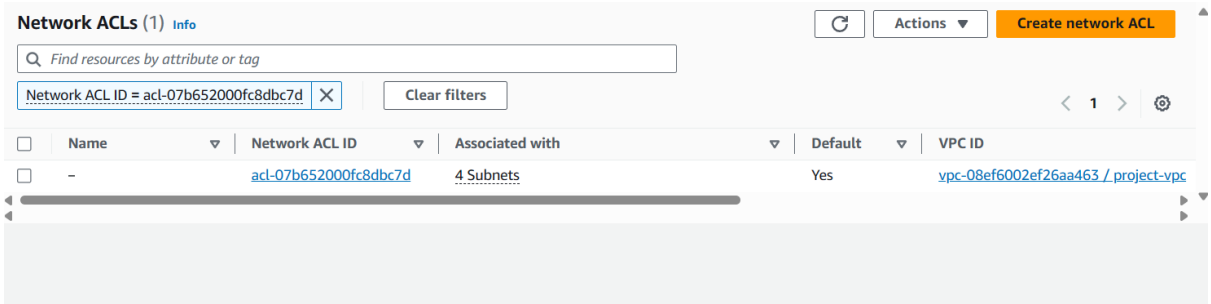
```
root@ip-10-0-13-165:~# echo "Welcome to AWS Services" > /var/www/html/index.html
```

This command enters the text into the index.html file and gets displayed when we again refresh the http page.

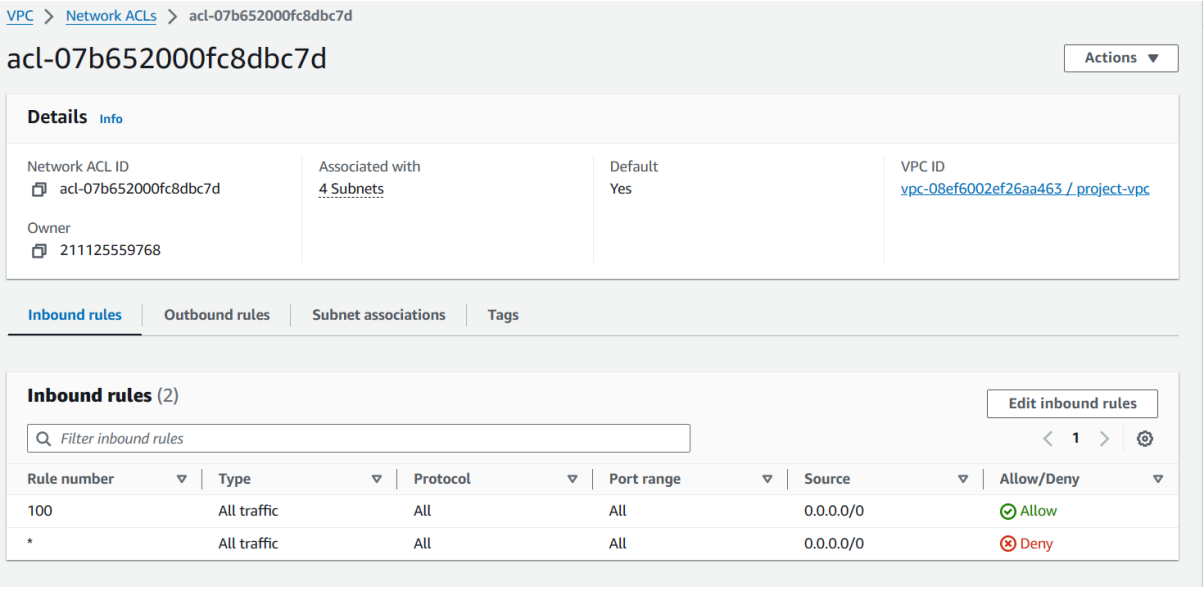


Welcome to AWS Services

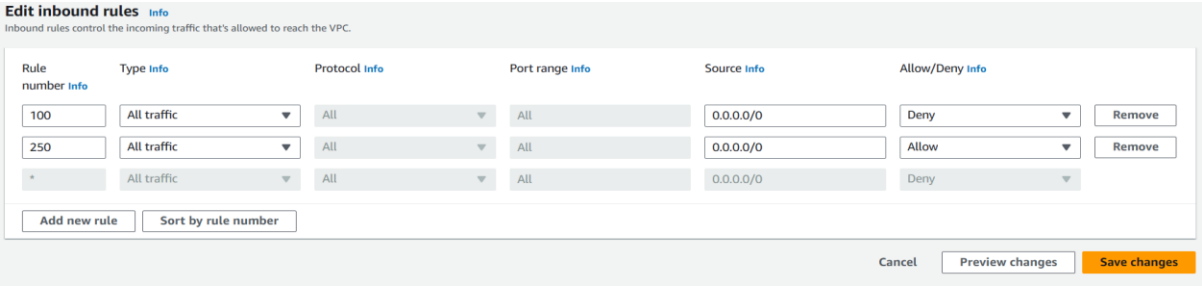
Now, We see how NACL can be used and the main difference between SG and NACL. Choose the NACL ID that is already created for the VPC.



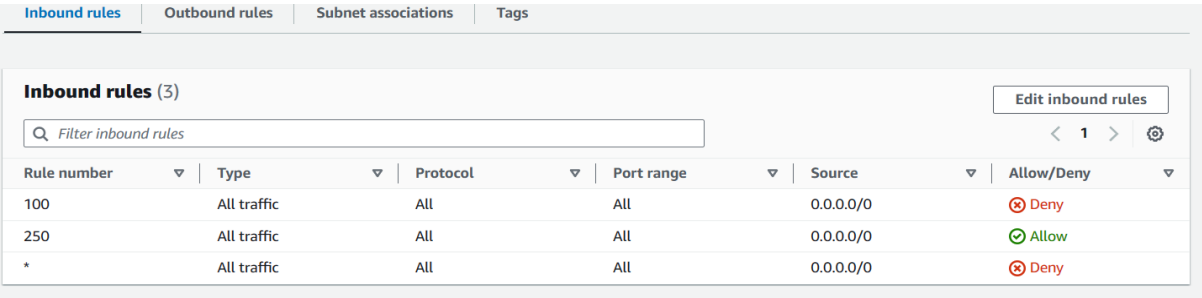
We can see, the inbound rules are in an order i.e the NACL verifies the first rule that is mentioned in order and allows or denies traffic accordingly.



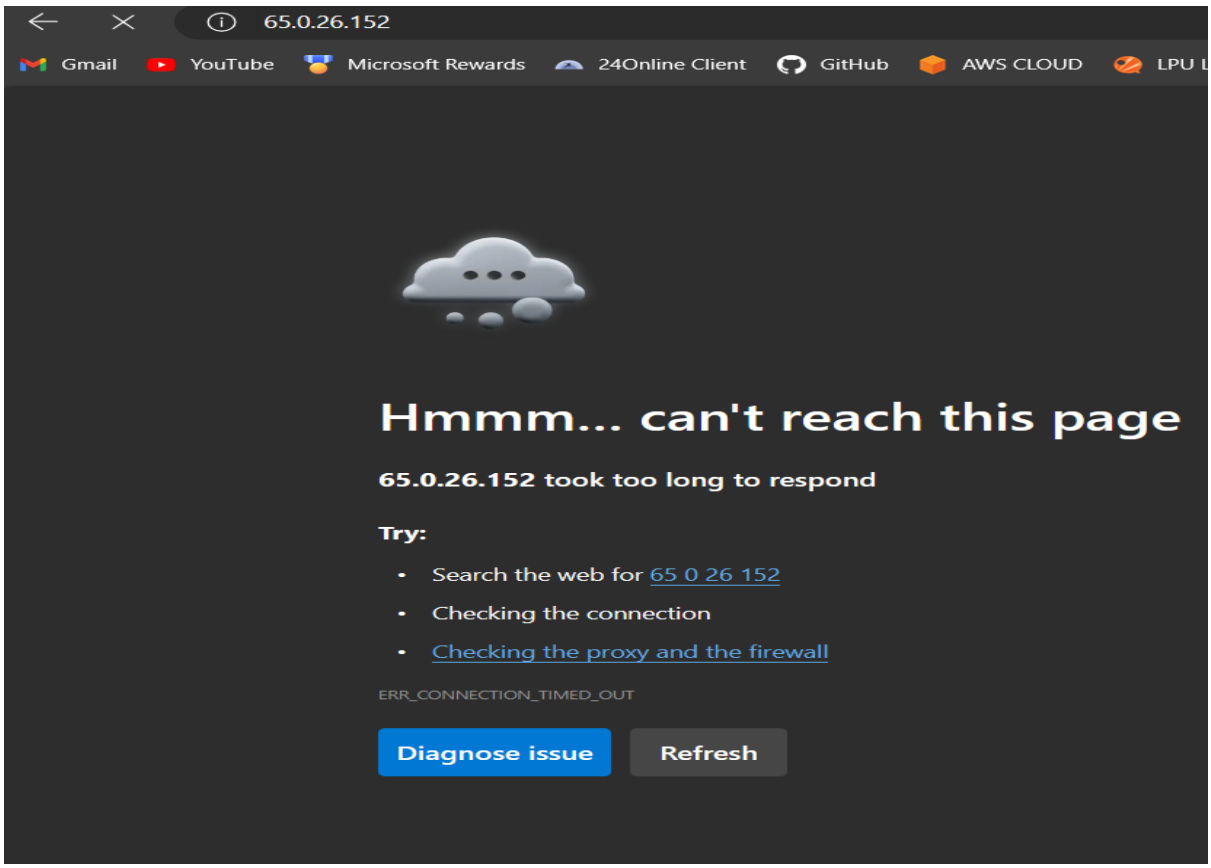
Choose edit inbound rules. Add new rule and give rule number and change the configuration accordingly mentioned below. Save the changes.



We can see, the rule number 100 has the priority and it is denied to allow the traffic. Now, open the instance ip on new page and let's see what happens.



We can see that it denied the access to the http server.



A small discussion on subnets i.e whenever a VPC is created, both public and private subnets get created for VPC in the availability zones that currently you belong to and a default route table also gets created.