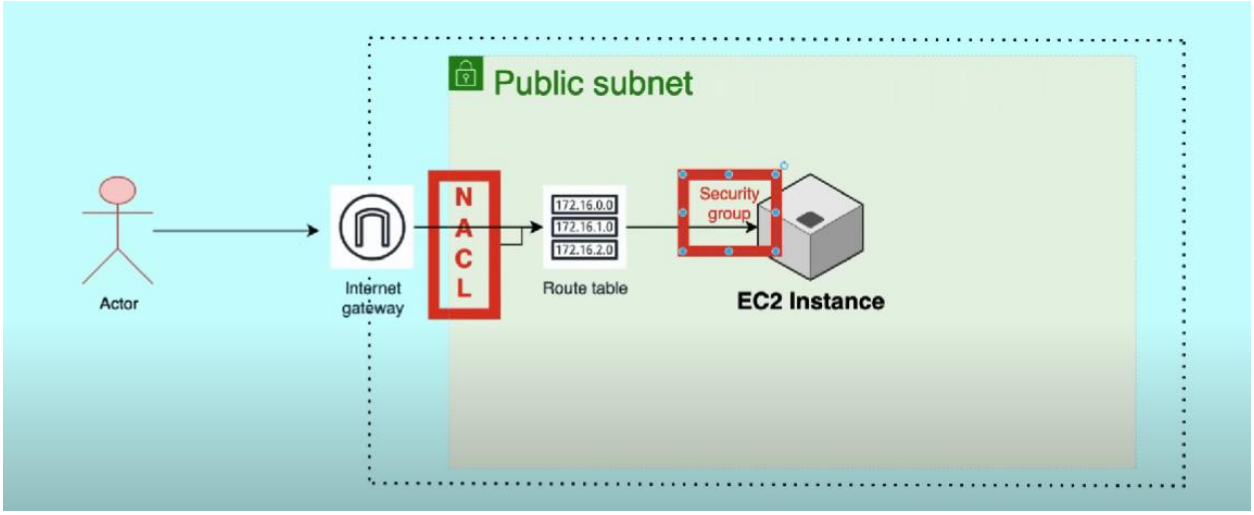
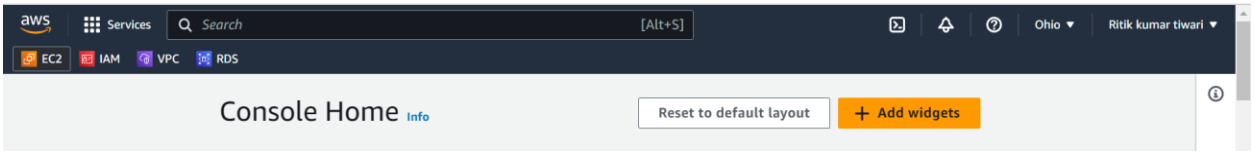
Hands-On Practical Note**

🔒🌐 Unlock the Power of Security Groups and NACLs in AWS! 🚀🔐

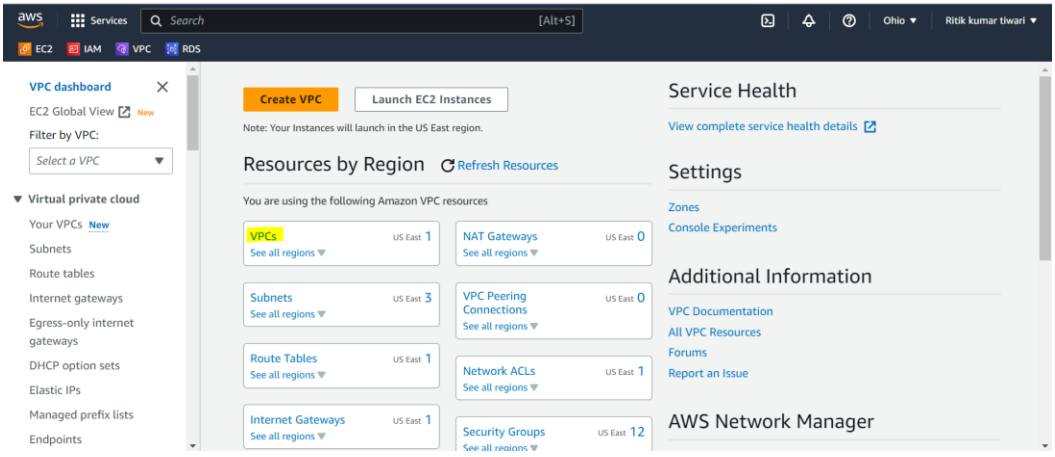


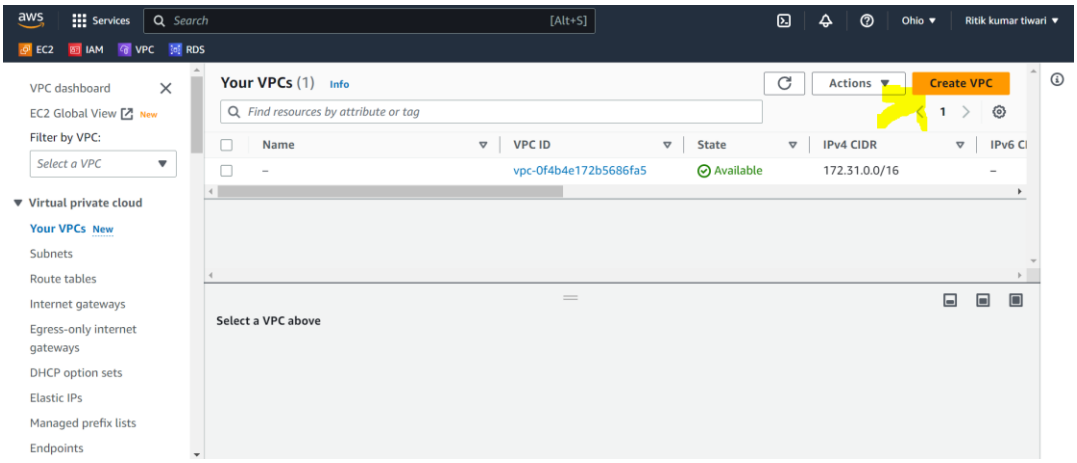
How to create VPC (Virtual private cloud):



1st:

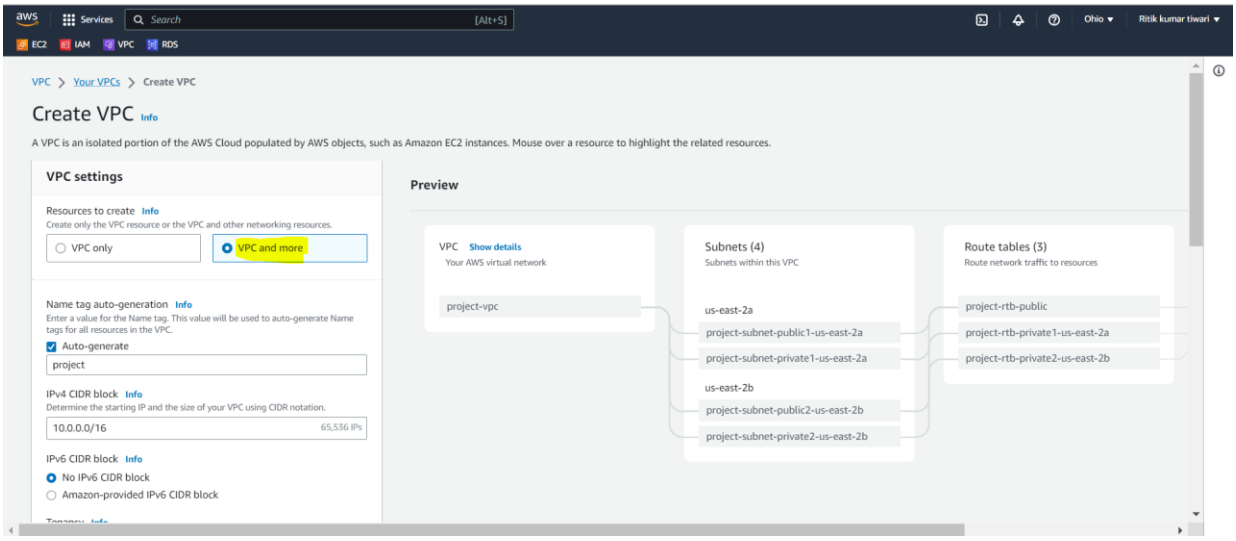
First Go to VPC and Create VPC:

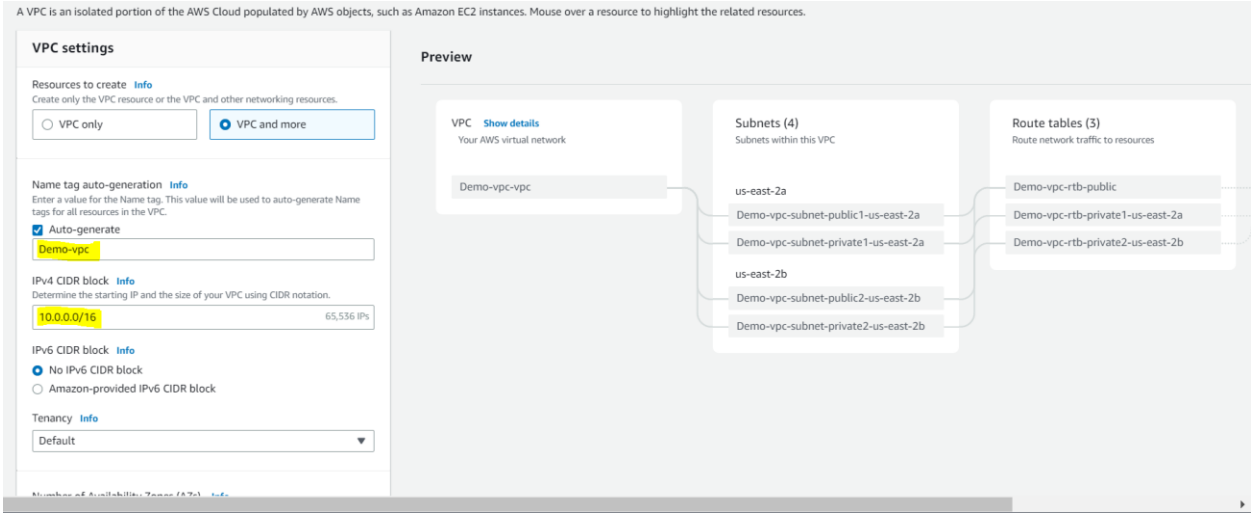




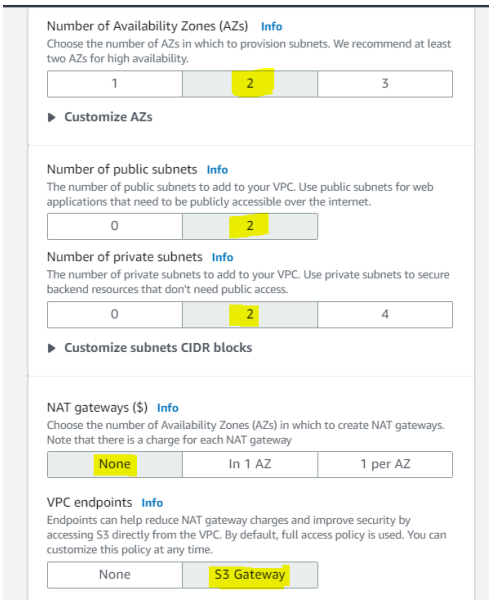
Go with VPC and More because AWS will provide you default resource, which is already configured, we don't need to configure lots of things.

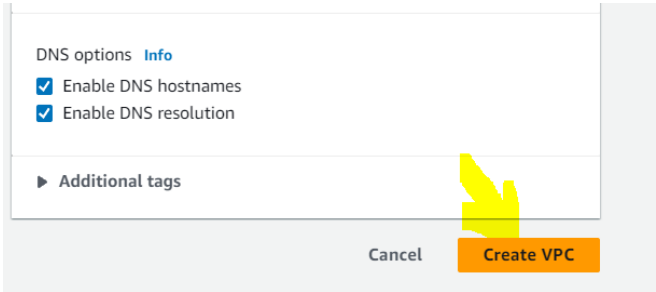
Like: VPC, Subnets for both the regions as a (public & Private) and route tables etc.

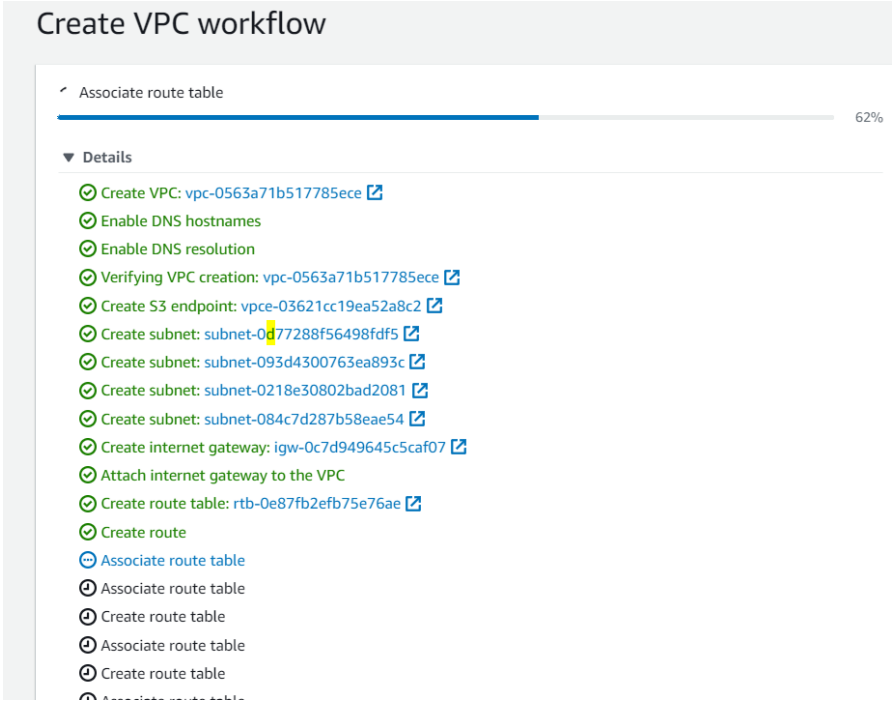


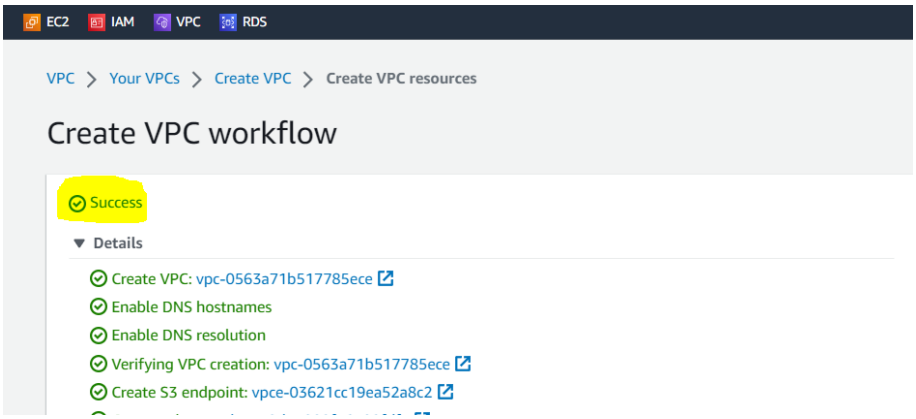


You can modify IPv4 CIDR block according to your requirement.



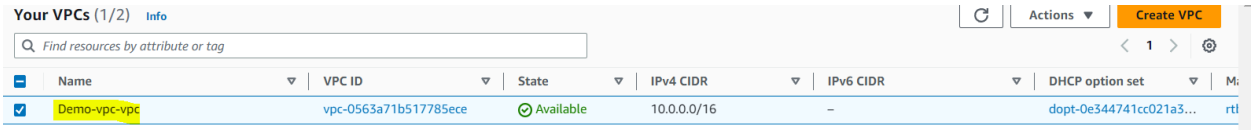






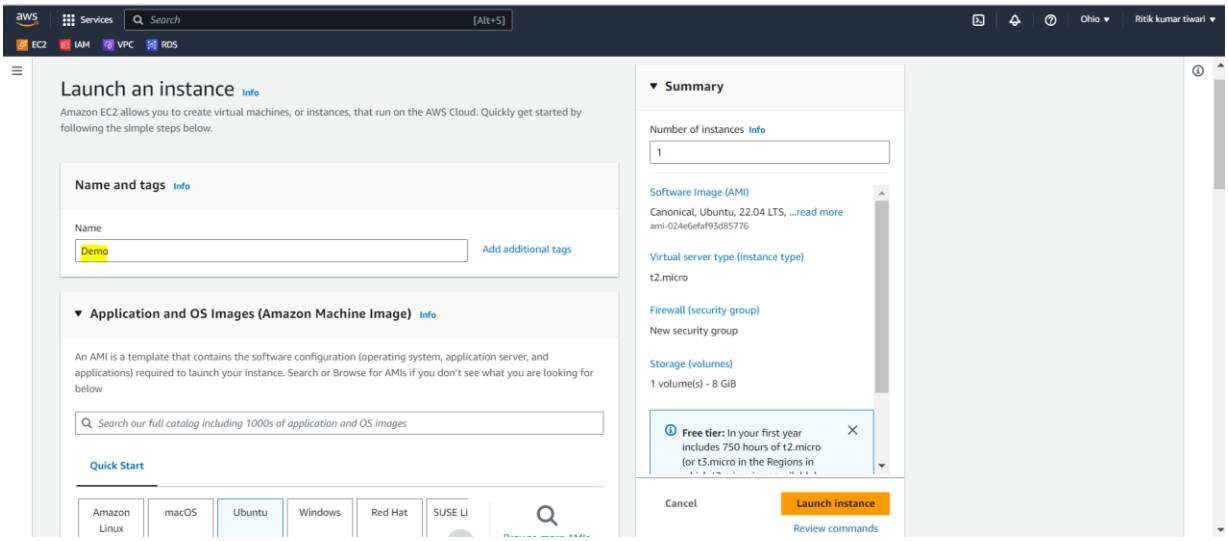
Click on **View VPC**

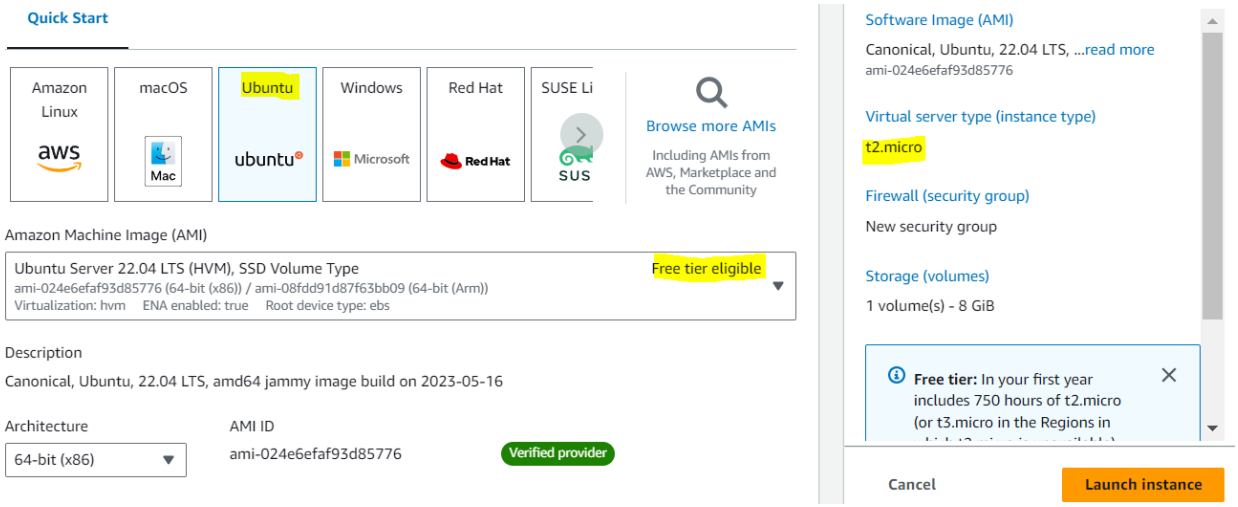
Wait for some time it will create and then you can see.

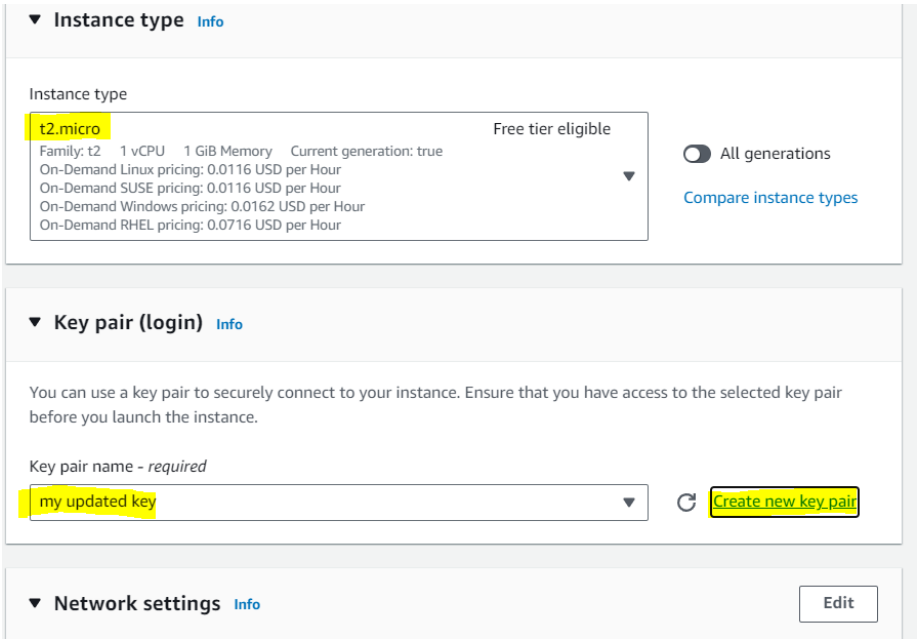


Now we will create EC2 instance where we are going to demonstrate security group and NACL:

Go to instance



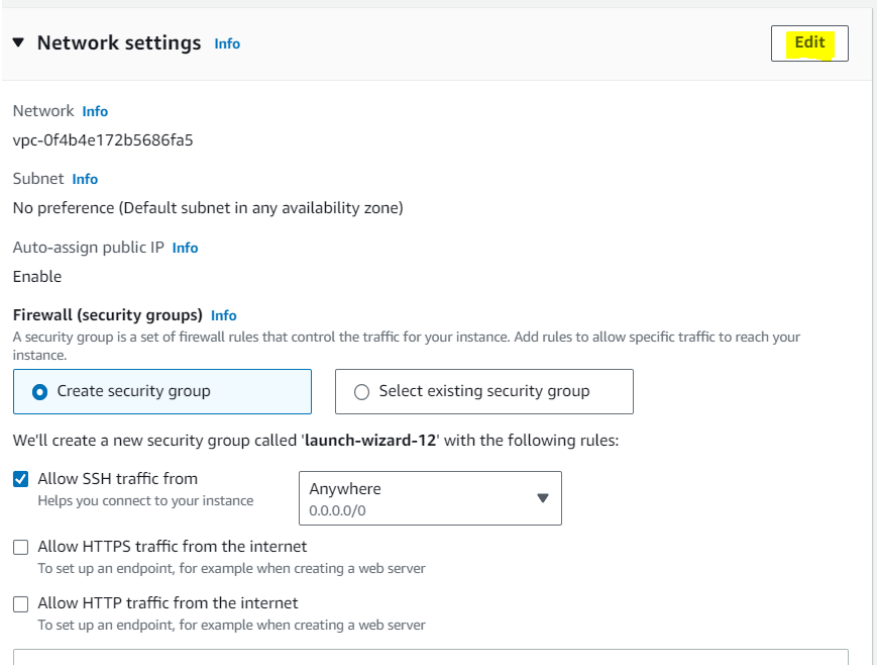


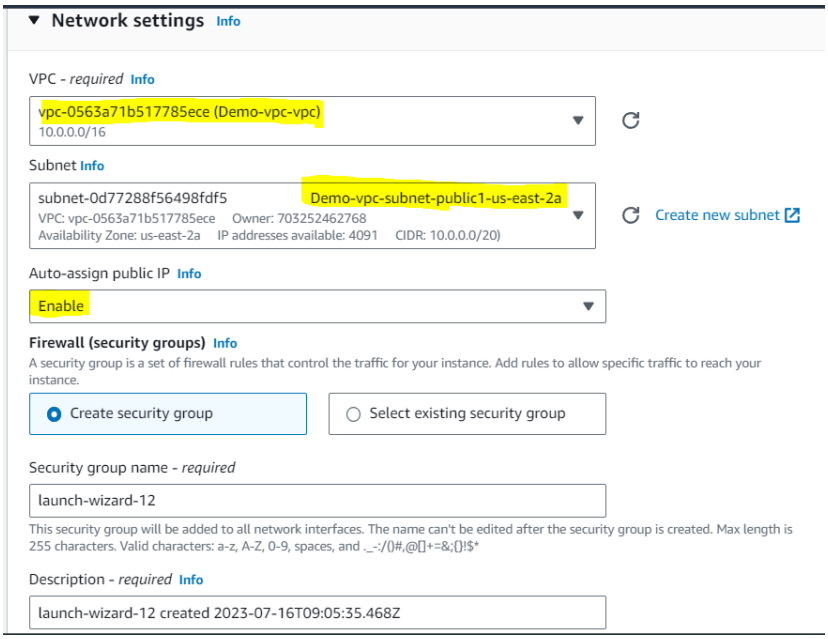


You can create new key pair or existing one:

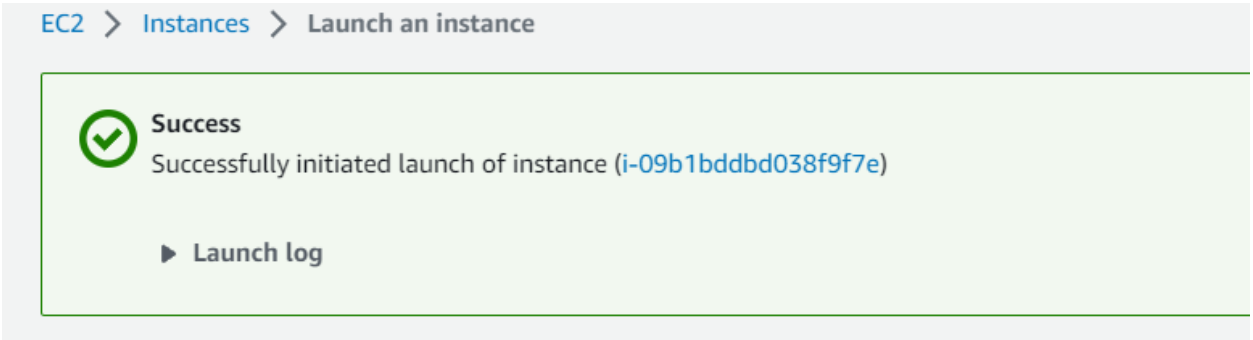
Click on EDIT:

Please don't go with default VPC, select your own VPC as we created previous **Demo VPC**

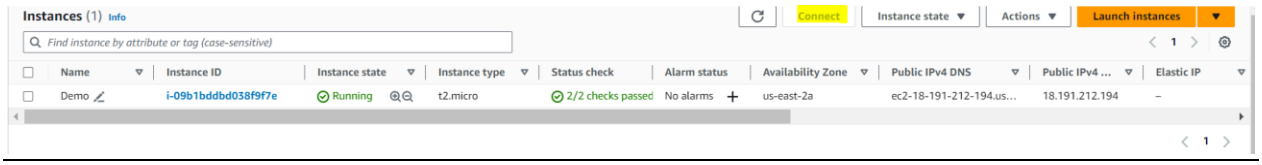




Rest of things should be default and click on Launch instance.



Now we install Python, and we will deploy and run that application on EC2 Port No. 8000, it will be block by default, but we need to enable that. Let see.



sudo apt update

python3 (check python is installed or not)

```
ubuntu@ip-10-0-14-242:~$ python3
Python 3.10.6 (main, Mar 10 2023, 10:55:28) [GCC 11.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

Ctrl+D go main server:

Pyhon3 -m http.server 8000

It is running on this server…

```
ubuntu@ip-10-0-14-242:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

If we want to access this application through instance Public IP address, it will not show the page…

i-09b1bddbd038f9f7e (Demo)

PublicIPs: 18.191.212.194 PrivateIPs: 10.0.14.242

Copy the public ip : http://18.191.212.194:8000/

This site can't be reached

18.191.212.194 took too long to respond.

Try:

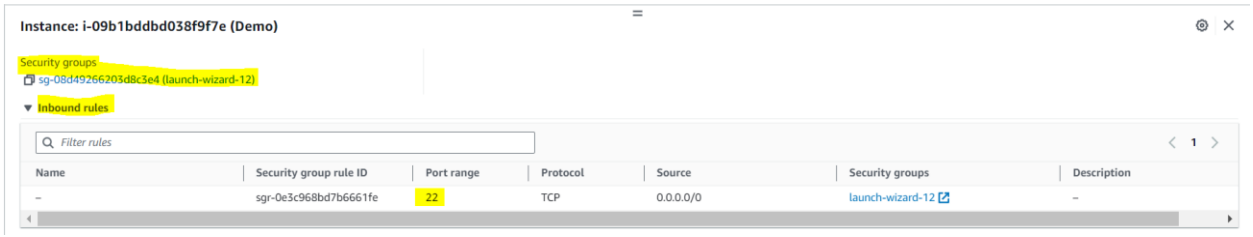
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Reload

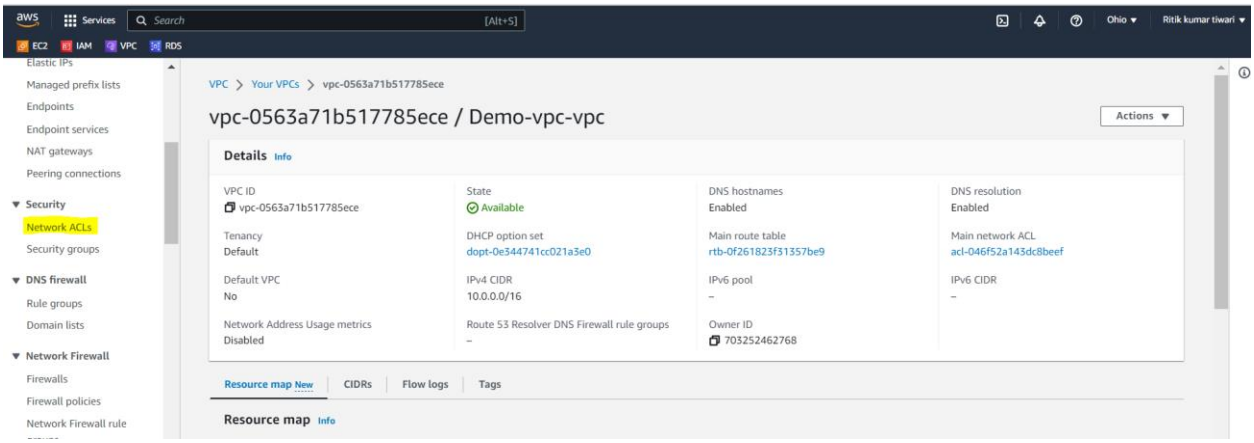
It will throw site can't find.

Go to instance > security > security group > inbound rule port 22> aws by default allow.. there is no 8000 port.

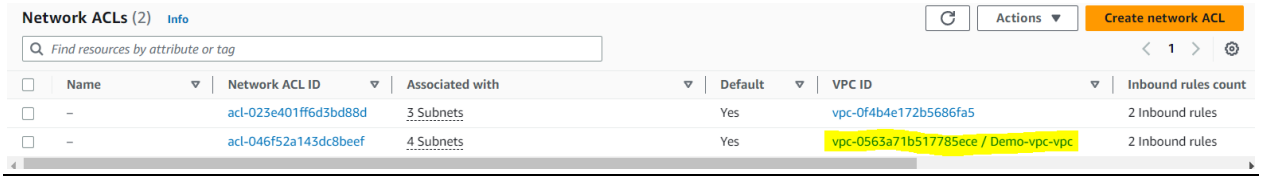


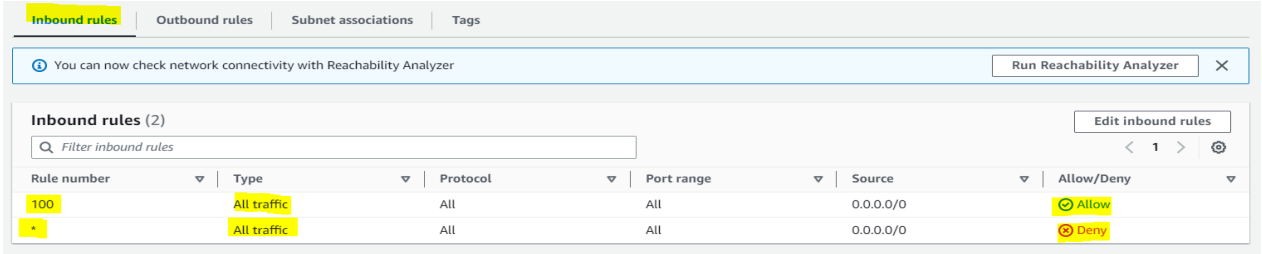
Now we will investigate NACL concept:

Go-to VPC > click on your newly created VPC > click on Network CALs



Click on Network ACL ID:



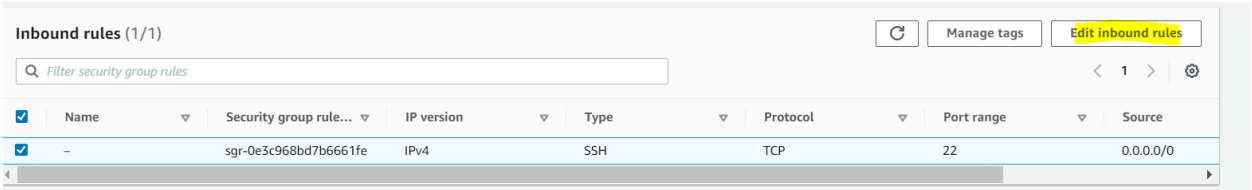


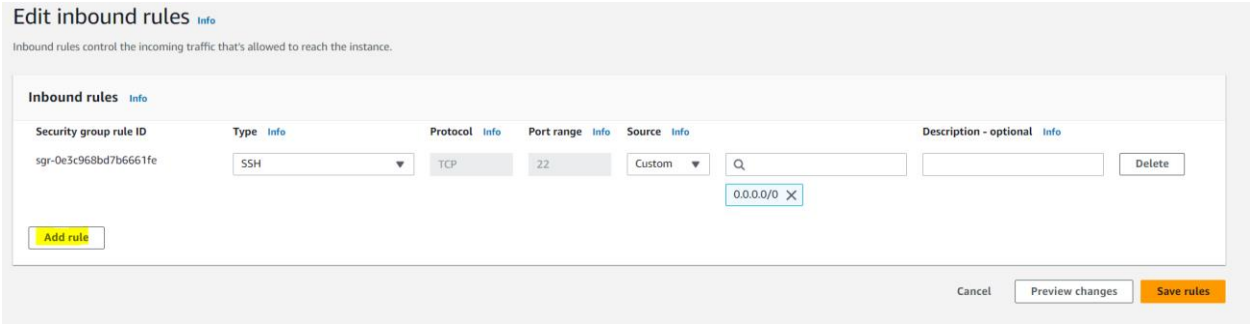
There is rule 100, it will check if requirement meet it will pass otherwise it will fail,

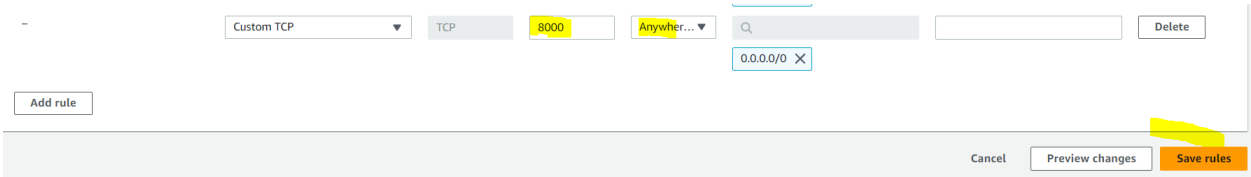
So as of now… we need to edit the inbound rule in security group.

Go to instance > security > security group > inbound rule port 22> aws by default allow. there is not 8000 port.

Now we need to allow port no. 8000

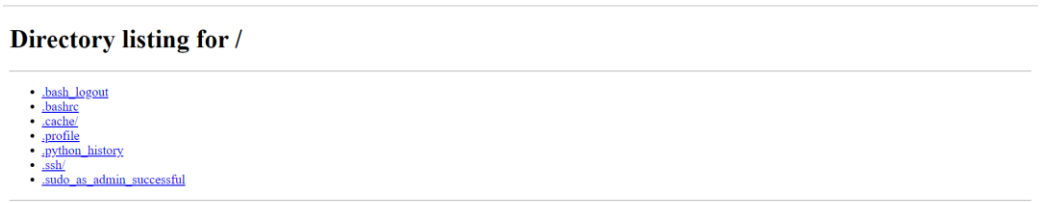






Copy the public ip and paste it on browser: http://18.191.212.194:8000/

Now paste the URL, we will see simple http sever, where all the files are present in this folders this is the output:

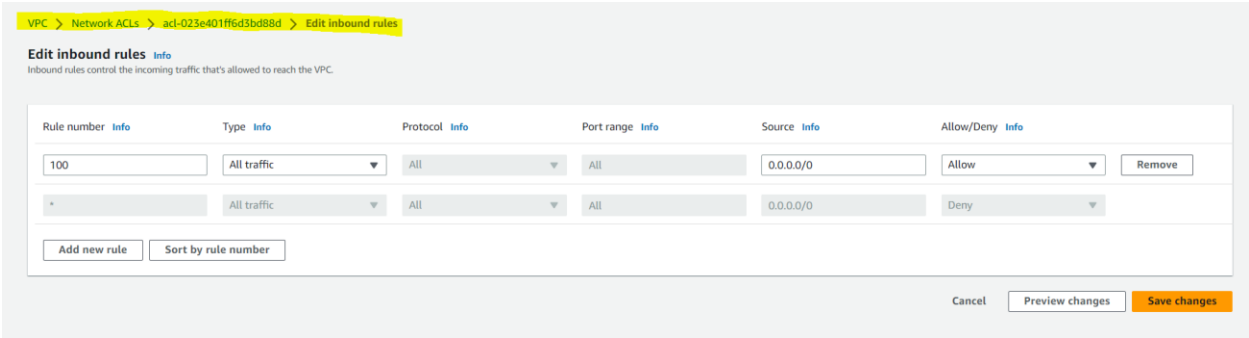


```
ubuntu@ip-10-0-14-242:~$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
49.36.169.138 - - [16/Jul/2023 09:54:34] "GET / HTTP/1.1" 200 -
49.36.169.138 - - [16/Jul/2023 09:54:41] "GET / HTTP/1.1" 200 -
```

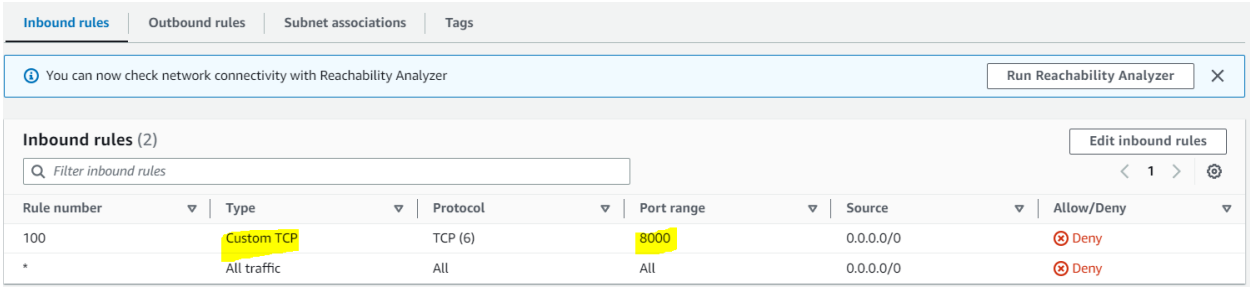
If you will refresh the web page, then you will see the response 200.

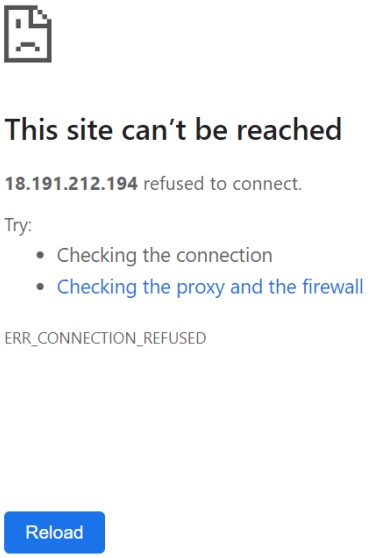
🔒🌐 Strengthening Security with NACLs: Blocking Port 8000 to Enforce Strict Rules! 🚫🔒

As a DevOps engineer. Suppose in your organization has very strict rule that we cannot allow permission to enable the port no. 8000, then I will block the port 8000 in NACL on subnet level



Then request will not go to the application team, or that application will not open.





So, who has permission of the NACL, they can block the all the IP-addresses over all the subnet level.

Note:

We have understood the topic of NACL and security group, with respect to allowing and blocking the access.

Follow for more on LinkedIn: https://www.linkedin.com/in/ritikktiwari/