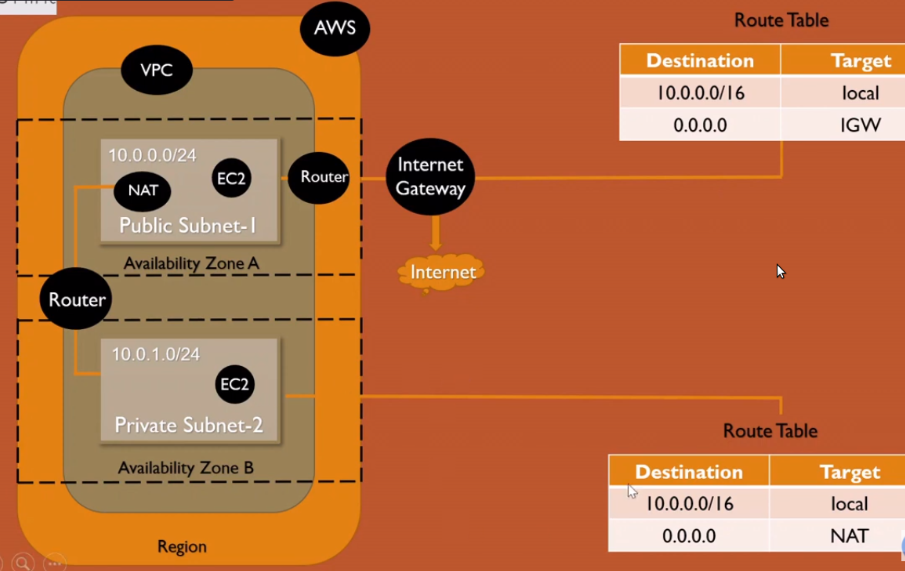
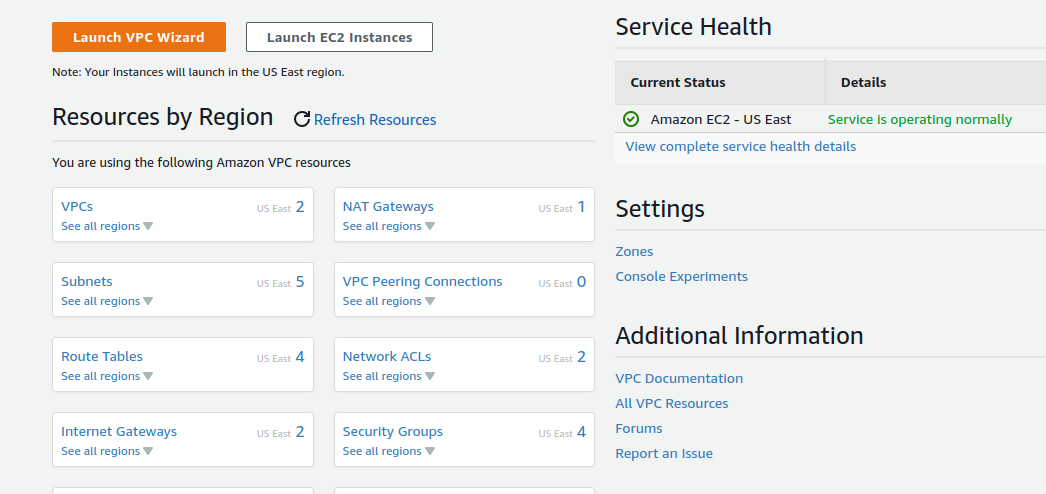
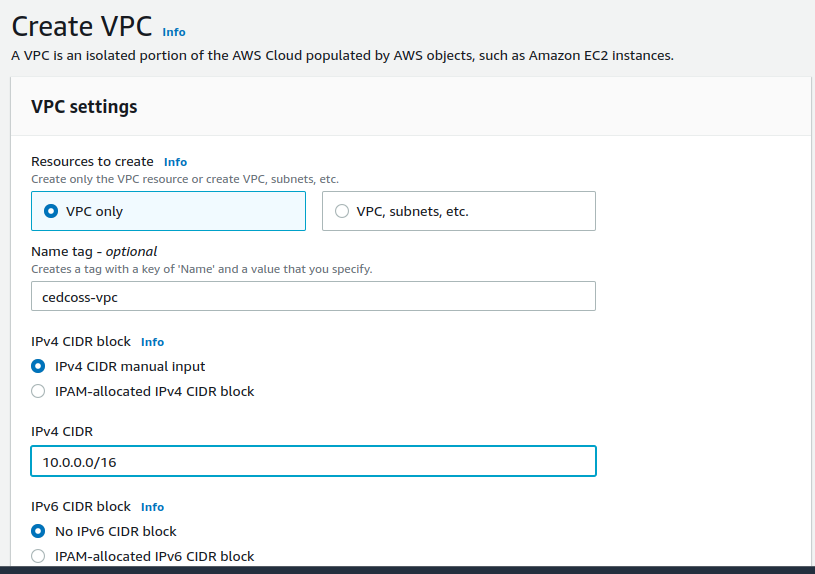
**NAT Gateway For Private Subnet Internet Access**

****

Login to AWS console -----> Go to services choose -----> VPC



Choose VPC’s -----> Click on create VPC



Click create VPC button.

Back to VPC’s dashboard -----> Click on Subnet -----> Choose create Subnet

Select your VPC ID & scroll down --> Create your Subnet Name ---> Create CIDR Block .

“Here we are create two subnet one public and one private subnet”

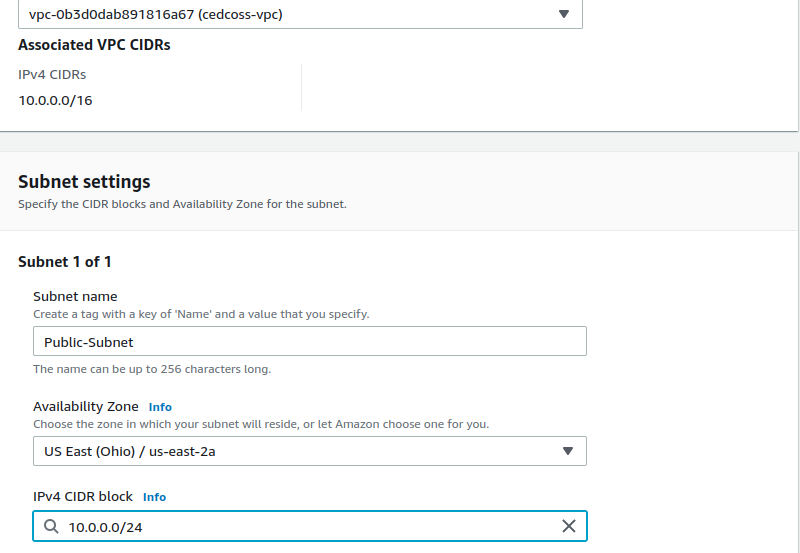
**Public Subnet :**

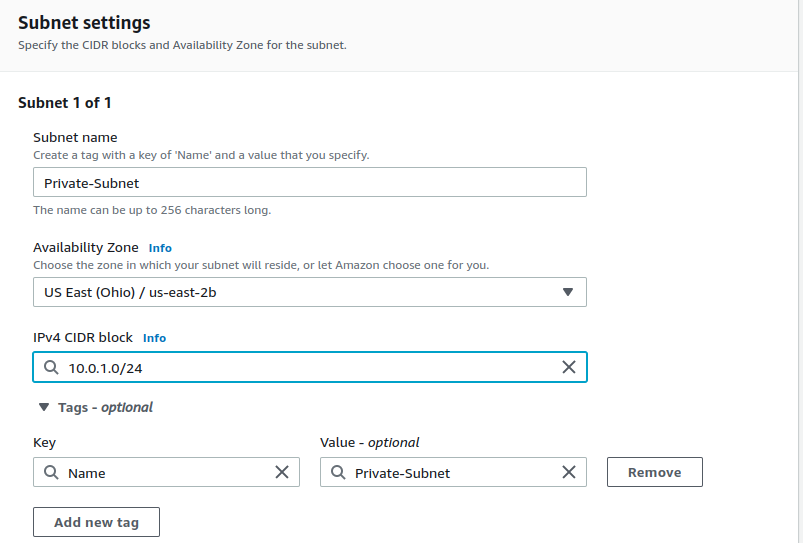
“A subnet that's associated with a route table that has a route to an internet gateway”

**Private subnet :**

“back-end servers that don't need to accept incoming traffic from the internet and therefore do not have public IP addresses”

**Public Subnet**

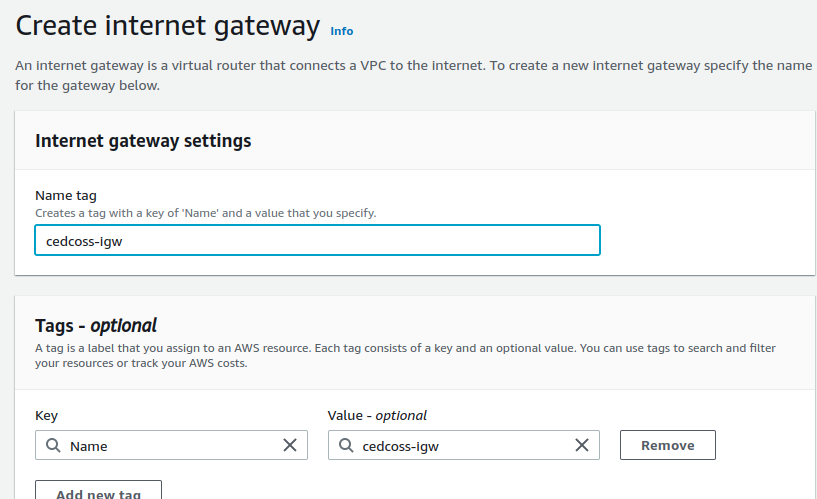
****

**Private Subnet**

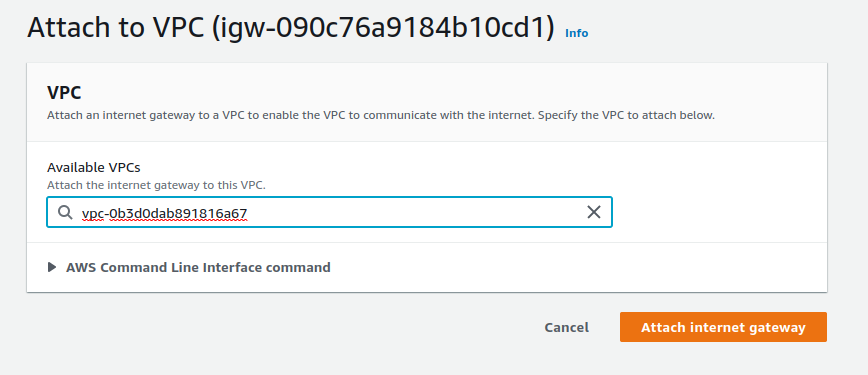
Click on Create Subnet -----> Back to VPC’s Dasboard ----> Click on Internet Gateway (IGW) ----> here you have default IGW (ignore them) ---> Just Choose create Internet Gateway

**Internet Gateway :**

“A network "node" that connects two different networks that use different protocols (rules) for communicating”



Create you Internet Gateway Name ----> Back to Internet Gateway dashboard



You have a notification ‘Attach to VPC’ Choose your VPC.

Back to VPC’s dashboard click on Route Table ---> Choose create Route Table

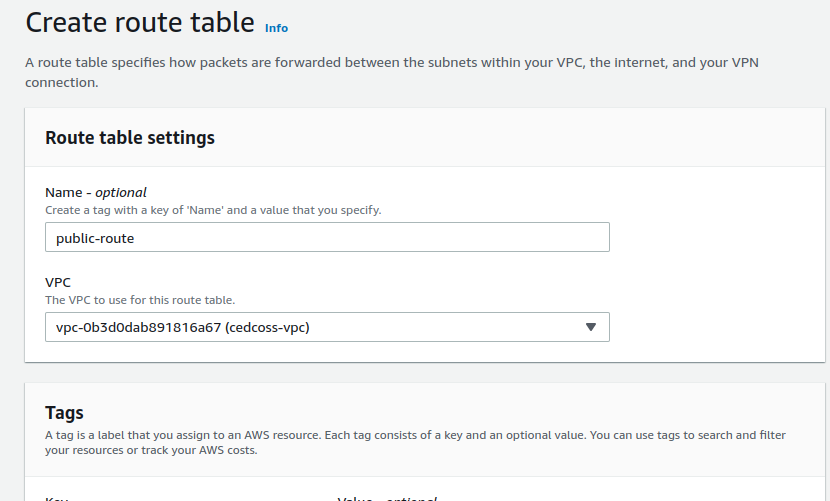
create two Route Table :

1 : Public Route Table

2 : Private route Table

**Route Table :**

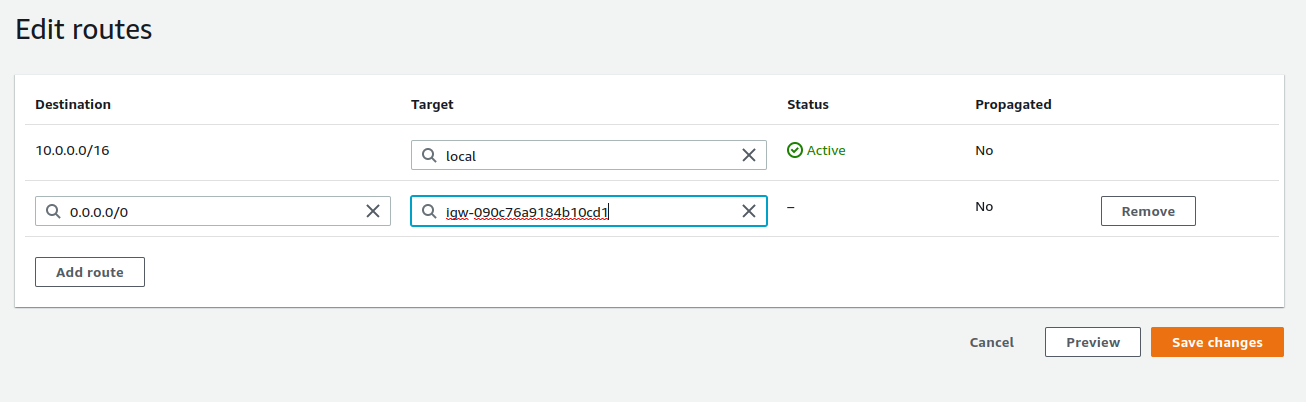
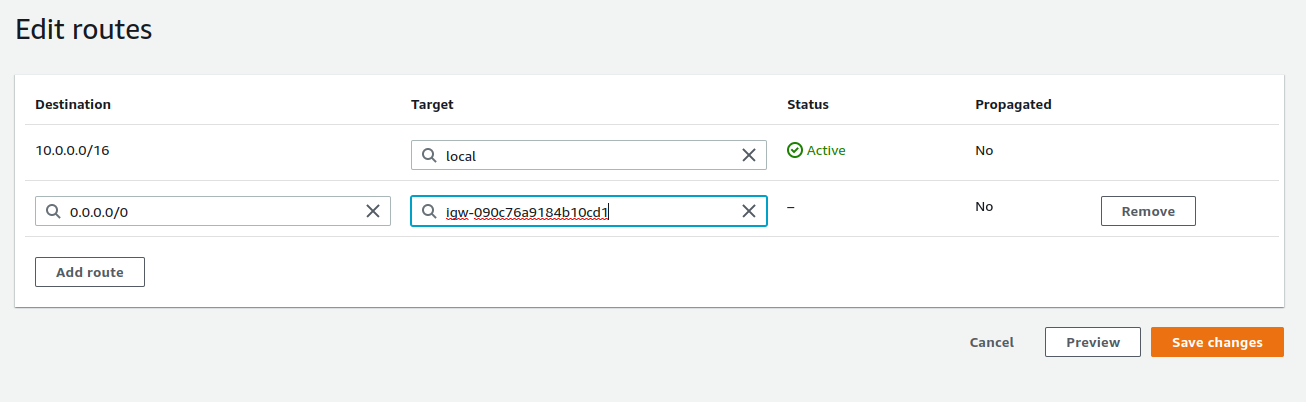
“Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). A subnet can be explicitly associated with custom route table”



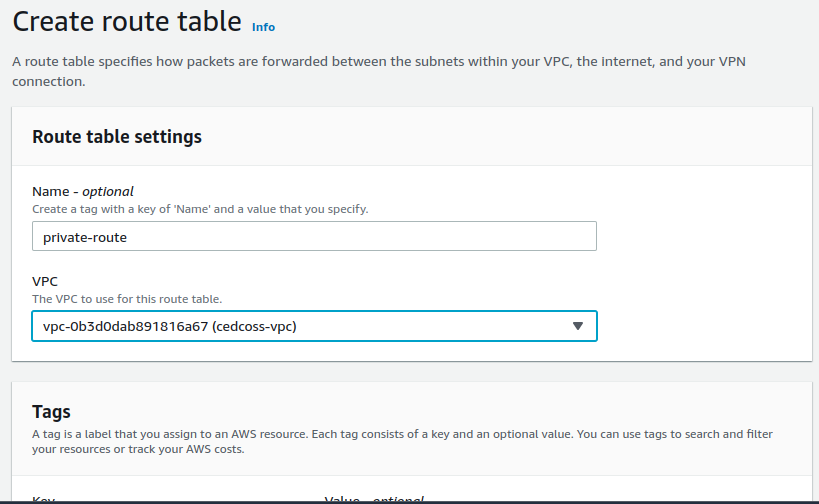
“Contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed”

“A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table”

Go inside of route table ---> click on route ---> Edite route

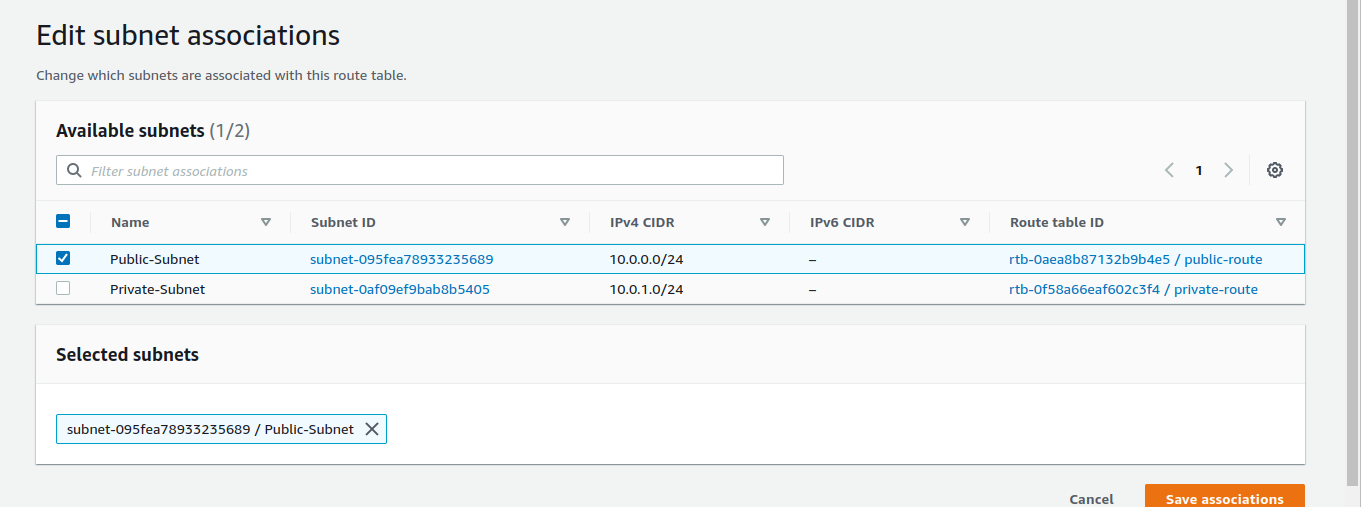
click on Save change.

Back to Route table ---> choose create route table “Private Route Table”

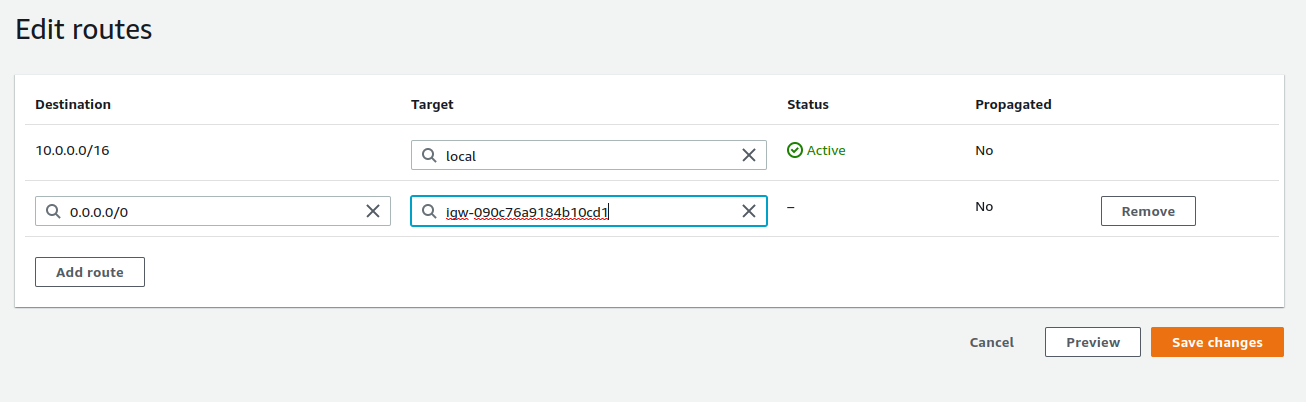
****

Back to route table dashboard click on Public Route Table go inside it --- > click on Subnet association ---> edite subnet association ---> select public subnet & -->

save changes.



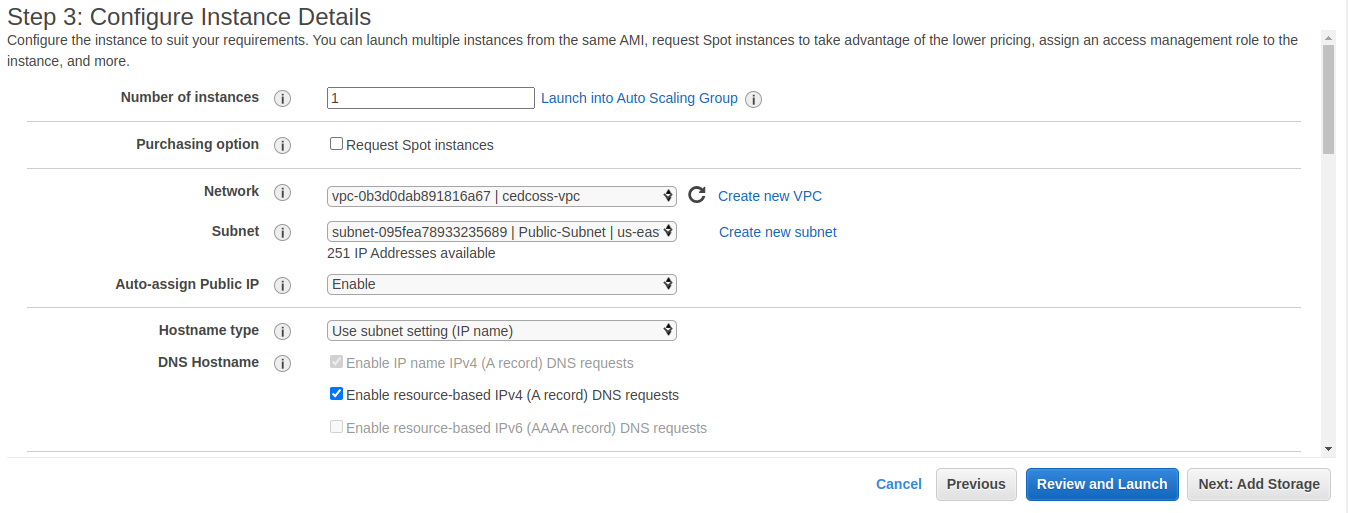
Back to Route tAble & click on route ----> click on edite route table ---> click ‘add route & Internategateway for public subnet key & value pair 0.0.0.0/0 igw-. ---> click save change.

****

After adding Internet Gateway in Public Route Table -----> go to services click on EC2 --->

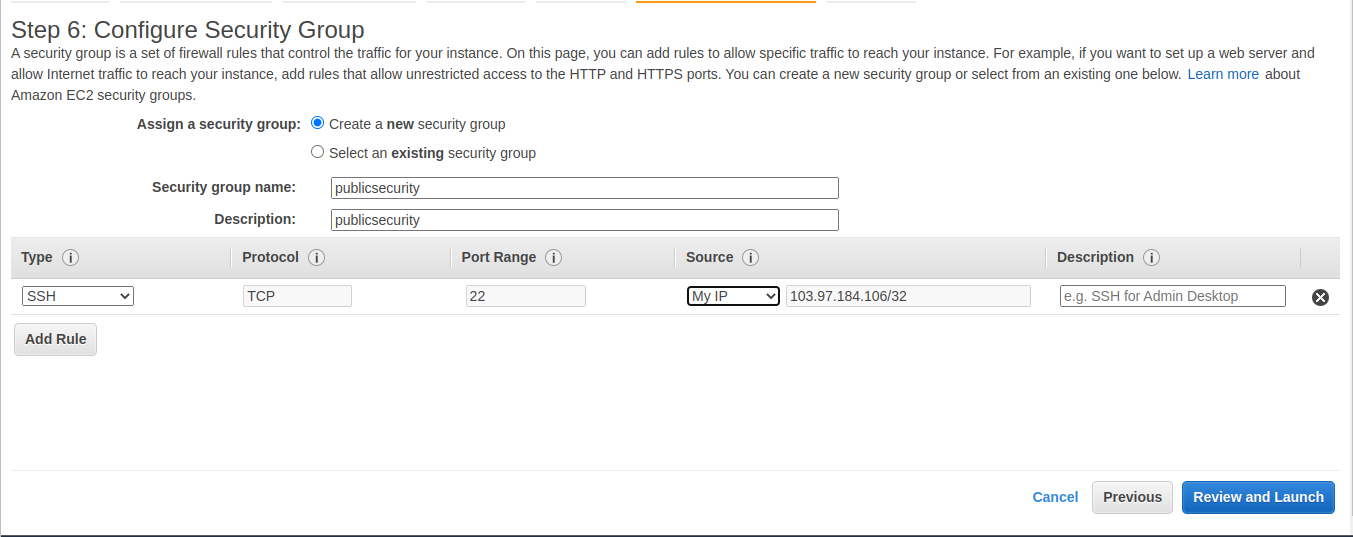
Here we have to create two instance one for public & one for Private.

Create Public EC2 instance :



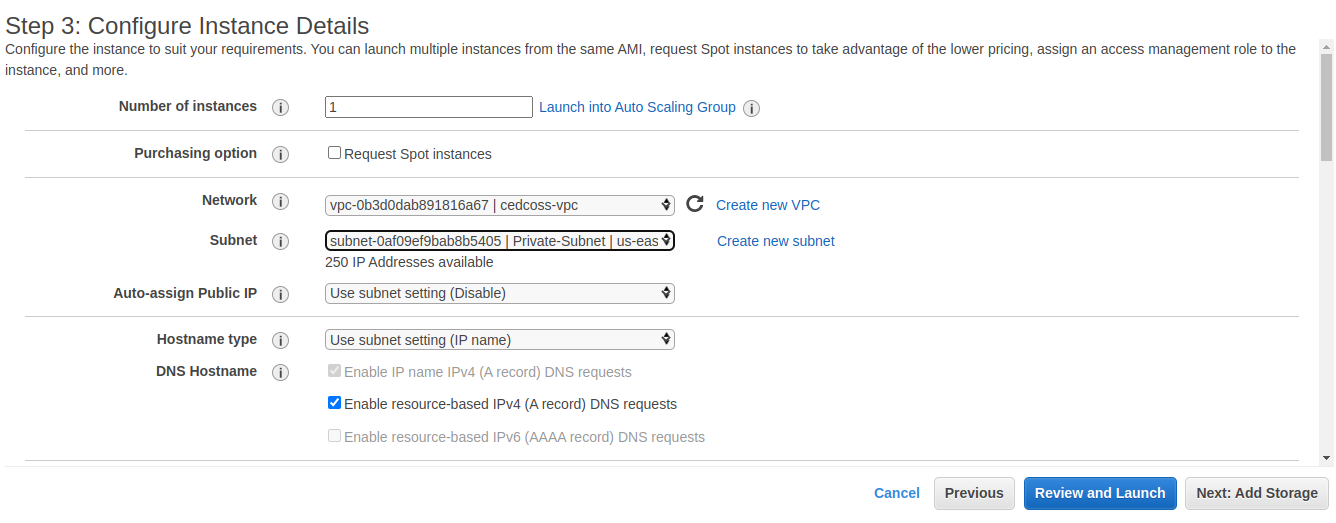
**Note :** Change vpc (select your vpc those you create) & select Public Subnet -----> enable **Auto-assign Public IP** ---> click on next.

Configure Security Group (Step 6) **Must Add** in source My IP ---> review and launch (follow other steps according to your requirment).



Afetr create Public EC2 Instance then create one Private EC2 Instance.

Create Private EC2 instance :



**Note :** Change vpc (select your vpc those you create) & select **Private Subnet** -----> then click on next.

Configure Security Group (Step 6) Must Add in source **Public CIDR Range**

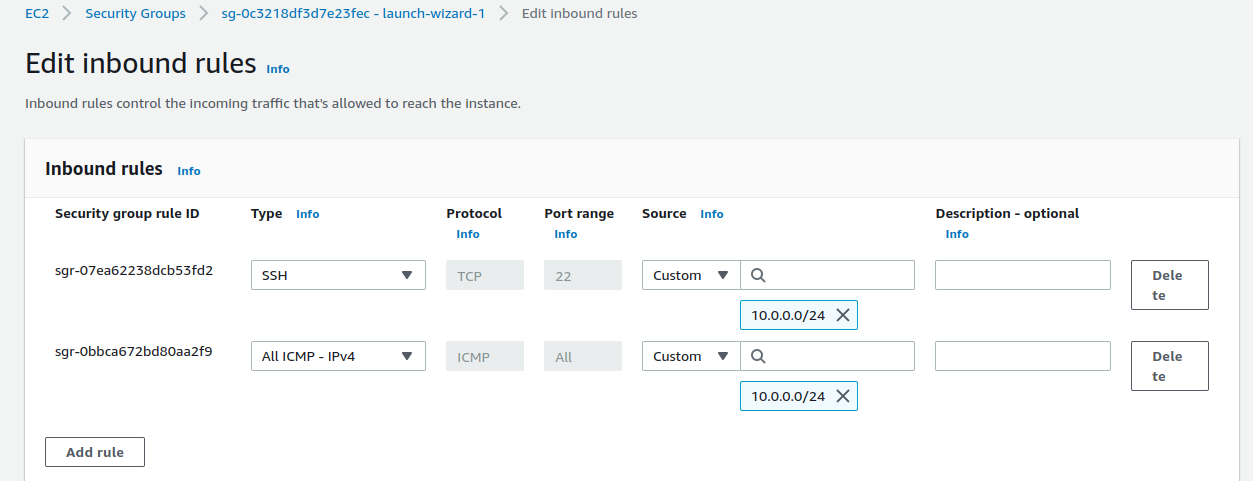
eg : source = 10.0.0.0/24 ---> review and launch (follow other steps according to your requirment).

Note : Add two Rules in Private Security Group for now. You can add later according to requierment.

Type Protocal Port Source

1 : SSH TCP 22 custom 10.0.0.0/2

2 : ALL ICMP Ipv4 ICMP 0-65535 custom 10.0.0.0/24



Click review & launch.

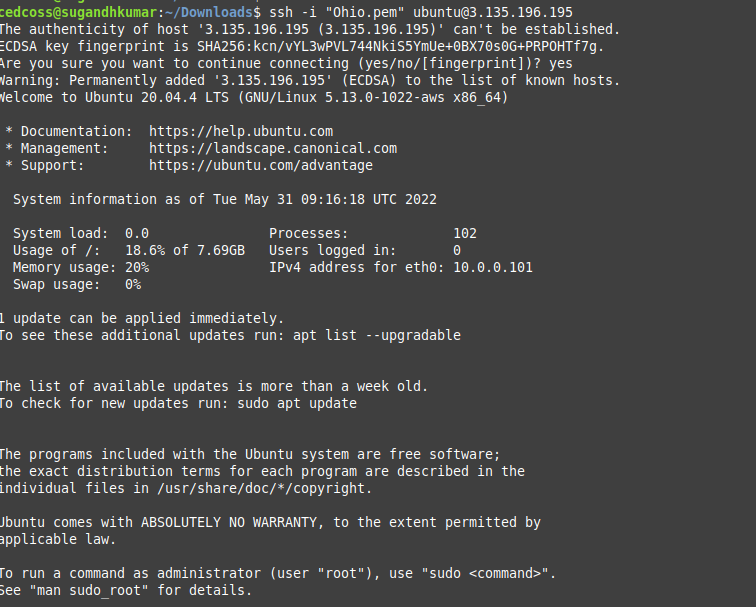
SSH/Connet EC2 instance in the Private Subnet.

Step 1 : SSH connect Public Instance (Subnet)

Take SSH & connect to your terminal.

ping google.com

**Note :** you see your private instance (subnet not accesible from internet)



(Public Instance (subnet) Access Internet But problem is here how to connect private subnet to the internet)

So now we have to do under public subnet we create a key (.pem)

for eg : my Public Key .pem name Ohio.pem : open this file and copy the text

- in the terrminal we create a file with the any text editer in my case use nano.

- sudo nano Ohio.pem & pest the text here.

- save ctrl + o and exit.

- now give permission newly created file Ohio.pem

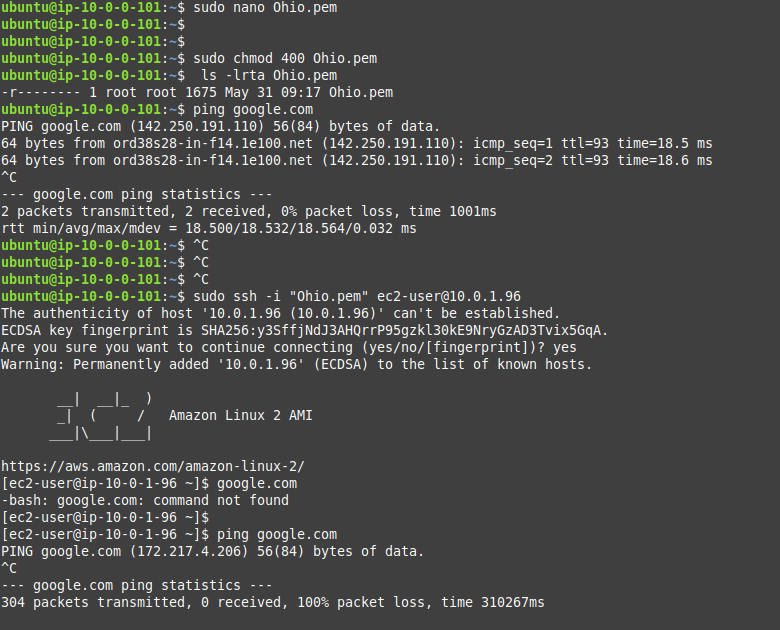
- sudo chmod 400 Ohio.pem

- now connect your private instance (subnet) under public instance (subnet)

- take SSH of private instance & connect it on terrminal.

- sudo ssh -i "Ohio.pem" [ec2-user@10.0.1.96](mailto:ec2-user@10.0.1.96) “its private ssh.

after connect ssh, check inertnet accesss or not.

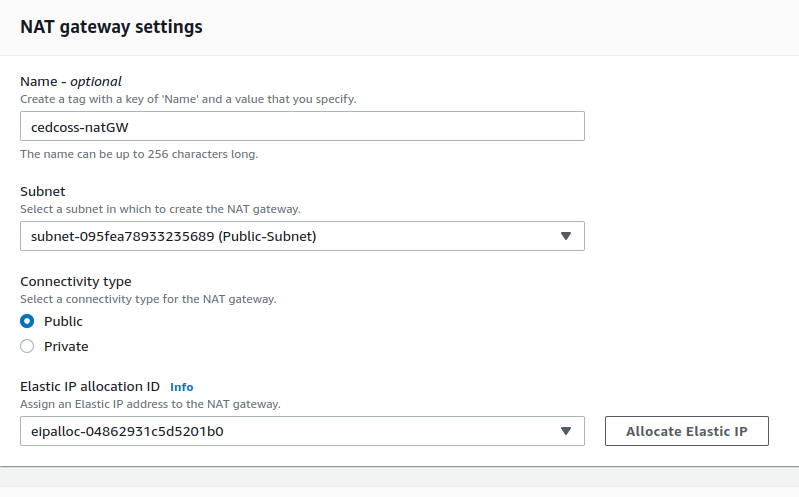


Here we see internet now accessible in private subnet.

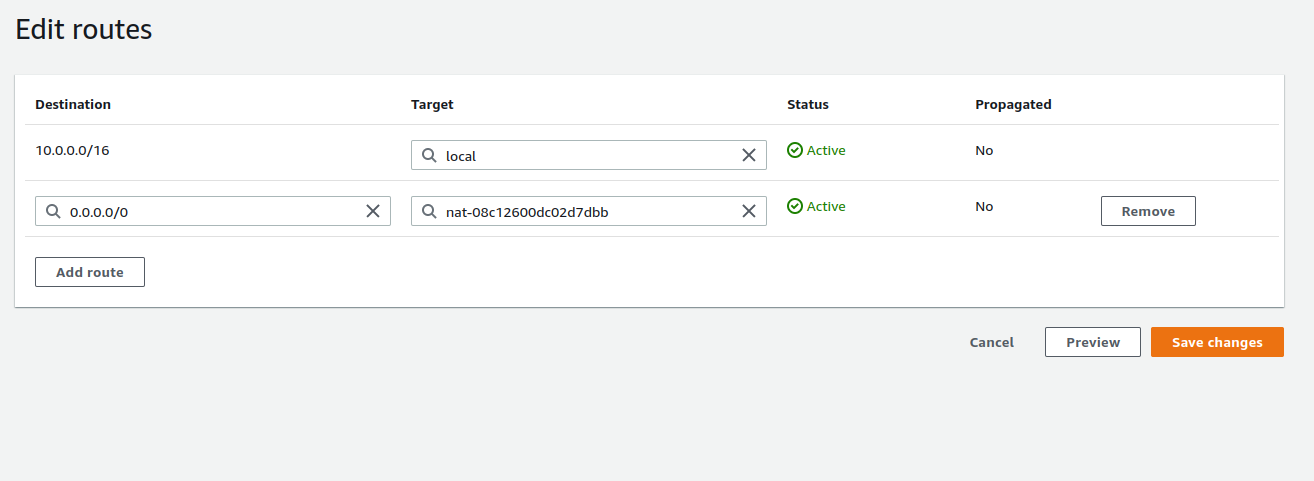
so now we have to create a **NAT GATEWAY**

Go to VPC dashboard & choose NAT Gateway ---- > click on create NAT Gateway.

Create NAT Gateway name & select Public Subnet ---- > Allocate Elastic IP for our Nat Gateway ----> now click on create Nat Gateway



After creating Nate Gateway ---- > got to route table click on private route table --> go inside of **private route table** ---> click on route (by default you are there) --> click on edite route ---> add route ---> in the **target box select nat gateway**



After active your Nat Gateway ---> check on your terrminal, your private instance (subnet accessible from internet)

Done!