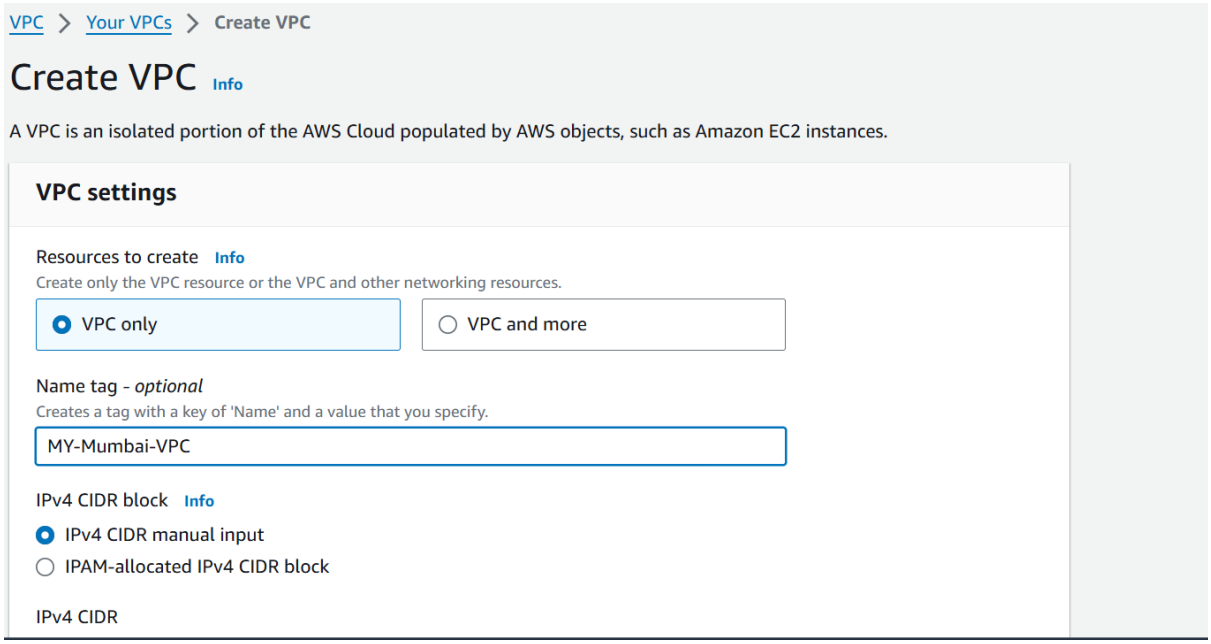
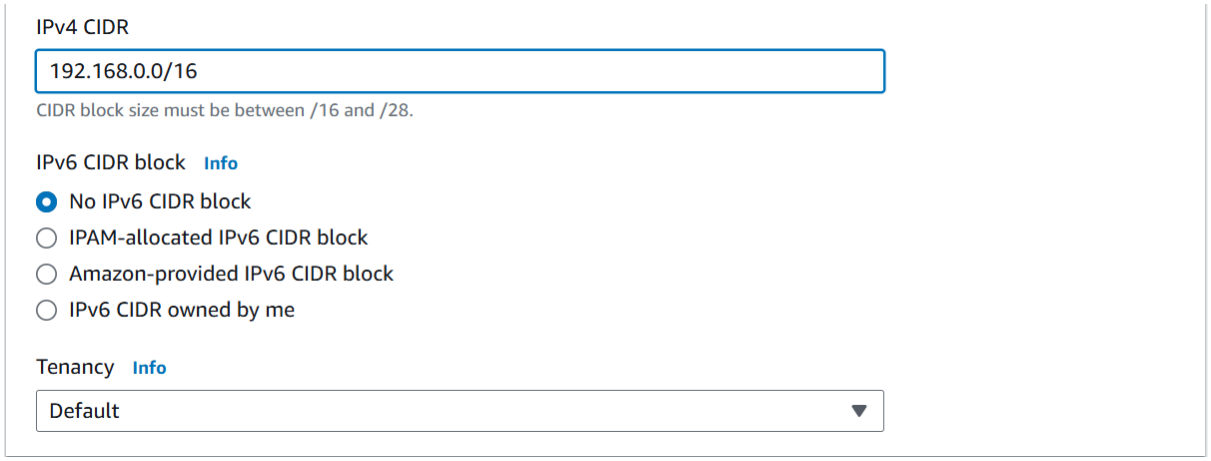
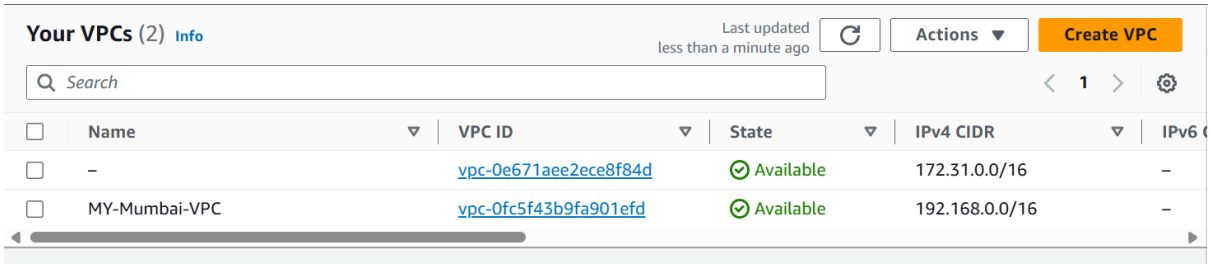
VPC

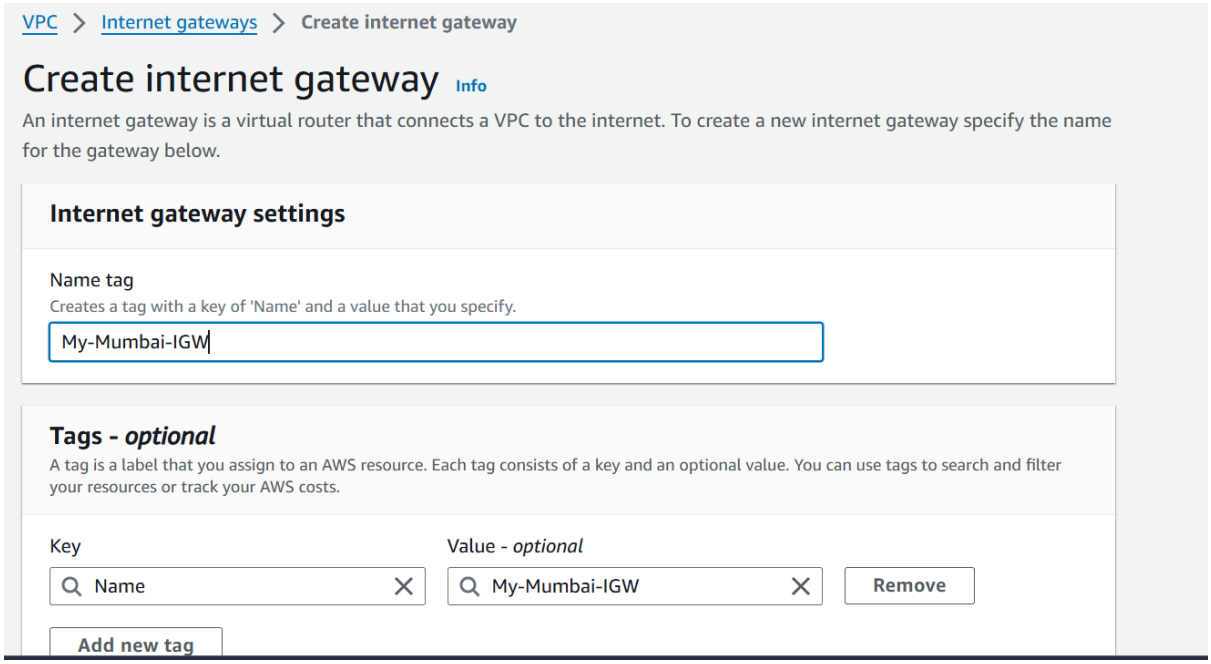
1. Create VPC

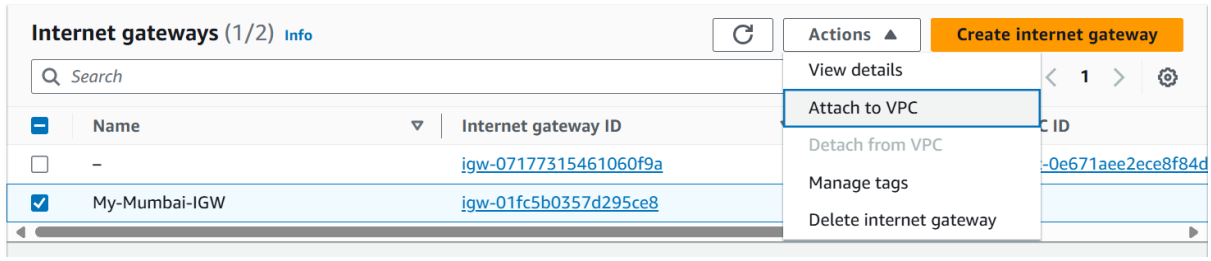


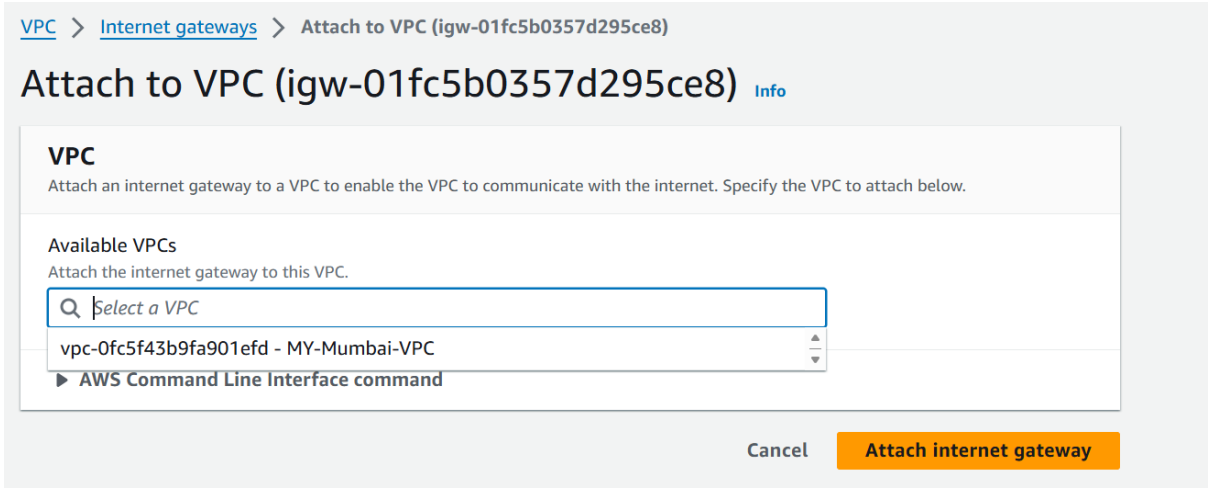




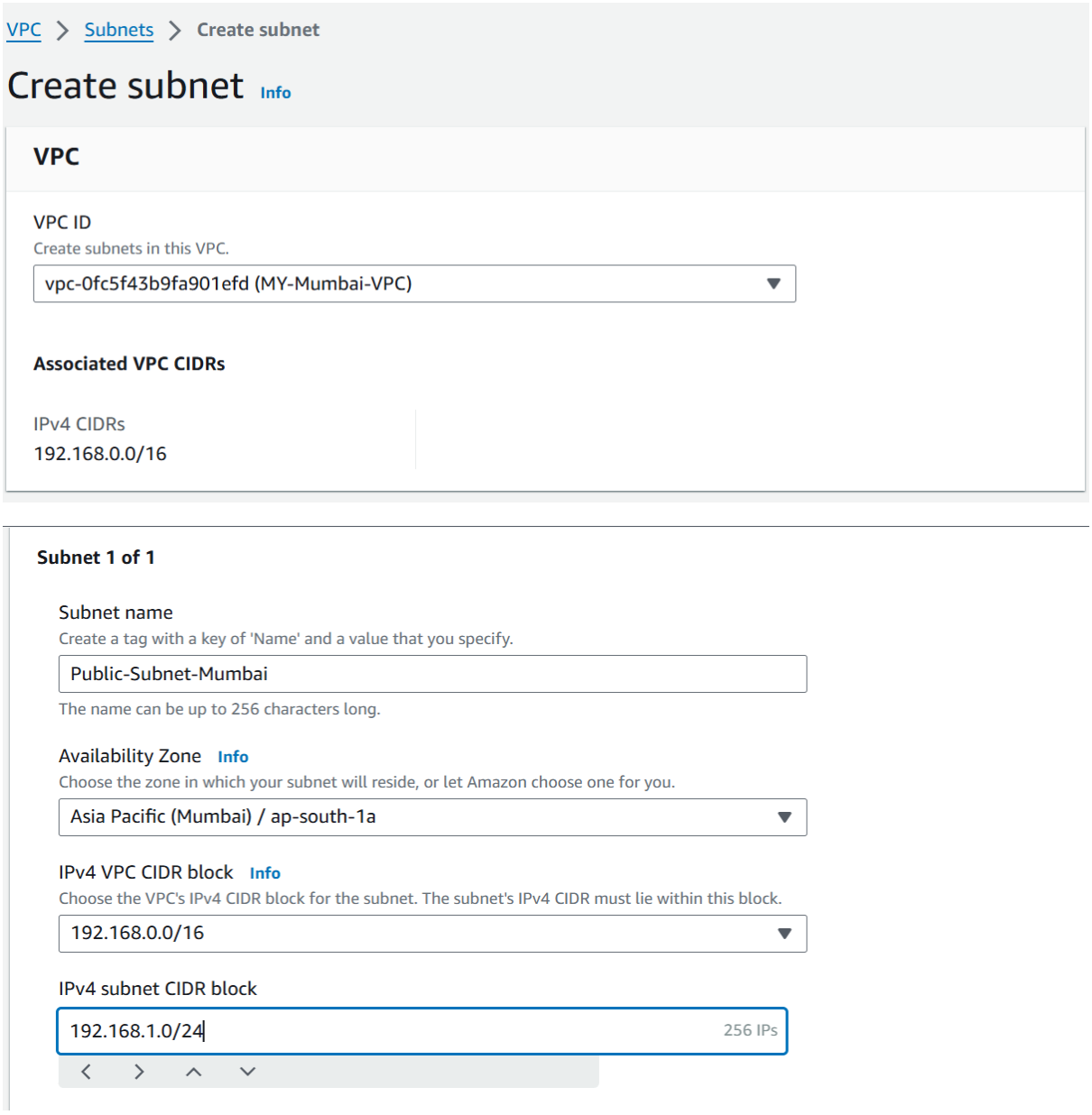
2. Create Internet Gateway (IGW)







3. Creating Public and Private Subnets



Subnet 2 of 2

Subnet name

Create a tag with a key of 'Name' and a value that you specify.

Private-Subnet-Mumbai

The name can be up to 256 characters long.

Availability Zone Info

Choose the zone in which your subnet will reside, or let Amazon choose one for you.

Asia Pacific (Mumbai) / ap-south-1b

IPv4 VPC CIDR block Info

Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

192.168.0.0/16

IPv4 subnet CIDR block

192.168.2.0/24 256 IPs

Subnets (5) Info

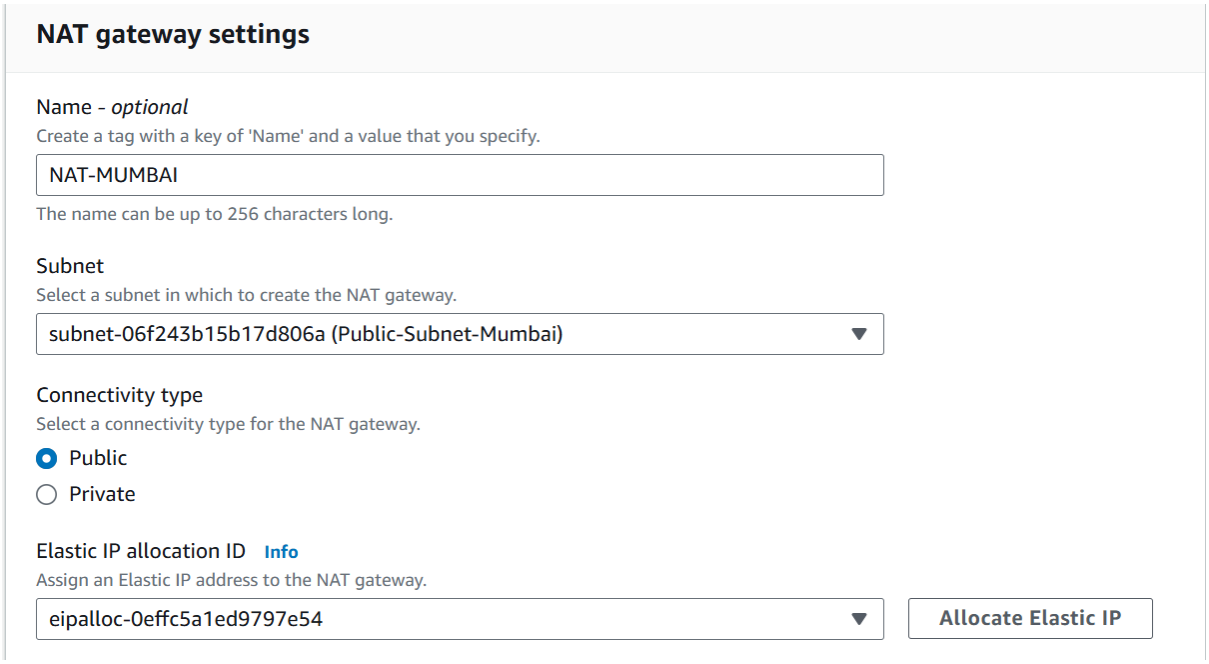
Last updated less than a minute ago | Actions | Create subnet

Find resources by attribute or tag

1

Name	Subnet ID	State	VPC
–	subnet-05e5889bf6211dee0	Available	vpc-0e671aee2ece8f84d
–	subnet-051c7044b0230918d	Available	vpc-0e671aee2ece8f84d
Private-Subnet-Mumbai	subnet-08c1547242085bd01	Available	vpc-0fc5f43b9fa901efd | MY-
Public-Subnet-Mumbai	subnet-06f243b15b17d806a	Available	vpc-0fc5f43b9fa901efd | MY-

4. Creating NAT Gateway



[Click on Allocate Elastic IP]

5. Create Routing Tables

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

Private-RouteTable

VPC

The VPC to use for this route table.

vpc-0fc5f43b9fa901efd (MY-Mumbai-VPC)

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*

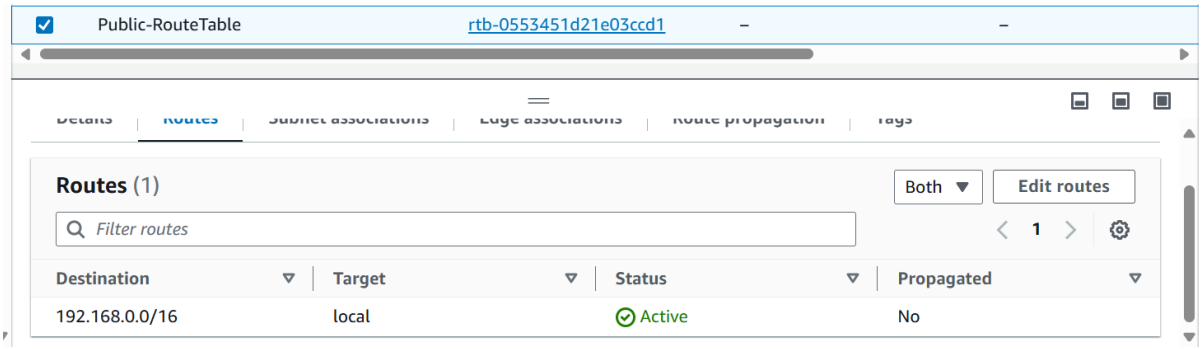
Create a tag with a key of 'Name' and a value that you specify.

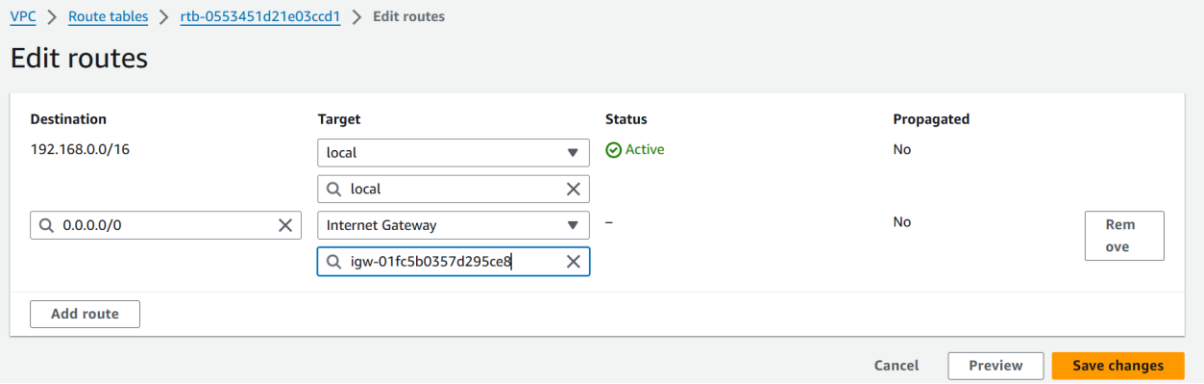
Public-RouteTable

VPC

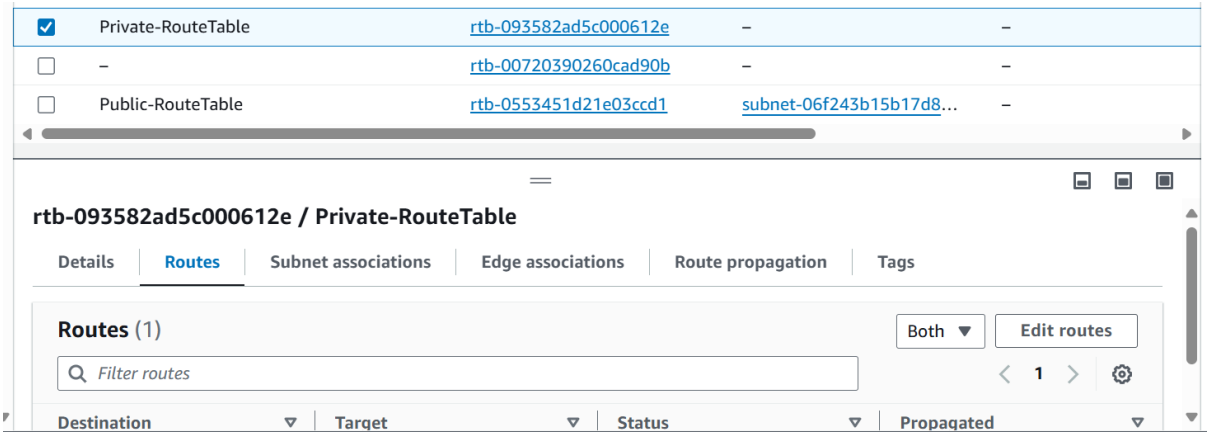
The VPC to use for this route table.

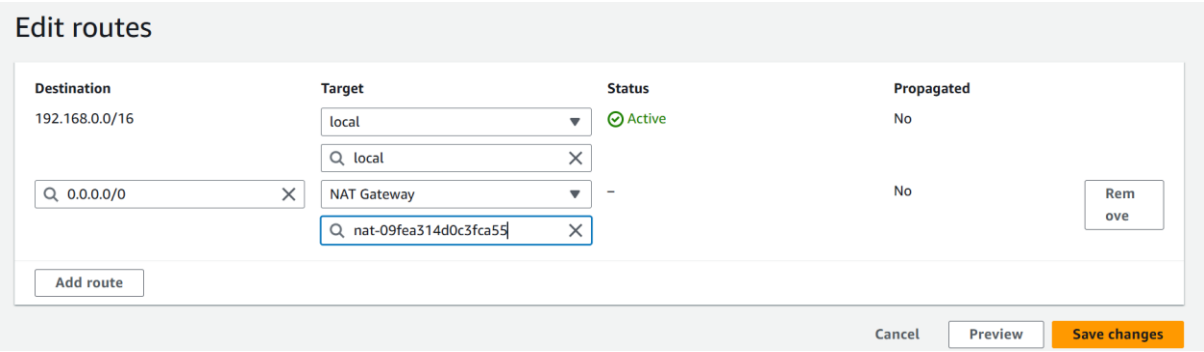
vpc-0fc5f43b9fa901efd (MY-Mumbai-VPC)



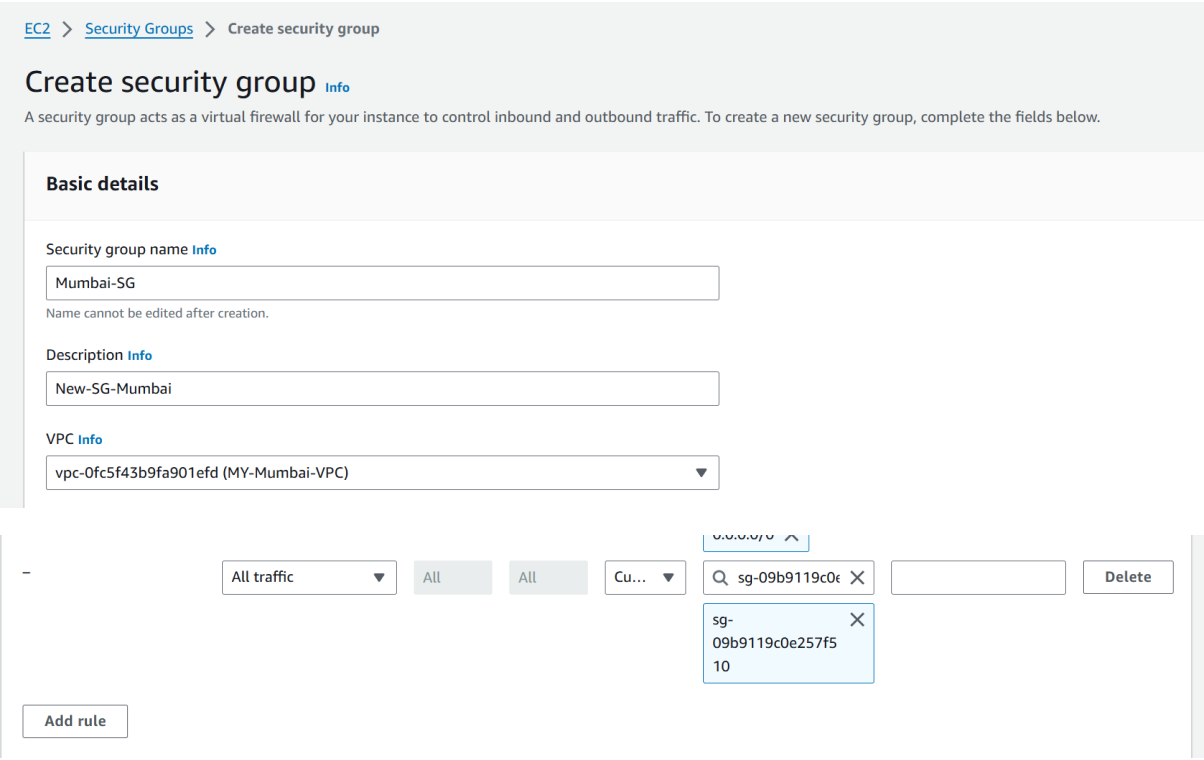


[Added Public subnet association to Public Route table]



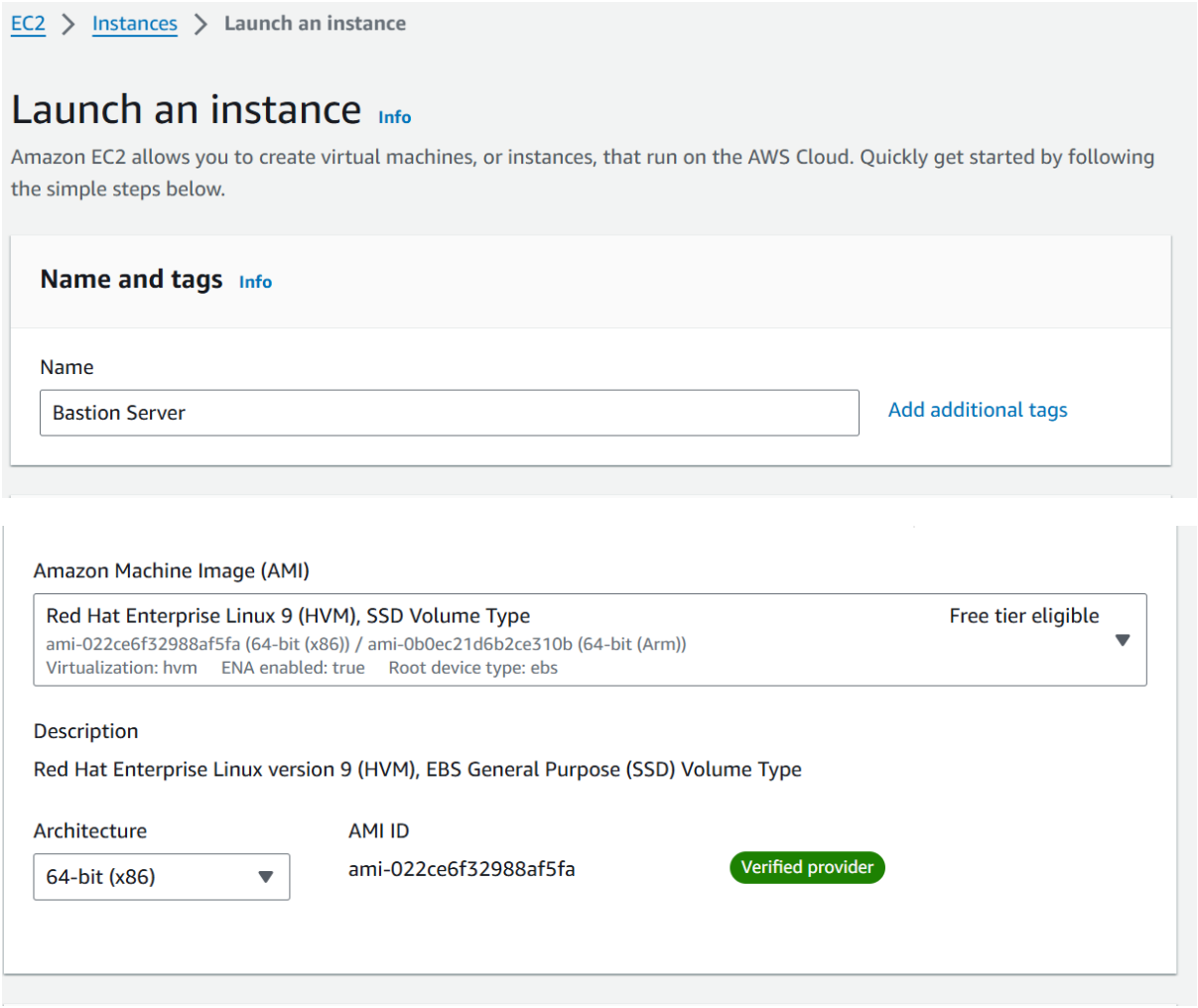


6. Creating Security Group



[Inbound rule must be self also]

7. Creating EC2 Instances – Bostion/ Jump Instance + Private Instance



Network settings Info

VPC - *required* Info

vpc-0fc5f43b9fa901efd (MY-Mumbai-VPC)
192.168.0.0/16

Subnet Info

subnet-06f243b15b17d806a Public-Subnet-Mumbai
VPC: vpc-0fc5f43b9fa901efd Owner: 966481983228
Availability Zone: ap-south-1a Zone type: Availability Zone
IP addresses available: 250 CIDR: 192.168.1.0/24)

Create new subnet

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

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 Info

Select security groups

Mumbai-SG sg-09b9119c0e257f510
VPC: vpc-0fc5f43b9fa901efd

Compare security group rules

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

EC2 > Instances > Launch an instance

Launch an instance Info

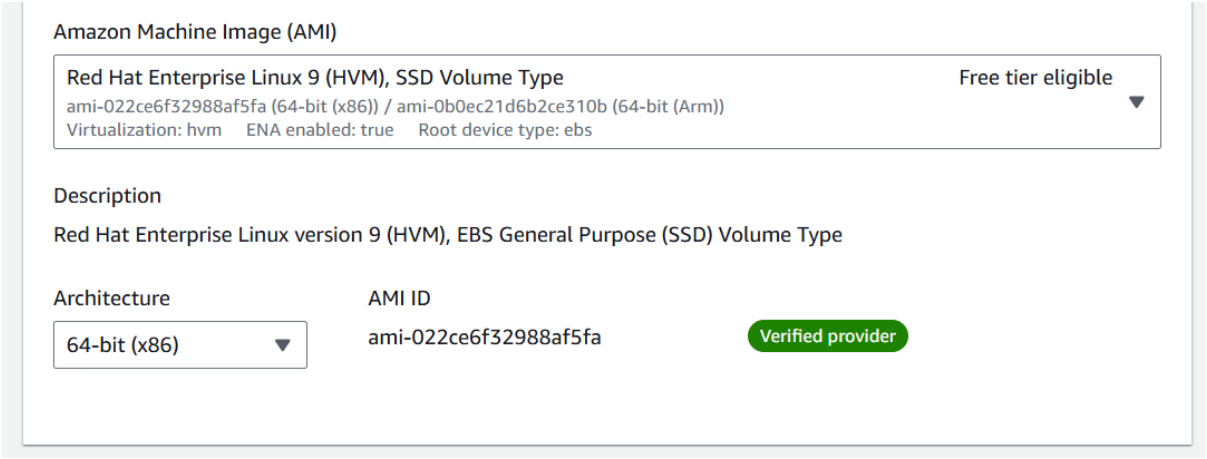
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

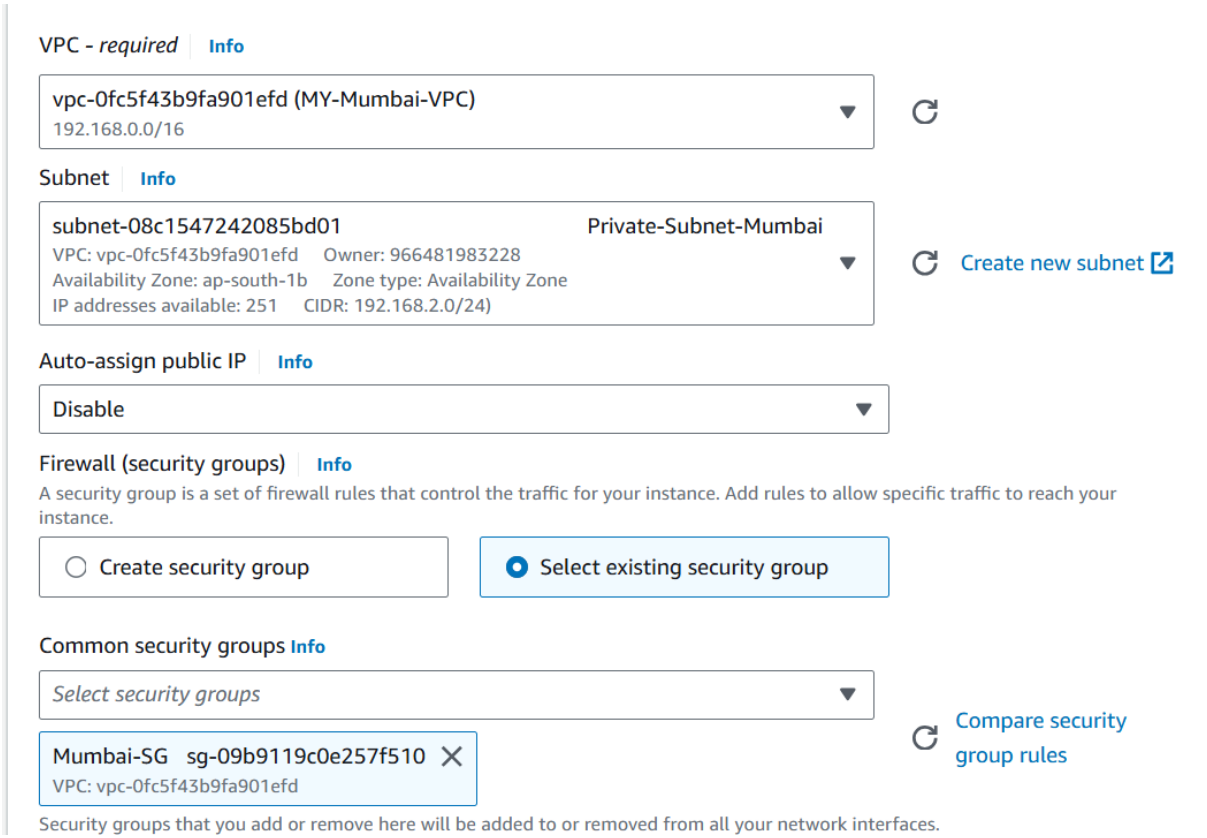
Name and tags Info

Name

Private Server

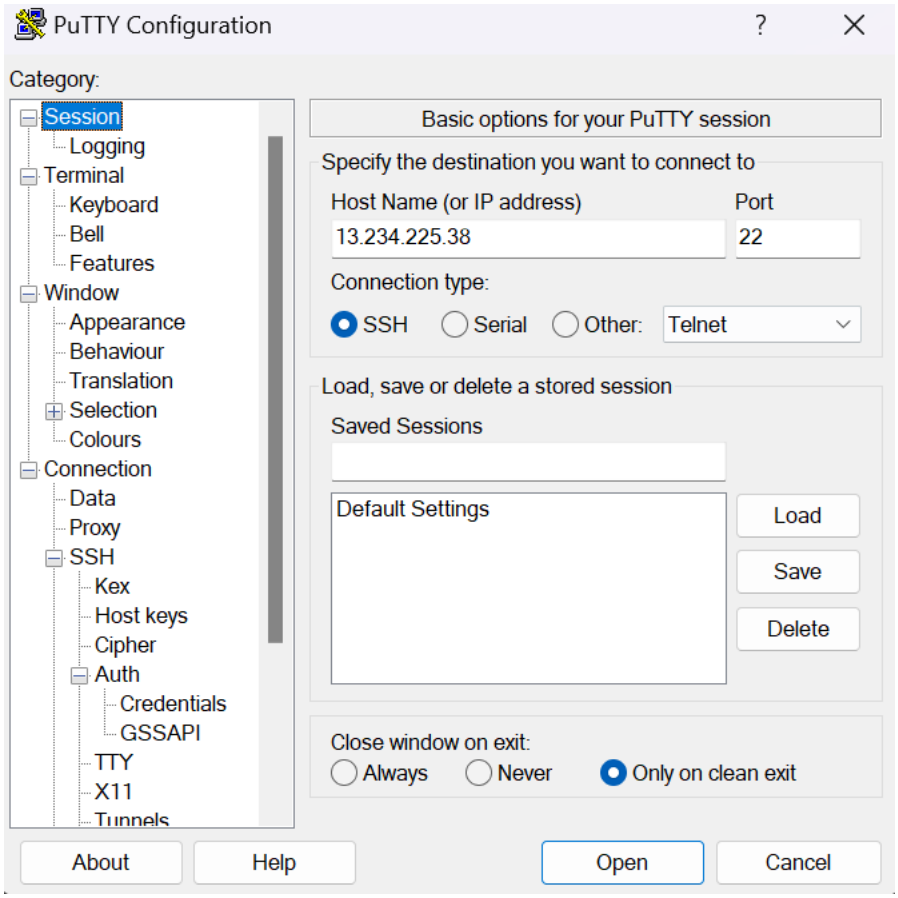
Add additional tags

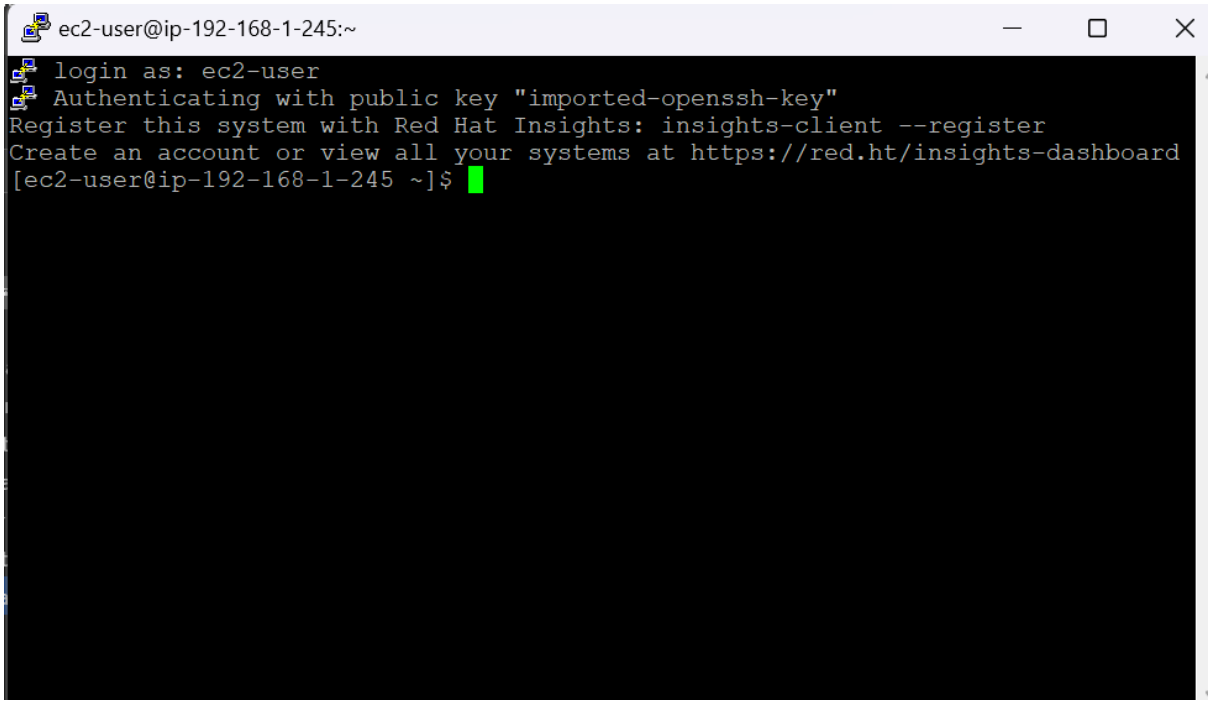




8. Connecting to Bastion Server

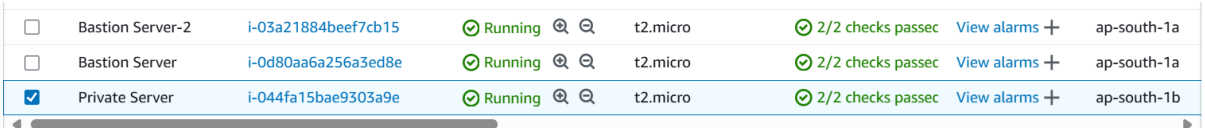
If our VPC is successful then only our bastion server will work



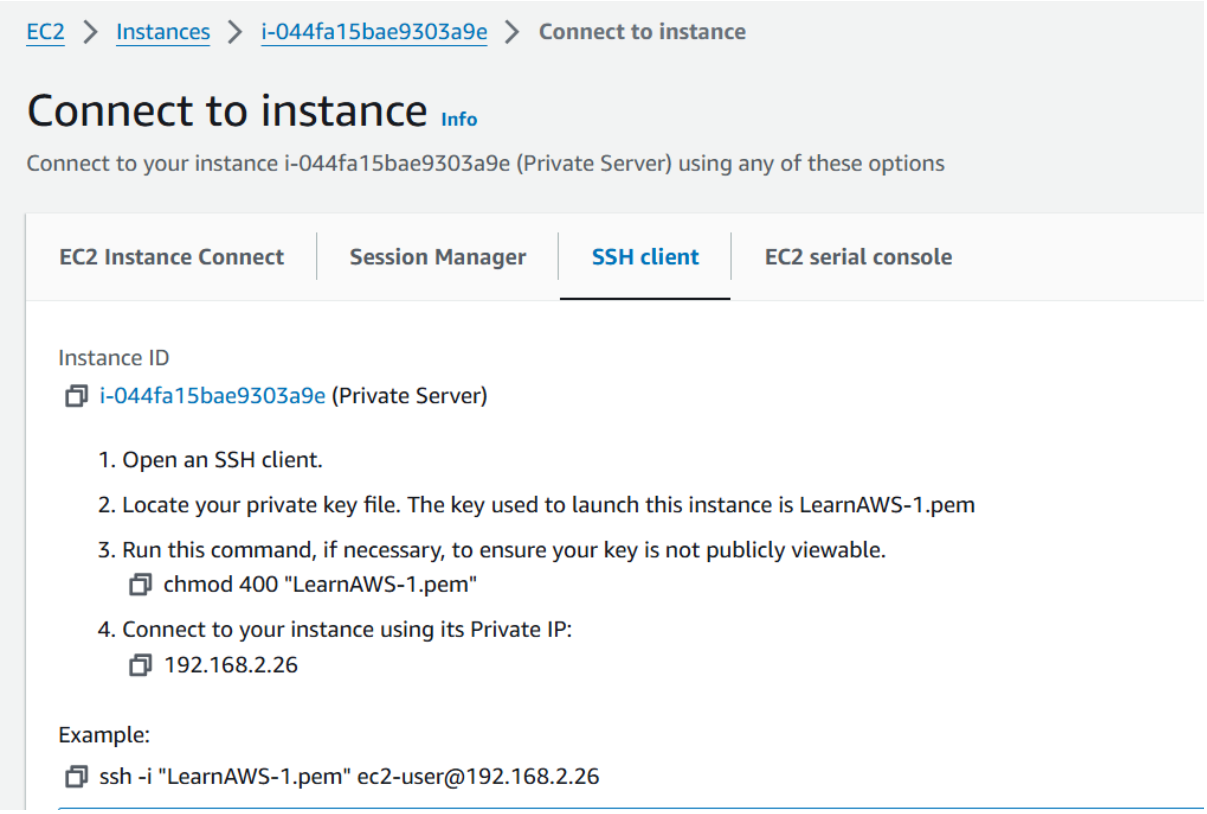


[We can see our IP is started with 192.168.1.---] that means public subnet.

// Now we will try to connect to Private server using Bostion server



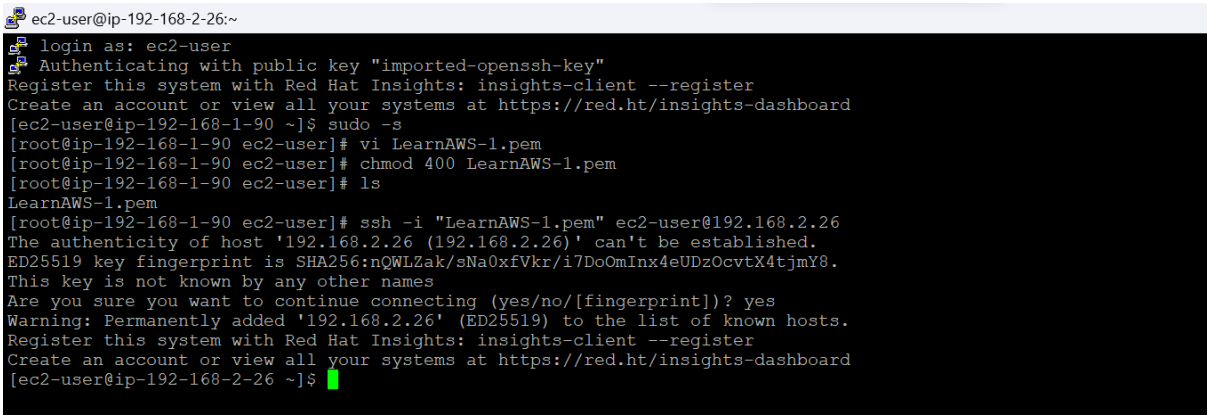
[Press Connect]



[Copy Example Line & paste in Bastion server]

[Permission Denied→ we need to have the pem file inside the Bastion server

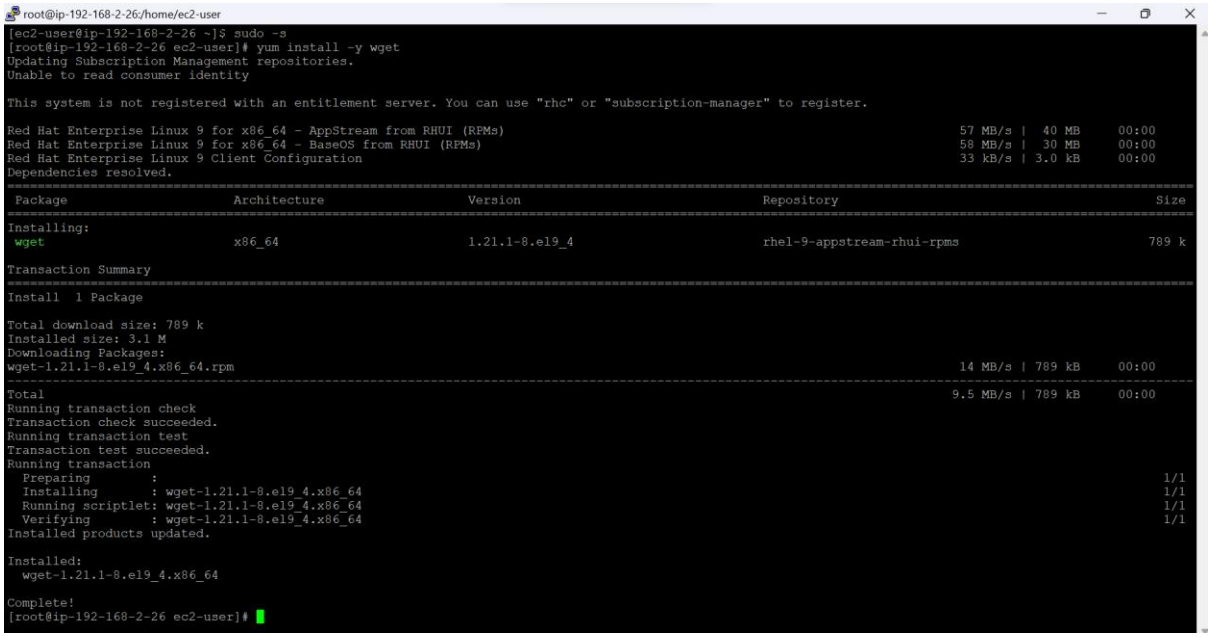
For that simple way is to copy the complete pemfile data and create a new file in the bastion server and then use the command again→ It will work]



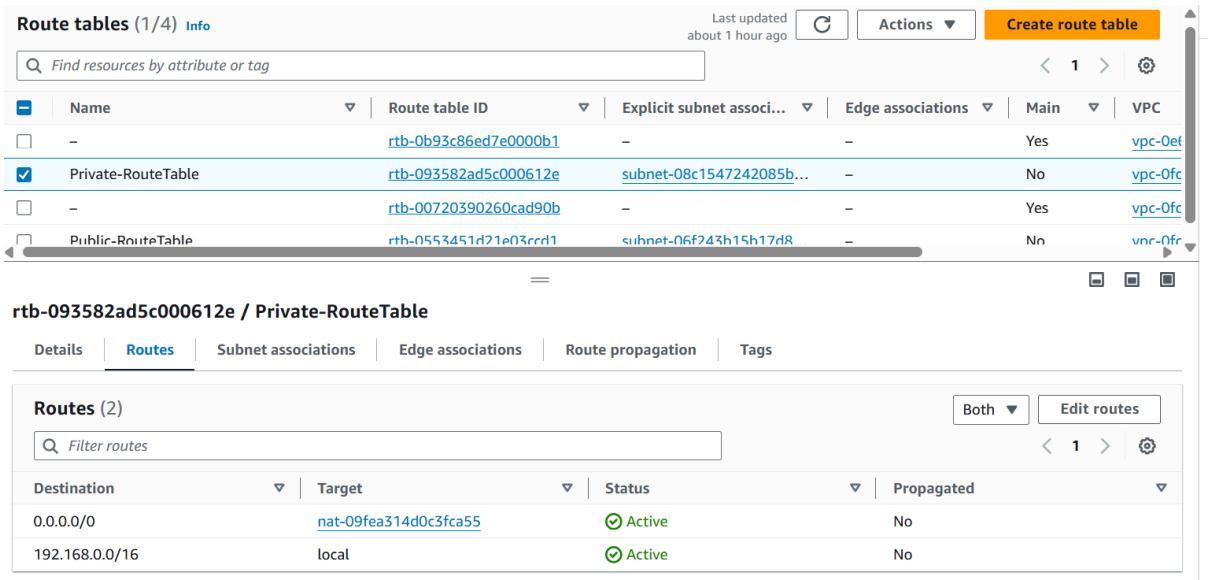
Connected to Private Server Using Bostion server

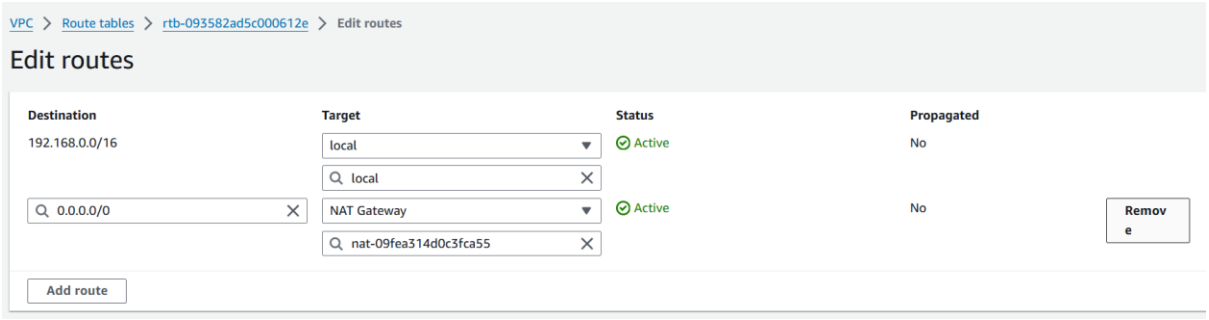
We have attached NAT gateway to the Private Route table which is connected to Private subnets and we are in private server which is located in private subnet.

NAT is present that means we have internet access, to test it will download a sample in the ec2

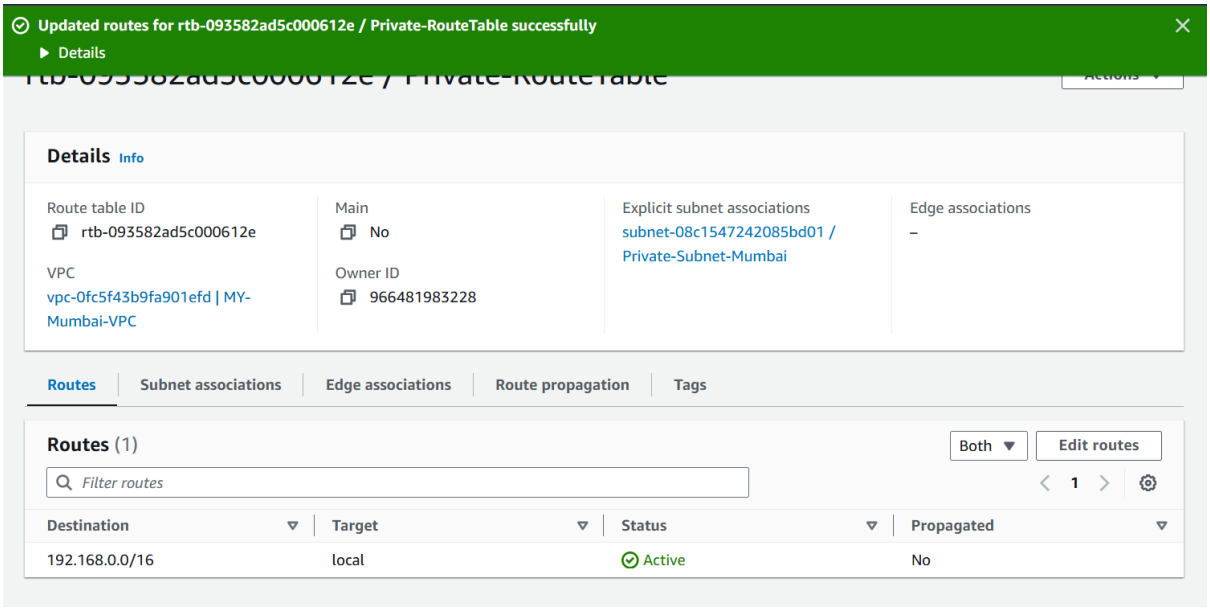


Now we try to stop the internet access, for that we need to remove the routes access (NAT) from private route table.

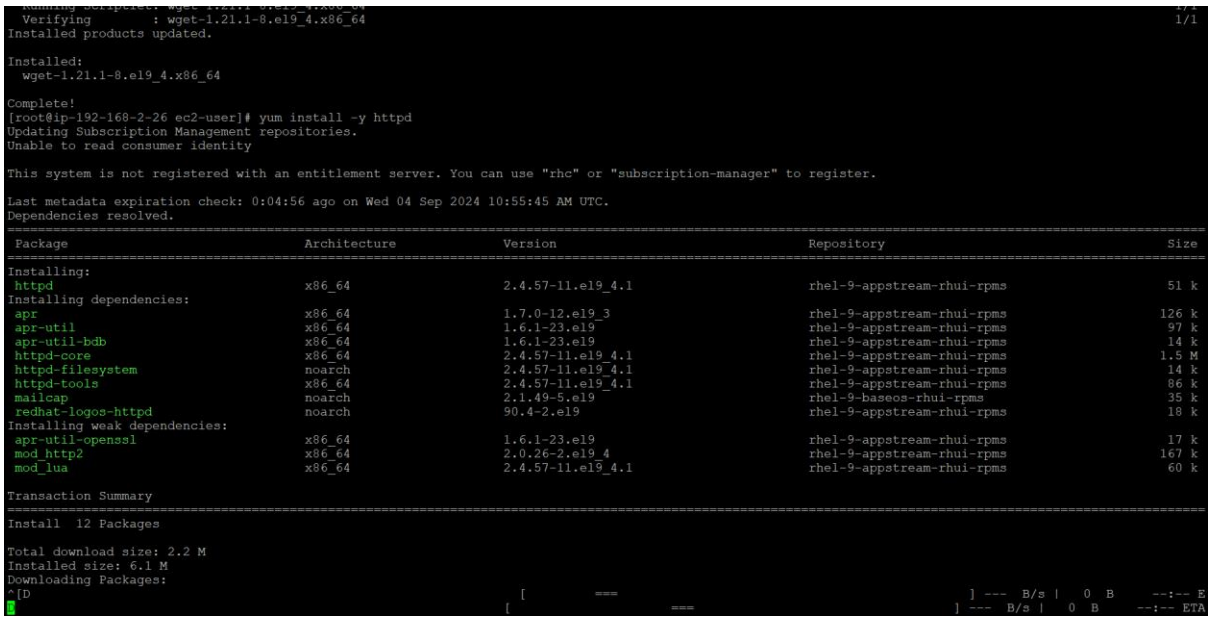


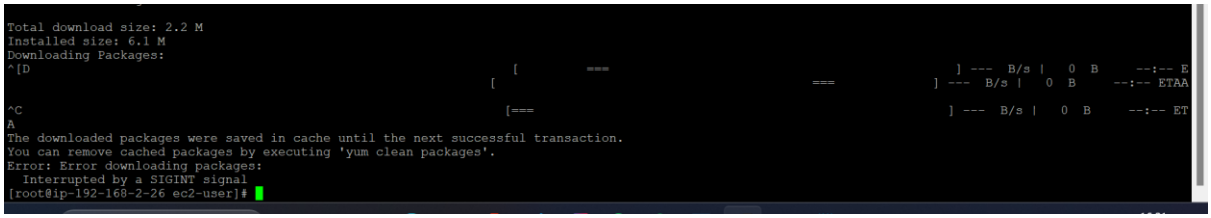


[Remove NAT Gateway]

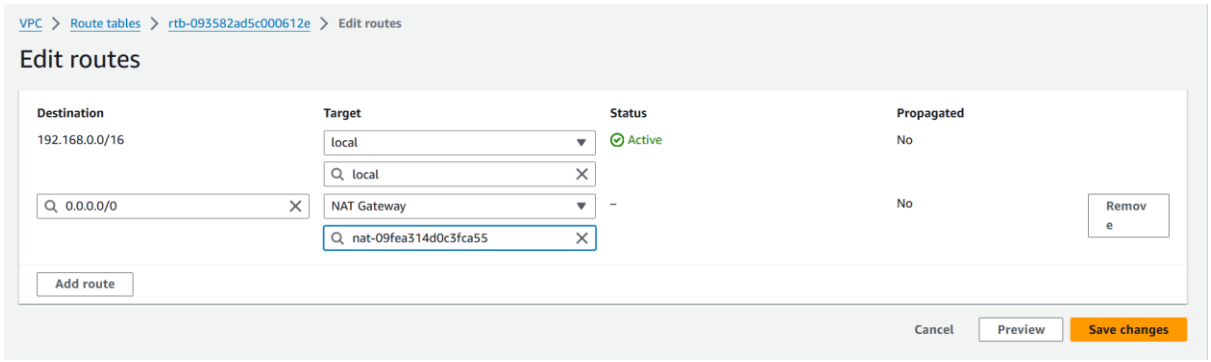


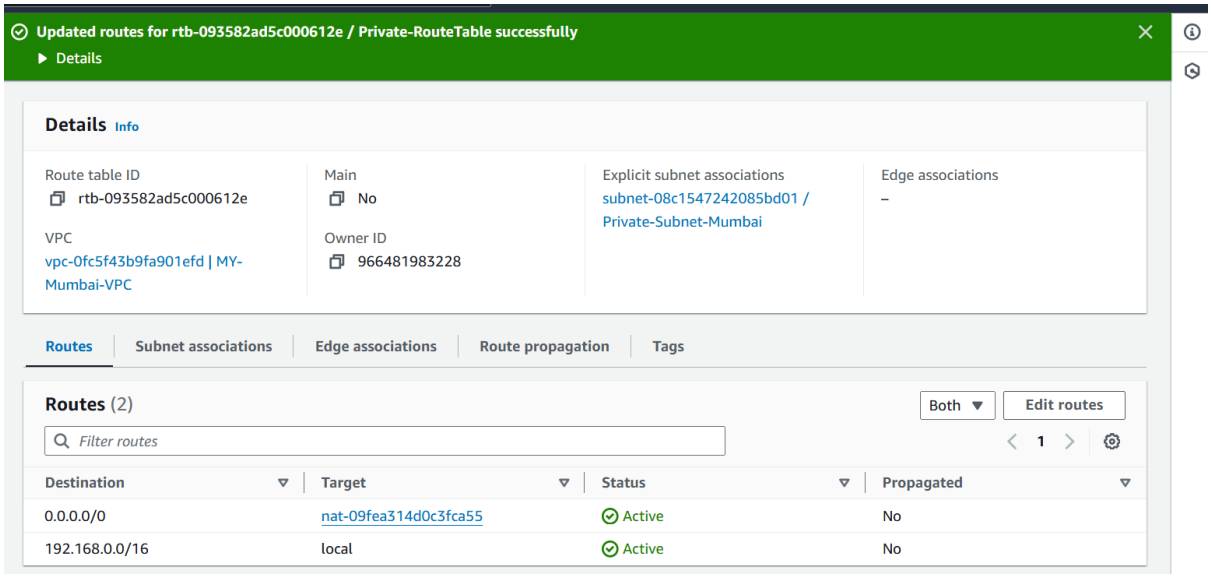
Now we will test the Private server internet access





To get internet access again just add the NAT gateway again in the routes





Check Internet access is working or not..

```
(12/12): httpd-core-2.4.57-11.el9_4.1.x86_64.rpm                                    31 MB/s | 1.5 MB     00:00
--------------------------------------------------------------------------------------------------------------------------
Total                                                                               13 MB/s | 2.2 MB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                          1/1
  Installing       : apr-1.7.0-12.el9_3.x86_64                                                                1/12
  Installing       : apr-util-bdb-1.6.1-23.el9.x86_64                                                         2/12
  Installing       : apr-util-openssl-1.6.1-23.el9.x86_64                                                     3/12
  Installing       : apr-util-1.6.1-23.el9.x86_64                                                             4/12
  Installing       : httpd-tools-2.4.57-11.el9_4.1.x86_64                                                     5/12
  Installing       : mailcap-2.1.49-5.el9.noarch                                                              6/12
  Running scriptlet: httpd-filesystem-2.4.57-11.el9_4.1.noarch                                                7/12
  Installing       : httpd-filesystem-2.4.57-11.el9_4.1.noarch                                                7/12
  Installing       : httpd-core-2.4.57-11.el9_4.1.x86_64                                                      8/12
  Installing       : mod_lua-2.4.57-11.el9_4.1.x86_64                                                         9/12
  Installing       : redhat-logos-httpd-90.4-2.el9.noarch                                                    10/12
  Installing       : mod_http2-2.0.26-2.el9_4.x86_64                                                         11/12
  Installing       : httpd-2.4.57-11.el9_4.1.x86_64                                                          12/12
  Running scriptlet: httpd-2.4.57-11.el9_4.1.x86_64                                                          12/12
  Verifying        : apr-util-1.6.1-23.el9.x86_64                                                             1/12
  Verifying        : apr-util-bdb-1.6.1-23.el9.x86_64                                                         2/12
  Verifying        : apr-util-openssl-1.6.1-23.el9.x86_64                                                     3/12
  Verifying        : redhat-logos-httpd-90.4-2.el9.noarch                                                     4/12
  Verifying        : apr-1.7.0-12.el9_3.x86_64                                                                5/12
  Verifying        : mod_http2-2.0.26-2.el9_4.x86_64                                                          6/12
  Verifying        : httpd-2.4.57-11.el9_4.1.x86_64                                                           7/12
  Verifying        : httpd-core-2.4.57-11.el9_4.1.x86_64                                                      8/12
  Verifying        : httpd-filesystem-2.4.57-11.el9_4.1.noarch                                                9/12
  Verifying        : httpd-tools-2.4.57-11.el9_4.1.x86_64                                                    10/12
  Verifying        : mod_lua-2.4.57-11.el9_4.1.x86_64                                                        11/12
  Verifying        : mailcap-2.1.49-5.el9.noarch                                                             12/12
Installed products updated.

Installed:
  apr-1.7.0-12.el9_3.x86_64          apr-util-1.6.1-23.el9.x86_64             apr-util-bdb-1.6.1-23.el9.x86_64               apr-util-openssl-1.6.1-23.el9.x86_64
  httpd-2.4.57-11.el9_4.1.x86_64     httpd-core-2.4.57-11.el9_4.1.x86_64      httpd-filesystem-2.4.57-11.el9_4.1.noarch      httpd-tools-2.4.57-11.el9_4.1.x86_64
  mailcap-2.1.49-5.el9.noarch        mod_http2-2.0.26-2.el9_4.x86_64          mod_lua-2.4.57-11.el9_4.1.x86_64               redhat-logos-httpd-90.4-2.el9.noarch

Complete!
[root@ip-192-168-2-26 ec2-user]#
```

VPC - END POINTS

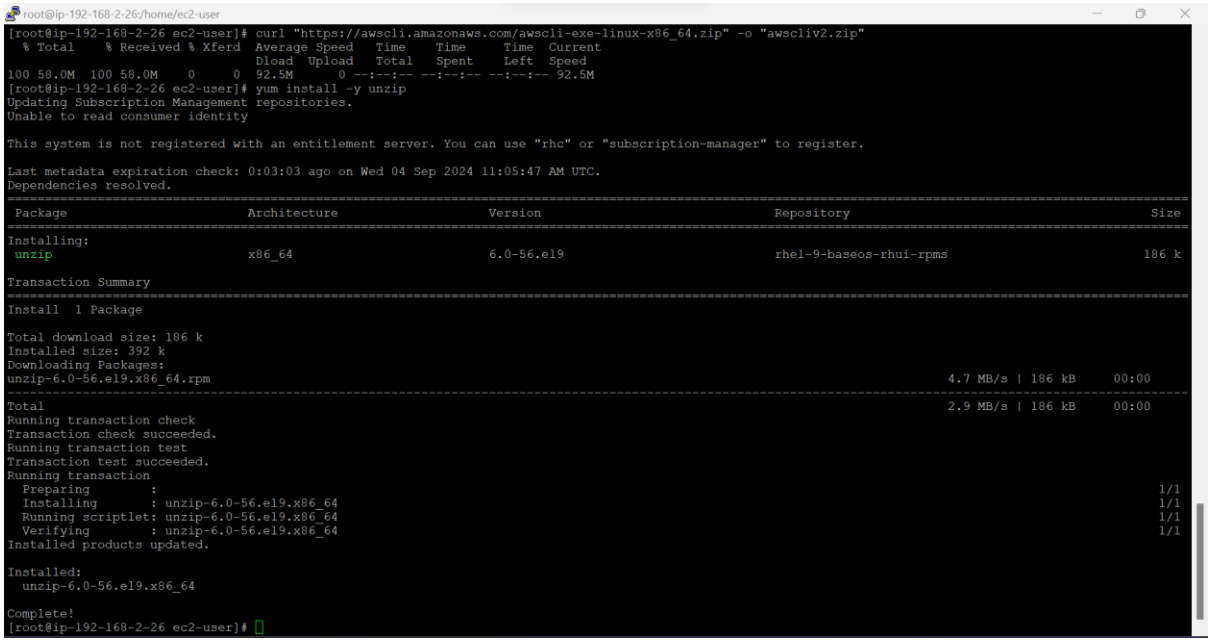
9. Install AWS cli in EC2

(Optional) The following command block downloads and installs the AWS CLI without first verifying the integrity of your download. To verify the integrity of your download, use the below step by step instructions.

To install the AWS CLI, run the following commands.

```
$ curl "https://awscli.amazonaws.com/awscli
unzip awscliv2.zip
sudo ./aws/install
```

To update your current installation of the AWS CLI, add your existing symlink and installer information to construct the `install` command using the `--bin-dir`, `--install-dir`, and `--update` parameters. The following



[unzip awscliv2.zip]

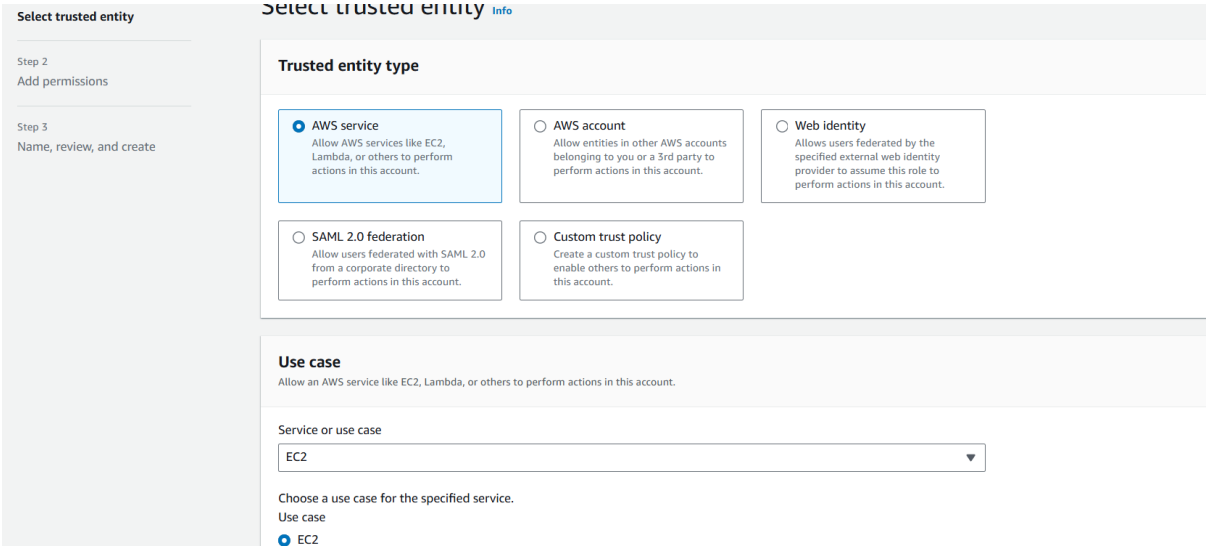
```
[root@ip-192-168-2-26 ec2-user]# ls
aws  awscliv2.zip
[root@ip-192-168-2-26 ec2-user]#
```

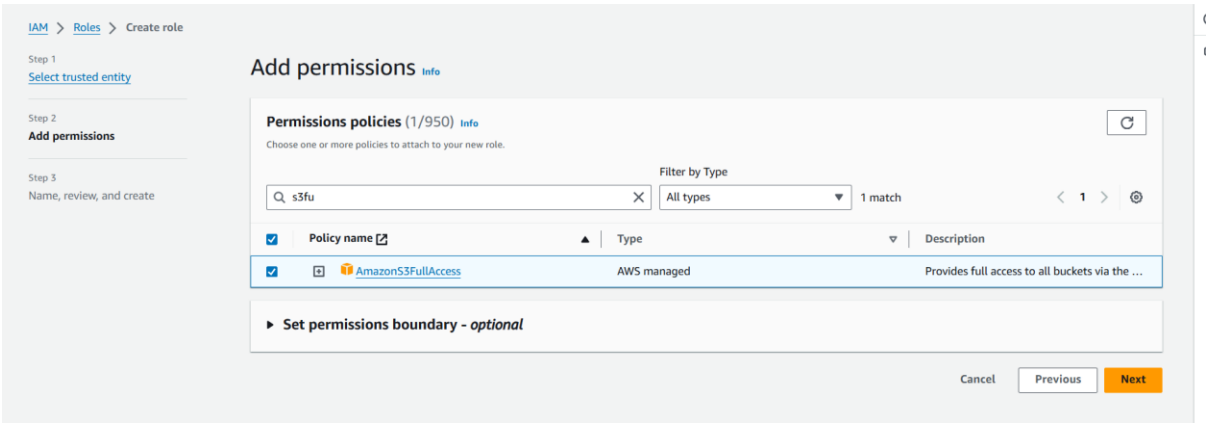
```
[root@ip-192-168-2-26 ec2-user]# sudo ./aws/install
You can now run: /usr/local/bin/aws --version
[root@ip-192-168-2-26 ec2-user]# ^C
[root@ip-192-168-2-26 ec2-user]# /usr/local/bin/aws --version
aws-cli/2.17.43 Python/3.11.9 Linux/5.14.0-427.20.1.el9_4.x86_64 exe/x86_64.rhel.9
[root@ip-192-168-2-26 ec2-user]#
```

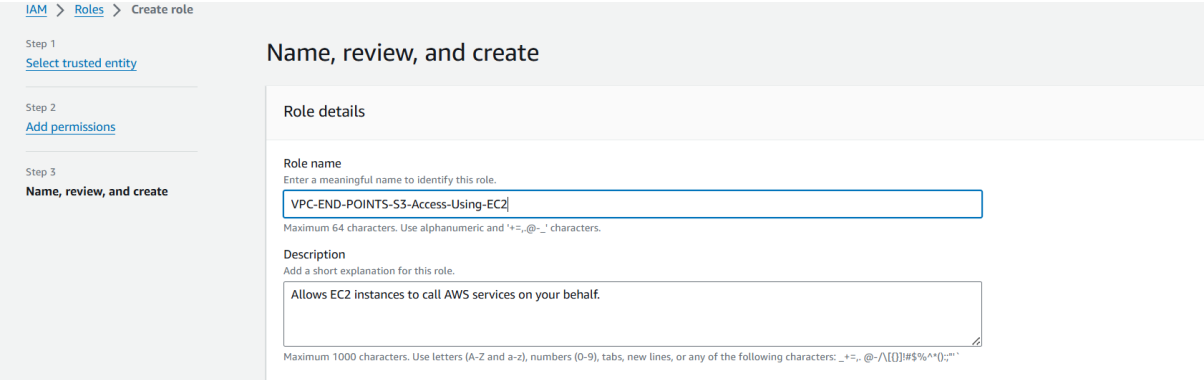
I want to access the AWS, for that we have ways

1. Access Key and super Key (Security Concerns)
2. Using IAM Roles (High Security)

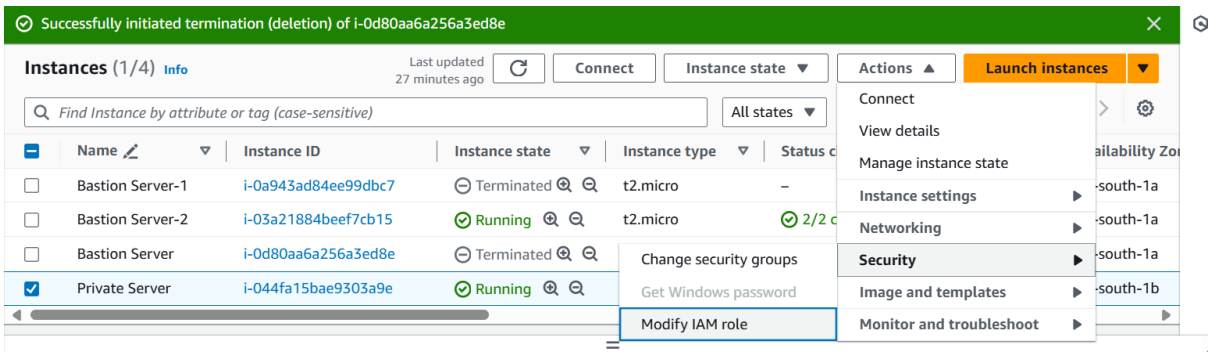
So lets attach a IAM role to the private server[bcz we are accessing the private server]

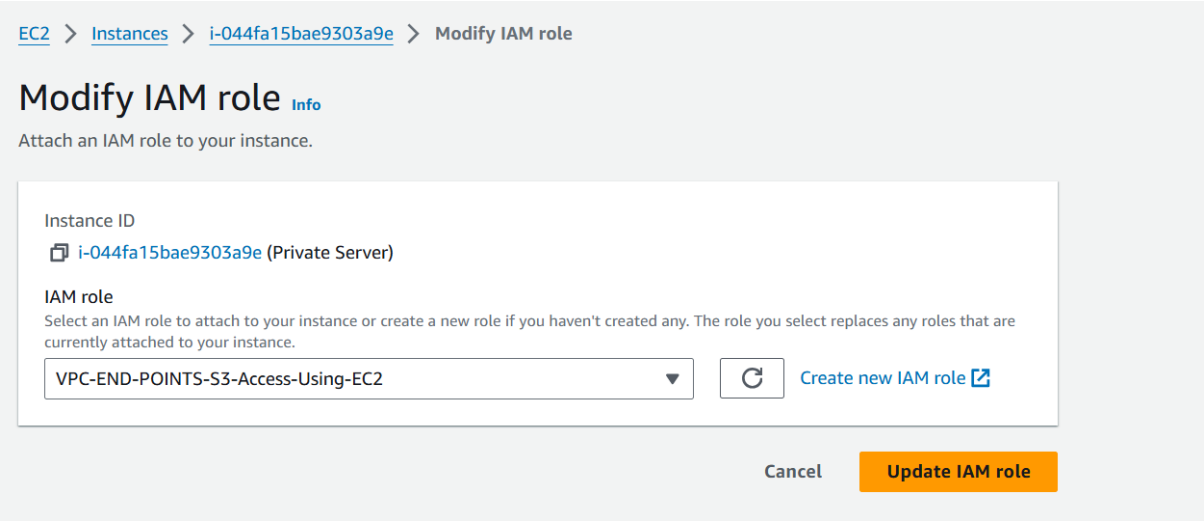






Now Attach the IAM role to EC2 [private server]





// Now we have the complete S3 access in Private server.

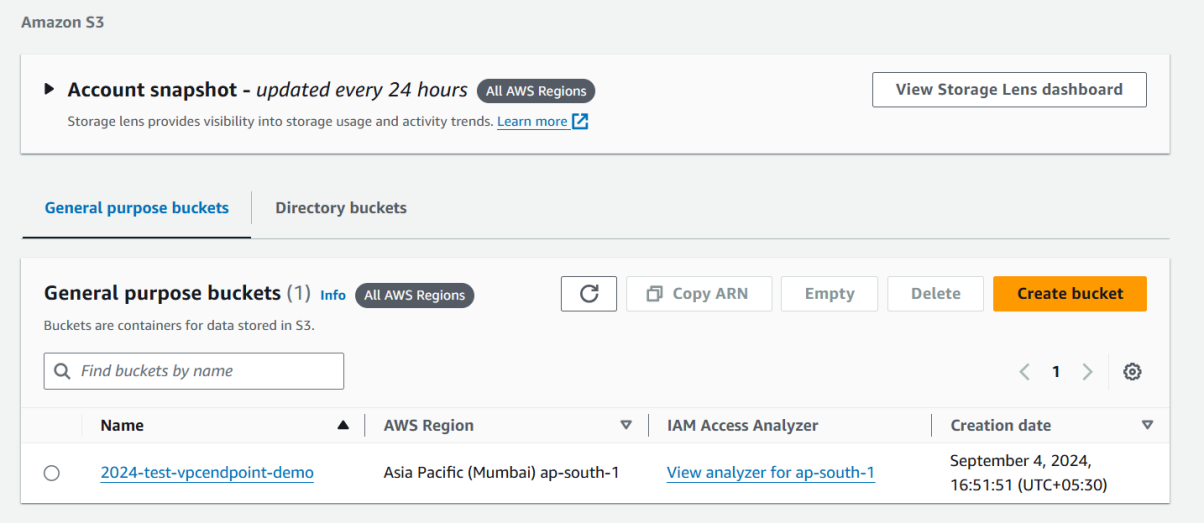
// Creating a Bucket using EC2

```
[root@ip-192-168-2-26 ec2-user]# /usr/local/bin/aws s3 mb s3://2024-test-vpcendpoint-demo --region ap-south-1
make_bucket: 2024-test-vpcendpoint-demo
[root@ip-192-168-2-26 ec2-user]#
```

[Bucket Created]

Bucket Name: 2024-test-vpcendpoint-demo

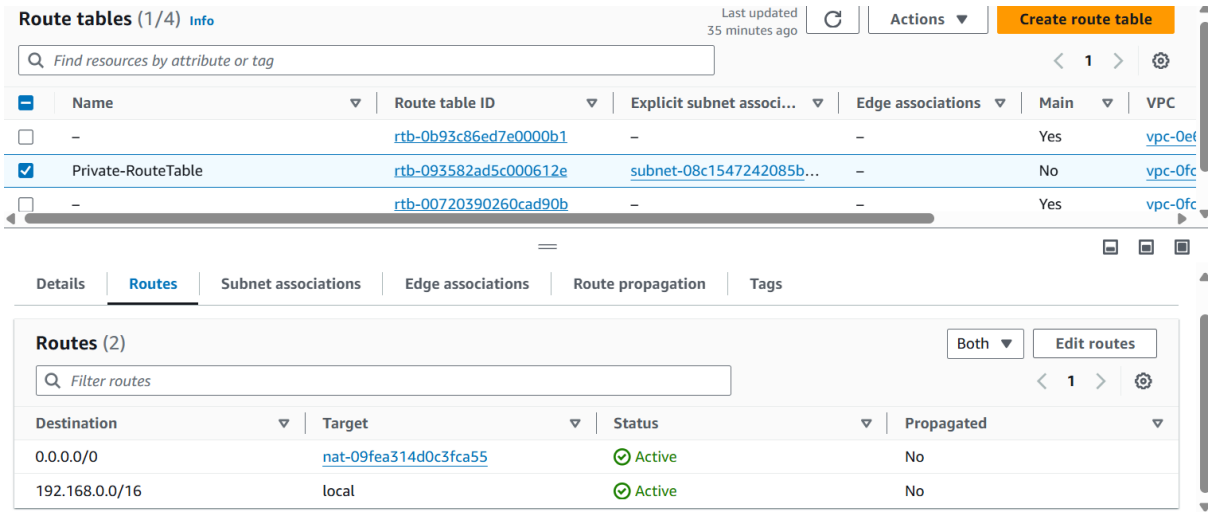
Region : ap-south-1 [Mumbai]

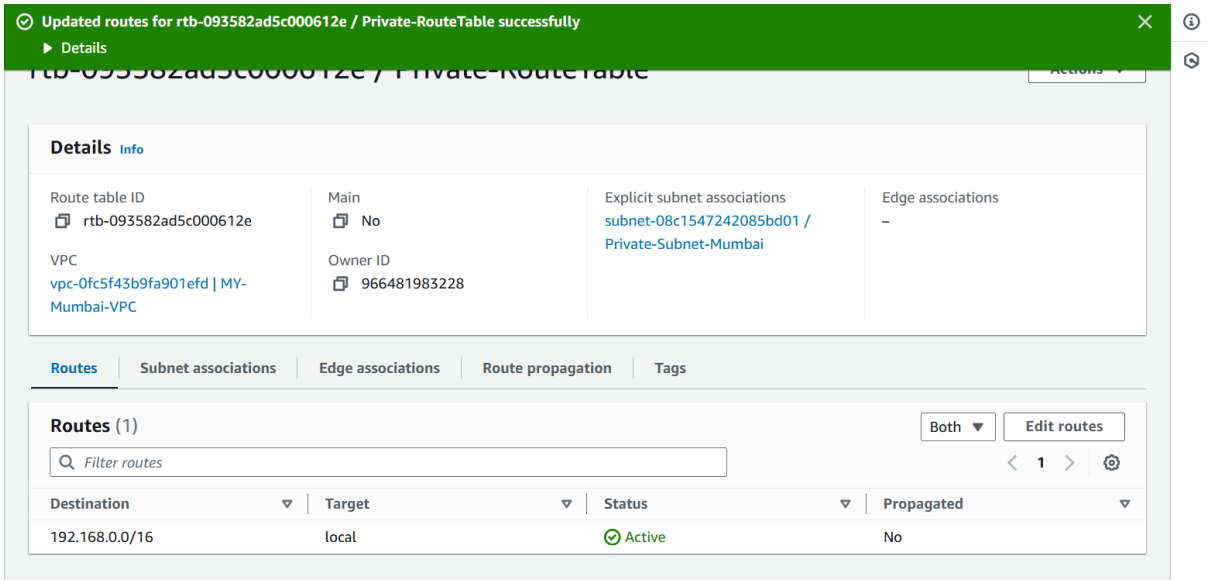


// I want to access the S3 with out internet

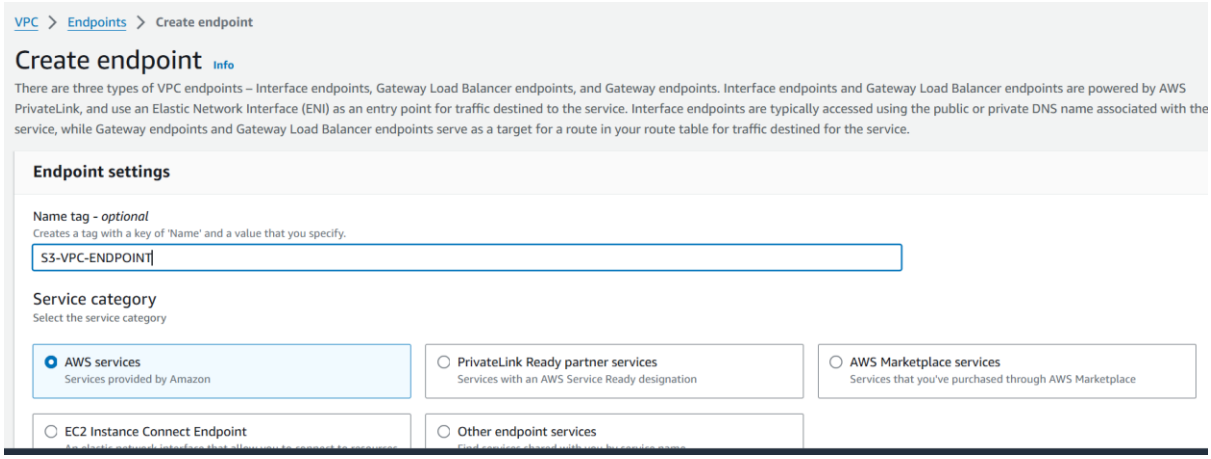
For this I have to create a END Point in VPC and attach it to the private sever

[Remove the NAT route from private routes]

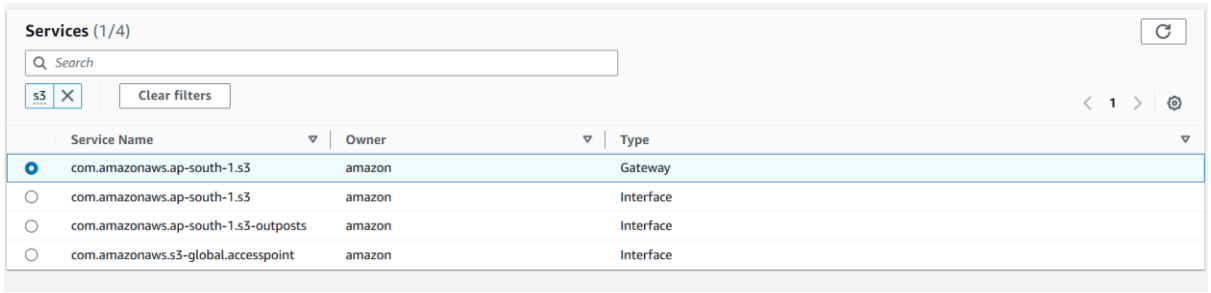


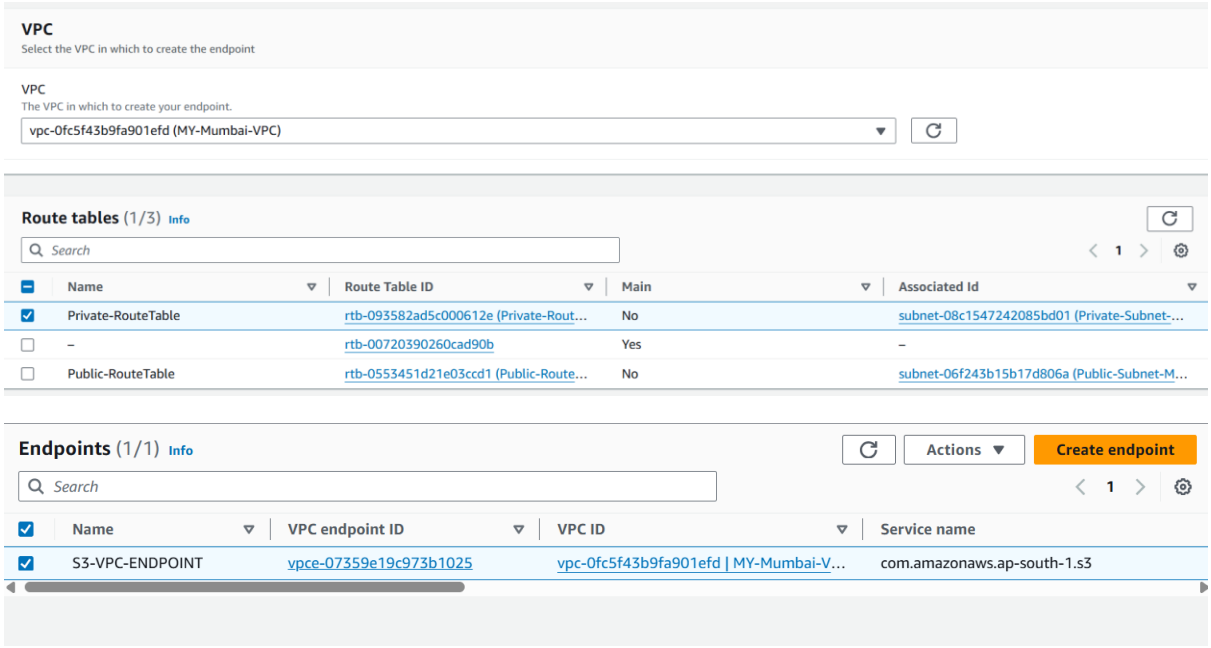


CREATE END POINTS

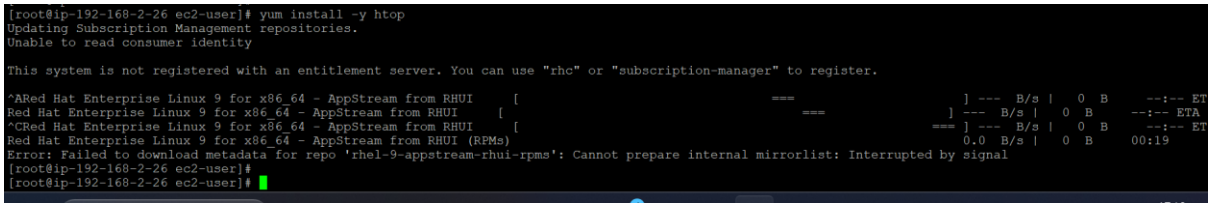


Using only Gateway Interface

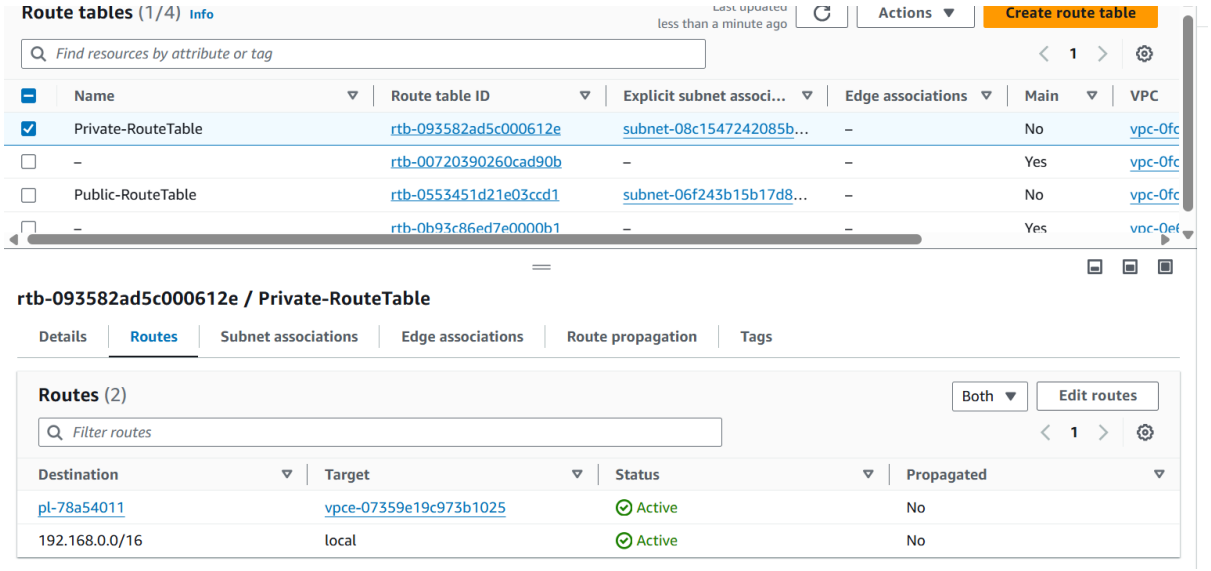




Internet Access is removed

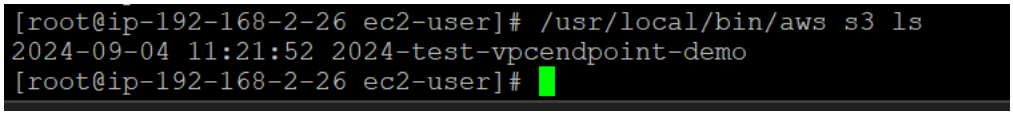


// But we can access the s3 because of VPC Endpoint [AWS Internet]

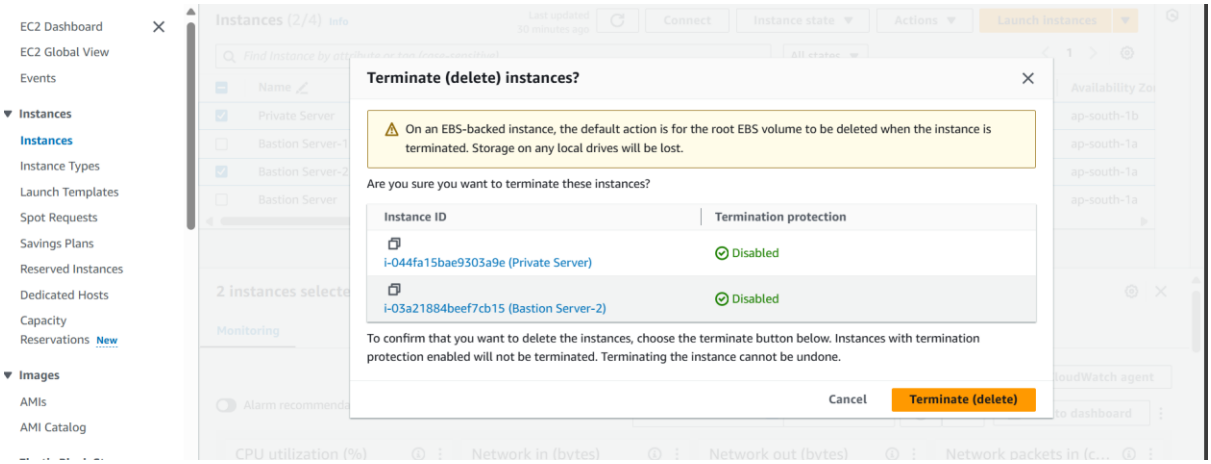


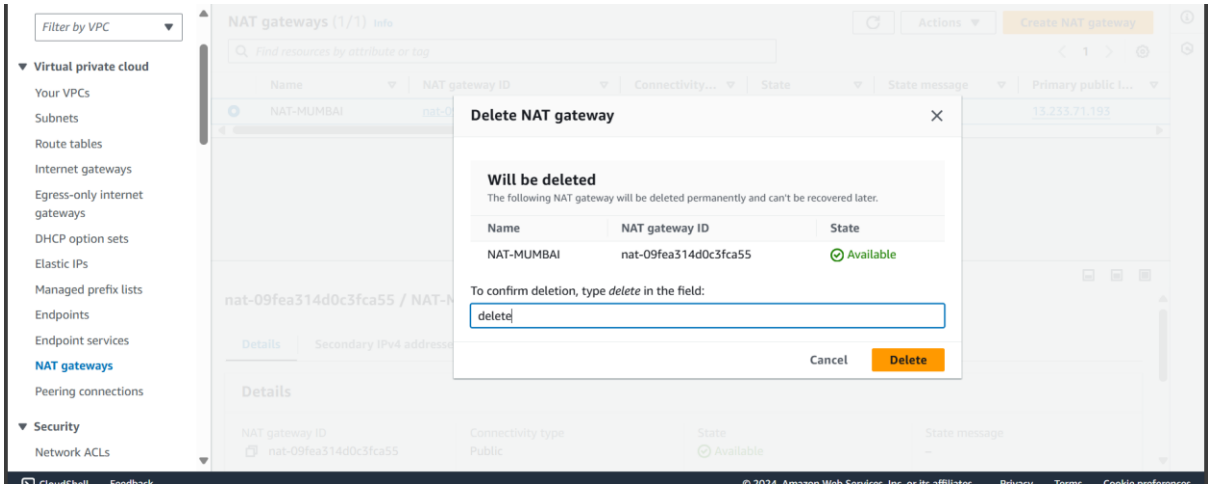
[Automatically assigned the Prefix List]

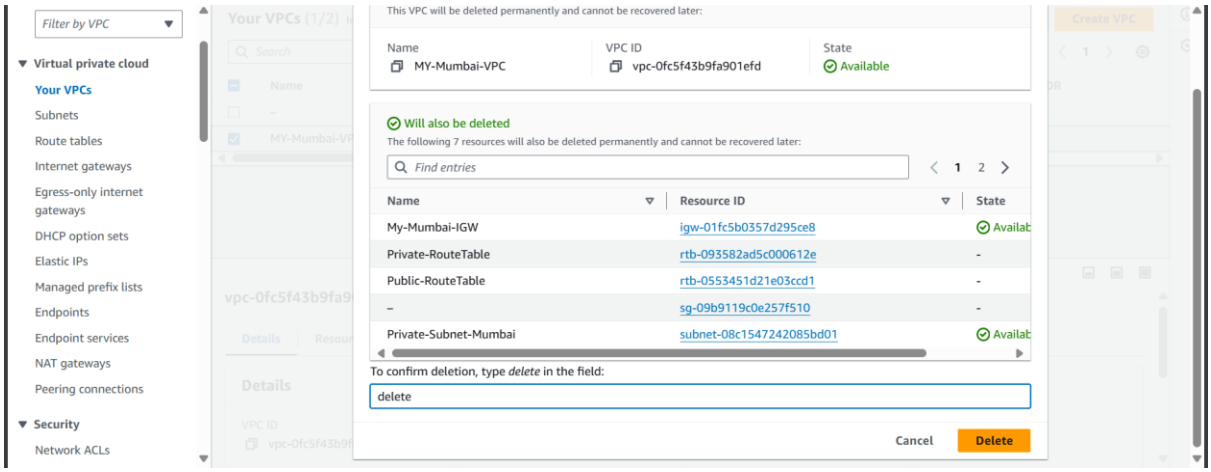
Now we will access the S3 bucket from EC2

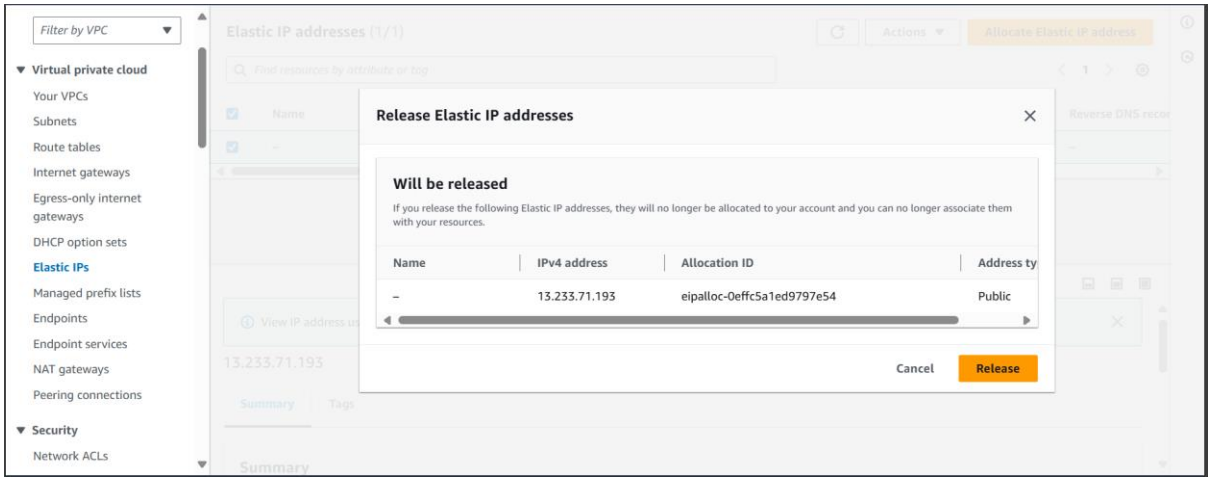


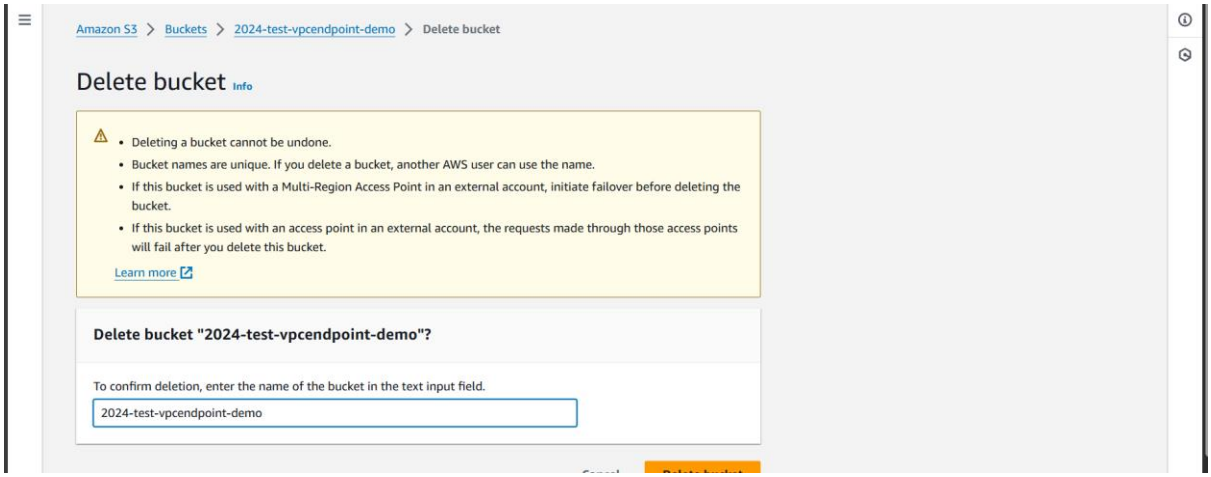
10. DISMANTLE








Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Elastic IP addresses (1/1)
Actions
Allocate Elastic IP address
Release Elastic IP addresses
Will be released
If you release the following Elastic IP addresses, they will no longer be allocated to your account and you can no longer associate them with your resources.
Name
IPv4 address
Allocation ID
Address ty
–
13.233.71.193
eipalloc-0effc5a1ed9797e54
Public
Cancel
Release
13.233.71.193
Summary
Tags
Summary


Amazon S3
Buckets
2024-test-vpcendpoint-demo
Delete bucket
Delete bucket Info
Deleting a bucket cannot be undone.
Bucket names are unique. If you delete a bucket, another AWS user can use the name.
If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.
Learn more
Delete bucket "2024-test-vpcendpoint-demo"?
To confirm deletion, enter the name of the bucket in the text input field.
2024-test-vpcendpoint-demo