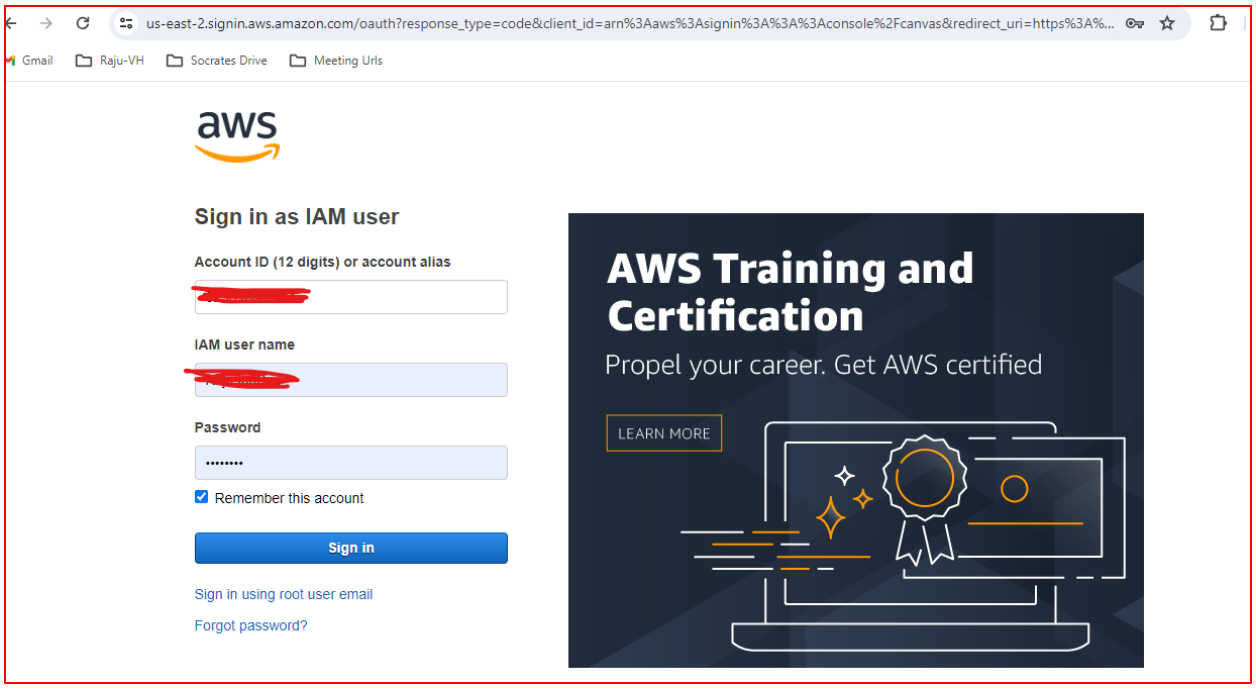
Setup EC2 And VPC – AWS

In this Document Covered these

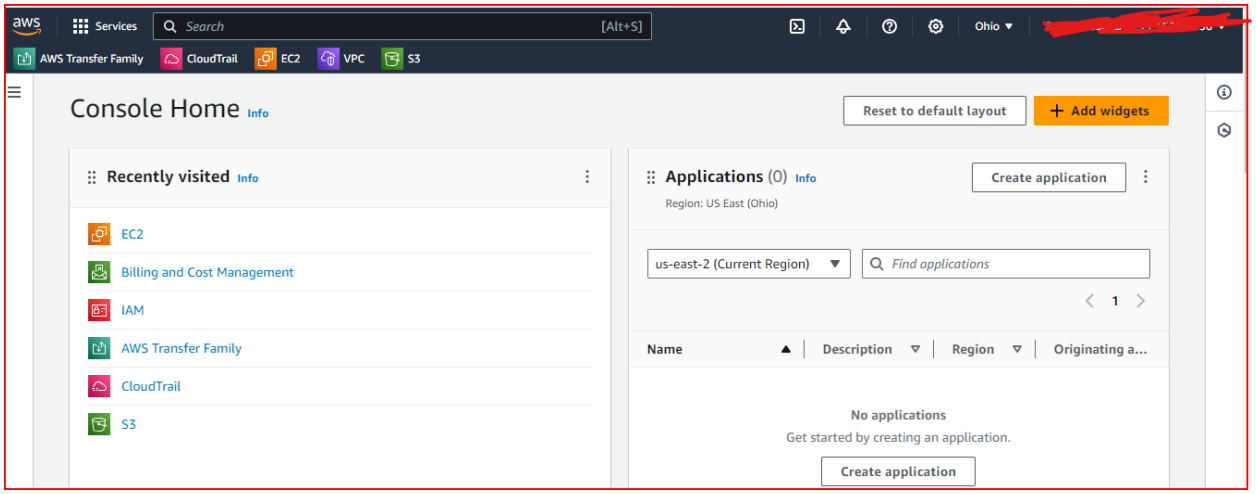
1 How to connect private ip address of aws ec2 instance
2. How many methods we have to connect instance
3. Complete setup of VPC- Subnets, Route tables, IGW, NAT.

Launch EC2 VM :

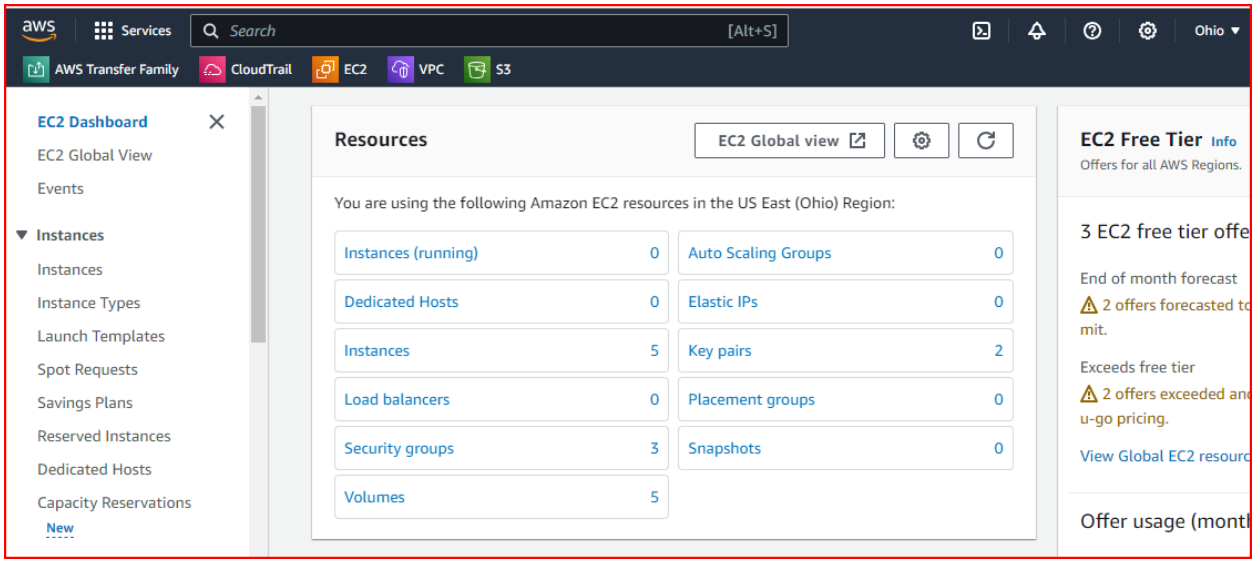
Step1: Login to AWS Console with user credentials



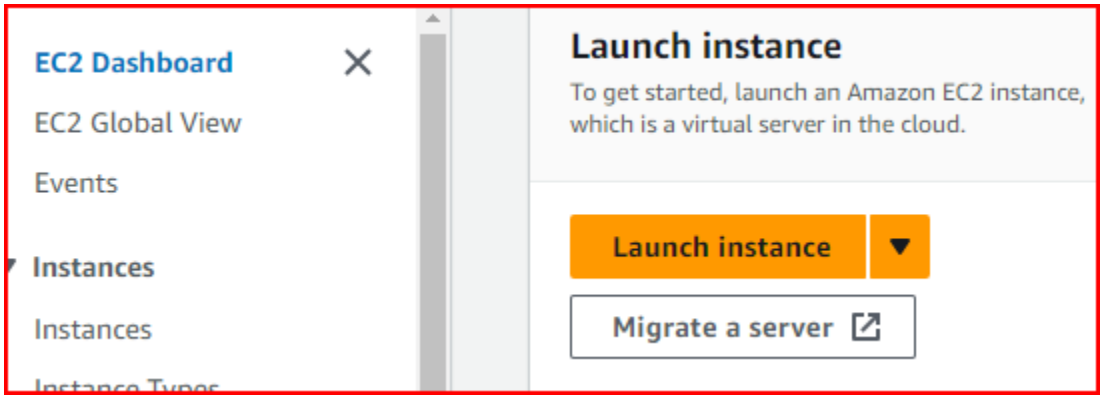
Step 2: After login into the account then go to home page of aws console



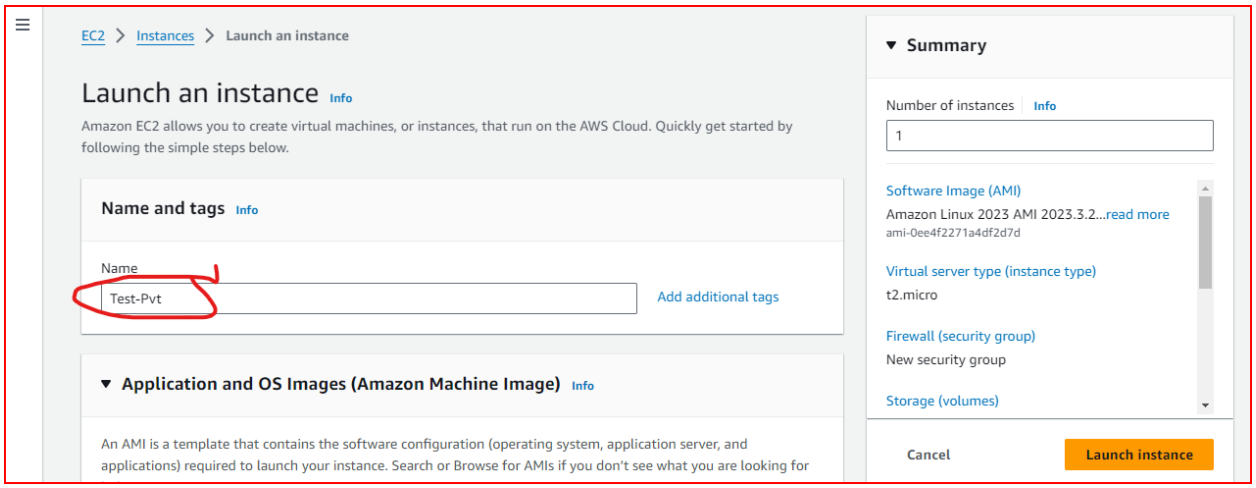
Step 3 : search ec2 home page



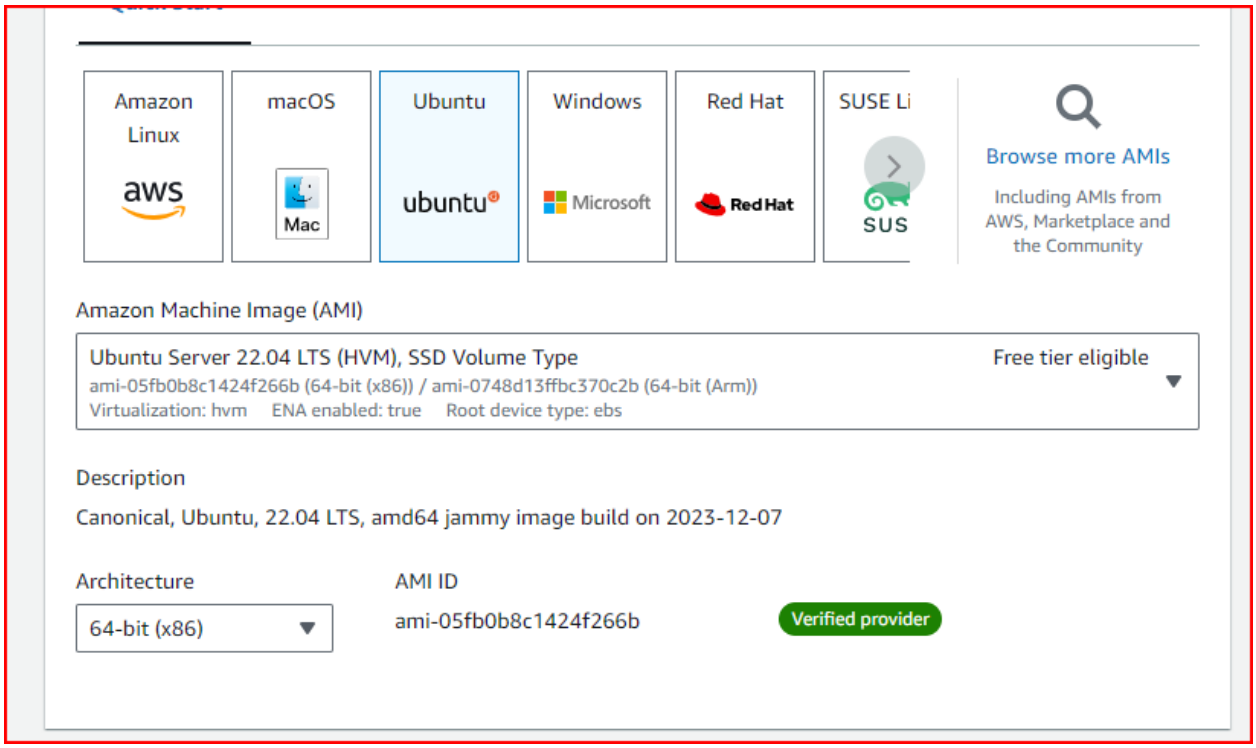
Step 4: Launch instance



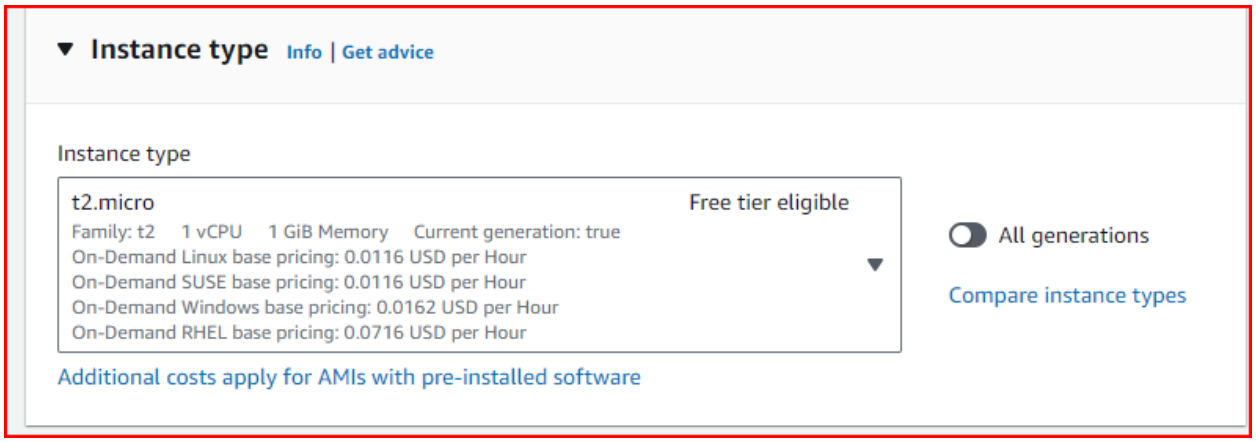
Give the instance name as per requirement



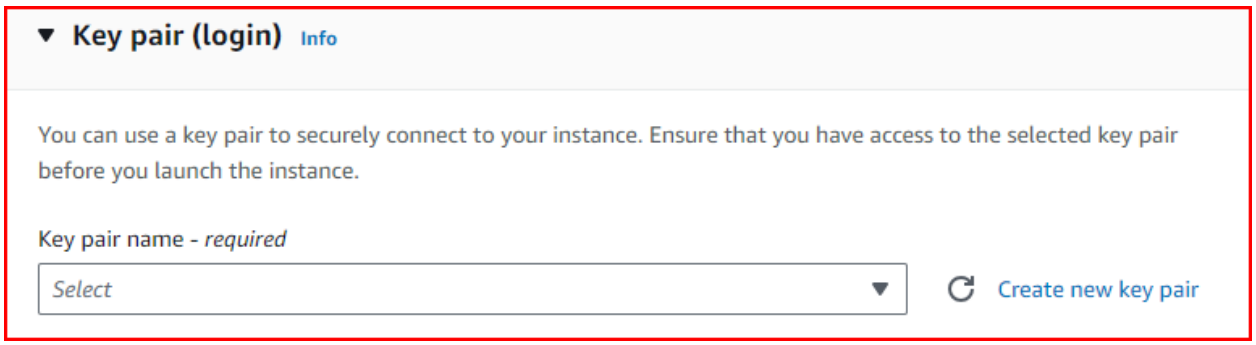
Choose the AMI image like below as per requirement under drop down menu



Choose instance type as per requirement

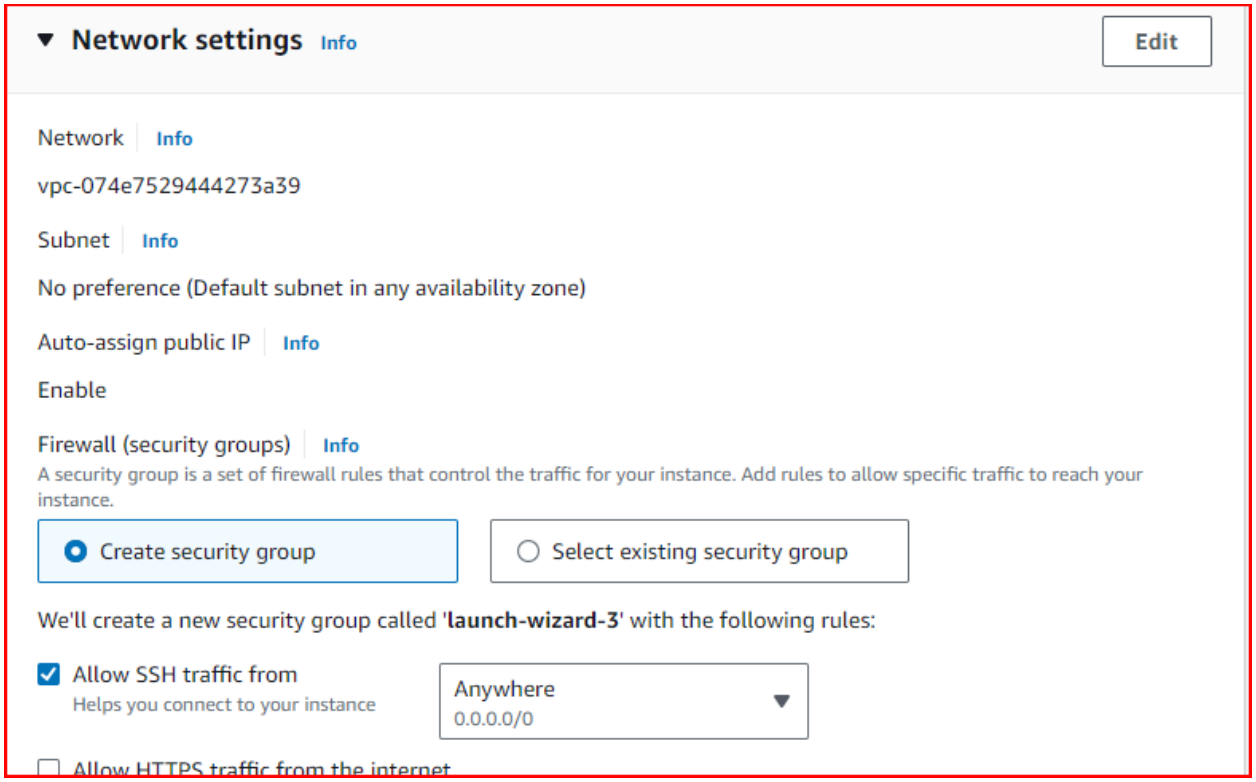


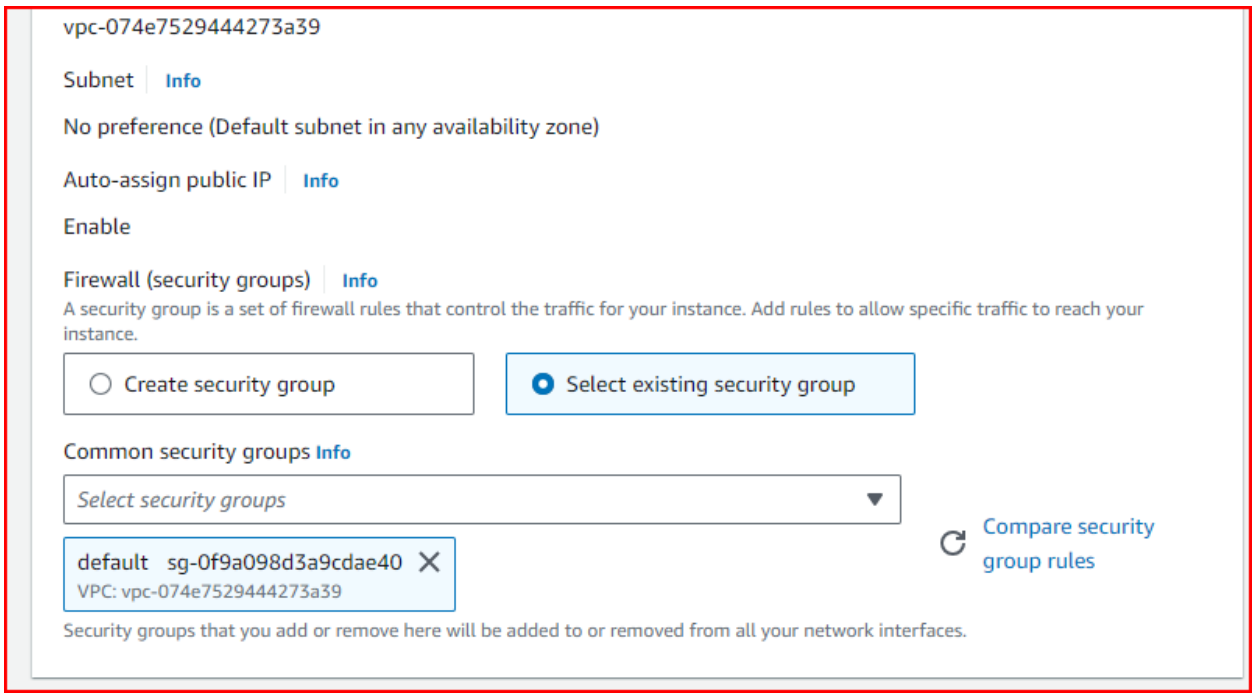
Due to security connectivity of the instance key pair is generated . here if key pair is generated choose that in drop down menu otherwise create new key pair .pem or .ppk files these file stored in local machine under download folder.



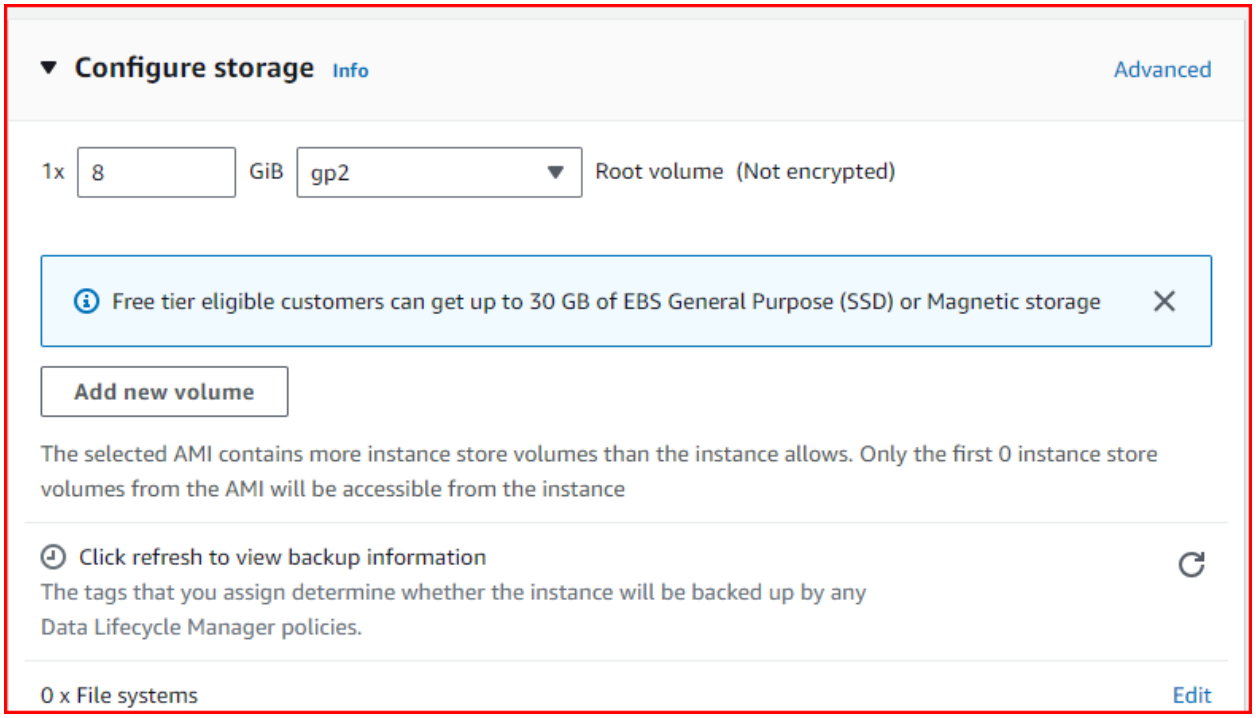
Choose the vpc and security group

If the firewall is an existing security group choose default otherwise create a new security group as per requirement to allow or block the ports and ips.

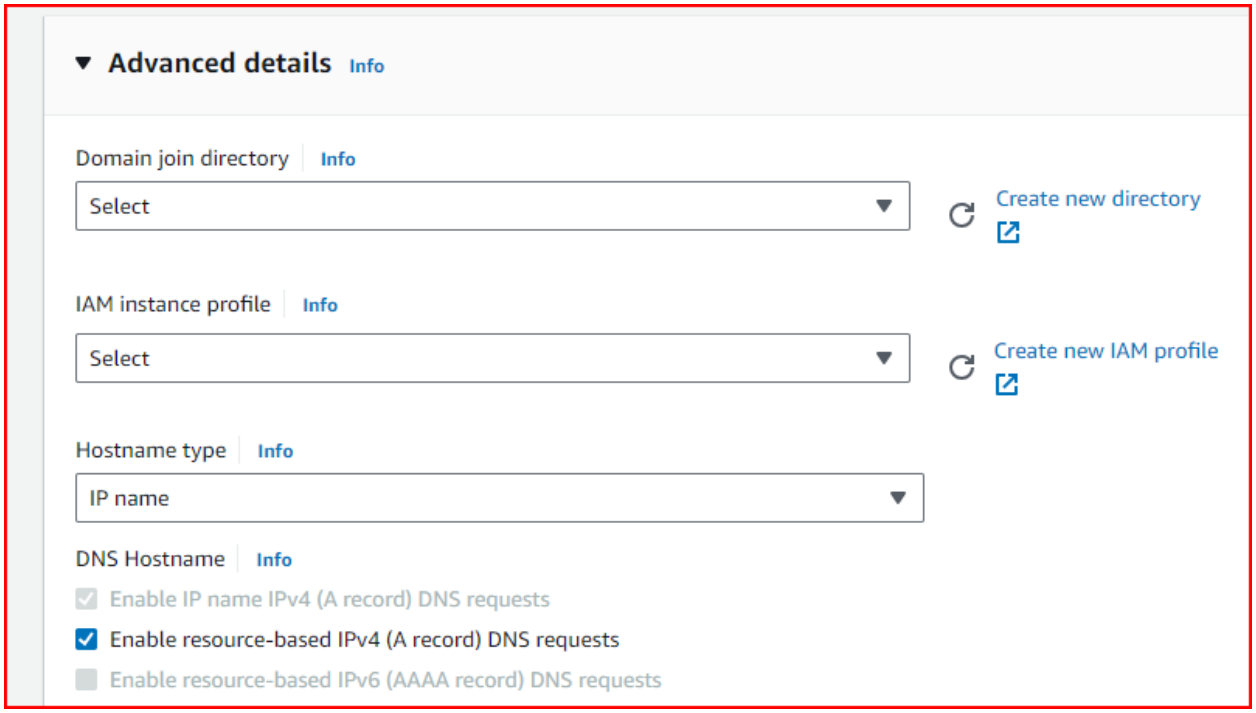




Size of the instance i.e volume



If added in the extra details choose advanced options under instance creation setup.



Instance auto-recovery Info

Select

Shutdown behavior Info

Stop

Stop - Hibernate behavior Info

Select

Termination protection Info

Select

Stop protection Info

Select

Detailed CloudWatch monitoring Info

Select

Elastic GPU Info

Elastic inference Info

Add Elastic Inference accelerators

Amazon Elastic Inference is no longer available to new customers. For new and existing customers, we recommend using an alternative, such as AWS Inferentia, which offers better performance at a lower cost. Learn more

Credit specification Info

Select

Placement group Info

Select

Create new placement group

EBS-optimized instance Info

Disable

Purchasing option Info

None

Capacity reservation Info

Select

Tenancy Info

Select

RAM disk ID Info

Select

Kernel ID Info

Select

Nitro Enclave Info

Select

Nitro Enclaves are not compatible with instance types that have less than 2 vCPUs.

License configurations Info

Select

The selected instance type does not support CPU options.

AMD SEV-SNP Info

Select

AMD SEV-SNP is not supported with the selected instance type and the selected AMI.

Metadata accessible Info

Enabled

Metadata transport

Select

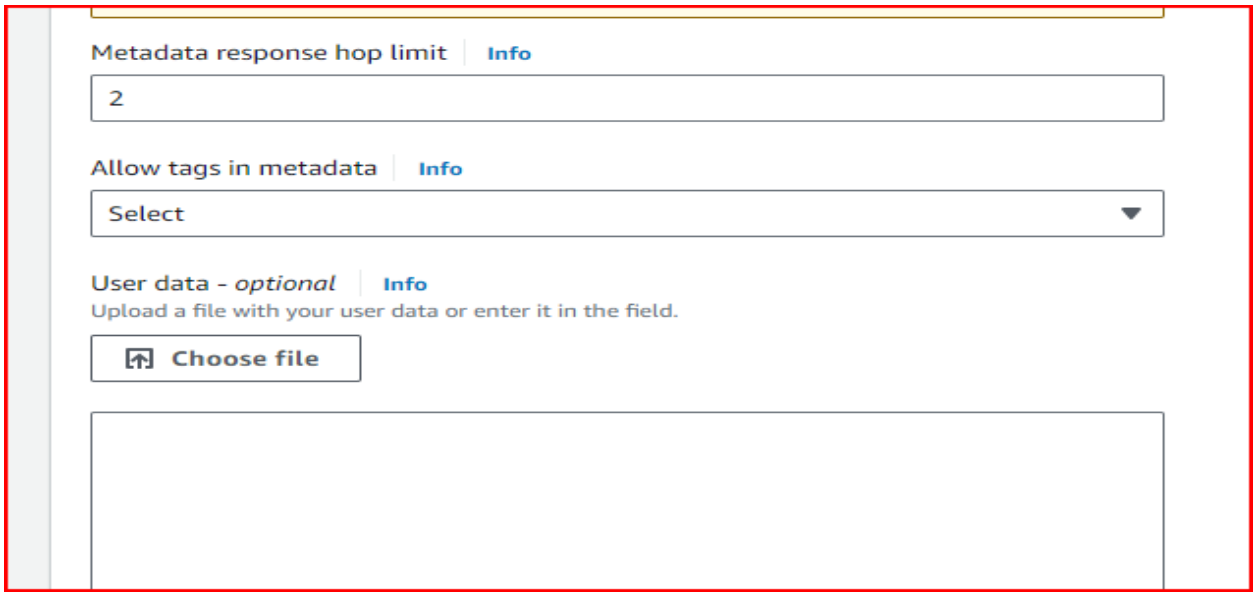
Metadata version Info

V2 only (token required)

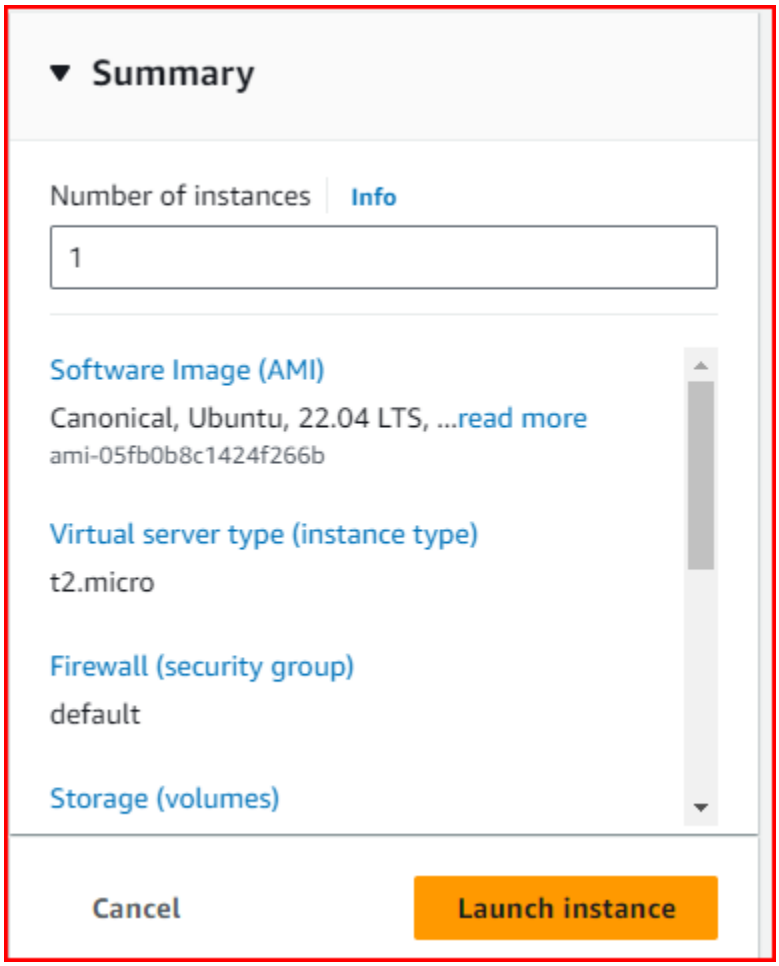
For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.

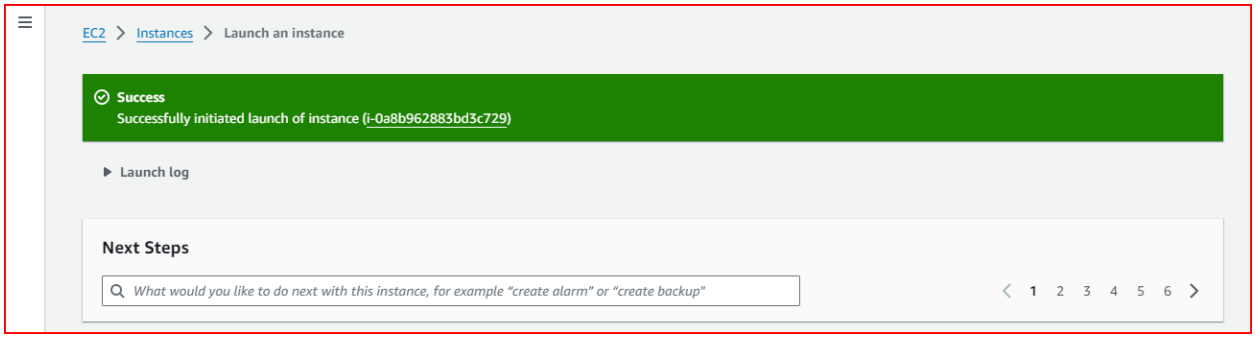
Metadata response hop limit Info

Here Under User data we need to insert the bash or any script to install the packages directly while on launching

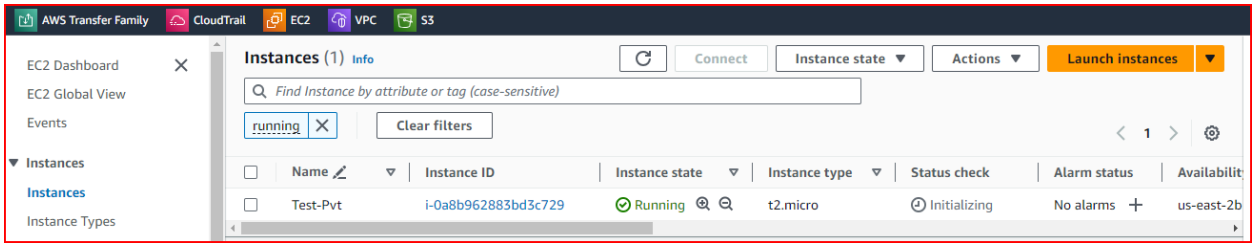


Summery

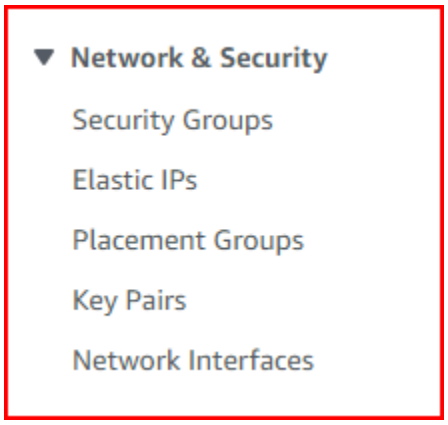


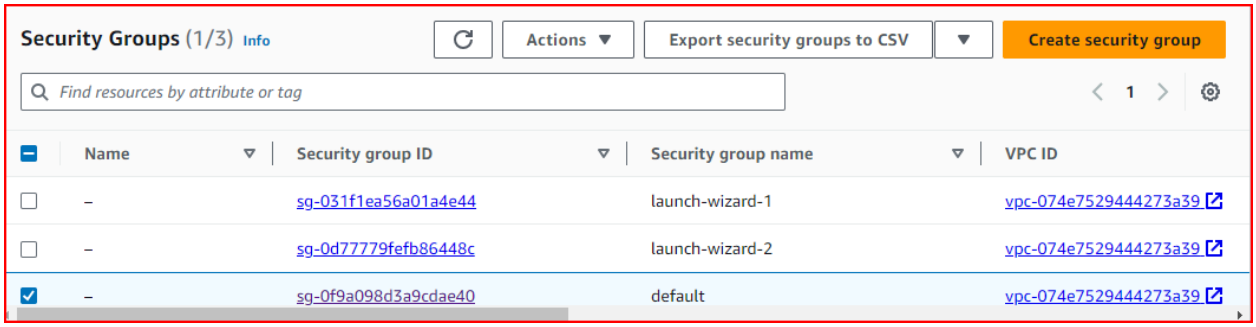


Step 5: Instance is running



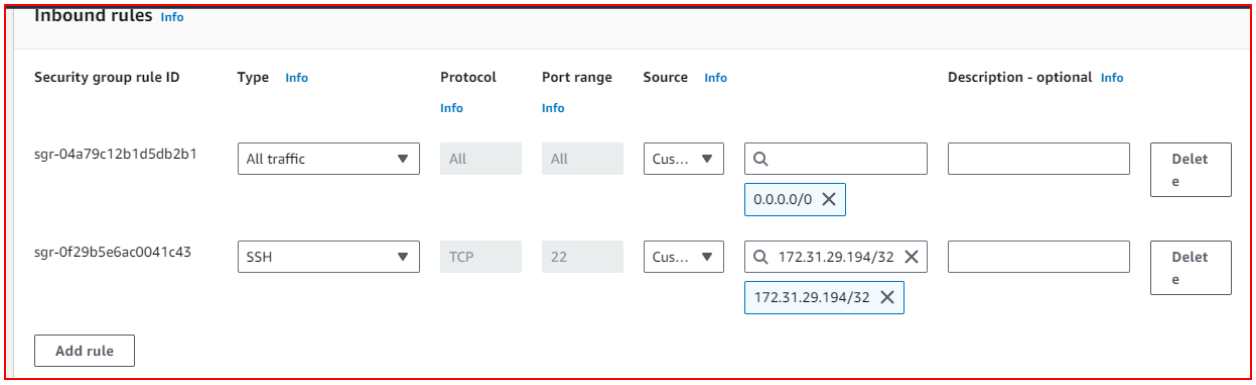
Step 6 : adding the security group inbound and outbound rules
At ec2 dashboard goto network and security choose security groups



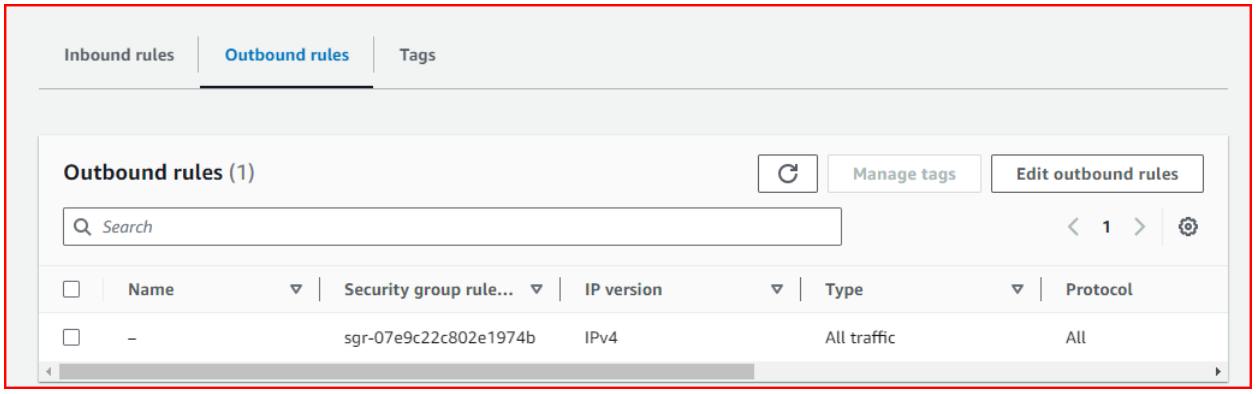


Here under inbound rules add custom tcp port 22 why because port 22 is default ssh connection

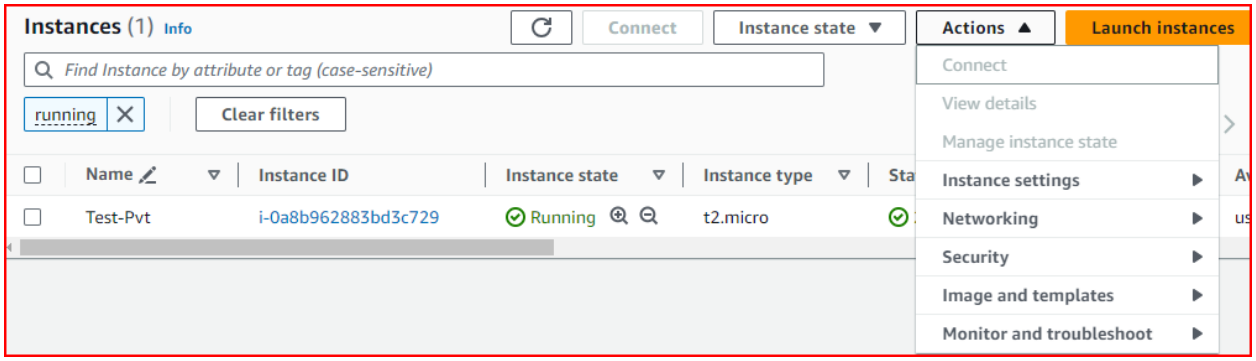
Inbound rules



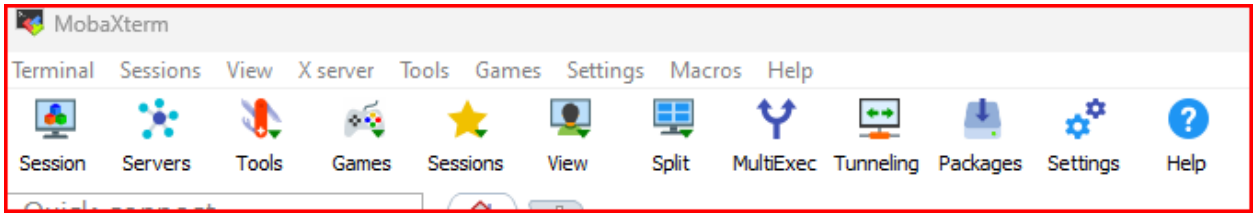
Outbound rules all traffic



Step 7 : Any changes in ec2 instance goto actions



Step 8:



Session settings

SSH | Telnet | Rsh | Xdmcp | RDP | VNC | FTP | SFTP | Serial | File | Shell | Browser | Mosh | Aws S3 | WSL

Basic SSH settings

Remote host * Specify username Port 22

Advanced SSH settings | Terminal settings | Network settings | Bookmark settings

Secure Shell (SSH) session

OK Cancel

Session settings

SSH | Telnet | Rsh | Xdmcp | RDP | VNC | FTP | SFTP | Serial | File | Shell | Browser | Mosh | Aws S3 | WSL

Basic SSH settings

Remote host * 172[redacted] Specify username ubuntu Port 22

Advanced SSH settings | Terminal settings | Network settings | Bookmark settings

X11-Forwarding Compression Remote environment: Interactive shell

Execute command: Do not exit after command ends

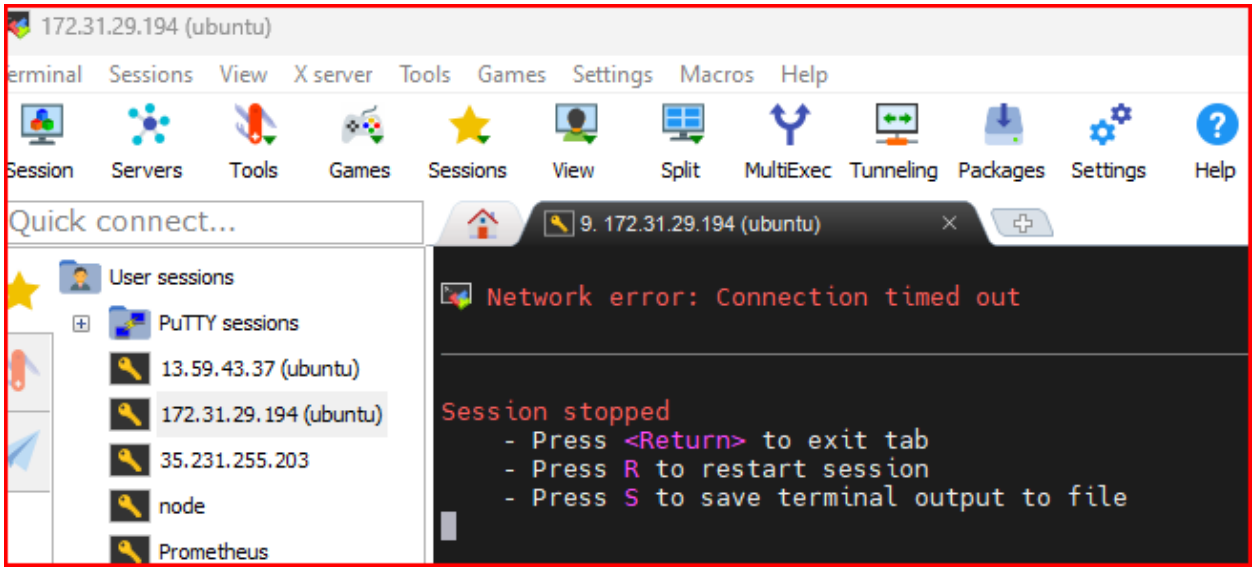
SSH-browser type: SFTP protocol Follow SSH path (experimental)

Use private key C:[redacted]\key: Expert SSH settings

Execute macro at session start: <none>

OK Cancel

Connect aws instance using private ip address getting error

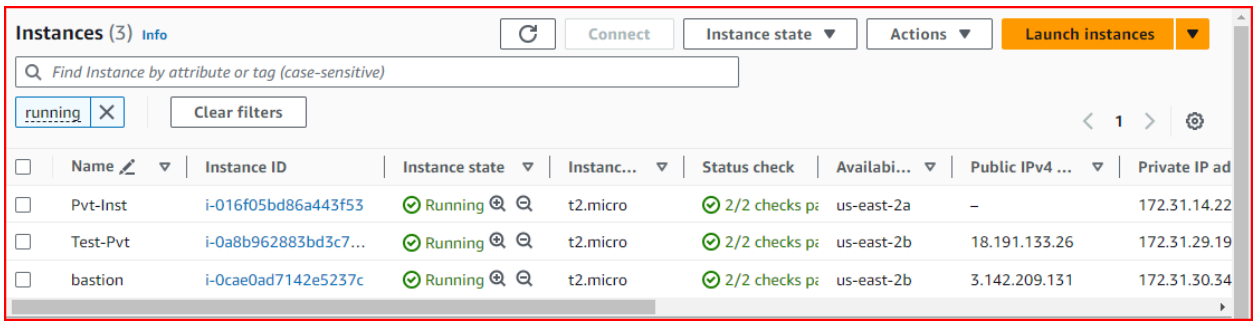


To connect Private IP addresses in aws we having two methods:

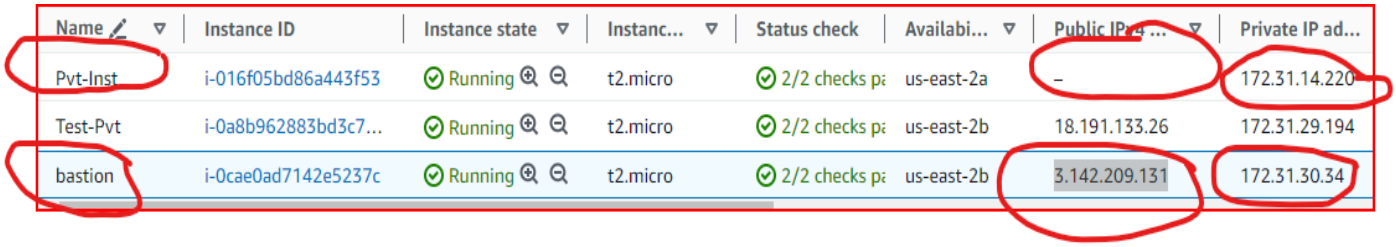
1- Bastion Host or Jump Server
2- EIC (EC2 Instance connect).

1- Bastion Host or Jump Server:

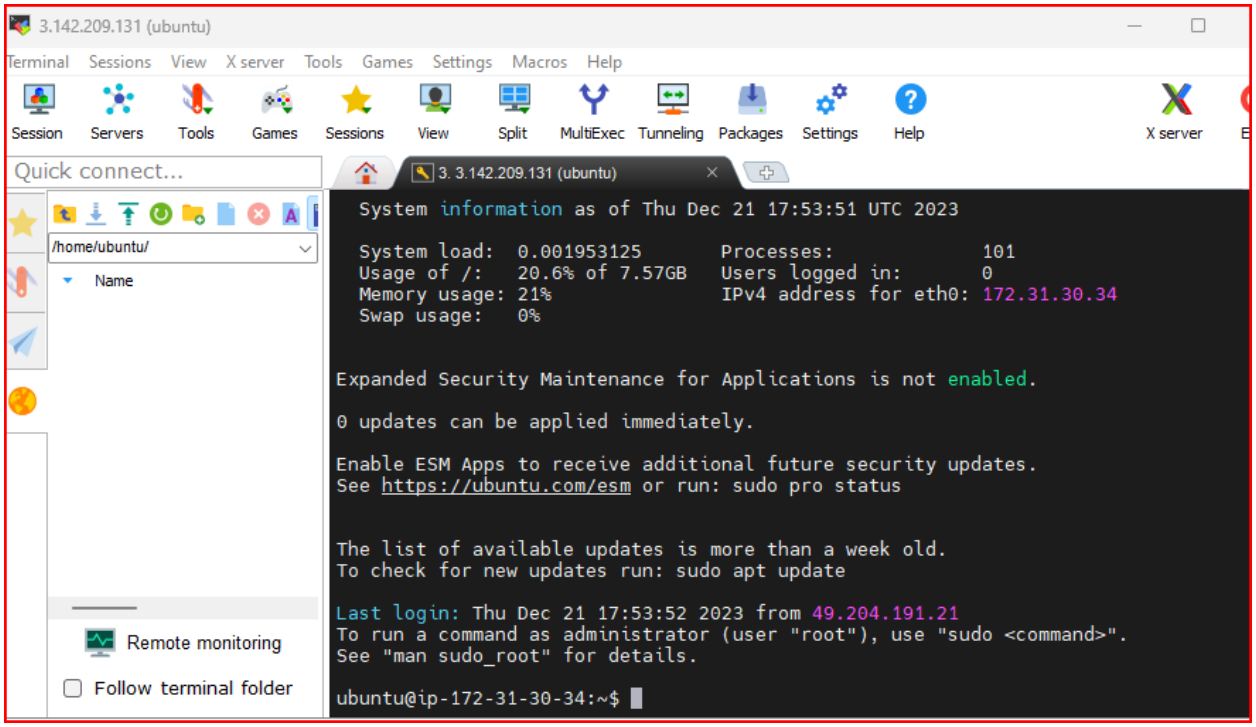
There is no public Ip for pvt-inst so only private ip address



Here we need to connect the Pvt-Inst using a bastion server.
First copy the bastion server ip and ssh into any client.

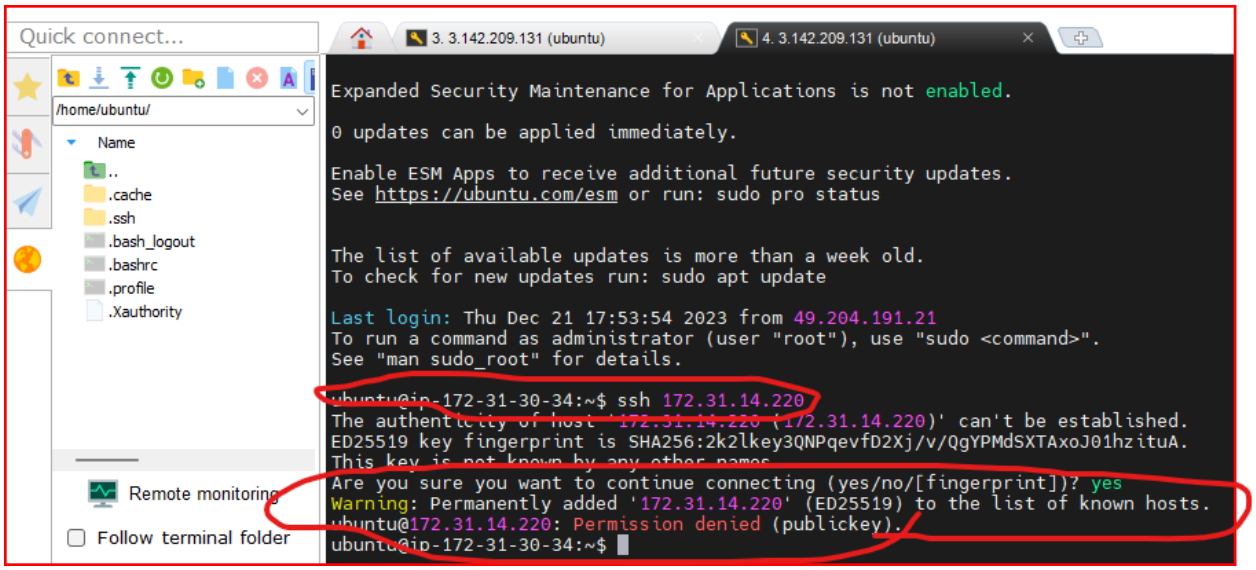


This is **bastion server** connectivity check private ip



Now connect Pvt-inst server in bastion server

But I am getting following error because in bastion server there is no .pem or .ppk file of pvt-inst server so copy that in bastion machine server.



First copy the pem file two ways

1. Direct upload the file into client like mobaxterm
2. Using SCP Command to copy the local pem file into bastion machine.

```
[redacted]:~/Downloads$ sudo scp -i public_instance.pem instance_key_pair.pem ubuntu@3
4.242.113.73:/home/ubuntu/private_instance_key.pem
instance_key_pair.pem                                 100% 1678     9.1KB/s   00:00
[redacted]:~/Downloads$
```

```
Quick connect...
/home/ubuntu/
Name
..
.cache
.ssh
.bash_logout
.bashrc

3. 3.142.209.131 (ubuntu)
4. 3.142.209.131 (ubuntu)

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

```
/home/ubuntu/
Name
..
.cache
.ssh
.bash_logout
.bashrc
.profile
.Xauthority
prometheus.ppk
Remote monitoring

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Thu Dec 21 17:53:54 2023 from 49.204.191.21
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-30-34:~$ ssh 172.31.14.220
The authenticity of host '172.31.14.220 (172.31.14.220)' can't be established.
ED25519 key fingerprint is SHA256:2k2lkey3QNPqevfD2Xj/v/QgYPMdSXTAxoJ01hzituA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.31.14.220' (ED25519) to the list of known host
```

```
Terminal  Sessions  View  X server  Tools  Games  Settings  Macros  Help
Session  Servers  Tools  Games  Sessions  View  Split  MultiExec  Tunneling  Packages  Settings  Help  X server  Exit
Quick connect...
/home/ubuntu/
Name
..
.cache
.ssh
.bash_logout
.bashrc
.profile
.Xauthority
prometheus.ppk
Remote monitoring
Follow terminal folder

3. 3.142.209.131 (ubuntu)
4. 3.142.209.131 (ubuntu)

ED25519 key fingerprint is SHA256:2k2lkey3QNPqevfD2Xj/v/QgYPMdSXTAxoJ01hzituA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.31.14.220' (ED25519) to the list of known hosts.
ubuntu@172.31.14.220: Permission denied (publickey).
ubuntu@ip-172-31-30-34:~$ ssh 172.31.14.220
ubuntu@172.31.14.220: Permission denied (publickey).
ubuntu@ip-172-31-30-34:~$ ssh -i prometheus.ppk ubuntu@172.31.14.220
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0664 for 'prometheus.ppk' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "prometheus.ppk": bad permissions
ubuntu@172.31.14.220: Permission denied (publickey).
ubuntu@ip-172-31-30-34:~$ chmod 400 prometheus.ppk
ubuntu@ip-172-31-30-34:~$ ssh 172.31.14.220
ubuntu@172.31.14.220: Permission denied (publickey).
ubuntu@ip-172-31-30-34:~$ ssh -i prometheus.ppk ubuntu@172.31.14.220
Load key "prometheus.ppk": error in libcrypto
ubuntu@172.31.14.220: Permission denied (publickey).
ubuntu@ip-172-31-30-34:~$ puttygen prometheus.ppk -O private-openssh -o prometheus
.pem
```

I am getting error here so

Putty:

The error "Load key 'prometheus.ppk': error in libcrypto" indicates a problem with loading or processing the private key file due to a cryptographic library issue. To address this, you can try the following steps:

Use OpenSSH Private Key:

- **Convert the PuTTY private key** (prometheus.ppk) to OpenSSH format using the puttygen tool. Run the following command in your local terminal:

```
puttygen prometheus.ppk -O private-openssh -o prometheus.pem
```

- Use the converted key (prometheus.pem) in your SSH command:

```
ssh -i prometheus.pem ubuntu@172.31.14.220
```

Check Key Permissions:

- Ensure that the permissions for the private key file (prometheus.pem) are set correctly:

```
chmod 600 prometheus.pem
```

Verify Key Format:

- Double-check that the private key file is in the correct format (OpenSSH format) after the conversion.

Update SSH Client:

- Ensure that you are using an up-to-date version of the OpenSSH client on your local machine. You can update it using your package manager:
  For Ubuntu/Debian:

```
sudo apt-get update
sudo apt-get install openssh-client
```

- For CentOS/RHEL:

```
sudo yum update
sudo yum install openssh-clients
```

Check SSH Agent:

- If you have an SSH agent running, try restarting it or clearing loaded keys:

```
eval "$(ssh-agent -s)"
ssh-add -D # Clears all identities from the agent
ssh-add prometheus.pem
```

Check Crypto Libraries:

- Ensure that the cryptographic libraries on your system are up to date. Perform a system update and upgrade:
  For Ubuntu/Debian:

sudo apt-get update
sudo apt-get upgrade

- For CentOS/RHEL:

sudo yum update

Check Key Passphrase:

- If the private key has a passphrase, make sure you are entering it correctly when prompted.

Generate a New Key Pair (Optional):

- If the issue persists, consider generating a new key pair and updating the public key on the remote server.

Mobaxterm:

The error "Load key 'prometheus.ppk': error in libcrypto" suggests an issue with the private key file or its compatibility with the SSH client. Since you are using MobaXterm, you might want to ensure that the key file is correctly loaded and that MobaXterm is handling the key conversion properly.
Here are steps you can take to resolve the issue:

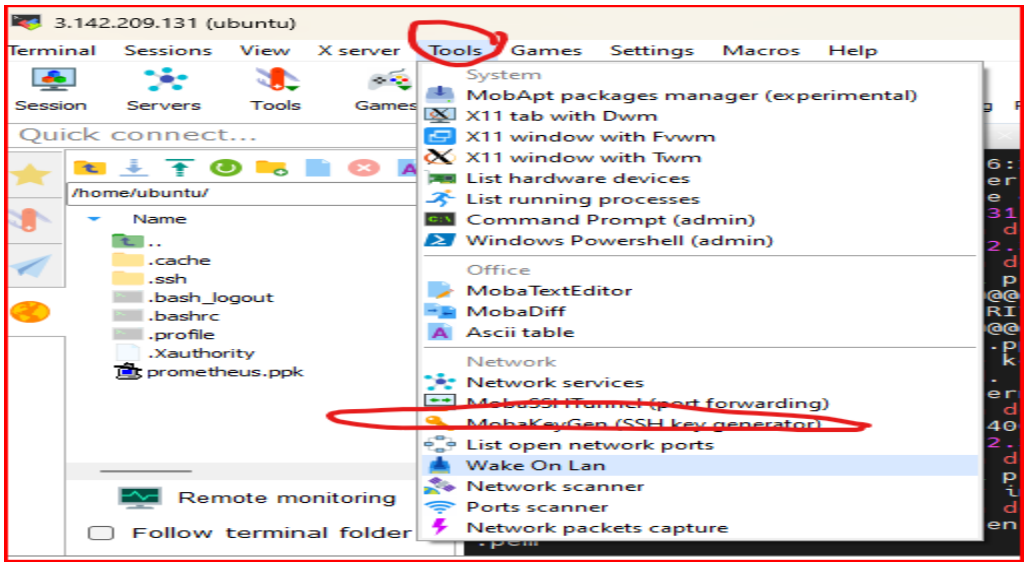
Check Key Format:

- Ensure that the private key file (prometheus.ppk) is in the correct format. MobaXterm uses its own private key format, so it's important to make sure the key is in the right format for OpenSSH.

Convert Key to OpenSSH Format:

- Use MobaXterm itself to convert the key to OpenSSH format:
  - Open MobaXterm.
  - Go to the "Tools" menu.
  - Select "MobaKeyGen."
  - Load your private key (prometheus.ppk).
  - In the "Conversions" menu, choose "Export OpenSSH key" and save the key with a .pem extension.

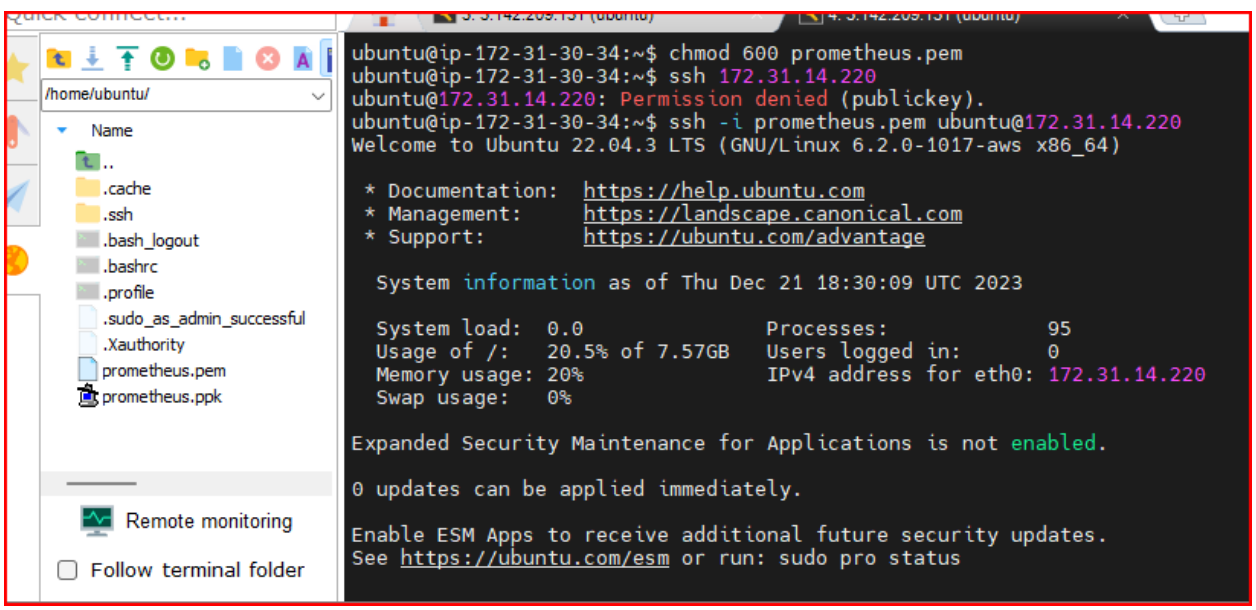
chmod 600 prometheus.pem



Use the Converted Key:

- After converting the key, use the new OpenSSH key (prometheus.pem) in your SSH command:

ssh -i prometheus.pem ubuntu@172.31.14.220
Successfully connected pvt ip address in bastion host server if doubt check the ip addresses. 172.31.30.34 172.31.14.220



Ensure Key is Loaded in MobaXterm:

- Open MobaXterm.
- In the terminal, check if the private key is loaded using the following command:

ssh-add -l

- If the key is not listed, add it using:

ssh-add /path/to/prometheus.pem

Verify Permissions:

- Ensure that the permissions for the private key file are set correctly:

chmod 600 prometheus.pem

Check MobaXterm Settings:

- In MobaXterm, go to "Settings" > "Configuration."
- Under the "SSH" tab, make sure that the "Use internal SSH agent" option is selected.

Restart MobaXterm:

- Sometimes, restarting MobaXterm can resolve certain issues. Close and reopen the application.

Check MobaXterm Logs:

- MobaXterm may log information about key loading and authentication attempts. Check the logs for any relevant error messages.

Update MobaXterm:

- Ensure that you are using the latest version of MobaXterm. If not, consider updating to the latest release.

2- EIC (EC2 Instance connect):

On June 13th, AWS launched a new service called EC2 Instance Connect Endpoint (EIC Endpoint). Which Allows to have secure SSH and RDP connectivity to private EC2 instances without using public IP addresses.
This Article discusses working of EIC Endpoint and demonstrates how to create and use it to SSH/RDP to an instance from the Internet.

EC2 Instance Endpoint Connect any resources:

✴️ Use "EC2 instance Connect" to connect to RDS and other VPC resources — no VPN required, no EC2 Bastion instance needed 🔥

1️⃣Upgrading the AWS CLI to version 2.12+
2️⃣Create (if you haven't already) an EC2 Instance Connect Endpoint

• aws ec2 create-instance-connect-endpoint --region `us-east-1` --subnet-id `subnet-0123456789abcdef`
⚠️ Change "region" and "subnet-id" to your values.

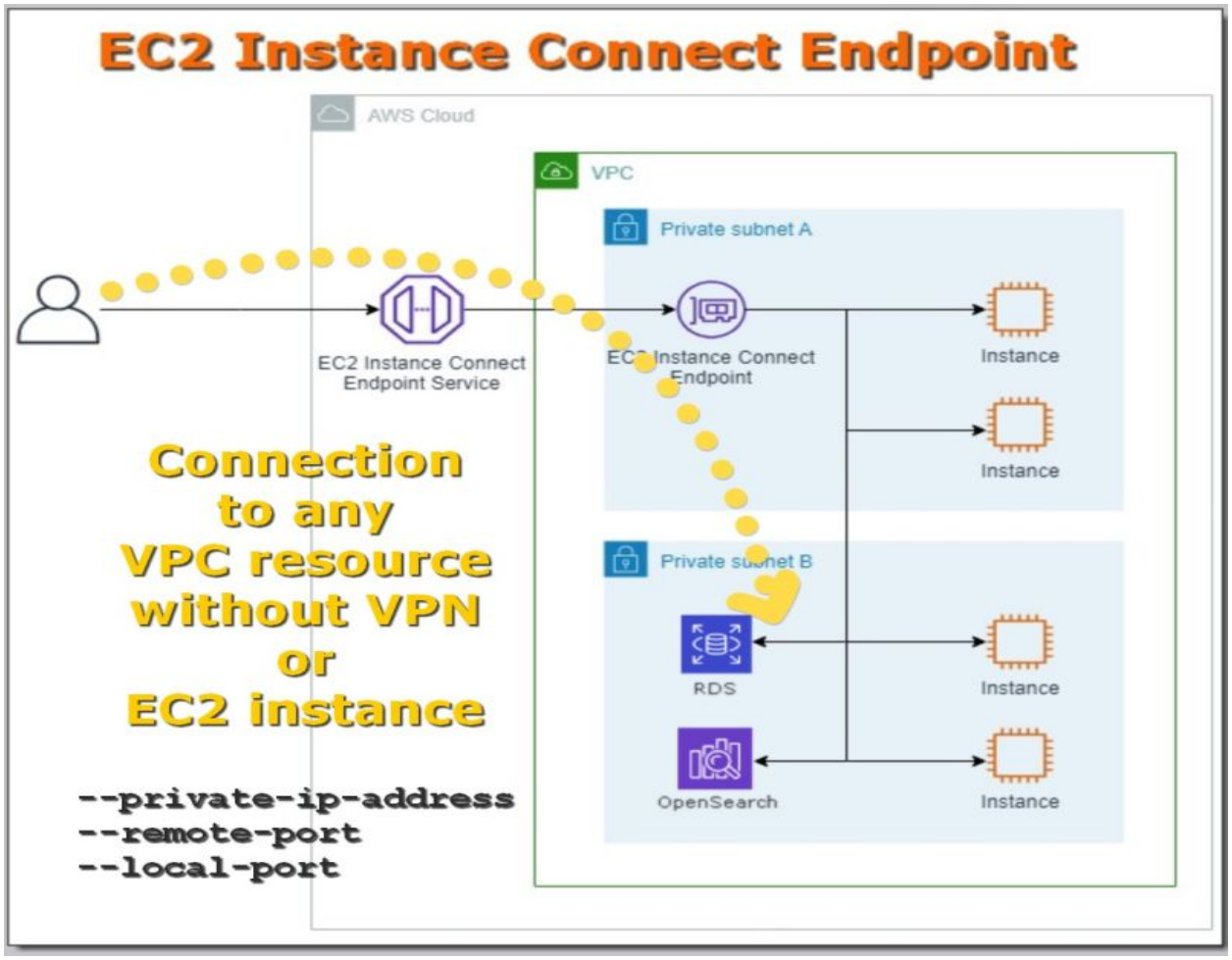
After creation you use "InstanceConnectEndpointId".

3️⃣Connecting to EC2 Instance Connect Endpoint
The EC2 User Guide so far only lists connection to an EC2 instance by "instance-id". However, the AWS CLI v2 lists others for "ec2-instance-connect open-tunnel", in particular "private-ip-address" and "remote-port".
So we use this command:

• aws ec2-instance-connect open-tunnel --private-ip-address <`your-private-IP-here`> --instance-connect-endpoint-id `eice-0123456789abcdef12` --remote-port `5432` --local-port `5432`

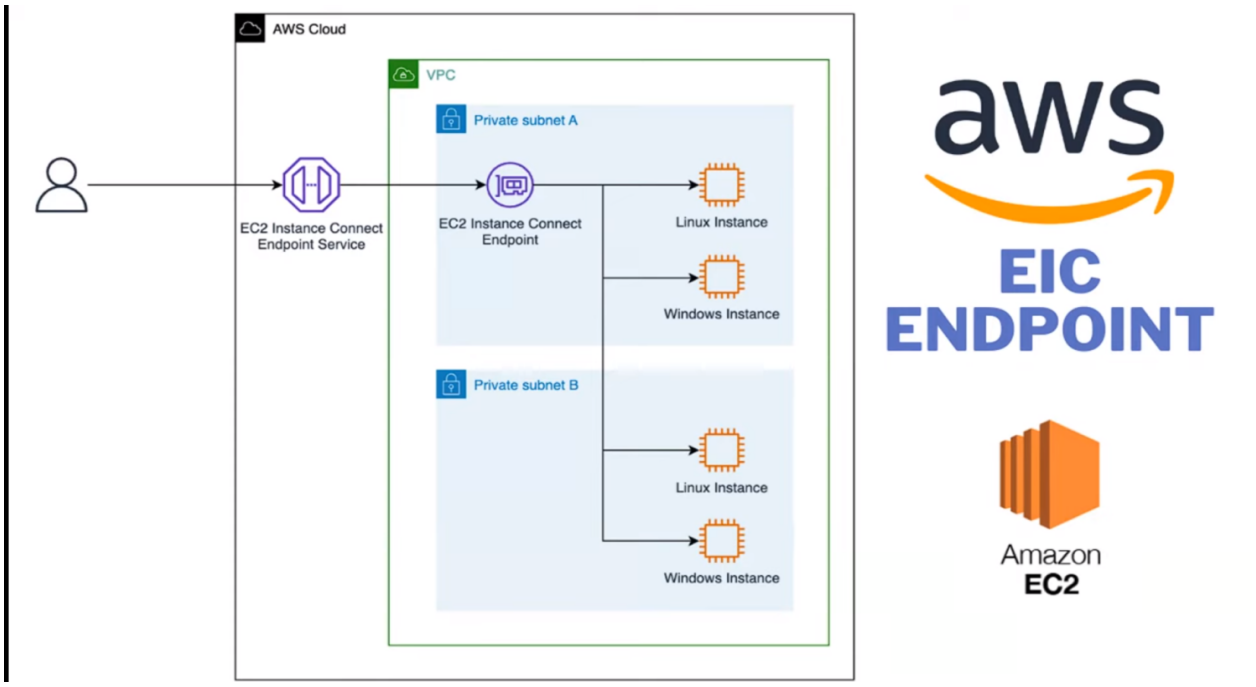
⚠️ Change "private-ip-address", "instance-connect-endpoint-id" (obtained during creation), "remote-port" and "local-port" to your values.
The result will be a tunnel:
• Listening for connections on port 5432.
• [1] Accepted new tcp connection, opening websocket tunnel.

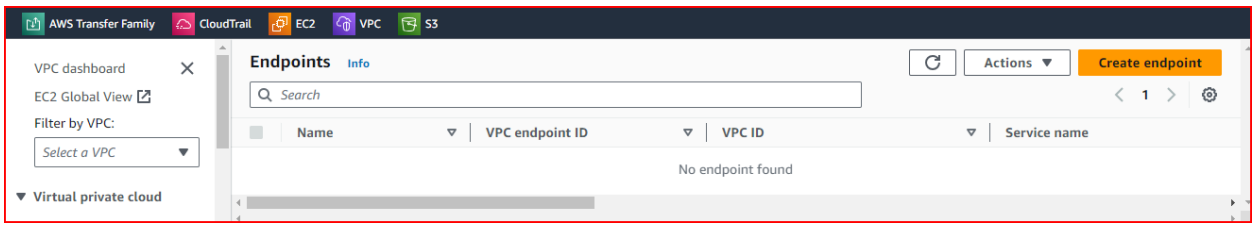
4️⃣Connect to the local port (localhost:5432 from the example above) and that's it! 👍
It definitely works for IPs from other VPCs connected via VPC Peering. I haven't tried it for another — let me know if it doesn't work.

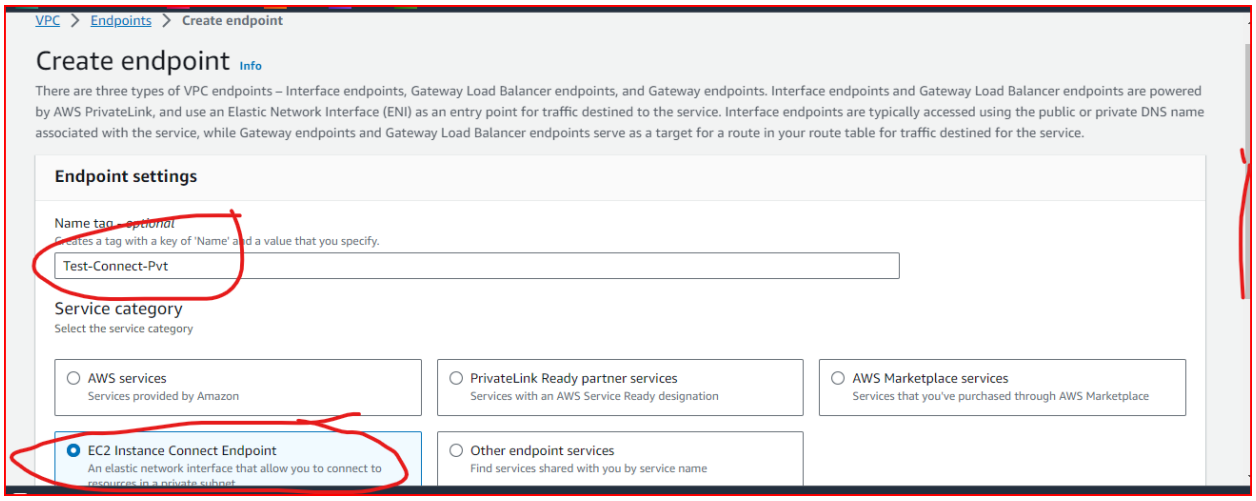


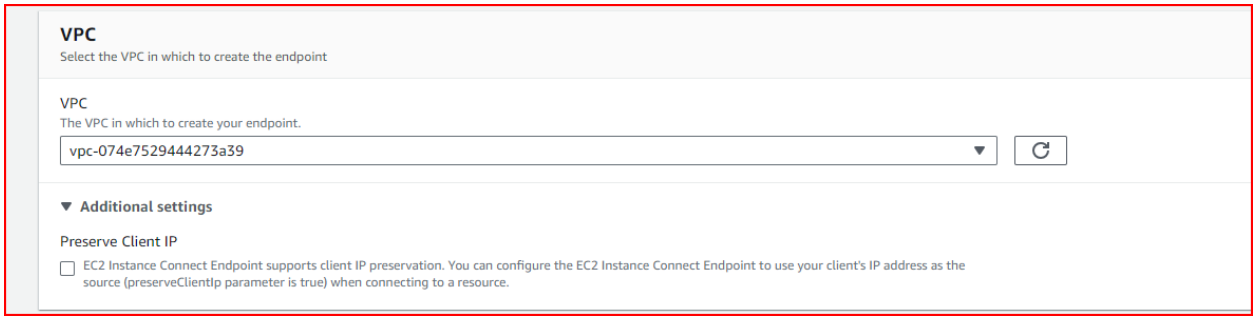
Creation of the Endpoint Under VPC Dashboard:

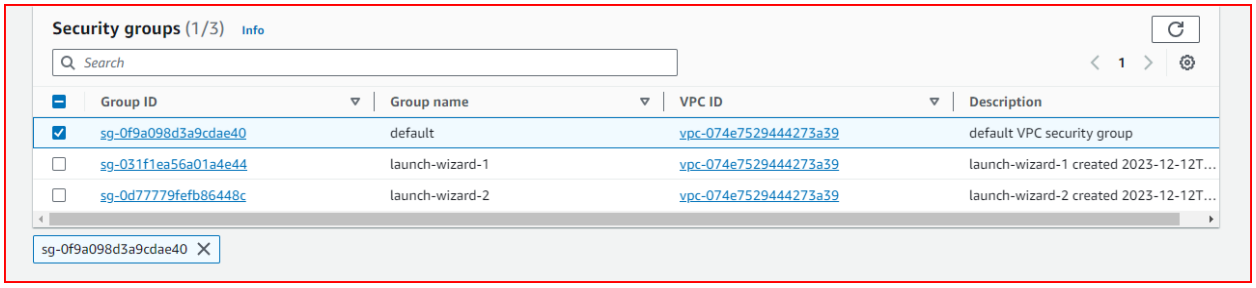
EIC EndPoint:

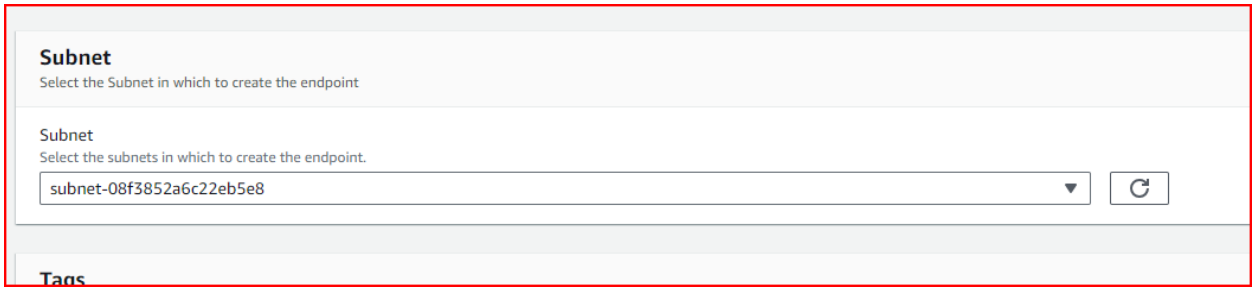


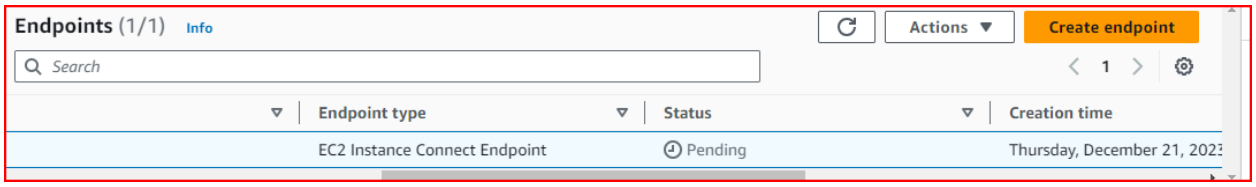


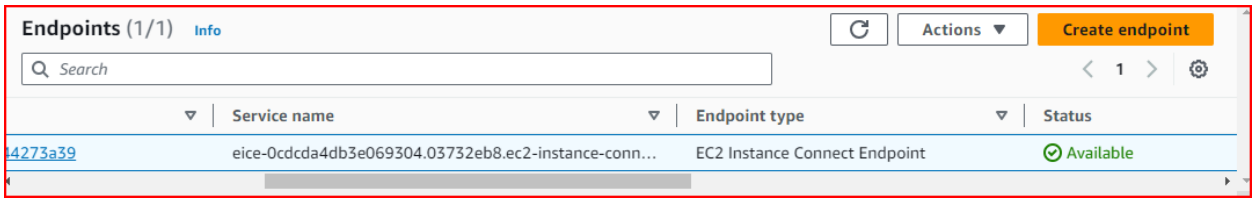












IAM Inline Policy is created Under the specific User:

IAM > Users > Raju-IndCog > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor Visual | JSON | Actions

Select a service

Specify what actions can be performed on specific resources in a service.

Service

Choose a service

+ Add more permissions

Cancel | Next

Step 2
Review and create

Policy editor Visual | JSON | Actions

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Sid": "Statement1",
6              "Effect": "Allow",
7              "Action": [],
8              "Resource": []
9          }
10     ]
11 }
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

Step 2
Review and save

Policy editor Visual | JSON | Actions

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Sid": "AllowAllEC2Actions",
6              "Effect": "Allow",
7              "Action": [
8                  "ec2:DescribeInstances",
9                  "ec2:DescribeInstanceConnectEndpoints"
10             ],
11             "Resource": "*"
12         },
13         {
14             "Sid": "AllowSpecificActionsForUserARN",
15             "Effect": "Allow",
16             "Action": [
17                 "ec2-instance-connect:OpenTunnel",
18                 "ec2-instance-connect:SendSSHPublicKey"
19             ],
20             "Resource": [
21                 "arn:aws:ec2:us-east-2:0235[redacted]:instance-connect-endpoint/eice-0cdcda4db3e069304",
22                 "arn:aws:ec2:us-east-2:0235[redacted]:instance/i-0a8b962883bd3c729"
23             ]
24         }
25     ]
26 }
```

+ Add new statement

Edit statement Remove
AllowAllEC2Actions

Add actions

Choose a service

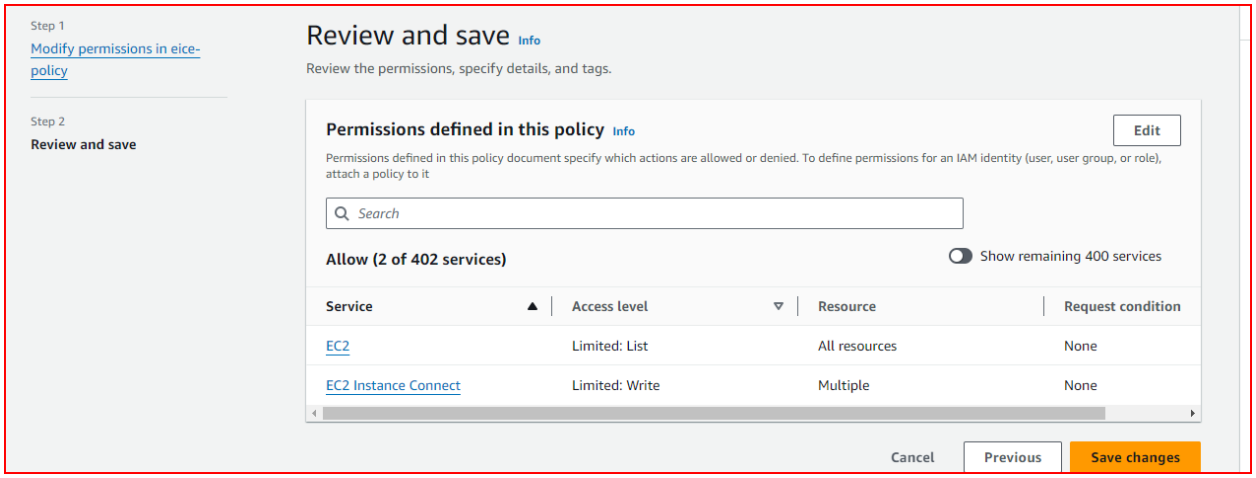
Filter services

Included
EC2

Available
AMP
API Gateway
API Gateway V2
ASC
Access Analyzer
Account
Activate

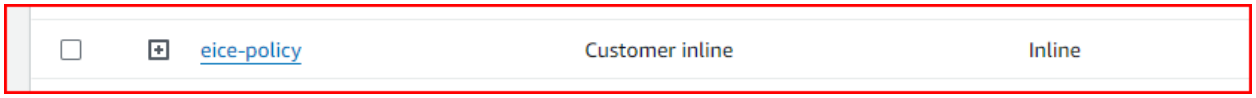
Add a resource Add

Add a condition (optional) Add

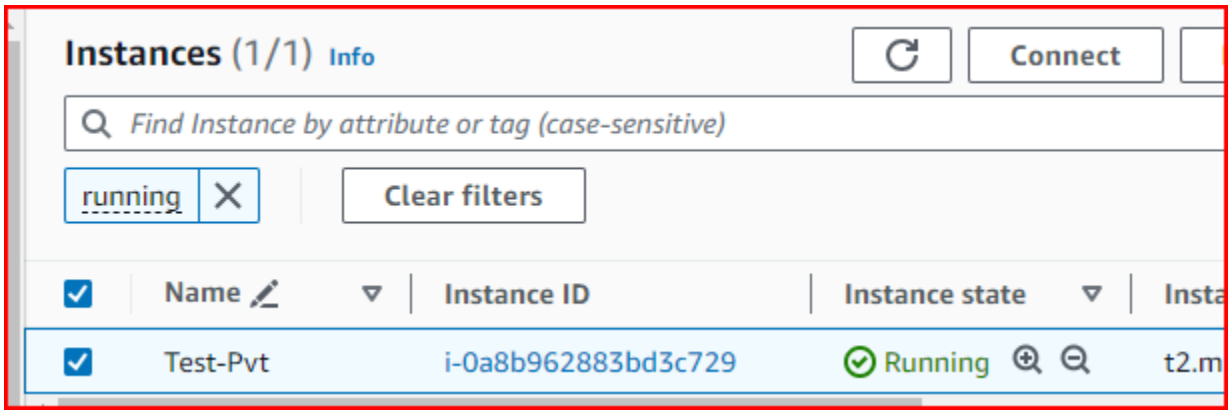


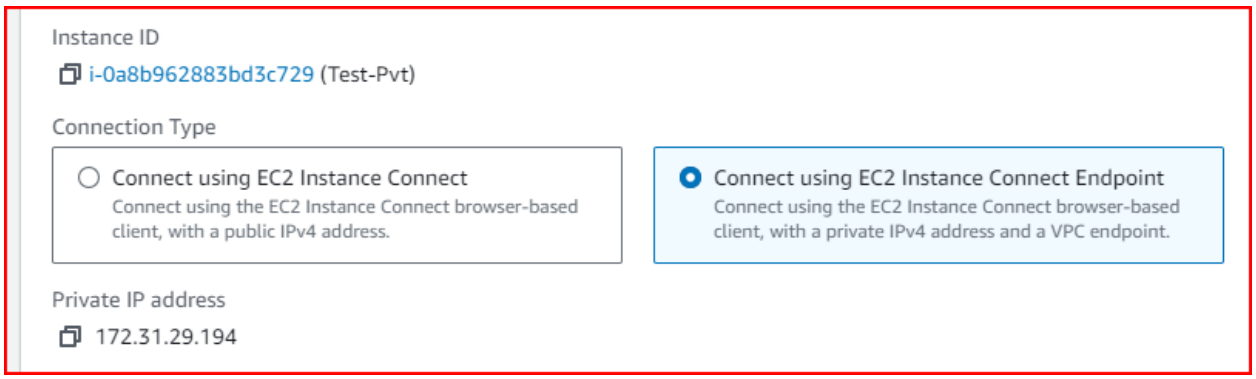
This is the policy of eice-ploicy inline policy created under the user

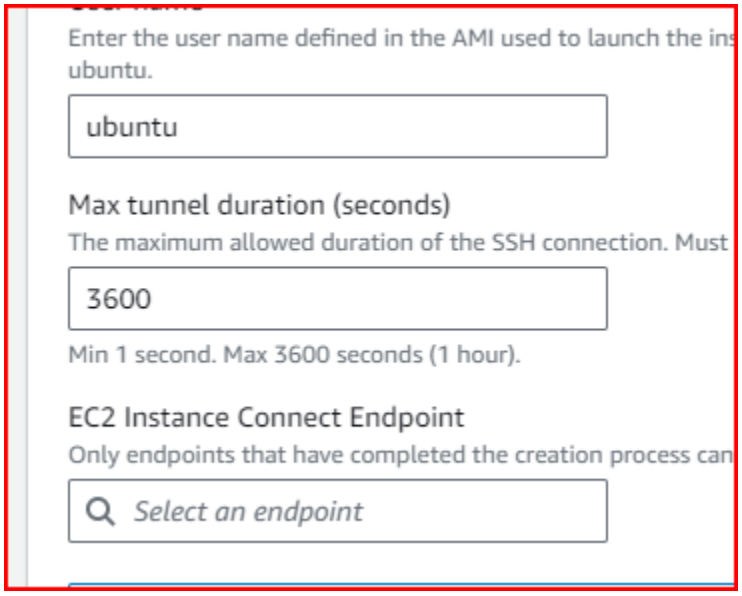
```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Sid": "AllowAllEC2Actions",
                        "Effect": "Allow",
                        "Action": [
                                "ec2:DescribeInstances",
                                "ec2:DescribeInstanceConnectEndpoints"
                        ],
                        "Resource": "*"
                },
                {
                        "Sid": "AllowSpecificActionsForUserARN",
                        "Effect": "Allow",
                        "Action": [
                                "ec2-instance-connect:OpenTunnel",
                                "ec2-instance-connect:SendSSHPublicKey"
                        ],
                        "Resource": [

"arn:aws:ec2:us-east-2:AccountNumber:instance-connect-endpoint/eice-0cdcda4db3e069304",
                                "arn:aws:ec2:us-east-2:Account Number
:instance/i-0a8b962883bd3c729"
                        ]
                }
        ]
}
```



Connect Private IP Address Testing :







Using Endpoint Successfully connect Pvt Ip Address :

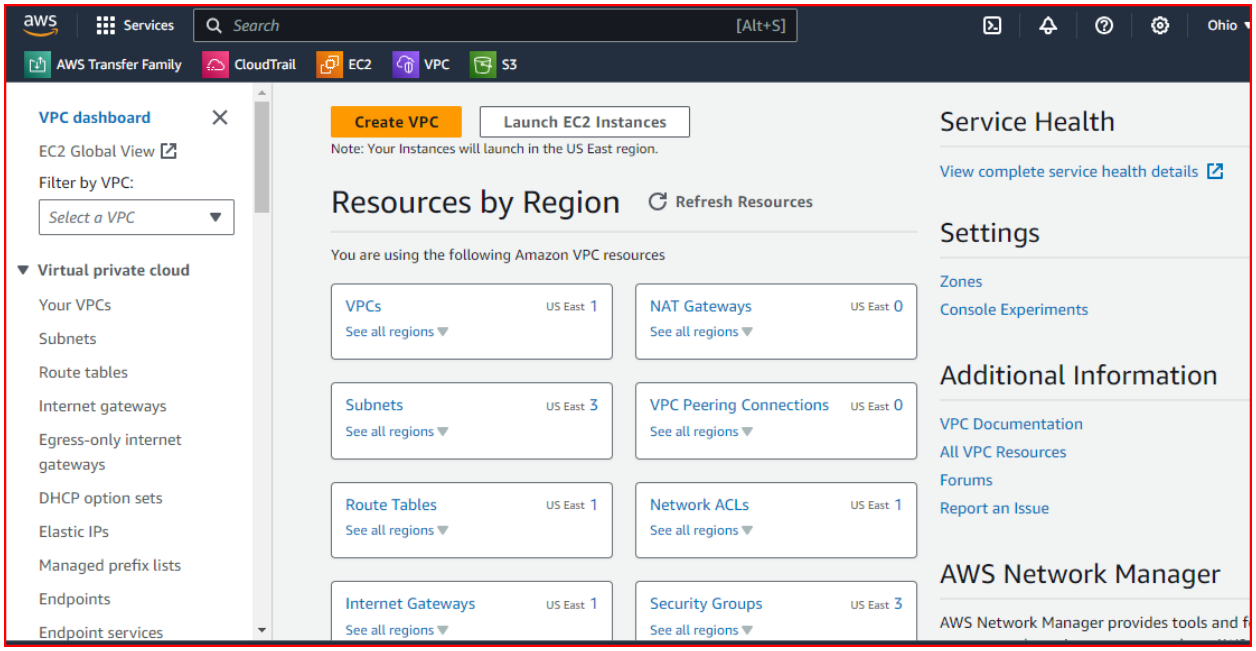
aws Services Search [Alt+S]

AWS Transfer Family CloudTrail EC2 VPC S3

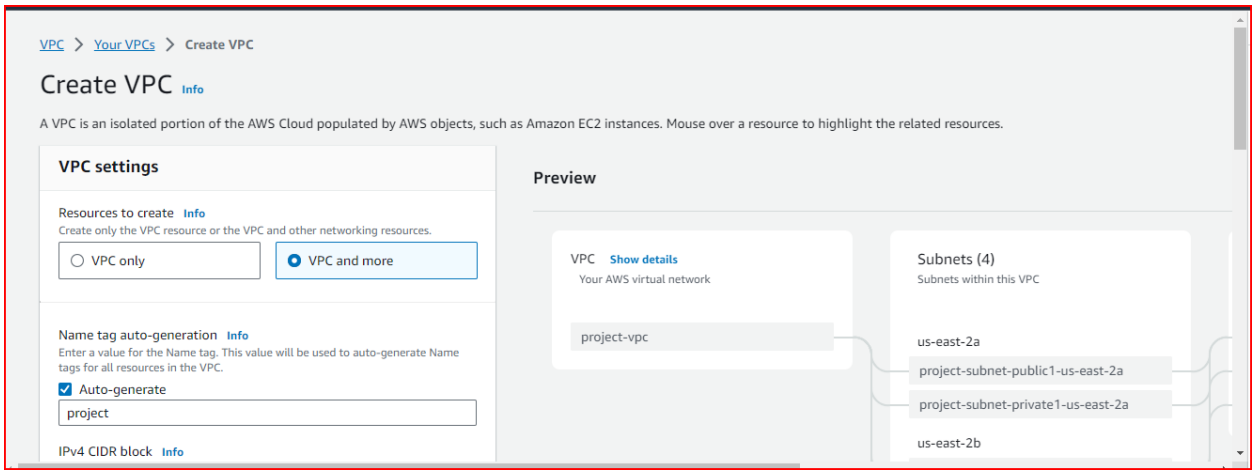
```
 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Dec 20 22:35:13 2023 from 172.31.21.161
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-29-194:~$
```

VPC Launch :

Step1: Goto AWS Console and search vpc and open vpc dashboard.



Click on Create VPC then enter the name of vpc



tags for all resources in the VPC.

☑ Auto-generate

stage

IPv4 CIDR block Info

Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

◉ No IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

Tenancy Info

Default

Number of Availability Zones (AZs) Info

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1	2	3

Preview

VPC Show details

Your AWS virtual network

stage-vpc

Subnets (4)

Subnets within this VPC

us-east-2a

stage-subnet-public1-us-east-2a

stage-subnet-private1-us-east-2a

us-east-2b

stage-subnet-public2-us-east-2b

stage-subnet-private2-us-east-2b

Number of public subnets Info

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0	2

Number of private subnets Info

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0	2	4

▶ Customize subnets CIDR blocks

NAT gateways ($) Info

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None	In 1 AZ	1 per AZ

VPC endpoints Info

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None	S3 Gateway

Preview

VPC Show details

Your AWS virtual network

stage-vpc

Subnets (4)

Subnets within this VPC

us-east-2a

stage-subnet-public1-us-east-2a

stage-subnet-private1-us-east-2a

us-east-2b

stage-subnet-public2-us-east-2b

stage-subnet-private2-us-east-2b

Route tables (3)

Route network traffic to resources

stage-rtb-public

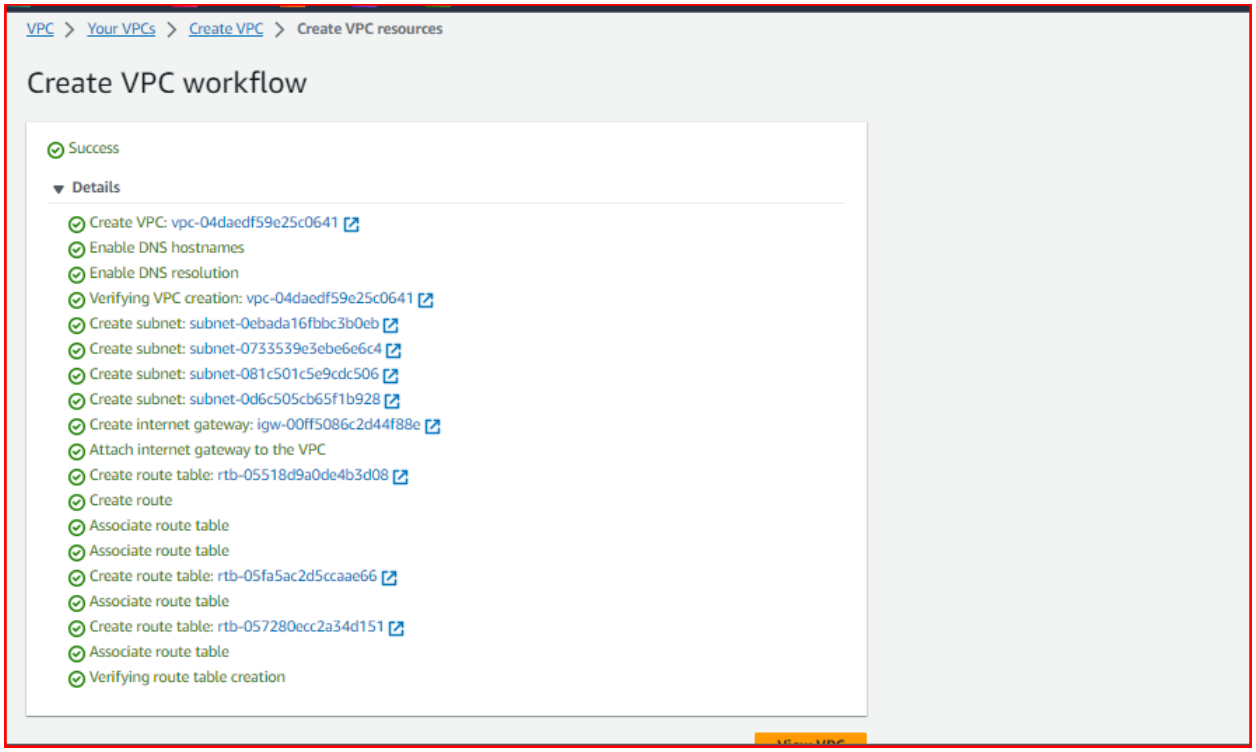
stage-rtb-private1-us-east-2a

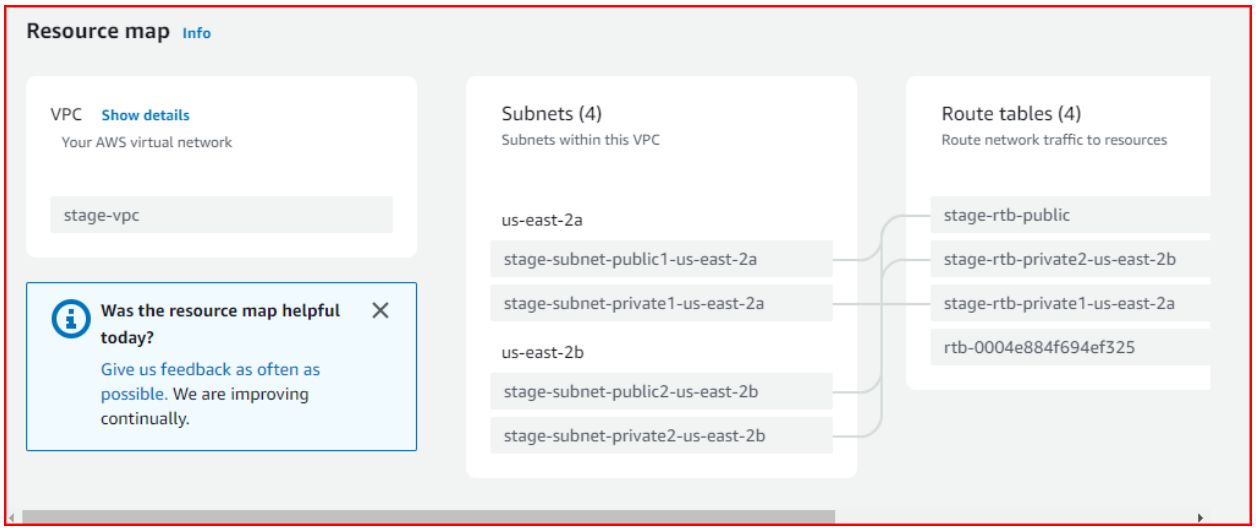
stage-rtb-private2-us-east-2b

Network connections (1)

Connections to other networks

stage-igw





Step2: Checking IGW is added in vpc if not attach the vpc

Why this? – Internet connectivity i.e public

VPC > Internet gateways > igw-00ff5086c2d44f88e

igw-00ff5086c2d44f88e / stage-igw

Actions

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-00ff5086c2d44f88e	Attached	vpc-04daedf59e25c0641 | stage-vpc	023516359556

Tags

Manage tags

Search tags

1

Key	Value
Name	stage-igw

Step3: Subnets

Create 2 Public and 2 Private Subnets in 2 AZs

Subnets (7) Info

Actions | Create subnet

Find resources by attribute or tag

1

Name	Subnet ID	State	VPC	IPv4 CIDR
stage-subnet-public2-us-east-2b	subnet-0733539e3ebe6e6c4	Available	vpc-04daedf59e25c0641 | stag...	10.0.16.0/20
stage-subnet-private2-us-east-2b	subnet-0d6c505cb65f1b928	Available	vpc-04daedf59e25c0641 | stag...	10.0.144.0/20
stage-subnet-private1-us-east-2a	subnet-081c501c5e9cdc506	Available	vpc-04daedf59e25c0641 | stag...	10.0.128.0/20
stage-subnet-public1-us-east-2a	subnet-0ebada16fbbc3b0eb	Available	vpc-04daedf59e25c0641 | stag...	10.0.0.0/20

Step4: Route Tables

Default Route Table is Public one then create pvt rt

Route tables (5) Info

Actions | Create route table

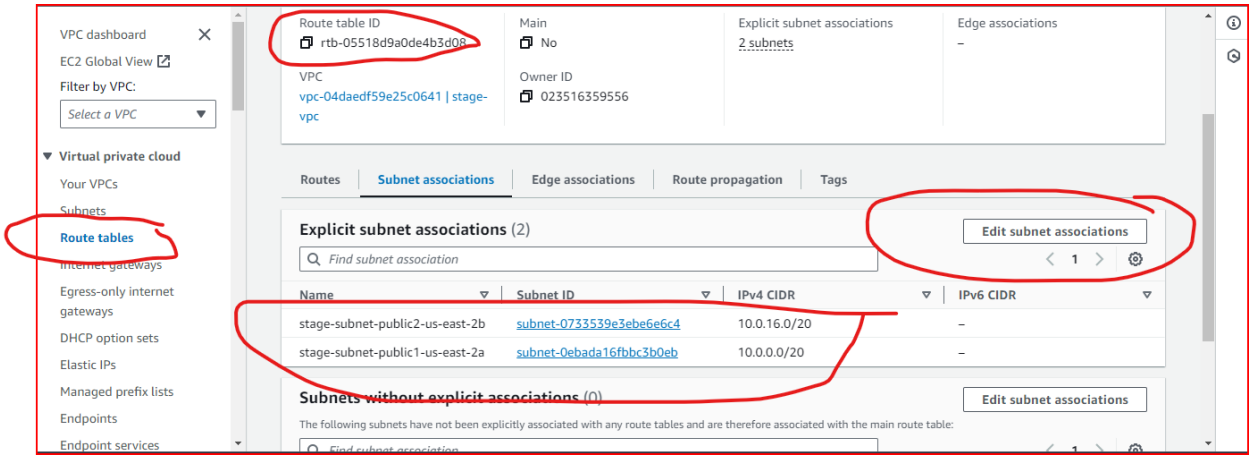
Find resources by attribute or tag

1

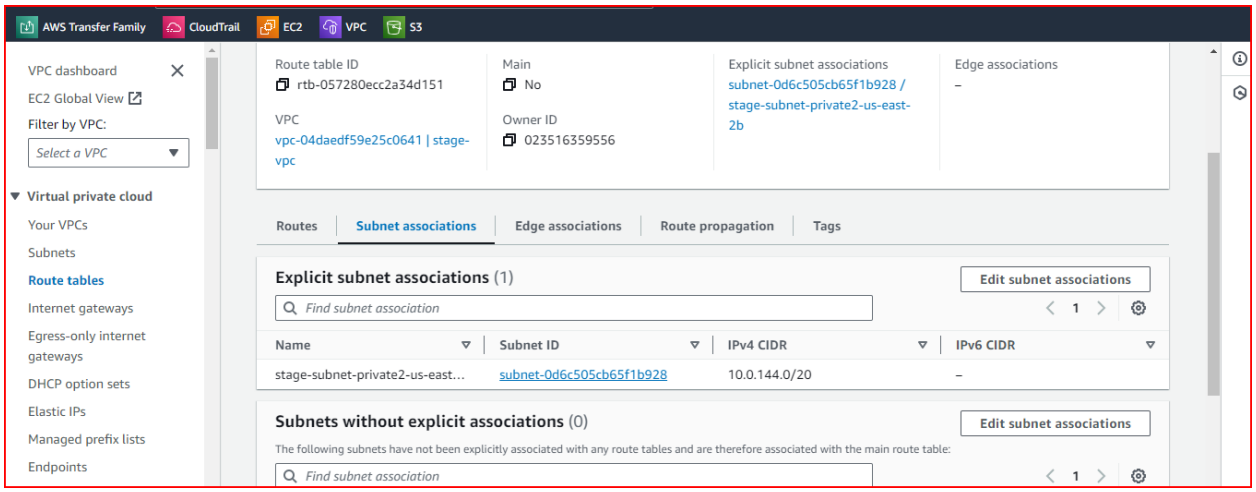
Name	Route table ID	Explicit subnet associati...	Edge associations	Main
stage-rtb-public	rtb-05518d9a0de4b3d08	2 subnets	–	No
stage-rtb-private2-us-east-2b	rtb-057280ecc2a34d151	subnet-0d6c505cb65f1b...	–	No
stage-rtb-private1-us-east-2a	rtb-05fa5ac2d5ccaae66	subnet-081c501c5e9cdc5...	–	No
–	rtb-02807e1bfb6400b69	subnet-08f3852a6c22eb...	–	Yes

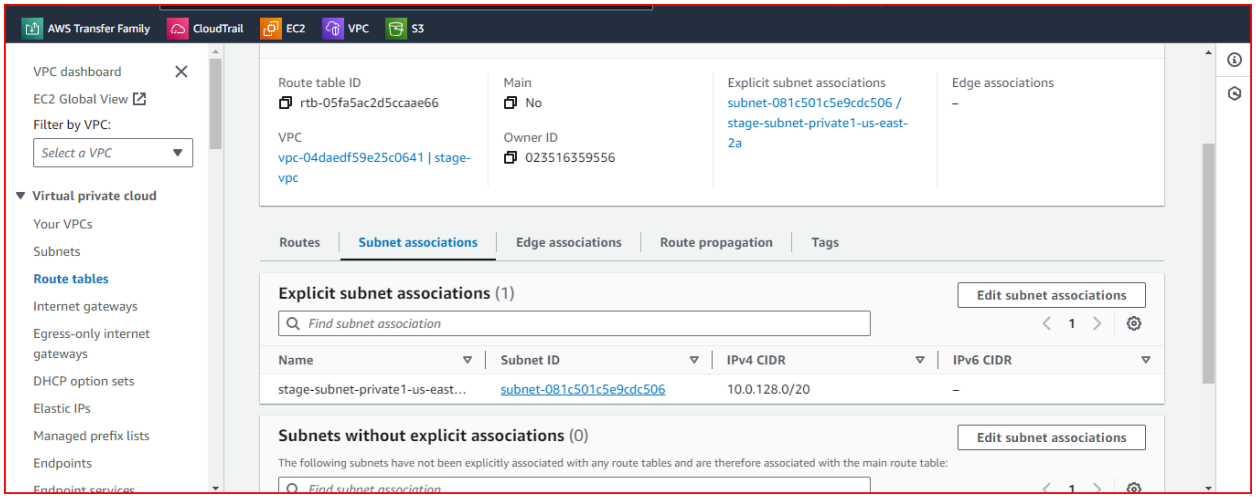
Step5: Route Table Subnets association

Adding public subnets into public route table

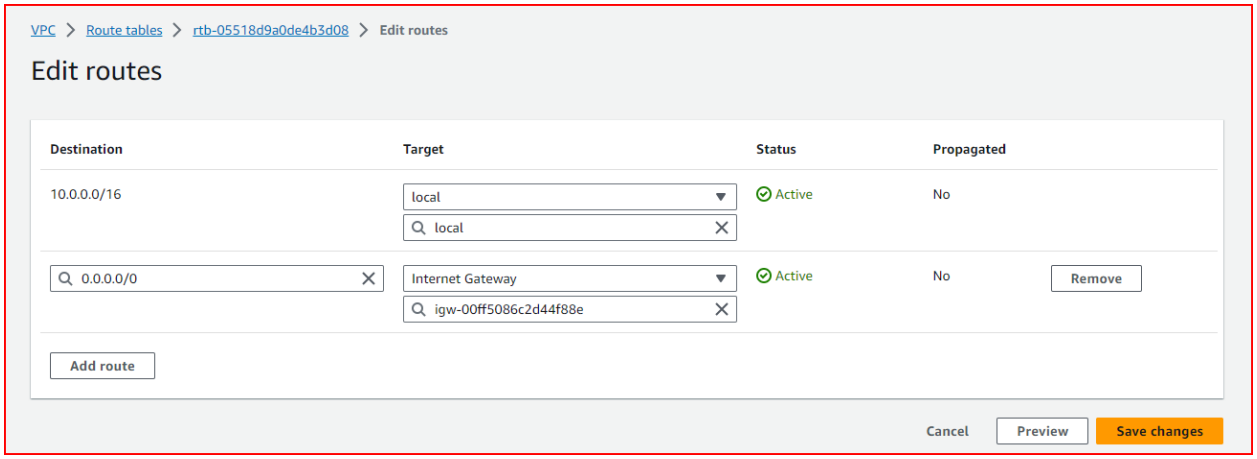


Adding private subnets into private route table



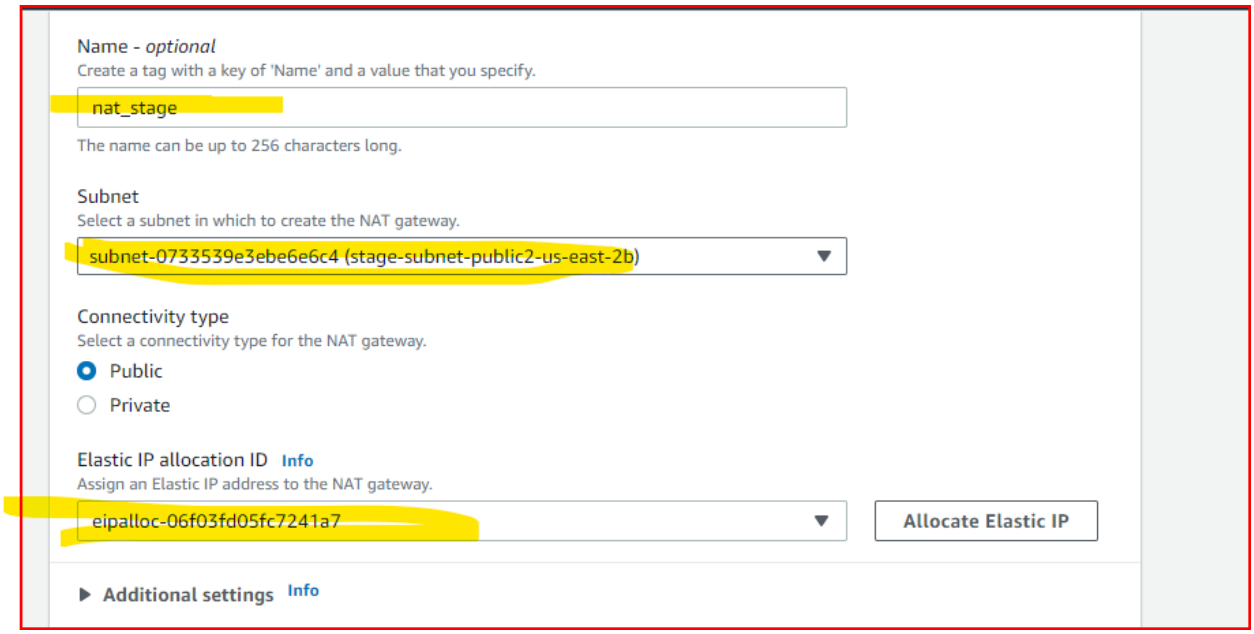


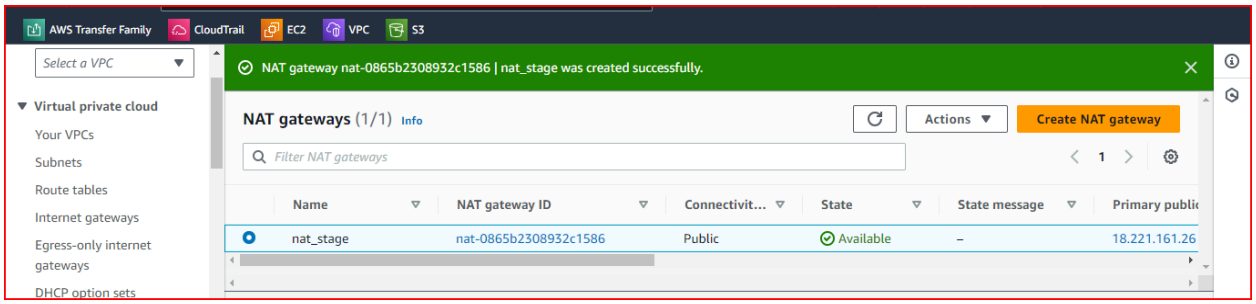
Step6: adding the Internet gateway to the public route table to explore the subnet to access from internet



Step7: Creating NAT Gateway

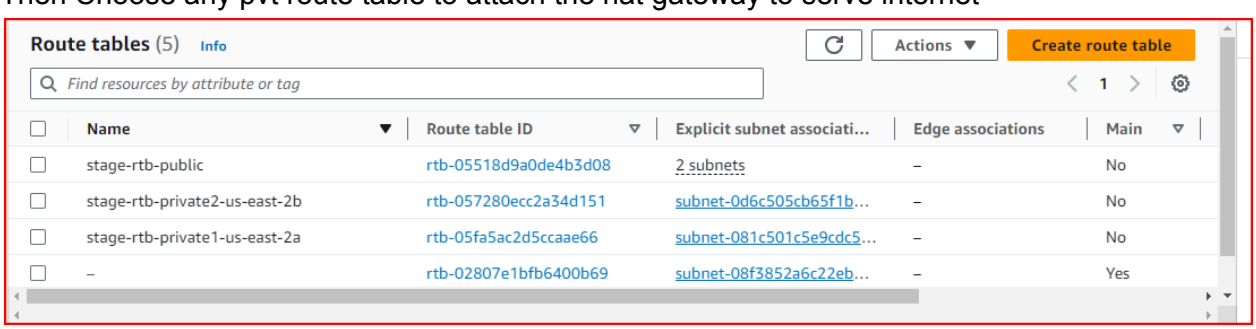
Creating NAT for private route table to provide internet to them
Here choose any pub subnet to access internet to the NAT gateway

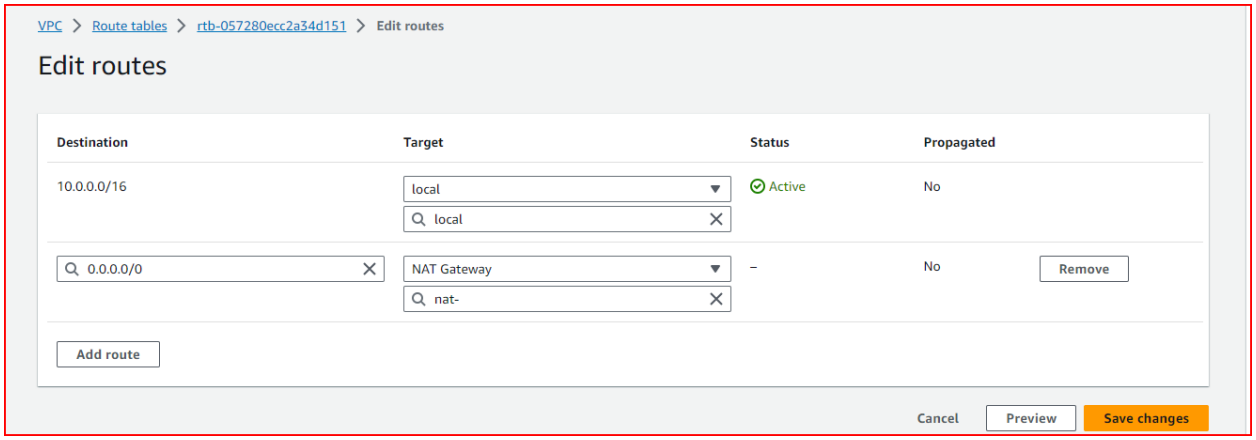




Step8: Add the nat gateway ino pvt route table under routes

Then Choose any pvt route table to attach the nat gateway to serve internet





Successfully configured vpc setup if any other services under the vpc we can add based on the requirements.