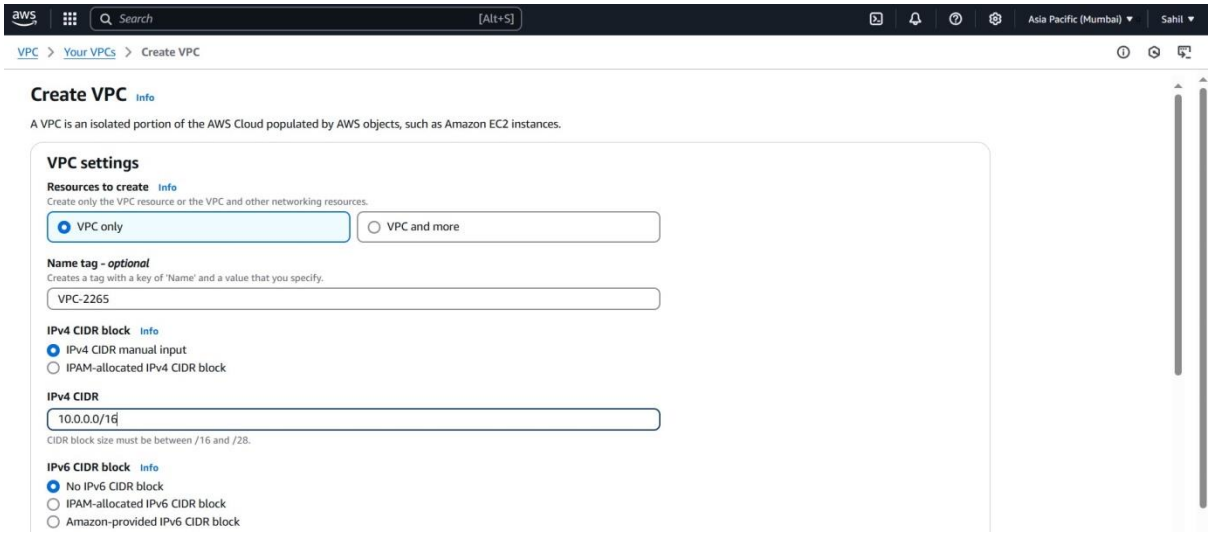
School of Computer Science, Engineering and Applications (SCSEA)
B. Tech TY (CCSA)
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade PRN: 20220802265

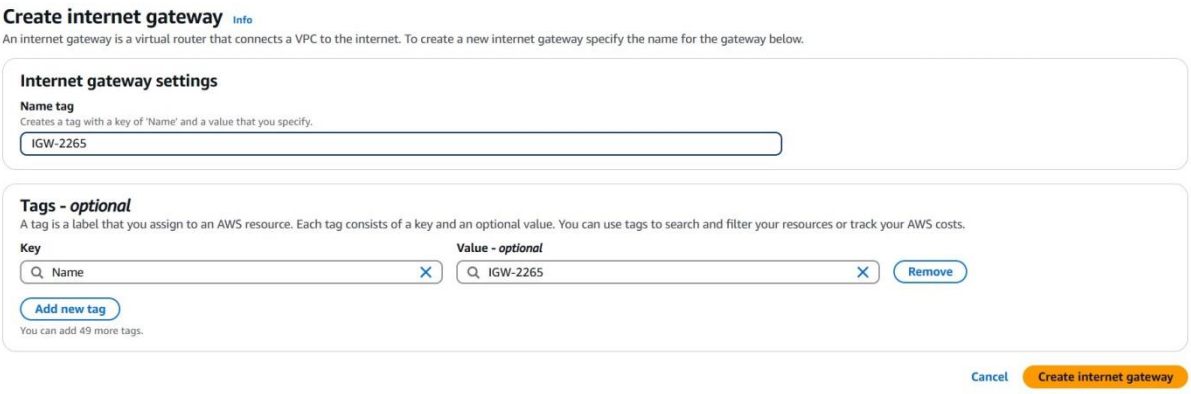
Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

Step 1: Create a VPC and connect Internet Gateway to it.

- Go to AWS console and search for VPC.
- Create VPC by selecting 'VPC Only' with valid name.
- Set IPv4 CIDR range as '10.0.0.0/16'.



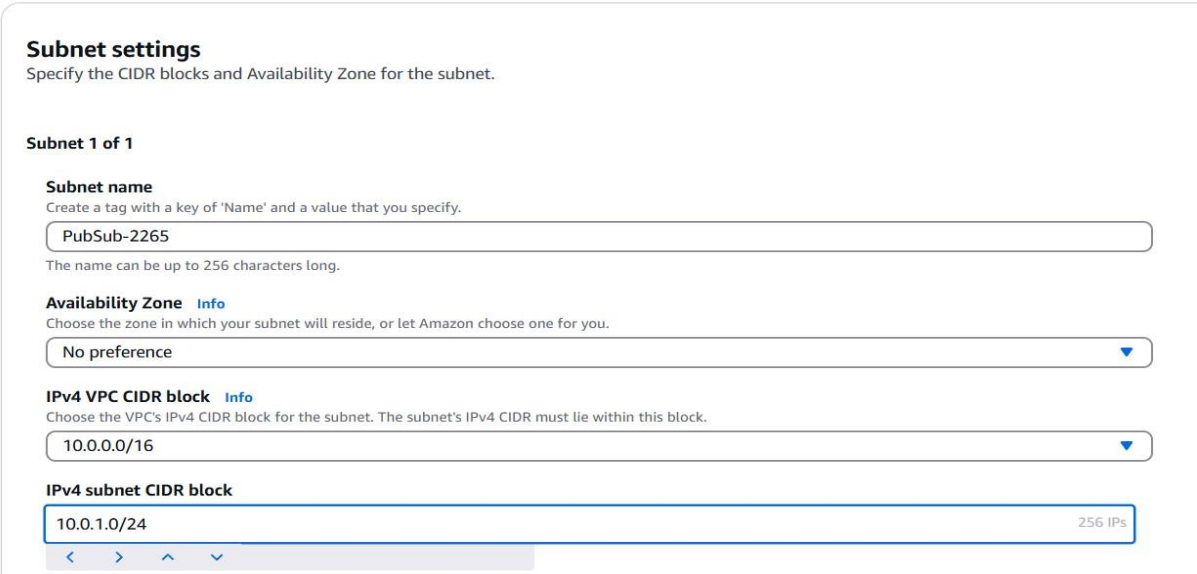
- Go to Internet Gateway.
- Create an Internet Gateway.



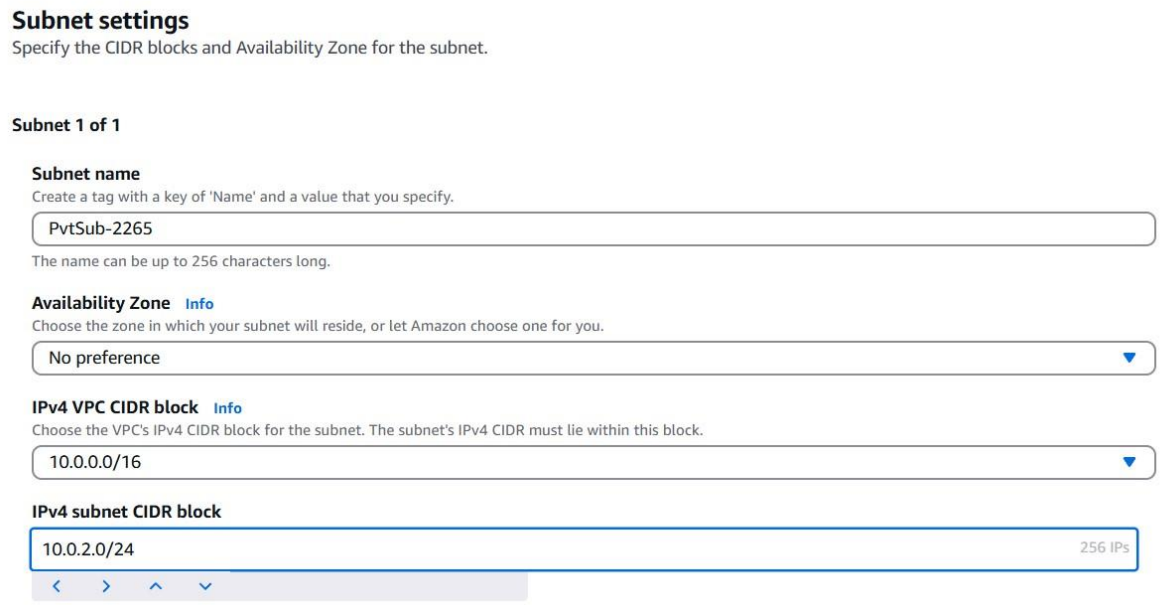
- Attach the IGW to the VPC.

Step 2: Create a Public Subnet and a Private Subnet and Route Tables respectively.

- Create a Public Subnet and name it 'PubSub-2265'.
- Enter IPV4 subnet CIDR block as "10.0.1.0/24", then click on "Create subnet".



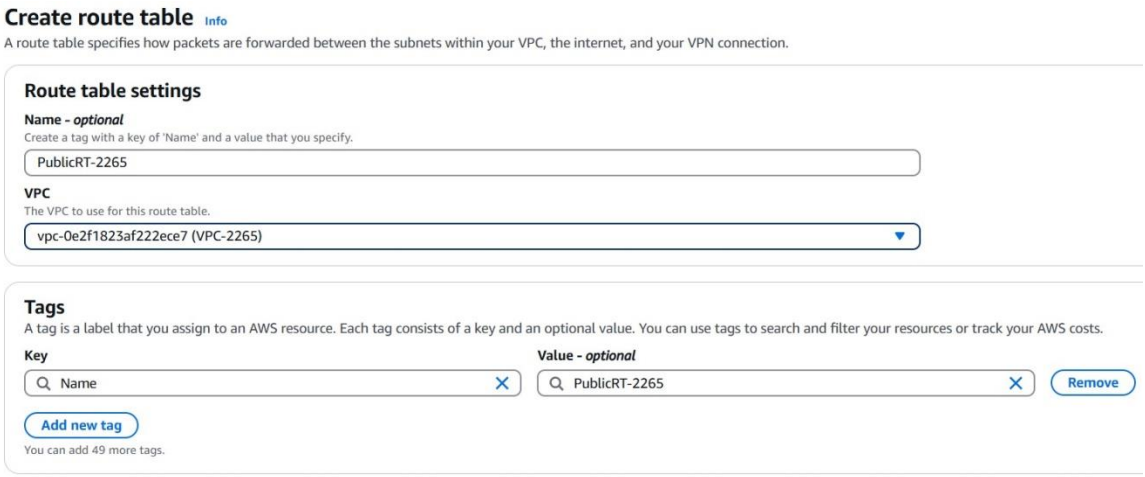
- Create a Private Subnet and name it 'PvtSub-2265'.
- Enter IPV4 subnet CIDR block as "10.0.2.0/24", then click on "Create subnet".

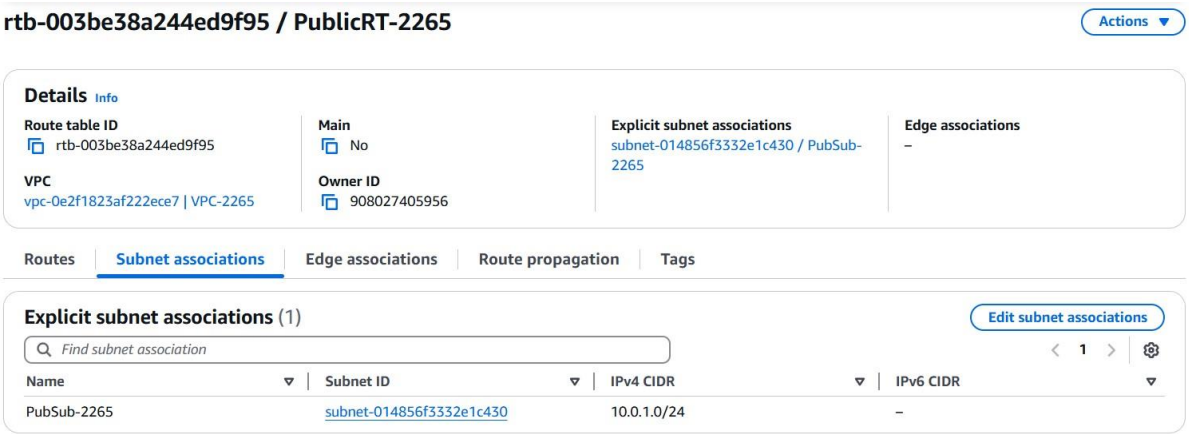


- After creating both the subnets, go to Public Subnet – 'Actions' – 'Edit subnet settings' – Tick the 'Enable auto-assign public IPv4 address'.

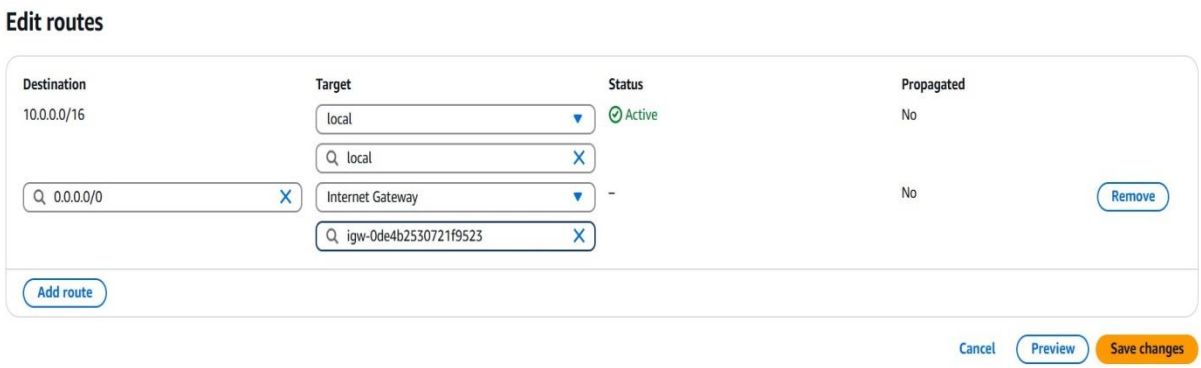
- Create a Public Route Table and name it 'PublicRT-2265' and select the VPC we created.

- Associate the Public Subnet to the Route Table.

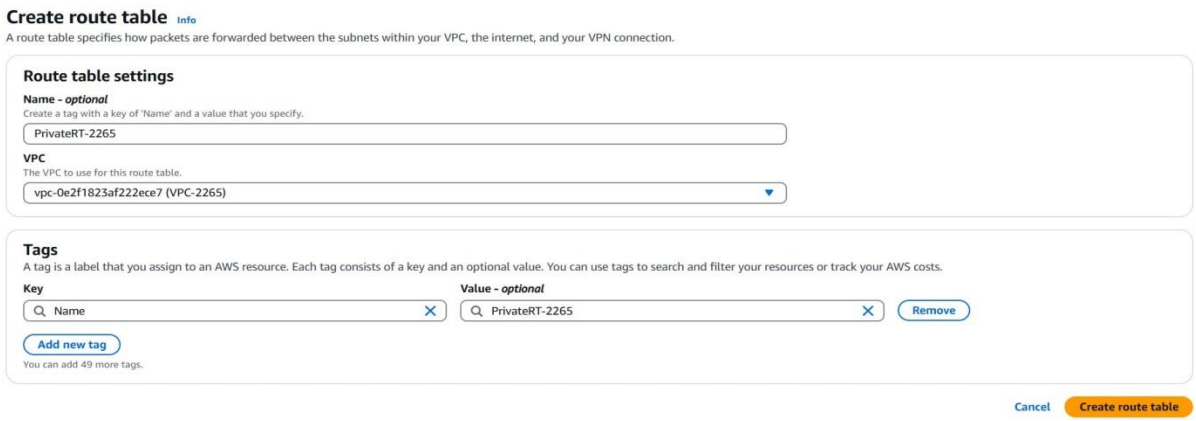




- Add a Route with Destination as '0.0.0.0./0' and Target as 'Internet Gateway' and select the internet gateway we created i.e. 'IGW-2265'.

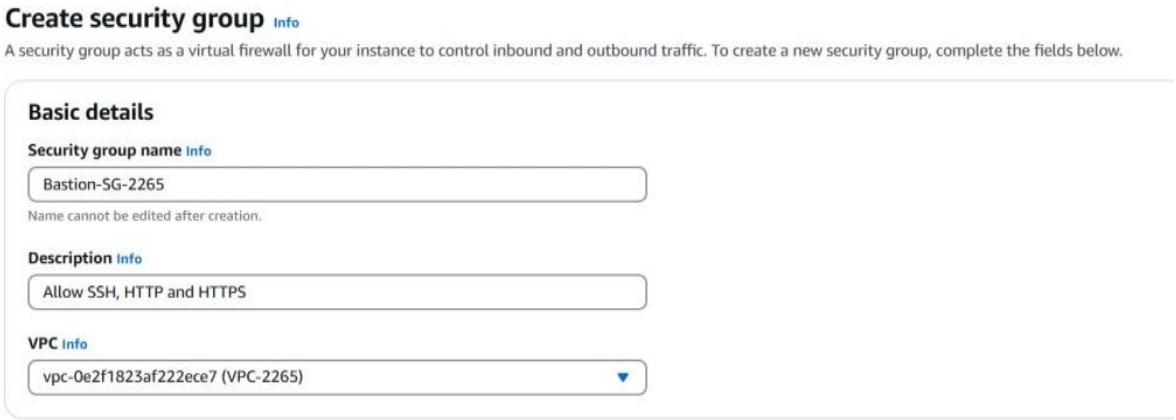


- Create a Private Route Table and name it 'PrivateRT-2265' and select the VPC we created.
- Associate the Private Subnet to the Route Table.

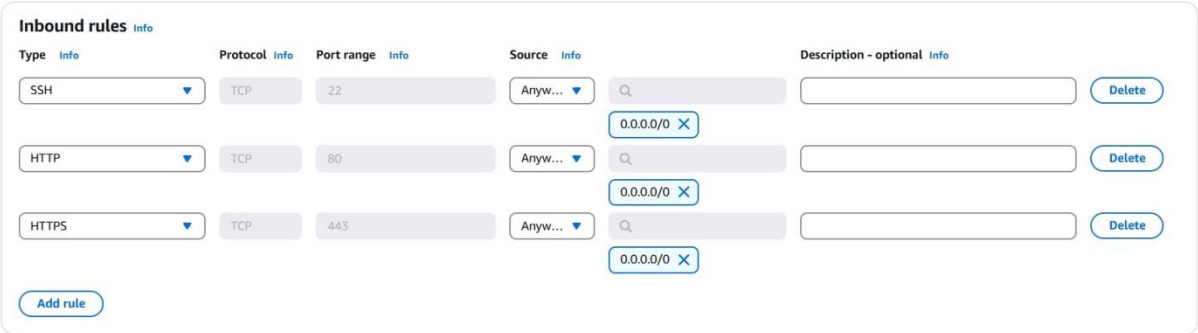


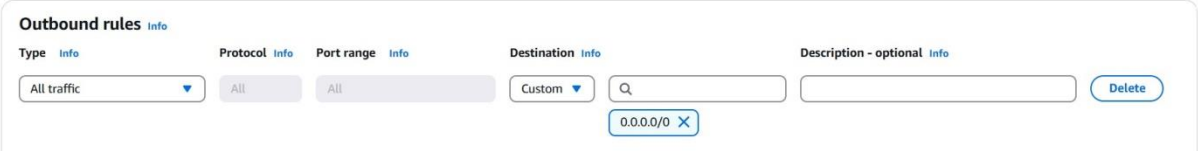
Step 3: Create Security Groups (for public and private instances) and attach the VPC.

- Create a Public Security Group and name it 'Bastion-SG-2265'.
- Add description and attach the VPC 'VPC-2265'.



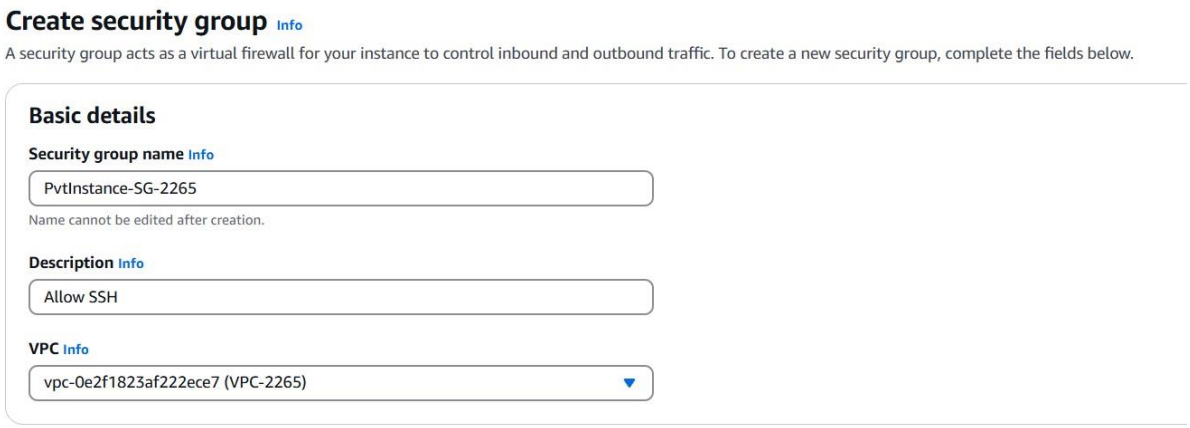
- Set Inbound Rules : SSH – Anywhere IPv4, HTTP – Anywhere IPv4 and HTTPS – Anywhere IPv4.



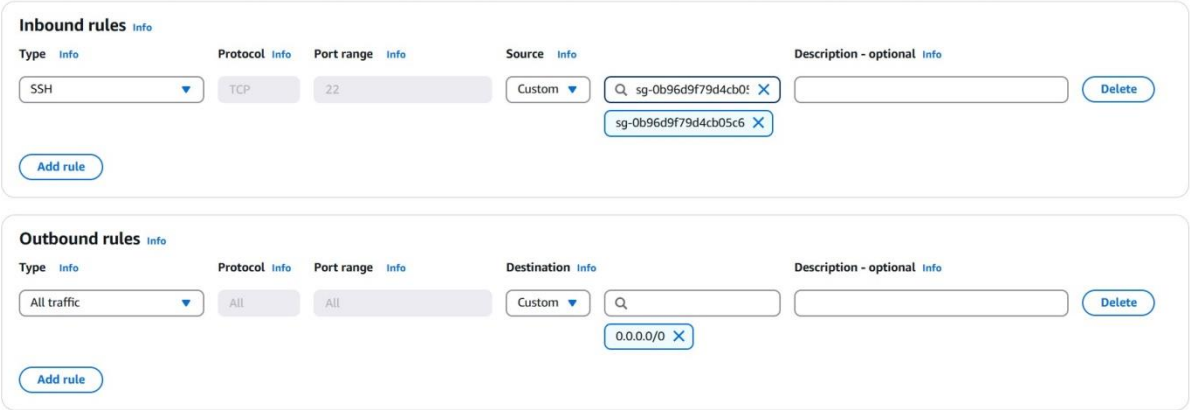


- Create a Private Security Group and name it 'PvtInstance-SG-2265'.

- Add description and attach the VPC 'VPC-2265'.

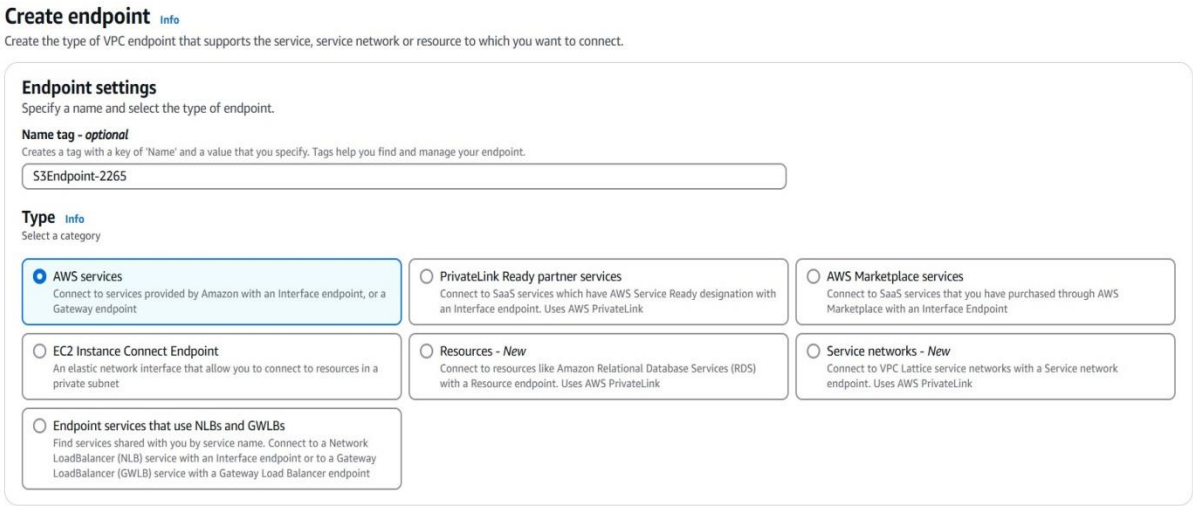


- Set Inbound Rules : SSH – Source – Custom – Bastion-SG-2265.

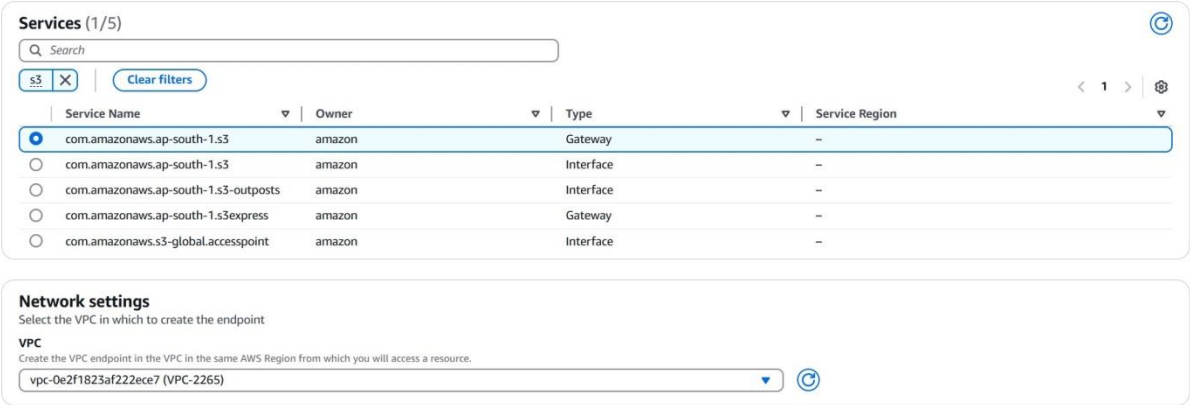


Step 4: Create an Endpoint.

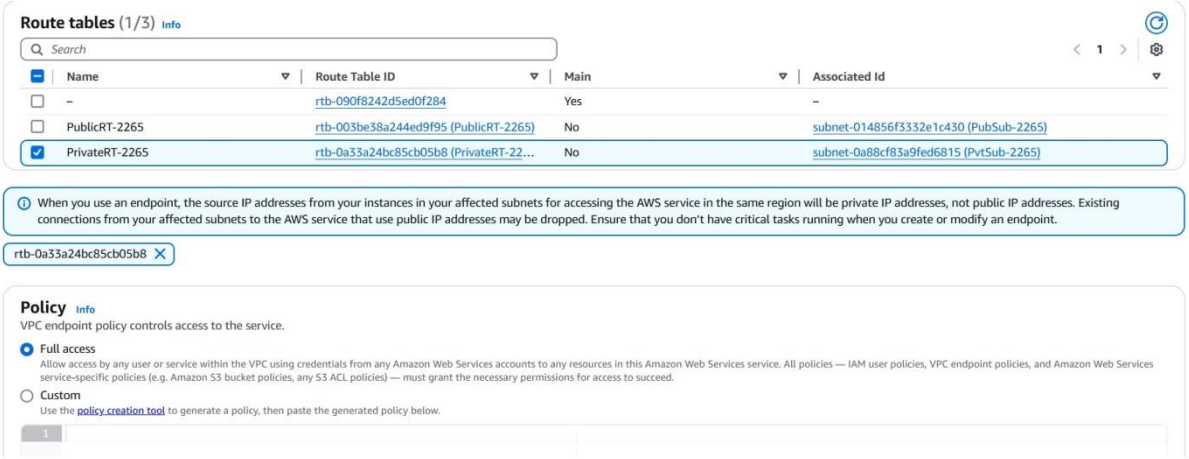
- Create an Endpoint with name 'S3Endpoint-2265'.
- Select Type as 'AWS services'.



- In Services Tab, search for 's3' and select the S3 service with the Type 'Gateway'.
- In Network settings, select our VPC 'VPC-2265'.

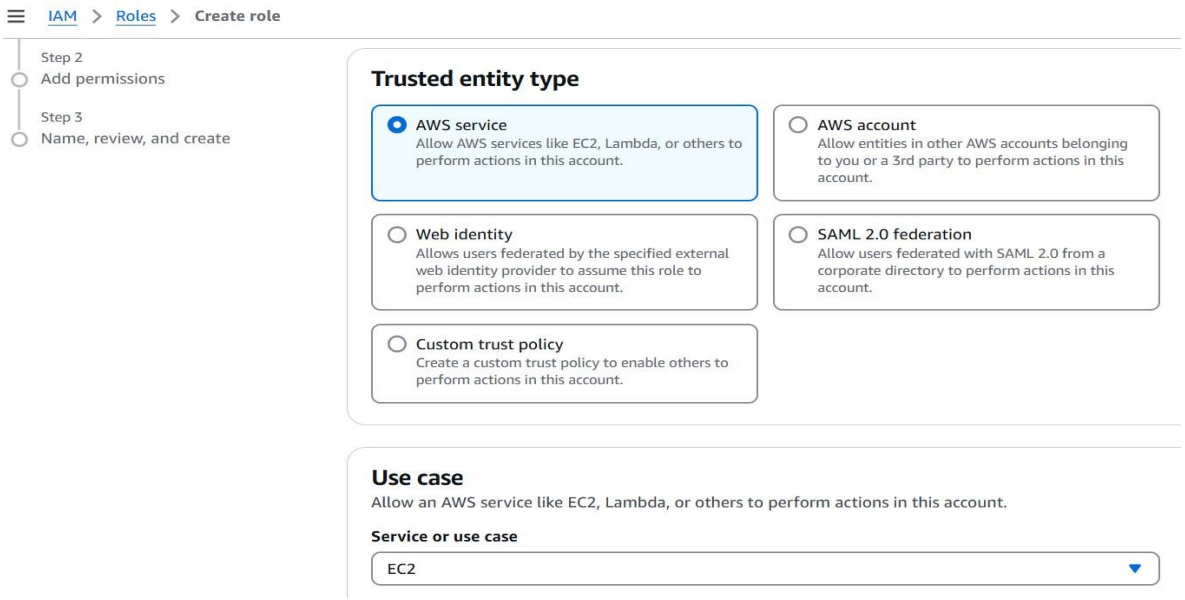


- Next select Private Route Table i.e. 'PrivateRT-2265'.
- Keep policy as 'Full access'and click 'Create endpoint'.

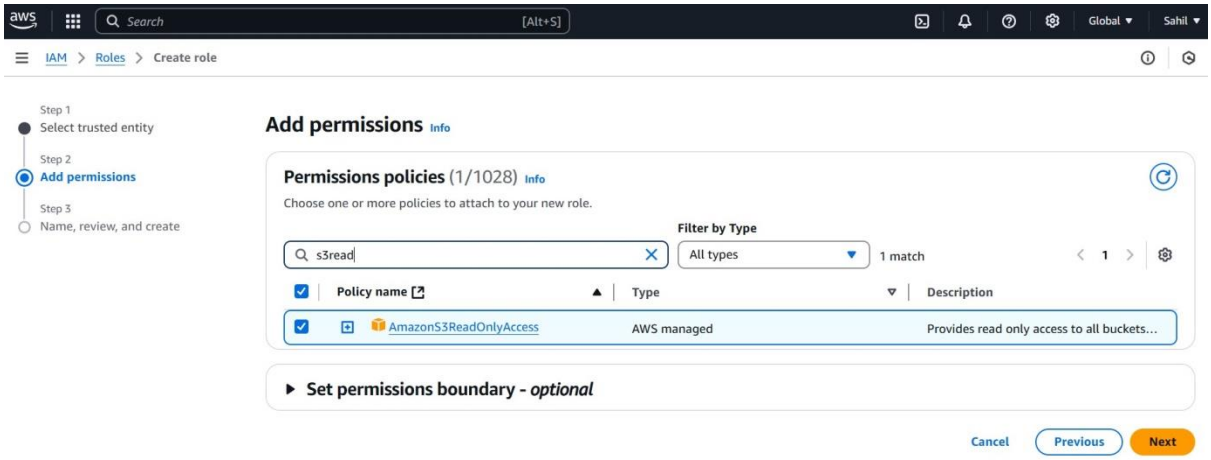


Step 5: Create IAM role.

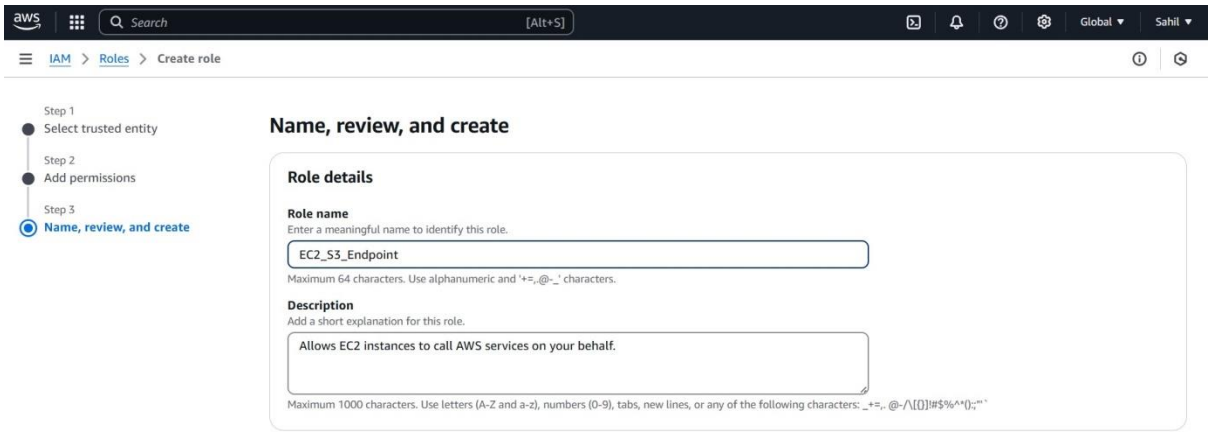
- Go to IAM dashboard.
- Go to 'Roles' and click on 'Create a role'.
- Select Trusted entity type – 'AWS service' and Use case – 'EC2' and Click 'Next'.



- For permissions, search and select 'AmazonS3ReadOnlyAccess' and click on 'Next'.

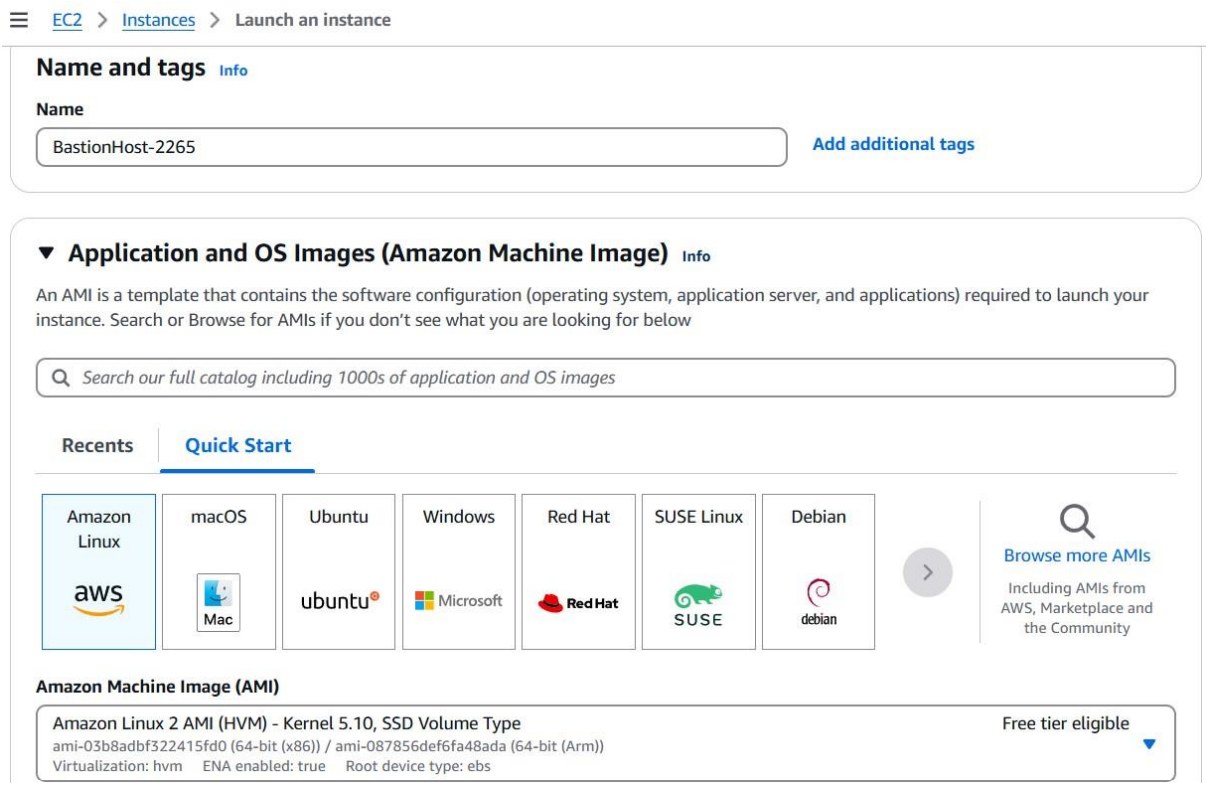


- Now, set role name as 'EC2_S3_Endpoint'.
- Click on Create.

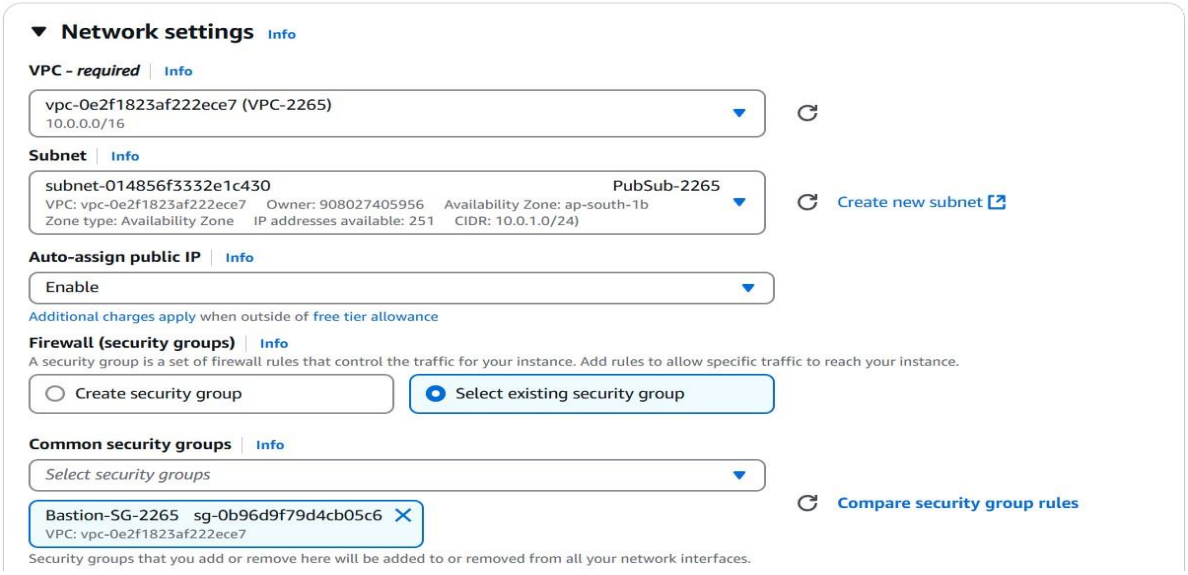


Step 6: Launch EC2 instances (Public and Private).

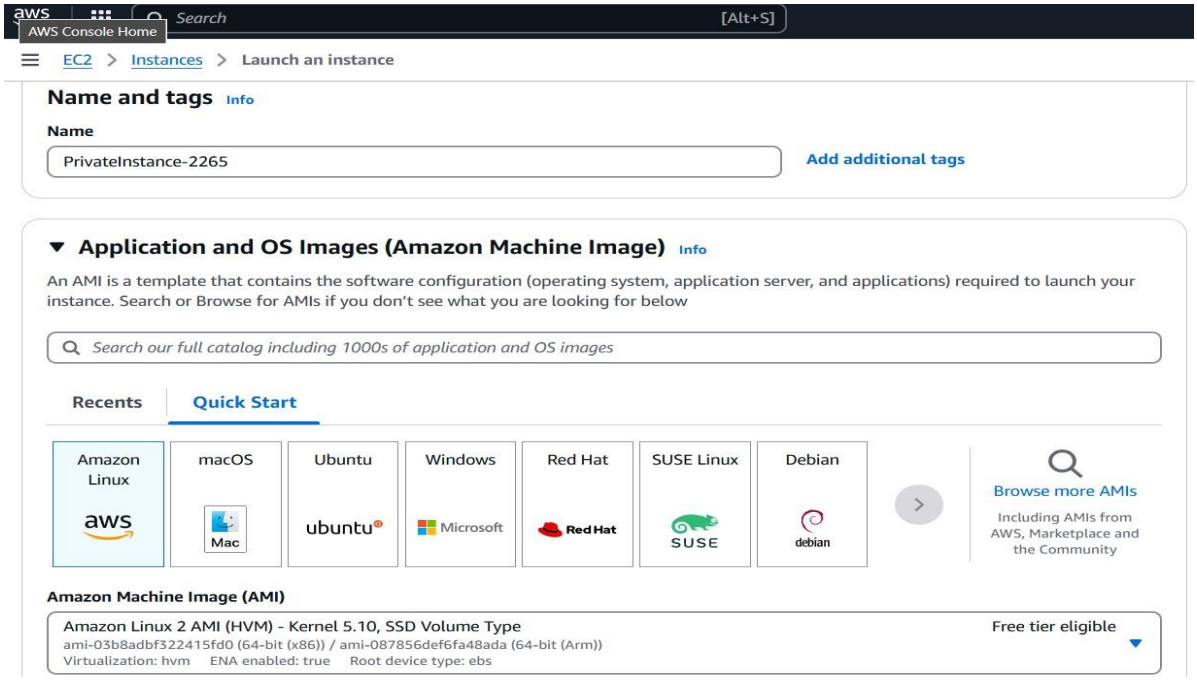
- Go to EC2 console and click on 'Launch Instances'.
- Name the public instance – 'BastionHost-2265'.
- Select AMI as 'Amazon Linux' and under that select 'Amazon Linux 2 AMI (HMV)'.



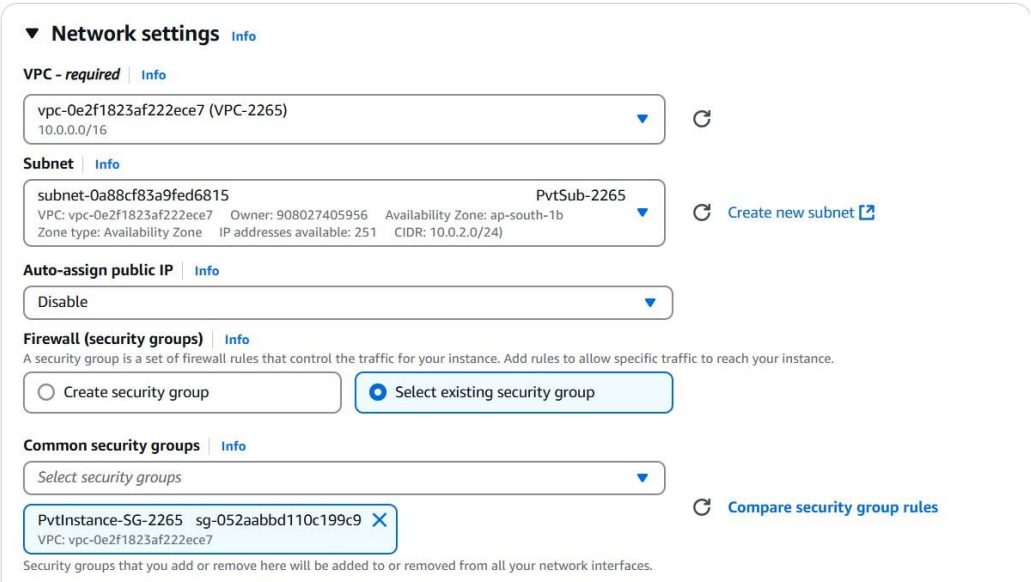
- Now, select Key Pair.
- Under Network settings – select VPC 'VPC-2265'.
- Subnet as 'PubSub-2265'.
- Enable auto-assign public IP.
- For Security group, select the public SG we created earlier i.e. 'Bastion-SG-2265'.
- Launch the instance.



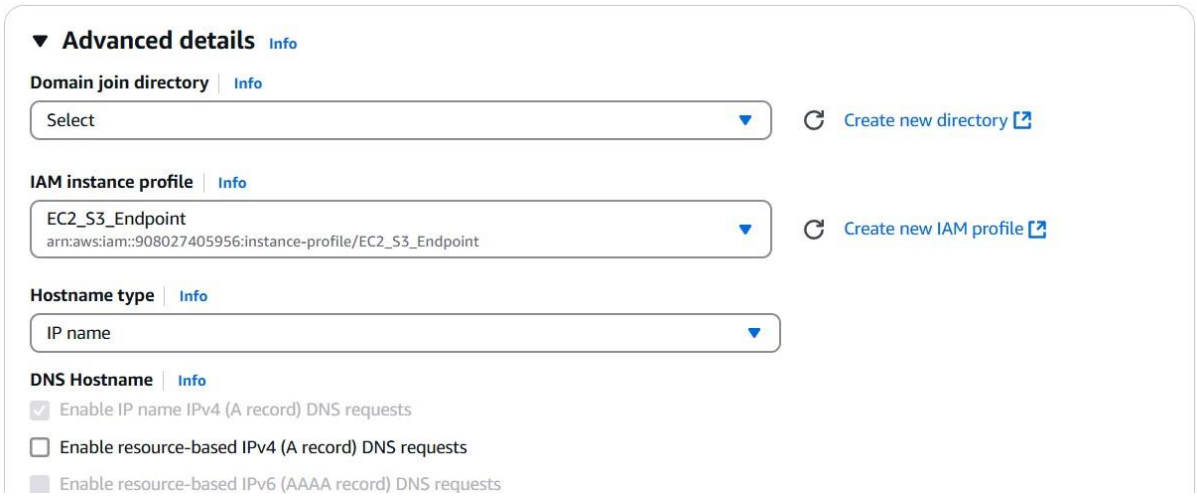
- Now, create a Private instance and name it 'PrivateInstance-2265'.
- Select AMI as 'Amazon Linux' and under that select '<u>Amazon Linux 2 AMI (HMV)</u>'.



- Now, select Key Pair.
- Under Network settings – select VPC 'VPC-2265'.
- Subnet as 'PvtSub-2265'.
- Do not enable auto-assign public IP.
- For Security group, select the public SG we created earlier i.e. 'PrivateInstance-SG-2265'.

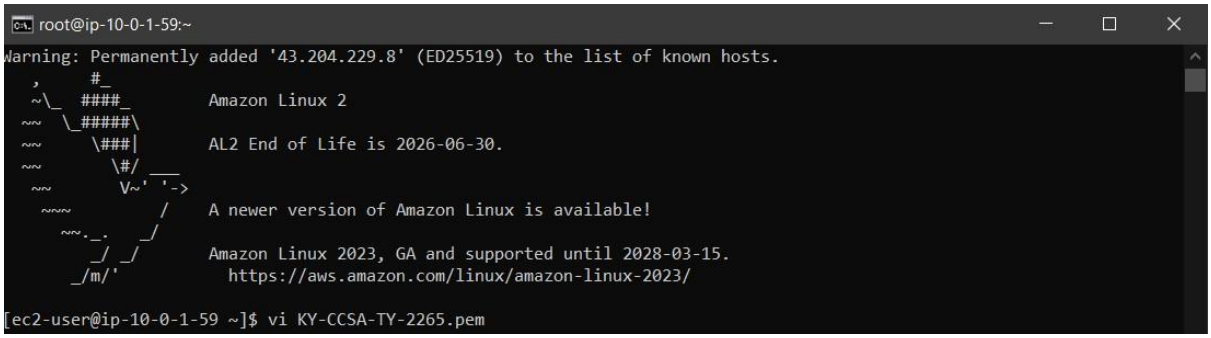


- Now, in Advanced details – IAM instance profile – select the role we created earlier i.e. 'EC2_S3_Endpoint'.
- Launch the instance.



Step 7: Connect Public instance in terminal.

- Go to the public instance 'BastionHost-2265' and connect it in terminal.
- Type the command 'vi KY-CCSA-TY-2265.pem' to create a Key pair in the Public instance so that we can launch the private instance inside this public instance.
- Open the Key on the device and copy the contents of the key and paste it in the terminal.
- After pasting the contents of the key in the terminal, press 'esc' key and type command ':wq' to save and exit the window.



- Now type the command 'chmod 400 KY-CCSA-TY-2265.pem' and press Enter button.
- Now, go to the private instance 'PrivateInstance-2265' and connect it in terminal.

```
[ec2-user@ip-10-0-1-59 ~]$ chmod 400 KY-CCSA-TY-2265.pem
[ec2-user@ip-10-0-1-59 ~]$ ssh -i "KY-CCSA-TY-2265.pem" ec2-user@10.0.2.60
       #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2026-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[ec2-user@ip-10-0-2-60 ~]$
```

- Now the private instance is connected inside the public instance.
- Now, type the command 'aws s3 ls' to list the S3 buckets.
- <u>Note:</u> There should already be a S3 bucket created.
- If it doesn't list any bucket, type command 'aws configure' and follow these steps-
  - In Security credentials, Generate AWS Access key ID and AWS Secret key.
  - Paste these in the terminal respectively.
  - Type the Default region name.
  - Press Enter.
- Now, type the previous command for listing buckets again i.e. 'aws s3 ls'.
- It will show the buckets now (bucket-2265).
- Access the bucket using command 'aws s3 ls s3://bucket-2265'.
- Here we can see the 'HelloWorld.txt' file in the bucket.

Name of the Student: Sahil S. Mandawgade **PRN:** 20220802265

Title of Practical: 4. Private Access to S3 via VPC Endpoint in a Secure VPC Architecture.

```
[root@ip-10-0-2-60 ~]# aws s3 ls
^C
[root@ip-10-0-2-60 ~]# aws configure
AWS Access Key ID [None]: [redacted]
AWS Secret Access Key [None]: [redacted]
Default region name [None]: ap-south-1
Default output format [None]:
[root@ip-10-0-2-60 ~]# aws s3 ls
2025-02-06 09:29:15 bucket-2265
[root@ip-10-0-2-60 ~]# aws s3 ls s3://bucket-2265
2025-02-06 09:31:34         12 HelloWorld.txt
[root@ip-10-0-2-60 ~]#
```