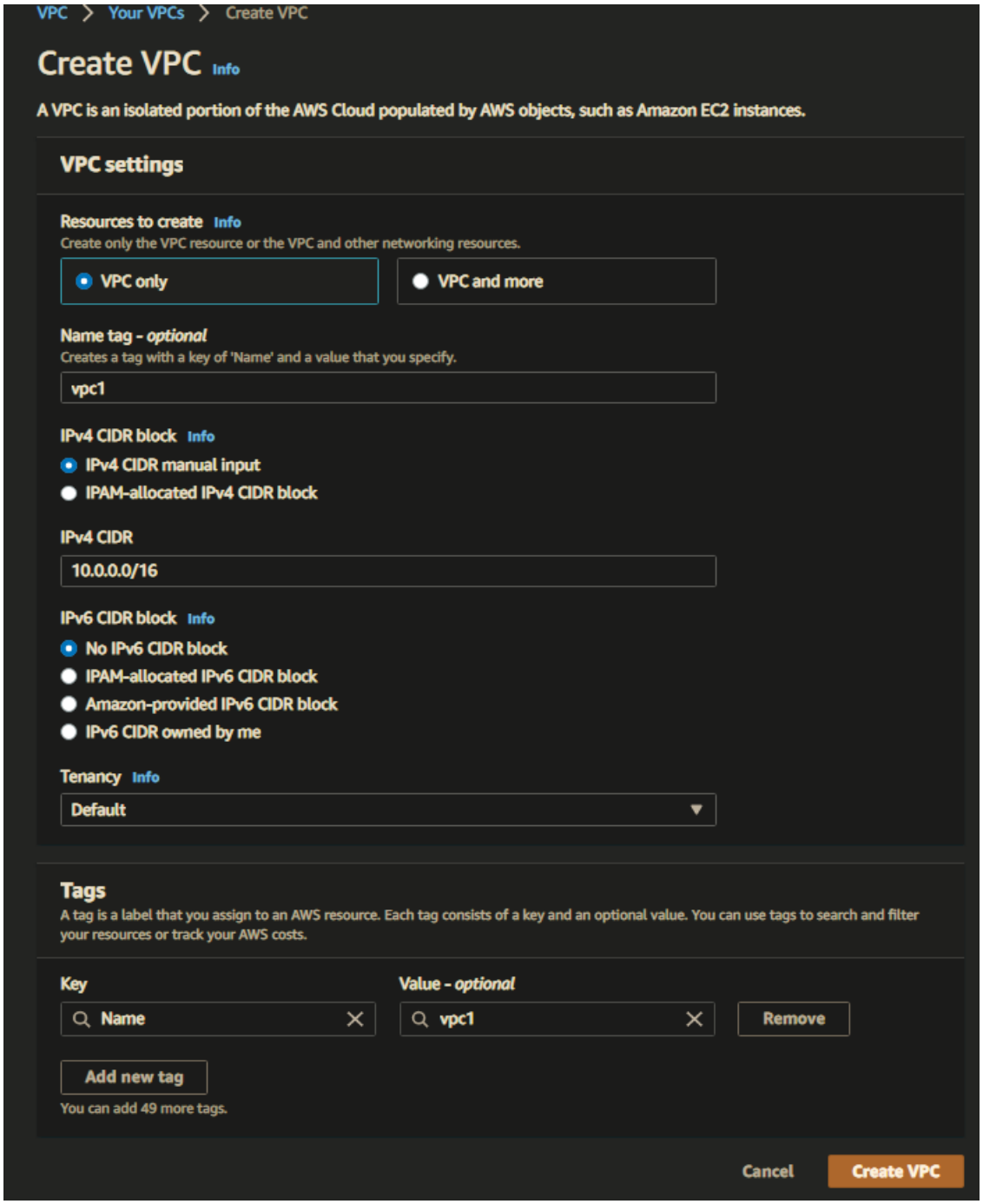
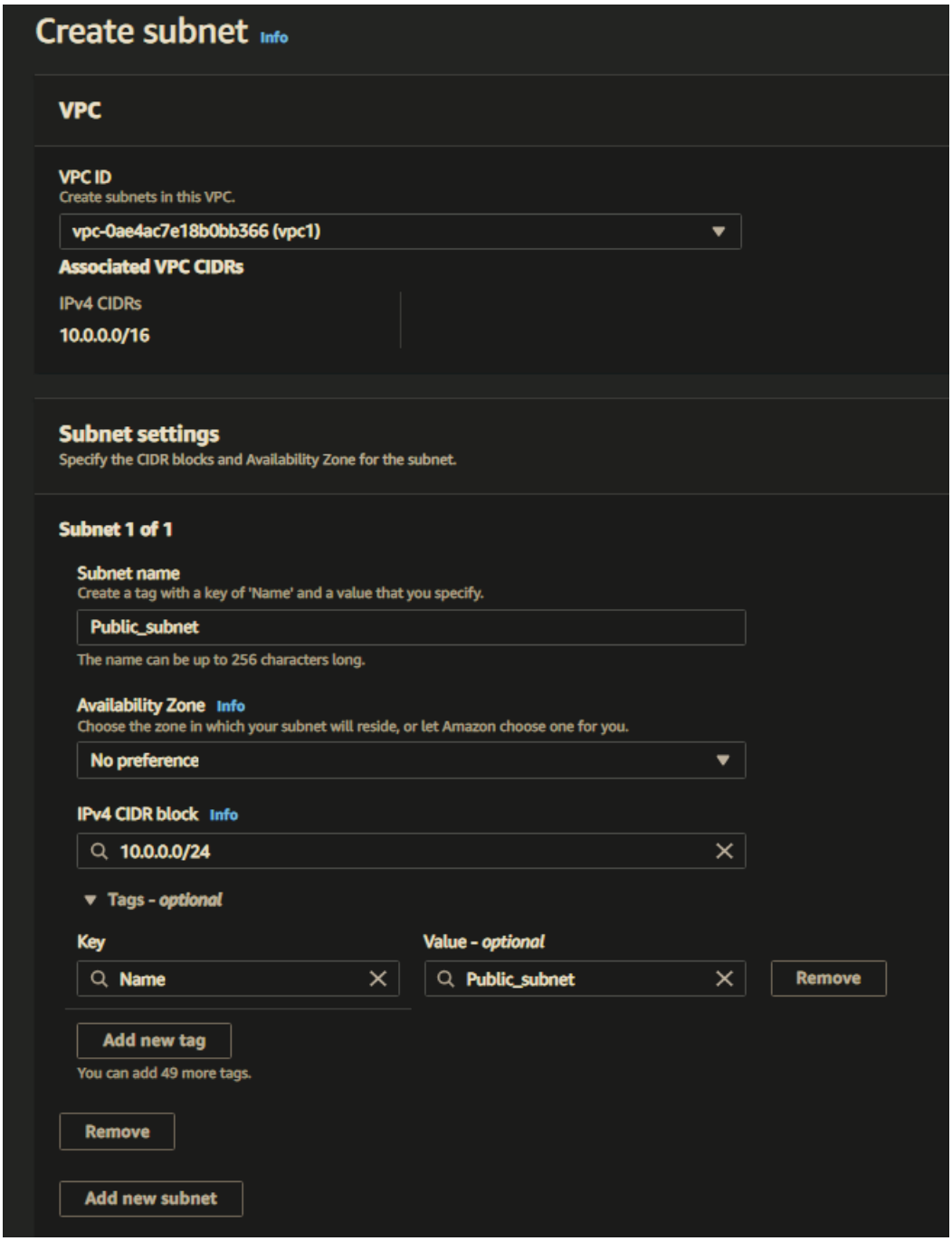
VPC ENDPOINT LAB

Create a VPC

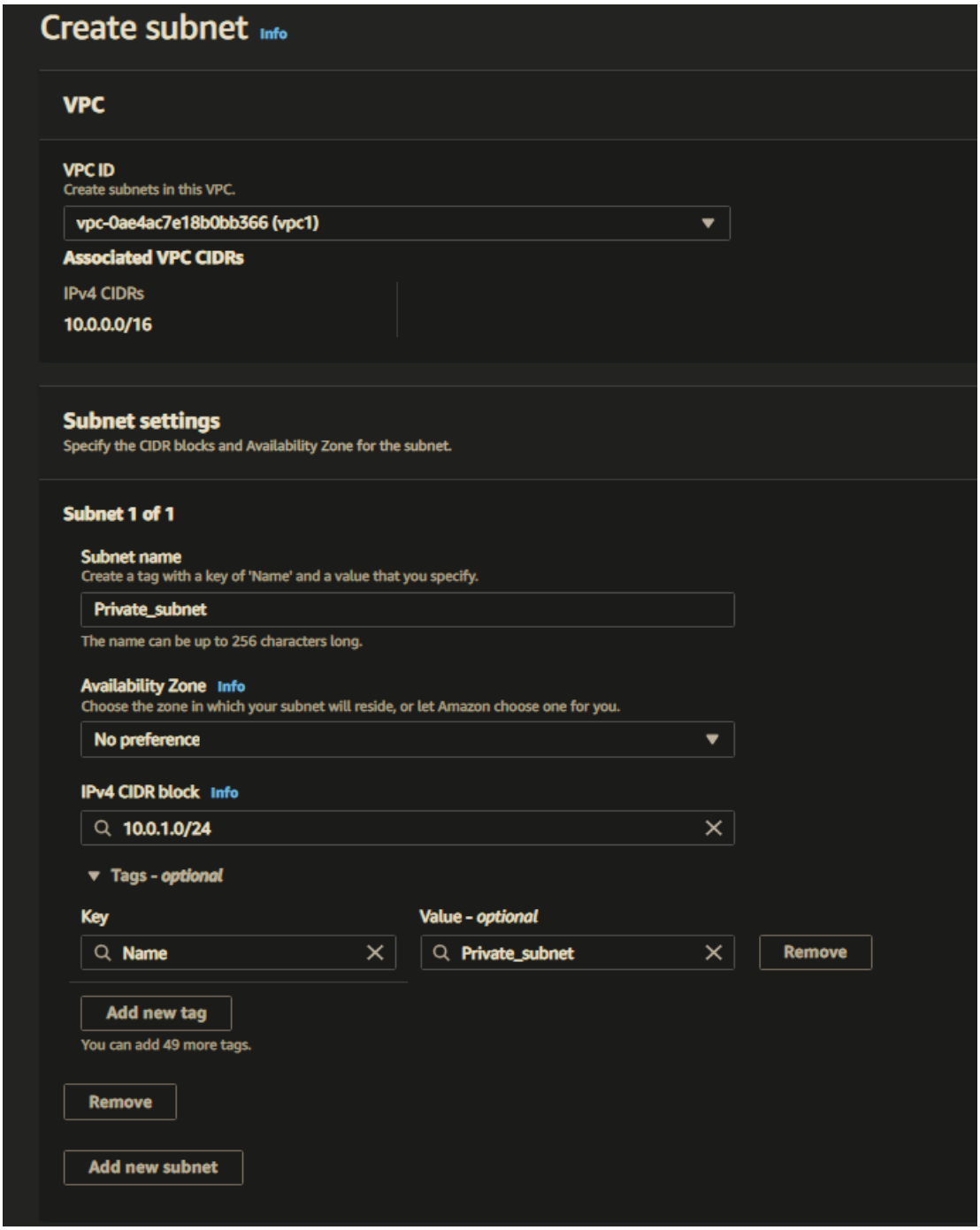


Create Subnets one for public and one for private

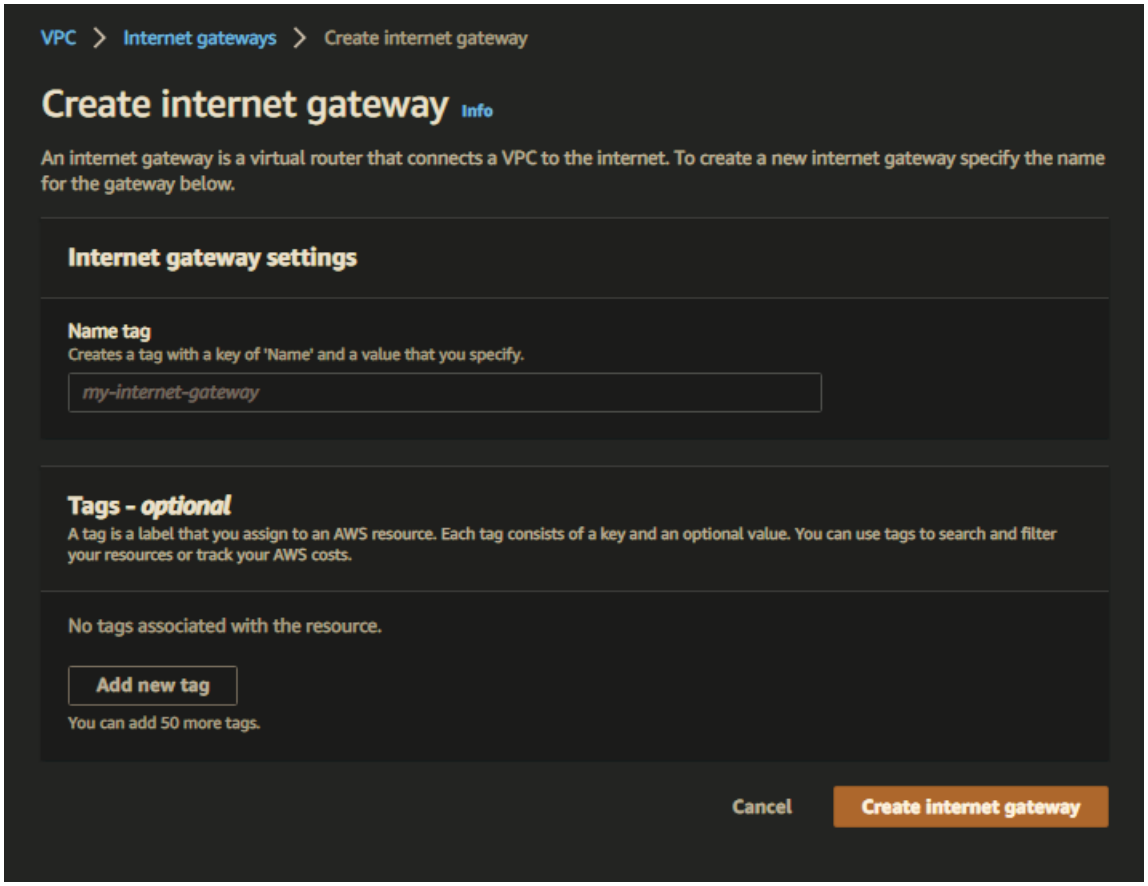
- Public



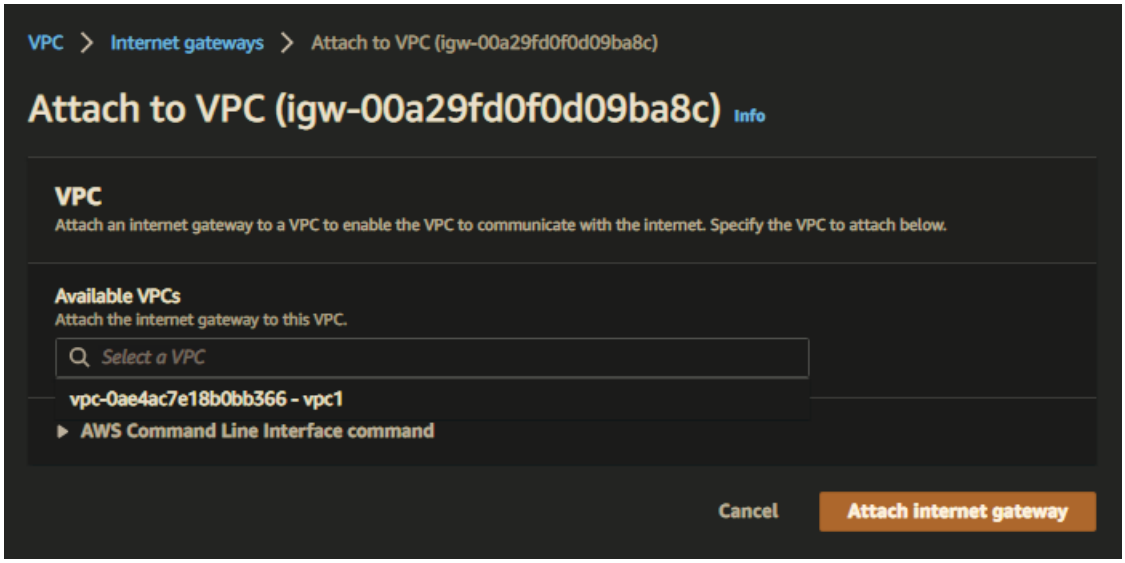
- Private


Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-0ae4ac7e18b0bb366 (vpc1)
Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
Private_subnet
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.
No preference
IPv4 CIDR block Info
10.0.1.0/24
Tags - optional
Key
Value - optional
Name
Private_subnet
Remove
Add new tag
You can add 49 more tags.
Remove
Add new subnet

Create Internet Gateway and attach it to the VPC you have created

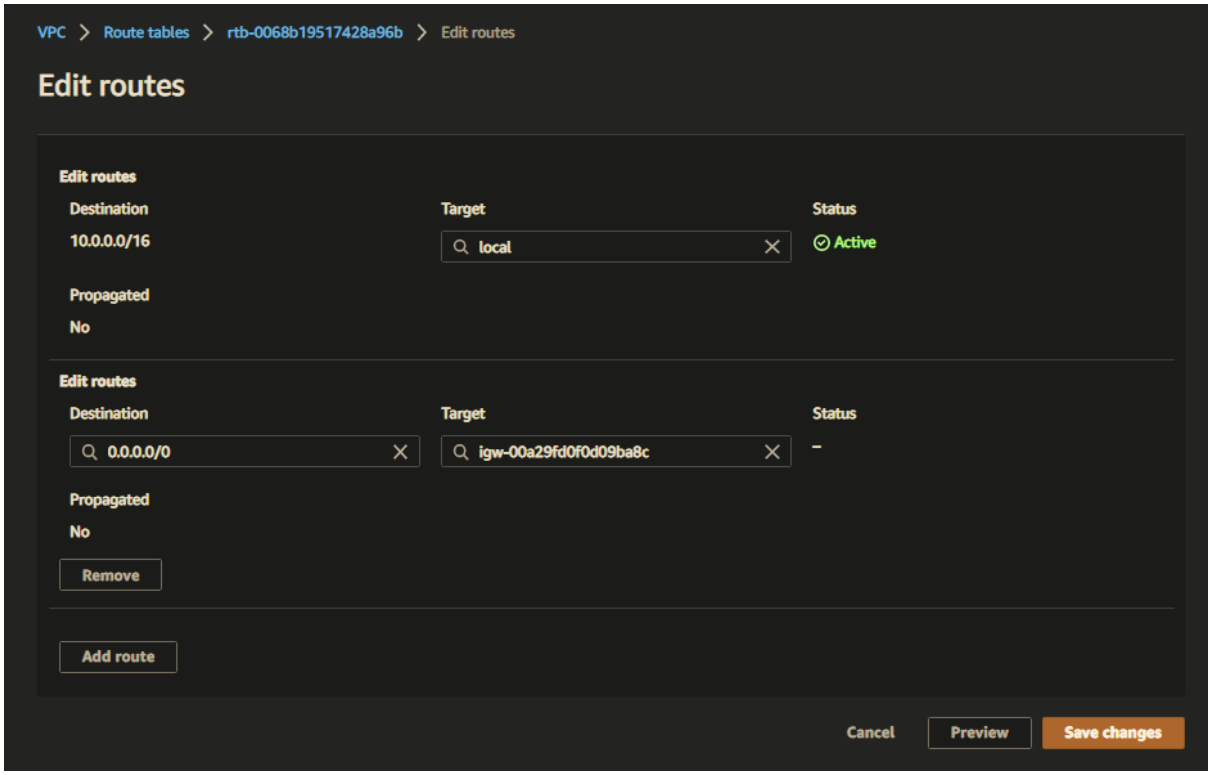


Select you Internet Gateway and click actions there you will find attach option, after clicking on it you can attach you IG to a VPC

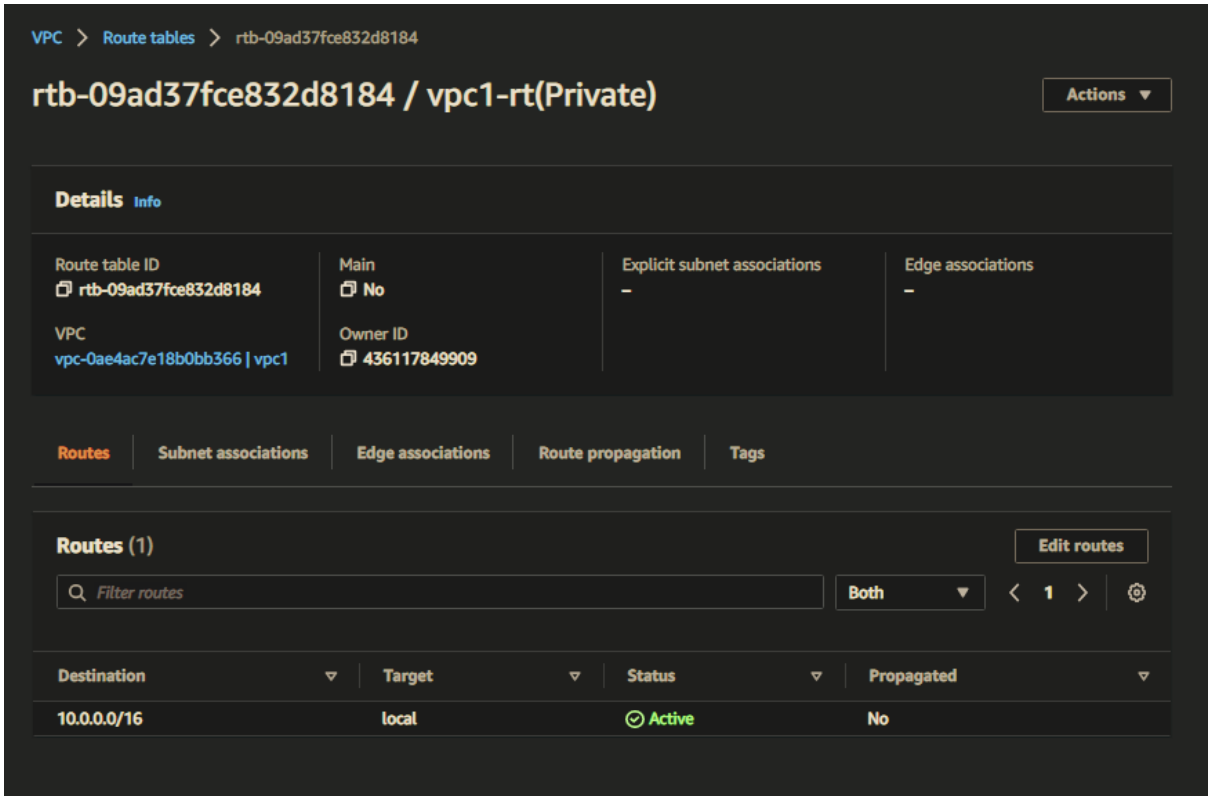


You can see here your IG is attached to the VPC you have created

Go to route table and add Internet gateway to your main route table:



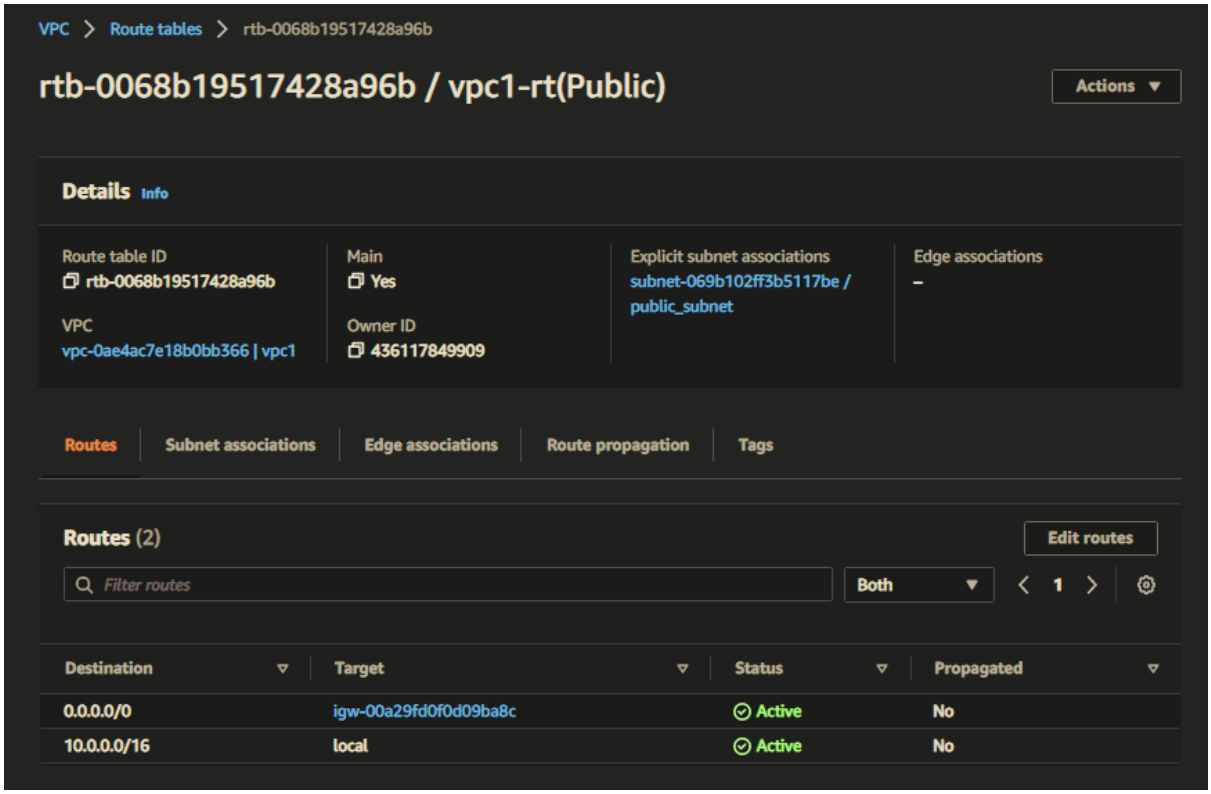
Create another Route table for the VPC with no IG attached to it



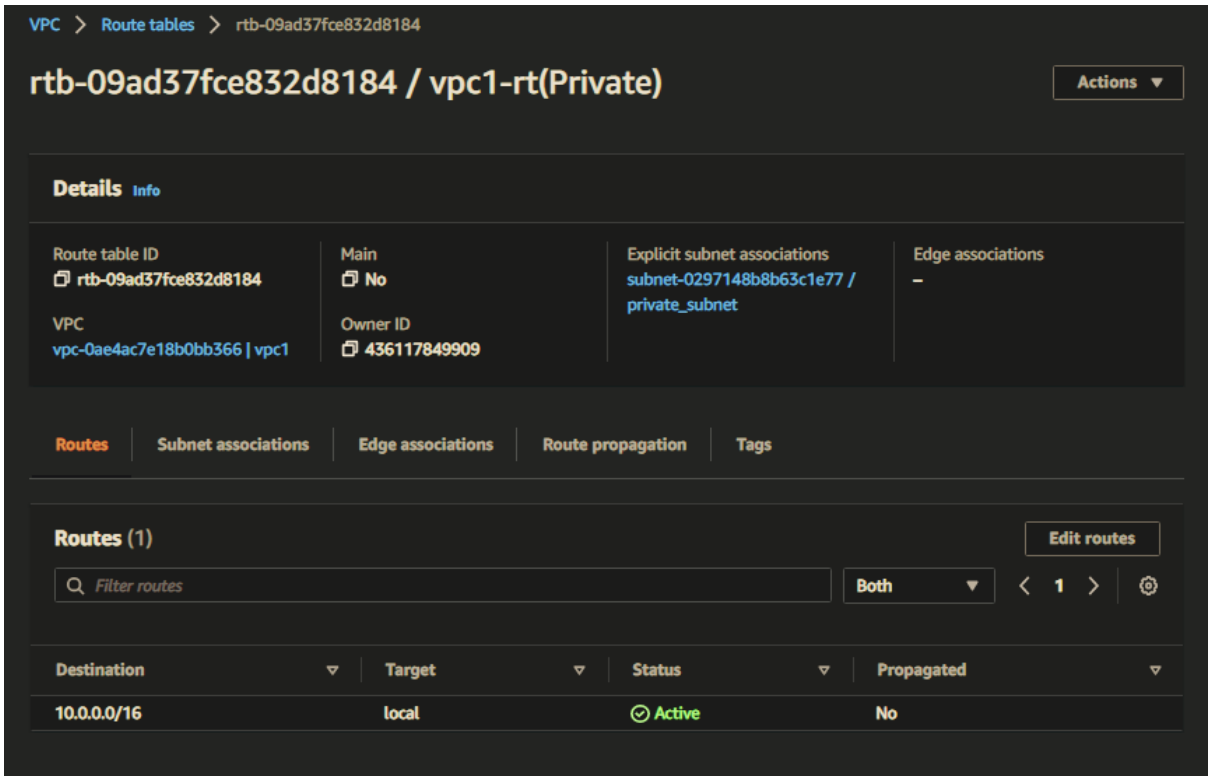
Associate Subnets to the route table by edit subnet association:

- Here public subnet will be attached to the route table with IG such that main route table of vpc1
- And private subnet to the route table with no IG association

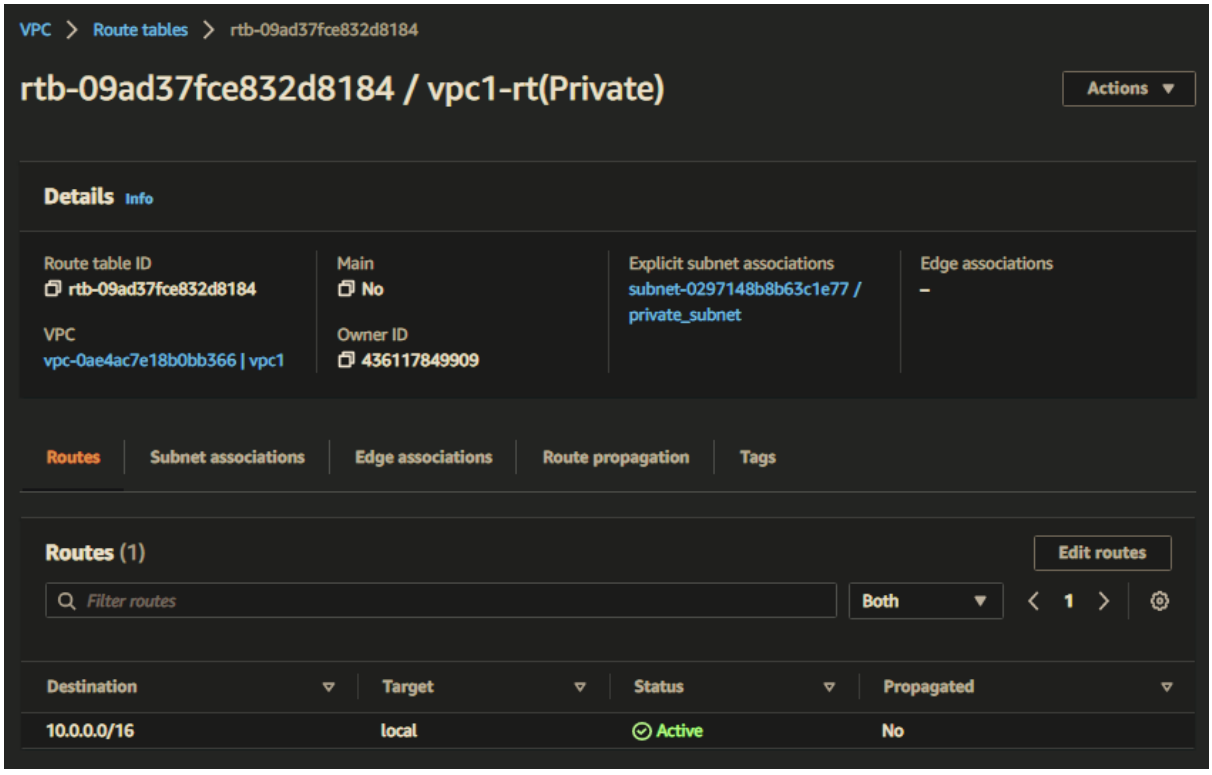
Below image shows the public subnet being associated to the route table with IG(click on the section of explicit subnet association to verify which subnet is attached to the route table)



Similarly attach the private subnet to the route table with no IG associated to it.

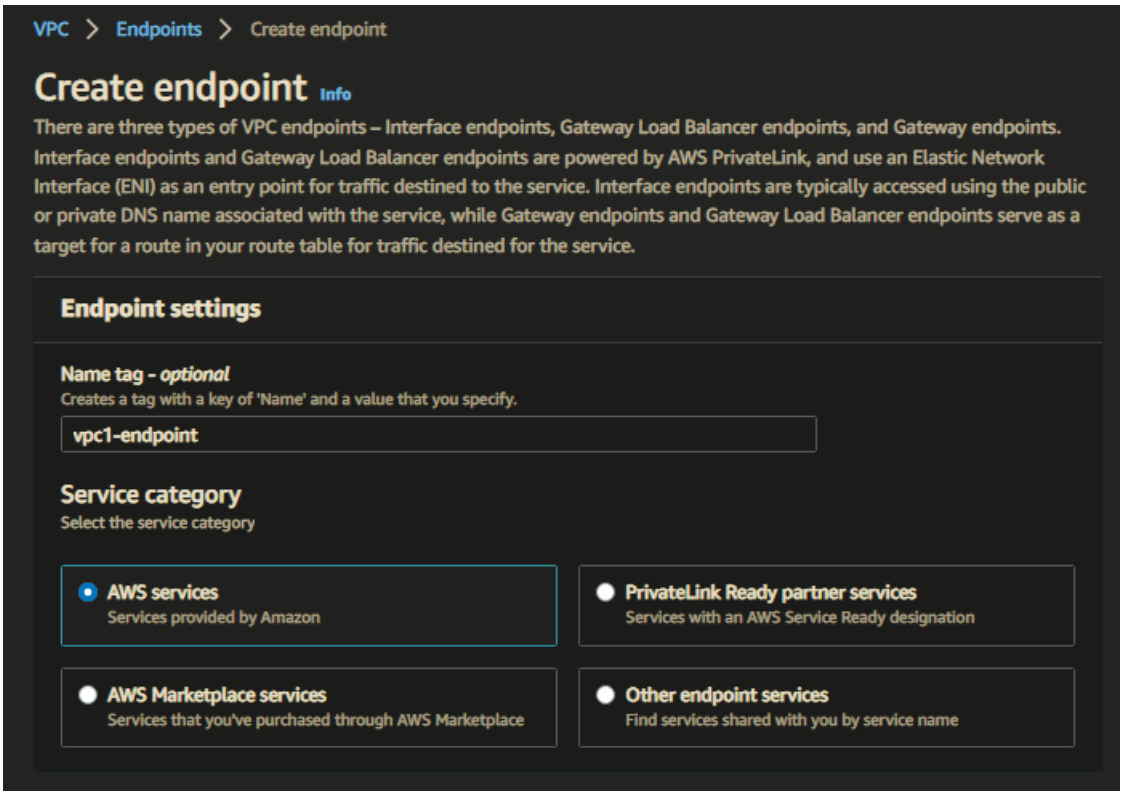


Below image shows your private subnet associated with the route table with no IG associated to it

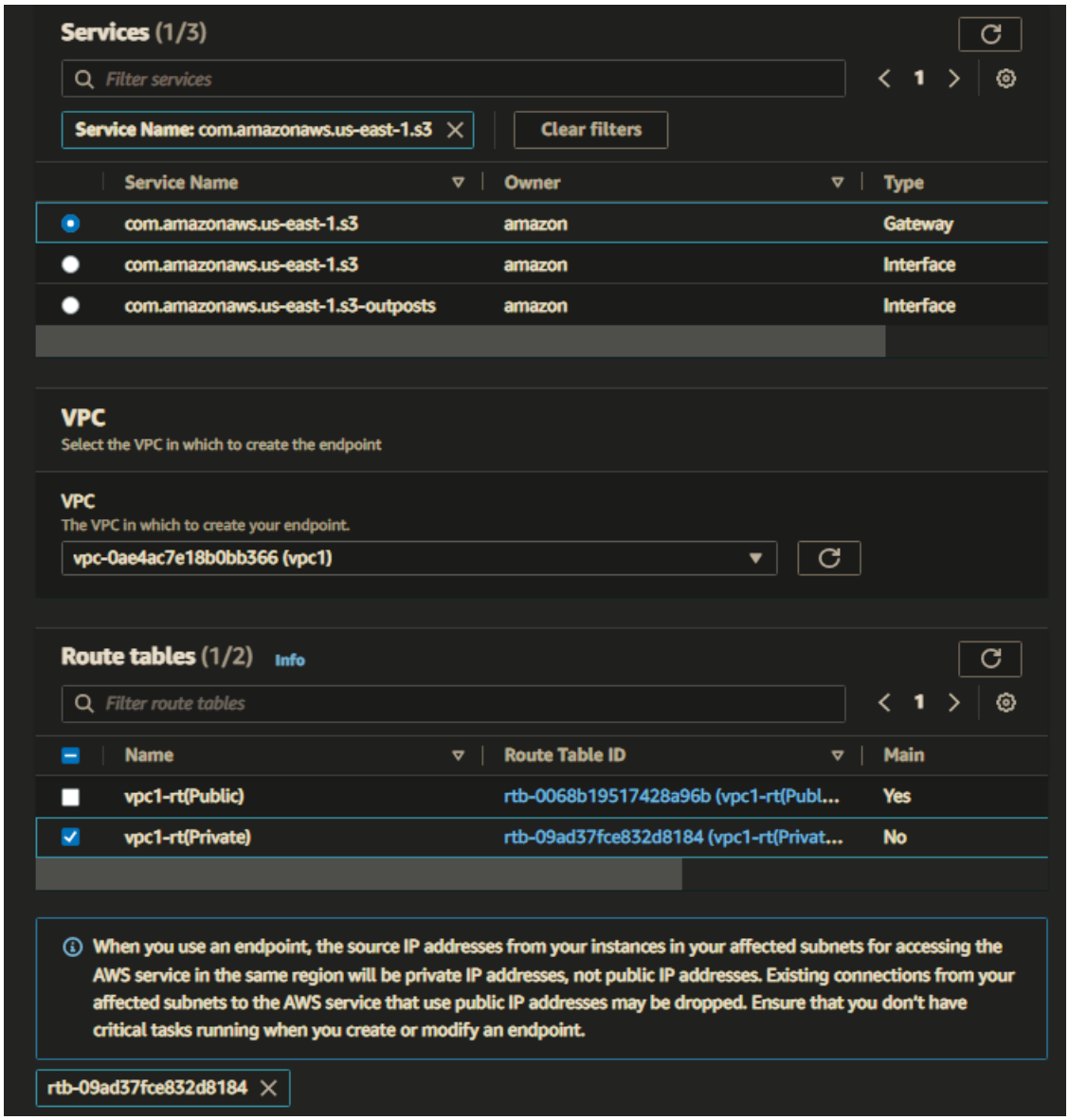


Create VPC Endpoint

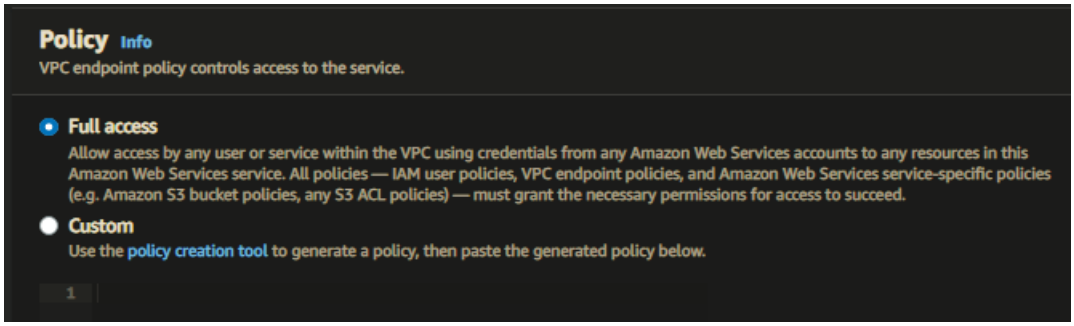
- Select the service category and name your endpoint Here we want to access our S3 service with the private subnet in the vpc1and S3 comes
- under AWS services category



- Select the service name and select endpoint gateway of S3 and select the route table with private subnet as we wanted to access our S3 service from the Private subnet

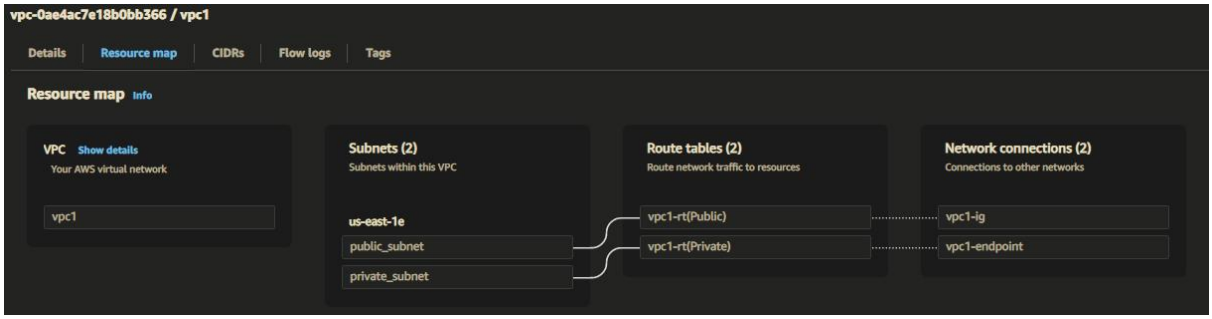


- you can make or select the default full access policy here we are selecting s3 full access policy and click on create VPC endpoint.



Check the resource map you will see the routes you have created

- Below you can see how you have associated your public subnet to the IG and private subnet with no IG

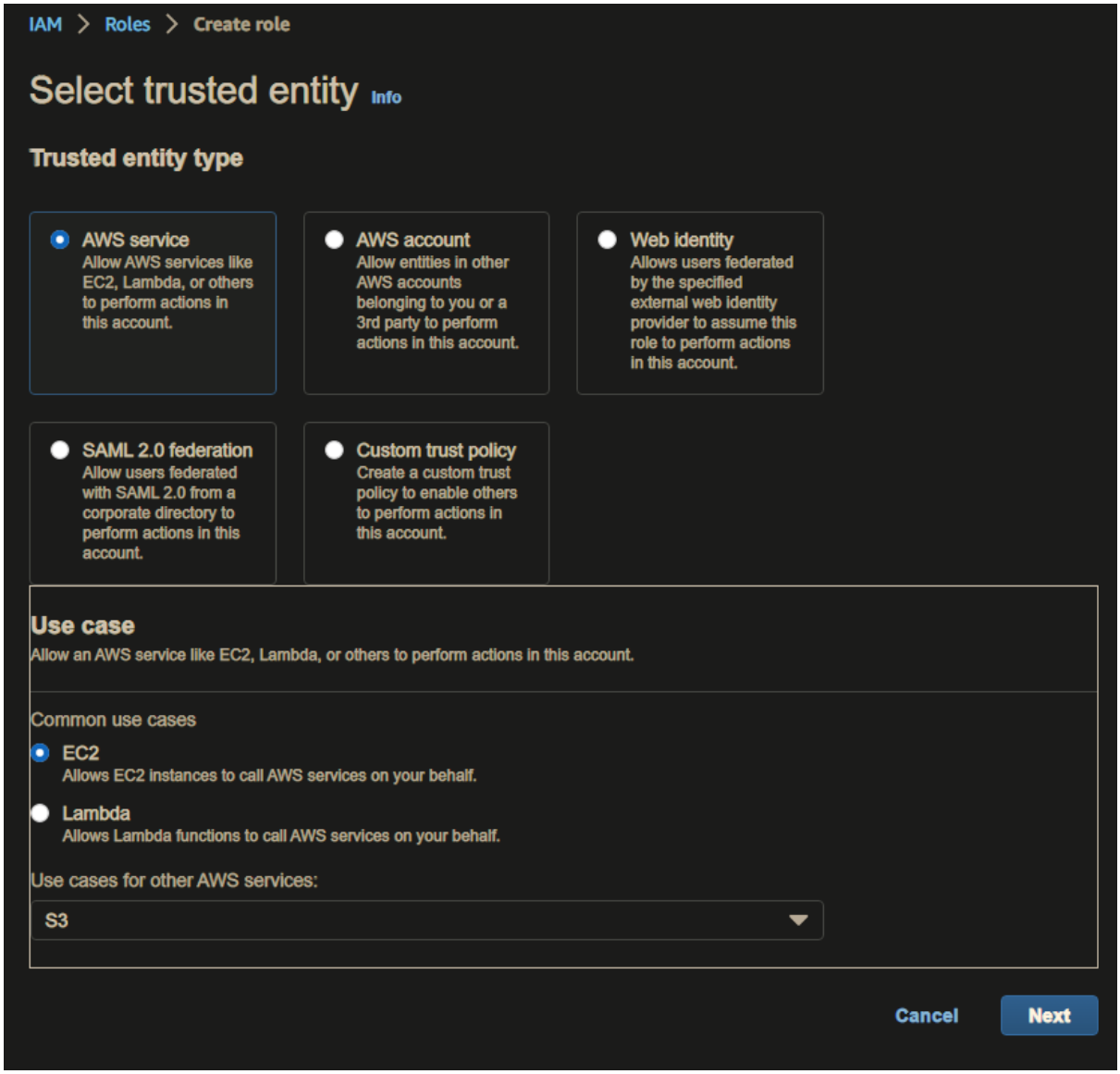


Create Linux EC2 instance(machine) in the public and private subnets

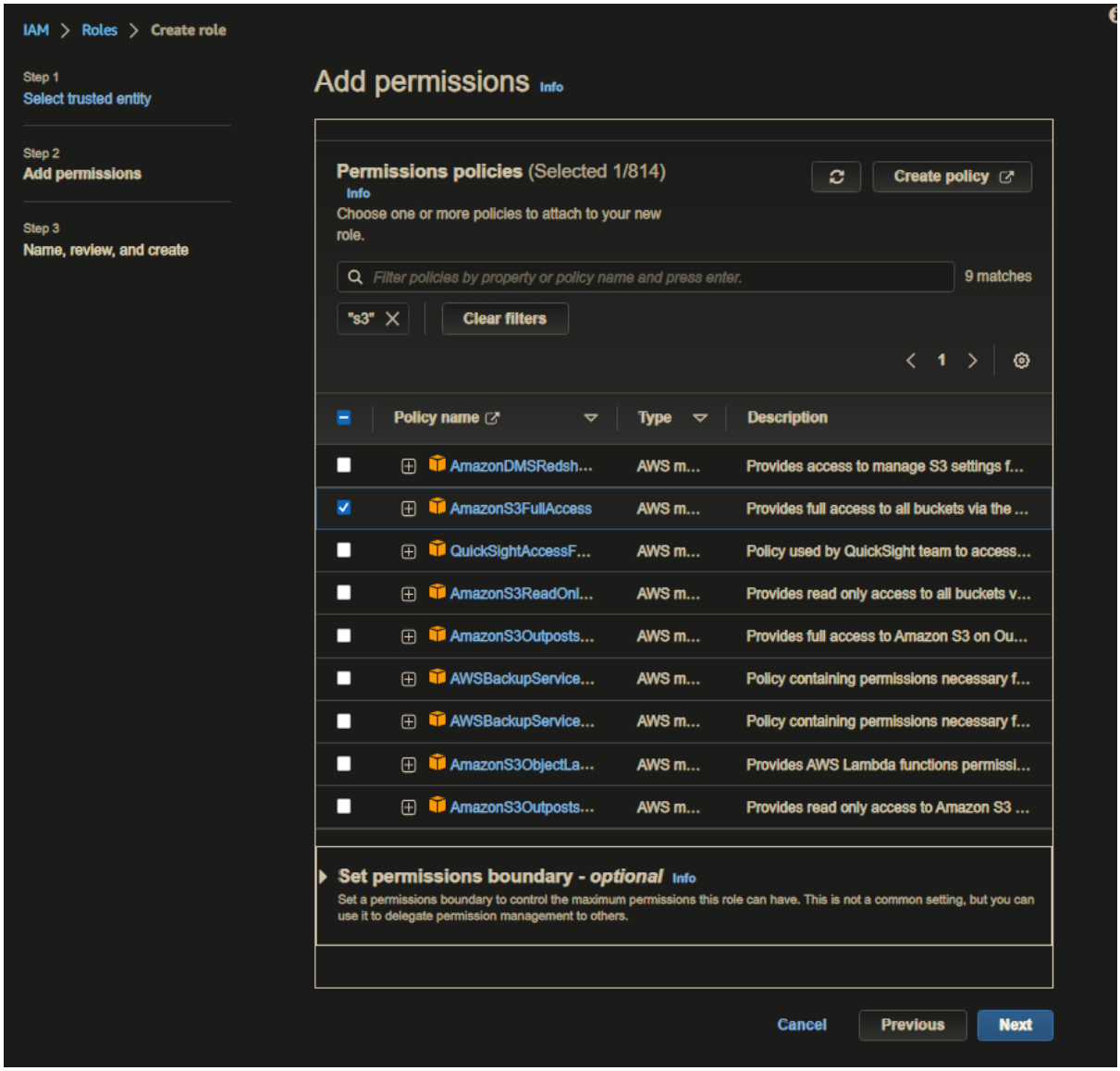
- Edit network settings while creating EC2 instances, select public subnet and enable auto-assign public IP to make ec2 publicly accessible and select private subnet for private ec2 and disable auto-assign public IP. Create common security group vpc1-sg for both instances

Create an IAM role for S3 access:

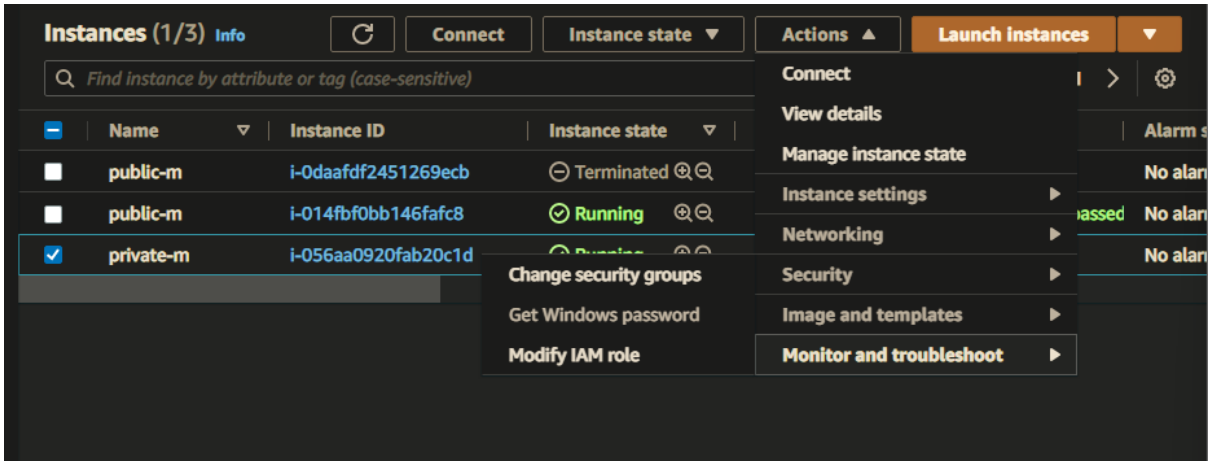
Go to IAM service console and select roles and then select create IAM roles and in Use case select EC2 instances and select S3 in use cases for other AWS services.



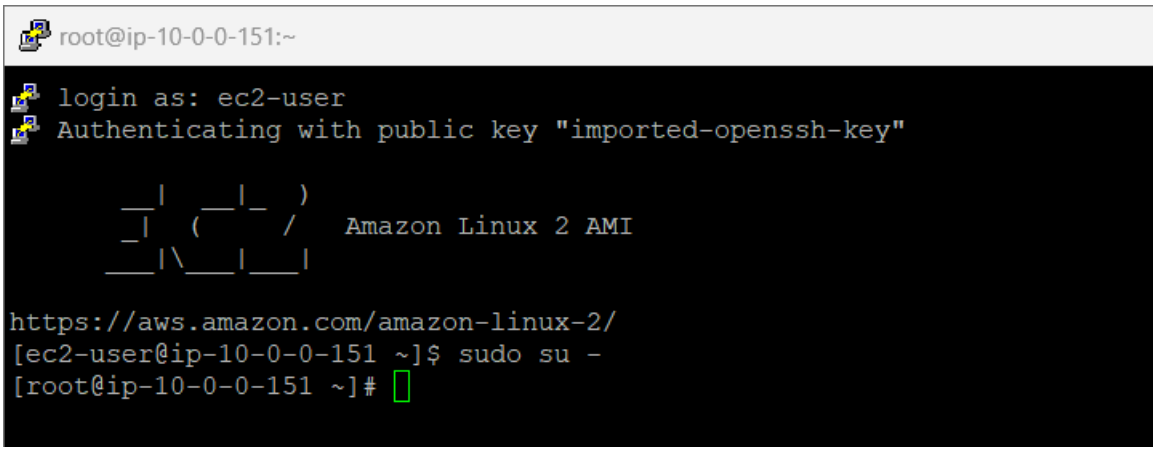
Select the S3 full Access in the add permissions and click next there in Role details make your role name and create role



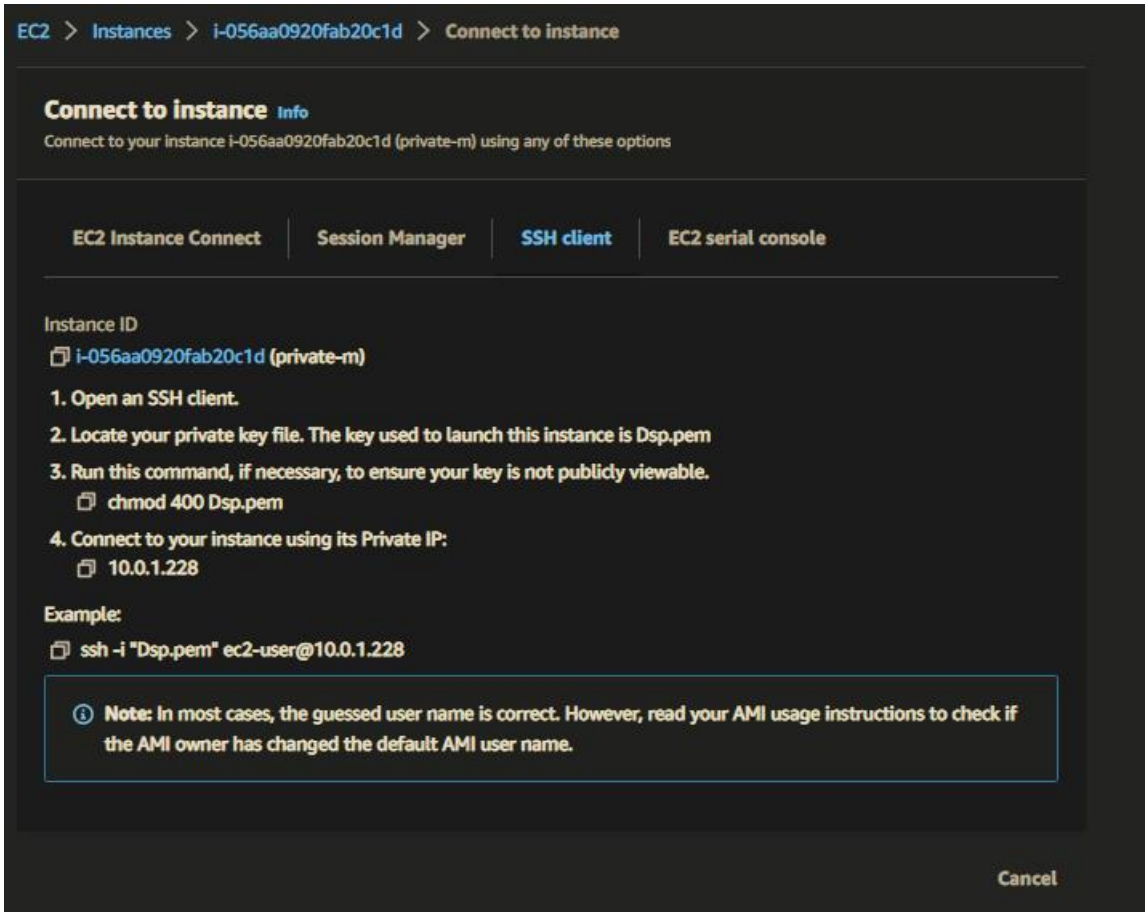
Modify IAM role for the Private Instance:



- Open Public instance using putty and enter sudo su – command to switch to root user

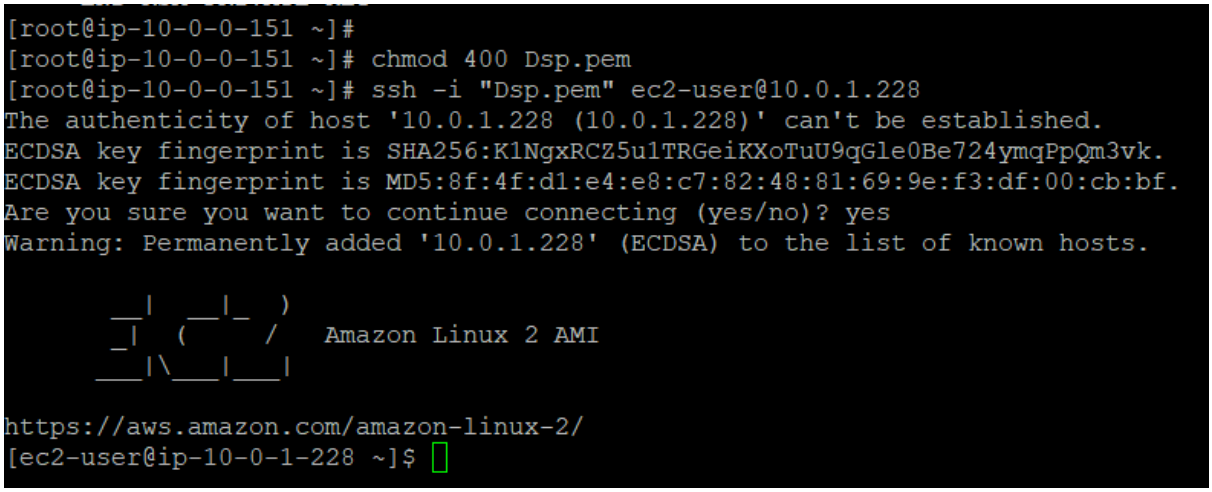


- Now you have to access your private subnet from the public subnet for that go to private Ec2 instance we have created and click on connect and then click on SSH client, you will see the following procedure there



Execute following in your linux CLI :

- vi Dsp.pem
- open your .pem file of your key assigned to the instance in Notepad and copy the key
- In CLI press I you will enter into insert mode and now paste the copied key.
- Now copy the commands from the connect to instance ,as shown in the image above
- After successful connection you will see the following



- Type “sudo su –“ command and switch to root user
- Now you can access you S3 and upload or download files from the S3 using private subnet or say private instance with use of VPC endpoint Gateway
- Create dummy files using “touch file1” command

```
[root@ip-10-0-1-228 ~]# touch file1
[root@ip-10-0-1-228 ~]# touch file2
```

- Type “aws s3 ls” command this will show you the list of buckets you have in your S3.below you can see I have dsp2 bucket in my S3

```
[root@ip-10-0-1-228 ~]# aws s3 ls
2023-02-19 14:34:06 dsp2
```

- Type “aws s3 cp /root/file1 s3://dsp2” command it will copy the file1 and upload it to the S3 bucket dsp2.

```
[root@ip-10-0-1-228 ~]# aws s3 cp /root/file1 s3://dsp2
upload: ./file1 to s3://dsp2/file1
```

- Now go to your S3 bucket and check for the file1, you would see you file being uploaded to the bucket dsp2