VPC\_Endpoints: -

**Problem Statement:**

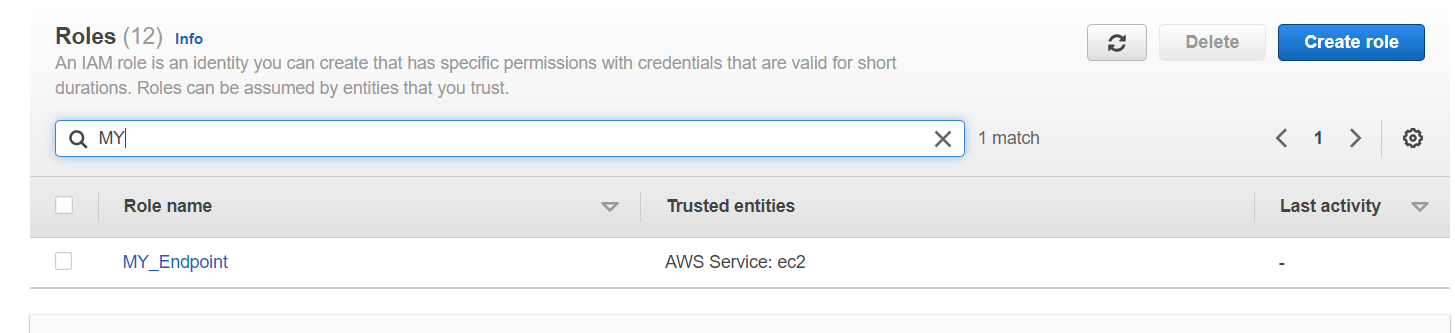
Working for an organization, you are required to provide them a safe and secure environment for the deployment of their resources. They might require different types of connectivity.

Implement the following to fulfill the requirements of the company. Tasks To Be Performed:

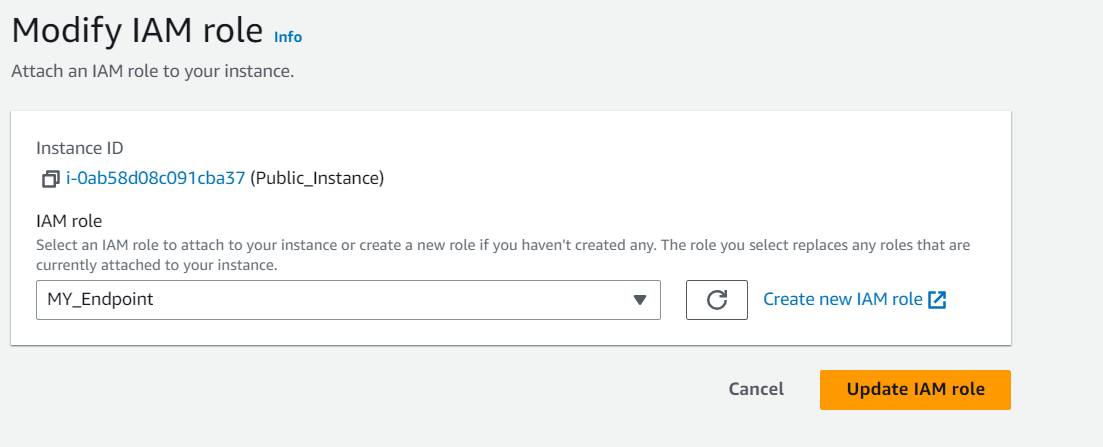
1. Create a VPC endpoint for a S3 bucket of your choice for secure access to the files.

**Procedure**: -

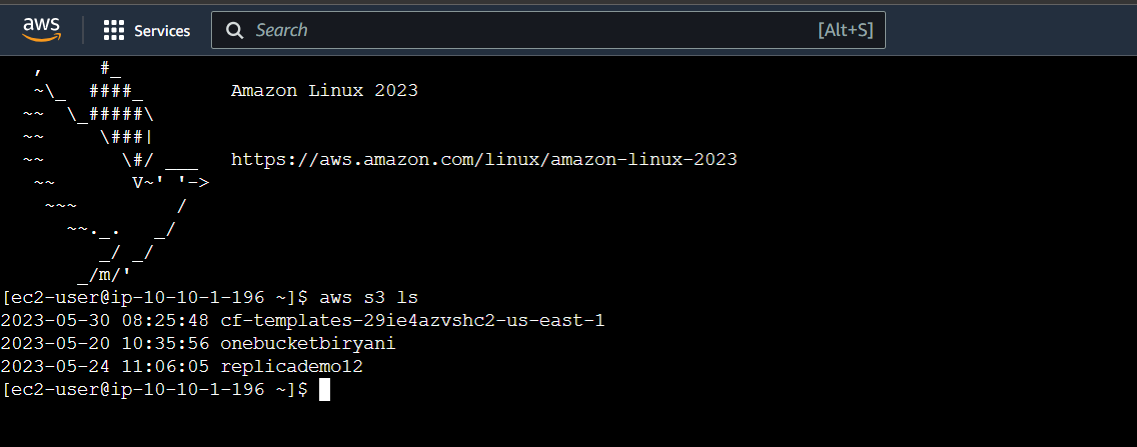
* Create the VPC and a public instance and the private instance.
* Search for Iam and Click on role and create role, select the AWS service, and select the EC2.
* Search for s3 and select the s3. In the permission policies search for s3 and choose the option as AmazonS3FullAccess. Click on next and give the name for the role and click on create role. Therefore, the role is created.



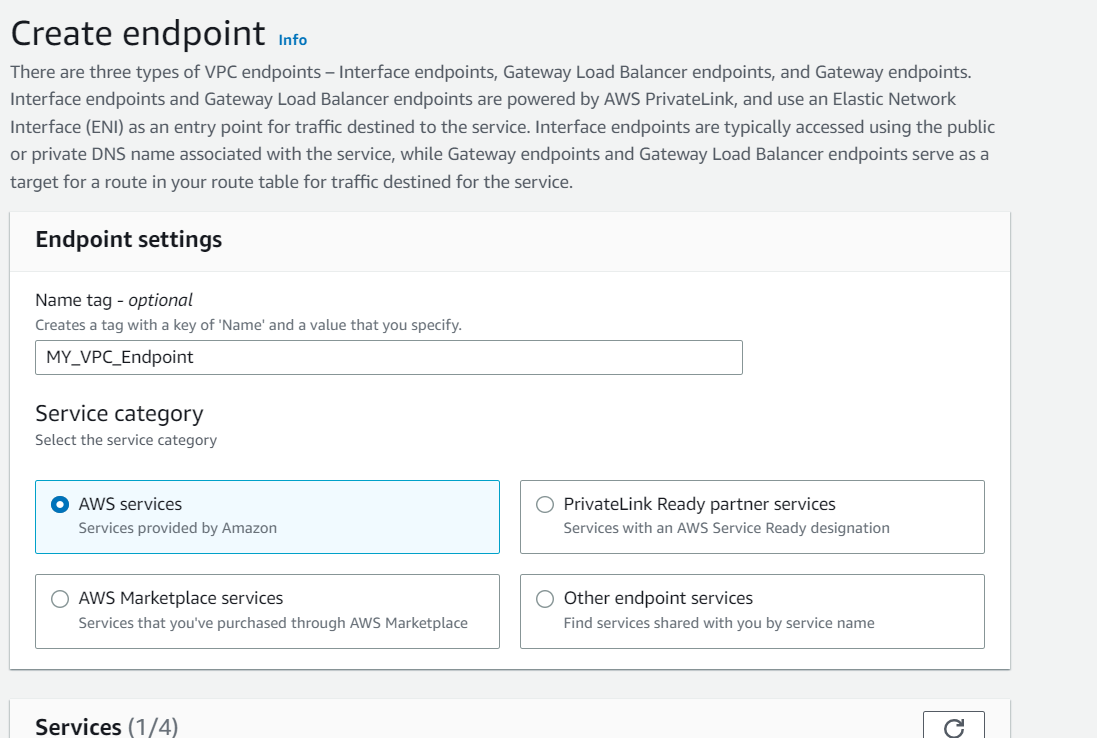
* Now select the Public\_Instance and click on actions>>security>>Modify Iam role.
* Choose the IAM role as MY\_Endpoint and Update IAM role.



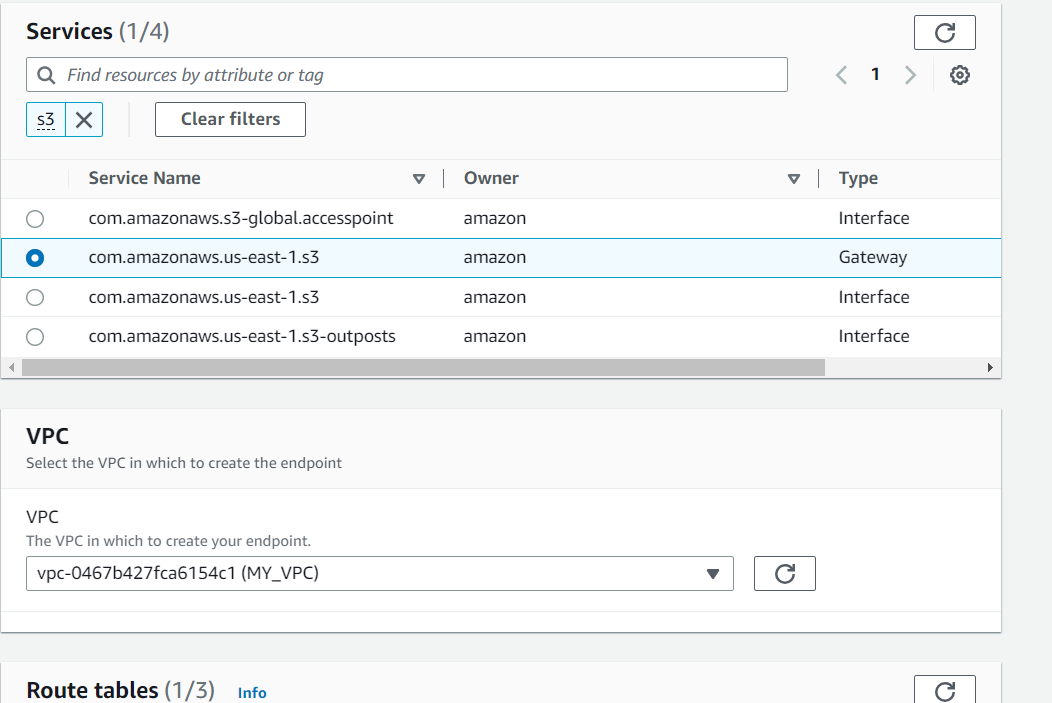
* Connect the Public instance and open the command prompt.
* Run the following command.
* aws s3 ls
* You will see that you are able to access the s3. Your will see the list of s3 buckets created.

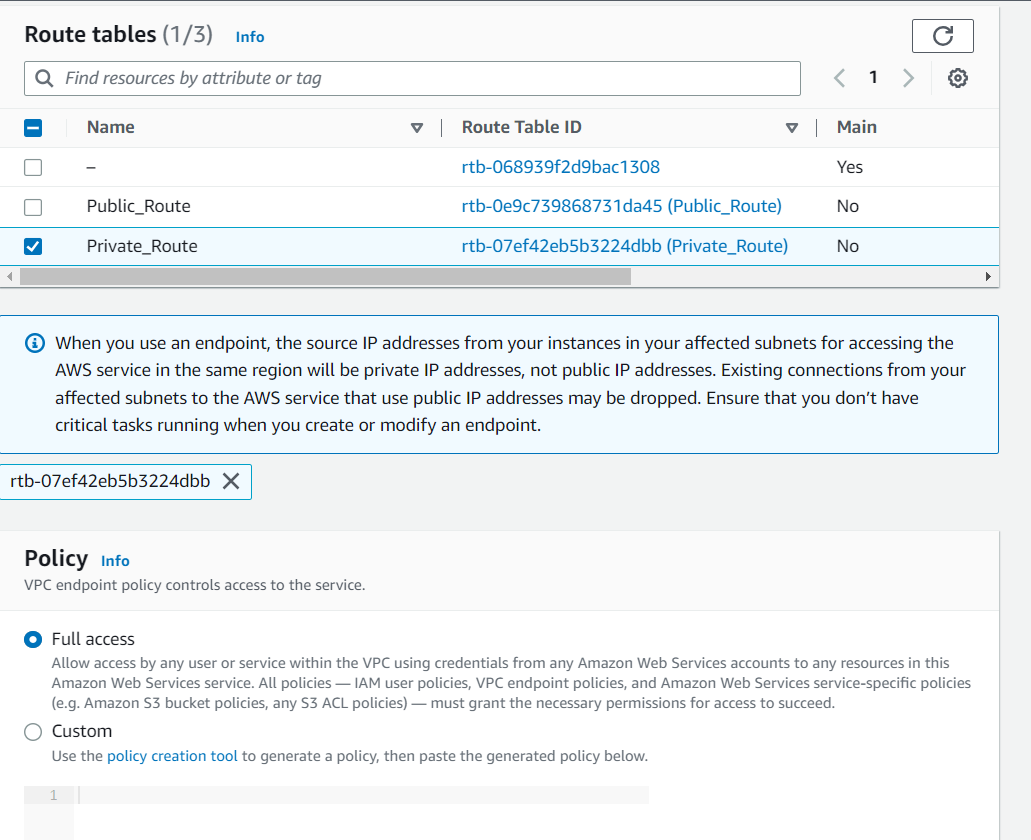


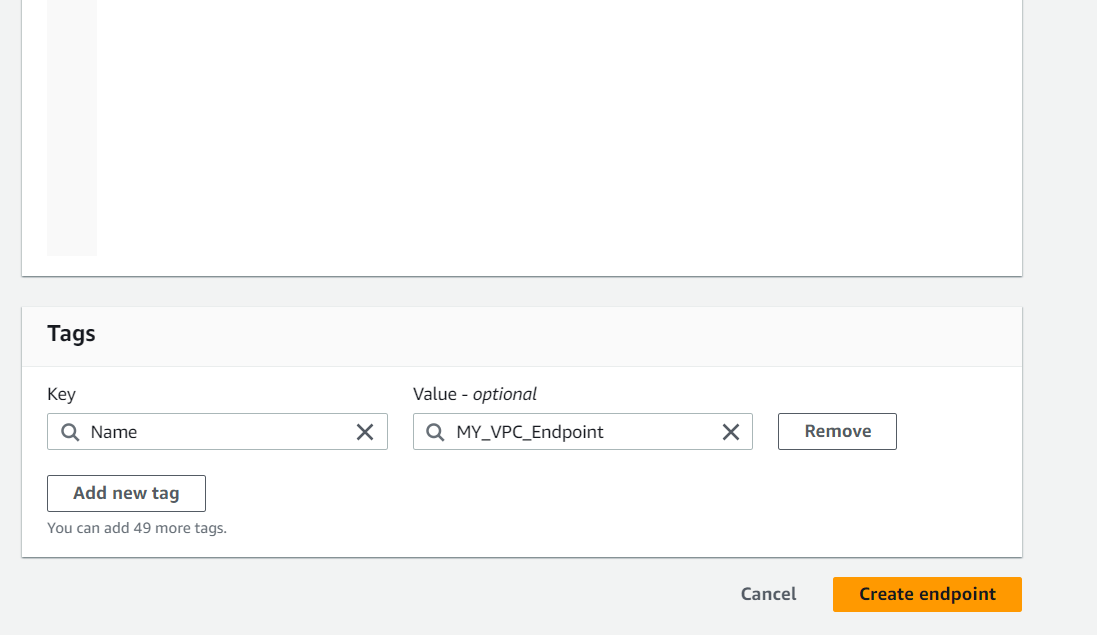
* **Conclusion:** We can access the public instance with **IAM Role.** No Endpont is needed.
* Now we will try to access the s3 bucket with the private instance. For this we need two things.
* IAM Role
* VPC endpoint
* Therefore, we need to create the endpoint. Goto VPC>>Endpoint>>create Endpoint.



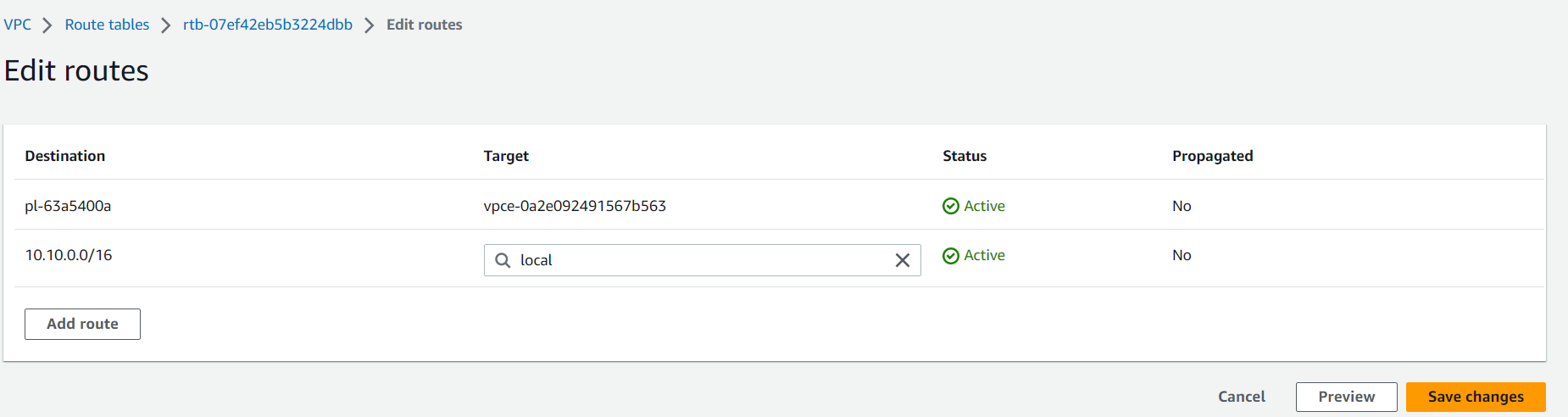
* Simply create on endpoint.

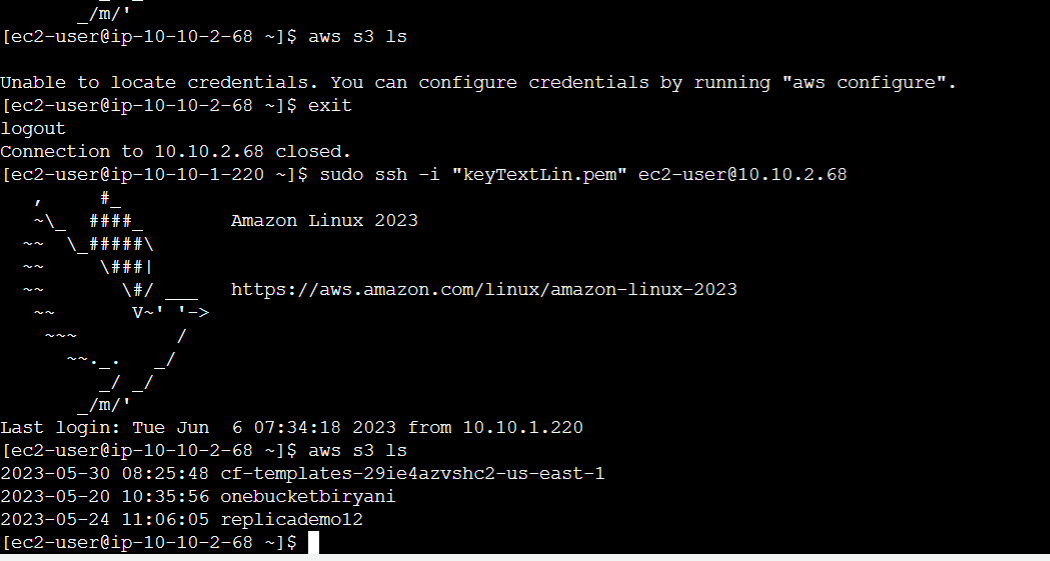


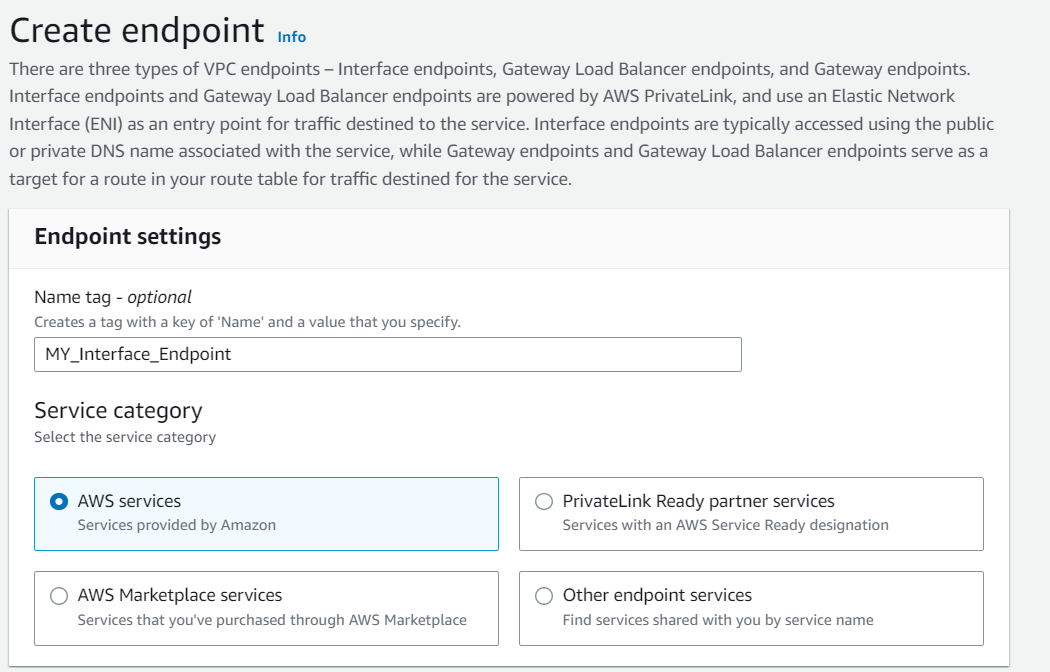


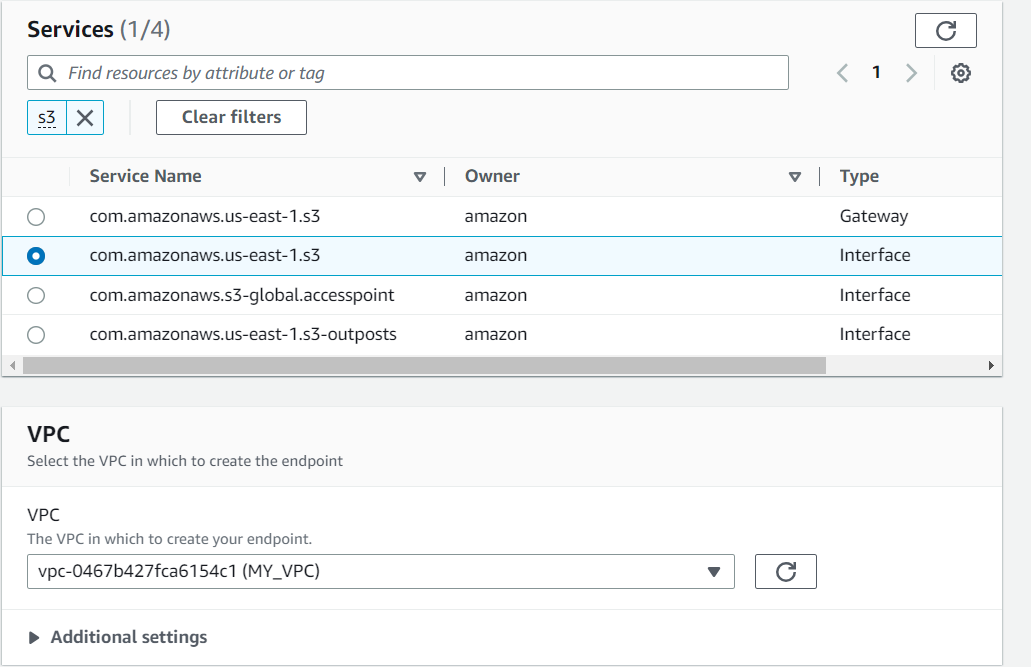


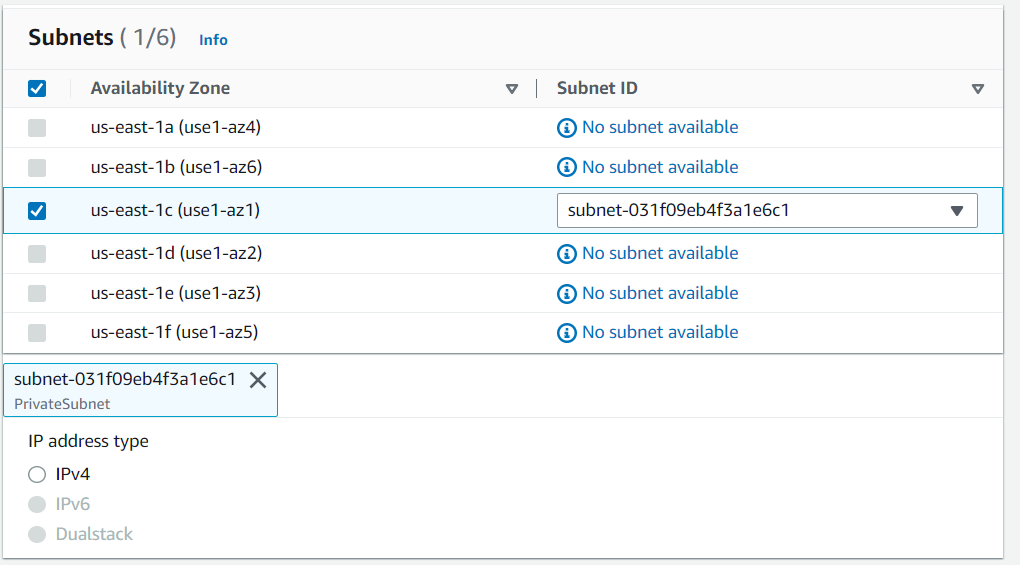
* Now if we go to Route tables>>Private\_Route>>Routes>>edit routes.
* You will see the the MY\_VPC\_Endpoint will automatically appear.

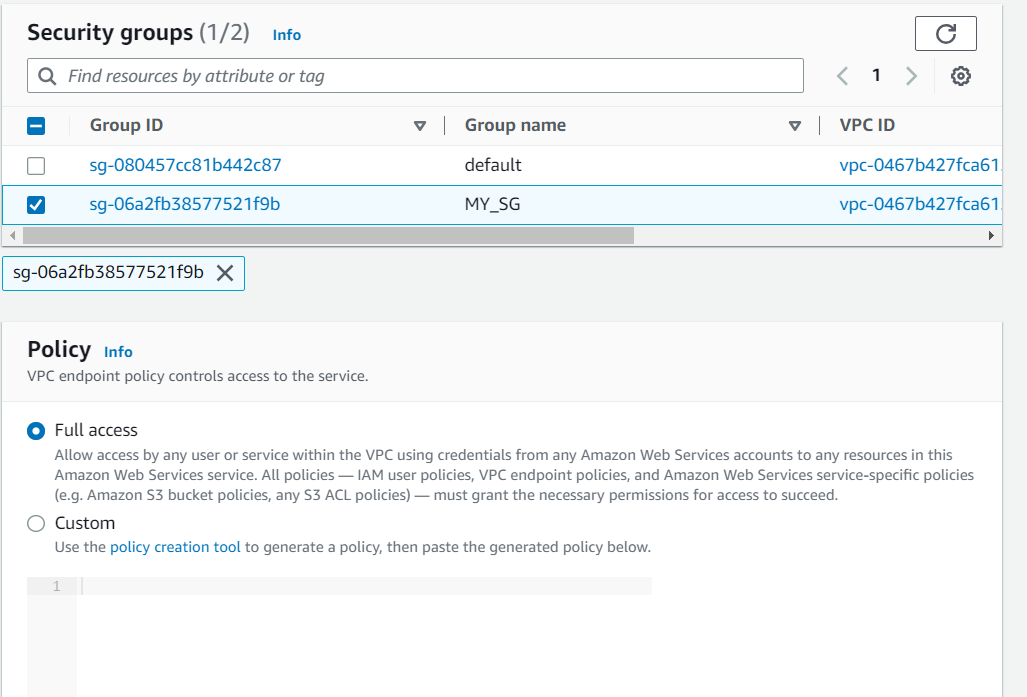


* When we create the endpoint the route table automatically targets the vpc endpoint.
* Now let us access the private instance from the public instance.
* sudo nano keyTextLin.pem (create a pem file).
* ls (to check the file)
* sudo chmod 400 keyTextLin.pem
* sudo ssh -i "keyTextLin.pem" [ec2-user@10.10.2.68](mailto:ec2-user@10.10.2.68)
* Goto Private\_Instance>>actions>>security>>Modify IAM role. Select the MY\_Endpoint and update IAM role.
* Now on the command prompt logout and login the private\_instance.
* exit
* sudo ssh -i "keyTextLin.pem" [ec2-user@10.10.2.68](mailto:ec2-user@10.10.2.68)
* aws s3 ls
* Now you will see that you will be able to access the s3 bucket through private\_Instance with the help of **IAM role and VPC Endpoint.**
* The above example was for **Gateway endpoints**
* Now we will performe for the **interface endpoints.**
* Let us create the new endpoint. Gotto Endpoint>>create endpoint.

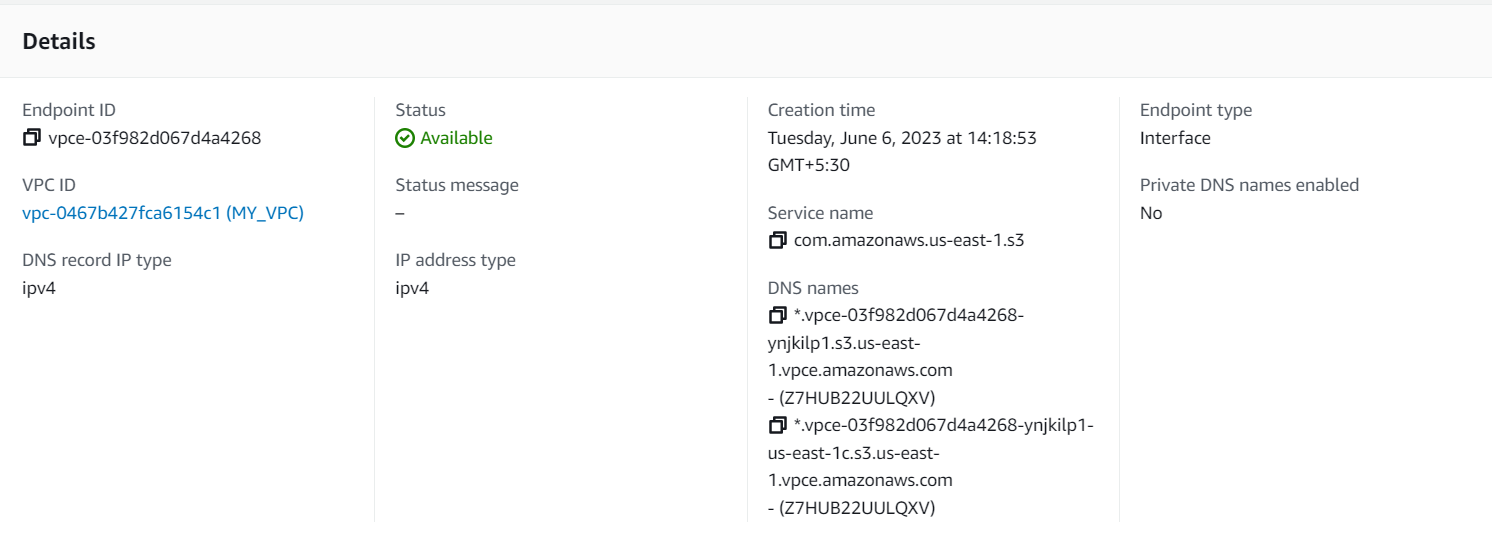








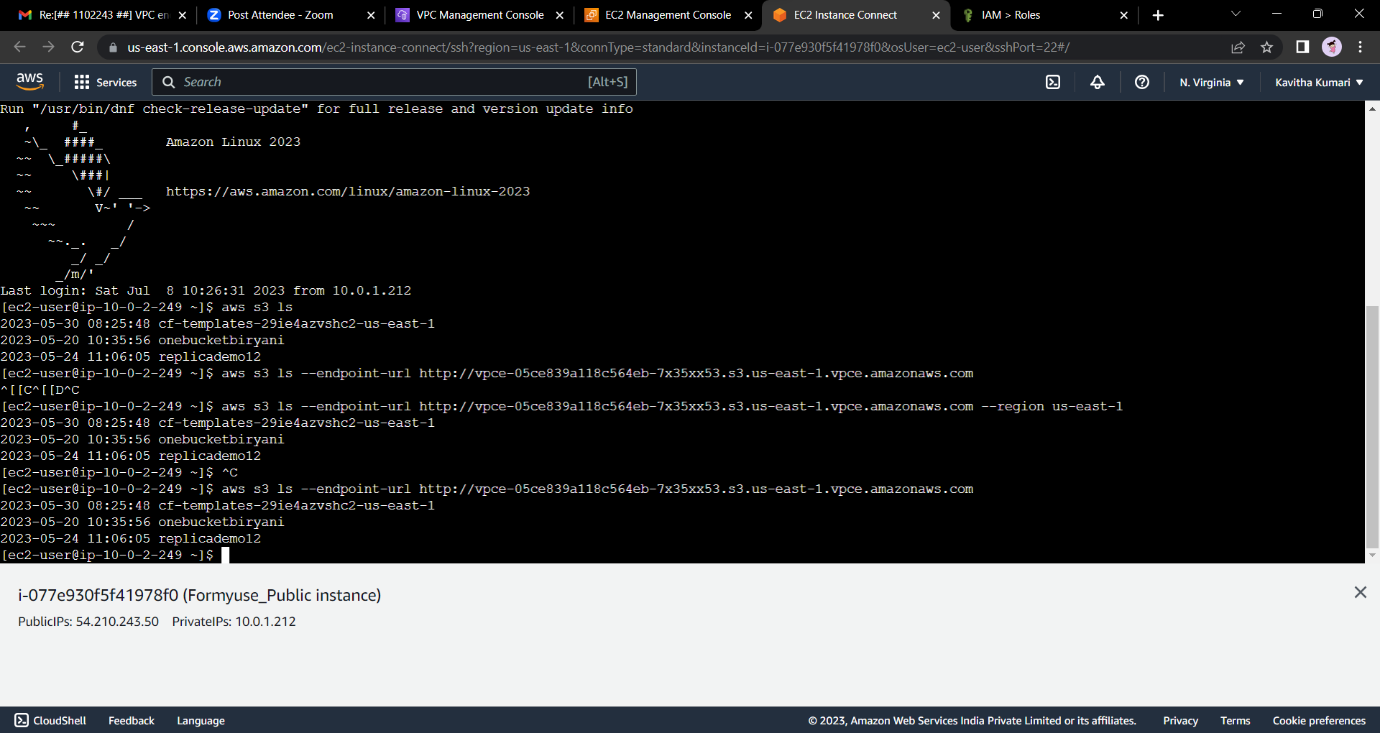
* Click on create end point.
* Logout and login from the private machine.
* Now we should be able to access the s3 bucket using the dns.
* Run the following command
* aws s3 ls --endpoint-url http://vpce-03f982d067d4a4268-ynjkilp1.s3.us-east-1.vpce.amazonaws.com



* aws s3 ls --endpoint-url http://vpce-03f982d067d4a4268-ynjkilp1-us-east-1c.s3.us-east-1.vpce.amazonaws.com



**Important note:** WE also need to provide the http rule in the private instance because we are accessing the s3 bucket through the Private instance.



--------End---------