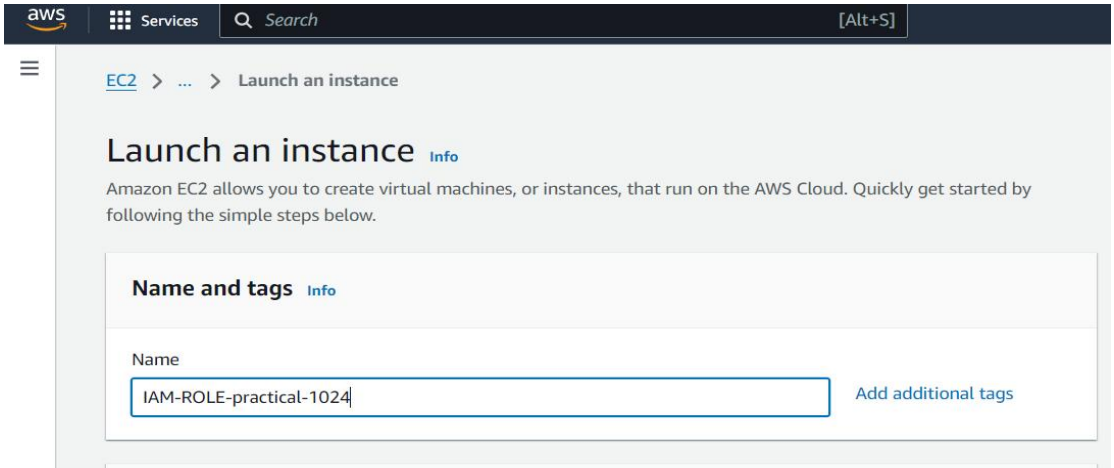
Name of the Student: **Shrushti Krishna Shrivastav** **PRN: 20220801024**

Title of Practicle : Access S3 bucket through EC2 using IAM role

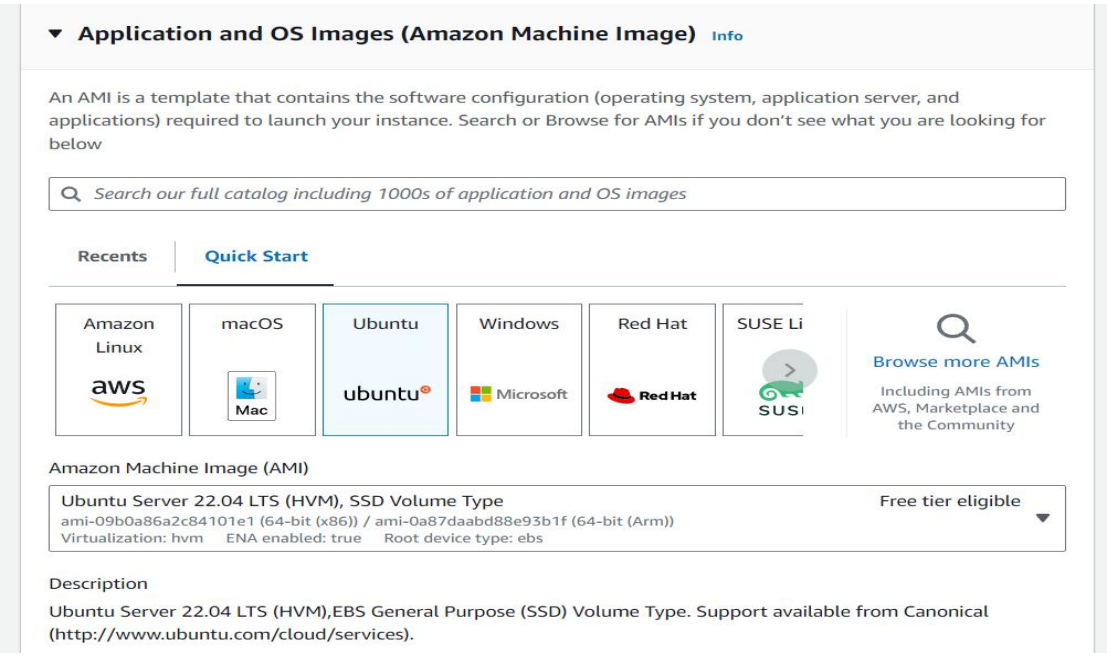
STEP1: LOG IN AND create one ec2 instance

Go to EC2 service and launch one instance

Name--(IAM-ROLE-practical-1024)

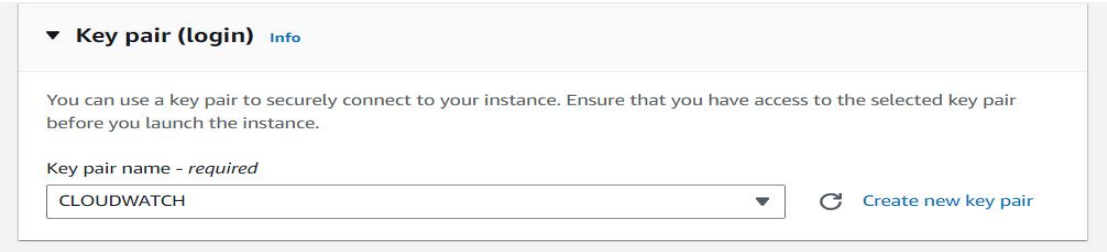


AMI---ubuntu linux

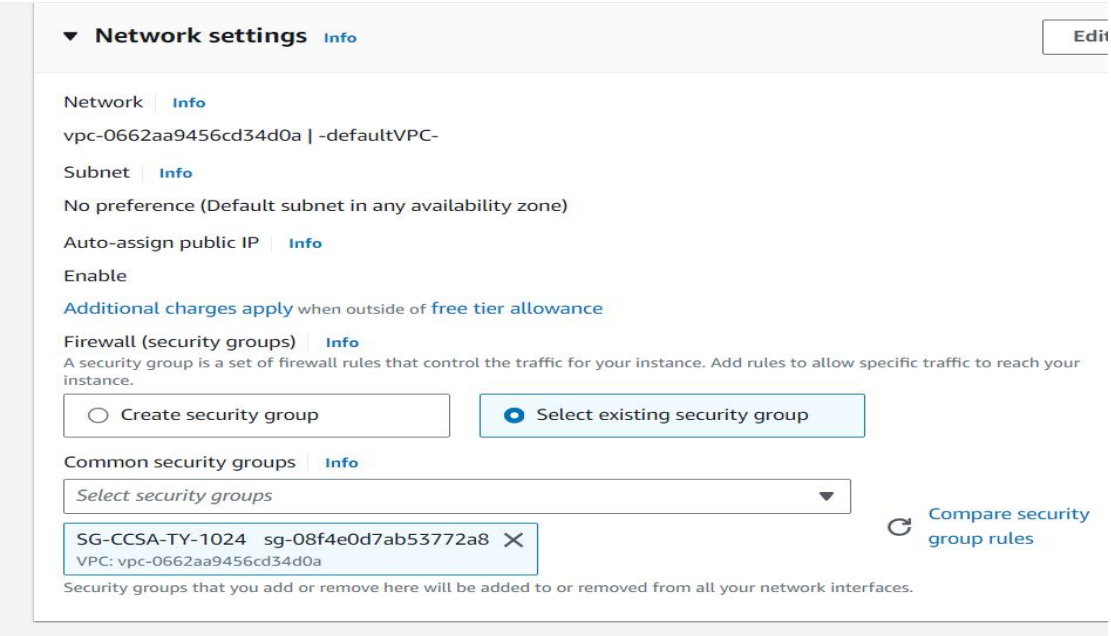


Instance type--- t2.micro

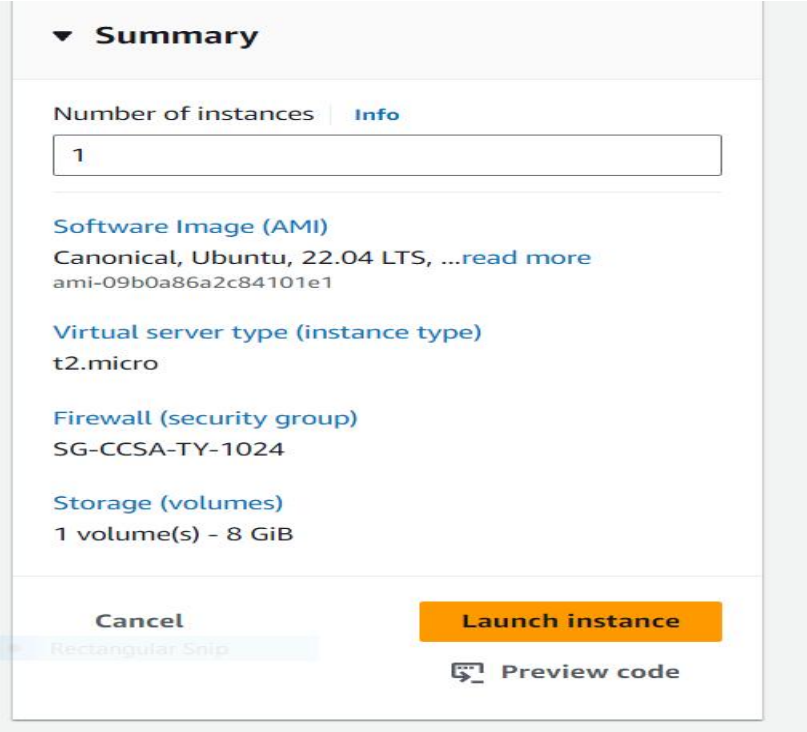
Attach keypair or create new one.



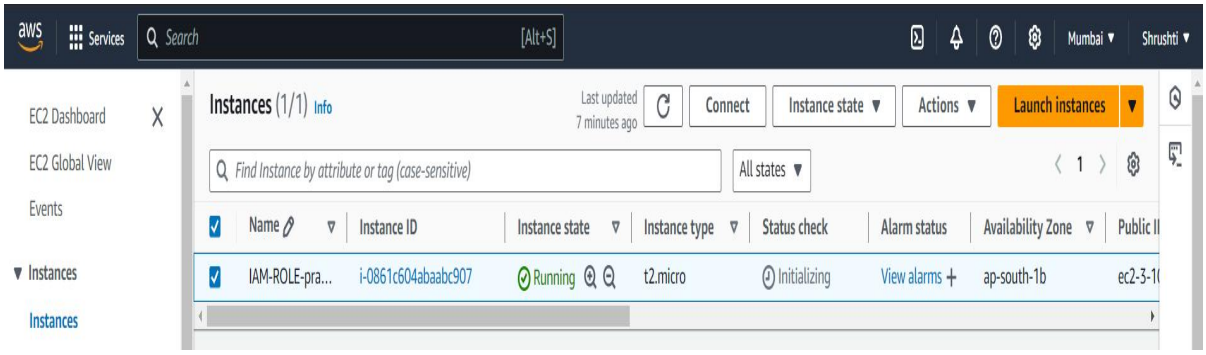
Attach or create new security group(allow ssh and http)



Launch instance

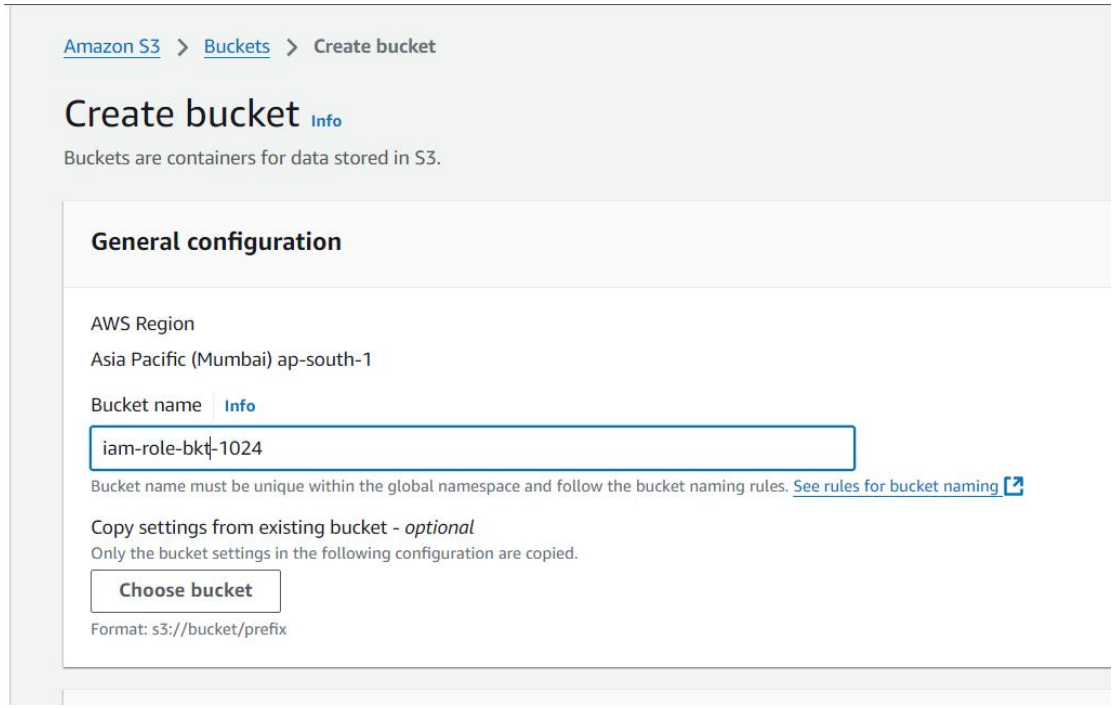


Our instance is created

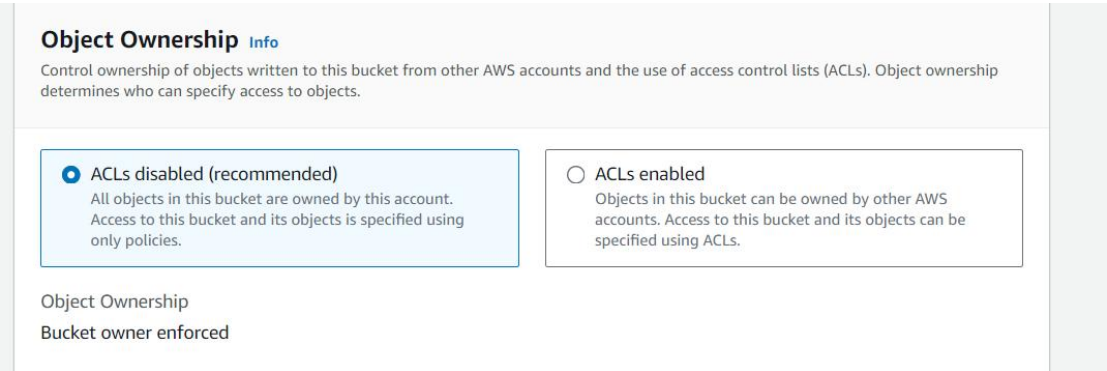


STEP2: Now create one s3 bucket--

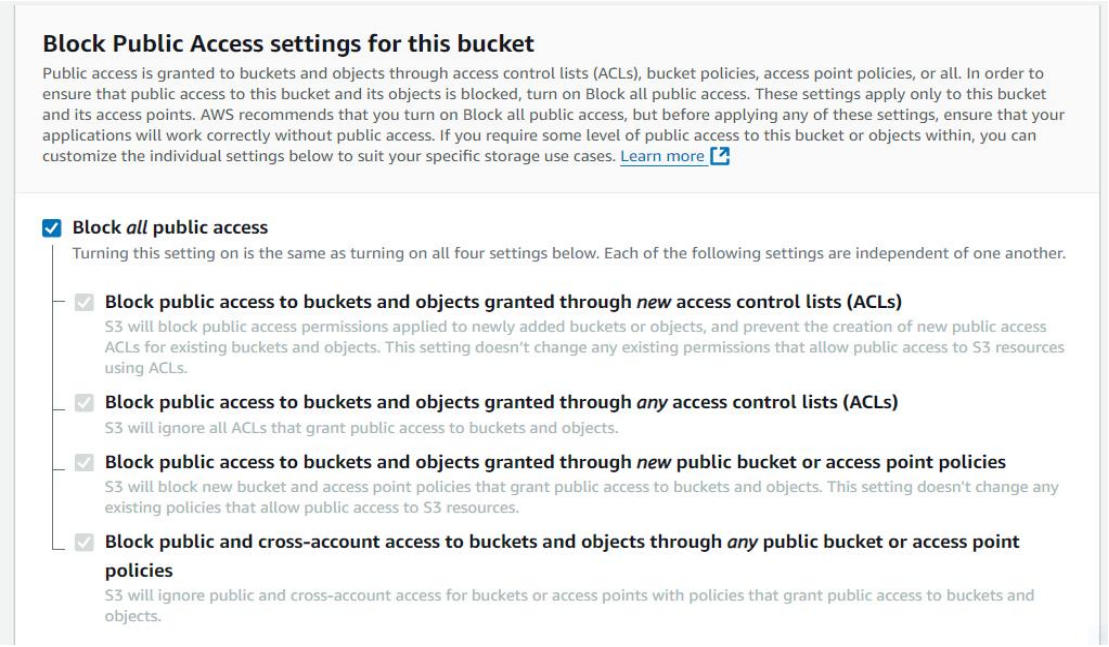
Name--iam-role-bkt-1024



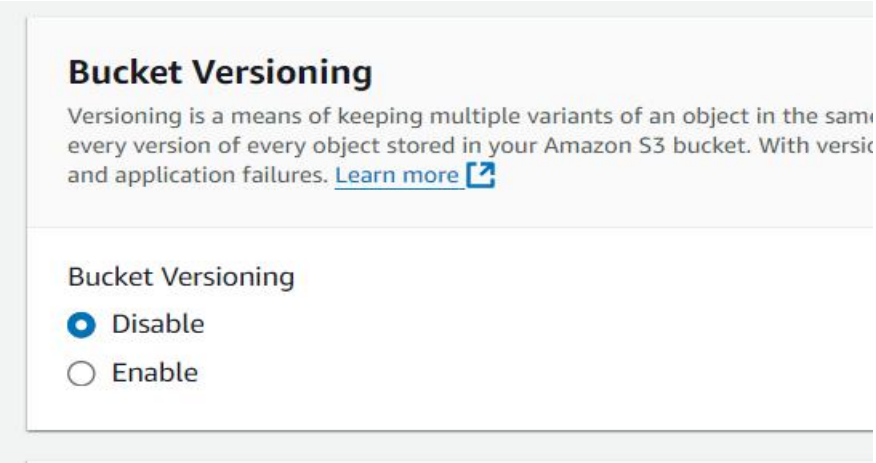
Ownership--- ACLs disabled



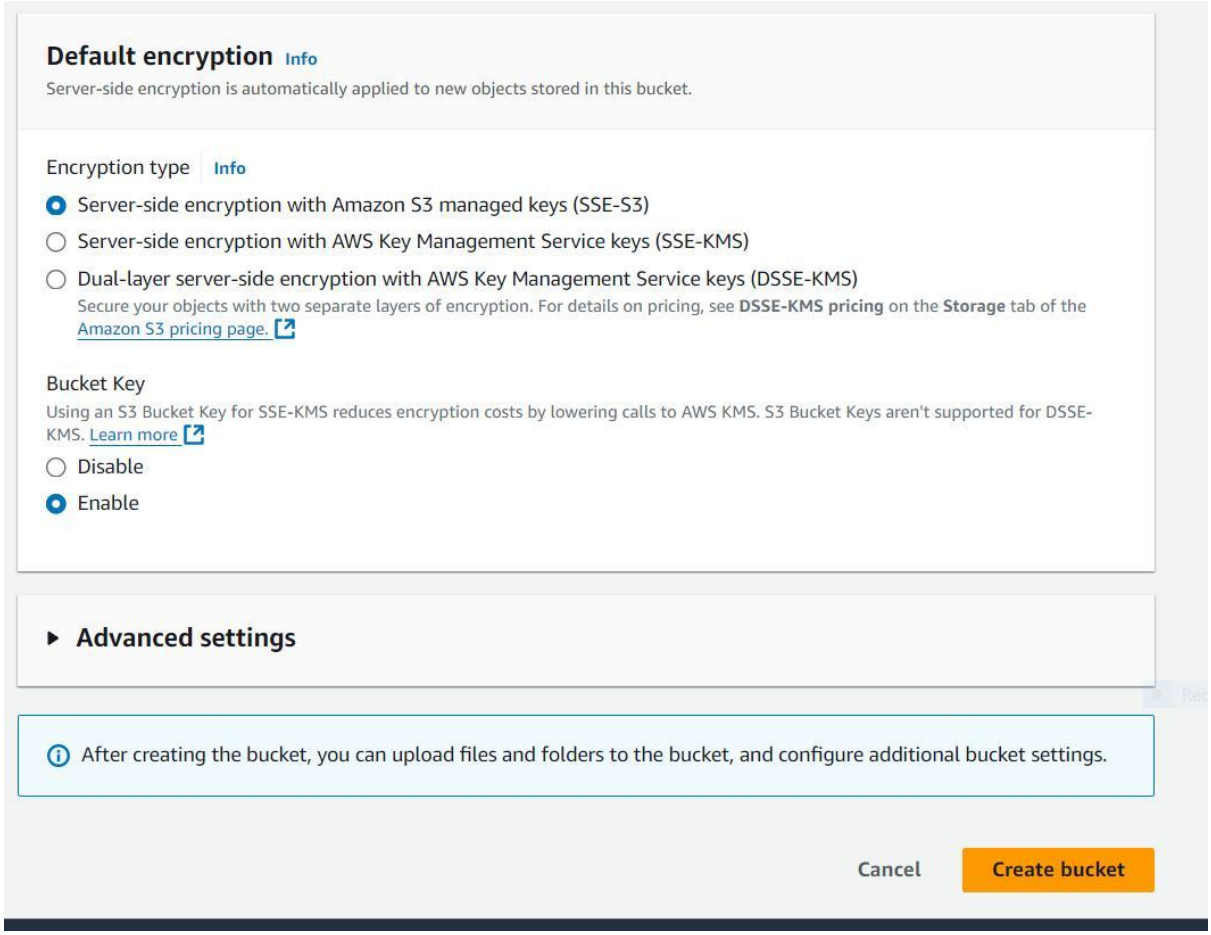
Block all public access



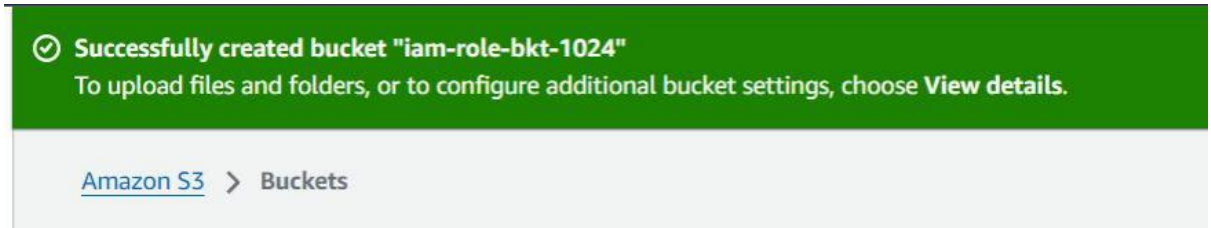
Bucket versioning is disabled



Default setting---



Create bucket



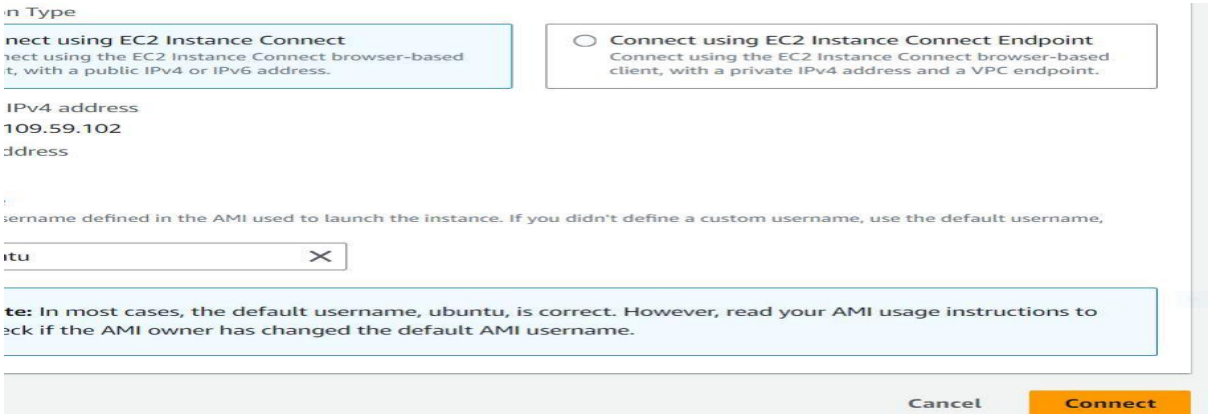
STEP3: Install AWS CLI on ec2 instance--

Note: Before running the aws S3 ls command, ensure you've created at least one empty S3 bucket via the AWS Management Console to see results.

Run the following commands to install the AWS CLI:

- sudo apt install unzip
- curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
- unzip awscliv2.zip
- sudo ./aws/install
- aws --version
- aws s3 ls [To check S3 buckets (none should appear yet)] basically this command will give error because it does not have permissions to access s3.

Now connect your instance and run the above commands in terminal---



```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ sudo apt install unzip
```

```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
```

```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ unzip awscliv2.zip
```

```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ sudo ./aws/install
You can now run: /usr/local/bin/aws --version
```

```
ubuntu@ip-172-31-10-121:~$ aws --version
aws-cli/2.18.16 Python/3.12.6 Linux/6.8.0-1015-aws exe/x86_64.ubuntu.22
```

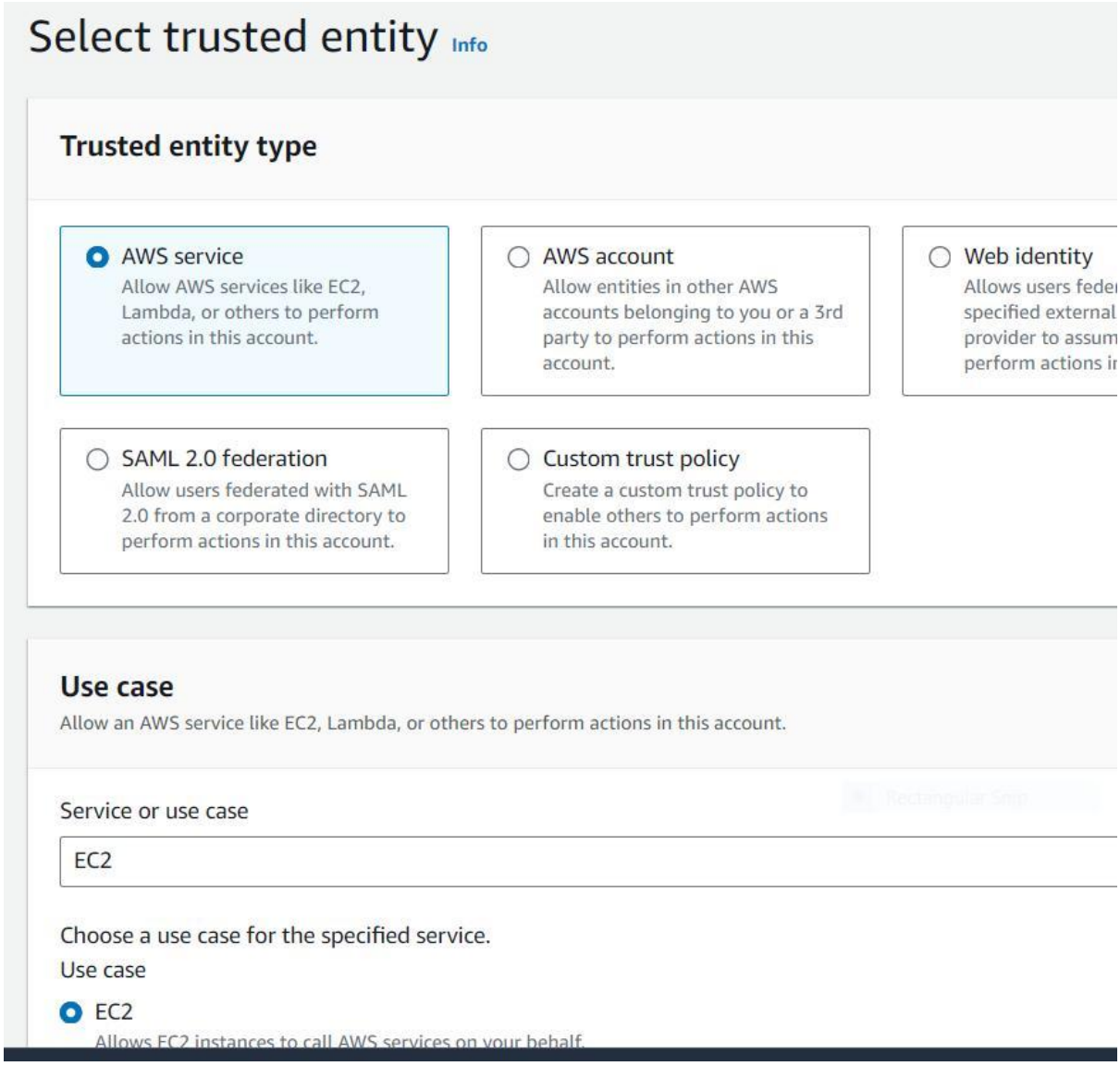
```
ubuntu@ip-172-31-10-121:~$
ubuntu@ip-172-31-10-121:~$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
ubuntu@ip-172-31-10-121:~$
```

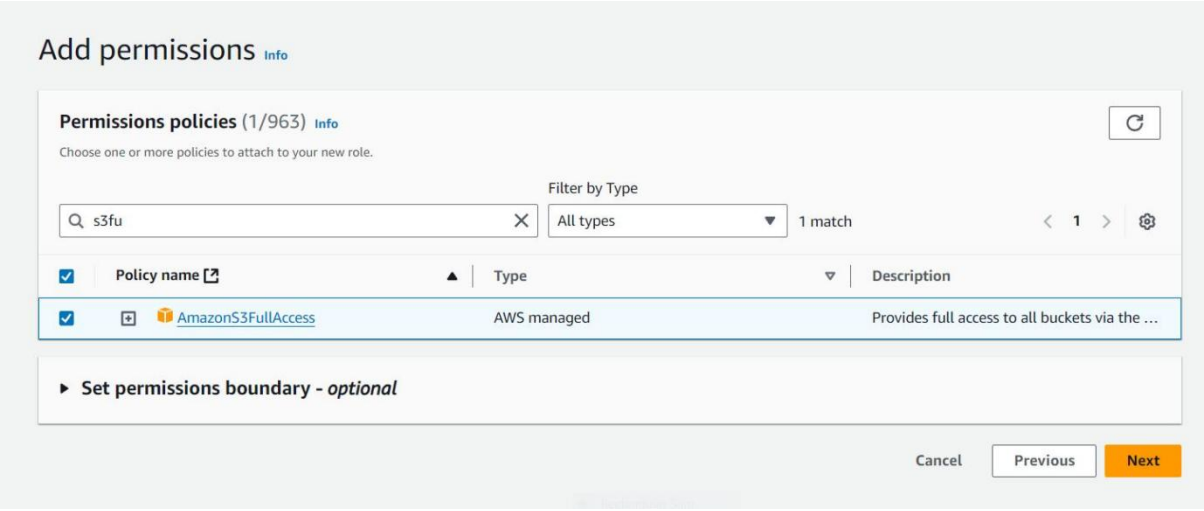
We got the error as we don't have permissions yet.

STEP4: Create a Role and Attach S3FullAccess Policy--

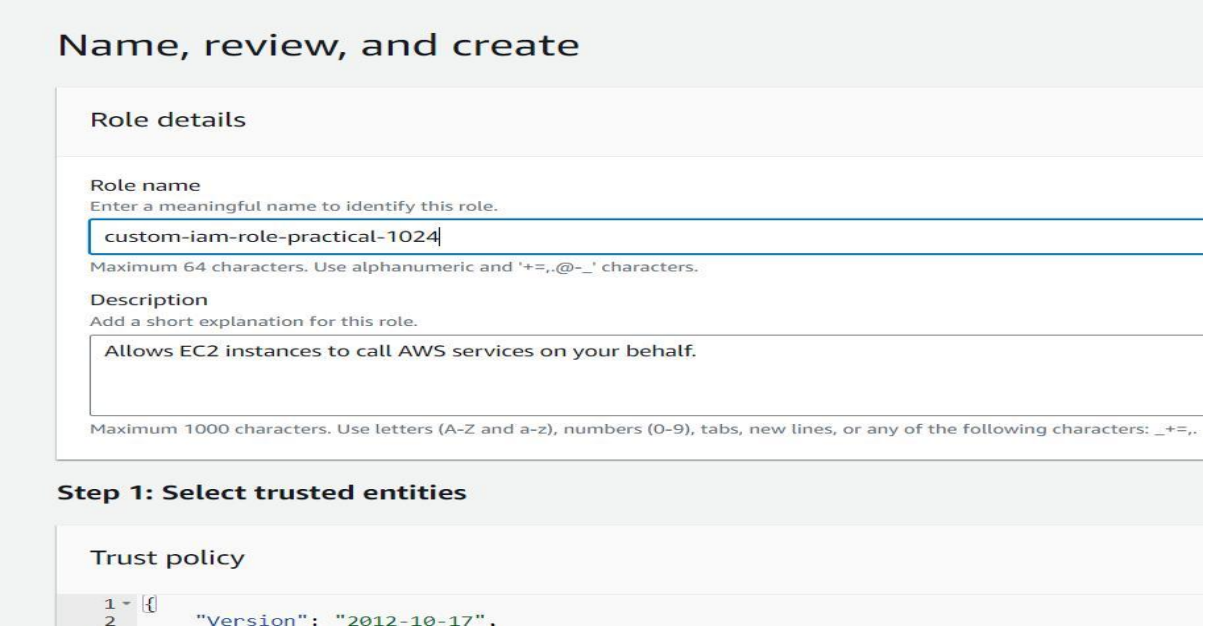
- Navigate to the IAM console, Create a new role, selecting the EC2 service as the trusted entity.

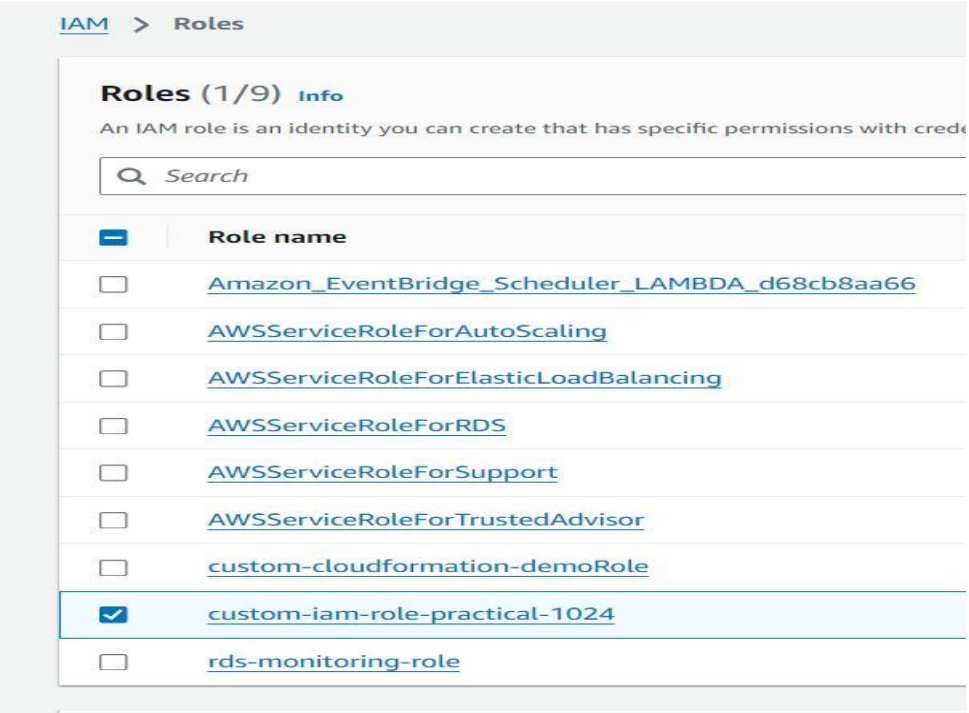


- Attach the AmazonS3FullAccess policy to the role.



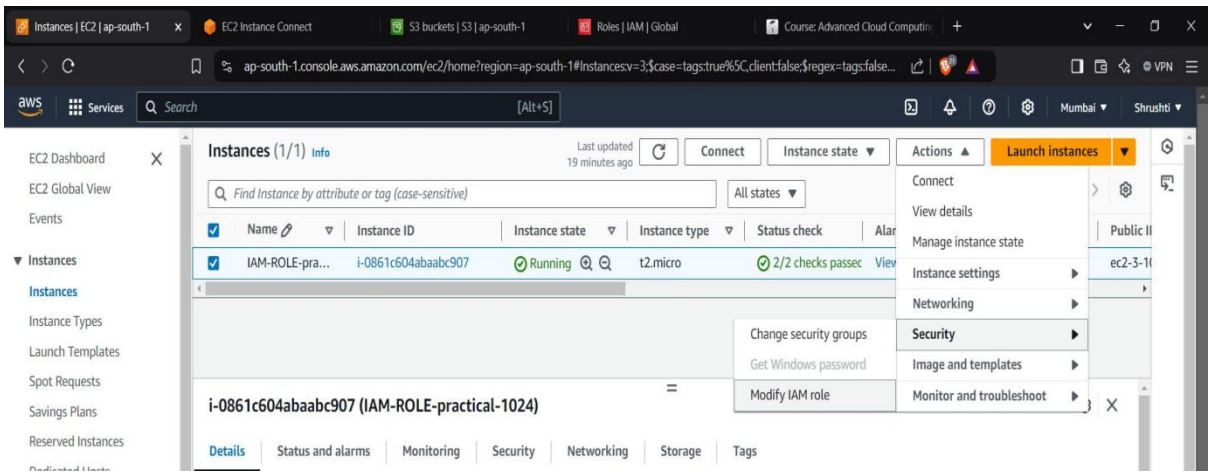
- Name your role and create it.



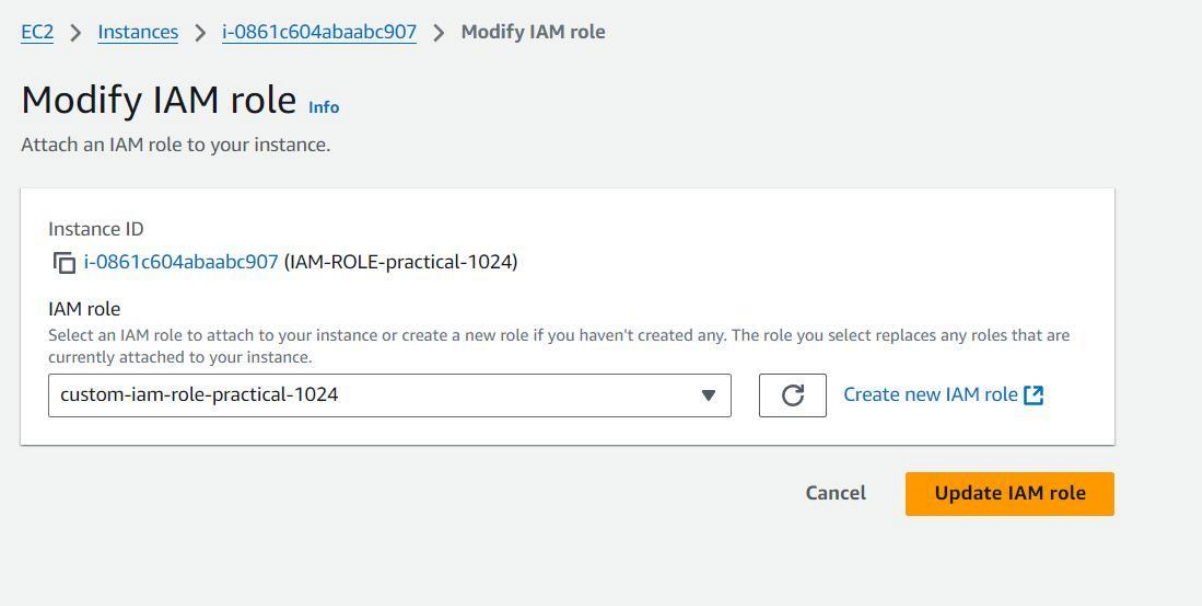


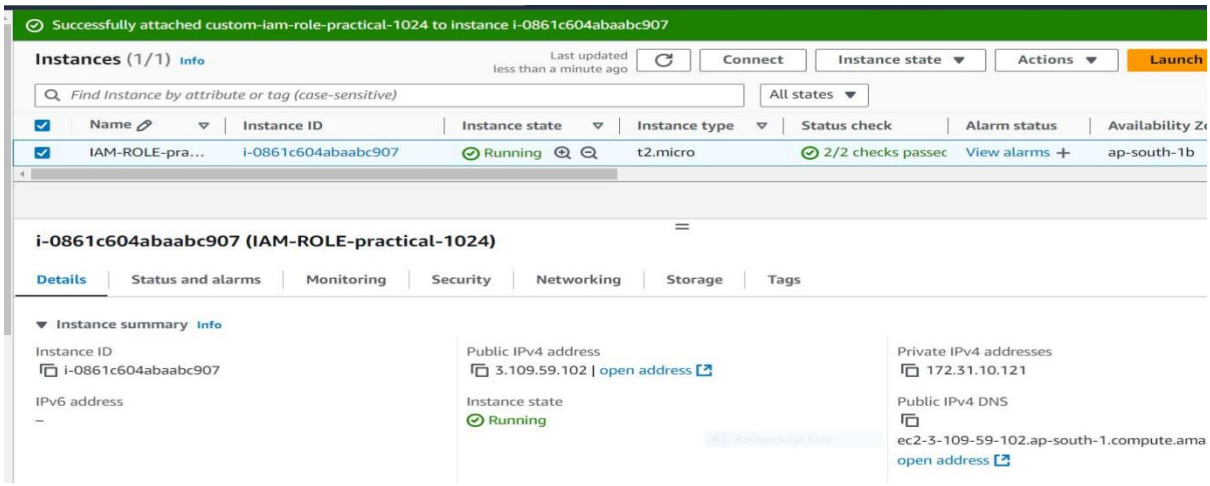
Step5: Modify EC2 Instance Role

- Go back to the EC2 dashboard.



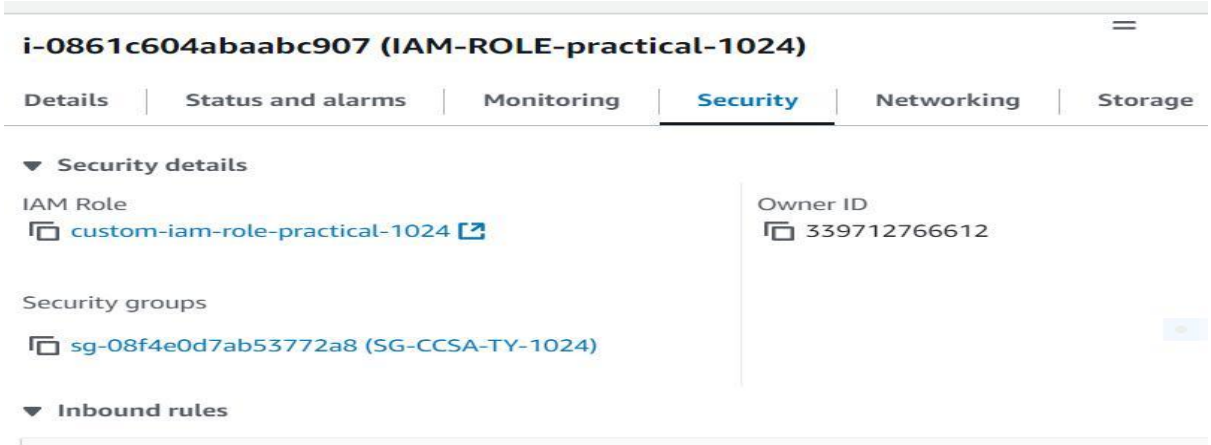
- Select your instance, then click on Actions > Security > Modify IAM Role.





Step6: Verify Permissions

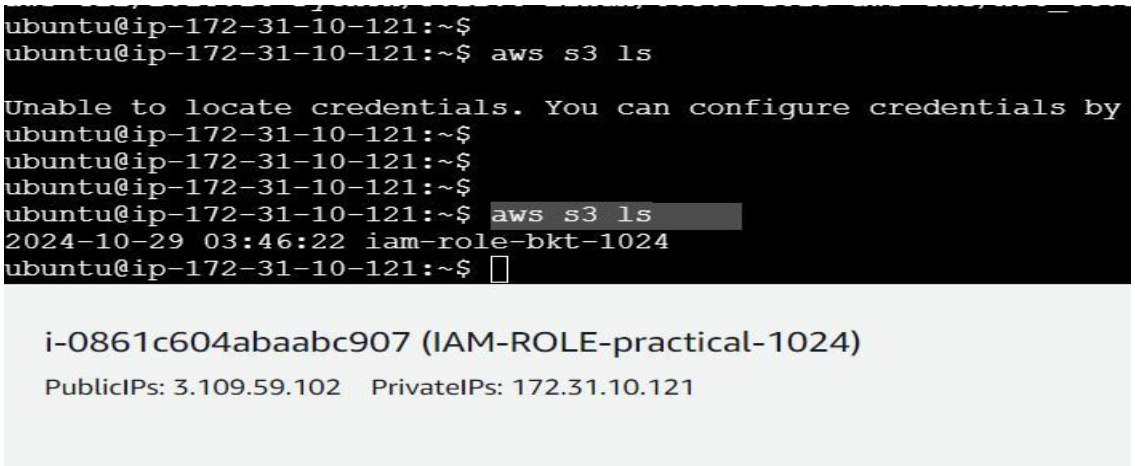
- With the role attached, your instance should now have permissions to access S3.



Step 7: List S3 Buckets Again

- aws s3 ls

You should now see the buckets you created.



We are able to access s3 service from ec2 service using IAM role.

Done.