Guidelines for creating Roles in AWS

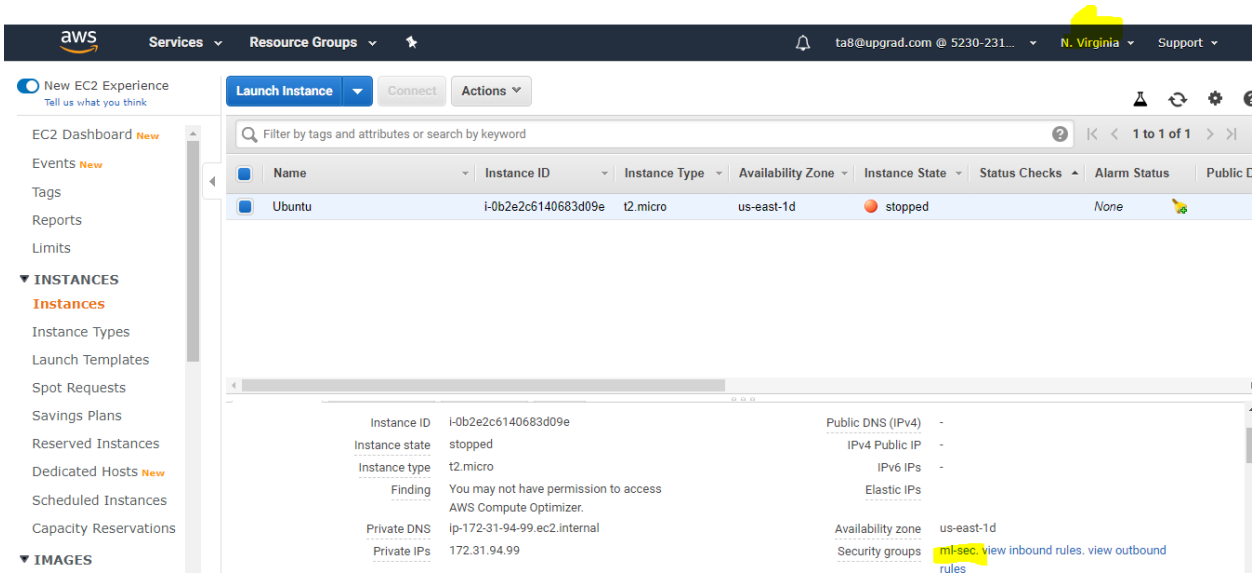
Case: Creating a role for accessing S3 bucket from EC2 instance

Prerequisites:

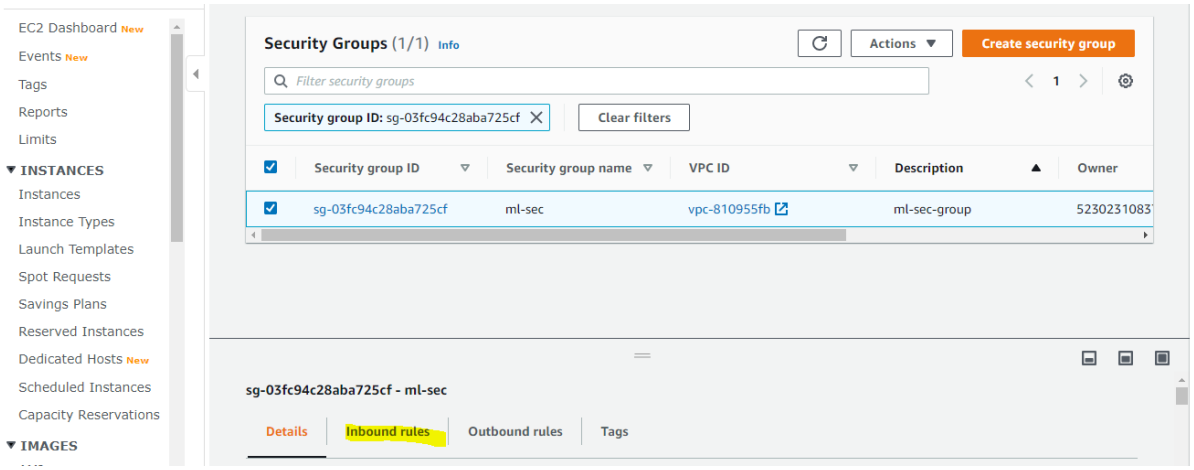
- S3 bucket and EC2 instance should be the same region - **N. Virginia.**
- S3 bucket should be available in your account.

1. Edit the security group with my IP before starting the EC2 instance.

2. Select EC2 and click on the security group - **ml-sec**

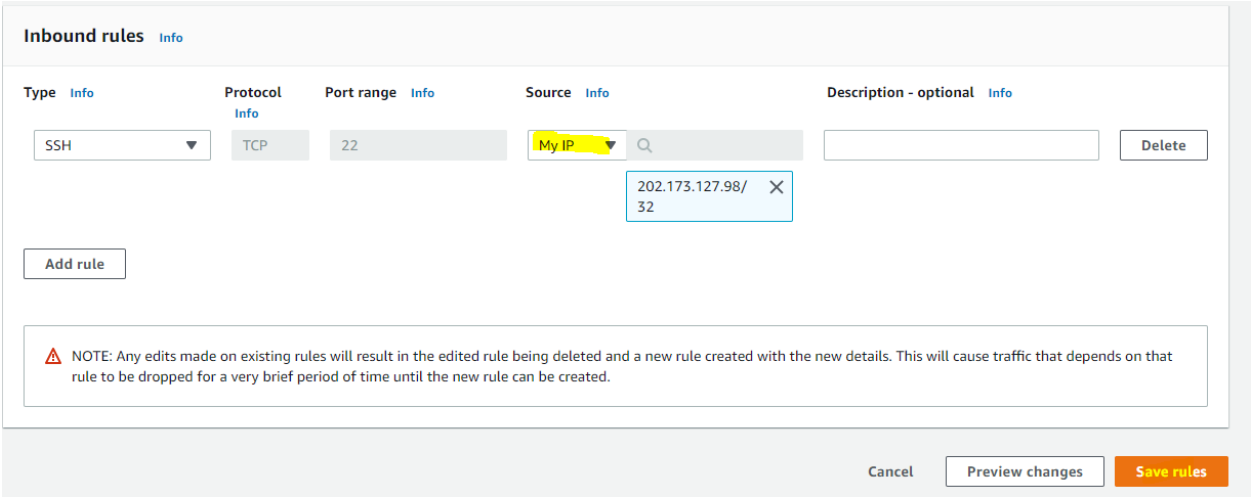


3. Next, click on **Inbound rules**:

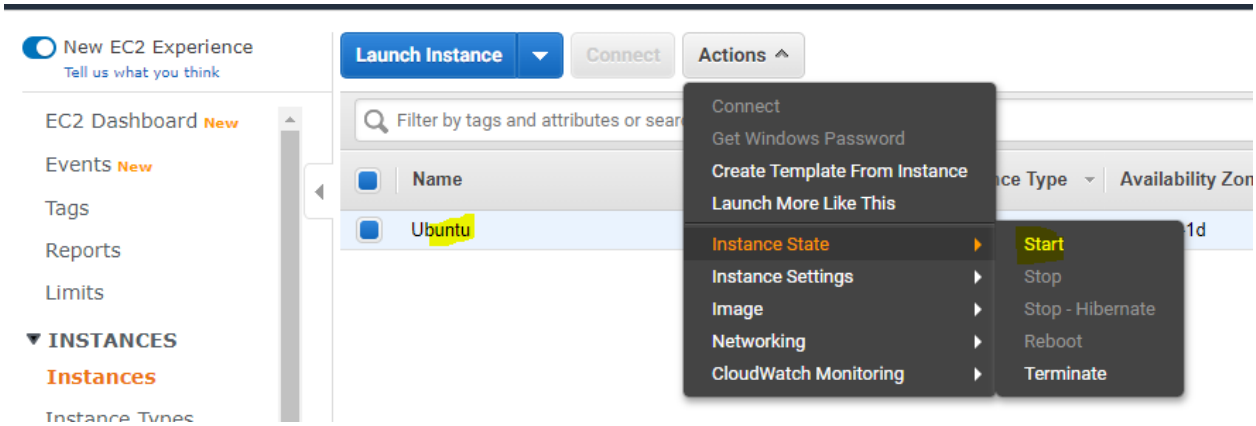


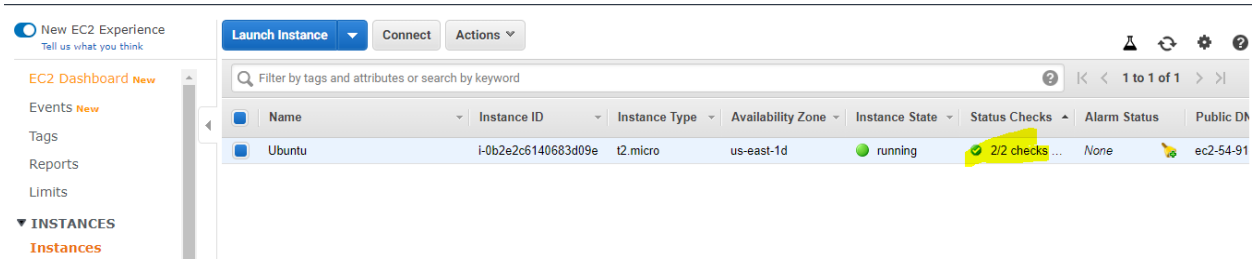
4. Click on **Edit inbound rules**:

5. Edit source with My IP and click on **Save rules**.

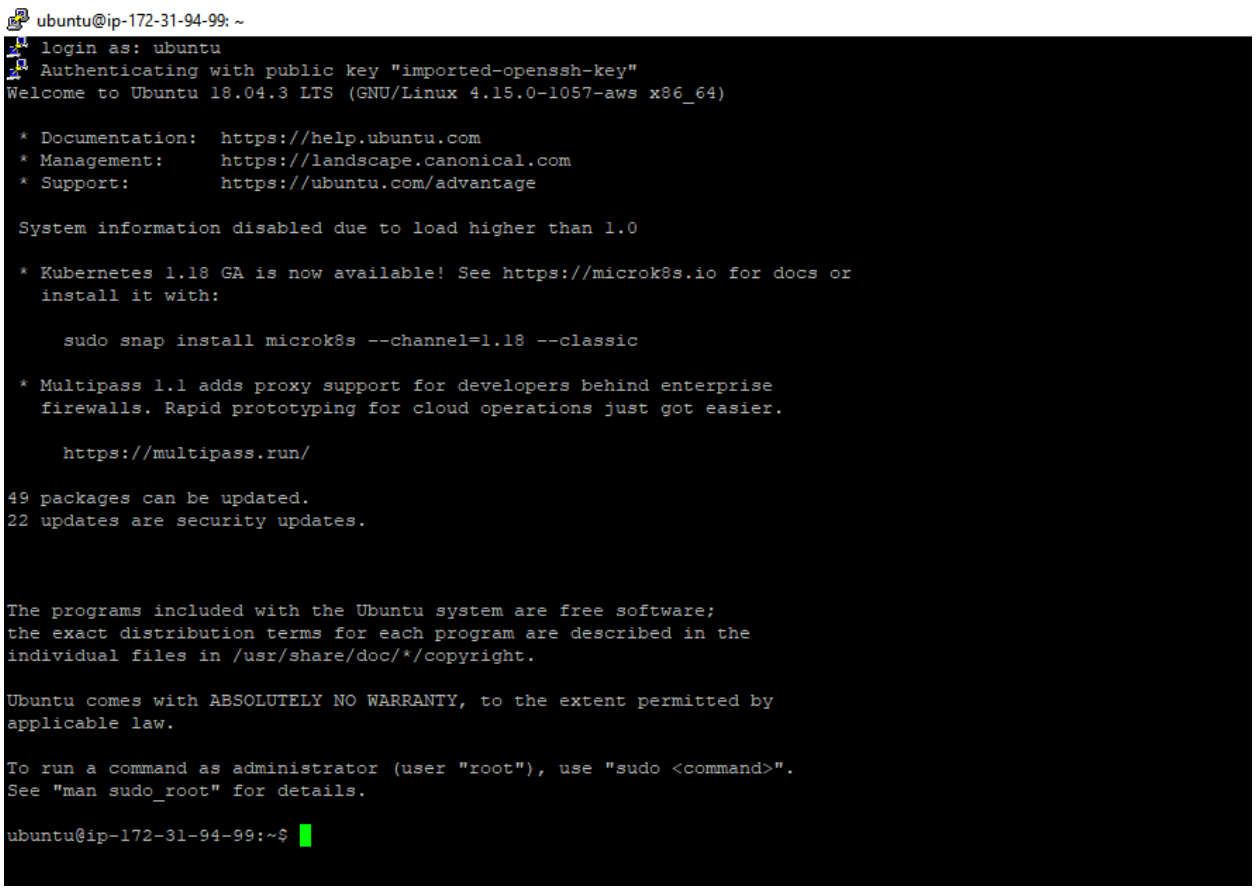


6. Navigate back to the EC2 dashboard and **start** the EC2 instance.





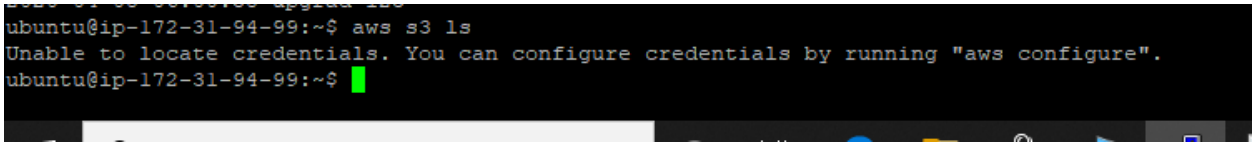
7. Then, access the EC2 instance from PuTTy or Linux/MAC shell.



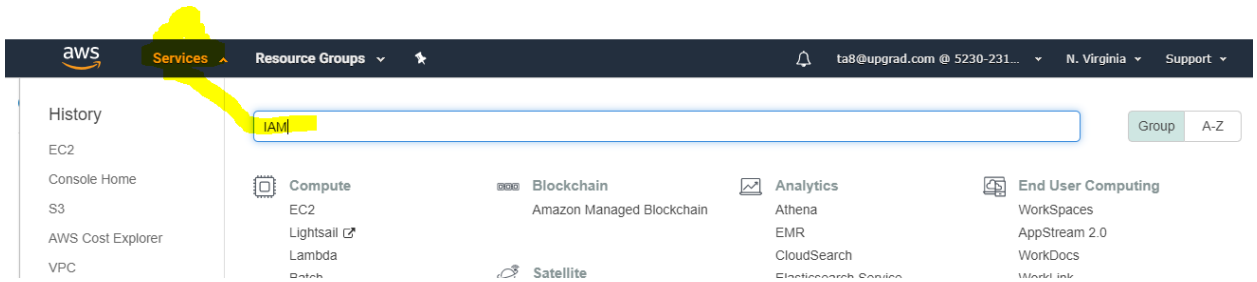
8. Run below command and access s3 bucket from instance.

sudo apt-get update
sudo apt-get install awscli

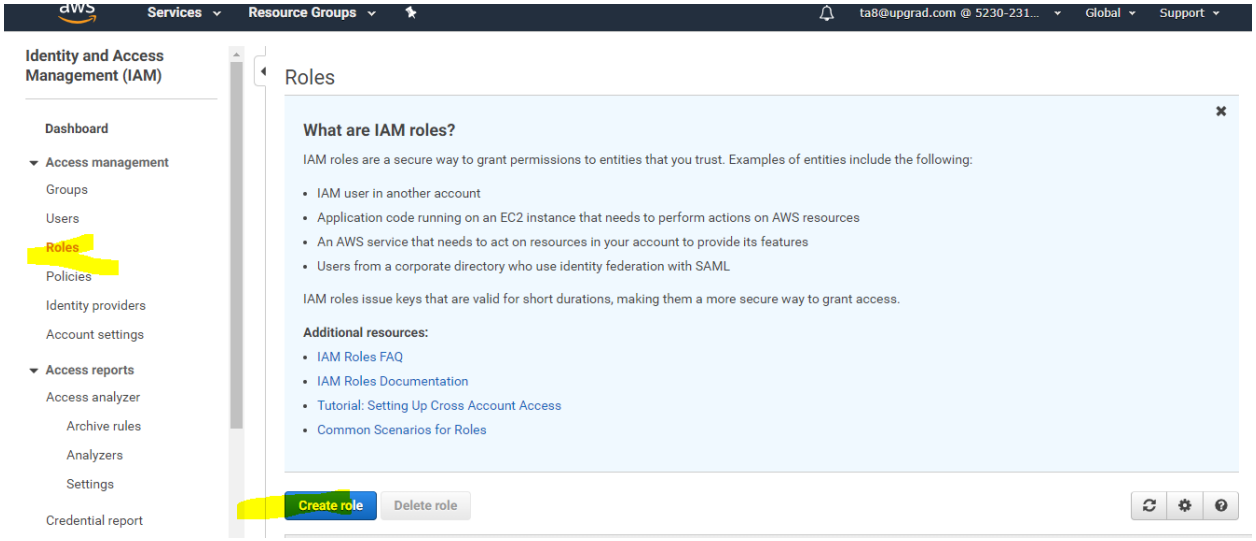
9. Enter **aws s3 ls**



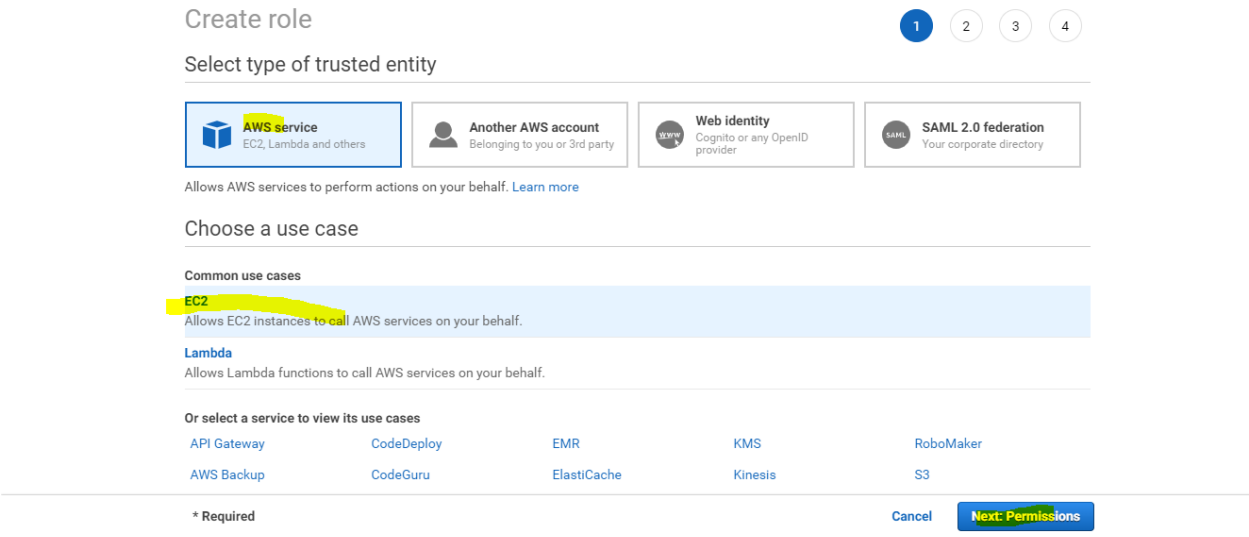
10. Presently, you are not able to access the bucket. Go back to the AWS management console and search for the **IAM** service.



11. Click on **Roles** and **Create role**.

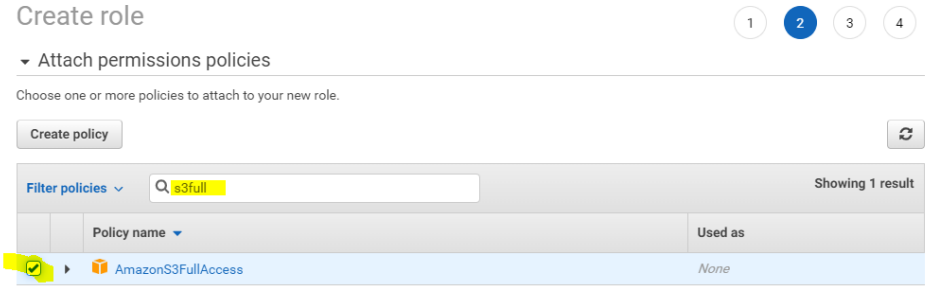


12. Select **EC2** in the use case list and click on **Next Permissions**.

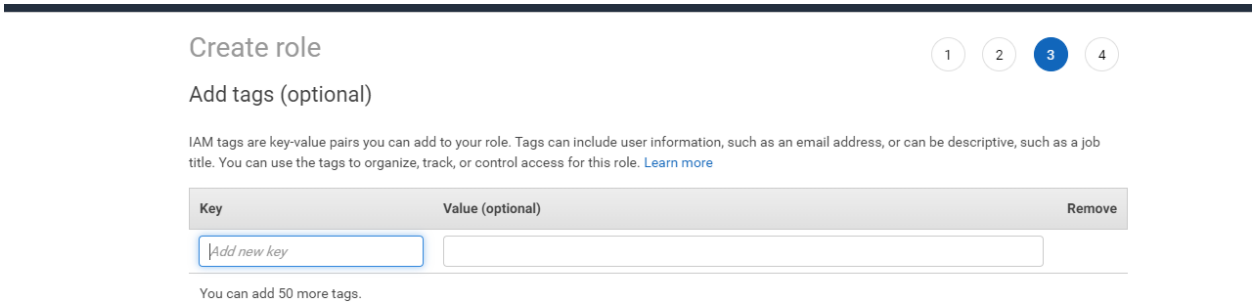


13. In the search tab, search policy **s3full** and select the checkbox for **AmazonS3full access**.

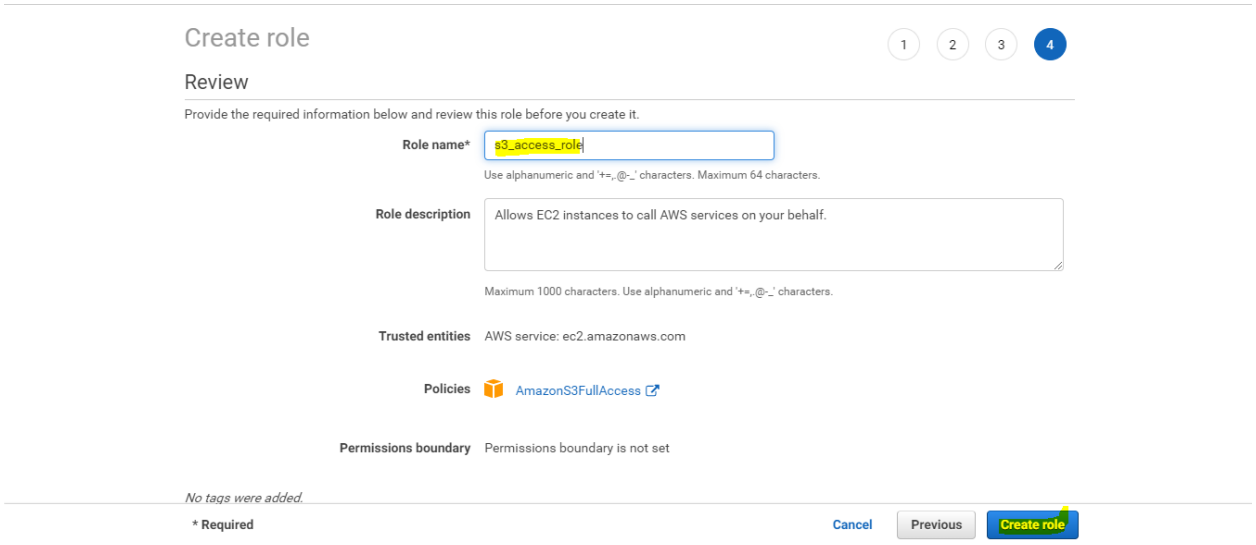
    Policy- AmazonS3FullAccess



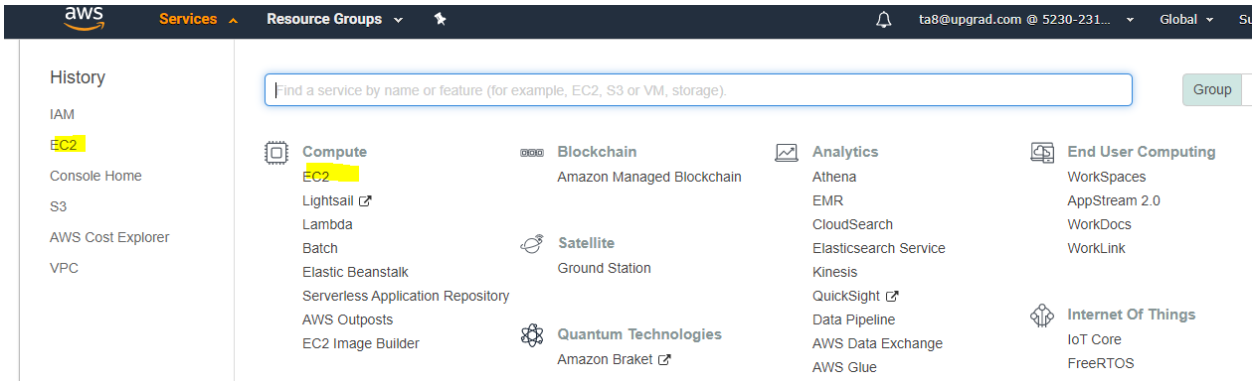
14. Click on Next numbered tab



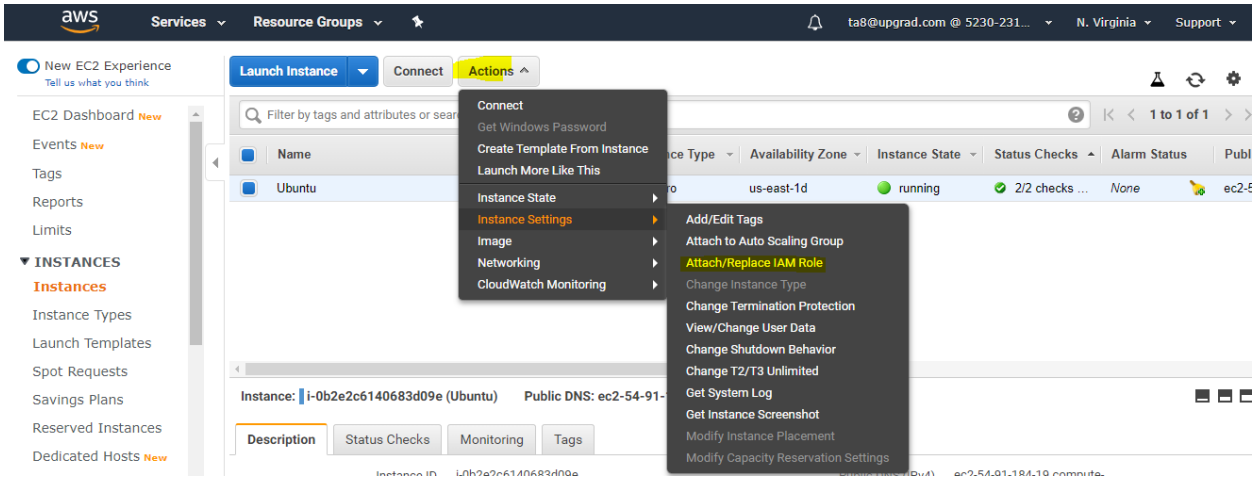
15. Give the role name: **s3_access_role** and click on create role.



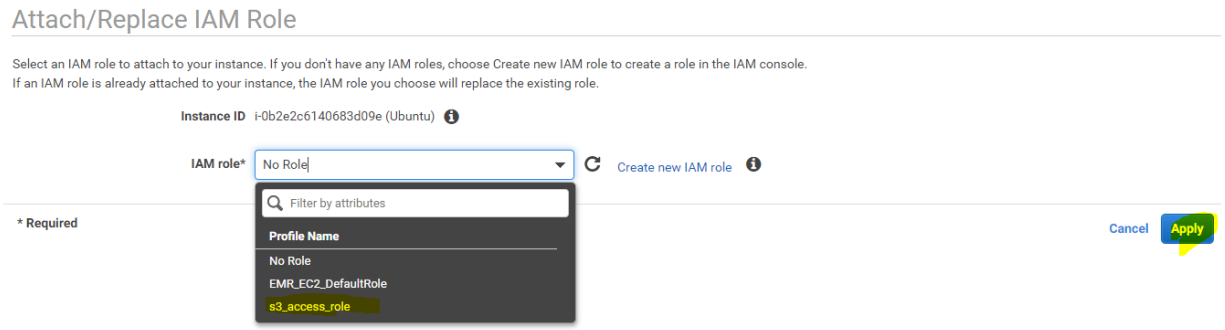
16. Navigate back to the EC2 service.

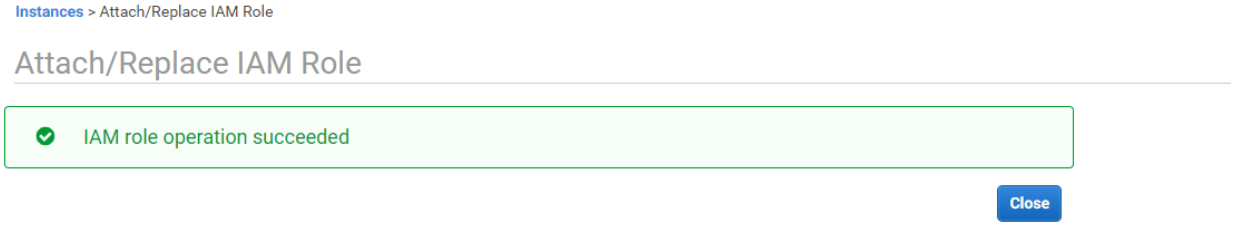


17. Go to EC2 instance> Action> instance setting> **Attach/Replace IAM role**



18. Select your role: **s3_access_role** and **Apply**.





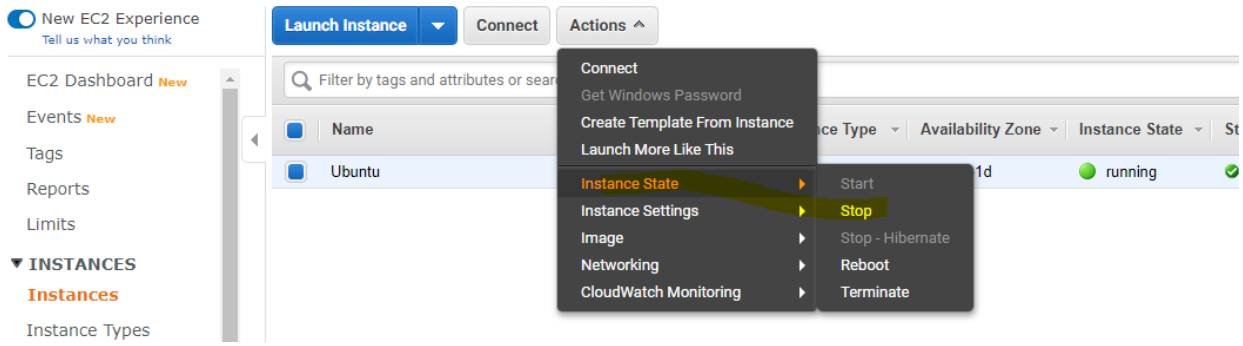
19. Switch back to the instance terminal.

aws s3 ls

```
ubuntu@ip-172-31-94-99:~$ aws s3 ls
2020-01-23 06:08:10 test-agaw
2020-04-08 06:00:58 upgrad-123
ubuntu@ip-172-31-94-99:~$
```

You can view the contents of the S3 bucket now.

Note: Please stop the instance when not in use or save the budget. If the instance is no longer required, terminate the instance.



Please verify the instance status - Stopped with Red.