AWS LAB Secure Architecture | Monarch Nigam

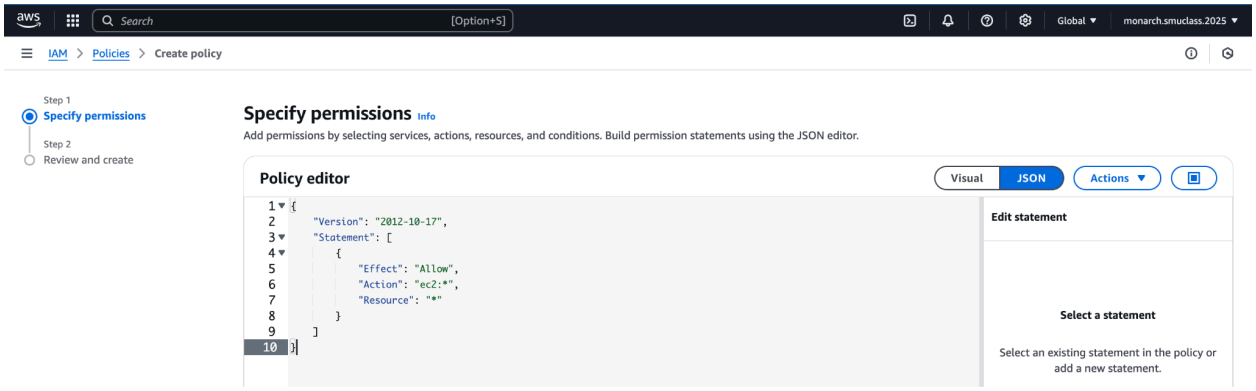
EXERCISE 12.1

Create a Limited Administrative User

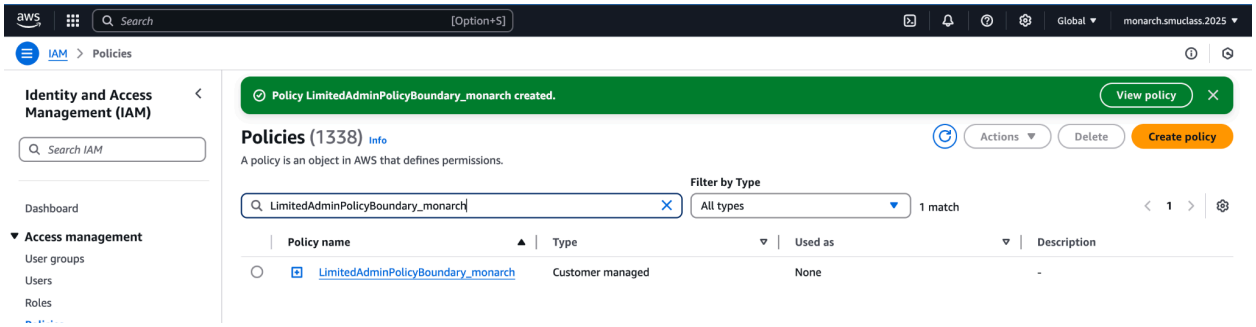
In this exercise We will create an IAM user with limited administrative privileges. You'll use policy boundary permissions to allow the user to perform only actions in the EC2 service.

1. Create a customer-managed policy called LimitedAdminPolicyBoundary. Populate the policy document with the following content:

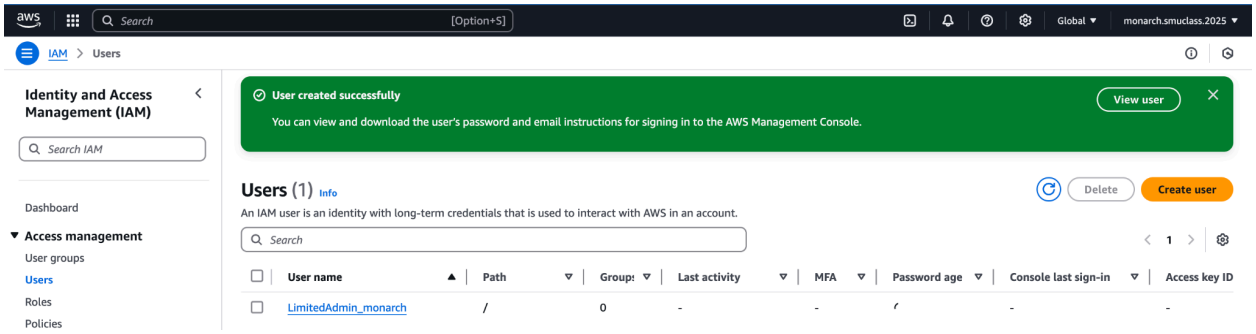
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        }
    ]
}
```



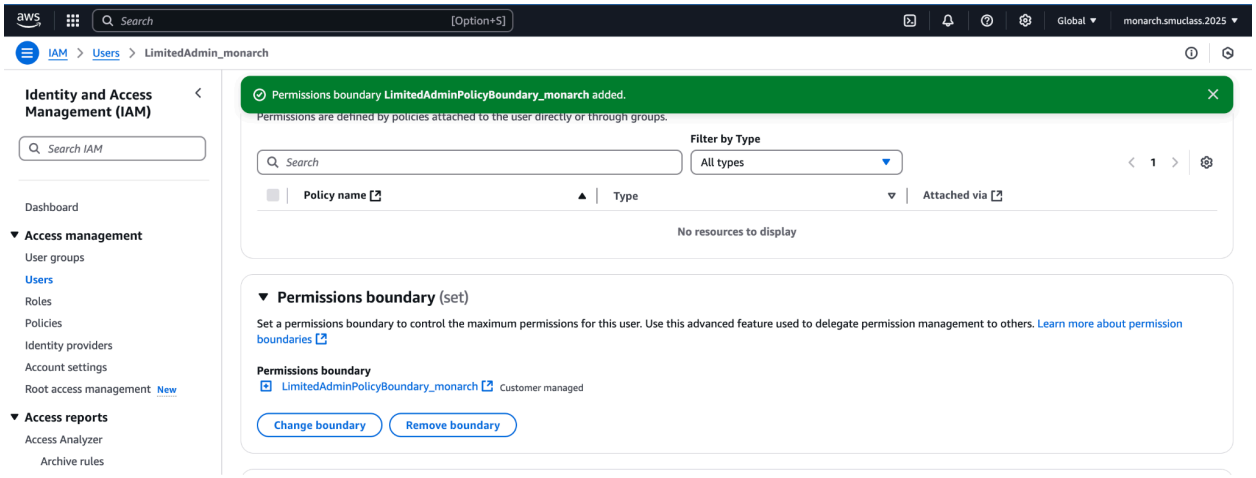
2. Create an IAM user with the name of your choice, such as LimitedAdmin.



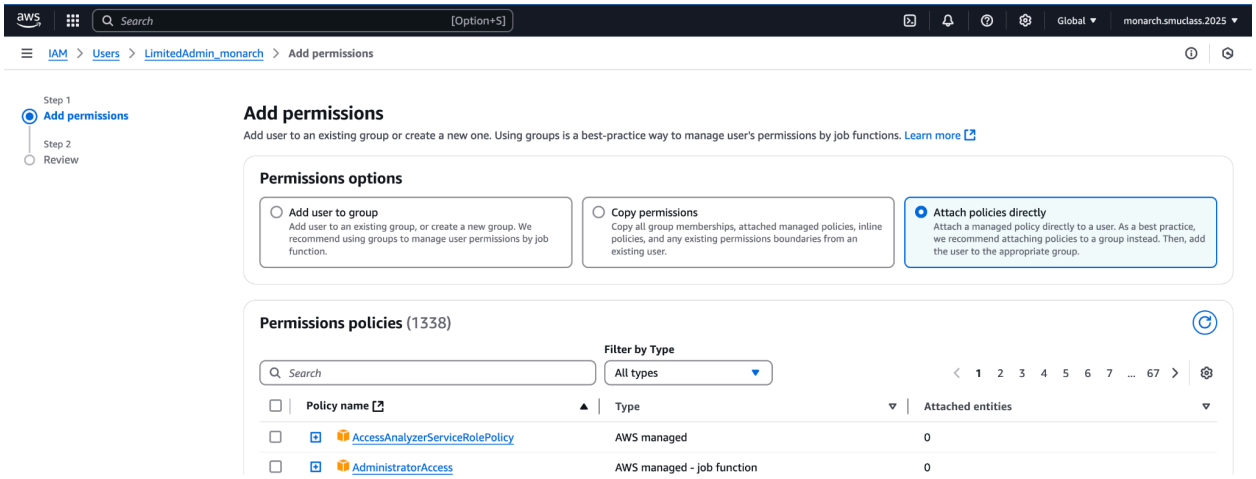
3. In the IAM Dashboard, click the Users option and then click the username you created.



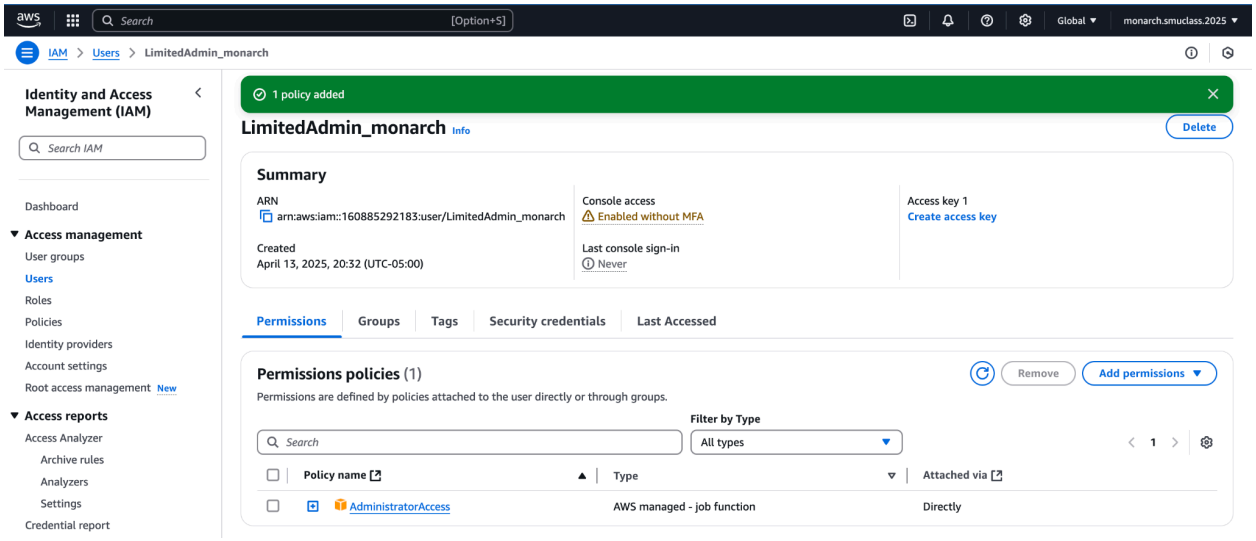
4. Under Permissions Boundary, click the Set Boundary button.
5. Select the LimitedAdminPolicyBoundary option and click the Set Boundary button.



6. Under Permissions Policy, click Add Permissions.
7. Click the Attach Existing Policies Directly button.



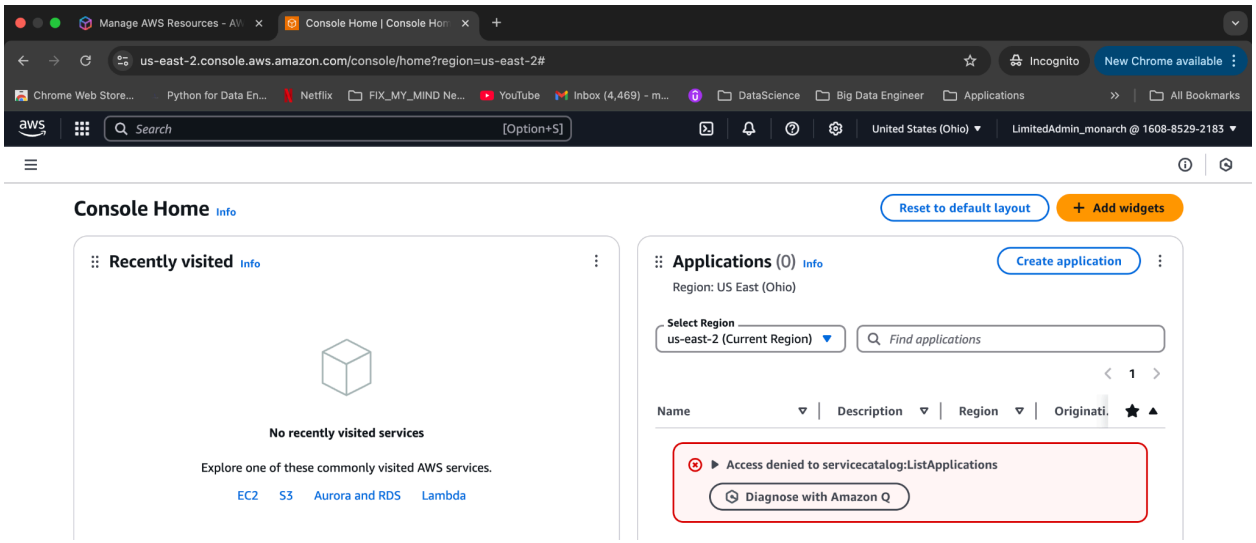
8. Select the AdministratorAccess policy and click the Next: Review button.
9. Click the Add Permissions button.



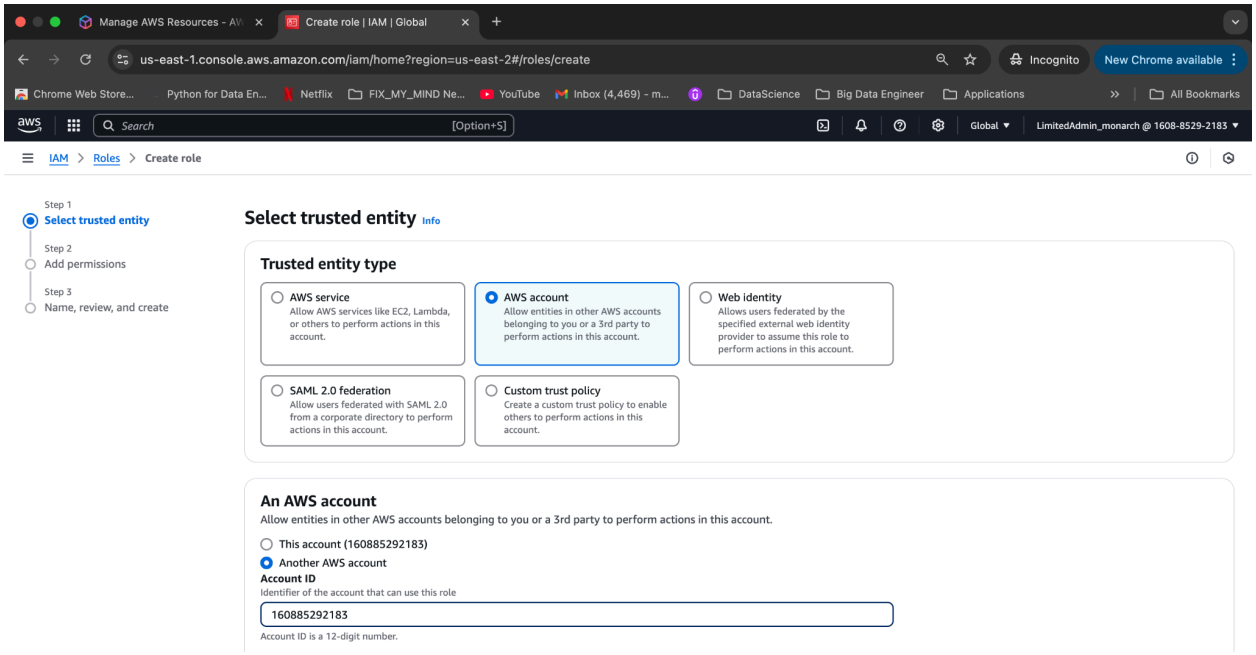
EXERCISE 12.2

In this exercise, we will create a role and assume it.

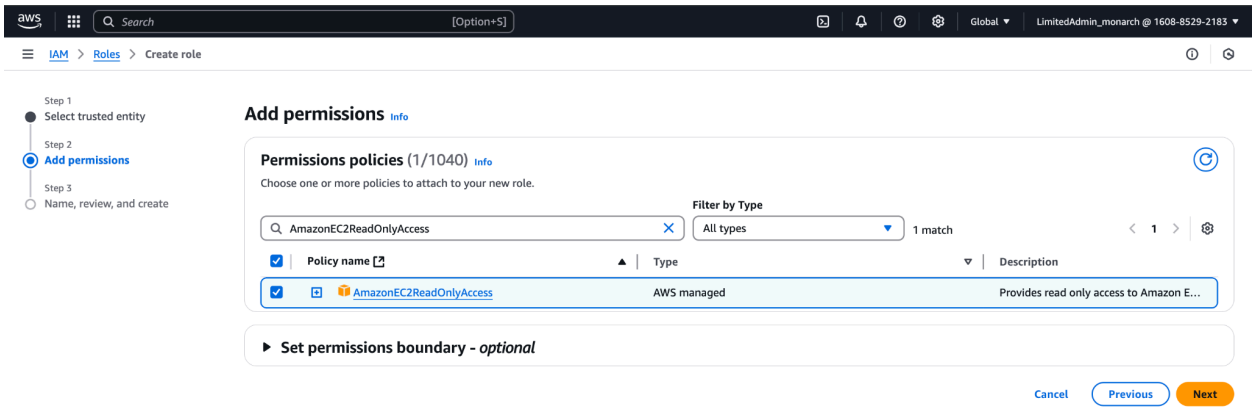
- While logged in as an administrative IAM user, click Roles on the menu on the left side of the IAM Dashboard screen and then click the Create Role button.



- Under Select Type Of Trusted Entity, click the Another AWS Account button.
- Under Account ID, enter your AWS account number. Click the Next: Permissions button.

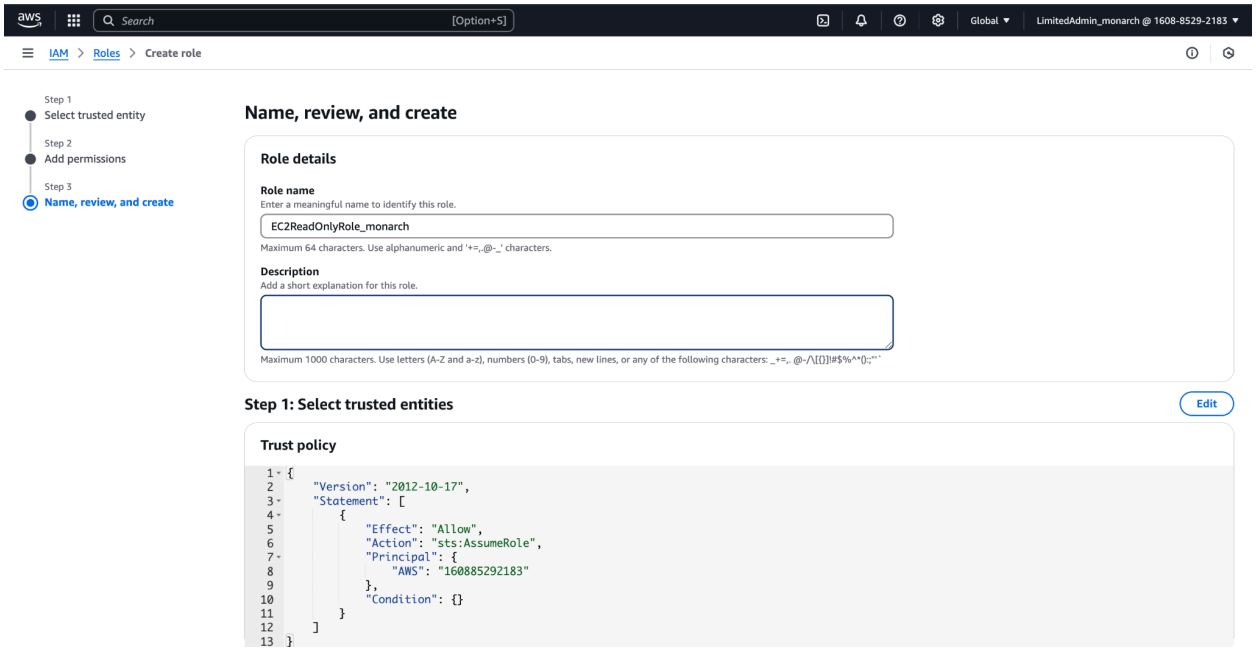


- Select the AmazonEC2ReadOnlyAccess AWS managed policy and click the Next: Tags button.

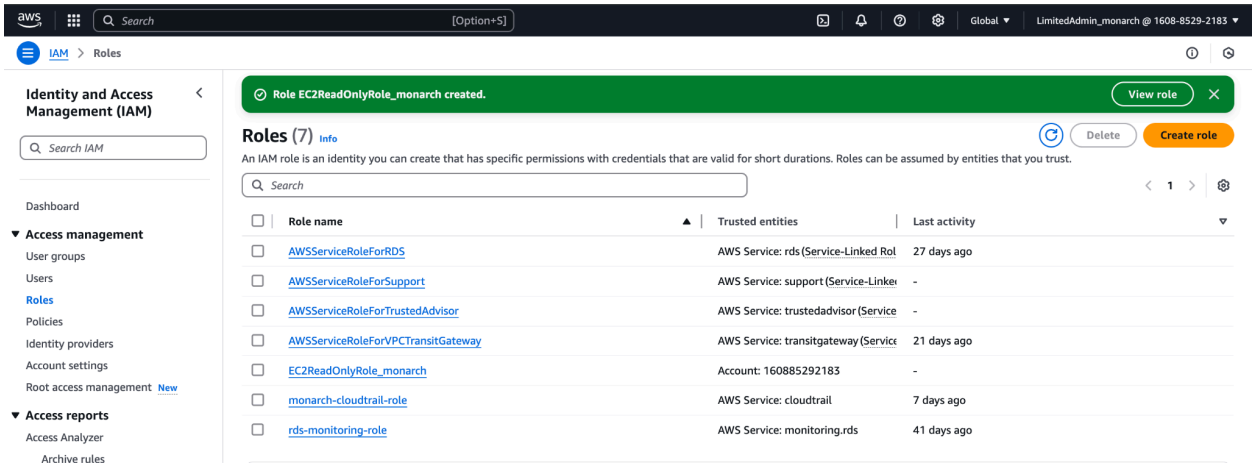


- Click the Next: Review button.
- Enter a name for the role, such as EC2ReadOnlyRole

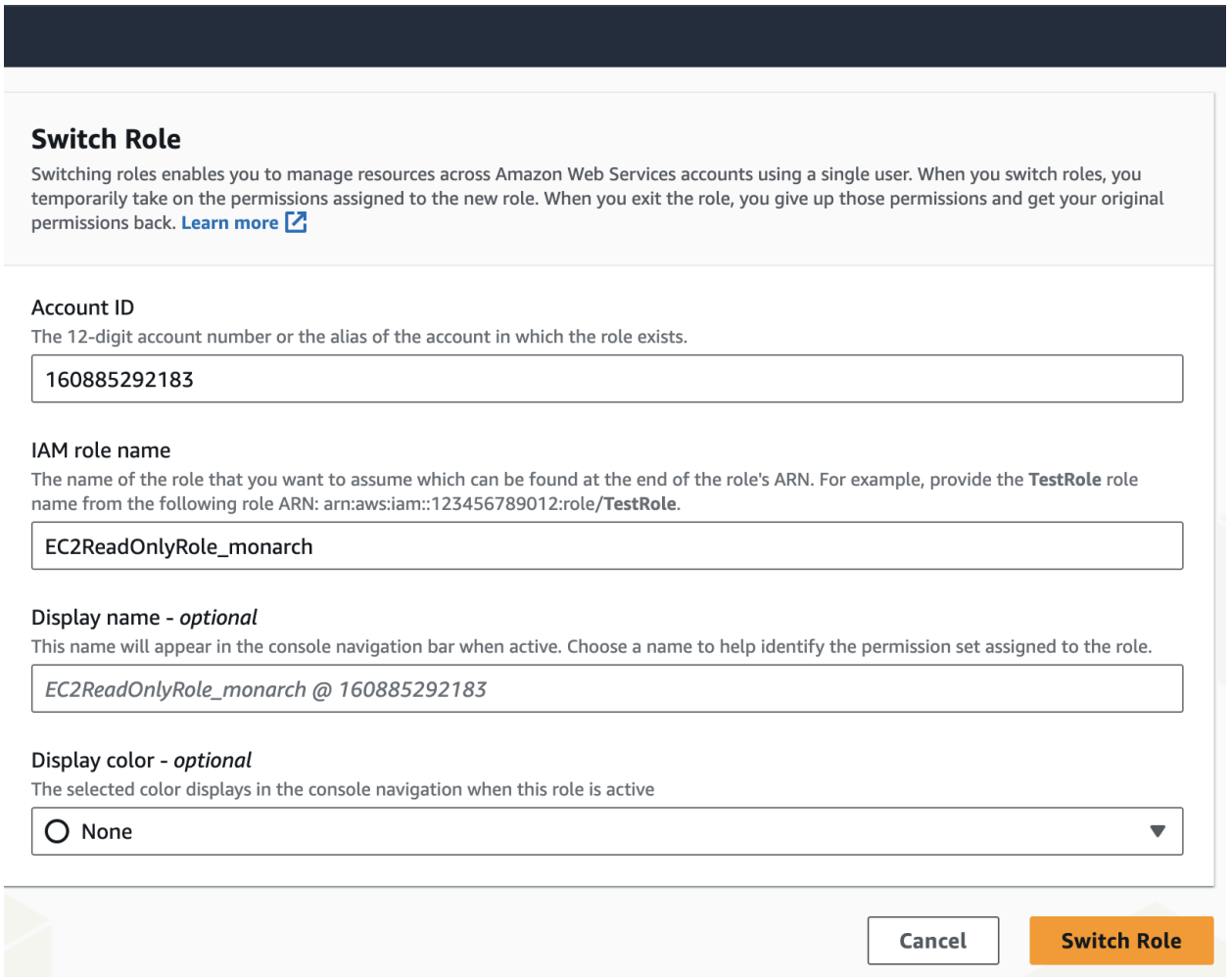
.



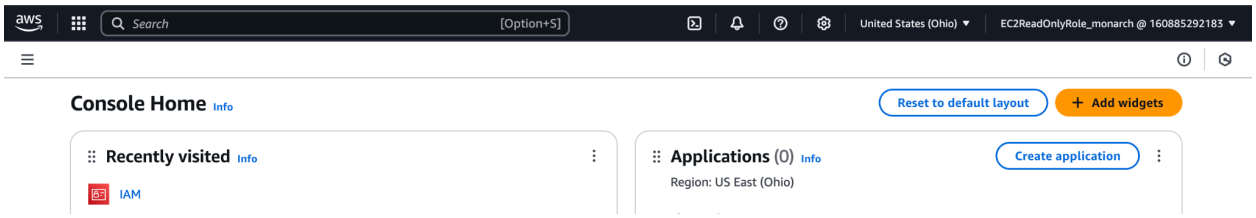
- Click the Create Role button.



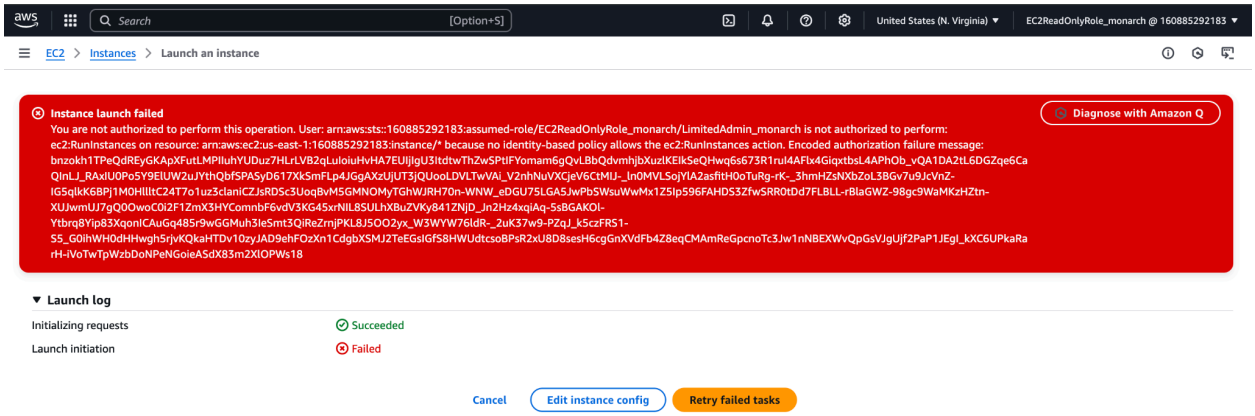
- On the navigation bar at the top of the AWS Management Console, click your IAM account name. A drop-down menu will appear.
- Click the Switch Role link in the drop-down menu, as shown here.
- Snapshot of entering the fields.
- Click the Switch Role button.
- Enter your 12-digit AWS account number or alias and the name of the role you created in step 6. The following shows an example of a Switch Role screen with the account and role specified.
- Snapshot of entering the fields.



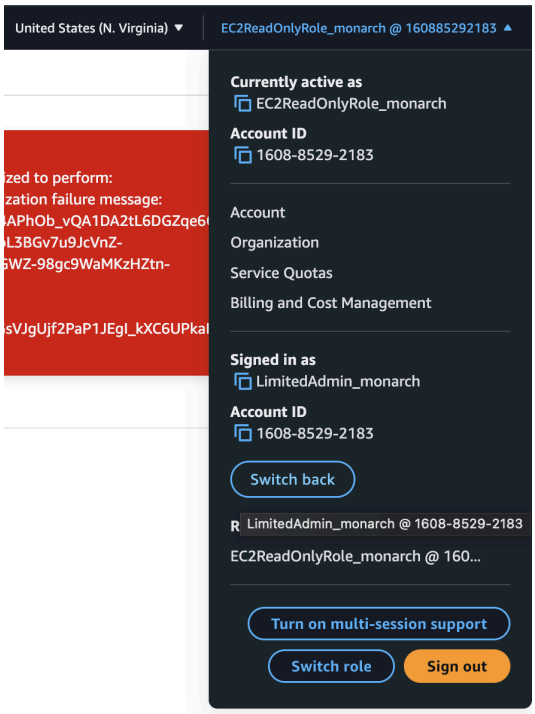
- Click the Switch Role button. The name of the role followed will appear in the top navigation bar. You will now be operating under the role you created.



- Try to launch an EC2 instance. It will fail because the assumed role doesn't have the RunInstances permission. As we can see in the below snapshot we are not able to create the EC2 instance



- To switch back to your IAM user, click the upper-right menu bar where the name of the role followed by your AWS account number is. Then click the link that reads Back To [your IAM username].

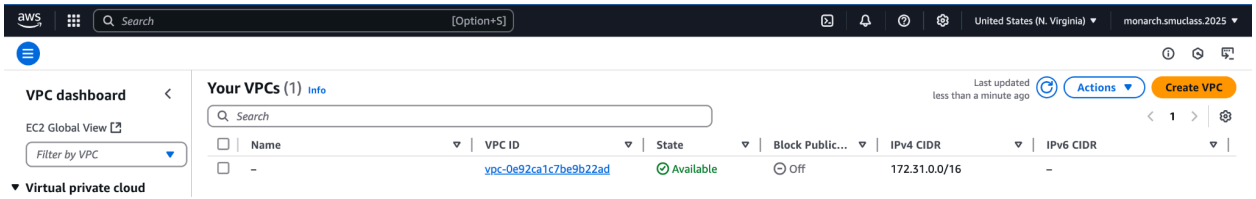


EXERCISE 12.3

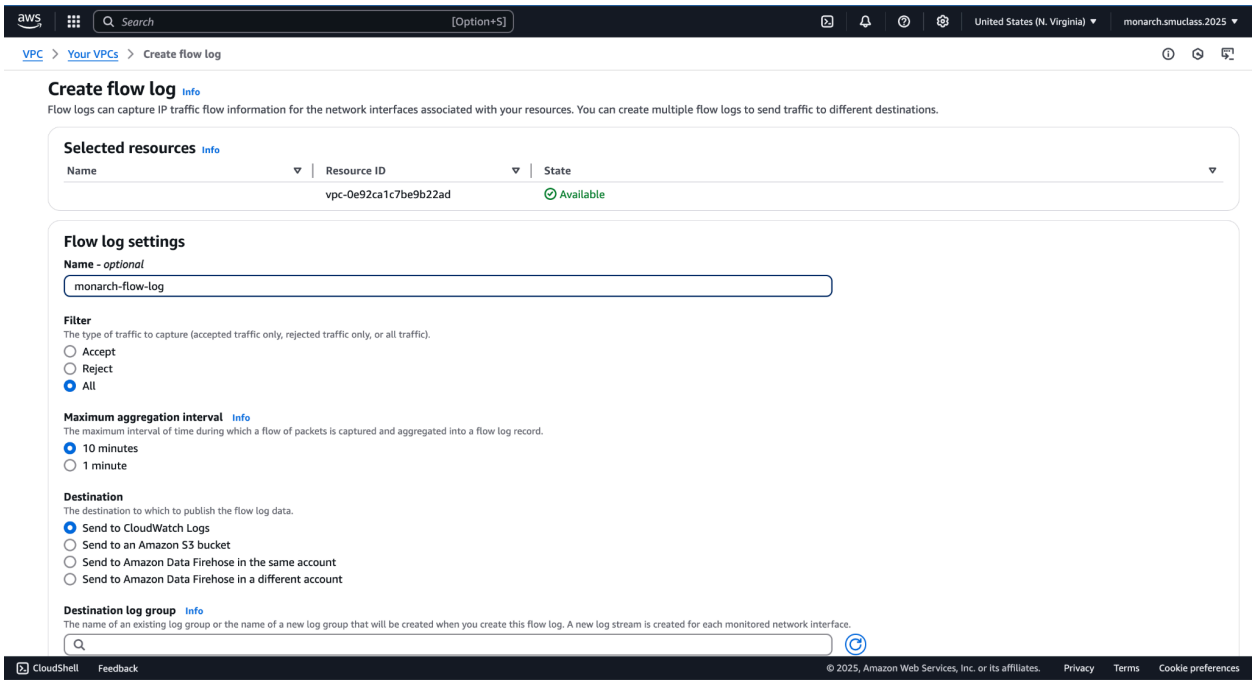
Configure VPC Flow Logging

In this exercise, we will configure VPC flow logging to deliver flow logs to a CloudWatch Logs log group.

1. In the VPC Dashboard, select a VPC you want to log traffic for. Click the Flow Logs tab.

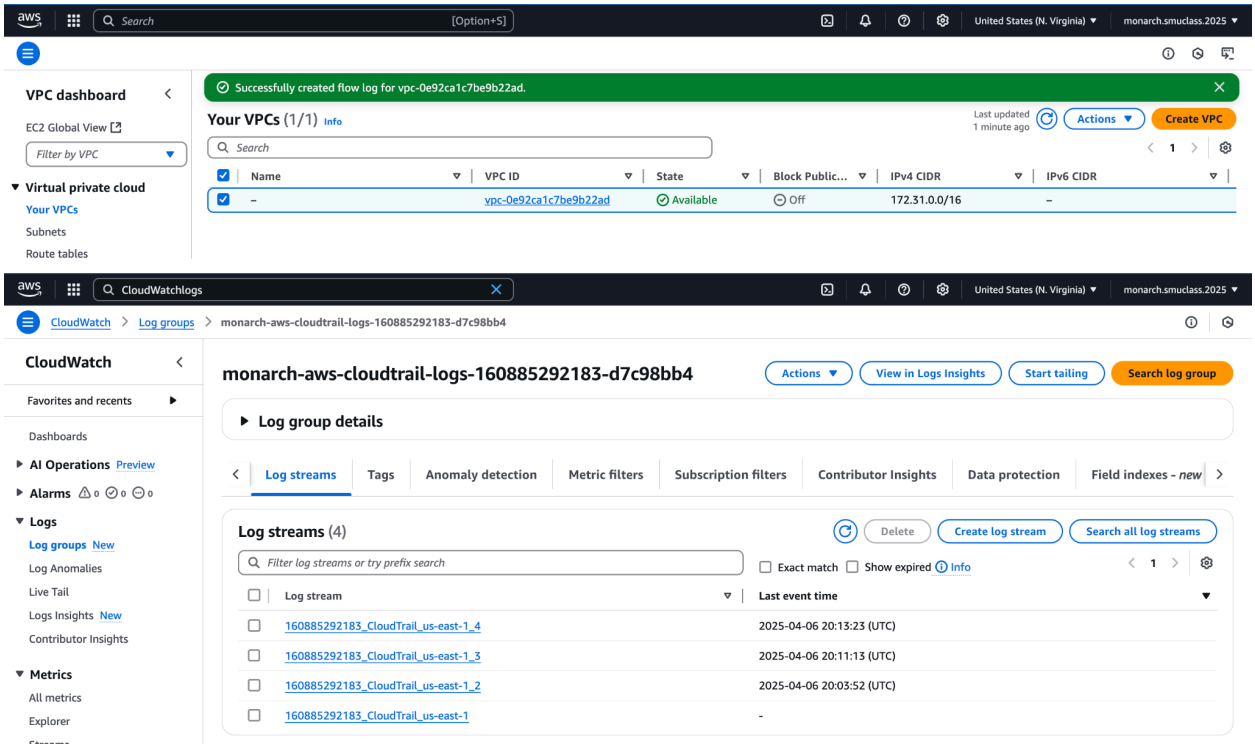


2. Click the Create Flow Log button.



3. In the Destination Log Group field, enter a name of your choice, such as **FlowLogs**.

4. You'll need to specify a role, which AWS can create for you. Click the Set Up Permissions link.
5. A new browser tab will open. Click the Allow button. AWS will create a role called FlowlogsRole.
6. Return to the previous tab with the Create Flow Log Wizard. Select the FlowlogsRole.
7. Click the Create button.

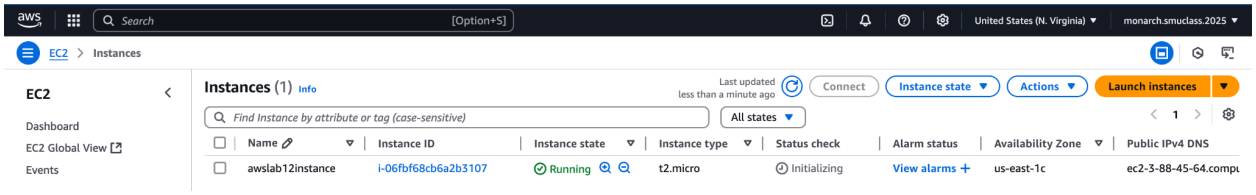


EXERCISE 12.4

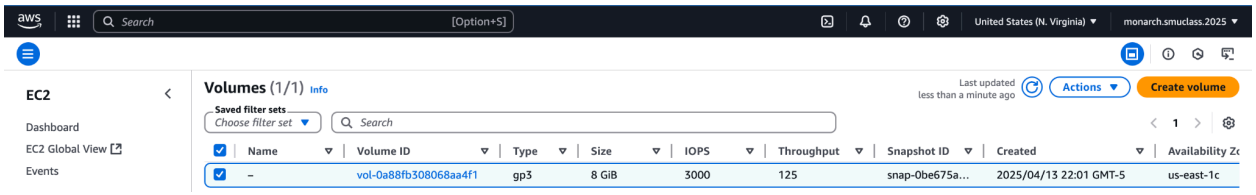
Encrypt an EBS Volume

For this exercise, we Will encrypt an unencrypted volume attached to a running EC2 instance.

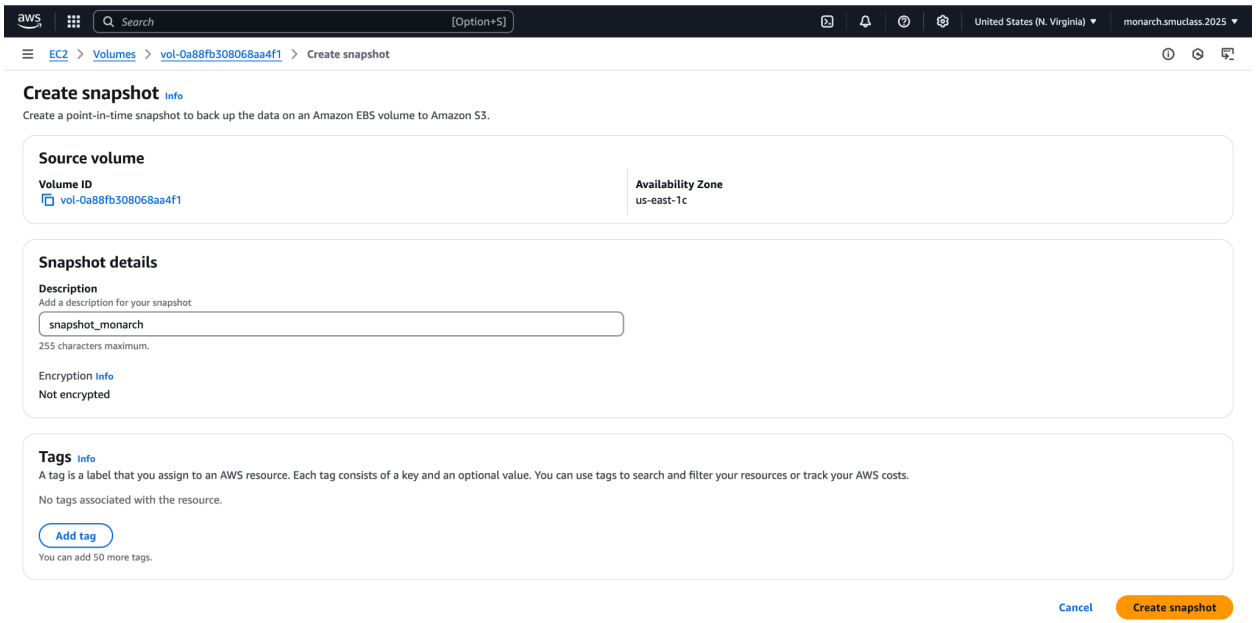
1. Create an EC2 instance from an unencrypted snapshot or AMI. If you already have one you can bear to part with, you may use that.



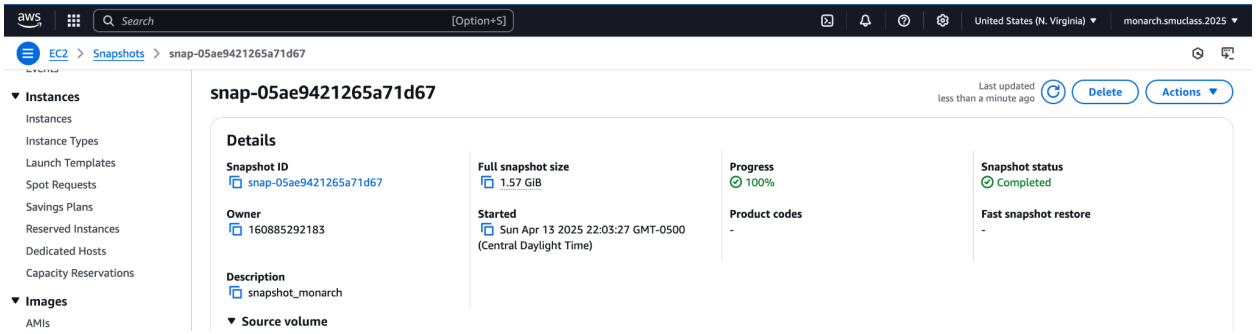
2. At the EC2 Dashboard, click Volumes in the left-side menu.
3. Select the volume attached to your instance.



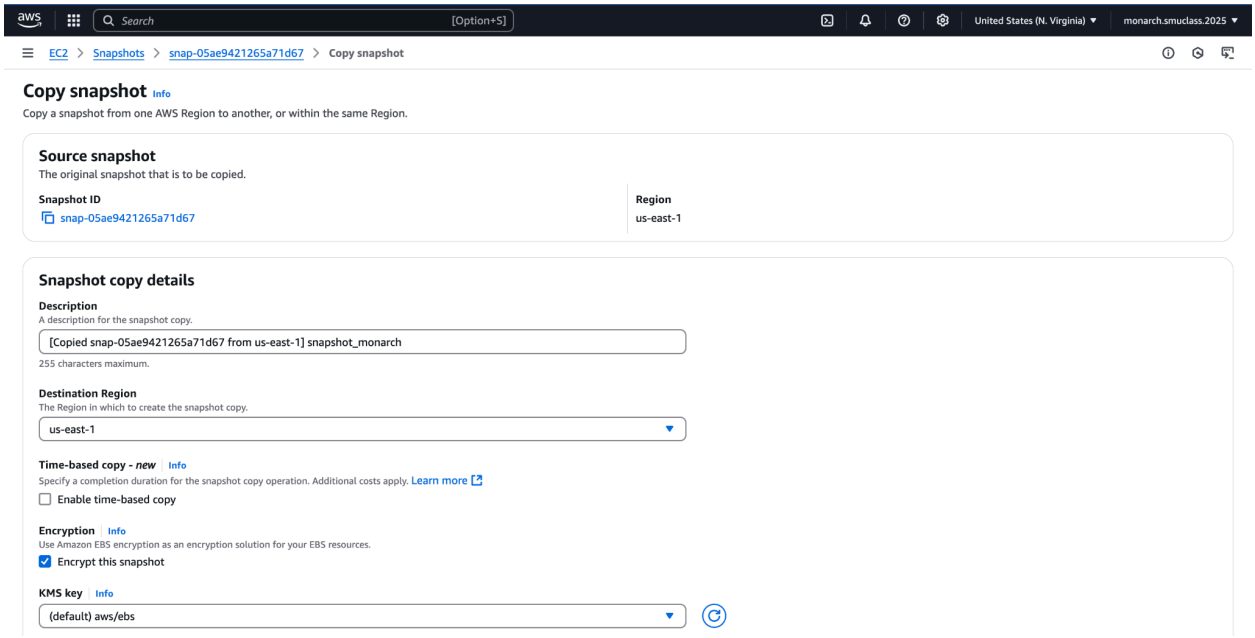
4. Under the Actions menu, click Create Snapshot. EBS will begin creating an unencrypted snapshot of the volume.



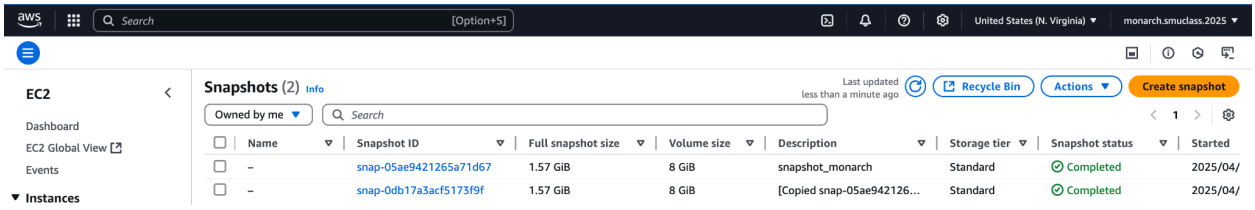
5. On the left-side menu, click Snapshots. Wait for the snapshot to complete.



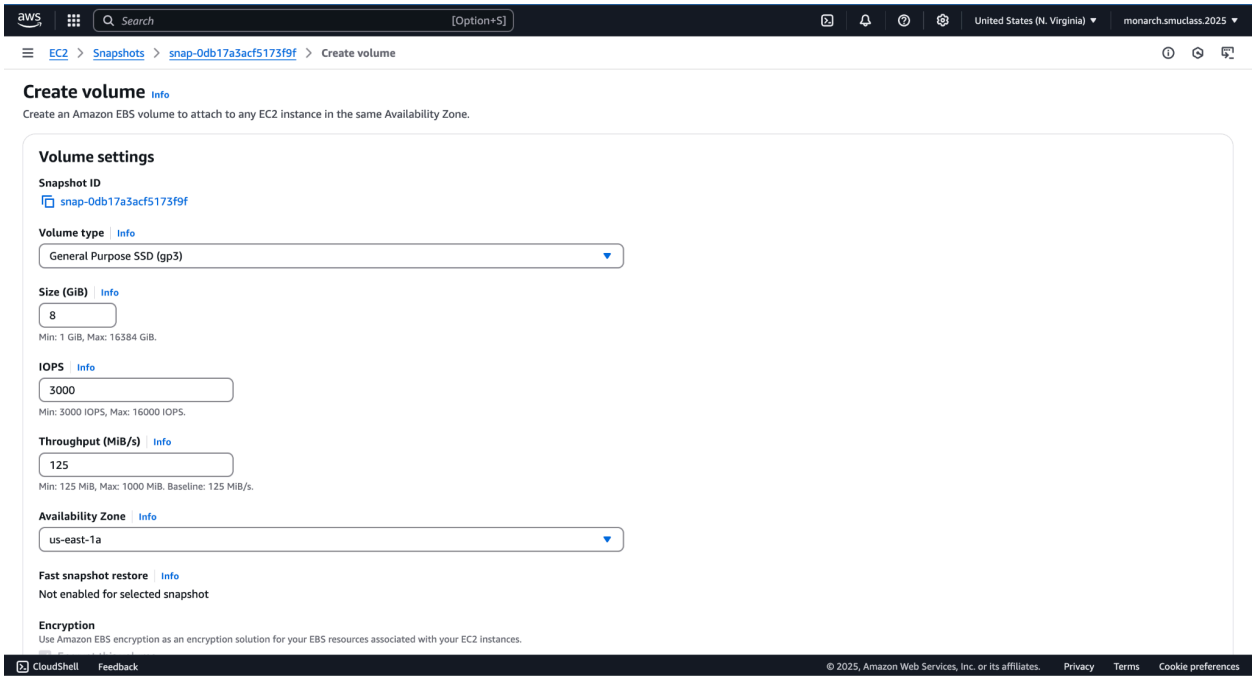
6. Select the snapshot and under the Actions menu, click Copy.
7. Select the Encrypt This Snapshot check box.
8. Next to the Master Key drop-down, select the KMS key you'd like to use to encrypt the snapshot. You can use your own customer master key or the default AWS/EBS key.



9. Click the Copy button. EBS will begin creating an encrypted copy of the snapshot. The larger the volume, the longer the encryption process takes. A good rule of thumb is about 3 gigabytes per minute.



10. Select the encrypted snapshot and under the Actions menu, click Create Volume.
11. Choose the volume type, size, and availability zone, which can be different than the original volume.



12. Click the Create Volume button. The new volume will be encrypted using the same key that was used to encrypt the snapshot.