ATTACK DEFENSE

by PentesterAcademy

Name	EC2 Unencrypted EBS disks
URL	https://attackdefense.com/challengedetails?cid=2452
Type	AWS Cloud Security : EC2

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

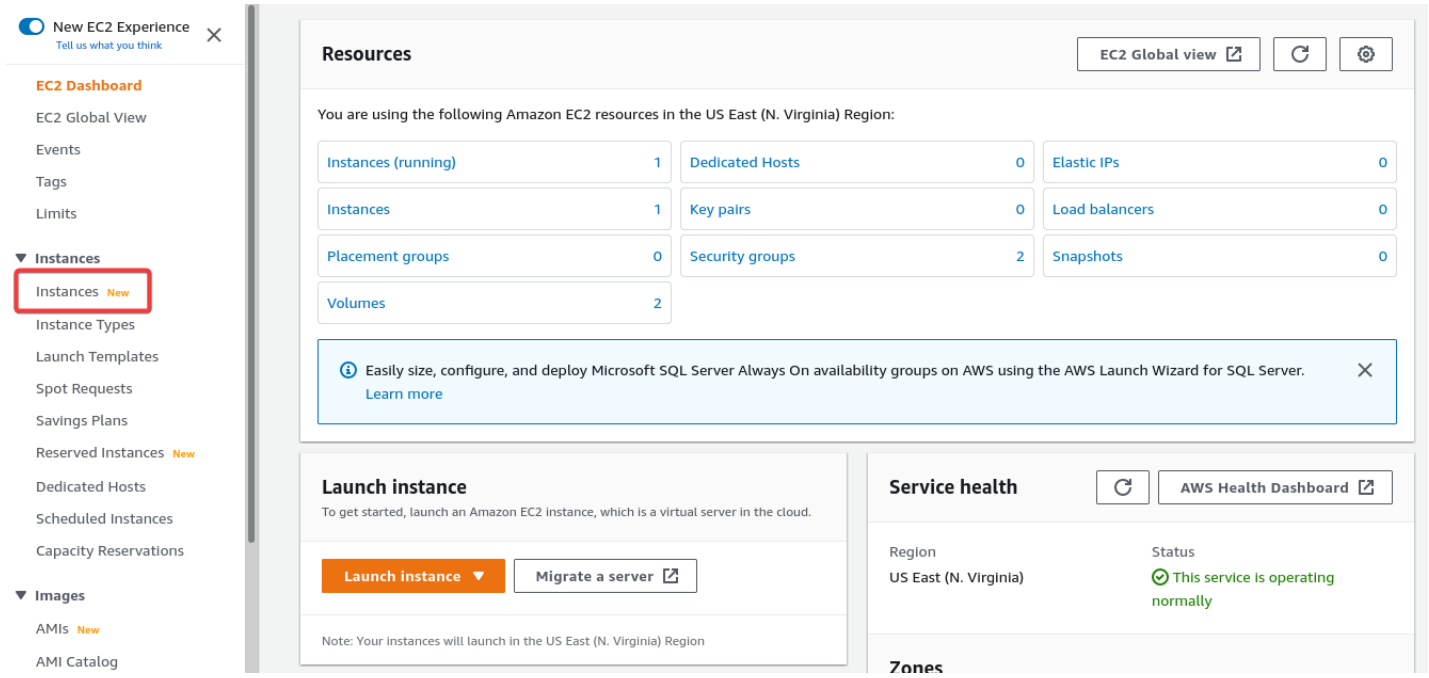
Solution:

Step 1: Click on the lab link button to get access credentials. Login to aws console.

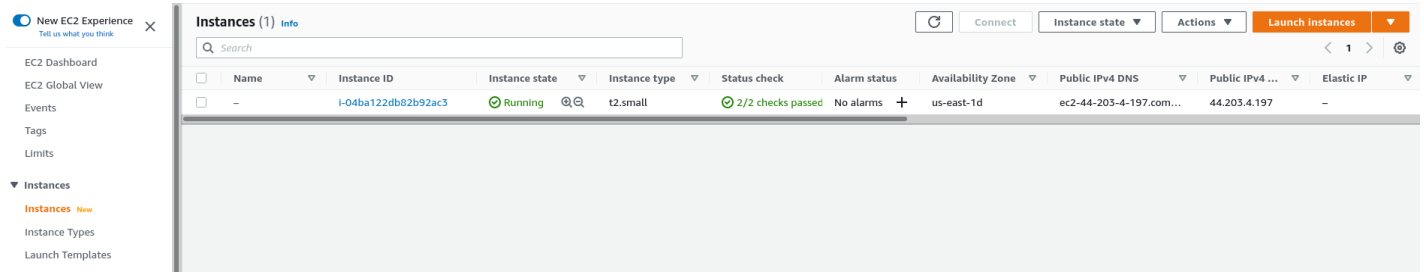
Access Credentials to your AWS lab Account

Login URL	https://854627651693.signin.aws.amazon.com/console
Region	US East (N. Virginia) us-east-1
Username	mark
Password	Ad4V8cMTkeYRA5a3

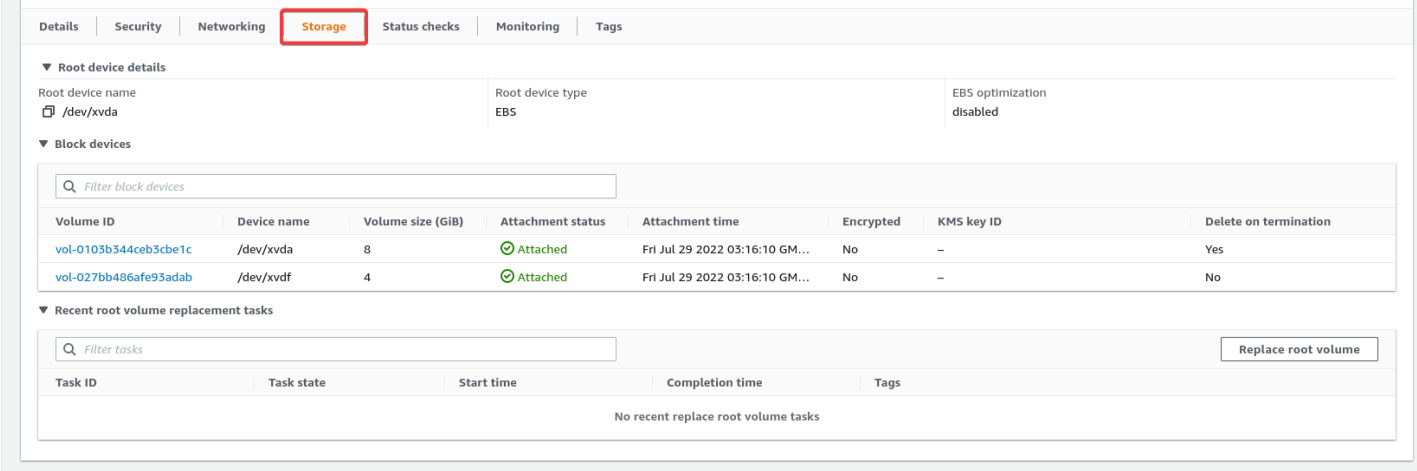
Step 2: Navigate to the EC2 dashboard and click on instances.



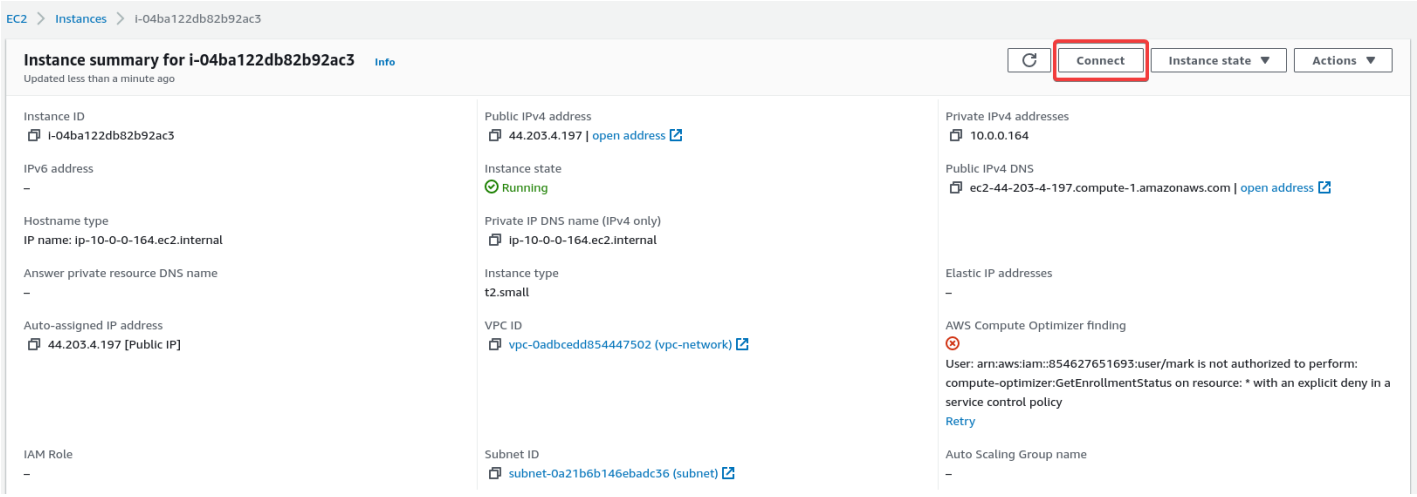
Step 3: Click on instance id and find the storage details.



Step 4: Click on storage.



Step 5: Try to connect with the instance.



Try to connect instance with EC2 Instance connect.

EC2 > Instances > i-04ba122db82b92ac3 > Connect to instance

Connect to instance Info

Connect to your instance i-04ba122db82b92ac3 using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID

i-04ba122db82b92ac3

Public IP address

44.203.4.197

User name

root

Connect using a custom user name, or use the default user name root for the AMI used to launch the instance.

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel | Connect

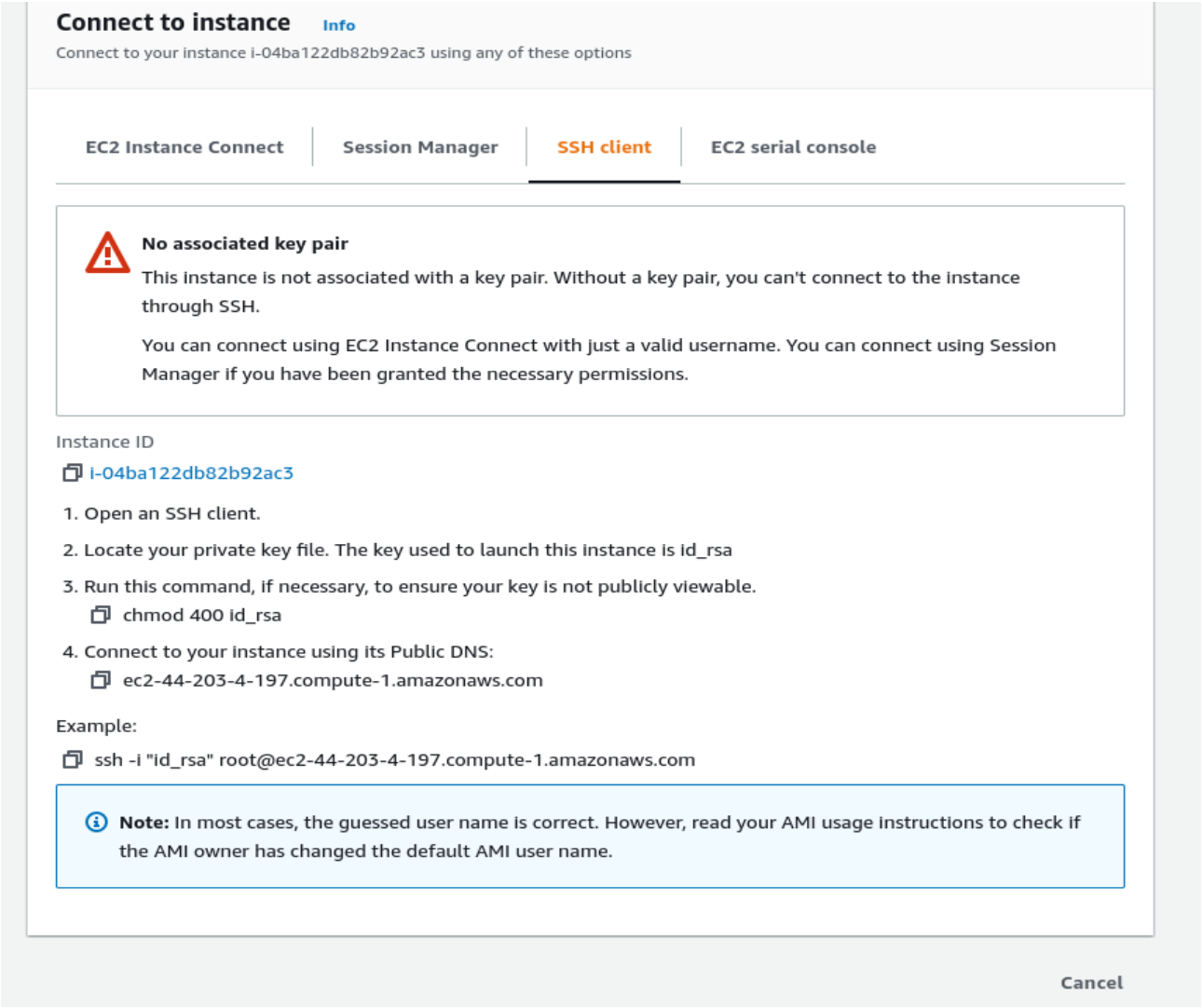
User does not have access to the instance.

aws | Services | Search for services, features, blogs, docs, and more [Alt+S]

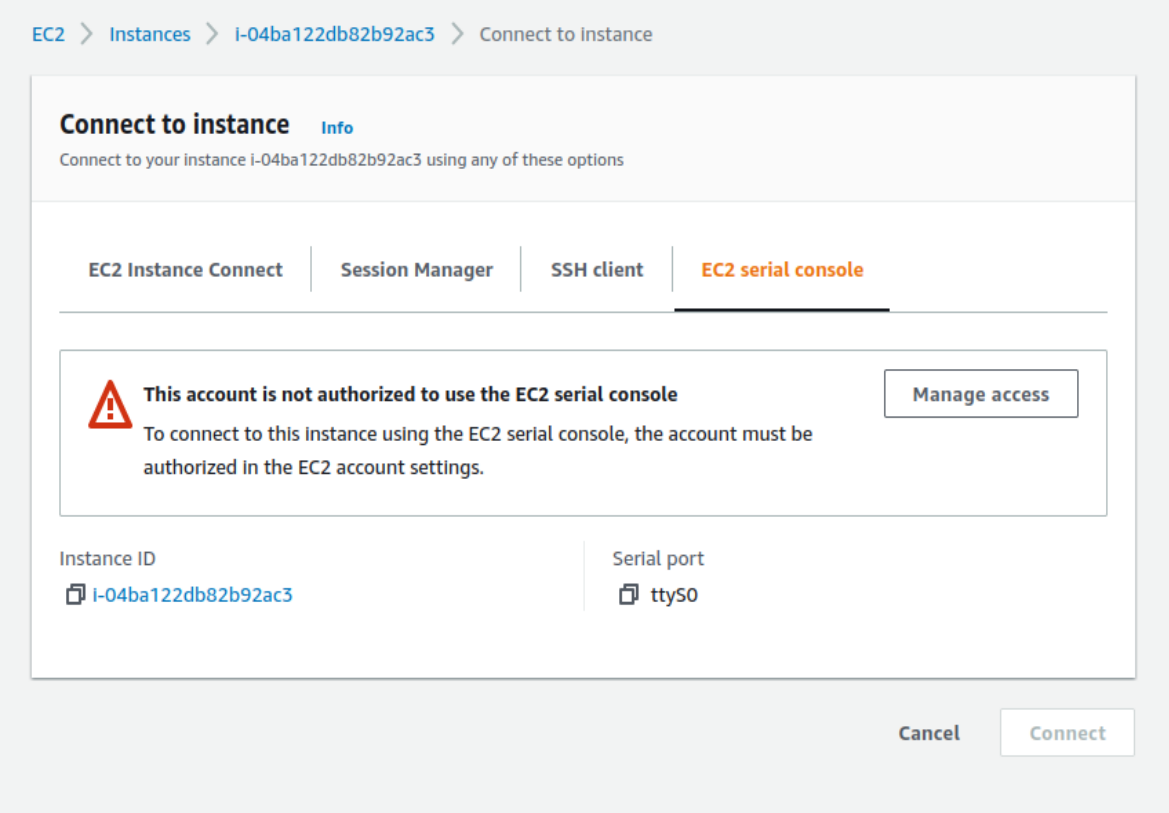
Failed to connect to your instance

Access denied by EC2 Instance Connect. Either your AWS credentials are not valid or you do not have access to the EC2 instance.

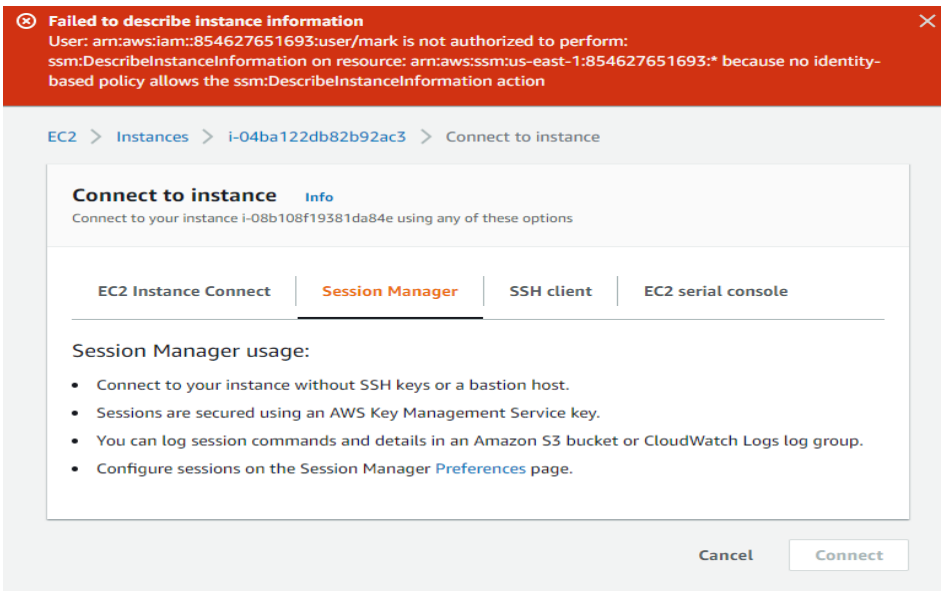
Key pair is not created. So the connection to EC2 instance with the SSH client is not possible.



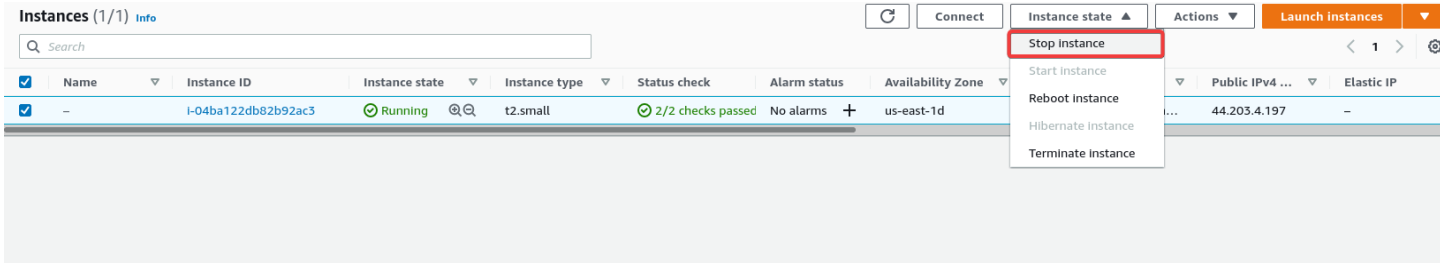
EC2 serial console is not authorized to connect with the instance.



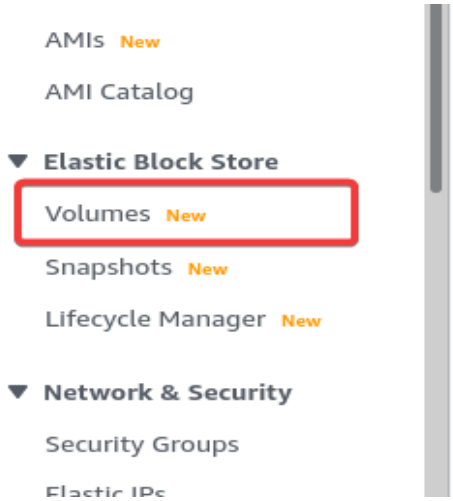
SSM is not authorized to connect with the instance. So this states that there is no access to the instance. Thus we cannot check the data inside volumes.



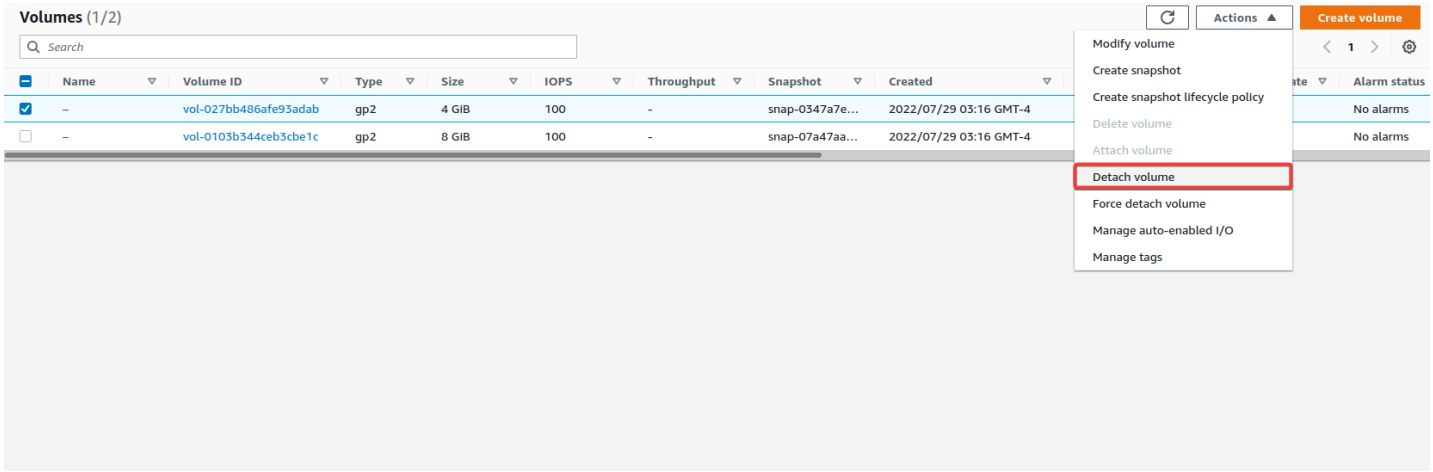
Step 6: Stop the running instance.



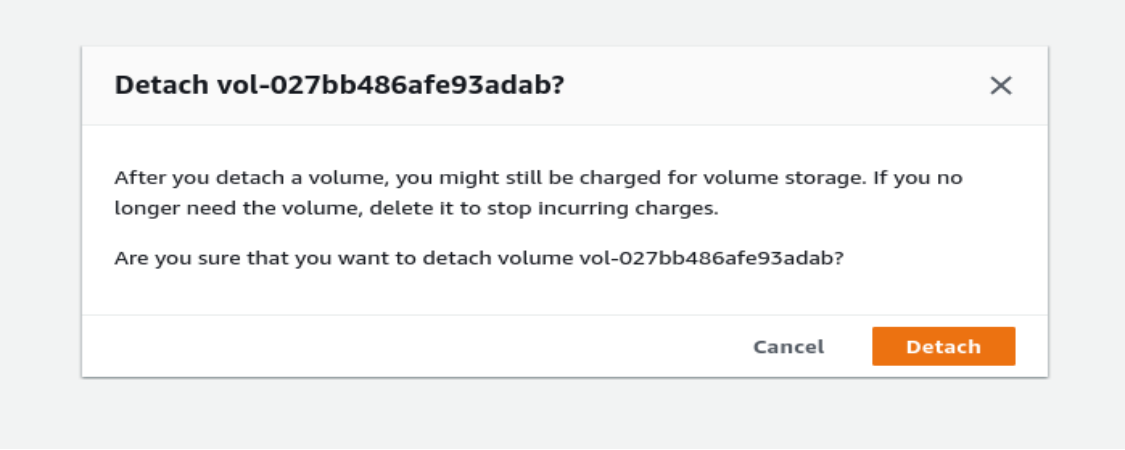
Step 7: Navigate to volumes.



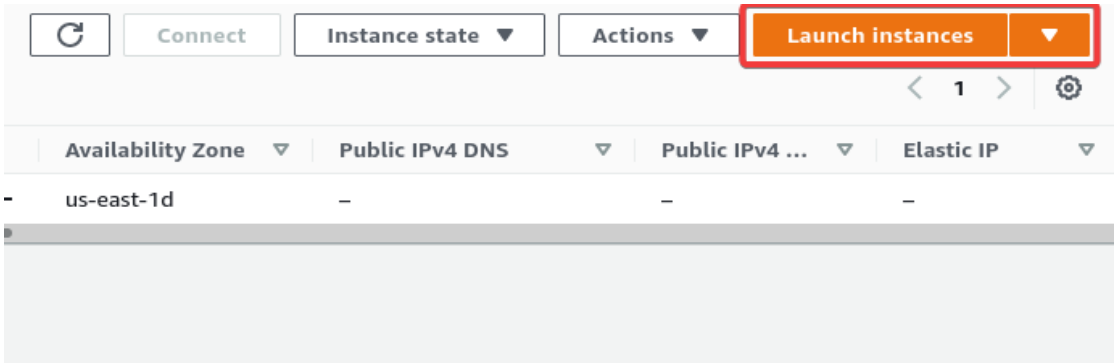
Step 8: Detach the additionally attached volume from the instance.



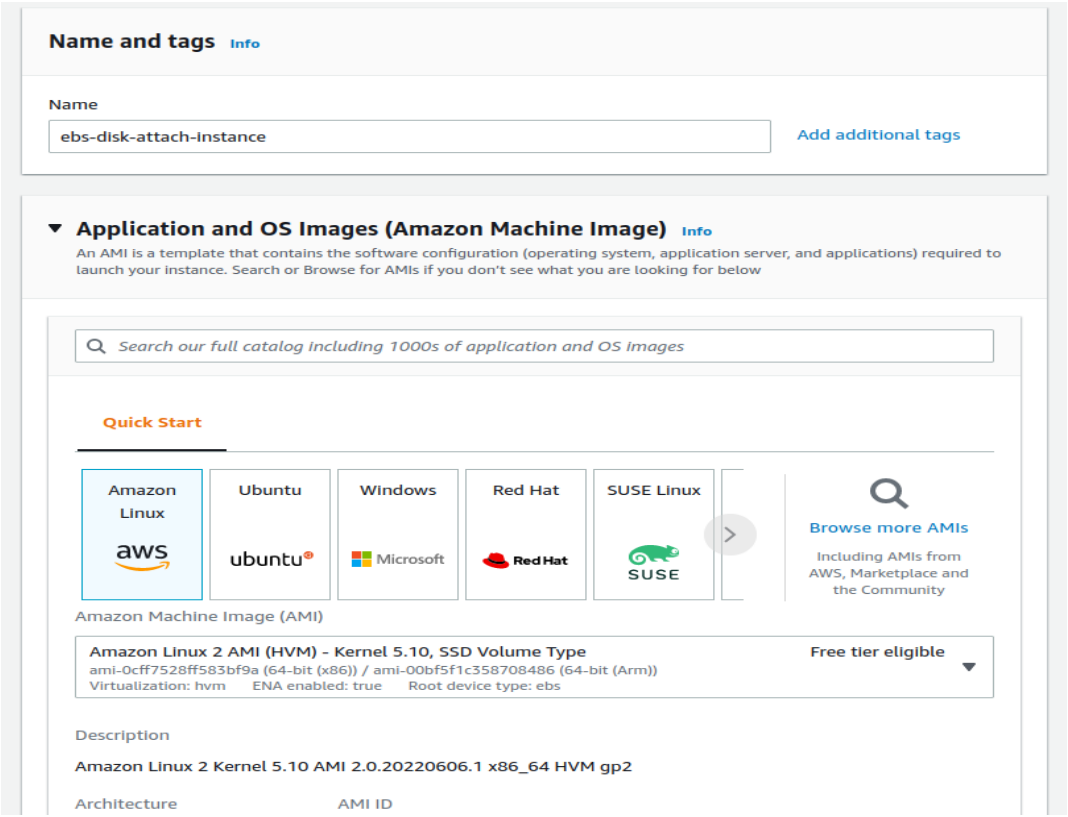
Step 9: Click on detach.



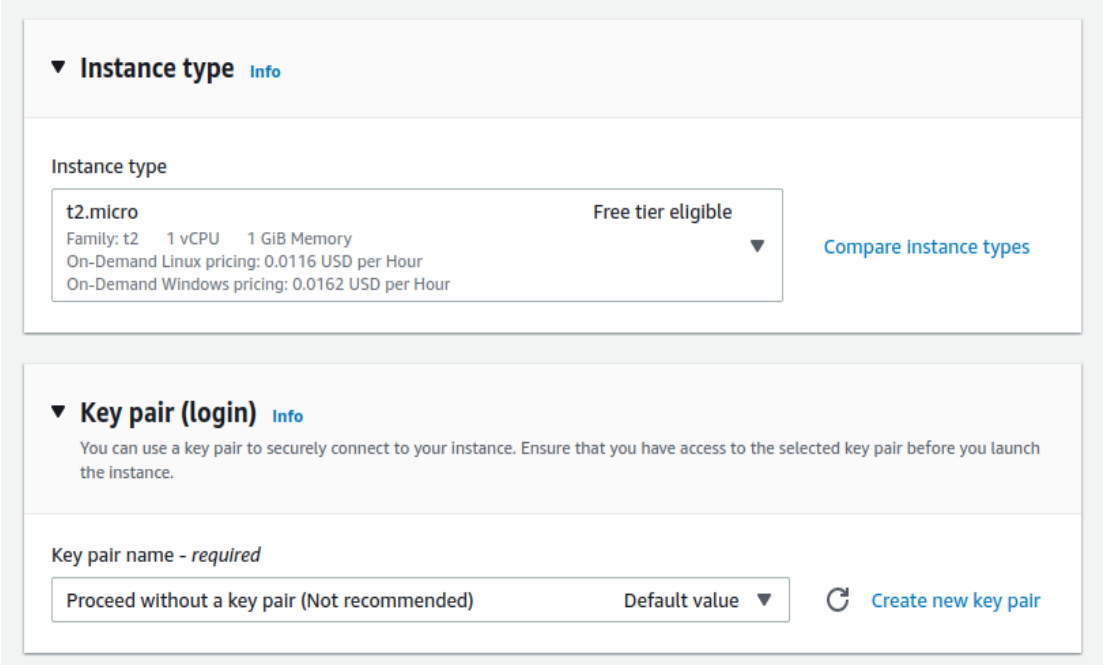
Step 10: Now create a new instance and attach the detached volume and retrieve the data from it. Navigate back to the instance and click on launch instance.



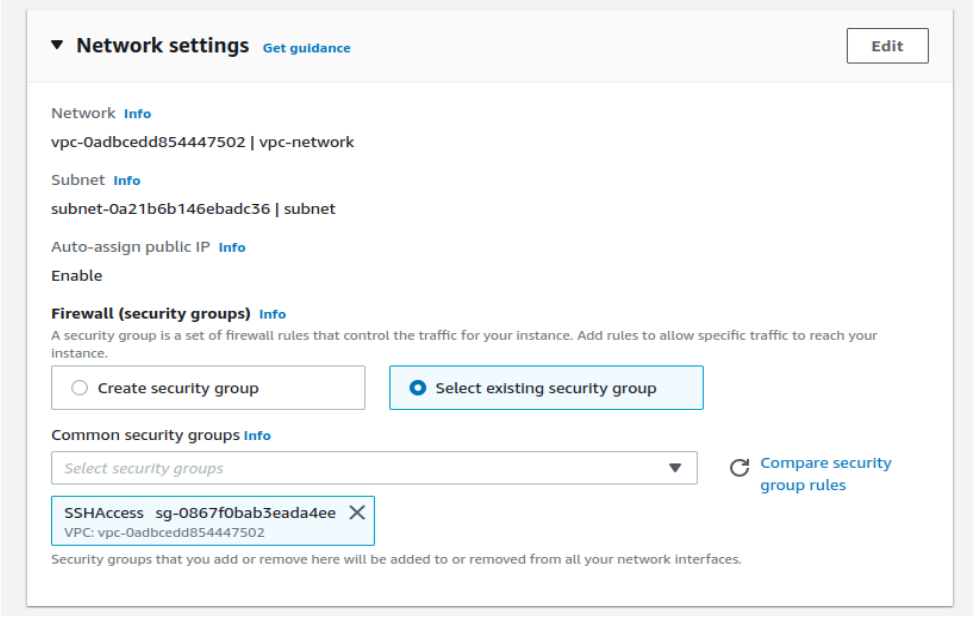
Step 11: Set a name and select amazon Linux as AMI.



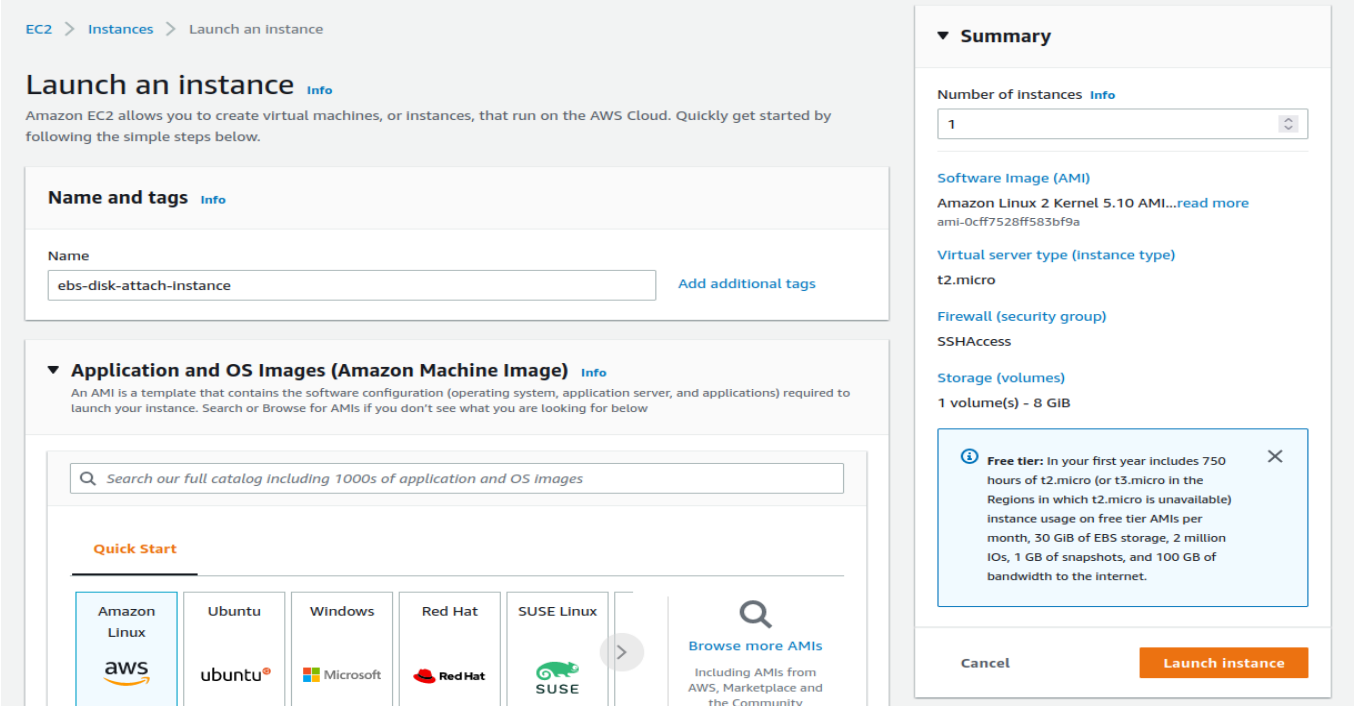
Step 12: Set instance type to t2.micro and proceed without key pair.



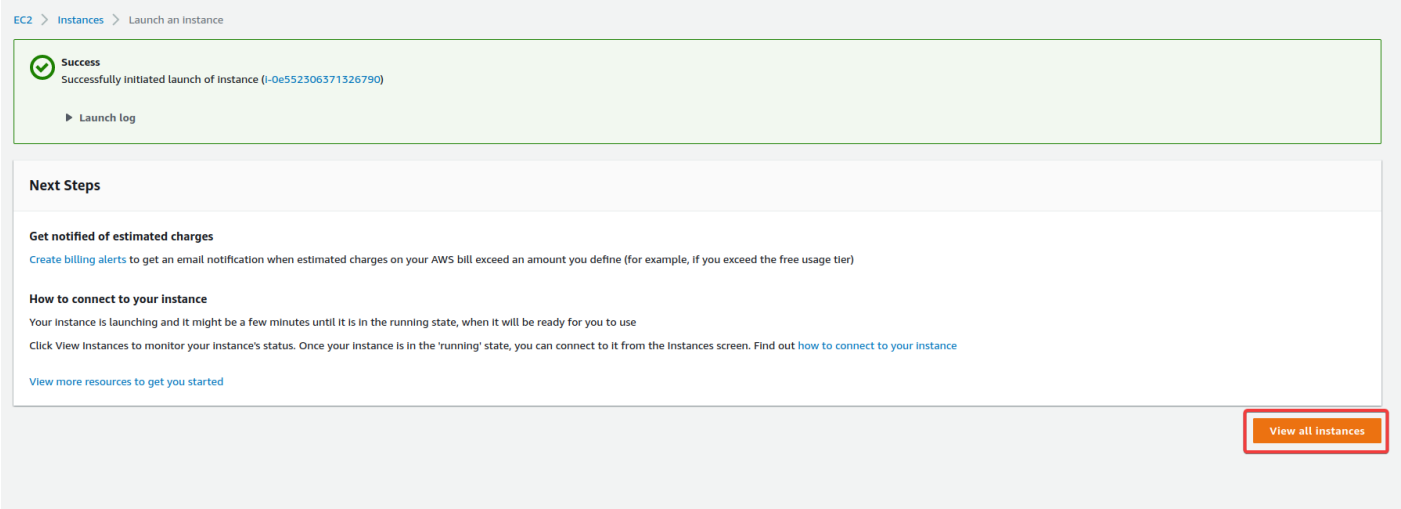
Step 13: Select "SSHAccess" as the security group.



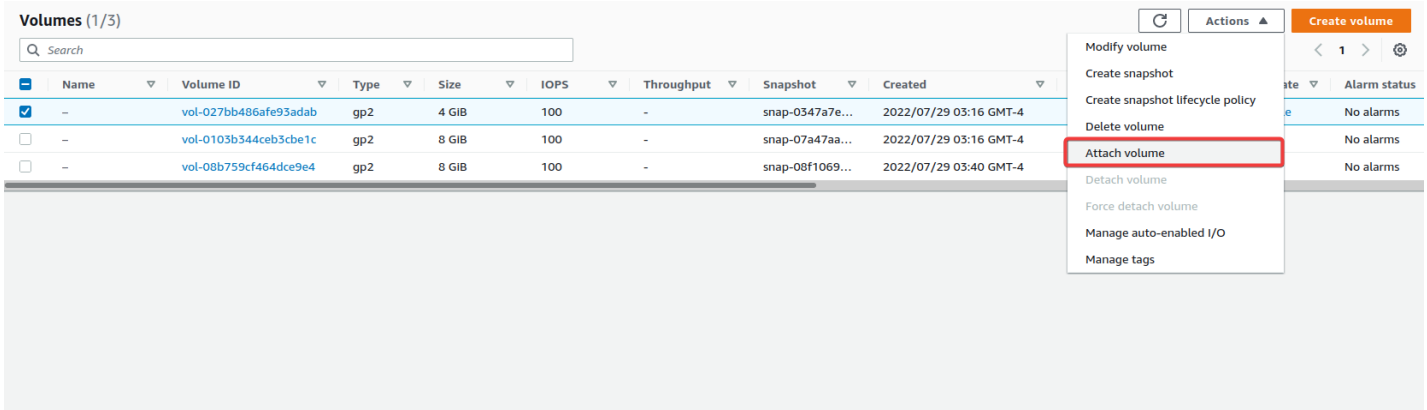
Step 14: Leave other settings as default and click on Launch instance.



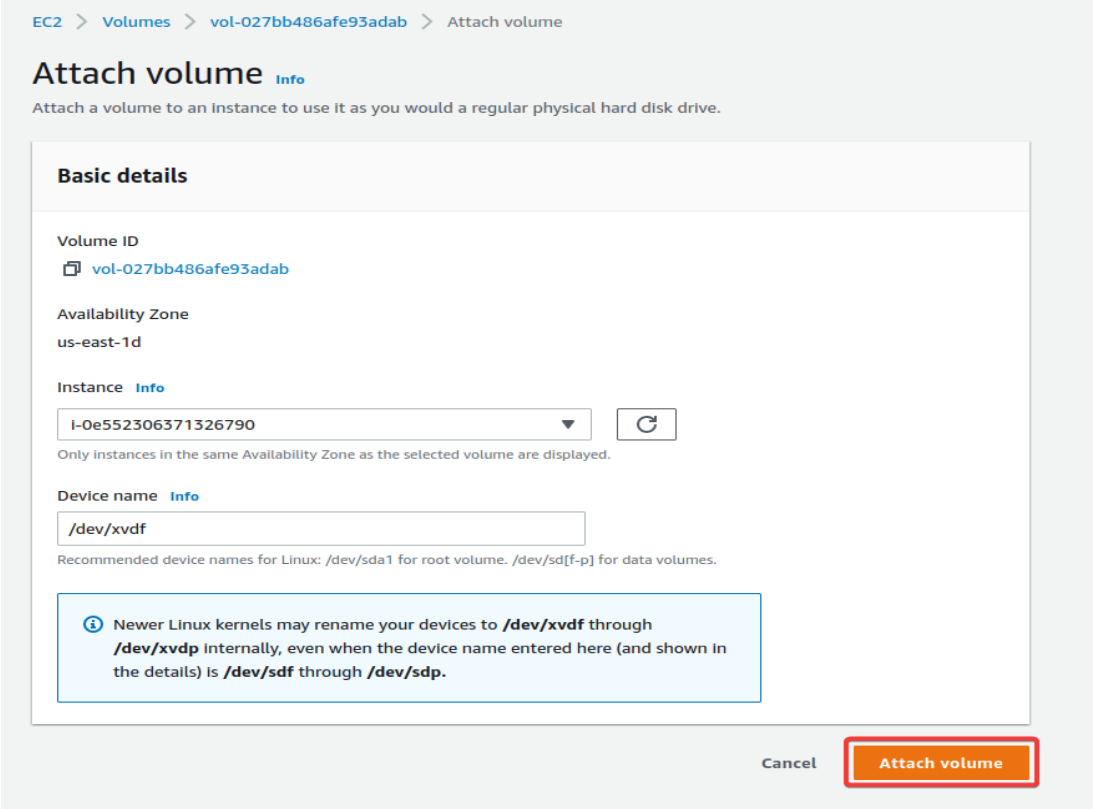
Successfully initiated the launch of instance. Now click on View all instances.



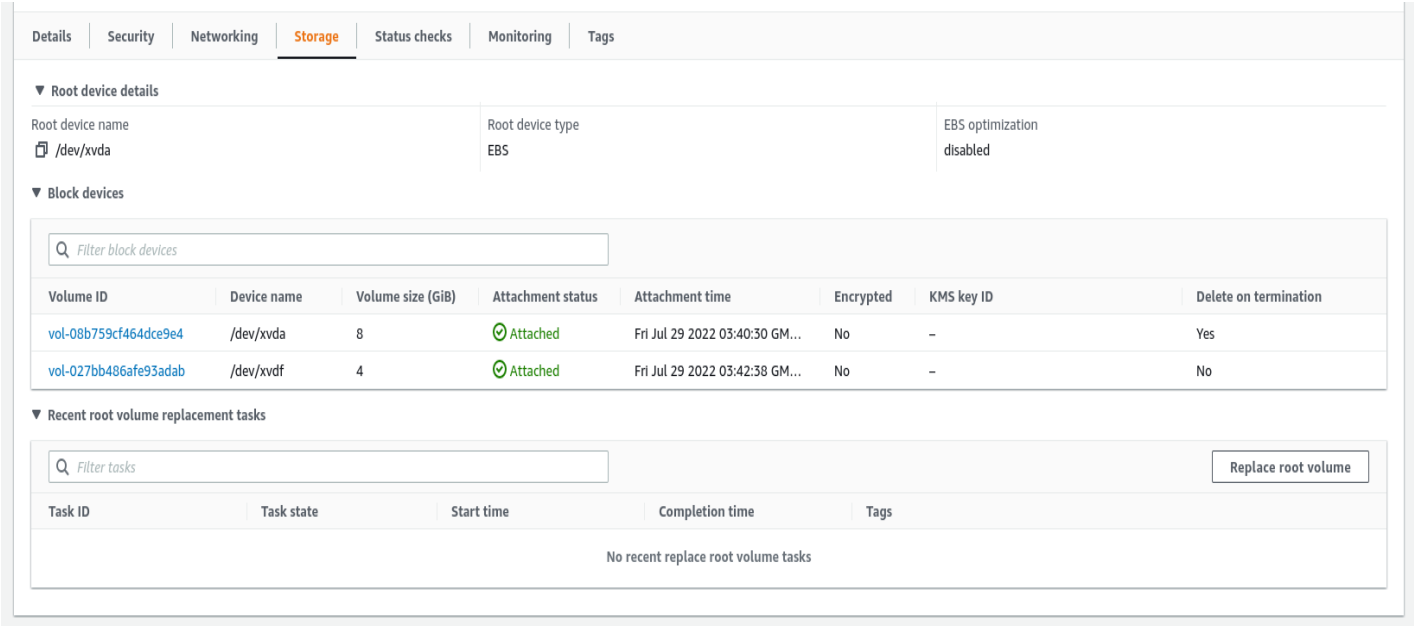
Step 15: Navigate back to volumes and select the detached volume. Click on attach from the actions drop-down.



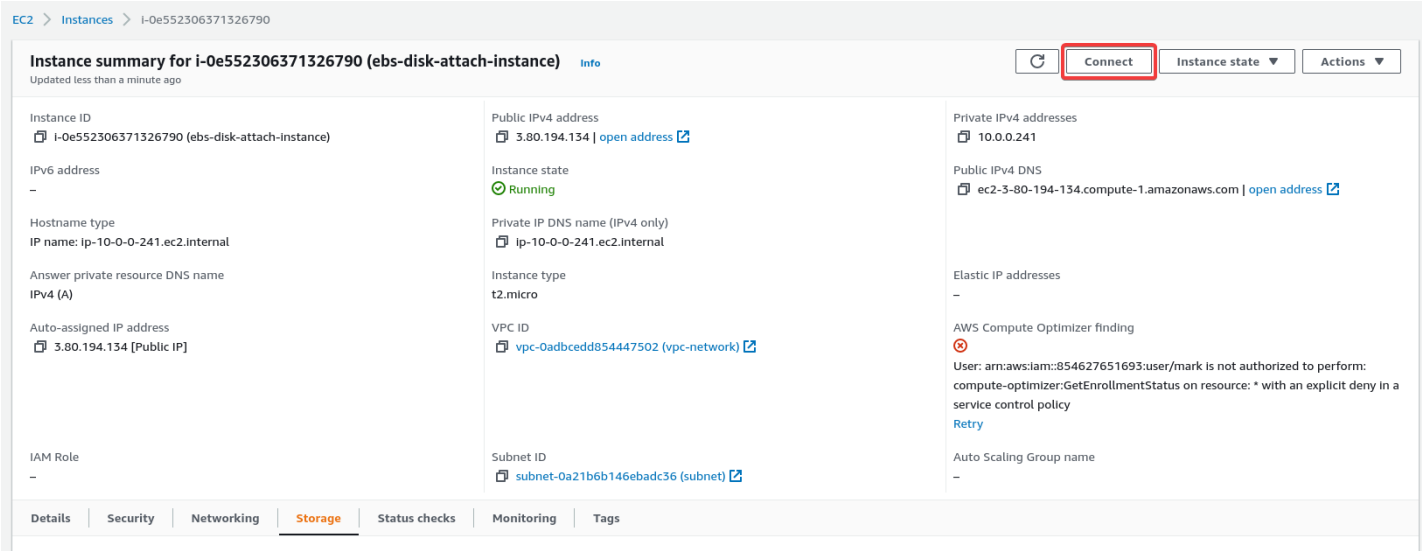
Step 16: Attach the volume with the newly created instance.



Now the volumes will list in the storage section of EC2 instance.



Step 17: Navigate back to instances and try to connect with the created instance using EC2 instance connect.



Click on connect.

EC2 > Instances > i-0e552306371326790 > Connect to instance

Connect to instance Info

Connect to your instance i-0e552306371326790 (ebs-disk-attach-instance) using any of these options

EC2 Instance Connect | Session Manager | SSH client | EC2 serial console

Instance ID

i-0e552306371326790 (ebs-disk-attach-instance)

Public IP address

3.80.194.134

User name

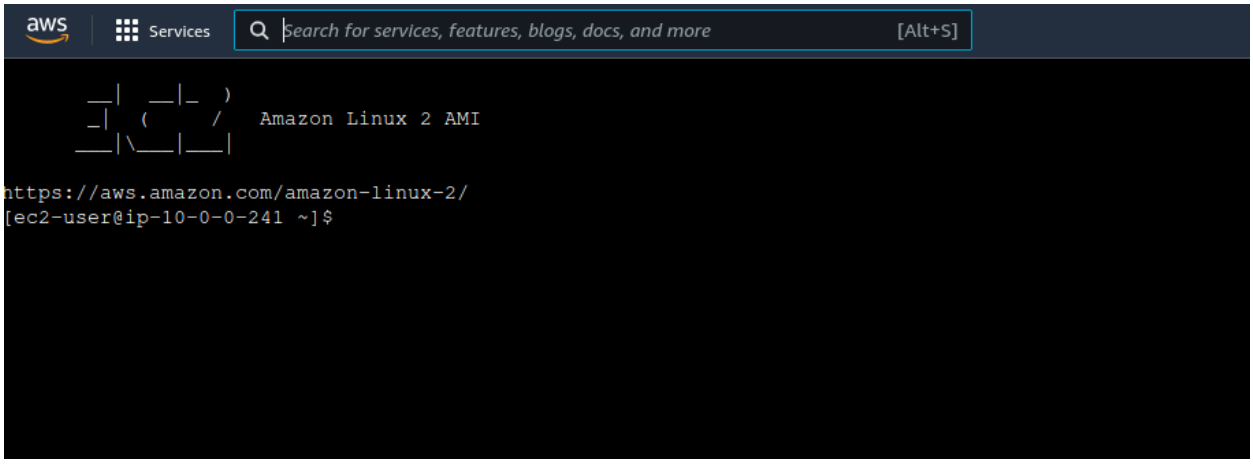
ec2-user

Connect using a custom user name, or use the default user name ec2-user for the AMI used to launch the instance.

Note: In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel Connect

Successfully connected to the instance.



Step 18: List the available volumes.

Command: lsblk

Step 19: Check the file system of the attached disk.

Command: sudo file -s /dev/xvdf

```
[ec2-user@ip-10-0-0-241 ~]$ sudo file -s /dev/xvdf
/dev/xvdf: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
[ec2-user@ip-10-0-0-241 ~]$
```

Step 20: Create a mount point directory for the volume and mount the volume at that directory. Now this will mount the data present inside the volume to the data folder in the root.

Command: sudo mkdir /data
sudo mount /dev/xvdf /data

```
[ec2-user@ip-10-0-0-241 ~]$ sudo mkdir /data
[ec2-user@ip-10-0-0-241 ~]$ sudo mount /dev/xvdf /data
[ec2-user@ip-10-0-0-241 ~]$
```

Step 21: Retrieve the flag.

Command: ls /data
cat /data/flag

```
[ec2-user@ip-10-0-0-241 ~]$ ls /data
flag
[ec2-user@ip-10-0-0-241 ~]$ cat /data/flag
1a0c77264e3e32c9e5cd777cd55f8c83
[ec2-user@ip-10-0-0-241 ~]$
```

Flag: 1a0c77264e3e32c9e5cd777cd55f8c83

References:

1. AWS EC2 documentation (https://docs.aws.amazon.com/ec2/index.html)