Placement Empowerment Program

Cloud Computing and DevOps Centre

Back Up and Restore a Cloud Instance : Take a snapshot of your cloud VM. Terminate the VM and restore it from the snapshot.

Name: Vignesh V

Department: CSE

Introduction

In today's cloud-driven world, ensuring data availability and reliability is paramount. This Proof of Concept (POC) focuses on the Backup and Restore process for a cloud instance, showcasing how critical data can be safeguarded and restored efficiently in AWS. By taking a snapshot, terminating the instance, and restoring it from the snapshot, this POC demonstrates the ease and reliability of AWS Elastic Block Store (EBS).

Overview

This POC involves working with Amazon Web Services (AWS) to perform the following tasks:

1. Launching an EC2 instance.
2. Creating an EBS snapshot of the instance's volume to back up its data.
3. Terminating the instance to simulate a failure or cost-saving scenario.
4. Restoring the instance using the snapshot by creating a new volume and attaching it to a new EC2 instance.

The step-by-step approach ensures no unnecessary charges while maintaining data integrity and availability.

Objective

The objective of this POC is to:

1. Demonstrate the process of creating and managing backups in AWS.
2. Explore the capabilities of EBS snapshots for disaster recovery.
3. Understand how to restore a terminated instance and verify data integrity.
4. Highlight cost-saving techniques using AWS Free Tier while ensuring operational readiness.

Importance

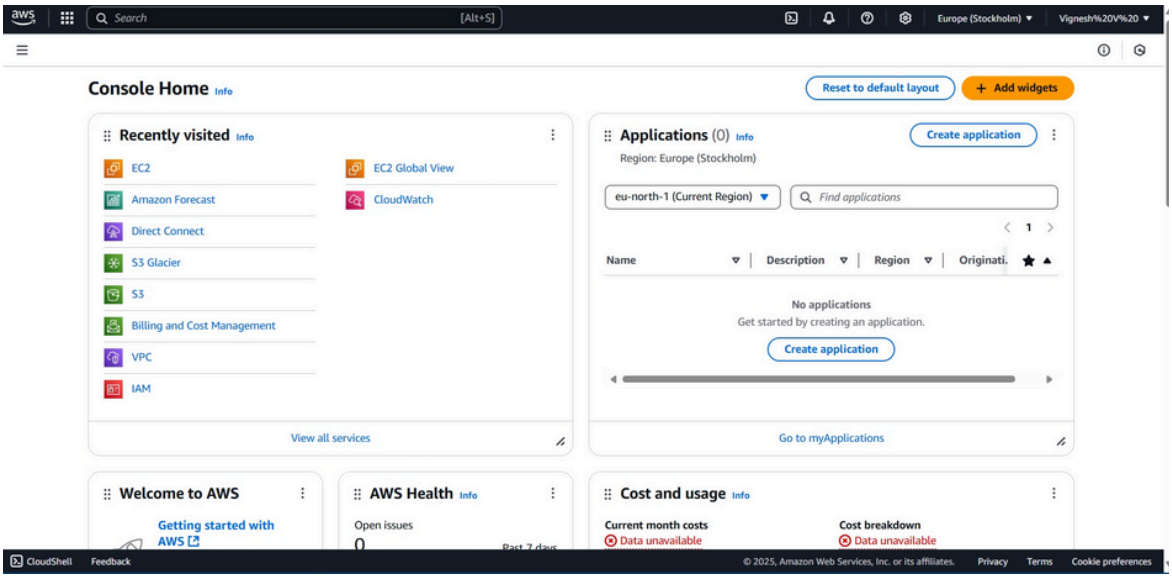
1. Disaster Recovery: Ensures that critical data can be restored quickly in case of an unexpected failure.
2. Cost Optimization: Demonstrates terminating unused instances and restoring them only when required.
3. Scalability and Flexibility: Showcases AWS's ability to manage snapshots and volumes across regions and availability zones.
4. Practical Knowledge: Provides hands-on experience in working with EC2, EBS, and snapshot-based recovery processes.

Step-by-Step Overview

Step 1:

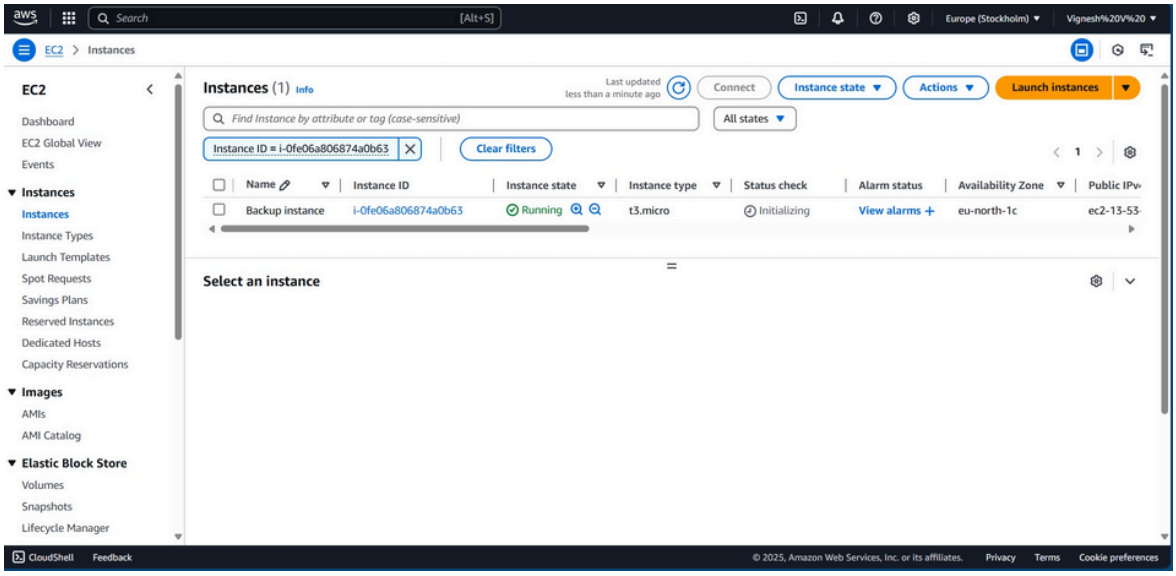
1. Go to AWS Management Console.

2. Enter your username and password to log in.



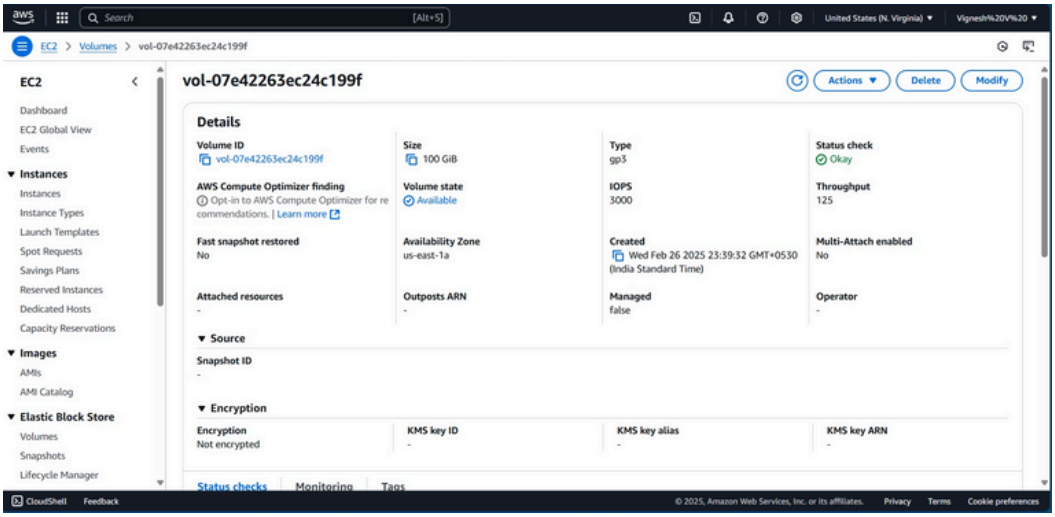
Step 2:

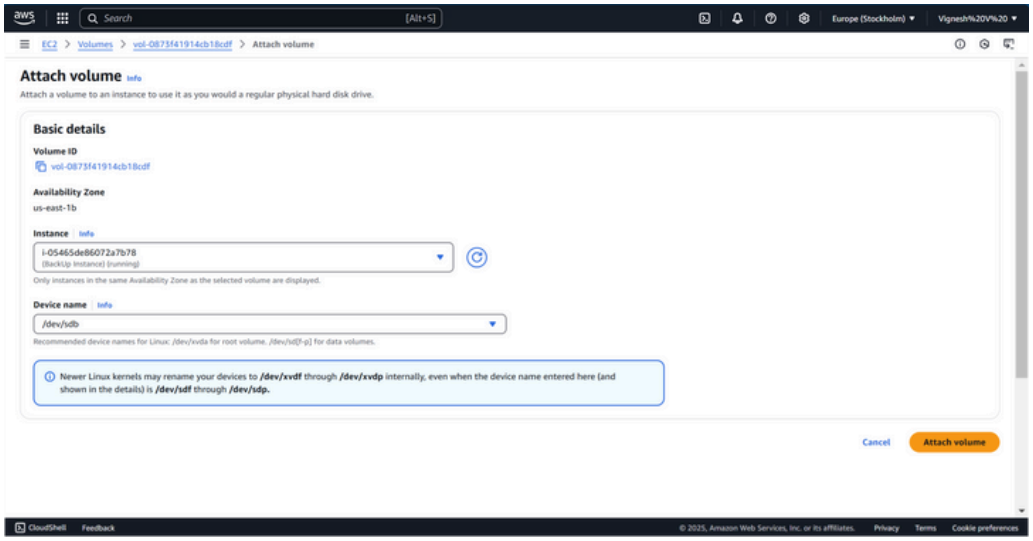
Launch an Ec2 instance.(Backup Instance)



Step 3:

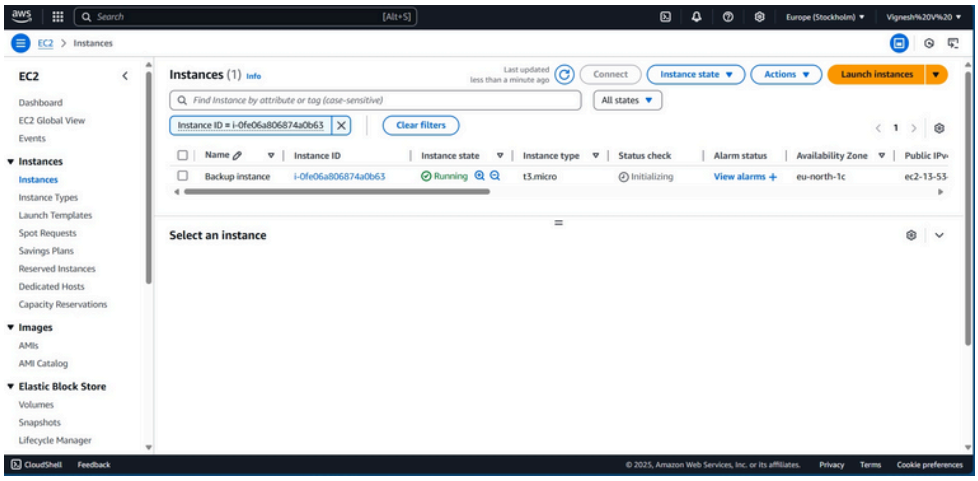
To create a new EBS volume in AWS, go to the EC2 Dashboard in the AWS Management Console by selecting EC2 from the Services menu. In the left-hand menu, under Elastic Block Store, click on Volumes, then click the Create Volume button. Select General Purpose SSD (gp3) for the volume type, set the size (e.g., 8 GiB, within Free Tier limits), and choose the availability zone that matches your EC2 instance (e.g., us-east-1b). Leave the other options as default, then click Create Volume. Be sure to note the Volume ID for future reference.

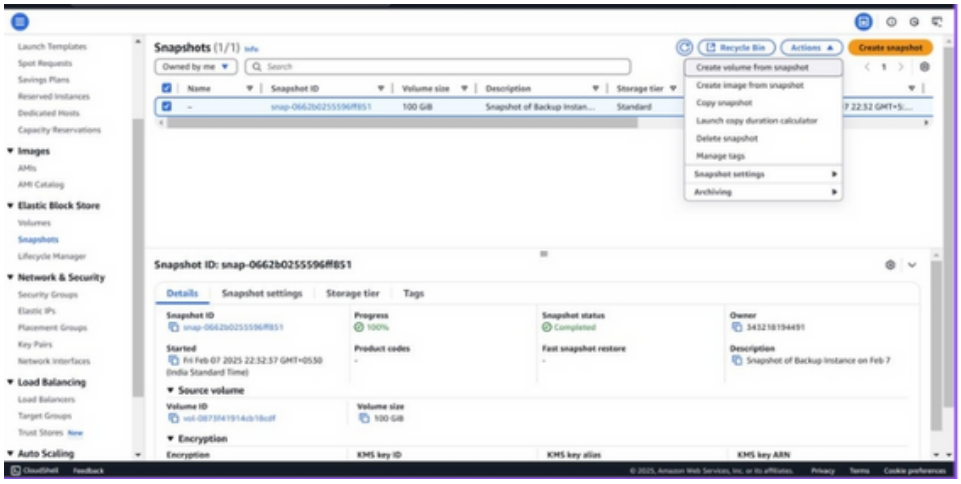




Step 4:

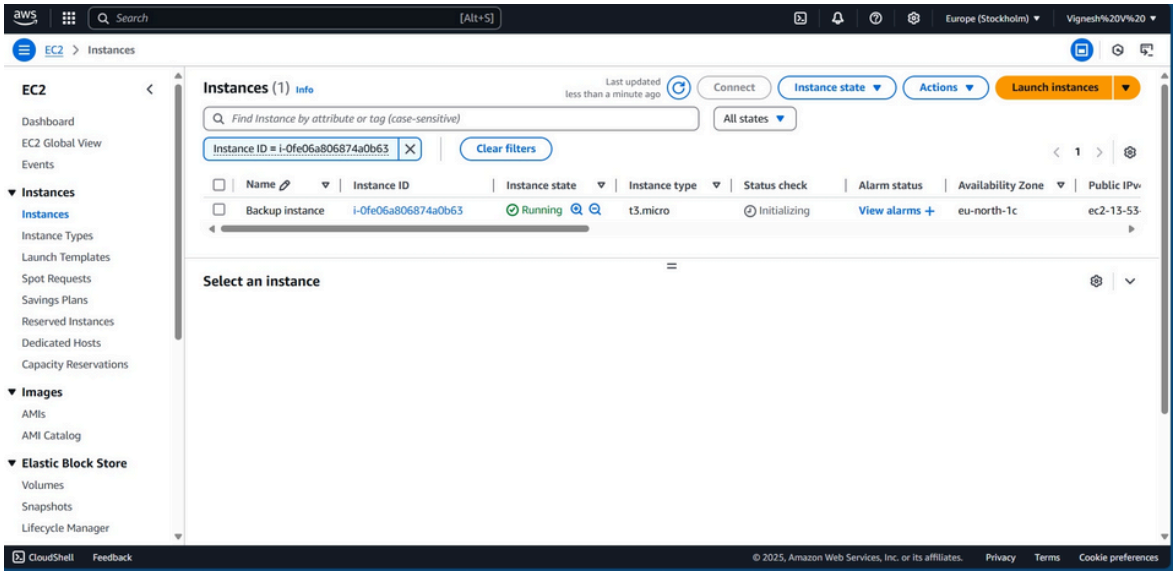
To create a snapshot of your EBS volume, navigate to the EC2 Dashboard in the AWS Management Console and click on Volumes under the Elastic Block Store section. Locate the volume attached to your instance (it should match the instance name or ID), select it, then click Actions > Create Snapshot. Add a meaningful description (e.g., "Snapshot of Backup Instance on Feb 7") and click Create Snapshot. To monitor its status, go to Snapshots under Elastic Block Store in the left menu and wait for the status to change to Completed.





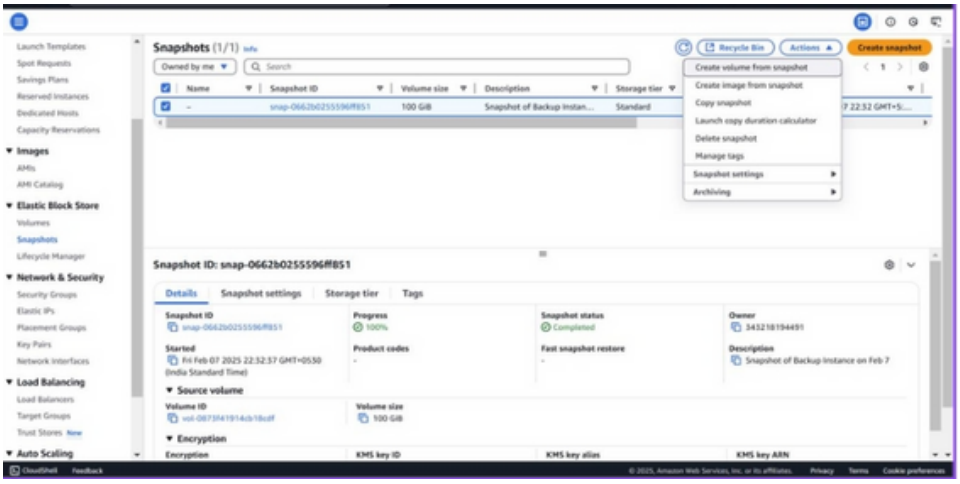
Step 5:

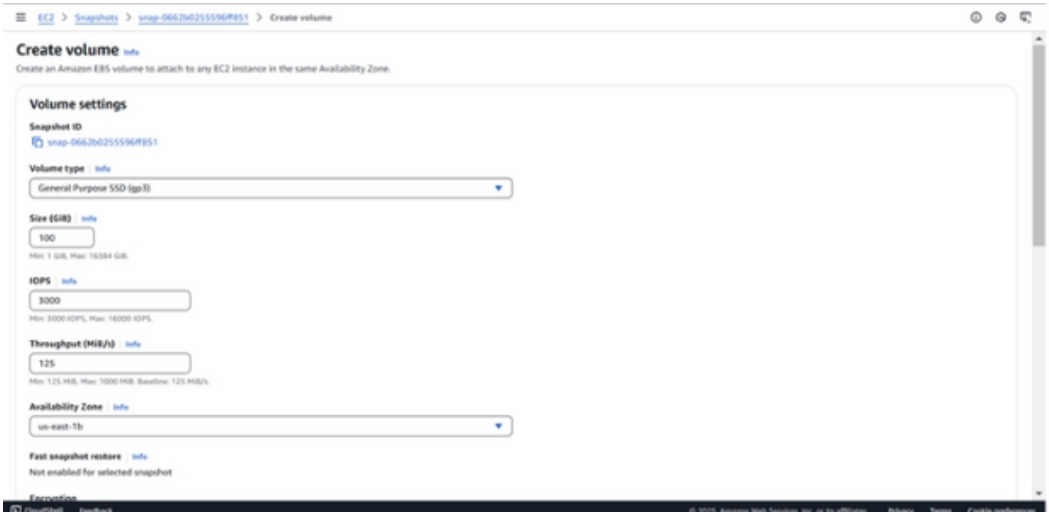
To terminate an EC2 instance, navigate to the EC2 Dashboard in the AWS Management Console and click on Instances under the Instances section. Locate the instance you want to terminate, then select it and click Actions > Instance State > Terminate Instance. Confirm the termination by clicking Terminate, and refresh the page after a few moments to see the instance state change to Terminated.



Step 6:

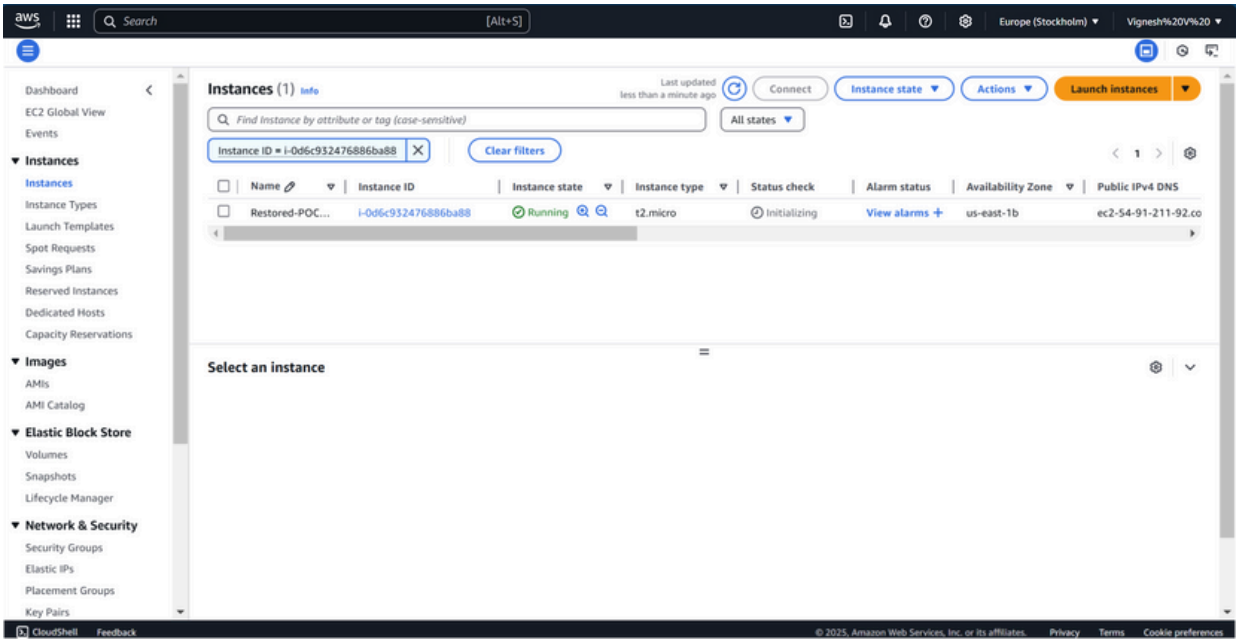
To create a new volume from the snapshot, go to the EC2 Dashboard and click on Snapshots under the Elastic Block Store section in the left menu. Select the snapshot you created earlier, then click Actions at the top and choose Create Volume. In the configuration settings, leave the Size as is (it will match the snapshot size) and select the same Availability Zone where you want to restore your instance (e.g., us-east-1a). Finally, click Create Volume to complete the process.





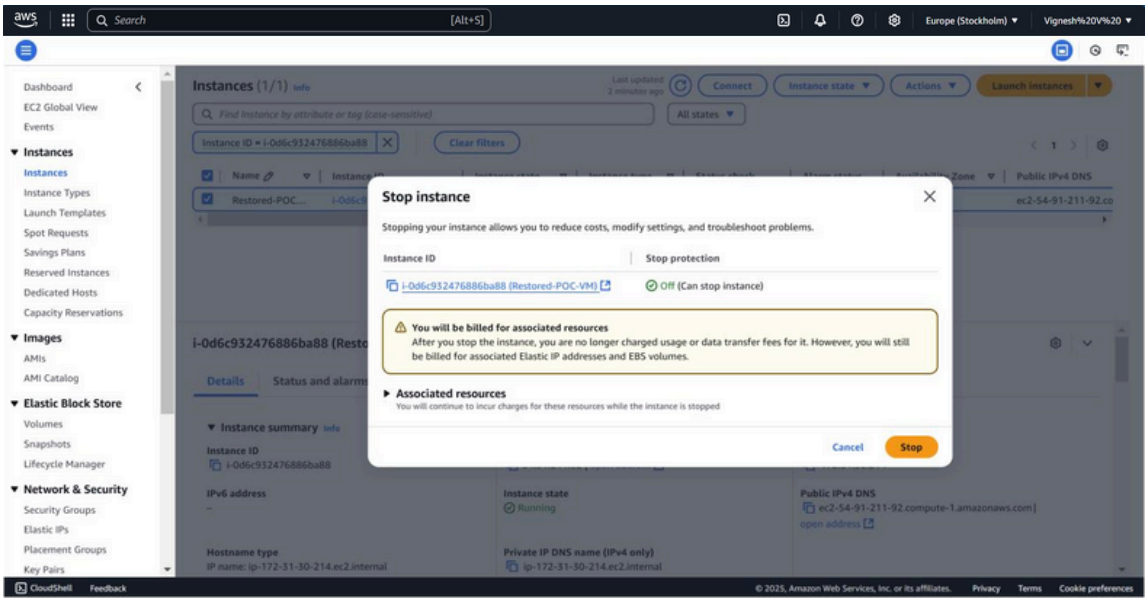
Step 7:

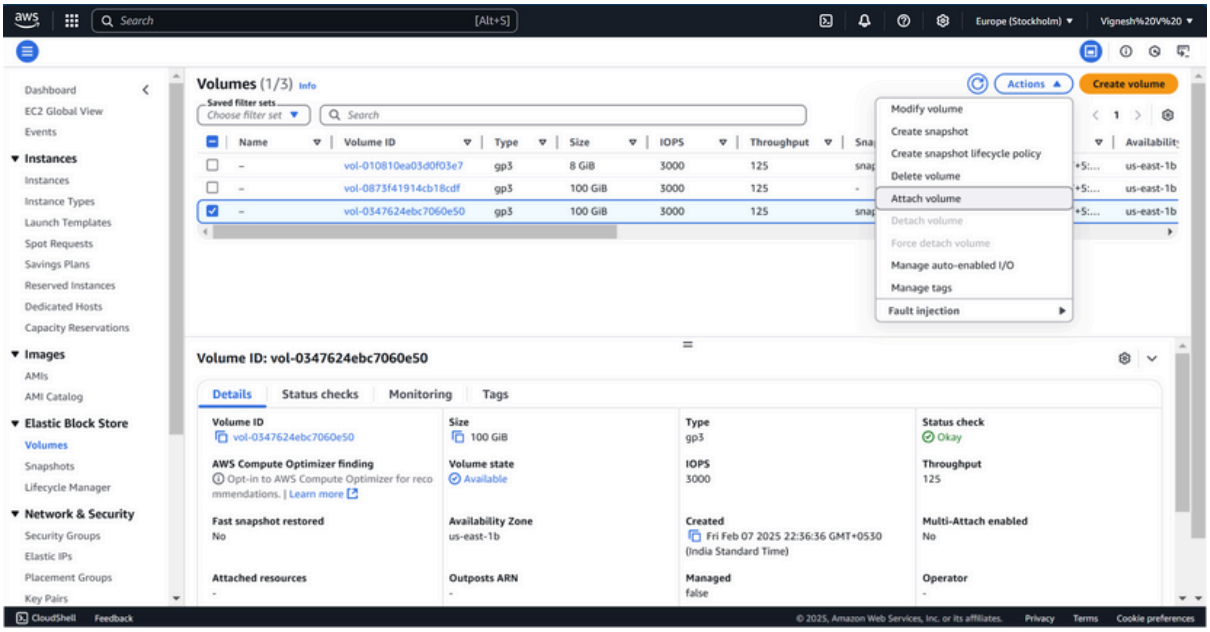
To launch a new instance, go to the EC2 Dashboard and click Launch Instances. Set the name of the new instance (e.g., Restored-POC- VM) and choose the same AMI (e.g., Amazon Linux 2023 Free Tier eligible) as the original instance. Select t2.micro for the instance type (Free Tier eligible). Configure the instance as needed, but skip the storage section for now.

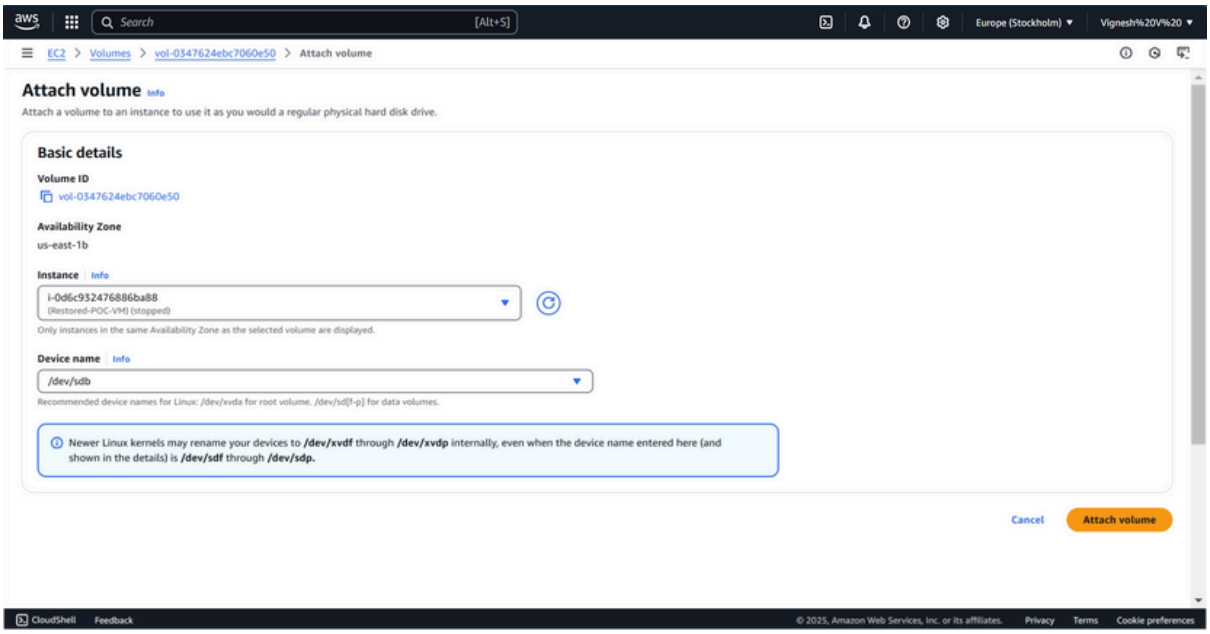


Step 8:

To attach the volume to the instance, first, stop the instance temporarily after it is launched by selecting the new instance, then click Actions > Instance State > Stop Instance. Next, go to Volumes in the left menu and select the new volume created from the snapshot. Click Actions > Attach Volume, and in the pop-up window, choose the new instance to attach the volume.







Verify the Restoration

1. Connect to the instance using SSH or other methods.

2. Check if the files, data, and configurations match the original setup.

POC is completed successfully:

1. Created a Snapshot of your instance.
2. Terminated the Instance to avoid extra charges.
3. Restored the Instance using the snapshot by creating a volume and attaching it to a new VM.

Outcome

By completing this POC of Back Up and Restore a Cloud Instance in AWS, you will:

1. Create and manage snapshots of EC2 instances, enabling easy backup of instance data without manual intervention.
2. Terminate instances while ensuring that important data remains intact through the backup snapshot.
3. Restore an instance from a snapshot by creating a new EBS volume and attaching it to a fresh EC2 instance.
4. Verify the restoration process, ensuring data integrity and proper functionality after the instance is restored.
5. Gain practical knowledge of AWS services like EC2, EBS snapshots, and how to use them for backup and recovery, which is vital for disaster recovery and business continuity in the cloud.