T Dinesh Kumar 23BIT023

Lab Experiment 3: AWS - Instance Management

Aim:

The objective of this experiment is to perform the following tasks using AWS EC2:

Procedure:

Step 1: Create and Launch an Instance

1. Log in to AWS Console:

Open a web browser and go to AWS Console.

Click on "Sign in to the Console" and enter your AWS credentials.

Navigate to the AWS EC2 Dashboard by searching for "EC2" in the search bar.

2. Launch an EC2 Instance:

In the EC2 dashboard, click on "Launch Instance".

Enter a name for the instance (e.g., "MyFirstEC2").

3. Select an Amazon Machine Image (AMI):

Choose "Amazon Linux 2023 AMI".

Click "Select" to proceed.

4. Choose an Instance Type:

Select "t2.micro" for free-tier eligibility (1 vCPU, 1GB RAM).

Click "Next: Configure Instance Details".

5. Configure Instance Details:

Leave default settings as they are.

Enable "Auto-assign Public IP" for internet access.

Click "Next: Add Storage".

6. Add Storage:

Keep the default root volume size (8GB) or modify as needed.

Set the volume type to "General Purpose SSD (gp3)".

Click "Next: Add Tags".

7. Add Tags (Optional):

Add a tag with Key = "Name" and Value = "MyEC2Instance".

Click "Next: Configure Security Group".

8. Configure Security Group:

Create a new security group (e.g., "MyEC2SecurityGroup").

Ensure SSH (port 22) is open, and add HTTP (port 80) or HTTPS (port 443) if hosting a web server.

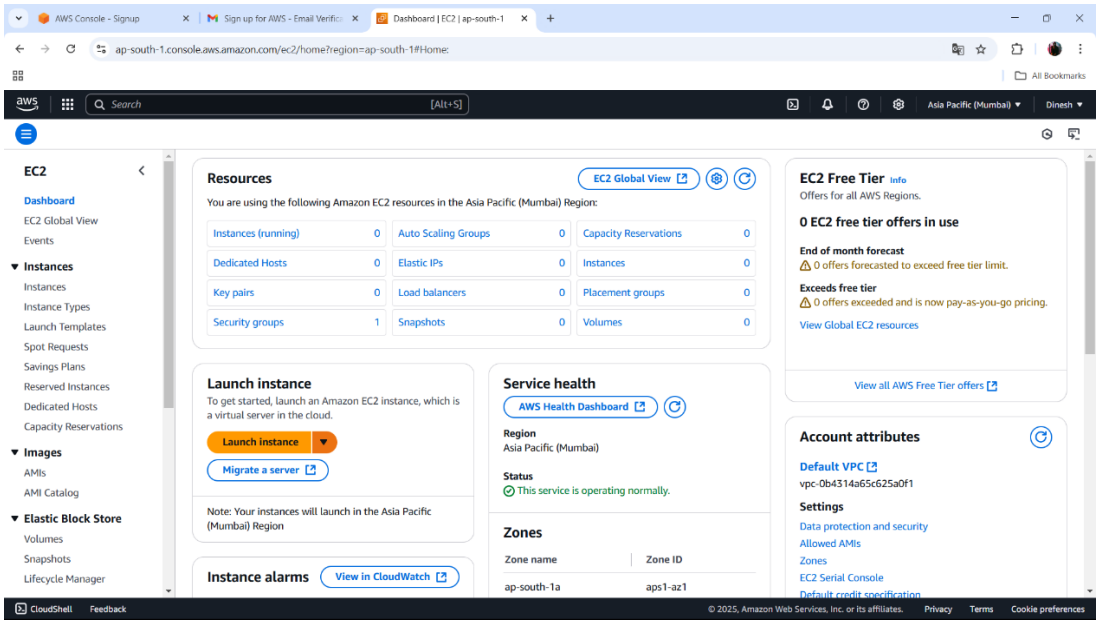
Click "Review and Launch".

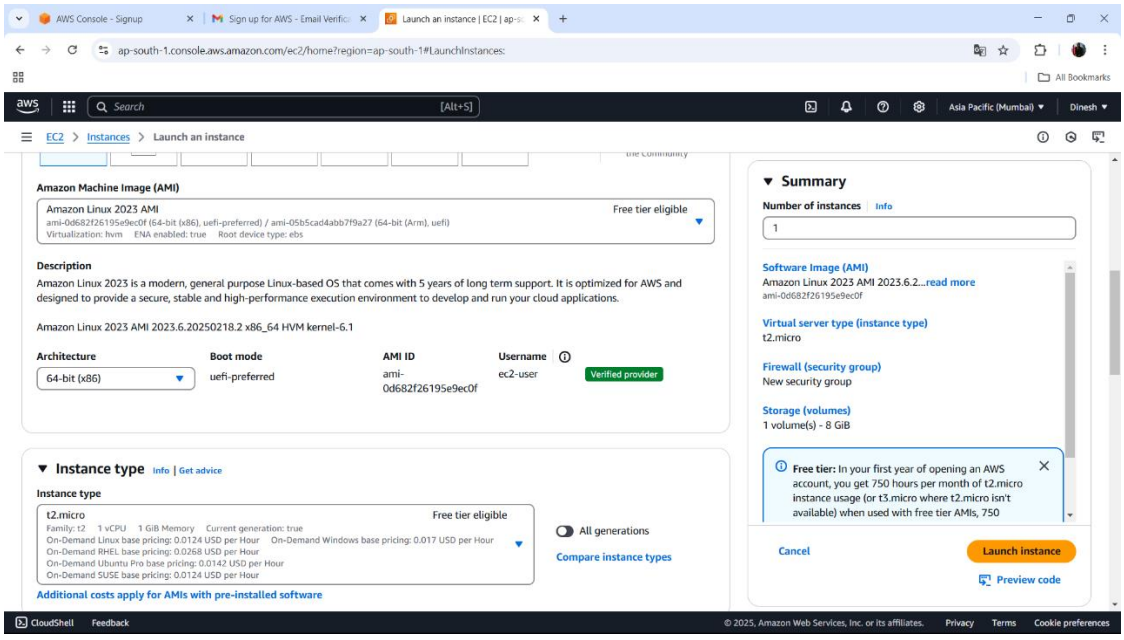
9. Launch the Instance:

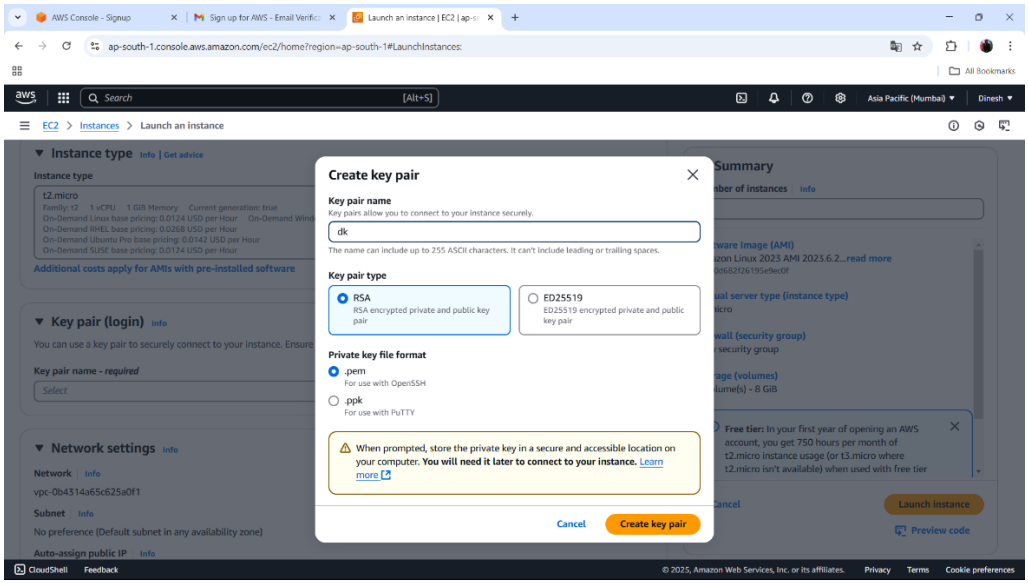
Review configurations, click "Launch".

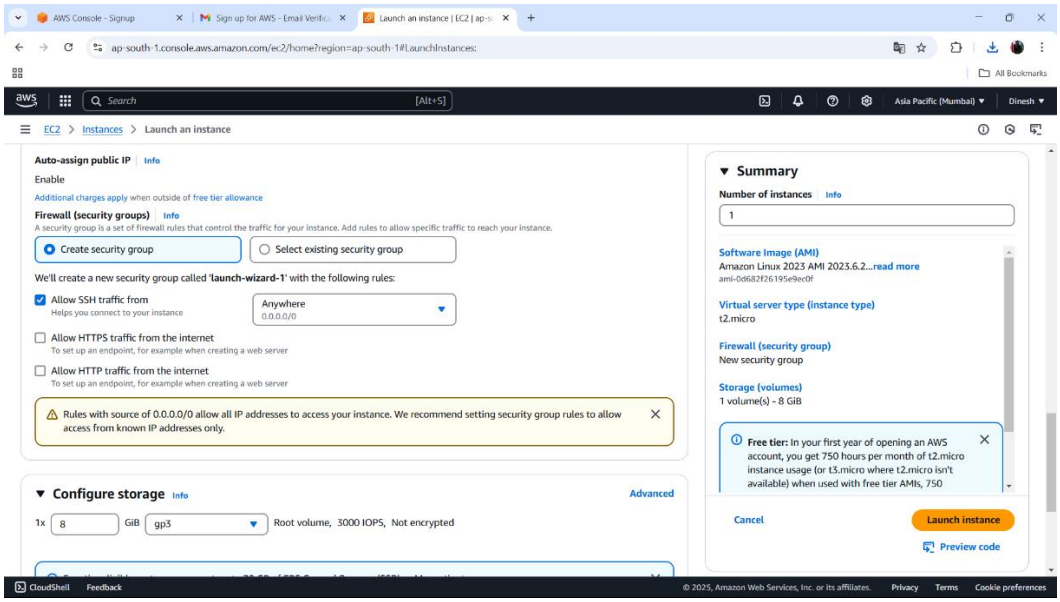
Create and download a key pair (e.g., "MyEC2KeyPair.pem").

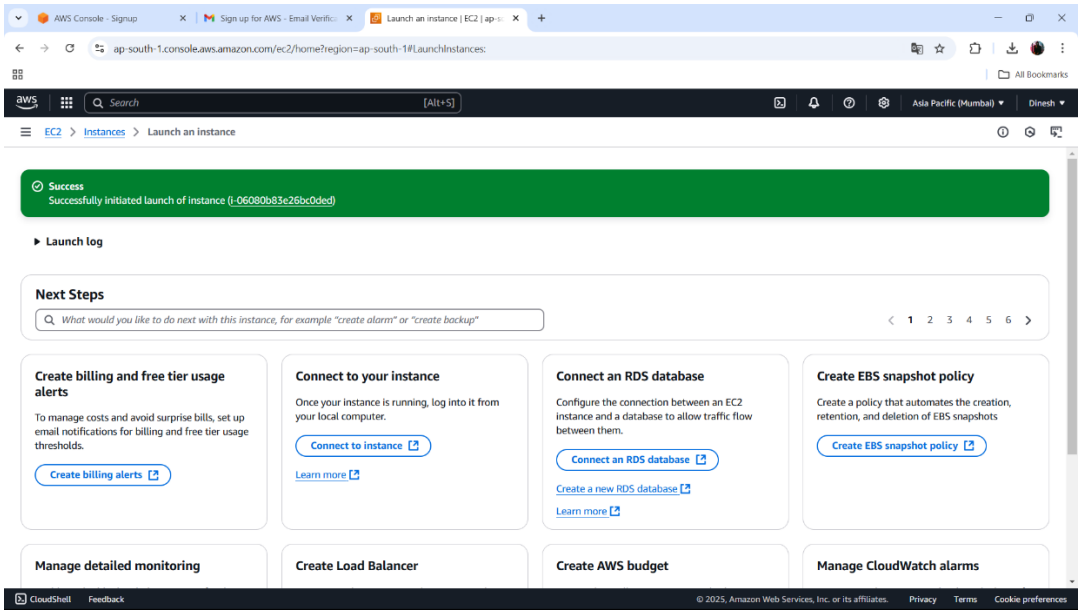
Click "Launch Instances".

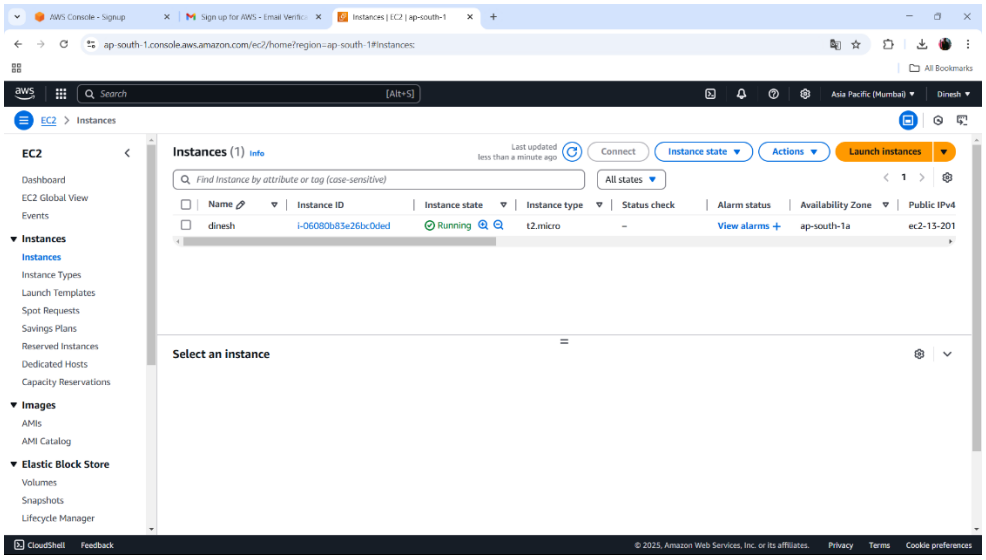





Create key pair
Key pair name
Key pairs allow you to connect to your instance securely.
dk
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.
Key pair type
RSA
RSA encrypted private and public key pair
ED25519
ED25519 encrypted private and public key pair
Private key file format
.pem
For use with OpenSSH
.ppk
For use with PuTTY
When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. Learn more
Cancel
Create key pair
Summary
Launch instance
Preview code


Auto-assign public IP
Enable
Firewall (security groups)
Create security group
Select existing security group
We'll create a new security group called 'launch-wizard-1' with the following rules:
Allow SSH traffic from
Anywhere
0.0.0.0/0
Allow HTTPS traffic from the internet
Allow HTTP traffic from the internet
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Configure storage
Advanced
1x
8
GiB
gp3
Root volume, 3000 IOPS, Not encrypted
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750
Cancel
Launch instance
Preview code


Success
Successfully initiated launch of instance (i-06080b83e26bc0ded)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts
Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more
Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more
Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots
Create EBS snapshot policy
Manage detailed monitoring
Create Load Balancer
Create AWS budget
Manage CloudWatch alarms



Step 2: Connect to the Instance

1. Navigate to the EC2 dashboard and locate your instance.

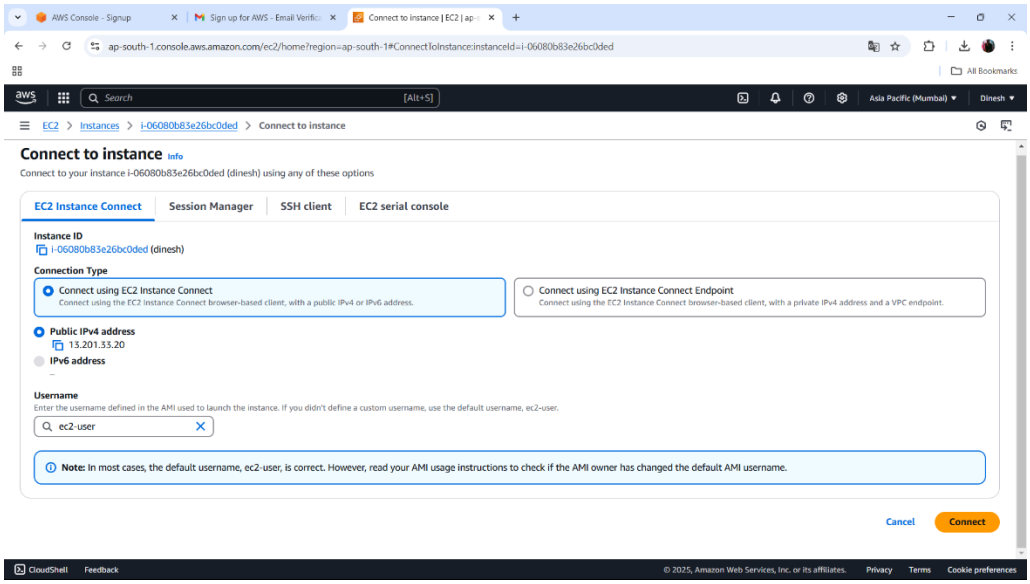
2. Copy the public IP address of the instance.

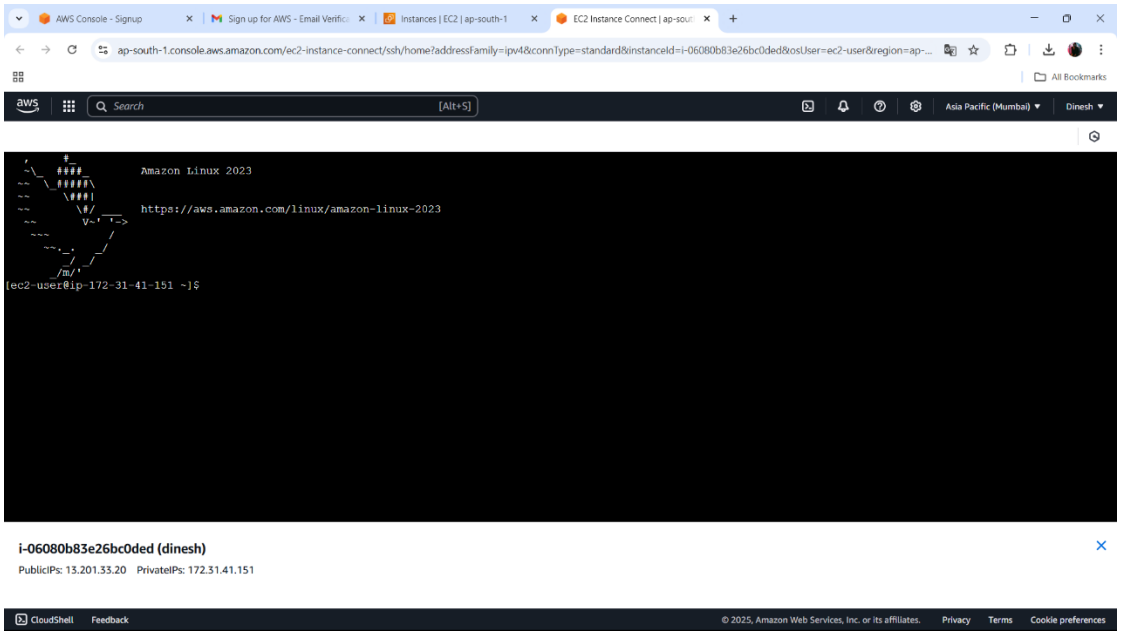
3. Open a terminal (Mac/Linux) or use PuTTY (Windows) for SSH access.

4. Use the command to connect:

ssh -i MyEC2KeyPair.pem ec2-user@your-instance-ip

5. If successful, you will be connected to your EC2 instance.





Step 3: Create a New Volume

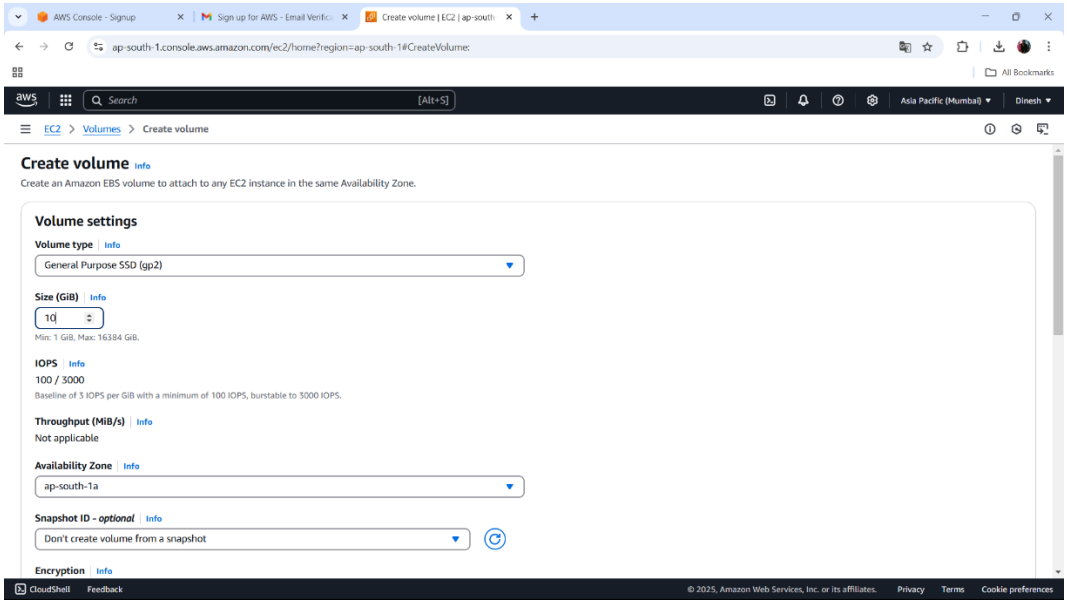
1. In the AWS Console, navigate to the "Volumes" section under "Elastic Block Store".

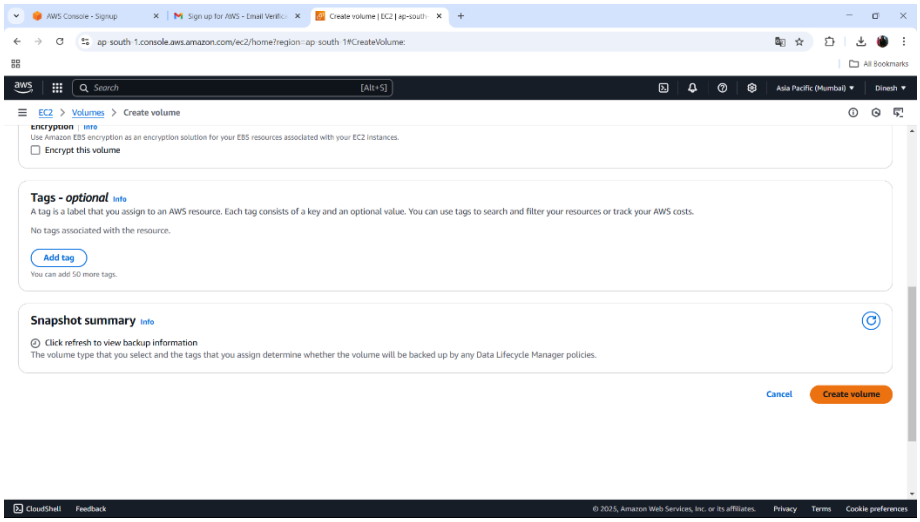
2. Click on "Create Volume".

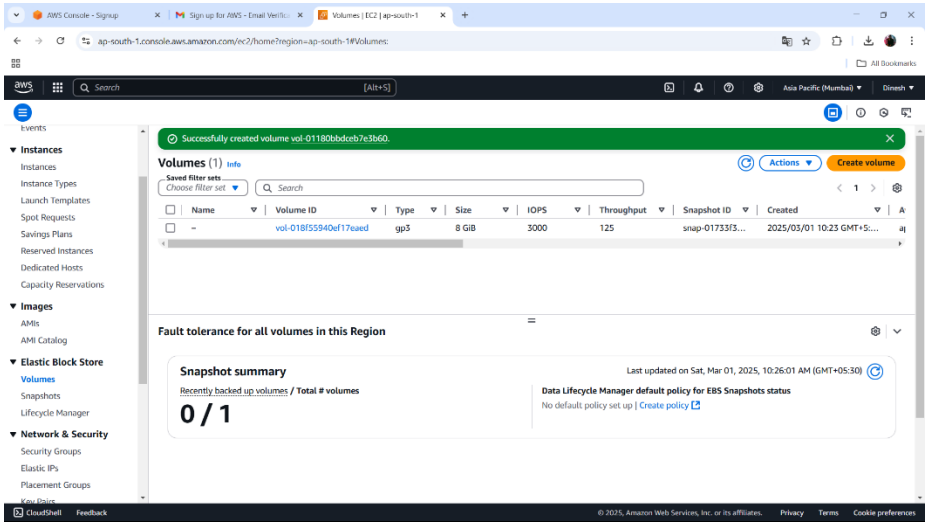
Specify size (e.g., 5GB) and type (e.g., gp3).

Select the same Availability Zone as your EC2 instance.

Click "Create Volume".





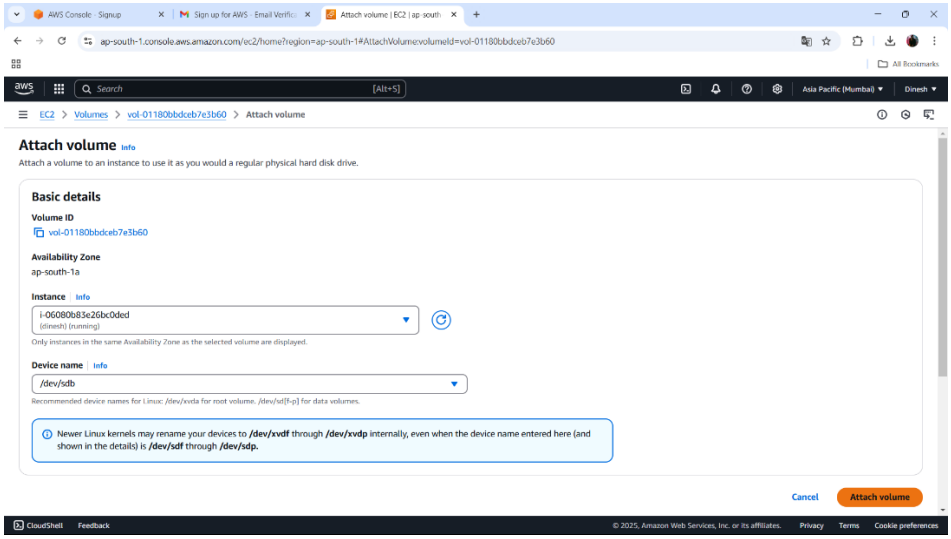


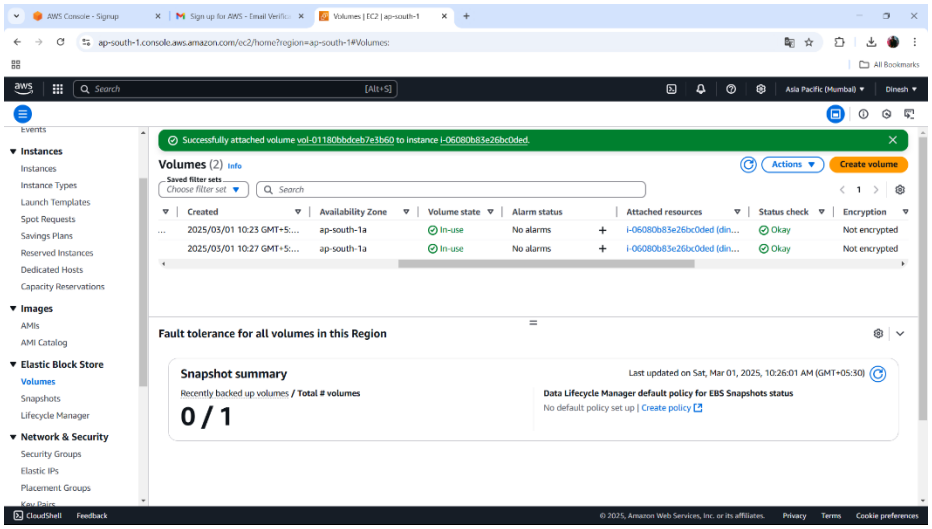
Step 4: Attach Volume to the Instance

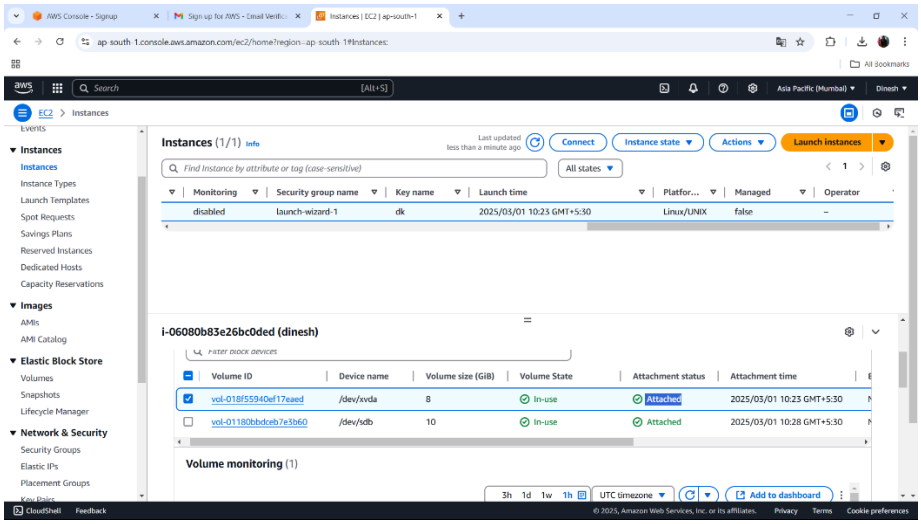
1. Locate the newly created volume.

2. Select the volume, click "Actions", and choose "Attach Volume".

3. Select the target instance and click "Attach".





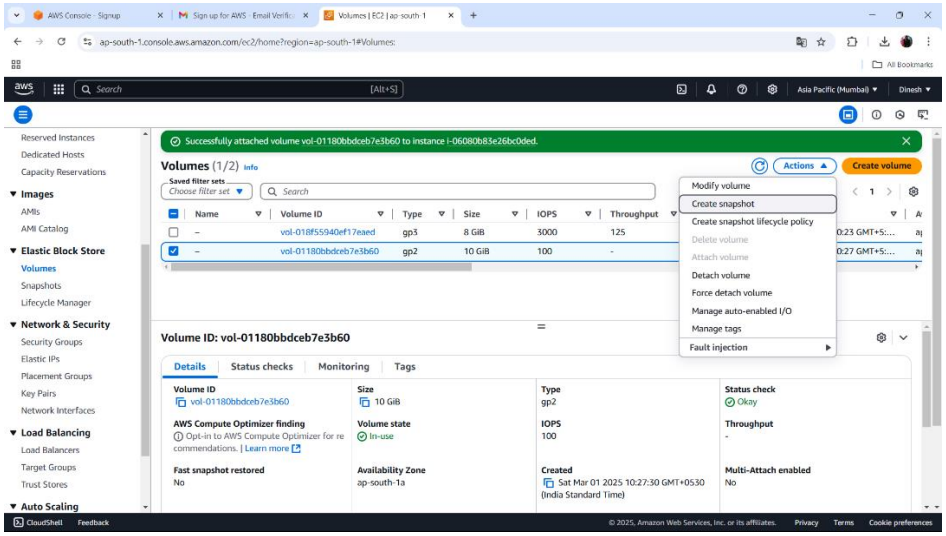


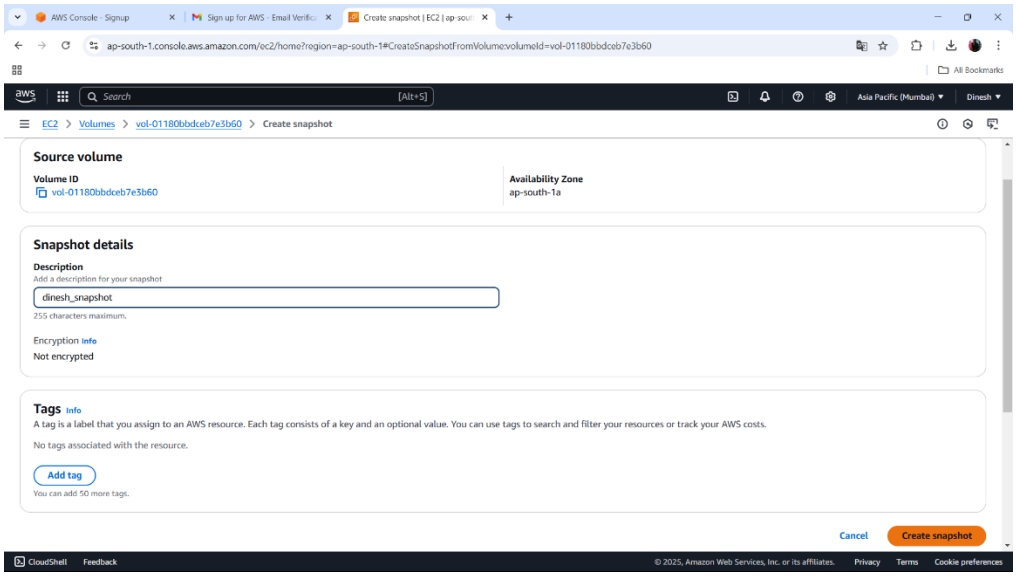
Step 5: Create a Snapshot of the Volume

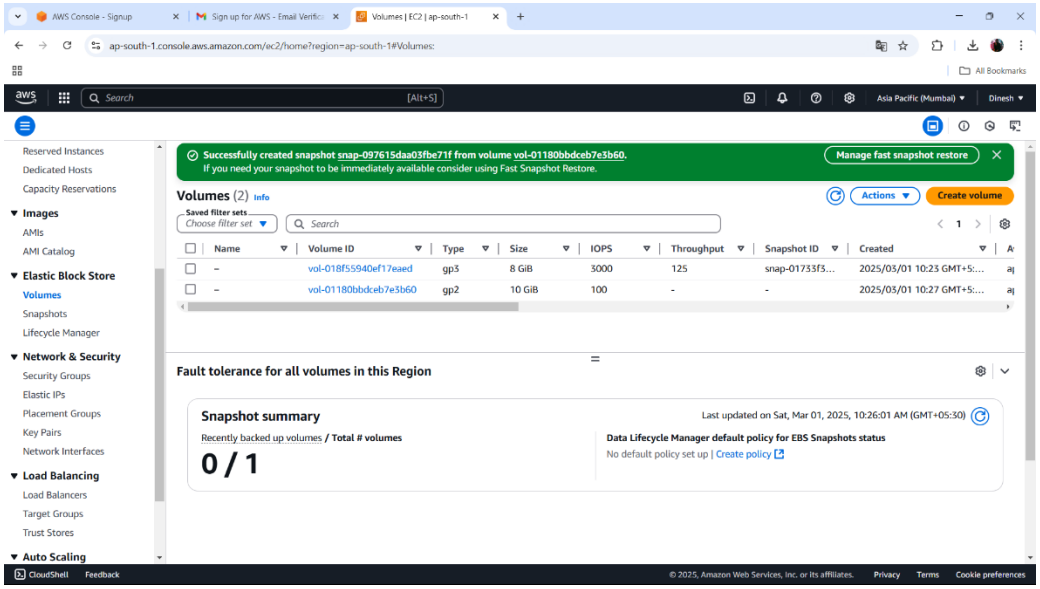
1. In the "Volumes" section, select the attached volume.

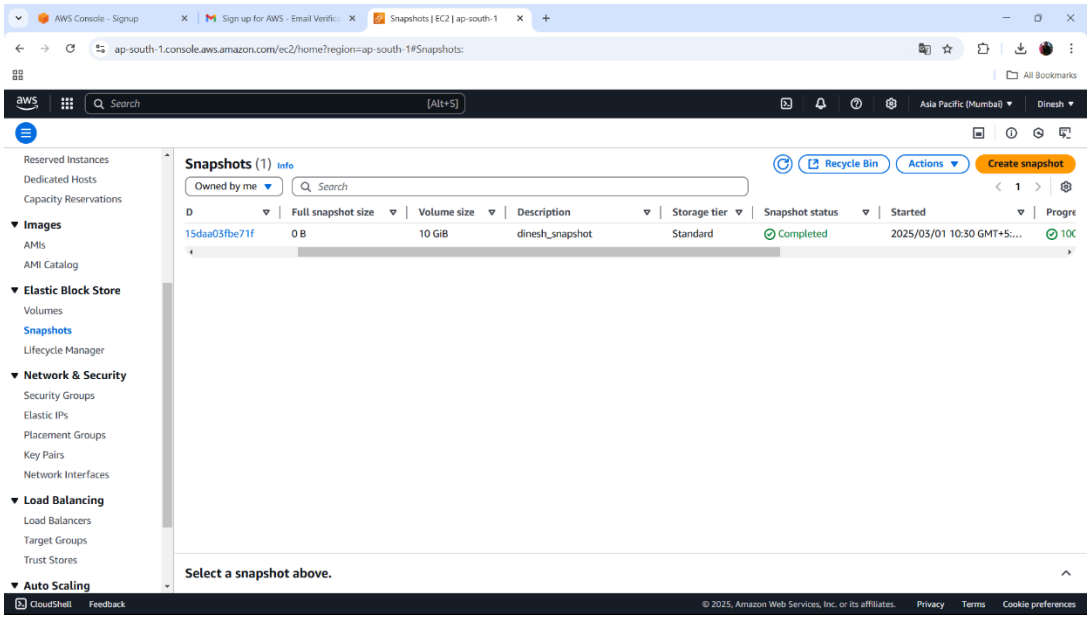
2. Click "Actions" and choose "Create Snapshot".

3. Provide a description for the snapshot and click "Create Snapshot".




Source volume
Volume ID
vol-01180bbdceb7e3b60
Availability Zone
ap-south-1a
Snapshot details
Description
Add a description for your snapshot
dinesh_snapshot
255 characters maximum.
Encryption Info
Not encrypted
Tags Info
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
No tags associated with the resource.
Add tag
You can add 50 more tags.
Cancel
Create snapshot


Successfully created snapshot snap-097615daa03fbe71f from volume vol-01180bbdceb7e3b60.
If you need your snapshot to be immediately available consider using Fast Snapshot Restore.
Manage fast snapshot restore
Volumes (2) Info
Actions
Create volume
Fault tolerance for all volumes in this Region
Snapshot summary
Last updated on Sat, Mar 01, 2025, 10:26:01 AM (GMT+05:30)
Recently backed up volumes / Total # volumes
0 / 1
Data Lifecycle Manager default policy for EBS Snapshots status
No default policy set up | Create policy


Snapshots (1) Info
Recycle Bin
Actions
Create snapshot
Owned by me
15daa03fbe71f
0 B
10 GiB
dinesh_snapshot
Standard
Completed
Select a snapshot above.

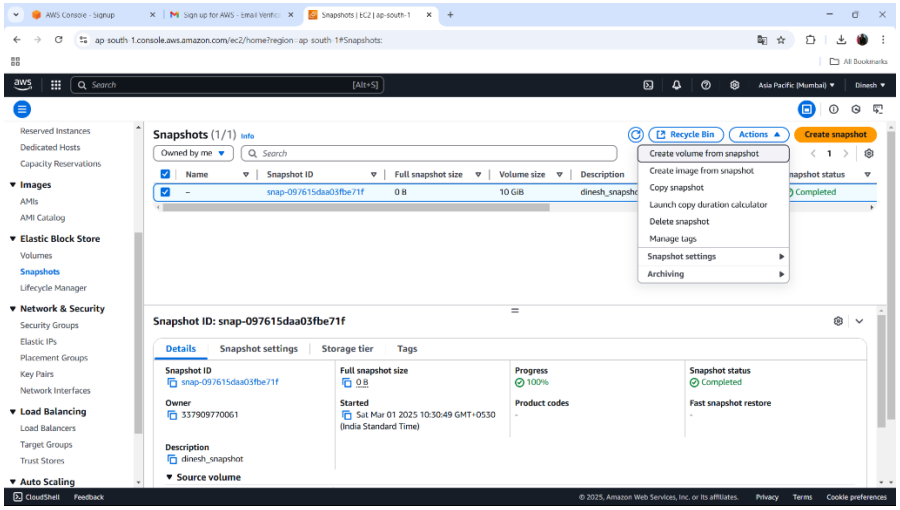
Step 6: Create a New Volume from the Snapshot

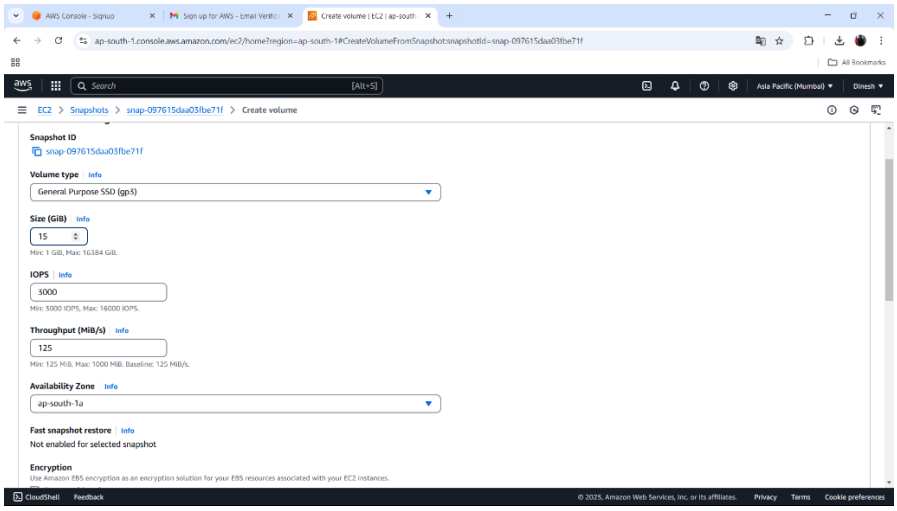
1. Navigate to the "Snapshots" section.

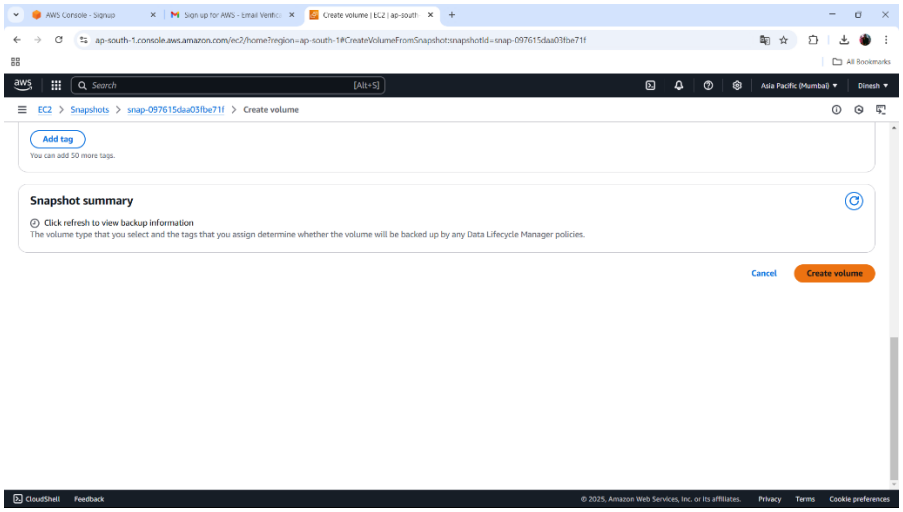
2. Select the created snapshot and click "Actions" > "Create Volume".

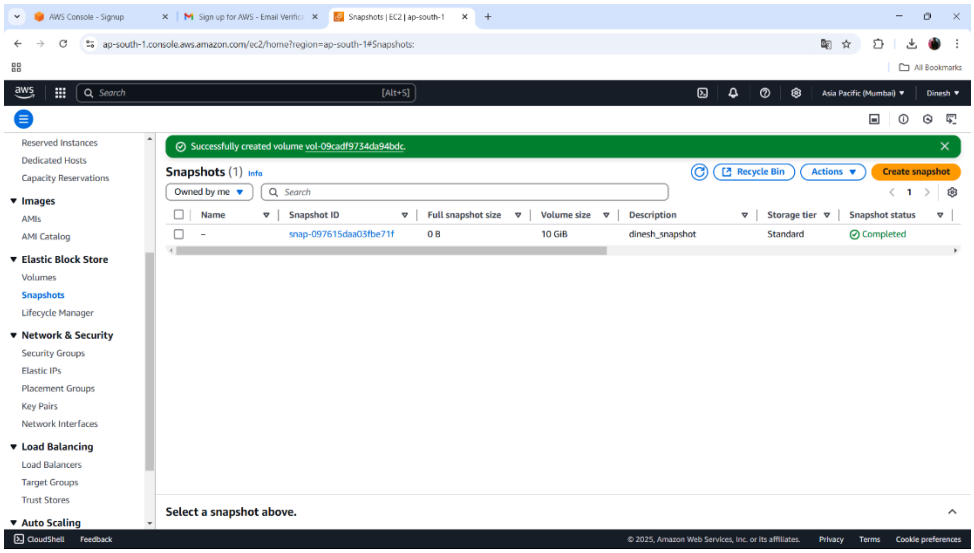
3. Specify the size and Availability Zone to match the instance.

4. Click "Create Volume".





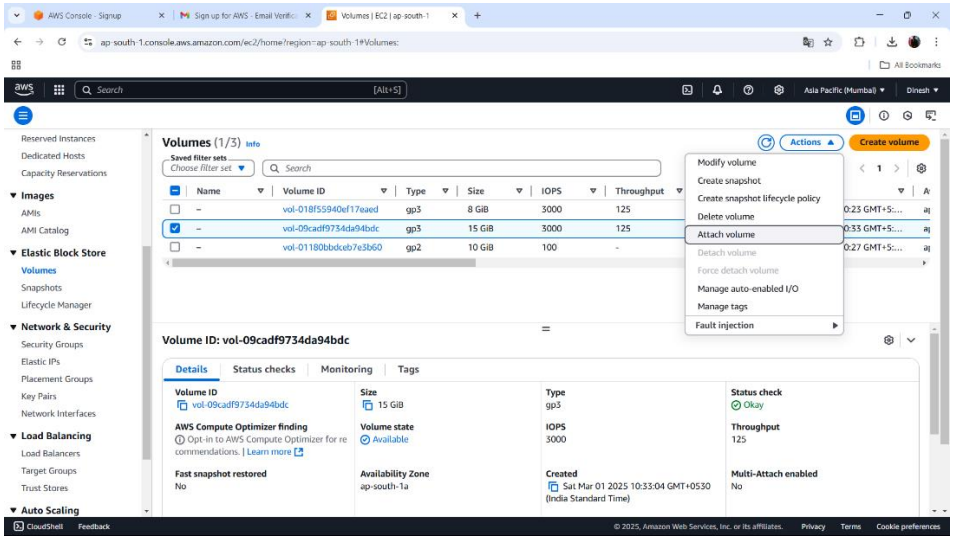


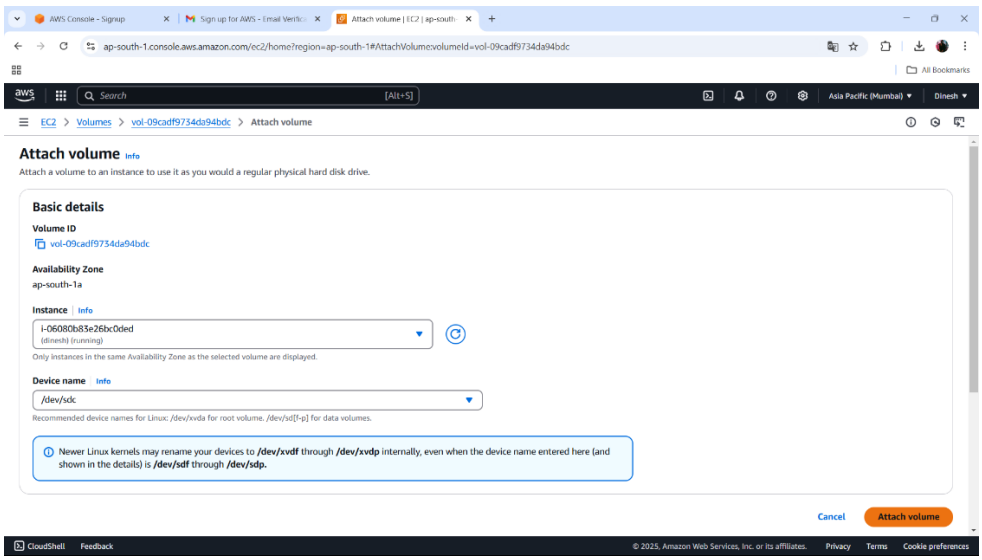


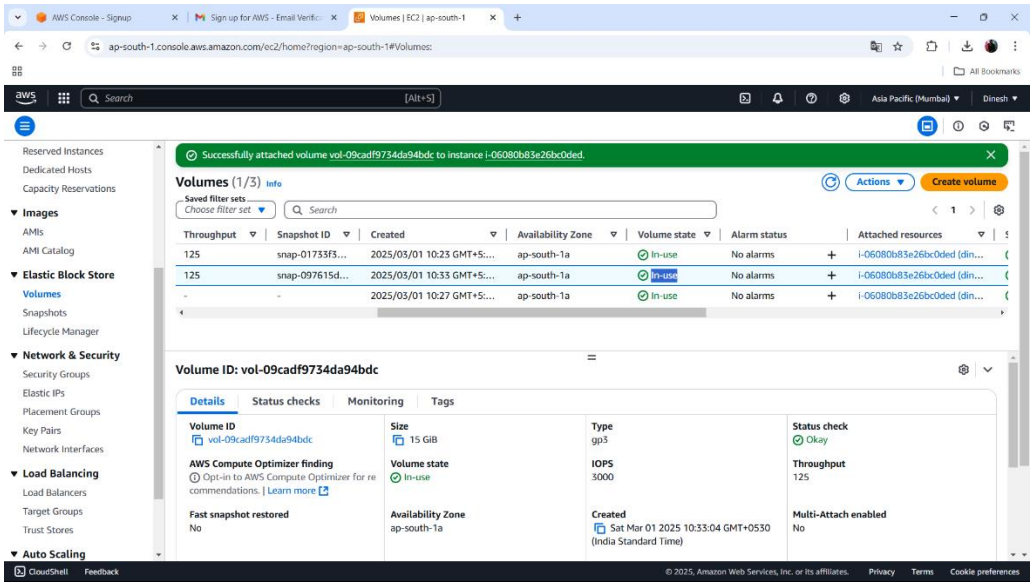
Step 7: Attach the New Volume

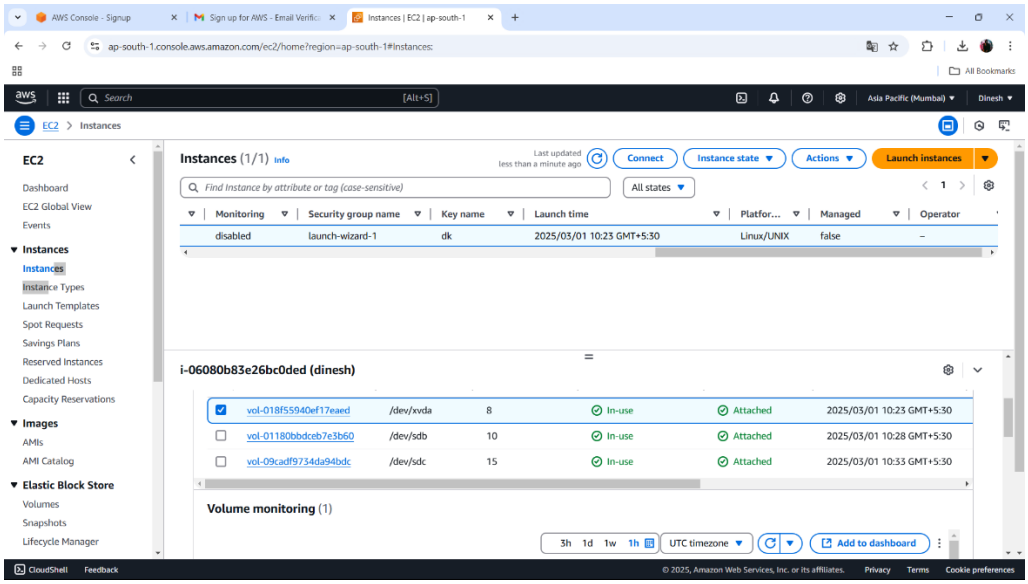
1. Locate the new volume created from the snapshot.

2. Attach the volume to the instance using the same steps as in Step 4.









Step 8: Terminate All Resources

1. Detach Volumes:

Navigate to the "Volumes" section and detach all attached volumes.

2. Delete Volumes:

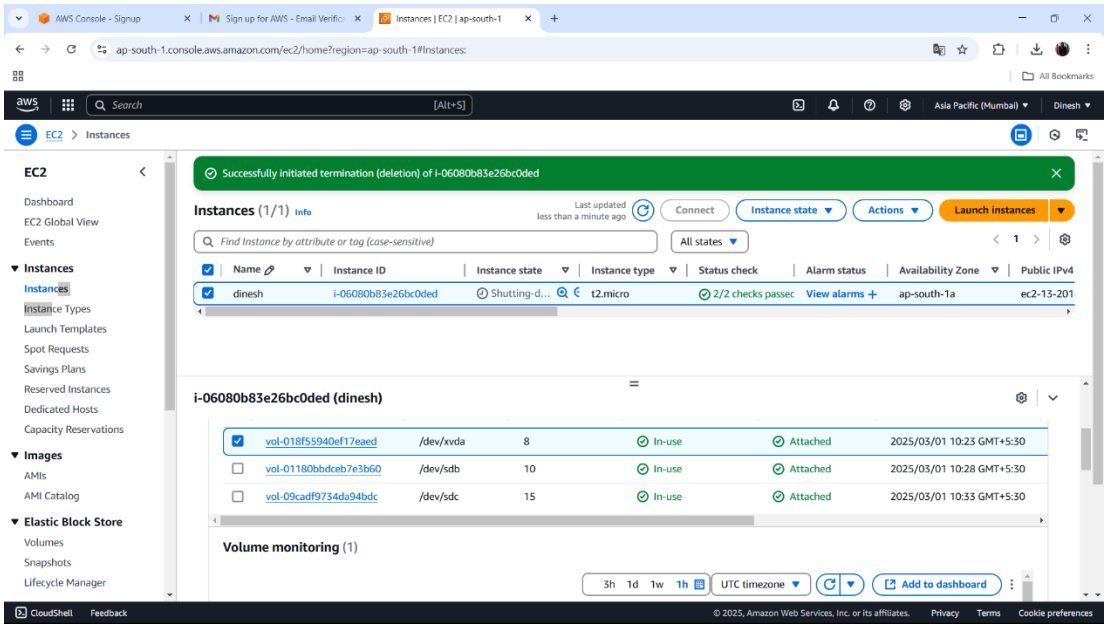
Select the volumes and delete them.

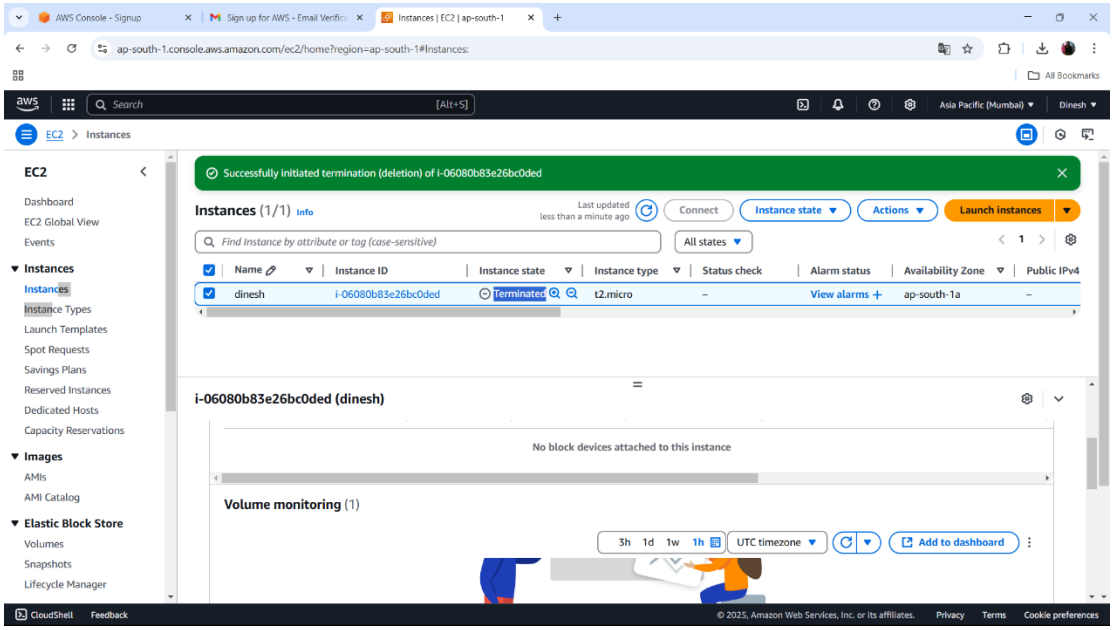
3. Terminate the Instance:

Go to the EC2 dashboard, select the instance, and click "Actions" > "Terminate Instance".

4. Delete Snapshots:

Navigate to the "Snapshots" section and delete all snapshots.





Result:

An AWS EC2 instance was successfully created, configured, accessed, and managed by performing volume attachment, snapshot creation, and resource termination.