Department of Computer Science & Engineering
ChitkaraUniversityInstituteofEngineering&Technology
(AccreditedbyNAACwithGrade'A+')

Practical File

Cloud Computing (23CS009)

BACHELOR OF ENGINEERING

in

Computer Science and Engineering

Submitted By:
Ramanjot Singh
2310992347
G-15
5th Sem 3rd Year

Submitted To
Dr. Astha Gupta
Assistant Professor

CHITKARA UNIVERSITY, PUNJAB
CHANDIGARH- PATIALA NATIONAL HIGHWAY RAJPURA (PATIALA) PUNJAB-140401 (INDIA)

INDEX

Practical No. 1:

Practical Title: Sign up for AWS, Explore Free-Tier Services, and Launch EC2 Instances using Ubuntu/Linux and Windows operating systems.

Objective:

A. To create an AWS account and explore free-tier services and understand it's usage.

B. To launch an EC2 instance with Ubuntu/Linux and Windows OS.

A. To create an AWS account and explore free-tier services.

Step 1: AWS Account Signup

1. First step is to check the mail inbox on college email id, search the mail with name "Course Invitation". Click on Get Started button as described

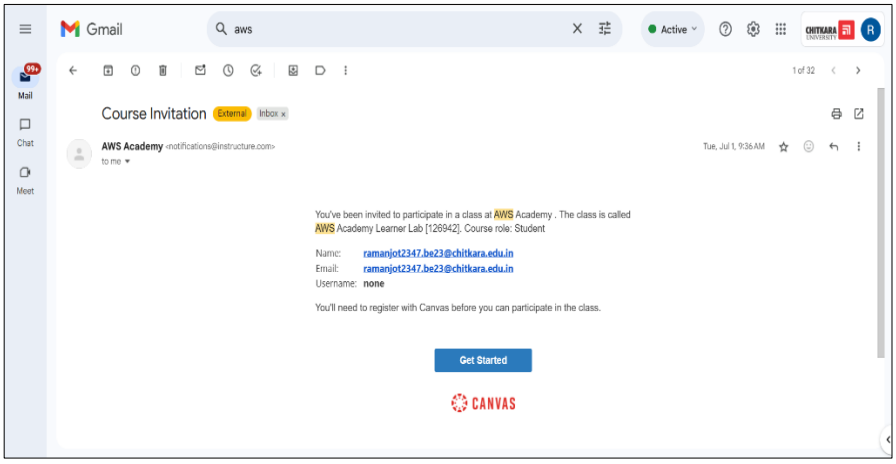


Figure 1.1 Invitation mail of AWS Cloud Computing

2. Visit AWS Portal: Open AWS Official Website (https://aws.amazon.com/) and click on "Create an AWS Account".

Figure 1.2 Click on Login Button

3. Enter Account Details: Provide your email address, set an AWS account name, and click "Continue".
4. Identity Verification: Enter the OTP received on your registered mobile number.
5. Select Support Plan: Choose "Free Tier (Basic Support)".
6. Sign in to AWS Console: Once the account is activated, log in using your credentials.

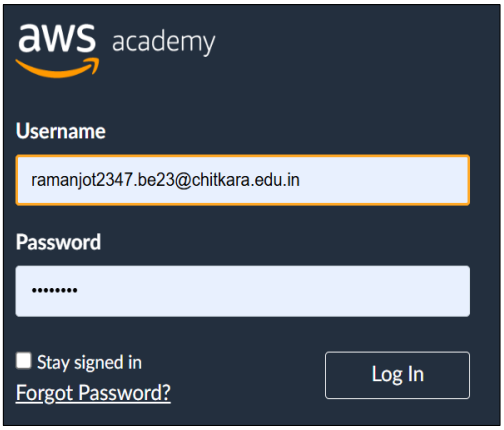


Figure 1.3 Fill up Username and Password to Log In

7. Next, we will reach the home page of the AWS Academy Learner Lab.

Figure 1.4 Home Page of the AWS Learner's Academy

8. Click on modules section from the Home Page.

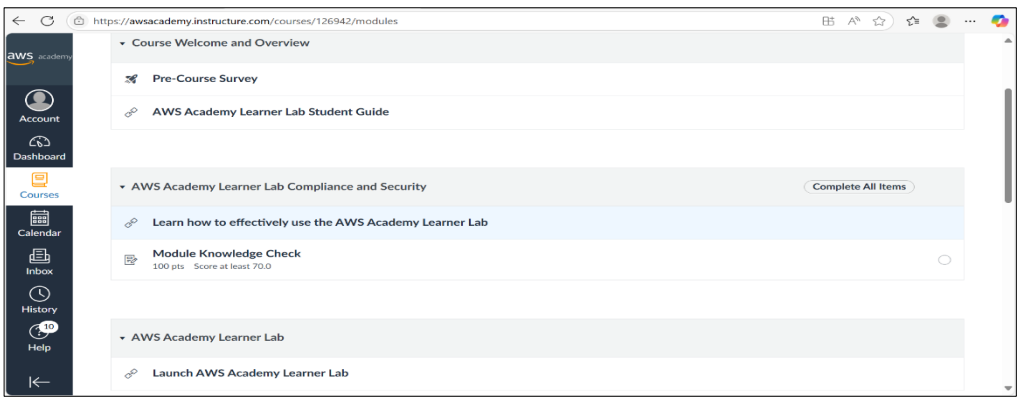


Figure 1.5 Courses Section of Learner's Academy

9. In this select "Launch AWS Academy Lerner Lab" option.

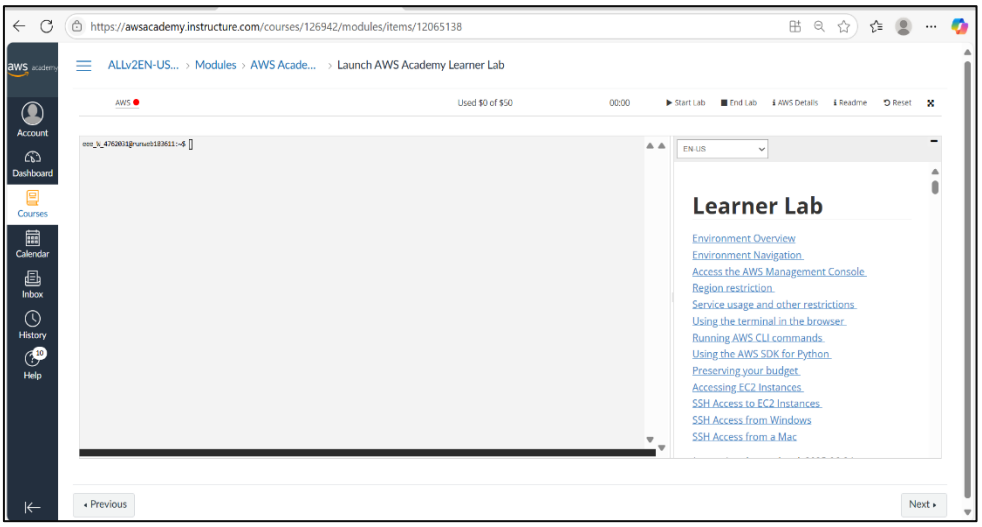


Figure 1.6 Opened AWS Labs

10. Now, click on Start Lab to initialize the environment.

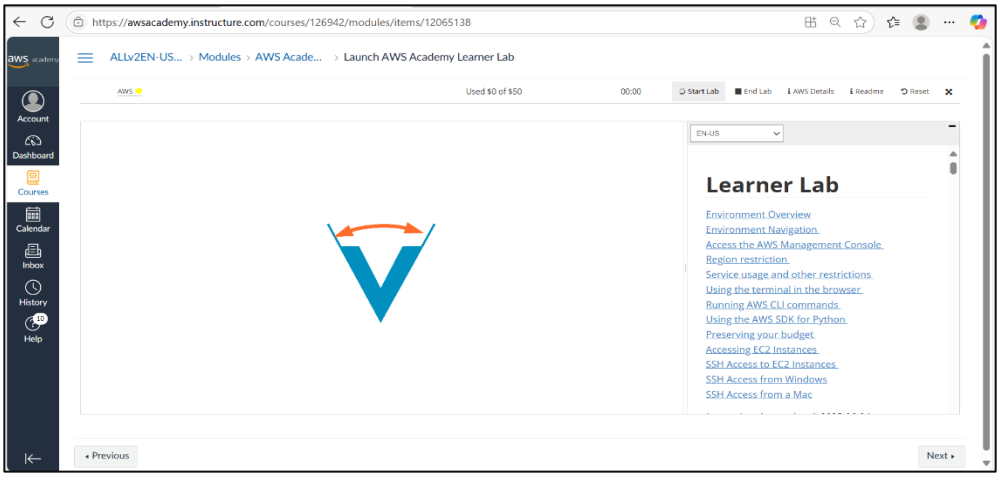


Figure 1.6 Launching AWS Labs

11. Wait for activation, as it will take a few moments to set up necessary AWS resources.

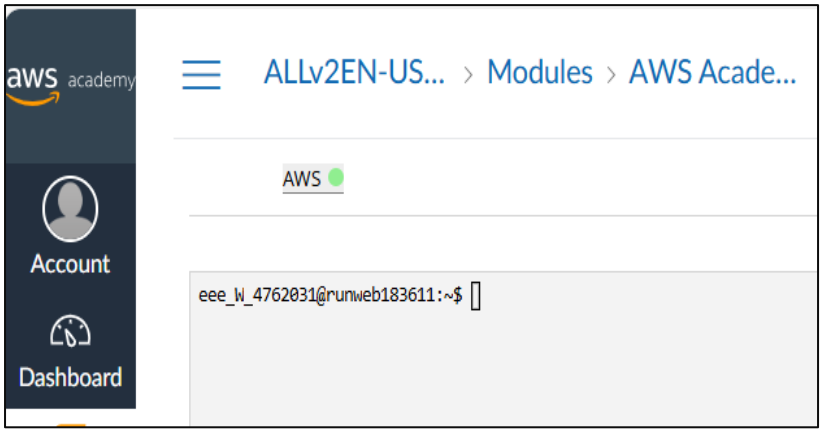


Figure 1.7 Click on Green Button to open AWS Console

12. Finally, after following the above steps one can easily access the AWS Console and end lab after working with the cloud.

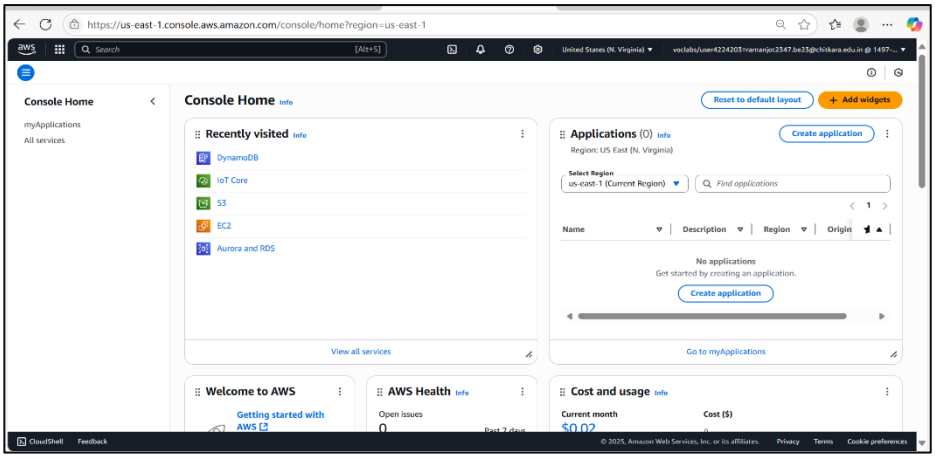


Figure 1.8 Dashboard of AWS Console

Step 2: Exploring AWS Free-Tier Services

AWS offers a Free Tier to help new customers test out cloud services for free. It includes:

1. **Free Tier Services:** Year-round services with consumption limits (such as one million AWS Lambda queries per month) are always free.
2. **12-Month Free:** After creating an account, you can use the EC2 t2.micro instance for free for 12 months (750 hours per month, for example).
3. **Trial-Based Free:** A few providers provide free, time-limited trials (like Amazon SageMaker's 30-day trial). This tier is ideal for learning, testing, and small-scale deployments.

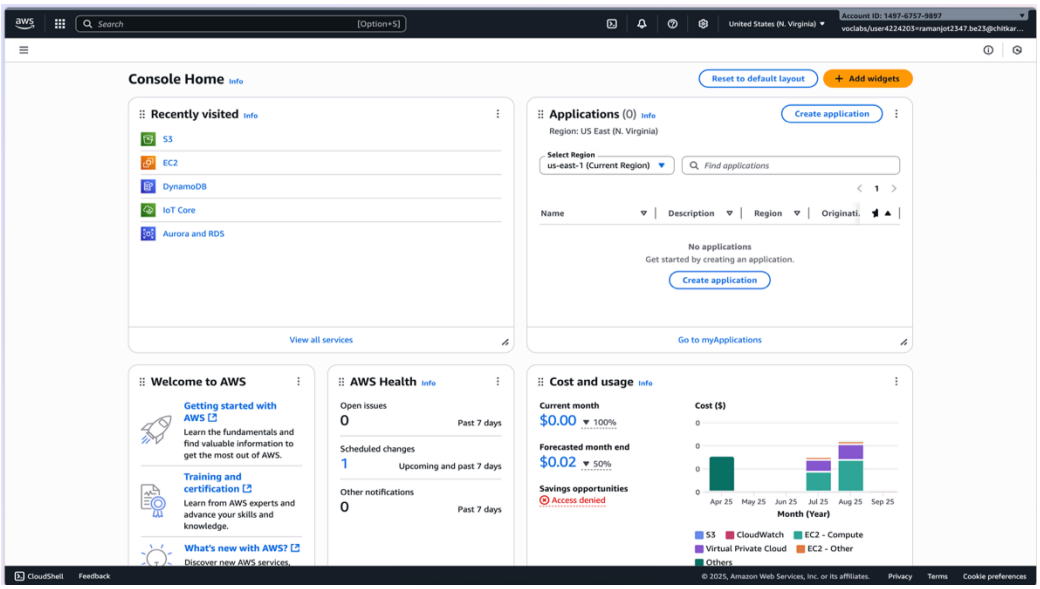


Figure 1.9 Free Tier Service

B. Launching EC2 Instances (Linux & Windows)

1. Open EC2 Service: Navigate to AWS Management Console. Search EC2 (Amazon Elastic Compute Cloud)

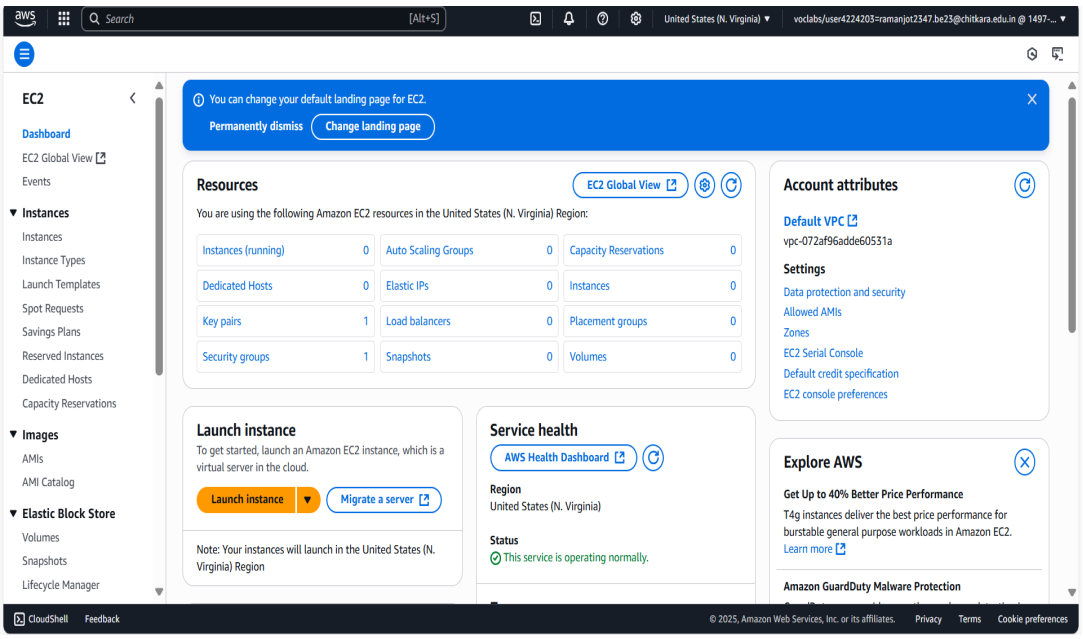


Figure 1.10 Navigating to EC2 Dashboard

2. Lauch the instance. Choose Amazon Machine Image (AMI): Select Linux 22.04 LTS (Free-Tier Eligible).

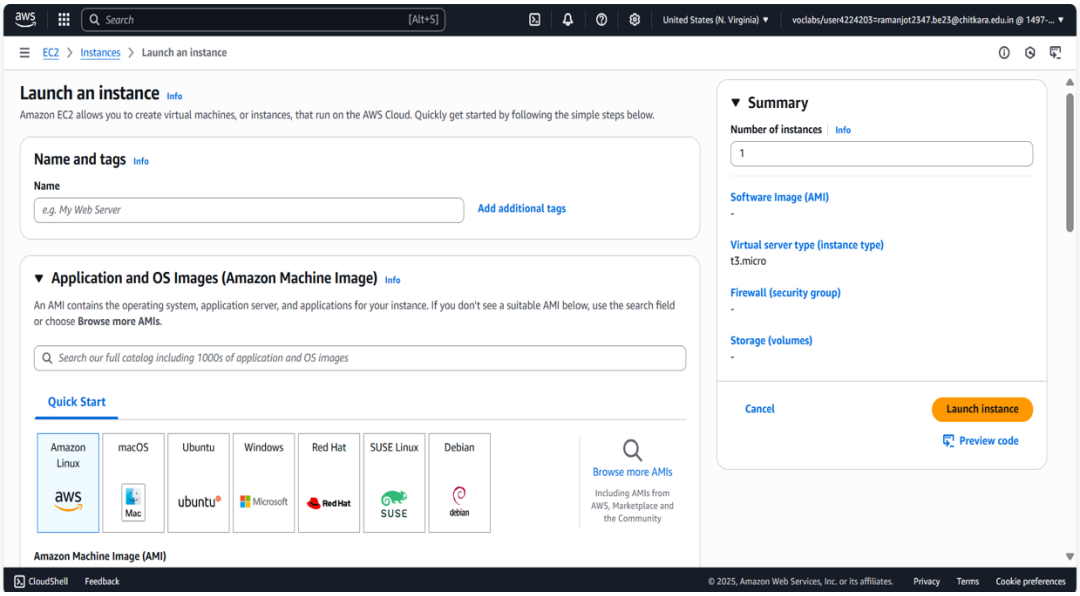


Figure 1.11 Give name to the server and select the AMI

3. Choose Instance Type: Select t3.micro. Configure Instance: Keep default settings
4. Add Storage: Default 8GB EBS is selected.

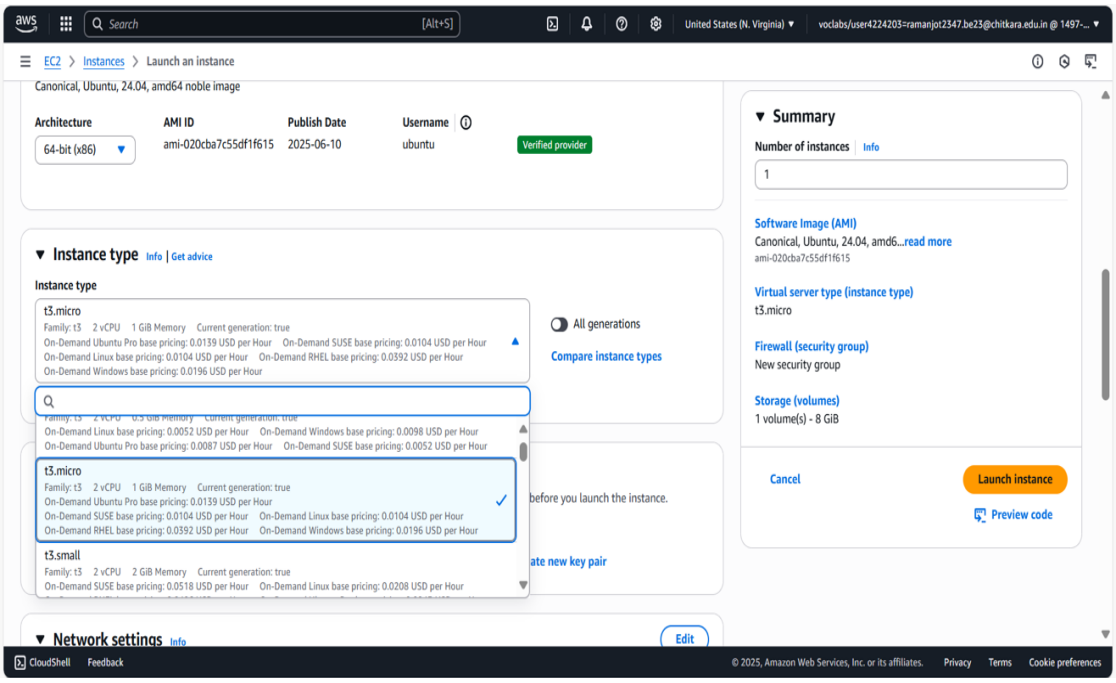


Figure 1.12 Selecting the Instance type

5. Add Tags: Add Name → Linux_Instance
6. Configure Security Group: Allow SSH (Port 22) for remote access.

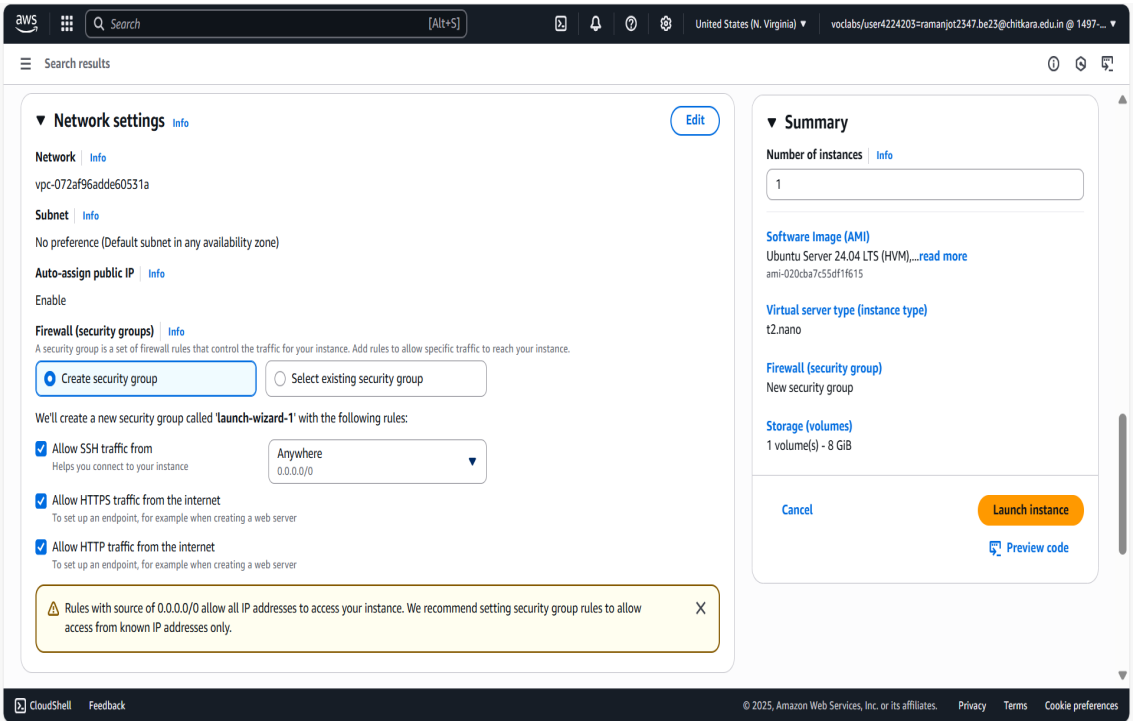


Figure 1.13 Click on allow HTTPS, HTTP

7. Create Key Pair: Create a new key pair (e.g., linux-key.pem) and download it.
8. Review and Launch: Click "Launch" and wait for the instance to start.

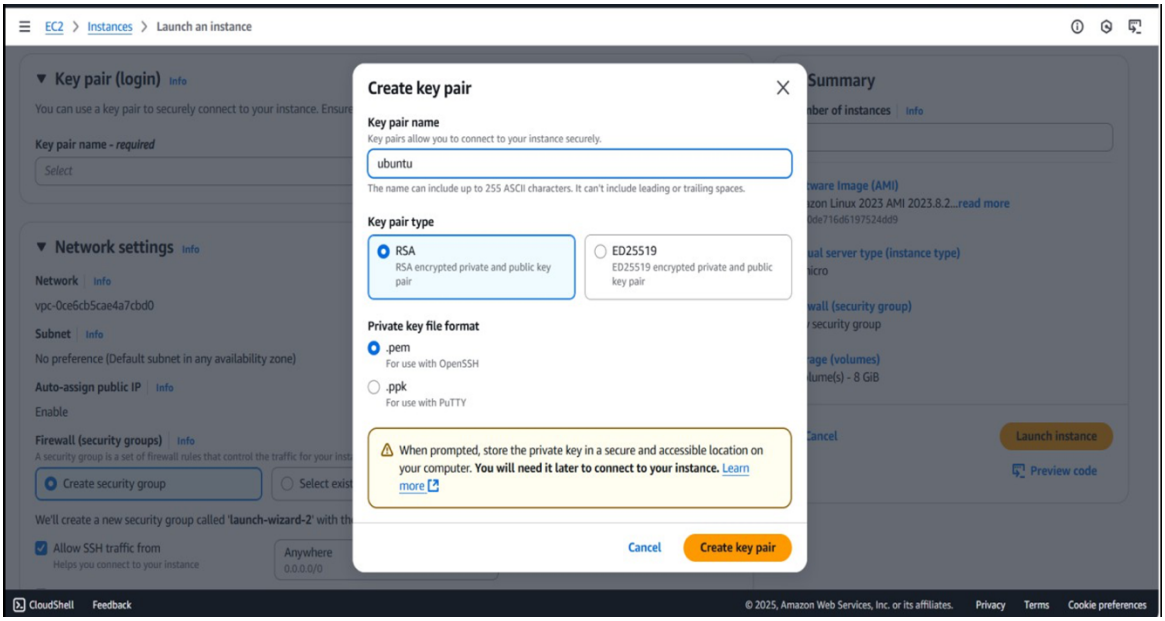


Figure 1.14 Download the key pair (.pem)

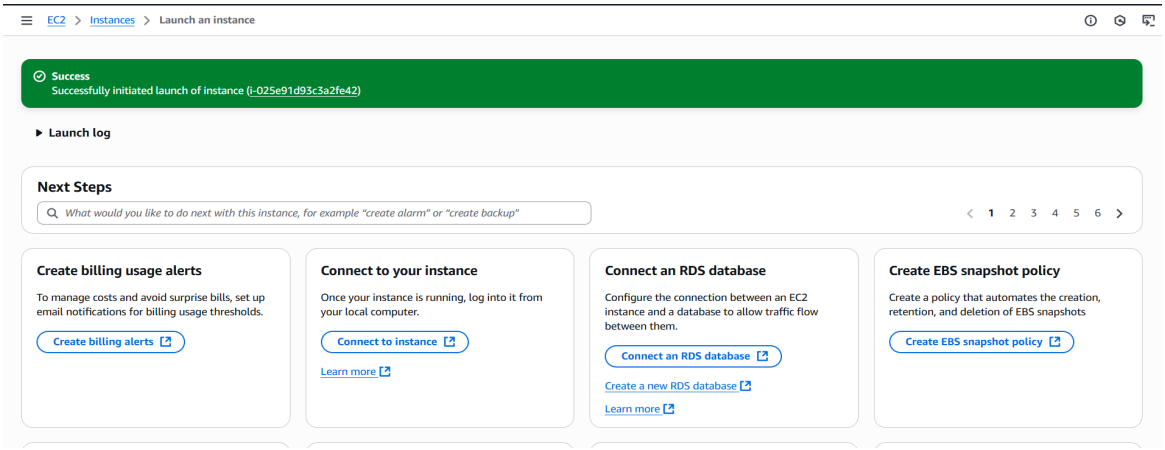


Figure 1.15 Instance Created Successfully

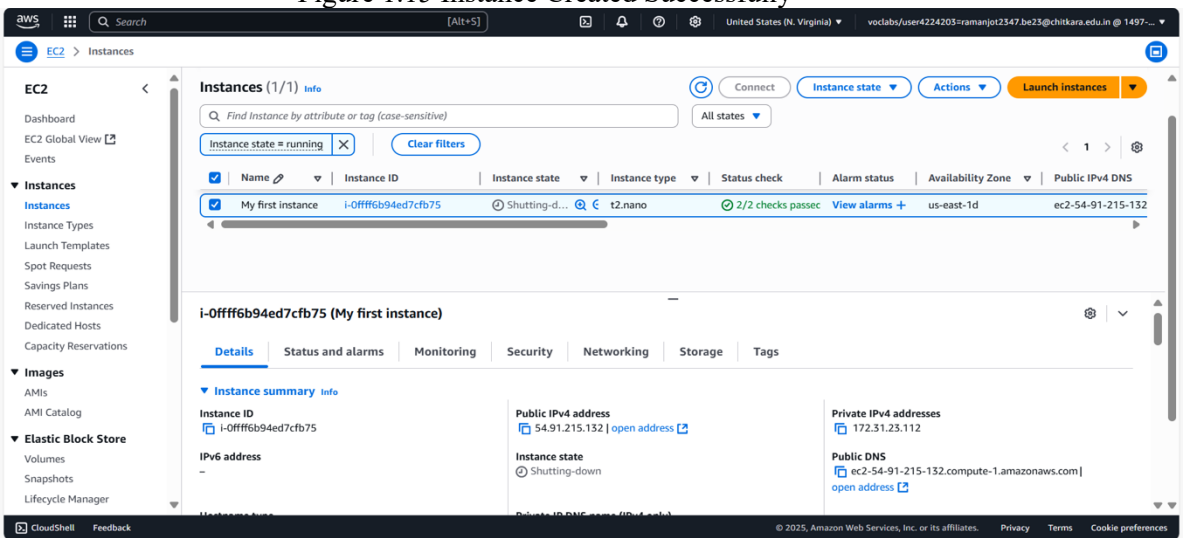


Figure 1.16 Instance Running Successfully

9. Connect to Ubuntu Instance using SSH: ssh -i linux-key.pem linux@<Public_IP>

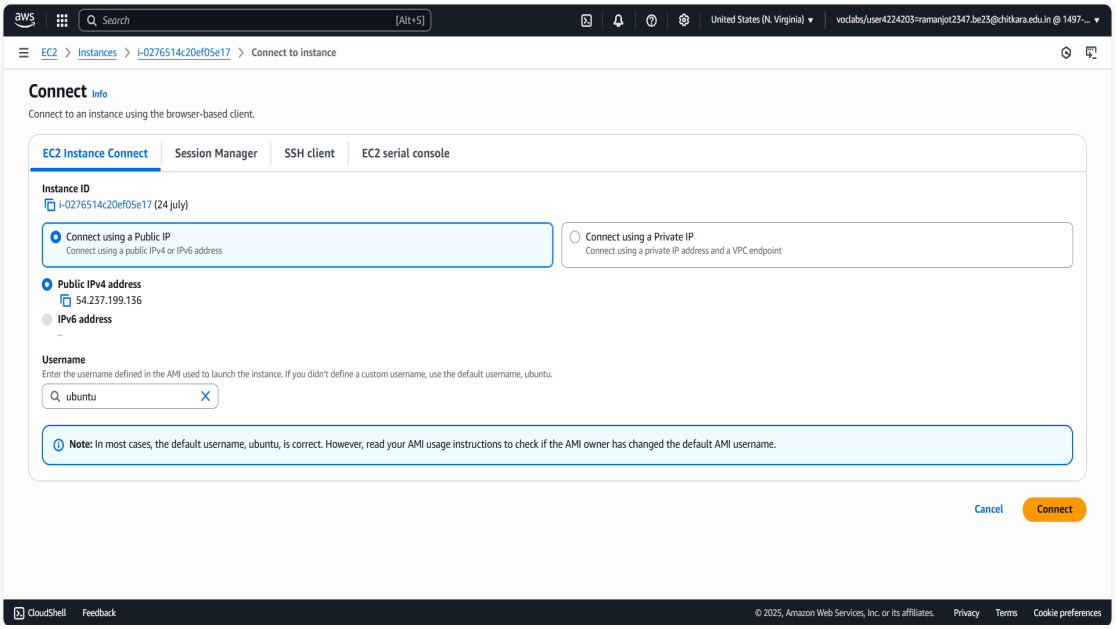


Figure 1.17 Connect the Instance using SSH

10. Open the terminal and go to the directory where pem file is present.

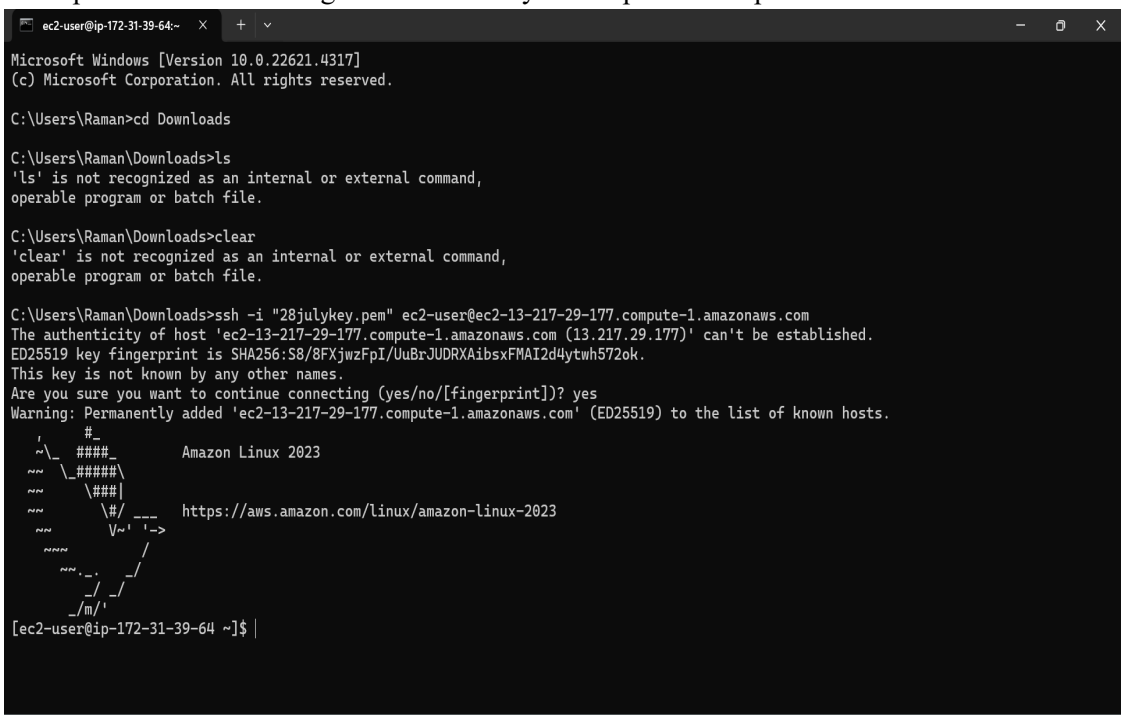


Figure 1.18 Connect the Instance using SSH

11. For running EC2 Instance on Windows, select Microsoft Windows Server 2025 Base.

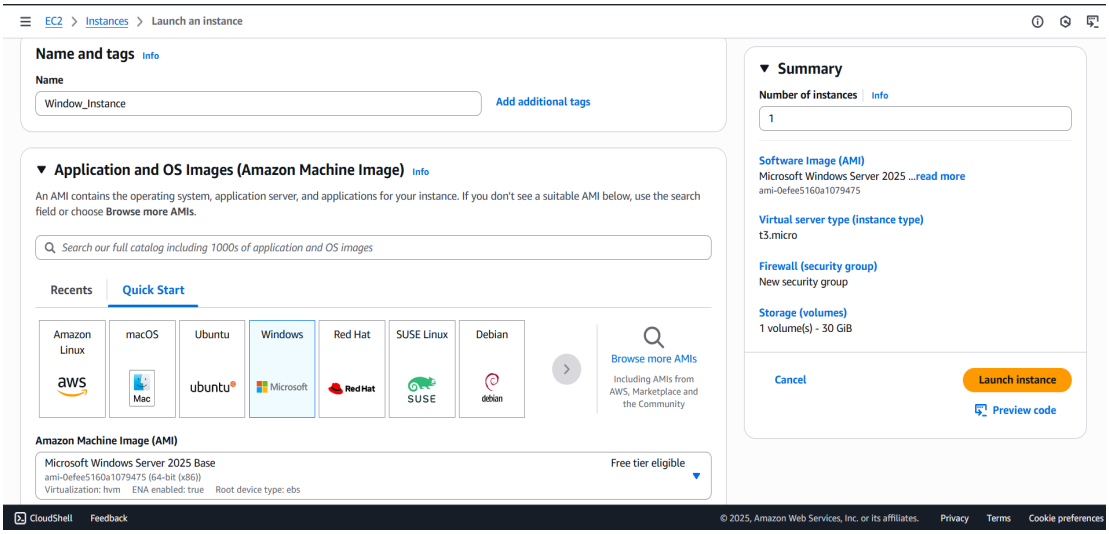


Figure 1.19 Select AMI as Windows

12. Allow RDP (Port 3389).
13. Download key file for password decryption.

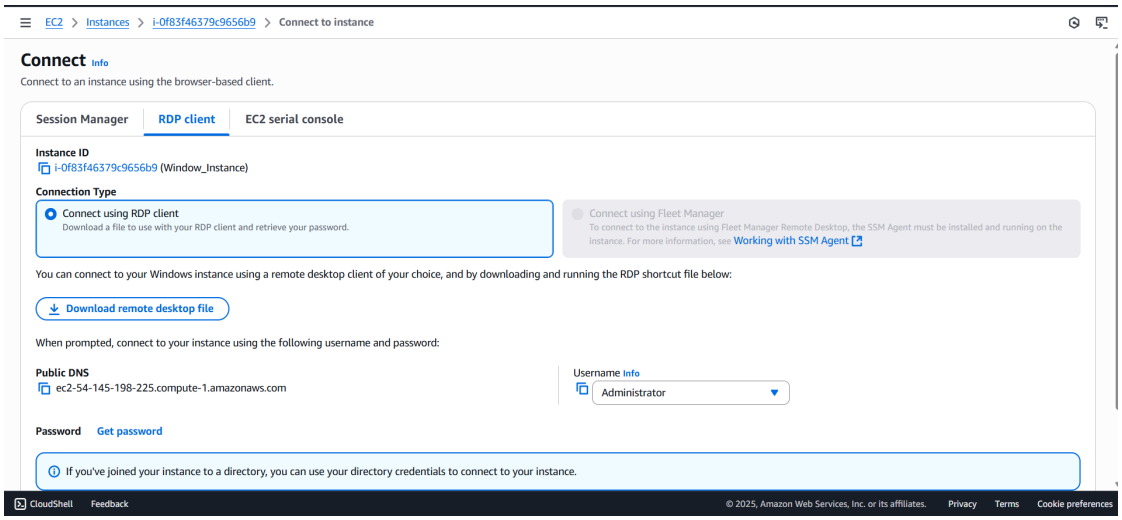


Figure 1.19 Connect Instance Using RDP client

14. Launch and Get password, followed by decrypting with the keyfile.

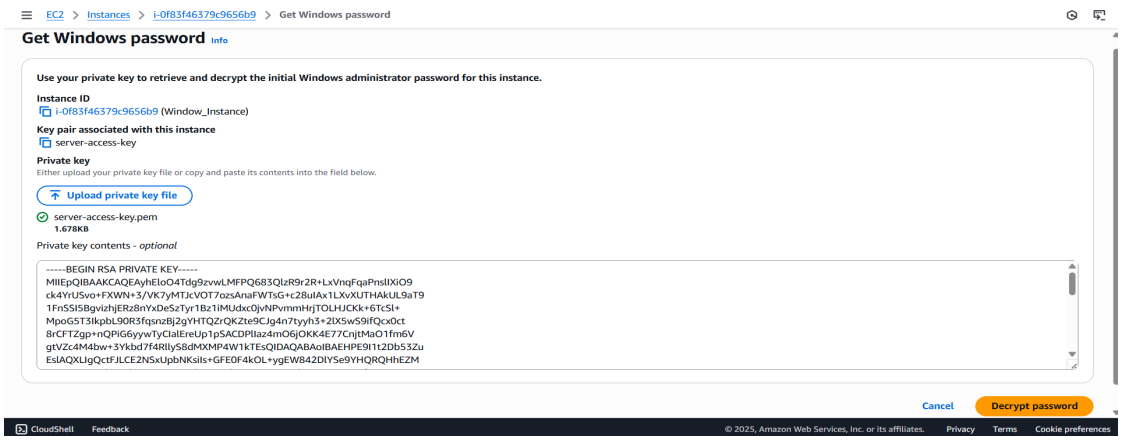


Figure 1.20 Get the Password

15. Connect using Remote Desktop Connection (RDP).

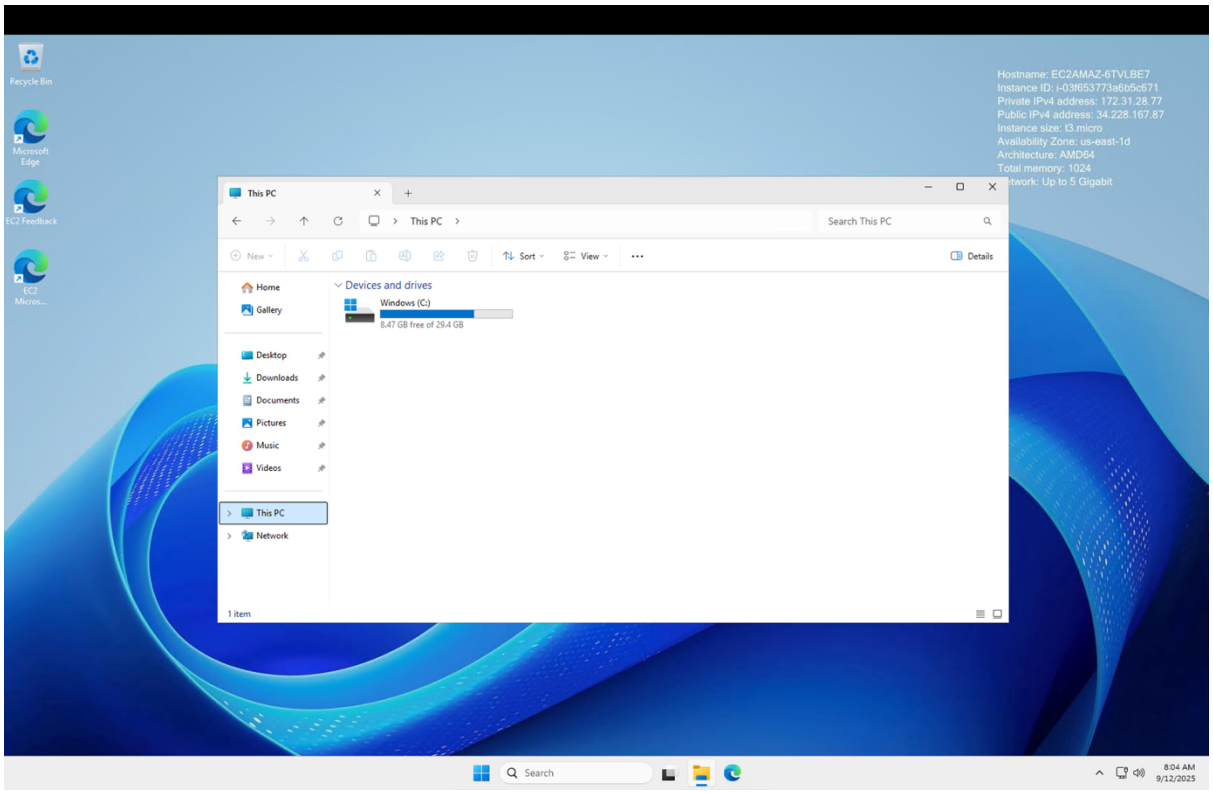


Figure 1.21 Connected to RDP

Learning Outcomes:

- Successfully signed up for AWS and explored free-tier services.
- Launched and connected to EC2 instances using both Ubuntu/Linux and Windows.
- AWS provides a free-tier environment for cloud computing. We created EC2 instances and accessed them using SSH (Ubuntu) and RDP (Windows). This experiment demonstrated the fundamentals of launching and managing virtual machines on AWS.

Practical No. 2:

Practical Title: Connect to an EC2 instance via EC2 Connect, SSH Client, AWS CLI, and PuTTY SSH Client using a key pair file.Access and modify Security Group inbound and outbound rules to control traffic for EC2 instances.

Objective:

1.1 Connect to an EC2 instance using a key pair file via
- A. EC2 Connect
- B. SSH Client and
- C. PuTTY SSH Client

1.2 Access and modify Security Group inbound and outbound rules to control traffic for EC2 instances.

2.1(A) Connect to an EC2 instance via EC2

Connect Step 1: Launch an EC2 Instance

1. Open AWS Management Console → EC2 → Launch Instance.
2. Select Ubuntu 22.04 LTS AMI (Free-Tier Eligible).
3. Choose t2.micro instance type.
4. Create a key pair and download it.
5. In Security Group, allow:
   - SSH (Port 22) from your IP.
   - HTTP (Port 80) for web access.

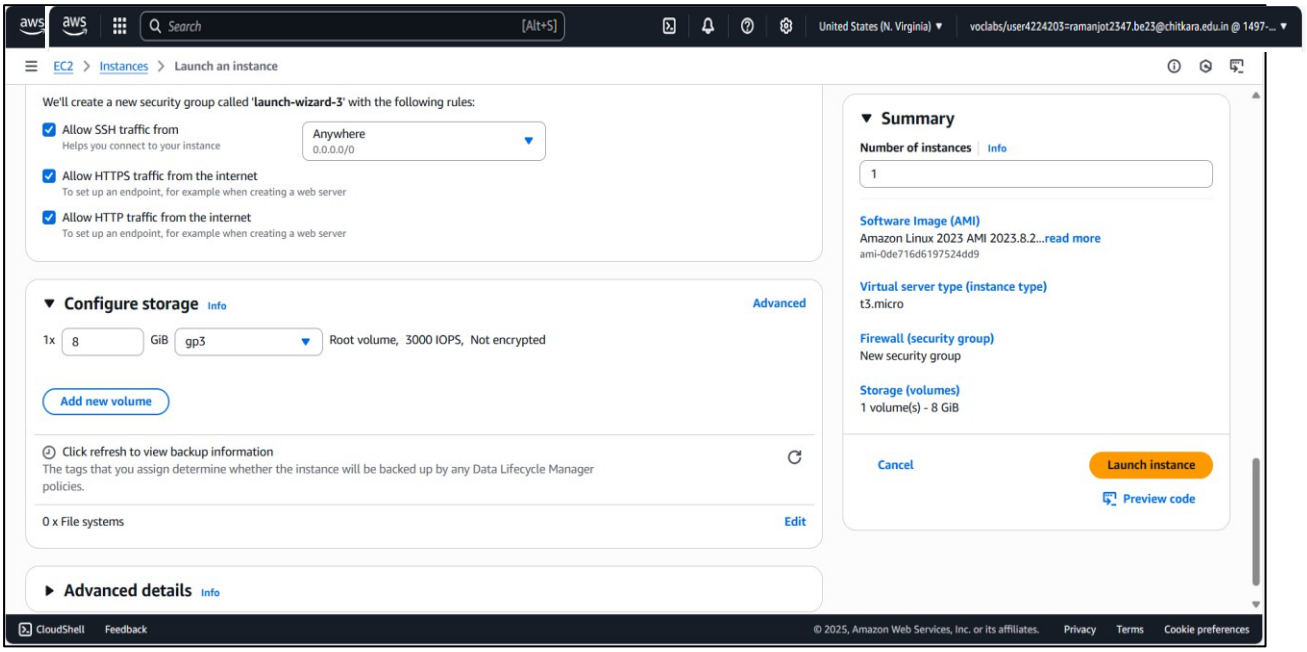


Figure 2.1 Connect to Instance

Step 2: Connect to EC2 Instance

(A) EC2 Instance Connect (Browser-Based)

1. Go to EC2 → Instances → Select Instance → Connect.
2. Choose EC2 Instance Connect tab.

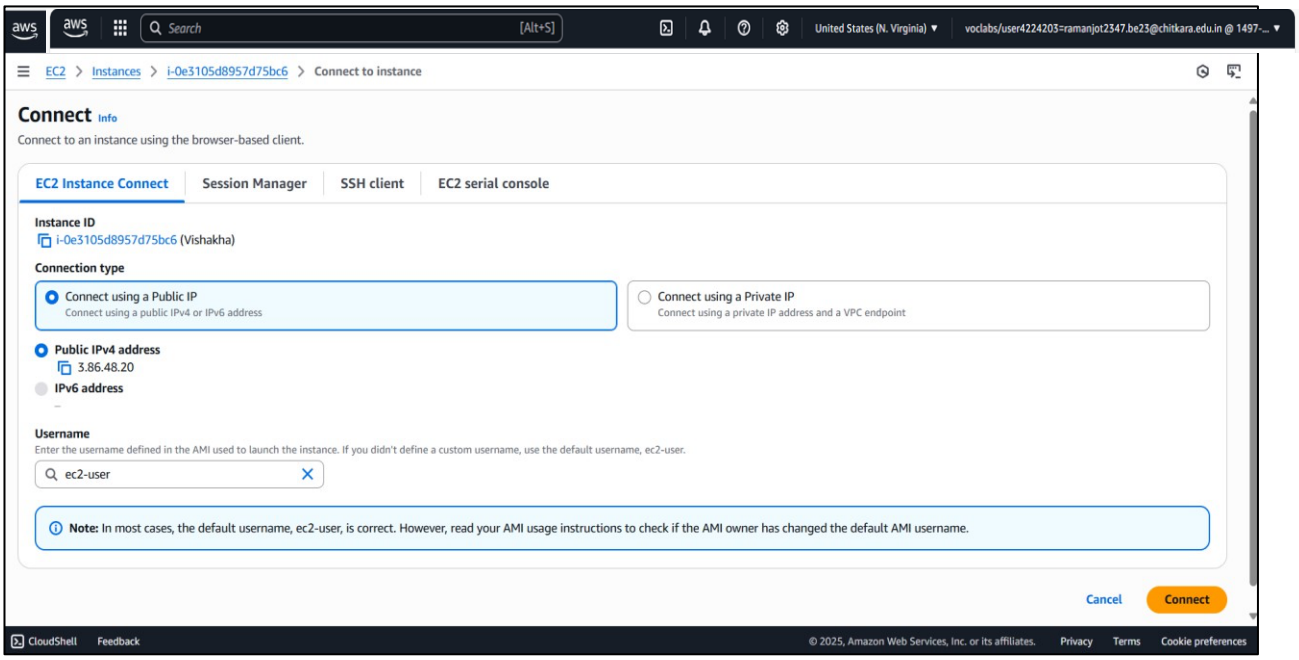


Figure 2.2 Connect with EC2 Instance Connect

3. Click Connect → browser-based terminal opens.

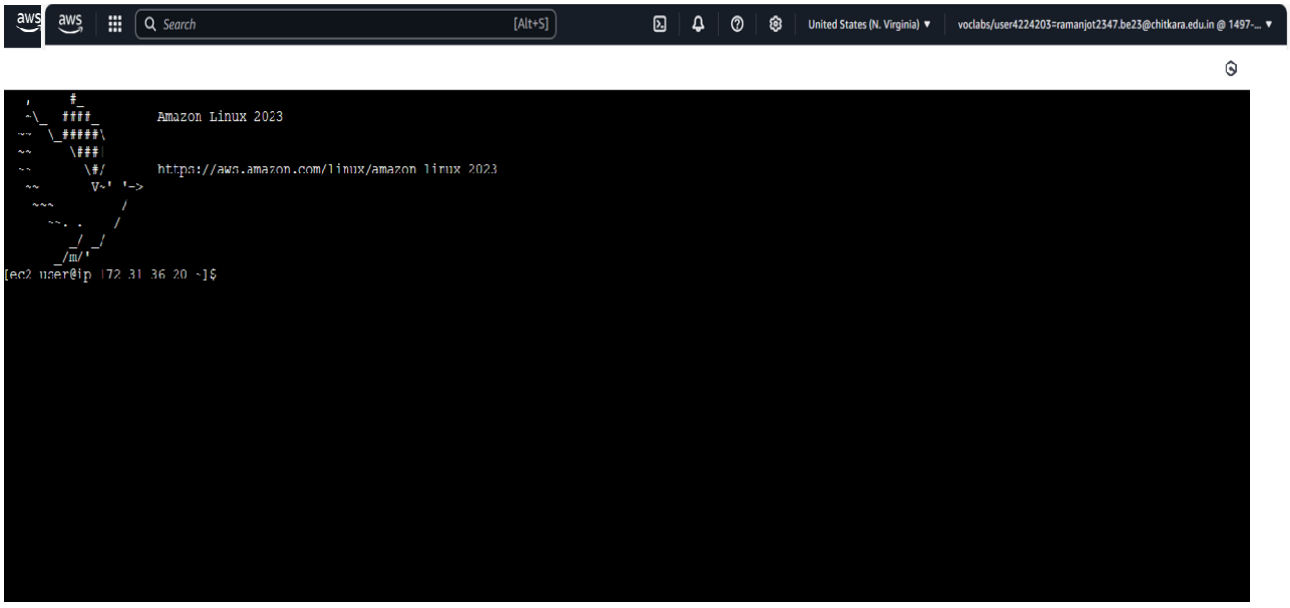


Figure 2.3 Connected to Instance

(B) SSH Client (Linux/macOS Terminal)

Connect Using SSH Client on Linux/Mac

1. Open Terminal
2. Navigate to the folder where your .pem file is saved: cd /path/to/your/file
3. Change Permissions of the Key File
   - Type this command: chmod 400 my-key.pem
   - Replace my-key.pem with your actual key file name.
4. Connect to Your EC2 Instance
5. Type the SSH command: ssh -i my-key.pem ec2-user@<your-public-ip>
6. Replace <your-public-ip> with the Public IPv4 address of your EC2 instance Example: ssh -i my-key.pem ec2-user@13.234.145.21

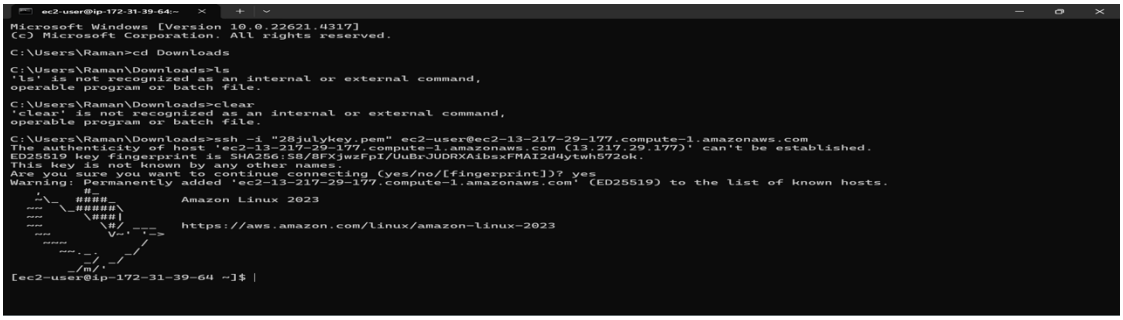


Figure 2.4 Connect to SSH

(C) PuTTY (Windows)

1. Convert .pem to .ppk using PuTTYgen.
2. Open PuTTY, enter the EC2 Public IP.
3. Under SSH → Auth, load the .ppk key file.
4. Click Open → log in as ubuntu

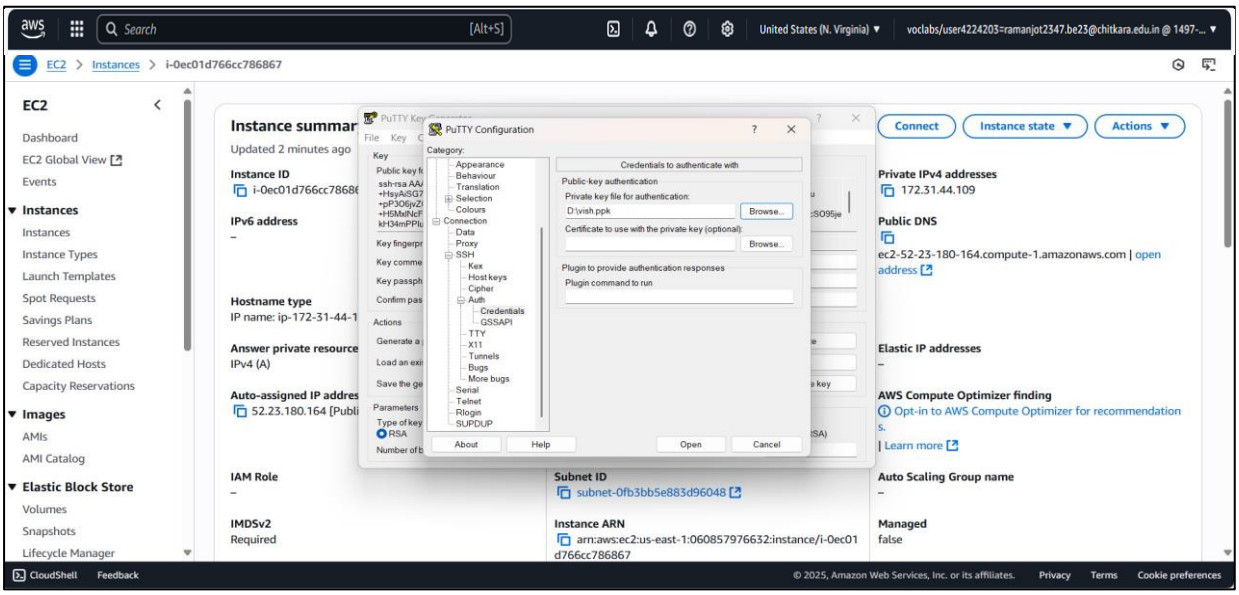


Figure 2.5 Configuring the Putty

2.2 Access and modify Security Group inbound and outbound rules to control traffic for EC2 instances.

(A) Edit Inbound Rules

1. Go to EC2 → Security Groups → Select SG → Edit inbound rules.
2. Add a rule to allow HTTP (Port 80) from Anywhere (0.0.0.0/0).
3. Remove or restrict SSH access if not needed.

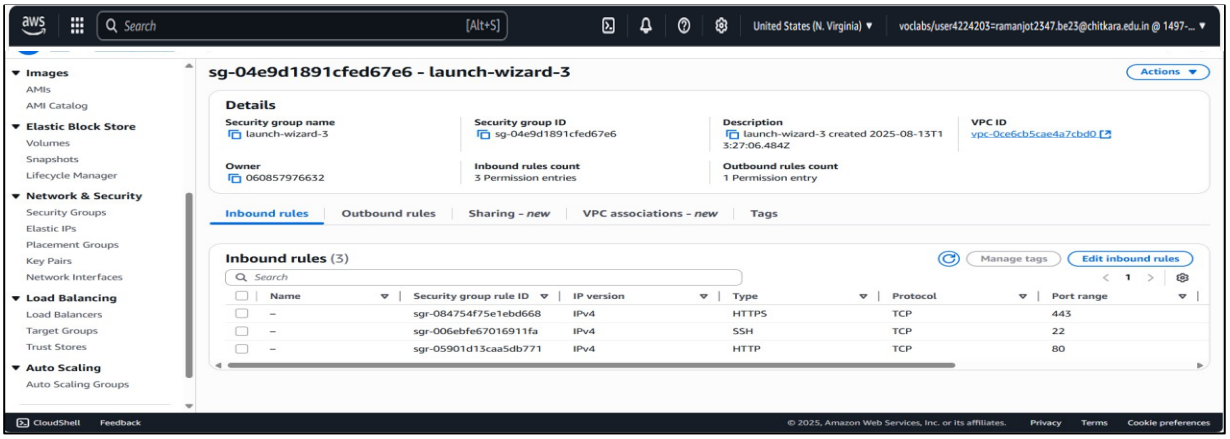


Figure 2.6 Navigate to Security Groups Section under EC2

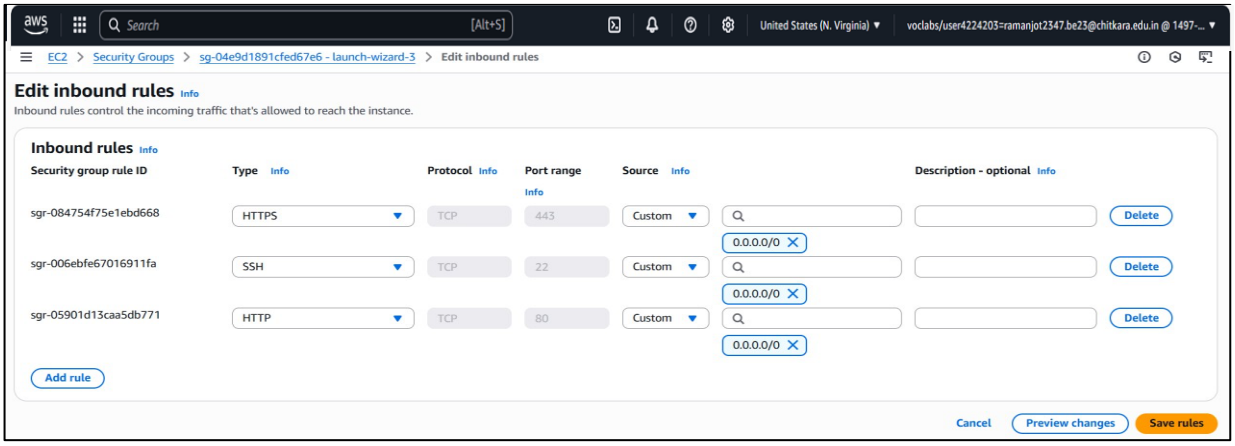


Figure 2.7 Editing the Inbound Rules

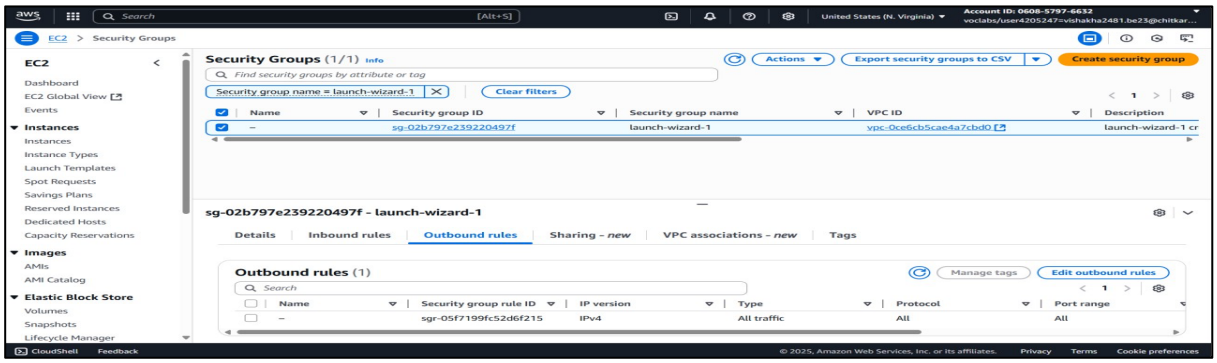


Figure 2.8 Click on Outbound Rules in Security Groups

(A) Edit Outbound Rules:

1. Go to Outbound rules.
2. Configure allowed outbound traffic (default: all traffic).
3. Save changes.

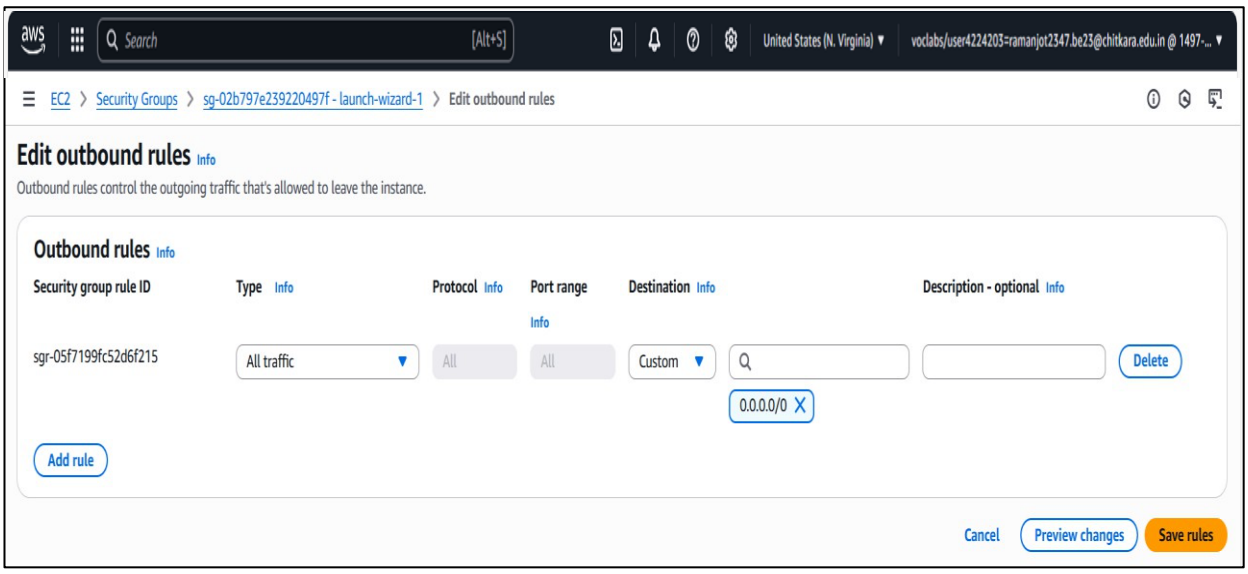


Figure 2.9 Configuring Outbound Rules

Learning Outcomes

- Connected to EC2 instances using EC2 Instance Connect, SSH Client, AWS CLI, and PuTTY.
- Used a key pair file for secure authentication.
- Accessed and modified Security Group inbound/outbound rules to manage network traffic.
- Understood how security groups act as a virtual firewall for AWS resources

Practical No. 3

Practical Title: Set up and configure web servers on EC2 instances, including Apache and Nginxserver. Configure auto-scaling for EC2 instances to handle variable traffic.

Objective:

A. To install and configure Apache and Nginx web servers on EC2 instances.
B. To configure Auto Scaling Groups (ASG) for EC2 instances to handle variable traffic automatically.

(A) Install and Configure Apache and Nginx web servers on EC2 instances Step 1: Launch EC2 Instances

1. Open AWS Management Console → EC2 → Launch Instance.
2. Choose Ubuntu 22.04 LTS AMI (Free-Tier Eligible
3. Select t3.micro instance type.
4. Create/select a key pair (e.g., web-key.pem).
5. Configure Security Group to allow:
   - HTTP (Port 80)
   - HTTPS (Port 443)
   - SSH (Port 22)

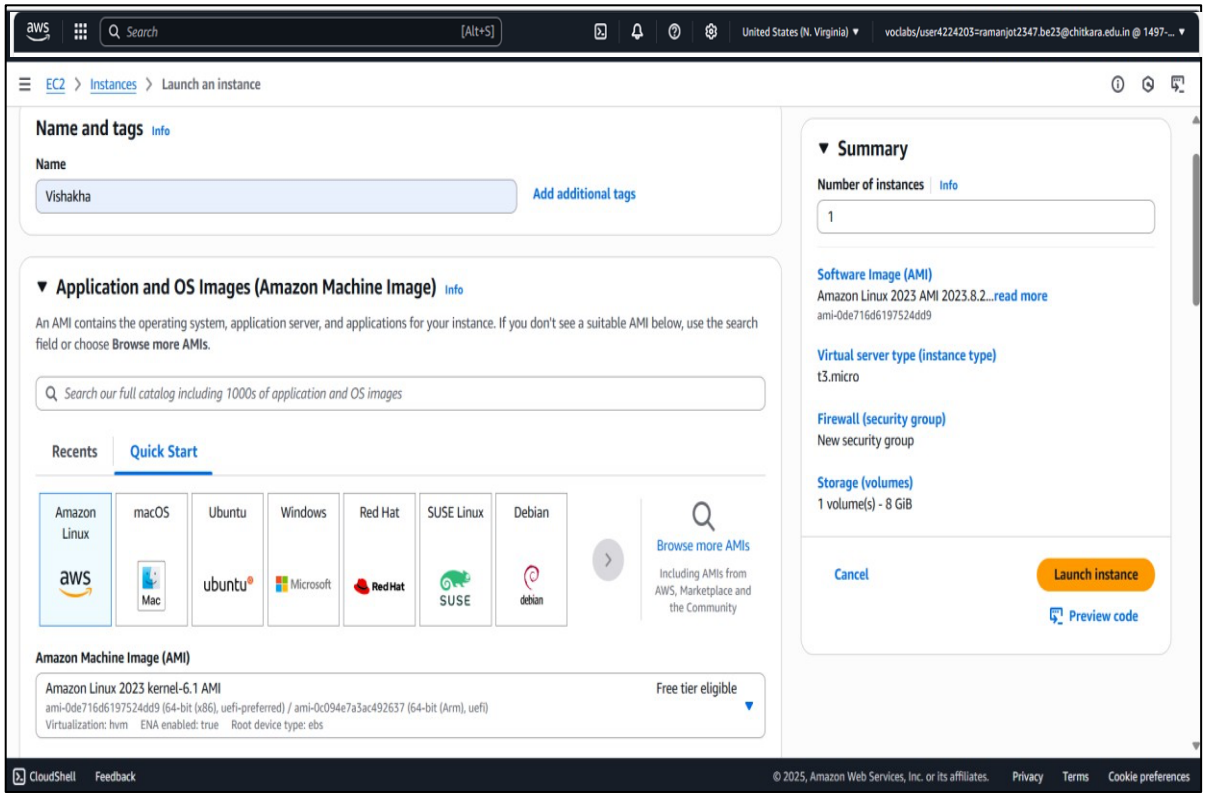


Figure 3.1 Creating an EC2 Instance

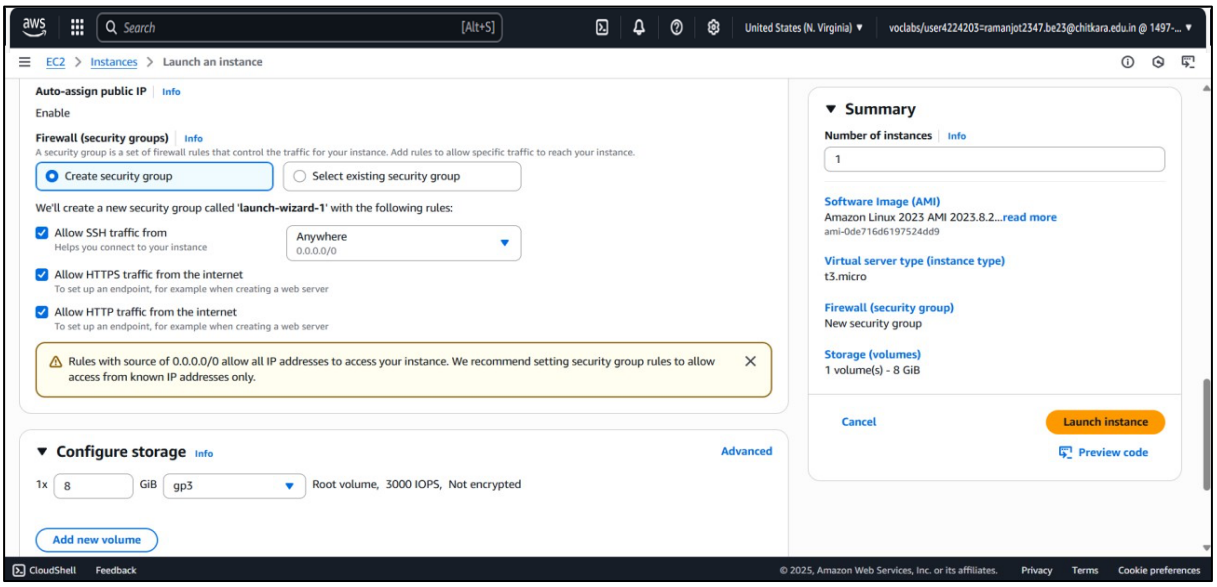


Figure 3.2 Allow traffic on SSH, HTTP

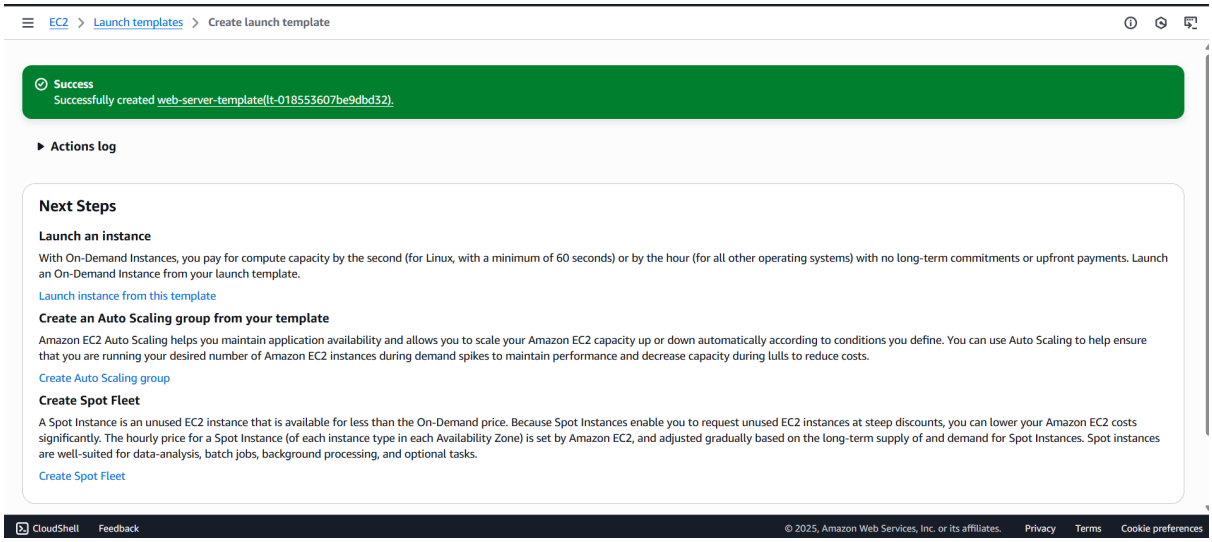


Figure 3.3 Instance Created

Step 2: Update and upgrade the instance

- Run this first to ensure all packages are up to date: sudo apt update -y

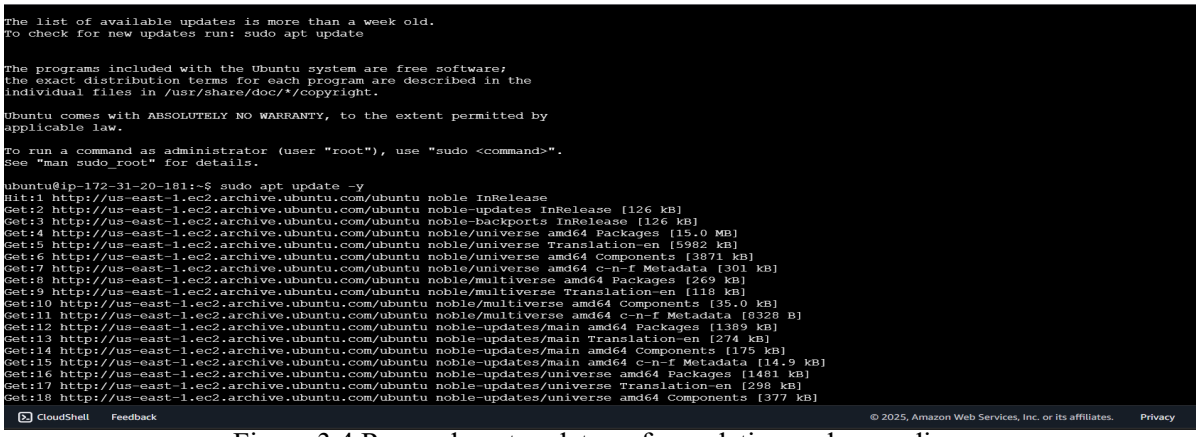


Figure 3.4 Run sudo apt update -y for updating and upgrading

Step 3: Install Apache

- sudo apt install apache2 -

```
ubuntu@ip-172-31-20-181:~$ sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom www-browser
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3 libaprutil1-ldap libaprutil1t64 liblua5.4-0 ssl-cert
0 upgraded, 10 newly installed, 0 to remove and 0 not upgraded.
Need to get 2086 kB of archives.
After this operation, 8090 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 libapr1t64 amd64 1.7.2-3.1ubuntu0.1 [108 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1t64 amd64 1.6.3-1.1ubuntu7 [91.9 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-dbd-sqlite3 amd64 1.6.3-1.1ubuntu7 [11.2 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 libaprutil1-ldap amd64 1.6.3-1.1ubuntu7 [9116 B]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2 [166 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-bin amd64 2.4.58-1ubuntu8.8 [1331 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-data all 2.4.58-1ubuntu8.8 [163 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2-utils amd64 2.4.58-1ubuntu8.8 [97.7 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble-updates/main amd64 apache2 amd64 2.4.58-1ubuntu8.8 [90.2 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntu1 [17.8 kB]
Fetched 2086 kB in 0s (32.9 MB/s)
Preconfiguring packages ...
Selecting previously unselected package libapr1t64:amd64.
(Reading database ... 103354 files and directories currently installed.)
Preparing to unpack .../0-libapr1t64_1.7.2-3.1ubuntu0.1_amd64.deb ...
Unpacking libapr1t64:amd64 (1.7.2-3.1ubuntu0.1) ...
Selecting previously unselected package libaprutil1t64:amd64.
Preparing to unpack .../1-libaprutil1t64_1.6.3-1.1ubuntu7_amd64.deb ...
Unpacking libaprutil1t64:amd64 (1.6.3-1.1ubuntu7) ...
Selecting previously unselected package libaprutil1-dbd-sqlite3:amd64.
Preparing to unpack .../2-libaprutil1-dbd-sqlite3_1.6.3-1.1ubuntu7_amd64.deb ...
CloudShell  Feedback  © 2025, Amazon Web Services, Inc. or its affiliates.  Privacy  Terms  Cookie preferences
```

Figure 3.5 Install Apache

- sudo systemctl start apache2 - start Apache immediately
- sudo systemctl enable apache2 - make it start automatically on boot
- sudo systemctl status apache2 - verifies apache is working

```
Restarting the system to load the new kernel will not be handled automatically, so you should consider rebooting.

Restarting services...

Service restarts being deferred:
 systemctl restart networkd-dispatcher.service
 systemctl restart unattended-upgrades.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-20-181:~$ sudo systemctl start apache2
ubuntu@ip-172-31-20-181:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
ubuntu@ip-172-31-20-181:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-09-07 10:30:19 UTC; 5min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 7264 (apache2)
      Tasks: 55 (limit: 1008)
     Memory: 5.3M (peak: 5.4M)
        CPU: 55ms
     CGroup: /system.slice/apache2.service
             ├─7264 /usr/sbin/apache2 -k start
             ├─7266 /usr/sbin/apache2 -k start
             └─7267 /usr/sbin/apache2 -k start

Sep 07 10:30:19 ip-172-31-20-181 systemd[1]: Starting apache2.service - The Apache HTTP Server...
Sep 07 10:30:19 ip-172-31-20-181 systemd[1]: Started apache2.service - The Apache HTTP Server.
ubuntu@ip-172-31-20-181:~$
CloudShell  Feedback  © 2025, Amazon Web Services, Inc. or its affiliates.  Privacy
```

Figure 3.6 Running the above following to check if apache is working

Step4: Test in browser:

- Copy your EC2 public IP from the AWS console.
- Open in your browser - http://<your-public-ip>/

Figure 3.7 Test in Browser

Step 5: Customizing Web Pages using Apache:

- Run this command in the ubuntu terminal

1. echo '<body style="background-color:lavender; color:darkblue; font-family:sans-serif;"><h1>My Styled Apache Page</h1> This page has custom colors! </body>' | sudo tee /var/www/html/index.html

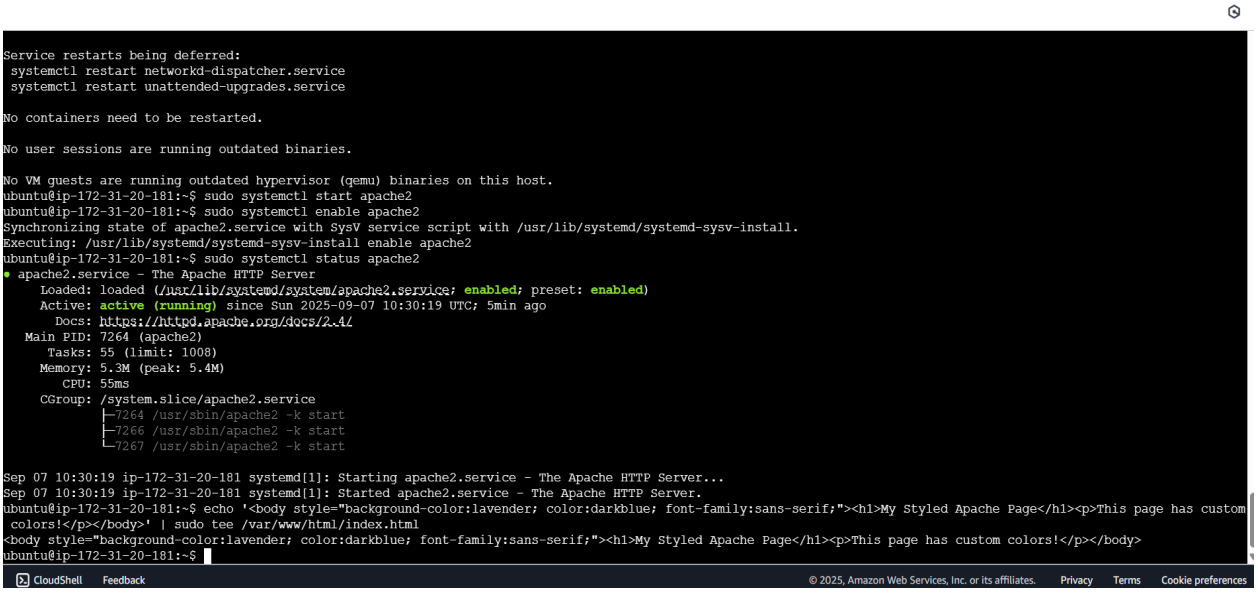


Figure 3.8 Customizing Web Page

2. After running this command, refresh your browser page and you will see the changes

Figure 3.9. Apache Server Running on Localhost

3. echo "<h1>Welcome to My Apache Server\!</h1>" | sudo tee /var/www/html/index.html

```
ubuntu@ip-172-31-20-181:~$ echo "<h1>Welcome to My Apache Server\!</h1>" | sudo tee /var/www/html/index.html
<h1>Welcome to My Apache Server\!</h1>
ubuntu@ip-172-31-20-181:~$
```

Figure 3.10. Command to start the server

4. After running this command, refresh your browser page and you will see the changes

Figure 3.11. Changes Made

Step 6: For NGINX

1. Stop and disable Apache2 by running the below commands
   - sudo systemctl stop apache2
   - sudo systemctl disable apache2

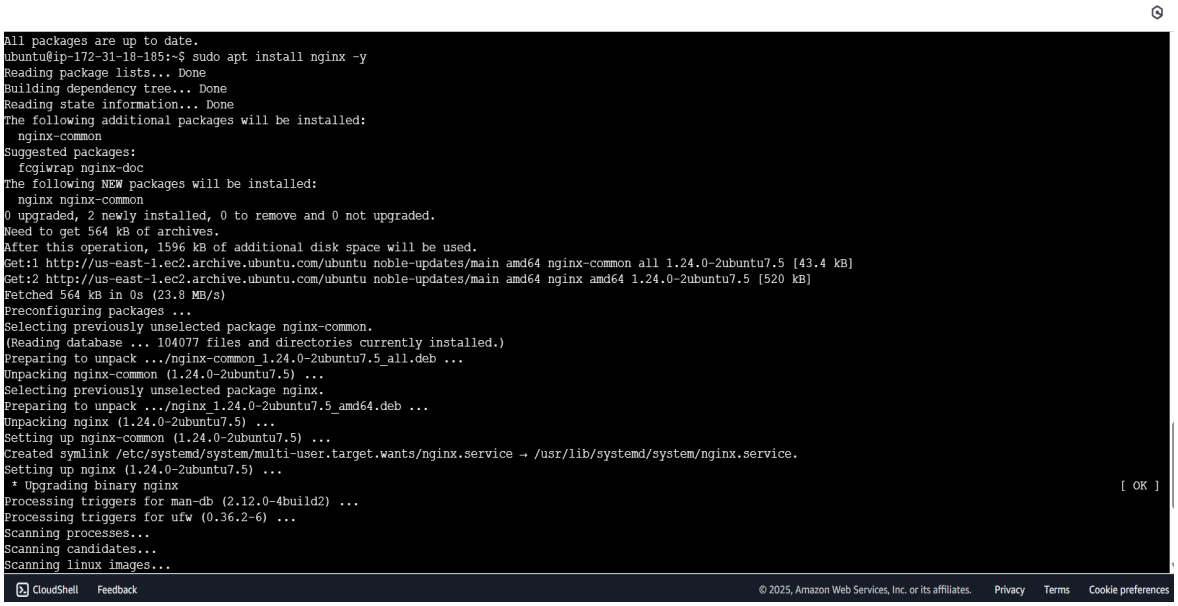
   This will free up port 80

```
ubuntu@ip-172-31-18-185:~$ sudo systemctl stop apache2
ubuntu@ip-172-31-18-185:~$ sudo systemctl disable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install disable apache2
Removed "/etc/systemd/system/multi-user.target.wants/apache2.service".
ubuntu@ip-172-31-18-185:~$
```

Figure 3.11. Stop Apache

2. Install Nginx (if not already installed)
   - sudo apt update refreshes the package list.
   - sudo apt install nginx -y installs Nginx and automatically confirms installation.

Figure 3.12. Install Nginx



- sudo systemctl start nginx - Start Nginx
- sudo systemctl enable nginx - Ensures Nginx starts automatically when Ubuntu restarts.

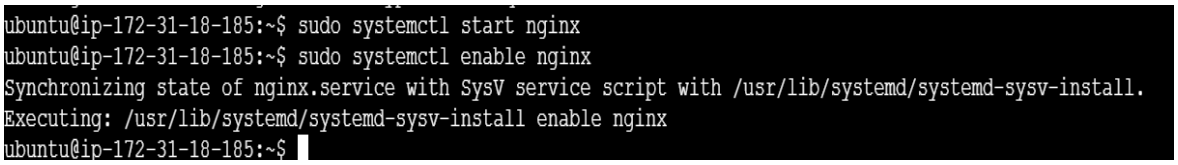


Figure 3.13. Automatically Starting Nginx

Step 7: Access Nginx in your browser

1. Find your Ubuntu server's public IP - hostname -I
2. Open a browser and visit - http://<Public_IP>
3. Make sure that nginx is using Port 80 by running the below command

- sudo nano /etc/nginx/sites-enabled/default

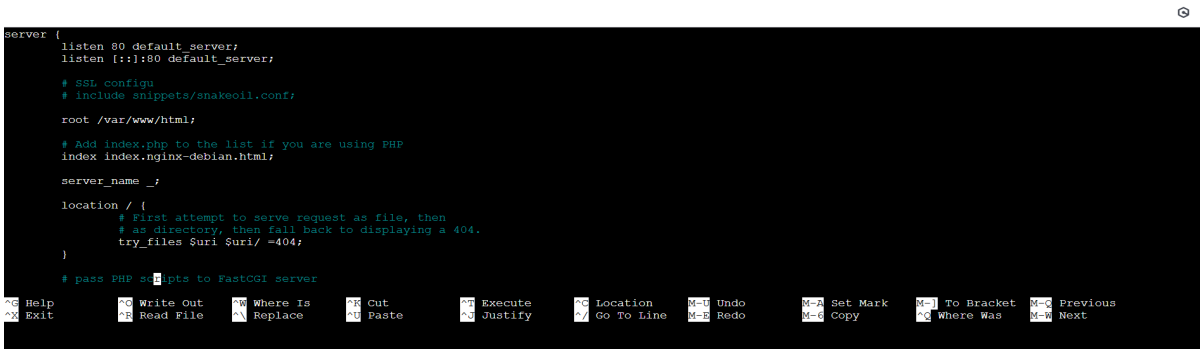


Figure 3.14. Edit and write code to display on server

4. After running the above command restart the nginx - sudo systemctl restart nginx

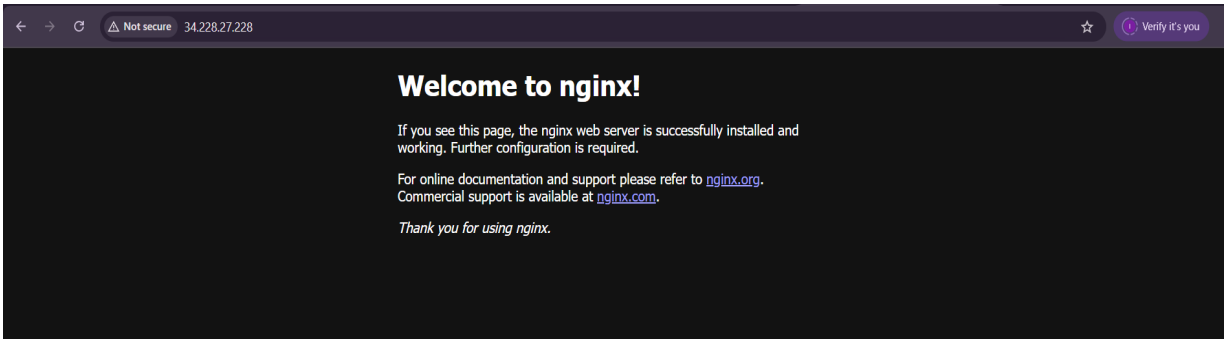


Figure 3.15. Accessing Nginx on Browser

Step 8: Customize Nginx Page

1. echo "<h1>Welcome to My Nginx Server!</h1>" | sudo tee /usr/share/nginx/html/index.html

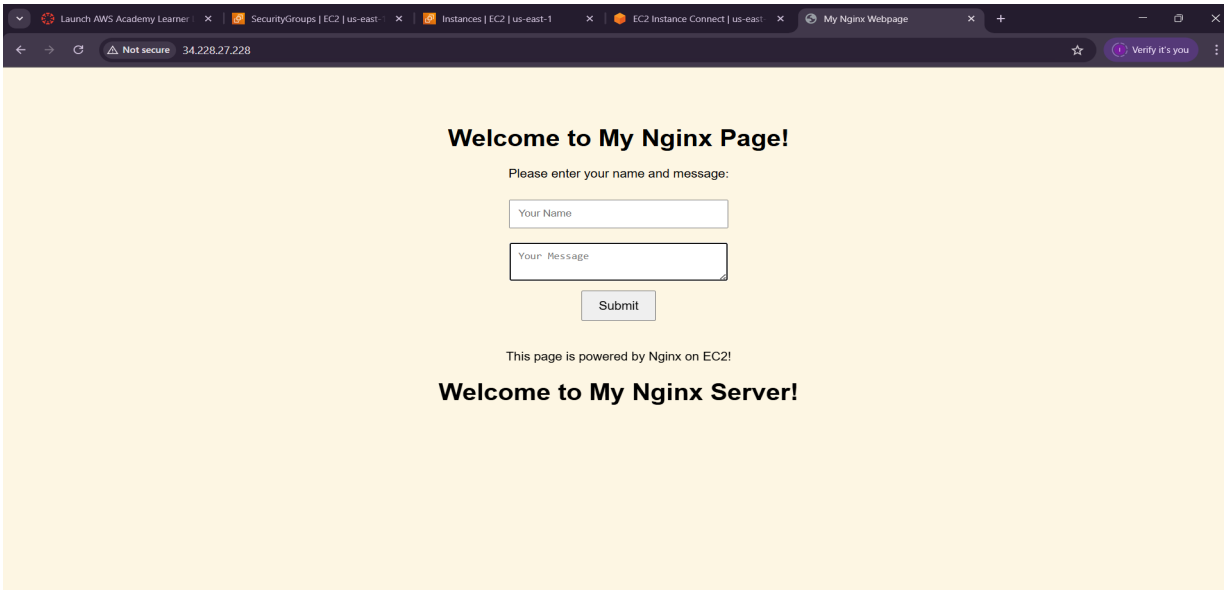
Figure 3.16 Customizing Ngix

2. Create a Full HTML Page with Form and Style

```
<!DOCTYPE html>
<html>
<head>
  <title>My Nginx Webpage</title>
  <style>
    body {
      background-color: #fdf6e3;
      font-family: Arial, sans-serif;
      text-align: center;
      padding: 50px;
    }
    input, textarea {
      padding: 10px;
      margin: 10px;
      width: 250px;
    }
    button {
      padding: 10px 20px;
      font-size: 16px;
    }
  </style>
</head>
<body>
  <h1>Welcome to My Nginx Page!</h1>
  <p>Please enter your name and message:</p>
  <form onsubmit="alert('Thank you for submitting!'); return false;">
    <input type="text" placeholder="Your Name" required><br>
    <textarea placeholder="Your Message" required></textarea><br>
    <button type="submit">Submit</button>
  </form>
  <p style="margin-top:40px;">This page is powered by Nginx on EC2!</p>
</body>
</html>
```

Figure 3.17 Customizing the webpage

Figure 3.17 Webpage running using Nginx



(B) Configure auto-scaling for EC2 instances to handle variable traffic. Step 1: Create a Launch Template

1. **Go to EC2 Console → Launch Templates** → Click **Create launch template**.
2. **Fill in Basic Information:**
   - **Name:** e.g., web-server-template
   - **AMI ID:** Use the custom AMI you created.
   - **Instance type:** e.g., t2.micro or t3.micro
   - **Key pair:** Select your existing key.
   - **Security Group:** Ensure it allows HTTP (port 80) or 8080.
   - **User Data:** (Optional) Add shell script to auto-install web server if not in AMI.
3. Click **Create launch template**.

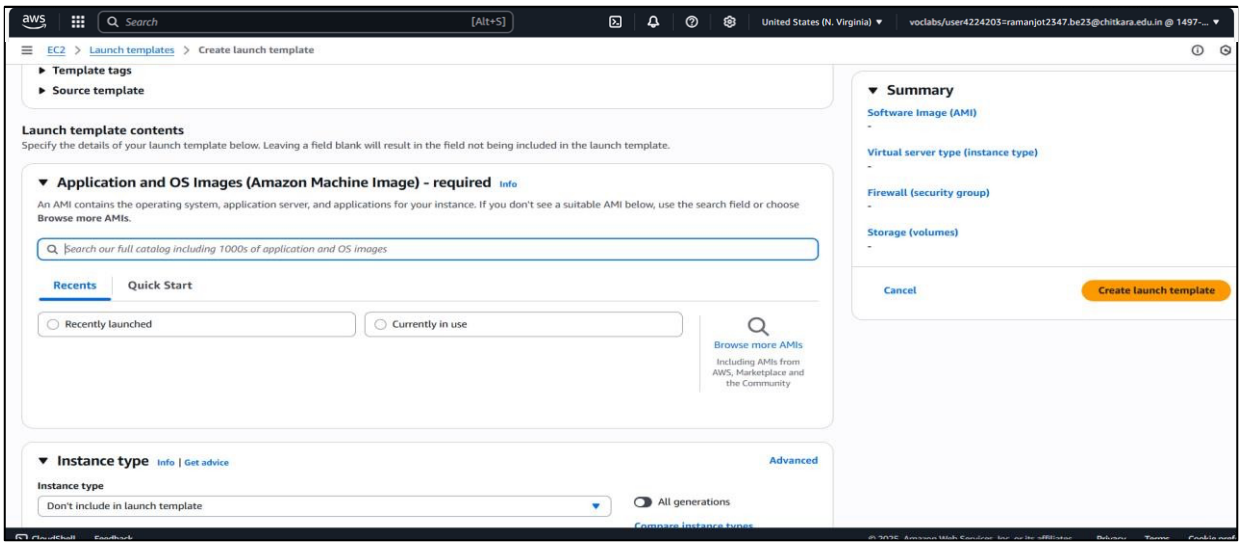


Figure 3.18 Navigate to Launch Template

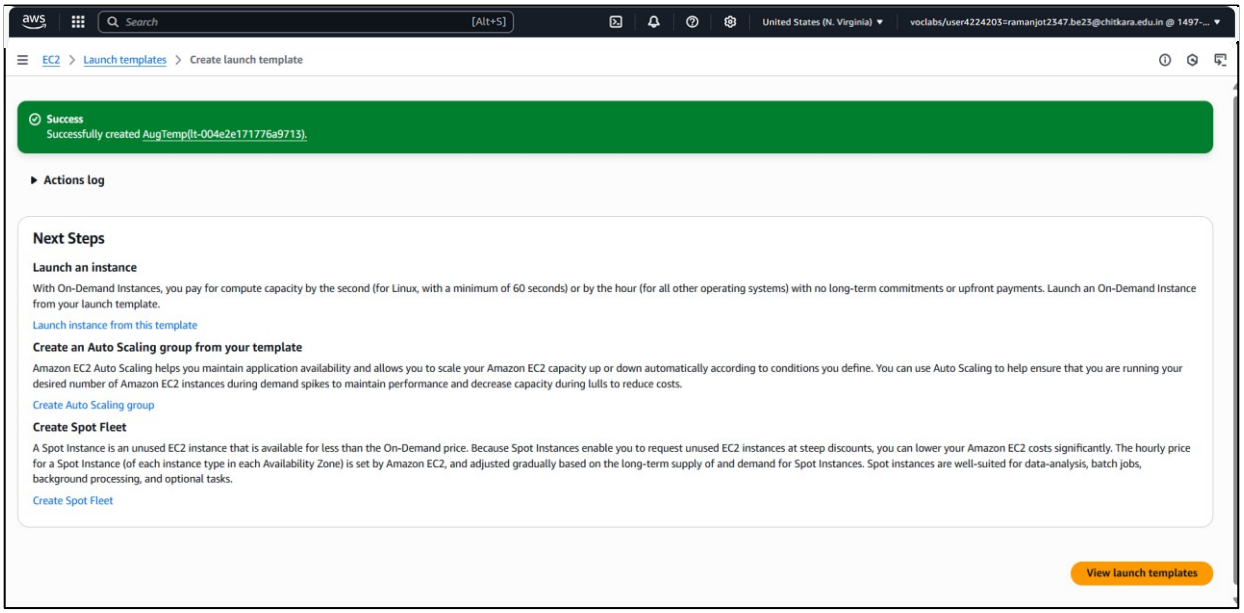


Figure 3.19 Instance Created

Step 2: Create an Auto Scaling Group (ASG)

1. Go to **EC2 Console → Auto Scaling Groups →** Click **Create Auto Scaling group**.

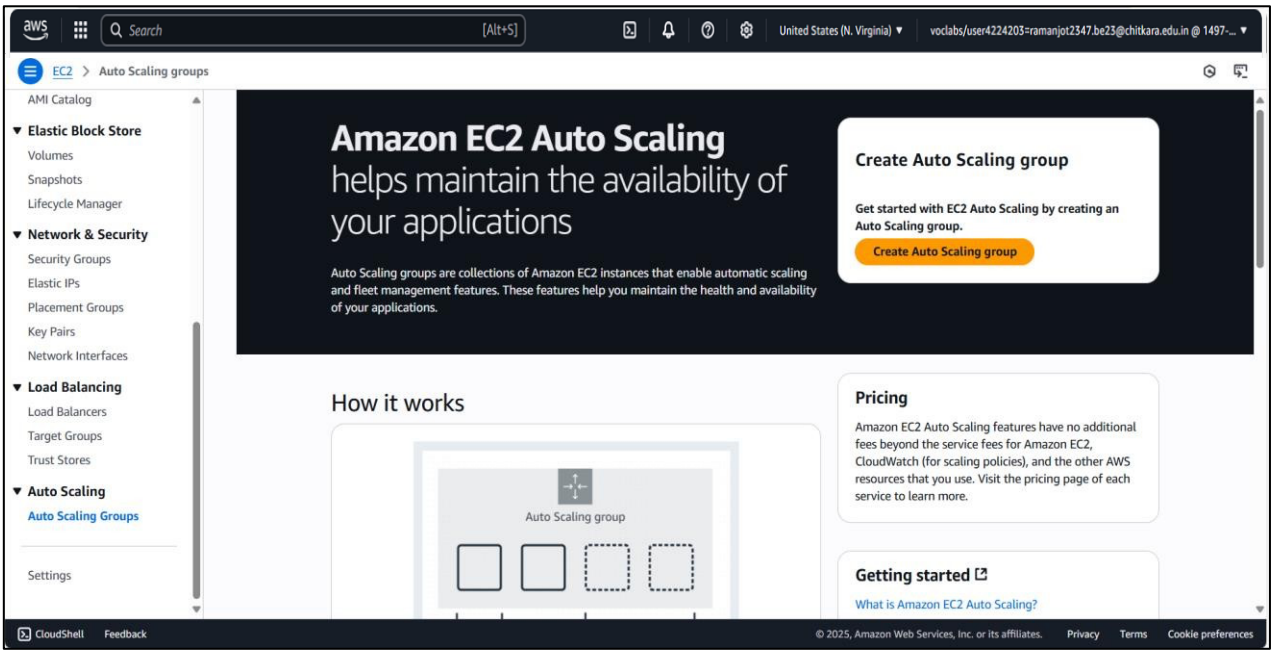


Figure 3.20 Click on Create Auto Scaling Group

2. **Name:** e.g., web-auto-scaling
3. **Choose launch template:** Select the one you just created.
4. Click **Next**.

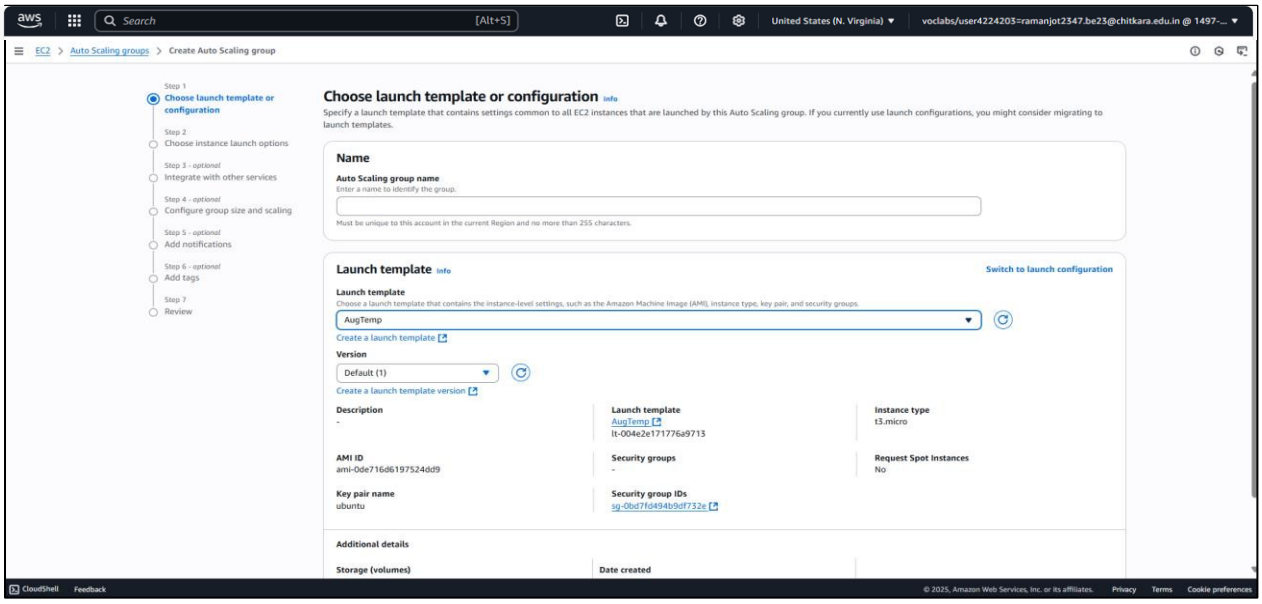


Figure 3.21 Choose the template

Step 3: Configure Network and Subnet

1. Select a **VPC** and **at least 2 subnets in different Availability Zones** (for high availability).
2. Enable **public IP** assignment if needed.

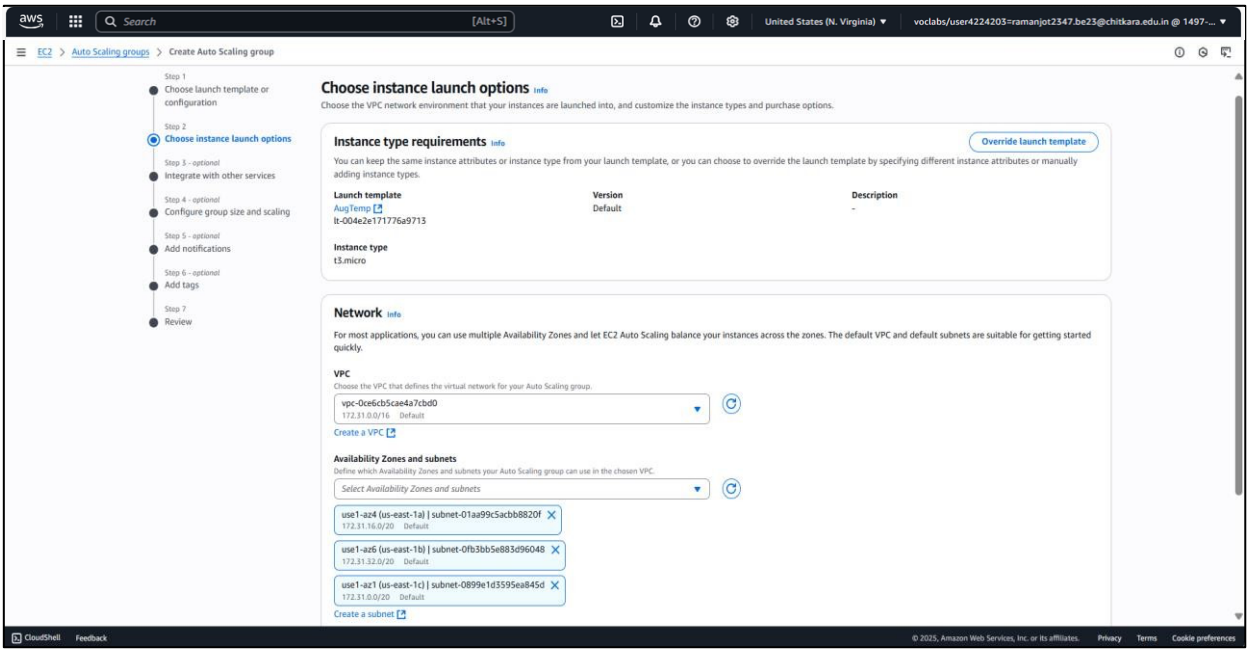


Figure 3.22 Configure Network

Step 4: Configure Load Balancer

1. Choose **Attach to a new load balancer** (Application Load Balancer).
2. Set:
    - **Load balancer name**

- **Scheme: Internet-facing**
- **Listeners: HTTP port 80**

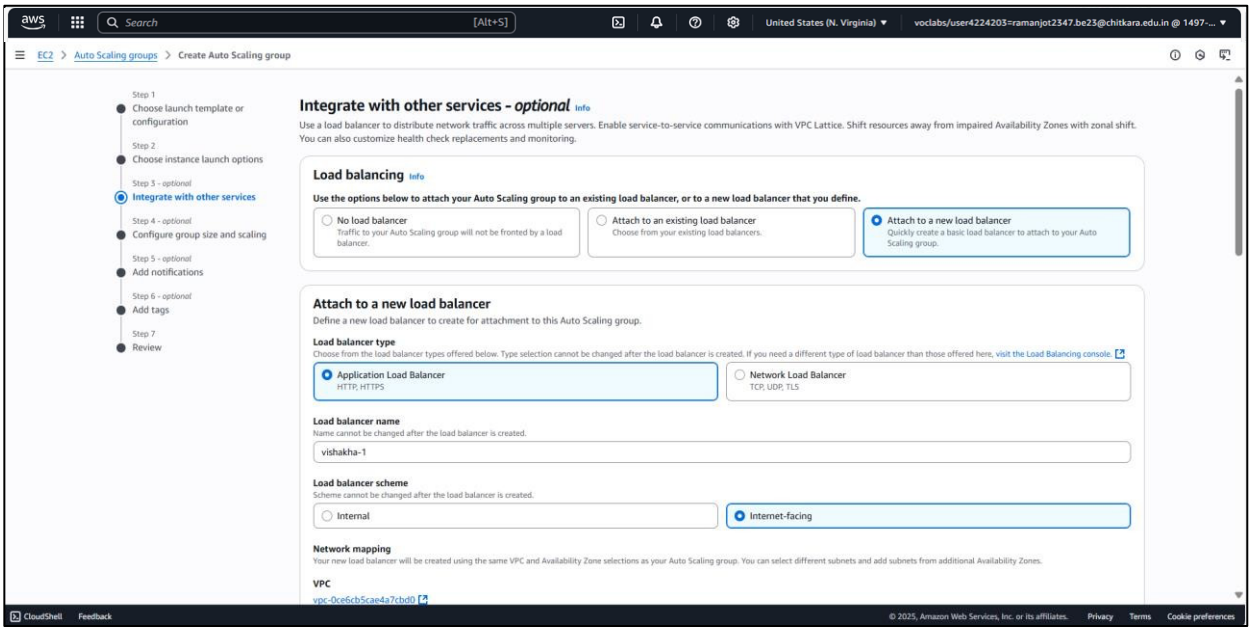


Figure 3.23 Configure Load Balancer

3. Add at least **2 Availability Zones**.
4. Create or select a **Target Group**, protocol: HTTP, port 80 (or 8080)

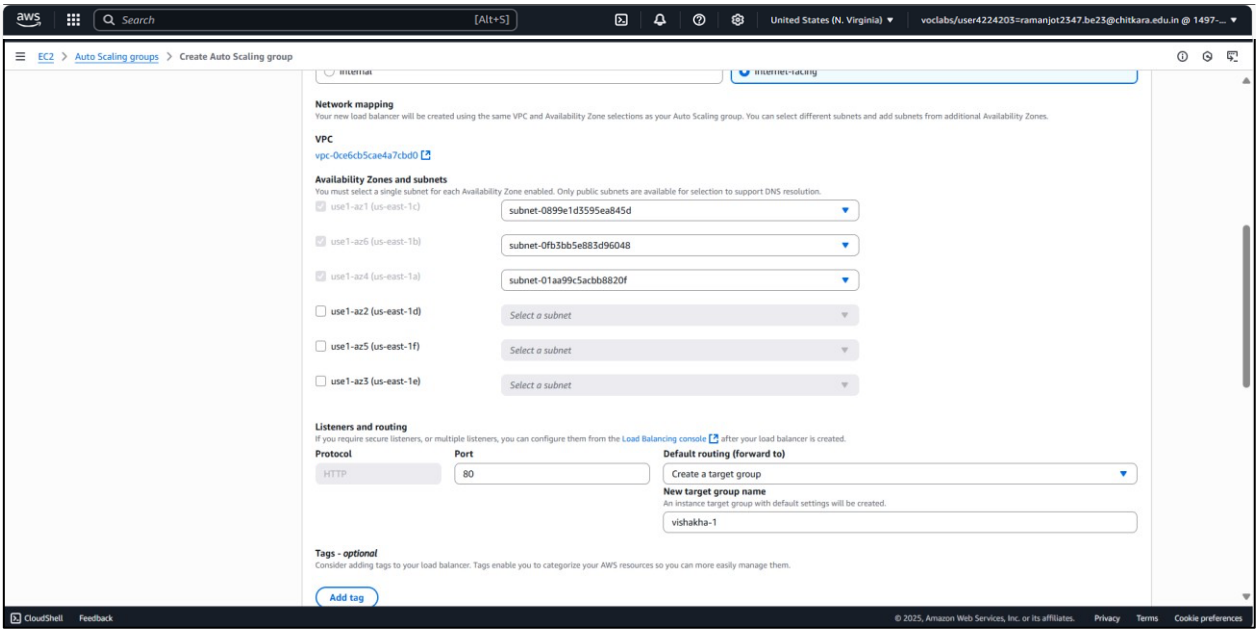


Figure 3.24 Create ASG

Step 5: Configure Scaling Policies

1. **Desired capacity:** 2 (minimum recommended)
2. **Minimum capacity:** 1
3. **Maximum capacity:** 3 (or higher based on expected traffic)

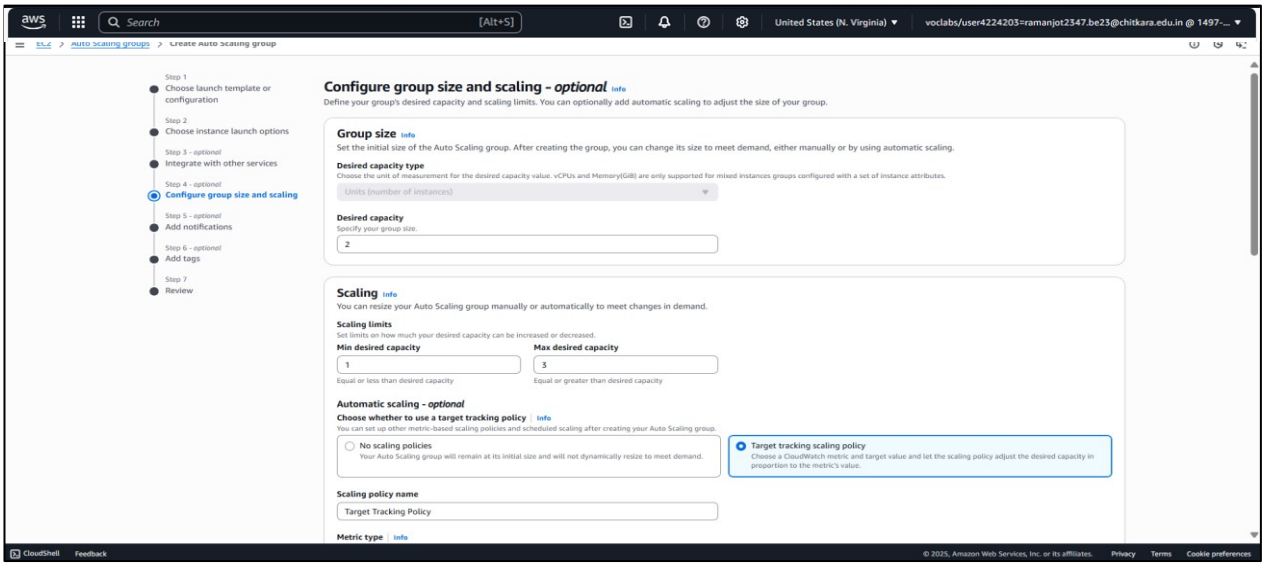


Figure 3.25 Configure group size and scaling

4. Choose **Target tracking scaling policy**:
    - Metric type: **Average CPU utilization**
    - Target value: e.g., **60%**
    - This means add or remove instances to keep average CPU at 60%.

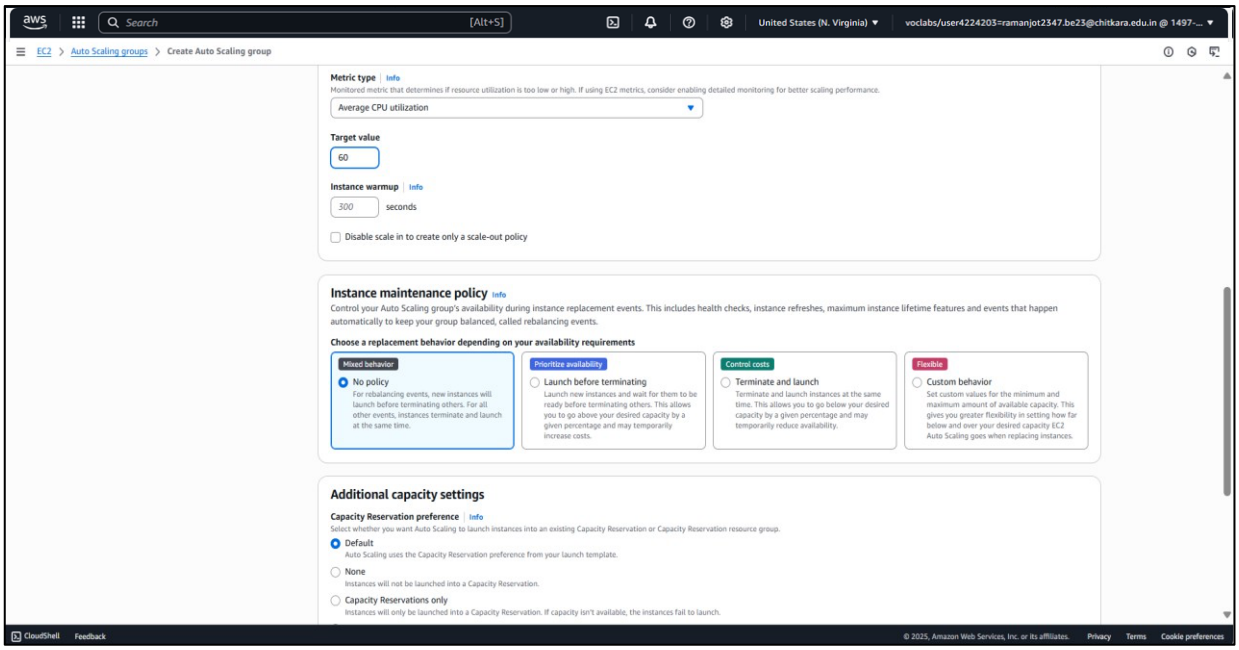


Figure 3.26. Set Target value to 60

Step 6: Review and Create

- Review all configuration.
- Click **Create Auto Scaling group**.

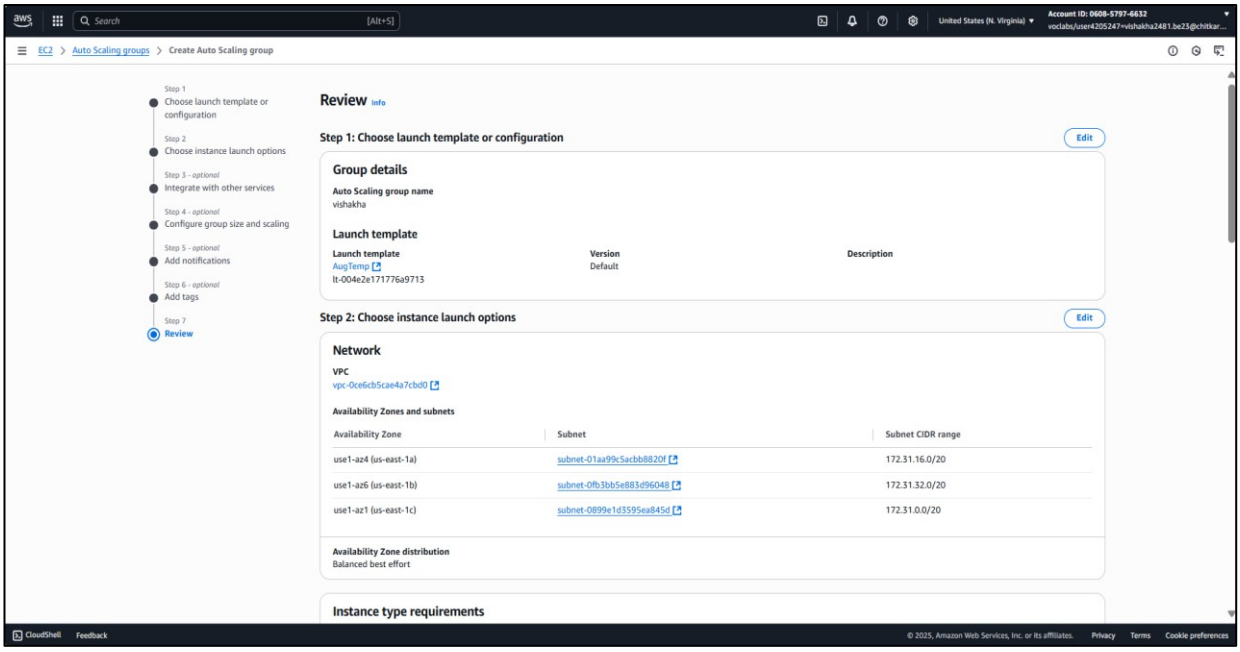


Figure 3.27. Review the above Steps

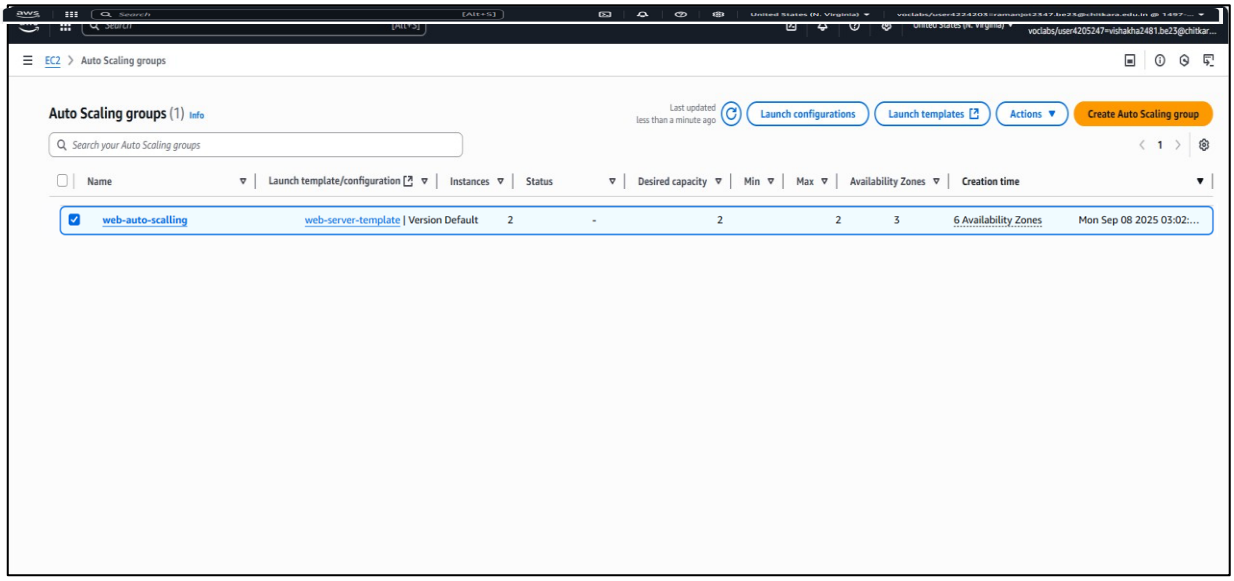


Figure 3.28. Auto Scaling Group Created

Learning Outcomes:

- Installed and configured Apache and Nginx web servers on AWS EC2.
- Created and used Launch Templates for quick instance deployment.
- Configured Auto Scaling Groups to automatically adjust the number of instances based on traffic load.
- Understood the importance of scalability and high availability in cloud environments.

Practical No. 4

Practical Title: Create an Amazon S3 bucket, upload objects, set up access controls with bucket policies, and use it for hosting static content.

Objective:

1. To create an Amazon S3 bucket for storing data.
2. To upload objects (files such as HTML, CSS, images) into the S3 bucket.
3. To configure access controls using bucket policies for secure and controlled access.
4. To enable static website hosting on the S3 bucket.
5. To make the hosted static content (web pages) accessible publicly through the bucket's endpoint.

Step 1: Create an S3 Bucket

1. Sign in to your **AWS Management Console** → Go to **S3 service**.

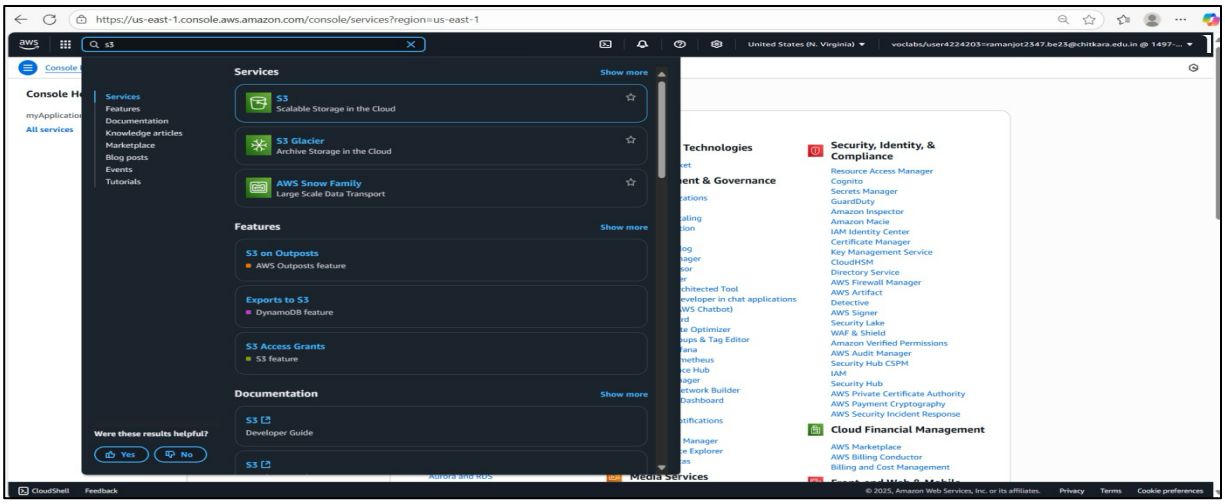


Figure 4.1 Search S3

2. Click on **Create bucket**.

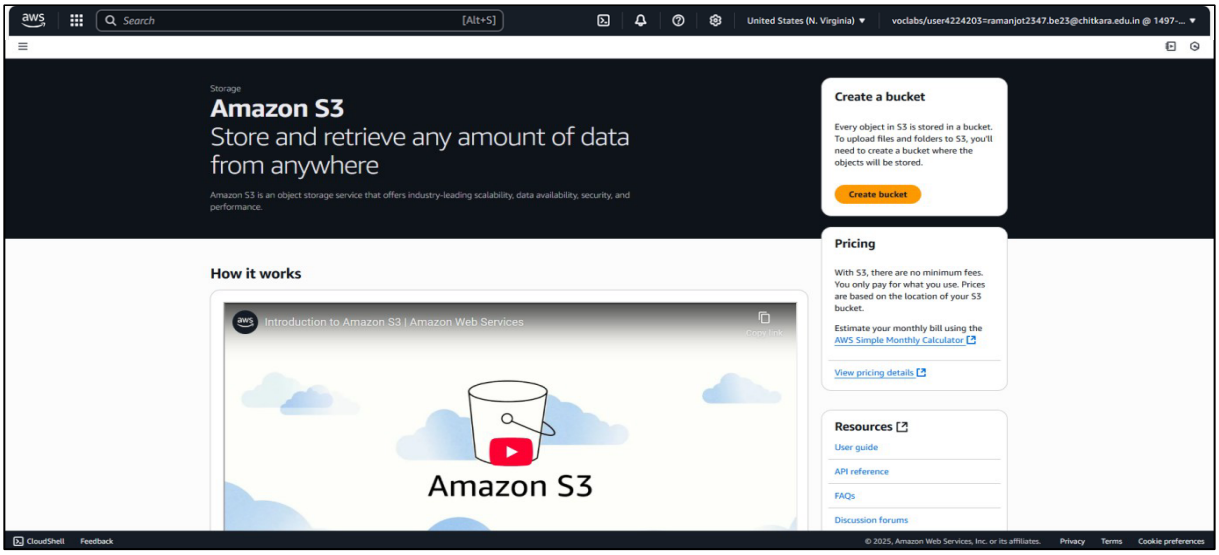


Figure 4.2 Create Bucket

3. Bucket names must be globally unique.

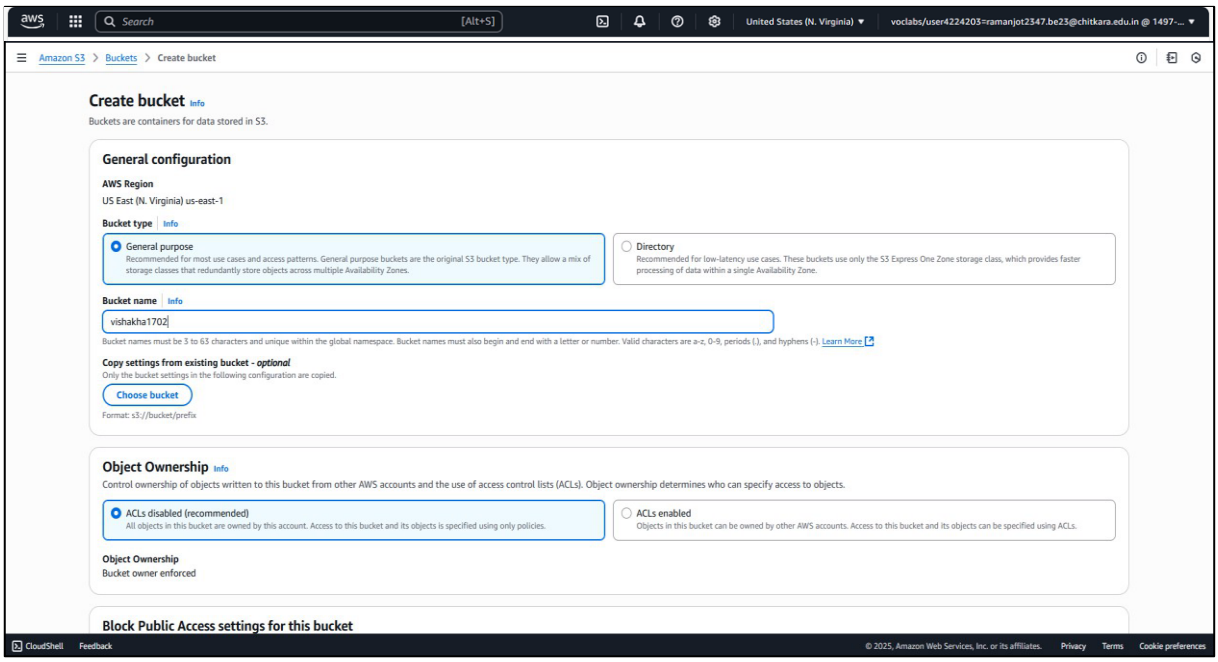


Figure 4.3 Bucket name should be Global

4. Select an **AWS Region** (pick the one closest to your users).
5. In **Block Public Access settings**, **uncheck "Block all public access"** → Confirm the warning (since you need the bucket public for hosting).

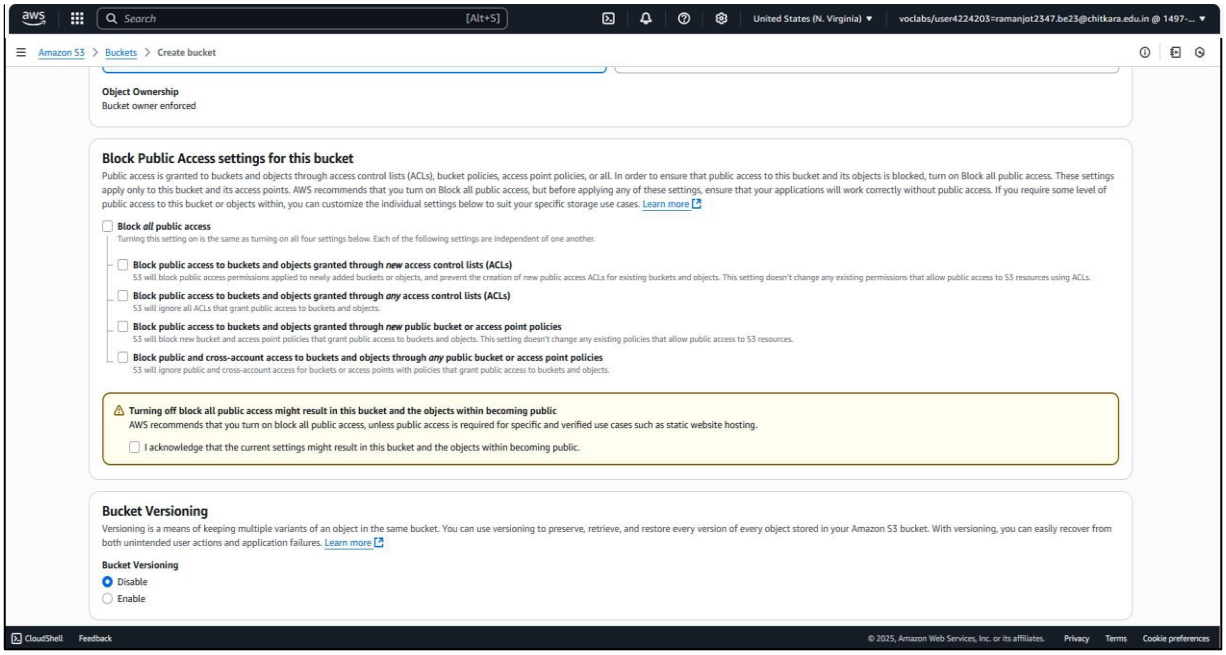


Figure 4.4 Block all public access

6. Click **Create bucket**.

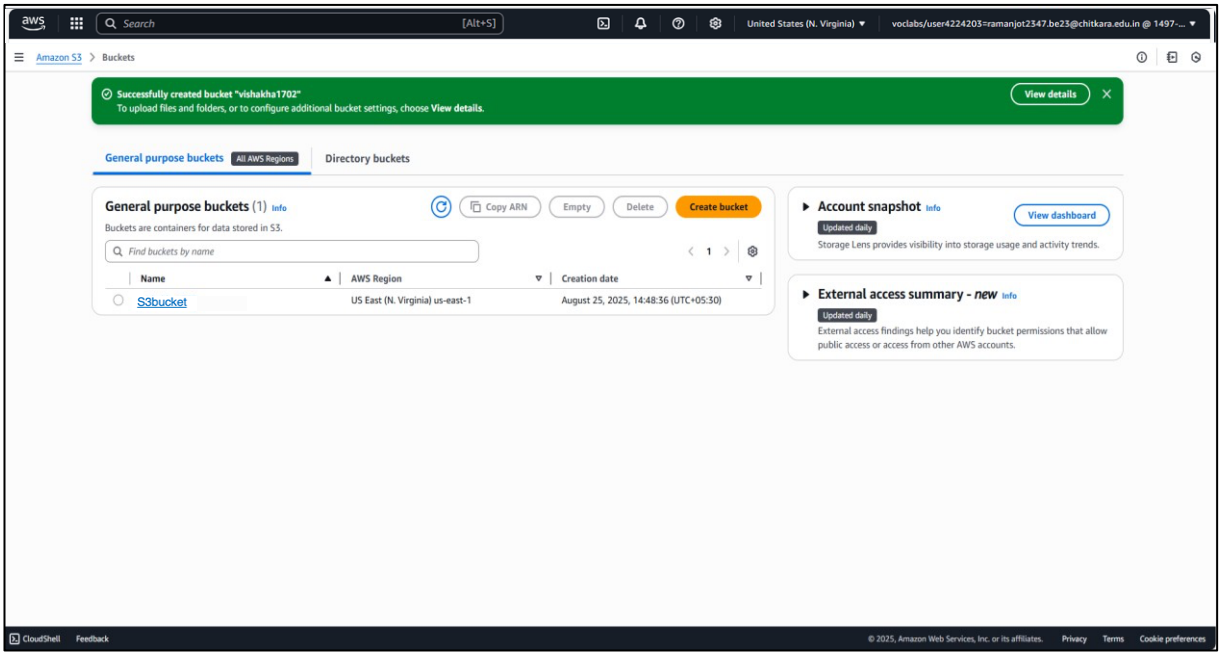


Figure 4.5 Create Bucket

Step 2: Upload Objects (HTML, CSS, JS, Images)

1. Open your bucket.
2. Click **Upload**.

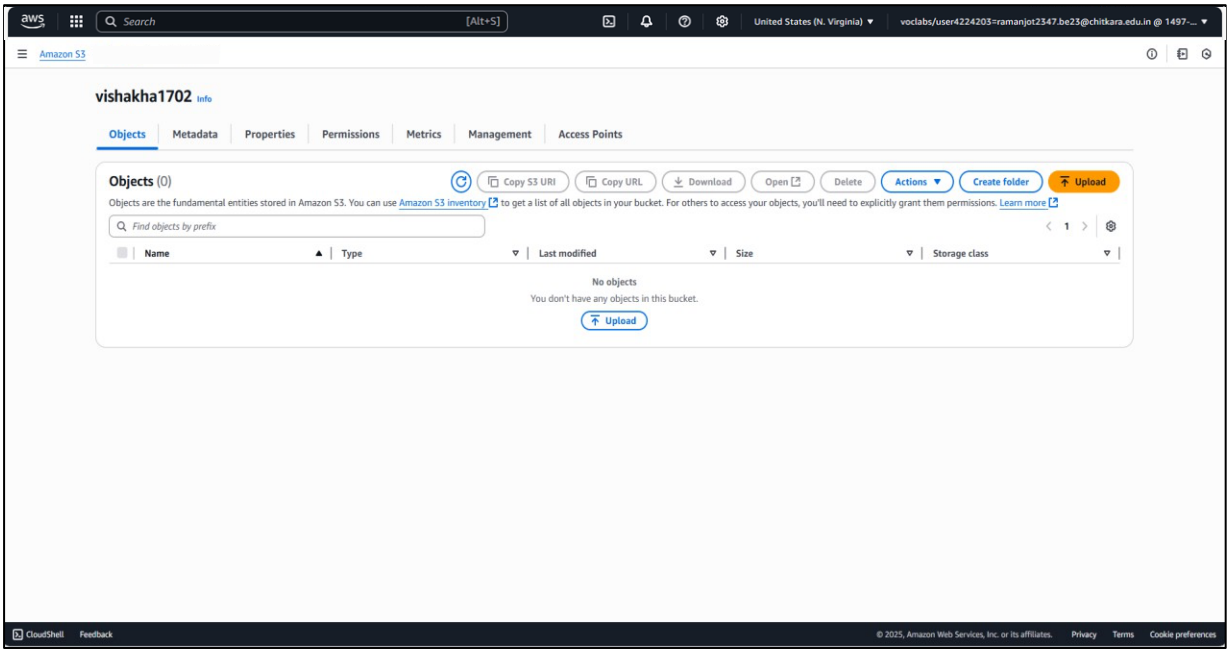


Figure 4.6 Upload Object

3. Select your **index.html**, CSS, JS, or image files.

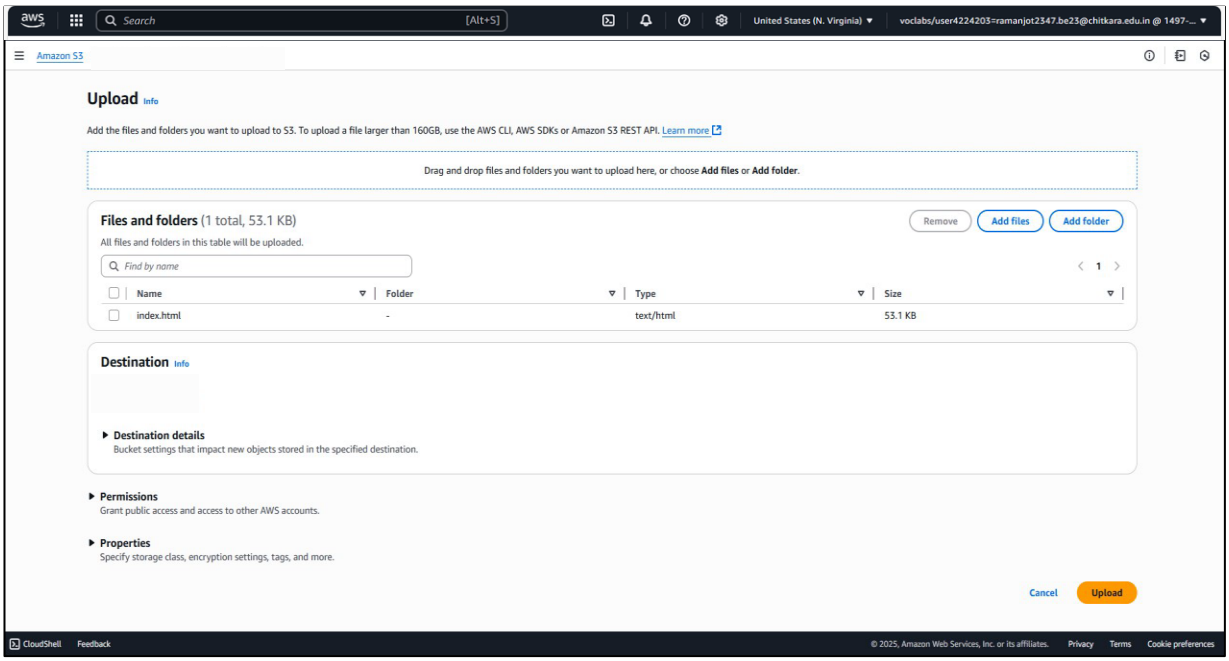


Figure 4.7 Select your index.html

4. Click **Upload**.

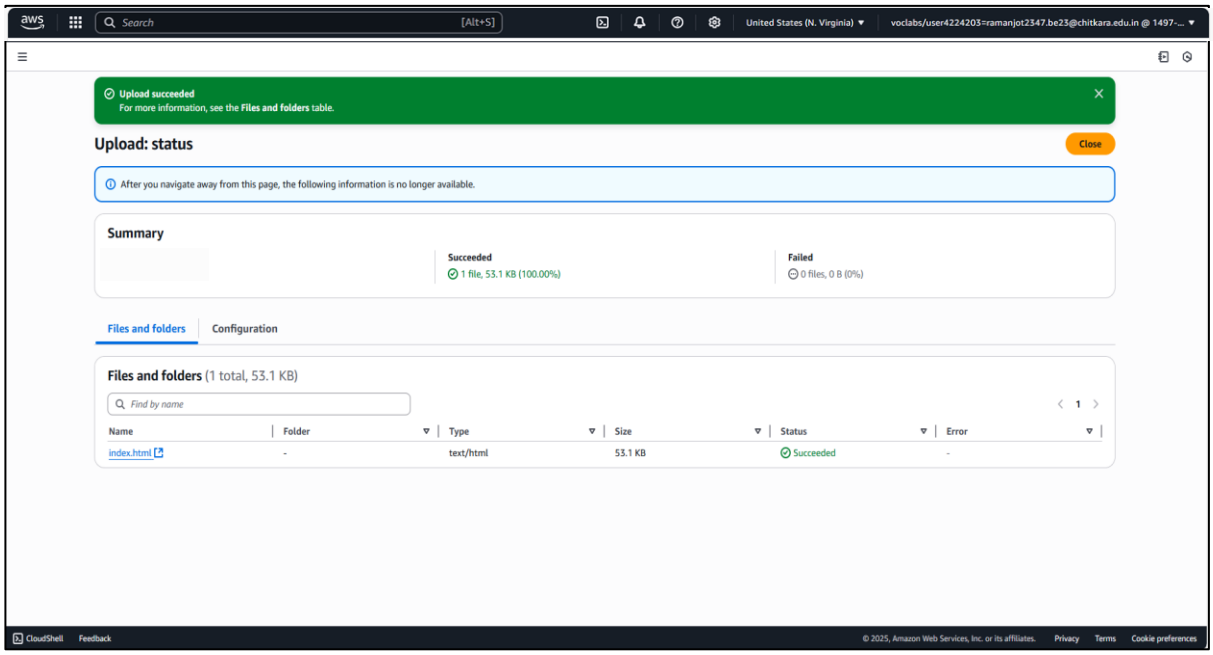


Figure 4.8 Click upload

Step 3: Set Permissions with a Bucket Policy

Since you want users to access your files, you need to set a **bucket policy**.

1. Go to **Permissions tab → Bucket Policy**.
2. Open your bucket → **Permissions** tab → **Bucket Policy** → **Policy Generator**.
3. Select:
    - **Policy Type:** S3 Bucket Policy
    - **Effect:** Allow
    - **Principal:** * (means everyone)
    - **Actions:** choose → GetObject
    - **ARN:** all resources
4. Click **Add Statement** → Then **Generate Policy**.

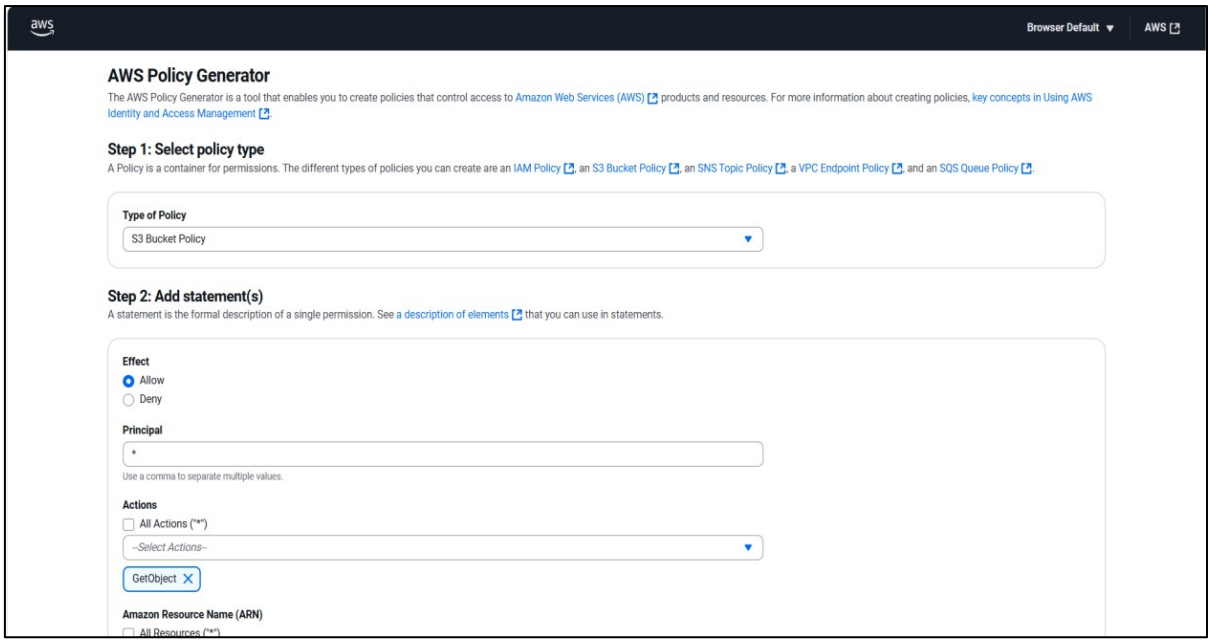


Figure 4.9 Click add statement

5. Copy the generated JSON and paste it into your **Bucket Policy editor**.

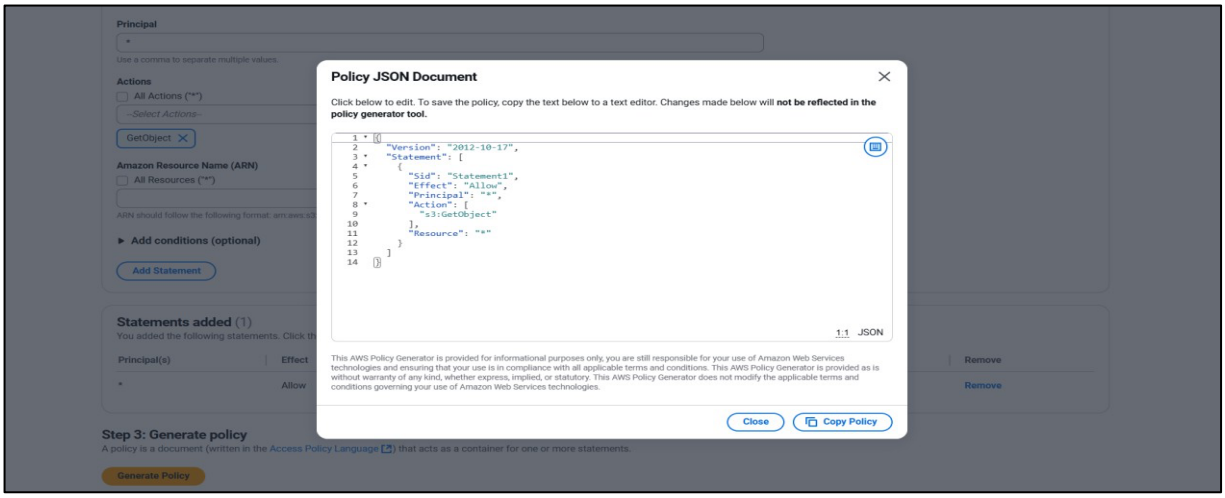


Figure 4.10 Write the Policy

6. It will look like this (example for my-static-site-bucket):**Add Resource": "arn:aws:s3:::*urbucketname*/*"**

(Don't forget the / so it applies to all files in the bucket!)*

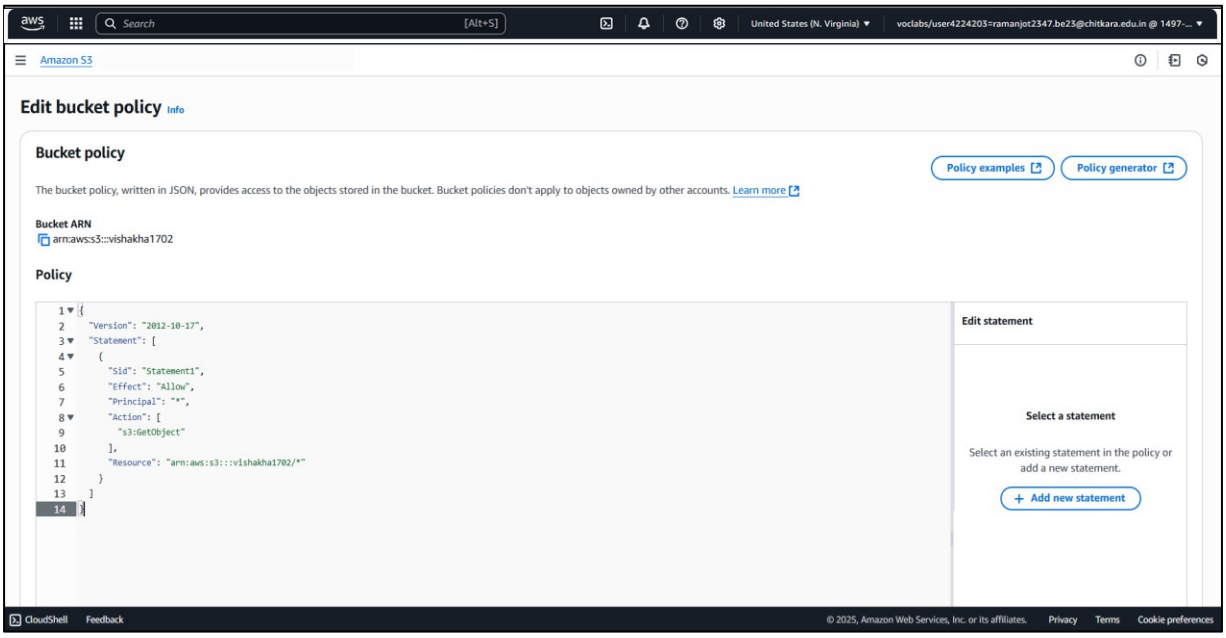


Figure 4.11 Add Resource and make sure to add /*

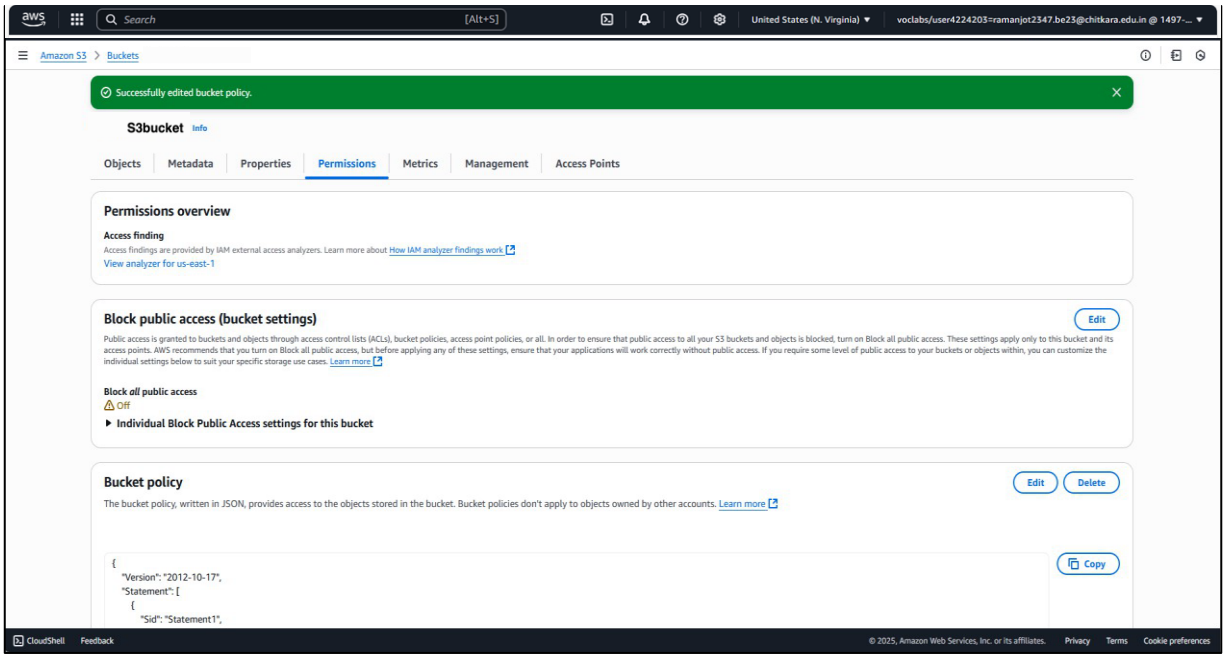


Figure 4.12 Set Permission

7. Save the policy.

✓ This allows public read access to all objects in your bucket.

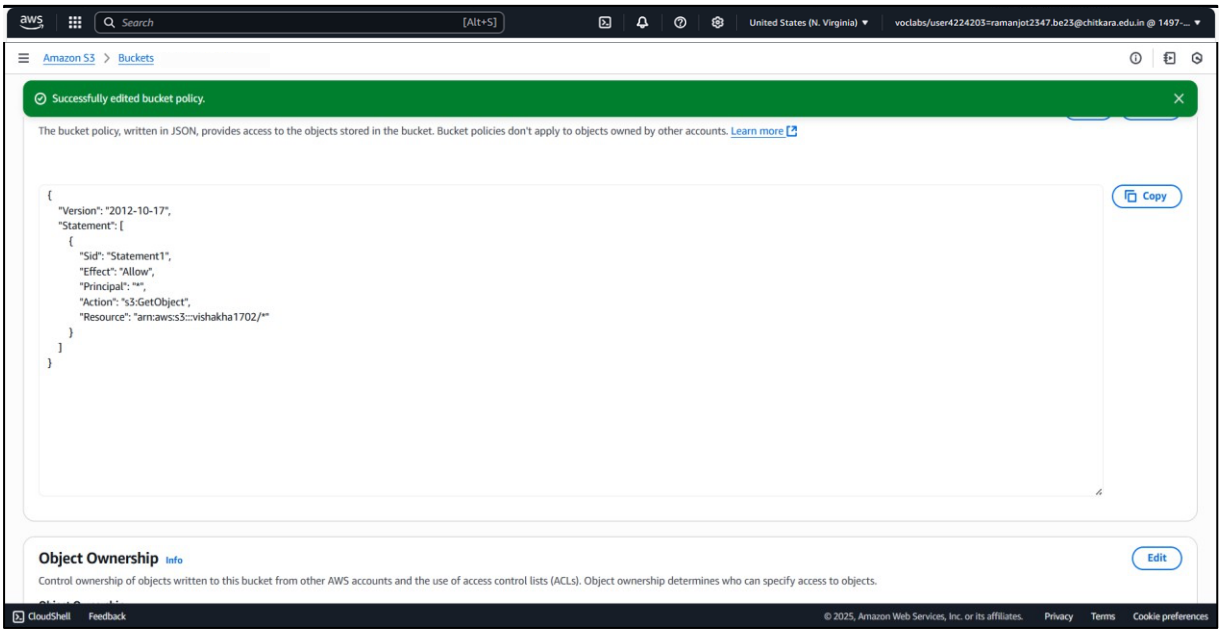


Figure 4.13 Save the policy

Step 4: Enable Static Website Hosting

1. Go to your bucket → **Properties tab**.

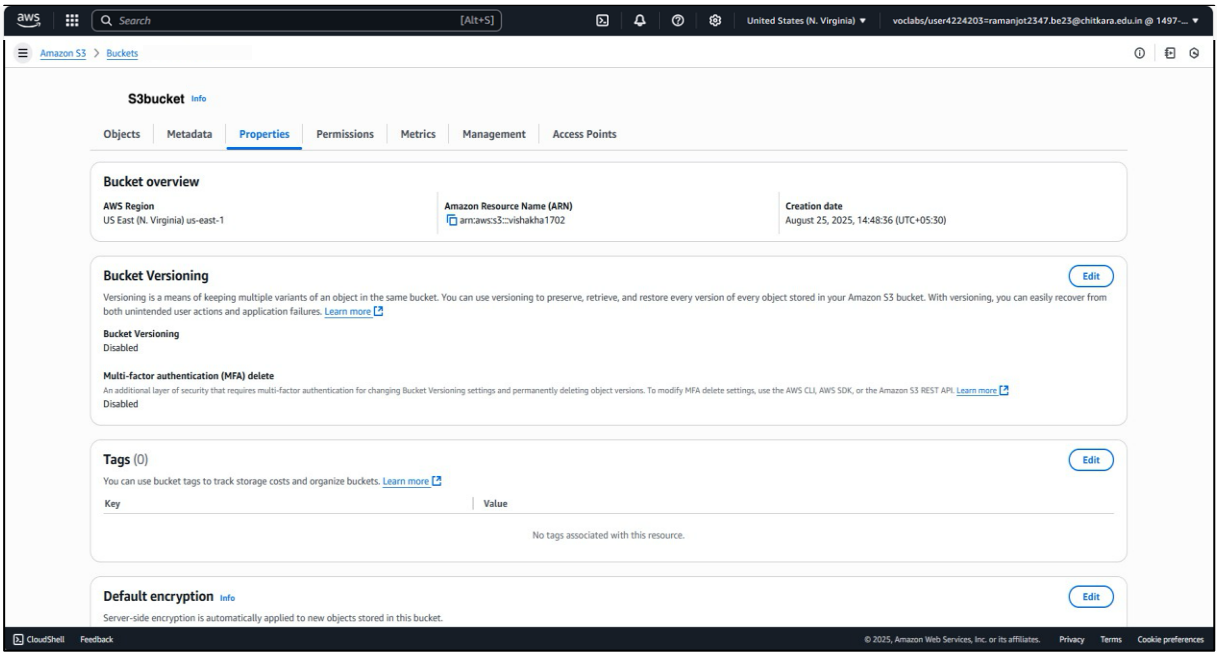


Figure 4.14 Enabling Static Website Hosting

2. Scroll to **Static website hosting** → Click **Edit**.
3. Select **Enable**.
4. For **Index document**, type: index.html.
5. (Optional) For **Error document**, type: error.html.

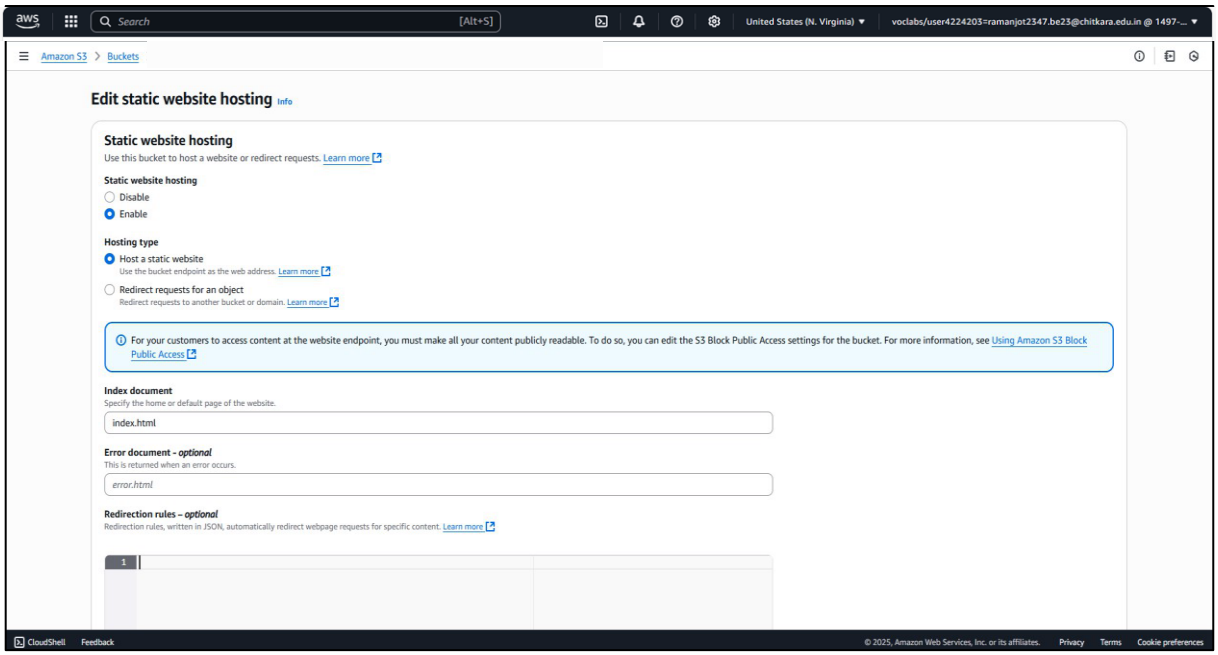


Figure 4.15 Select Enable

6. Save changes.

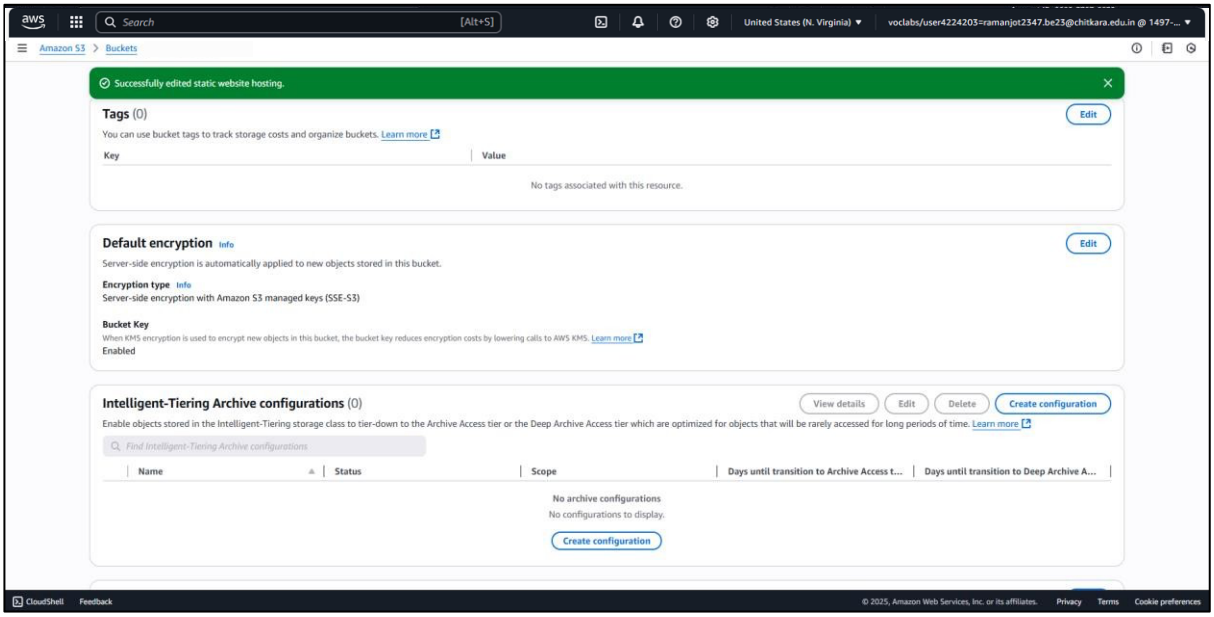


Figure 4.16 Save the Current Status

Step 5: Access Your Website

- After enabling hosting, AWS gives you a **bucket website endpoint URL**,

  something like: http://my-static-site-bucket.s3-website-us-east-

  1.amazonaws.com

- Share this URL → Your static website is live!

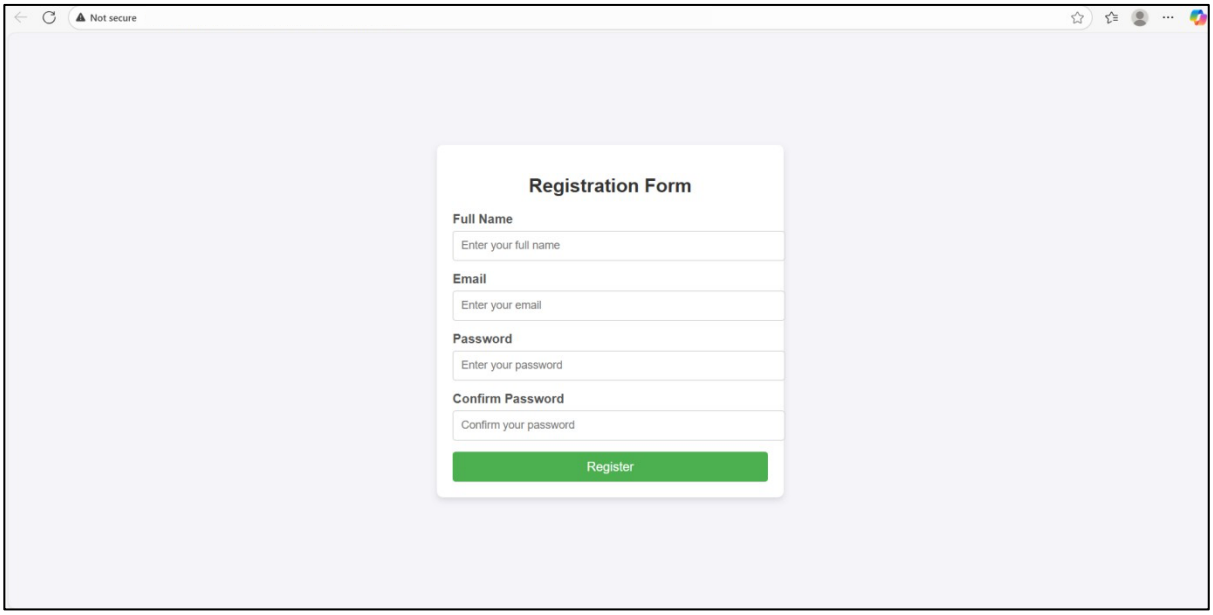


Figure 4.17 Access the link

Learning Outcomes:

- Created an Amazon S3 bucket and understood its role in cloud storage.
- Uploaded and managed objects within an S3 bucket.
- Configured bucket policies and access controls to secure data and manage permissions.
- Enabled and tested static website hosting using Amazon S3.
- Understood how S3 can be used for cost-effective, scalable, and highly available content delivery.

Practical No. 5:

Practical Title: Set up an AWS Elastic Load Balancer (ELB) to distribute traffic among EC2 instances.

Objective:

- **To set up and configure a Load Balancer.**
- **To create a Target Group and register instances.**
- **To verify the traffic distribution across EC2 instances.**

Step-by-Step Procedure with Screenshots:

Step 1. Create Security Groups:

1. Navigate to the EC2 Dashboard and go to **Security Groups**.
2. Click **Create security group**.
3. Create a security group for the load balancer (e.g., SG-ALB).
4. Add an inbound rule: Type **HTTP**, Protocol **TCP**, Port **80**, Source **Anywhere** (0.0.0.0/0).
5. Click **Create security group**.
6. Create another security group for the EC2 instances (e.g., SG-EC2).
7. Add two inbound rules:
    - Type **SSH**, Protocol **TCP**, Port **22**, Source **Anywhere** (0.0.0.0/0).
    - Type **HTTP**, Protocol **TCP**, Port **80**, Source **Custom**, and select the load balancer security group you created (SG-ALB). This allows the load balancer to send traffic to the instances.
8. Click **Create security group**.

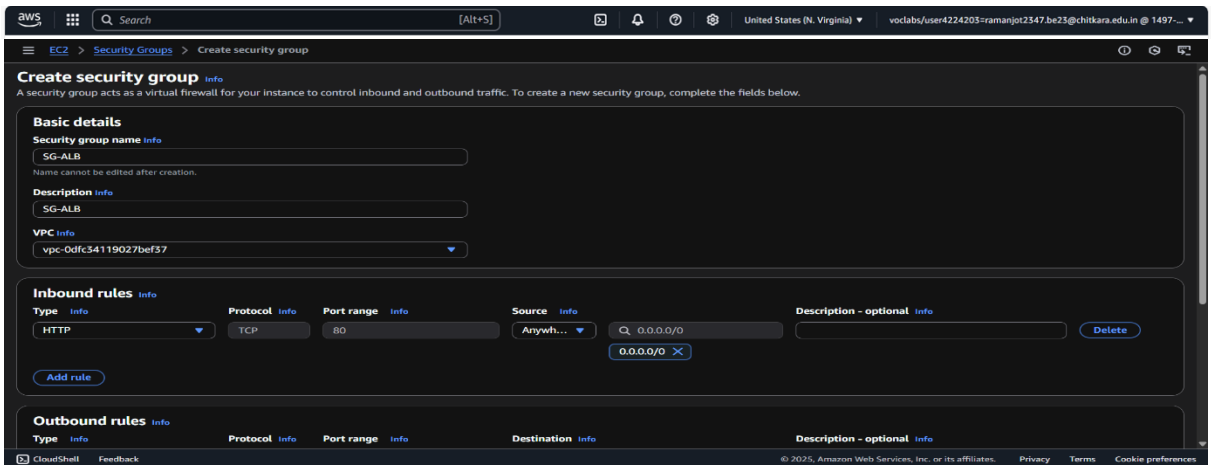


Fig 5.1 Creating Security Group

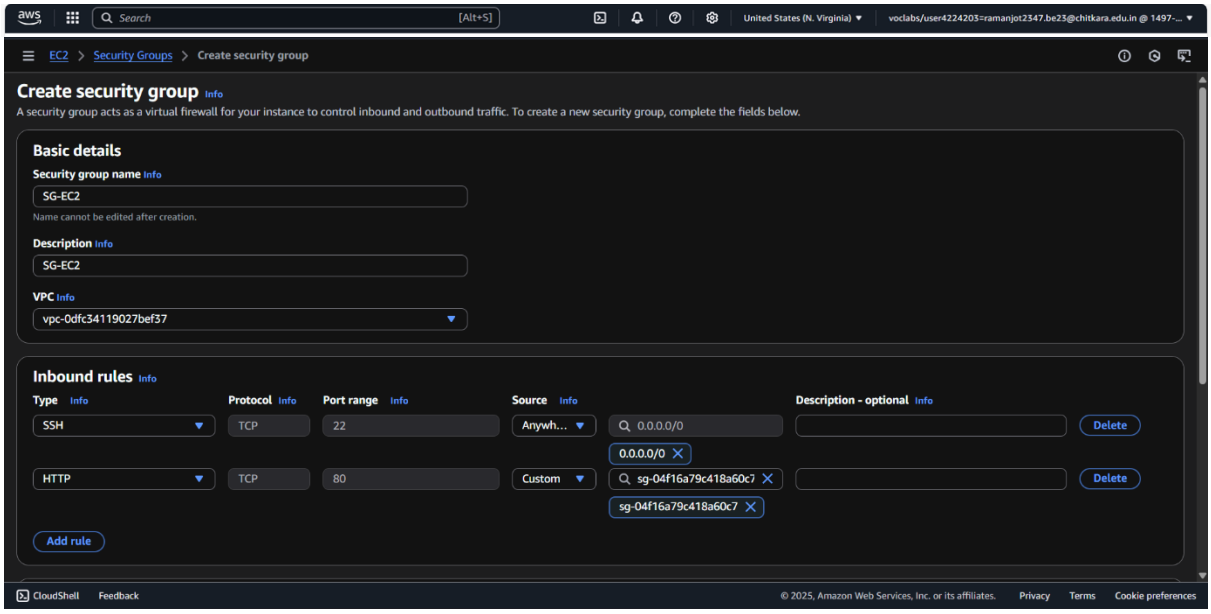


Fig 5.2 Write Security Group

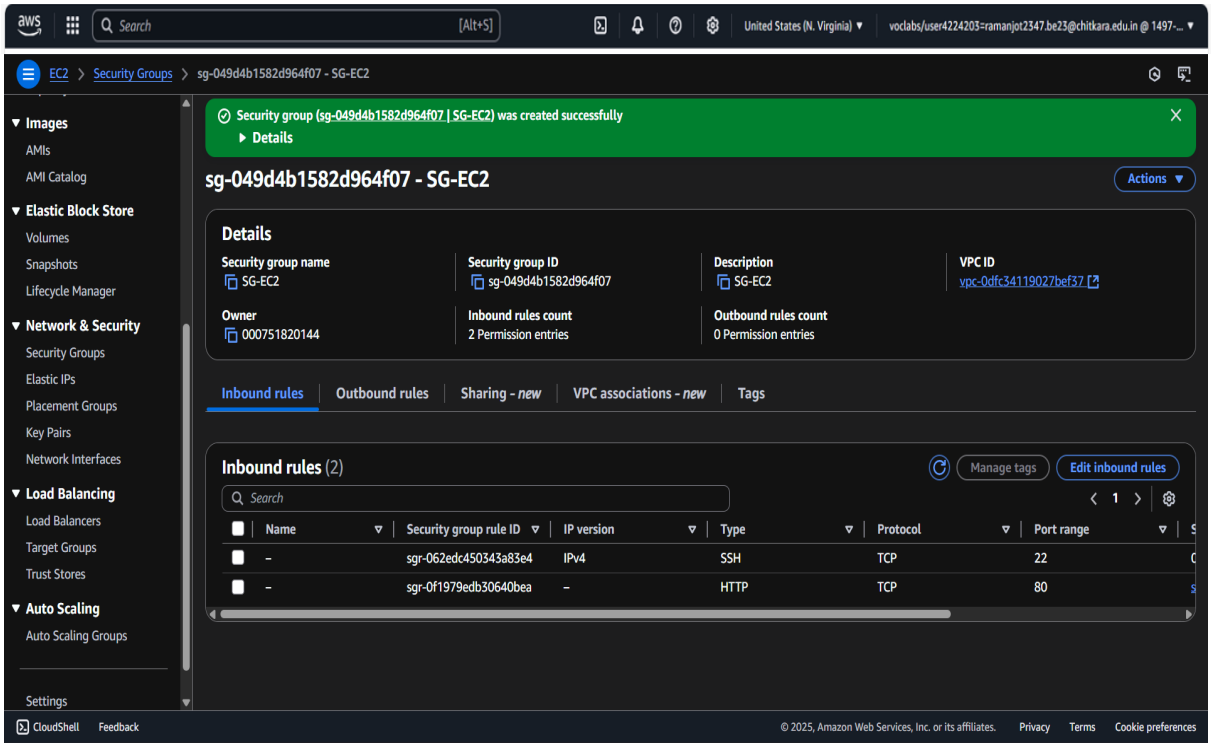


Fig 5.3 Security Group Created

Step 2. Launch EC2 Instances:

1. Launch two EC2 instances with a web server configured using user data.

2. For each instance:

    - Choose an AMI (e.g., Amazon Linux 2023).

- Select an instance type (e.g., t2.micro).
- Select the SG-EC2 security group you created.
- In **Advanced Details**, add user data to install and start a web server. For example: #!/bin/bash yum update -y yum install httpd -y echo "<html><body> <h1>This is web page 1.</h1> </body></html>" > /var/www/html/index.html systemctl start httpd systemctl enable httpd
- Launch both instances. Name them Instance 1 and Instance 2.

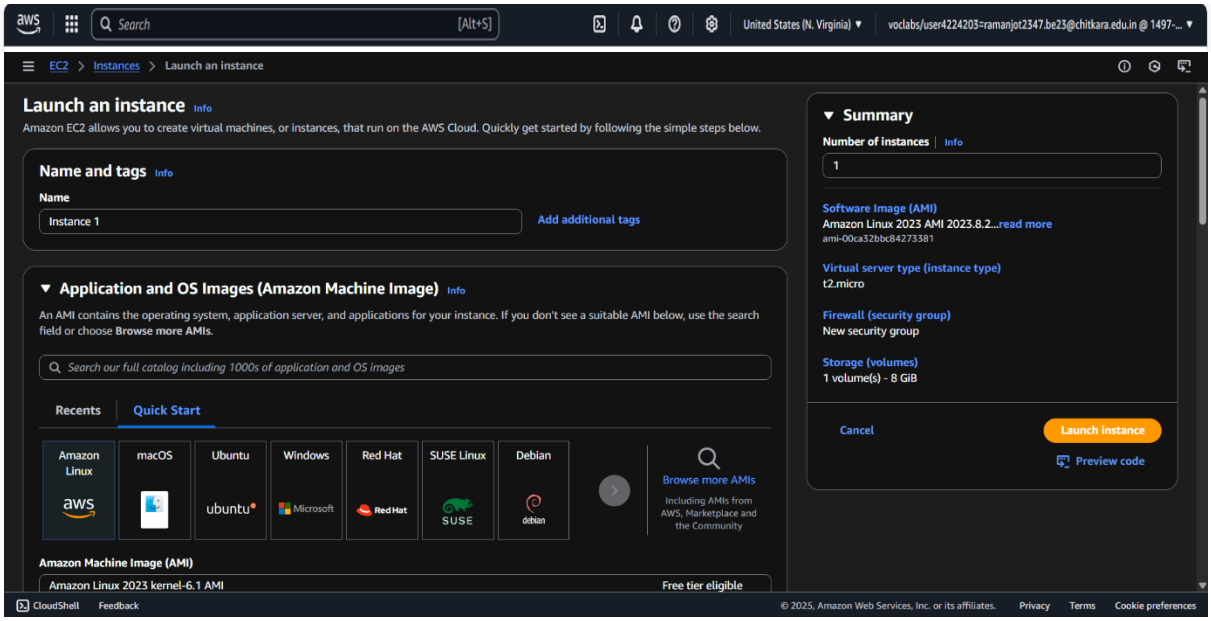


Fig 5.4 Launching EC2 Instance

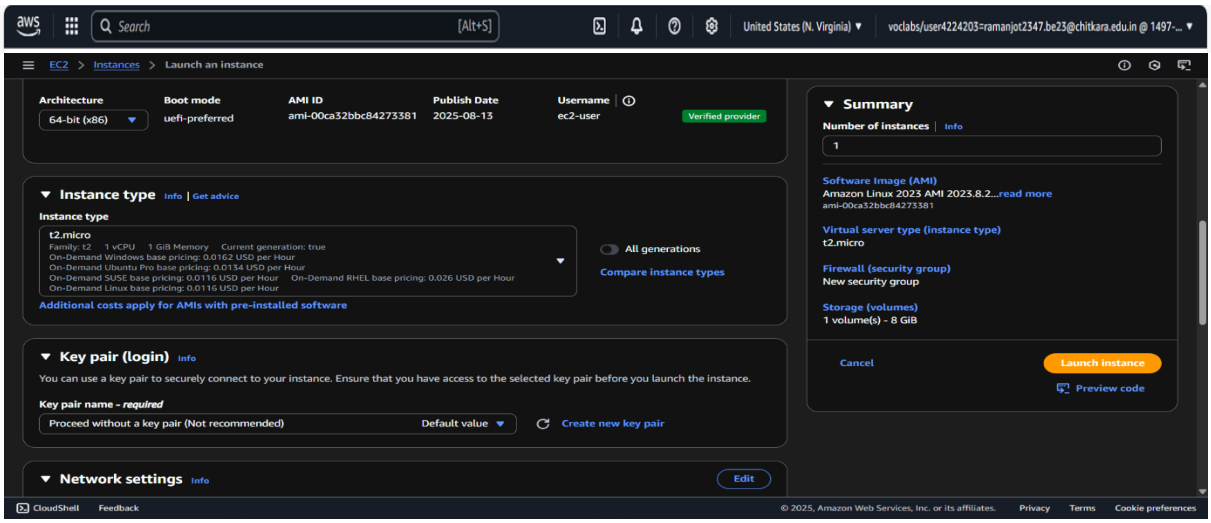


Fig 5.5 Selecting Key Pair

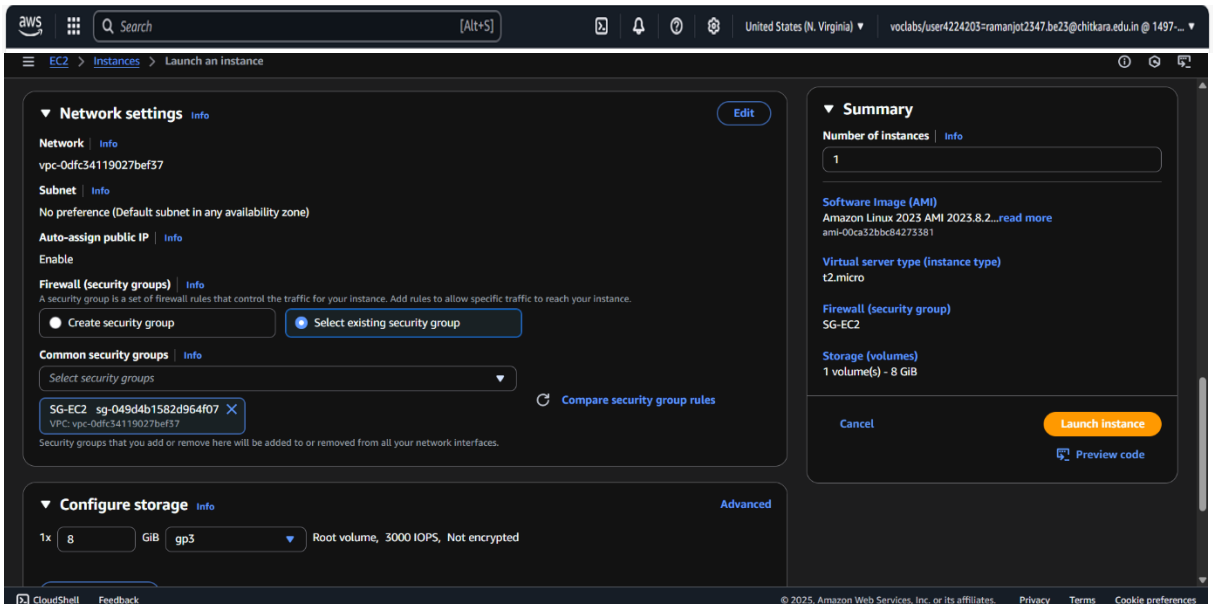


Fig 5.7 Doing Configuration

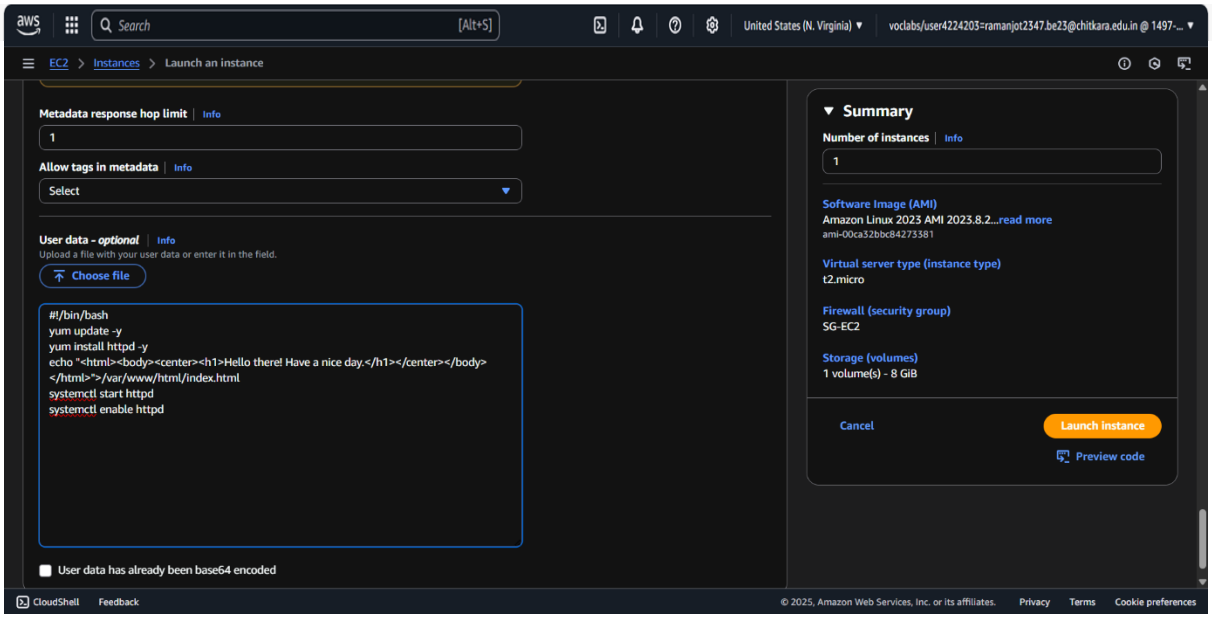


Fig 5.8 Setting the Server Configuration

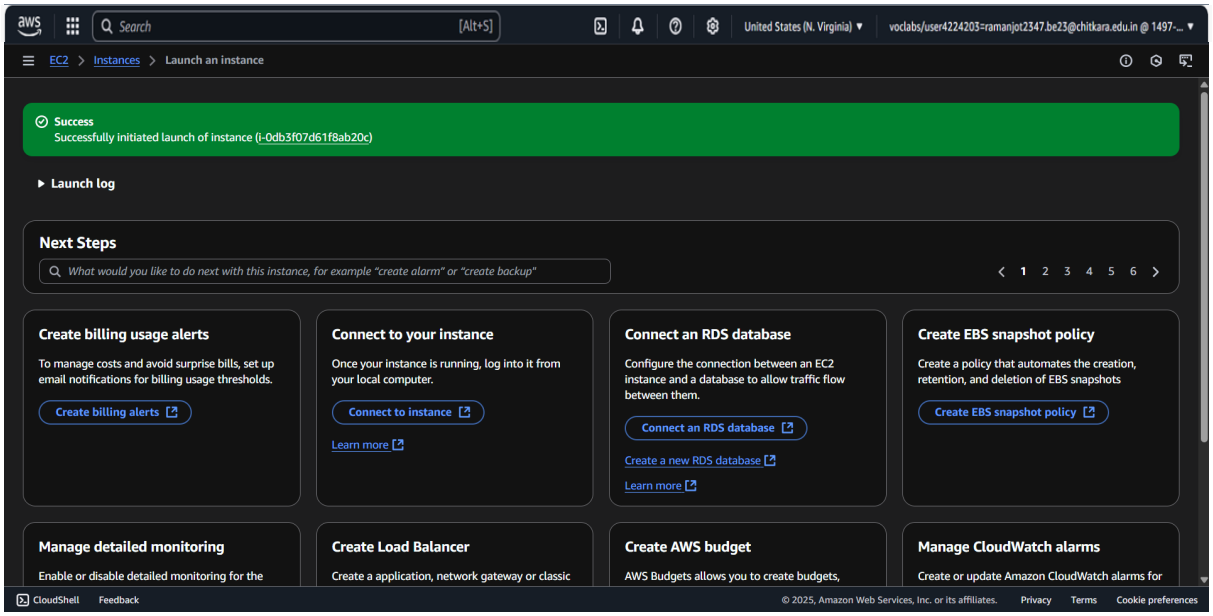


Fig 5.9 Successfully Launched Instance

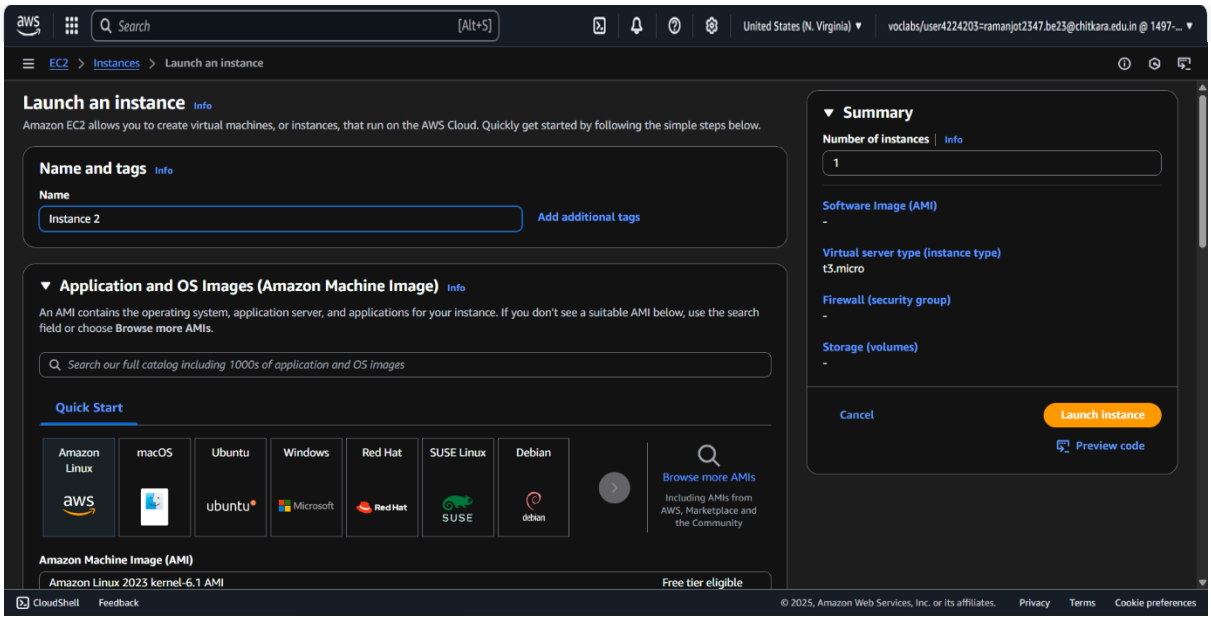


Fig 5.10 2nd Instance

Step 3. Create a Target Group:

1. Navigate to the EC2 Dashboard and go to **Target Groups**.
2. Click **Create target group**.
3. Choose a target type: **Instances**.
4. Give it a name (e.g., `DemoTG`).

5. Select the VPC.
6. Under **Health checks**, set the protocol to **HTTP** and the health check path to `/index.html`.
7. Click **Next**.
8. Select your two EC2 instances (`Instance 1` and `Instance 2`) and click **Include as pending below**.
9. Click **Create target group**.

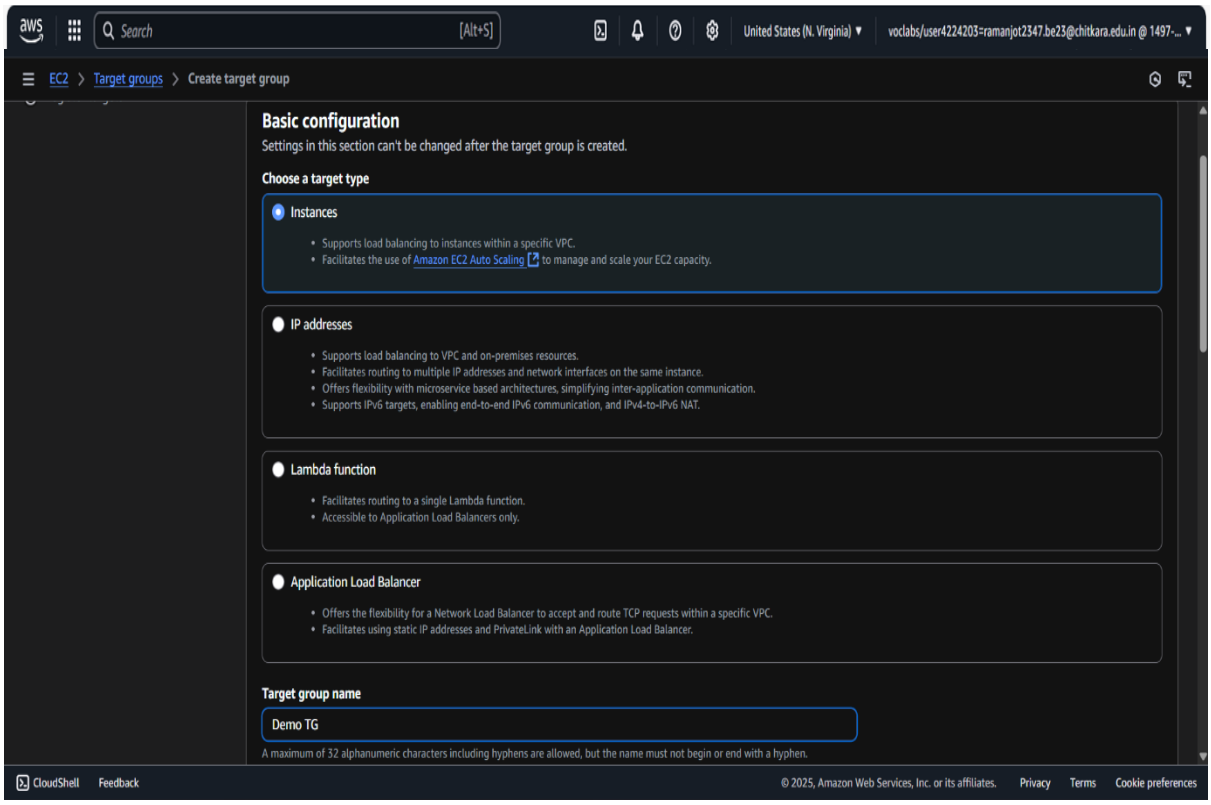


Fig 5.11 Target Group

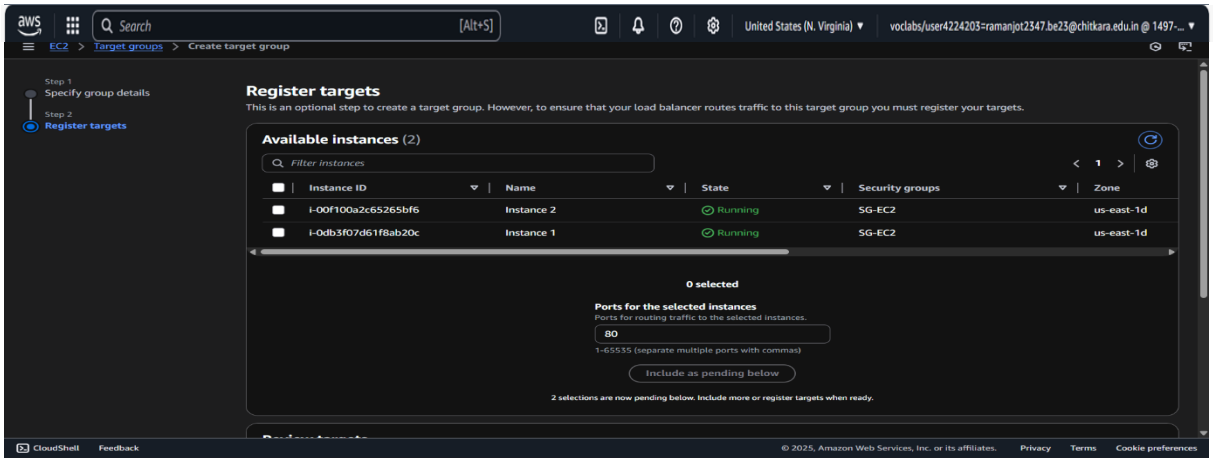


Fig 5.12 Created Target Groups

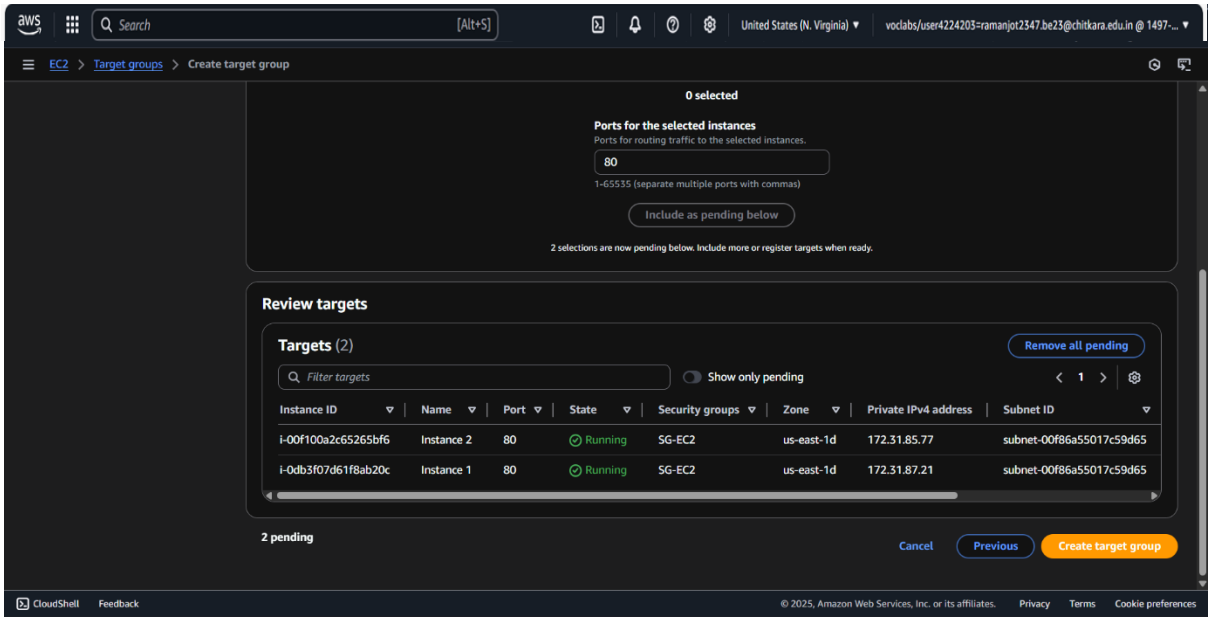


Fig 5.13 Review

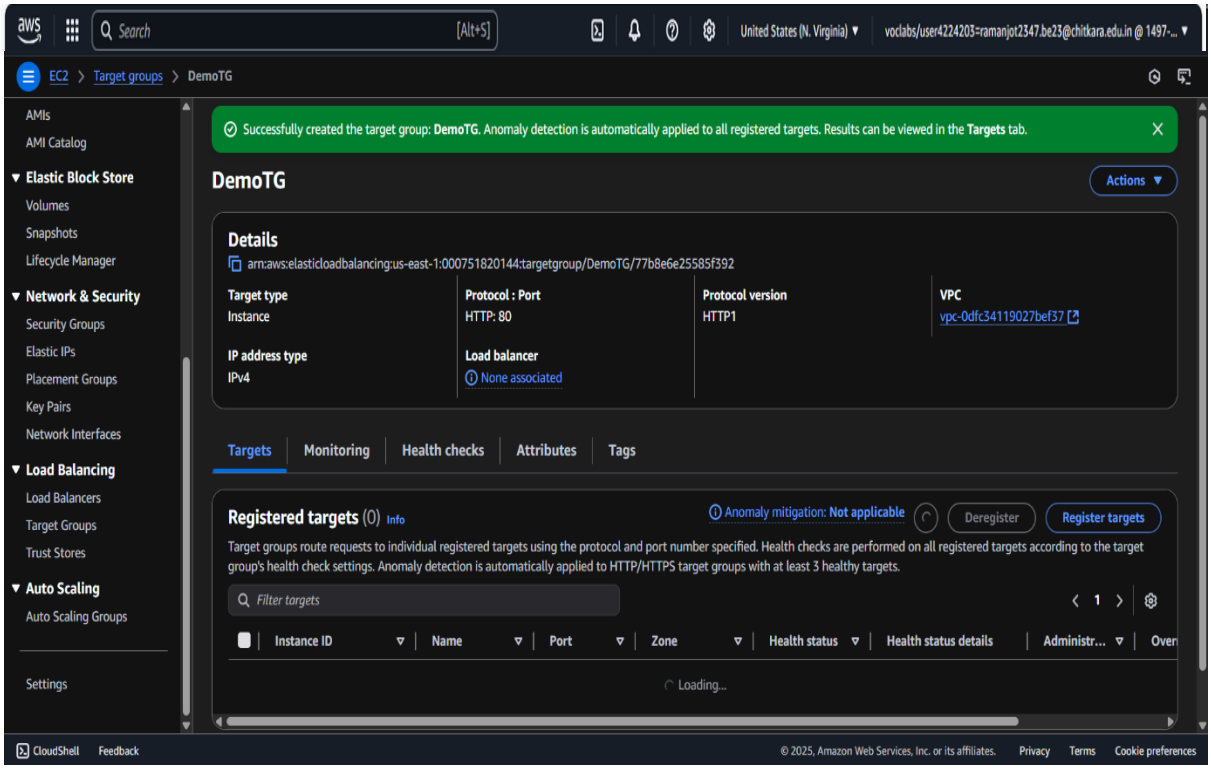


Fig 5.14 Created

Step 4. Create a Load Balancer:

1. Navigate to the EC2 Dashboard and go to Load Balancers.
2. Click Create Load Balancer.
3. Choose Application Load Balancer.
4. Name it (e.g., ALB).

5. Set the scheme to Internet-facing.
6. Select your VPC and all available subnets in different Availability Zones.
7. Under Security groups, select the SG-ALB security group.
8. Under Listeners and routing, set the protocol to HTTP, port 80, and forward to your target group (DemoTG).
9. Click Create load balancer.

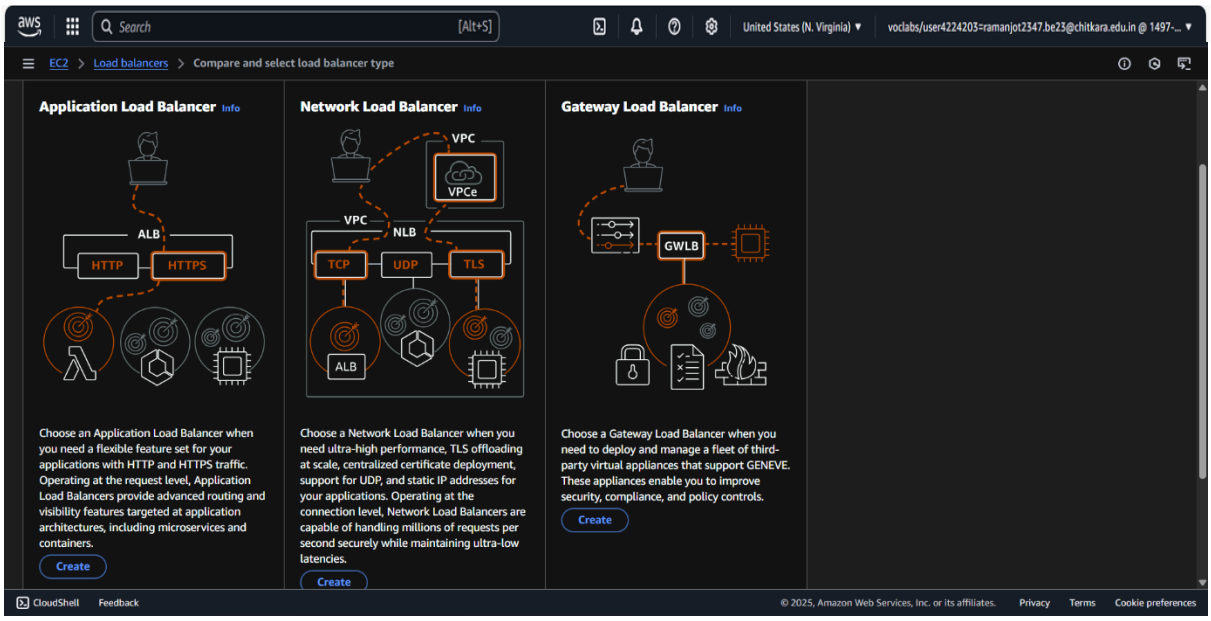


Fig 5.15 Create Load Balancer

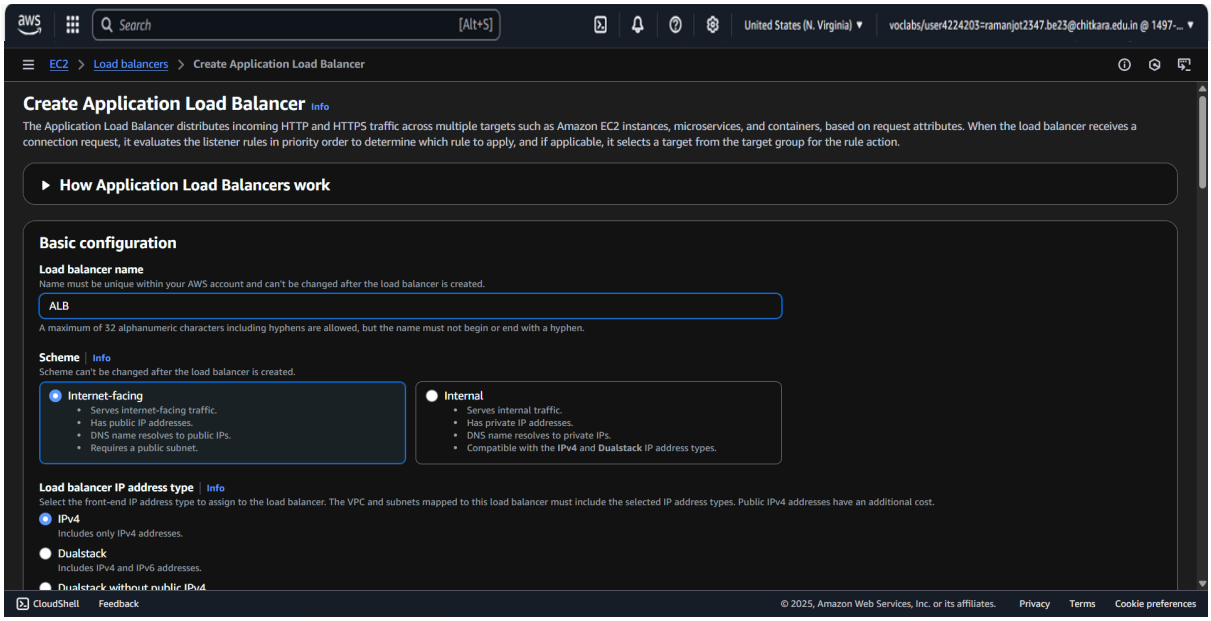


Fig 5.16 Application Load Balancer

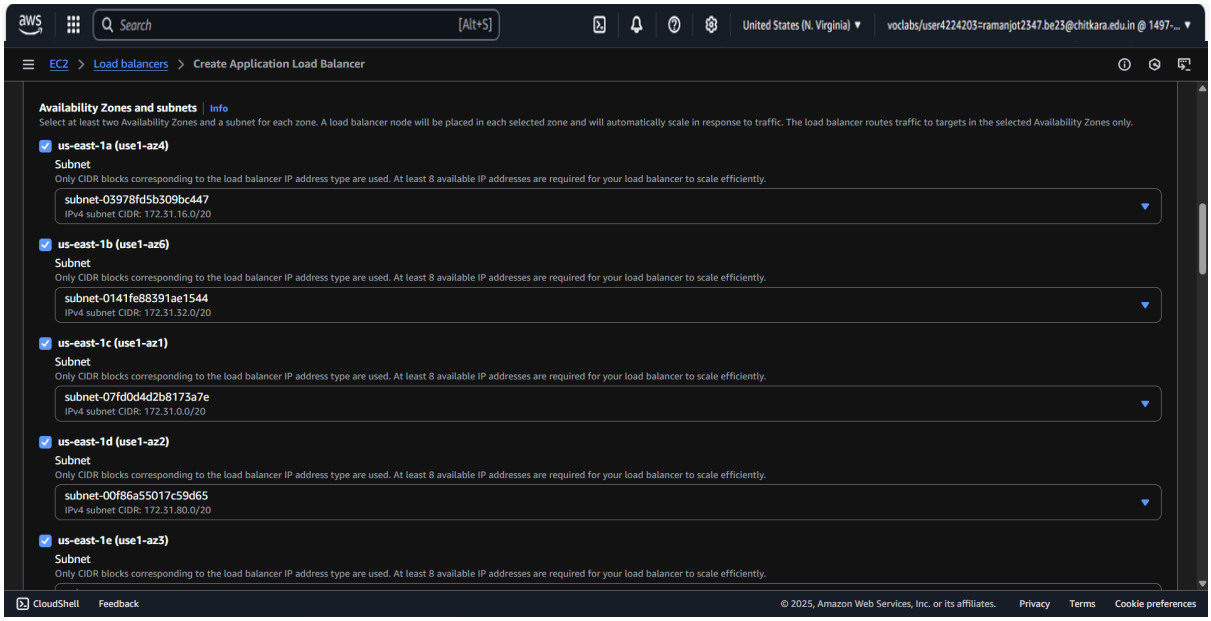


Fig 5.17 Select all availability zones

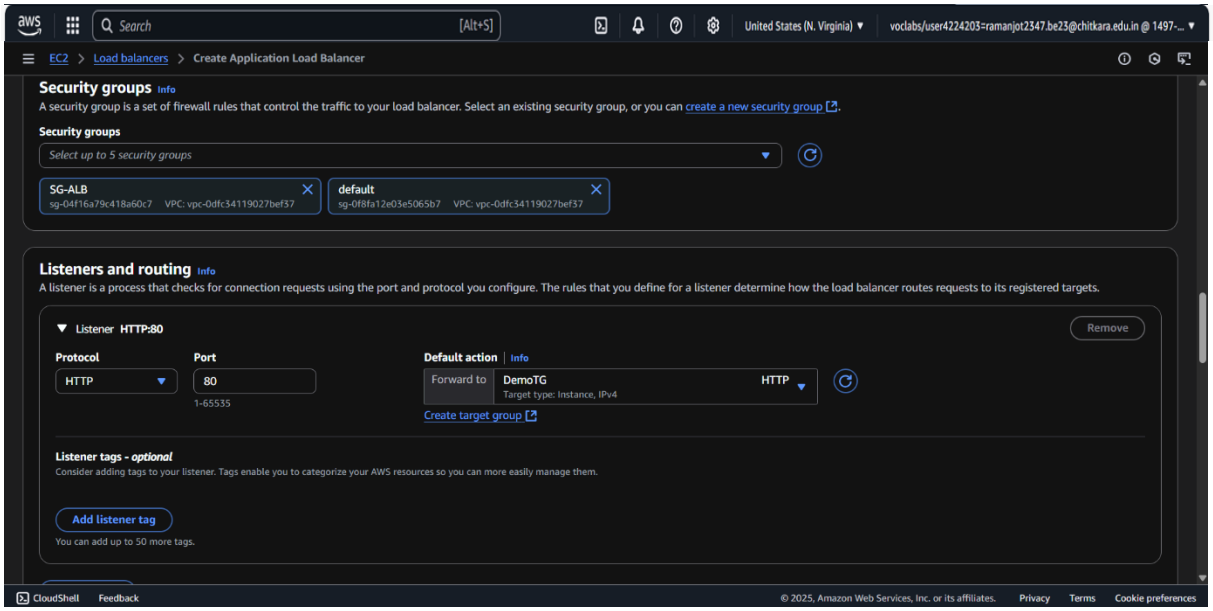


Fig 5.18 Select target group

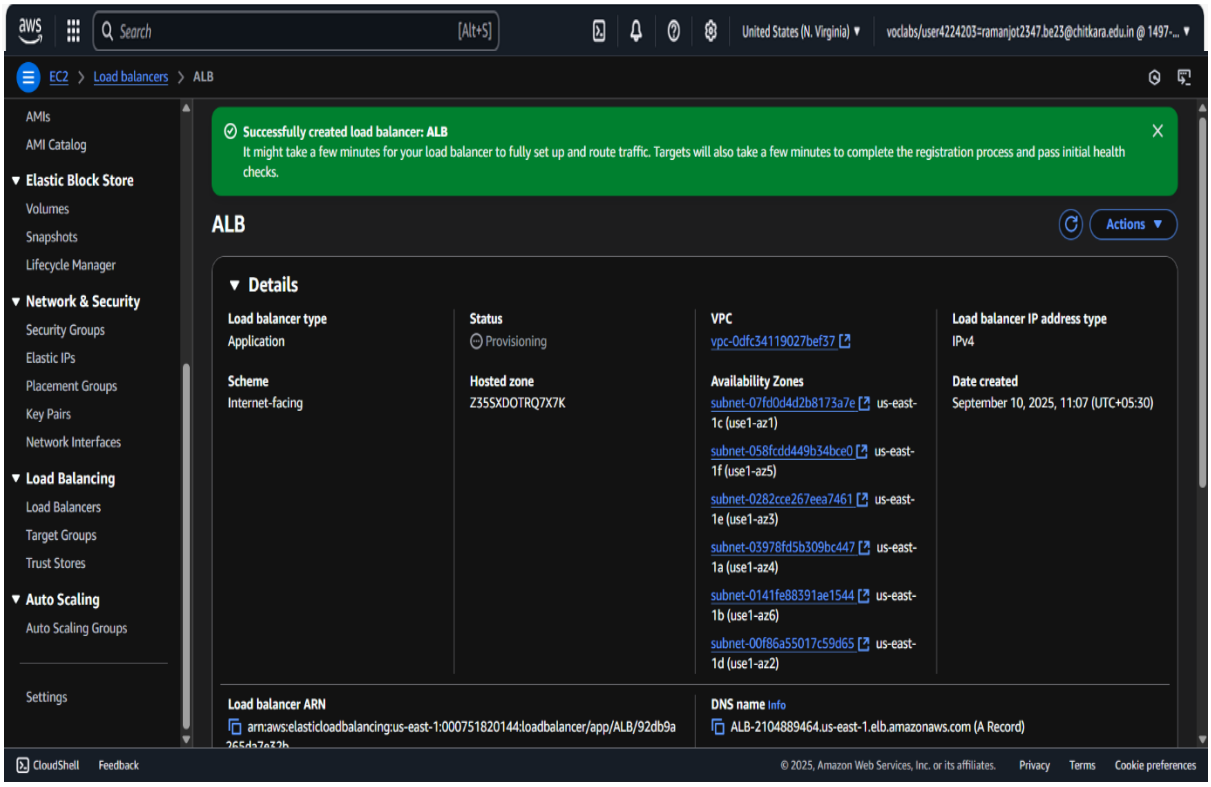


Fig 5.19 ALB

Step 5. Verify Load Balancer Functionality:

1. Once the load balancer is created, go to its details page.
2. Copy the **DNS name**.
3. Paste the DNS name into your web browser. Each time you refresh the page, the load balancer should distribute the traffic, and you will see the content from Instance 1 or Instance 2 alternatingly, proving that the load balancer is working as intended.

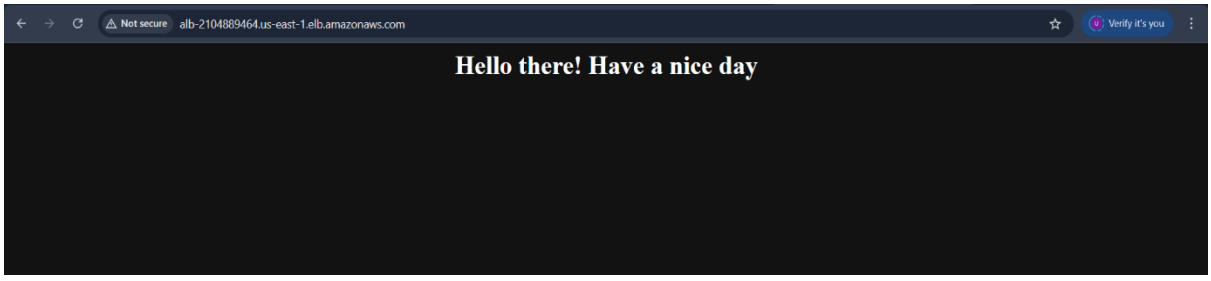


Fig 5.20 Load Balancer

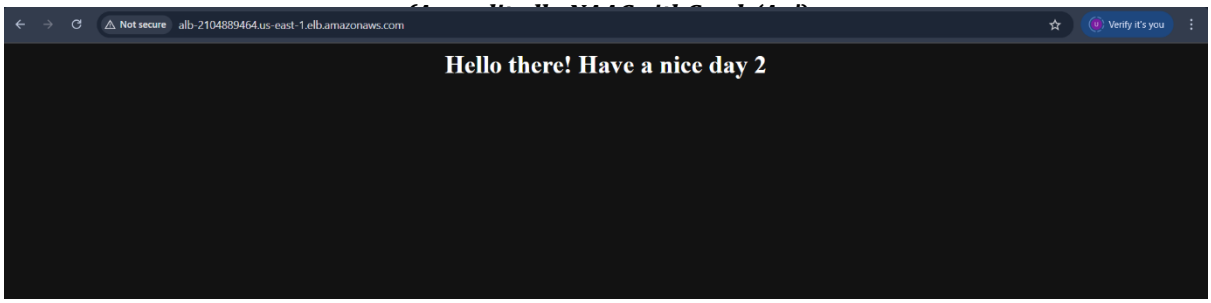


Fig 5.21 Ctrl+ R load balanced to another instance

Learning Outcomes:

- Successfully set up an Application Load Balancer to distribute incoming web traffic.
- Created a Target Group and registered EC2 instances to receive traffic.
- Verified the round-robin distribution of requests, demonstrating high availability and scalability for web applications.

Practical No. 6:

Practical Title: Set up Amazon VPC networking, including subnets, route tables, security groups.
Scenario 1: VPC With a Public Subnet Only (Standalone Web)
Scenario 2: VPC with Public and Private Subnets (3 Tier App)

Objective:

Set up Amazon VPC networking, including subnets, route tables, security groups.
Scenario 1: VPC With a Public Subnet Only (Standalone Web)
Scenario 2: VPC with Public and Private Subnets (3 Tier App

Step-by-Step Procedure with Screenshots:

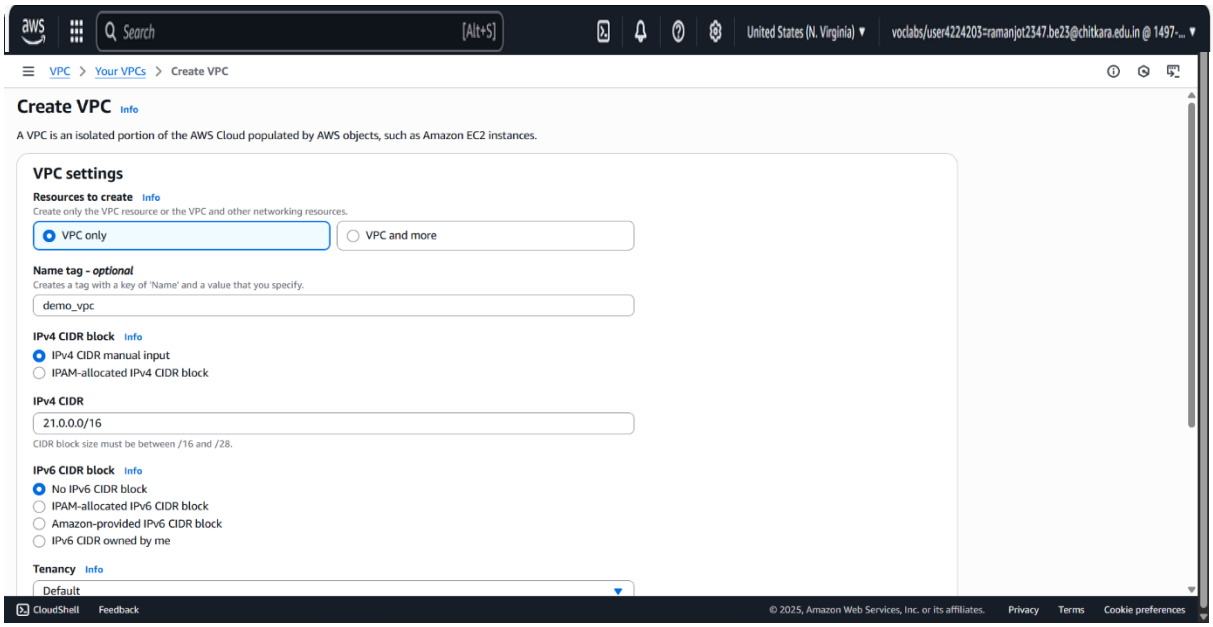


Fig 6.1 Create vpc

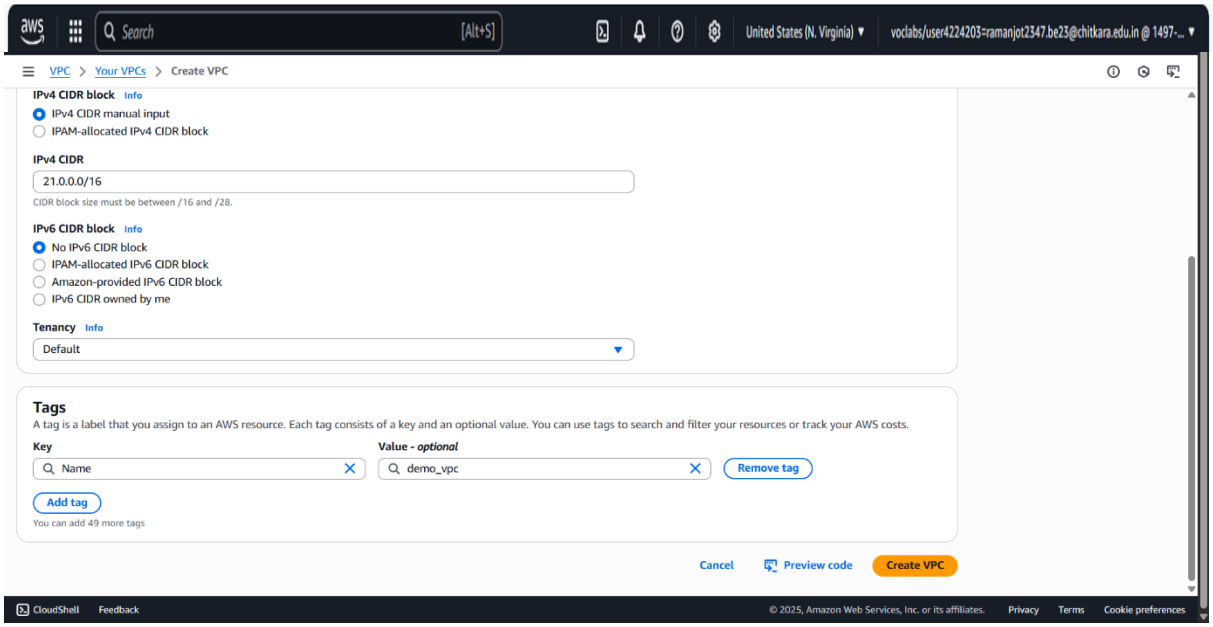


Fig 6.2 ipv4 vpc

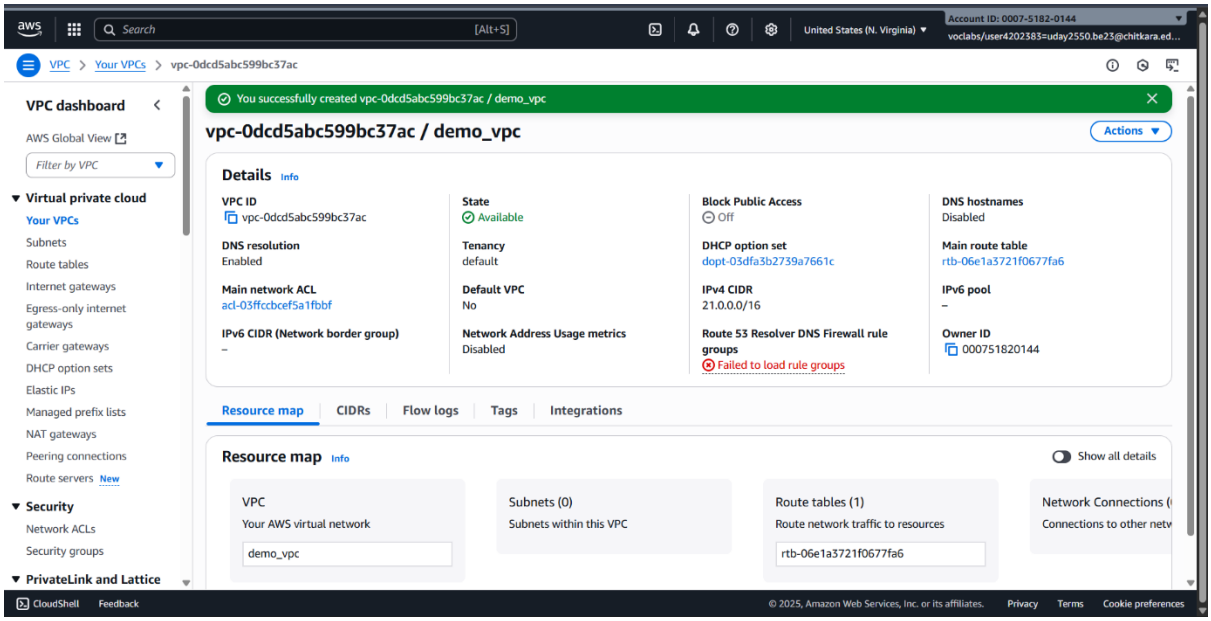


Fig 6.3 demo_vpc

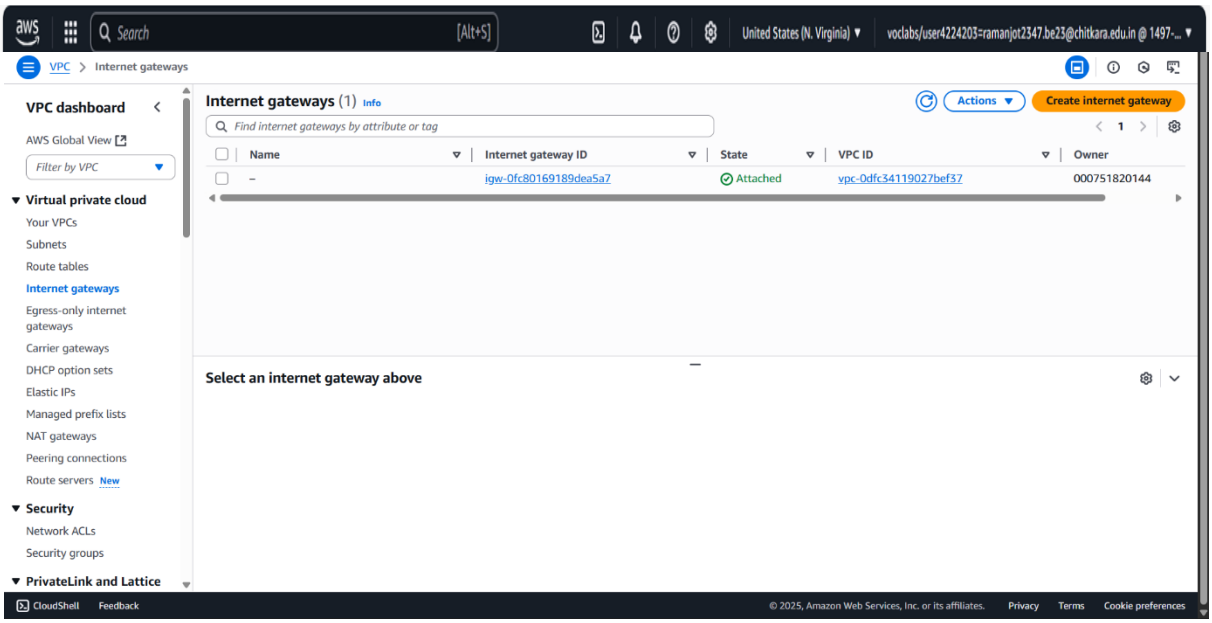


Fig 6.4 Internet Gateway

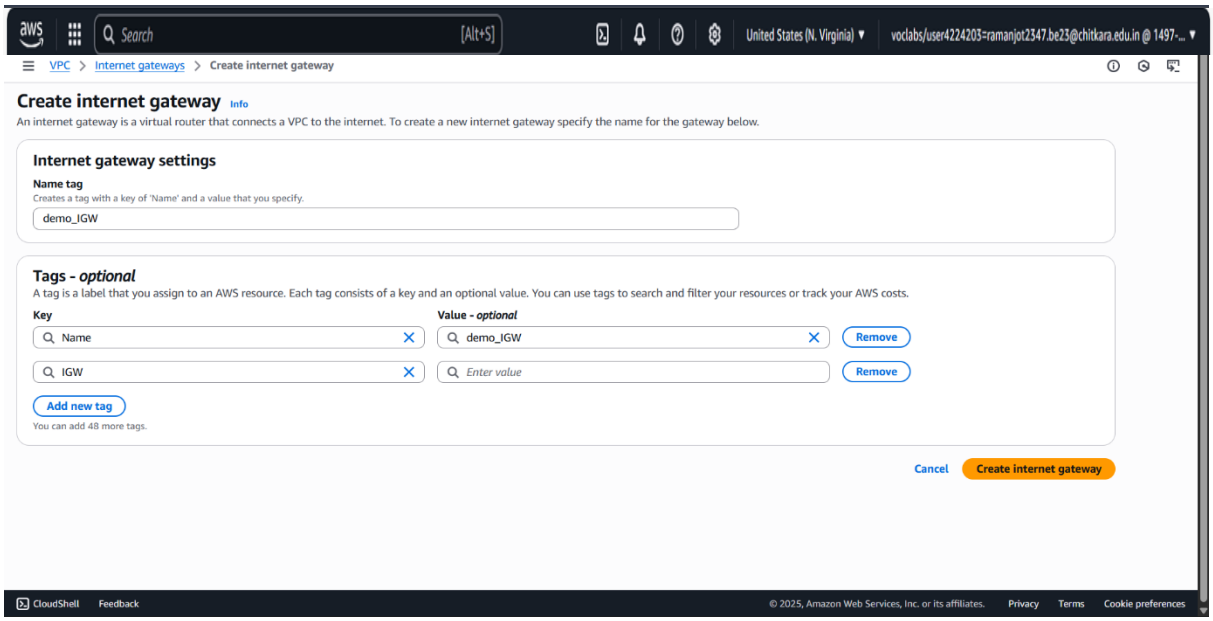
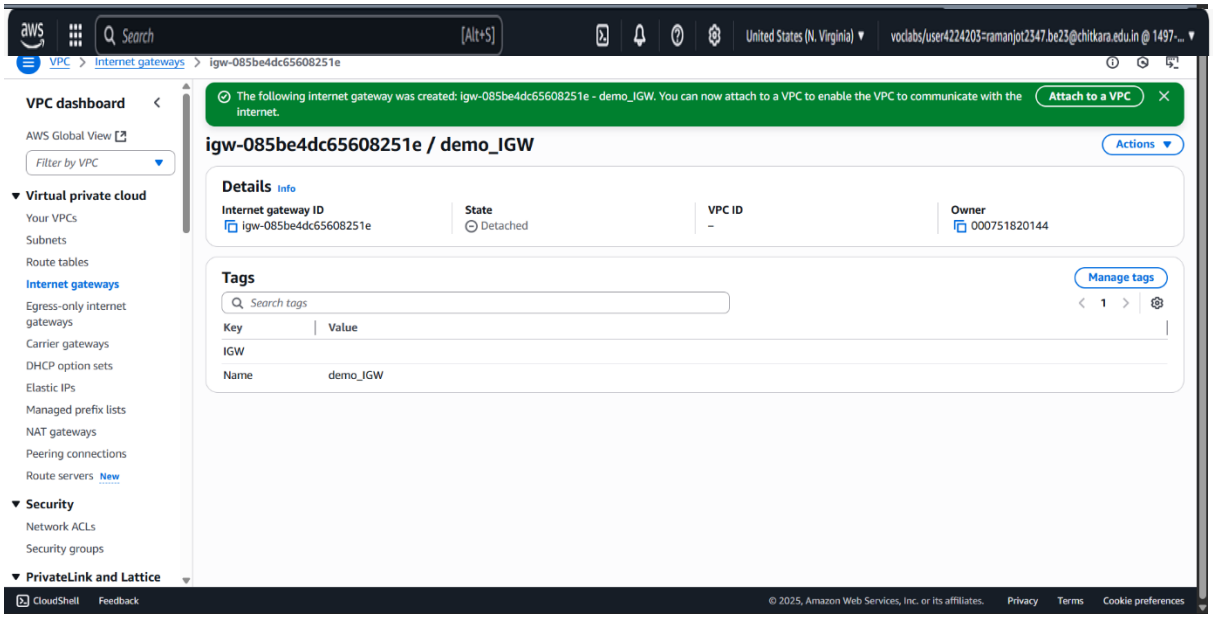
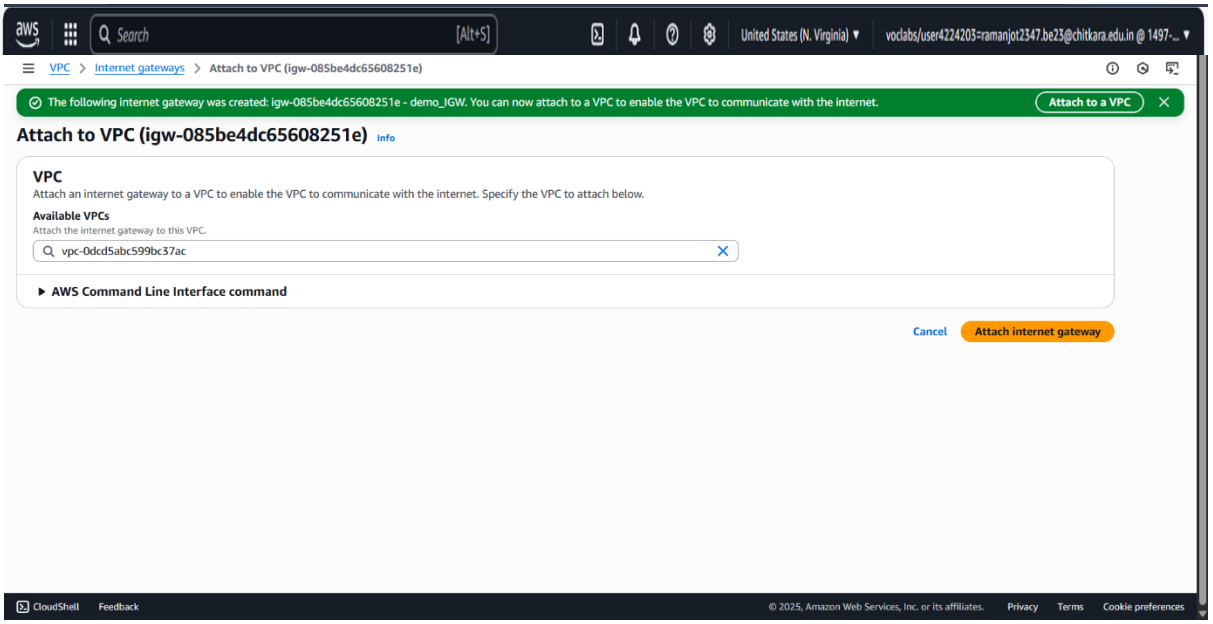
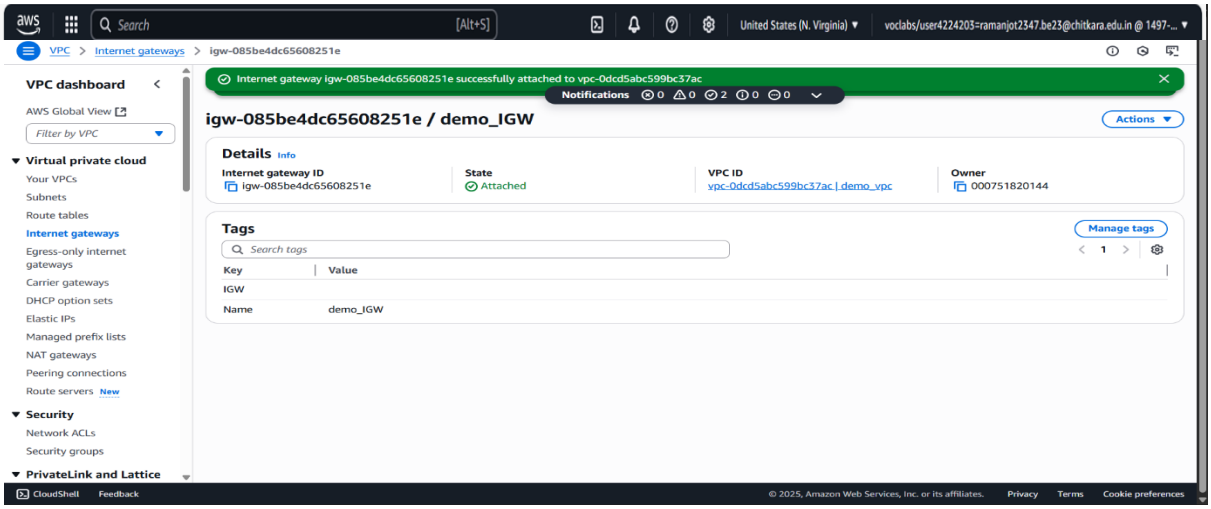
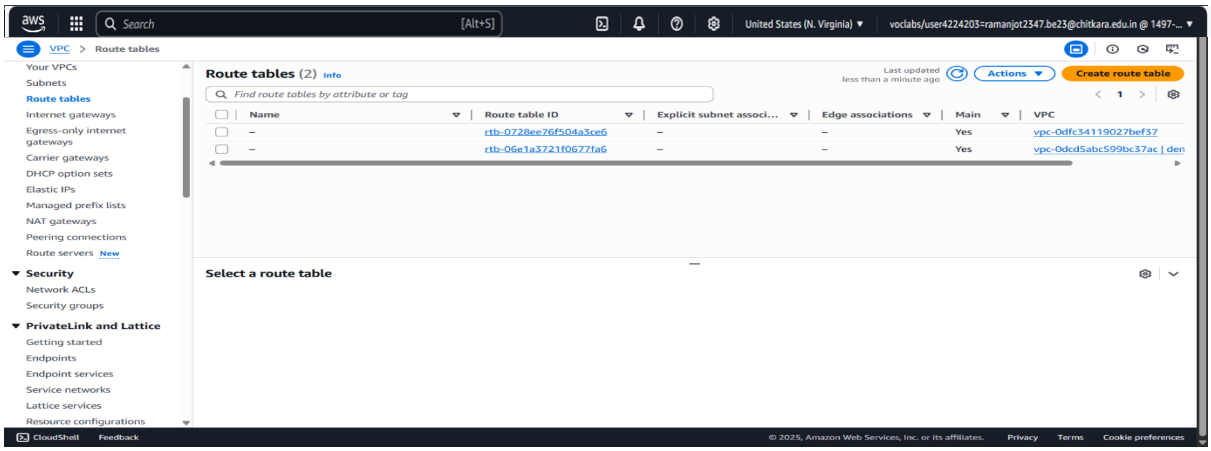


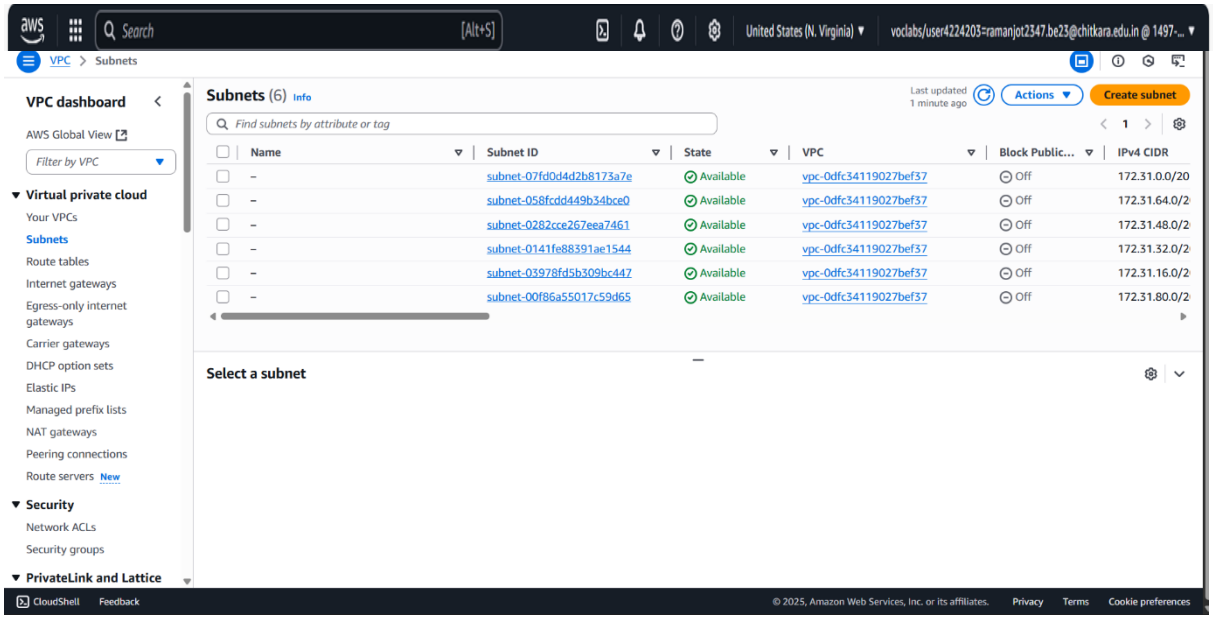
Fig 6.5 Create it

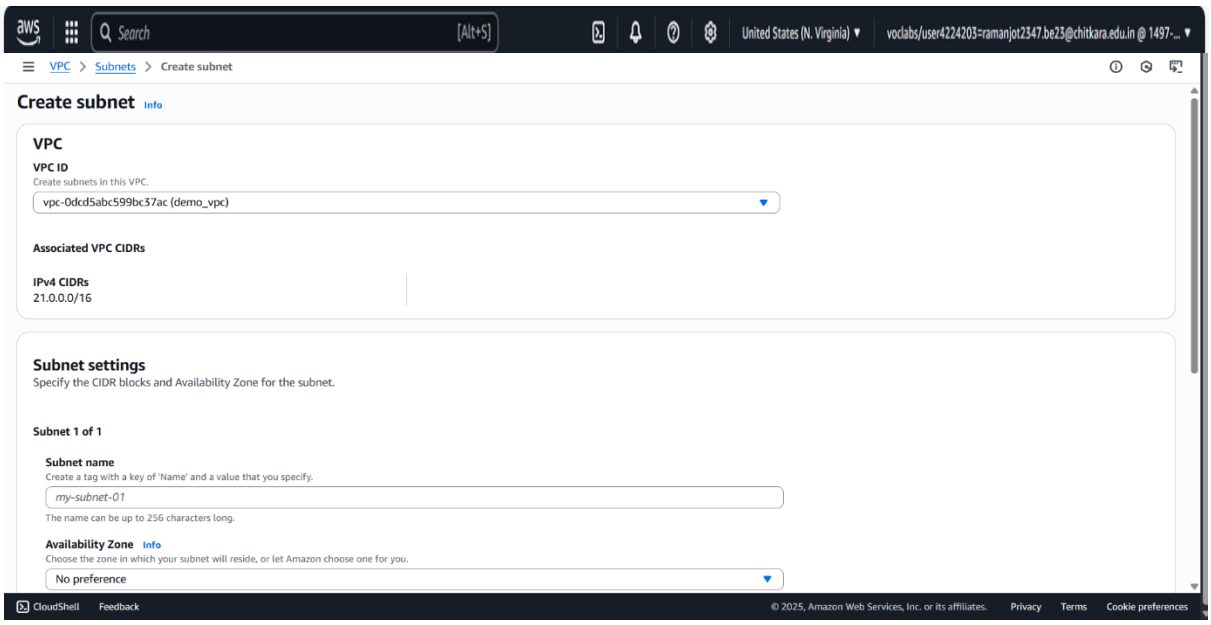

VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups
PrivateLink and Lattice
The following internet gateway was created: igw-085be4dc65608251e - demo_IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
igw-085be4dc65608251e / demo_IGW
Actions
Details
Internet gateway ID
igw-085be4dc65608251e
State
Detached
VPC ID
–
Owner
000751820144
Tags
Manage tags
Search tags
Key
Value
IGW
Name
demo_IGW
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

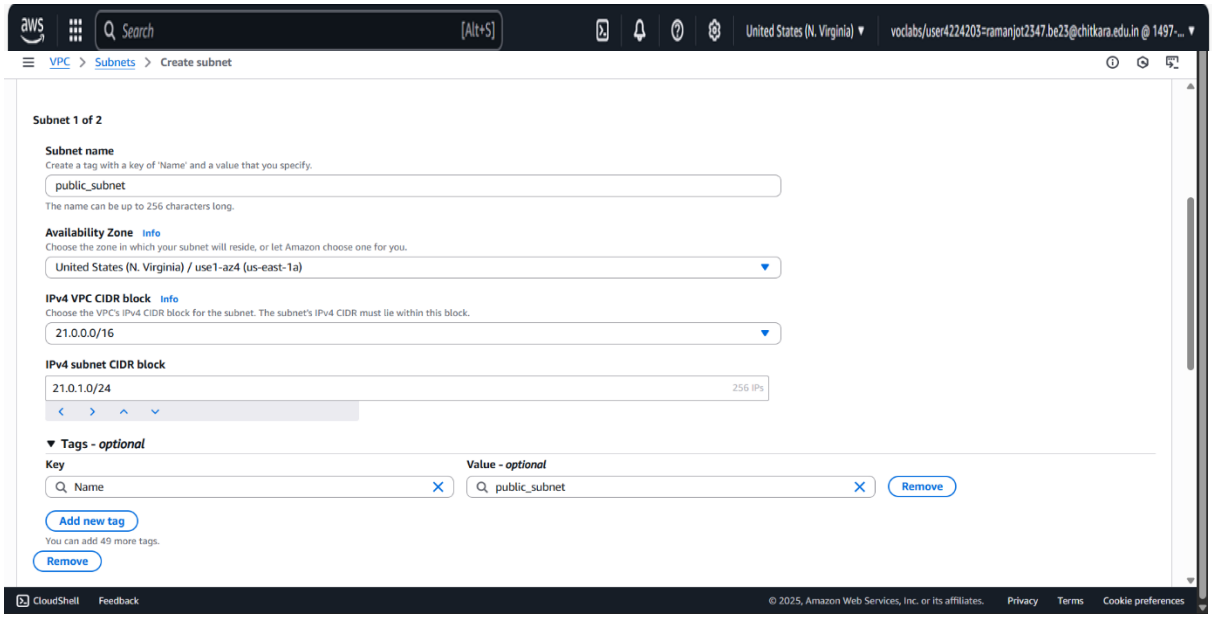

Attach to VPC (igw-085be4dc65608251e)
The following internet gateway was created: igw-085be4dc65608251e - demo_IGW. You can now attach to a VPC to enable the VPC to communicate with the internet.
Attach to a VPC
Attach to VPC (igw-085be4dc65608251e)
VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.
Available VPCs
Attach the internet gateway to this VPC.
vpc-0dcd5abc599bc37ac
AWS Command Line Interface command
Cancel
Attach internet gateway
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

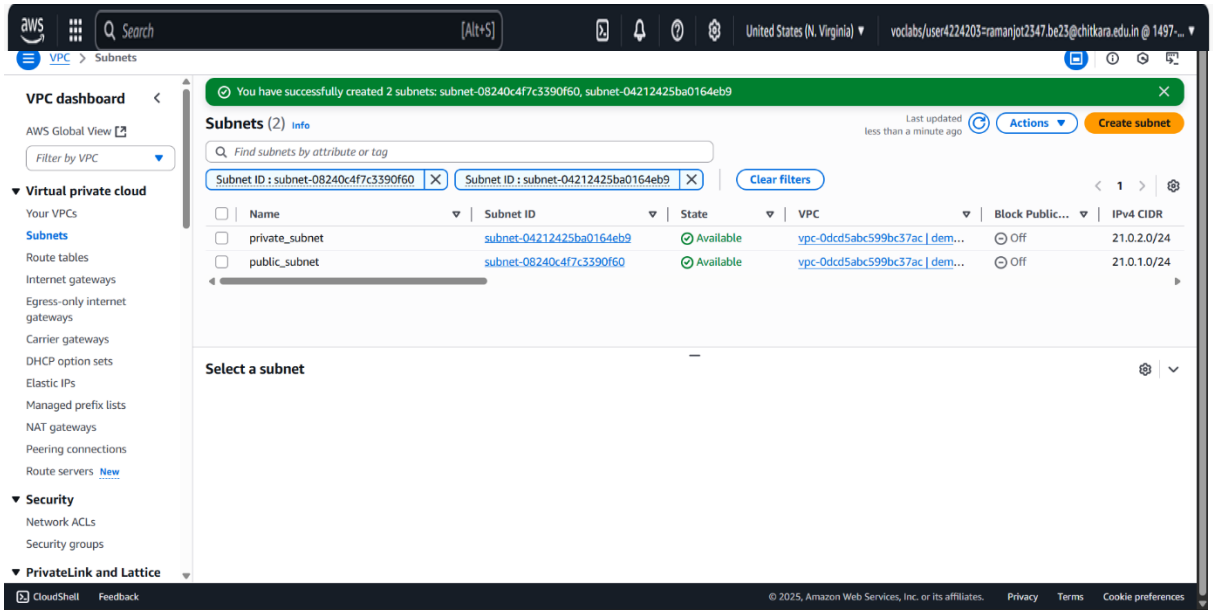

Internet gateway igw-085be4dc65608251e successfully attached to vpc-0dcd5abc599bc37ac
igw-085be4dc65608251e / demo_IGW
Actions
Details
Internet gateway ID
igw-085be4dc65608251e
State
Attached
VPC ID
vpc-0dcd5abc599bc37ac | demo_vpc
Owner
000751820144
Tags
Manage tags
Key
Value
IGW
Name
demo_IGW

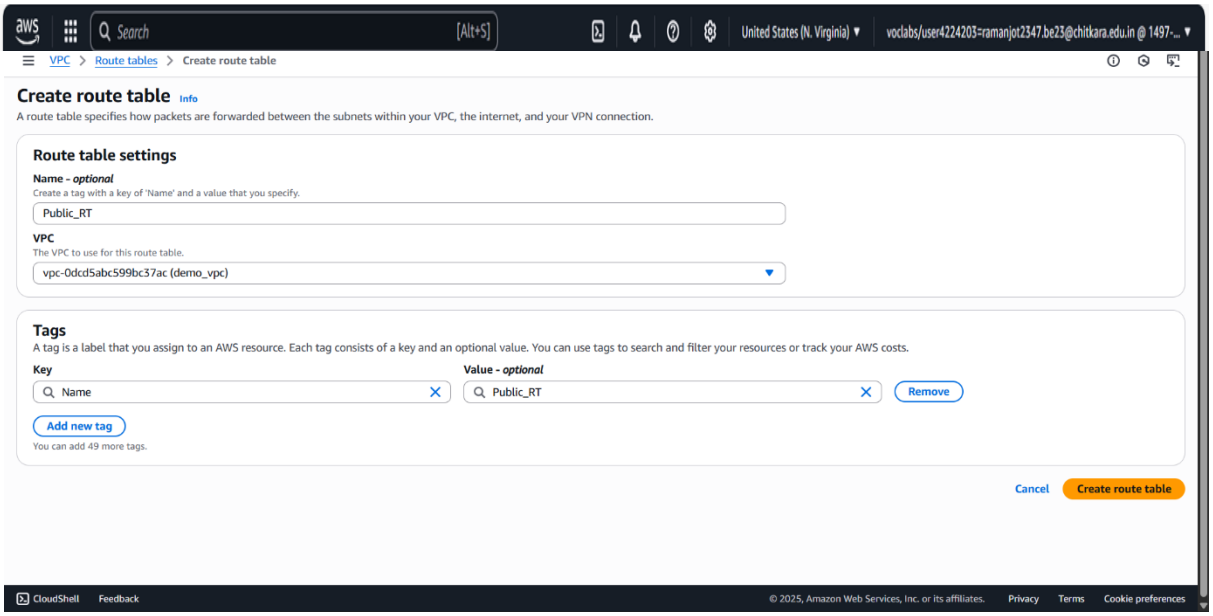

Route tables (2)
Create route table
Select a route table

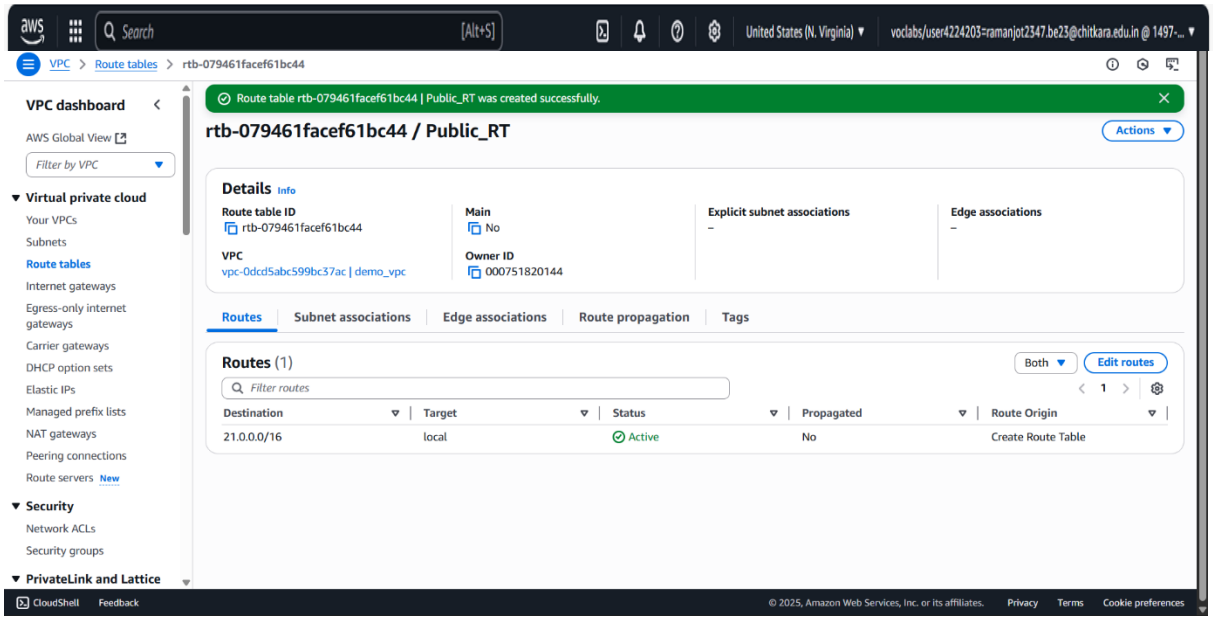

Subnets (6)
Create subnet
Select a subnet

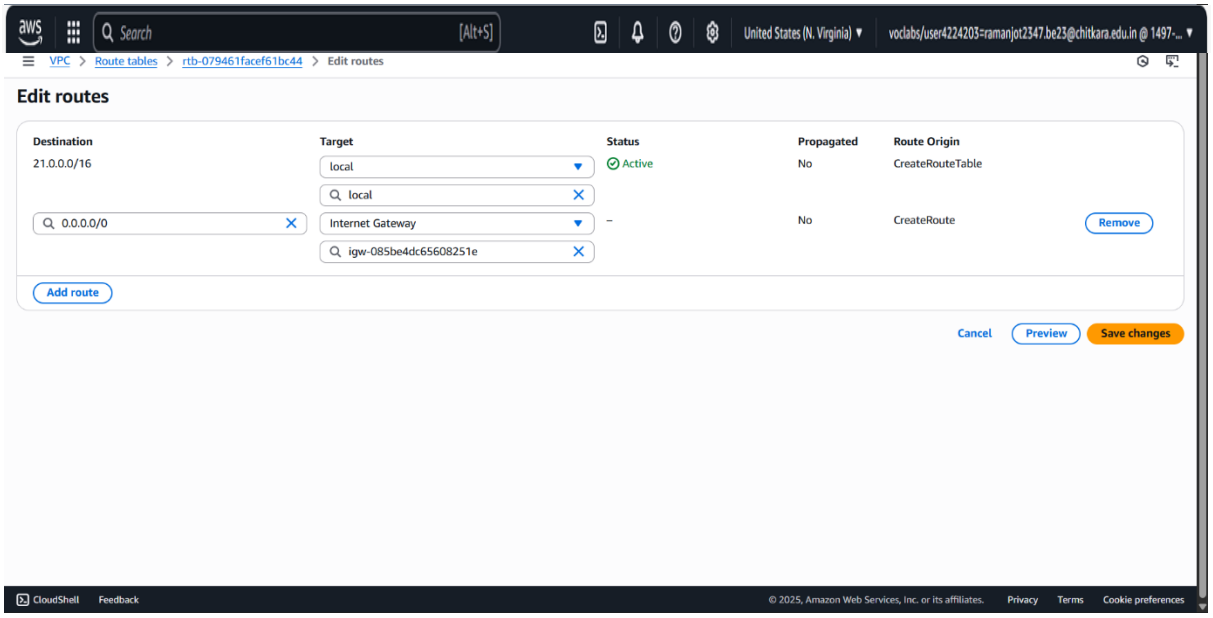

Search [Alt+S]
United States (N. Virginia)
VPC > Subnets > Create subnet
Create subnet Info
VPC
VPC ID
Create subnets in this VPC.
vpc-0dcd5abc599bc37ac (demo_vpc)
Associated VPC CIDRs
IPv4 CIDRs
21.0.0.0/16
Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.
Subnet 1 of 1
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
my-subnet-01
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

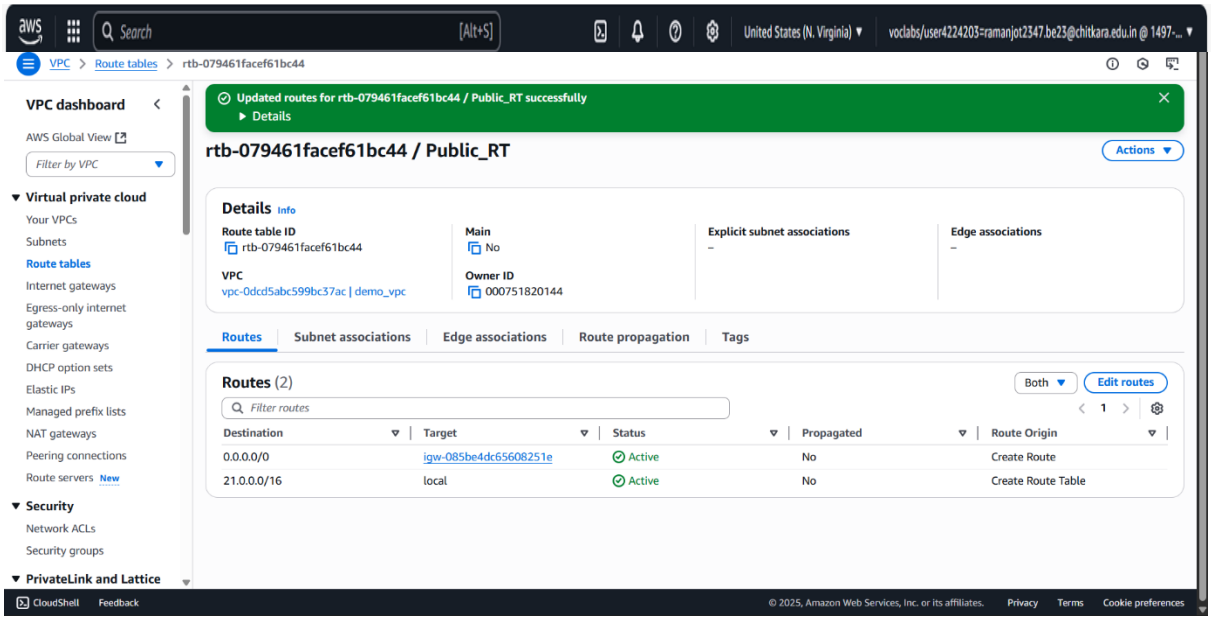

Search [Alt+S]
United States (N. Virginia)
VPC > Subnets > Create subnet
Subnet 1 of 2
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public_subnet
The name can be up to 256 characters long.
Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / use1-az4 (us-east-1a)
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
21.0.0.0/16
IPv4 subnet CIDR block
21.0.1.0/24
256 IPs
Tags - optional
Key
Value - optional
Name
public_subnet
Remove
Add new tag
You can add 49 more tags.
Remove
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

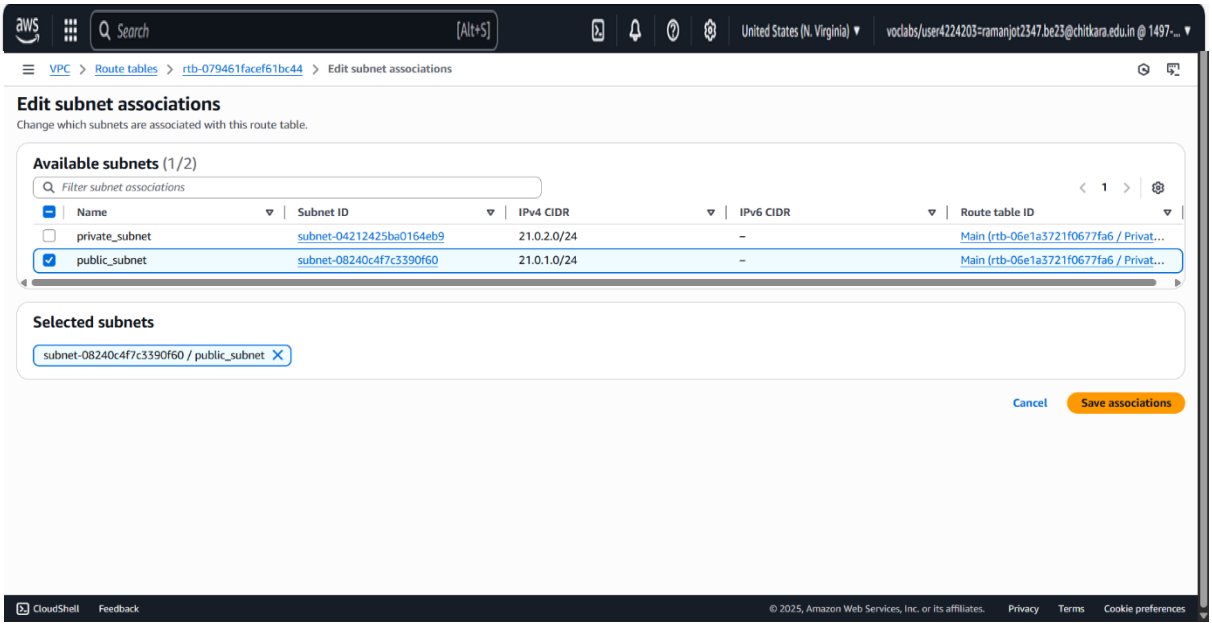

VPC dashboard
You have successfully created 2 subnets: subnet-08240c4f7c3390f60, subnet-04212425ba0164eb9
Subnets (2)
Actions
Create subnet
private_subnet
public_subnet
Select a subnet

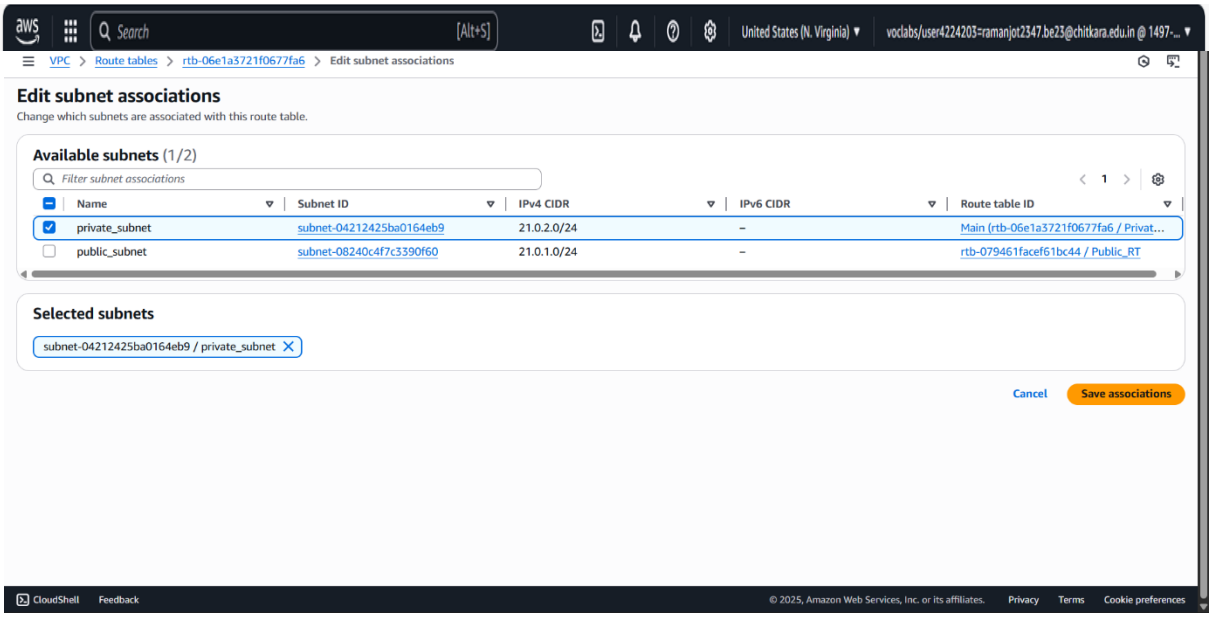

Create route table
Route table settings
Public_RT
vpc-0dcd5abc599bc37ac (demo_vpc)
Tags
Add new tag
Cancel
Create route table

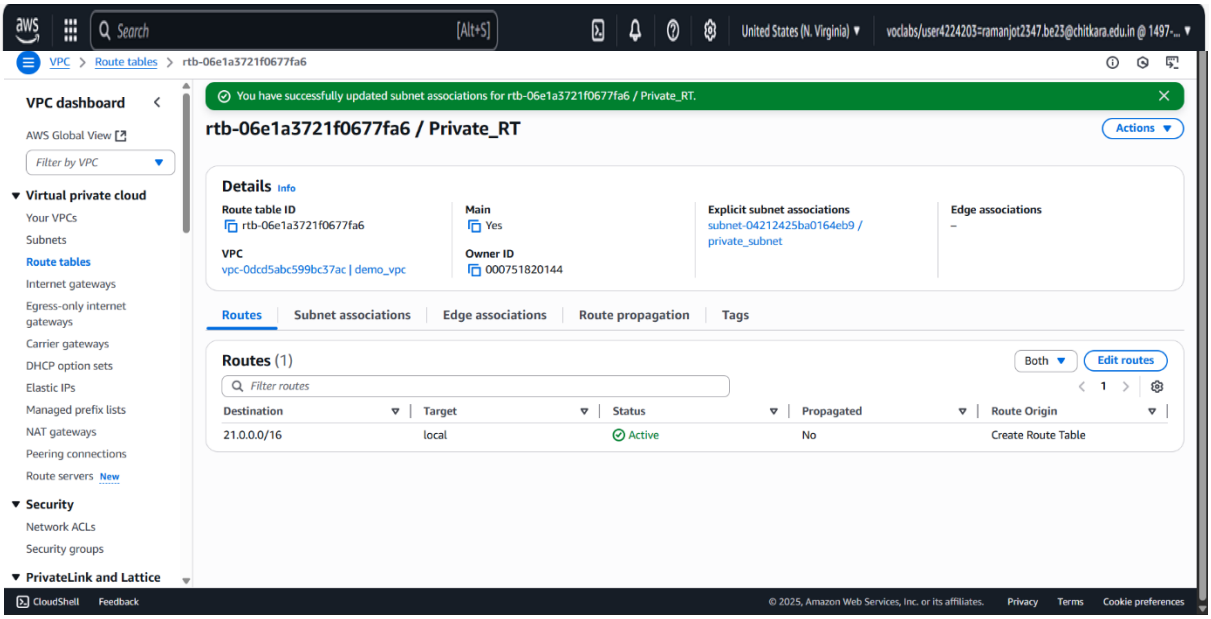

Search
[Alt+S]
United States (N. Virginia)
VPC > Route tables > rtb-079461facef61bc44
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups
PrivateLink and Lattice
Route table rtb-079461facef61bc44 | Public_RT was created successfully.
rtb-079461facef61bc44 / Public_RT
Actions
Details Info
Route table ID
rtb-079461facef61bc44
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0dcd5abc599bc37ac | demo_vpc
Owner ID
000751820144
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Filter routes
Both
Edit routes
Destination
Target
Status
Propagated
Route Origin
21.0.0.0/16
local
Active
No
Create Route Table
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

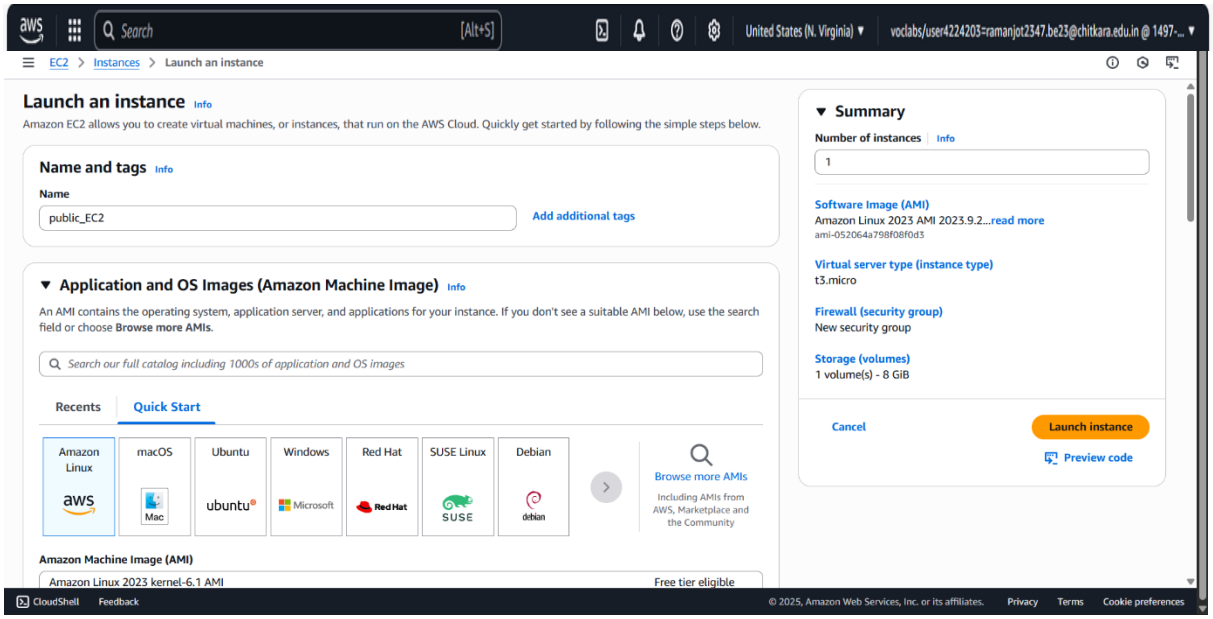

Search
[Alt+S]
United States (N. Virginia)
VPC > Route tables > rtb-079461facef61bc44 > Edit routes
Edit routes
Destination
Target
Status
Propagated
Route Origin
21.0.0.0/16
local
Active
No
CreateRouteTable
local
0.0.0.0/0
Internet Gateway
–
No
CreateRoute
Remove
igw-085be4dc65608251e
Add route
Cancel
Preview
Save changes
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

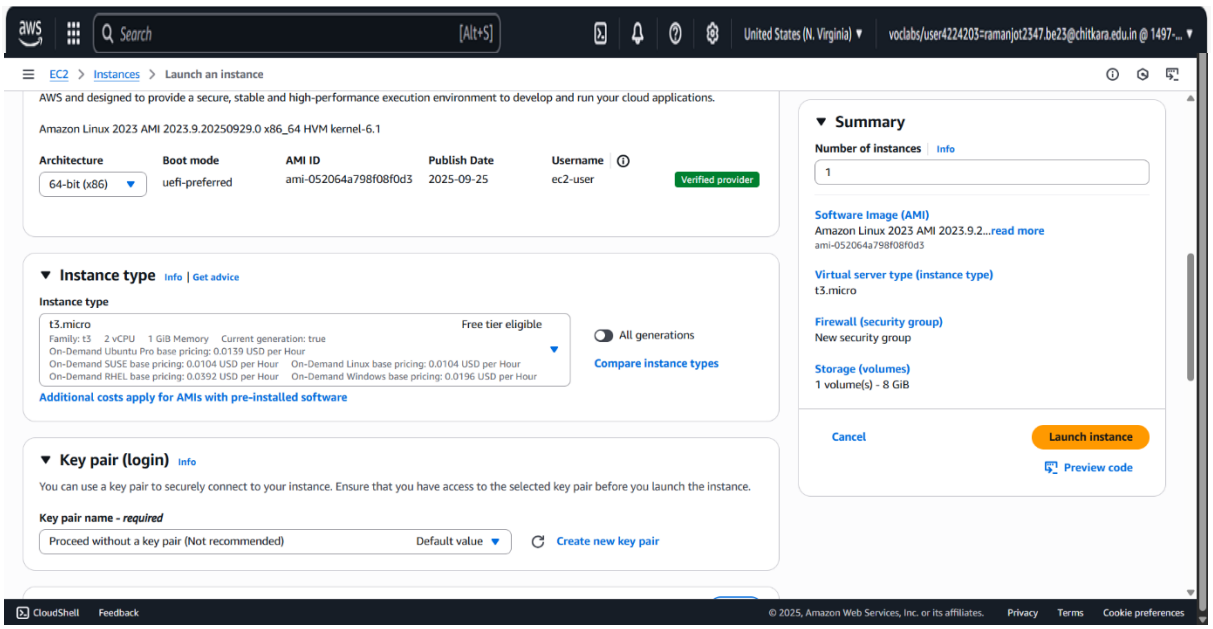

Search [Alt+S]
United States (N. Virginia)
VPC > Route tables > rtb-079461facef61bc44
VPC dashboard
AWS Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers New
Security
Network ACLs
Security groups
PrivateLink and Lattice
Updated routes for rtb-079461facef61bc44 / Public_RT successfully
Details
rtb-079461facef61bc44 / Public_RT
Actions
Details Info
Route table ID
rtb-079461facef61bc44
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-0dcd5abc599bc37ac | demo_vpc
Owner ID
000751820144
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
Route Origin
0.0.0.0/0
igw-085be4dc65608251e
Active
No
Create Route
21.0.0.0/16
local
Active
No
Create Route Table
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

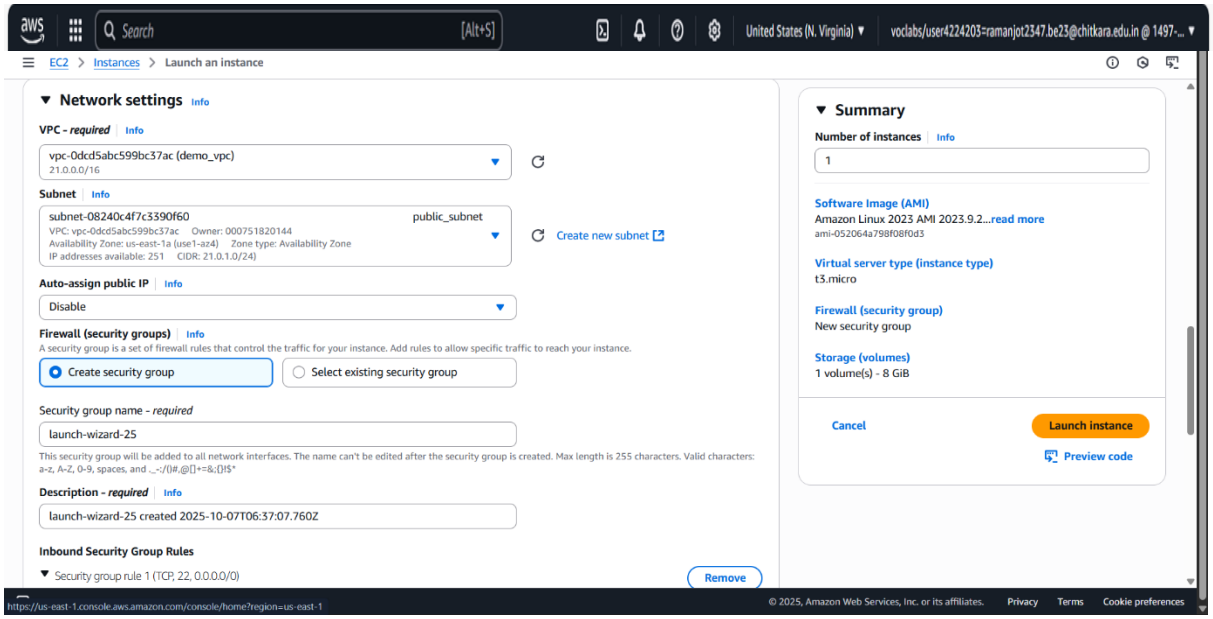

Search [Alt+S]
United States (N. Virginia)
VPC > Route tables > rtb-079461facef61bc44 > Edit subnet associations
Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
private_subnet
subnet-04212425ba0164eb9
21.0.2.0/24
–
Main (rtb-06e1a3721f0677fa6 / Privat...
public_subnet
subnet-08240c4f7c3390f60
21.0.1.0/24
–
Main (rtb-06e1a3721f0677fa6 / Privat...
Selected subnets
subnet-08240c4f7c3390f60 / public_subnet
Cancel
Save associations
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

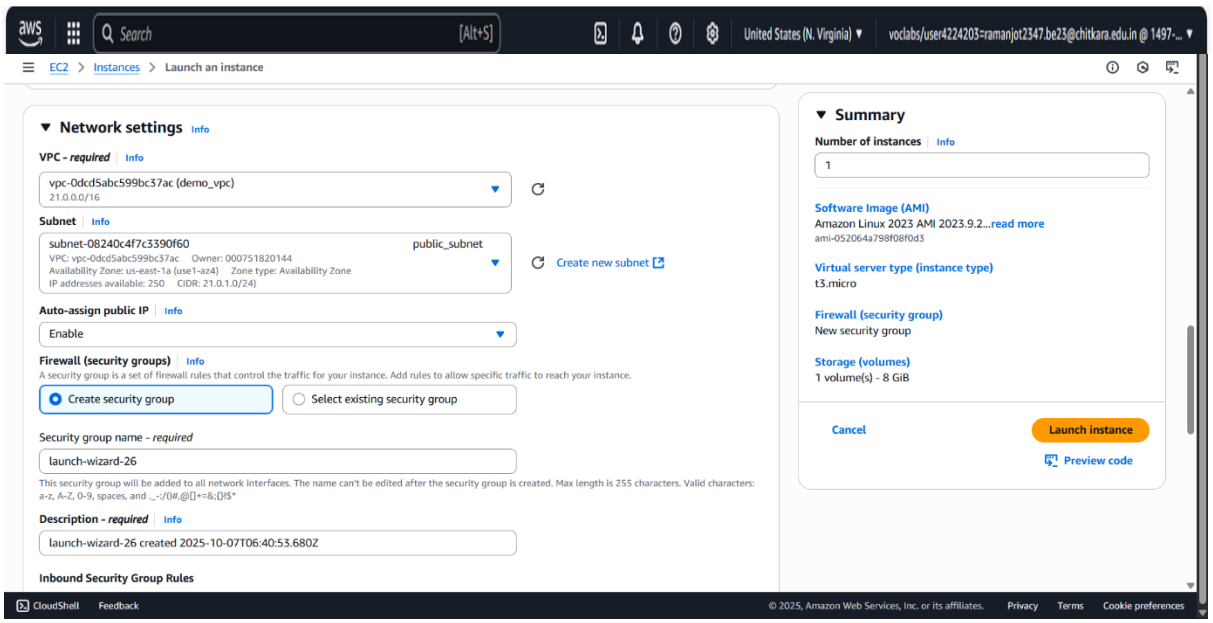

Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (1/2)
Filter subnet associations
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
private_subnet
subnet-04212425ba0164eb9
21.0.2.0/24
Main (rtb-06e1a3721f0677fa6 / Privat...
public_subnet
subnet-08240c4f7c3390f60
21.0.1.0/24
rtb-079461facef61bc44 / Public_RT
Selected subnets
subnet-04212425ba0164eb9 / private_subnet
Cancel
Save associations

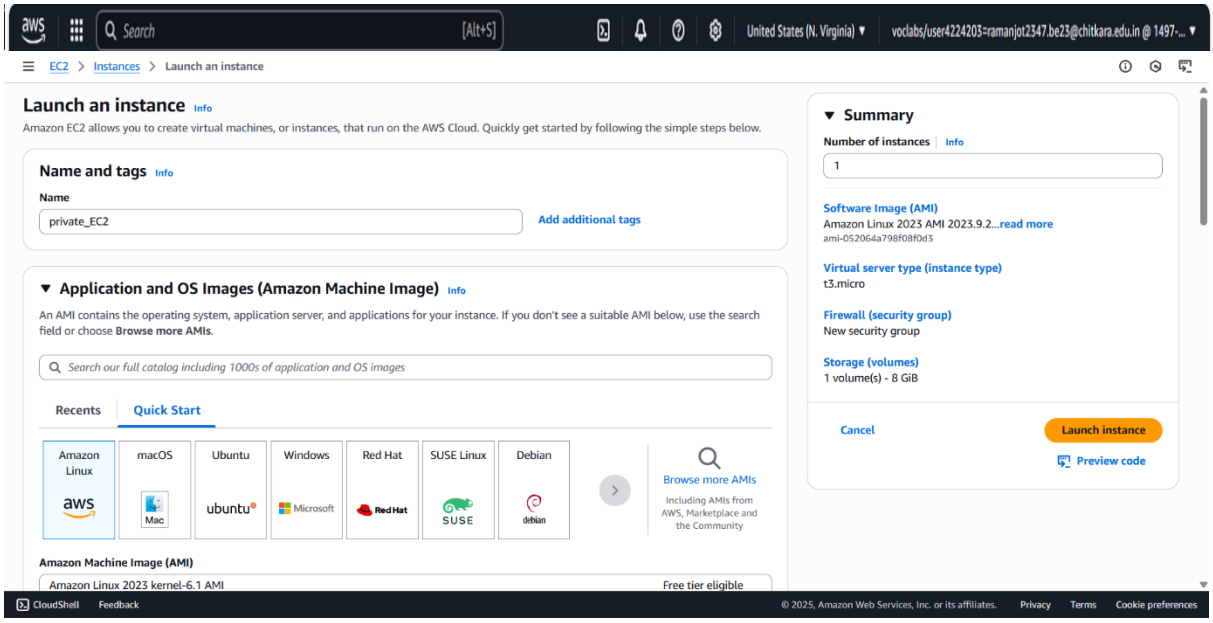

You have successfully updated subnet associations for rtb-06e1a3721f0677fa6 / Private_RT.
rtb-06e1a3721f0677fa6 / Private_RT
Actions
Details
Route table ID
rtb-06e1a3721f0677fa6
Main
Yes
Explicit subnet associations
subnet-04212425ba0164eb9 / private_subnet
Edge associations
VPC
vpc-0dcd5abc599bc37ac | demo_vpc
Owner ID
000751820144
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (1)
Both
Edit routes
Destination
Target
Status
Propagated
Route Origin
21.0.0.0/16
local
Active
No
Create Route Table

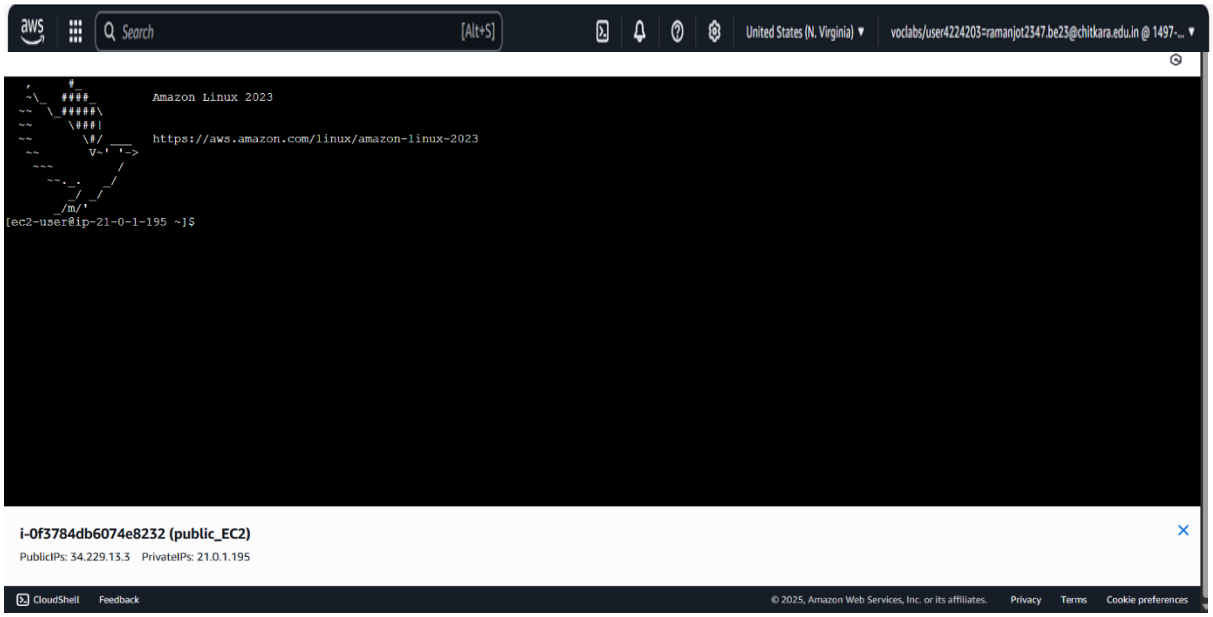

Launch an instance
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags
Name
public_EC2
Add additional tags
Application and OS Images (Amazon Machine Image)
An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Amazon Linux 2023 kernel-6.1 AMI
Free tier eligible
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

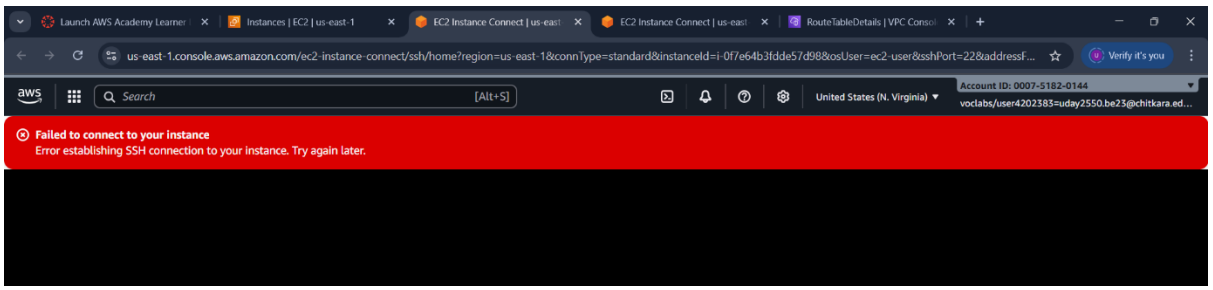

AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.
Amazon Linux 2023 AMI 2023.9.20250929.0 x86_64 HVM kernel-6.1
Architecture
64-bit (x86)
Boot mode
uefi-preferred
AMI ID
ami-052064a798f08f0d3
Publish Date
2025-09-25
Username
ec2-user
Verified provider
Instance type
Instance type
t3.micro
Free tier eligible
Family: t3 2 vCPU 1 GiB Memory Current generation: true
On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour
On-Demand SUSE base pricing: 0.0104 USD per Hour
On-Demand Linux base pricing: 0.0104 USD per Hour
On-Demand RHEL base pricing: 0.0392 USD per Hour
On-Demand Windows base pricing: 0.0196 USD per Hour
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software
Key pair (login)
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
Proceed without a key pair (Not recommended)
Default value
Create new key pair
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
United States (N. Virginia)
EC2 > Instances > Launch an instance
Network settings Info
VPC - required Info
vpc-0dcd5abc599bc37ac (demo_vpc)
21.0.0.0/16
Subnet Info
subnet-08240c4f7c3390f60 public_subnet
VPC: vpc-0dcd5abc599bc37ac Owner: 000751820144
Availability Zone: us-east-1a (use1-az4) Zone type: Availability Zone
IP addresses available: 251 CIDR: 21.0.1.0/24)
Create new subnet
Auto-assign public IP Info
Disable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
launch-wizard-25
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-25 created 2025-10-07T06:37:07.760Z
Inbound Security Group Rules
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
United States (N. Virginia)
EC2 > Instances > Launch an instance
Network settings Info
VPC - required Info
vpc-0dcd5abc599bc37ac (demo_vpc)
21.0.0.0/16
Subnet Info
subnet-08240c4f7c3390f60 public_subnet
VPC: vpc-0dcd5abc599bc37ac Owner: 000751820144
Availability Zone: us-east-1a (use1-az4) Zone type: Availability Zone
IP addresses available: 250 CIDR: 21.0.1.0/24)
Create new subnet
Auto-assign public IP Info
Enable
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
launch-wizard-26
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-26 created 2025-10-07T06:40:53.680Z
Inbound Security Group Rules
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Launch an instance
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags
Name
private_EC2
Add additional tags
Application and OS Images (Amazon Machine Image)
An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose Browse more AMIs.
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Amazon Machine Image (AMI)
Amazon Linux 2023 kernel-6.1 AMI
Free tier eligible
Summary
Number of instances
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2...read more
ami-052064a798f08f0d3
Virtual server type (instance type)
t3.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Cancel
Launch instance
Preview code


Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-21-0-1-195 ~]$
i-0f3784db6074e8232 (public_EC2)
PublicIPs: 34.229.13.3 PrivateIPs: 21.0.1.195


Failed to connect to your instance
Error establishing SSH connection to your instance. Try again later.

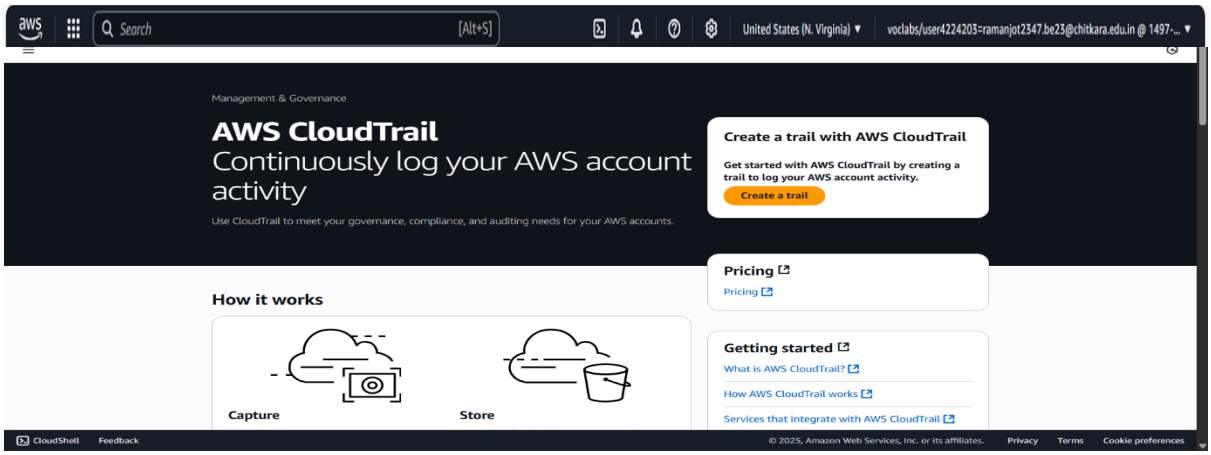
Practical No. 7:

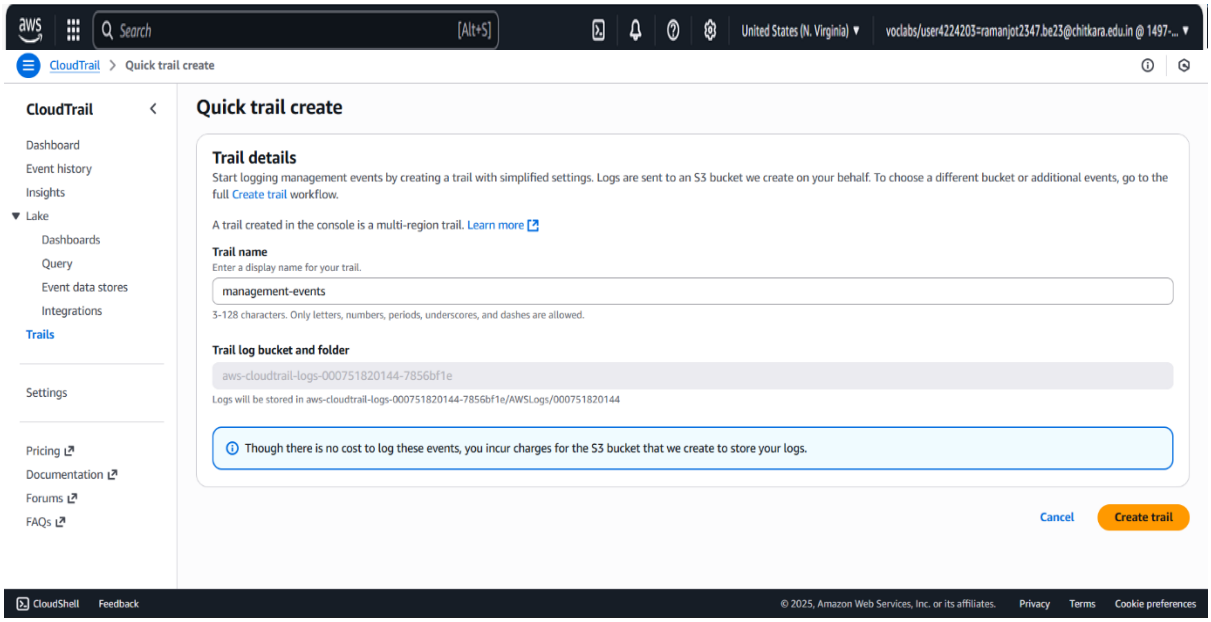
Practical Title: Configure Amazon CloudWatch to monitor EC2 instance metrics and set up alarms.

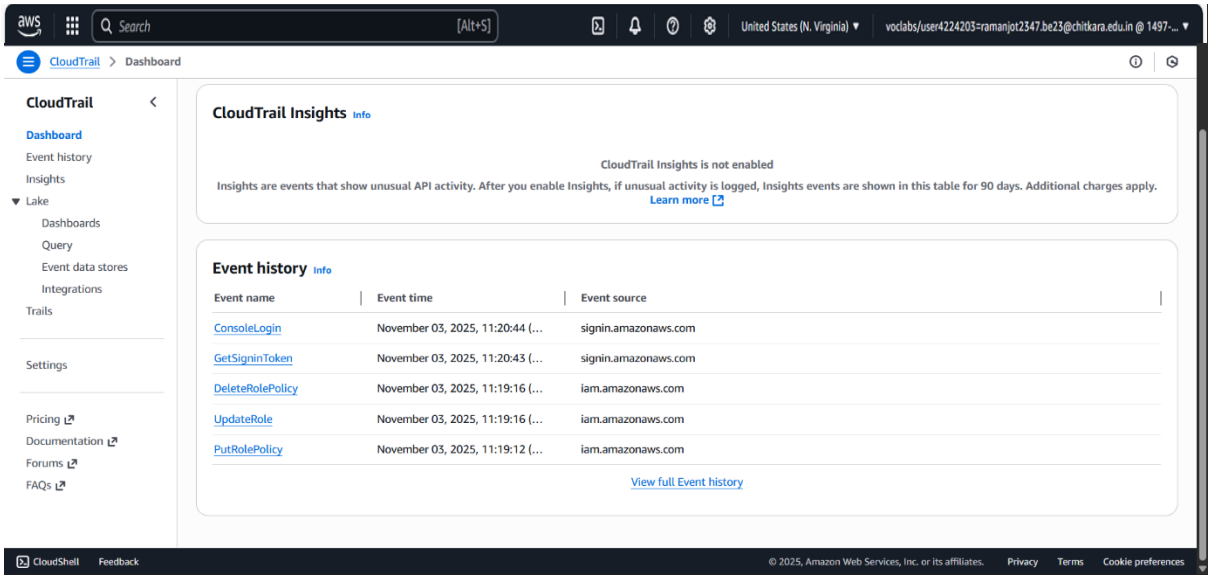
Objective:

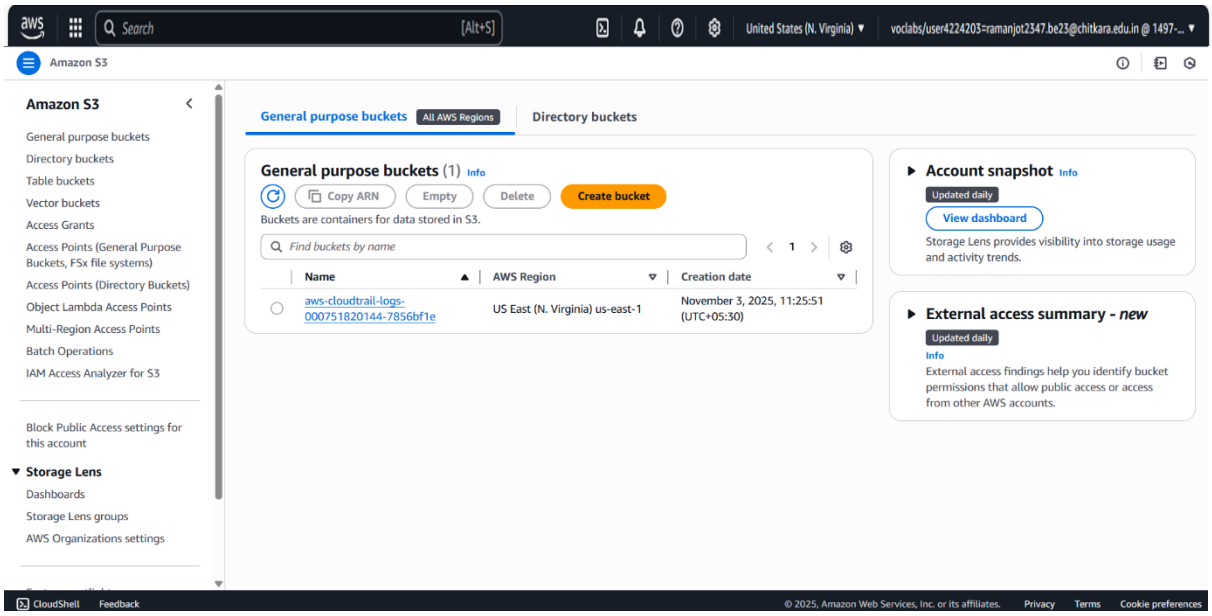
- **Configure Amazon CloudWatch to monitor EC2 instance metrics and set up alarms.**

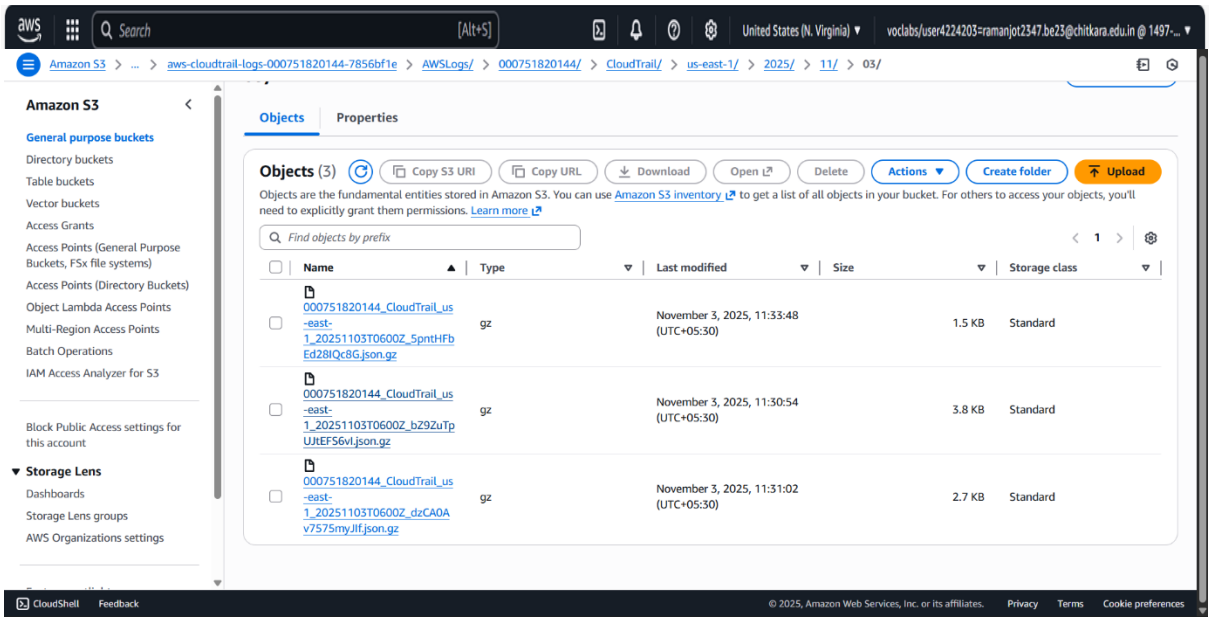
Step-by-Step Procedure with Screenshots:

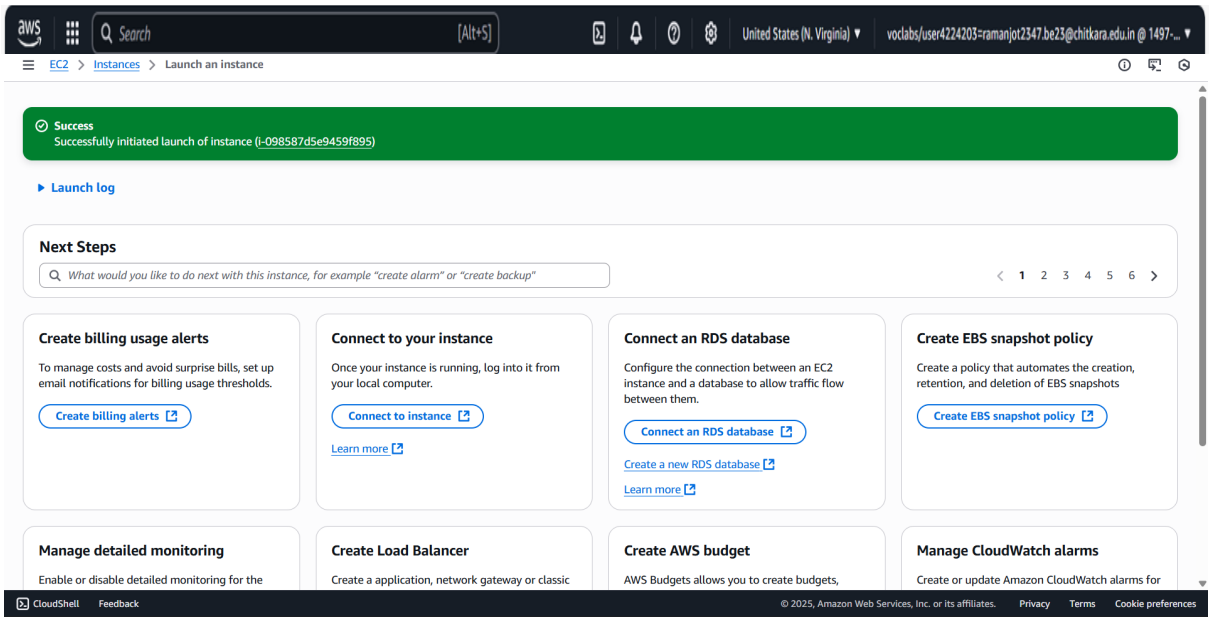


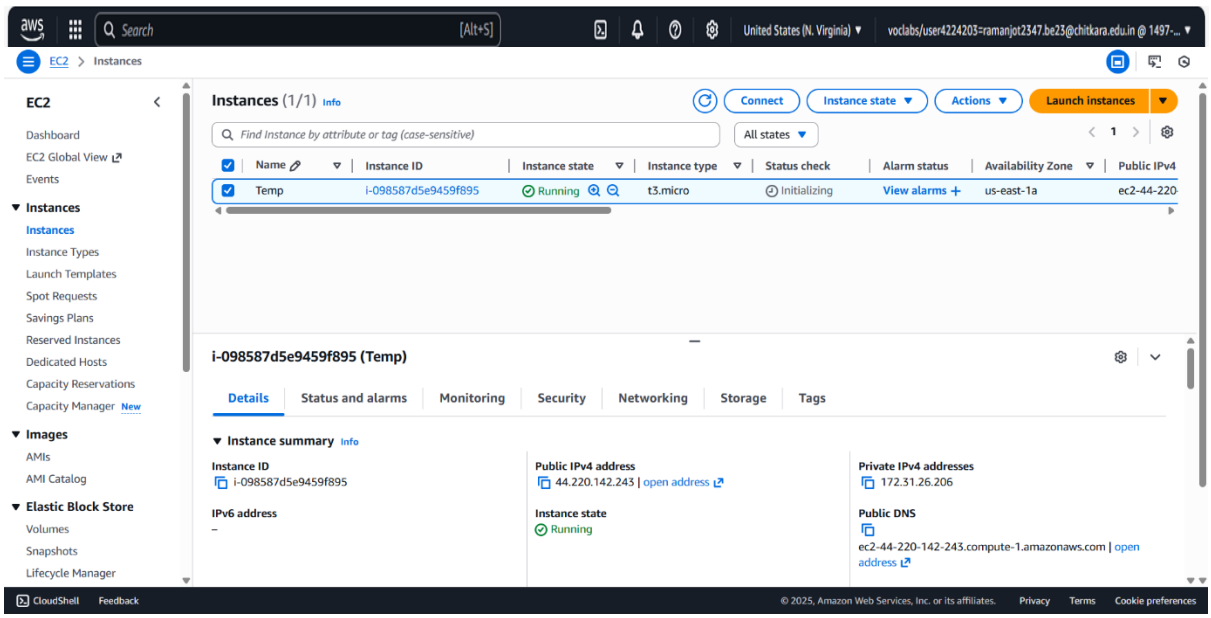


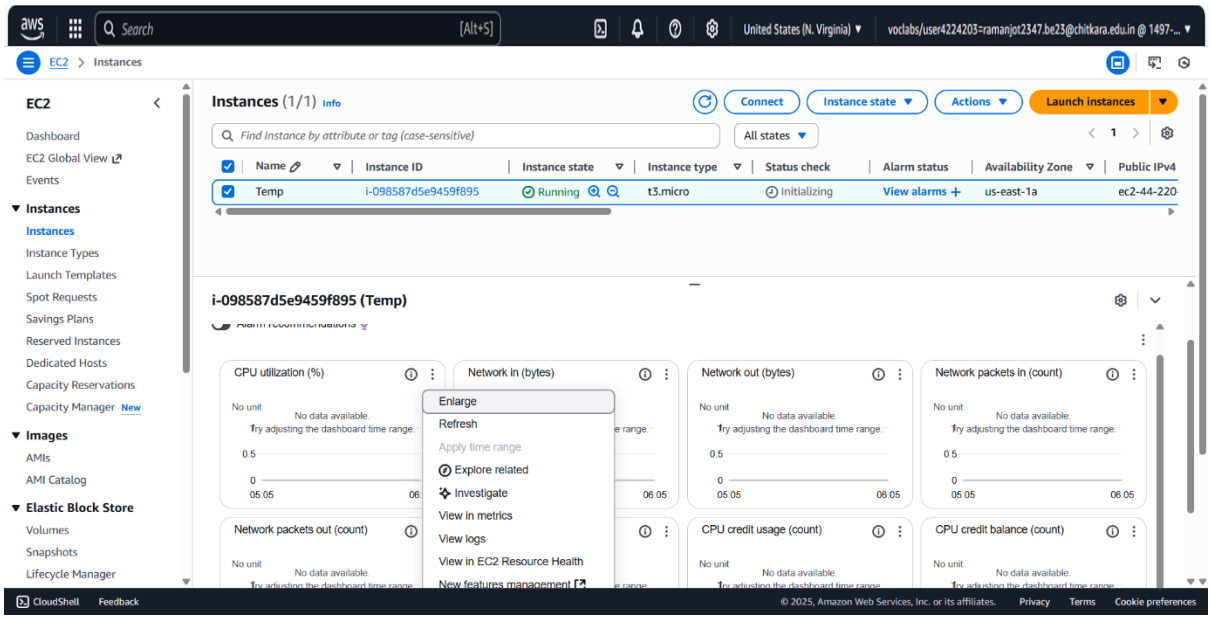

Search
[Alt+S]
United States (N. Virginia)
CloudTrail > Dashboard
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboards
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
CloudTrail Insights Info
CloudTrail Insights is not enabled
Insights are events that show unusual API activity. After you enable Insights, if unusual activity is logged, Insights events are shown in this table for 90 days. Additional charges apply.
Learn more
Event history Info
Event name
Event time
Event source
ConsoleLogin
November 03, 2025, 11:20:44 (...
signin.amazonaws.com
GetSigninToken
November 03, 2025, 11:20:43 (...
signin.amazonaws.com
DeleteRolePolicy
November 03, 2025, 11:19:16 (...
iam.amazonaws.com
UpdateRole
November 03, 2025, 11:19:16 (...
iam.amazonaws.com
PutRolePolicy
November 03, 2025, 11:19:12 (...
iam.amazonaws.com
View full Event history
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

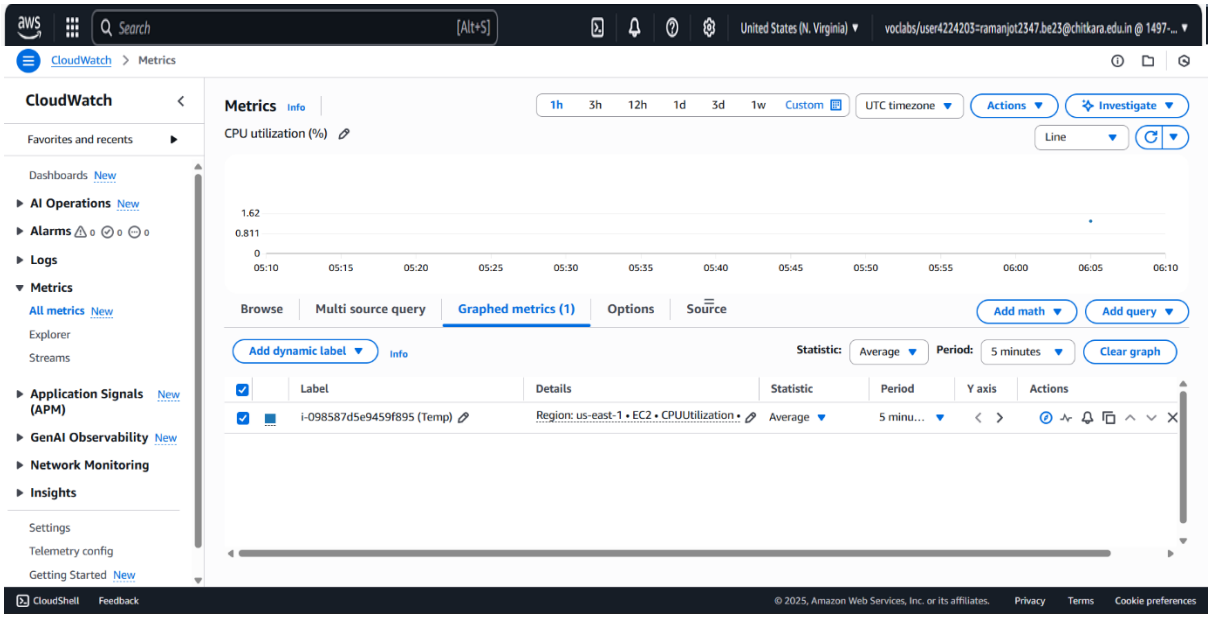

Search
[Alt+S]
United States (N. Virginia)
Amazon S3
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Vector buckets
Access Grants
Access Points (General Purpose Buckets, FSx file systems)
Access Points (Directory Buckets)
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
General purpose buckets
All AWS Regions
Directory buckets
General purpose buckets (1) Info
Copy ARN
Empty
Delete
Create bucket
Buckets are containers for data stored in S3.
Find buckets by name
Name
AWS Region
Creation date
aws-cloudtrail-logs-000751820144-7856bf1e
US East (N. Virginia) us-east-1
November 3, 2025, 11:25:51 (UTC+05:30)
Account snapshot Info
Updated daily
View dashboard
Storage Lens provides visibility into storage usage and activity trends.
External access summary - new
Updated daily
Info
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

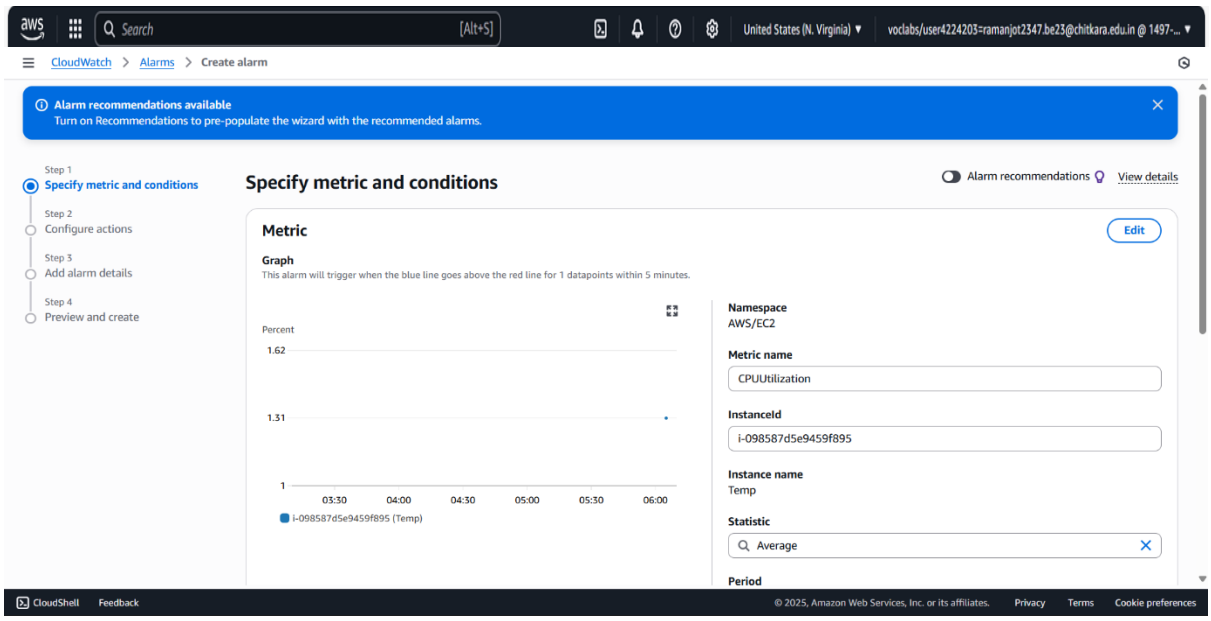

Search
[Alt+S]
United States (N. Virginia)
Amazon S3
aws-cloudtrail-logs-000751820144-7856bf1e
AWSLogs/
000751820144/
CloudTrail/
us-east-1/
2025/
11/
03/
Amazon S3
General purpose buckets
Directory buckets
Table buckets
Vector buckets
Access Grants
Access Points (General Purpose Buckets, FSx file systems)
Access Points (Directory Buckets)
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Objects
Properties
Objects (3)
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Name
Type
Last modified
Size
Storage class
000751820144_CloudTrail_us-east-1_20251103T0600Z_5pntHFbEd28IQc8G.json.gz
gz
November 3, 2025, 11:33:48 (UTC+05:30)
1.5 KB
Standard
000751820144_CloudTrail_us-east-1_20251103T0600Z_bZ9ZuTpUJtEFS6vI.json.gz
gz
November 3, 2025, 11:30:54 (UTC+05:30)
3.8 KB
Standard
000751820144_CloudTrail_us-east-1_20251103T0600Z_dzCA0Av7575myJIf.json.gz
gz
November 3, 2025, 11:31:02 (UTC+05:30)
2.7 KB
Standard
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

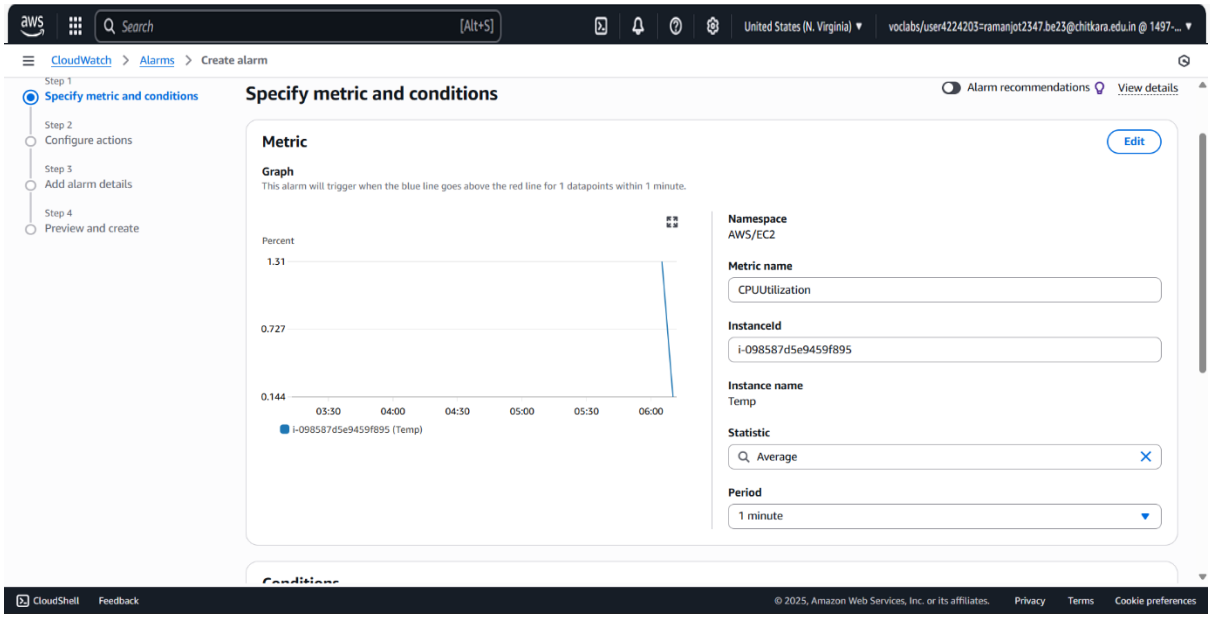

Search
[Alt+S]
United States (N. Virginia)
EC2
Instances
Launch an instance
Success
Successfully initiated launch of instance (i-098587d5e9459f895)
Launch log
Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"
Create billing usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing 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
Enable or disable detailed monitoring for the
Create Load Balancer
Create a application, network gateway or classic
Create AWS budget
AWS Budgets allows you to create budgets,
Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

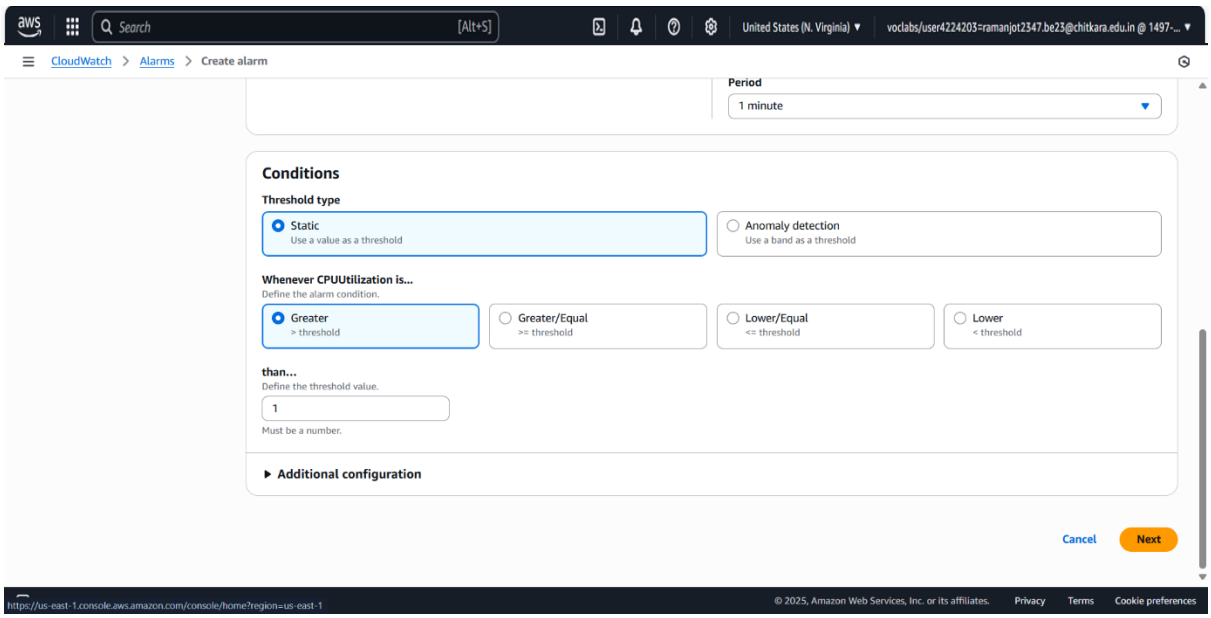

Search [Alt+S]
United States (N. Virginia)
EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4
Temp
i-098587d5e9459f895
Running
t3.micro
Initializing
View alarms
us-east-1a
ec2-44-220
i-098587d5e9459f895 (Temp)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-098587d5e9459f895
Public IPv4 address
44.220.142.243 | open address
Private IPv4 addresses
172.31.26.206
IPv6 address
–
Instance state
Running
Public DNS
ec2-44-220-142-243.compute-1.amazonaws.com | open address
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

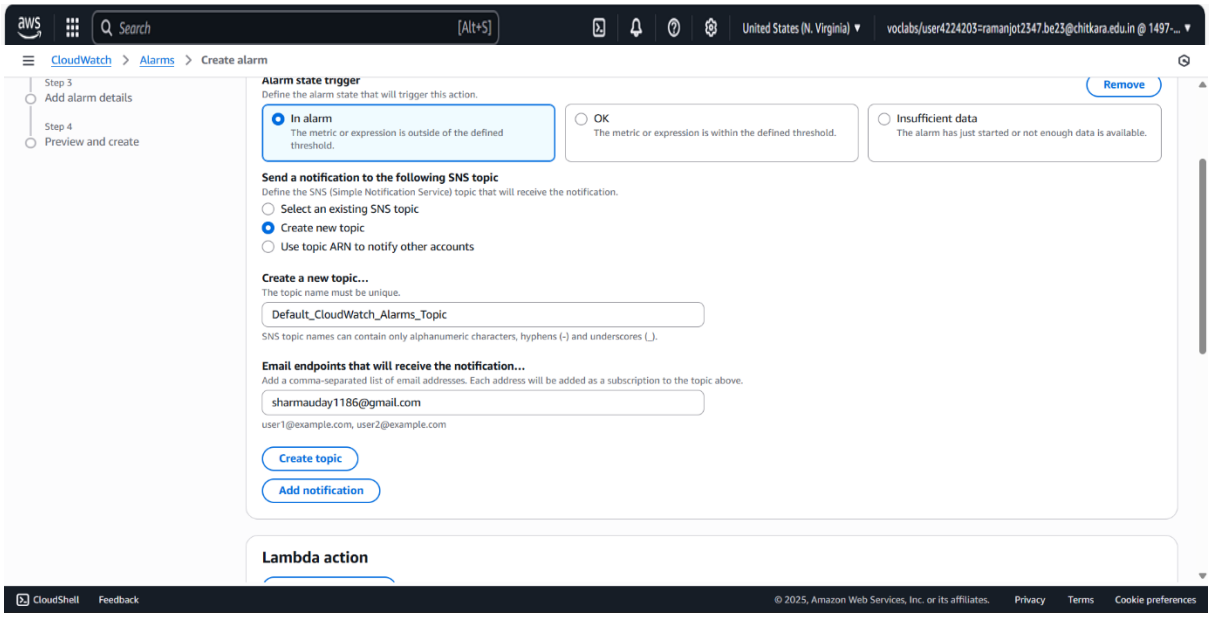

Search [Alt+S]
United States (N. Virginia)
EC2 > Instances
EC2
Instances (1/1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4
Temp
i-098587d5e9459f895
Running
t3.micro
Initializing
View alarms
us-east-1a
ec2-44-220
i-098587d5e9459f895 (Temp)
CPU utilization (%)
Network in (bytes)
Network out (bytes)
Network packets in (count)
Network packets out (count)
CPU credit usage (count)
CPU credit balance (count)
No data available.
Try adjusting the dashboard time range.
Enlarge
Refresh
Apply time range
Explore related
Investigate
View in metrics
View logs
View in EC2 Resource Health
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

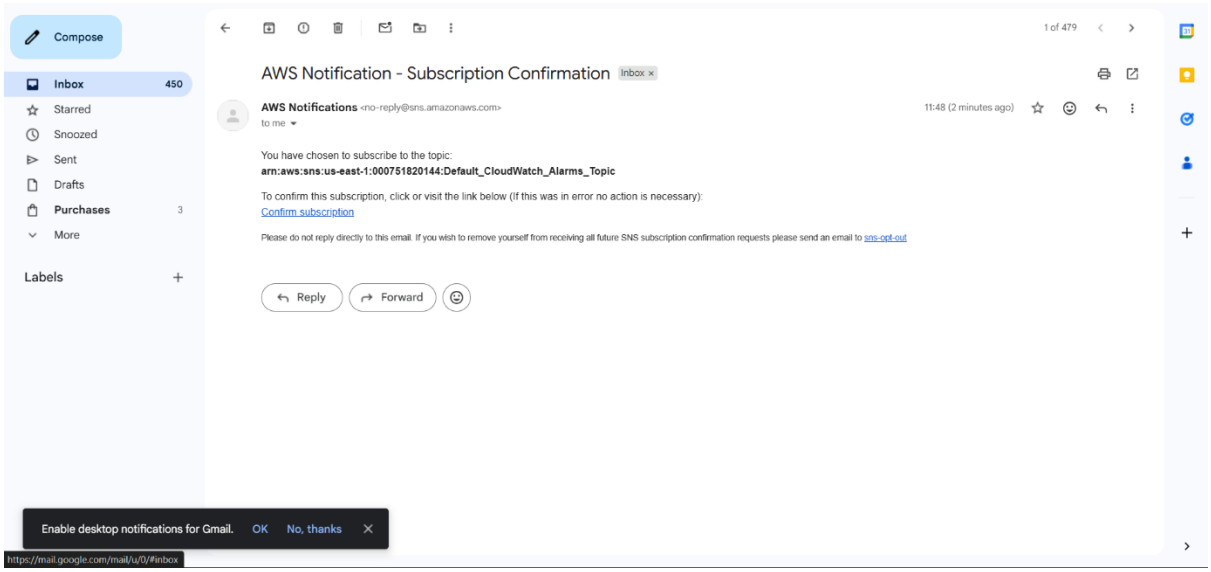

Search
[Alt+S]
United States (N. Virginia)
CloudWatch
Metrics
CloudWatch
Favorites and recents
Dashboards New
AI Operations New
Alarms
Logs
Metrics
All metrics New
Explorer
Streams
Application Signals (APM) New
GenAI Observability New
Network Monitoring
Insights
Settings
Telemetry config
Getting Started New
Metrics Info
CPU utilization (%)
1h 3h 12h 1d 3d 1w Custom
UTC timezone
Actions
Investigate
Line
1.62
0.811
0
05:10 05:15 05:20 05:25 05:30 05:35 05:40 05:45 05:50 05:55 06:00 06:05 06:10
Browse
Multi source query
Graphed metrics (1)
Options
Source
Add math
Add query
Add dynamic label
Info
Statistic: Average
Period: 5 minutes
Clear graph
Label
Details
Statistic
Period
Y axis
Actions
i-098587d5e9459f895 (Temp)
Region: us-east-1 • EC2 • CPUUtilization •
Average
5 minu...
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

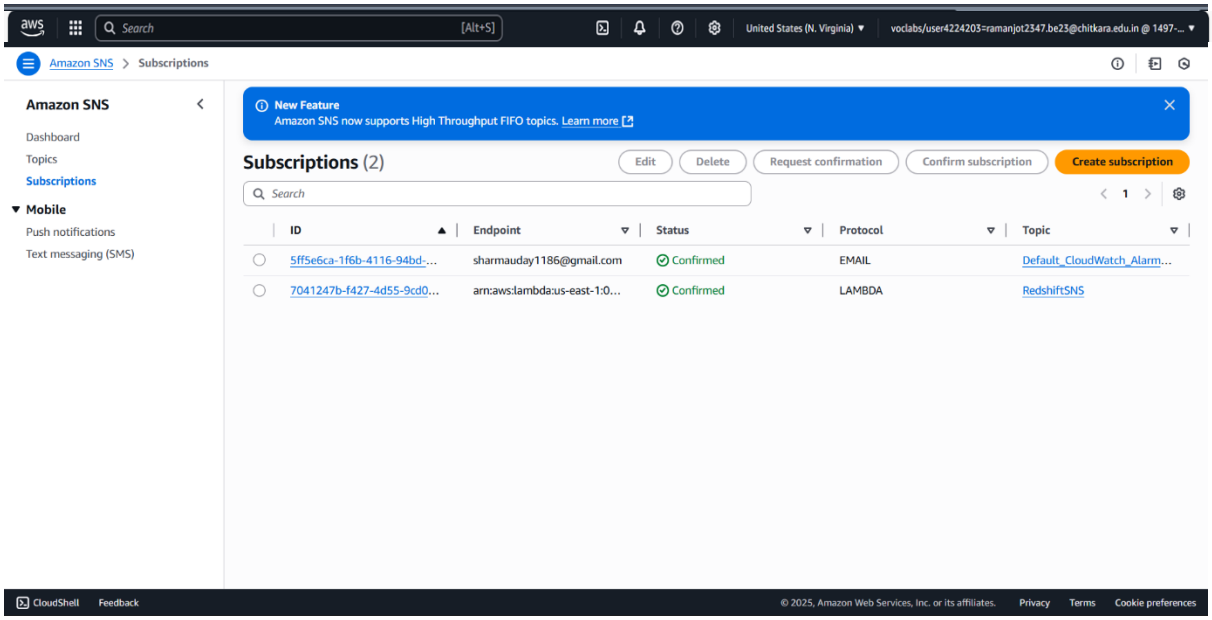

Search
[Alt+S]
United States (N. Virginia)
CloudWatch
Alarms
Create alarm
Alarm recommendations available
Turn on Recommendations to pre-populate the wizard with the recommended alarms.
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add alarm details
Step 4
Preview and create
Specify metric and conditions
Alarm recommendations
View details
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.
Percent
1.62
1.31
1
03:30 04:00 04:30 05:00 05:30 06:00
i-098587d5e9459f895 (Temp)
Namespace
AWS/EC2
Metric name
CPUUtilization
InstanceId
i-098587d5e9459f895
Instance name
Temp
Statistic
Average
Period
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

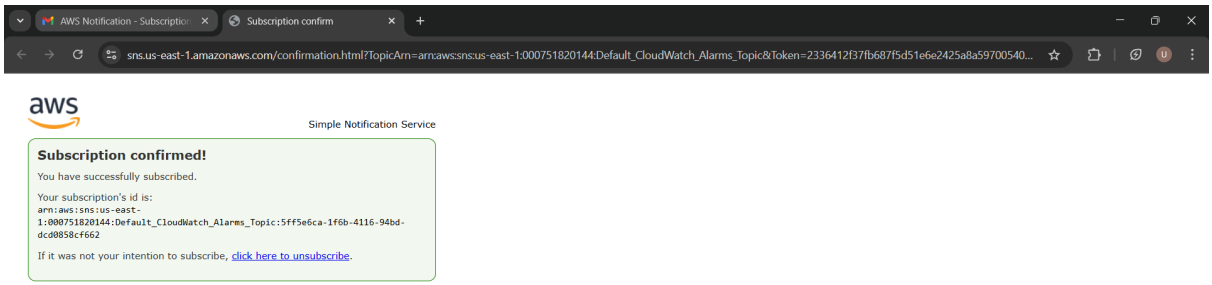

Search [Alt+S]
United States (N. Virginia)
CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add alarm details
Step 4
Preview and create
Specify metric and conditions
Alarm recommendations
View details
Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.
Percent
1.31
0.727
0.144
03:30
04:00
04:30
05:00
05:30
06:00
i-098587d5e9459f895 (Temp)
Namespace
AWS/EC2
Metric name
CPUUtilization
InstanceId
i-098587d5e9459f895
Instance name
Temp
Statistic
Average
Period
1 minute
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

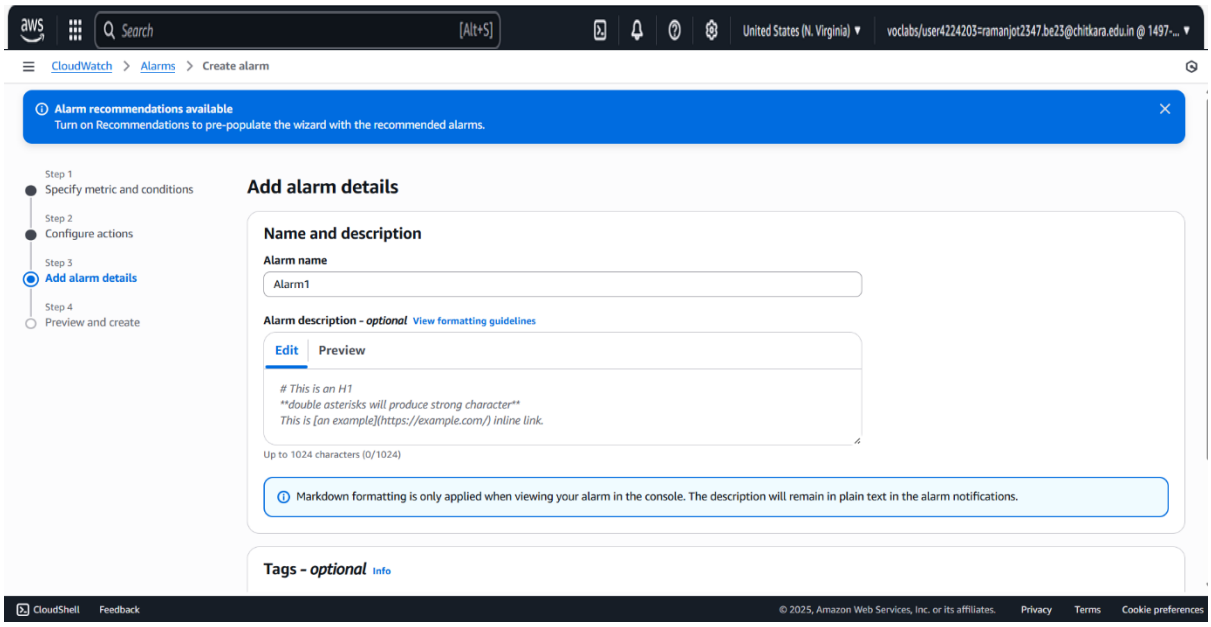

Search [Alt+S]
United States (N. Virginia)
CloudWatch > Alarms > Create alarm
Period
1 minute
Conditions
Threshold type
Static
Use a value as a threshold
Anomaly detection
Use a band as a threshold
Whenever CPUUtilization is...
Define the alarm condition.
Greater
> threshold
Greater/Equal
>= threshold
Lower/Equal
<= threshold
Lower
< threshold
than...
Define the threshold value.
1
Must be a number.
Additional configuration
Cancel
Next
https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

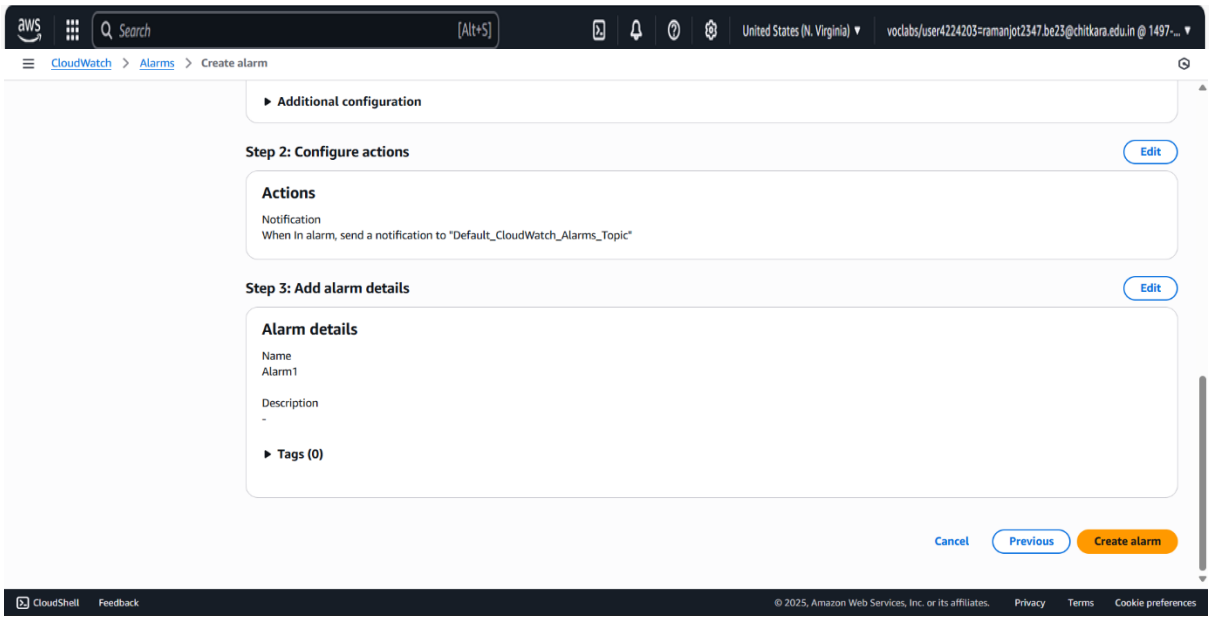

Search
[Alt+S]
United States (N. Virginia)
CloudWatch
Alarms
Create alarm
Step 3
Add alarm details
Step 4
Preview and create
Alarm state trigger
Define the alarm state that will trigger this action.
Remove
In alarm
The metric or expression is outside of the defined threshold.
OK
The metric or expression is within the defined threshold.
Insufficient data
The alarm has just started or not enough data is available.
Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.
Select an existing SNS topic
Create new topic
Use topic ARN to notify other accounts
Create a new topic...
The topic name must be unique.
Default_CloudWatch_Alarms_Topic
SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).
Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.
sharmauday1186@gmail.com
user1@example.com, user2@example.com
Create topic
Add notification
Lambda action
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Compose
Inbox 450
Starred
Snoozed
Sent
Drafts
Purchases 3
More
Labels
1 of 479
AWS Notification - Subscription Confirmation
Inbox
AWS Notifications <no-reply@sns.amazonaws.com>
to me
11:48 (2 minutes ago)
You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:000751820144:Default_CloudWatch_Alarms_Topic
To confirm this subscription, click or visit the link below (if this was in error no action is necessary):
Confirm subscription
Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out
Reply
Forward
Enable desktop notifications for Gmail.
OK
No, thanks
https://mail.google.com/mail/u/0/#inbox

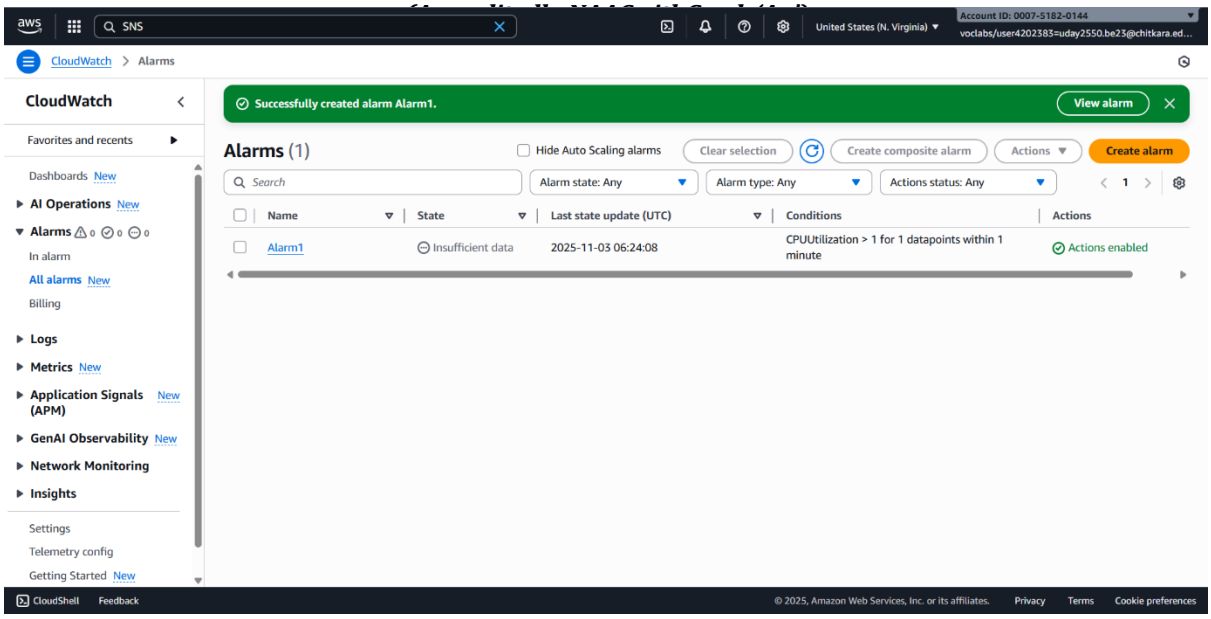

Search
[Alt+S]
United States (N. Virginia)
Amazon SNS > Subscriptions
Amazon SNS
Dashboard
Topics
Subscriptions
Mobile
Push notifications
Text messaging (SMS)
New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more
Subscriptions (2)
Edit
Delete
Request confirmation
Confirm subscription
Create subscription
Search
ID
Endpoint
Status
Protocol
Topic
5ff5e6ca-1f6b-4116-94bd-...
sharmauday1186@gmail.com
Confirmed
EMAIL
Default_CloudWatch_Alarm...
7041247b-f427-4d55-9cd0...
arn:aws:lambda:us-east-1:0...
Confirmed
LAMBDA
RedshiftSNS
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

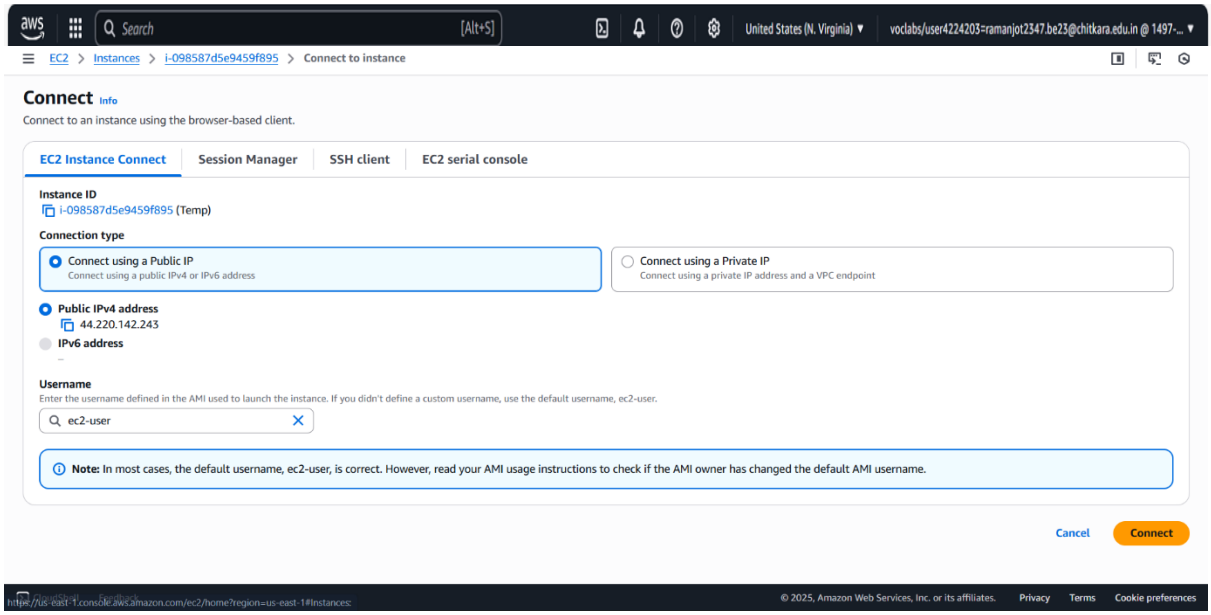

AWS Notification - Subscription
Subscription confirm
sns.us-east-1.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-east-1:000751820144:Default_CloudWatch_Alarms_Topic&Token=2336412f37fb687f5d51e6e2425a8a59700540...
aws
Simple Notification Service
Subscription confirmed!
You have successfully subscribed.
Your subscription's id is:
arn:aws:sns:us-east-1:000751820144:Default_CloudWatch_Alarms_Topic:5ff5e6ca-1f6b-4116-94bd-dcd0858cf662
If it was not your intention to subscribe, click here to unsubscribe.


Search [Alt+S]
United States (N. Virginia)
CloudWatch > Alarms > Create alarm
Alarm recommendations available
Turn on Recommendations to pre-populate the wizard with the recommended alarms.
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add alarm details
Step 4
Preview and create
Add alarm details
Name and description
Alarm name
Alarm1
Alarm description - optional View formatting guidelines
Edit
Preview
This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.
Up to 1024 characters (0/1024)
Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.
Tags - optional Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

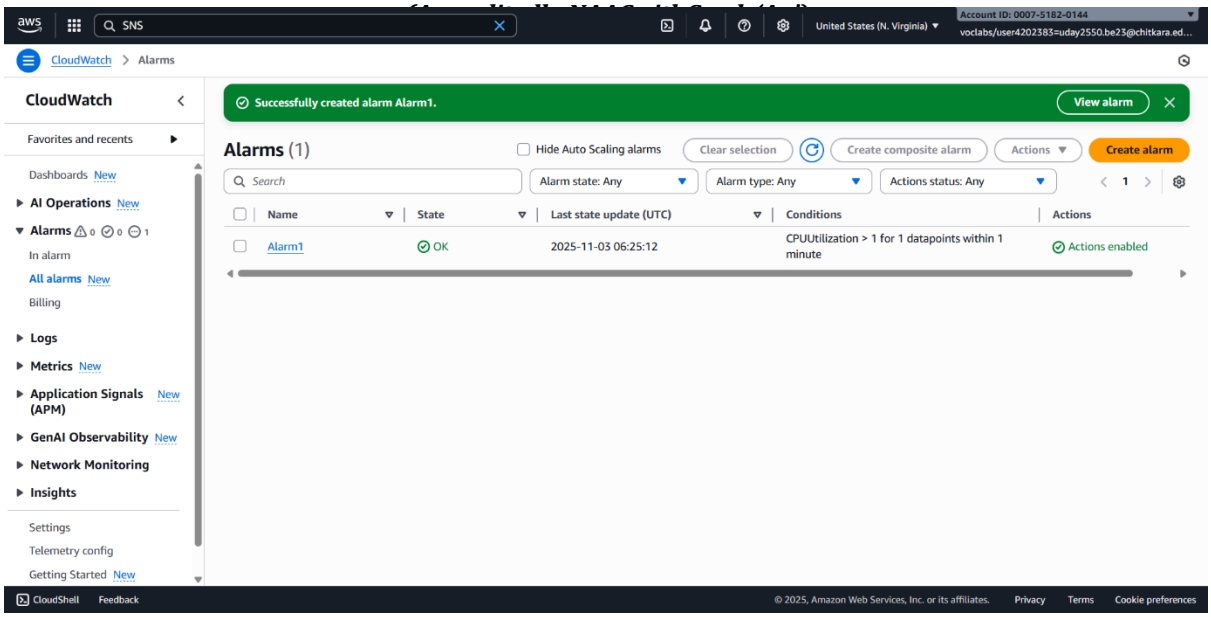

Search [Alt+S]
United States (N. Virginia)
CloudWatch > Alarms > Create alarm
Additional configuration
Step 2: Configure actions
Edit
Actions
Notification
When In alarm, send a notification to "Default_CloudWatch_Alarms_Topic"
Step 3: Add alarm details
Edit
Alarm details
Name
Alarm1
Description
-
Tags (0)
Cancel
Previous
Create alarm
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

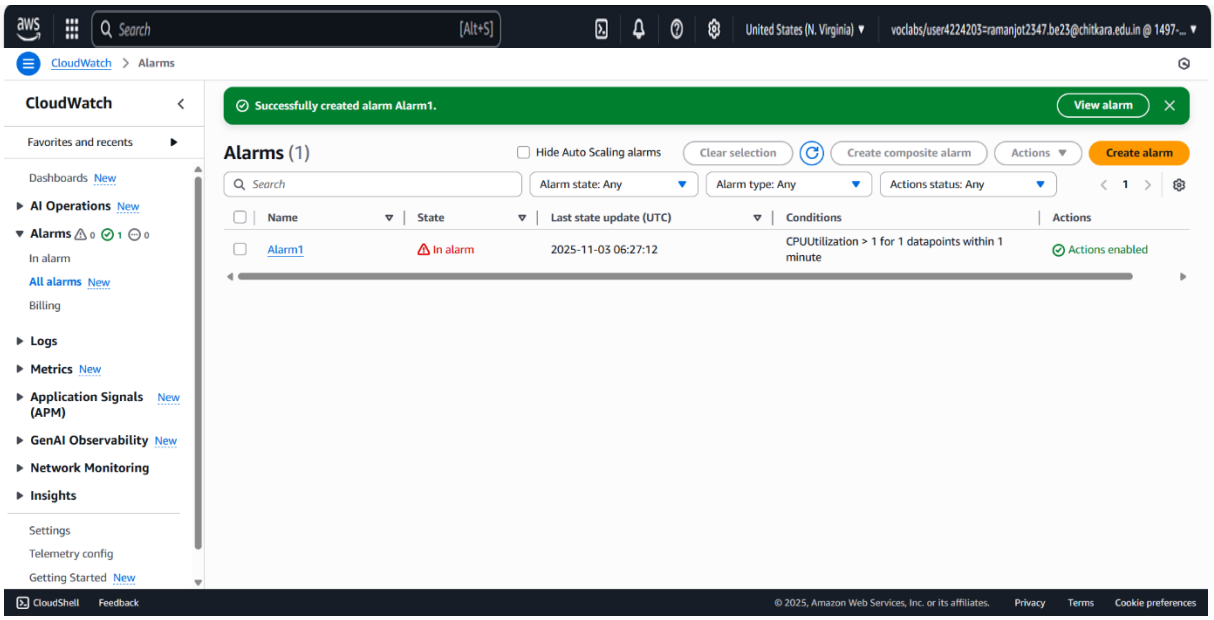

Search [Alt+S]
United States (N. Virginia)

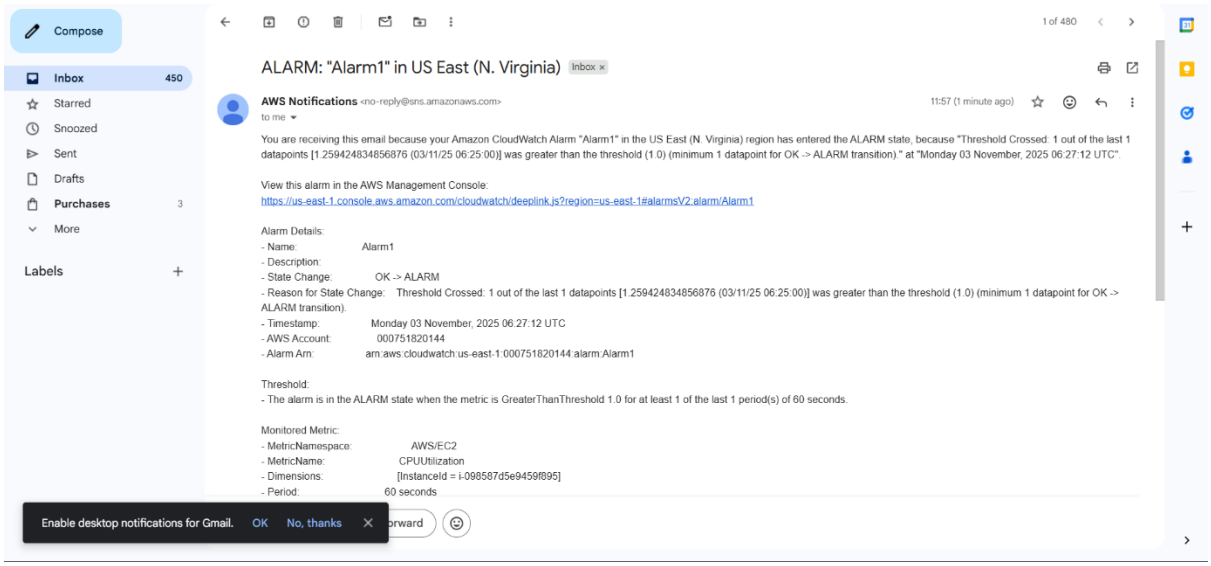

SNS
United States (N. Virginia)
Account ID: 0007-5182-0144
CloudWatch > Alarms
CloudWatch
Successfully created alarm Alarm1.
View alarm
Favorites and recents
Dashboards New
AI Operations New
Alarms
In alarm
All alarms New
Billing
Logs
Metrics New
Application Signals (APM) New
GenAI Observability New
Network Monitoring
Insights
Settings
Telemetry config
Getting Started New
Alarms (1)
Hide Auto Scaling alarms
Clear selection
Create composite alarm
Actions
Create alarm
Search
Alarm state: Any
Alarm type: Any
Actions status: Any
Name
State
Last state update (UTC)
Conditions
Actions
Alarm1
Insufficient data
2025-11-03 06:24:08
CPUUtilization > 1 for 1 datapoints within 1 minute
Actions enabled
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
United States (N. Virginia)
EC2 > Instances > i-098587d5e9459f895 > Connect to instance
Connect Info
Connect to an instance using the browser-based client.
EC2 Instance Connect
Session Manager
SSH client
EC2 serial console
Instance ID
i-098587d5e9459f895 (Temp)
Connection type
Connect using a Public IP
Connect using a public IPv4 or IPv6 address
Connect using a Private IP
Connect using a private IP address and a VPC endpoint
Public IPv4 address
44.220.142.243
IPv6 address
Username
Enter the username defined in the AMI used to launch the instance. If you didn't define a custom username, use the default username, ec2-user.
ec2-user
Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.
Cancel
Connect
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
United States (N. Virginia)


SNS
United States (N. Virginia)
CloudWatch > Alarms
CloudWatch
Successfully created alarm Alarm1.
View alarm
Favorites and recents
Dashboards New
AI Operations New
Alarms
In alarm
All alarms New
Billing
Logs
Metrics New
Application Signals (APM) New
GenAI Observability New
Network Monitoring
Insights
Settings
Telemetry config
Getting Started New
Alarms (1)
Hide Auto Scaling alarms
Clear selection
Create composite alarm
Actions
Create alarm
Search
Alarm state: Any
Alarm type: Any
Actions status: Any
Name
State
Last state update (UTC)
Conditions
Actions
Alarm1
OK
2025-11-03 06:25:12
CPUUtilization > 1 for 1 datapoints within 1 minute
Actions enabled
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
United States (N. Virginia)
CloudWatch > Alarms
CloudWatch
Successfully created alarm Alarm1.
View alarm
Favorites and recents
Dashboards New
AI Operations New
Alarms
In alarm
All alarms New
Billing
Logs
Metrics New
Application Signals (APM) New
GenAI Observability New
Network Monitoring
Insights
Settings
Telemetry config
Getting Started New
Alarms (1)
Hide Auto Scaling alarms
Clear selection
Create composite alarm
Actions
Create alarm
Search
Alarm state: Any
Alarm type: Any
Actions status: Any
Name
State
Last state update (UTC)
Conditions
Actions
Alarm1
In alarm
2025-11-03 06:27:12
CPUUtilization > 1 for 1 datapoints within 1 minute
Actions enabled
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Compose
Inbox 450
Starred
Snoozed
Sent
Drafts
Purchases 3
More
Labels
1 of 480
ALARM: "Alarm1" in US East (N. Virginia)
Inbox ×
AWS Notifications <no-reply@sns.amazonaws.com>
11:57 (1 minute ago)
to me
You are receiving this email because your Amazon CloudWatch Alarm "Alarm1" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [1.259424834856876 (03/11/25 06:25:00)] was greater than the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Monday 03 November, 2025 06:27:12 UTC".
View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/Alarm1
Alarm Details:
- Name: Alarm1
- Description:
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [1.259424834856876 (03/11/25 06:25:00)] was greater than the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Monday 03 November, 2025 06:27:12 UTC
- AWS Account: 000751820144
- Alarm Arn: arn:aws:cloudwatch:us-east-1:000751820144:alarm:Alarm1
Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanThreshold 1.0 for at least 1 of the last 1 period(s) of 60 seconds.
Monitored Metric:
- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-098587d5e9459f895]
- Period: 60 seconds
Enable desktop notifications for Gmail.
OK
No, thanks
orward

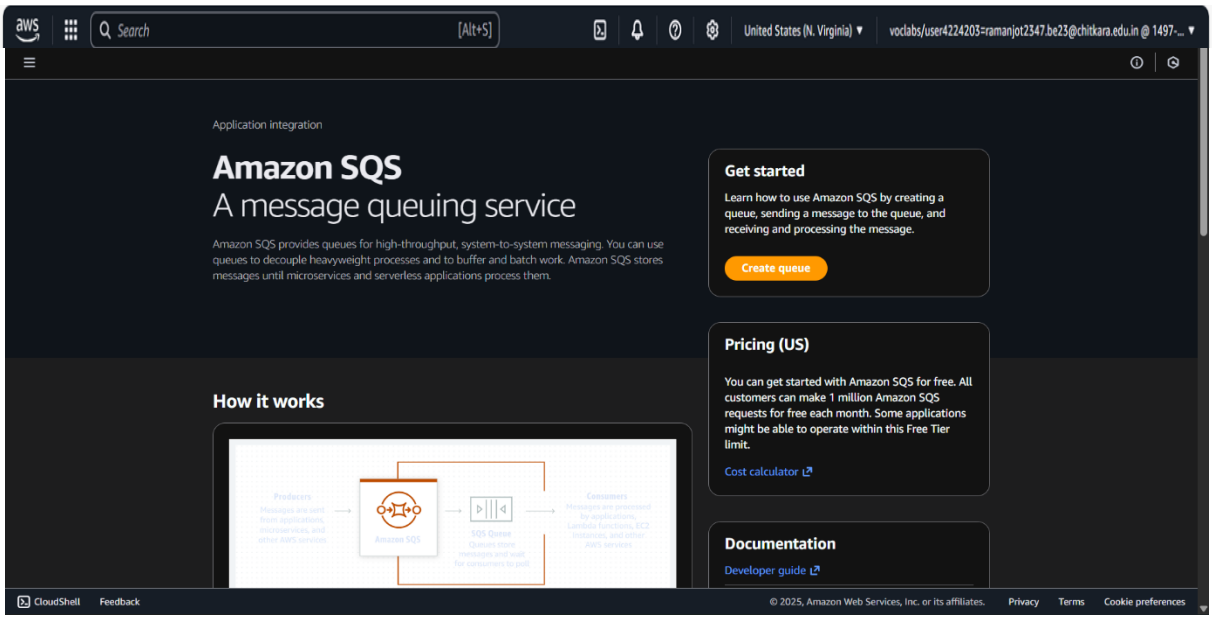
Practical No. 8:

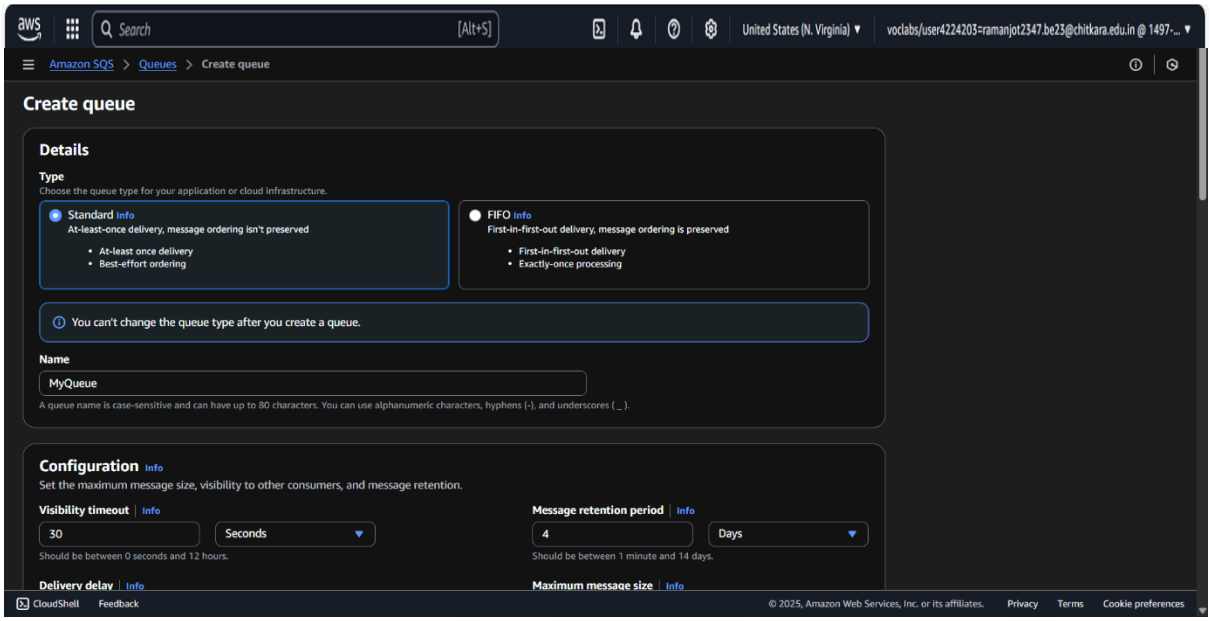
Practical Title: Create an SNS, subscribe and publish a message, set up an SQS queue, integrate it with an EC2 instance, and use SES to send event notifications via email.

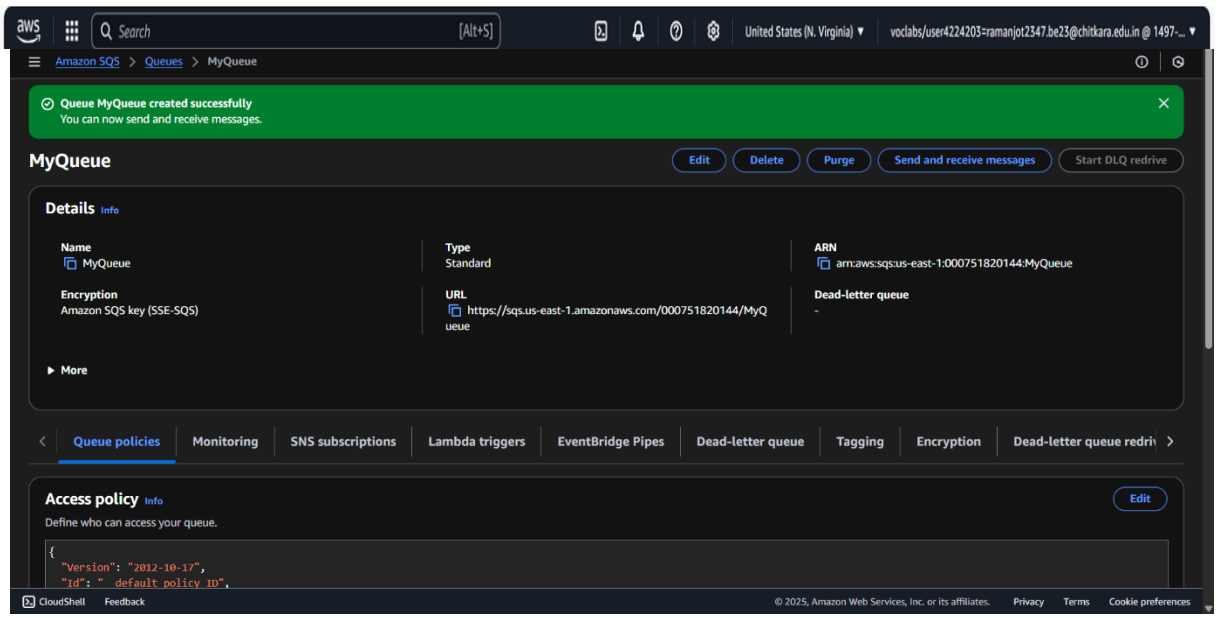
Objective:

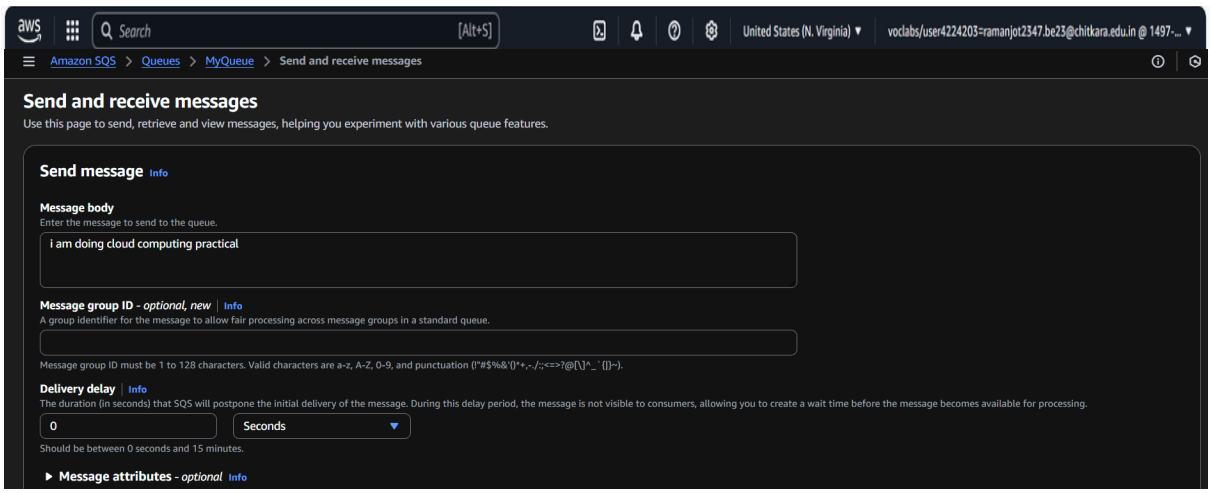
Create an SNS, subscribe and publish a message, set up an SQS queue, integrate it with an EC2 instance, and use SES to send event notifications via email.

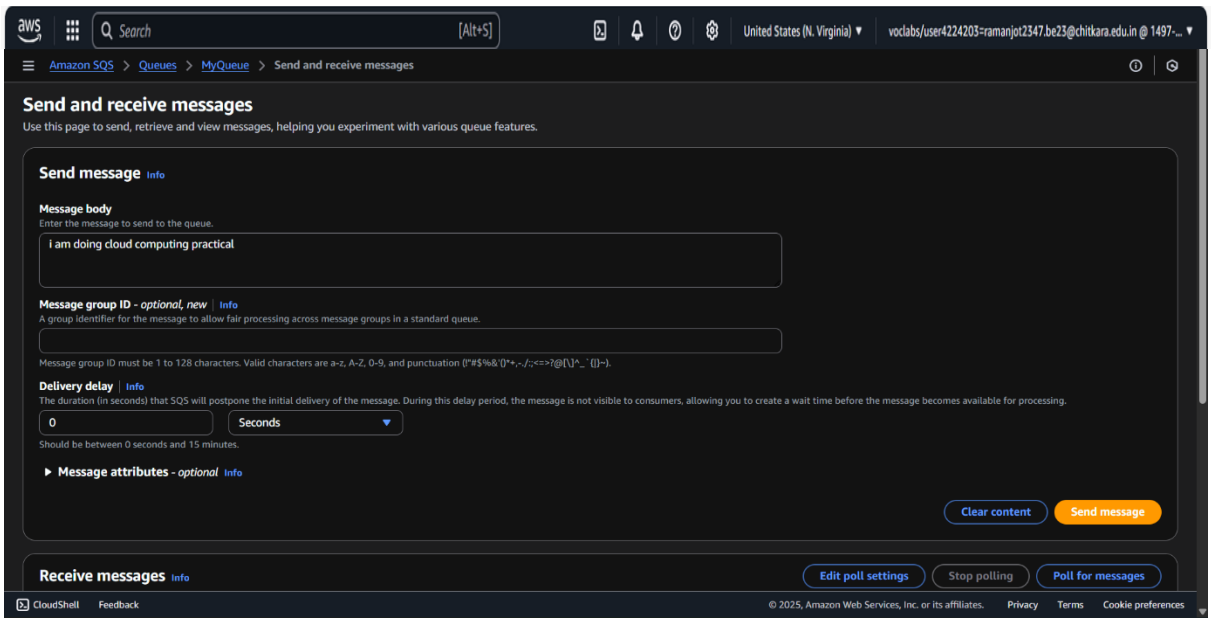
Step-by-Step Procedure with Screenshots:

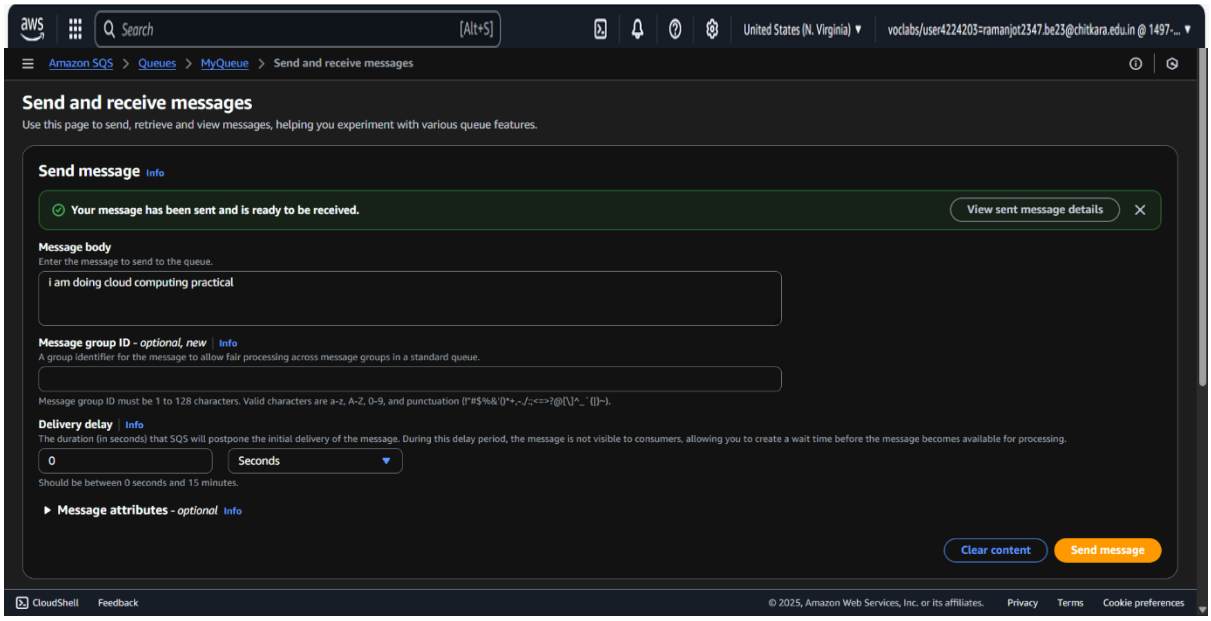


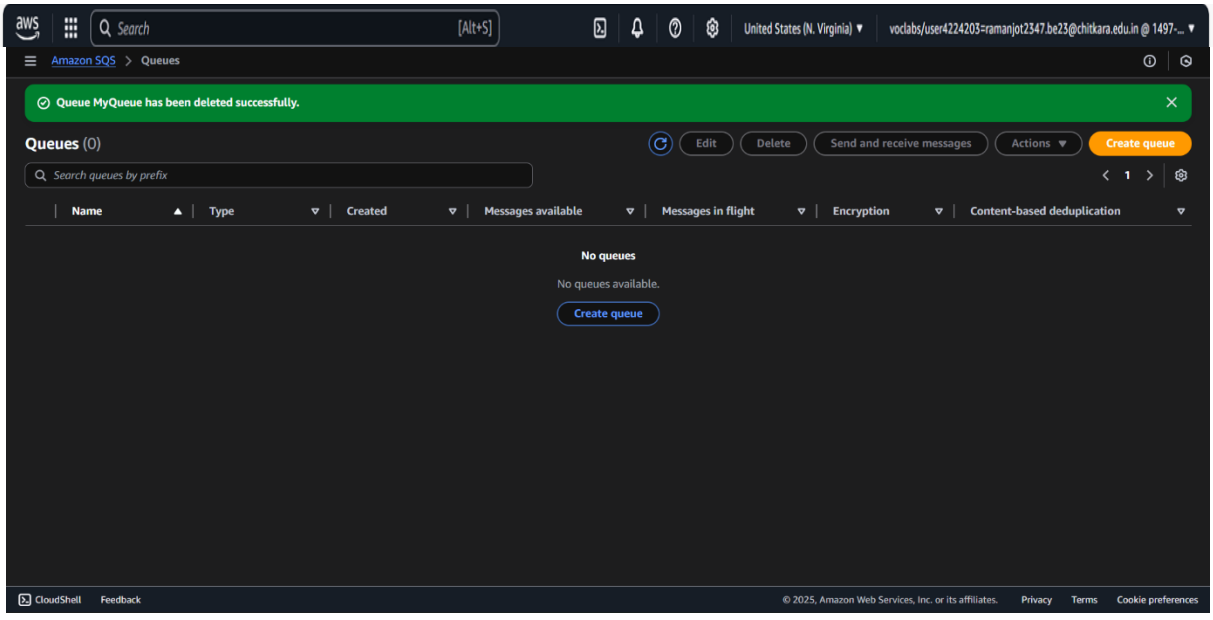

Search
[Alt+S]
United States (N. Virginia)
Amazon SQS > Queues > Create queue
Create queue
Details
Type
Choose the queue type for your application or cloud infrastructure.
Standard Info
At-least-once delivery, message ordering isn't preserved
At-least once delivery
Best-effort ordering
FIFO Info
First-in-first-out delivery, message ordering is preserved
First-in-first-out delivery
Exactly-once processing
You can't change the queue type after you create a queue.
Name
MyQueue
A queue name is case-sensitive and can have up to 80 characters. You can use alphanumeric characters, hyphens (-), and underscores (_).
Configuration Info
Set the maximum message size, visibility to other consumers, and message retention.
Visibility timeout | Info
30
Seconds
Should be between 0 seconds and 12 hours.
Message retention period | Info
4
Days
Should be between 1 minute and 14 days.
Delivery delay | Info
Maximum message size | Info
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
United States (N. Virginia)
Amazon SQS > Queues > MyQueue
Queue MyQueue created successfully
You can now send and receive messages.
MyQueue
Edit
Delete
Purge
Send and receive messages
Start DLQ redrive
Details Info
Name
MyQueue
Type
Standard
ARN
arn:aws:sqs:us-east-1:000751820144:MyQueue
Encryption
Amazon SQS key (SSE-SQS)
URL
https://sqs.us-east-1.amazonaws.com/000751820144/MyQueue
Dead-letter queue
-
More
Queue policies
Monitoring
SNS subscriptions
Lambda triggers
EventBridge Pipes
Dead-letter queue
Tagging
Encryption
Dead-letter queue redri
Access policy Info
Define who can access your queue.
Edit
{
"Version": "2012-10-17",
"id": " default policy ID",
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
United States (N. Virginia)
Amazon SQS > Queues > MyQueue > Send and receive messages
Send and receive messages
Use this page to send, retrieve and view messages, helping you experiment with various queue features.
Send message Info
Message body
Enter the message to send to the queue.
i am doing cloud computing practical
Message group ID - optional, new Info
A group identifier for the message to allow fair processing across message groups in a standard queue.
Message group ID must be 1 to 128 characters. Valid characters are a-z, A-Z, 0-9, and punctuation (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~).
Delivery delay Info
The duration (in seconds) that SQS will postpone the initial delivery of the message. During this delay period, the message is not visible to consumers, allowing you to create a wait time before the message becomes available for processing.
0
Seconds
Should be between 0 seconds and 15 minutes.
Message attributes - optional Info


Search
[Alt+S]
United States (N. Virginia)
Amazon SQS > Queues > MyQueue > Send and receive messages
Send and receive messages
Use this page to send, retrieve and view messages, helping you experiment with various queue features.
Send message Info
Message body
Enter the message to send to the queue.
i am doing cloud computing practical
Message group ID - optional, new Info
A group identifier for the message to allow fair processing across message groups in a standard queue.
Message group ID must be 1 to 128 characters. Valid characters are a-z, A-Z, 0-9, and punctuation (!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~).
Delivery delay Info
The duration (in seconds) that SQS will postpone the initial delivery of the message. During this delay period, the message is not visible to consumers, allowing you to create a wait time before the message becomes available for processing.
0
Seconds
Should be between 0 seconds and 15 minutes.
Message attributes - optional Info
Clear content
Send message
Receive messages Info
Edit poll settings
Stop polling
Poll for messages
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
United States (N. Virginia)
Amazon SQS > Queues > MyQueue > Send and receive messages
Send and receive messages
Use this page to send, retrieve and view messages, helping you experiment with various queue features.
Send message Info
Your message has been sent and is ready to be received.
View sent message details
Message body
Enter the message to send to the queue.
i am doing cloud computing practical
Message group ID - optional, new Info
A group identifier for the message to allow fair processing across message groups in a standard queue.
Delivery delay Info
The duration (in seconds) that SQS will postpone the initial delivery of the message. During this delay period, the message is not visible to consumers, allowing you to create a wait time before the message becomes available for processing.
0
Seconds
Should be between 0 seconds and 15 minutes.
Message attributes - optional Info
Clear content
Send message
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search
[Alt+S]
United States (N. Virginia)
Amazon SQS > Queues
Queue MyQueue has been deleted successfully.
Queues (0)
Edit
Delete
Send and receive messages
Actions
Create queue
Search queues by prefix
Name
Type
Created
Messages available
Messages in flight
Encryption
Content-based deduplication
No queues
No queues available.
Create queue
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences