

**SCOPE**

FALL SEMESTER 2025-2026

# **LAB ASSESSMENT -4**

**Slot:** L13+L14

**Class**: VL2025260105679

**Programme Name & Branch:** B. Tech CSBS

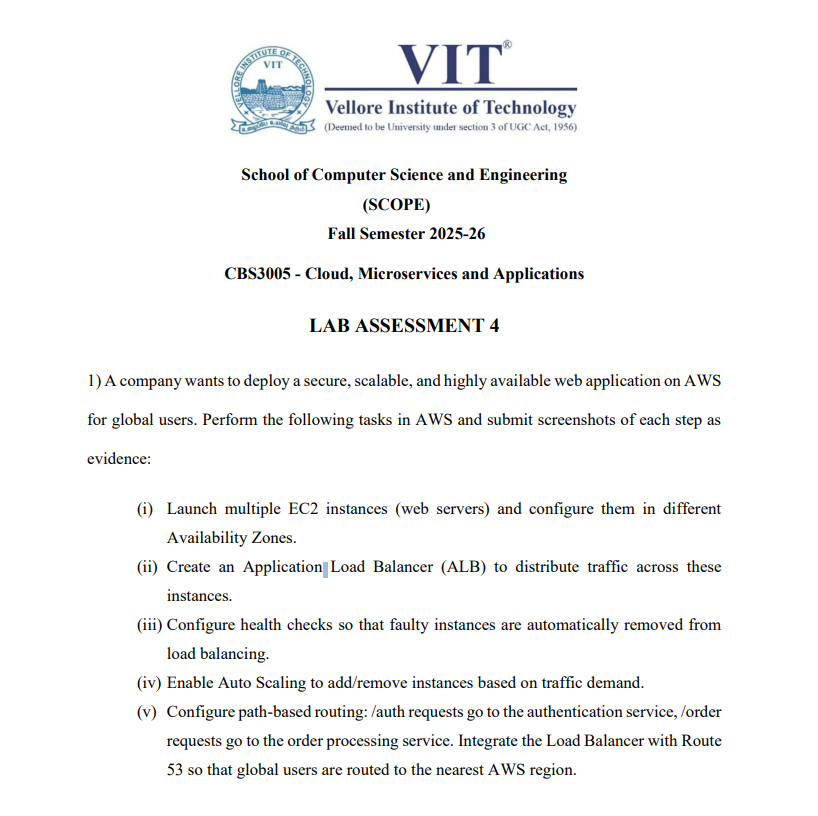
**Course code & Title**: CBS3005- CLOUD, MICROSERVICES AND APPLICATIONS LAB BASED COMPONENTS

**Faculty Name**: NITHYA K

**SUBMITTED BY: -**DIPANGSHU KUNDU

**REGISTRATION NUMBER**: -22BBS0148

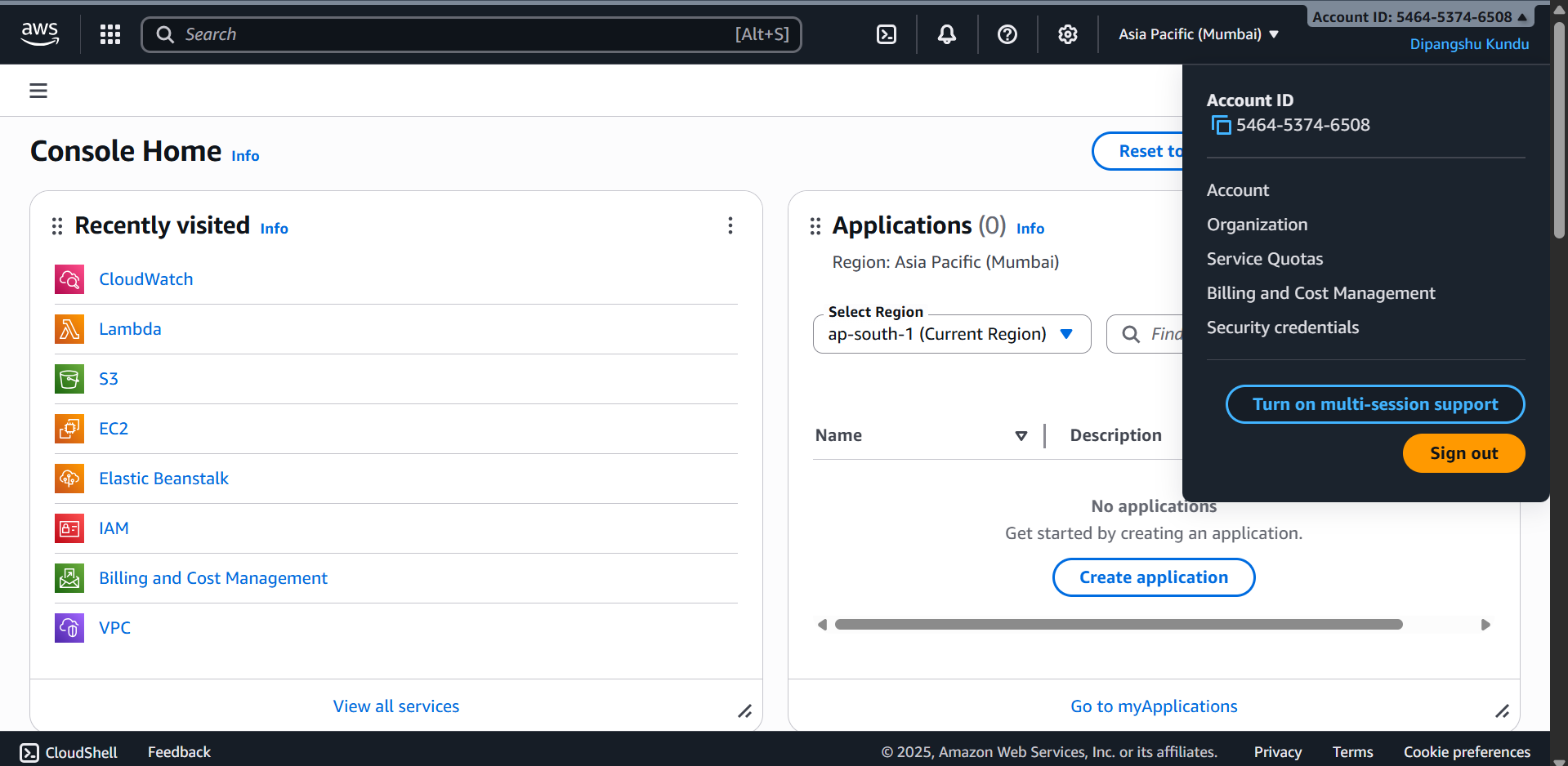
**QUESTION:**

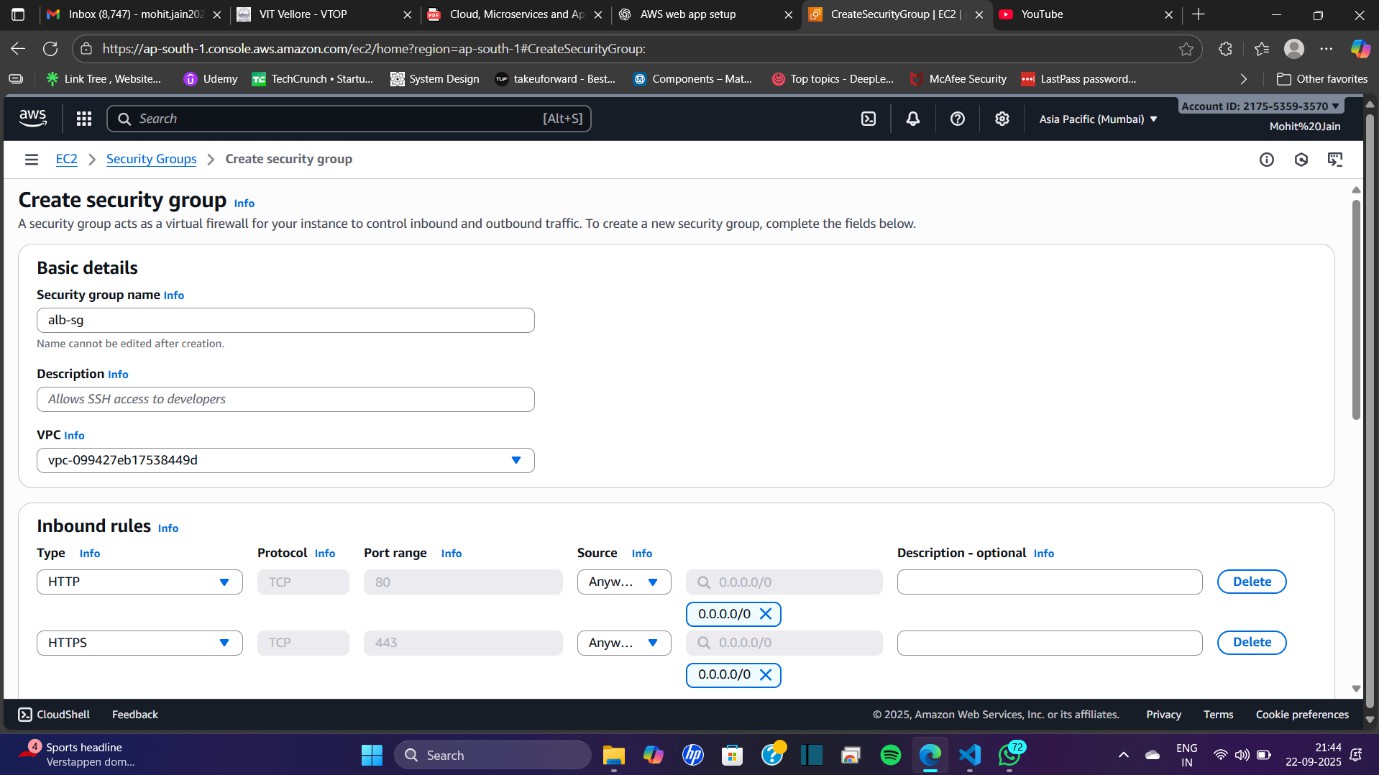
****

**SOLUTION: -**

**Step 1: Create ALB Security Group (in ap-south-1, then repeat in us-east-1)**

1. Go to **AWS Console → Services → EC2 → Network & Security → Security Groups → Create security group**.
2. Enter:
   * **Name tag**: alb-sg
   * **Description**: Allow HTTP/HTTPS from Internet
   * **VPC**: Select **Default VPC** (or your custom VPC).
3. Add **Inbound rules**:
   * HTTP, Port 80, Source 0.0.0.0/0
   * HTTPS, Port 443, Source 0.0.0.0/0 *(optional)*
4. Leave **Outbound rules** as default (allow all).
5. Click **Create security group**.

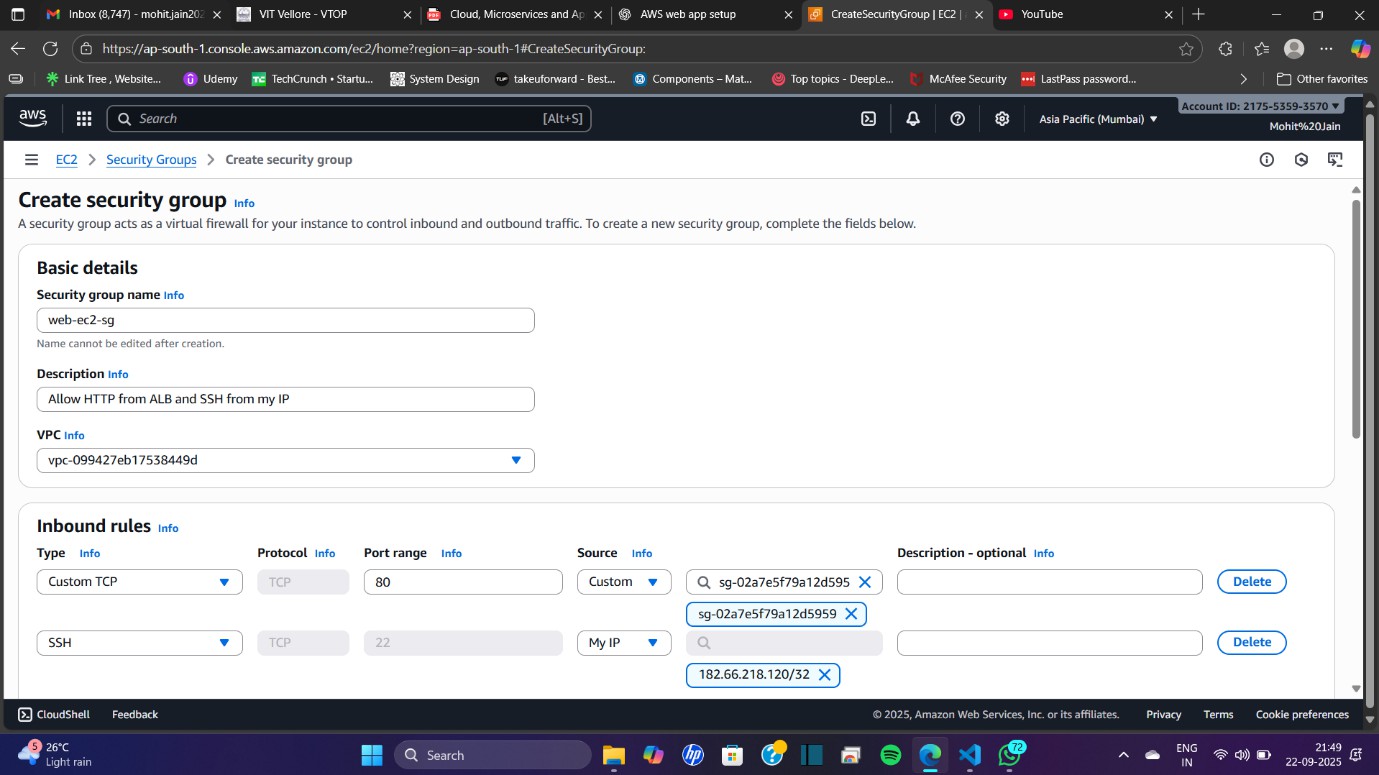


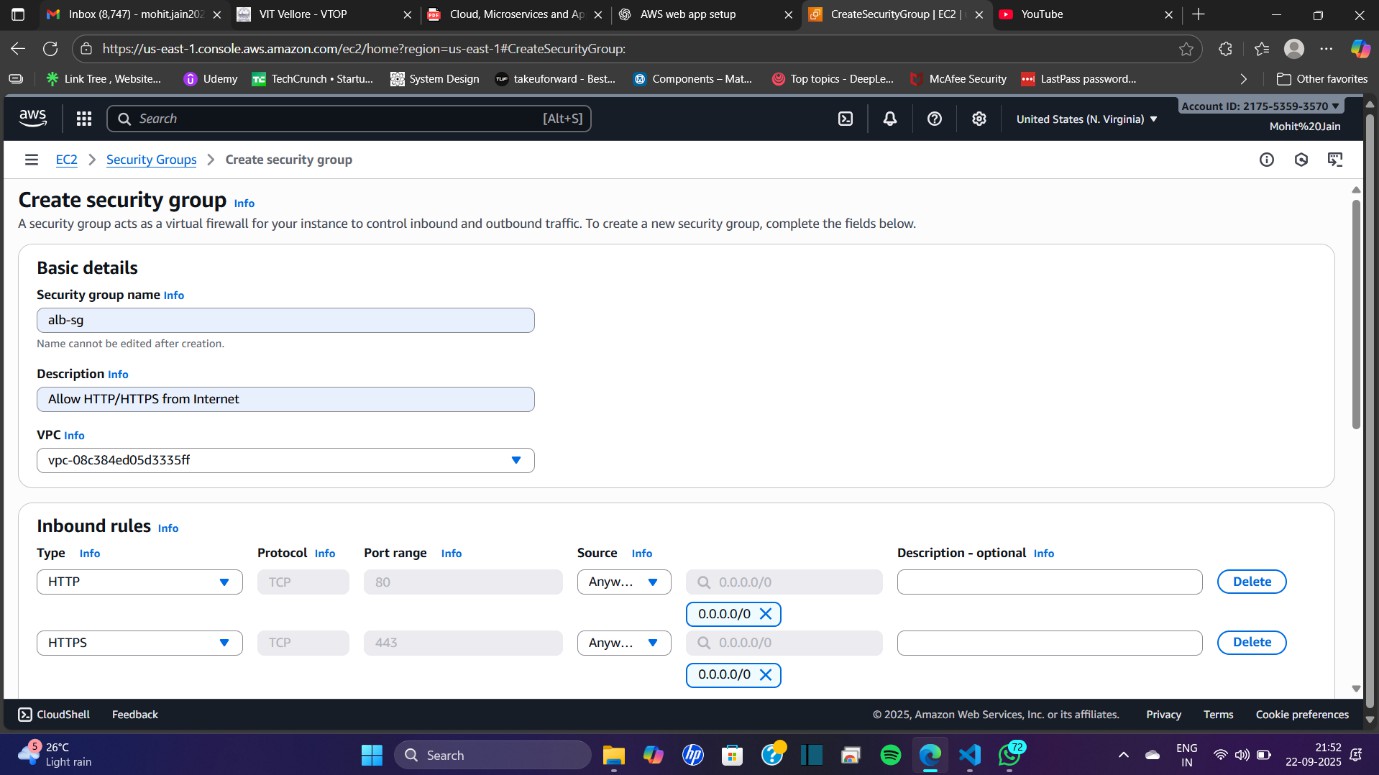


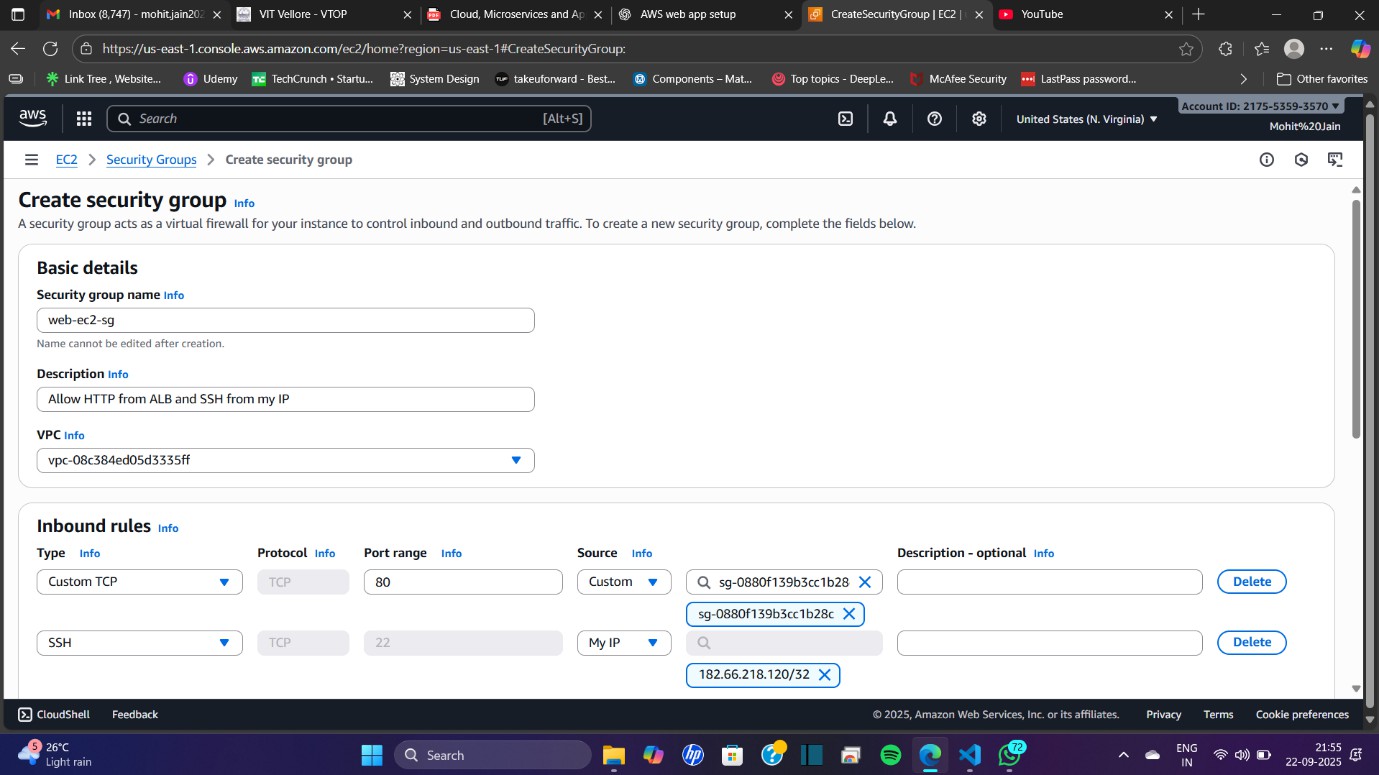


**Step 2: Create EC2 / Web Security Group (in ap-south-1, then repeat in us-east-1)**

1. Click **Create security group** again.
2. Enter:
   * **Name tag**: web-ec2-sg
   * **Description**: Allow HTTP from ALB and SSH from my IP
   * **VPC**: Select the **same VPC** used for the ALB security group.
3. Add **Inbound rules**:
   * **Custom TCP Rule**: Port 80 → Source: **Custom → Security Group → select alb-sg** (this ensures only the ALB can access EC2 on port 80).
   * **SSH**: Port 22 → Source: **My IP** (your public IP, in /32 format).
4. Leave **Outbound rules** as default (allow all).
5. Click **Create security group**.







**Step 3: Launch EC2 Instances (Web Servers)**

In **ap-south-1**, create 4 instances (auth-1, auth-2, order-1, order-2) — each service spread across two Availability Zones (AZ1 & AZ2). Later, repeat in **us-east-1**.

1. Go to **EC2 → Instances → Launch instances**.
2. Configure the first instance:
   * **Name**: auth-1
   * **AMI**: Amazon Linux 2 (HVM)
   * **Instance type**: t3.micro
   * **Key pair**: Select or create (download .pem)
   * **Network settings**:
     + VPC: Default (or your VPC)
     + Subnet: AZ1 (e.g., ap-south-1a)
     + Auto-assign Public IP: Enable
     + Security group: web-ec2-sg

* **User data**:

#!/bin/bash

yum update -y

yum install -y httpd

echo "Auth Service - $(curl -s http://169.254.169.254/latest/meta-data/instance-id)" > /var/www/html/index.html

echo "OK" > /var/www/html/health

systemctl enable httpd

systemctl start httpd

* Click **Launch instance**.

1. Launch auth-2 the same way, but choose a **different subnet** (AZ2, e.g., ap-south-1b) and change the **Name** to auth-2.
2. Launch order-1 and order-2 in the same way, but change the **Name** and **User data**:

#!/bin/bash

yum update -y

yum install -y httpd

echo "Order Service - $(curl -s http://169.254.169.254/latest/meta-data/instance-id)" > /var/www/html/index.html

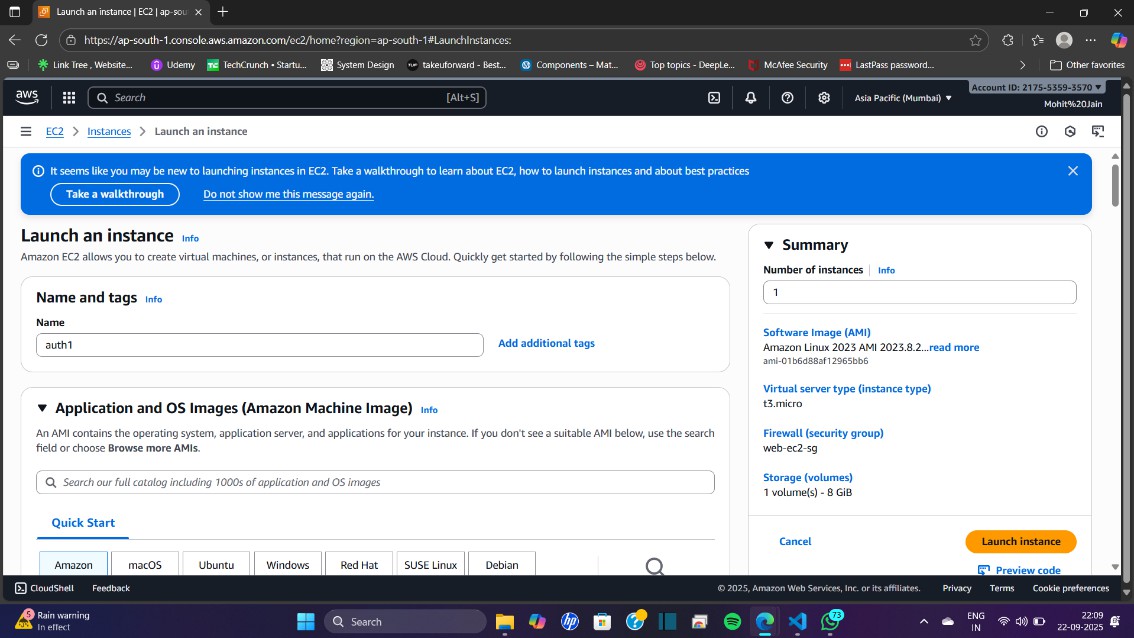
echo "OK" > /var/www/html/health

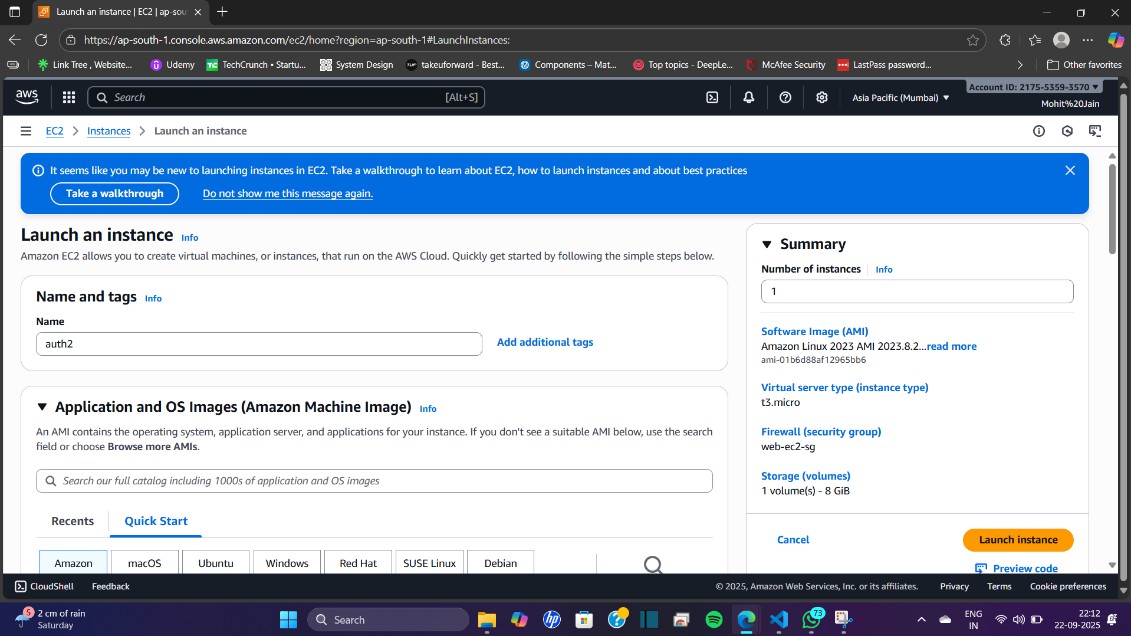
systemctl enable httpd

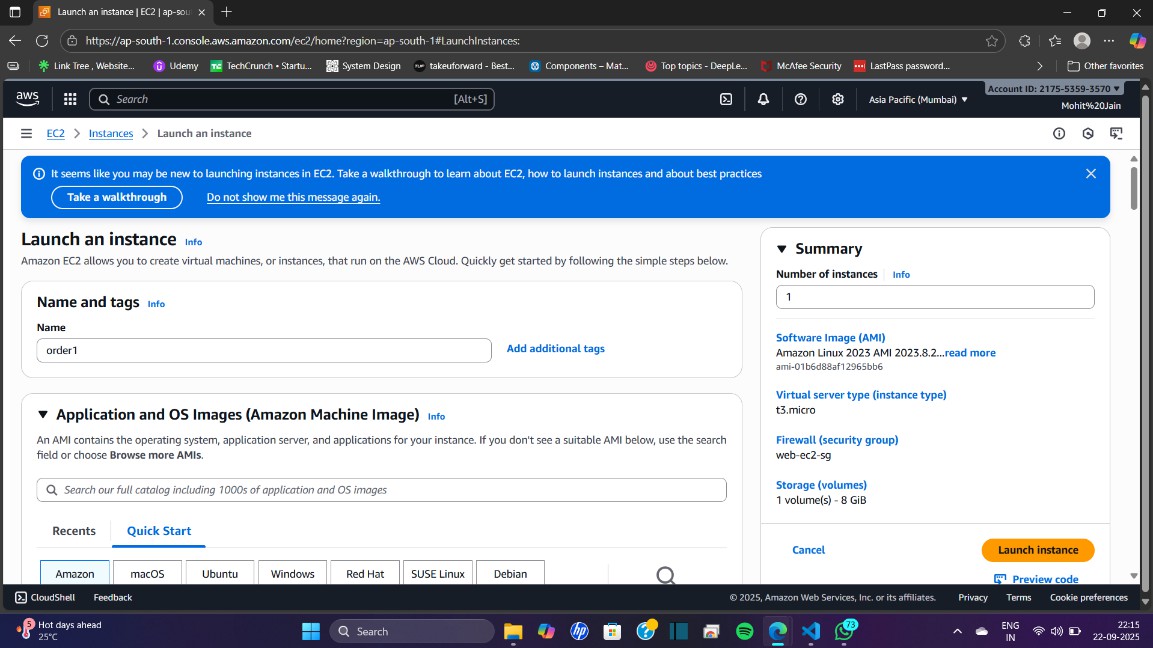
systemctl start httpd

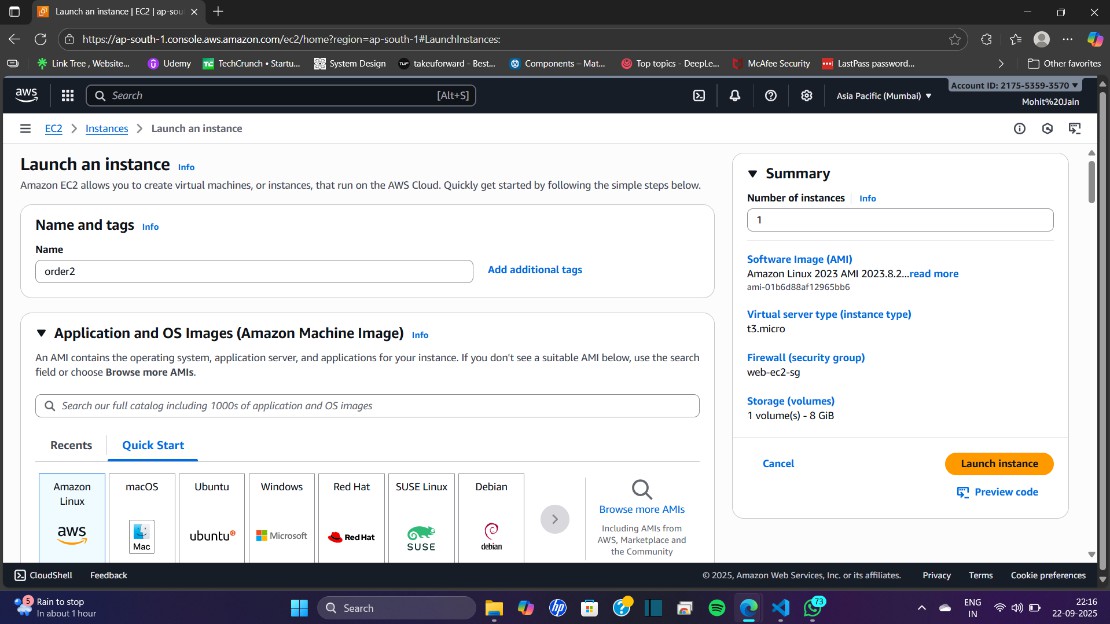
* order-1: AZ1 (e.g., ap-south-1a)
* order-2: AZ2 (e.g., ap-south-1b)

1. Confirm all four instances (auth-1, auth-2, order-1, order-2) are running in **different AZs** and note their private/public IPs.
2. Repeat the same process in **us-east-1** with consistent naming (e.g., us-auth-1, us-auth-2, us-order-1, us-order-2).







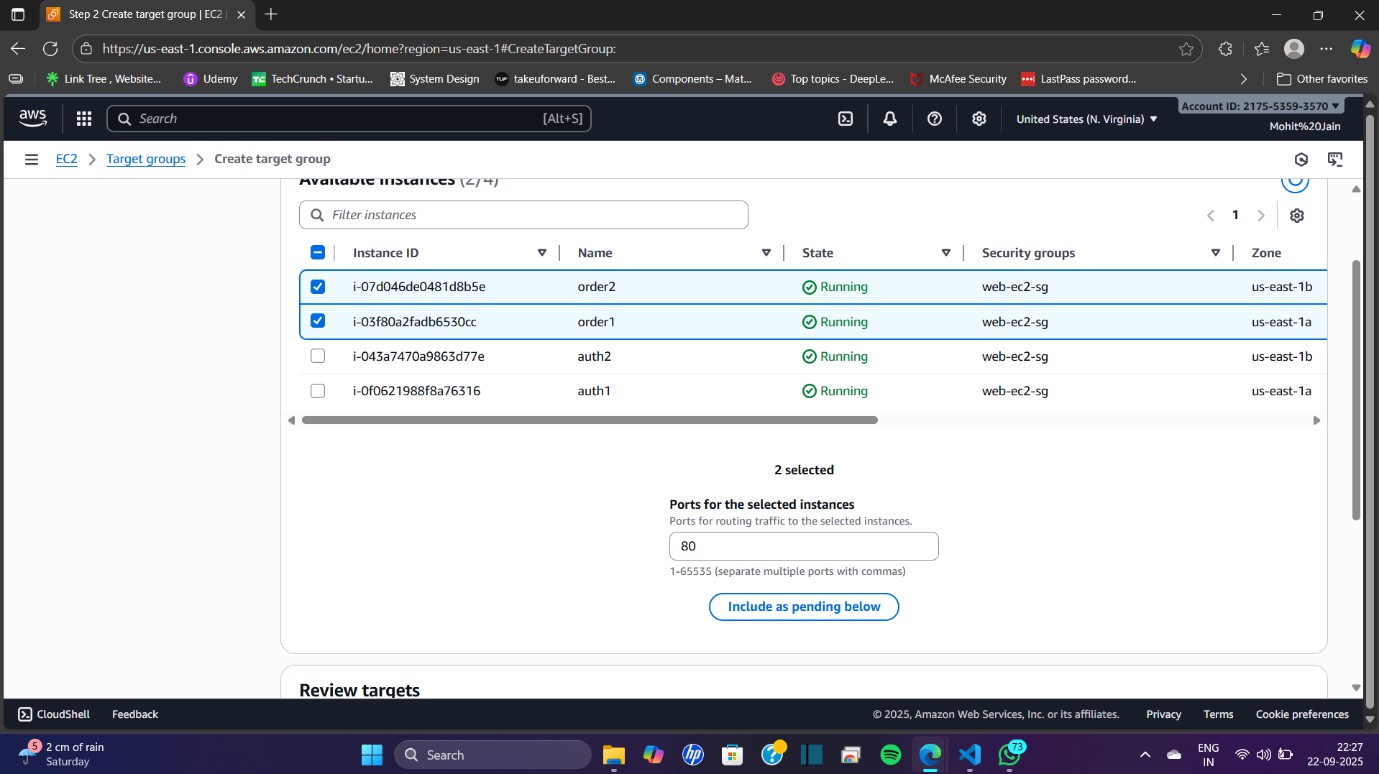


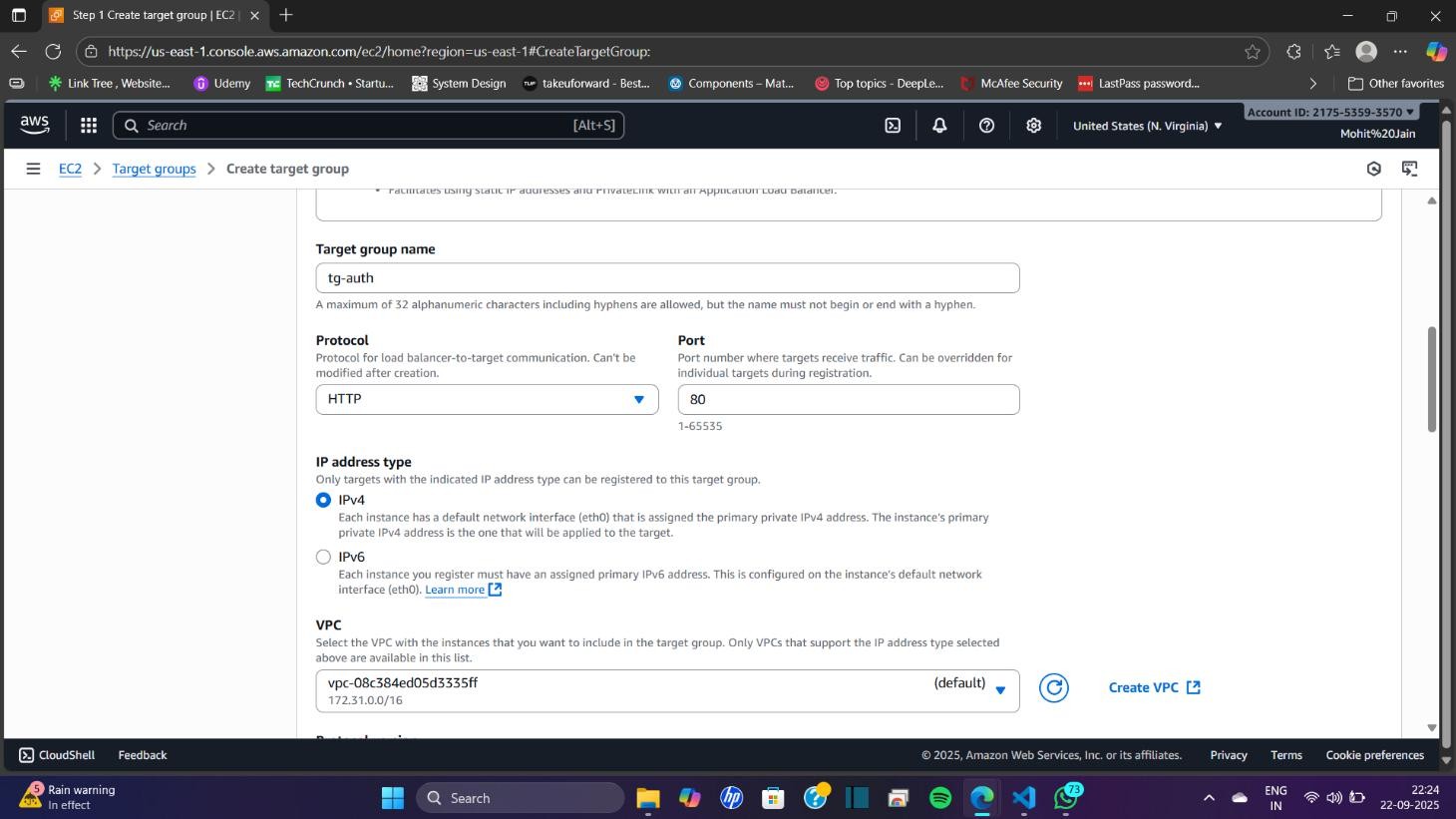
**Step 4: Create Target Groups (per region, per service)**

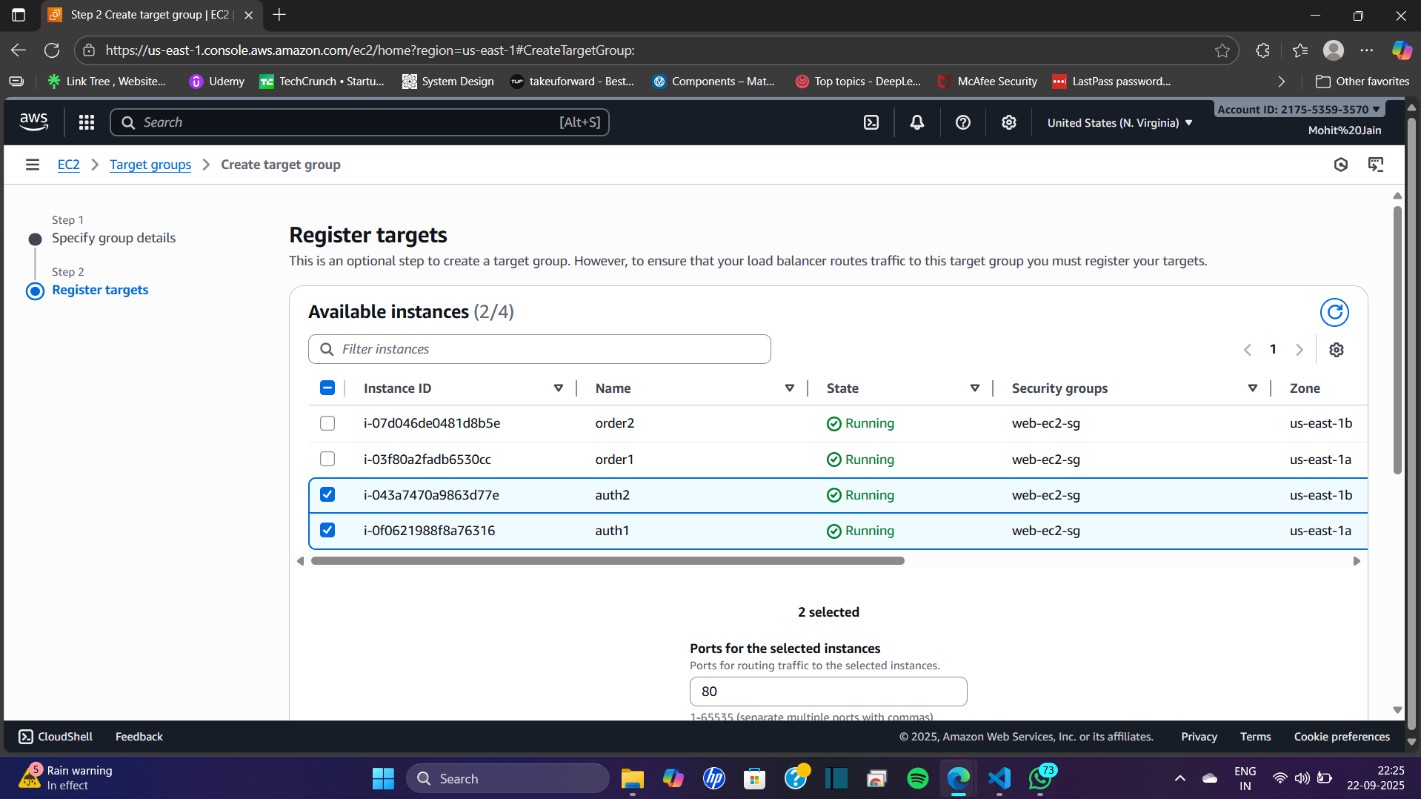
In each region, create two target groups: **tg-auth** and **tg-order**.

1. Go to **EC2 → Load Balancing → Target Groups → Create target group**.
2. Configure the first target group:
   * **Target type**: Instance
   * **Protocol**: HTTP
   * **Port**: 80
   * **VPC**: Select your VPC
   * **Name**: tg-auth
3. Configure **Health checks**:
   * Protocol: HTTP
   * Path: /health
   * Success codes: 200
   * Interval: 30s
   * Healthy threshold: 3
   * Unhealthy threshold: 3
4. Click **Create target group**.
5. After creation, go to the **Targets** tab → **Register targets** → select **auth-1** and **auth-2** → Port 80 → **Register**.
6. Repeat the same process to create **tg-order**, then register **order-1** and **order-2**.









**Step 5: Create Application Load Balancer (ALB) and Configure Path-Based Routing**

Create **1 ALB per region** and set up path-based listener rules.

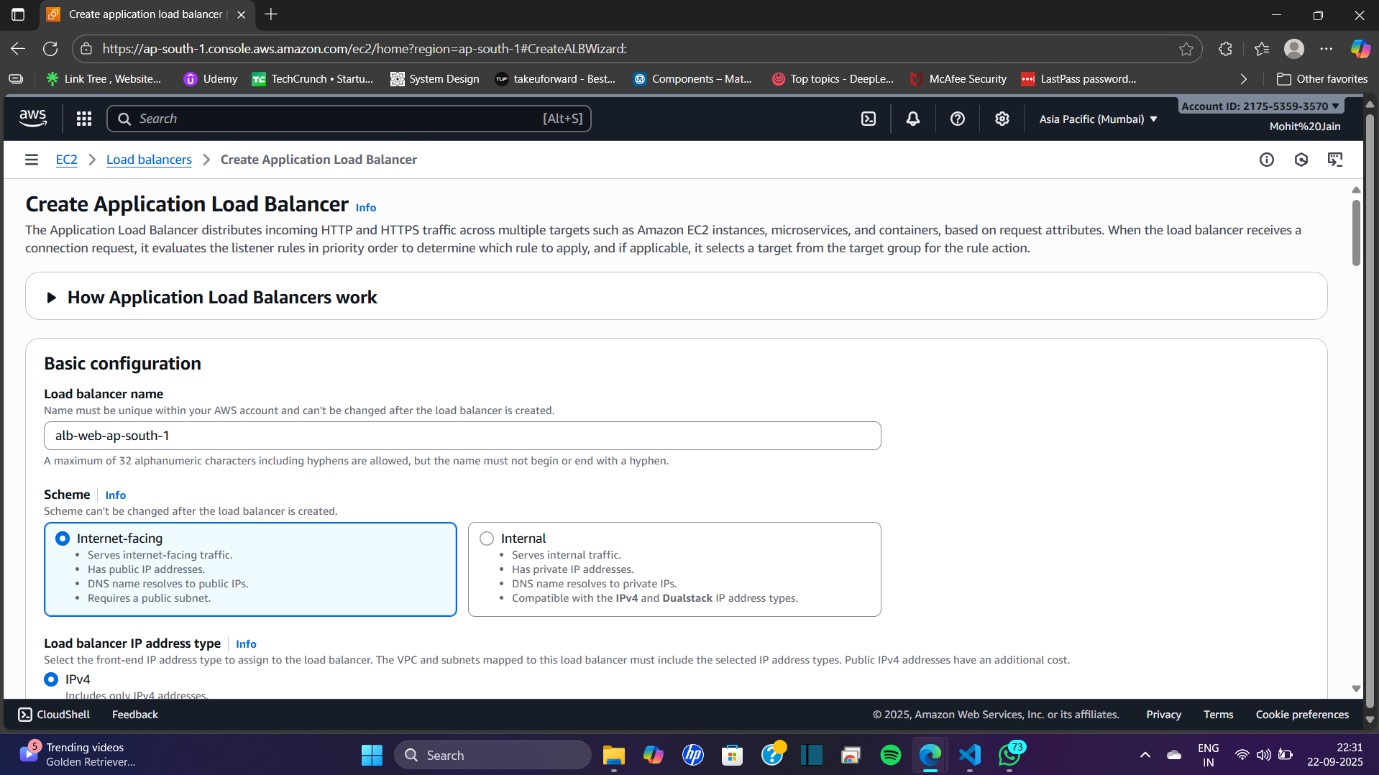
1. Go to **EC2 → Load Balancers → Create Load Balancer → Application Load Balancer**.
2. **Basic configuration**:
   * Name: alb-web-ap-south-1 (for Mumbai region; adjust name per region).
   * Scheme: Internet-facing.
   * IP address type: IPv4.
3. **Listeners**:
   * Add HTTP : 80 (optionally add HTTPS : 443 later if certificates are available).
4. **Availability Zones**:
   * VPC: Default (or your VPC).
   * Select at least **2 subnets** (one per AZ) so ALB spans multiple AZs.
5. **Security group**: Select **alb-sg**.
6. **Configure routing**:
   * Default target group: Select tg-auth (or create a tg-default if you prefer a dummy).
7. Click **Create load balancer** and wait until it is provisioned.

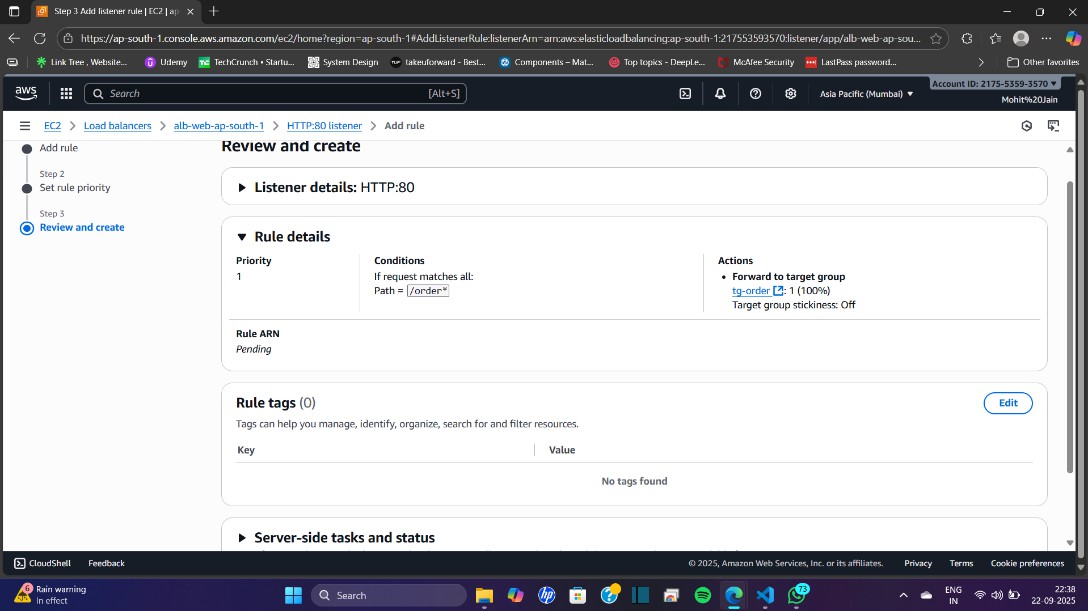
**A. Configure Listener Rules (Path-Based Routing)**

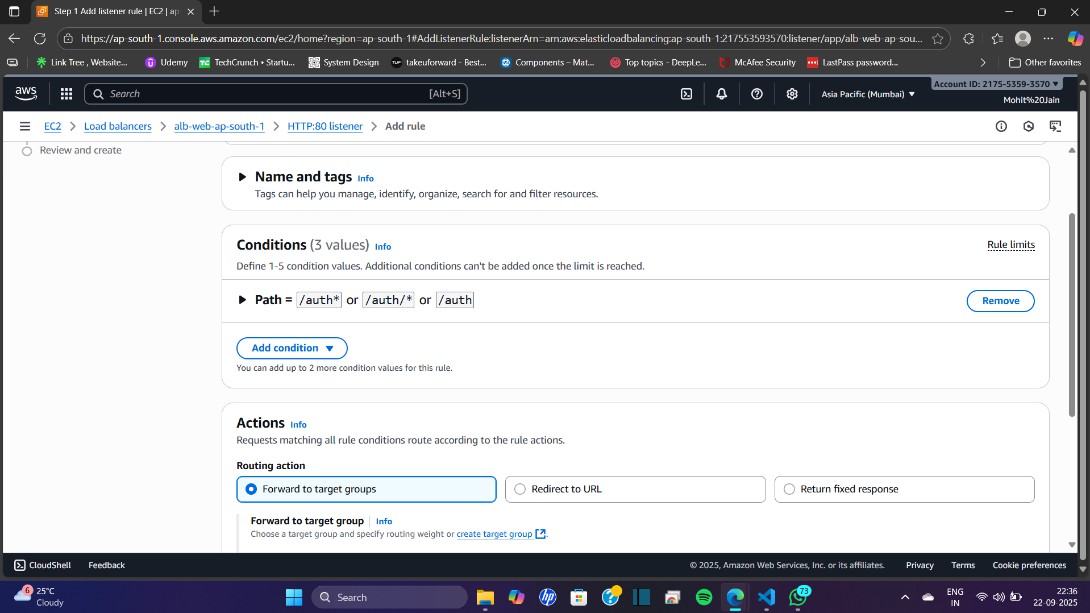
1. In the **Load Balancers list**, select **alb-web-ap-south-1** → go to **Listeners** tab → choose **HTTP:80** listener → click **View/edit rules**.
2. Add rules before the default:
   * Rule 1:
     + Condition: Path is /auth\*
     + Action: Forward to **tg-auth**
   * Rule 2:
     + Condition: Path is /order\*
     + Action: Forward to **tg-order**
3. Save rules. Ensure the **default rule** points to some target group (e.g., tg-auth or tg-default) or returns 404.

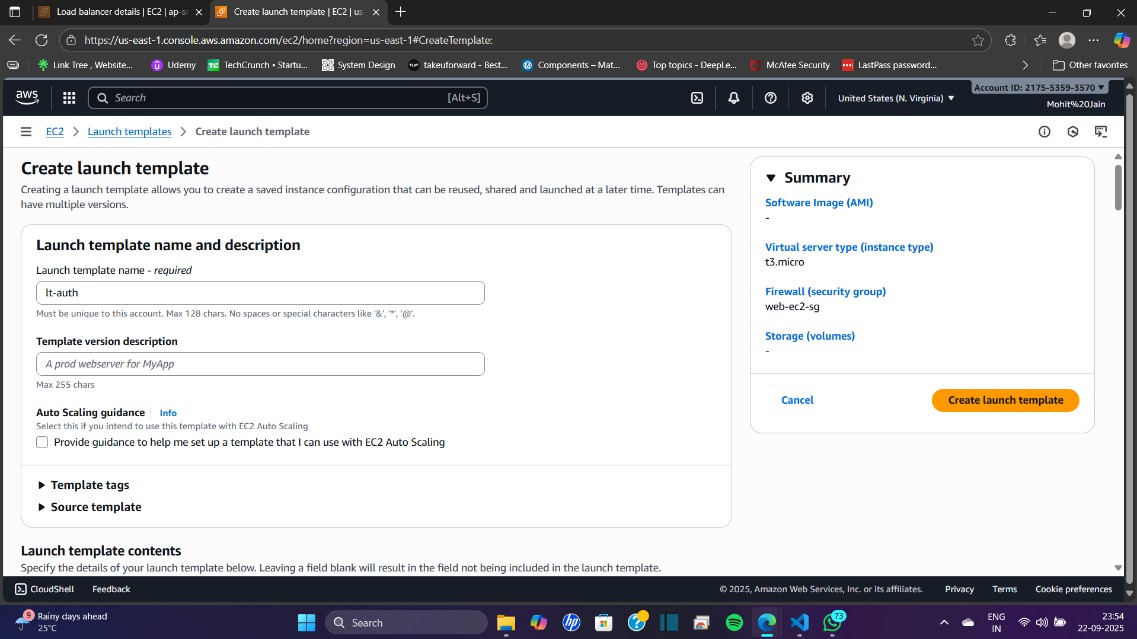
**B. Verify ALB and Target Health**

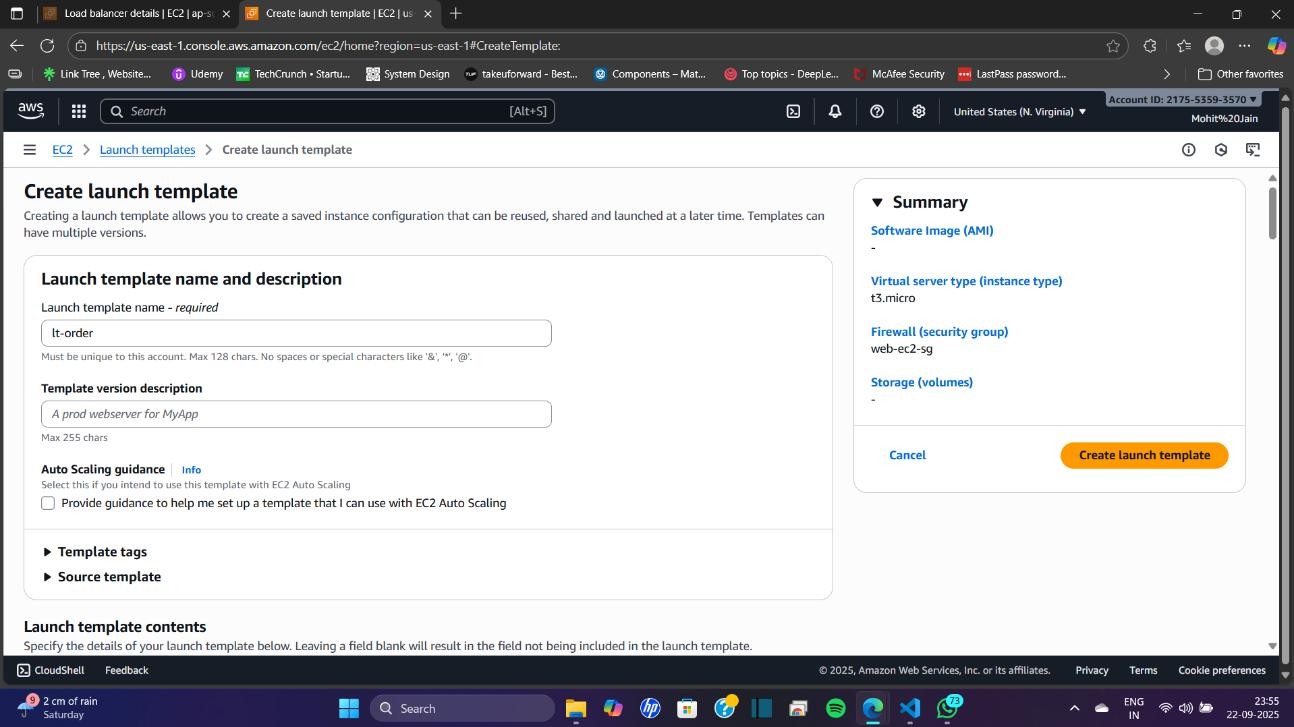
1. Go to **Load Balancers → select ALB → Target groups tab**.
2. Select tg-auth → **Targets** → confirm targets (auth-1, auth-2) show as **healthy**.
3. Repeat for tg-order.
4. If unhealthy, check the EC2 instance **user-data** and confirm the /health endpoint works.











**Step 6: Configure Auto Scaling (per region, per service) — GUI Only**

We’ll create **Launch Templates** and **Auto Scaling Groups (ASGs)** for each service. The ASGs will attach to the ALB target groups and automatically register/deregister instances.

**A. Create Launch Templates**

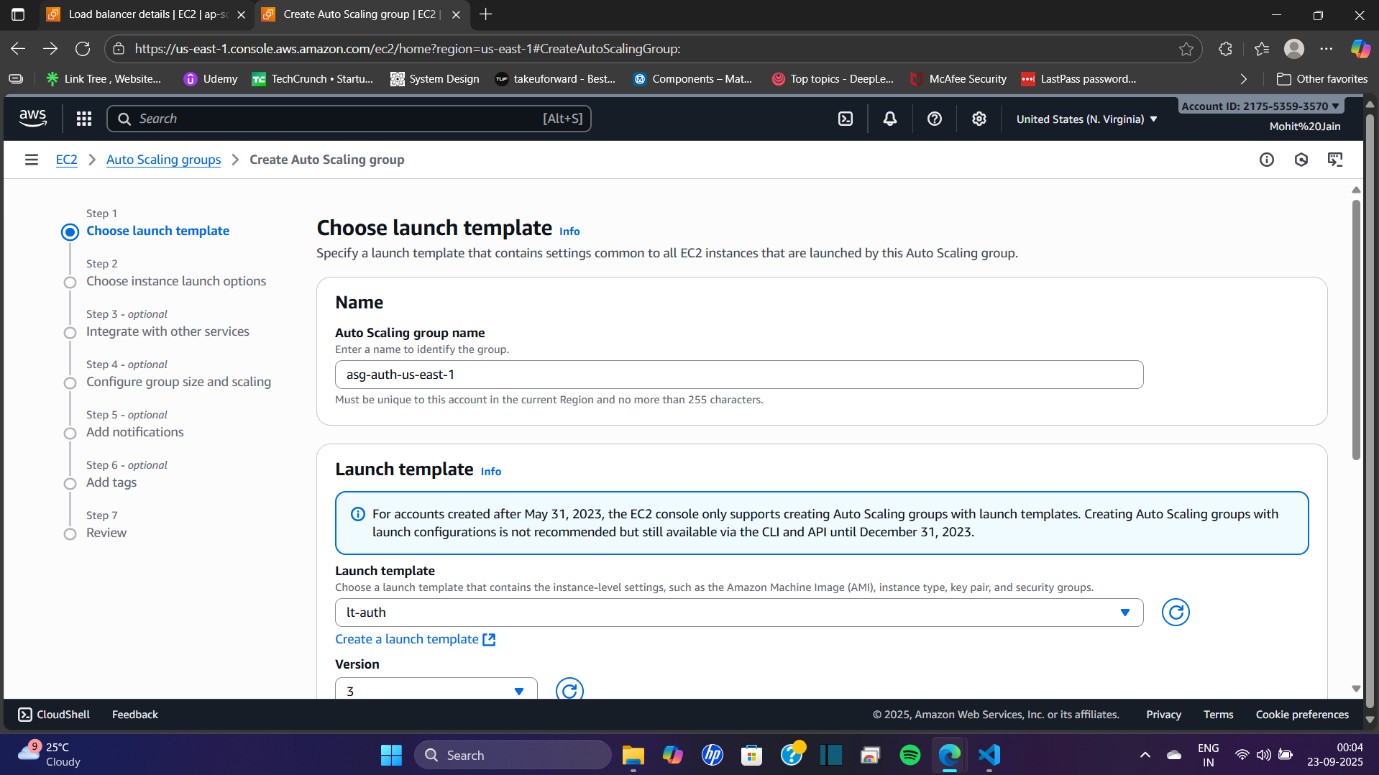
1. Go to **EC2 → Launch Templates → Create launch template**.
2. Configure:
   * **Name**: lt-auth (for the auth service).
   * **AMI**: Amazon Linux 2.
   * **Instance type**: t3.micro.
   * **Key pair**: Same as used earlier.
   * **Network settings**: Leave blank (ASG will assign subnets).
   * **Security group**: web-ec2-sg.
   * **Advanced user data**: Use the same startup script from the manual auth instances (so they serve /health).
3. Click **Create launch template**.
4. Repeat to create **lt-order** (with the order service user-data).

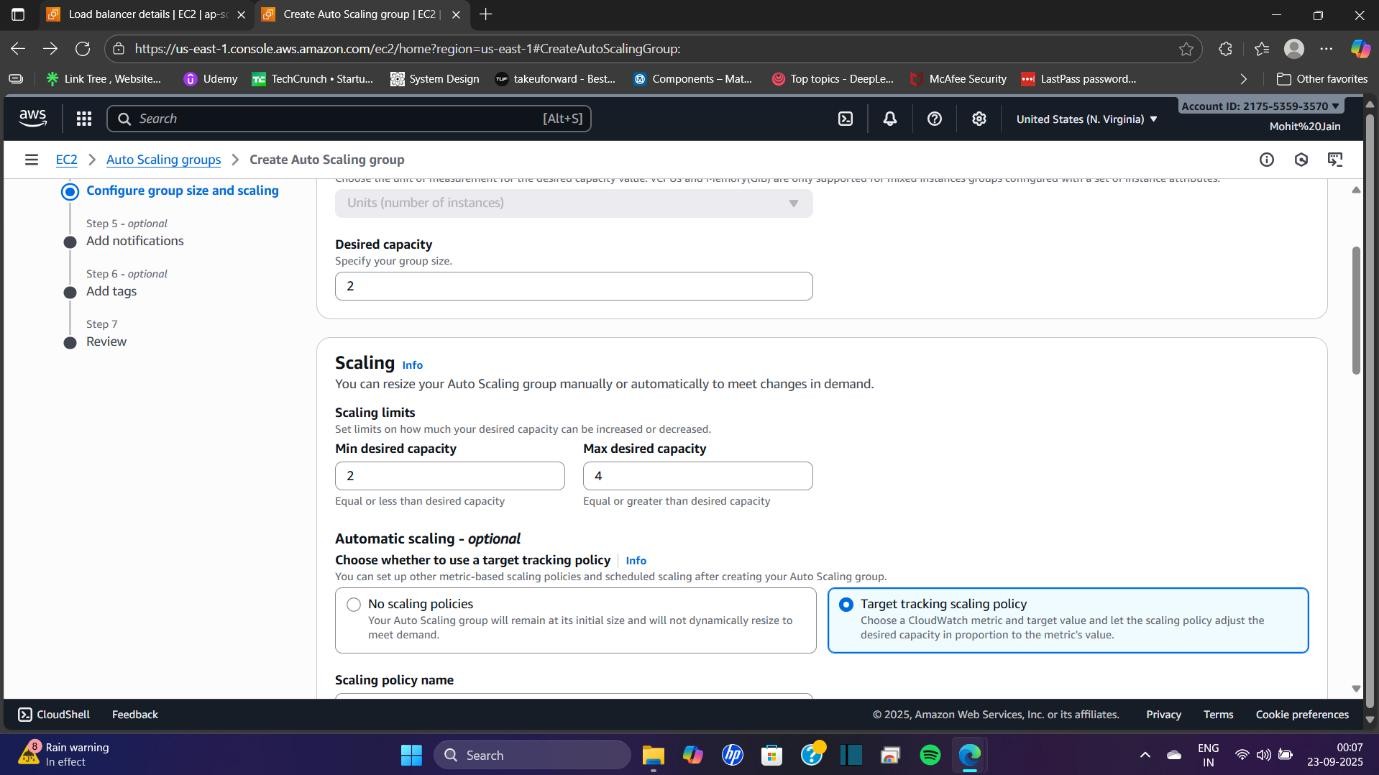
**B. Create Auto Scaling Groups**

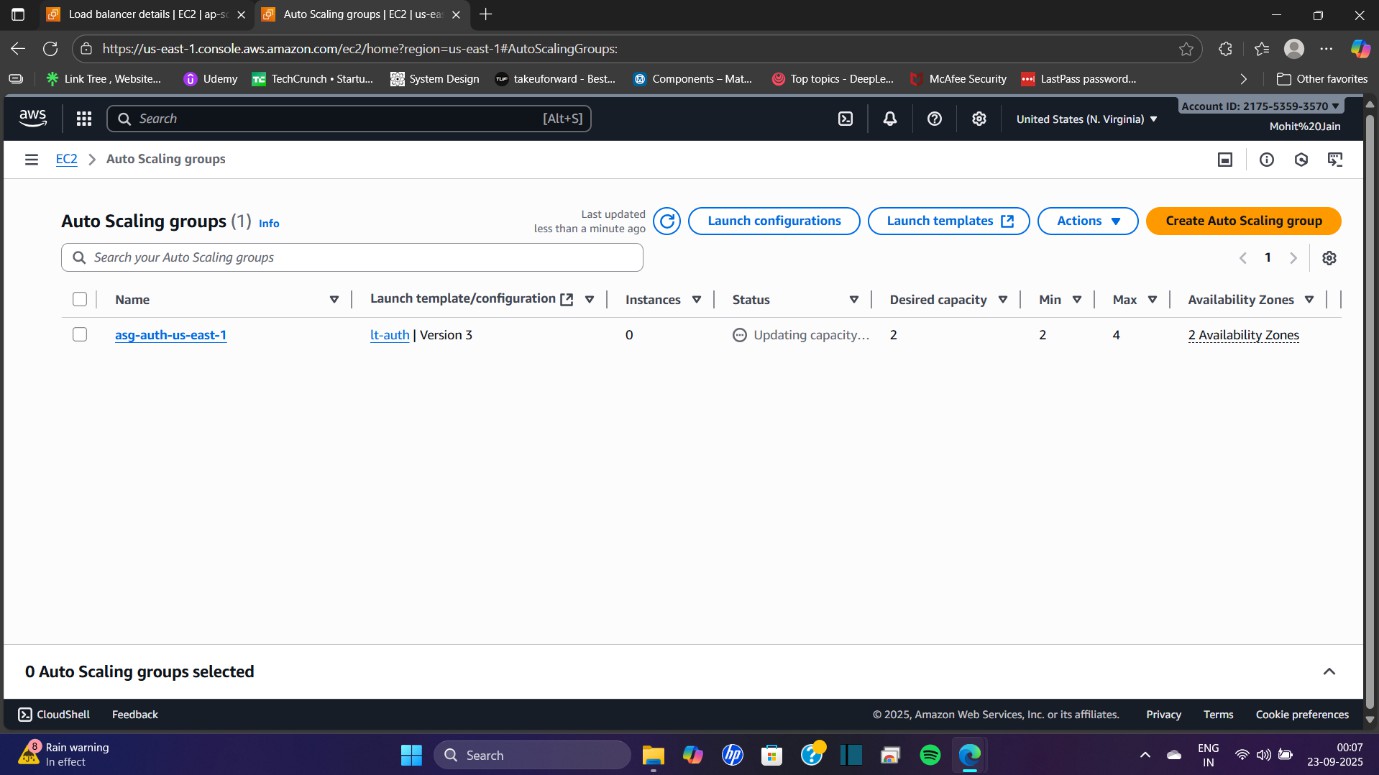
1. Go to **EC2 → Auto Scaling Groups → Create Auto Scaling group**.
2. Select the **launch template** (lt-auth).
3. **ASG name**: asg-auth-ap-south-1.
4. Select **VPC** and choose **two subnets** (AZ1 + AZ2).
5. **Attach to load balancer**:
   * Choose **Attach to an existing load balancer** → select **alb-web-ap-south-1**.
   * Target group: **tg-auth**.
6. **Set group size**:
   * Minimum: 2
   * Desired: 2
   * Maximum: 4
7. **Scaling policies**:
   * Choose **Target tracking** (e.g., Average CPU utilization target = 50%).
   * Or use **ALB request count per target** (e.g., 50 requests per instance).
8. Review and click **Create Auto Scaling group**.
9. Repeat the same process to create **asg-order-ap-south-1** using **lt-order** and attach to **tg-order**.

**C. Verify Auto Scaling**

1. Go to **Auto Scaling Groups → select an ASG → Instances tab**.
2. Confirm new EC2 instances are launched automatically (names generated by ASG).
3. Verify these instances appear as **healthy** in their associated target groups.







**Step 7: Configure Route 53 for Global DNS (Latency-Based Routing)**

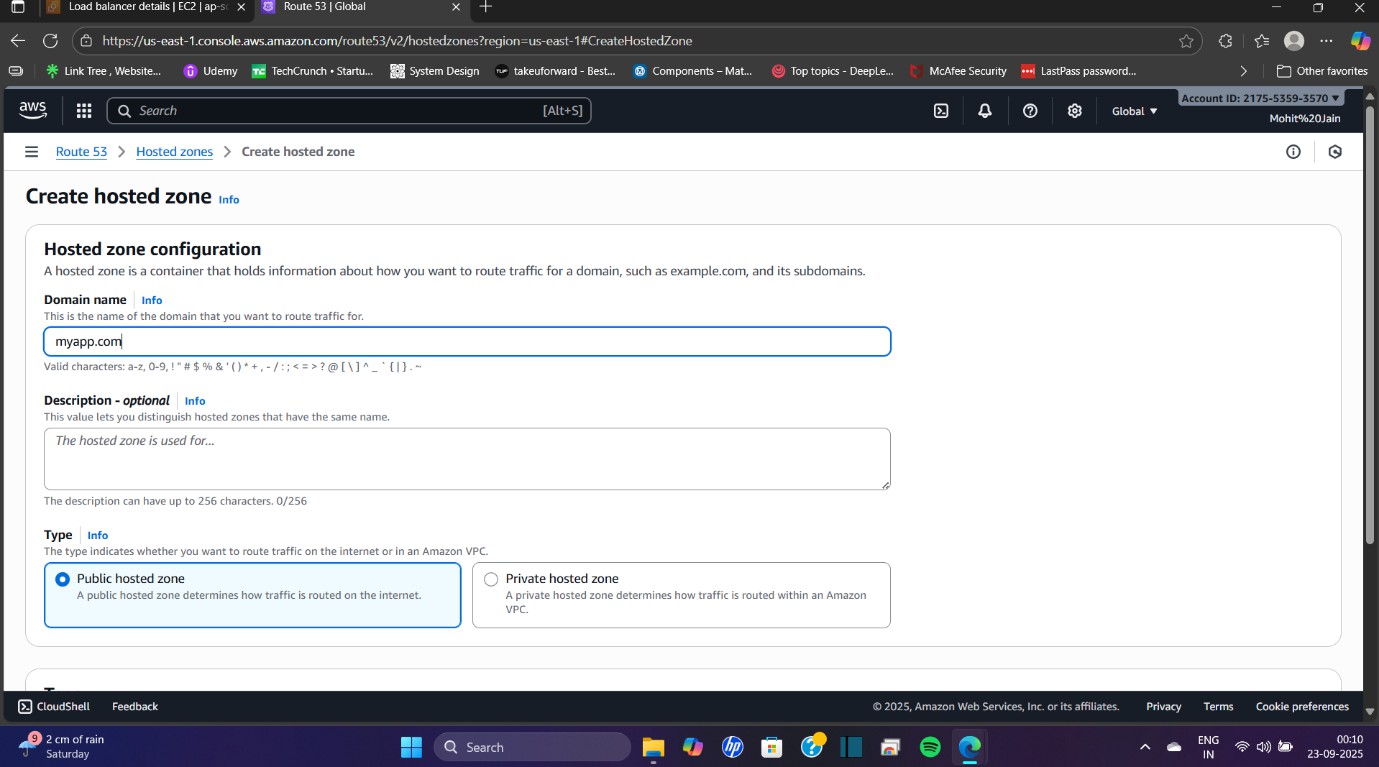
Integrate the regional ALBs with **Route 53** so users are routed to the nearest healthy ALB/region.

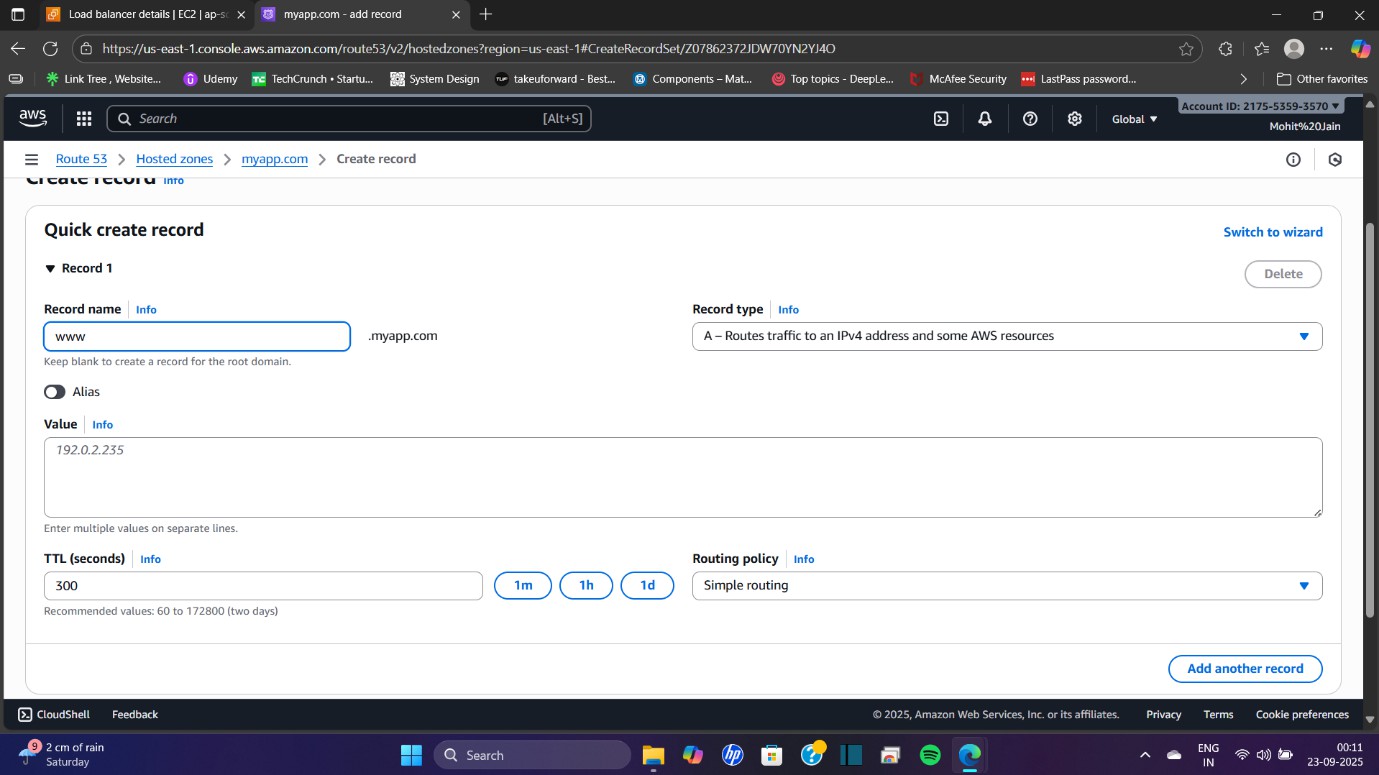
**A. Create or Use a Hosted Zone**

1. Go to **Route 53 → Hosted zones → Create hosted zone** (skip if you already have one).
2. Enter:
   * **Domain name**: yourdomain.com
   * **Type**: Public hosted zone
3. Click **Create hosted zone**.  
   📷 Screenshot: Hosted zone created (e.g., 16-hosted-zone.png).

**B. Create Latency Records for ALBs**

1. Inside the hosted zone, click **Create record**.
2. **Record name**: www (or @ for root domain).
3. **Routing policy**: **Latency**.
4. First record → **ap-south-1 ALB**:
   * Alias → **Application and Classic Load Balancer**
   * Region: **Asia Pacific (Mumbai)**
   * Select **alb-web-ap-south-1** from dropdown
   * **Evaluate target health**: Yes
   * Save record.
5. Second record → **us-east-1 ALB**:
   * Same record name: www
   * Routing policy: **Latency**
   * Alias → **ALB in US East (N. Virginia)**
   * Select **alb-web-us-east-1**
   * **Evaluate target health**: Yes
   * Save record.





**LIVE WEBSITE**

