AWS Task-3

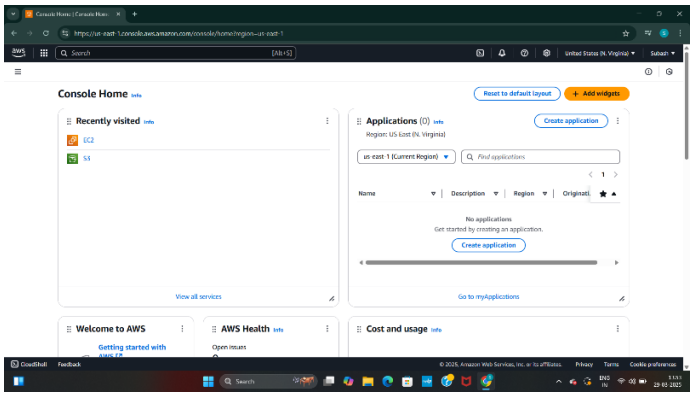
TASKS

1. **Create a S3 bucket, with no public access and upload files to the bucket & view the logs using cloudwatch for the uploaded files.**

Step 1: Create an S3 Bucket (No Public Access)

✓ **Log in to AWS Management Console:**

- Go to **[AWS Console]** (https://aws.amazon.com/console/), and log in with your credentials.



✓ **Navigate to S3:**

- In the search bar at the top, type S3 and click on it.

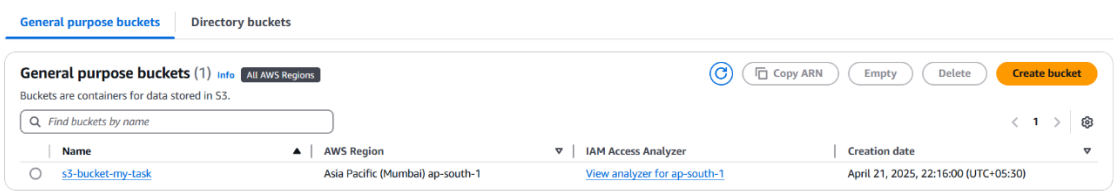
✓ **Create Bucket:**

- Click the orange “Create bucket” button.

✓ **Configure Bucket Settings:**

- Bucket name: Choose a unique name (e.g., s3-bucket-my-task)
- Region: Pick the region closest to you or your app
- Uncheck the "Block all public access" checkbox? NO! Leave it checked — this ensures your bucket stays private.
- Keep default settings for versioning, tags, encryption unless you need them.

✓ **Click "Create bucket" at the bottom.**



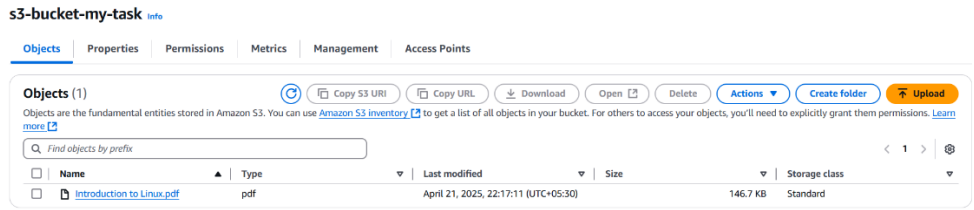
Step 2: Upload Files to the Bucket

✓ From the list of buckets, click on your bucket name (e.g., s3-bucket-my-task).

✓ Click the “Upload” button.

✓ Drag and drop your file or click “Add files”.

✓ Click “Upload” .

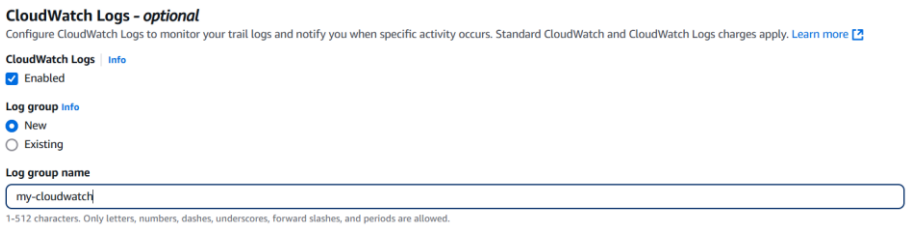


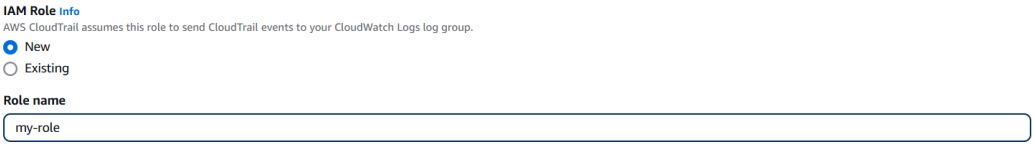
Step 3: Enable Logging for File Uploads Using CloudTrail & View in CloudWatch

S3 doesn't log directly to CloudWatch for uploads. You need to use CloudTrail, which sends logs to CloudWatch Logs.

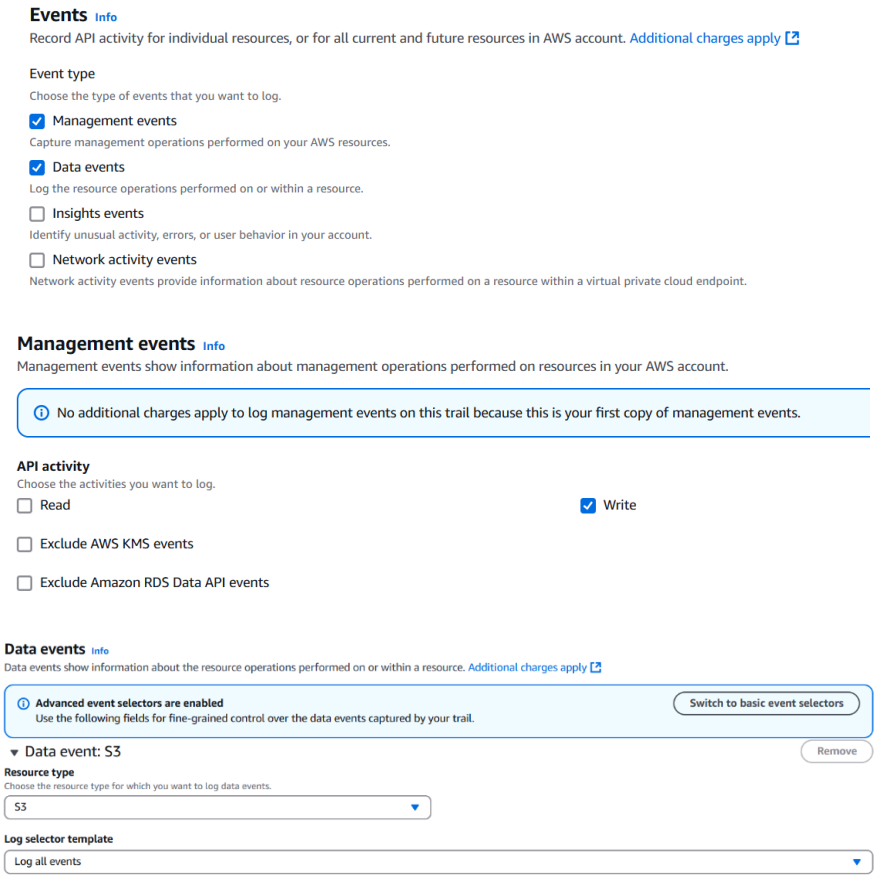
Step 3.1: Create a CloudTrail Trail

- ✓ Go to CloudTrail from the AWS Console (search "CloudTrail").
- ✓ Click on "Trails" in the sidebar → then click "Create trail"
- ✓ Give your trail a name (e.g., my-s3-uploads-trail)
- ✓ Choose "Create a new S3 bucket" or choose an existing one for the logs.
- ✓ **Scroll down and enable CloudWatch Logs:**
    - Check "Enabled"
    - Choose a log group (or create one)
    - Create a new IAM role when prompted (CloudTrail will create permissions for you)

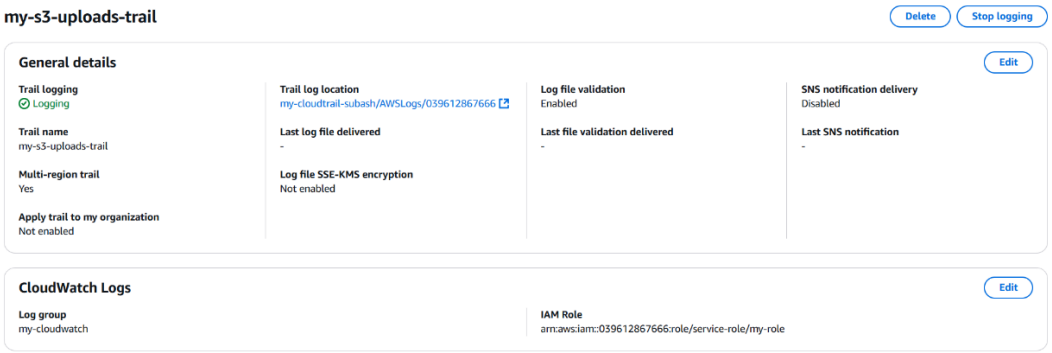




- ✓ **Click Next → Select "Management events":**
    - Read and Write events: Choose Write-only (since you're interested in uploads)
    - Select S3 as the data resource
    - Add your bucket

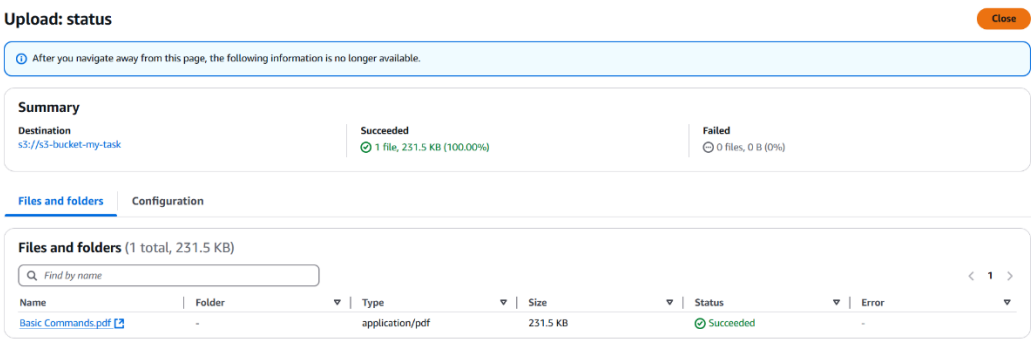


✓ **Click through the rest of the steps and Create Trail.**



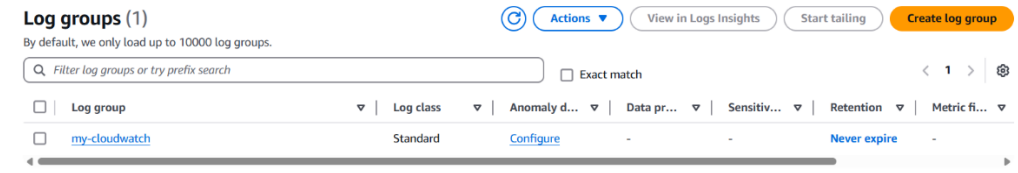
Step 3.2: Upload a File to Test the Logs

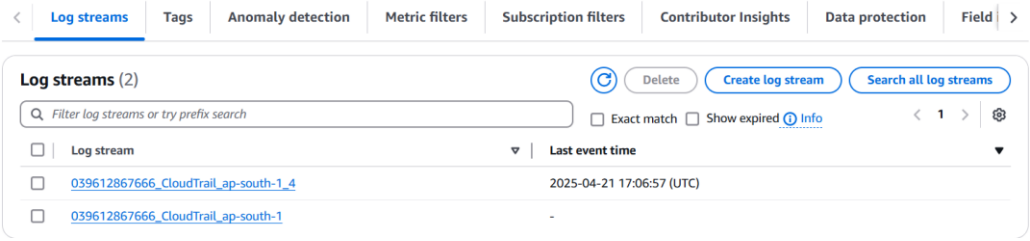
- Go back to S3 and upload a file again.
- Wait a few minutes (CloudTrail takes a bit of time to process events).

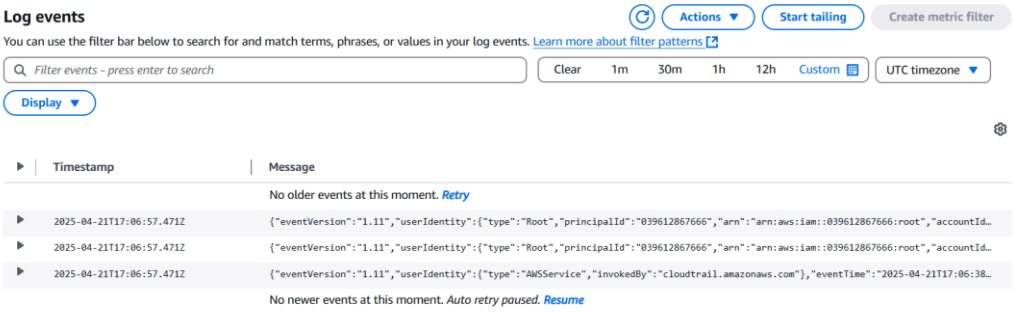


Step 4: View Logs in CloudWatch

- ✓ Go to CloudWatch from the AWS Console.
- ✓ In the sidebar, click “Logs” → then “Log groups”
- ✓ Find the log group from your trail (e.g., /aws/cloudtrail/logs)
- ✓ Click the latest log stream (you’ll see one with today's date).



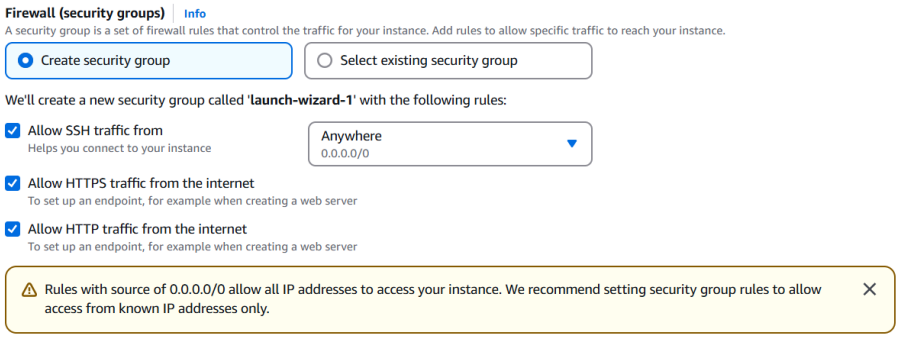




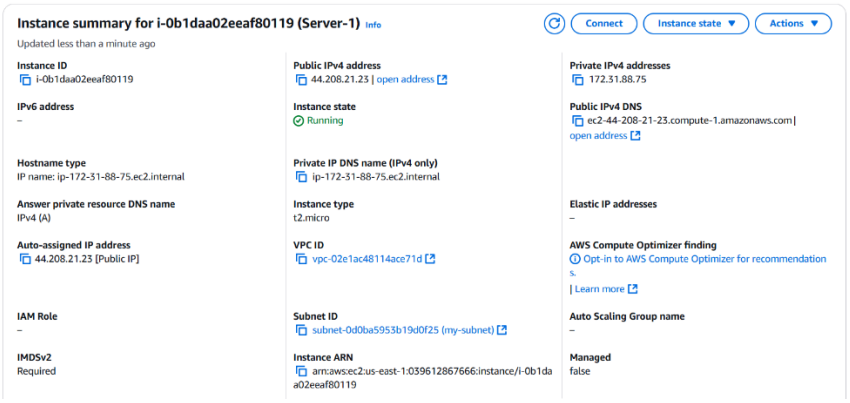
2. **Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address.**

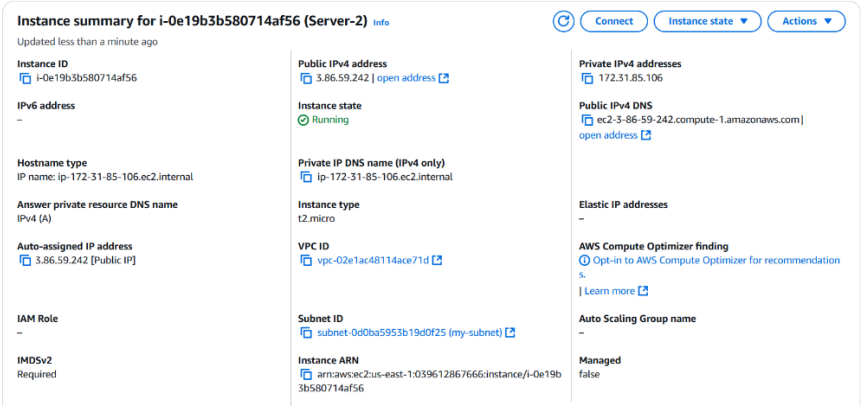
Step 1: Launch Two EC2 Instances

- ✓ Go to EC2 → Launch Instance.
- ✓ AMI: Amazon Linux 2.
- ✓ Instance type: t2.micro (for free tier) or anything else.
- ✓ **Network settings:**
  - Select VPC(default) and Subnet .
  - Auto-assign Public IP: Enable.
- ✓ **Security Group:**
  - Allow HTTP (80) and SSH (22) inbound from your IP (for admin) and the Load Balancer's security group.



- Launch two instances. Name them Server-1 and Server-2.



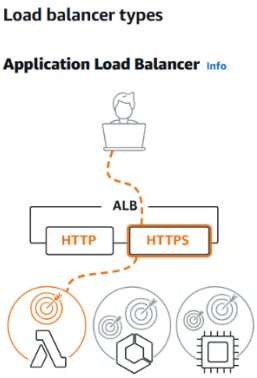


Step 2: Install Web Server on Each Instance

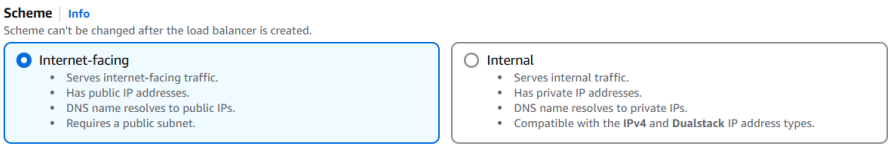
- ✓ Install an web server on both instance. To install an web server the command is:
  - sudo yum update -y
  - sudo yum install httpd -y
  - sudo systemctl start httpd
  - sudo systemctl enable httpd
- ✓ And, now you can host an webpage you want ,move the index.html file to the below location.
  - /var/www/html/index.html.

Step 3: Create an Application Load Balancer

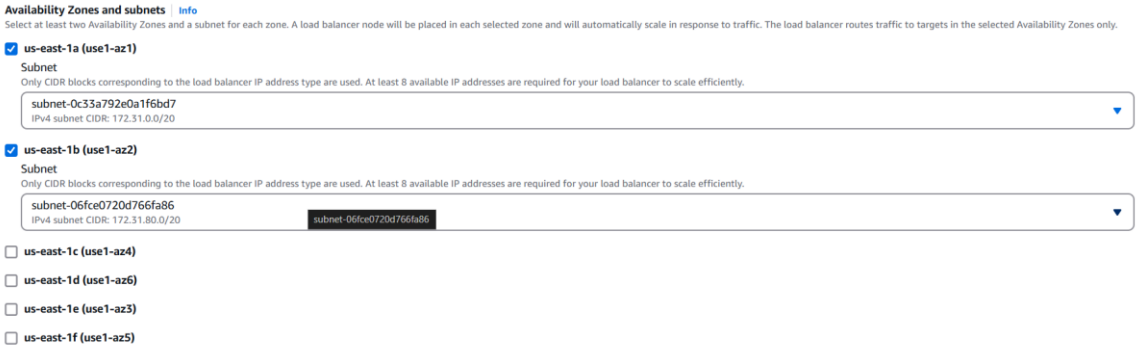
- ✓ Go to **EC2 ➔ Load Balancers ➔ Create Load Balancer ➔ Application Load Balancer**.



- ✓ **Basic Configuration**:
  - Name: My-ALB
  - Scheme: Internet-facing
  - IP address type: IPv4

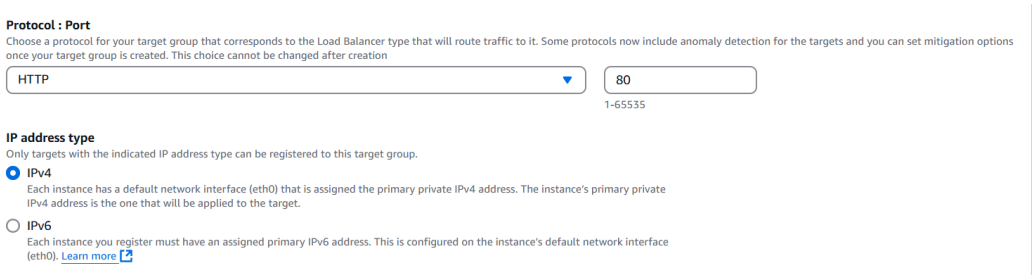


- ✓ **Network Mapping**:
  - VPC: Select your existing VPC (or default).
  - Availability Zones: Select 2 AZs where your EC2s are.



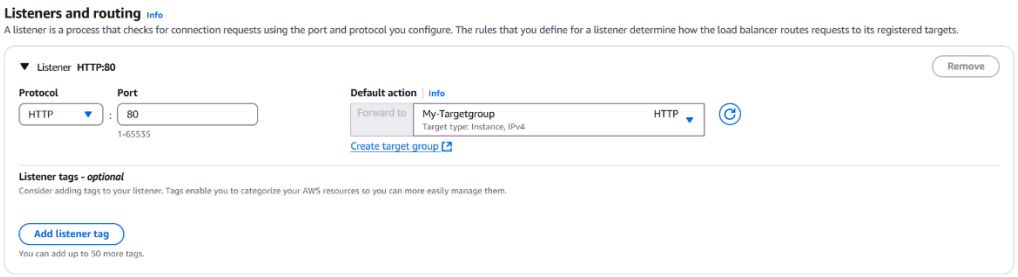
✓ **Security Groups**:

- Create or select one allowing **HTTP (80)** inbound.



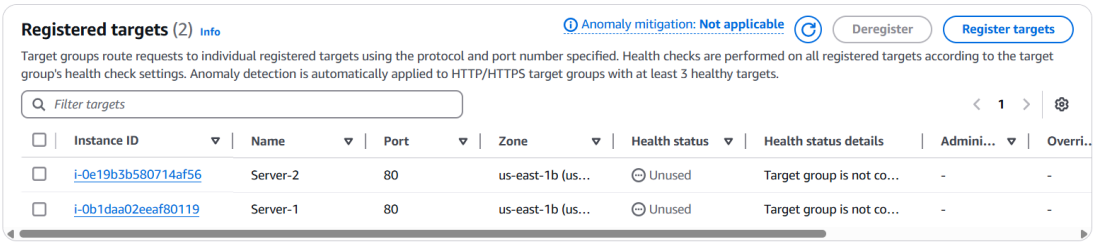
✓ **Listeners and Routing**:

- Listener: Port 80 ➔ Forward to **Target Group**.

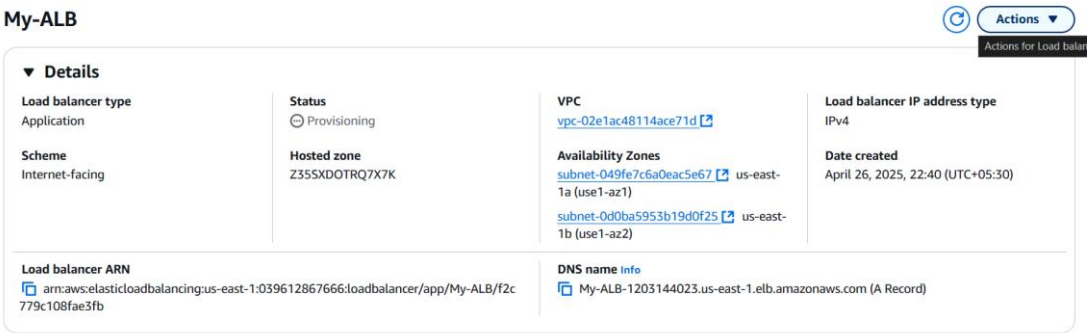


✓ **Create a Target Group**:

- Target type: **Instance**
- Protocol: **HTTP**
- Port: **80**
- Health checks: HTTP on /
- Register both EC2 instances to the Target Group.

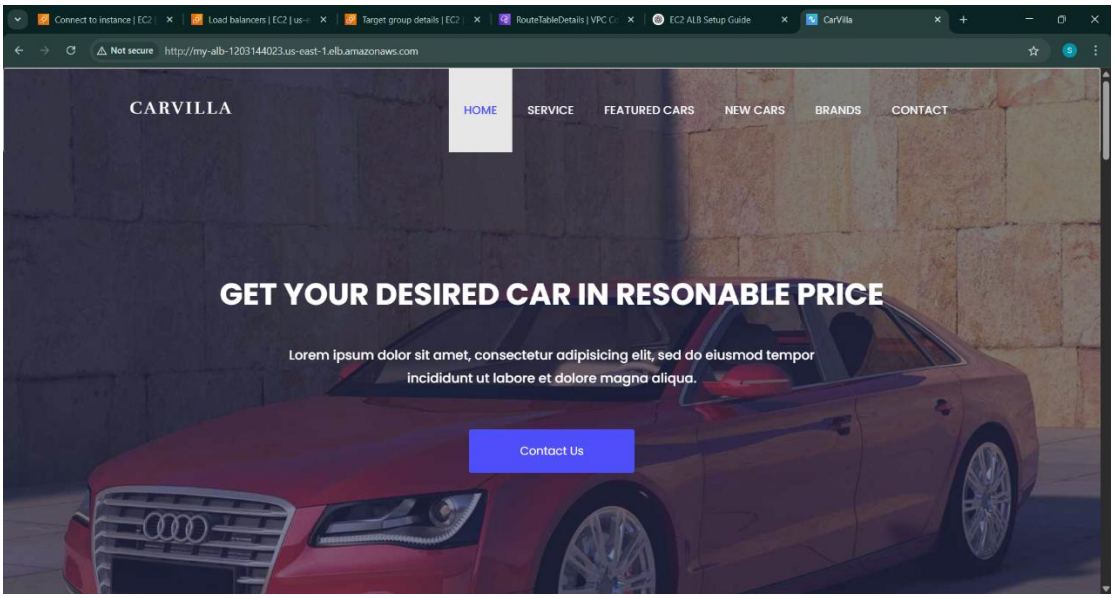


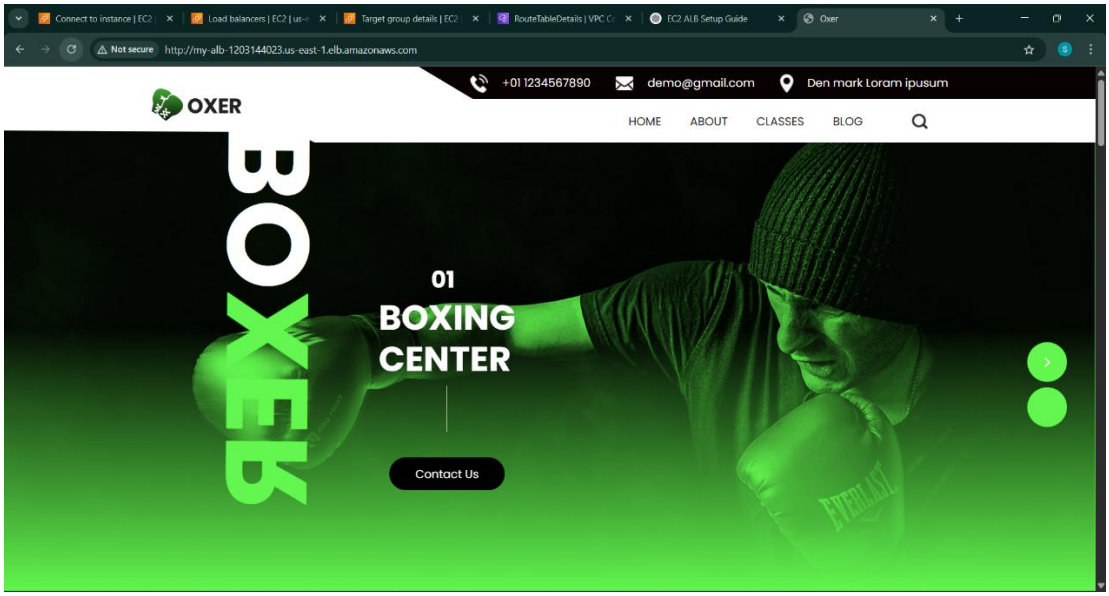
✓ Finalize and **Create Load Balancer**.



Step 4: Test the Setup

- ✓ Find your ALB DNS name (something like My-ALB-1203144023.us-east-1.elb.amazonaws.com).
- ✓ Open the ALB DNS name in browser:
    - Refresh multiple times ➔ you should see responses switching between Server 1 and Server 2 (round robin).





********** **TASK COMPLETED** **********