AWS Project VPC with public-private subnet in production

This example demonstrates how to create a VPC that you can use for servers in a production environment. To improve resiliency, you deploy the servers in two Availability Zones, by using an Auto Scaling group and an Application Load Balancer. For additional security, you deploy the servers in private subnets. The servers receive requests through the load balancer. The servers can connect to the internet by using a NAT gateway. To improve resiliency, you deploy the NAT gateway in both Availability Zones.

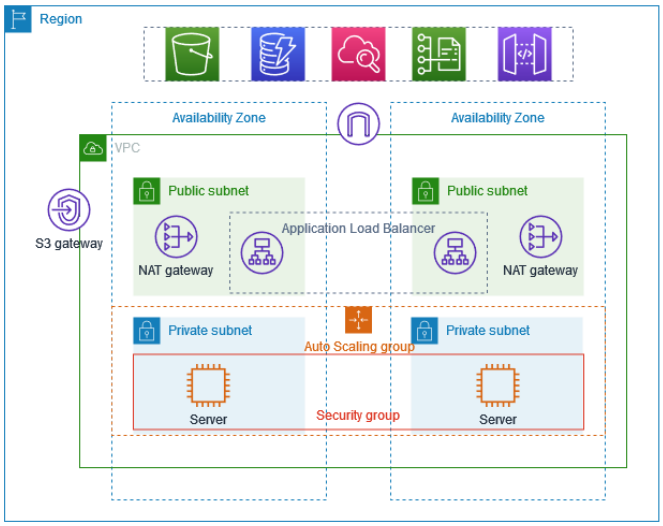
Overview

The following diagram provides an overview of the resources included in this example. The VPC has public subnets and private subnets in two Availability Zones. Each public subnet contains a NAT gateway and a load balancer node. The servers run in the private subnets, are launched and terminated by using an Auto Scaling group, and receive traffic from the load balancer. The servers can connect to the internet by using the NAT gateway. The servers can connect to Amazon S3 by using a gateway VPC endpoint.

Architecture Overview

The project creates a robust cloud infrastructure using the following AWS services:

- **VPC (Virtual Private Cloud)** - Isolated network environment
- **Public & Private Subnets** - Network segmentation across multiple AZs
- **EC2 Auto Scaling** - Automatic scaling based on demand
- **Application Load Balancer** - Traffic distribution and high availability
- **Target Groups** - Health monitoring and routing
- **EC2 -Bastion Host** - Secure access to private resources
- **Security Groups** - Network-level security control



🛠️ Components Breakdown

1. VPC (Virtual Private Cloud)

- CIDR Block: 10.0.0.0/16
- Purpose: Isolated network environment for all resources
- **Features:**
  - DNS resolution enabled
  - DNS hostnames enabled
  - Dedicated tenancy (optional)

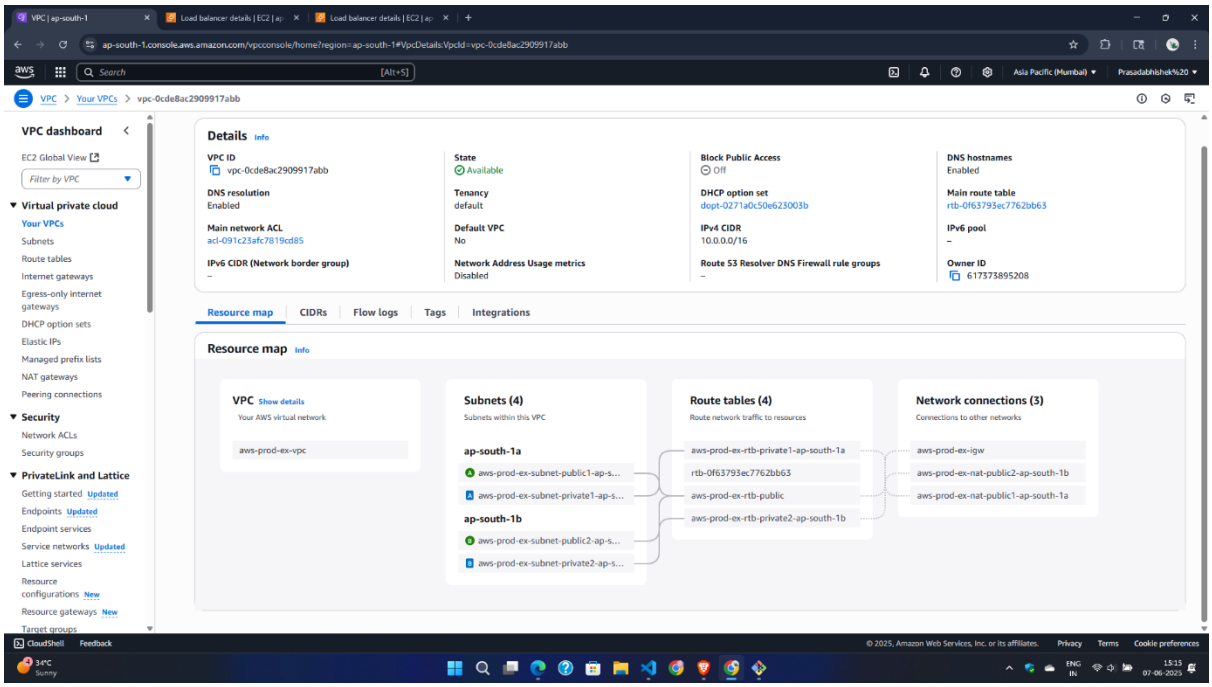
2. Subnets Configuration

Public Subnets

- Public Subnet 1: 10.0.1.0/24 (AZ-1a)
- Public Subnet 2: 10.0.2.0/24 (AZ-1b)
- **Features:**
  - Internet Gateway attached
  - Auto-assign public IP enabled
  - Hosts Load Balancer and Bastion Host

Private Subnets

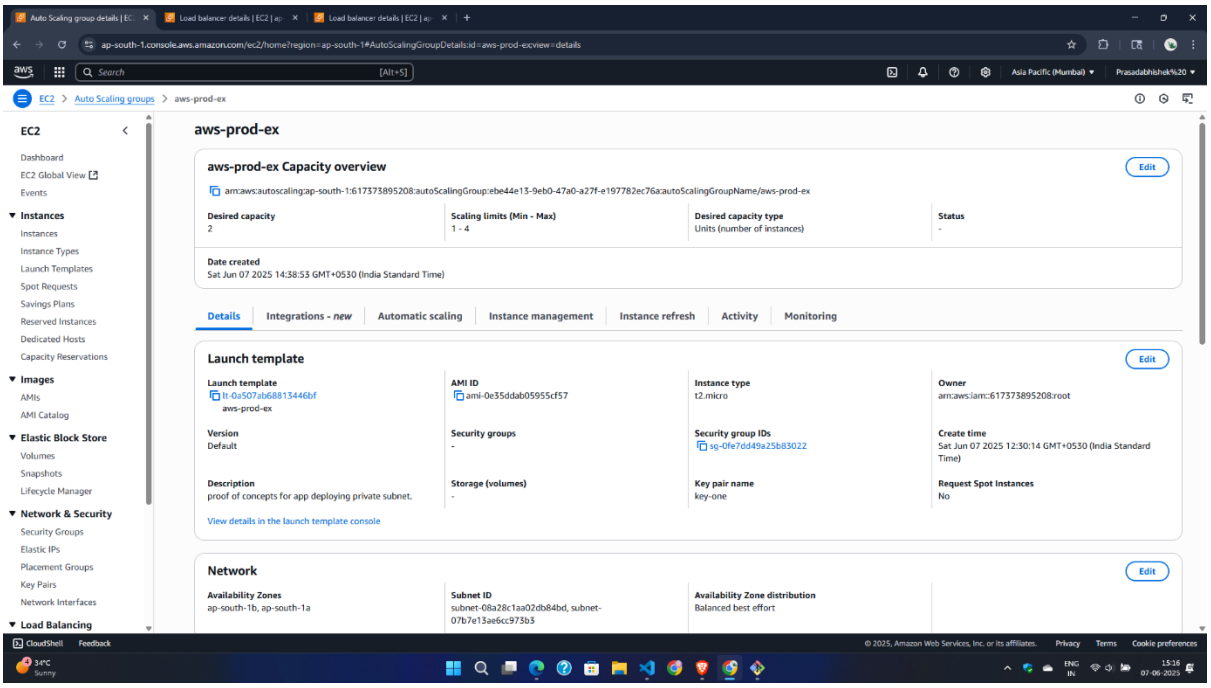
- Private Subnet 1: 10.0.3.0/24 (AZ-1a)
- Private Subnet 2: 10.0.4.0/24 (AZ-1b)
- **Features:**
  - NAT Gateway for outbound internet access
  - Hosts application servers
  - No direct internet access



VPC

3. EC2 Auto Scaling Group

- **Configuration**:
  - Minimum instances: 2
  - Maximum instances: 6
  - Desired capacity: 2
  - Health check type: ELB
  - Health check grace period: 300 seconds
- **Scaling Policies**:
  - Scale up when CPU > 70%
  - Scale down when CPU < 30%
- **Launch Template**:
  - Instance type: t3.micro (or t2.micro for free tier)
  - AMI: Amazon Linux 2
  - User data script for web server setup

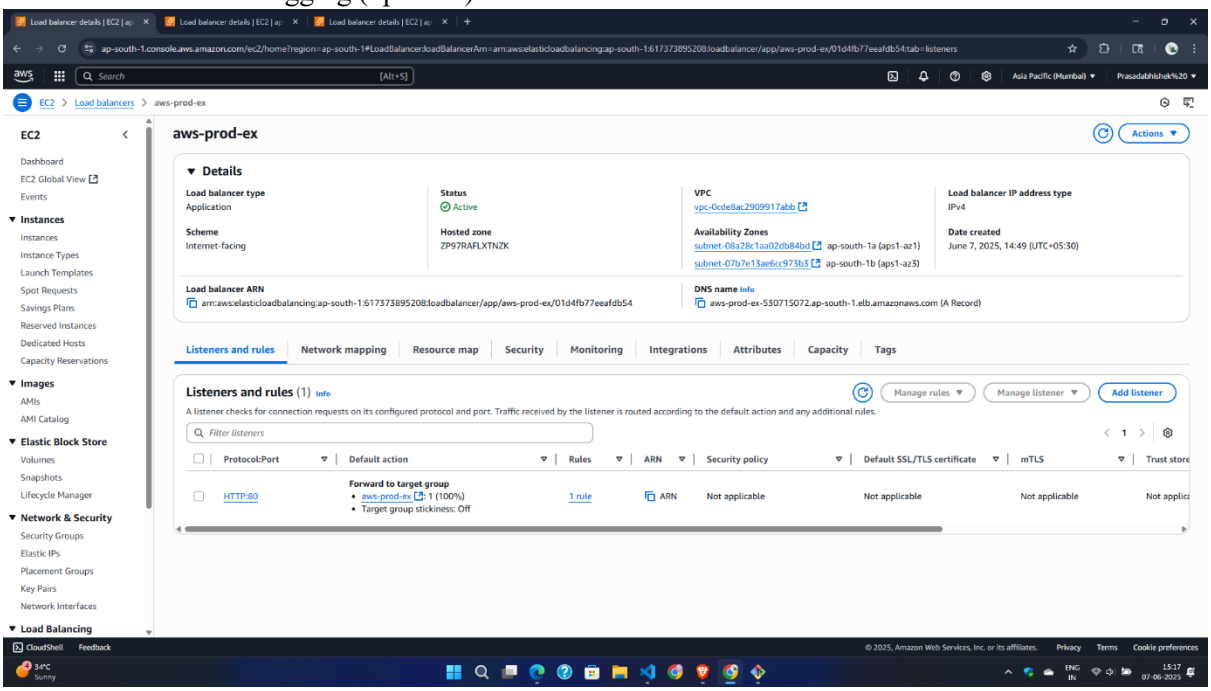


EC2 Auto Scaling

4. Application Load Balancer (ALB)

- **Type**: Application Load Balancer
- **Scheme**: Internet-facing
- **Listeners**: HTTP (Port 80), HTTPS (Port 443)
- **Availability Zones**: Both AZ-1a and AZ-1b
- **Features**:
  - Cross-zone load balancing
  - Deletion protection

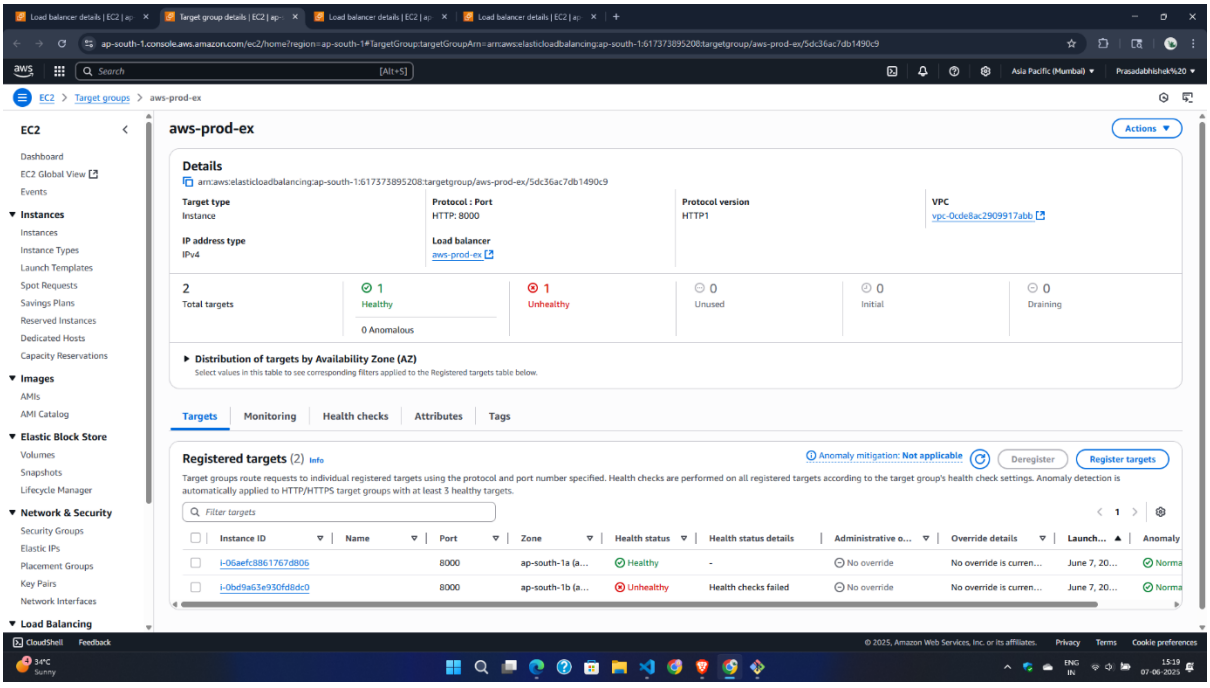
Access logging (optional)



Load Balancer

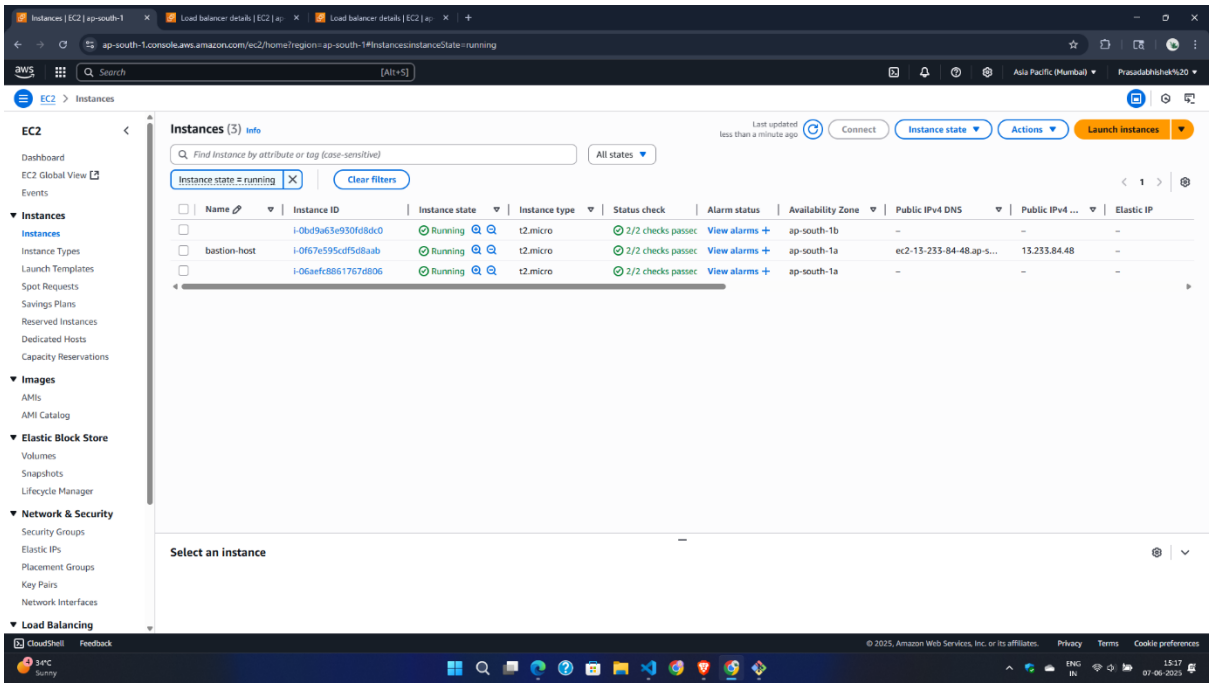
5. Target Group

- **Target Type**: Instance
- **Protocol**: HTTP
- **Port**: 80
- **Health Check**:
  - Path: /health or /
  - Interval: 30 seconds
  - Timeout: 5 seconds
  - Healthy threshold: 2
  - Unhealthy threshold: 5



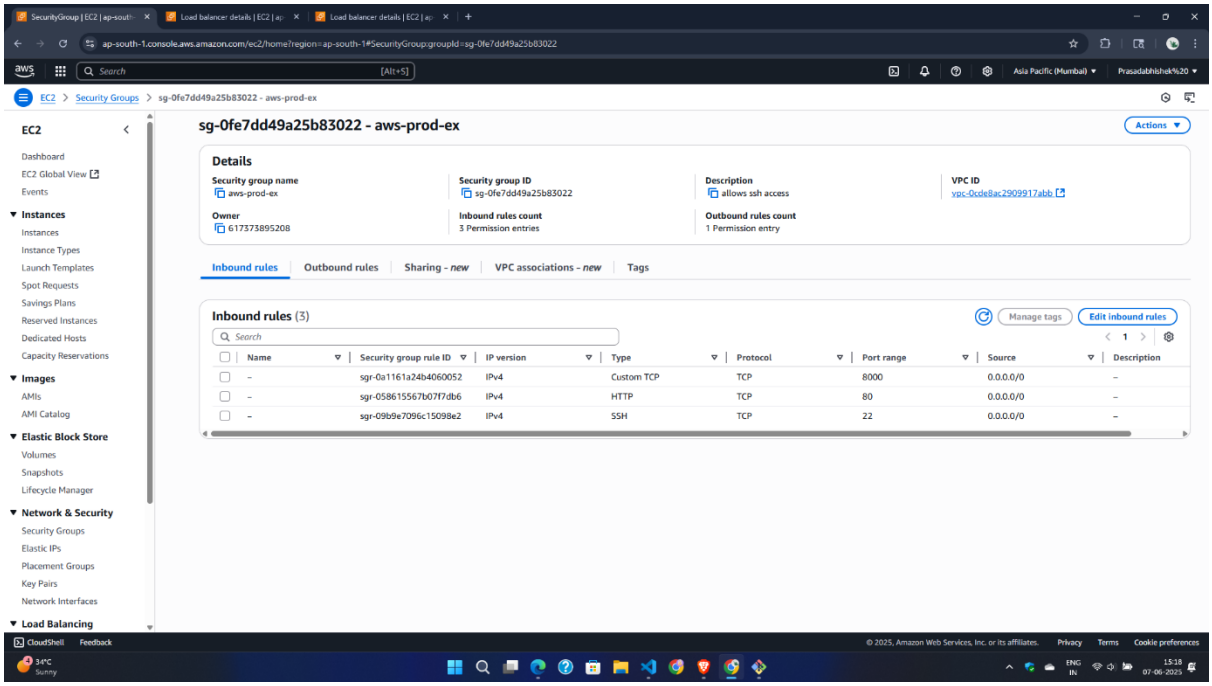
Target *Group*

6. Bastion Host (Jump Server)

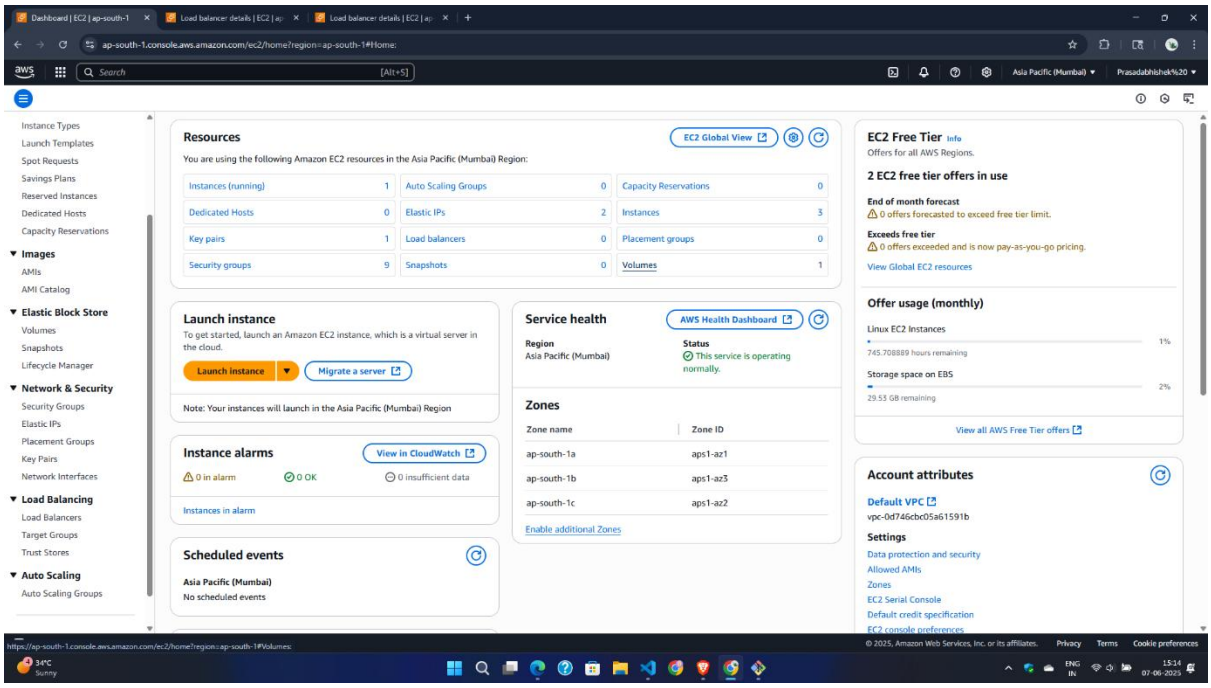


7. Security Groups

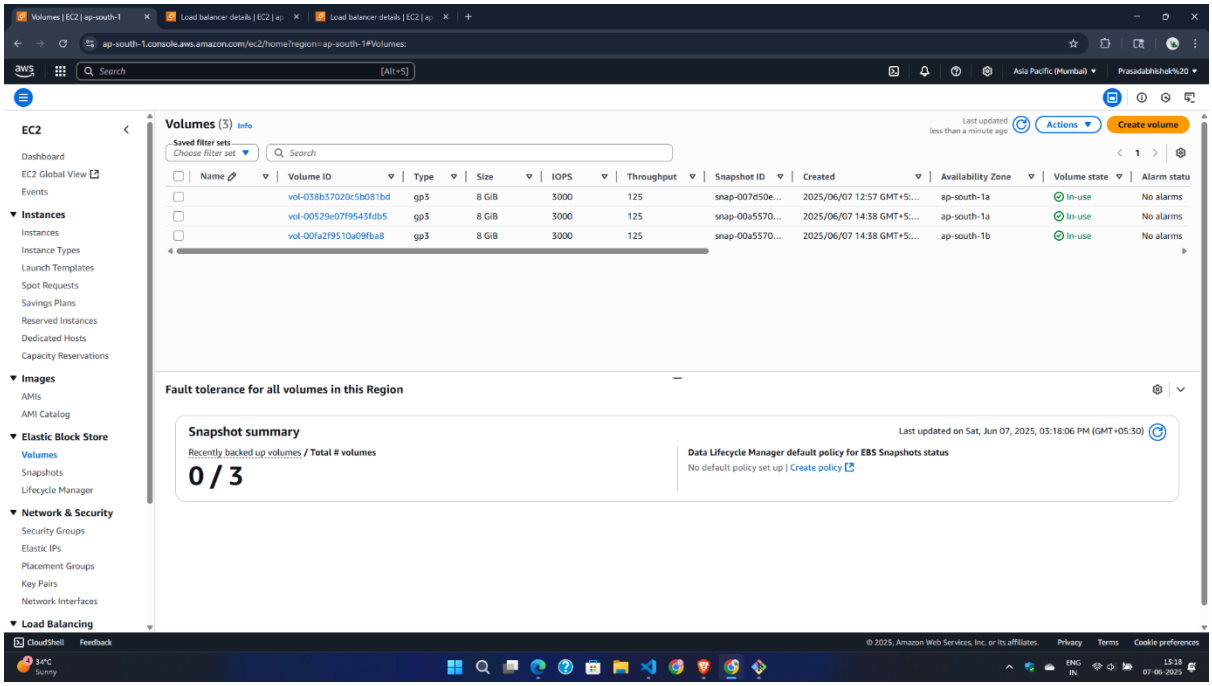
- Load Balancer Security Group
- Web Server Security Group
- Bastion Host Security Group



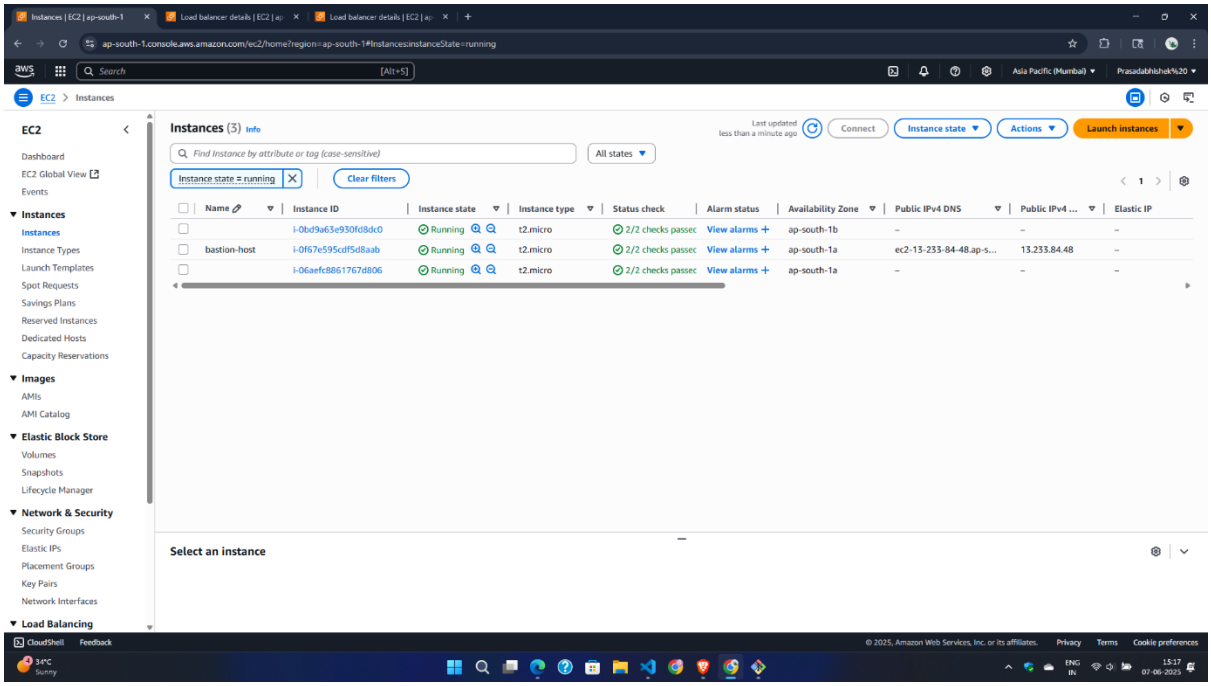
Resources



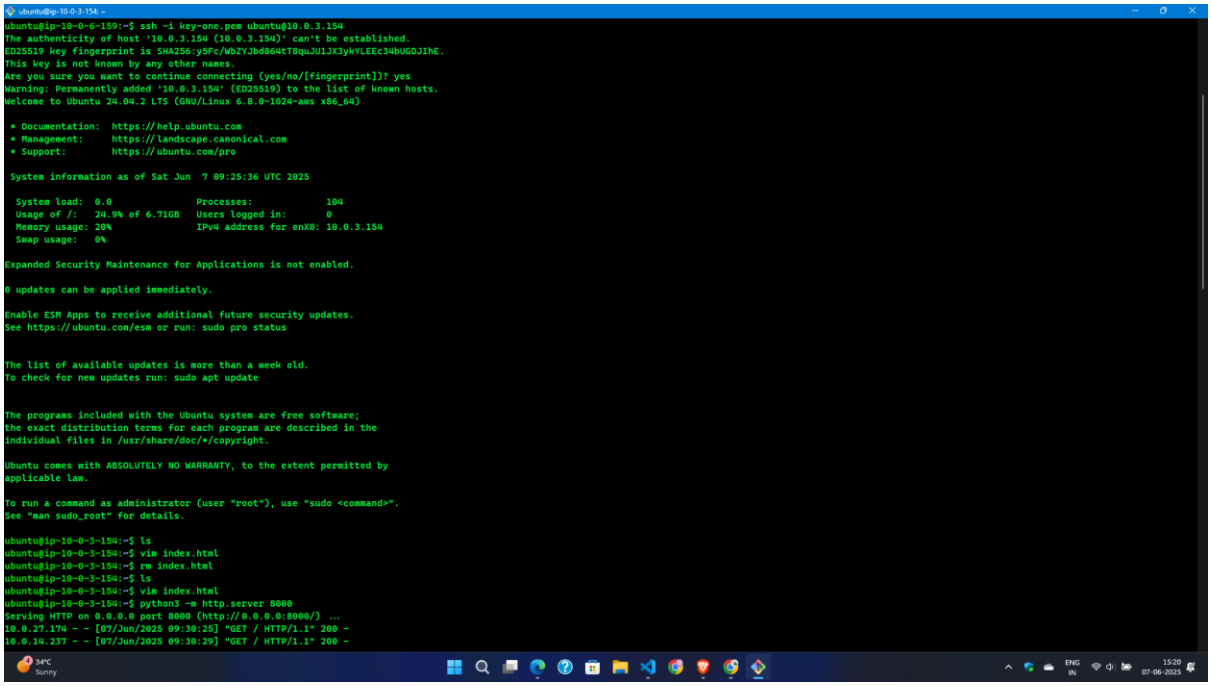
Volume



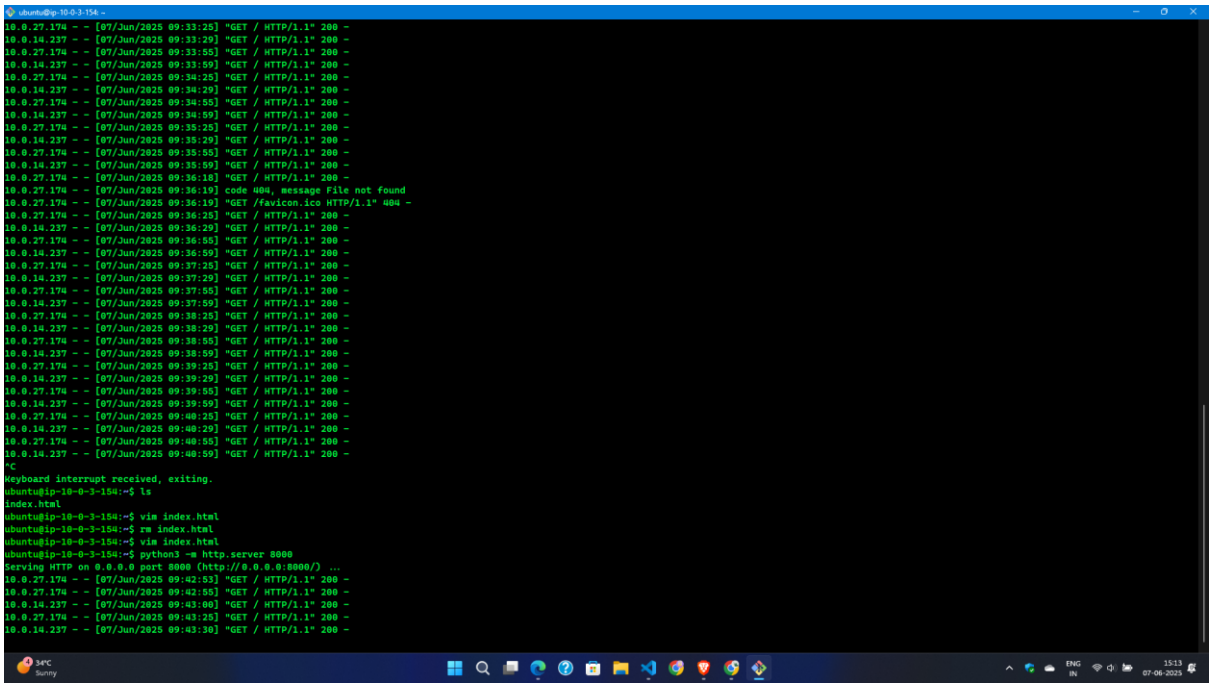
EC2 Instance



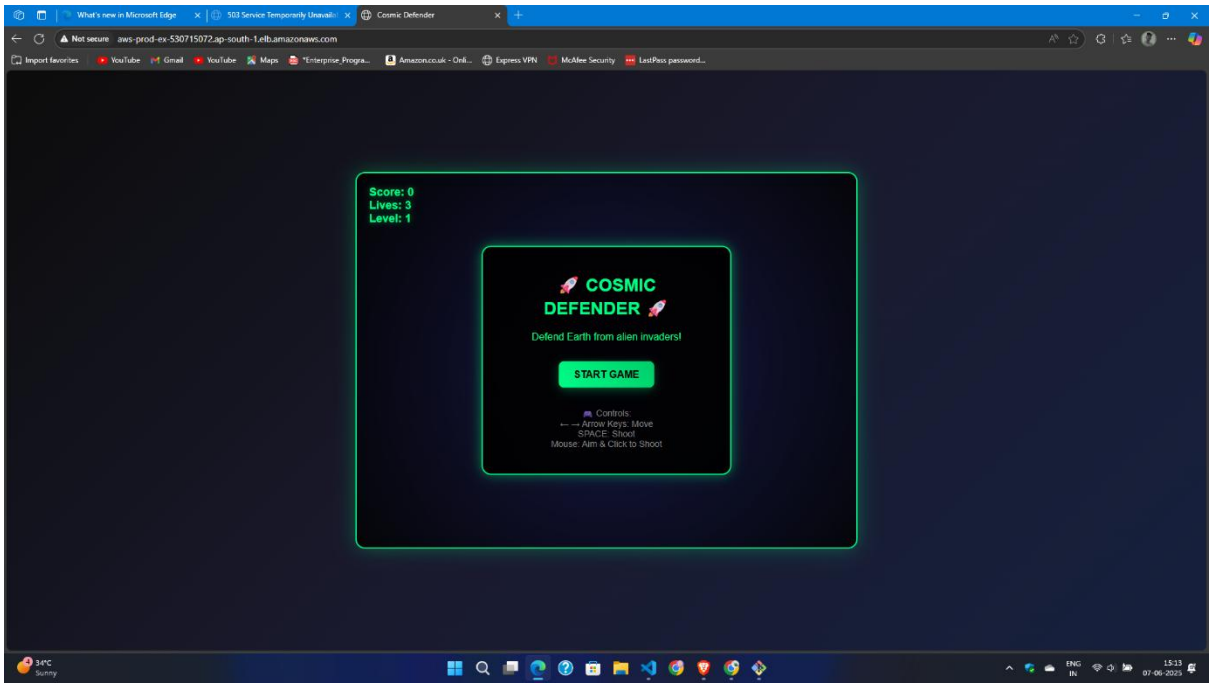
Command

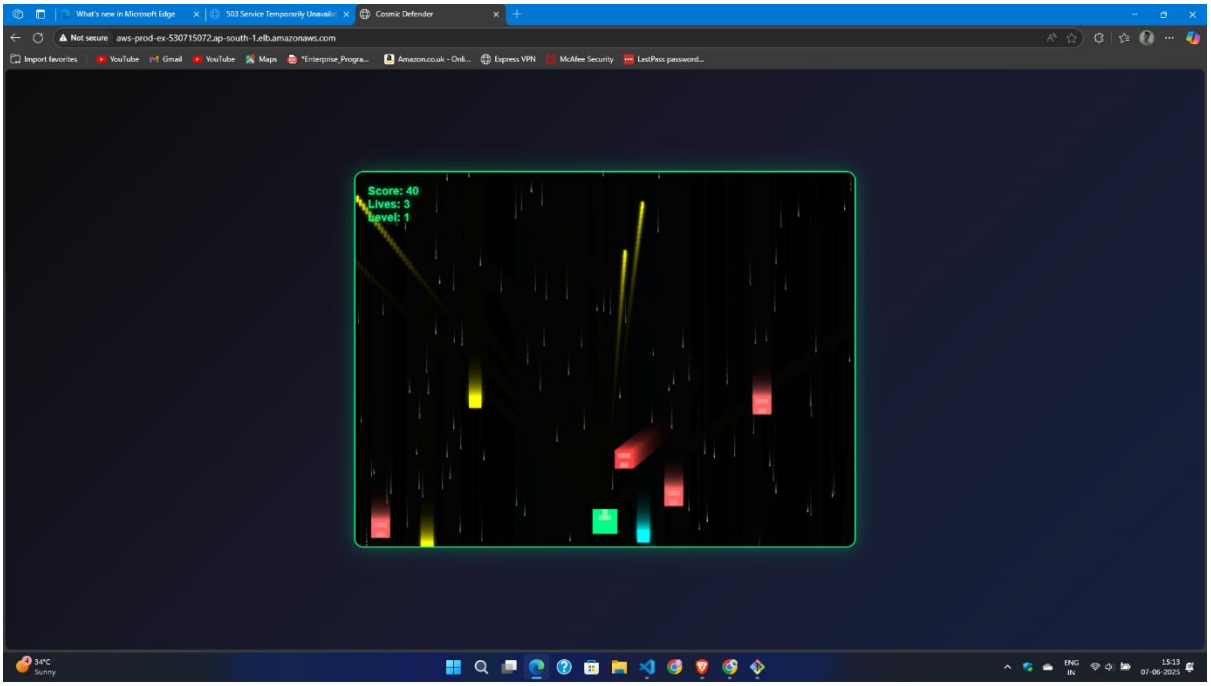


Response



Final OutPut :




What's new in Microsoft Edge
503 Service Temporarily Unavailable
Cosmic Defender
Not secure
aws-prod-ex-530715072.ap-south-1.elb.amazonaws.com
Import favorites
YouTube
Gmail
YouTube
Maps
Amazon.co.uk - Onli...
Express VPN
McAfee Security
LastPass password...
Score: 40
Lives: 3
Level: 1
34°C
Sunny
ENG
IN
15:13
07-06-2025