A Project Documentation on

"Highly Available Web Application with Secure VPC, S3 Storage & SNS Alerts"

Project Objective

Design and deploy a secure, scalable web application on AWS using:

- EC2 for compute
- S3 for static content & backups
- VPC for networking & security
- SNS for system notifications and alerts

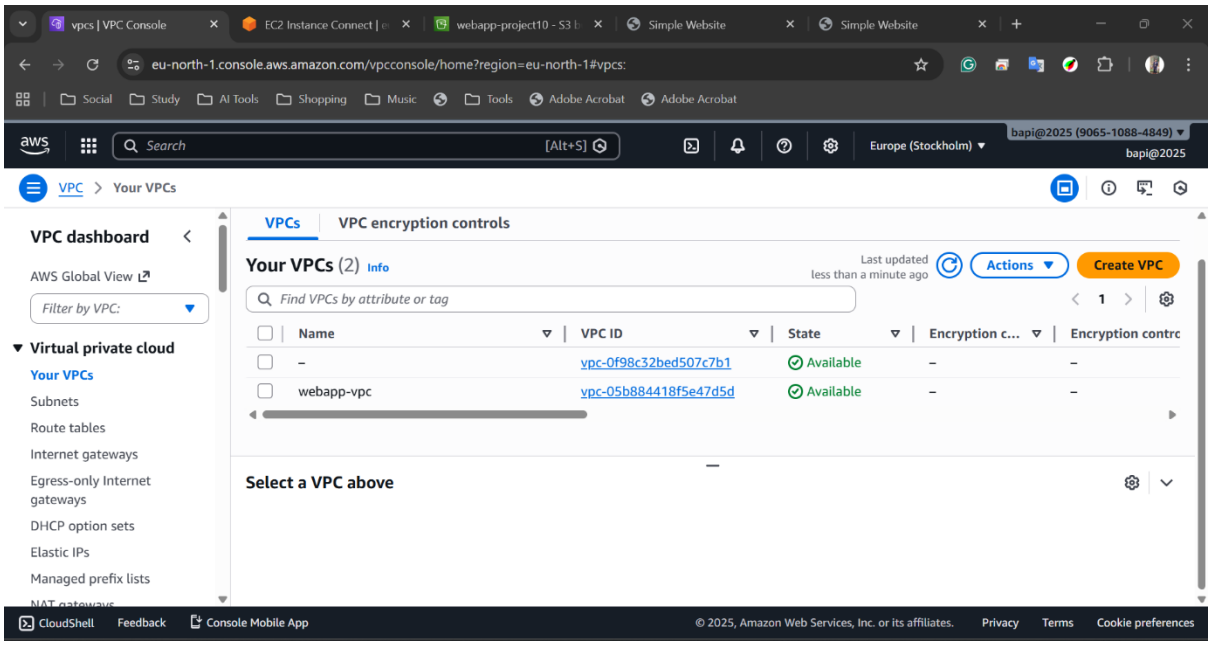
Steps:-

Step 1: Create a Custom VPC

- Go to VPC → Create VPC
- Select VPC only

Enter:

- Name: **webapp-vpc**
- IPv4 CIDR: 10.0.0.0/16
- Click Create VPC

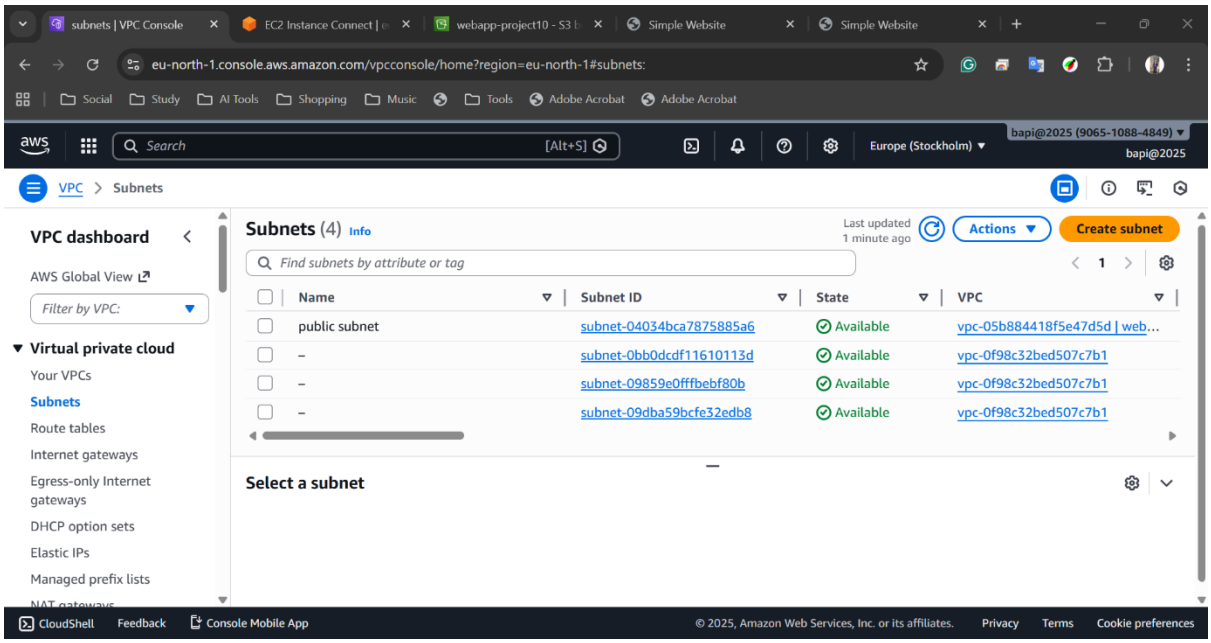


Step 2: Create a Public Subnet

- Go to VPC → Subnets → Create subnet
- Select webapp-vpc

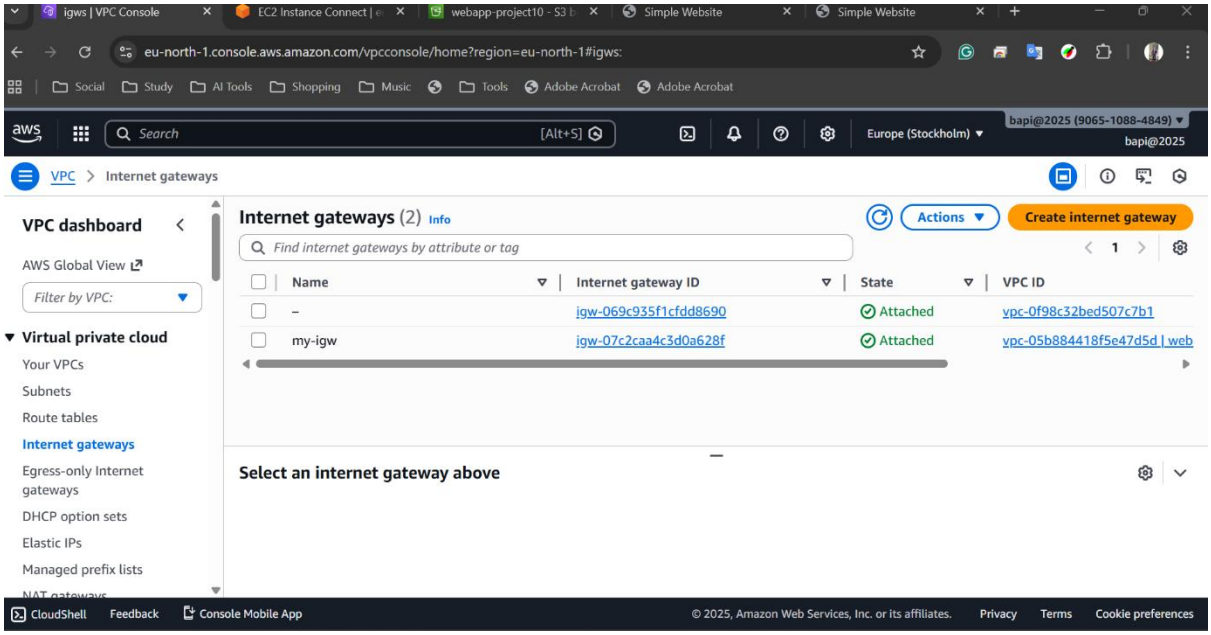
Enter:

- Subnet name: **public-subnet**
- Availability Zone: any (e.g., us-east-1a)
- CIDR: 10.0.1.0/24
- Enable Auto-assign public IPv4
- Click Create subnet



Step 3: Create and Attach Internet Gateway

- Go to VPC → Internet Gateways
- Click Create internet gateway
- Name: **my-igw**
- Attach it to webapp-vpc



Step 4: Configure Route Table

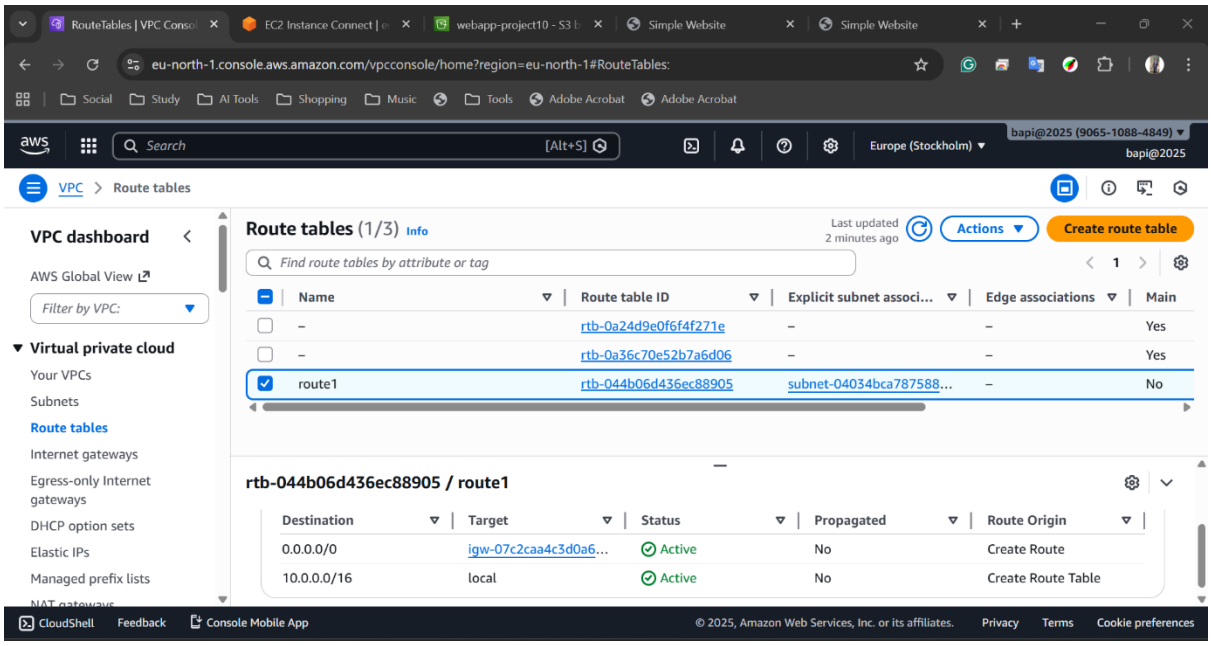
- Go to VPC → Route Tables

Create a route table:

- Name: **route1**
- VPC: webapp-vpc

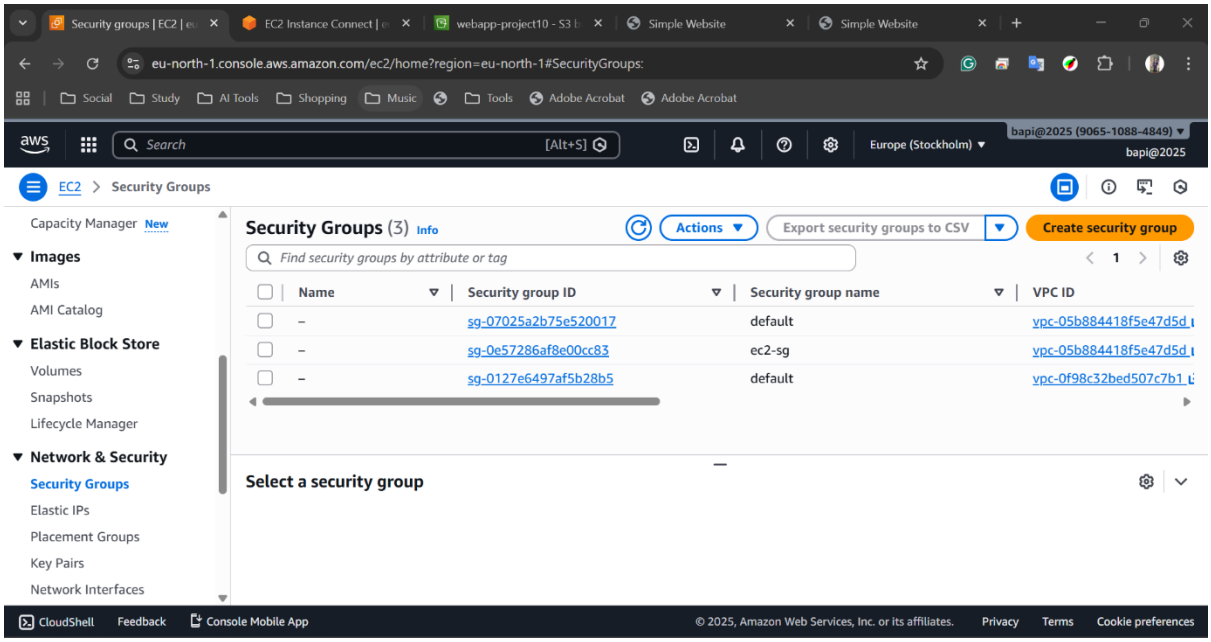
Add route:

- Destination: 0.0.0.0/0
- Target: Internet Gateway
- Associate the route table with Public-Subnet



Step 5: Create Security Group

- Go to EC2 → Security Groups → Create
- Name: **ec2_sg**
- VPC: webapp-vpc
- Inbound rules:
- HTTP – Port 80 – Source: 0.0.0.0/0
- SSH – Port 22 – Source: My IP
- Outbound: Allow all traffic
- Create security group



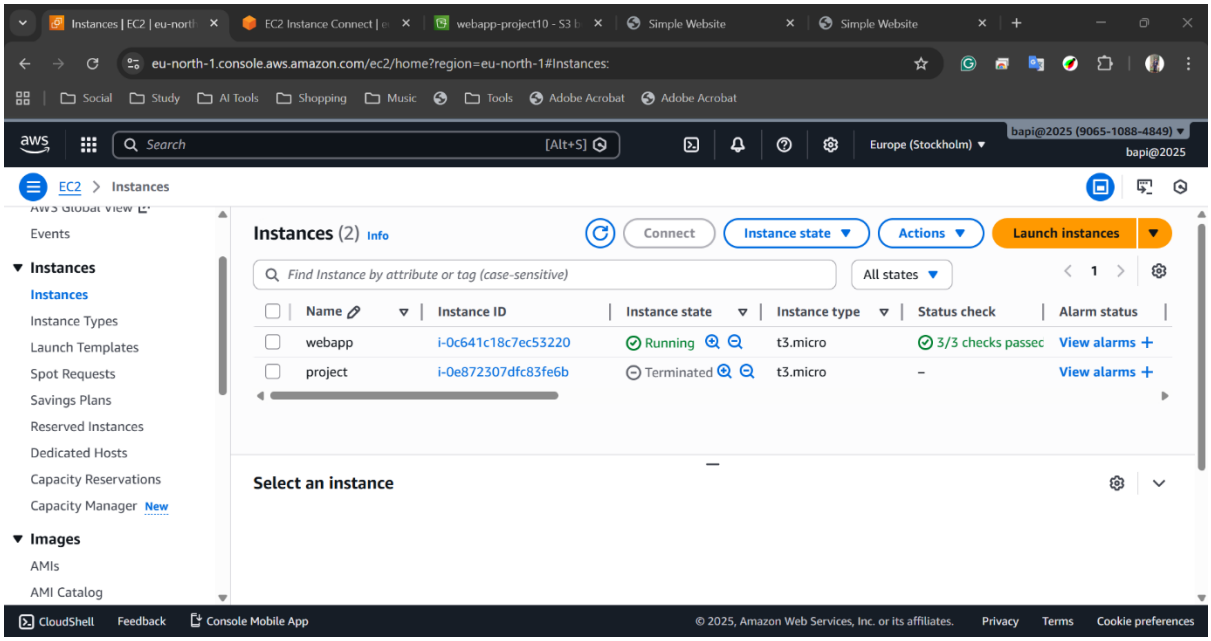
Step 6: Launch EC2 Instance

- Go to EC2 → Launch Instance
- Name: **webapp**
- AMI: Amazon Linux 2
- Instance type: t3.micro (Free tier)
- Key pair: created a project.pem
- Network settings:
- VPC: webapp-vpc
- Subnet: public-subnet
- Auto-assign Public IP: Enabled
- Security group: ec2_sg

- User data:

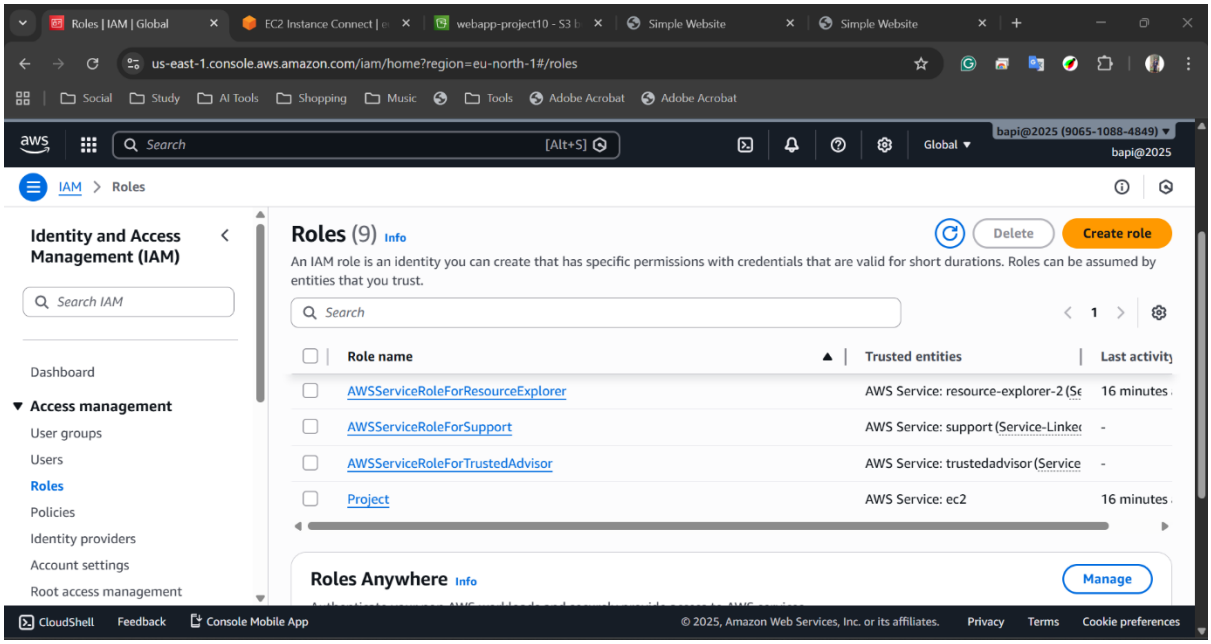
```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "Welcome to Highly Available Web App" > /var/www/html/index.html
```

- Launch instance



Step 7: Create IAM Role

- Go to IAM → Roles
- Create Role
- Trusted Entity: AWS Service
- Use case: EC2
- Permission policies: AmazonS3FullAccess
- Name: project
- Create Role

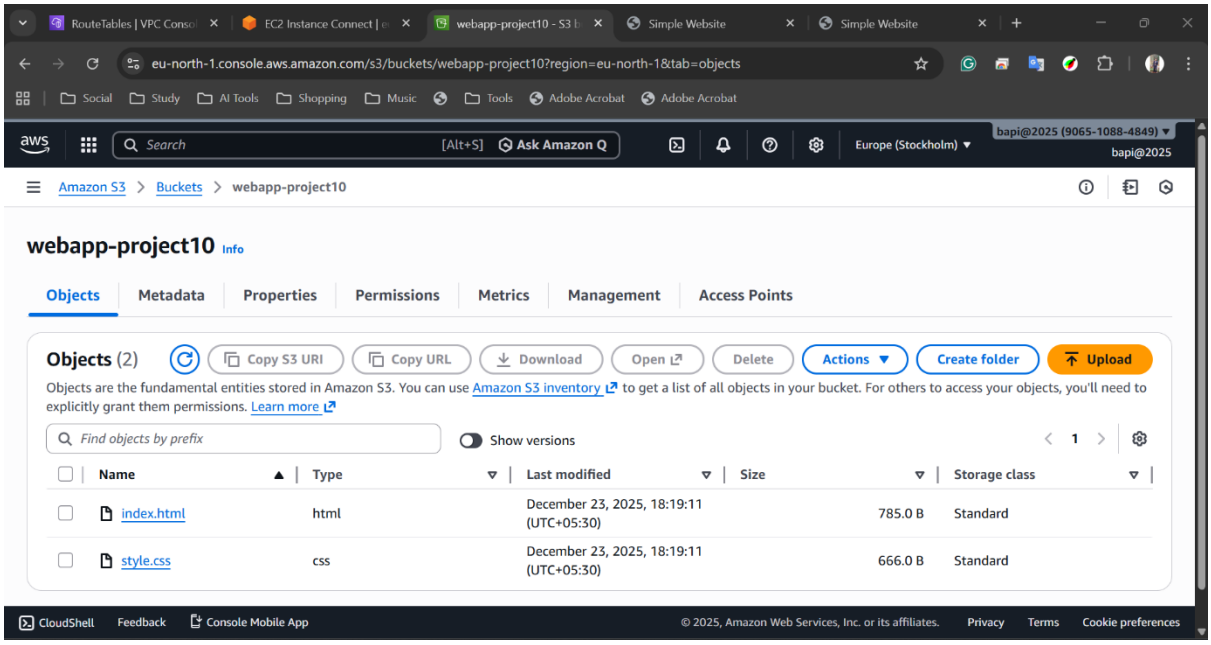


Step 8: Create S3 Bucket

- Go to S3 → Create bucket
- Bucket name: **webapp-project10**
- Region: same as EC2
- Enable:
- Versioning
- Block public access
- Create bucket

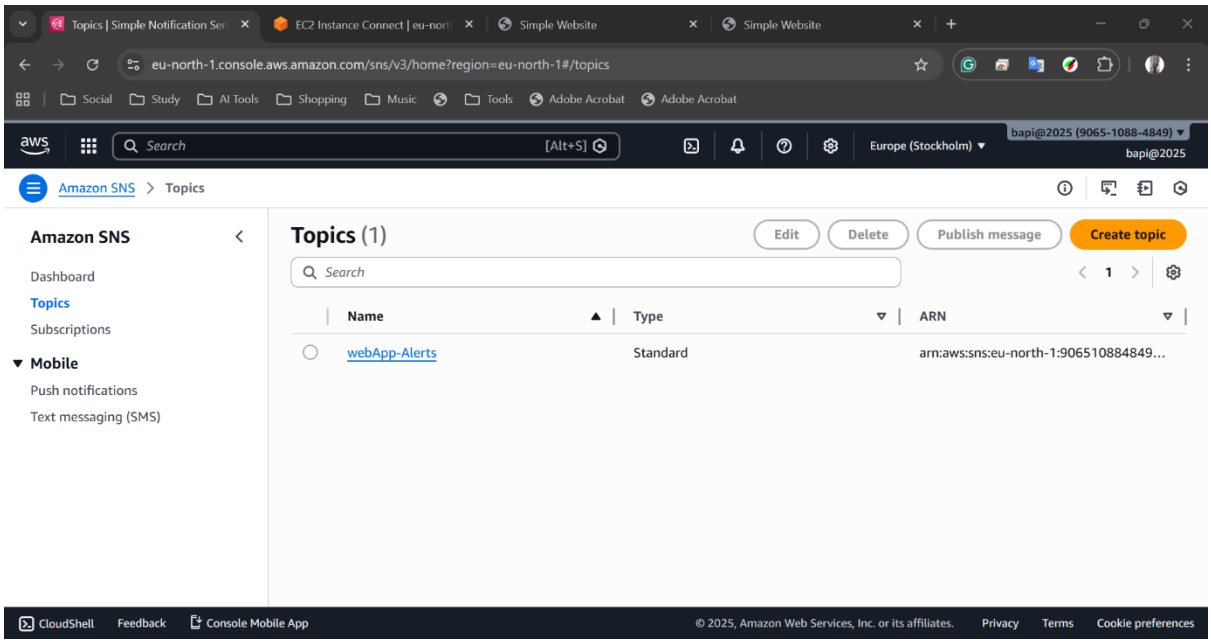
Step 9: Upload Static Content to S3

- Open the S3 bucket
- Upload:
    - index.html
    - style.css
    - script.js



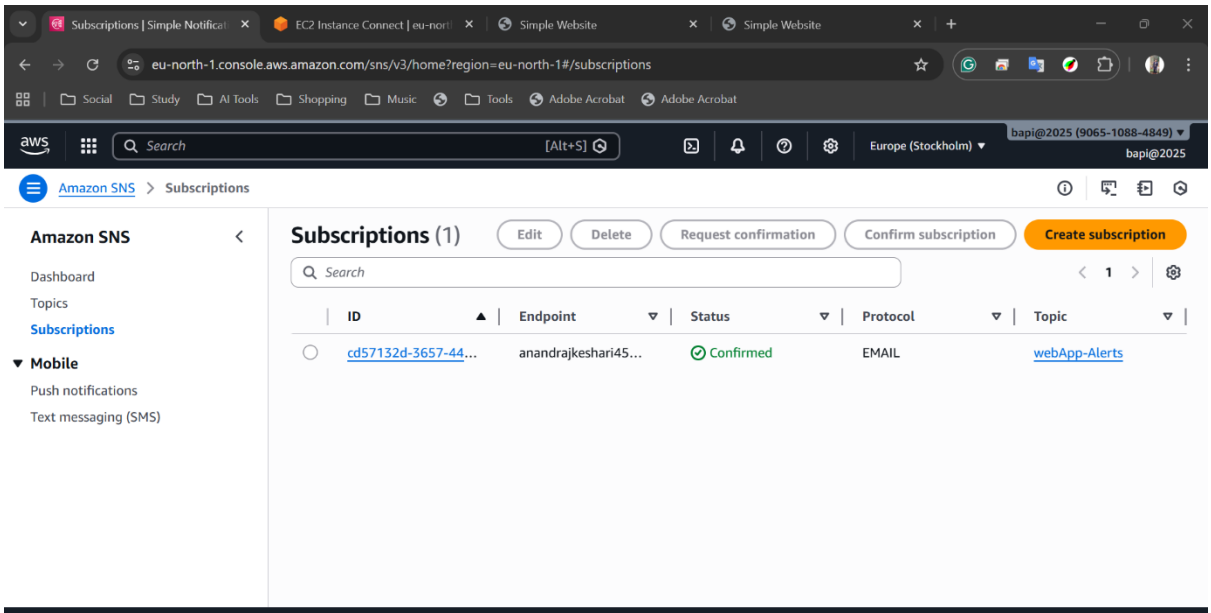
Step 10: Create SNS Topic

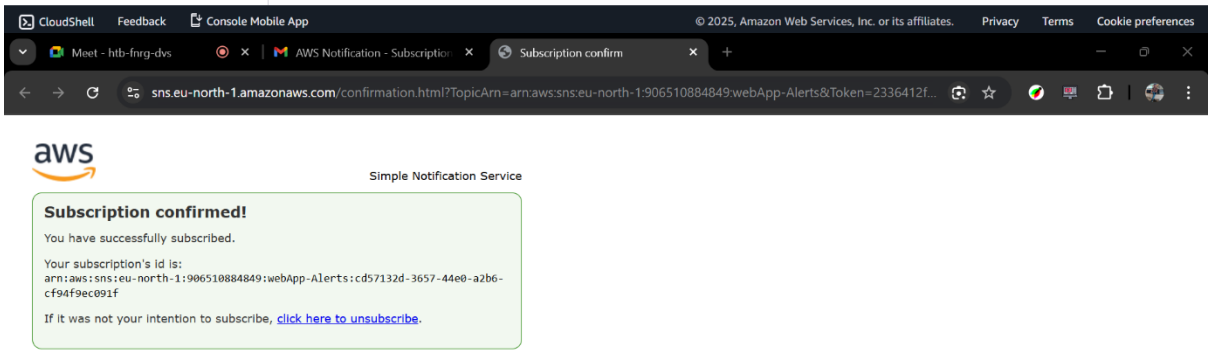
- Go to SNS → Topics
- Click Create topic
- Type: Standard
- Name: **webapp-alerts**
- Create topic



Step 11: Subscribe to SNS Topic

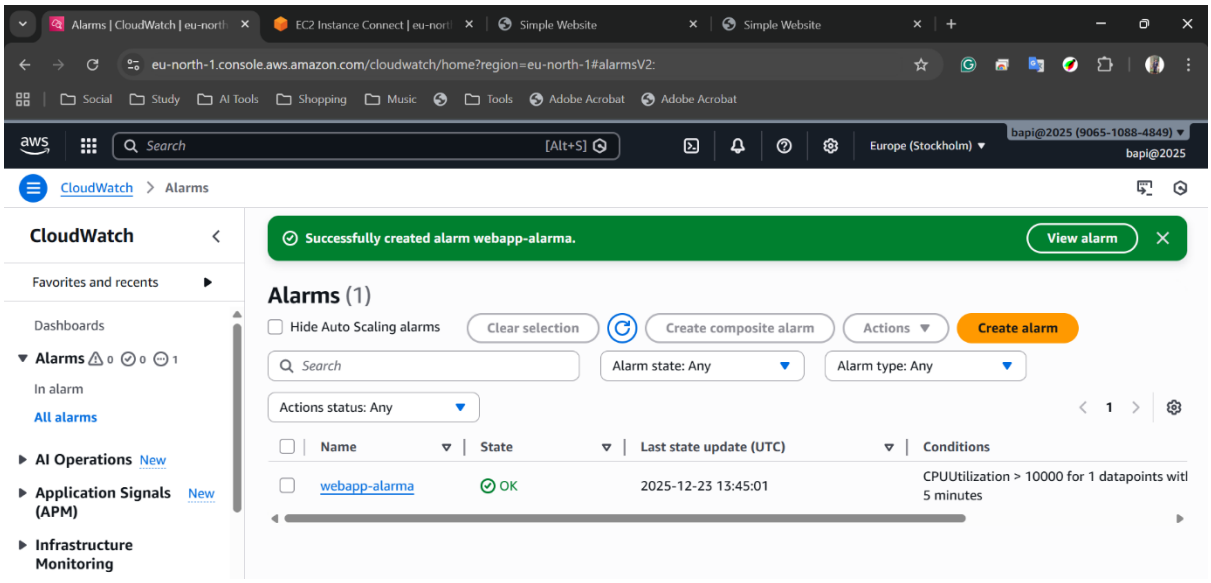
- Open webapp-alerts
- Click Create subscription
- Protocol: Email
- Endpoint: your email address → dishahota23@gmail.com
- Confirm subscription from email





Step 12: Connect SNS with Monitoring

- Go to CloudWatch
- Create alarm (example):
- EC2 CPU utilization > 80%
- Set alarm action → SNS topic
- Save alarm



Step 13: Test the Application

- Copy EC2 public IP → **16.170.223.116**
- Paste into browser → Web page loads
- Stop EC2 instance → verify SNS alert (if alarm configured)
- Check S3 uploads