

Task 2

Objective: EC2 Static Website Hosting Task

Steps Performed:

1. EC2 Instance Setup:

- Launched a **Free Tier EC2 instance** (Amazon Linux 2023) in a public subnet.
- Created a **key pair** for SSH access.
- Configured **security group** to allow HTTP (80), HTTPS (443), and SSH (22) access.

2. Nginx Installation & Configuration:

- Installed Nginx using: sudo dnf install nginx -y.
- Enabled and started the Nginx service.
- Confirmed Nginx was running on port 80.

3. Static Website Deployment:

- Prepared a **resume website** (index.html, style.css, profile.jpg).
- Uploaded the website files to EC2 using scp.
- Moved files to /usr/share/nginx/html/ and set proper permissions.
- Restarted Nginx to serve the site.

4. Hardening & Best Practices:

- Restricted SSH access to specific IP addresses (where possible).
- Applied OS updates using sudo dnf update -y.
- Ensured file permissions followed the least-privilege principle.

Outcome:

- The resume website is successfully hosted and accessible via the public IP:
<http://40.192.119.95/>
- Nginx is serving the static site reliably.

EC2 Instance

The screenshot shows the AWS EC2 Instances page. The left sidebar includes options like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, and AMI Catalog. The main content area displays one instance: i-05dfda7b41982fb0c, which is running and has an instance type of t3.micro. It lists Public IPv4 (40.192.119.95), Private IP DNS name (ip-172-31-0-174.ap-south-2.compute.internal), and a Public DNS (ec2-40-192-119-95.ap-south-2.compute.amazonaws.com). The bottom of the page includes CloudShell, Feedback, and Console Mobile App links.

Security Group screenshot

The screenshot shows the AWS Security Groups page. The left sidebar includes Options, Instances (selected), Images, and Elastic Block Store. The main content area shows the sg-0fd6a53b5ef73d3b8 security group, which was created by launch-wizard-1. It has 3 inbound rules: one for HTTP (port 80), one for SSH (port 22), and one for HTTPS (port 443). The bottom of the page includes CloudShell, Feedback, and Console Mobile App links.

Browser screenshot of the resume website

