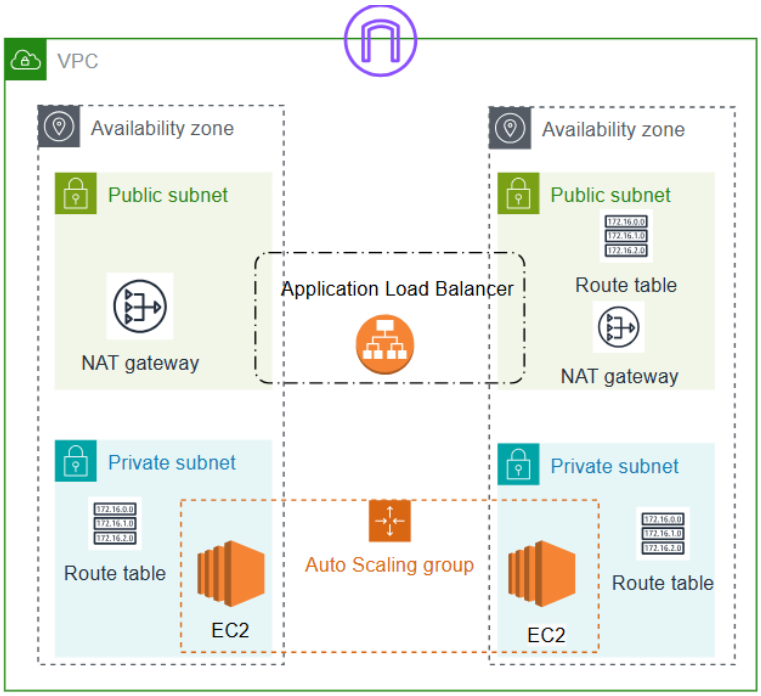
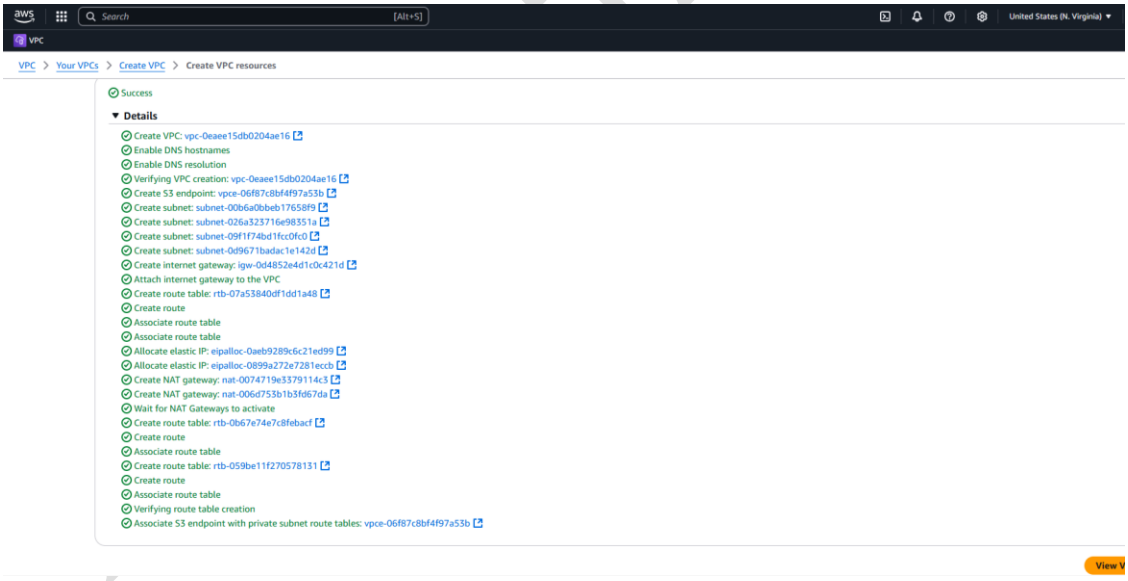
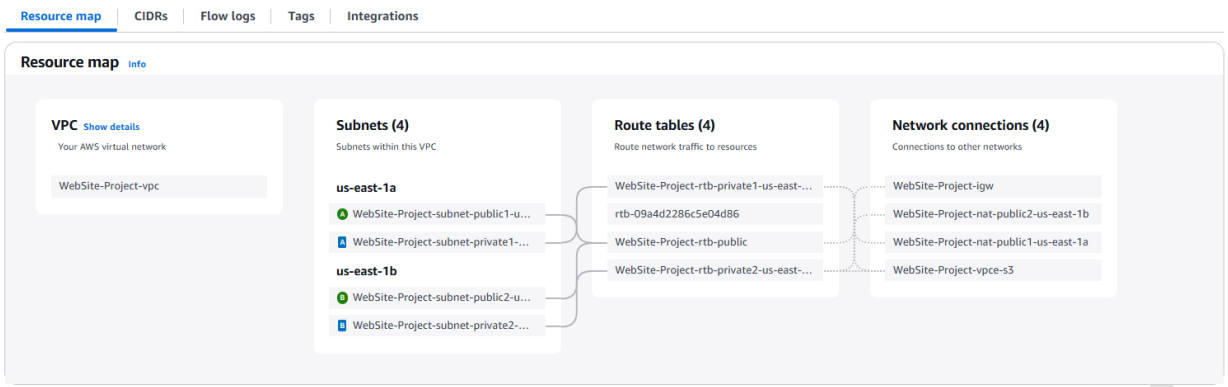
AWS Secure Website Project



Created By ***Ajitpal Singh Sidhu***

1) Create VPC





2) Create two subnets (Two Private ,Two Public)

Subnets (4/10) Info

Find resources by attribute or tag

Name	Subnet ID	State	VPC
WebSite-Project-subnet-private2-us-ea...	subnet-0d9671badac1e142d	Available	vpc-0eaee15db0204ae16 | Web...
WebSite-Project-subnet-private1-us-ea...	subnet-09f1f74bd1fcc0fc0	Available	vpc-0eaee15db0204ae16 | Web...
WebSite-Project-subnet-public1-us-eas...	subnet-00b6a0bbeb17658f9	Available	vpc-0eaee15db0204ae16 | Web...
–	subnet-070f5bf497c402d0a	Available	vpc-0a224c52cb20f24b0
WebSite-Project-subnet-public2-us-eas...	subnet-026a323716e98351a	Available	vpc-0eaee15db0204ae16 | Web...

3) Create Three route tables (one for public and two for private)

rtb-07a53840df1dd1a48 / WebSite-Project-rtb-public Actions

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-07a53840df1dd1a48	No	2 subnets	–

VPC: vpc-0eaee15db0204ae16 | WebSite-Project-vpc

Owner ID:

Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (2) Edit subnet associations

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
WebSite-Project-subnet-public1-us-east-1a	subnet-00b6a0bbeb17658f9	10.0.0.0/20	–
WebSite-Project-subnet-public2-us-east-1b	subnet-026a323716e98351a	10.0.16.0/20	–

4) Configure route table for subnets

rtb-07a53840df1dd1a48 / WebSite-Project-rtb-public Actions

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-07a53840df1dd1a48	No	2 subnets	–

VPC: vpc-0eaee15db0204ae16 | WebSite-Project-vpc

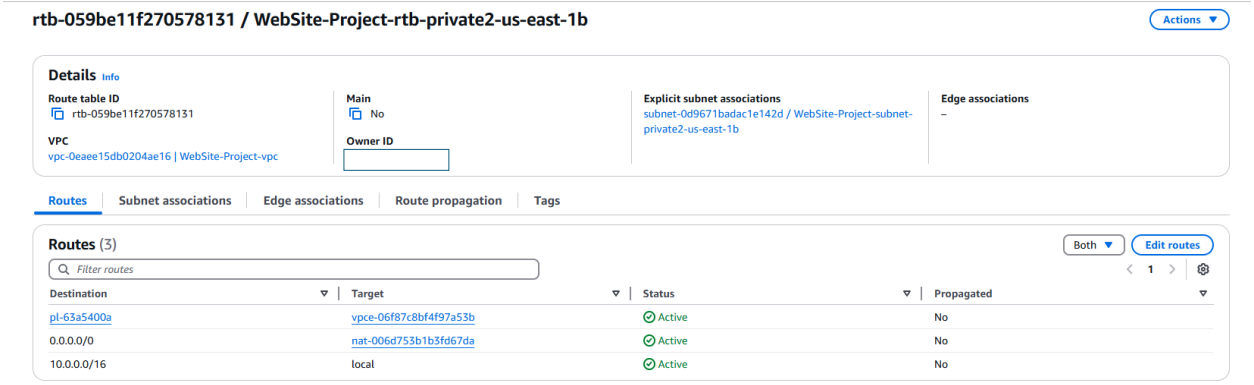
Owner ID:

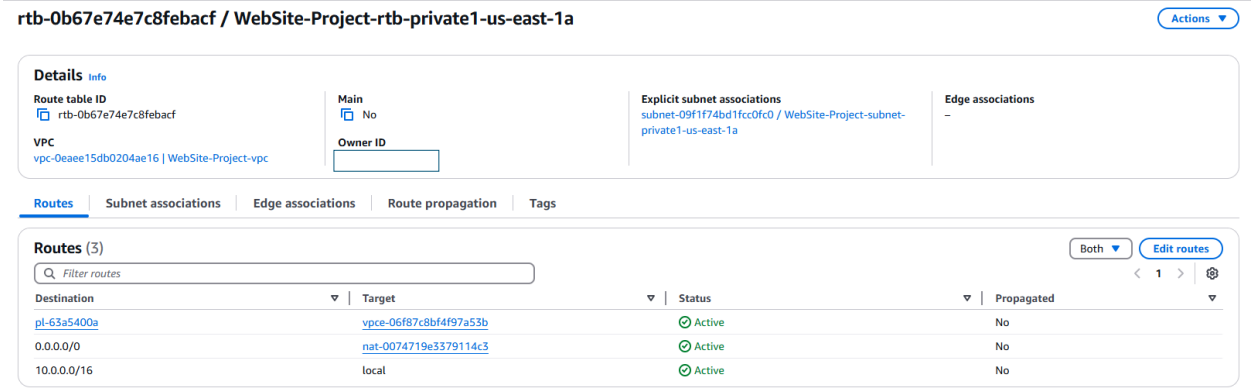
Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2) Both Edit routes

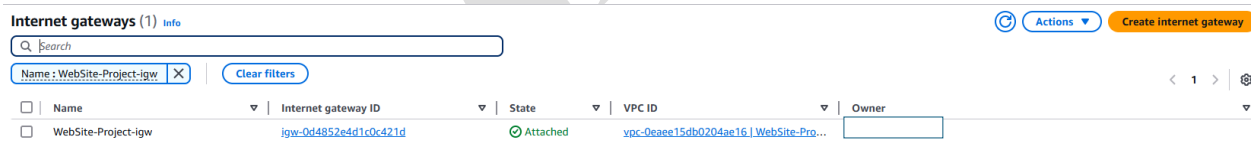
Filter routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0d4852e4d1c0c421d	Active	No
10.0.0.0/16	local	Active	No

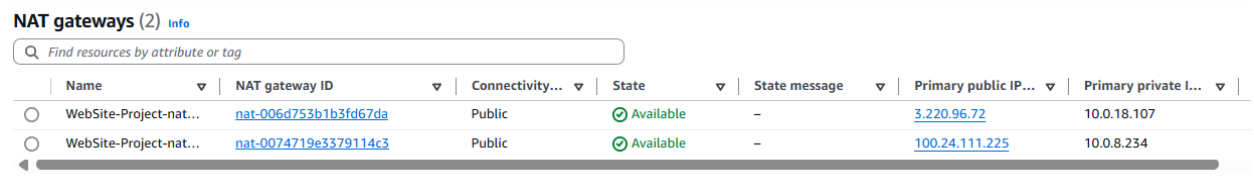


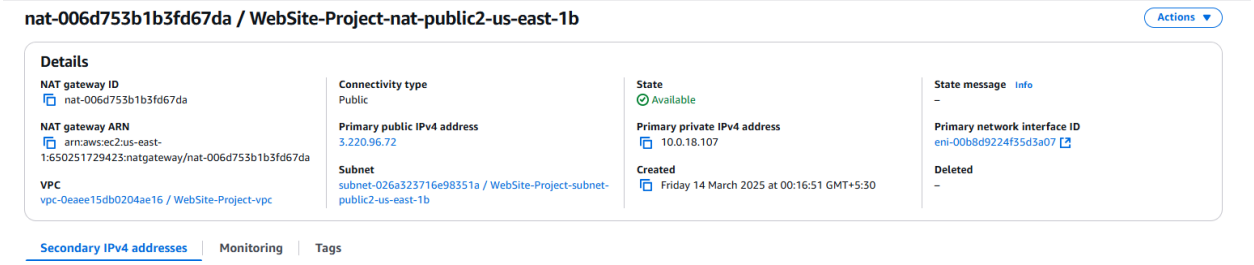


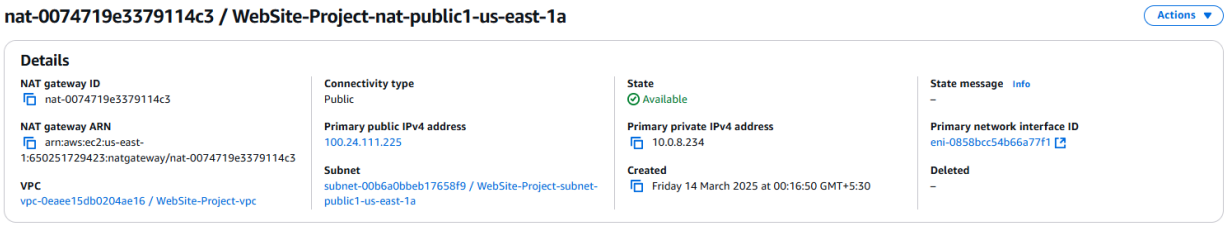
5) Create Internet Gateway for attach to VPC



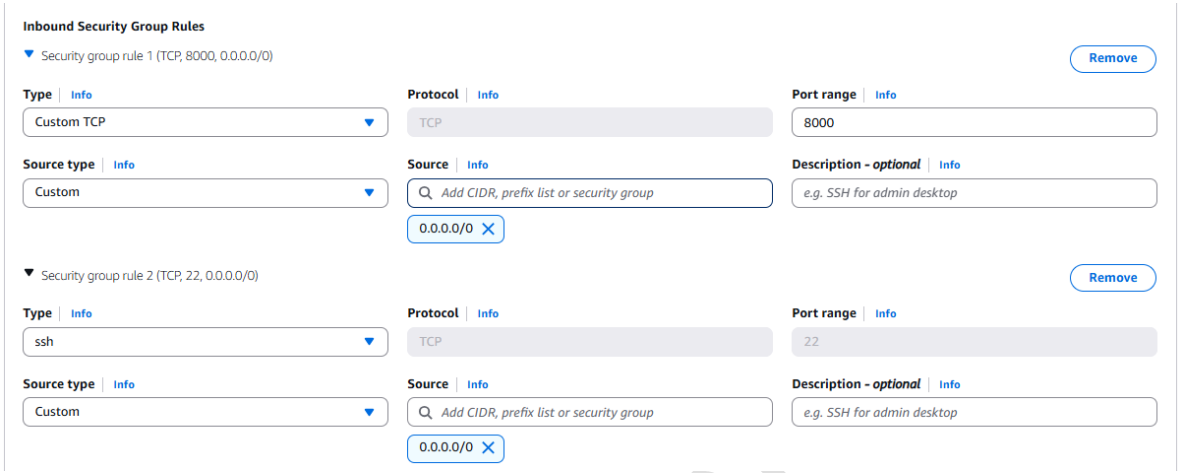
6) Create Nat Gateway and attach to each private subnet



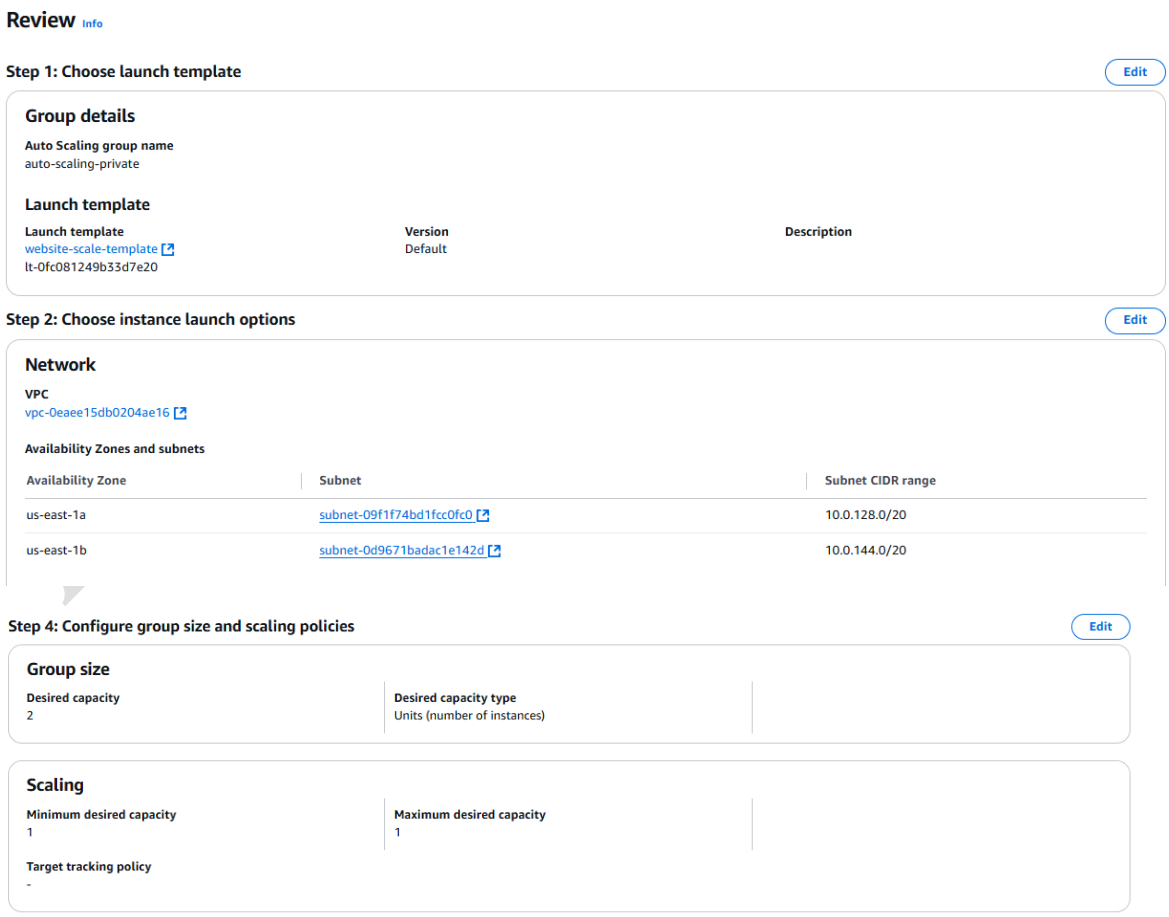


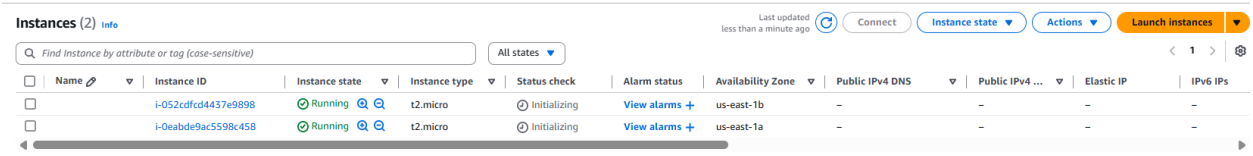


7) Security Group settings in Auto Scaling

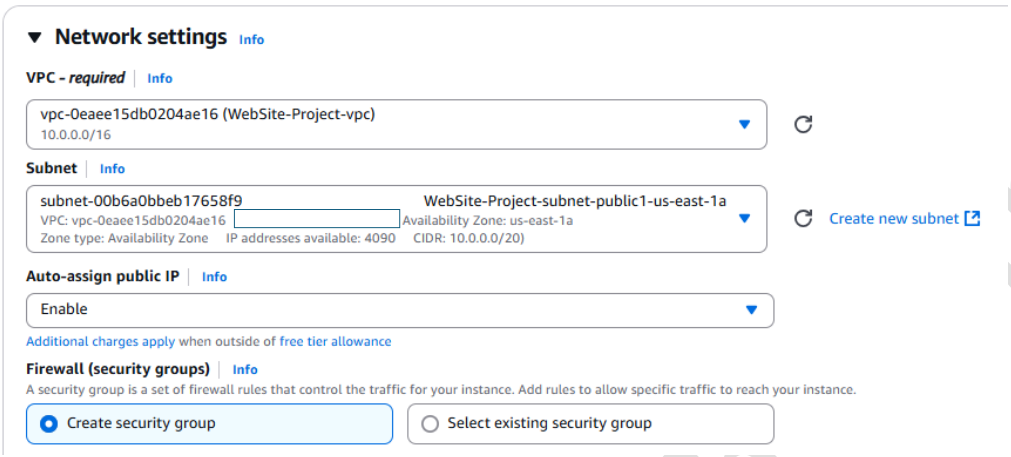


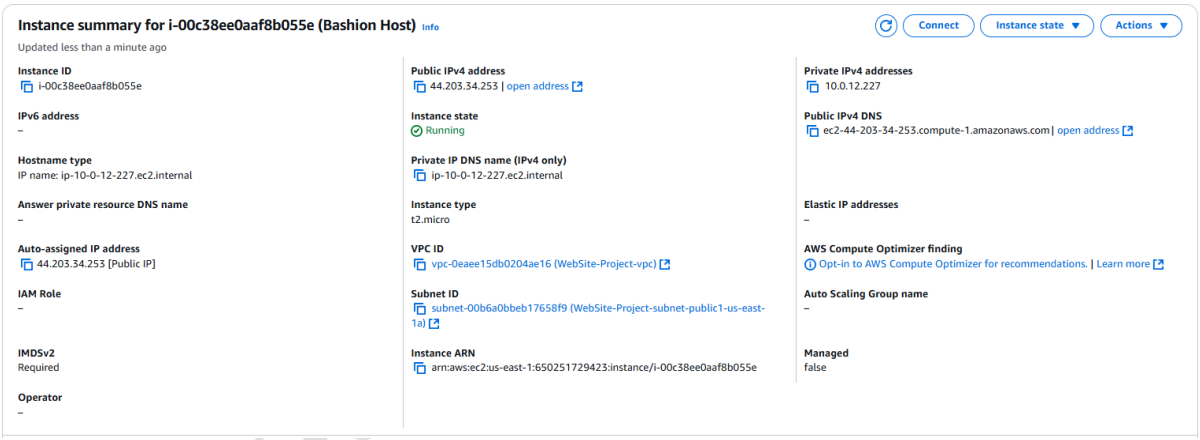
8) Create Template for Auto Scaling Group





9) Create Bastion Host (in same VPC)





10) Copy Private Key to bastion host and SSH to Bastion Host

For SCP (Secure Copy):

Format: scp -i key file remote_username<IP>

scp -i /Users/ajit/Downloads/EC2_Instance.pem /Users/ ajit /Downloads/ EC2_Instance.pem ec2-user@44.203.34.253:/home/ec2-user
(default username in Amazon AMI is ***ec2-user***)

```
C:                >scp -i              \EC2_Instance.pem              \EC2_Instance.pem ec2-user@44.203.34.253:/home/ec2-user
The authenticity of host '44.203.34.253 (44.203.34.253)' can't be established.
ED25519 key fingerprint is SHA256
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Warning: Permanently added '44.203.34.253' (ED25519) to the list of known hosts.
EC2_Instance.pem                                              100% 1674     5.7KB/s   00:00
```

```
C:[redacted]>ssh -i D:\Work\AWS\EC2_Instance.pem ec2-user@44.203.34.253
       #_
   ,     ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-12-227 ~]$ ls
EC2_Instance.pem
```

11)SSH to one of EC2 server in private subnet

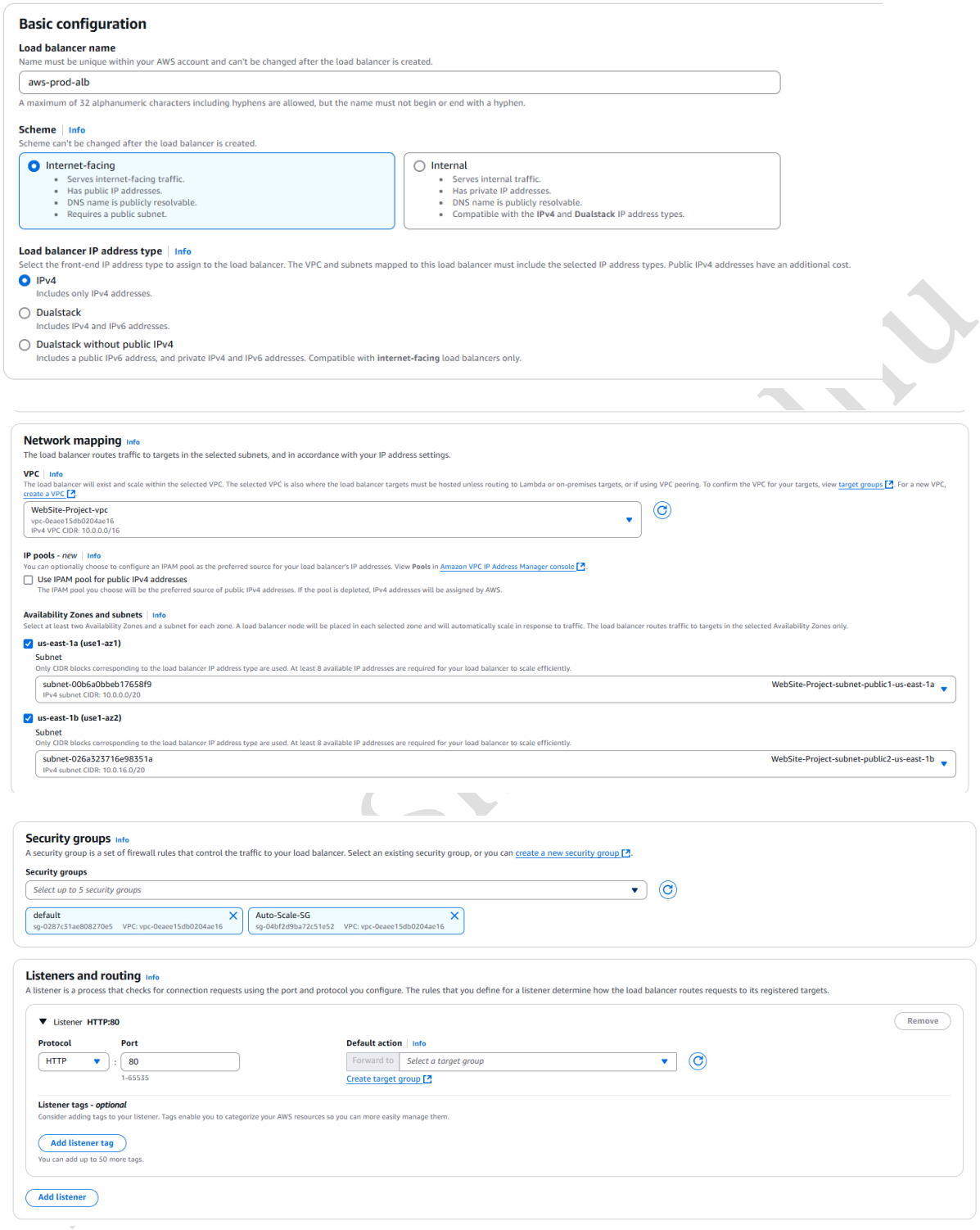
```
[ec2-user@ip-10-0-12-227 ~]$ chmod 400 EC2_Instance.pem
[ec2-user@ip-10-0-12-227 ~]$ ssh -i EC2_Instance.pem ec2-user@10.0.156.191
       #_
   ,     ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-156-191 ~]$
```

12) Setup Website in EC2 server in private subnet

```
[ec2-user@ip-10-0-156-191 ~]$ vim demo.html
"demo.html" [New] 10L, 146B written
[ec2-user@ip-10-0-156-191 ~]$ cat demo.html
<!DOCTYPE html>
<html>
<head>
<title>Happy Holi</title>
</head>
<body>

<h1>This is an AWS Demo Production in Private Subnet</h1>
</body>
</html>
[ec2-user@ip-10-0-156-191 ~]$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

13) Create Load Balancer



14) Create Target Group consisting of private EC2

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

- (•) Instances
  - Supports load balancing to instances within a specific VPC.
  - Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity.
- ( ) IP addresses
  - Supports load balancing to VPC and on-premises resources.
  - Facilitates routing to multiple IP addresses and network interfaces on the same instance.
  - Offers flexibility with microservice based architectures, simplifying inter-application communication.
  - Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.
- ( ) Lambda function
  - Facilitates routing to a single Lambda function.
  - Accessible to Application Load Balancers only.
- ( ) Application Load Balancer
  - Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
  - Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

PrivateEc2target

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP : 8000

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

- (•) IPv4
  Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.
- ( ) IPv6
  Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). Learn more

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

WebSite-Project-vpc
vpc-0eaee15db0204ae16
IPv4 VPC CIDR: 10.0.0.0/16

0 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

8000

1-65535 (separate multiple ports with commas)

Include as pending below

2 selections are now pending below. Include more or register targets when ready.

Review targets

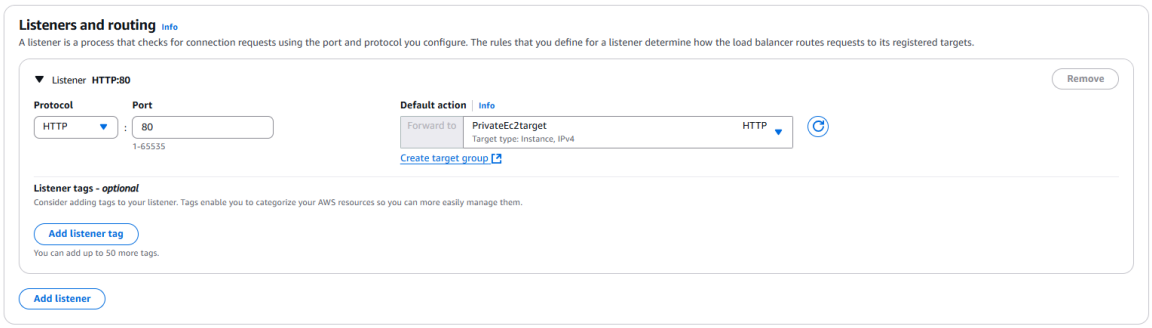
Targets (2)

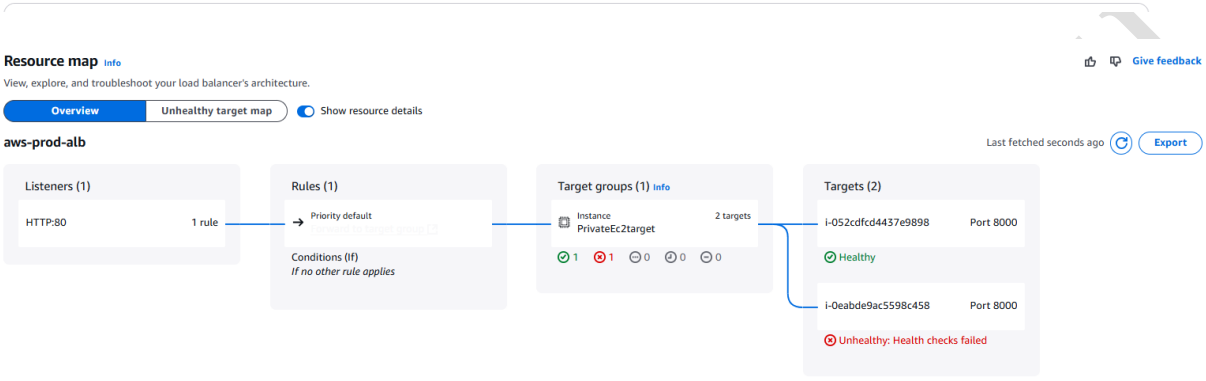
Remove all pending

Filter targets | Show only pending | 1

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-052cdfcd4437e9898		8000	Running	Auto-Scale-SG	us-east-1b	10.0.156.191	subnet-0d9671badac1e142d	March 14, 2025, 01:05 (UTC+05:30)
i-0eabde9ac5598c458		8000	Running	Auto-Scale-SG	us-east-1a	10.0.136.127	subnet-09f1f74bd1fcc0fc0	March 14, 2025, 01:05 (UTC+05:30)

Back to ***load balancer Screen***

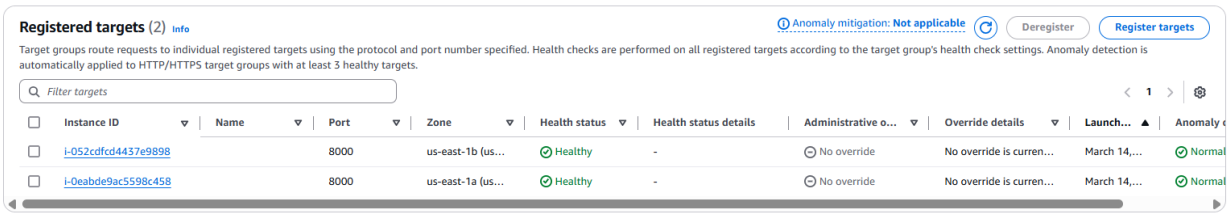




Security Group for Load Balancer: Ports-80,8000

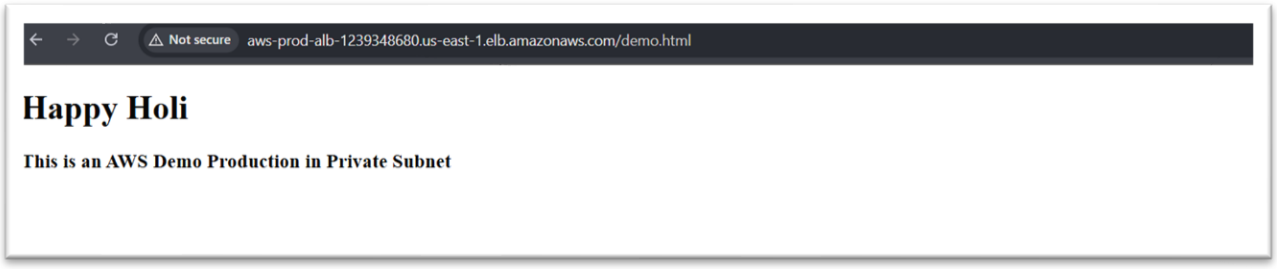
Security Group for Auto Scaling:Ports-*22,8000*

When both EC2 Servers are Live

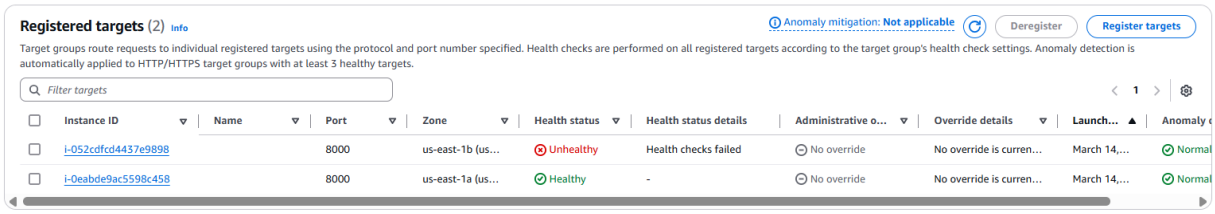



```
[ec2-user@ip-10-0-136-127 ~]$  python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.18.54 - - [13/Mar/2025 21:05:57] "GET / HTTP/1.1" 200 -
10.0.9.120 - - [13/Mar/2025 21:06:10] "GET / HTTP/1.1" 200 -
```

```
[ec2-user@ip-10-0-156-191 ~]$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.0.9.120 - - [13/Mar/2025 20:45:09] "GET / HTTP/1.1" 200 -
10.0.18.54 - - [13/Mar/2025 20:45:26] "GET / HTTP/1.1" 200 -
```



When One of Server is down



Connect with me on LinkedIn: *Click Here*