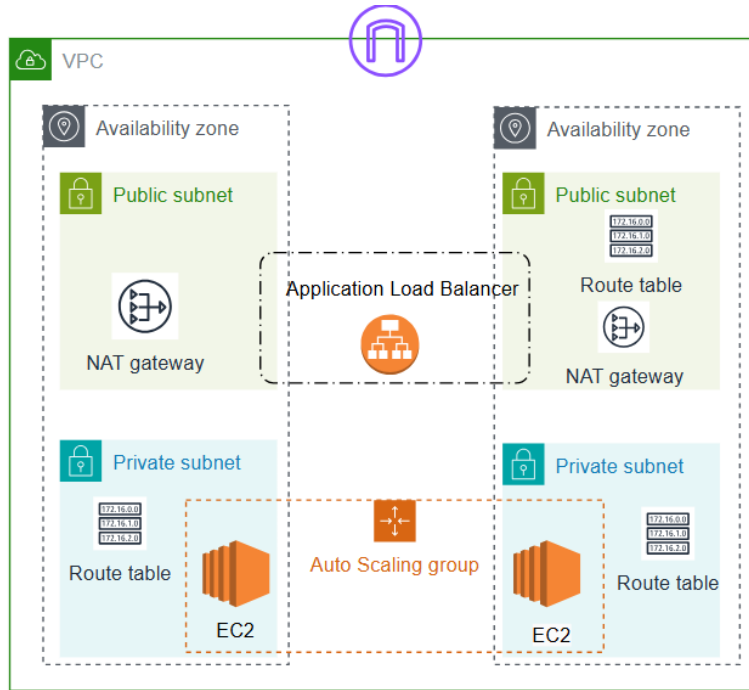


AWS Secure Website Project



Created By **Ajitpal Singh Sidhu**

1) Create VPC

aws [Alt+S] United States (N. Virginia)

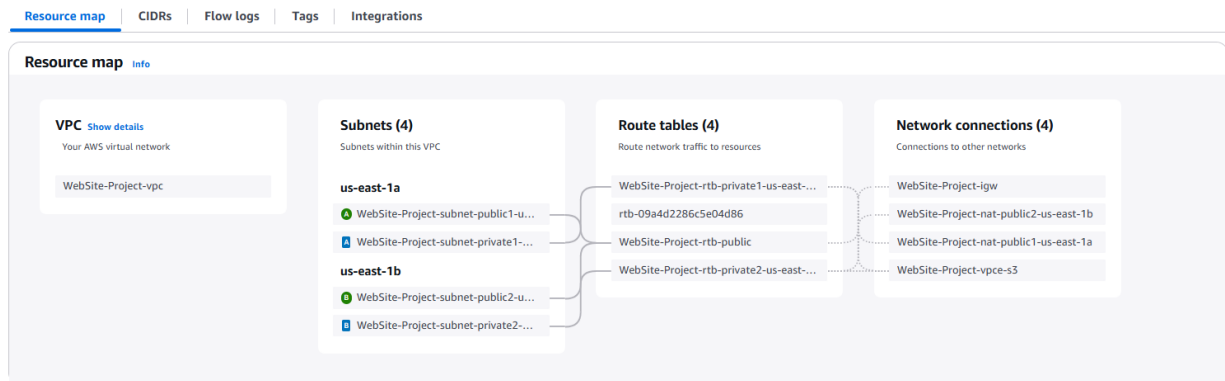
VPC > Your VPCs > Create VPC > Create VPC resources

Success

Details

- ✔ Create VPC: vpc-0eae15db0204ae16
- ✔ Enable DNS hostnames
- ✔ Enable DNS resolution
- ✔ Verifying VPC creation: vpc-0eae15db0204ae16
- ✔ Create S3 endpoint: vpce-06f87c8bf4f97a53b
- ✔ Create subnet: subnet-00b6a0bbeb17658f9
- ✔ Create subnet: subnet-026a323716e98351a
- ✔ Create subnet: subnet-09f1f74bd1fcc0f0c
- ✔ Create subnet: subnet-0d9671badac1e142d
- ✔ Create internet gateway: igw-9d4852e4d10c421d
- ✔ Attach internet gateway to the VPC
- ✔ Create route table: rtb-07a53840df1dd1a48
- ✔ Create route
- ✔ Associate route table
- ✔ Associate route table
- ✔ Allocate elastic IP: eipalloc-0aeb9289c6c21ed99
- ✔ Allocate elastic IP: eipalloc-0899a272e7281ecb
- ✔ Create NAT gateway: nat-0074719e3379114c3
- ✔ Create NAT gateway: nat-006d753b1b3f067da
- ✔ Wait for NAT gateways to activate
- ✔ Create route table: rtb-0b67e74e7c8febadf
- ✔ Create route
- ✔ Associate route table
- ✔ Create route table: rtb-059be11f270578131
- ✔ Create route
- ✔ Associate route table
- ✔ Verifying route table creation
- ✔ Associate S3 endpoint with private subnet route tables: vpce-06f87c8bf4f97a53b

View



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

Subnets (4/10) Info

Find resources by attribute or tag

	Name	Subnet ID	State	VPC
<input checked="" type="checkbox"/>	WebSite-Project-subnet-private2-us-east-1b	subnet-0d9671badac1e142d	Available	vpc-0eae15db0204ae16 WebSite-Project-vpc
<input checked="" type="checkbox"/>	WebSite-Project-subnet-private1-us-east-1a	subnet-09f1f74bd1fcc0fc0	Available	vpc-0eae15db0204ae16 WebSite-Project-vpc
<input checked="" type="checkbox"/>	WebSite-Project-subnet-public1-us-east-1a	subnet-00b6a0bbeb17658f9	Available	vpc-0eae15db0204ae16 WebSite-Project-vpc
<input type="checkbox"/>	-	subnet-070f5bf497c402d0a	Available	vpc-0a224c52cb20f24b0
<input checked="" type="checkbox"/>	WebSite-Project-subnet-public2-us-east-1b	subnet-026a323716e98351a	Available	vpc-0eae15db0204ae16 WebSite-Project-vpc

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

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

Actions

Details Info

Route table ID
[rtb-07a53840df1dd1a48](#)

VPC
[vpc-0eae15db0204ae16 | WebSite-Project-vpc](#)

Main
☒ No

Owner ID

Explicit subnet associations
2 subnets

Edge associations
-

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
[rtb-07a53840df1dd1a48](#)

VPC
[vpc-0eae15db0204ae16 | WebSite-Project-vpc](#)

Main
☒ No

Owner ID

Explicit subnet associations
2 subnets

Edge associations
-

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

Details

Route table ID

rtb-059be11f270578131

VPC

vpc-0eae15db0204ae16 / WebSite-Project-vpc

Main

No

Owner ID

Explicit subnet associations

subnet-0d9671badac1e142d / WebSite-Project-subnet-private2-us-east-1b

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (3)

Filter routes

Both

Edit routes

Destination	Target	Status	Propagated
pl-63a5400a	vpce-06f87c8bf4f97a53b	Active	No
0.0.0.0/0	nat-006d753b1b3fd67da	Active	No
10.0.0.0/16	local	Active	No

Details

Route table ID

rtb-0b67e74e7c8febaf

VPC

vpc-0eae15db0204ae16 / WebSite-Project-vpc

Main

No

Owner ID

Explicit subnet associations

subnet-09f1f74bd1fcc0fc0 / WebSite-Project-subnet-private1-us-east-1a

Edge associations

-

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (3)

Filter routes

Both

Edit routes

Destination	Target	Status	Propagated
pl-63a5400a	vpce-06f87c8bf4f97a53b	Active	No
0.0.0.0/0	nat-0074719e3379114c3	Active	No
10.0.0.0/16	local	Active	No

5) Create Internet Gateway for attach to VPC

Internet gateways (1)

Search



Actions

Create internet gateway

Name: WebSite-Project-igw

Clear filters

Name	Internet gateway ID	State	VPC ID	Owner
WebSite-Project-igw	igw-0d4852e4d1c0c421d	Attached	vpc-0eae15db0204ae16 / WebSite-Pro...	

6) Create Nat Gateway and attach to each private subnet

NAT gateways (2)

Find resources by attribute or tag

	Name	NAT gateway ID	Connectivity...	State	State message	Primary public IP...	Primary private I...
<input type="radio"/>	WebSite-Project-nat...	nat-006d753b1b3fd67da	Public	Available	-	3.220.96.72	10.0.18.107
<input type="radio"/>	WebSite-Project-nat...	nat-0074719e3379114c3	Public	Available	-	100.24.111.225	10.0.8.234

Details

NAT gateway ID

nat-006d753b1b3fd67da

NAT gateway ARN

arn:aws:ec2:us-east-1:650251729423:natgateway/nat-006d753b1b3fd67da

VPC

vpc-0eae15db0204ae16 / WebSite-Project-vpc

Connectivity type

Public

Primary public IPv4 address

3.220.96.72

Subnet

subnet-026a323716e98351a / WebSite-Project-subnet-public2-us-east-1b

State

Available

Primary private IPv4 address

10.0.18.107

Created

Friday 14 March 2025 at 00:16:51 GMT+5:30

State message

-

Primary network interface ID

eni-00b8d9224f5d3a07

Deleted

-

Secondary IPv4 addresses

Monitoring

Tags

Details

NAT gateway ID

nat-0074719e3379114c3

NAT gateway ARN

arn:aws:ec2:us-east-1:650251729423:natgateway/nat-0074719e3379114c3

VPC

vpc-0eae15db0204ae16 / WebSite-Project-vpc

Connectivity type

Public

Primary public IPv4 address

100.24.111.225

Subnet

subnet-00b6a0bbeb17658f9 / WebSite-Project-subnet-public1-us-east-1a

State

Available

Primary private IPv4 address

10.0.8.234

Created

Friday 14 March 2025 at 00:16:50 GMT+5:30

State message

Info

-

Primary network interface ID

eni-0858bcc54b66a77f1

Deleted

-

7) Security Group settings in Auto Scaling

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 8000, 0.0.0.0/0)

Type

Info

Custom TCP

Source type

Info

Custom

Protocol

Info

TCP

Source

Info

0.0.0.0/0

Port range

Info

8000

Description - optional

Info

e.g. SSH for admin desktop

Remove

▼ Security group rule 2 (TCP, 22, 0.0.0.0/0)

Type

Info

ssh

Source type

Info

Custom

Protocol

Info

TCP

Source

Info

0.0.0.0/0

Port range

Info

22

Description - optional

Info

e.g. SSH for admin desktop

Remove

8) Create Template for Auto Scaling Group

Review

Step 1: Choose launch template

Edit

Group details

Auto Scaling group name
auto-scaling-private

Launch template

Launch template
website-scale-template
lt-0fc081249b33d7e20**Version**
Default**Description**

Step 2: Choose instance launch options

Edit

Network

VPC

vpc-0eae15db0204ae16

Availability Zones and subnets

Availability Zone	Subnet	Subnet CIDR range
us-east-1a	subnet-09f1f74bd1fcc0fc0	10.0.128.0/20
us-east-1b	subnet-0d9671badac1e142d	10.0.144.0/20

Step 4: Configure group size and scaling policies

Edit

Group size

Desired capacity
2**Desired capacity type**
Units (number of instances)

Scaling

Minimum desired capacity
1**Maximum desired capacity**
1**Target tracking policy**
-

Instances (2) [Info](#)

Find instance by attribute or tag (case-sensitive) [All states](#)

Last updated less than a minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
<input type="checkbox"/>		i-052cdfcd4437e9898	Running	t2.micro	Initializing	View alarms	us-east-1b	-	-	-	-
<input type="checkbox"/>		i-0eabde9ac5598c458	Running	t2.micro	Initializing	View alarms	us-east-1a	-	-	-	-

9) Create Bastion Host (in same VPC)

Network settings [Info](#)

VPC - required [Info](#)

vpc-0eae15db0204ae16 (WebSite-Project-vpc)
10.0.0.0/16

Subnet [Info](#)

subnet-00b6a0bbeb17658f9 WebSite-Project-subnet-public1-us-east-1a
VPC: vpc-0eae15db0204ae16 Availability Zone: us-east-1a
Zone type: Availability Zone IP addresses available: 4090 CIDR: 10.0.0.0/20

Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Instance summary for i-00c38ee0aaf8b055e (Bashion Host) [Info](#)

Updated less than a minute ago [Connect](#) [Instance state](#) [Actions](#)

Instance ID i-00c38ee0aaf8b055e	Public IPv4 address 44.203.34.253 open address	Private IPv4 addresses 10.0.12.227
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-44-203-34-253.compute-1.amazonaws.com open address
Hostname type IP name: ip-10-0-12-227.ec2.internal	Private DNS name (IPv4 only) ip-10-0-12-227.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 44.203.34.253 [Public IP]	VPC ID vpc-0eae15db0204ae16 (WebSite-Project-vpc)	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-00b6a0bbeb17658f9 (WebSite-Project-subnet-public1-us-east-1a)	Managed false
IMDSv2 Required	Instance ARN arn:aws:ec2:us-east-1:650251729423:instance/i-00c38ee0aaf8b055e	
Operator -		

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
```

The screenshot shows the following terminal session:

```
#_  
~\_ ##### Amazon Linux 2023  
~~ \_#####\  
~~ \###|  
~~ \|/  
~~ V'-'> https://aws.amazon.com/linux/amazon-linux-2023  
   ^  
  ^.  
 _./_.  
-/ /  
_/m/' /
```

This indicates a successful SSH connection to an Amazon Linux 2023 instance.

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

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

aws-prod-alb

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

Scheme | Info

Scheme can't be changed after the load balancer is created.

☒ Internet-facing

- Serves Internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

☐ Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name is publicly resolvable.
- Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type | Info

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

☒ IPv4

Includes only IPv4 addresses.

☐ Dualstack

Includes IPv4 and IPv6 addresses.

☐ Dualstack without public IPv4

Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **Internet-facing** load balancers only.

Network mapping | Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC | Info

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#). For a new VPC, [create a VPC](#).

WebSite-Project-vpc
vpc-0eae115db0204ae16
IPv4 VPC CIDR: 10.0.0.0/16

IP pools | new | Info

You can optionally choose to configure an IPAM pool as the preferred source for your load balancer's IP addresses. View [Pools](#) in [Amazon VPC IP Address Manager console](#).

☐ Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted, IPv4 addresses will be assigned by AWS.

Availability Zones and subnets | Info

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

☒ us-east-1a (use1-az1)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-00b6a0bbeb17658f9
IPv4 subnet CIDR: 10.0.0.0/20

WebSite-Project-subnet-public1-us-east-1a

☒ us-east-1b (use1-az2)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-026a323716e98351a
IPv4 subnet CIDR: 10.0.16.0/20

WebSite-Project-subnet-public2-us-east-1b

Security groups | Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups

default
sg-0287c31ae808270e5 VPC: vpc-0eae115db0204ae16

Auto-Scale-SG
sg-04bf2d9ba72c51e52 VPC: vpc-0eae115db0204ae16

Listeners and routing | Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Remove

Protocol

HTTP

Port

80

1-65535

Default action | Info

Forward to

Select a target group

[Create target group](#)

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

[Add listener tag](#)

You can add up to 50 more tags.

[Add listener](#)

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

Private: c2target

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-0e0ee15db0204ae16

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)

Filter targets

Show only pending

Remove all pending

< 1 > ⚙

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
i-052cdffd4437e9898		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

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Protocol

HTTP

Port

80

1-65535

Default action

Forward to

PrivateEc2target

HTTP

Target type: Instance, IPv4

[Create target group](#)

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add listener tag

You can add up to 50 more tags.

Add listener



Security Group for Load Balancer: Ports-80,8000

Security Group for Auto Scaling: Ports-22,8000

When both EC2 Servers are Live

Registered targets (2) [Info](#)

Anomaly mitigation: **Not applicable** [Deregister](#) [Register targets](#)

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Filter targets

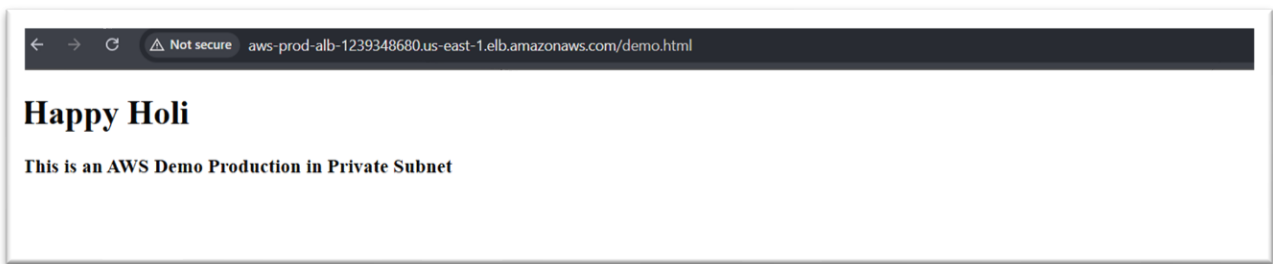
<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Administrative o...	Override details	Launch...	Anomaly
<input type="checkbox"/>	i-052cdfcd4437e9898		8000	us-east-1b (us...)	Healthy	-	No override	No override is curren...	March 14,...	Normal
<input type="checkbox"/>	i-0eabde9ac5598c458		8000	us-east-1a (us...)	Healthy	-	No override	No override is curren...	March 14,...	Normal

```
[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 -
```

← → ↺ **Not secure** aws-prod-alb-1239348680.us-east-1.elb.amazonaws.com/demo.html

This is an AWS Demo Production in Private Subnet



When One of Server is down

Registered targets (2) [Info](#) Anomaly mitigation: **Not applicable** Deregister Register targets

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

Filter targets

<input type="checkbox"/>	Instance ID	Name	Port	Zone	Health status	Health status details	Administrative o...	Override details	Launch...	Anomaly c
<input type="checkbox"/>	i-052c0fcd4437e9898		8000	us-east-1b (us...	Unhealthy	Health checks failed	No override	No override is curren...	March 14,...	Normal
<input type="checkbox"/>	i-0eabde9ac5598c458		8000	us-east-1a (us...	Healthy	-	No override	No override is curren...	March 14,...	Normal

Connect with me on LinkedIn: [Click Here](#)