

## Lesson 03 Demo 07

### Configuring an Application Load Balancer

**Objective:** To demonstrate the process of setting up and testing an Application Load Balancer in AWS

**Tools required:** AWS Management Console, AWS EC2, and web browser

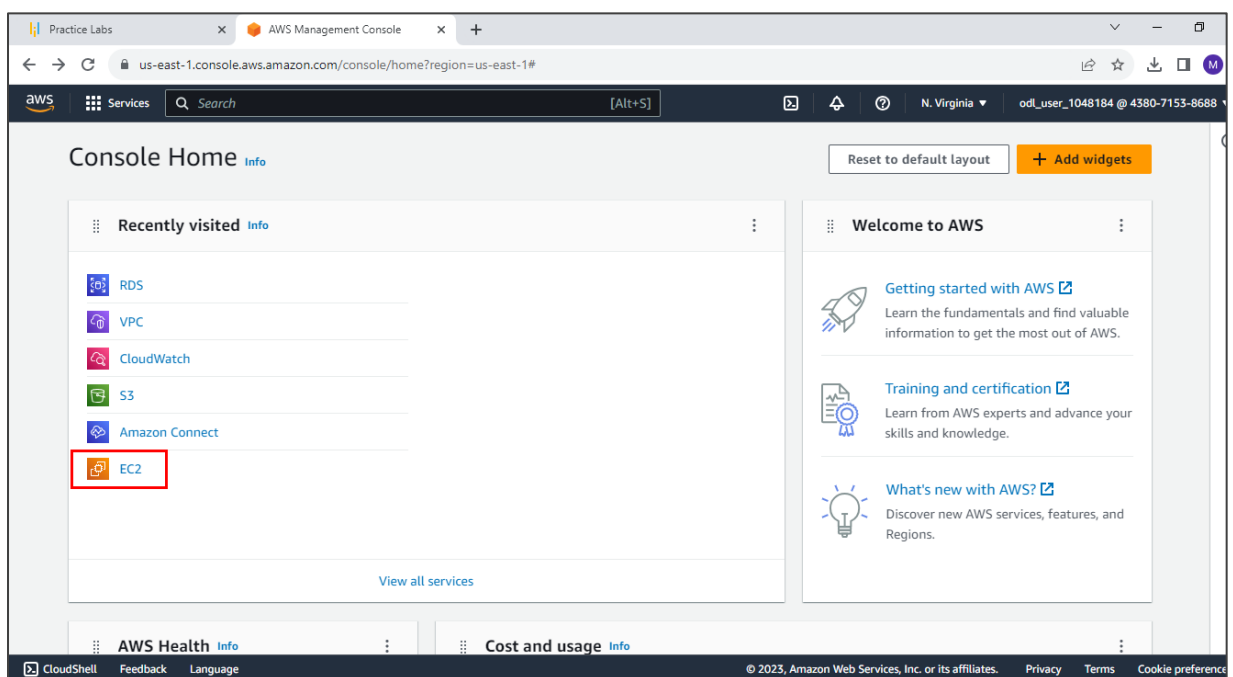
**Prerequisites:** None

Steps to be followed:

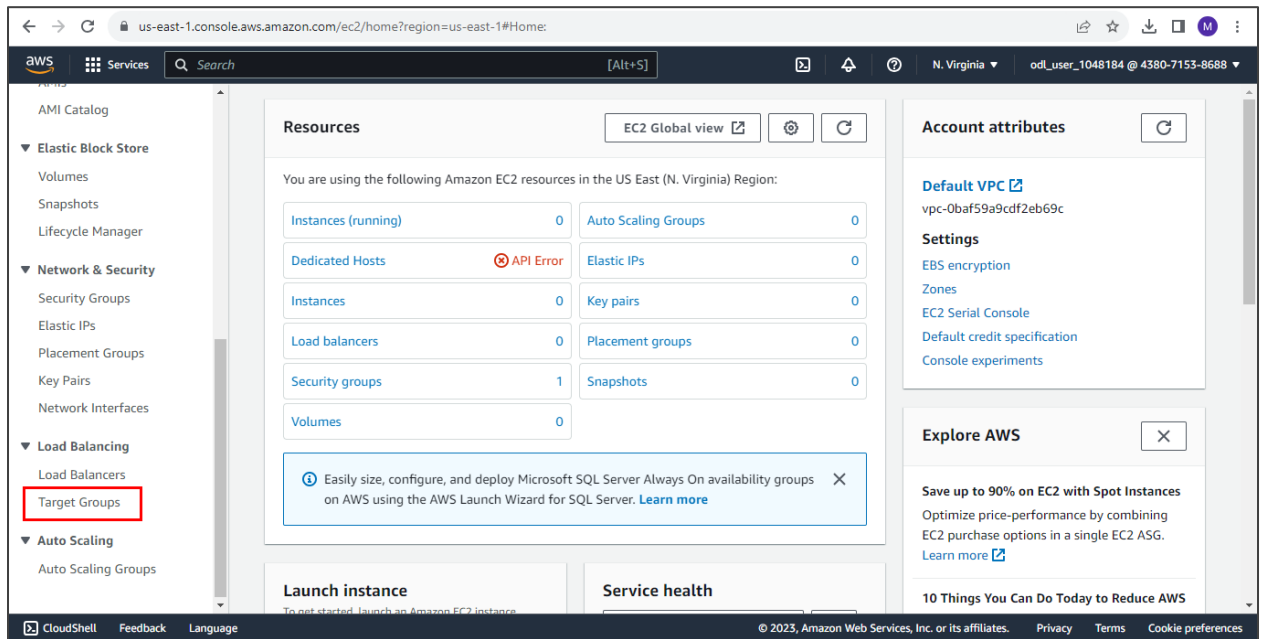
1. Create a target group
2. Launch EC2 instances
3. Configure the target group
4. Create a Load Balancer
5. Test the Load Balancer

#### Step 1: Create a target group

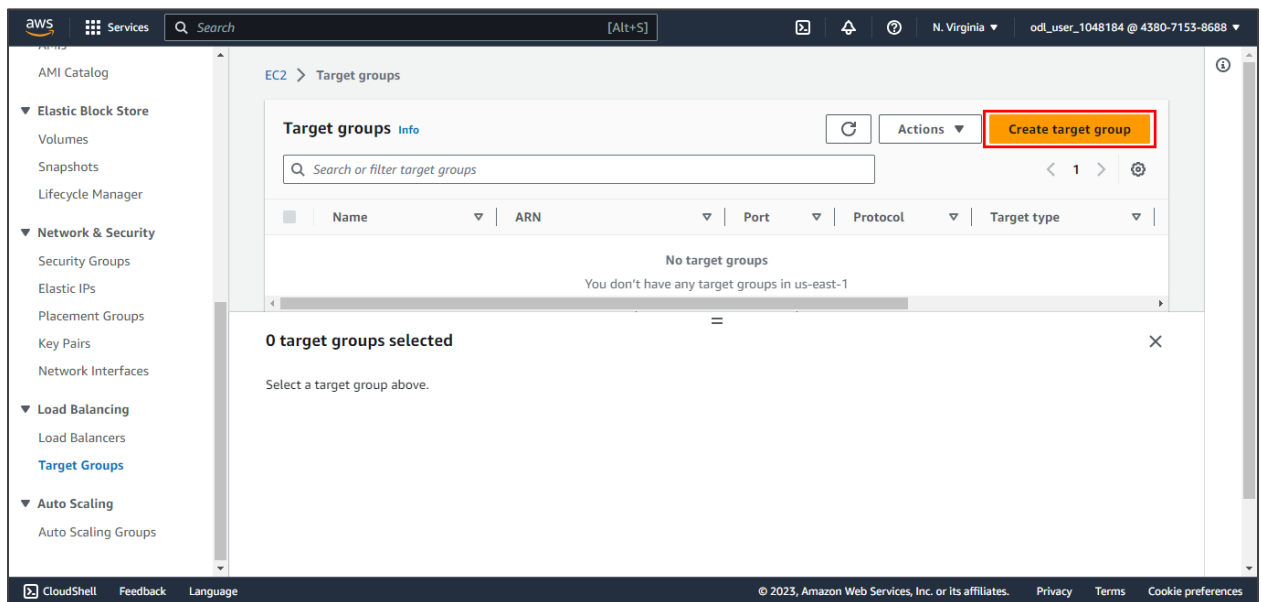
1.1 Log in to your AWS account, and open the Amazon EC2 console



## 1.2 Navigate to the Load Balancing section and click on Target Groups



## 1.3 Click on Create target group



#### 1.4 In the **Basic configuration** section:

- Choose **Instances** for the target type
- Enter a name for the target group such as **MyTargetGroup**

aws Services Search [Alt+S] N. Virginia odl\_user\_1048184 @ 4380-7153-8688

EC2 > Target groups > Create target group

Step 1  
Specify group details

Step 2  
Register targets

### 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

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws Services Search [Alt+S] N. Virginia odl\_user\_1048184 @ 4380-7153-8688

Target group name

MyTargetGroup

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

Protocol Port

HTTP : 80

1-65535

VPC

Select the VPC with the instances that you want to include in the target group.

vpc-0ba5f59a9cdf2eb69c  
IPv4: 172.31.0.0/16

Protocol version

☒ **HTTP1**

Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

☐ HTTP2

Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

☐ gRPC

Send requests to targets using gRPC. Supported when the request protocol is gRPC.

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

### 1.5 In the **Health checks** section:

- Set the protocol to **HTTP**
- Set the path to **/index.html**

**Health checks**  
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol  
HTTP

Health check path  
Use the default path of "/" to ping the root, or specify a custom path if preferred.  
/index.html  
Up to 1024 characters allowed.

► **Advanced health check settings**

**Attributes**

ⓘ Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

### 1.6 Click **Next**

**Health check path**  
Use the default path of "/" to ping the root, or specify a custom path if preferred.  
/index.html  
Up to 1024 characters allowed.

► **Advanced health check settings**

**Attributes**

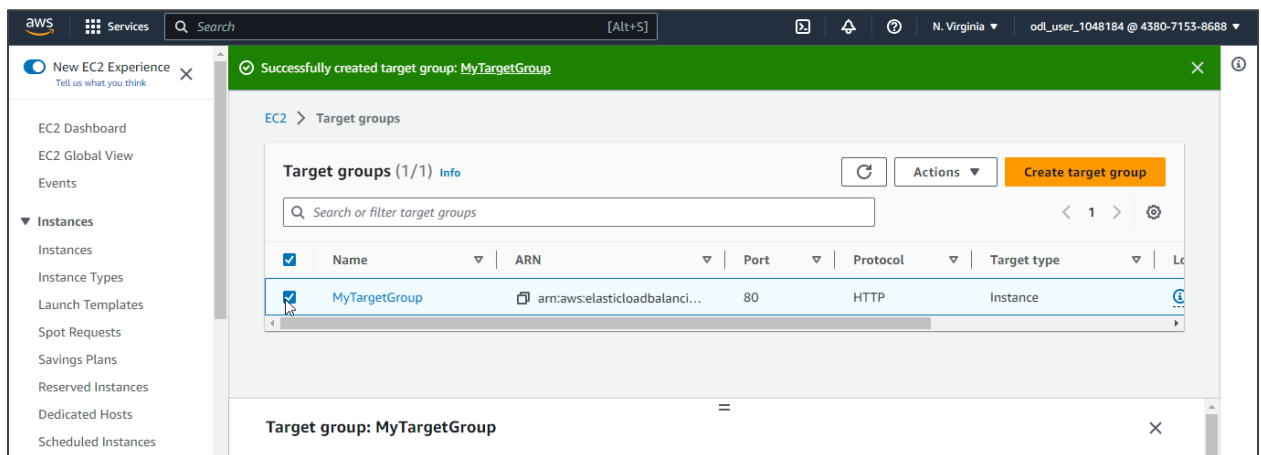
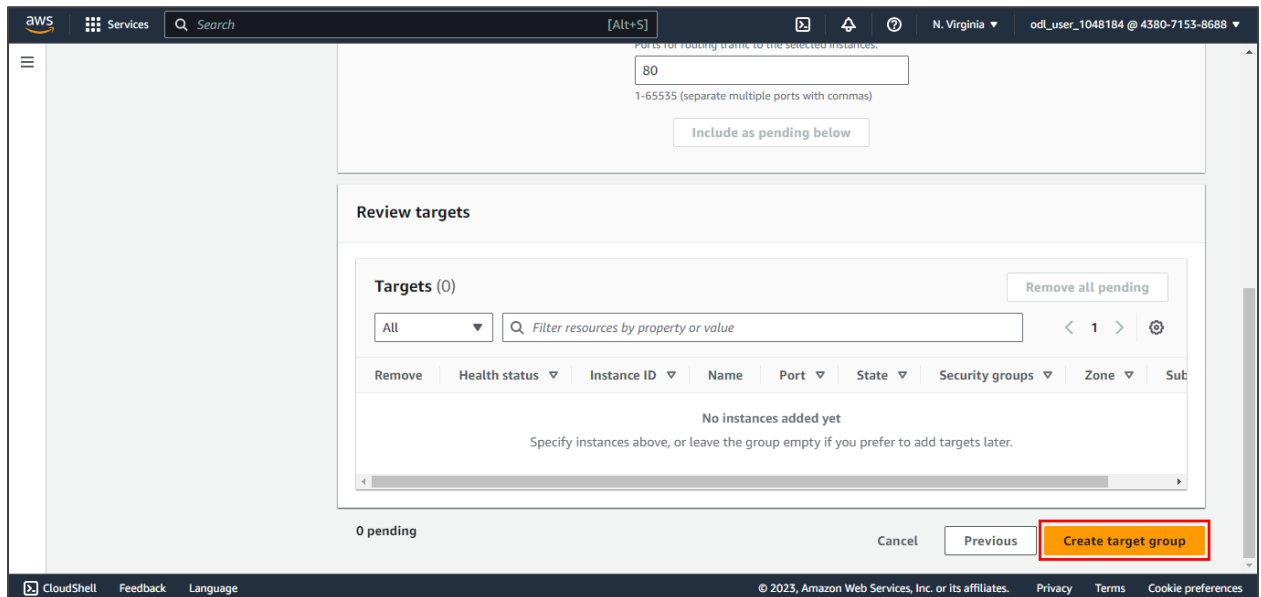
ⓘ Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

► **Tags - optional**  
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Cancel **Next**

CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

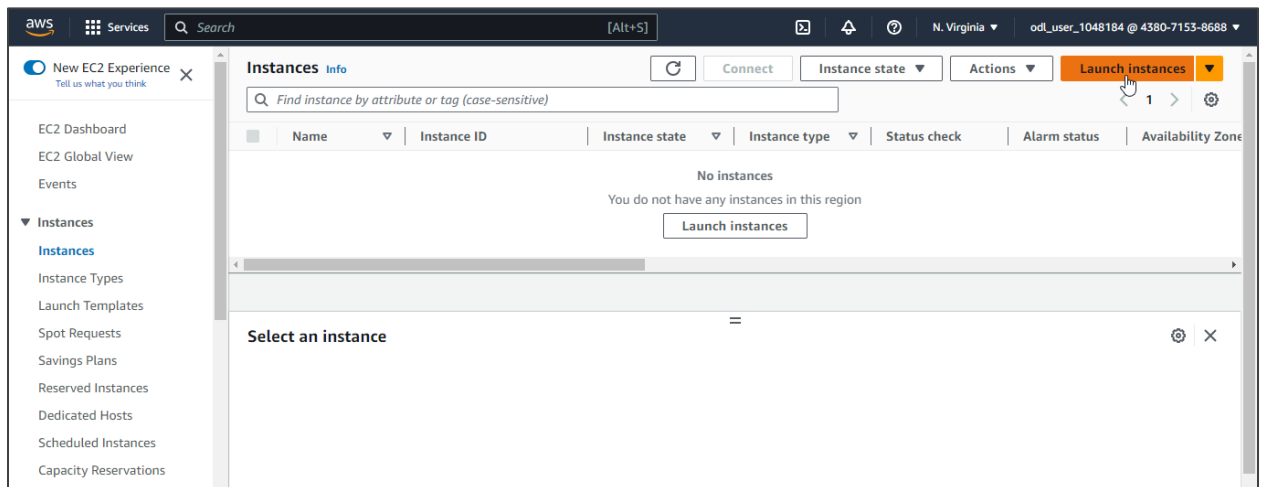
## 1.7 Review the configurations and click **Create target group**



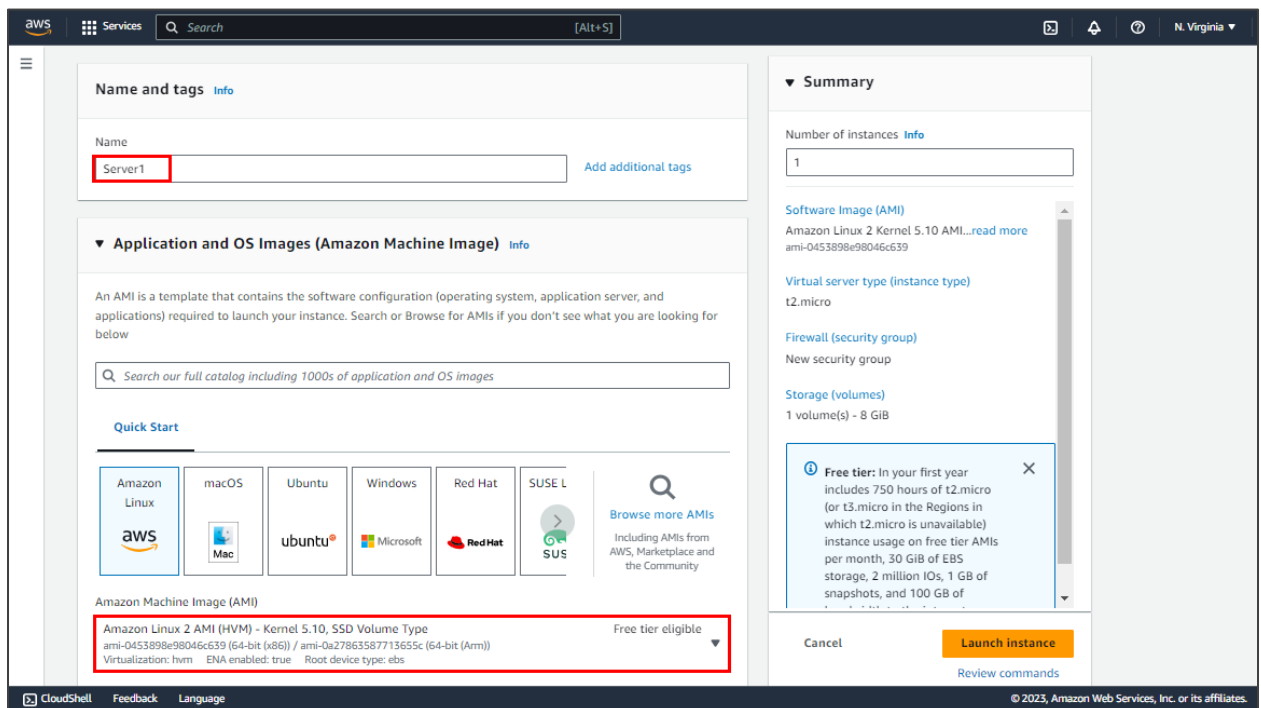
The target group has been successfully created.

## Step 2: Launch EC2 instances

### 2.1 Navigate to the **Instances** section, and click on **Launch instances**



### 2.2 Provide a name for the instance, and choose an appropriate AMI (**Amazon Linux 2**)



## 2.3 Configure instance details such as instance type, subnet, and security group

**Network settings**

VPC - *required* [Info](#)  
 vpc-0baf59a9cdf2eb69c (default) [Refresh](#)

Subnet [Info](#)  
 No preference [Refresh](#) [Create new subnet](#)

Auto-assign public IP [Info](#)  
 Enable

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

Security group name - *required*  
 launch-wizard-1  
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./[!@#%&\*~`{}|'"]\$\*

Description - *required* [Info](#)  
 launch-wizard-1 created 2023-08-22T10:21:39.983Z

**Summary**

Number of instances [Info](#)  
 1

Software Image (AMI)  
 Amazon Linux 2 Kernel 5.10 AMI...[read more](#)  
 ami-0453898e98046c639

Virtual server type (instance type)  
 t2.micro

Firewall (security group)  
 New security group

Storage (volumes)  
 1 volume(s) - 8 GiB

[Free tier: In your first year](#) [X](#)

[Cancel](#) [Launch instance](#) [Review commands](#)

**Firewall (security groups)**

Type [Info](#)  
 ssh

Protocol [Info](#)  
 TCP

Port range [Info](#)  
 22

Source type [Info](#)  
 Anywhere

Source [Info](#)  
[Add CIDR, prefix list or security](#)  
 0.0.0.0/0 [X](#)

Description - *optional* [Info](#)  
 e.g. SSH for admin desktop

Security group rule 2 (TCP, 80, 0.0.0.0/0) [Remove](#)

Type [Info](#)  
 HTTP

Protocol [Info](#)  
 TCP

Port range [Info](#)  
 80

Source type [Info](#)  
 Anywhere

Source [Info](#)  
[Add CIDR, prefix list or security](#)  
 0.0.0.0/0 [X](#)

Description - *optional* [Info](#)  
 e.g. SSH for admin desktop

[Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.](#) [X](#)

[Add security group rule](#)

**Summary**

Number of instances [Info](#)  
 1

Software Image (AMI)  
 Amazon Linux 2 Kernel 5.10 AMI...[read more](#)  
 ami-0453898e98046c639

Virtual server type (instance type)  
 t2.micro

Firewall (security group)  
 New security group

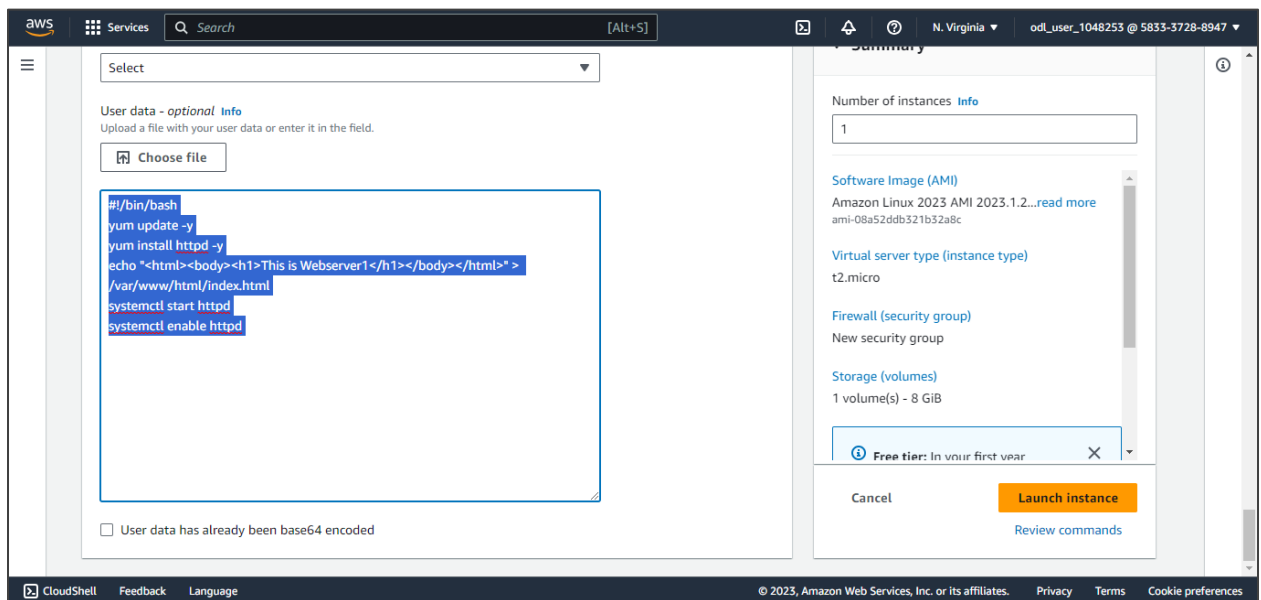
Storage (volumes)  
 1 volume(s) - 8 GiB

[Free tier: In your first year](#) [X](#)

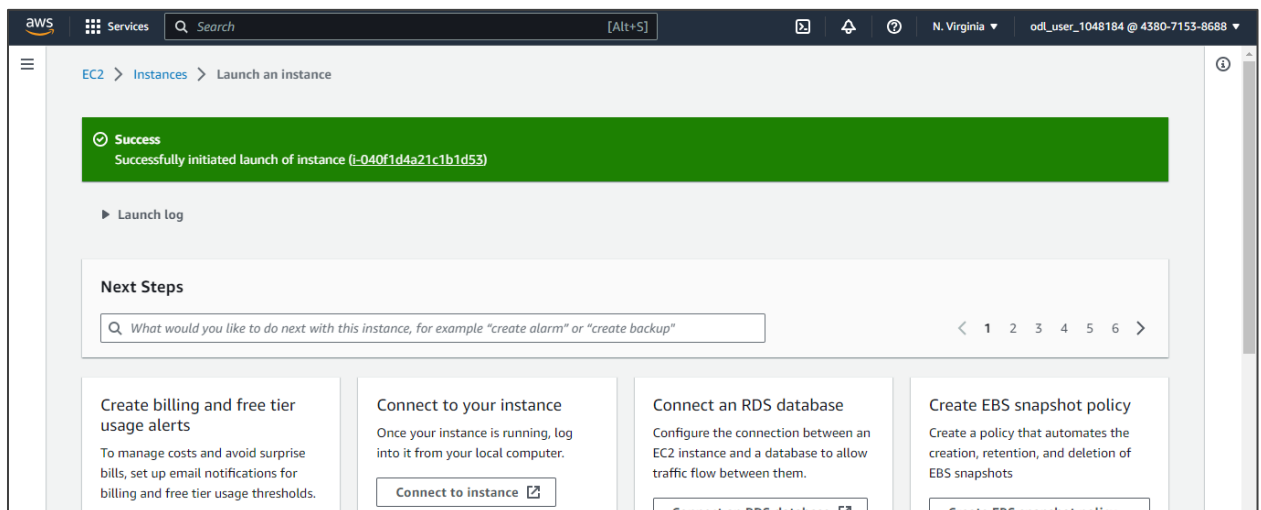
[Cancel](#) [Launch instance](#) [Review commands](#)

2.4 Under **Advanced Details**, enter the following user data script:

```
#!/bin/bash
yum update -y
yum install httpd -y
echo "<html><body><h1>This is Webserver1</h1></body></html>" >
/var/www/html/index.html
systemctl start httpd
systemctl enable httpd
```

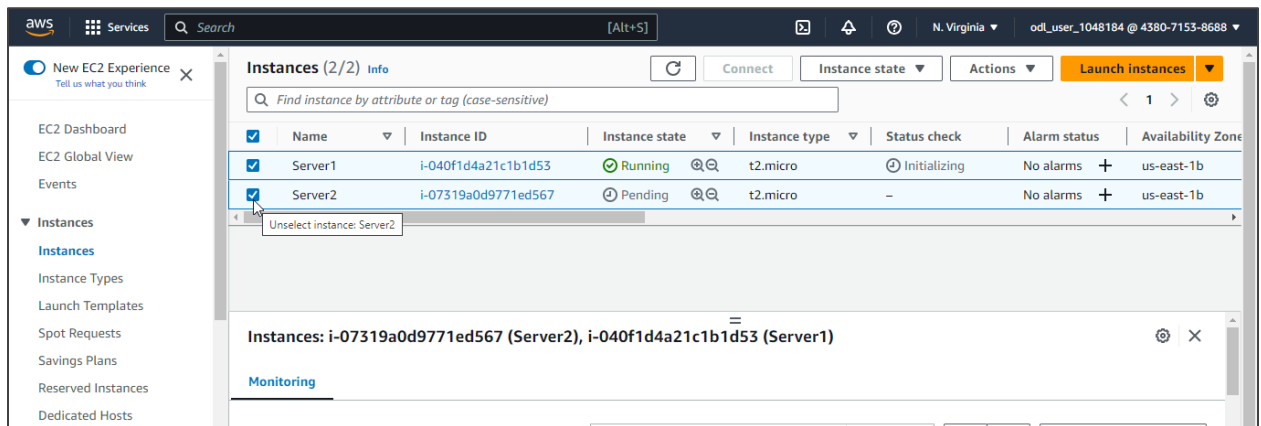


2.5 Complete the instance launch process by choosing a key pair, reviewing, and launching the instance





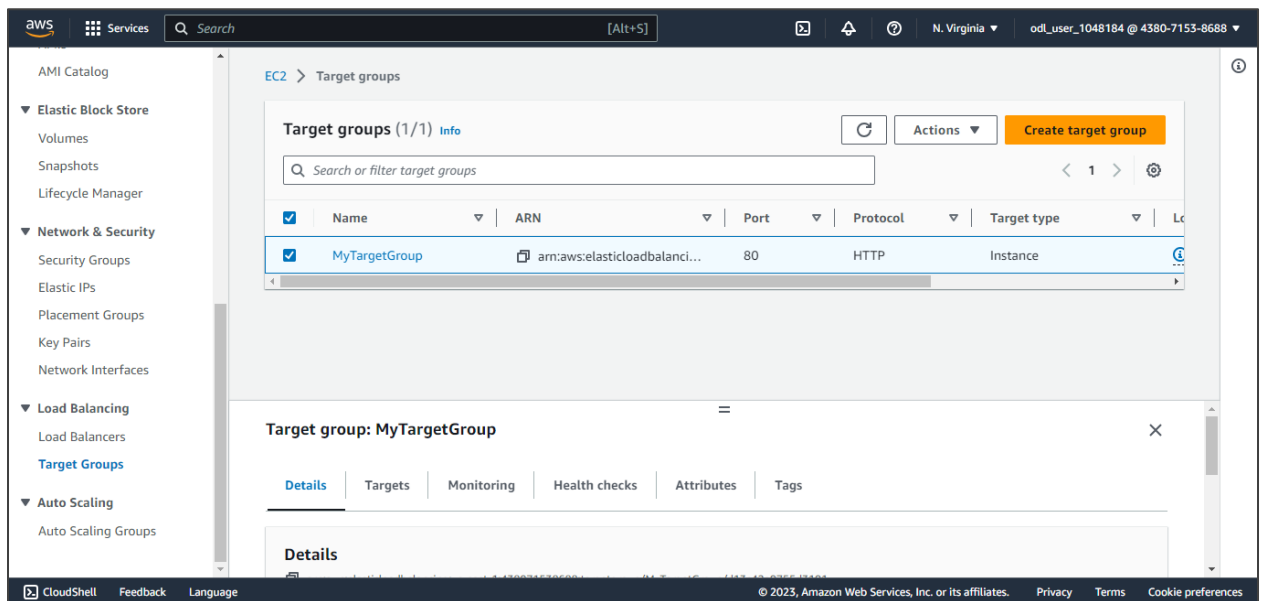
## 2.6 Launch another EC2 instance using the same steps, but modify the user data script to display the message **This is Webserver2**



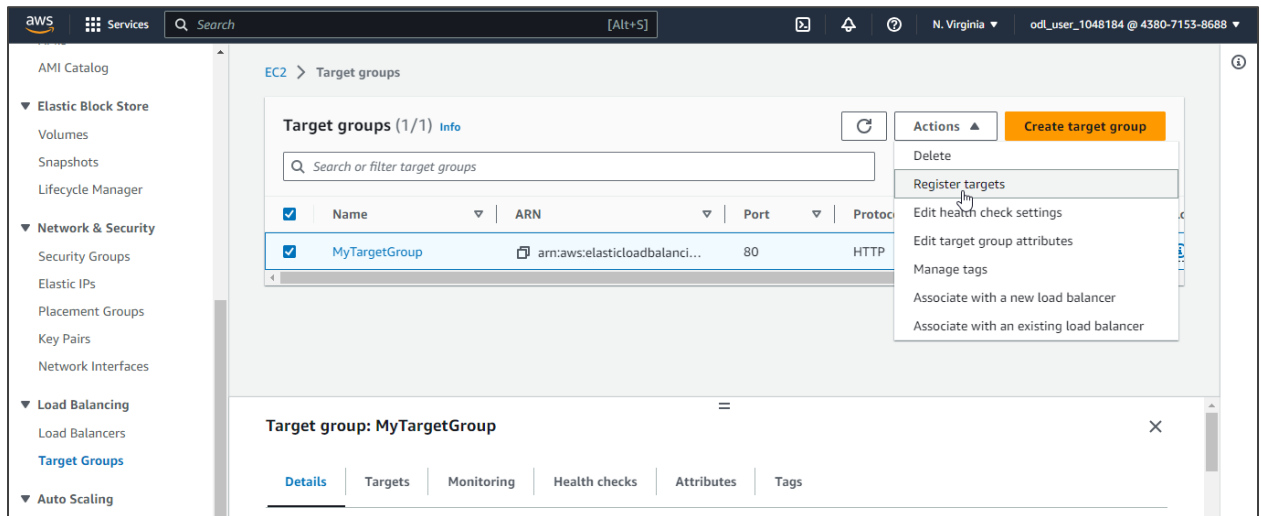
The EC2 instances are successfully launched.

## Step 3: Configure the target group

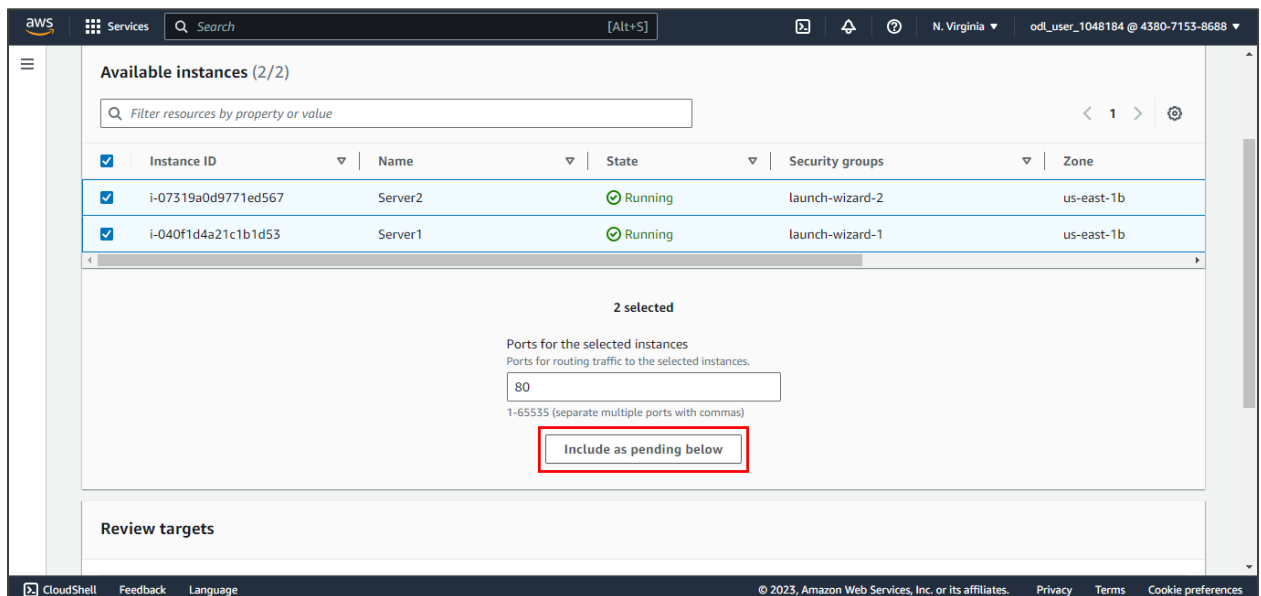
### 3.1 Navigate to the **Target Groups** section, and select the target group created in Step 1



### 3.2 Click on **Register targets** from the **Actions** menu



### 3.3 Select the instances (**Server1** and **Server2**) that were launched in Step 2 and click **Include as pending below**



### 3.4 Click **Register pending targets** to register the instances with the target group

The screenshot shows the AWS Management Console interface for the 'Review targets' step. At the top, there is a search bar and navigation links. Below the search bar, there is a text input field for '1-65535 (separate multiple ports with commas)' and a button labeled 'Include as pending below'. A message states '2 selections are now pending below. Include more or register targets when ready.' The main section is titled 'Review targets' and contains a table of 'Targets (2)'. The table has columns: Remove, Health status, Instance ID, Name, Port, State, Security groups, Zone, IPv4 address, and Subnet. Two targets are listed, both with a 'Pending' health status. At the bottom right, there is a red-bordered button labeled 'Register pending targets'.

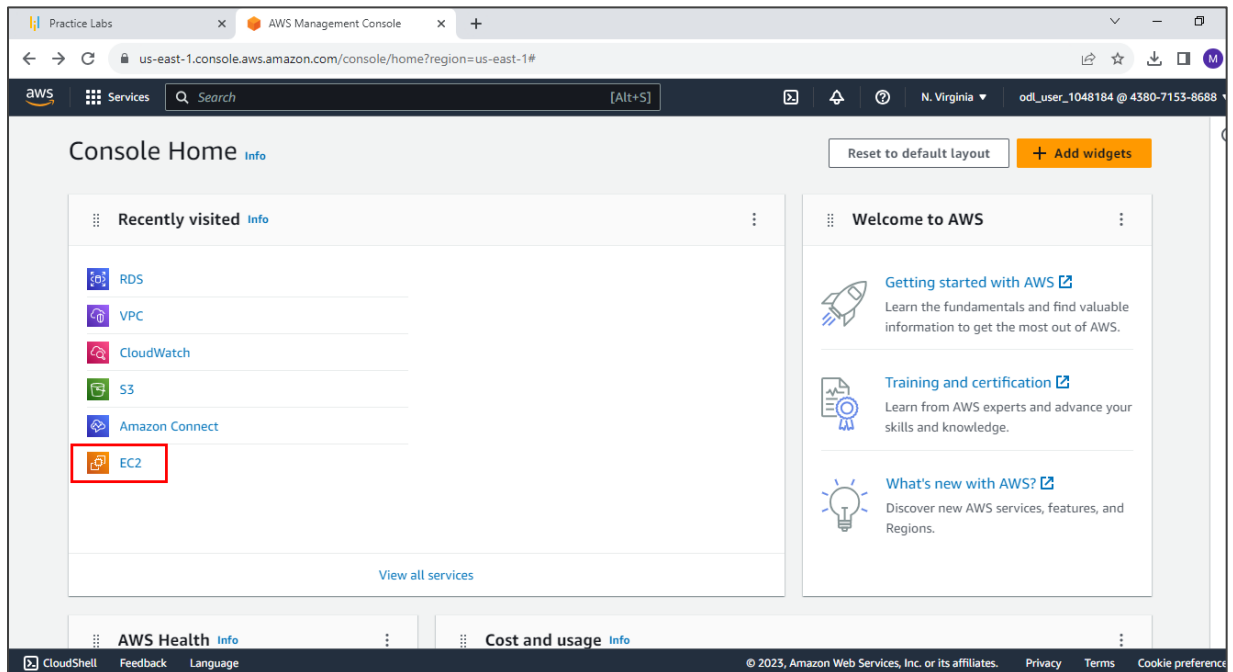
Remove	Health status	Instance ID	Name	Port	State	Security groups	Zone	IPv4 address	Subnet
X	Pending	i-07319a0d9771ed567	Server2	80	Running	launch-wizard-2	us-east-1b	52.201.196.166	subnet-
X	Pending	i-040f1d4a21c1b1d53	Server1	80	Running	launch-wizard-1	us-east-1b	54.224.142.83	subnet-

The screenshot shows the AWS Management Console interface for the 'Target groups' page. A green banner at the top indicates '2 targets registered successfully to MyTargetGroup.' Below the banner, there is a section titled 'Target groups (1/1) Info' with a search bar and a table of target groups. The table has columns: Name, ARN, Port, Protocol, and Target type. One target group, 'MyTargetGroup', is listed. Below the table, there is a section titled 'Target group: MyTargetGroup' with tabs for Details, Targets, Monitoring, Health checks, Attributes, and Tags. The 'Details' tab is selected, showing the details of the target group.

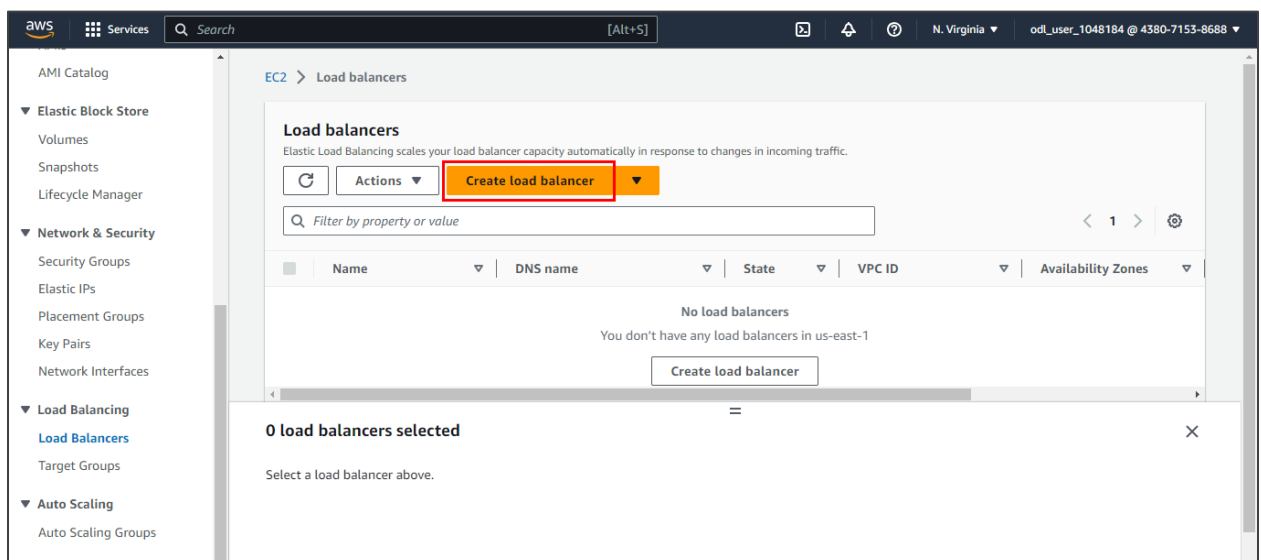
Name	ARN	Port	Protocol	Target type
MyTargetGroup	arn:aws:elasticloadbalanci...	80	HTTP	Instance

## Step 4: Create a Load Balancer

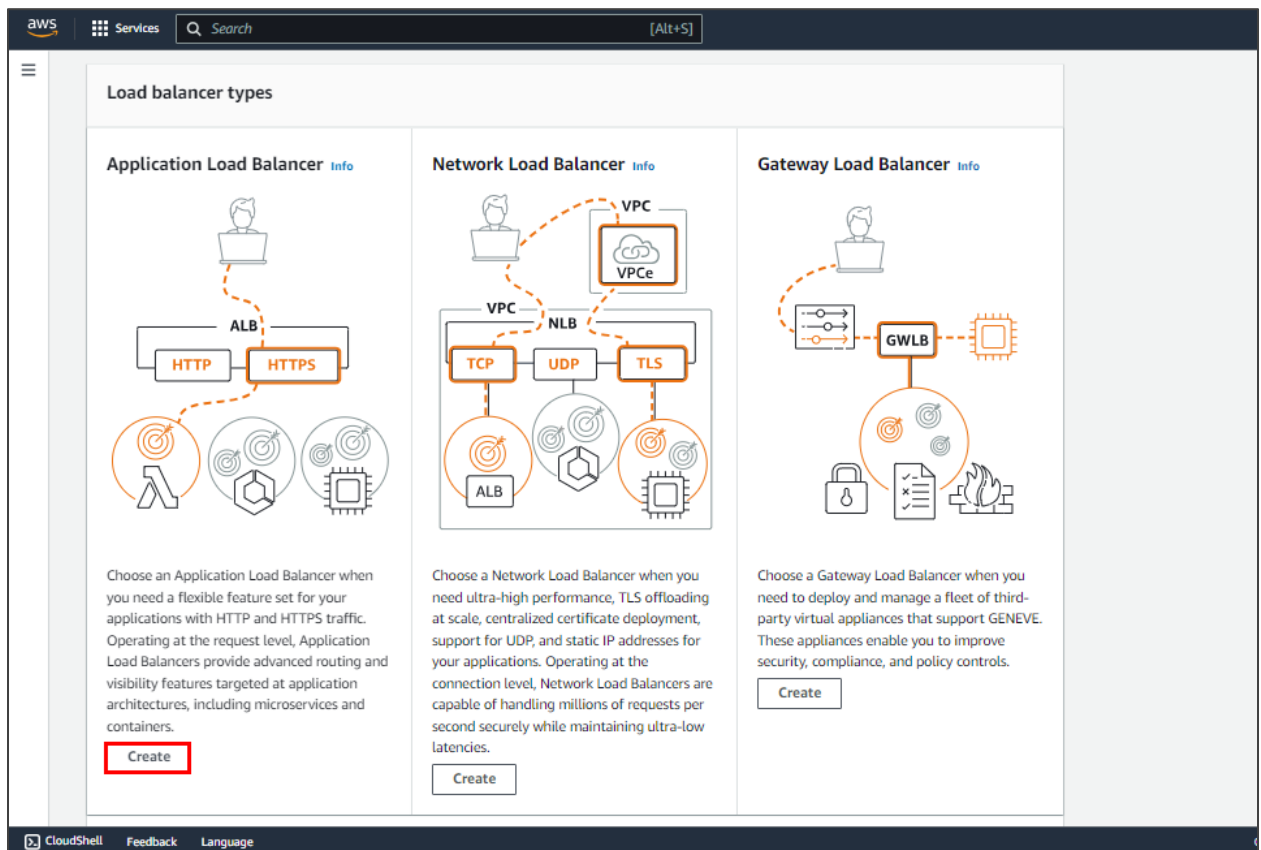
### 4.1 Open the Amazon EC2 console



### 4.2 Navigate to the Load Balancers section under Load Balancing and click Create load balancer

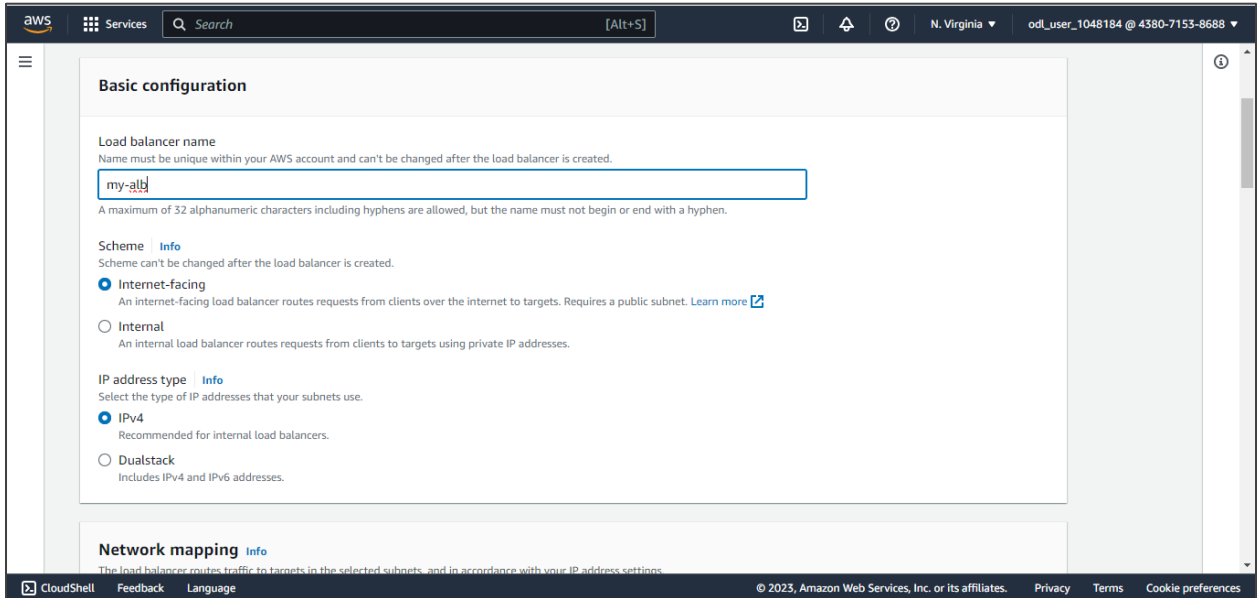


### 4.3 Choose **Application Load Balancer** and click **Create**



#### 4.4 Configure the load balancer settings:

- Enter a name for the load balancer such as **my-alb**
- Choose availability zones such as **us-east-1a** and **us-east-1b**



**Basic configuration**

**Load balancer name**  
Name must be unique within your AWS account and can't be changed after the load balancer is created.  
my-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**  
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

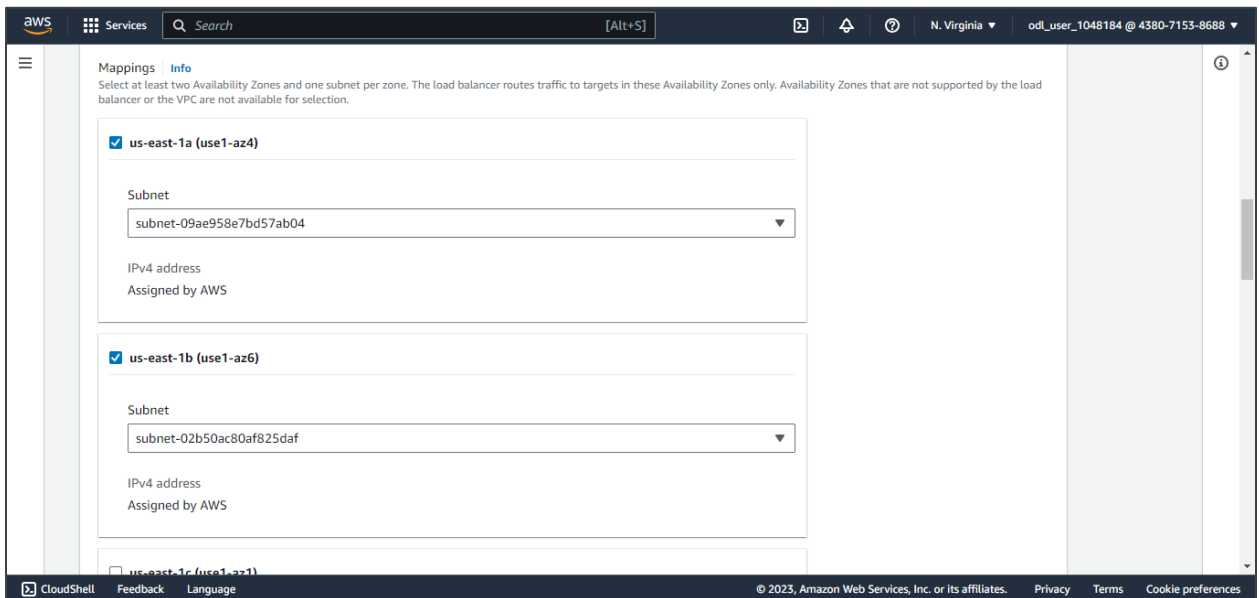
☐ **Internal**  
An internal load balancer routes requests from clients to targets using private IP addresses.

**IP address type** [Info](#)  
Select the type of IP addresses that your subnets use.

☒ **IPv4**  
Recommended for internal load balancers.

☐ **Dualstack**  
Includes IPv4 and IPv6 addresses.

**Network mapping** [Info](#)  
The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.



**Mappings** [Info](#)  
Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

☒ **us-east-1a (use1-az4)**

Subnet  
subnet-09ae958e7bd57ab04

IPv4 address  
Assigned by AWS

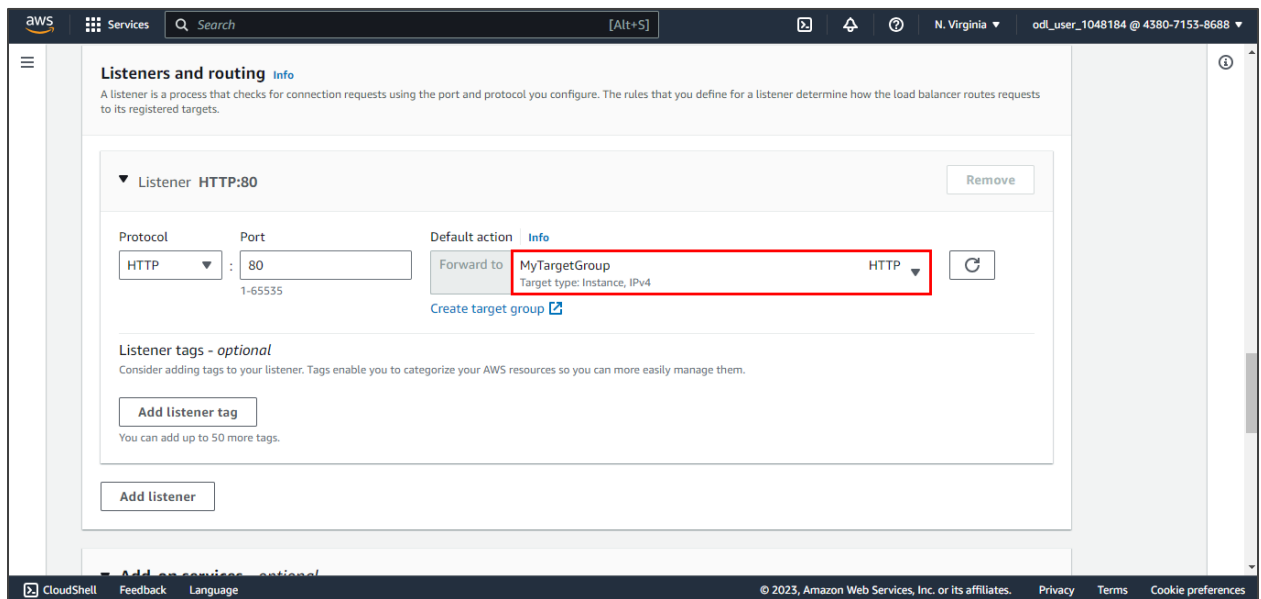
☒ **us-east-1b (use1-az6)**

Subnet  
subnet-02b50ac80af825daf

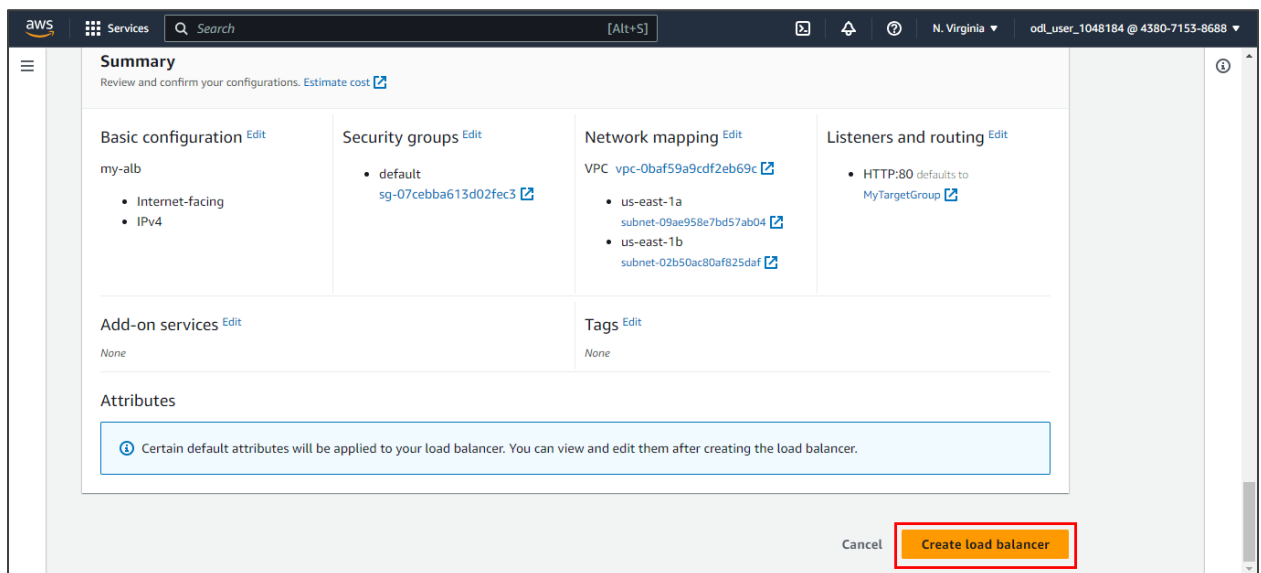
IPv4 address  
Assigned by AWS

☐ **us-east-1c (use1-az1)**

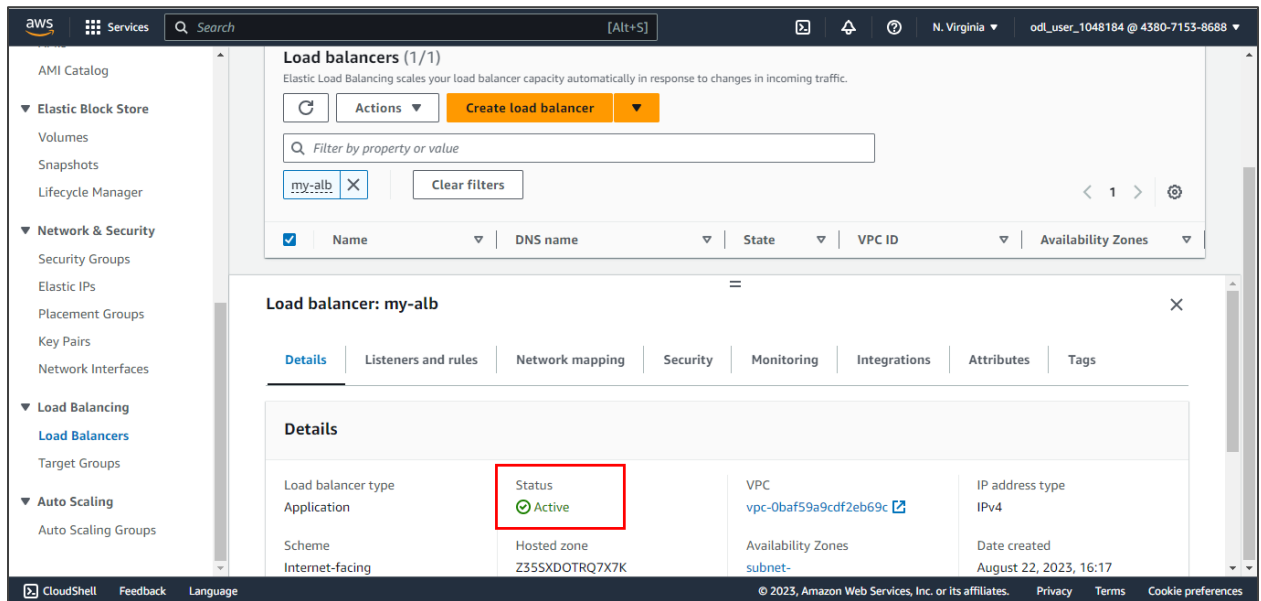
4.5 Choose the default action for the listener configuration to accept HTTP traffic on port **80**, and select the target group created in Step 1



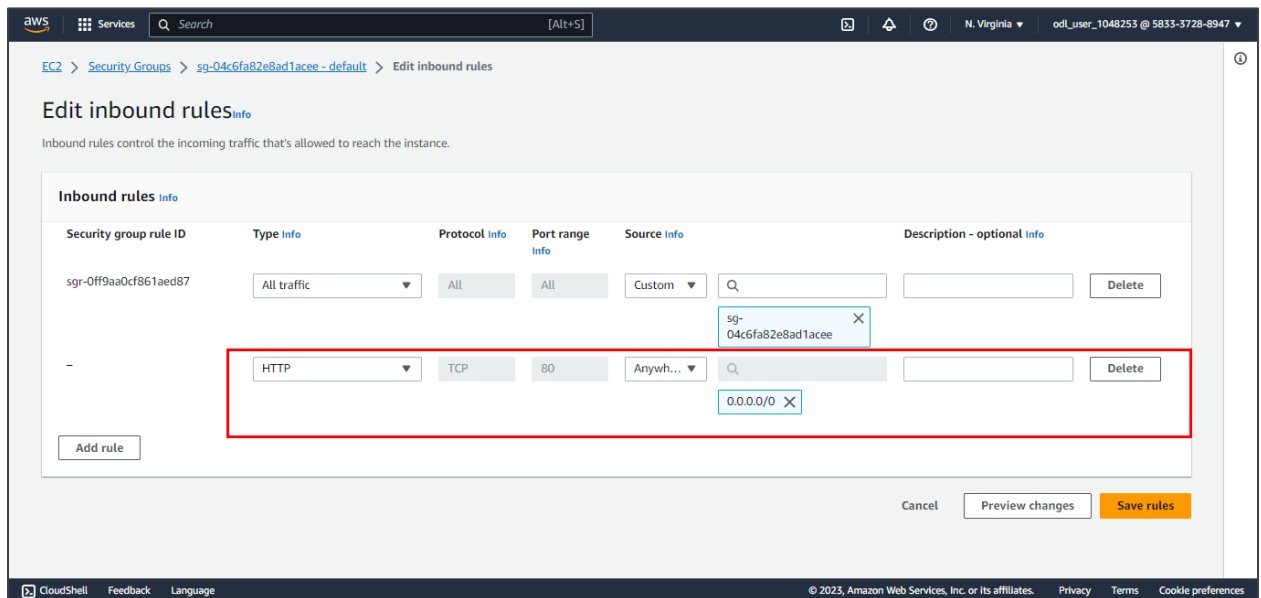
4.6 Review the configuration and click **Create load balancer**



Wait until the **Status** changes from **Provisioning** to **Active**



4.7 Create an inbound rule within the Load Balancer's security groups to permit port 80 access for all





## Step 5: Test the Load Balancer

### 5.1 Navigate to the Target Groups section, and select the target group you created

The screenshot shows the AWS Management Console interface. On the left, the navigation pane is open, showing the 'Load Balancing' section with 'Target Groups' selected. The main content area displays the 'Target groups (1/1)' list. A table lists the target groups, with 'MyTargetGroup' selected. Below the table, the 'Details' tab for 'MyTargetGroup' is active, showing various configuration details.

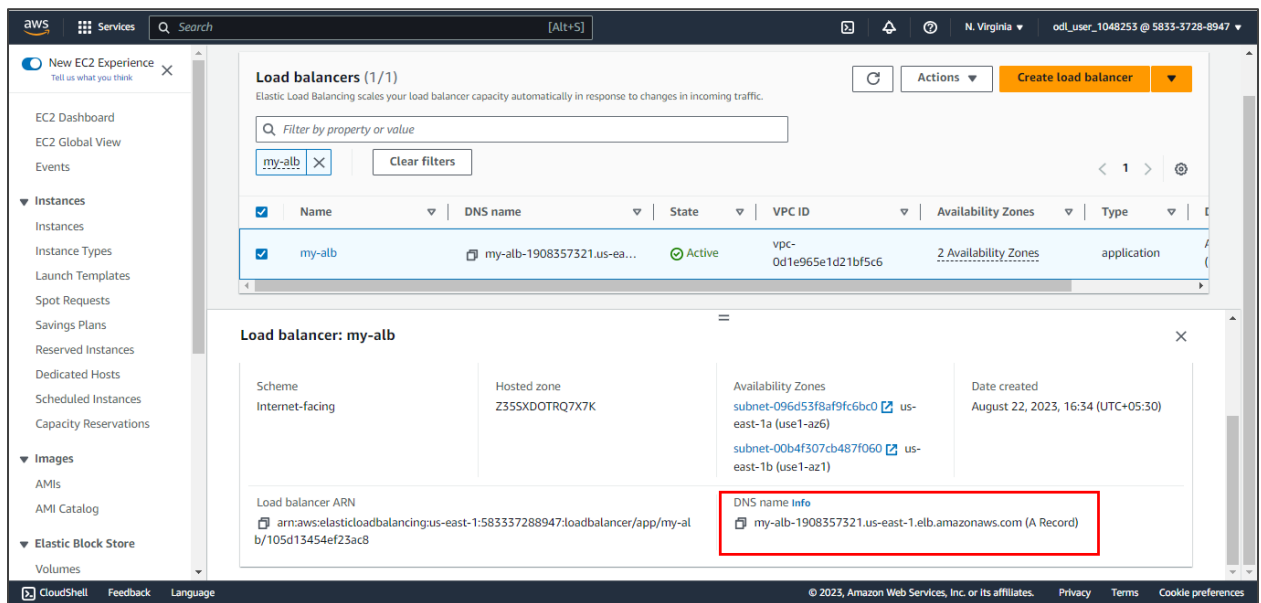
Name	ARN	Port	Protocol	Target type	Load balancer
MyTargetGroup	arn:aws:elasticloadbalancing...	80	HTTP	Instance	my-alb

### 5.2 Click on Details to verify that your instances are registered and healthy

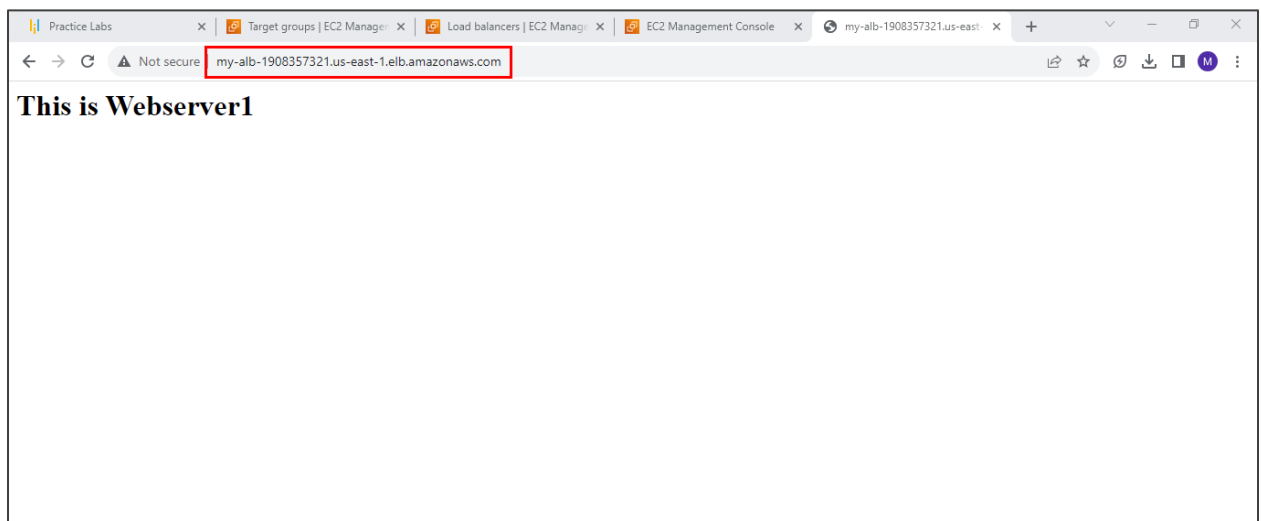
The screenshot shows the AWS Management Console interface. On the left, the navigation pane is open, showing the 'Load Balancing' section with 'Target Groups' selected. The main content area displays the 'Target groups (1/1)' list. A table lists the target groups, with 'MyTargetGroup' selected. Below the table, the 'Details' tab for 'MyTargetGroup' is active, showing various configuration details. The 'Healthy' status is highlighted with a red box.

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
2	2	0	0	0	0

### 5.3 Navigate to the **Load Balancers** section and copy the DNS name of the Load Balancer

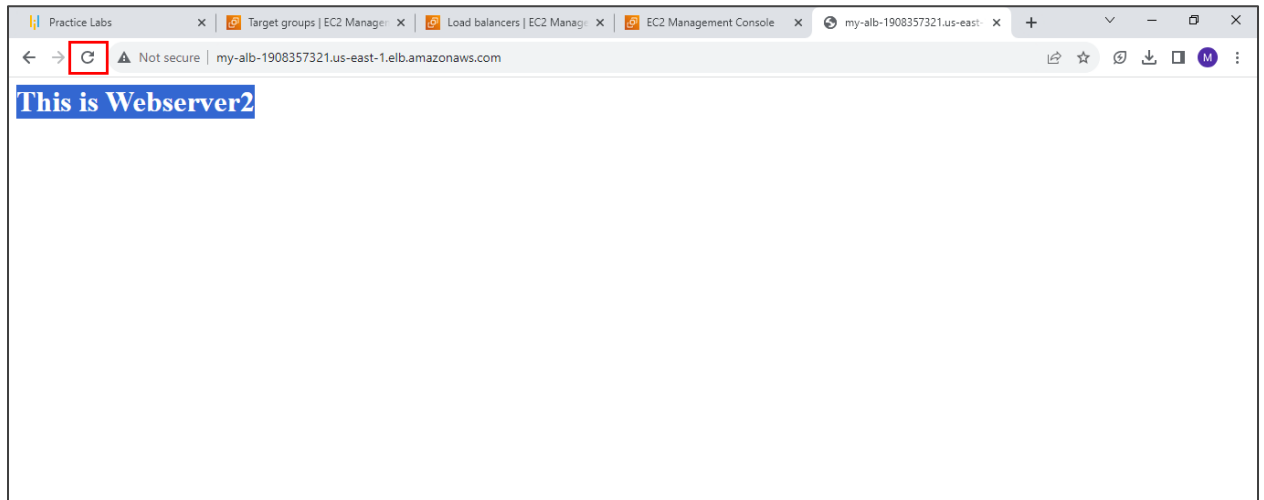


### 5.4 Open the browser window and paste the DNS URL into the address bar



You will observe the header message originating from the **Server1** instance.

5.5 Refresh the web page multiple times to witness the header message originating from the **Server2** instance



By following these steps, you have successfully set up an AWS Application Load Balancer, launched instances, and verified load balancing functionality.