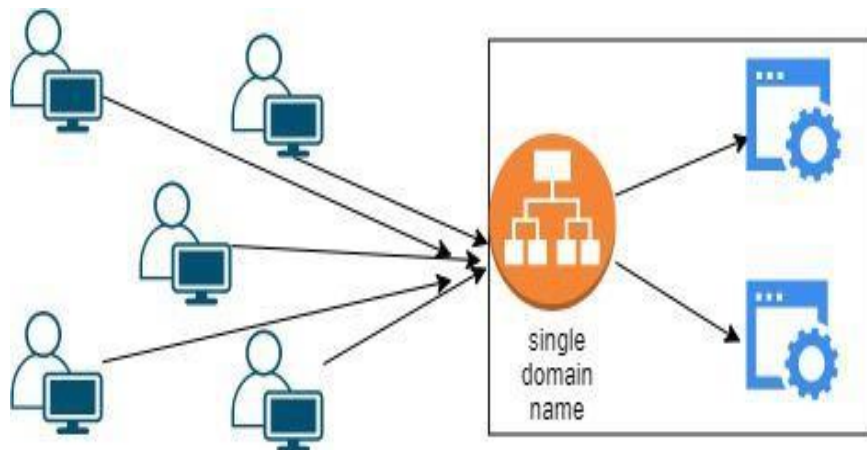


AWS
Documentation

No:-	Content
1.	Load balancer.
2.	Types of Load balancer.

Load balancer:

Elastic Load Balancing automatically distributes your incoming traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in one or more Availability Zones. It monitors the health of its registered targets, and routes traffic only to the healthy targets. Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.



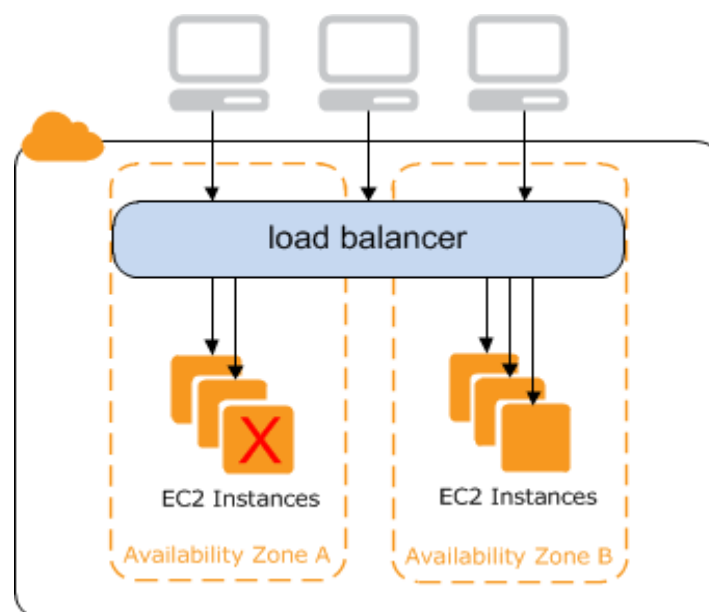
Types of Load Balancer:

- [User Guide for Application Load Balancers](#)
- [User Guide for Network Load Balancers](#)
- [User Guide for Gateway Load Balancers](#)
- [User Guide for Classic Load Balancers](#)

Classic Load Balancer:

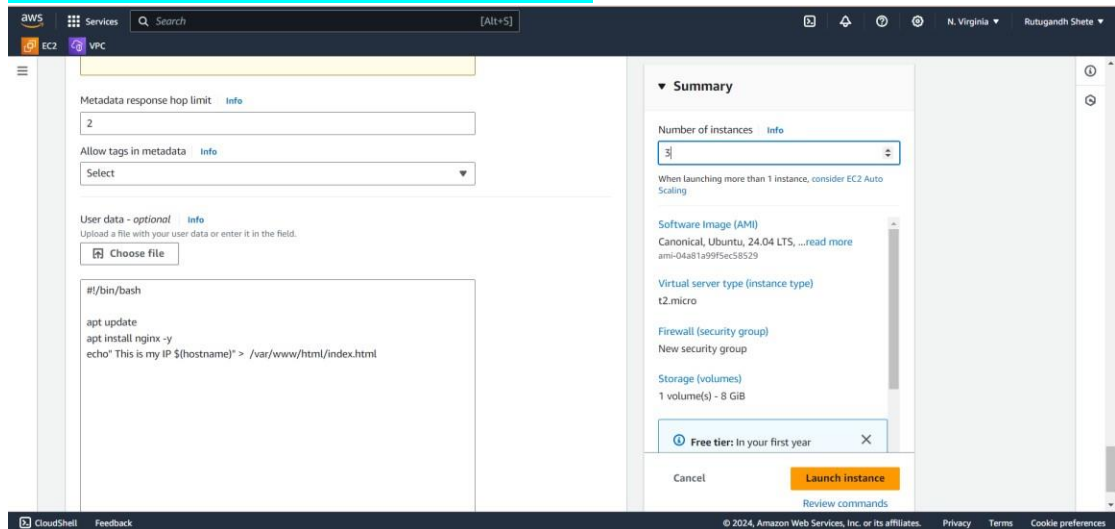
A load balancer distributes incoming application traffic across multiple EC2 instances in multiple Availability Zones. This increases the fault tolerance of your applications. Elastic Load Balancing detects unhealthy instances and routes traffic only to healthy instances.

Your load balancer serves as a single point of contact for clients. This increases the availability of your application. You can add and remove instances from your load balancer as your needs change, without disrupting the overall flow of requests to your application. Elastic Load Balancing scales your load balancer as traffic to your application changes over time. Elastic Load Balancing can scale to the vast majority of workloads automatically.

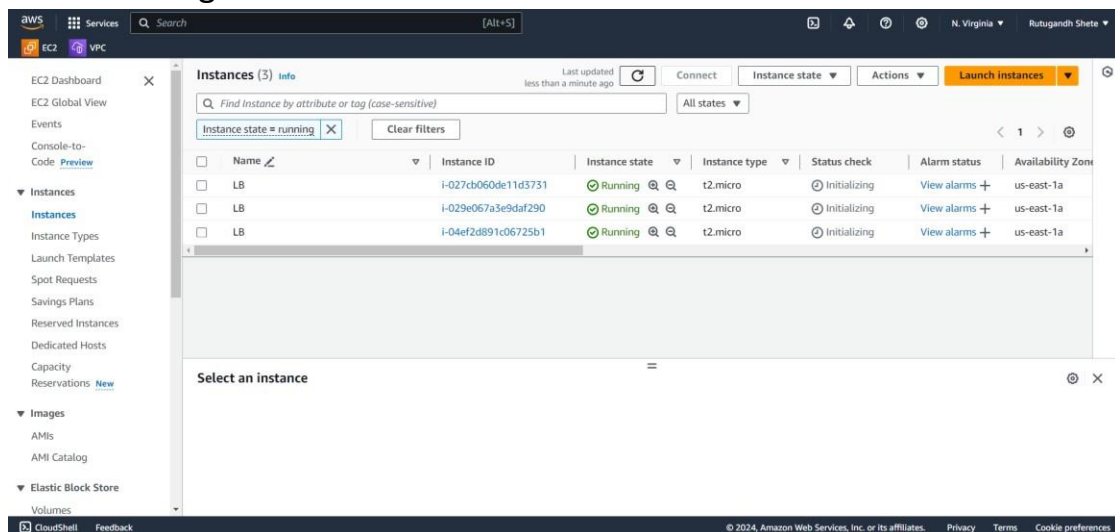


Steps:

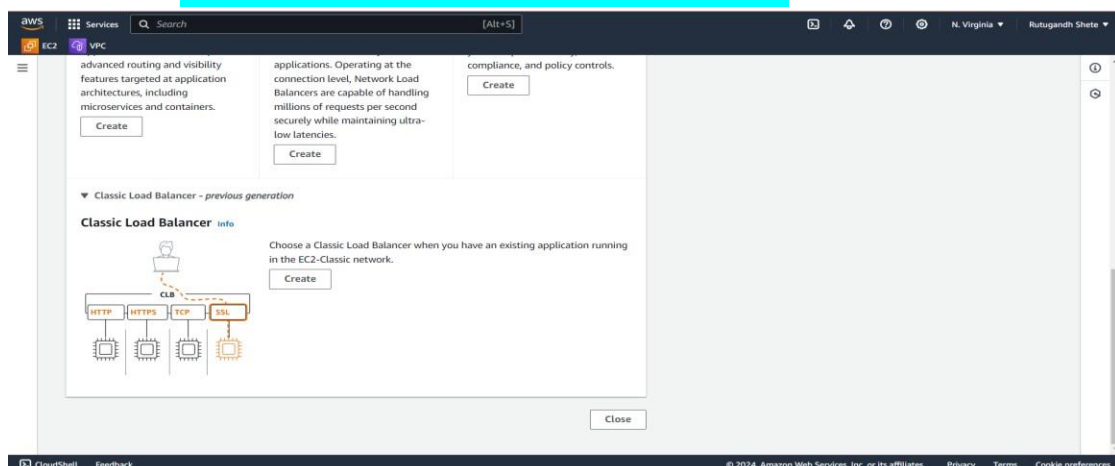
- Let's create **more than one instances**, suppose for time being 3 instances. While creating instances edit networking settings and add http to security group. In advanced settings add script.



- After creating Instances



- Go to Load **balancer→create→classic load balancer**



- Create classic → Name → description → select zone according to instances → we can select default security group and we can create accordingly → add inbound and outbound rule.

Google Chrome isn't your default browser [Set as default](#)

AWS Services Search [Alt+S] N. Virginia Rutugandhi Shete

EC2 > Security Groups > Create security group

Create security group [info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [info](#)
New_LB
Name cannot be edited after creation.

Description [info](#)
LB

VPC [info](#)
vpc-05ddac7397bf4a7fd (Default)

Inbound rules [info](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Select security group (we can select existing security group but we can add/create another security group also). While creating security group check we are attaching it to instances/load balancer etc.

AWS Services Search [Alt+S] N. Virginia Rutugandhi Shete

EC2 > VPC > Listeners and routing

us-east-1d (use1-az4)
us-east-1e (use1-az3)
us-east-1f (use1-az5)

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 [link](#).

Security groups
Select up to 5 security groups

New_LB
sg-0c1cfa983b97559e6 VPC: vpc-05ddac7397bf4a7fd

Listeners and routing [info](#)

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

▼ Listener HTTP:80
Instance HTTP:80 [Remove](#)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- In health check → Advanced health check settings → we can alter healthy and unhealthy threshold

AWS Services Search [Alt+S] N. Virginia Rutugandhi Shete

EC2 > VPC > Health checks

Health checks [info](#)

Your load balancer automatically performs health checks to test the availability of all registered instances. Traffic is only routed to healthy instances, which is determined on their response to the health check.

Ping target
The health check ping is sent using the protocol and port you specify. If using HTTP/HTTPS protocol, you must also provide the destination path.

Ping protocol Ping port Ping path
HTTP 80 /index.html

Advanced health check settings [Restore defaults](#)

Response timeout
Time to wait for EC2 instances to respond to health checks.
2 seconds
2-60 seconds. Must be less than the health check interval.

Interval
Amount of time between health checks sent to EC2 instances.
5 seconds
5-300 seconds. Must be greater than the health check response timeout.

Unhealthy threshold
Number of consecutive health check failures before declaring an EC2 instance unhealthy.
2
2-10

Healthy threshold
Number of consecutive health check successes before declaring an EC2 instance healthy.
4
2-10

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- In add instances we have to add instances and while creating it add script into User data.

Metadata response hop limit: 2

Allow tags in metadata: Select

User data - optional

```
#!/bin/bash
apt update
apt install nginx -y
echo "This is my IP $(hostname)?" > /var/www/html/index.html
```

Summary

Number of instances: 3

When launching more than 1 instance, consider EC2 Auto Scaling

Software Image (AMI): Canonical, Ubuntu, 24.04 LTS, ...
ami-04a81a99f5ec58529

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

Launch instance

Add instances

Select EC2 instances to register to your load balancer. Requests will be routed to registered instances that meet the health check requirements. For maximum fault tolerance, we recommend maintaining approximately equivalent numbers of instances in each Availability Zone enabled for the load balancer. If demand on your instances changes, you can register or deregister instances without disrupting the flow of requests to your application. [Learn more](#)

VPC: vpc-05ddac7397bf4a7fd

Available instances (3/3)

Instance ID	Name	State	Security groups	Zone	Public IP
i-027cb060de11d3731	LB	Running	launch-wizard-20	us-east-1a	54.175.20
i-029e067a3e9daf290	LB	Running	launch-wizard-20	us-east-1a	35.173.21
i-04ef2d891c06725b1	LB	Running	launch-wizard-20	us-east-1a	3.88.255.1

Confirm

- After creating load balancer.

Load balancers (1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Filter load balancers: 1 match

Name	DNS name	State	VPC ID	Availability Zones	Type
clb	clb-1193023192.us-east-1...	Running	vpc-05ddac7397bf4a7fd	us-east-1a (use1-a26)	classic

0 load balancers selected

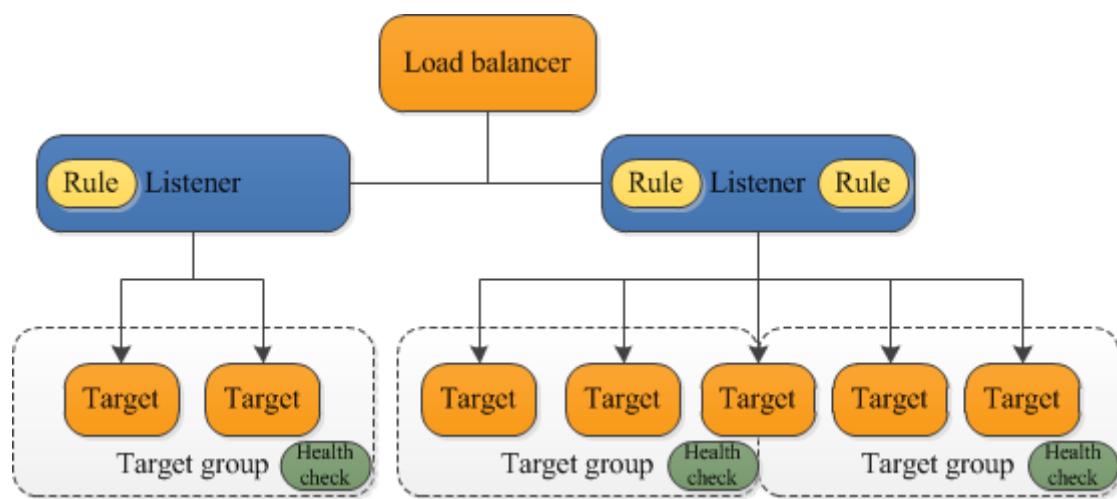
Select a load balancer above.

- Copy DNS name mentioned in DNS Name and paste it on browser. **clb-1193023192.us-east-1.elb.amazonaws.com**

IP ip-172-31-43-17

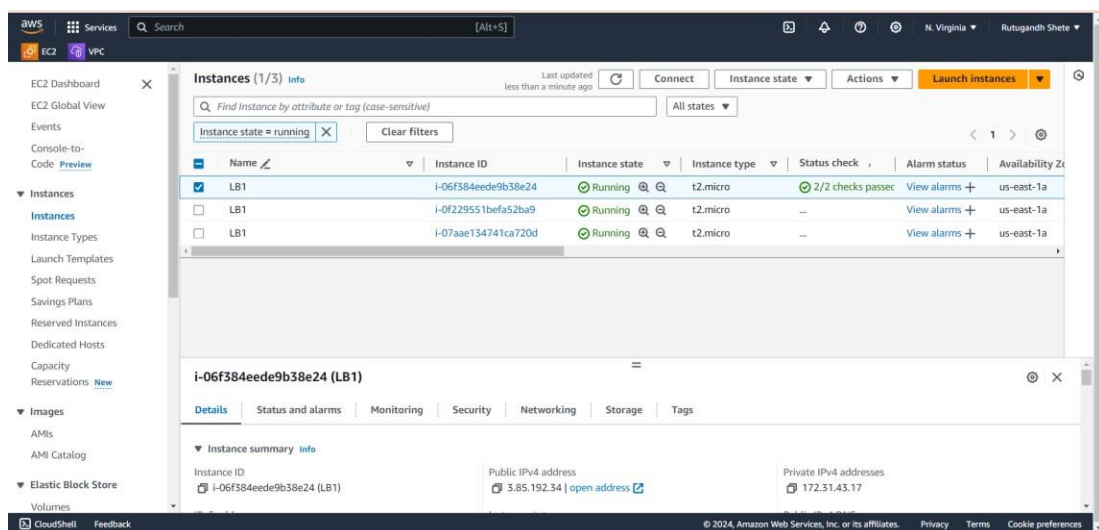
Application Load Balancer:

A *load balancer* serves as the single point of contact for clients. The load balancer distributes incoming application traffic across multiple targets, such as EC2 instances, in multiple Availability Zones. This increases the availability of your application. You add one or more listeners to your load balancer. Each *target group* routes requests to one or more registered targets, such as EC2 instances, using the protocol and port number that you specify. You can register a target with multiple target groups. You can configure health checks on a per target group basis. Health checks are performed on all targets registered to a target group that is specified in a listener rule for your load balancer.

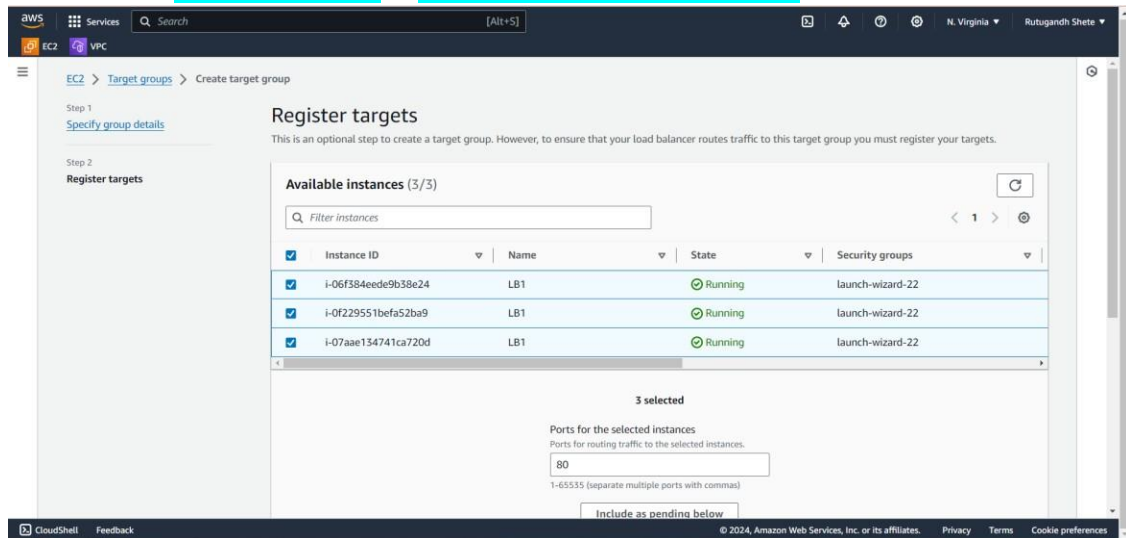


Steps:

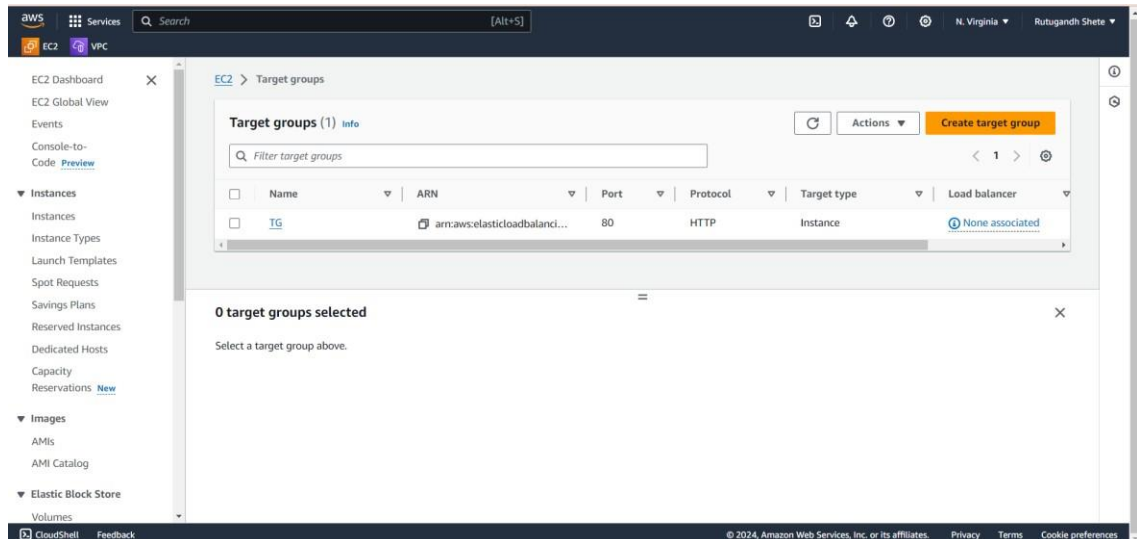
- Create instances.



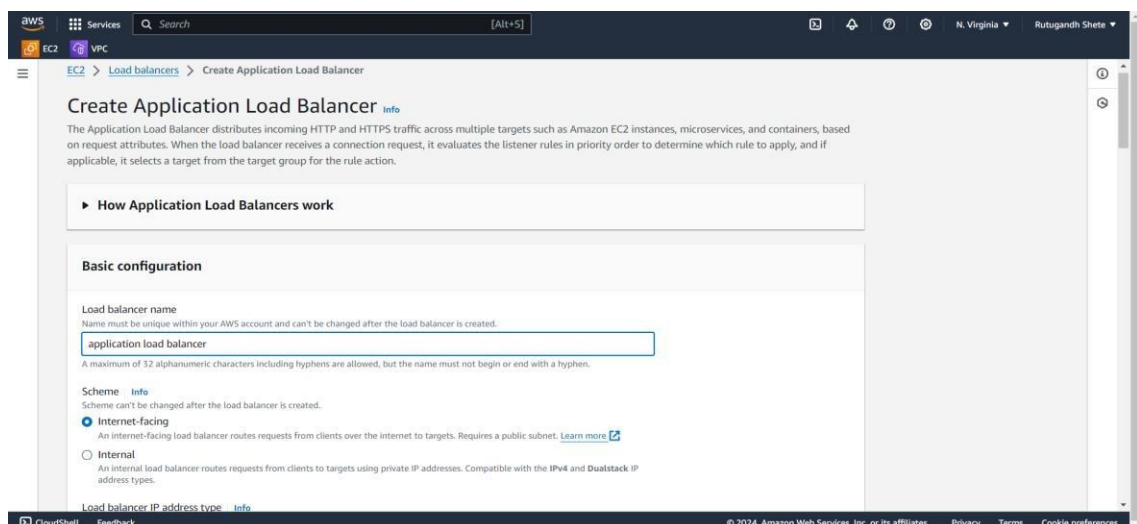
- Create target groups. Load balancing → Target groups → create → Name → add instances → include as pending below → create.



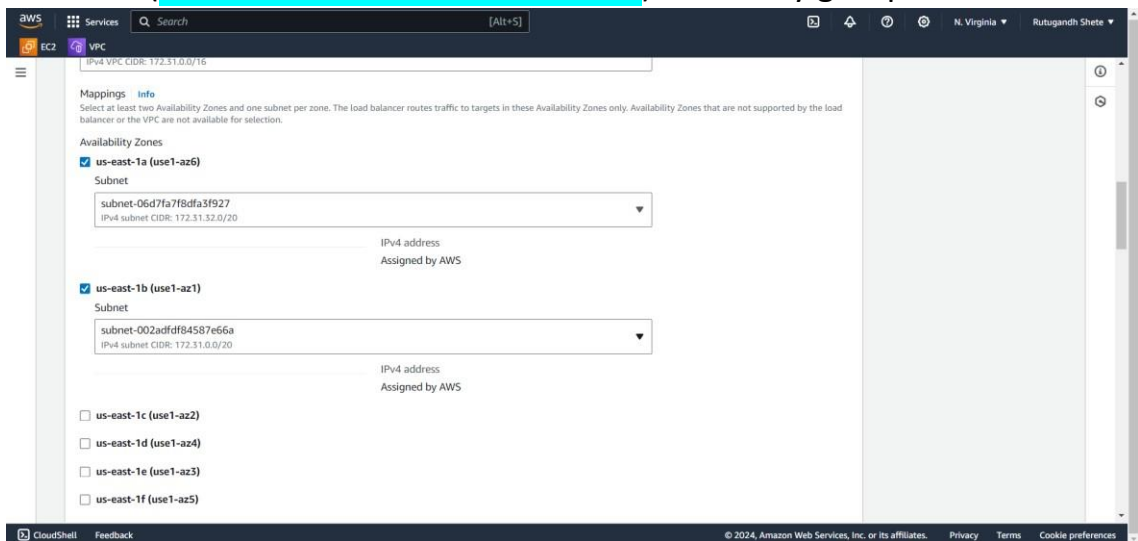
- After creation of target group.



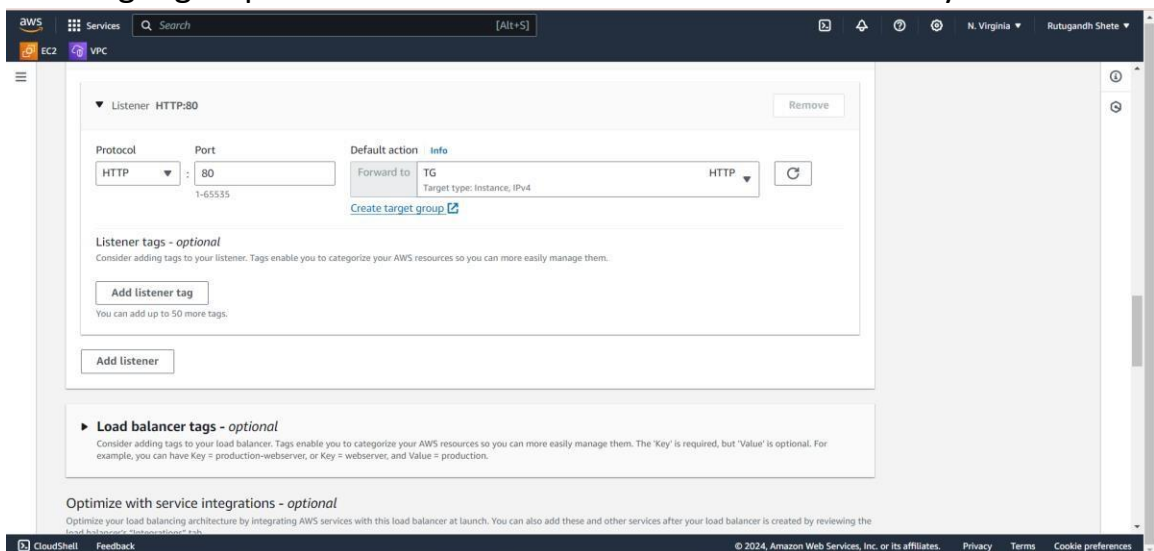
- Create application load balancer → load balancers → create → application load balancer → name.



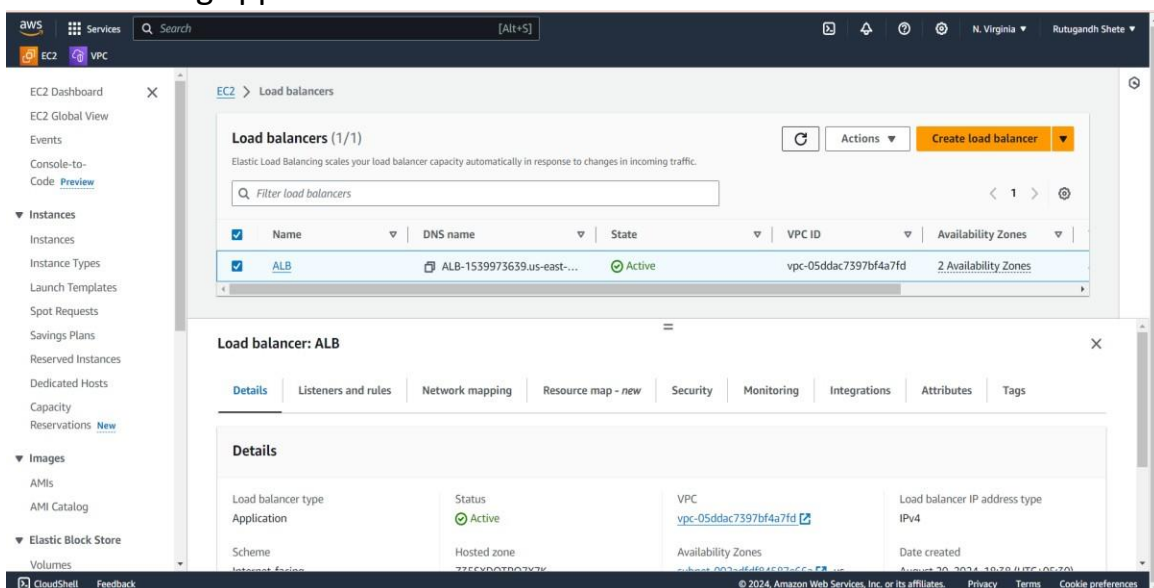
- Add zone(atleast 2 zones should be added)→security group



- Add target group in load balancer that we have created already.



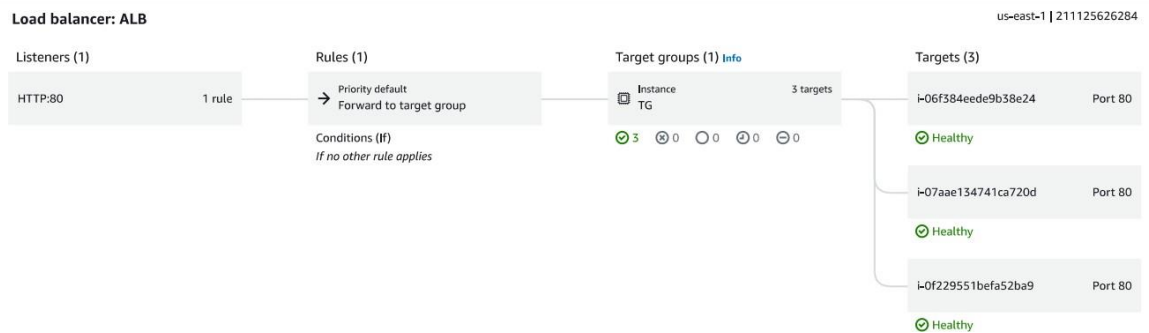
- After creating application load balancer.



- After pasting DNS to browser.

IP ip-172-31-41-248

- In below diagram we can see that we have associated only one target group to application load balancer.



- Now **create another target group**, for that we have to create instances .

Instances (5) Info

Last updated less than a minute ago

Connect Instance state Actions Launch instances

Find Instance by attribute or tag (case-sensitive)

Instance state = running Clear filters

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	target_instance	i-0642792209d410ca2	Running	t2.micro	Initializing	View alarms +	us-east-1a
<input type="checkbox"/>	target_instance	i-096626f7e56a17fb0	Running	t2.micro	Initializing	View alarms +	us-east-1a
<input type="checkbox"/>	LB1	i-06f384eede9b38e24	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a
<input type="checkbox"/>	LB1	i-0f229551bfa52ba9	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a
<input type="checkbox"/>	LB1	i-07aae134741ca720d	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a

Select an instance

- Create another target group for another reason . load balancers→target groups→create→Name→add health check path.

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 perform health checks on the root, or specify a custom path if preferred.
/TG
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

- After this add instances→including instances as below→create

Register targets
This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (2/5)

Instance ID	Name	State	Security groups
<input checked="" type="checkbox"/> i-0642792209d410ca2	target_instance	Running	launch-wizard-23
<input checked="" type="checkbox"/> i-0966267e56a17fb0	target_instance	Running	launch-wizard-23
<input type="checkbox"/> i-06f584eede9b38e24	LB1	Running	launch-wizard-22
<input type="checkbox"/> i-0f229551bfa52ba9	LB1	Running	launch-wizard-22
<input type="checkbox"/> i-07aae134741ca720d	LB1	Running	launch-wizard-22

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.

- After creating another target group.

Target groups (1/2)

Name	ARN	Port	Protocol	Target type	Load balancer
TG2	arn:aws:elasticloadbalancing:us-east-1:211125626284:targetgroup/TG2/7800490215d16db	80	HTTP	Instance	None associated
TG	arn:aws:elasticloadbalancing:us-east-1:211125626284:targetgroup/TG/7800490215d16db	80	HTTP	Instance	None associated

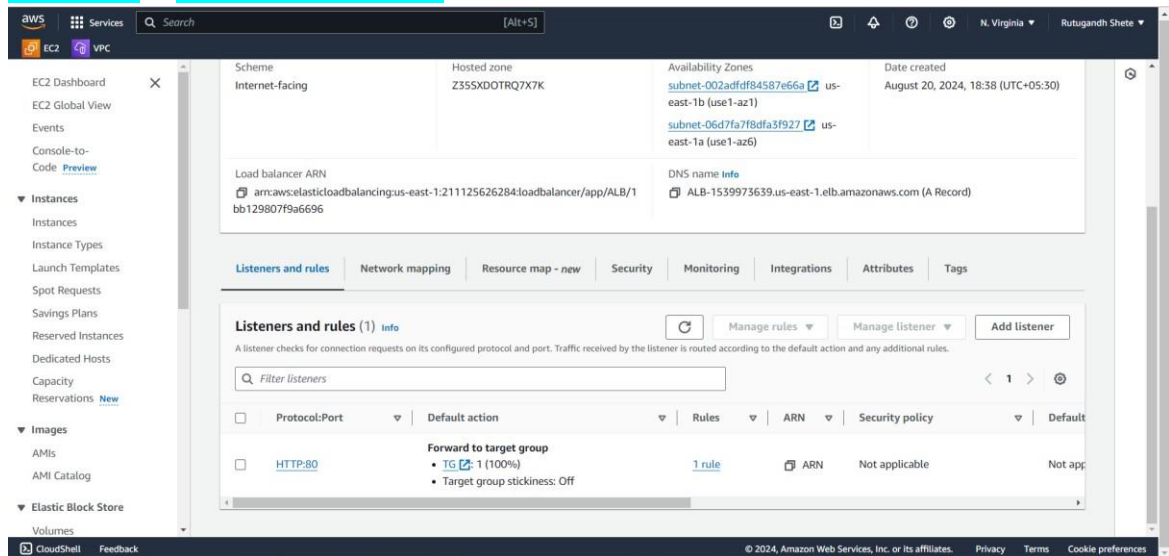
Target group: TG2

Details

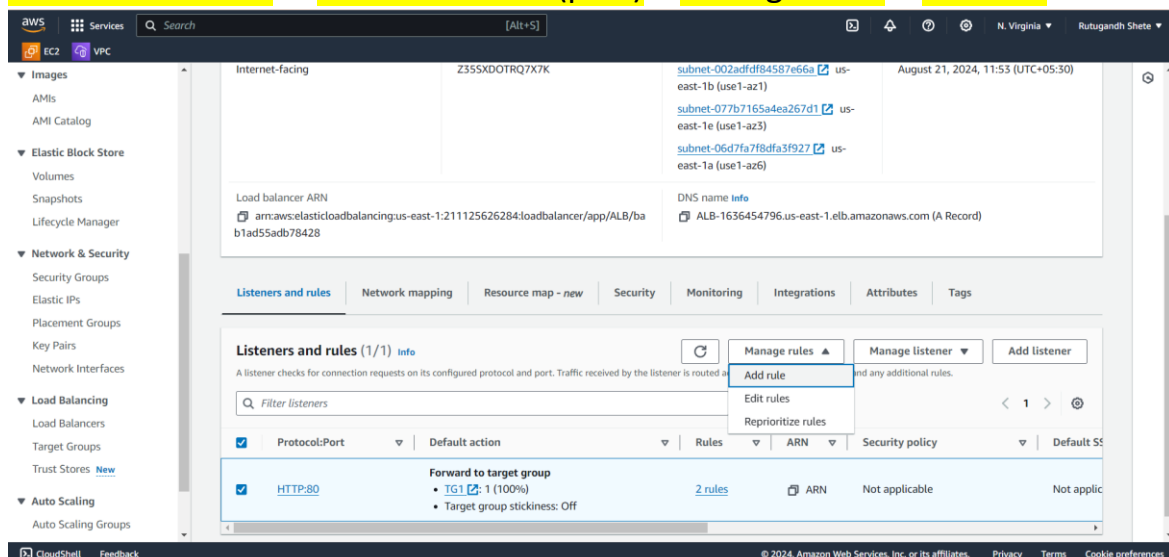
arn:aws:elasticloadbalancing:us-east-1:211125626284:targetgroup/TG2/7800490215d16db

Target type	Protocol : Port	Protocol version	VPC
Instance	HTTP: 80	HTTP1	vpc-05ddac7397bf4a7fd
ID address type	Load balancer		

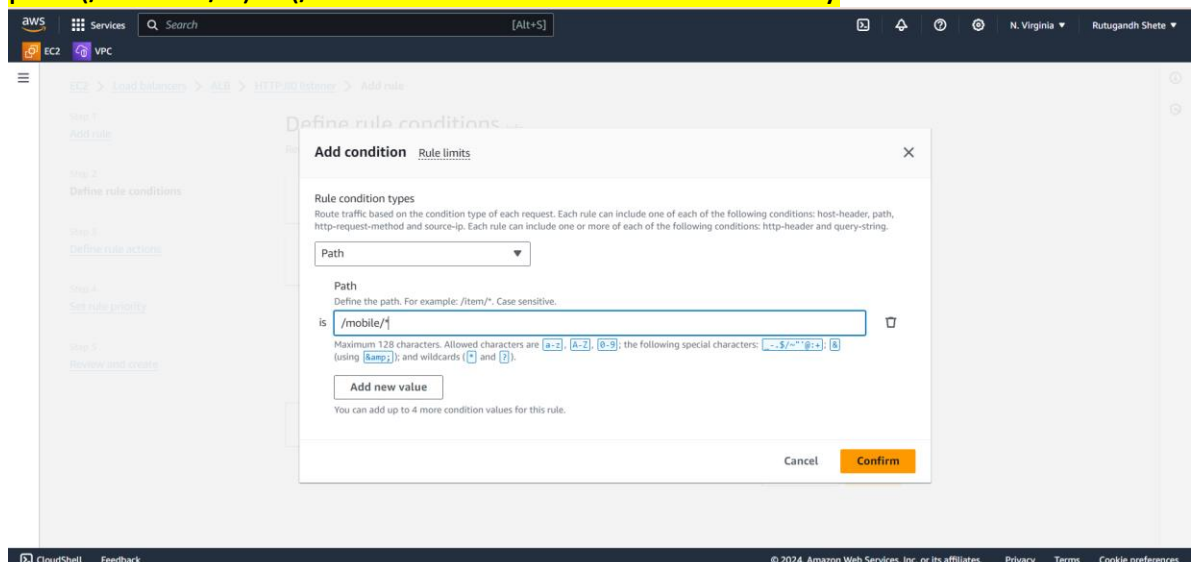
- For associating another target to same load balancer → **click on load balancer** → **listeners and rules**.



- Listeners and rules** → **click on HTTP80(port)** → **manage rules** → **add rule**



- Provide name → **click on next** → **add condition** → **click on path** → **provide path (/mobile/*)....(/* means all file after that directory)** → **confirm**



- Add target group → next

Define rule actions

Actions

Action types

Routing actions

☒ Forward to target group ☐ Redirect to URL ☐ Return fixed response

Forward to target group [Info](#)

Choose a target group and specify routing weight or [Create target group](#)

Target group

TG2 0-999

You can add up to 4 more target groups.

Target group stickiness [Info](#)

Enables the load balancer to bind a user's session to a specific target group. To use stickiness the client must support cookies. If you want to bind a user's session to a specific target, turn on the Target Group attribute Stickiness.

☐ Turn on target group stickiness

- Provide priority number → next → see all details → create

Listener details: HTTP:80

Rule: mobile

Priority

Rule priority controls the evaluation order of a rule within the listener's set of rules. You can leave gaps in priority numbers.

1 - 50000

Listener rules (2) [Info](#) [Rule limits](#)

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.

Name tag	Priority	Conditions (If)	Actions (Then)	ARN
mobile	1	Path Pattern is /mobile/*	Forward to target group <ul style="list-style-type: none"> TG2: 1 (100%) Target group stickiness: Off 	Pending

- After adding listener rule

HTTP:80 [ALB](#)

Forward to target group

- TG2: 1 (100%)
- Target group stickiness: Off

Listener ARN

arn:aws:elasticloadbalancing:us-east-1:211125626284:listener/app/ALB/bab1ad55adb78428/c556f7e9687494b9

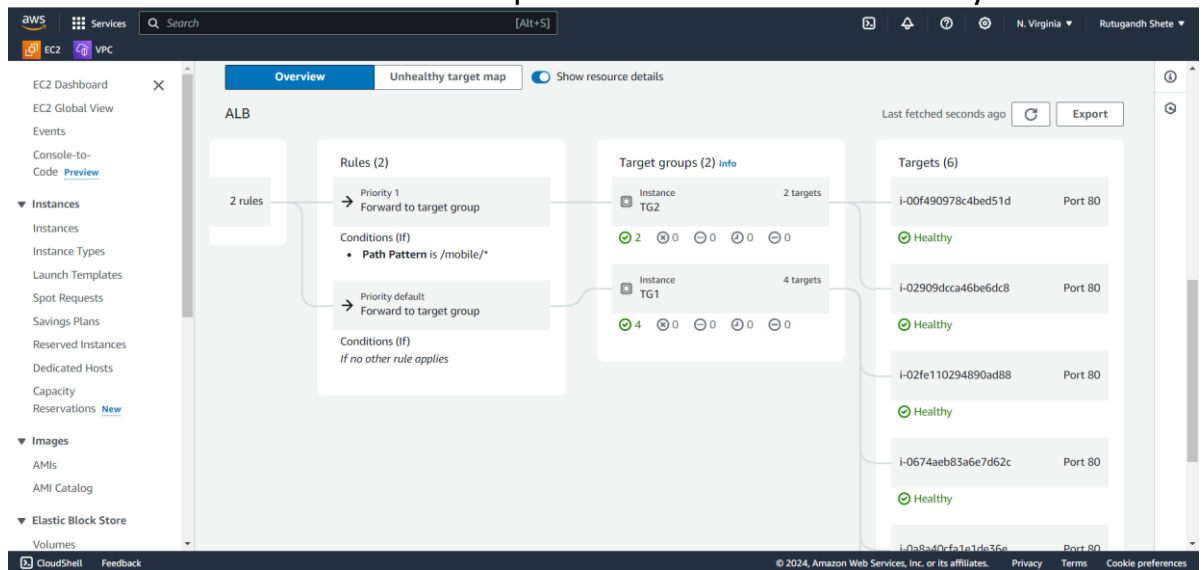
Rules **Tags**

Listener rules (2) [Info](#) [Rule limits](#) [Actions](#)

Traffic received by the listener is routed according to the default action and any additional rules. Rules are evaluated in priority order from the lowest value to the highest value.

<input type="checkbox"/>	Name tag	Priority	Conditions (If)	Actions (Then)	ARN
<input type="checkbox"/>	mobile	1	Path Pattern is /mobile/*	Forward to target group <ul style="list-style-type: none"> TG2: 1 (100%) Target group stickiness: Off 	<input type="button" value="ARN"/>
<input type="checkbox"/>	Default	Last (default)	If no other rule applies	Forward to target group <ul style="list-style-type: none"> TG1: 1 (100%) Target group stickiness: Off 	<input type="button" value="ARN"/>

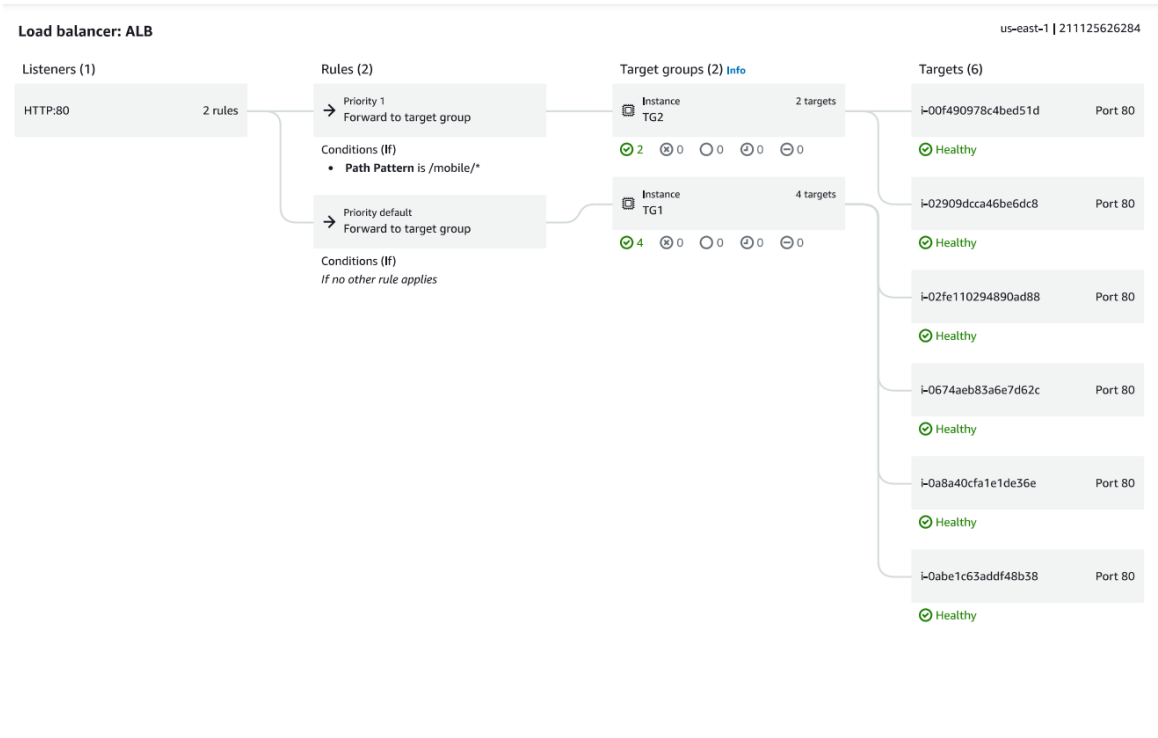
- To check whether the instances added are healthy or not then click application load balancer → resource and map → check instances are healthy or not



- As we can see that after pasting DNS of application load balancer on browser we are able to navigate through target one and for target group 2 “DNSpath link/mobile/” add this path and after pasting it we are able to navigate through target group 2.

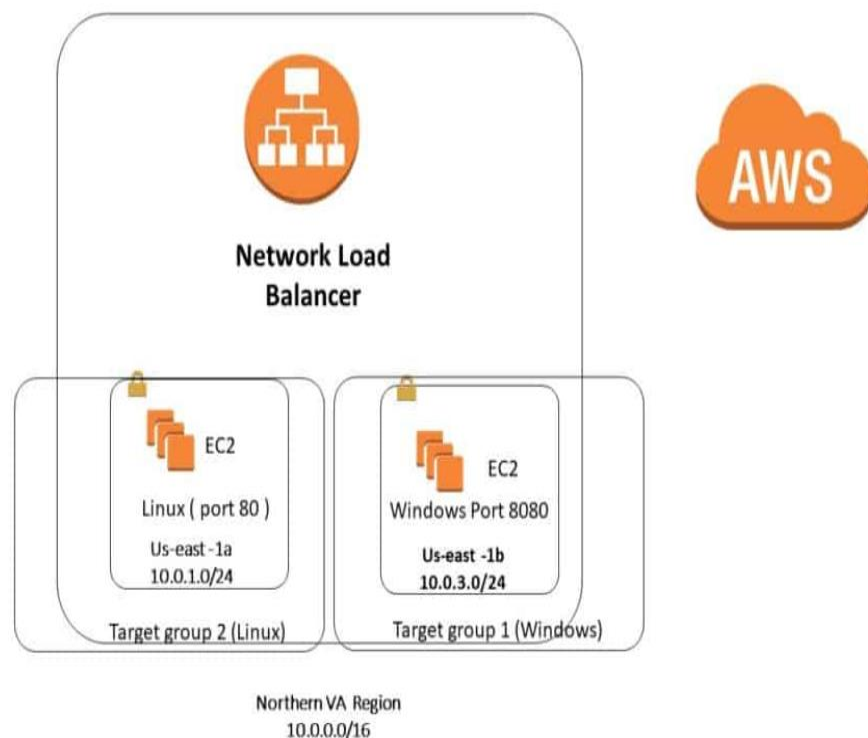


- In this diagram we can see that after adding target group there are healthy checks.



Network load balancer:

Network Load Balancer target groups support the TCP, UDP, TCP_UDP, and TLS protocols. You can register a target with multiple target groups. You can configure health checks on a per target group basis. Health checks are performed on all targets registered to a target group that is specified in a listener rule for your load balancer. A Network Load Balancer functions at the fourth layer of the Open Systems Interconnection (OSI) model. It can handle millions of requests per second. After the load balancer receives a connection request, it selects a target from the target group for the default rule. It attempts to open a TCP connection to the selected target on the port specified in the listener configuration.



Steps:

- Create **more than one instances** for time being and while creating it add script to user data.

Metadata response hop limit: 2

Allow tags in metadata: Select

User data - optional: Upload a file with your user data or enter it in the field.

Choose file

```
#!/bin/bash
apt update
apt install nginx -y
echo " This is my IP $(hostname) " > /var/www/html/index.html
```

Summary

Number of instances: 1

When launching more than 1 instance, consider EC2 Auto Scaling

Software Image (AMI): Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0a4d1a99f5ec58529

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

Launch instance

Instances (6)

Find Instance by attribute or tag (case-sensitive)

Instance state = running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
instance-2	i-00f490978c4bed51d	Terminated	t2.micro	2/2 checks passed	View alarms	us-east-1e
instance-2	i-02909dcca46be6dc8	Terminated	t2.micro	2/2 checks passed	View alarms	us-east-1e
instance-1	i-0abe1c63addf48b38	Running	t2.micro	2/2 checks passed	View alarms	us-east-1e
instance-1	i-0674aeb83a6e7d62c	Running	t2.micro	2/2 checks passed	View alarms	us-east-1e
instance-1	i-02fe110294890ad88	Running	t2.micro	2/2 checks passed	View alarms	us-east-1e
instance-1	i-0a8a40cfa1e1de36e	Running	t2.micro	2/2 checks passed	View alarms	us-east-1e

- Go to load balancers → create → network load balancer → provide name

Basic configuration

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

Scheme: Scheme can't be changed after the load balancer is created. Internet-facing (selected)

Load balancer IP address type: 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. IPv4 (selected)

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

- Select zones as per the instances zones and select security group that we have attached to instances

IPv4 subnet CIDR: 172.31.48.0/20

IPv4 address
The front-end IPv4 address of the load balancer in the selected Availability Zone.

☒ Assigned by AWS ☐ Use an Elastic IP address

☐ us-east-1f (use1-az5)

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 - recommended
Security groups support on Network Load Balancers can only be enabled at creation by including at least one security group. You can change security groups after creation. The security groups for your load balancer must allow it to communicate with registered targets on both the listener port and the health check port. For PrivateLink Network Load Balancers, security group rules are enforced on PrivateLink traffic; however, you can turn off inbound rule evaluation after creation within the load balancer's Security tab or using the API.

Select up to 5 security groups

SG-1
sg-0c94811af6ac2f840 VPC: vpc-05ddac7397bf4a7fd

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.

- Add target group for that we have to create target group → click on target group → add name

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

network_tg

- After that → next → include all instances → create.

1-65535 (separate multiple ports with commas)

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

Review targets

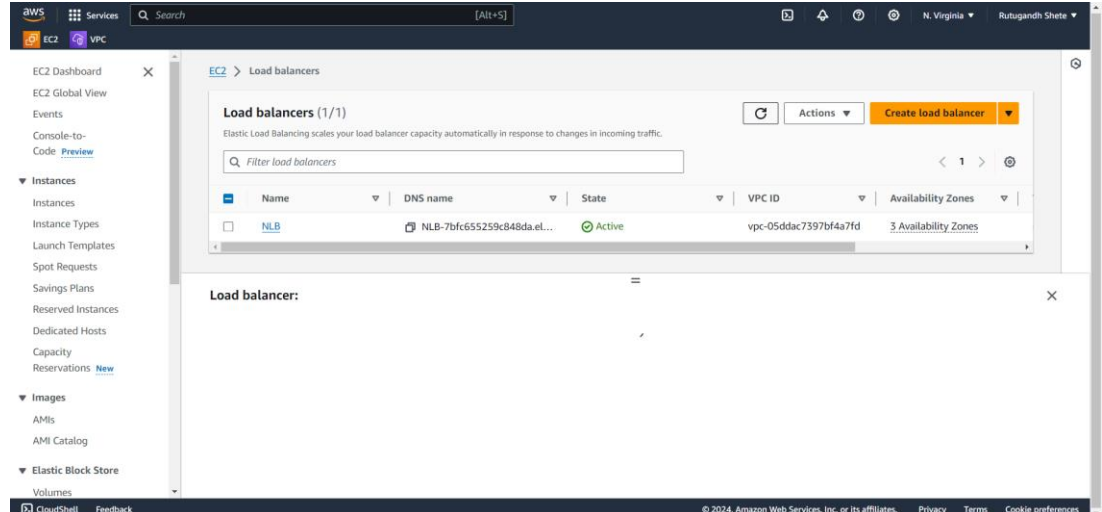
Targets (4)

☐ Show only pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID
i-0abe1c63addf48b38	instance -1	80	Running	SG-1	us-east-1e	172.31.63.236	subnet-077
i-0674aeb83a6e7d62c	instance -1	80	Running	SG-1	us-east-1e	172.31.63.95	subnet-077
i-02fe110294890ad88	instance -1	80	Running	SG-1	us-east-1e	172.31.61.211	subnet-077
i-0a8a40cfa1e1de36e	instance -1	80	Running	SG-1	us-east-1e	172.31.62.228	subnet-077

4 pending

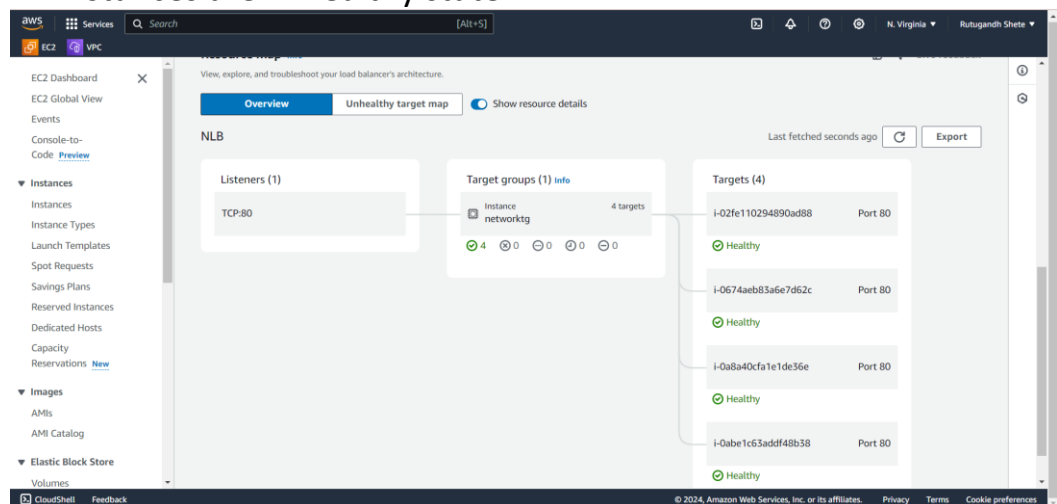
- After creating network load balancer



- Copy DNS on browser

this is IP ip-172-31-63-236

- All instances are in healthy state.



- Imagine you have a web application running on multiple EC2 instances across different Availability Zones. You would set up an NLB with a listener on port 443 (HTTPS), create a target group with your EC2 instances, and enable health checks. When users access your web application, the NLB routes the traffic to the healthiest and nearest EC2 instance, balancing the load efficiently while providing high availability.