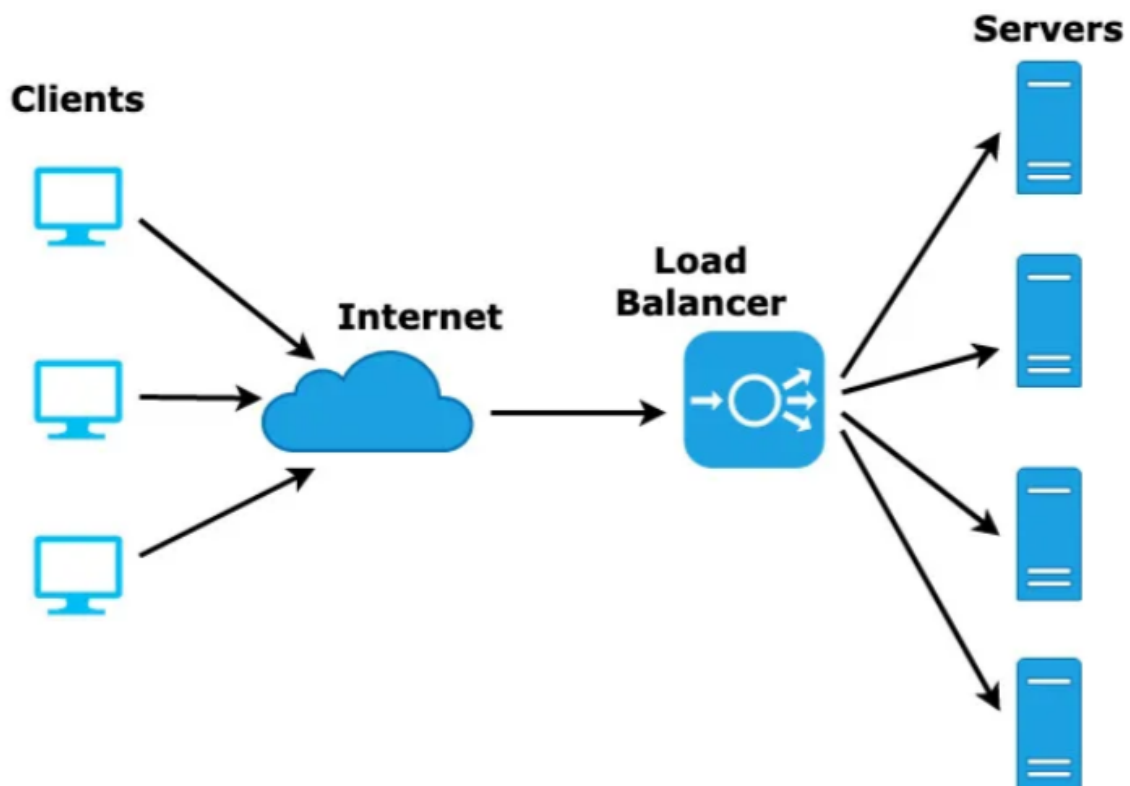


LOAD BALANCE

LAUNCHING IN TWO MACHINE

Load balance is takes traffic from user /customer and distribute traffic of server / target machine(it follows the round robin method)

Load balance continuously monitors the health registered targets of the server and route traffic only healthy target.it will send pins requested to the server. every 5 second send ping request if server not response ping request twice . load balance treated as unhealthy machine and stop traffic and distribute traffic to another machine. Once the server turns to a healthy state it resumes the traffic to healthy targets



Load balance can be classified into three types

Application Load balance

Network Load balance

Gateway Load balance

Application load balance :

Application load balance can be used in http and Https traffic routing

Its load balance works the application layer of the OSI model.

The load balancer also supports the dynamic host port mapping

Launching in Application load balancer in AWS console

For launching the load balancer you need two instances and one load balancer is required and security group used to handle the inbound and outbound traffic and it acts as a firewall

1. Launch an EC2 instance (two machines and install the web server)
2. Launch a load balancer
3. Create the security group

Go the aws console serch ec2 instance

1. Choose the ami(image)

EC2 > Instances > Launch an instance

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

mylinux

Add additional tags

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q linux

×

[AMI from catalog](#)

Quick Start

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI
ami-0416c18e75bd69567

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

Cancel

Launch instance

[Review commands](#)

Activate Windows

2. choose the instance type (os Ram)

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Amazon Linux 2023 AMI 2023.2.2...[read more](#)
ami-0416c18e75bd69567

Virtual server type (instance type)

t3.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

3.configure the instance type (go the user data install the web server given command below)

The screenshot shows the AWS Management Console for an EC2 instance. The 'User data' field is populated with the following bash script:

```
#!/bin/bash
yum update-y
yum install -y httpd -y
cd /var/www/html
echo "application of server1">index.html
service start httpd
chkconfig httpd on
```

The 'Summary' panel on the right shows the following configuration:

- Number of instances: 1
- Software Image (AMI): Amazon Linux 2023 AMI (ami-0416c18e75bd69567)
- Virtual server type (instance type): t3.micro
- Firewall (security group): New security group
- Storage (volumes): 1 volume(s) - 8 GiB

Buttons at the bottom include 'Cancel', 'Launch instance', and 'Review commands'.

4.add the storage aws provided default as (8gb ram)

The screenshot shows the 'Configure storage' section of the AWS Management Console. It displays a root volume configuration:

- 1x 8 GiB gp3 Root volume (Not encrypted)

A notification box states: "Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage".

Below the notification, there is a button labeled "Add new volume".

At the bottom, there is a section for backup information with a refresh icon and a link to "Edit".

5.add the tags

▼ Name and tags [Info](#)

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

Key [Info](#)

Value [Info](#)

Resource types [Info](#)

You can add up to 48 more tags.

6.choose the security group and allow the http traffic

▼ Network settings [Info](#)

Network [Info](#)

vpc-076d0ca61d174d027

Subnet [Info](#)

No preference (Default subnet in any availability zone)

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

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

0.0.0.0/0

☐ Allow HTTPS traffic from the internet

To set up an endpoint, for example when creating a web server

☒ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

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.

7.review the and launch instance

Go to the EC2 details, copy the public IP address and paste in Google browser because webserver working correctly or not

The screenshot displays the AWS Management Console interface for an EC2 instance. At the top, there's a header for 'Instances (1/1)' with a search bar and buttons for 'Connect', 'Instance state', 'Actions', and 'Launch instances'. Below this is a table with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. A single instance is listed with ID 'i-027960345dabba462', state 'Running', type 't3.micro', and status '2/2 checks passed'. Below the table, the details for instance 'i-027960345dabba462' are shown in a card format. The card includes sections for 'Instance summary', 'Public IPv4 address' (51.20.134.201), 'Private IPv4 addresses' (172.31.18.47), 'Instance state' (Running), 'Public IPv4 DNS' (ec2-51-20-134-201.eu-north-1.compute.amazonaws.com), 'Private IP DNS name (IPv4 only)' (ip-172-31-18-47.eu-north-1.compute.internal), and 'Hostname type' (IP name: ip-172-31-18-47.eu-north-1.compute.internal). There is also a note to 'Activate Windows'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
	i-027960345dabba462	Running	t3.micro	2/2 checks passed	No alarms	eu-north-1a	ec2-51-20-134-201.eu-north-1.compute.amazonaws.com

Instance: i-027960345dabba462

Instance summary

Instance ID: i-027960345dabba462

IPv6 address: -

Hostname type: IP name: ip-172-31-18-47.eu-north-1.compute.internal

Answer private resource DNS name

Public IPv4 address: 51.20.134.201 [open address](#)

Instance state: **Running**

Private IP DNS name (IPv4 only): ip-172-31-18-47.eu-north-1.compute.internal

Private IPv4 addresses: 172.31.18.47

Public IPv4 DNS: ec2-51-20-134-201.eu-north-1.compute.amazonaws.com [open address](#)

Activate Windows: Go to Settings to activate Windows.

Launch the another instance as shown a below

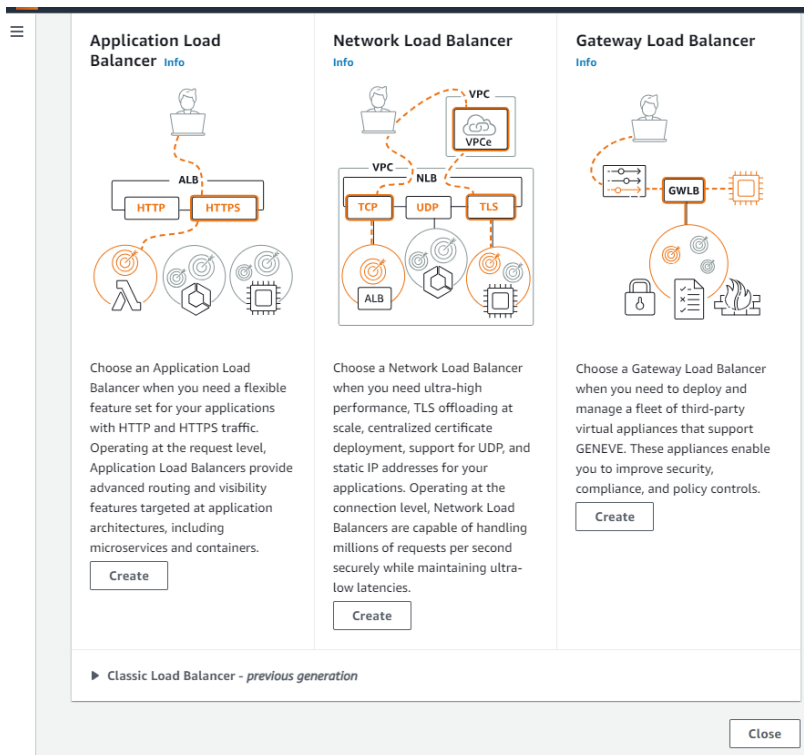
2. Choose the load balance as shown in below

The screenshot shows the 'Load balancers' page in the AWS Management Console. The page title is 'Load balancers' with a subtitle 'Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.' There is a search bar and a 'Create load balancer' button. Below this is a table with columns: Name, DNS name, State, VPC ID, Availability Zones, Type, and Date. The table is currently empty, and a message states 'No load balancers. You don't have any load balancers in eu-north-1'.

Name	DNS name	State	VPC ID	Availability Zones	Type	Date
------	----------	-------	--------	--------------------	------	------

No load balancers
You don't have any load balancers in eu-north-1

Steps to create load balance as shown below



1. Created as Application load balance it allow the http and https traffic as shown as below

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 loadbalancer

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.

When we deal with public ip go the internet-facing and internal ip means the public ip

Choose the both ipv4 and ipv6 go the dual stack as mentioned as below figure

2. choose the network mapping as shown in figure and check and ec2 - instance availability zone mentioned checkbox as below two mapping one default and another one you need mentioned .

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

VPC [Info](#)
Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

-
vpc-076d0ca61d174d027
IPv4: 172.31.0.0/16

↺

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.

☒ **eu-north-1a (eun1-az1)**

Subnet

subnet-068fec48f07d4190d

IPv4 address
Assigned by AWS

IPv6 address
None

☐ **eu-north-1b (eun1-az2)**

☐ **eu-north-1c (eun1-az3)**

3. choose the security group and mentioned ec2 instance security group one default and another one is ec2 security group

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

↺

↻

launch-wizard-1
sg-0a92f0eca18a10145 VPC: vpc-076d0ca61d174d027

×

default
sg-0a4581da509181b1f VPC: vpc-076d0ca61d174d027

×

4.Application load balance allow only http and https as below

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

Port

Default action

[Info](#)

HTTP ▼

:

80

Forward to

Select a target group ▼

↺

1-65535

[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

5.created target group as below and given the target group name

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

kamalnadh

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 ▼

80

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.

6. change the health check and unhealthy check as below as save and go the next

▼ Advanced health check settings

Restore defaults

Health check port

The port the load balancer uses when performing health checks on targets. By default, the health check port is the same as the target group's traffic port. However, you can specify a different port as an override.

☒ Traffic port

☐ Override

Healthy threshold

The number of consecutive health checks successes required before considering an unhealthy target healthy.

2-10

Unhealthy threshold

The number of consecutive health check failures required before considering a target unhealthy.

2-10

Timeout

The amount of time, in seconds, during which no response means a failed health check.

seconds

2-120

Interval

The approximate amount of time between health checks of an individual target

seconds

5-300

Success codes

The HTTP codes to use when checking for a successful response from a target. You can specify multiple values (for example, "200,202") or a range of values (for example, "200-299").

7. register two instance in target group as click on pending status

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 (2/2)

☒

i-05ec0424727dcfa85

linux2

Running

launch-wizard-1

eu-north-1a

☒

i-027960345dabba462

linux1

Running

launch-wizard-1

eu-north-1a

2 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

1-65535 (separate multiple ports with commas)

Include as pending below

Review targets

Targets (0)

Show only pending

Remove all pending

Go to Settings to activate Windows

Review targets

Targets (2)

Remove all pending

☐ Show only pending

< 1 > ⚙

Remove	Health status ▾	Instance ID ▾	Name ▾	Port ▾	State ▾	Security groups
✕	Pending	i-05ec0424727dcfa85	linux2	80	✔ Running	launch-wizard-1
✕	Pending	i-027960345dabba462	linux1	80	✔ Running	launch-wizard-1

2 pending

Cancel

Previous

Create target group

Go to Settings to activate Windows

Targets | Monitoring | Health checks | Attributes | Tags

Registered targets (2/2) [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.

< 1 > ⚙

<input checked="" type="checkbox"/>	Instance ID ▾	Name ▾	Port ▾	Zone ▾	Health status ▾	Health status details	Anomaly detect
<input checked="" type="checkbox"/>	i-05ec0424727dcfa85	linux2	80	eu-north-1a	⏸ Unused	Target group is not co...	✔ Normal
<input checked="" type="checkbox"/>	i-027960345dabba462	linux1	80	eu-north-1a	⏸ Unused	Target group is not co...	✔ Normal

Activate Windows

Go the load balance is the copy as DNS and paste

EC2 > Load balancers > sita

sita

⌂

Actions

▼ Details

Load balancer type

Application

Status

✔ Active

VPC

[vpc-076d0ca61d174d027](#)

IP address type

IPv4

Scheme

Internet-facing

Hosted zone

Z23TAZ6LKFMNIO

Availability Zones

[subnet-05bbcb37296e00684](#) eu-north-1c (eun1-az3)

[subnet-068fec48f07d4190d](#) eu-north-1a (eun1-az1)

Date created

December 1, 2023, 17:01 (UTC+09:00)

Load balancer ARN

arn:aws:elasticloadbalancing:eu-north-1:576366148202:loadbalancer/app/sita/88d5826dd8aa6249

DNS name [info](#)

sita-1829200149.eu-north-1.elb.amazonaws.com (A Record)

The paste dns and google chrome if traffic move on one server to another server as shown as figure

← → ↻

⚠ Not secure

sita-1829200149.eu-north-1.elb.amazonaws.com

🔖

☆

my application server

← → ↻

⚠ Not secure

sita-1829200149.eu-north-1.elb.amazonaws.com

🔖

☆

my applicationserver1

Then you refresher as server then move traffic to another webserver as shown in figure

