

# AWS EC2 Application Load Balancer – Step-by-Step

## Introduction to AWS Load Balancer

An **AWS Load Balancer** automatically distributes incoming application traffic across multiple **Amazon EC2 instances**, ensuring:

- High availability
- Fault tolerance
- Better performance
- Scalability

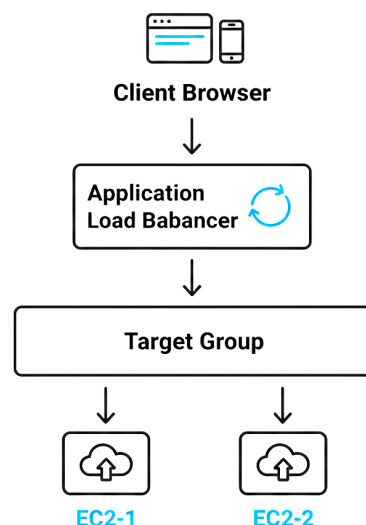
AWS provides this service through **Elastic Load Balancing (ELB)**.

## OBJECTIVE

To configure an Application Load Balancer (ALB) using the AWS Management Console and distribute HTTP traffic across multiple EC2 instances with health checks.

## ARCHITECTURE OVERVIEW

Client Browser → Application Load Balancer → Target Group → EC2 Instances (Multi-AZ)



## STEP 1: Launch EC2 Instances (Console Steps)

1. Launch at least 2 EC2 instances.

**User data (Optional but recommended for testing):** To easily differentiate which instance the load balancer is sending traffic to, you can install a simple web server with custom content.

- Select "As text" and paste the following (adjusting the content for **Instance 1** and **Instance 2** for each instance):

### Instance 1

```
#!/bin/bash
sudo su
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "hii Aswin" > /var/www/html/index.html
```

### Instance 2

```
#!/bin/bash
sudo su
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "hii Aswin vtk" > /var/www/html/index.html
```

# STEP 2: Create Target Group (Console Steps)

- 1. Go to EC2 Dashboard
- 2. Click Target Groups → Create target group
- 3. Choose:

- Target type: Instance
- Target group name: my-target-group

- Protocol: HTTP

- Port: 80

- VPC: Default

## 4. Health Check:

- Protocol: HTTP

- Path: /

Create target group

A target group can be made up of one or more targets. Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Settings - immutable

Choose a target type and the load balancer and listener will route traffic to your target. These settings can't be modified after target group creation.

Target type

Indicate what resource type you want to target. Only the selected resource type can be registered to this target group.

Instances

Supports load balancing to instances in a VPC. Integrate with Auto Scaling Groups or ECS services for automatic management.

Suitable for: ALB NLB GWLB

IP addresses

Supports load balancing to VPC and on-premises resources. Facilitates routing to IP addresses and network interfaces on the same instance. Supports IPv6 targets.

Suitable for: ALB NLB GWLB

Lambda function

Supports load balancing to a single Lambda function. ALB required as traffic source.

Suitable for: ALB

Application Load Balancer

Allows use of static IP addresses and PrivateLink with an Application Load Balancer. NLB required as traffic source.

Suitable for: NLB

Target group name

Name must be unique per Region per AWS account.

Accepts: a-z, A-Z, 0-9, and hyphen (-). Can't begin or end with hyphen. 1-32 total characters; Count: 0/32

Protocol

Protocol for communication between the load balancer and targets.

HTTP

Port

Port number where targets receive traffic. Can be overridden for individual targets during registration.

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.

IPv6

Each instance must have a configured secondary IPv6 address. This is configured on the instance's default network interface (eth0) using the `ipv6-addr` parameter.

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.

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.

/

Up to 1024 characters allowed.

Advanced health check settings

Target optimizer - optional

Use a target control port when the target has a strict concurrency limit.

Target control port

The port on which the target communicates its capacity. This value can't be modified after target group creation.

Enter target control port

Valid range: 1-65535

Attributes

1

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

Tags - optional

## 5. Click Next

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)

Filter instances

<input checked="" type="checkbox"/>	Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID
<input checked="" type="checkbox"/>	i-00827b19b830a770b		Running	mysg	ap-south-2c	172.31.17.132	subnet-016448d4c28ee547e
<input checked="" type="checkbox"/>	i-0b66a21630748fe00	aswin	Running	mysg	ap-south-2c	172.31.24.167	subnet-016448d4c28ee547e

2 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

80

1-65535 (separate multiple ports with commas)

Include as pending below

Review targets

Targets (0)

Filter targets

Show only pending

Remove all pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
No instances added yet								
Specify instances above, or leave the group empty if you prefer to add targets later.								

## 6. Select EC2 instances → click the button below " included as pending below " Add to registered

Filter instances

<input type="checkbox"/>	Instance ID	Name	State	Security groups	Zone	Private IPv4 address	Subnet ID
<input type="checkbox"/>	i-00827b19b830a770b		Running	mysg	ap-south-2c	172.31.17.132	subnet-016448d4c28ee547e
<input type="checkbox"/>	i-0b66a21630748fe00	aswin	Running	mysg	ap-south-2c	172.31.24.167	subnet-016448d4c28ee547e

0 selected

Ports for the selected instances

Ports for routing traffic to the selected instances.

80

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

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
<a href="#">i-00827b19b830a770b</a>		80	Running	mysg	ap-south-2c	172.31.17.132	subnet-016448d4c28ee547e	December 28, 2025, 12:26 (UTC+05:30)
<a href="#">i-0b66a21630748fe00</a>	aswin	80	Running	mysg	ap-south-2c	172.31.24.167	subnet-016448d4c28ee547e	December 28, 2025, 12:24 (UTC+05:30)

2 pending

Cancel Previous Next

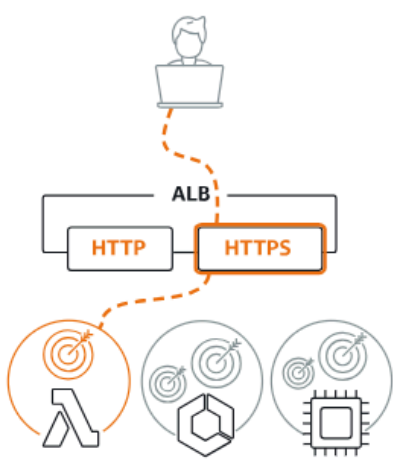
## 7. Click Create target group

# STEP 3: Load Balancer (Console Steps)

## Type of Loadbalancer

### Load balancer types

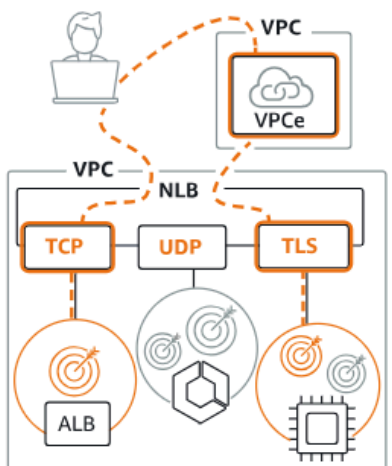
#### Application Load Balancer [Info](#)



Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

Create


#### Network Load Balancer [Info](#)



Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Create

#### Gateway Load Balancer [Info](#)

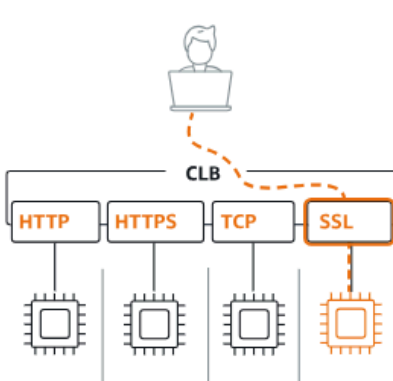


Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

### ▼ Classic Load Balancer - *previous generation*

#### Classic Load Balancer [Info](#)



Choose a Classic Load Balancer when you have an existing application running in the EC2-Classical network.

Create

## Continue with Application Loadbalancer

1. Go to EC2 → Load Balancers
2. Click Create Load Balancer
3. Select Application Load Balancer
4. Basic Configuration:

- Name:
- Scheme: Internet-facing
- IP address type: IPv4

**Basic configuration**

**Load balancer name**  
Name must be unique within your AWS account and can't be changed after the load balancer is created.  
  
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 resolves to public IPs.
- Requires a public subnet.

☐ **Internal**

- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- 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.

5. Network Mapping:

- Select VPC
- **Select minimum two Availability Zones**

**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](#).

(default) [Create VPC](#)

**IP pools** | [Info](#)  
You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view [Pools](#) in the [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.

☐ **ap-south-2a (aps2-az1)**

☐ **ap-south-2b (aps2-az2)**

☐ **ap-south-2c (aps2-az3)**

6. Security Groups: - Select or create SG allowing HTTP (80)

**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**  
 [Create](#)

## 7. Listener:

- HTTP:80 → Forward to my-target-group

**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](#)  
The default action is used if no other rules apply. Choose the default action for traffic on this listener.

**Routing action**

☒ Forward to target groups ☐ 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	Weight	Percent
<input type="text" value="Select a target group"/>	<input type="text" value="1"/> <small>0-999</small>	<input type="text" value="100%"/>

[+ Add target group](#)  
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. 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

**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.

## 8. Click Create Load Balancer

### STEP 4 : Update EC2 Security Group

1. Go to EC2 → Security Groups
2. Select EC2 instance security group
3. Edit Inbound Rules:
  - HTTP (80) → Source: Load Balancer Security Group
  - SSH (22) → My IP
4. Save rules

### STEP 5 : Verify Target Health

1. Go to EC2 → Target Groups
2. Select my-target-group
3. Open Targets tab
4. Confirm Status = Healthy

## STEP 7: Test Load Balancer

1. Go to EC2 → Load Balancers
2. Copy Load Balancer DNS name
3. Paste DNS in browser
4. Refresh multiple times
5. Observe response switching between EC2 servers

