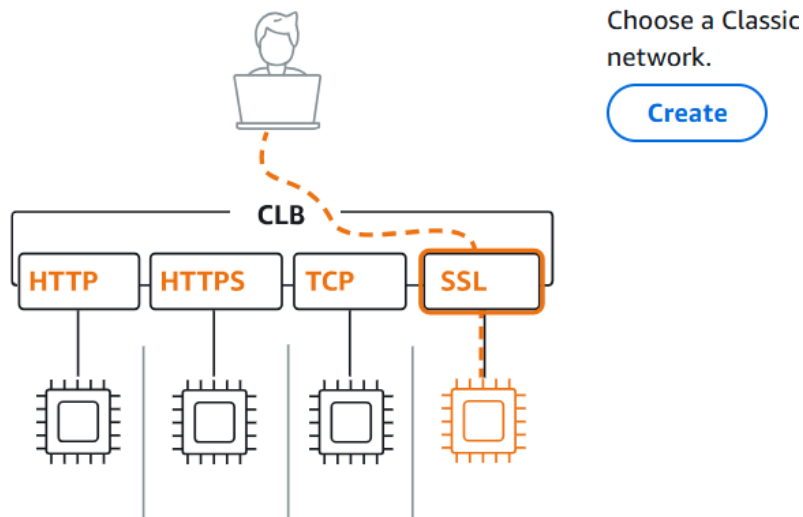


# Load Balancers

1. Configure Classic Load balancer.
  - Open aws console
  - Navigate to ec2 > launch an instance
  - Install httpd in ec2 instance
  - Now go to load balancer
  - create a classic load balancer,

## ▼ Classic Load Balancer - *previous generation*

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



- 
- Attach vpc and subnets from different availability zones
- Add one running instance

## Add instances

Select EC2 instances to register to your load balancer. Requests will be routed to registered instances that meet the health check requirement maintaining approximately equivalent numbers of instances in each Availability Zone enabled for the load balancer. If demand on your instances without disrupting the flow of requests to your application. [Learn more](#)

### VPC

vpc-0ad3c0b33fedc285e

### Available instances (1/2)

Filter available instances

<input type="checkbox"/>	Instance ID	Name	State	Security groups
<input checked="" type="checkbox"/>	i-0bc2cb72c8ca6f030	classic load	Running	default
<input type="checkbox"/>	i-01f12a13e564aefbb	autosacding-private	Stopped	default

- 
- Add ssl certificate

## Secure listener settings [Info](#)

These settings will apply to all of your secure listeners. Once created, you can manage these settings per listener.

### Security policy

[Info](#)

Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with

ELBSecurityPolicy-2016-08

[Customize policy](#)

### Default SSL/TLS server certificate

The certificate used if there are no matching certificates. This certificate will automatically be added to your listener certificate list.

#### Certificate source

☒ From ACM

☐ From IAM

#### Certificate (from ACM)

The certificate used if there are no matching certificates. This certificate will automatically be added to your listener certificate list.

kamalll.shop  
bb3f802e-8fcc-4ef3-93a6-0661c7cfe480



[Request new ACM certificate](#)

- Backend authentication certificate - optional

To enable backend server authentication and encryption, provide the public key certificates to trust. These certificates will apply to all

- Click create

### Successfully created load balancer: classic-lb

It might take a few minutes for your load balancer to be fully set up and ready to route traffic. Targets will also take a registration process and pass initial health checks.

### Introducing URL rewrite for Application Load Balancer

Modify host headers and URL paths of incoming requests before they reach your targets. To get started, add a rule to transform. [Learn more](#)

- Make sure, httpd is running, and `?var/ww/html/` contain webpage , if you check , `http://<instance public>` it should open in webpage,
- Then, when you create a load balancer, and adding the same instance to load balancer after creating you get a dns name > copy that and paste it in browser, the same webpage will appear
- Now copy the dns name provided by load balancer, and paste it in browser

**classic-lb**

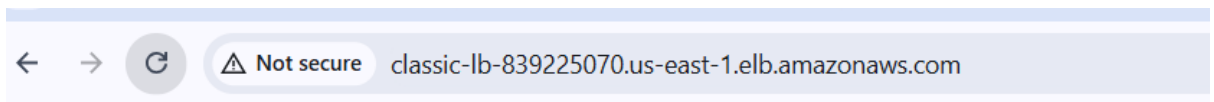
**▼ Details**

<b>Load balancer type</b> Classic	<b>Status</b> 1 of 1 instance in service	<b>VPC</b> <a href="#">vpc-0ad3c0b33fec285e</a>
<b>Scheme</b> Internet-facing	<b>Hosted zone</b> Z35SXDOTRQ7X7K	<b>Availability Zones</b> <a href="#">subnet-0e890e6d482e183aa</a> us-east-1a (use1-az4) <a href="#">subnet-01e8c875b370cd0aa</a> us-east-1b (use1-az6)

**DNS name** [Info](#)  
[classic-lb-839225070.us-east-1.elb.amazonaws.com](#) (A Record)

✔ DNS name copied

- Web page appears



## Welcome to my website via Load Balancer

- 
- To verify again , go to load balancer, in the below find target instance, see for health

Listeners | Network mapping | Security | Health checks | **Target instances** | Monitoring | Attribute

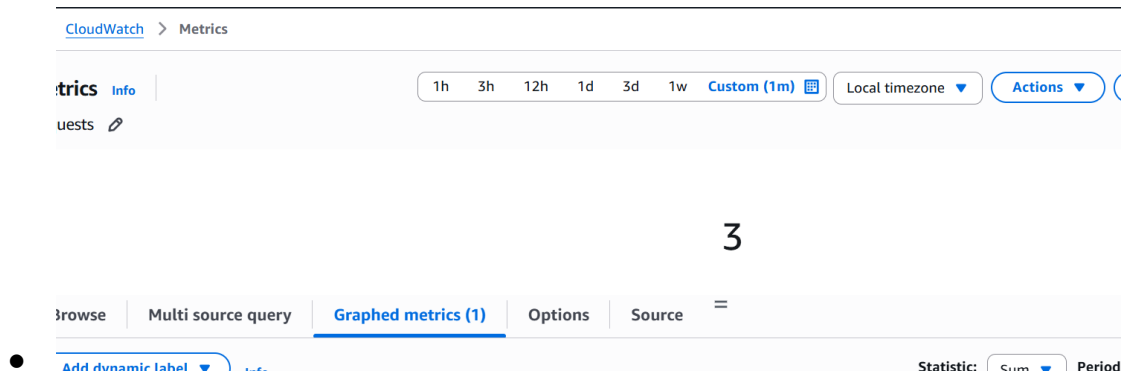
**Target instances (1)**
Connection draining: On (300 seconds)
Deregister

Instances currently registered to your load balancer are displayed. To deregister instances, select them, then choose Deregister. To register an instance simultaneously, choose Manage instances.

<input type="checkbox"/>	Instance ID	Name	Health status	Health status description
<input type="checkbox"/>	<a href="#">i-0bc2cb72c8ca6f030</a>	classic load	<span>✔ In-service</span>	Not applicable

- Status should be IN SERVICE

- Can monitor the requests from monitoring
- No of users are accessing our website.
- Only with dns name.



## 2.Configure Application Load balancer

WE NEED TO CREATE TARGET GROUPS FIRST FOR APPLICATION LOAD BALANCER.

- Ec2 > navigate to target groups
- Give name,
- Add vpc, and subnet,
- Select target instance and select pending as below

application-lb

Successfully created the target group: **application-lb**. Anomaly detection is automatically applied to all registered targets. Results can be viewed in the **Targets** tab.

**application-lb** [Actions](#)

**Details**

arn:aws:elasticloadbalancing:us-east-1:414691912691:targetgroup/application-lb/ae16eb95b5737e8

<b>Target type</b> Instance	<b>Protocol : Port</b> HTTP: 80	<b>Protocol version</b> HTTP1	<b>VPC</b> <a href="#">vpc-0ad3c0b33fec285e</a>
<b>IP address type</b> IPv4	<b>Load balancer</b> <a href="#">None associated</a>		

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

► **Distribution of targets by Availability Zone (AZ)**  
Select values in this table to see corresponding filters applied to the Registered targets table below.

- Now navigate load balancer
- Create an application load balancer
- Add vpc And subnets of different availability zone

..... 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 ☐ Re

**Forward to target group** | [Info](#)  
Choose a target group and specify routing weight or [create target group](#).

**Target group**

application-lb HTTP **Weight** 1 **Percent** 100%  
Target type: Instance, IPv4 | Target stickiness: Off 0-999

[+ Add target group](#)  
You can add up to 4 more target groups.

**Target group stickiness** | [Info](#)

- 
- Select the target group.
- Add acm certificate
- Create application load balancer,
- Copy dns name and paste it in browser and verify

← → ↻ ⚠ Not secure application-lb-1781086393.us-east-1.elb.amazonaws.com

## Welcome to my website via Load Balancer

- 
- Try this dns name in different devices, instances will be shuffling.

### 3. Configure Network Load balancer.

- EC2 > make sure 3 instances are running
- Installed with httpd in it and in running state

**Instances (3)** [Info](#) [Connect](#) [Instance state ▼](#) [Actions ▼](#) [Launch instances](#)

🔍 Find Instance by attribute or tag (case-sensitive) [All states ▼](#)

[Instance state = running](#) [Clear filters](#) < 1 >

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
<input type="checkbox"/>	testing-applic...	i-0a4cbcc0493321880	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>	us-east-1.
<input type="checkbox"/>	classic load	i-0bc2cb72c8ca6f030	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>	us-east-1.
<input type="checkbox"/>	network-lb	i-06ce380ec2ae29cd9	Running	t3.micro	3/3 checks passed	<a href="#">View alarms +</a>	us-east-1.

- Create target groups add 3 instances .

[Target groups](#) > Create target group

Register targets - *recommended*

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 y

Available instances (3/3)

Filter instances

<input checked="" type="checkbox"/>	Instance ID	Name	State	Security groups
<input checked="" type="checkbox"/>	i-06ce380ec2ae29cd9	network-lb	Running	default
<input checked="" type="checkbox"/>	i-0a4cbcc0493321880	testing-applicationlb	Running	default
<input checked="" type="checkbox"/>	i-0bc2cb72c8ca6f030	classic load	Running	default

- Group created

network-lb-group

Successfully created the target group: **network-lb-group**. Anom  
Targets tab.

## network-lb-group

**Details**

arn:aws:elasticloadbalancing:us-east-1:414691912691:targetgr

<b>Target type</b> Instance	<b>Protocol : Port</b> HTTP: 80
<b>IP address type</b> IPv4	<b>Load balancer</b> <a href="#">None associated</a>

3 Total targets	0 Healthy	0 Unhealt
	0 Anomalous	

- 
- Now navigate toLOAD BALANCER >> NETWORK LOAD BALANCER
- Add VPC and subnet of different availability zone.(because we need to add differently availability zone subnets only its mandatory).
- Add target group

▼ Listener HTTP:80

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

Forward to target group [Info](#)

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

Target group

network-lb-group

Target type: Instance, IPv4 | Target stickiness: Off

HTTP



Weight

1

0-999

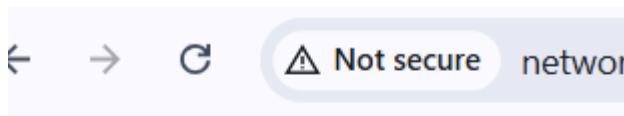
Percent

100%

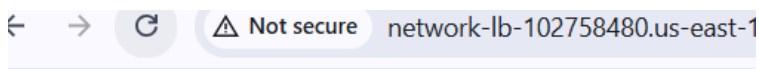
[+ Add target group](#)

You can add up to 4 more target groups.

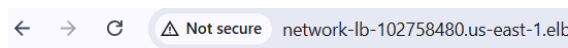
- Click create
- Now copy dns name in network load balancer and paste it in browser, you can see the web page shuffling from 1 > 2 > 3 when I try to refresh many times



this is 3 instance



Welcome — This is Instance 1



Welcome — This is Instance 2

#### 4 . Attach SSL for application load balancer.

- Create target group add 2 running instances
- Now go to application load balancer,
- Add name vpc and subnet
- Add one more listener
- Add https:443
- So it asks for acm certificate then we can add certificate.

[EC2](#) > [Load balancers](#) > [Create Application Load Balancer](#)

### Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules to registered targets.

▶ Listener HTTP:80

▼ Listener HTTPS:443

Protocol

HTTPS

Port

443

1-65535

### Default action [Info](#)

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

### Authentication action - optional [Info](#)

Authentication requires IPv4 connectivity to authentication endpoints. [Learn more](#)

☐ Authenticate users

Configure user authentication through either OpenID Connect (OIDC) or Amazon Cognito.

### Routing action

☒ Forward to target groups

☐ Redirect to URI

- Add certificate.

certificate. This certificate will automatically be added to your listener certificate.

### Certificate source

☒ From ACM

### Certificate (from ACM)

The selected certificate will be applied as the default SSL/TLS server certificate

kamalll.shop  
bb3f802e-8fcc-4ef3-93a6-0661c7cfe480

[Request new ACM certificate](#)



- Also add target group for second listener .

Configure user authentication through either OpenID Connect (OIDC) or Amazon Cognito.

Routing action

☒ Forward to target groups

☐ Redirect to URL

**Forward to target group** | [Info](#)  
Choose a target group and specify routing weight or [create target group](#).

**Target group**

application-lb-2-ssl

HTTP

Target type: Instance, IPv4 | Target stickiness: Off

[+ Add target group](#)

You can add up to 4 more target groups

- 

SSL added successfully

Load balancers

application-lb-2-ssl

HTTPS:443 listener

ew

s

lates

s

ances

sts

rvations

ager

Default certificate: kamalll.shop

Certificate ID

bb3f802e-8fcc-4ef3-93a6-0661c7cfe480

Name or domain

kamalll.shop

Status

Valid

SAN

1

Expiration

November 29, 2026, 05:29 (UTC+05:30)

Service

ACM

ARN

arn:aws:acm:us-east-1:414691912691:certificate/bb3f802e-8fcc-4ef3-93a6-0661c7cfe480

Type

Amazon-issued

Listener certificates for SNI (1)

Remove

Add certificate

Additional certificates support Server Name Indication (SNI). This enables the load balancer to support multiple domains on the same port and provide a different certificate for each domain.

Filter certificates

Certificate ID	Name or domain	Status	SAN	Expiration	Service	ARN
bb3f802e-8fcc-4ef3...	kamalll.shop	Valid	1	November 29, 2026, 05:...	ACM	arn:aw

## 5 . Map Application load balancer to R53.

- Open existing application load balancer,
- Copy dns name from application load balancer dash board

The screenshot displays the AWS Management Console interface for an Application Load Balancer. The top navigation bar shows 'application-lb' and a status of 'Active'. The main content area is titled 'Details' and contains several key pieces of information:

- Load balancer type:** Application
- Status:** Active (indicated by a green checkmark)
- VPC:** vpc-0ad3c0b33fec285e
- Load balancer IP address type:** IPv4
- Scheme:** Internet-facing
- Hosted zone:** Z35SXDOTRQ7X7K
- Availability Zones:** subnet-0e890e6d482e183aa (us-east-1a) and subnet-01e8c875b370cd0aa (us-east-1a)
- Date created:** November 5, 2025, 13:14 (UTC+05:30)
- Load balancer ARN:** arn:aws:elasticloadbalancing:us-east-1:414691912691:loadbalancer/app/application-lb/008805ced5e83732
- DNS name:** application-lb-1781086393.us-east-1.elb.amazonaws.com (A Record)

A green notification bubble with a checkmark and the text 'DNS name copied' is overlaid on the DNS name field. At the bottom, a horizontal menu includes tabs for 'Listeners and rules', 'Network mapping', 'Resource map', 'Security', 'Monitoring', 'Integrations', and 'Attributes'.

- Now navigate to R53 .
- We have already have hosted our domain from r53
- So open hosted zone and add records
- Click records
- Add type A
- Name : www
- Turn ALIAS
- Choose end point as ALIAS TO CLASSIC AND APPLICATION LOAD BALANCER.
- CHOOSE REGION – WHERE OUR APPLICATION LOAD BALANCER IS HOSTED, SELECT THAT REGION .
- Paste the copied dns name from load balancer here

Keep blank to create a record for the root domain.

☒ Alias

Route traffic to [Info](#)

Alias to Application and Classic Load Balancer

US East (N. Virginia)

Q application-lb-1781086393.us-east-1.elb.amazonaws.com|

Use: "application-lb-1781086393.us-east-1.elb.amazonaws.com"

dualstack.[application-lb-1781086393.us-east-1.elb.amazonaws.com](https://application-lb-1781086393.us-east-1.elb.amazonaws.com)

dualstack.application-lb-1781086393.us-east-1.elb.amazonaws.com

- Evaluate target health - ON.
- Now open browser and verify with www
- [www.kamalll.shop](http://www.kamalll.shop)

← → ↻ ⚠ Not secure kamalll.shop


# Welcome — This is Instance 1


6. Push the application load balancer logs to S3.

- Create a s3 bucket ,
- Write a policy script
- Open bucket go to permissions,
- For application logs to s3
- {
- "Version": "2012-10-17",
- "Statement": [- {
- "Sid": "AWSALBLoggingPermissions",
- "Effect": "Allow",
- "Principal": {

- "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
- },
- "Action": "s3:PutObject",
- "Resource": "arn:aws:s3:::application-lb-1/AWSLogs/\*"
- }
- ]
- }

 [Amazon S3](#) > [Buckets](#) > [application-lb-1](#)

 Successfully edited bucket policy.

 Public access is blocked because Block Public Access settings are turned on for this bucket. To determine which settings are turned on, check your Block Public Access settings.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSALBLoggingPermissions",
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::application-lb-1/AWSLogs/*"
    }
  ]
}
```

- Navigate to application load balancer
- Below find ATTRIBUTES

[Resource map](#)
[Security](#)
[Monitoring](#)
[Integrations](#)
[Attributes](#)
[Capacity](#)
[Tags](#)

Manage rules
Manage listener
Add listener

on its configured protocol and port. Traffic received by the listener is routed according to the default action and any

< 1 >

Default action	Rules	ARN	Security policy
<ul style="list-style-type: none"> <li>Forward to target group <a href="#">application-lb</a>: 1 (100%) Target group stickiness: Off</li> </ul>	<a href="#">1 rule</a>	ARN	ELBSecurityPolicy-TLS13-1-2-...
<ul style="list-style-type: none"> <li>Forward to target group <a href="#">application-lb</a>: 1 (100%) Target group stickiness: Off</li> </ul>	<a href="#">1 rule</a>	ARN	Not applicable

- OPEN ATTRIBUTES
- Edit attributes
- Monitoring add acces logs and attach s3 bucket

[EC2](#) > [Load balancers](#) > application-lb

[Snapshots](#)
[Lifecycle Manager](#)

### Network & Security

[Security Groups](#)
[Elastic IPs](#)
[Placement Groups](#)
[Key Pairs](#)
[Network Interfaces](#)

### Load Balancing

[Load Balancers](#)
[Target Groups](#)
[Trust Stores](#)

### Auto Scaling

[Auto Scaling Groups](#)

Preserve host header  
Off

### Availability Zone routing configuration

 Cross-zone load balancing  
On

### Protection

 Deletion protection  
Off

### Monitoring

 Access logs  
S3 location: [application-lb-1](#)

- Logs will appear in S3 BUCKET.