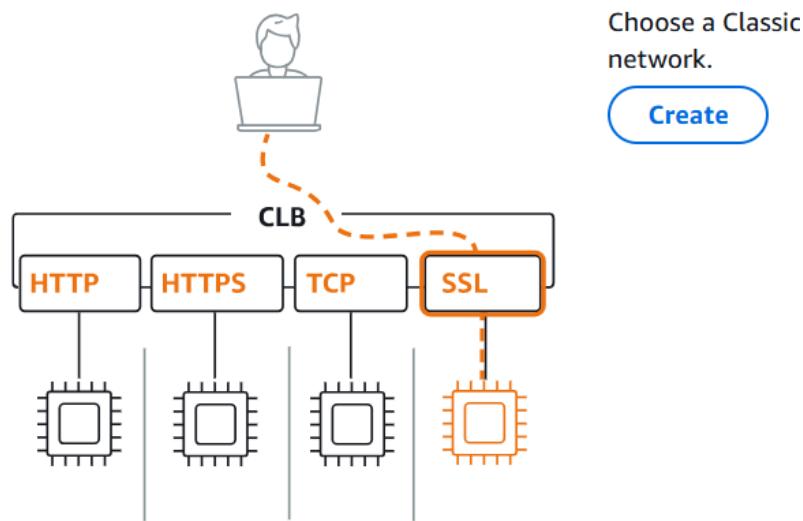


Load Balancers

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

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

kamall.shop

bb3f802e-8fcc-4ef3-93a6-0661c7fce480



[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 targets.

- 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

Load balancer type Classic	Status 1 of 1 instance in service	VPC vpc-0ad3c0b33fecd285e ↗
Scheme Internet-facing	Hosted zone Z35SXDOTRQ7X7K	Availability Zones subnet-0e890e6d482e183aa ↗ us-east-1a (use1-az4) subnet-01e8c875b370cd0aa ↗ us-east-1b (use1-az6)

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

● DNS name copied

● Web opage appears

← → ⏪ Not secure classic-lb-839225070.us-east-1.elb.amazonaws.com

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

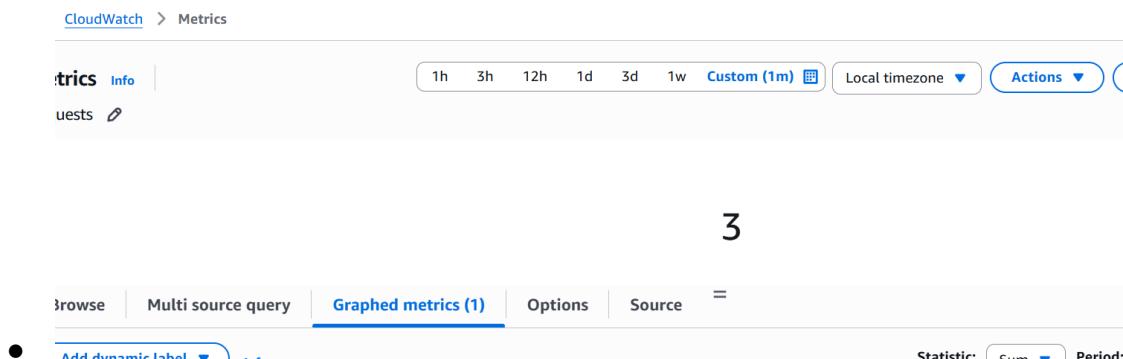
Instances currently registered to your load balancer are displayed. To deregister instances, select them, then choose Deregister. To register an simultaneously, choose Manage instances.

Filter target instances

<input type="checkbox"/> Instance ID	Name	Health status	Health status descri.
i-0bc2cb72c8ca6f030	classic load	In-service	Not applicable

-
- Status should be IN SERVICE

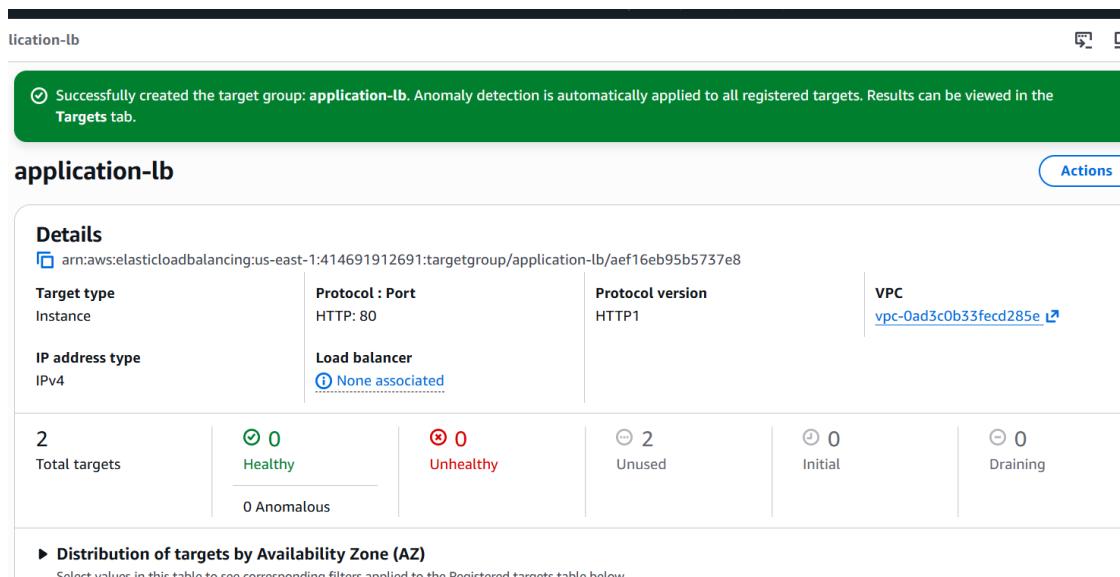
- Can monitor the requests from monitoring
- No of users are accessing our website.
- Only with dns name.



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



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

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

[+ 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 shuffled.

3 . Configure Network Load balancer.

- Ec2 > make sure 3 instances are running
- Installed with httpd in it and in running state

Instances (3) [Info](#)

[C](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find Instance by attribute or tag (case-sensitive)

[All states](#)

Instance state = running [X](#) [Clear filters](#)

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

Available instances (3/3)

Instance ID	Name	State	Security groups
i-06ce380ec2ae29cd9	network-lb	Running	default
i-0a4cbcc0493321880	testing-applicationlb	Running	default
i-0bc2cb72c8ca6f030	classic load	Running	default

- Group created

etwork-lb-group

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

network-lb-group

Details

arn:aws:elasticloadbalancing:us-east-1:414691912691:targetgroup/network-lb-group/12345678901234567890

Target type
Instance

Protocol : Port
HTTP: 80

IP address type
IPv4

Load balancer
[None associated](#)

3
Total targets

0

Healthy

0

Unhealthy

0 Anomalous

- Now navigate to LOAD 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

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.

- 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



his 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 tell the load balancer how to handle traffic from clients. You can add multiple listeners to your load balancer to support different protocols or port numbers.

▶ Listener HTTP:80

▼ Listener HTTPS:443

Protocol	Port
HTTPS	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.

kamall.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

Default certificate: kamall.shop Info		Change default	
The server certificate you specify when you first create a secure listener is taken as the default certificate. You can replace the default certificate after you create the listener.			
Certificate ID bb3f802e-8fcc-4ef3-93a6-0661c7cf480	Name or domain kamall.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-4ef3-93a6-0661c7cf480	Type Amazon-issued

Listener certificates for SNI (1) Info		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.															
<table border="1"> <thead> <tr> <th>Filter certificates</th> <th colspan="2">< 1 ></th> <th>Edit</th> </tr> <tr> <th><input type="checkbox"/> Certificate ID</th> <th>Name or domain</th> <th>Status</th> <th>SAN</th> </tr> </thead> <tbody> <tr> <td>bb3f802e-8fcc-4ef3...</td> <td>kamall.shop</td> <td>Valid</td> <td>1</td> </tr> </tbody> </table>				Filter certificates	< 1 >		Edit	<input type="checkbox"/> Certificate ID	Name or domain	Status	SAN	bb3f802e-8fcc-4ef3...	kamall.shop	Valid	1
Filter certificates	< 1 >		Edit												
<input type="checkbox"/> Certificate ID	Name or domain	Status	SAN												
bb3f802e-8fcc-4ef3...	kamall.shop	Valid	1												

5 . Map Application load balancer to R53.

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

The screenshot shows the AWS Application Load Balancer (ALB) configuration page. The 'Listeners and rules' tab is active. In the 'Details' section, the 'VPC' row shows the VPC ID 'vpc-0ad3c0b33fecd285e'. A tooltip 'DNS name copied' is displayed over the 'DNS Name' field, which contains the value 'application-lb-1781086393.us-east-1.elb.amazonaws.com (A Record)'. Other tabs visible include 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)

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](#)

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

← → ⌂ ⚠ 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

The screenshot shows the AWS Load Balancer configuration page. At the top, there are tabs: Resource map, Security, Monitoring, Integrations, Attributes, Capacity, and Tags. Below the tabs are buttons for Manage rules, Manage listener, and Add listener. A note below the buttons states: "on its configured protocol and port. Traffic received by the listener is routed according to the default action and any". There is a navigation bar with back, forward, and search icons. The main table has columns: Default action, Rules, ARN, and Security policy. Two rows are listed:

- Forward to target group application-lb**: 1 (100%)
Target group stickiness: Off
1 rule ARN ELBSecurityPolicy-TLS13-1-2-...
This row has a link labeled "application-lb" with a blue arrow icon.
- Forward to target group application-lb**: 1 (100%)
Target group stickiness: Off
1 rule ARN Not applicable
This row has a link labeled "application-lb" with a blue arrow icon.

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

The screenshot shows the AWS Load Balancer configuration page under the EC2 > Load balancers > application-lb path. The left sidebar has sections: Volumes, 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), and a ... button. The main content area has sections: Preserve host header (Off), Availability Zone routing configuration (Cross-zone load balancing On), Protection (Deletion protection Off), and Monitoring (Access logs S3 location: application-lb-1). The "Access logs" section includes a link labeled "application-lb-1" with a blue arrow icon.

- Logs will appear in S3 BUCKET.