

1. Configure Classic Load balancer.

Go to load balancers and create classic load balancer.

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.

Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your network settings.

VPC Info loadBalancers.vpcDescription.ClbInternetFacing [Learn more](#)

vpc-06cf45eaab13624fe (default) (default) [Create VPC](#)

Availability Zones and subnets

Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Availability Zones that are not available or the VPC are not available for selection.

us-east-1a (use1-az6)

Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0a192382de0e2bf6a default-p
IPv4 subnet CIDR: 172.31.0.0/16

Go to ec2-instances and create 2 instances with different zones.while creating add the data of installing httpd and server-no and httpd configuration and index.html file.

```
#!/bin/bash
sudo yum -y install httpd
echo "welcome to server-02" >> /var/www/html/index.html
sudo systemctl start httpd
```

Instances (2/4) <small>Info</small>								
Last updated 12 minutes ago								
Actions Launch instances								
Find Instance by attribute or tag (case-sensitive)								
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP	
instance-us-1b	i-027e4cf530d144227	Terminated	t3.micro	-	View alarms +	us-east-1b	-	
instance-us-ea...	i-073389abc90d423a3	Terminated	t3.micro	-	View alarms +	us-east-1a	-	
<input checked="" type="checkbox"/> server-01	i-0f434750791bbc6f3	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1a	ec2-13-21...	
<input checked="" type="checkbox"/> server-02	i-035abf01fd3af62a2	Running	t3.micro	3/3 checks passed	View alarms +	us-east-1b	ec2-3-21!	

Check whether it was running or not with port 80.

Go to loadbalancers and go to target instances and manage instances and add 2 instances.

The screenshot shows the AWS EC2 Load Balancers interface. A message at the top states: "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 few minutes to complete the registration process and pass initial health checks." The 'Load balancers (1/1)' section shows a single entry for 'classic-loadbalancer'. The 'Target instances' tab is selected, displaying two registered instances:

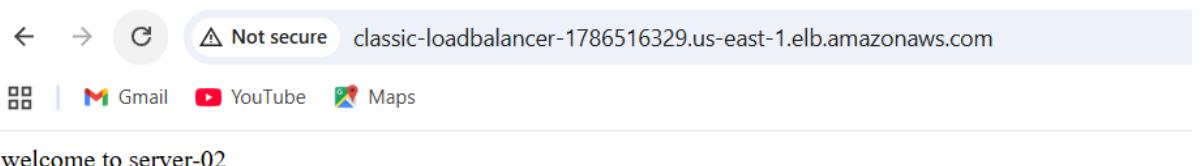
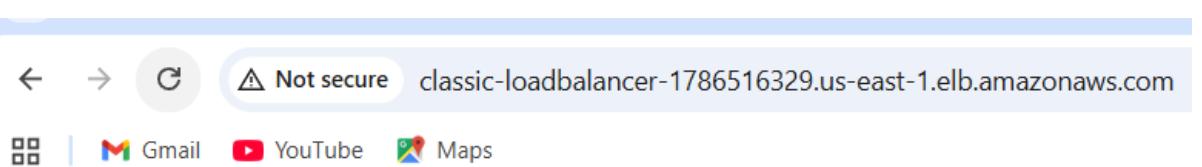
Registration status	Instance ID	Name	State	Security groups
Not registered	i-035abf01fd3af62a2	server-02	Running	default
Not registered	i-0f434750791bbc6f3	server-01	Running	default

Copy the DNS name of load balancer and paste in browser.

The screenshot shows the AWS EC2 Load Balancers console. The left sidebar has sections for Volumes, Snapshots, Lifecycle Manager, Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers, Target Groups, Trust Stores), and Auto Scaling (Auto Scaling Groups, Settings). The main area is titled "classic-loadbalancer" and contains a "Details" section with the following information:

Load balancer type	Status	VPC
Classic	2 of 2 instances in service	vpc-06cf45eaab13624fe
Scheme	Hosted zone	Availability Zones
Internet-facing	Z35SXDOTRQ7X7K	subnet-04f12a817188fcad 1b (use1-az1) subnet-0a192382de0e2bf6a 1a (use1-az6)

Below this, there's a "DNS name" field containing "classic-loadbalancer-1786516329.us-east-1.elb.amazonaws.com (A Record)". A note says: "This Classic Load Balancer can be migrated to a next generation load balancer. Migration wizard uses your load balancer configurations to create a new load balancer. [Learn more](#)". Finally, a "Distribution of targets by Availability Zone (AZ)" section is shown.



2. Configure Application Load balancer.

Go to load balancers and click on application load balancer and create application load balancer.

The screenshot shows the AWS EC2 Load Balancers Create Application Load Balancer interface. At the top, there's a navigation bar with the AWS logo, search bar, and various icons. Below it, the breadcrumb navigation shows EC2 > Load balancers > Create Application Load Balancer.

Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request and connection rules. It evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▶ How Application Load Balancers work

Basic configuration

Load balancer name
Name must be unique within your AWS account and can't be changed after the load balancer is created.
application-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
• 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 associated with them.

The screenshot shows the Listener configuration section of the Create Application Load Balancer page. It displays a list of listeners, with one listener named "HTTP:80" currently selected.

Listener HTTP:80

Protocol	Port
HTTP	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

Select a target group

Weight

1
0-999

+ 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 group. To use stickiness the client must support cookies. If you want to bind a user to a target group, turn on target group stickiness.

Turn on target group stickiness

CloudShell **Feedback**

For this we need target groups so, go to target groups and create target groups.



Step 1

Create target group

Step 2

Register targets

Create target group

Your load balancer routes requests to the targets in a target group and performs health checks on them.

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 instances.

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 translation.

Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

The screenshot shows the 'Target group name' field with 'images' typed in. Below it, a note says 'A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.' Under 'Protocol', 'HTTP' is selected. To its right, the 'Port' field is set to '80'. A note next to the port says 'Port number where targets receive traffic. Can be overridden for individual targets during registration.' Below the protocol and port settings, the 'IP address type' section is shown. 'IPv4' is selected, with a note explaining that each instance has a default network interface (eth0) assigned the primary private IPv4 address. The 'IPv6' option is also available. The 'VPC' section allows selecting a VPC for the target group. A dropdown menu shows 'vpc-06cf45aab13624fe (default)' and '172.31.0.0/16'. There are buttons for '(default)', 'Create VPC', and a circular icon.

Step 1

- Create target group
- Step 2
- Register targets**

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 (1/2)

Instance ID	Name	State	Security groups
i-035abf01fd3af62a2	server-02	Running	default
<input checked="" type="checkbox"/> i-0f434750791bbc6f3	server-01	Running	default

1 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](#)

Go to creating loadbalancer and give the default path and create.

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

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

Target group

images Target type: Instance, IPv4 Target stickiness: Off	HTTP	Weight	Percent
	<input checked="" type="radio"/>	1	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 group. To use stickiness the client must support cookies. If you want to bind a user's session to a specific target, turn on target group stickiness.

Listener tags - optional

If we go to target groups and go to targets it will be initialising.

The screenshot shows the AWS Lambda Targets page. At the top, there's a header with tabs: Targets (which is selected), Monitoring, Health checks, Attributes, and Tags. Below the header, a section titled "Registered targets (1) Info" is shown. It contains a table with one row. The table columns are: Instance ID, Name, Port, Zone, Health status, and Admin... (with a dropdown arrow). The single entry is: i-0f434750791bbc6f3, server-01, 80, us-east-1a (us...), Initial, and Target registration is i.... There are also buttons for "Anomaly mitigation: Not applicable" (with a circular icon), "Deregister", and "Register targets". A "Filter targets" input field is at the top left of the table. At the bottom right of the table, there are navigation arrows and a refresh icon. The footer of the page includes links for Feedback, Privacy, Terms, and Cookie policy.

Copy loadbalancer dns and add port 80

The screenshot shows a web browser window. The address bar displays the URL "application-loadbalancer-1634892184.us-east-1.elb.amazonaws.com". The browser interface includes standard navigation buttons (back, forward, search, etc.), a toolbar with icons for Gmail, YouTube, and Maps, and a status bar indicating "Not secure". The main content area of the browser shows the text "welcome to server-01".

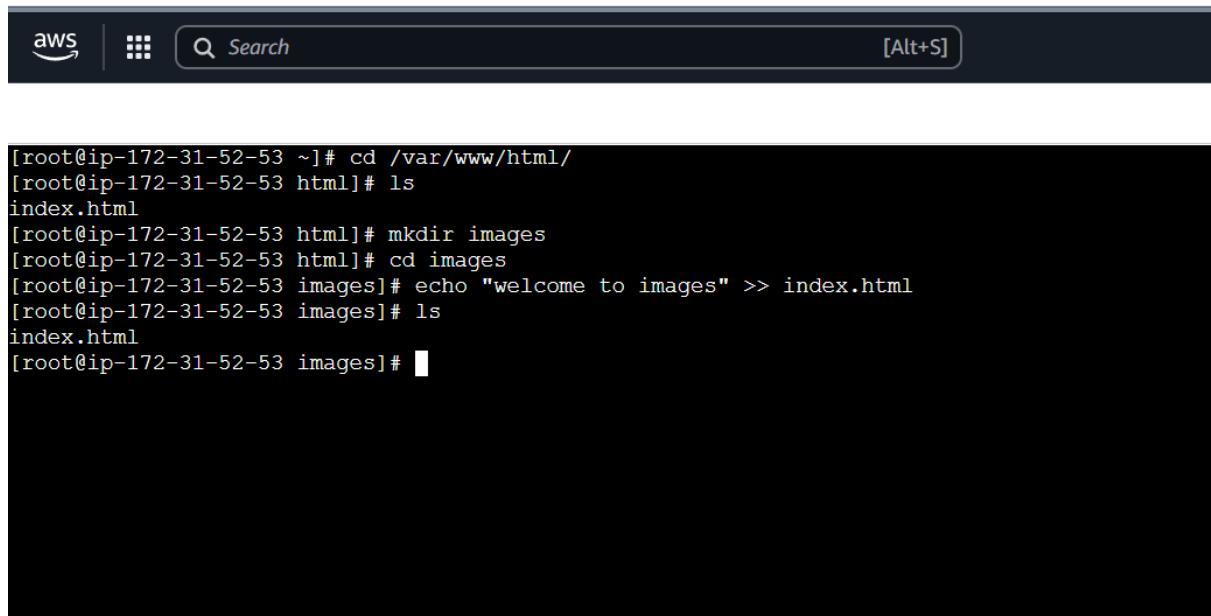
When we do with port number and /images it shows not found.

The screenshot shows a web browser window with the URL "application-loadbalancer-1634892184.us-east-1.elb.amazonaws.com/images" in the address bar. The browser interface includes standard navigation buttons, a toolbar with icons for Gmail, YouTube, and Maps, and a status bar indicating "Not secure". The main content area displays the text "Not Found".

Not Found

The requested URL was not found on this server.

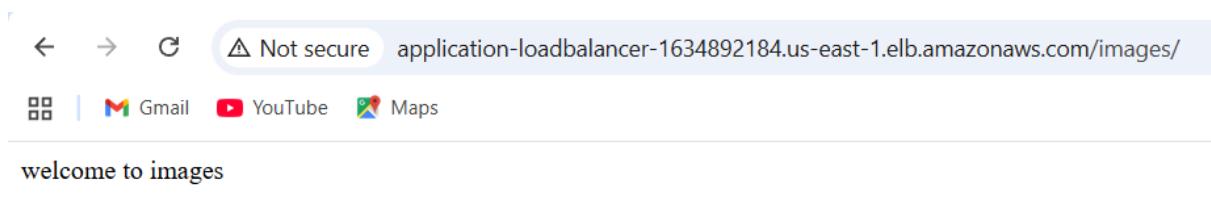
So we need to configure that images so, we need to login to that server and go to create a directory mkdir images and create echo "welcome to images">>>index.html



A screenshot of an AWS Lambda function editor. At the top, there's a header with the AWS logo, a search bar containing "Search", and a keybinding "[Alt+S]". The main area shows a terminal window with the following command-line session:

```
[root@ip-172-31-52-53 ~]# cd /var/www/html/
[root@ip-172-31-52-53 html]# ls
index.html
[root@ip-172-31-52-53 html]# mkdir images
[root@ip-172-31-52-53 html]# cd images
[root@ip-172-31-52-53 images]# echo "welcome to images" >> index.html
[root@ip-172-31-52-53 images]# ls
index.html
[root@ip-172-31-52-53 images]#
```

Now if you access that page it will redirect to images.



3. Configure Network Load balancer.

Go to load balancers and create network load balancer.

aws | Search [Alt+S] | ☰ | 🔍

☰ EC2 > Load balancers > Create Network Load Balancer

Create Network Load Balancer Info

The Network Load Balancer distributes incoming TCP and UDP traffic across multiple targets such as Amazon EC2 instances, microservices, and containers. It based on the protocol and port that are specified in the listener configuration, and the routing rule specified as the default action.

▶ How Network Load Balancers work

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
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.

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.
 IPv4

Create target groups

aws | Search [Alt+S] | ☰ | 🔍 | 🌐 | ⚙️

☰ EC2 > Target groups > Create target group

Step 1
 Create target group
 Step 2
Register targets

Create target group

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

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.

EC2 > Target groups > Create target group

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

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol
Protocol for load balancer-to-target communication. Can't be modified after creation.
TCP

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 you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC
Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy

Register targets

Select instances, specify ports, and add the instances to the list of pending targets. Repeat to add additional combinations of instances and ports to the list of pending targets. Once you are satisfied with your selections, click Register pending targets.

Available instances (2)

Instance ID	Name	State	Security groups	Zone	Private IPv4 address
i-0252f731635de4637	server-02	Running	default	us-east-1b	172.31.159.201
i-056fbf494a46d2ce2	server-01	Running	default	us-east-1a	172.31.75.82

aws | Search [Alt+S] | United States (N. Virginia) ▾

EC2 > Load balancers > network-loadbalancer

AMI Catalog

▼ Elastic Block Store
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

Settings

Successfully created load balancer

network-loadbalancer

Details

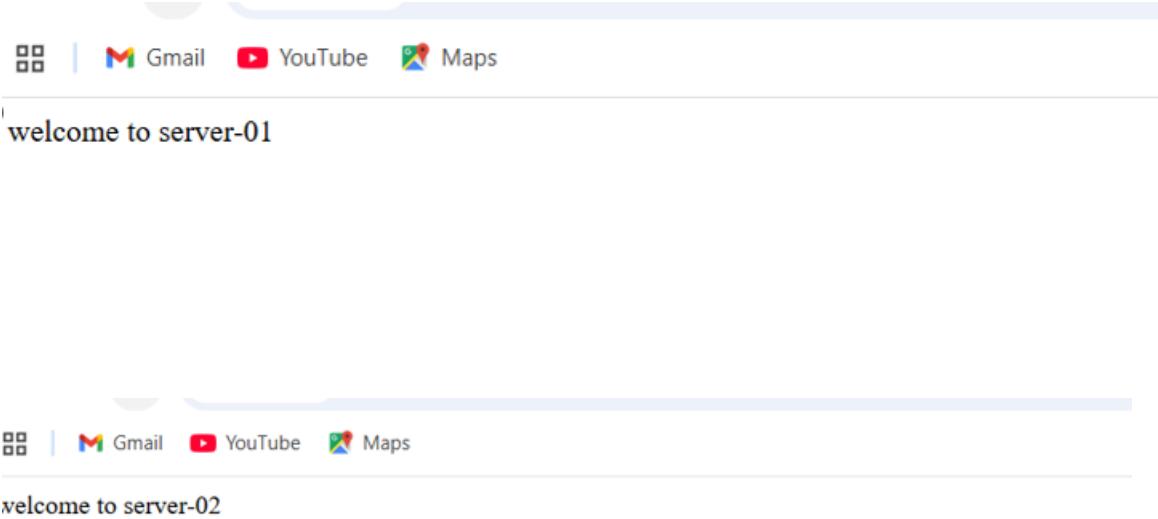
Load balancer type Network	Status Provisioning	VPC vpc-06cf45aab13624fe	Load balancer IP IPv4
Scheme Internet-facing	Hosted zone Z26RNL4JYFTOTI	Availability Zones subnet-04f12a817188fcad us-east-1b (use1-az1) subnet-0a192382de0e2bf6a us-east-1a (use1-az6)	Date created October 10, 2021
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:235351028455:loadbalancer/net/network-loadbalancer/293373af9e053025	DNS name info network-loadbalancer-293373af9e053025.elb.us-east-1.amazonaws.com		

Listeners Network mapping Resource map Security Monitoring Integrations Attributes Capacity

Listeners (1)

Actions ▾

Copy the load balancer url and paste it.



4. Attach SSL for application load balancer.

Go to loadbalancers and select your ALB and go to listeners and rules and select add rule-HTTPS-443.

The screenshot shows the AWS EC2 Load Balancers interface. The top navigation bar includes the AWS logo, a search bar, and a [Alt+S] keyboard shortcut. Below the navigation is a breadcrumb trail: EC2 > Load balancers > application-loadbalancer > Add listener. On the left, there's a sidebar with a 'Listeners' section. The main content area is titled 'Add listener' with a 'Info' link. A sub-section title 'Load balancer details: application-loadbalancer' is shown with a right-pointing arrow. The 'Listener: HTTPS:443' section describes what a listener does. Below it, the 'Protocol' field is set to 'HTTPS' and the 'Port' field is set to '443'. The 'Default action' section says it's used if no other rules apply. The 'Authentication action - optional' section notes it requires IPv4 connectivity and includes a 'Learn more' link. Finally, the 'Protocol settings' section shows the port as '1-65535'.

Add a listener to your Application Load Balancer (ALB) to define how client requests and network traffic are routed within your application. Every listener is made up of additional rules can be added, edited and deleted from the listener.

▶ **Load balancer details:** application-loadbalancer

Listener: HTTPS:443

A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how registered targets.

Protocol
Used for connections from clients to the load balancer.

Port
The port on which the load balancer is listening for connections.

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.

Create your target groups for https and select your acm certificate

aws | Search [Alt+S] | United States (N. Virginia)

EC2 > Target groups > Create target group

Target group name: 443-target-groups
A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol: HTTPS
Port: 443
1-65535

IP address type: IPv4
Only targets with the indicated IP address type can be registered to this target group.
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 you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

VPC
Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

EC2 > Load balancers > application-loadbalancer > Add listener

Secure listener settings [Info](#)

Security policy [Info](#)

Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. [Compa](#)

Security category

All security policies

Policy name

ELBSecurityPolicy-TLS13-1-2-Res-2021-06 (recomm)

Default SSL/TLS server certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager. A new certificate will automatically be added to your listener certificate list.

Certificate source

From ACM

From IAM

Certificate (from ACM)

The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

mujju.co.in

66b0e303-ccc9-435e-8769-214eaee3a835



[Request new ACM certificate](#)

Client certificate handling [Info](#)

Client certificates are used to make authenticated requests to remote servers. [Learn more](#)

Mutual authentication (mTLS)

Mutual TLS (Transport Layer Security) authentication offers two-way peer authentication. It adds a layer of security over TLS and allows your server to verify the identity of the client.

The screenshot shows the AWS CloudFormation console with a stack named "MyFirstCloudFormationStack". The "Outputs" tab is active, showing one output: "MyFirstCloudFormationOutput" with the value "https://myfirstcloudformation-123456789012.us-east-1.elb.amazonaws.com". There is a note below stating "This output is used by the Lambda function 'MyFirstCloudFormationLambdaFunction'." The "Outputs" section also includes a "Description" field and a "Details" link.

5. Map Application load balancer to R53.

Go to ec2 and select your alb load balancer copy the DNS name and go to route53 and select your domain

The screenshot shows the AWS Route 53 console with the domain "mujju.co.in". The "Hosted zones" section is selected. The "Records" tab is active, showing two records:

- mujju.co.in (NS, Simple, Alias, No)
- mujju.co.in (SOA, Simple, Alias, No)

A "Create record" button is visible at the top right of the records table.

Select create record and select alias,route traffic to ALB,select region, select load balancer create record.

The screenshot shows two consecutive screenshots of the AWS Route 53 console.

Screenshot 1: Create Record

- Record name:** subdomain (Info)
- Record type:** A – Routes traffic to an IPv4 address and some AWS resources (Info)
- Route traffic to:** Alias (selected)
- Route traffic to details:**
 - Alias to Application and Classic Load Balancer
 - US East (N. Virginia)
 - Value: dualstack.application-loadbalancer-453965773.us-east-1.elb.amazonaws.com
 - Use: "dualstack.application-loadbalancer-453965773.us-east-1.elb.amazonaws.com"
 - Simple routing (selected)

Screenshot 2: Hosted Zones

- Route 53:** Hosted zones (mujju.co.in)
- Records (3) Info:** Record for mujju.co.in was successfully created. Route 53 propagates your changes to all of the Route 53 authoritative DNS servers within 60 seconds. Use "View status" button to check propagation status.
- Records Table:**

Record ...	Type	Routing p...	Differ...	Alias	Value/Route traffic to
mujju.co.in	A	Simple	-	Yes	dualstack.application-loadba...
mujju.co.in	NS	Simple	-	No	ns-1625.awsdns-11.co.uk...
mujju.co.in	SOA	Simple	-	No	ns-1625.awsdns-11.co.uk. a...

go to browser and search for your domain the alias record will redirect the page to nginx that you are installed application init.

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

welcome to server-02

6. Push the application load balancer logs to S3.

Go to s3 buckets and go to permissions and add the script.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service":  
                    "logdelivery.elasticloadbalancing.amazonaws.com"  
            },  
            "Action": "s3:PutObject",  
            "Resource": "arn:aws:s3:::amzn-s3-demo-  
bucket/prefix/AWSLogs/123456789012/*"  
    ]  
}
```

]

}

The screenshot shows the AWS S3 Bucket policy editor. At the top, there's a green success message: "Successfully edited bucket policy." Below it is the JSON code for the policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::app-bucket02345/prefix/AWSLogs/235351028455/*"
    }
  ]
}
```

Go to ALB and select attributes and enable access logs

The screenshot shows the AWS Load Balancer configuration page for an application load balancer. Under the "Monitoring" section, the "Access logs" checkbox is checked, and the S3 URI is set to "s3://app-bucket02345".

Access logs
Access logs deliver detailed logs of all requests made to your Elastic Load Balancer. Choose an existing S3 location. If you don't specify a prefix, the logs are stored in the root of the bucket. Additional charges apply. [Learn more](#)

S3 URI: X View B

Connection logs
Connection logs deliver detailed logs of all connections made to your Elastic Load Balancer. Choose an existing S3 location. If you don't specify a prefix, the logs are stored in the root of the bucket. Additional charges apply. [Learn more](#)

