

Load balancer Tasks

1) Configure Classic Load balancer.

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

Create Classic Load Balancer [Info](#)

The Classic Load Balancer distributes incoming application traffic across multiple EC2 instance targets in multiple Availability Zones. This increases the fault tolerance of your applications. Elastic Load Balancing detects unhealthy instances and routes traffic only to healthy instances.

► How Classic 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.

S3 Athena CloudTrail CloudWatch

✔ Successfully created load balancer: **task-1**
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.

[EC2](#) > [Load balancers](#) > task-1

Load balancers (1)

⌂ Actions ▼ Create load balancer ▼

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

1 match

0 load balancers selected ✕

Select a load balancer above.

← → ↻ ⚠ Not secure task-1-1047601164.us-east-1.elb.amazonaws.com

hello world techihorize

2) Configure 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 attributes. When the load balancer receives a connection request, 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.

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

[Schema](#) [Info](#)

✓ Successfully created the target group: **task-2-target**.

0 0 1 1 0 0

task-2-target

Actions ▼

Details

arn:aws:elasticloadbalancing:us-east-1:183631301772:targetgroup/task-2-target/3014b63100a3479a

Target type

Application Load Balancer

Protocol : Port

TCP: 80

VPC

[vpc-0b03cdd70722fc884](#)

IP address type

IPv4

Load balancer

[None associated](#)



Use this target group with a Network Load Balancer

To use this target group, you must first set up a Network Load Balancer and add a listener to it that forwards traffic to this target group. Then you can enable AWS

Create Network Load Balancer



S3AthenaCloudTrailCloudWatch

Successfully created load balancer: task-2

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

EC2 > Load balancers > task-2

task-2

Details

Load balancer type	Status	VPC	Load balancer IP address type
Application	Provisioning	vpc-0b03cdd70722fc884	IPv4
Scheme	Hosted zone	Availability Zones	Date created
Internet-facing	Z35SXDOTRQ7X7K	subnet-00b68e7b1fbef77a7 us-east-1c (use1-az4)	November 21, 2024, 15:08 (UTC+05:30)
		subnet-0e2d2e82509314a58 us-east-1a (use1-az1)	

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preference

task-2-1218659583.us-east-1.elb.amazonaws.com

hello world techihorize

3) Configure Network Load balancer.

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. When the load balancer receives a connection request, it selects a target based on the protocol and port that are specified in the listener configuration, and the routing rule specified as the default action.



Network Load Balancer now supports UDP for Dualstack

Set your IP address type as dualstack and enable prefix for IPv6 source NAT. Then configure UDP-based listeners to route to IPv6 targets.



► 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.



✓ Successfully created the target group: **task3-target**.



EC2 > Target groups > task3-target

task3-target

Actions ▼

Details

arn:aws:elasticloadbalancing:us-east-1:183631301772:targetgroup/task3-target/79acb32d938c91f5

Target type
Instance

Protocol : Port
TCP: 80

VPC
[vpc-0b03cdd70722fc884](#)

IP address type
IPv4

Load balancer
[None associated](#)

Total targets
2

Healthy
 0

Unhealthy
 0

Unused
 2

Initial
 0

Draining
 0

S3AthenaCloudTrailCloudWatch

Successfully created load balancer

EC2 > Load balancers > task-3

task-3

Details

Load balancer type Network	Status Provisioning	VPC vpc-0b03cdd70722fc884	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z26RNL4JYFTOTI	Availability Zones subnet-00b68e7b1fbef77a7 us-east-1c (use1-az4) subnet-0e2d2e82509314a58 us-east-1a (use1-az1)	Date created November 21, 2024, 15:17 (UTC+05:30)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:183631301772:loadbalance		DNS name Info task-3-17707dac8cb2b7ab.elb.us-east-1.amazonaws.com (A Record)	

Listeners

Network mapping

Resource map - new

Security

Monitoring

Integrations

Attributes

Ca

Listeners (1)

A listener checks for connection requests using the protocol and port that you configure. Traffic received by a Network Load Balancer listener is forwarded to the selected target group.

Filter listeners

< 1 >

<input type="checkbox"/>	Protocol:Port	Default action	ARN	Security policy	Default SSL/TLS cert
<input type="checkbox"/>	TCP:80	Forward to target group <ul style="list-style-type: none">task3-target	<input type="checkbox"/> ARN	Not applicable	Not applicable

Not secure

task-3-17707dac8cb2b7ab.elb.us-east-1.amazonaws.com

hello world techihorize

4) Attach SSL for application load balancer.

SSAthenaCloud TrailCloudWatch

EC2 > Load balancers

Load balancers (1/1)

Actions

Create load balancer

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Filter load balancers

< 1 >

☒

Name

DNS name


State

VPC ID

Availability Zones

☒

[task-4](#)

 task-4-1778840615.us-eas...

Active

vpc-0b03cdd70722fc8...

2 Availability Zones

Load balancer: task-4

< Details

Listeners and rules

Network mapping

Resource map - new

Security

Monitoring

Integrations

>

Details

EC2 > Load balancers > task-4 > Add listener

Add listener [Info](#)

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 a default action that's required and can only be edited. Additional rules can be added, edited and deleted from the listener.

Load balancer details: task-4

Listener details: 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 the Application Load Balancer routes requests to its registered targets.

Listener configuration

The listener will be identified by the protocol and port.

Protocol

Used for connections from clients to the load balancer.

HTTPS

Port

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

443

1-65535



Successfully requested certificate with ID 9a3eaede-4782-4d4f-815d-9197cfdcd09b
 A certificate request with a status of pending validation has been created. Further action is needed to complete the validation and approval of the certificate.

[View certificate](#)



9a3eaede-4782-4d4f-815d-9197cfdcd09b

[Delete](#)

Certificate status

Identifier

9a3eaede-4782-4d4f-815d-9197cfdcd09b

Status

Pending validation [Info](#)

ARN

arn:aws:acm:us-east-1:183631301772:certificate/9a3eaede-4782-4d4f-815d-9197cfdcd09b

Type

Amazon Issued

**Fully
dom
(FQD**

A fully
(FQDN
organi
Intern
domai
.org.

Type t
name
secure
(for ex
Use ar
wildca
severa
For ex:
protec
site.ex
image

Listeners and rules (2) [Info](#)



[Manage rules](#)

[Manage listener](#)

[Add listener](#)

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

< 1 >

<input type="checkbox"/>	Protocol:Port	Default action	Rules	ARN	Security policy
<input type="checkbox"/>	HTTP:80	Forward to target group <ul style="list-style-type: none"> task-4: 1 (100%) Target group stickiness: Off 	1 rule	ARN	Not applicable
<input type="checkbox"/>	HTTPS:443	Forward to target group <ul style="list-style-type: none"> task-4: 1 (100%) Target group stickiness: Off 	1 rule	ARN	ELBSecurityPolicy-TLS



<https://rakeshpagidimarri.shop>

hello world techihorize

5) Map Applciation load balancer to R53.

[s](#) > rakeshpagidimarri.shop

Record for rakeshpagidimarri.shop 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.

[View status](#)

Records (4) [Info](#) [Delete record](#) [Import zone file](#) [Create record](#)

Automatic mode is the current search behavior optimized for best filter results. [To change modes go to settings.](#)

<input type="checkbox"/>	Record ... ▾	Type ▾	Routin... ▾	Differ... ▾	Alias ▾	Value/Route tra
<input type="checkbox"/>	rakeshpag...	A	Simple	-	Yes	dualstack.task-4-
<input type="checkbox"/>	rakeshpag...	NS	Simple	-	No	ns-874.awsdns-4- ns-509.awsdns-6- ns-1662.awsdns- ns-1342.awsdns-
<input type="checkbox"/>	rakeshpag...	SOA	Simple	-	No	ns-874.awsdns-4-
<input type="checkbox"/>	_969bf3b...	CNAME	Simple	-	No	_73a6dd82cd16f

0 records selected

Select a record to see its details

6) Push the application load balancer logs to s3.

[EC2](#) > [Load balancers](#) > [task-4](#) > Edit load balancer attributes

Edit load balancer attributes

Restore defaults

► **Load balancer details:** task-4

Traffic configuration

☐ **TLS version and cipher headers**
When on, the load balancer adds two TLS headers (x-amzn-tls-version and x-amzn-tls-cipher-suite) to the client request before sending it to the target.

☐ **WAF fail open**
Allows requests through to backend target(s) when the application load balancer is unable to contact AWS Web Application Firewall (WAF).

☒ **HTTP/2**
Send requests to the load balancer using the protocol version HTTP/2.

Connection idle timeout [Info](#)
The amount of time a client or target connection can be idle before the load balancer closes it. Valid range is 1 - 4000 seconds. The default is 60 seconds, or 1 minute.

H:MM:SS

Seconds

S3AthenaCloudTrailCloudwatch

Successfully modified load balancer attributes.

EC2 > Load balancers > task-4

task-4

Refresh

Actions

Details

Load balancer type	Status	VPC	Load balancer IP address type
Application	Active	vpc-0b03cdd70722fc884	IPv4
Scheme	Hosted zone	Availability Zones	Date created
Internet-facing	Z35SXDTRQ7X7K	subnet-00b68e7b1fbef77a7 us-east-1c (use1-az4)	November 21, 2024, 15:41 (UTC+05:30)
		subnet-0e2d2e82509314a58 us-east-1a (use1-az1)	
Load balancer ARN	DNS name		
arn:aws:elasticloadbalancing:us-east-1:183631301772:loadbalance	task-4-1778840615.us-east-1.elb.amazonaws.com (A Record)		

my-s3-rakesh2 Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Permissions overview

Access finding
Access findings are provided by IAM external access analyzers. Learn more about [How IAM analyzer findings work](#)
[View analyzer for us-east-1](#)

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, these settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your application without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Off
Individual Block Public Access settings for this bucket

my-s3-rakesh2 > AWSLogs/ > 183631301772/

Objects | Properties

Objects (2) Info

Copy S3 URI

Copy URL

Download

Open

Delete



Actions

Create folder

Upload

Find objects by prefix

< 1 > ⚙

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input type="checkbox"/>	 ELBAccessLogTestFile	-	November 21, 2024, 17:45:29 (UTC+05:30)	81.0 B	Standard
<input type="checkbox"/>	 ELBConnectionLogTestFile	-	November 21, 2024, 17:45:29 (UTC+05:30)	85.0 B	Standard