

Creating Load Balancer

click on create load balancer

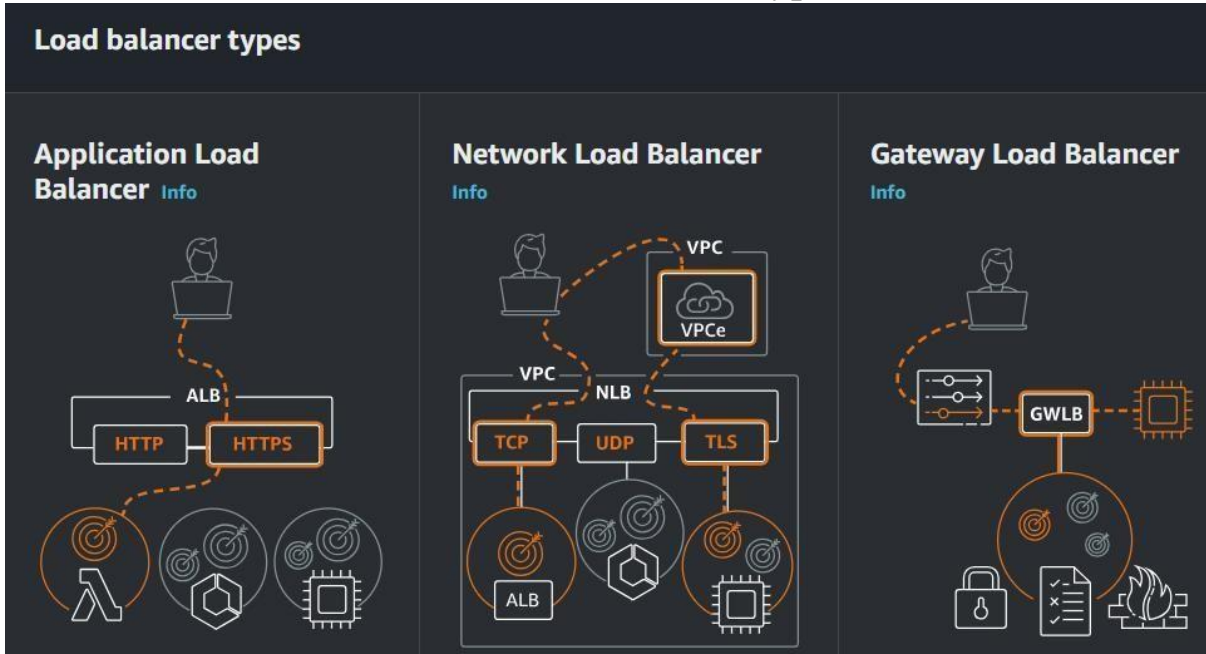
Load balancers (1/2) Actions Create load balancer

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

Filter load balancers

	Name	DNS name	State	VPC ID	Availability Zones	Type
<input checked="" type="checkbox"/>	fundoo-backend-load-...	internal-fundoo-backend-l...	Active	vpc-0471a5c29c0cc770b	2 Availability Zones	application
<input type="checkbox"/>	fundoo-frontend-load-...	fundoo-frontend-load-bal...	Active	vpc-0471a5c29c0cc770b	2 Availability Zones	application

choose an load balancer type



Click on create button

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

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

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

Give load balancer name

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.

Select an scheme based upon your vm ,, like frontend instance means internet

facing , backend instance means internal

Scheme [Info](#)

Scheme can't be changed after the load balancer is created.

☒ **Internet-facing**
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

☐ **Internal**
An internal load balancer routes requests from clients to targets using private IP addresses. Compatible with the IPv4 and Dualstack IP address types.

Select ipv4 or ipv6 or dual

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.

Select vpc ,, where your load balancer should be located

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](#). For a new VPC, [create a VPC](#).

vpc-079471e1f2ea7de9e
IPv4 VPC CIDR: 172.31.0.0/16

Mappings [Info](#)

select an subnets where your load balancer should mange load based upon your subnets which you mentioned.

Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

Availability Zones

☐ ap-south-1a (aps1-az1)

☐ ap-south-1b (aps1-az3)

☐ ap-south-1c (aps1-az2)

Select security group ,, or you have to create an security group for your load balancer and select that security group.

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

Select up to 5 security groups

default

Mentions listens ,, source target group ,, and you have to create an target group as well before it self.

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	Port	Default action	Info
HTTP ▼	: 80 1-65535	Forward to Select a target group ▼	Create target group ↗

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.

Add listener

Give an tags which will be useful for recognize purpose

▼ **Load balancer tags - optional**

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

No tags associated with this load balancer.

Add new tag

You can add up to 50 tags.

Check once whatever you have give and mentions details of load balancer

Summary

Review and confirm your configurations. [Estimate cost](#) ↗

Basic configuration Edit <i>Load balancer name not defined</i> <ul style="list-style-type: none"> Internet-facing IPv4 	Security groups Edit <ul style="list-style-type: none"> default sg-0c5996b74ed43e9b0 ↗ 	Network mapping Edit VPC vpc-079471e1f2ea7de9e ↗ <i>Subnet not defined</i>	Listeners and routing Edit <ul style="list-style-type: none"> HTTP:80 defaults to <i>Target group not defined</i>
Service integrations Edit AWS WAF: None AWS Global Accelerator: None		Tags Edit None	

Attributes

ⓘ Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Finally click on create load balancer you successfully created an load balancer

Cancel

Create load balancer

Create target group

Click on create load balancer

Target groups (2) <small>Info</small>							
<input type="text" value="Filter target groups"/>				< 1 >			
<input type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer	
<input type="checkbox"/>	fundoo-backend-targe...	arn:aws:elasticloadbalanci...	8000	HTTP	Instance	fundoo-backend-load..	
<input type="checkbox"/>	fundoo-frontend-targ...	arn:aws:elasticloadbalanci...	80	HTTP	Instance	fundoo-frontend-load..	

Check on which type you want create an target group

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.

☐ **Lambda function**

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

☐ **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.

Give an target group name in meaning full way ..

Target group name

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

Give port

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP

80

1-65535

Select ip address type


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](#) 

Select vpc

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.

-
vpc-079471e1f2ea7de9e
IPv4 VPC CIDR: 172.31.0.0/16

Select protocol

Protocol version

☒ HTTP1

Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

☐ HTTP2

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.

Give an path which it check instance is healthy or not like /home , /swagger

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

Restore defaults

Health check port

The port the load balancer uses when performing health checks on targets. By default, the health check port is the same as the target group's traffic port. However, you can specify a different port as an override.

☒ Traffic port

☐ Override

Healthy threshold

The number of consecutive health checks successes required before considering an unhealthy target healthy.

5

2-10

Unhealthy threshold

The number of consecutive health check failures required before considering a target unhealthy.

2

2-10

Timeout

The amount of time, in seconds, during which no response means a failed health check.

5

seconds

2-120

Interval

The approximate amount of time between health checks of an individual target

30

seconds

5-300

Success codes

The HTTP codes to use when checking for a successful response from a target. You can specify multiple values (for example, "200,202") or a range of values (for example, "200-299").

200

Select an instance for which your target group should assign

Available instances (3)

Filter instances

< 1 >



<input type="checkbox"/>	Instance ID	Name	State	Security groups
<input type="checkbox"/>	i-089fcfa2b91f1ab5d	backend-server	Running	backend-security-group
<input type="checkbox"/>	i-0f2d3e1203aefec09	frontend-server	Running	frontend-security-group
<input type="checkbox"/>	i-0be62aef3598b774	database-server	Running	database-security-group

Give port ,, click on include as pending belowbutton

Ports for the selected instances
Ports for routing traffic to the selected instances.

1-65535 (separate multiple ports with commas)

Include as pending below

Click on create button

Review targets

Targets (1) Remove all pending

Show only pending < 1 > ⚙

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address
i-Of2d3e1203aefec09	frontend-server	80	Running	frontend-security-group	ap-south-1a	20.0.0.221

1 pending

Cancel Previous Create target group