

Elastic Load Balancer (ELB)



Distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, IP addresses, and Lambda functions.



Introduction to Elastic Load Balancer (ELB)

Load Balancers can be physical hardware or virtual software that accepts incoming traffic, and then distributes the traffic to multiple targets. They can **balance** the load via different rules. These rules vary based on types of load balancers.

Elastic Load Balancer (ELB) is the AWS solution for load balancing traffic, and there are 3 types available:

1. Application Load Balancer ALB (HTTP/HTTPS)
2. Network Load Balancer NLB (TCP/UDP)
3. Classic Load Balancer CLB (Legacy)



ELB - The Rules of Traffic

Listeners

Incoming traffic is evaluated against listeners. Listeners evaluate any traffic that is matches the Listener's port. For Classic Load Balancer, EC2 instances are directly registered to the Load Balancer.

Rules (Not available for Classic Load Balancer)

Listeners will then invoke rules to decide what to do with the traffic. Generally the next step is to forward traffic to a Target Group

Target Groups (Not available for Classic Load Balancer)

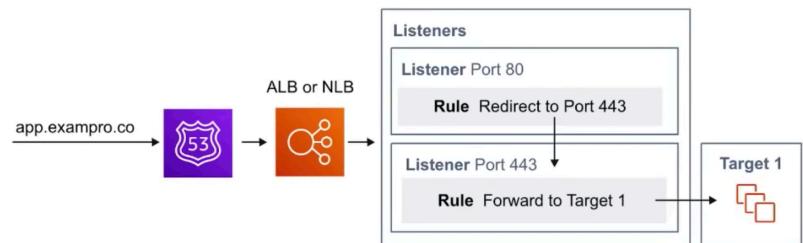
EC2 instances are registered as targets to a Target Group



ELB - The Rules of Traffic

For Application Load Balancer (ALB) or Network Load Balancer (NLB) traffic is sent to the Listeners.

When the port matches it then checks the rules what do to. The rules will forward the traffic to a Target Group. The target group will evenly distribute the traffic to instances registered to that target group.



Description **Listeners** Monitoring Integrated services Tags

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

Add listener Edit Delete

Listener ID	Security policy	SSL Certificate
HTTP : 80	N/A	N/A
arn...08e1a3165cec5d22		
HTTPS : 443	ELBSecurityPolicy	Default: a213d84c-4210-4fc7-3569-9113c39394fb (ACM)
arn...a64254b4731fa5c1		

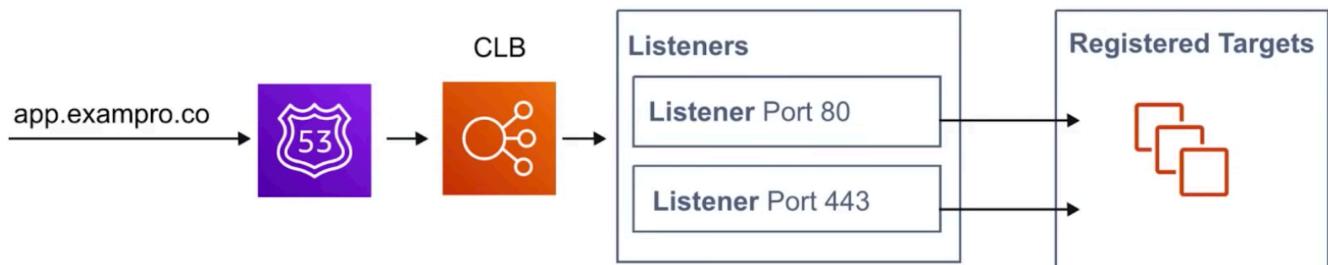
Rules are only for ALB

Rules
Default: redirecting to HTTPS://#{host}:443/#{path}?#{query}
View/edit rules
Default: forwarding to production
View/edit rules



ELB - The Rules of Traffic

For Classic Load Balancer (CLB) traffic is sent to the Listeners. When the port matches it then it forwards the traffic to any EC2 instances that are registered to the Classic Load Balancer. CLB does not allow you to apply rules to listeners





Application Load Balancer (ALB)

Application Load Balancers are designed to balance **HTTP** and **HTTPS** traffic.

They **operate at Layer 7 (of the OSI Model)**.

ALB has a feature called **Request Routing** which allows you to add routing rules to your listeners based on the HTTP protocol.

Web Application Firewall (WAF) can be attached to ALB.

Great for Web Applications

OSI Layers

Layer 7	Application
Layer 6	Presentation
Layer 5	Session
Layer 4	Transport
Layer 3	Network
Layer 2	Data Link
Layer 1	Physical



Network Load Balancer (NLB)

Network Load Balancers are designed to balance TCP/UDP.

They **operate at Layer 4 (of the OSI Model)**

Can handle **millions of requests per second** while still maintaining extremely low latency.

Can perform Cross-Zone Load Balancing

Great for Multiplayer Video Games or When network performance is critical

OSI Layers

Layer 7 Application

Layer 6 Presentation

Layer 5 Session

Layer 4 Transport

Layer 3 Network

Layer 2 Data Link

Layer 1 Physical



Classic Load Balancer (CLB)

It was AWS first load balancer (**legacy**)

Can balance **HTTP**, **HTTPS** or **TCP** traffic (not at the same time)

It can use **Layer 7-specific features (OSI Model)** such as **sticky sessions**.

It can also use **strict Layer 4 (OSI Model)** balancing for purely TCP applications.

Can perform Cross-Zone Load Balancing

It will respond with a **504 error (timeout)** if the underlying application is not responding. (**at the web-server or database level**)

Not recommended for use, instead use NLB or ALB

OSI Layers

Layer 7 Application

Layer 6 Presentation

Layer 5 Session

Layer 4 Transport

Layer 3 Network

Layer 2 Data Link

Layer 1 Physical



ELB - Sticky Sessions

Sticky Sessions is an advanced load balancing method that allows you to **bind a user's session to a specific EC2 instance.**

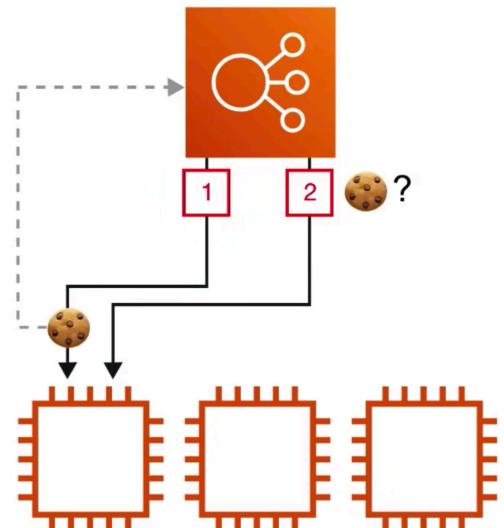
Ensures all **requests** from that session are **sent to the same instance.**

Typically **utilized** with a **Classic Load Balancer**

Can be enabled for ALB though can only be set on a Target Group not individual EC2 instances.

Cookies are used to remember which EC2 instance.

Useful when specific **information is only stored locally on a single instance**

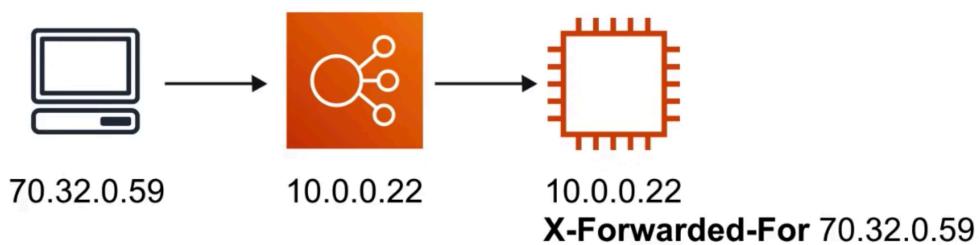




X-Forwarded-For (XFF) Header

If you **need the IPv4 address** of a user, check the **X-Forwarded-For** header

The **X-Forwarded-For (XFF)** header is a command method for identifying the **originating IP address** of a client connecting to a web server through an HTTP proxy or a load balancer.



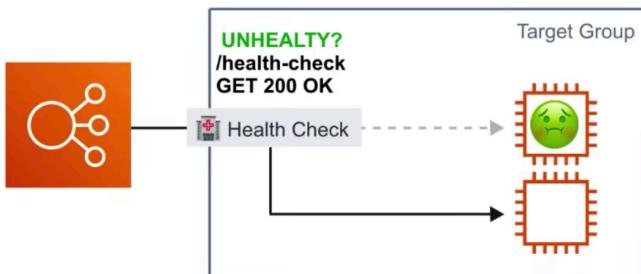


ELB - Health Checks

Instances that are monitored by the Elastic Load Balancer (ELB) report back Health Checks as **InService**, or **OutOfService**

Health Checks communicate directly with the instance to determine its state.

ELB does not terminate (kill) unhealthy instance. It will just redirect traffic to healthy instances



For ALB and NLB the Health checks are found on the **Target Group**

Screenshot of the AWS CloudFormation console showing the "Health checks" tab for a Target Group. The configuration includes:

Setting	Value
Protocol	HTTP
Path	/health-check
Port	traffic port
Healthy threshold	2
Unhealthy threshold	2
Timeout	5
Interval	10
Success codes	200

Edit health check

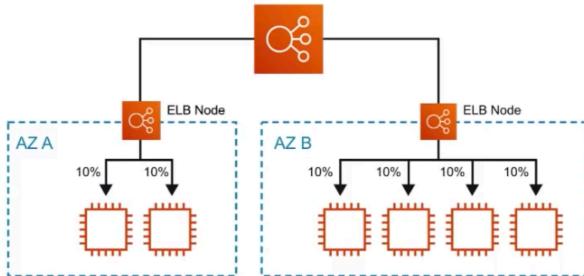


ELB - Cross-Zone Load Balancing

Only for **Classic** and **Network** Load Balancer

Cross-Zone Load Balancing Enabled

requests are distributed evenly across the instances **in all enabled** Availability Zones.



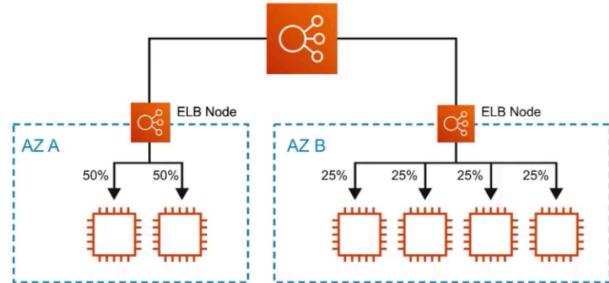
Attributes

Deletion protection	Disabled
Cross-Zone Load Balancing	Disabled
Access logs	Disabled

[Edit attributes](#)

Cross-Zone Load Balancing Disabled

requests are distributed evenly across the instances **in only its Availability Zone**.



Edit load balancer attributes

Delete Protection	<input type="checkbox"/> Enable
Cross-Zone Load Balancing	<input checked="" type="checkbox"/> Enable

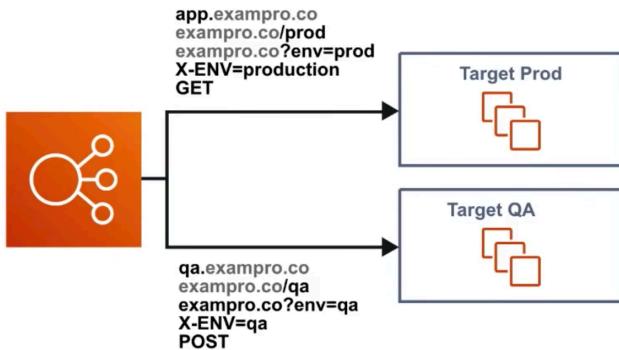
Regional data transfer charges may apply when cross-zone load balancing is enabled. See the [documentation](#) for more information.



ALB - Request Routing

Apply rules to incoming request and then **forward** or **redirect** traffic.

- | | |
|---------------|----------------------|
| ✓ Host header | ✓ Http header |
| ✓ Source IP | ✓ Http header method |
| ✓ Path | ✓ Query string |



The screenshot shows the AWS Lambda function configuration interface with two rule configurations:

- Rule 1 (Top):** IF (all match) `HTTP 443: default action`. THEN `Forward to production`.
- Rule 2 (Bottom):** IF `Requests otherwise not routed`. THEN `Forward to production`.



ELB *CheatSheet*

- There are three Elastic Load Balancers: **Network, Application** and **Classic** Load Balancer
- A Elastic Load Balancer must have **at least two** Availability Zones.
- Elastic Load Balancers **cannot go cross-region**. You must create one per region.
- ALB has **Listeners, Rules** and **Target Groups** to route traffic
- NLB use **Listeners** and **Target Groups** to route traffic
- CLB use **Listeners** and EC2 instances are **directly registered** as targets to CLB
- Application Load Balancer is for HTTP(S) traffic and the name implies it good for Web Applications
- Network Load Balancer is for TCP/UDP is good for high network throughput eg. Video Games
- Classic Load Balancer is legacy and its recommended to use ALB or NLB
- Use X-Forwarded-For (XFF) to get original IP of incoming traffic passing through ELB
- You can attach Web Application Firewall (WAF) to ALB but not to NLB or CLB
- You can attach Amazon Certification Manager SSL to any of the Elastic Load Balancers for SSL
- ALB has advanced Request Routing rules where you can route based on subdomain header, path and other HTTP(S) information
- Sticky Sessions can be enable for CLB or ALB and sessions are remembered via Cookie