



Universidad del
Rosario



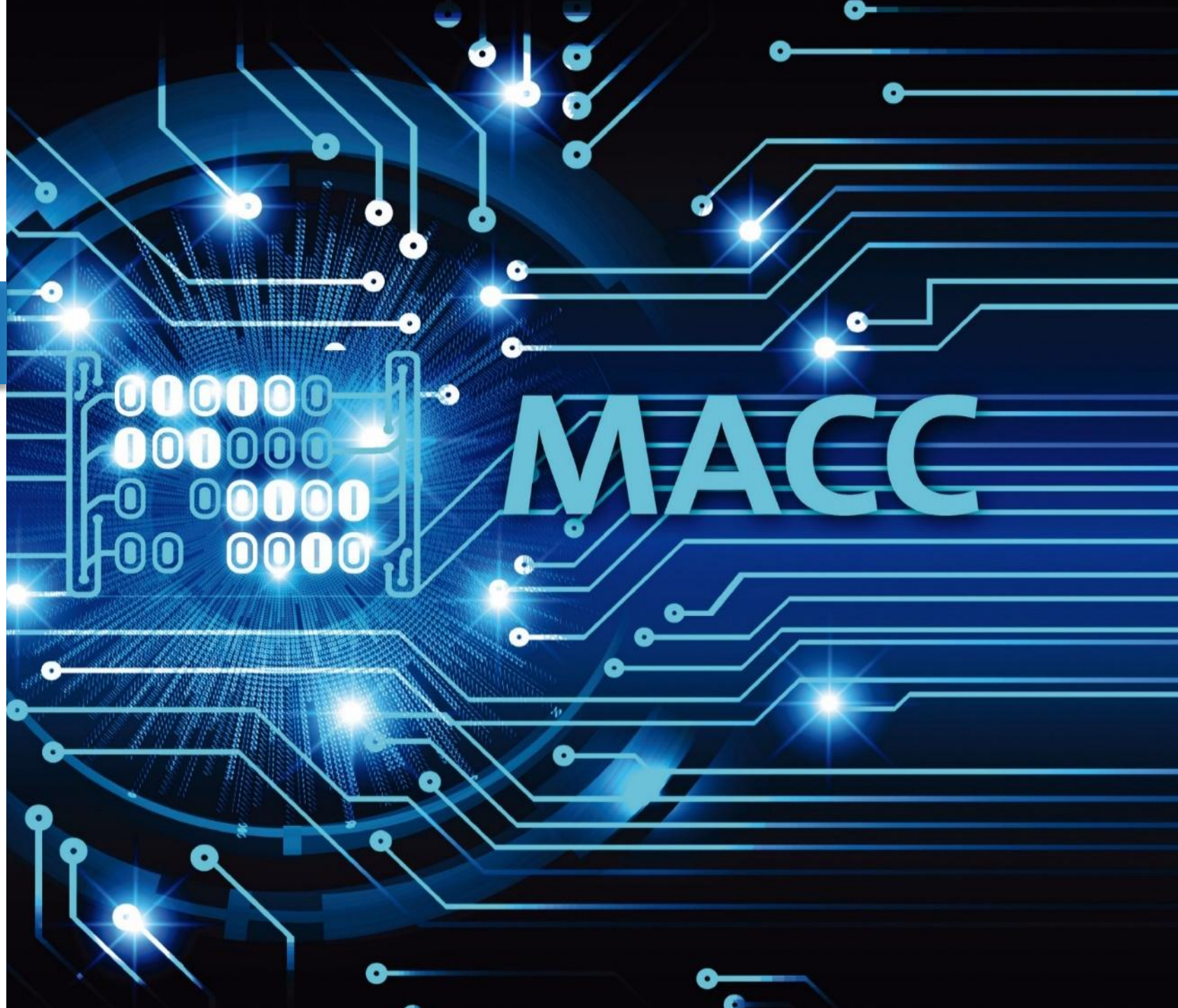
MACC
Matemáticas Aplicadas y
Ciencias de la Computación

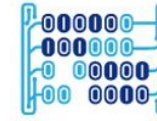
AWS Load Balancing

Ciberseguridad

Daniel Orlando Díaz López, PhD

Profesor principal
Departamento MACC
Universidad del Rosario
danielo.diaz@urosario.edu.co





Elastic Load Balancing

Cybersecurity

INTRODUCTION TO AWS CLOUD SECURITY

aws  educate

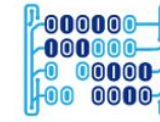
Elastic Load Balancing automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers: [Application Load Balancer](#) [↗], [Network Load Balancer](#) [↗] and [Classic Load Balancer](#) [↗].

Using Elastic Load Balancing in Your Amazon Virtual Private Cloud (VPC)

Elastic Load Balancing makes it easy to create an internet-facing entry point into your [Amazon Virtual Private Cloud \(VPC\)](#). You can assign security groups to your load balancer to control which ports are open to a list of allowed sources. Together, Elastic Load Balancing works with [Amazon Virtual Private Cloud \(VPC\)](#) to provide you the flexibility to centrally manage SSL settings and offload CPU intensive workloads from your applications.

Architecture of the Elastic Load Balancing Service and How It Works

There are two logical components in the Elastic Load Balancing service architecture: load balancers and a controller service. The load balancers are resources that monitor traffic and handle requests that come in through the Internet. The controller service monitors the load balancers, adds and removes capacity as needed, and verifies that load balancers are behaving properly. See figure below to observe the architecture of the AWS Elastic Load Balancing Service.



Introductory video: Getting Started with Elastic Load Balancing

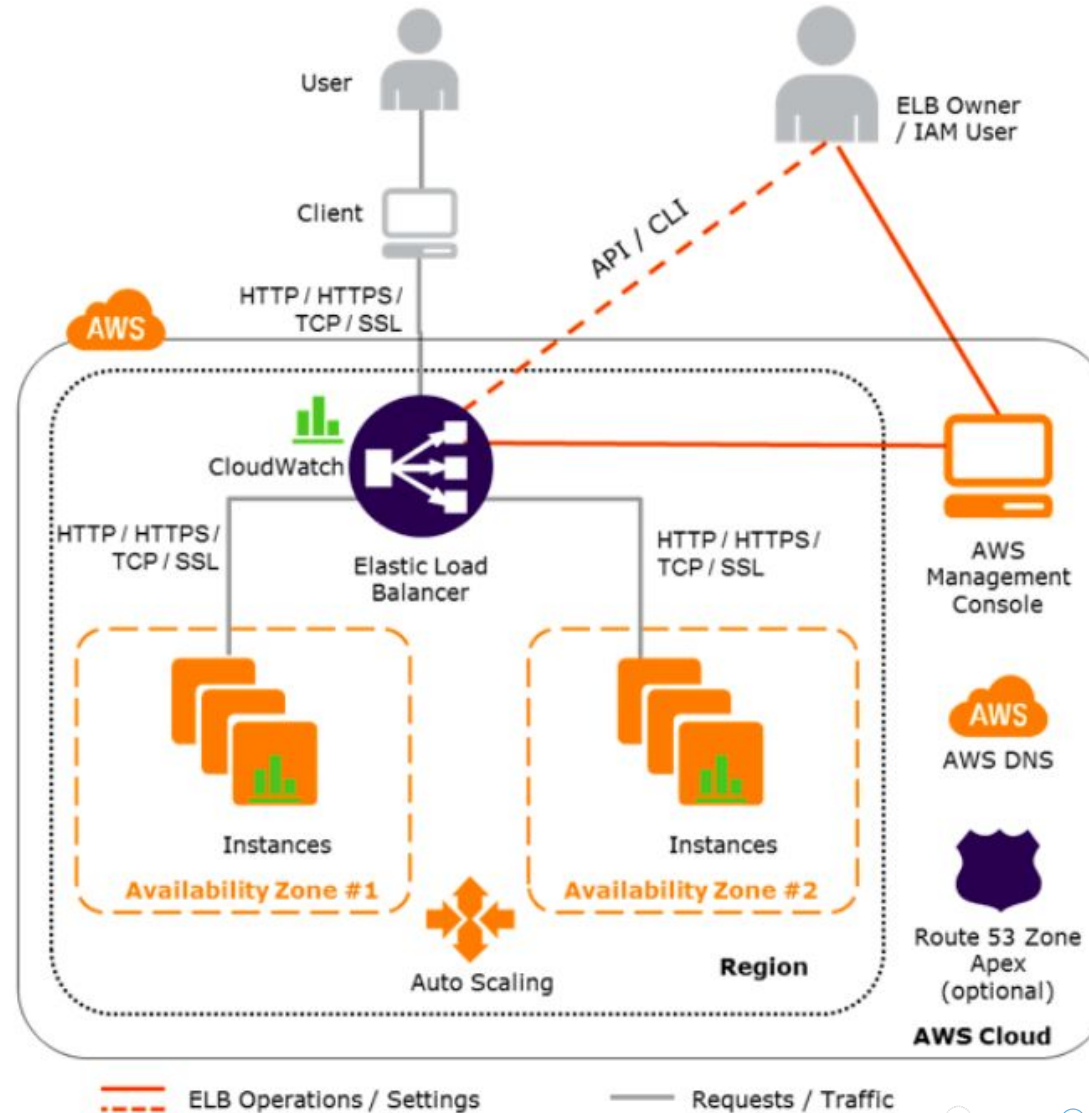
<https://www.youtube.com/watch?v=8KQ8aLoxVi0&feature=youtu.be>

The image shows a video player interface. At the top left, the Amazon Web Services logo is displayed next to the text 'amazon web services'. To the right of the logo, the text 'Getting Started' is visible. The main title of the video, 'Elastic Load Balancing', is centered in a large, bold, blue font. The background of the video frame shows a landscape with mountains and a blue sky with white clouds. At the bottom of the video player, there is a progress bar showing '0:02 / 5:04' and various control icons like play, pause, volume, and full screen.

Getting Started with Elastic Load Balancing

Steps:

1. Create a load balancer (Application Load Balancer or Network Load Balancer)
2. Specify a unique name and a network
3. Create listeners for your load balancer
 - a. HTTP or HTTPS for Application Load Balancer
 - b. TCP or UDP for Network Load Balancer
4. Configure health checks for your load balancer

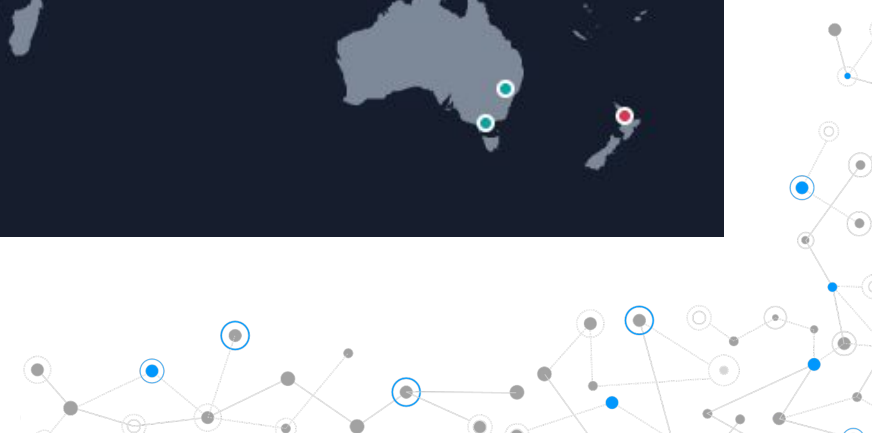


AWS Load Balancer benefits:

- Handle of load in one or multiple Availability Zones
- 1 additional security layer before the servers
- Control traffic for all servers
- Avoid DoS
- High availability services

Availability zones vs Regions

- There are 31 AWS regions around the world.
- Each regions may have one or more availability zones. In total there are 99 availability zones.
- Forecast of 5 more Availability Zones and 5 more AWS Regions in Canada, Israel, Malaysia, New Zealand, and Thailand.

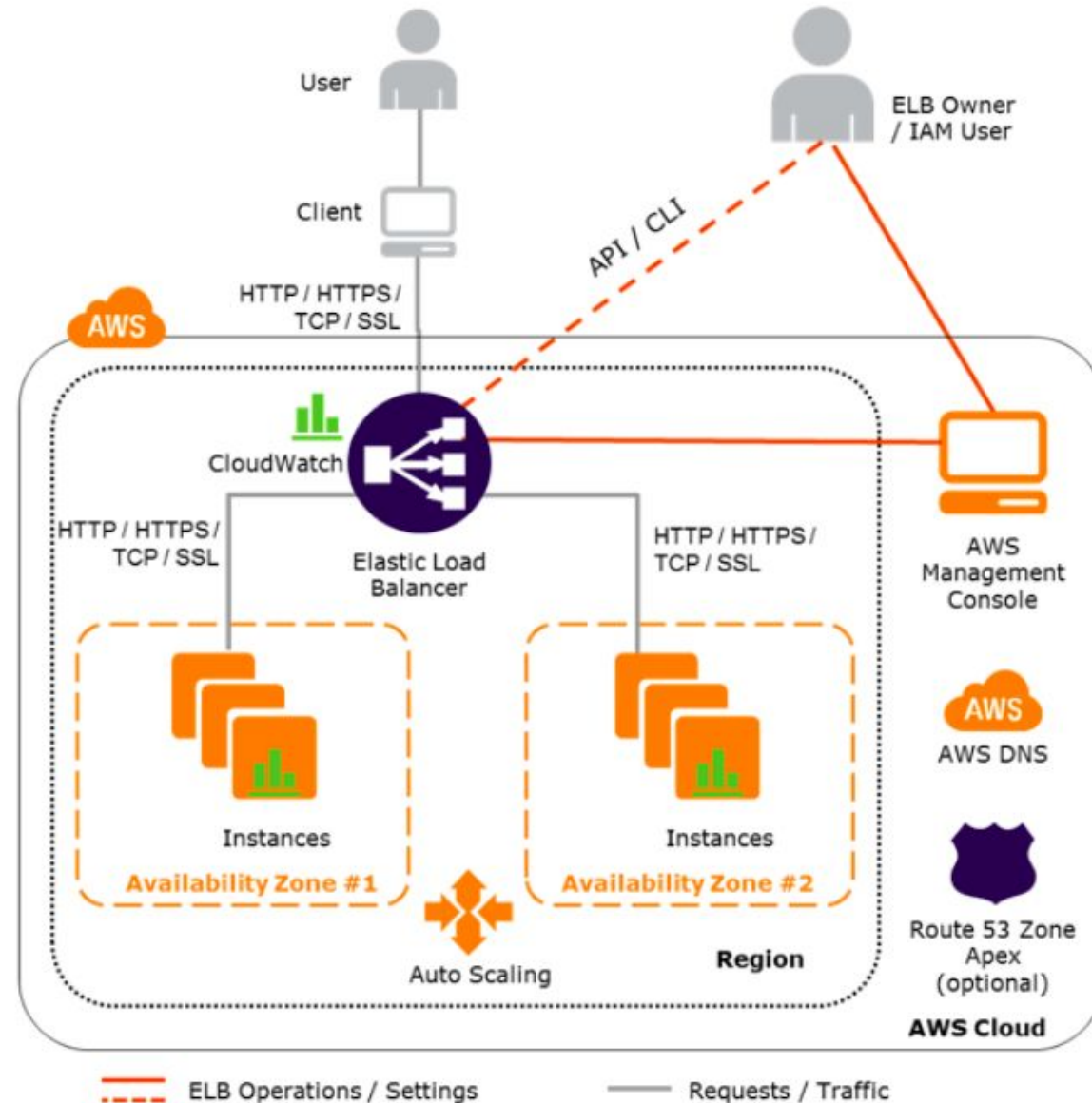


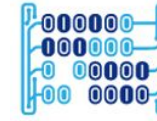
AWS Load Balancing



Follow the steps of the presentation about VPC to create a VPC with two instances as represented in the next topology:

Document everything and deliver two reports in e-aulas:
i. Creation of VPC (First Report)
ii. Implementation of the Load Balancer (Second Report)





Create a VPC

Filter by tags and attributes or search by keyword

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main Route table	Main Network ACL
VPC-Comp...	vpc-04c7932410c4c0947	available	10.0.0.0/16	-	dopt-f476808e	rtb-09164cdd4ba5bc58a	acl-01d73d8065a2deef2
Test-DD	vpc-04f2ccbd1e732f6cf	available	10.0.0.0/16	-	dopt-f476808e	rtb-0a3026a7a7d6bcbbd	acl-08fa98b6f3a9624bf

VPC: vpc-04c7932410c4c0947

VPC ID	vpc-04c7932410c4c0947	Tenancy	default
State	available	Default VPC	No
IPv4 CIDR	10.0.0.0/16	Classic link	Disabled
IPv6 CIDR	-	IPv6 Pool	-
DNS resolution	Enabled	Network ACL	acl-01d73d8065a2deef2
DNS hostnames	Enabled	DHCP options set	dopt-f476808e
ClassicLink DNS Support	Disabled	Route table	rtb-09164cdd4ba5bc58a
Owner	094295054279		

AWS Load Balancing

Configure a Security Group

Requirement:

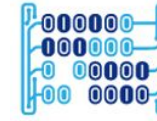
- The security group should allow servers connect to http/https servers in internet to download software or updates.
- The security group should allow servers connect to Email Servers through protocols POP3 and IMAPS
- The security group should allow servers connect to DNS servers so web pages can be requested by name and not only by IP
- The security group should allow servers connect to make connectivity test through ICMP (Ping tool)

Inbound rules	Outbound rules	Tags		
Outbound rules				
Type	Protocol	Port range	Destination	Description - optional
HTTP	TCP	80	0.0.0.0/0	Allow to download software
HTTP	TCP	80	::/0	Allow to download software
POP3	TCP	110	0.0.0.0/0	To allow that our servers contact Email servers
POP3	TCP	110	::/0	To allow that our servers contact Email servers
POP3S	TCP	995	0.0.0.0/0	To allow that our servers contact Email servers
POP3S	TCP	995	::/0	To allow that our servers contact Email servers
IMAPS	TCP	993	0.0.0.0/0	To allow that our servers contact Email servers
IMAPS	TCP	993	::/0	To allow that our servers contact Email servers
IMAP	TCP	143	0.0.0.0/0	To allow that our servers contact Email servers
IMAP	TCP	143	::/0	To allow that our servers contact Email servers
DNS (UDP)	UDP	53	0.0.0.0/0	To allow that our servers contact DNS servers
DNS (UDP)	UDP	53	::/0	To allow that our servers contact DNS servers
DNS (TCP)	TCP	53	0.0.0.0/0	To allow that our servers contact DNS servers
DNS (TCP)	TCP	53	::/0	To allow that our servers contact DNS servers
HTTPS	TCP	443	0.0.0.0/0	Allow to download software
HTTPS	TCP	443	::/0	Allow to download software
All ICMP - IPv4	ICMP	All	0.0.0.0/0	To allow that our servers validate connectivity
	ICMP	All	::/0	To allow that our servers validate connectivity

Inbound rules	Outbound rules	Tags		
Inbound rules				
Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	Web Access
HTTP	TCP	80	::/0	Web Access
SSH	TCP	22	0.0.0.0/0	SSH for administration
SSH	TCP	22	::/0	SSH for administration
HTTPS	TCP	443	0.0.0.0/0	Web Access
HTTPS	TCP	443	::/0	Web Access

Requirement:

- The security group should allow servers be reachable (Inbound Rules) from internet through protocol HTTP/HTTPS and, SSH



The VPC should have an Internet Gateway

- VPC Dashboard
- Filter by VPC:
- VIRTUAL PRIVATE CLOUD
 - Your VPCs
 - Subnets
 - Route Tables
 - Internet Gateways**
 - Egress Only Internet Gateways
 - DHCP Options Sets
 - Elastic IPs
 - Endpoints
 - Endpoint Services
 - NAT Gateways
 - Peering Connections
- SECURITY
 - Network ACLs
 - Security Groups
- VIRTUAL PRIVATE NETWORK (VPN)
 - Customer Gateways
 - Virtual Private Gateways
 - Site-to-Site VPN Connections
 - Client VPN Endpoints

Create internet gateway Actions ▾

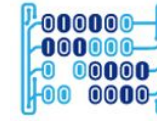
Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	ID	State	VPC	Owner
<input type="checkbox"/>		igw-05a05c7a1b4f80527	attached	vpc-04f2ccbd1e732f6cf Test-DD	094295054279
<input checked="" type="checkbox"/>		igw-0b5b39dd2f355b463	attached	vpc-04c7932410c4c0947 VPC-Company999	094295054279
<input type="checkbox"/>		igw-1567df6e	attached	vpc-67f8ad1d	094295054279

Our Internet Gateway

Each VPC has an “Internet Gateway”
to allow the access to internet

AWS Load Balancing



The VPC should have Route Tables

This route allow that instances of the subnets may communicate with other instances in the VPC

Thess routes allow that instances of the subnets may communicate with Internet

VPC Dashboard

Filter by VPC:
Select a VPC

- VIRTUAL PRIVATE CLOUD
- Your VPCs
- Subnets
- Route Tables**
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

- SECURITY
- Network ACLs
- Security Groups

- VIRTUAL PRIVATE NETWORK (VPN)
- Customer Gateways
- Virtual Private Gateways
- Site-to-Site VPN Connections
- Client VPN Endpoints

Filter by tags and attributes or search by keyword

Name	Route Table ID	Explicit subnet associations	Edge associations	Main	VPC ID
<input checked="" type="checkbox"/>	rtb-09164cdd4ba5bc58a	-	-	Yes	vpc-04c7932410c4c0947 VPC-Company999
<input type="checkbox"/>	rtb-07c4abcbedea8d9e7	subnet-0e5b43dfcaded5f86	-	No	vpc-04c7932410c4c0947 VPC-Company999

Route Table: rtb-09164cdd4ba5bc58a

- Summary
- Routes**
- Subnet Associations
- Edge Associations
- Route Propagation
- Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

Name	Route Table ID	Explicit subnet associations	Edge associations	Main	VPC ID
<input checked="" type="checkbox"/>	rtb-07c4abcbedea8d9e7	subnet-0e5b43dfcaded5f86	-	No	vpc-04c7932410c4c0947 VPC-Company999

Route Table: rtb-07c4abcbedea8d9e7

- Summary
- Routes**
- Subnet Associations
- Edge Associations
- Route Propagation
- Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-0b5b39dd2f355b463	active	No

AWS Load Balancing

Create the Web servers (2)

Requirements:

- Instances must be created in the same public subnet
- Both instances must be in the same security group

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	<input type="text" value="vpc-04c7932410c4c0947 VPC-Company999"/>	
Subnet	<input type="text" value="subnet-0e5b43dfcaded5f86 PubSubnet1 us-east-1"/>	250 IP Addresses available
Auto-assign Public IP	<input type="text" value="Use subnet setting (Disable)"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="text" value="Open"/>	
IAM role	<input type="text" value="None"/>	
Shutdown behavior	<input type="text" value="Stop"/>	
Stop - Hibernate behavior	<input type="checkbox"/> Enable hibernation as an additional stop behavior	
Enable termination protection	<input type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	
Tenancy	<input type="text" value="Shared - Run a shared hardware instance"/>	Additional charges will apply for dedicated tenancy.
Elastic Inference	<input type="checkbox"/> Add an Elastic Inference accelerator	

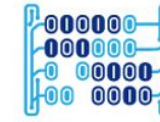
Instance: **i-04d5873230c900cfa (Web Server 1)** Private IP: 10.0.0.43

Description	Status Checks	Monitoring	Tags
Instance ID	i-04d5873230c900cfa	Public DNS (IPv4)	-
Instance state	stopped	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Finding	You may not have permission to access AWS Compute Optimizer.	Elastic IPs	-
Private DNS	ip-10-0-0-43.ec2.internal	Availability zone	us-east-1e
Private IPs	10.0.0.43	Security groups	AccessToPublicWebServers . view inbound rules . view outbound rules
Secondary private IPs		Scheduled events	-
VPC ID	vpc-04c7932410c4c0947 (VPC-Company999)	AMI ID	amzn2-ami-hvm-2.0.20200304.0-x86_64-gp2 (ami-0fc61db8544a617ed)
Subnet ID	subnet-0e5b43dfcaded5f86 (PubSubnet1)	Platform details	-
Network interfaces	eth0	Usage operation	-
IAM role	-	Source/dest. check	True
Key pair name	WebServer1000	T2/T3 Unlimited	Disabled

Instance: **i-003e6def12553b7fd (Web Server 2)** Private IP: 10.0.0.133

Description	Status Checks	Monitoring	Tags
Instance ID	i-003e6def12553b7fd	Public DNS (IPv4)	-
Instance state	stopped	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Finding	You may not have permission to access AWS Compute Optimizer.	Elastic IPs	-
Private DNS	ip-10-0-0-133.ec2.internal	Availability zone	us-east-1e
Private IPs	10.0.0.133	Security groups	AccessToPublicWebServers . view inbound rules . view outbound rules
Secondary private IPs		Scheduled events	-
VPC ID	vpc-04c7932410c4c0947 (VPC-Company999)	AMI ID	amzn2-ami-hvm-2.0.20200406.0-x86_64-gp2 (ami-0323c3dd2da7fb37d)
Subnet ID	subnet-0e5b43dfcaded5f86 (PubSubnet1)	Platform details	-
Network interfaces	eth0	Usage operation	-
IAM role	-	Source/dest. check	True
Key pair name	WebServer1001	T2/T3 Unlimited	Disabled

AWS Load Balancing



VPC Dashboard

Filter by VPC:

Select a VPC

- VIRTUAL PRIVATE CLOUD
 - Your VPCs
 - Subnets
 - Route Tables
 - Internet Gateways
 - Egress Only Internet Gateways
 - DHCP Options Sets
 - Elastic IPs**
 - Endpoints
 - Endpoint Services
 - NAT Gateways
 - Peering Connections
- SECURITY
 - Network ACLs
 - Security Groups
- VIRTUAL PRIVATE NETWORK (VPN)
 - Customer Gateways
 - Virtual Private Gateways
 - Site-to-Site VPN Connections
 - Client VPN Endpoints

Allocate new address Actions

Filter by tags and attributes or search by keyword

Name	Elastic IP	Allocation ID	Instance	Private IP address	Scope	Association ID	Network Interface ID
Public IP 1	3.224.44.132	eipalloc-0aabc9ca2c881da2f	i-04d5873230c900cfa	10.0.0.43	vpc	eipassoc-03cada8...	eni-09f9be6fa2e11d5b0
Public IP 2	52.200.146.119	eipalloc-0314df1f23fabb41d	i-003e6def12553b7fd	10.0.0.133	vpc	eipassoc-0f241c7...	eni-0bc49447a44007965

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
Amazon001	i-0f81c1687795979a4	t2.micro	us-east-1b	stopped		None	
Amazon002	i-0adb0d8780566fe69	t2.micro	us-east-1b	stopped		None	
Amazon003	i-0d4c3b97023baa82e	t2.micro	us-east-1b	stopped		None	
EthereumBastion	i-0003160e5669d0904	t2.micro	us-east-1e	stopped		None	
Web Server 1	i-04d5873230c900cfa	t2.micro	us-east-1e	stopped		None	ec2-3-224-44-132.com...
Web Server 2	i-003e6def12553b7fd	t2.micro	us-east-1e	stopped		None	ec2-52-200-146-119.co...
	i-00dcf2354f92be0a8	t2.micro	us-east-1b	stopped		None	

Instance: i-04d5873230c900cfa (Web Server 1) Elastic IP: 3.224.44.132

Description	Status Checks	Monitoring	Tags
Instance ID	i-04d5873230c900cfa	Public DNS (IPv4)	ec2-3-224-44-132.compute-1.amazonaws.com
Instance state	stopped	IPv4 Public IP	3.224.44.132
Instance type	t2.micro	IPv6 IPs	-
Finding	You may not have permission to access AWS Compute Optimizer.	Elastic IPs	3.224.44.132*
Private DNS	ip-10-0-0-43.ec2.internal	Availability zone	us-east-1e
Private IPs	10.0.0.43	Security groups	AccessToPublicWebServers. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	-
VPC ID	vpc-04c7932410c4c0947 (VPC-Company999)	AMI ID	amzn2-ami-hvm-2.0.20200304.0-x86_64-gp2 (ami-0fc61db8544a617ed)

Allocate one Elastic IP to each server



Connect to each Server

```
(base) daniel@probook-440:~/Dropbox/UR/Ciberseguridad/AWS$ ssh -i "WebServer1000.pem" ec2-user@ec2-3-224-44-132.compute-1.amazonaws.com
The authenticity of host 'ec2-3-224-44-132.compute-1.amazonaws.com (3.224.44.132)' can't be established.
ECDSA key fingerprint is SHA256:J3SWkvTLNEqncer958lm07hxx05wrw0EKwT7YSpPs+s.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-3-224-44-132.compute-1.amazonaws.com,3.224.44.132' (ECDSA) to the list of known hosts.
Last login: Thu Apr  2 21:11:01 2020 from static-190-24-131-147.static.etb.net.co

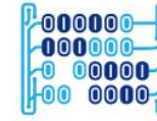
  _ | _ | _ )
  _ | ( _ | /  Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
5 package(s) needed for security, out of 11 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-43 ~]$
```

```
(base) daniel@probook-440:~/Dropbox/UR/Ciberseguridad/AWS$ ssh -i "WebServer1001.pem" ec2-user@ec2-52-200-146-119.compute-1.amazonaws.com
The authenticity of host 'ec2-52-200-146-119.compute-1.amazonaws.com (52.200.146.119)' can't be established.
ECDSA key fingerprint is SHA256:gLfD+/mkZWI2HIryBUvNf6Qy/0Y6vhglV6Rj23p/Tso.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-52-200-146-119.compute-1.amazonaws.com' (ECDSA) to the list of known hosts.
Warning: the ECDSA host key for 'ec2-52-200-146-119.compute-1.amazonaws.com' differs from the key for the IP address '52.200.146.119'
Offending key for IP in /home/daniel/.ssh/known_hosts:3
Are you sure you want to continue connecting (yes/no)? yes

  _ | _ | _ )
  _ | ( _ | /  Amazon Linux 2 AMI
  _ | \ _ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-0-133 ~]$
```



Install a web server on each Server

Install Apache Web Server with the following commands:

- Connect to your EC2 instance and install the Apache web server.

```
$ sudo yum -y install httpd
```

- Start the service.

```
$ sudo service httpd start
```

Validate that the Web servers are working:

← → ↻ ⓘ Not secure | 52.200.146.119



This page is used to test the proper operation of the Apache HTTP server after it has been installed. If yo

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

← → ↻ ⓘ Not secure | 3.224.44.132



This page is used to test the proper operation of the Apache HTTP server after it has been installed. If yo

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

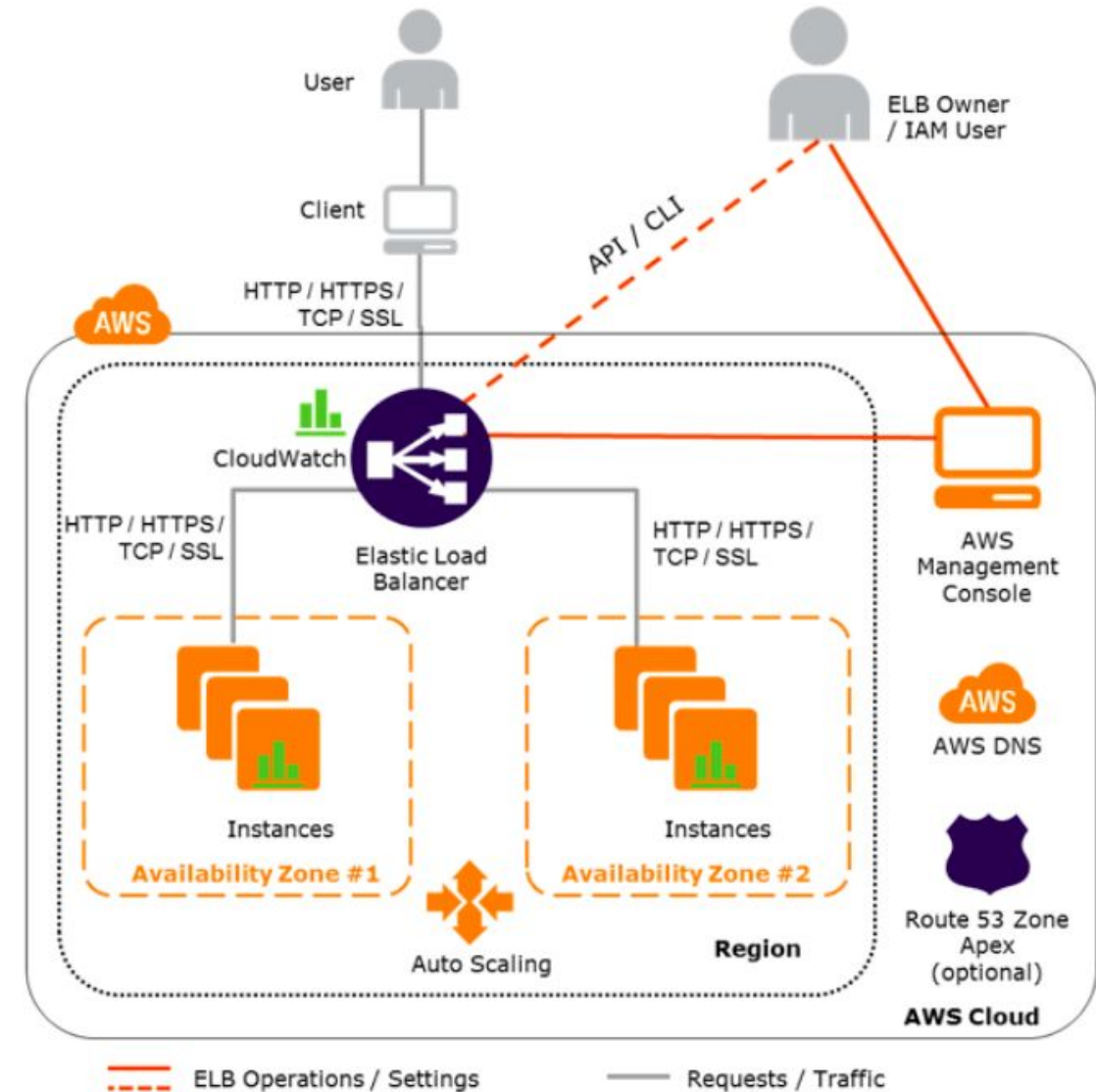
If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

Now we have our topology and we are ready to configure our Load Balancer!
(Second report)

Steps:

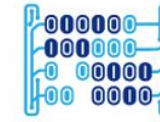
1. Create a load balancer (Application Load Balancer or Network Load Balancer)
2. Specify a unique name and a network
3. Create listeners for your load balancer
 - a. HTTP or HTTPS for Application Load Balancer
 - b. TCP or UDP for Network Load Balancer
4. Configure health checks for your load balancer



AWS Load Balancing



Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

New EC2 Experience
[Learn more](#)

- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts **New**
- Scheduled Instances
- Capacity Reservations

IMAGES

- AMIs
- Bundle Tasks

ELASTIC BLOCK STORE

- Volumes
- Snapshots
- Lifecycle Manager

NETWORK & SECURITY

- Security Groups **New**
- Elastic IPs **New**
- Placement Groups **New**
- Key Pairs **New**
- Network Interfaces

LOAD BALANCING

Load Balancers

Target Groups

AUTO SCALING

- Launch Configurations
- Auto Scaling Groups

Create Load Balancer

Actions

Filter by tags and attributes or search by keyw

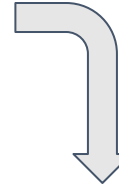
None found

Name

DNS name

State

You do not have any load balancers in this region.



Select load balancer type

Elastic Load Balancing supports three types of load balancers: Application Load Balancers, Network Load Balancers (new), and Classic Load Balancers. Choose the load balancer type that meets your needs. [Learn more about which load balancer is right for you](#)

Application Load Balancer

HTTP
HTTPS

Create

Choose an Application Load Balancer when you need a flexible feature set for your web 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.

[Learn more >](#)

Network Load Balancer

TCP
TLS
UDP

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 application. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

[Learn more >](#)

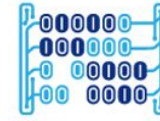
Classic Load Balancer

PREVIOUS GENERATION
for HTTP, HTTPS, and TCP

Create

Choose a Classic Load Balancer when you have an existing application running in the EC2-Classical network.

[Learn more >](#)



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 [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.

IP address type [Info](#)

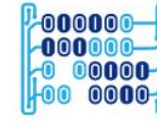
Select the type of IP addresses that your subnets use.

IPv4

Recommended for internal load balancers.

Dualstack

Includes IPv4 and IPv6 addresses.



Network mapping [Info](#)

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

VPC [Info](#)

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

-
vpc-0129cca7353dc8539
IPv4: 172.31.0.0/16



[Create new VPC](#)

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.

us-east-1a (use1-az2)

Subnet

subnet-0f6ab1652698fbbab

IPv4 address

Assigned by AWS

us-east-1b (use1-az4)

Subnet

subnet-08d07230a64d52c68

IPv4 address

Assigned by AWS




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

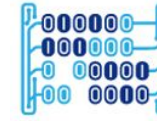
- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end 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.



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

Forward to

WebServersUR

HTTP ▼



1-65535

Target type: Instance, IPv4

[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



Target group name

WebServersUR

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

Protocol

HTTP



Port

80



1-65535

VPC

Select the VPC with the instances that you want to include in the target group.

-
vpc-0129cca7353dc8539
IPv4: 172.31.0.0/16

Protocol version

HTTP1

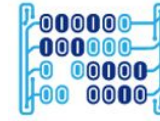
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

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.



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 ▼

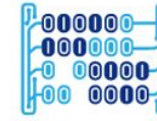
Health check path

Use the default path of "/" to ping the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

► **Advanced health check settings**



Successfully created target group: [WebServersUR](#)

EC2 > Target groups

Target groups (1/1) [Info](#)



Actions ▾

Create target group

Find resources by attribute or tag

< 1 > ⚙

<input checked="" type="checkbox"/>	Name ▾	ARN ▾	Port ▾	Protocol ▾	Target type ▾	Load balancer ▾	VPC ID ▾
<input checked="" type="checkbox"/>	WebServersUR	arn:aws:elasticloadbalanci...	80	HTTP	Instance	None associated	vpc-0129cca7353dc8539

Target group: WebServersUR

[Details](#) | [Targets](#) | [Monitoring](#) | [Health checks](#) | [Attributes](#) | [Tags](#)

Details

[arn:aws:elasticloadbalancing:us-east-1:499517898523:targetgroup/WebServersUR/888e26e104c39208](#)

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-0129cca7353dc8539
IP address type IPv4	Load balancer None associated		

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
0	✔ 0	✘ 0	⋮ 0	⬇ 0	⬇ 0



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

HTTP ▼

Port

80

1-65535

Default action [Info](#)

Forward to

WebServersUR

Target type: Instance, IPv4

HTTP ▼



[Create target group](#)

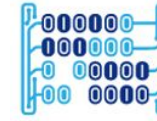
Listener tags - optional

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](#)



Summary

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

Basic configuration [Edit](#)

LB1

- Internet-facing
- IPv4

Security groups [Edit](#)

- default
[sg-01572dc9cb02ad66f](#)

Network mapping [Edit](#)

VPC [vpc-0129cca7353dc8539](#)

- us-east-1a
[subnet-0f6ab1652698fbbab](#)
- us-east-1b
[subnet-08d07230a64d52c68](#)

Listeners and routing [Edit](#)

- HTTP:80 defaults to
[WebServersUR](#)

Add-on services [Edit](#)

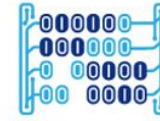
None

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.



✔ Successfully created load balancer: [LB1](#)

Note: 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](#) > [LB1](#) > [Create Application Load Balancer](#)

Create Application Load Balancer



Suggested next steps

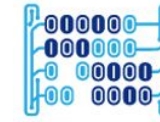
- Review, customize, or configure attributes for your load balancer and listeners using the **Description** and **Listeners** tabs within [LB1](#).
- Discover other services that you can integrate with your load balancer. Visit the **Integrated services** tab within [LB1](#).

[View load balancer](#)

AWS Load Balancing



Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

EC2 > Load balancers

Load balancers (1/1)

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

Find resources by attribute or tag

LB1

Clear filters

<input checked="" type="checkbox"/>	Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
<input checked="" type="checkbox"/>	LB1	LB1-605784927.us-east-1....	Active	vpc-0129cca7353dc8539	2 Availability Zones	application	May 23, 2023, 13:24 (UTC-05:00)

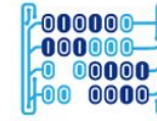
Load balancer: LB1

Details | Listeners | Network mapping | Security | Monitoring | Integrations | Attributes | Tags

Details

Load balancer type Application	Status Active	VPC vpc-0129cca7353dc8539	IP address type IPv4
Scheme Internet-facing	Hosted zone Z355XDOTRQ7X7K	Availability Zones subnet-0f6ab1652698fbbab us-east-1a (use1-az2) subnet-08d07230a64d52c68 us-east-1b (use1-az4)	Date created May 23, 2023, 13:24 (UTC-05:00)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:499517898523:loadbalancer/app/LB1/055b442ea4aa697a	DNS name LB1-605784927.us-east-1.elb.amazonaws.com (A Record)		

AWS Load Balancing



aws Services Search [Alt+S]

Rules + Edit Sort - LB1 | HTTP:80 ↕ Refresh Help

Click a location for your new rule. Each rule must include one action of type forward, redirect, fixed response.

✓ New rule was created successfully. ✕

LB1 | HTTP:80 (2 rules)

▼ Rule limits for condition values, wildcards, and total rules.

- 100 total rules per application load balancer
- 5 condition values per rule
- 5 wildcards per rule
- 5 weighted target groups per rule

[Learn more](#) ↗

+ Insert Rule

1 am...edc2a ▼

IF

✓ Source IP is 201.234.181.230/32

THEN

Return fixed response 503 (more...)

+ Insert Rule

last **HTTP 80: default action**

This rule cannot be moved or deleted

IF

✓ Requests otherwise not routed

THEN

Forward to
[WebServersUR: 1](#) (100%)
Group-level stickiness: Off



Universidad del
Rosario



MACC



HINNT

¡Gracias!

