

DOCUMENTACIÓN TÉCNICA – PROYECTO 2

JUAN CAMILO GUERRERO ALARCÓN

DANIEL GARCÍA GARCÍA

CÉSAR ANDRÉS GARCÍA POSADA

TÓPICOS ESPECIALES EN TELEMÁTICA

UNIVERSIDAD EAFIT

MEDELLÍN

2021-1

Ilustración 1 Despliegue de la aplicación Web Multi Availability Zone.....	3
Ilustración 2 VPC para el proyecto con IP 172.18.0.0/16.....	3
Ilustración 3 Conjunto de Subnets del proyecto.....	4
Ilustración 4 Internet Gateway	4
Ilustración 5 Grupo de seguridad para las instancias NAT	5
Ilustración 6 Instancia NAT para la Región A	5
Ilustración 7 Instancia NAT para la Región B.....	6
Ilustración 8 Tablas de rutas	6
Ilustración 9 Asociación de la tabla de rutas a la Subnet correspondiente	7
Ilustración 10 Al ser una Subnet pública, se asocia al Internet Gateway	7
Ilustración 11 Asociación de la tabla de rutas a la Subnet correspondiente	7
Ilustración 12 Al ser una Subnet privada, se asocia al NAT correspondiente.....	8
Ilustración 13 Asociación de la tabla de rutas a la Subnet correspondiente	8
Ilustración 14 Al ser una Subnet pública, se asocia al Internet Gateway	9
Ilustración 15 Asociación de la tabla de rutas a la Subnet correspondiente	9
Ilustración 16 Al ser una Subnet privada, se asocia al NAT correspondiente.....	10
Ilustración 17 Grupo de seguridad del Bastion Host.....	10
Ilustración 18 Configuración instancia Bastion Host Región A	11
Ilustración 19 Configuración instancia Bastion Host Región B.....	12
Ilustración 20 Grupo de seguridad para la base de datos.....	13
Ilustración 21 Grupo de subred para la base de datos	13
Ilustración 22 Subnets asociadas al grupo de Subnet de la base de datos.....	13
Ilustración 23 Base de datos en MySQL	14
Ilustración 24 EFS	14
Ilustración 25 Instancia del webserver.....	15
Ilustración 26 Imagen AMI para el servicio de Auto Scaling	16
Ilustración 27 Balanceador de carga	16
Ilustración 28 Grupo de Auto Scaling.....	17
Ilustración 29 Delegación del DNS a CloudFlare	18
Ilustración 30 Generación de certificados de seguridad.....	18
Ilustración 31 Configuración del balanceador de carga con el certificado de seguridad	19
Ilustración 32 Plugin de autenticación por 2 factores	19

En el siguiente documento se pretende mostrar en detalle el paso a paso que se realizó para el despliegue de la siguiente arquitectura en AWS.

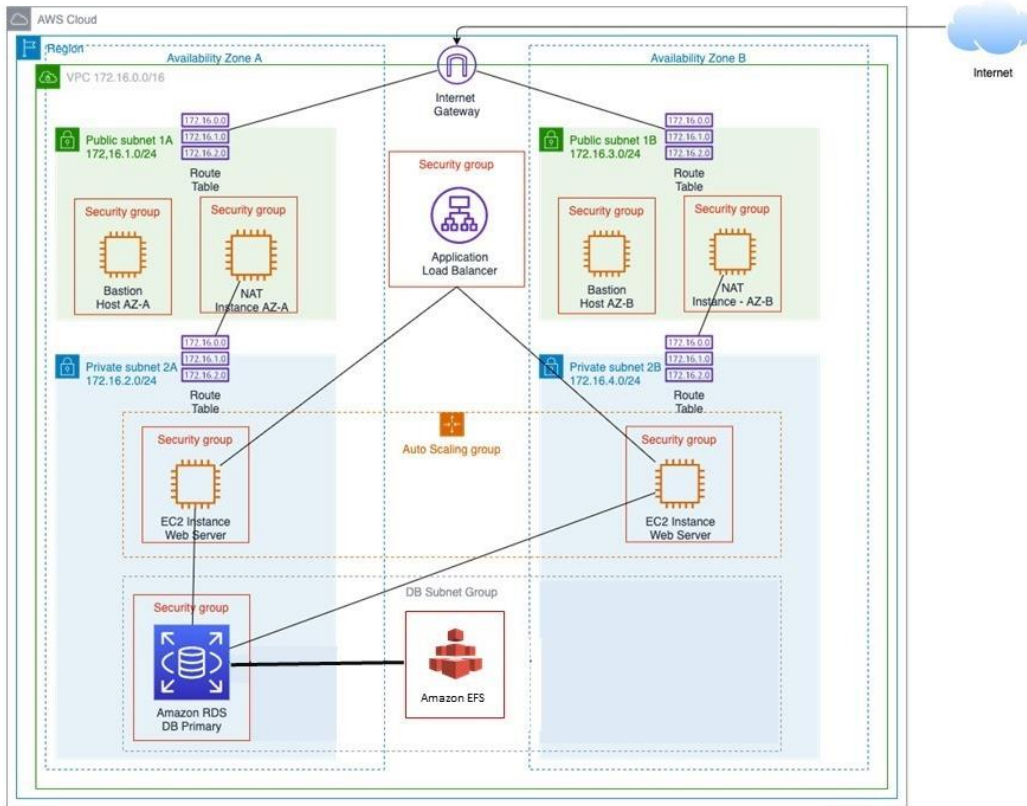


Ilustración 1 Despliegue de la aplicación Web Multi Availability Zone

En primer lugar, se tiene la creación y configuración de la VPC; en este caso la dirección IP seleccionada es 172.18.0.0/16

Your VPCs (1/2) Info						
<input type="text" value="Filter VPCs"/> 1						
<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network border group)	
<input checked="" type="checkbox"/>	MyWebAPP-VPC	vpc-0ea1002a70cf83fc2	Available	172.18.0.0/16	-	
<input type="checkbox"/>	-	vpc-6441fe19	Available	172.31.0.0/16	-	

Ilustración 2 VPC para el proyecto con IP 172.18.0.0/16

Después de crear la VPC, se procede con la creación de las Subnets. Acá es importante destacar que se tienen dos regiones (Región A y Región B) y para cada Región se crean dos Subnets; una pública y una privada.

En la siguiente imagen se pueden ver las cuatro Subnets y se puede apreciar que todas están enlazadas a la misma VPC (vpc-0ea1002a70cf83fc2|MyWebAPP-VPC) y a su vez se puede apreciar las direcciones IPs de cada Subnet

Subnets (10) Info						Actions
Filter subnets						
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	
<input type="checkbox"/>	-	subnet-a81976f7	Available	vpc-6441fe19	172.31.32.0/20	
<input type="checkbox"/>	-	subnet-1a8e382b	Available	vpc-6441fe19	172.31.48.0/20	
<input type="checkbox"/>	Public Subnet B	subnet-0f00af9f5d08ccf6b	Available	vpc-0ea1002a70cf83fc2 My...	172.18.4.0/24	
<input type="checkbox"/>	-	subnet-8f4d7fc2	Available	vpc-6441fe19	172.31.16.0/20	
<input type="checkbox"/>	Public Subnet A	subnet-0de558c4405646964	Available	vpc-0ea1002a70cf83fc2 My...	172.18.2.0/24	
<input type="checkbox"/>	Private Subnet A	subnet-063f72d71df2efd20	Available	vpc-0ea1002a70cf83fc2 My...	172.18.1.0/24	
<input type="checkbox"/>	-	subnet-fe204298	Available	vpc-6441fe19	172.31.0.0/20	
<input type="checkbox"/>	-	subnet-2cb8d10d	Available	vpc-6441fe19	172.31.80.0/20	
<input type="checkbox"/>	Private Subnet B	subnet-0674a3f9e597f556f	Available	vpc-0ea1002a70cf83fc2 My...	172.18.3.0/24	
<input type="checkbox"/>	-	subnet-2a6c4824	Available	vpc-6441fe19	172.31.64.0/20	

Subnets (10) Info						Actions
Filter subnets						
<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	
<input type="checkbox"/>	Public Subnet B	subnet-0f00af9f5d08ccf6b	Available	vpc-0ea1002a70cf83fc2 My...	172.18.4.0/24	us-east-1b
<input type="checkbox"/>	-	subnet-8f4d7fc2	Available	vpc-6441fe19	172.31.16.0/20	us-east-1b
<input type="checkbox"/>	Public Subnet A	subnet-0de558c4405646964	Available	vpc-0ea1002a70cf83fc2 My...	172.18.2.0/24	us-east-1a
<input type="checkbox"/>	Private Subnet A	subnet-063f72d71df2efd20	Available	vpc-0ea1002a70cf83fc2 My...	172.18.1.0/24	us-east-1a
<input type="checkbox"/>	-	subnet-fe204298	Available	vpc-6441fe19	172.31.0.0/20	us-east-1d
<input type="checkbox"/>	-	subnet-2cb8d10d	Available	vpc-6441fe19	172.31.80.0/20	us-east-1a
<input type="checkbox"/>	Private Subnet B	subnet-0674a3f9e597f556f	Available	vpc-0ea1002a70cf83fc2 My...	172.18.3.0/24	us-east-1b

Ilustración 3 Conjunto de Subnets del proyecto

Una vez configurada la VPC y las Subnets se procede a configurar el Internet Gateway, el cual permitirá enviar y recibir tráfico desde internet. En la siguiente imagen se puede apreciar el Internet Gateway configurado y a su vez la VPC a la que está asociado.

Internet gateways (1/2) Info					Actions	Create
Filter internet gateways						
<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID		
<input checked="" type="checkbox"/>	MyWebVPC-IGW	igw-0389e8c70ff18d520	Attached	vpc-0ea1002a70cf83fc2 MyWebAPP-...		
<input type="checkbox"/>	-	igw-961af8ec	Attached	vpc-6441fe19		

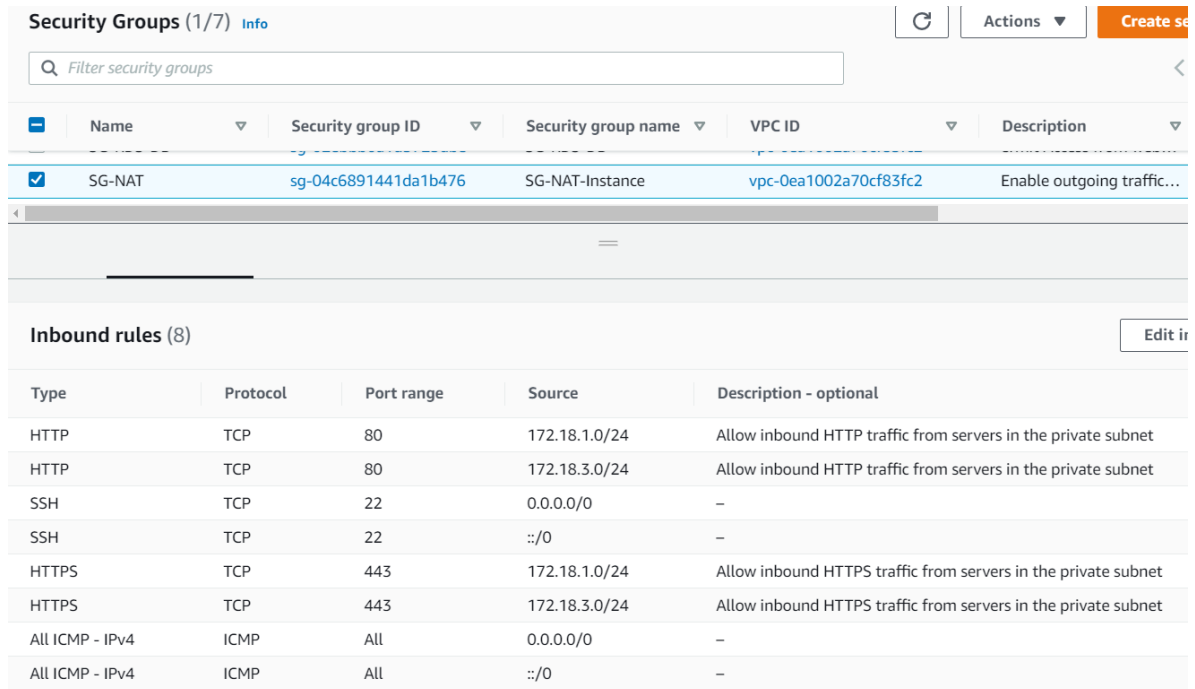
Ilustración 4 Internet Gateway

Haciendo una recapitulación, hasta ahora se tiene creado y configurado la VPC, las 4 Subnets y el Internet Gateway.

El siguiente paso será crear y configurar las instancias NAT, se debe crear una instancia NAT para cada zona (Región A y Región B). Estas instancias permiten enviar tráfico desde la red privada hacia internet.

Para la configuración de la NAT, primero es indispensable la creación de un grupo de seguridad para las instancias NAT.

En la siguiente imagen se puede observar todas las reglas que se añadieron al grupo de seguridad de las instancias NAT.



The screenshot shows the AWS Management Console for Security Groups. The 'SG-NAT' group is selected, and its inbound rules are displayed. The rules allow inbound traffic for HTTP, SSH, and HTTPS from specific source IP ranges, and allow all ICMP traffic.

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	172.18.1.0/24	Allow inbound HTTP traffic from servers in the private subnet
HTTP	TCP	80	172.18.3.0/24	Allow inbound HTTP traffic from servers in the private subnet
SSH	TCP	22	0.0.0.0/0	–
SSH	TCP	22	:::0	–
HTTPS	TCP	443	172.18.1.0/24	Allow inbound HTTPS traffic from servers in the private subnet
HTTPS	TCP	443	172.18.3.0/24	Allow inbound HTTPS traffic from servers in the private subnet
All ICMP - IPv4	ICMP	All	0.0.0.0/0	–
All ICMP - IPv4	ICMP	All	:::0	–

Ilustración 5 Grupo de seguridad para las instancias NAT

En la siguiente imagen se puede apreciar la configuración de la instancia NAT para la Región A. Se puede observar que esta instancia, está asociada a la VPC creada y a la Subnet publica de la Región A.



The screenshot shows the details of the 'NAT-Instance A' in the AWS EC2 console. The 'Redes' (Network) tab is selected, showing the instance's network configuration. The VPC and Subnet are highlighted with a green circle.

Detalle	Valor
Dirección IPv4 pública	3.82.198.124 dirección abierta
Direcciones IPv4 privadas	172.18.2.117
DNS de IPv4 pública	–
DNS IPv4 privado	ip-172-18-2-117.ec2.internal
ID de VPC	vpc-0ea1002a70cf83fc2 (MyWebAPP-VPC)
ID de subred	subnet-0de558c4405646964 (Public Subnet-A)

Ilustración 6 Instancia NAT para la Región A

De igual forma, se muestra la configuración de la instancia NAT para la región B



Ilustración 7 Instancia NAT para la Región B

El siguiente paso es la configuración de la tabla de rutas. Para el desarrollo del proyecto se requiere dos tablas de rutas por cada Región. Esto debido a que en cada Región se tiene dos Subnets (pública y privada).

De este modo se tiene una vista general de todas las tablas de rutas creadas

Route tables (6) Info						
<input type="text" value="Filter route tables"/>			Actions		Create route table	
<input type="checkbox"/>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input type="checkbox"/>	Public Route Ta... ✎	rtb-06e31def7d253d9db	subnet-0f00af9f5d08ccf...	-	No	vpc-0ea1002a70cf83fc2 My...
<input type="checkbox"/>	Private Route Table B	rtb-089b2766065352254	subnet-0674a3f9e597f...	-	No	vpc-0ea1002a70cf83fc2 My...
<input type="checkbox"/>	Private Route Table A	rtb-0022e49f88b2ba884	subnet-063f72d71df2ef...	-	No	vpc-0ea1002a70cf83fc2 My...
<input type="checkbox"/>	-	rtb-03423fabd70bcb8fa	-	-	Yes	vpc-0ea1002a70cf83fc2 My...
<input type="checkbox"/>	Public Route Table A	rtb-0faa3456ea3f0f0dd	subnet-0de558c440564...	-	No	vpc-0ea1002a70cf83fc2 My...
<input type="checkbox"/>	-	rtb-36cbf148	-	-	Yes	vpc-6441fe19

Ilustración 8 Tablas de rutas

La configuración de las tablas de ruta es dependiendo la procedencia. En primer lugar, se debe enlazar a cada Subnet correspondiente y a su vez se debe tener en cuenta lo siguiente para las rutas por defecto:

- Si la tabla de rutas es de una Subnet publica, entonces las rutas por defecto estarán asociadas al Internet Gateway.
- De otro modo, si la tabla de rutas es de una Subnet privada, entonces las rutas por defecto estarán asociadas al NAT correspondiente.

De este modo se tienen las siguientes tablas de rutas:

1. Tabla de ruta para la Subnet pública de la Región A:



Ilustración 9 Asociación de la tabla de rutas a la Subnet correspondiente

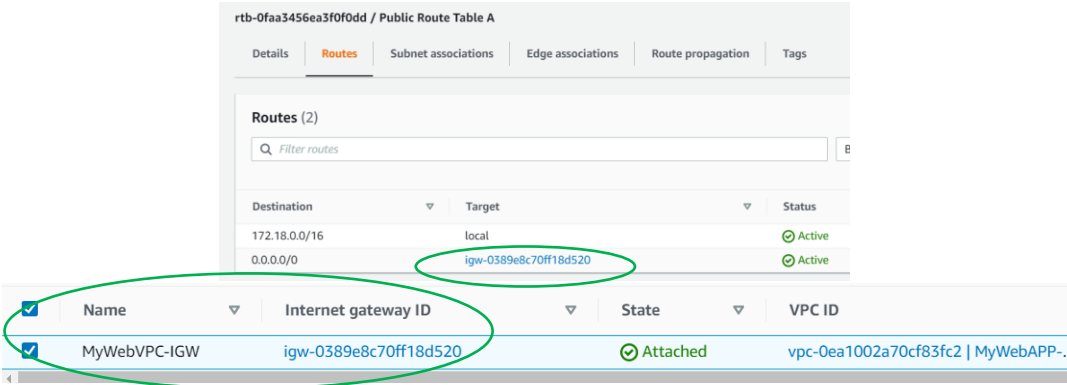


Ilustración 10 Al ser una Subnet pública, se asocia al Internet Gateway

2. Tabla de ruta para la Subnet privada de la Región A:

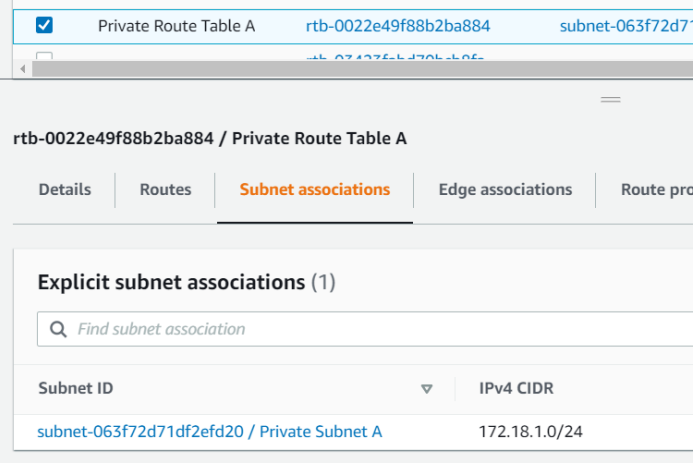


Ilustración 11 Asociación de la tabla de rutas a la Subnet correspondiente

<input checked="" type="checkbox"/>	Private Route Table A	rtb-0022e49f88b2ba884	subn						
<div>Routes (2)</div> <div><input type="text" value="Filter routes"/></div> <table><thead><tr><th>Destination</th><th>Target</th></tr></thead><tbody><tr><td>172.18.0.0/16</td><td>local</td></tr><tr><td>0.0.0.0/0</td><td>eni-0939e8e6ff5c7d6fd</td></tr></tbody></table>				Destination	Target	172.18.0.0/16	local	0.0.0.0/0	eni-0939e8e6ff5c7d6fd
Destination	Target								
172.18.0.0/16	local								
0.0.0.0/0	eni-0939e8e6ff5c7d6fd								
<input type="checkbox"/>	Name	ID de la interfaz de red	ID de subred	ID de VPC					
<input type="checkbox"/>	NAT-Instance A	eni-0939e8e6ff5c7d6fd	subnet-0de558c4405646964	vpc-0ea1002a70cf83fc2					

Ilustración 12 Al ser una Subnet privada, se asocia al NAT correspondiente

3. Tabla de ruta para la Subnet publica de la Región B:

Route tables (1/6) Info

Q Filter route tables

Name

Route table ID

Explicit subnet associat...

Public Route Table B

rtb-06e31def7d253d9db

subnet-0f00af9f5d08ccf...

Private Route Table B

rtb-089b2766065352254

subnet-0674a3f0e597f

rtb-06e31def7d253d9db / Public Route Table B

Details

Routes

Subnet associations

Edge associations

Route propagation

Explicit subnet associations (1)

Q Find subnet association

Subnet ID

IPv4 CIDR

subnet-0f00af9f5d08ccf6b / Public Subnet B

172.18.4.0/24

Ilustración 13 Asociación de la tabla de rutas a la Subnet correspondiente

The screenshot displays the AWS Management Console interface for a Public Route Table B (rtb-06e31def7d253d9db). The 'Routes' tab is selected, showing two routes. The first route has a destination of 172.18.0.0/16 and a target of 'local'. The second route has a destination of 0.0.0.0/0 and a target of 'igw-0389e8c70ff18d520', which is circled in green. Below this, a table lists internet gateways, with 'MyWebVPC-IGW' and its ID 'igw-0389e8c70ff18d520' also circled in green.

Destination	Target
172.18.0.0/16	local
0.0.0.0/0	igw-0389e8c70ff18d520

Name	Internet gateway ID
MyWebVPC-IGW	igw-0389e8c70ff18d520

Ilustración 14 Al ser una Subnet pública, se asocia al Internet Gateway

4. Tabla de ruta para la Subnet privada de la Región B:

The screenshot shows the AWS Management Console for a Private Route Table B (rtb-089b2766065352254). The 'Subnet associations' tab is selected, displaying one explicit subnet association. The table lists the Subnet ID as 'subnet-0674a3f9e597f556f / Private Subnet B' and the IPv4 CIDR as '172.18.3.0/24'.

Subnet ID	IPv4 CIDR
subnet-0674a3f9e597f556f / Private Subnet B	172.18.3.0/24

Ilustración 15 Asociación de la tabla de rutas a la Subnet correspondiente

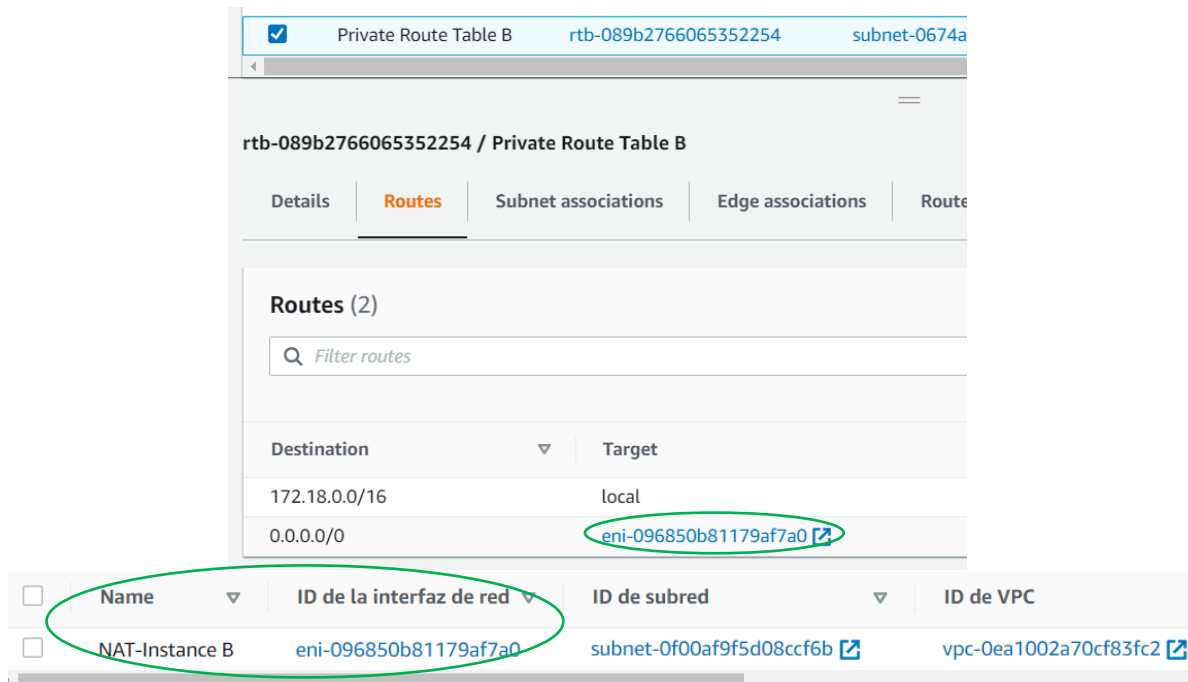


Ilustración 16 Al ser una Subnet privada, se asocia al NAT correspondiente

El siguiente paso es la creación de los Bastion Host; recordemos que un Bastion Host es el mecanismo con el cual se le brinda seguridad a las redes internas de ataques.

Es importante resaltar, que se debe crear un Bastion Host para cada una de las regiones (Región A y Región B).

En primer lugar, se debe configurar el grupo de seguridad del Bastion Host

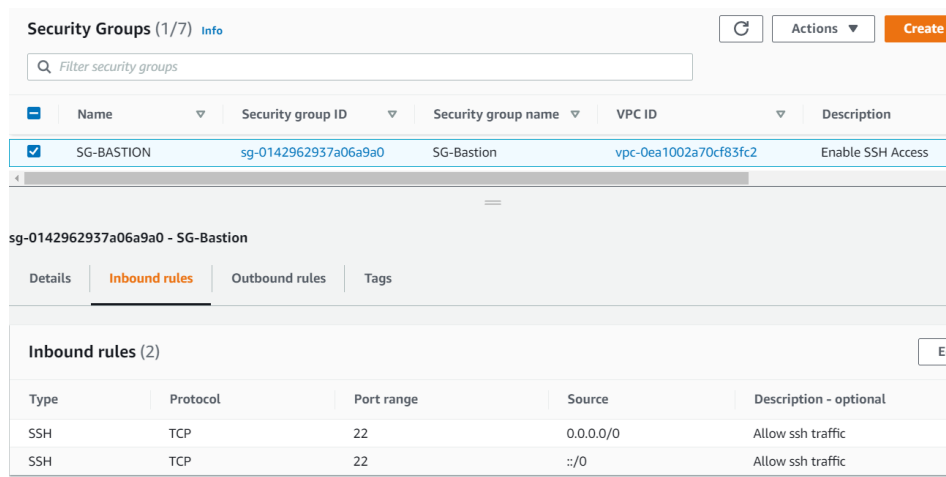


Ilustración 17 Grupo de seguridad del Bastion Host

Ahora para la creación de las instancias, se debe tener en cuenta que cada instancia Bastion Host irá asociada a la Subnet publica de cada región

En la siguiente imagen se muestra la configuración que se le dio a la instancia de Bastion Host para la Región A

The image displays two screenshots of the AWS Management Console. The top screenshot shows the 'Redes' (Network) configuration for the instance 'BASTION HOS...' (ID: i-03c3261ae71af4ea5). It is associated with VPC 'vpc-0ea1002a70cf83fc2 (MyWebAPP-VPC)' and Subnet 'subnet-0de558c4405646964 (Public Subnet A)'. The bottom screenshot shows the 'Seguridad' (Security) configuration for the same instance, associated with the security group 'sg-0142962937a06a9a0 (SG-Bastion)'. Both screenshots show the instance is in a 'running' state.

Detalle	Valor
Dirección IPv4 pública	3.86.252.61 dirección abierta
Direcciones IPv4 privadas	172.18.2.205
DNS de IPv4 pública	-
DNS IPv4 privado	ip-172-18-2-205.ec2.internal
ID de VPC	vpc-0ea1002a70cf83fc2 (MyWebAPP-VPC)
ID de subred	subnet-0de558c4405646964 (Public Subnet A)
Rol de IAM	-
ID del propietario	914417676034
Grupos de seguridad	sg-0142962937a06a9a0 (SG-Bastion)

Ilustración 18 Configuración instancia Bastion Host Región A

De igual forma se tiene la configuración de la instancia Bastion Host para la Región B (No olvidar que se debe de asociar a la Subnet publica de la región).

Instancias (1/8) Información

Conectar Estado de la instancia Acciones Lanzar instancias

Filtrar instancias

Estado de la instancia: running Quitar los filtros

	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la...	Zona de dispon...	DNS d
<input checked="" type="checkbox"/>	BASTION HOS...	i-097ac0016bd0d06ce	En ejecución	t2.micro	2/2 comprobador	1 alarma +	us-east-1b	-
<input type="checkbox"/>	Web Instance	i-05dc9338d17fd431d	En ejecución	t2.micro	2/2 comprobador	1 alarma +	us-east-1b	-

Instancia: i-097ac0016bd0d06ce (BASTION HOST B)

Detalles Seguridad Redes Almacenamiento Comprobaciones de estado Monitoreo Etiquetas

▼ Detalles de redes Información

Dirección IPv4 pública 3.81.227.223 dirección abierta	Direcciones IPv4 privadas 172.18.4.180	ID de VPC vpc-0ea1002a70cf83fc2 (MyWebAPP-VPC)
DNS de IPv4 pública -	DNS IPv4 privado ip-172-18-4-180.ec2.internal	ID de subred subnet-0f00af9f5d08ccf6b (Public Subnet B)

	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...
<input checked="" type="checkbox"/>	BASTION HOS...	i-097ac0016bd0d06ce	En ejecución	t2.micro	2/2 comprobador
<input type="checkbox"/>	Web Instance	i-05dc9338d17fd431d	En ejecución	t2.micro	2/2 comprobador

Instancia: i-097ac0016bd0d06ce (BASTION HOST B)

Detalles Seguridad Redes Almacenamiento Comprobaciones de estado Monitoreo Etiqueta

▼ Detalles de seguridad

Rol de IAM -	ID del propietario 914417676034
Grupos de seguridad sg-0142962937a06a9a0 (SG-Bastion)	

Ilustración 19 Configuración instancia Bastion Host Región B

Una parte fundamental de todo proyecto relacionado a aplicaciones web, se requiere tener una persistencia y trazabilidad de los datos. Para esto, se hace uso de las bases de datos.

En este apartado, se pretende mostrar la configuración realizada para la creación de la base de datos.

En primer lugar, se crea el grupo de seguridad de la Base de datos relacional, en la siguiente imagen se muestra las reglas de este grupo de seguridad. Con esta regla, se configura el grupo de seguridad de la bases de datos con el fin de que pueda aceptar las peticiones entrantes sobre el puerto 3306 desde cualquier instancia EC2 que esté asociada con este grupo de seguridad.

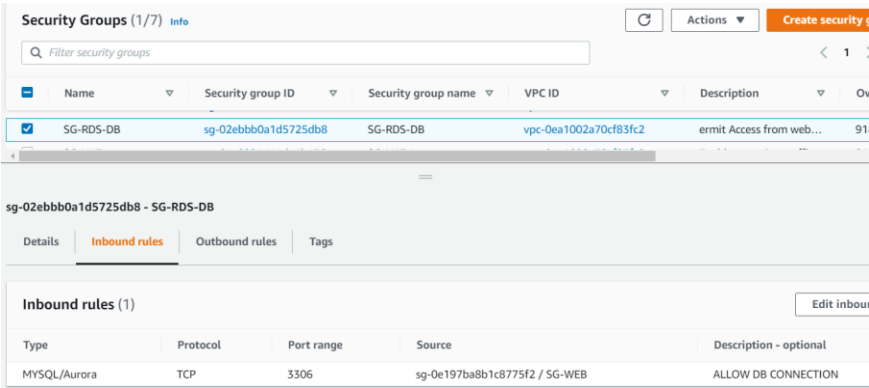


Ilustración 20 Grupo de seguridad para la base de datos

El siguiente paso para configurar la base de datos, se debe de crear un grupo de subred para el servicio de Base de Datos de AWS (RDS). Esta subred permite determinar cuáles subredes pueden ser usadas por esta.

En la siguiente imagen se puede ver la configuración del grupo de subred para la base de datos. Acá se puede apreciar que está enlazada a la VPC que se creo anteriormente.



Ilustración 21 Grupo de subred para la base de datos

En la siguiente imagen se puede observar todas las Subnets que están asociadas al grupo de Subred de la base de datos.

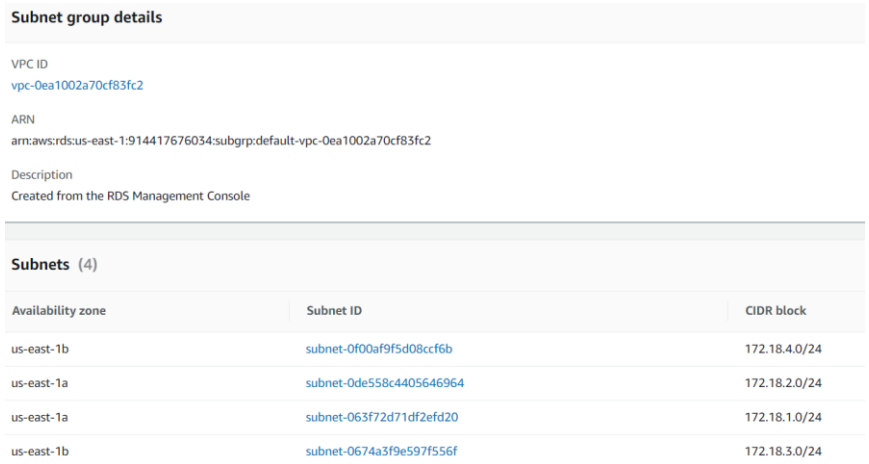


Ilustración 22 Subnets asociadas al grupo de Subnet de la base de datos

El siguiente paso es lanzar una instancia de base de datos MySql en un entorno de múltiples zonas de disponibilidad.

En la siguiente imagen se muestra la base de datos creada, en esta imagen se puede observar las Subnets a las que está asociada la base de datos, el grupo de seguridad de la base de datos y la VPC

exampleddb

Summary

DB identifier
exampleddb

CPU
2.30%

Status
Available

Class
db.t2.micro

Role
Instance

Current activity
0 Connections

Engine
MySQL Community

Region & AZ
us-east-1a

Connectivity & security

Monitoring

Logs & events

Configuration

Maintenance & backups

Tags

Connectivity & security

Endpoint & port

Endpoint
exampleddb.cyzkgsetos81.us-east-1.rds.amazonaws.com

Port
3306

Networking

Availability zone
us-east-1a

VPC
MyWebAPP-VPC (vpc-0ea1002a70cf83fc2)

Subnet group
default-vpc-0ea1002a70cf83fc2

Subnets
subnet-0674a3f9e597f556f
subnet-063f72d71df2efd20
subnet-0de558c4405646964
subnet-0f00af9f5d08ccf6b

Security

VPC security groups
SG-RDS-DB (sg-02ebbb0a1d5725db8) (active)
default (sg-09b6d4bd44ec596d6) (active)

Public accessibility
No

Certificate authority
rds-ca-2019

Certificate authority date
August 22, 2024 12:08

Ilustración 23 Base de datos en MySQL

Otra parte fundamental del proyecto es la gestión de los archivos compartidos, este sistema se denomina EFS. Este sistema permite compartir todos los archivos de la aplicación, de igual forma permite compartir los archivos estáticos que se manejan en un servidor CMS (Sistema de gestión de contenidos) tales como imágenes, PDFs, videos, entre otros.

En la siguiente imagen se puede apreciar el enlace que hay entre el EFS creado con las Subnets privadas de cada región.

Red

⌂

Administrar

⚙

Zona de disponibilidad	ID del destino de montaje	ID de la subred	Estado de destino de montaje	Dirección IP	ID de la interfaz de red	Grupos de seguridad
us-east-1a	fsmt-1c1bb0a9	subnet-063f72d71df2efd20	Disponible	172.18.1.124	eni-0e23cb1b680b7938d	sg-0e197ba8b1c8775f2 (SG-WEB)
us-east-1b	fsmt-121bb0a7	subnet-0674a3f9e597f556f	Disponible	172.18.3.29	eni-0f64bc10ce9f128e7	sg-0e197ba8b1c8775f2 (SG-WEB)

Ilustración 24 EFS

En la recta final del trabajo, se tiene que proceder con la creación de las instancias para el servidor web.

Es importante destacar que, al crear estas instancias, es necesario realizar una asociación con el File System creado anteriormente con el objetivo de que se tengan los archivos compartidos.

Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la...	Zona de dispon...	DNS de IPv4
Web Server	i-083641299d79faefe	En ejecución	t2.micro	2/2 comprobaci...	1 alarma	us-east-1a	-

Instancia: i-083641299d79faefe (Web Server)

Detalles

Seguridad

Redes

Almacenamiento

Comprobaciones de estado

Monitoreo

Etiquetas

▼ Detalles de redes

Información

Dirección IPv4 pública	Direcciones IPv4 privadas	ID de VPC
-	172.18.1.40	vpc-0ea1002a70cf83fc2 (MyWebAPP-VPC)
DNS de IPv4 pública	DNS IPv4 privado	ID de subred
-	ip-172-18-1-40.ec2.internal	subnet-063f72d71df2efd20 (Private Subnet A)
Direcciones IPv6	Direcciones IP IPv4 privadas secundarias	Zona de disponibilidad
-	-	us-east-1a
Direcciones IP del operador (efímeras)	ID de Outpost	

Ilustración 25 Instancia del webserver

Una vez se tenga la instancia creada, se procede a realizar la conexión SSH para poder instalar Docker, docker-compose y el archivo docker-compose.yml para el uso de Wordpress

Una parte fundamental para el desarrollo del proyecto es la escalabilidad y la estabilidad de la aplicación, para esto se hace uso del Auto Scaling el cual monitoriza sus aplicaciones y ajusta automáticamente la capacidad para mantener un desempeño predecible y estable al menor costo posible, en otras palabras, hace que cuando una instancia se cae, esta misma sea capaz de volver a funcionar correctamente.

Para configurar el Auto Scaling, en primer lugar, se debe crear una imagen AMI del servidor web. De esta forma se guardarán el contenido del boot disk y las nuevas instancias desplegadas a partir de esta se van a instanciar con un contenido idéntico. En otras palabras, las imágenes se convierten en plantillas que contiene una configuración básica la cual sirve para instanciar posteriormente máquinas.

Name	Nombre de AM	ID de AMI	Origen	Propietario	Visibilidad	Estado	Fecha de creación	PI
Web Server AMI	ami-0a5417facc54ff7a6	914417676034/...	914417676034	Privado	available	16 de mayo de 2021, 10:56:...	01	

Imagen: ami-0a5417facc54ff7a6

Detalles

Permisos Etiquetas

ID de AMI	ami-0a5417facc54ff7a6	Nombre de AMI	Web Server AMI
Propietario	914417676034	Origen	914417676034/Web Server AMI
Estado	available	Motivo del estado	-
Fecha de creación	16 de mayo de 2021, 10:56:33 UTC-5	Platform details	Linux/UNIX
Arquitectura	x86_64	Usage operation	RunInstances
Tipo de imagen	machine	Tipo de virtualización	hvm
Descripción	Lab AMI for Web Server	Nombre del dispositivo raíz	/dev/xvda
Tipo de dispositivo raíz	ebs	ID de disco de RAM	-
ID de kernel	-	Códigos de productos	-
Dispositivos de bloques	/dev/xvda=snap-09d221f3aee6f3923:8 true:gp2	Boot mode	-

Ilustración 26 Imagen AMI para el servicio de Auto Scaling

El siguiente paso es la creación de un balanceador de carga, el cual nos va a permitir distribuir las peticiones entrantes hacia múltiples instancias y en diferentes zonas de disponibilidad.

En la siguiente imagen se puede apreciar que las zonas de disponibilidad del balanceador de carga son las Subnets públicas de cada región. De igual forma se puede apreciar los grupos de seguridad dispuestos para el balanceador de carga.

Crear balanceador de carga

Acciones

Filtrar por etiquetas y atributos o buscar por palabra clave

Nombre	Nombre de DNS	Estado	ID de VPC	Zonas de disponibilidad	Tipo
ELB-MyWebApp	ELB-MyWebApp-141924157...	active	vpc-0ea1002a70cf83fc2	us-east-1a, us-east-1b	application

Esquema

Internet-facing

Tipo de dirección IP

Ipv4

[Editar el tipo de dirección IP](#)

VPC

[vpc-0ea1002a70cf83fc2](#)

Zonas de disponibilidad

[subnet-0de558c4405646964 - us-east-1a](#)

Dirección IPv4: Asignado por AWS

[subnet-0f00af9f5d08ccf6b - us-east-1b](#)

Dirección IPv4: Asignado por AWS

[Editar las subredes](#)

Zona hospedada

Z35SXDOTRQ7X7K

Hora de creación

16 de mayo de 2021, 10:44:45 UTC-5

Seguridad

Grupos de seguridad

[sg-0e197ba8b1c8775f2](#), **SG-WEB**

- Enable HTTP Acces

Ilustración 27 Balanceador de carga

El siguiente paso es crear el grupo de Auto Scaling, en la siguiente imagen se puede observar la configuración del grupo de Auto Scaling.

Un grupo de Auto Scaling comenzará iniciando tantas instancias como se especifique para la capacidad deseada. Si no hay políticas de escalado o acciones programadas asociadas al grupo Auto Scaling, el grupo de Auto Scaling mantiene la cantidad deseada de instancias y realiza comprobaciones periódicas de estado en las instancias del grupo. Las instancias que no son saludables se terminarán y se reemplazarán por otras nuevas.

Grupos de Auto Scaling: (1/1)								
<div> <div> <div>🔄</div> <div>Editar</div> <div>Eliminar</div> <div>Crear grupo de Auto Scaling</div> </div> <div> <div>🔍</div> <div>Buscar sus grupos de Auto Scaling</div> </div> <div> <div><</div> <div>1</div> <div>></div> <div>⚙️</div> </div> </div>								
<input checked="" type="checkbox"/>	Nombre	Plantilla de lanzamiento/config...	Instan...	Estado	Capacidad des...	M...	M...	Zonas
<input checked="" type="checkbox"/>	MyWebApp-Auto	MyWebbApp	2	-	2	2	3	us-east

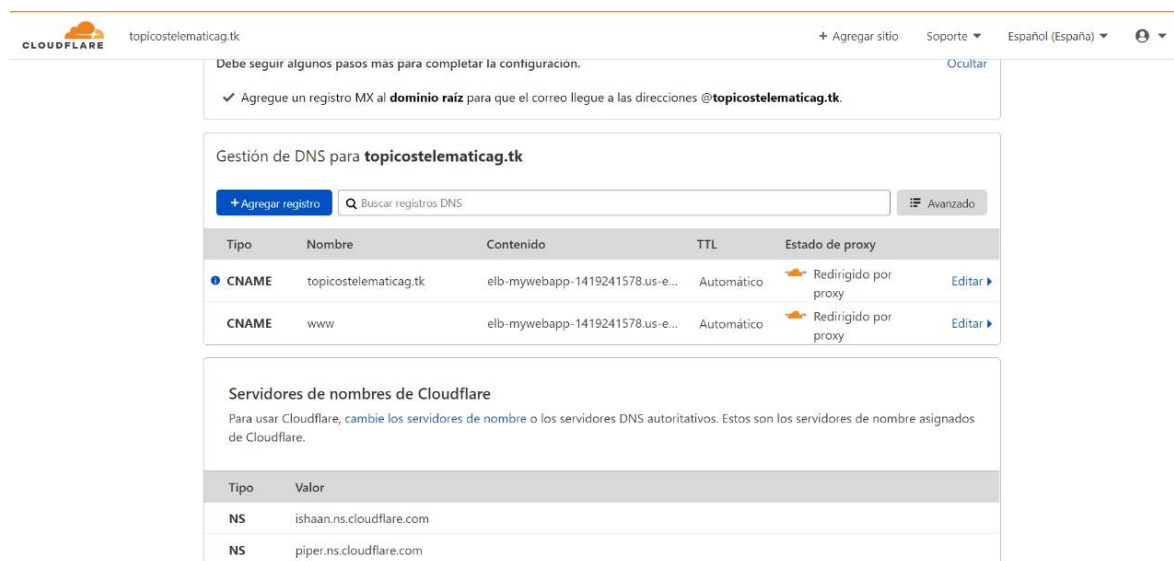
Capacidad deseada	2	Grupo de Auto Scaling
Capacidad mínima	2	MyWebApp-Auto Scaling Group
Capacidad máxima	3	Fecha de creación Sun May 16 2021 11:01:33 GMT-0500 (hora estándar de Colombia) Nombre de recurso de Amazon (ARN) arn:aws:autoscaling:us-east-1:914417676034:autoScalingGroup:c6243651-6abc-4bf5-97e3-0a923dc3be86:autoScalingGroupName/MyWebApp-Auto Scalino Group

Configuración de lanzamiento MyWebbApp	ID de AMI ami-0a5417facc54ff7a6	Grupos de seguridad sg-0e197ba8b1c8775f2 🔗
Tipo de instancia t2.micro	Nombre del par de claves ProyectoFinal	Hora de creación Sun May 16 2021 10:58:17 GMT-0500 (hora estándar de Colombia)
Almacenamiento (volúmenes) /dev/xvda		
Ver detalles en la consola de configuración de lanzamiento 🔗		
Zonas de disponibilidad us-east-1a, us-east-1b	ID de subred subnet-0de558c4405646964, subnet-0674a3f9e597f556f	
Balance de carga		
Grupos de destino del balanceador de carga TG-MyWebApp1 🔗	Balanceadores de carga clásicos -	

Ilustración 28 Grupo de Auto Scaling

El siguiente paso es obtener los certificados de seguridad, para esto se hace uso de CloudFlare. En primer lugar, se requiere delegar la gestión y el manejo del DNS y de los servidores web del proyecto a CloudFlare.

En la siguiente imagen se muestra cómo se realizó la delegación.



Debe seguir algunos pasos más para completar la configuración.

✓ Agregue un registro MX al **dominio raíz** para que el correo llegue a las direcciones @topicstelematicag.tk.

Gestión de DNS para **topicstelematicag.tk**

+ Agregar registro | Buscar registros DNS | Avanzado

Tipo	Nombre	Contenido	TTL	Estado de proxy	
CNAME	topicstelematicag.tk	elb-mywebapp-1419241578.us-e...	Automático	Redirigido por proxy	Editar
CNAME	www	elb-mywebapp-1419241578.us-e...	Automático	Redirigido por proxy	Editar

Servidores de nombres de Cloudflare

Para usar Cloudflare, cambie los servidores de nombre o los servidores DNS autoritativos. Estos son los servidores de nombre asignados de Cloudflare.

Tipo	Valor
NS	ishaan.ns.cloudflare.com
NS	pipeer.ns.cloudflare.com

Ilustración 29 Delegación del DNS a CloudFlare

El segundo paso es generar los certificados de seguridad por medio de CloudFlare para usuarios de tipo SSL/TSL.



Certificados de cliente

Proteja y autentique sus API y aplicaciones web con los certificados de cliente. Bloquee el tráfico de dispositivos que no tengan un certificado SSL/TLS de cliente válido con reglas mTLS.

Servidores

Elija qué servidor(es) desea habilitar mTLS

Ninguno [Editar](#)

[Crear certificado](#)

[Crear una regla mTLS](#)

Asunto del certificado	Autoridad	Expira el	Estado	
> CN=Cloudflare, C=US	CA administrado de Cloudflare para jcguerrera@eafit.edu.co	16 de may. de 2031	Activo	Revocar

Ilustración 30 Generación de certificados de seguridad

Seguido de esto, se le agrega el certificado SSL/TLS al balanceador de carga con el objetivo de que por el puerto 443 reciba las peticiones por medio del protocolo HTTPS (protocolo seguro).

En la siguiente imagen se muestra la configuración dada al balanceador de carga.

Load balancer: **ELB-MyWebApp**

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](#)

<input type="checkbox"/>	Listener ID	Security policy	SSL Certificate	Rules
<input type="checkbox"/>	HTTP : 80 am...57dd5134109efa10 ▾	N/A	N/A	Default: forwarding to TG-MyWebApp1 View/edit rules
<input type="checkbox"/>	HTTPS : 443 am...fd173a24d876095b ▾	ELBSecurityPolicy-2016-08	Default: Proyecto_2 (IAM) View/edit certificates	Default: forwarding to TG-MyWebApp1 View/edit rules

Ilustración 31 Configuración del balanceador de carga con el certificado de seguridad

Nota: Se implementó el inicio de sesión con Google y se intentó hacer el inicio de sesión autenticación de 2 factores porque hubo un problema entre este plugin y el de Google

Projecto 2 Telemática Plugins • Proyecto 2 Telemática Locked out for Login to the Workbench Laboratorio-ELB-AutoScaling Workbench

topicstelematicag.tk/wp-admin/plugins.php

Projecto 2 Telemática Añadir Forum Dashboard Hola, admin

Escritorio Entradas Medios Páginas Foros Comentarios Apariencia **Plugins** Plugins instalados Añadir nuevo Editor de Plugin Usuarios Herramientas Ajustes 4 Cerrar menú

<input type="checkbox"/>	Plugin	Descripción	Actualizaciones automáticas
<input type="checkbox"/>	Akismet Anti-Spam Ajustes Desactivar	Utilizado por millones de personas, Akismet es posiblemente la mejor manera de proteger tu blog del spam . Mientras duermes, mantiene el sitio protegido. Para comenzar, sólo ve a tu página de configuración de Akismet y configura tu clave de API. Versión 4.1.9 Por Automattic Ver detalles	Activar las actualizaciones automáticas
<input type="checkbox"/>	Google Apps Login Settings Desactivar	Simple secure login for Wordpress through users' Google Apps accounts (uses secure OAuth2, and MFA if enabled) Versión 3.4.4 Por Lever Technology LLC Ver detalles	Activar las actualizaciones automáticas
<input type="checkbox"/>	Hello Dolly Desactivar	Esto no es solo un plugin, simboliza la esperanza y entusiasmo de toda una generación resumidas en las dos palabras más famosas cantadas por Louis Armstrong: Hello, Dolly. Cuando lo actives verás frases al azar de Hello, Dolly en la parte superior derecha de cada página de tu pantalla de administración. Versión 1.7.2 Por Matt Mullenweg Ver detalles	Activar las actualizaciones automáticas
<input type="checkbox"/>	Really Simple SSL Actualizar a premium Soporte Ajustes Desactivar	Plugin ligero sin configuraciones que hace que tu sitio cargue con SSL Versión 4.0.15 Por Really Simple Plugins Ver detalles	Activar las actualizaciones automáticas
Wordfence Login Security se borró con éxito.			
Wordfence Security se borró con éxito.			
<input type="checkbox"/>	wpForo Settings Desactivar Uninstall	WordPress Forum plugin, wpForo is a full-fledged forum solution for your community. Comes with multiple modern forum layouts. Versión 1.9.6 Por gVectors Team Ver detalles	Activar las actualizaciones automáticas
<input type="checkbox"/>	Plugin	Descripción	Actualizaciones automáticas

Acciones en lote [Aplicar](#)

7 elementos

Ilustración 32 Plugin de autenticación por 2 factores