

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.

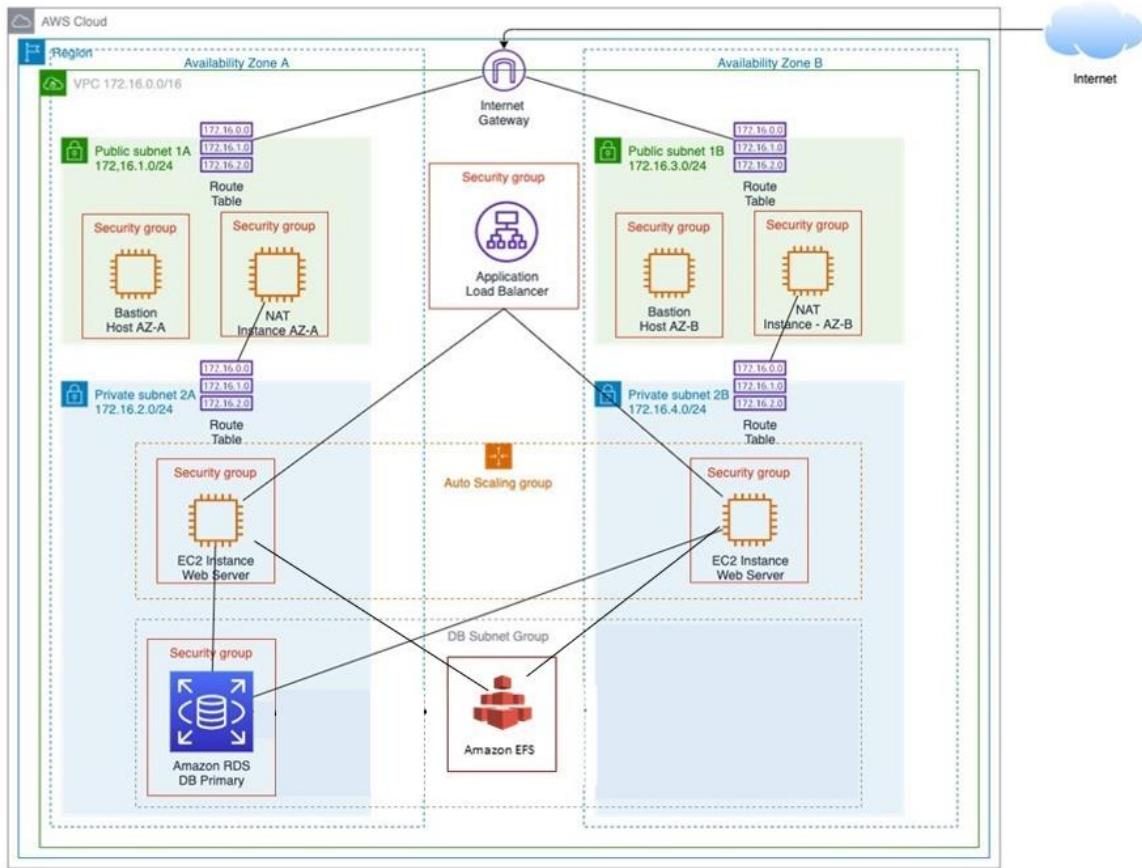


Ilustración 1 Despliegue de la aplicación Web Multi Availability Zone

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						
Actions Create VPC						
<input type="text"/> Filter VPCs						
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

	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					
Subnets (10) Info					
	Name	Subnet ID	State	VPC	IPv4 CIDR
<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

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.

	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 Security Groups console. At the top, there is a header with 'Security Groups (1/7) Info' and buttons for 'Actions' and 'Create security group'. Below the header is a search bar with the placeholder 'Filter security groups'. The main table lists one security group:

Name	Security group ID	Security group name	VPC ID	Description
SG-NAT	sg-04c6891441da1b476	SG-NAT-Instance	vpc-0ea1002a70cf83fc2	Enable outgoing traffic...

Below the table, a section titled 'Inbound rules (8)' is shown. It contains a table with columns: Type, Protocol, Port range, Source, and Description - optional. The rules listed are:

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 AWS Instances console. It displays two instances: 'NAT-Instance A' (selected) and 'BASTION HOS...'. The instance details are as follows:

<input checked="" type="checkbox"/> NAT-Instance A	i-07673711e327b08c3	En ejecución	t2.micro	2/2 comprobador	1 alarma	us-east-1a	-
<input type="checkbox"/> BASTION HOS...	i-03c3261ae71af4ea5	En ejecución	t2.micro	2/2 comprobador	1 alarma	us-east-1a	-

Below the table, a section titled 'Instancia: i-07673711e327b08c3 (NAT-Instance A)' is shown. It has tabs for 'Detalles', 'Seguridad', 'Redes' (selected), 'Almacenamiento', 'Comprobaciones de estado', 'Monitoreo', and 'Etiquetas'. Under the 'Redes' tab, it shows network details:

- Dirección IPv4 pública: 3.82.198.124 | [dirección abierta](#)
- Direcciones IPv4 privadas: 172.18.2.117
- DNS de 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

The screenshot shows the AWS CloudWatch Metrics interface for a NAT instance. The top navigation bar includes the instance ID (i-006570f69381dfe4b), status (En ejecución), instance type (t2.micro), metrics (2/2 comprobador, 1 alarma), and region (us-east-1b). Below the navigation bar, the main content area is titled "Instancia: i-006570f69381dfe4b (NAT-Instance B)". The "Redes" tab is active. The "Detalles" section shows the public IP (34.235.167.222) and DNS (ip-172-18-4-129.ec2.internal). The "Redes" section shows the private IP (172.18.4.129) and private DNS (ip-172-18-4-129.ec2.internal). A green oval highlights the "ID de VPC" field, which contains "vpc-0ea1002a70cf83fc2 (MyWebAPP-VPC)", and the "ID de subred" field, which contains "subnet-0f00af9f5d08ccf6b (Public Subnet 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	Actions	Create route table
	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 pública, 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:

Public Route Table A rtb-0faa3456ea3f0f0dd subnet-0de558c440564...

Explicit subnet associations (1)

Subnet ID	IPv4 CIDR
subnet-0de558c440564 / Public Subnet A	172.18.2.0/24

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

rtb-0faa3456ea3f0f0dd / Public Route Table A

Routes (2)

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

Internet gateway associations

Name	Internet gateway ID	State	VPC ID
MyWebVPC-IGW	igw-0389e8c70ff18d520	Attached	vpc-0ea1002a70cf83fc2 MyWebAPP-

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

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

Private Route Table A rtb-0022e49f88b2ba884 subnet-063f72d7

Explicit subnet associations (1)

Subnet ID	IPv4 CIDR
subnet-063f72d71df2efd20 / Private Subnet A	172.18.1.0/24

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

The screenshot shows the AWS Route Tables interface. At the top, a table lists route tables, with 'Private Route Table A' selected. Below it, the 'Routes (2)' section shows two routes: one to 'local' via '172.18.0.0/16' and another to a target 'eni-0939e8e6ff5c7d6fd' via '0.0.0/0'. The target is highlighted with a green oval. At the bottom, a table lists interfaces, with 'NAT-Instance A' selected. This interface is also highlighted with a green oval. The 'Name' column header and the row for 'NAT-Instance A' are also circled in green.

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

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

The screenshot shows the AWS Route Tables interface. It lists route tables, with 'Public Route Table B' selected. Below it, the details for 'rtb-06e31def7d253d9db / Public Route Table B' are shown. The 'Subnet associations' tab is active, displaying one explicit subnet association: 'subnet-0f00af9f5d08ccfb' with '172.18.4.0/24'.

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

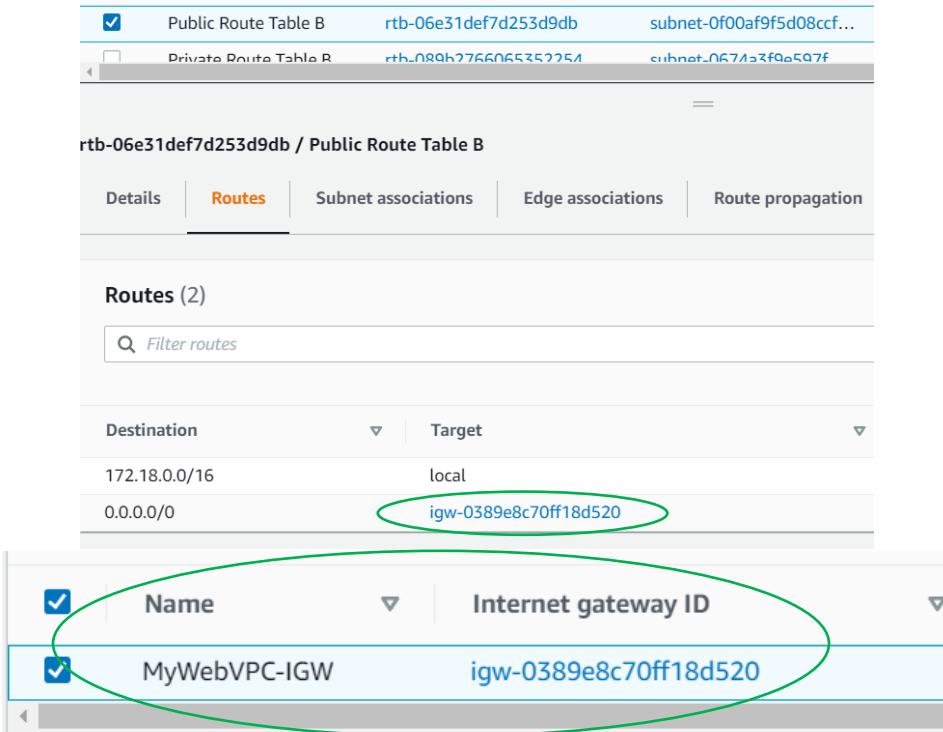


Ilustración 14 Al ser una Subnet pública, se asocia al Internet Gateway

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

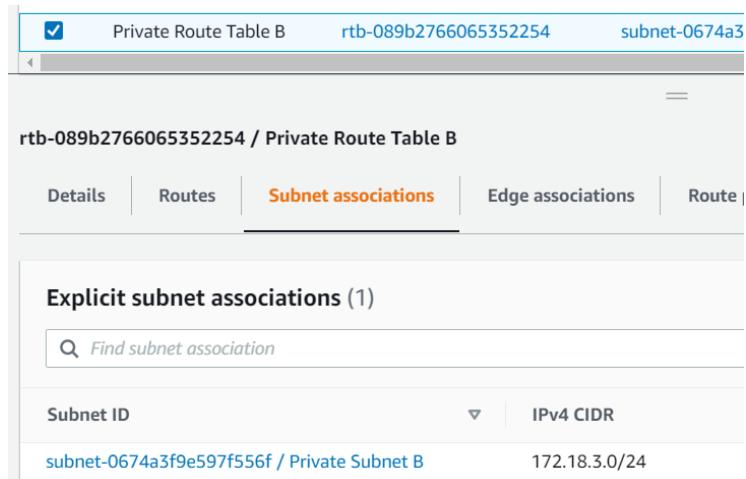


Ilustración 15 Asociación de la tabla de rutas a la Subnet correspondiente

The screenshot shows the AWS Route Table configuration for 'Private Route Table B'. The 'Routes' tab is active, showing two entries:

Destination	Target
172.18.0.0/16	local
0.0.0.0/0	eni-096850b81179af7a0

Below the routes, a table lists NAT instances:

Name	ID de la interfaz de red	ID de subred	ID de VPC
NAT-Instance B	eni-096850b81179af7a0	subnet-0f00af9f5d08ccf6b	vpc-0ea1002a70cf83fc2

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

The screenshot shows the AWS Security Groups configuration for 'SG-BASTION'. The 'Inbound rules' tab is active, displaying two entries:

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	0.0.0.0/0	Allow ssh traffic
SSH	TCP	22	::/0	Allow ssh traffic

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

Instancias (1/8) Información

Estado de la instancia: running X Quitar los filtros

Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la...	Zona de dispon...	DNS
BASTION HOS...	i-03c3261ae71af4ea5	En ejecución	t2.micro	2/2 comprobador	1 alarme	us-east-1a	-

Instancia: i-03c3261ae71af4ea5 (BASTION HOST A)

Detalles Seguridad Redes Almacenamiento Comprobaciones de estado Monitoreo Etiquetas

▼ Detalles de redes Información

Dirección IPv4 pública	Direcciones IPv4 privadas	ID de VPC
3.86.252.61 dirección abierta	172.18.2.205	vpc-0ea1002a70cf83fc2 (MyWebAPP-VPC)
DNS de IPv4 pública	DNS IPv4 privado	ID de subred
-	ip-172-18-2-205.ec2.internal	subnet-0de558c4405646964 (Public Subnet A)

Instancias (1/8) Información

Estado de la instancia: running X Quitar los filtros

Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comproba...
BASTION HOS...	i-03c3261ae71af4ea5	En ejecución	t2.micro	2/2 con...

▼ Detalles de seguridad

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

Filtrar instancias Estado de la instancia: running X 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-0f00af9f5d08ccff6b (Public Subnet B)

Instancia: i-097ac0016bd0d06ce (BASTION HOST B)

Detalles Seguridad Redes Almacenamiento Comprobaciones de estado Monitoreo Etiquetas

▼ 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.

The screenshot shows the AWS RDS Security Groups interface. A single security group, SG-RDS-DB, is listed. It is associated with a VPC ID (vpc-0ea1002a70cf83fc2) and has a description "permit Access from web...". One inbound rule is present, allowing MySQL/Aurora traffic on port 3306 from the SG-WEB subnet group.

Type	Protocol	Port range	Source	Description - optional
MySQL/Aurora	TCP	3306	sg-0e197ba8b1c8775f2 / SG-WEB	ALLOW DB CONNECTION

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 creó anteriormente.

The screenshot shows the AWS RDS Subnet Groups interface. A single subnet group, default-vpc-0ea1002a70cf83fc2, is listed. It is in a 'Complete' status and is associated with the VPC vpc-0ea1002a70cf83fc2.

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.

The screenshot shows the AWS RDS Subnet Group details page for the default-vpc-0ea1002a70cf83fc2 group. It displays the VPC ID (vpc-0ea1002a70cf83fc2), ARN (arn:aws:rds:us-east-1:914417676034:subgrp:default-vpc-0ea1002a70cf83fc2), and a description "Created from the RDS Management Console". The page also lists the four subnets associated with the group, categorized by availability zone: us-east-1b, us-east-1a, us-east-1a, and us-east-1b. Each subnet is assigned a specific Subnet ID and CIDR block.

Availability zone	Subnet ID	CIDR block
us-east-1b	subnet-0f00af9f5d08ccf6b	172.18.4.0/24
us-east-1a	subnet-0de558c4405646964	172.18.2.0/24
us-east-1a	subnet-063f72d71df2efd20	172.18.1.0/24
us-east-1b	subnet-0674a3f9e597f556f	172.18.3.0/24

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

Endpoint & port	Networking	Security
Endpoint exampledb.cykgsetos81.us-east-1.rds.amazonaws.com Port 3306	Availability zone us-east-1a VPC MyWebAPP-VPC (vpc-0ea1002a70cf83fc2) Subnet group default-vpc-0ea1002a70cf83fc2 Subnets subnet-0674a3f9e597f56f subnet-063f72d71df2ef20 subnet-0de558c4405646964 subnet-0ff0af9f5d08ccf6b	VPC security groups SG-RDS-DB (sg-02ebbb0a1d5725db8) (active) default (sg-09b6dd4bd44ec596d6) (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.

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-063f72d71df2ef20	Disponible	172.18.1.124	eni-0e23cb1b680b7938d	sg-0e197ba8b1c8775f2 (SG-WEB)
us-east-1b	fsmt-121bb0a7	subnet-0674a3f9e597f56f	Disponible	172.18.3.29	eni-0f64bc10ce9f128e7	sg-0e197ba8b1c8775f2 (SG-WEB)

Ilustración 24 EFS

En la recta final del trabajo, se tiene procede 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.

The screenshot shows the AWS CloudFormation console with a single stack named "Web Server". The stack contains one resource, "Web Server" (AWS::Serverless::Function), which is currently running. The configuration includes:

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

Below the main table, a detailed view for the "Web Server" resource is shown under the "Instancia: i-083641299d79faefe (Web Server)" section. The "Redes" tab is selected, showing the following network details:

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

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 AMI	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:...	Ot

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-09d2213aee6f3923:8: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			
<input type="text"/> Filtrar por etiquetas y atributos o buscar por palabra clave					
<input checked="" type="checkbox"/> Nombre <input type="text"/> Nombre de DNS <input type="checkbox"/> Estado <input type="text"/> ID de VPC <input type="checkbox"/> Zonas de disponibilidad <input type="checkbox"/> Tipo					
<input checked="" type="checkbox"/>	ELB-MyWebApp	ELB-MyWebApp-141924157...	active		
vpc-0ea1002a70cf83fc2	vpc-0ea1002a70cf83fc2	us-east-1a, us-east-1b	application		
Esquema	Internet-facing				
Tipo de dirección IP	ipv4	<input type="button" value="Editar el tipo de dirección IP"/>			
VPC	vpc-0ea1002a70cf83fc2				
Zonas de disponibilidad	subnet-0de558c4405646964 - us-east-1a	Dirección IPv4: Asignado por AWS			
	subnet-000af9f5d08ccf6b - us-east-1b	Dirección IPv4: Asignado por AWS			
		<input type="button" value="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.

The screenshot shows the AWS Auto Scaling Groups console. At the top, there is a search bar labeled "Buscar sus grupos de Auto Scaling" and buttons for "Editar" (Edit) and "Eliminar" (Delete). A prominent orange button on the right says "Crear grupo de Auto Scaling" (Create Auto Scaling Group). Below the header, a table lists one group: "MyWebApp-Auto" with a capacity of 2 instances. The table includes columns for Nombre, Plantilla de lanzamiento/config., Instancia, Estado, Capacidad deseada, Mínima, Máxima, and Zonas.

Nombre	Plantilla de lanzamiento/config.	Instancia	Estado	Capacidad deseada	Mínima	Máxima	Zonas
MyWebApp-Auto	MyWebApp	2	-	2	2	3	us-east-1

Below the table, detailed information is provided for the group:

Capacidad deseada 2	Grupo de Auto Scaling MyWebApp-Auto Scaling Group
Capacidad mínima 2	Fecha de creación Sun May 16 2021 11:01:33 GMT-0500 (hora estándar de Colombia)
Capacidad máxima 3	Nombre de recurso de Amazon (ARN) arn:aws:autoscaling:us-east-1:914417676034:autoScalingGroup:c6243651-6abc-4bfs-97e3-0a923dc3be06:autoScalingGroupName/MyWebApp-Auto Scaling Group

On the left side, there are sections for "Configuración de lanzamiento" (MyWebApp), "Tipo de instancia" (t2.micro), and "Almacenamiento (volúmenes)" (/dev/xvda). There is also a link "Ver detalles en la consola de configuración de lanzamiento" (View details in the launch configuration console).

On the right side, there are sections for "ID de AMI" (ami-0a5417facc54ff7a6), "Nombre del par de claves" (ProyectoFinal), "Grupos de seguridad" (sg-0e197ba8b1c8775f2), "Hora de creación" (Sun May 16 2021 10:58:17 GMT-0500), and "ID de subred" (subnet-0de558c4405646964, subnet-0674a3f9e597f556f).

Balance de carga

Groups of destination of the load balancer

TG-MyWebApp1

Load balancers of the classic type

-

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.

The screenshot shows the Cloudflare dashboard for the domain `topicostelematicag.tk`. At the top, there's a message: "Debe seguir algunos pasos más para completar la configuración." Below it, a note says: "✓ Agregue un registro MX al dominio raíz para que el correo llegue a las direcciones @`topicostelematicag.tk`". The main section is titled "Gestión de DNS para `topicostelematicag.tk`". It lists two CNAME records:

Tipo	Nombre	Contenido	TTL	Estado de proxy	Opciones
CNAME	<code>topicostelematicag.tk</code>	<code>elb-mywebapp-1419241578.us-e...</code>	Automático	Redirigido por proxy	Editar
CNAME	<code>www</code>	<code>elb-mywebapp-1419241578.us-e...</code>	Automático	Redirigido por proxy	Editar

Below the DNS section is a "Servidores de nombres de Cloudflare" section. It contains a table with two NS records:

Tipo	Valor
NS	<code>ishaan.ns.cloudflare.com</code>
NS	<code>piper.ns.cloudflare.com</code>

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.

The screenshot shows the Cloudflare interface for generating certificates. On the left, under "Certificados de cliente", it says: "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." Below this, under "Servidores", it says: "Elija qué servidor(es) desea habilitar mTLS". A dropdown menu shows "Ninguno" and an "Editar" link. To the right, there are two blue buttons: "Crear certificado" and "Crear una regla MTLS". The main table lists existing certificates:

Asunto del certificado	Autoridad	Expira el	Estado	Opciones
<code>CN=Cloudflare, C=US</code>	CA administrado de Cloudflare para <code>jguerrera@eafit.edu.co</code>	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.

Listener ID	Security policy	SSL Certificate	Rules
HTTP : 80 arn:...57dd5134109efa10~	N/A	N/A	Default: forwarding to TG-MyWebApp1 View/edit rules
HTTPS : 443 arn:...fd173a24d876095b~	ELBSecurityPolicy-2016-08	Default: Projeto_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 intento hacer el inicio de sesión autenticación de 2 factores porque hubo un problema entre este plugin y el de Google

Plugin	Descripción	Actualizaciones automáticas
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
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
Hello Dolly Desactivar	Este 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 Mullerweg Ver detalles	Activar las actualizaciones automáticas
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
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

Ilustración 32 Plugin de autenticación por 2 factores