DOCUMENTACIÓN TÉCNICA – PROYECTO 2

JUAN CAMILO GUERRERO ALARCÓN

DANIEL GARCÍA GARCÍA

CÉSAR ANDRÉS GARCÍA POSADA

TÓPICOS ESPECIALES EN TELEMÁTICA

UNIVERSIDAD EAFIT

MEDELLÍN

2021-1

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.

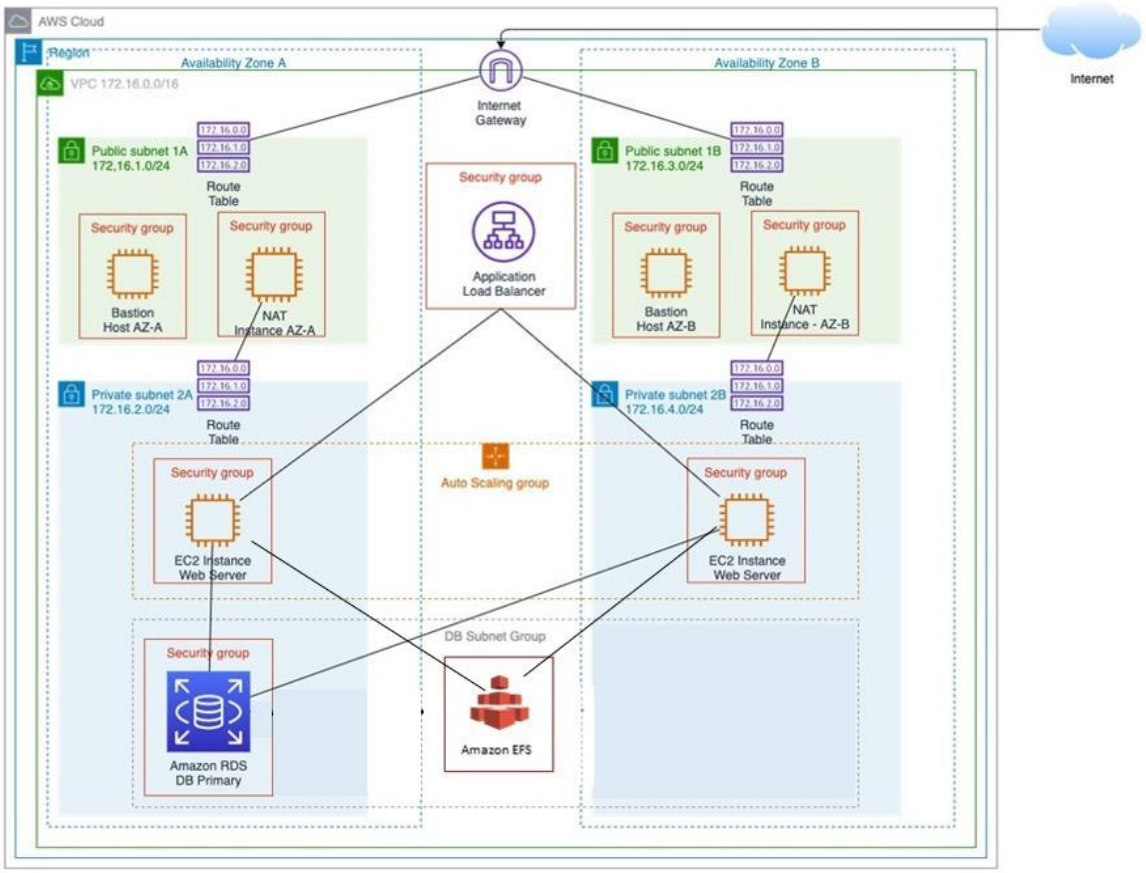


Ilustración 1 Despliegue de la aplicación Web Multi Availability Zone

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

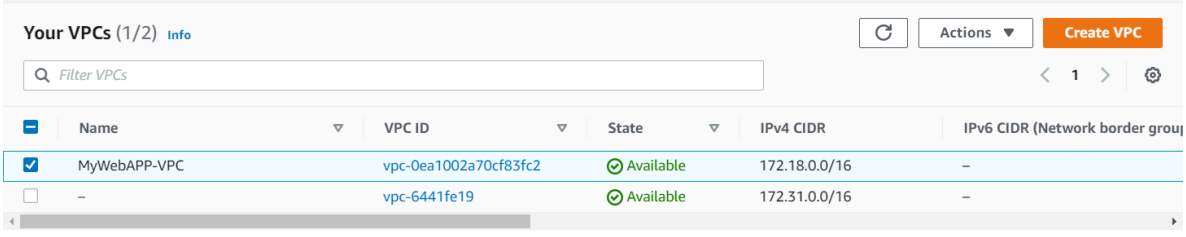


Ilustración 2 VPC para el proyecto con IP 172.18.0.0/16

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 publica 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

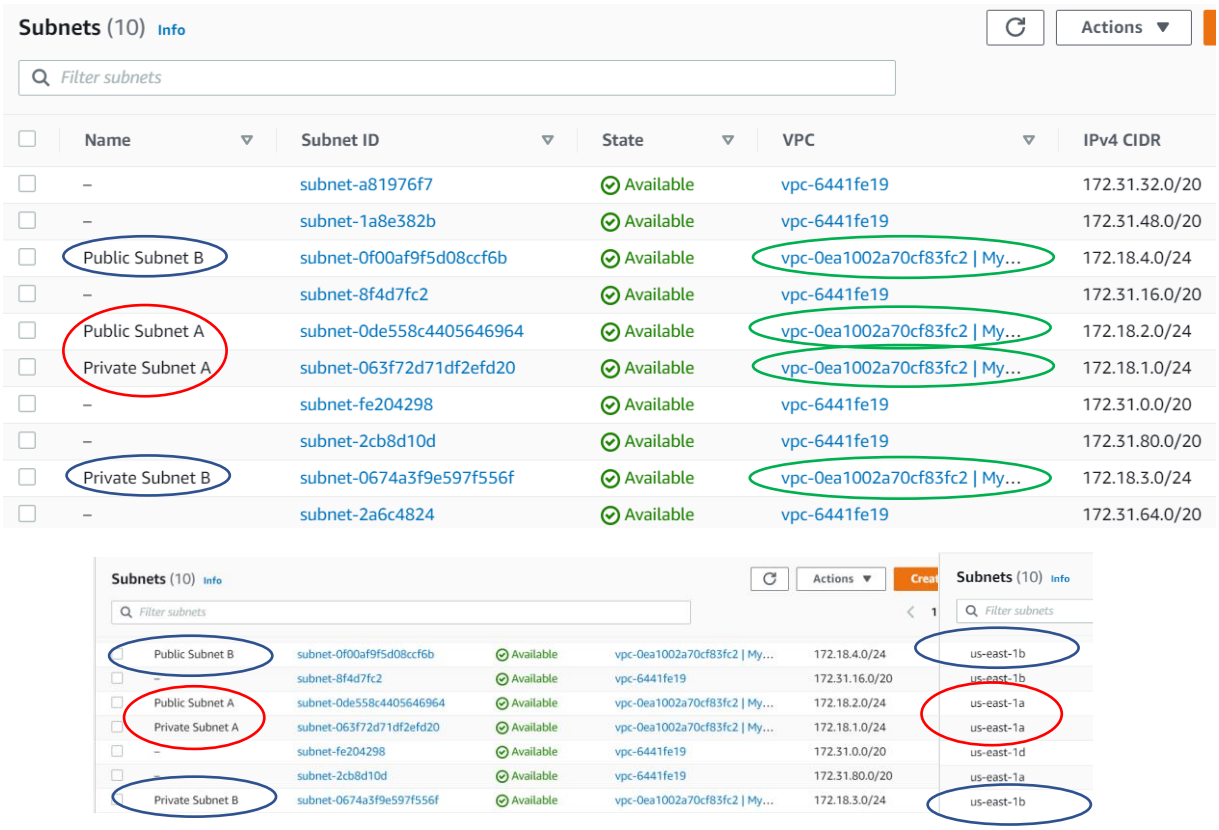


Ilustración 3 Conjunto de Subnets del proyecto

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.

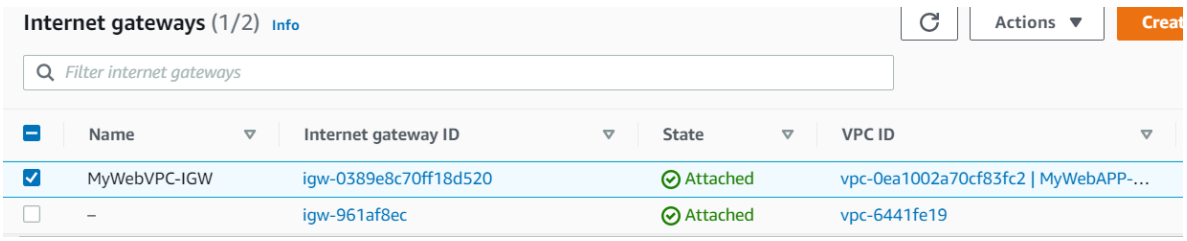


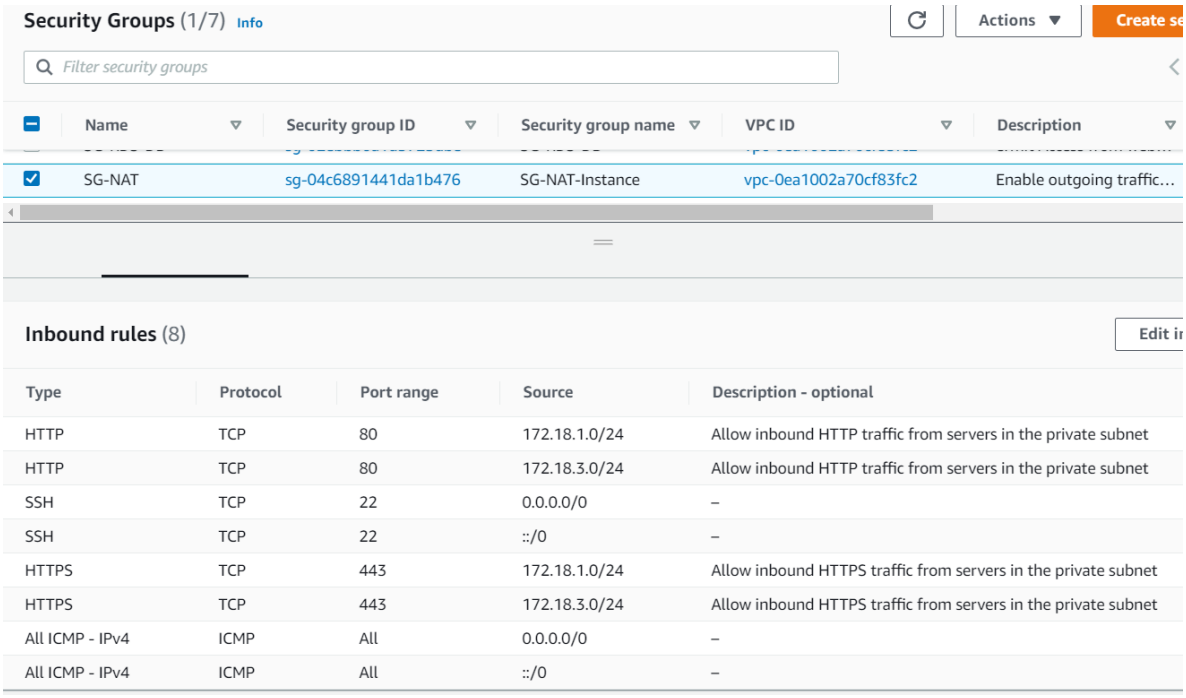
Ilustración 4 Internet Gateway

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.



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.

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

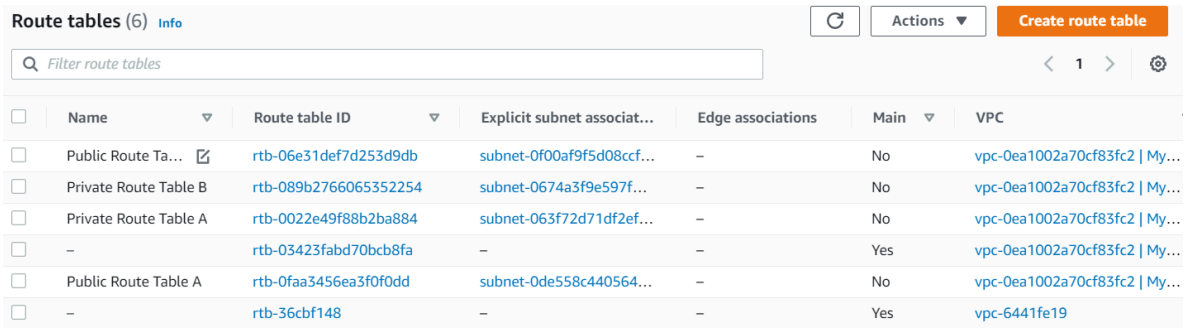


Ilustración 8 Tablas de rutas

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

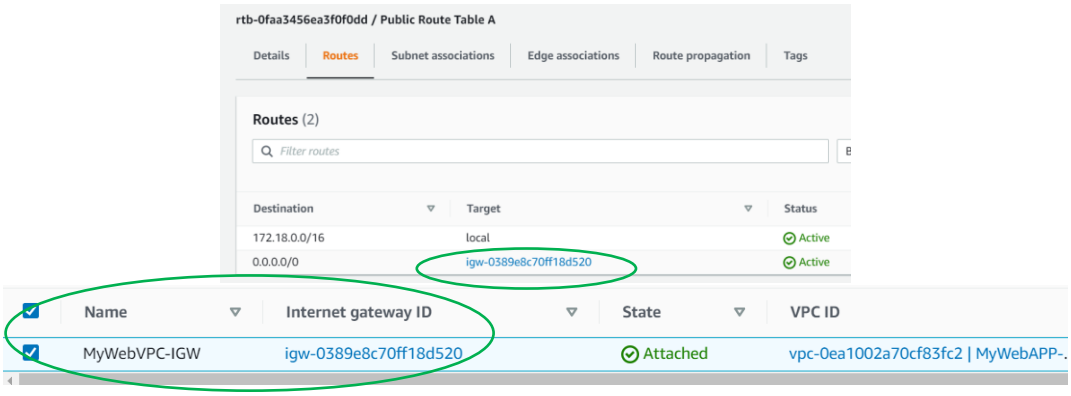


Ilustración 10 Al ser una Subnet pública, se asocia al Internet Gateway

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

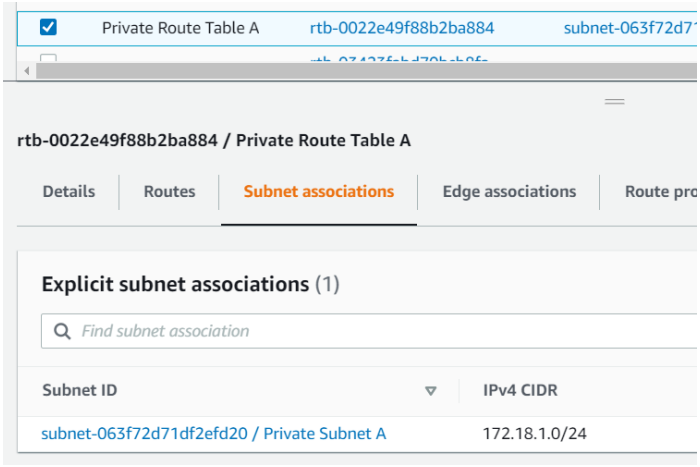


Ilustración 11 Asociación de la tabla de rutas a la Subnet correspondiente

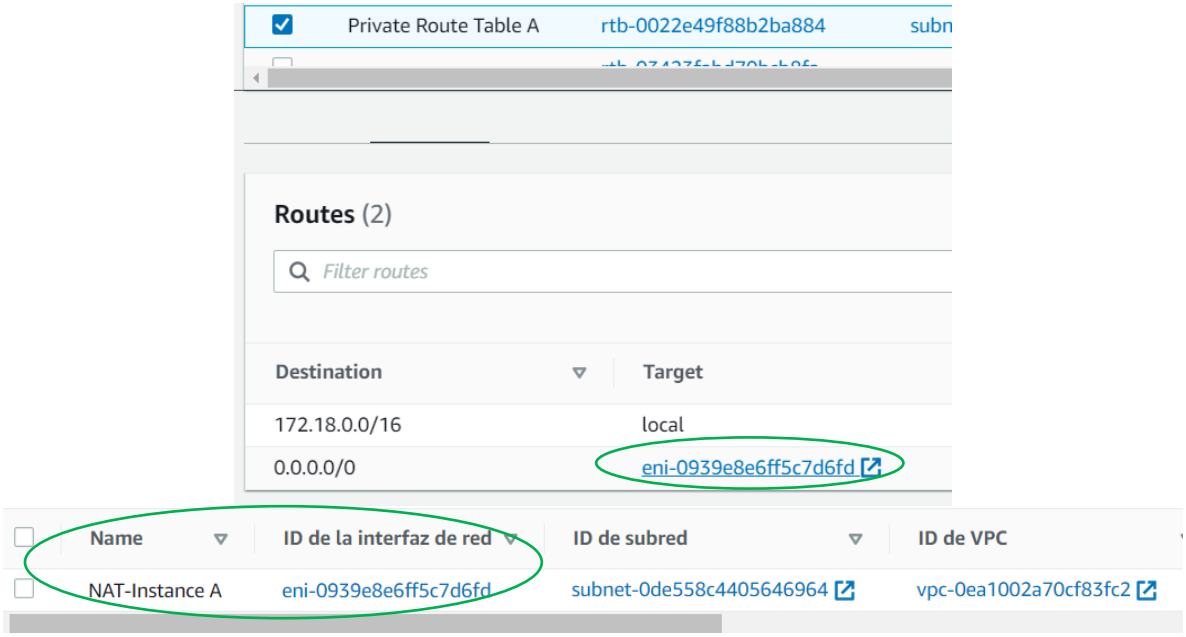


Ilustración 12 Al ser una Subnet privada, se asocia al NAT correspondiente

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

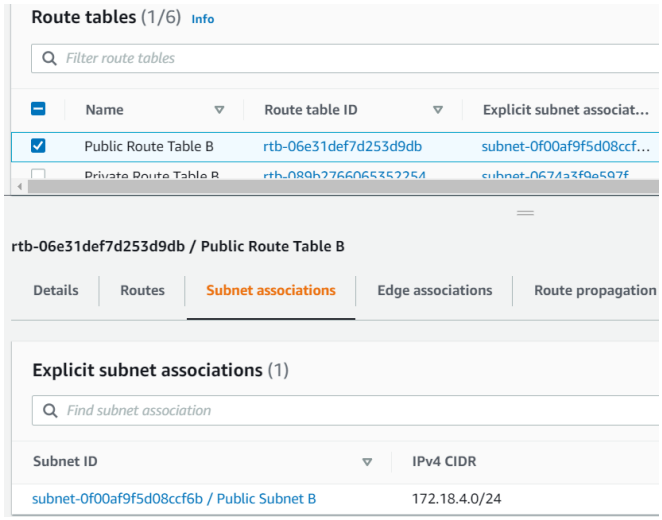


Ilustración 13 Asociación de la tabla de rutas a la Subnet correspondiente

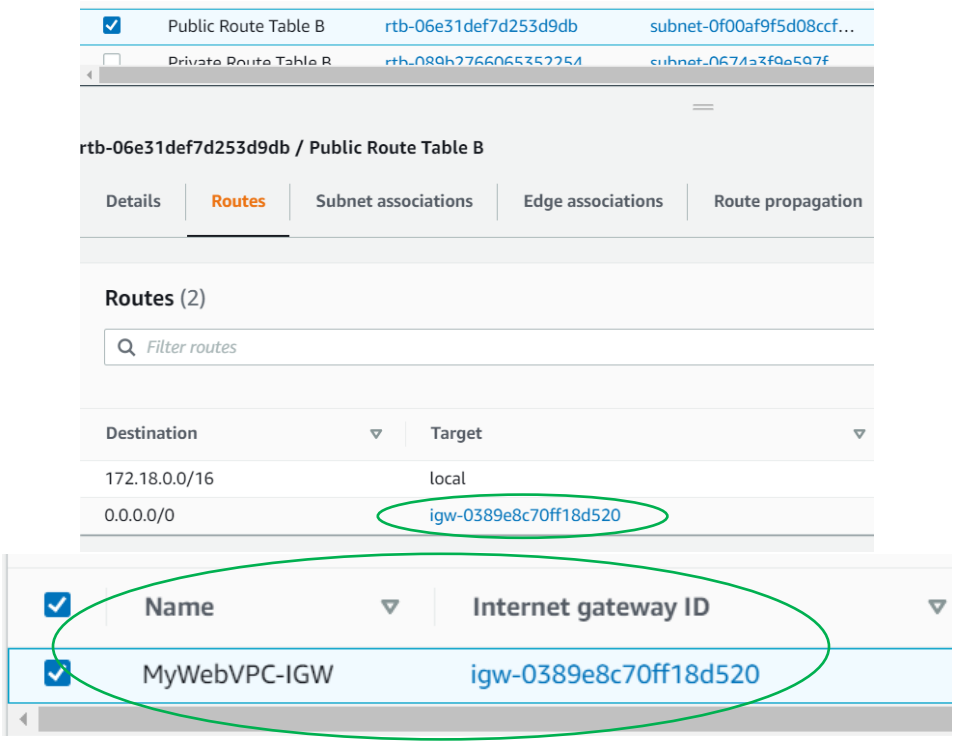


Ilustración 14 Al ser una Subnet pública, se asocia al Internet Gateway

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

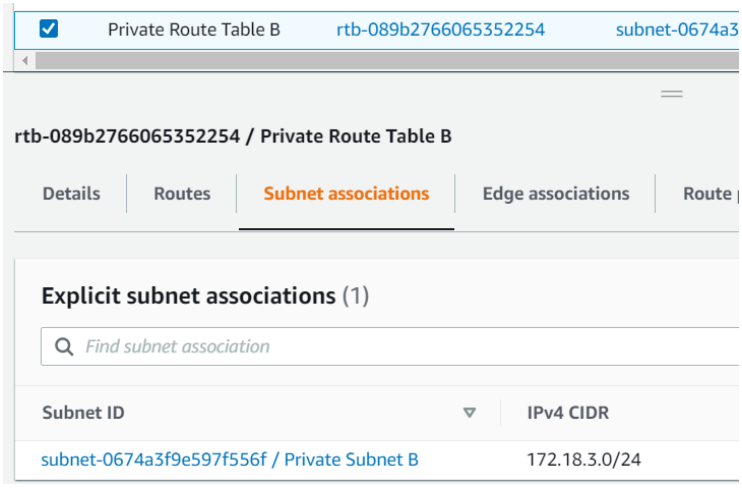


Ilustración 15 Asociación de la tabla de rutas a la Subnet correspondiente

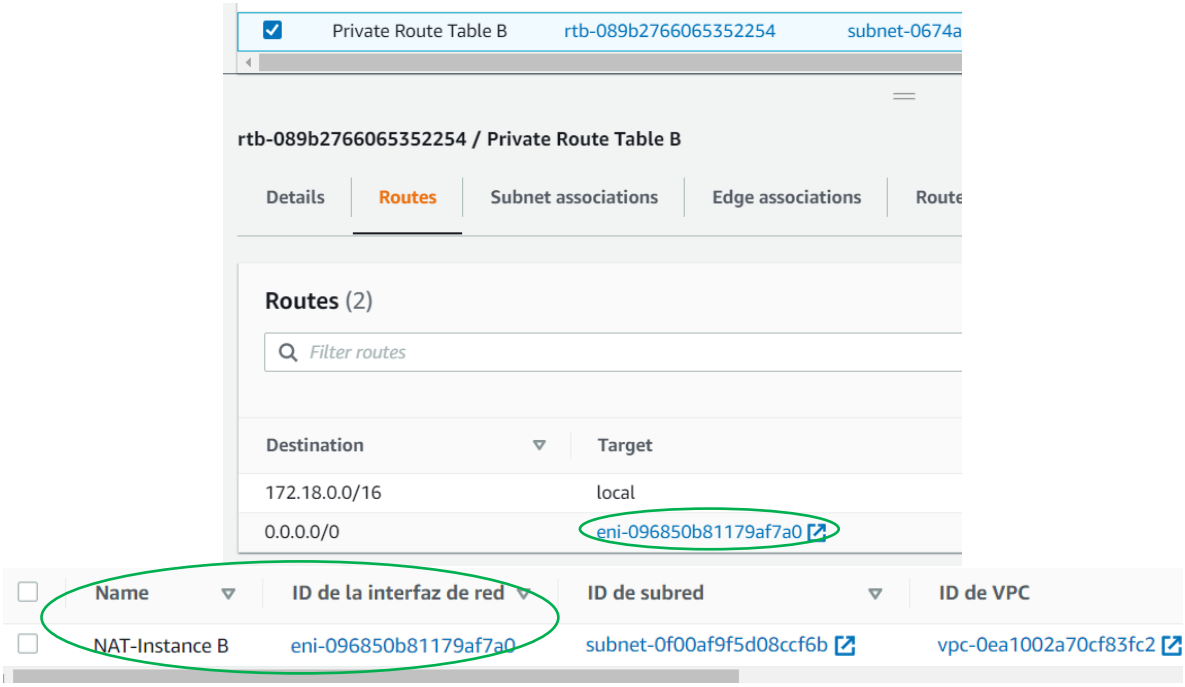


Ilustración 16 Al ser una Subnet privada, se asocia al NAT correspondiente

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

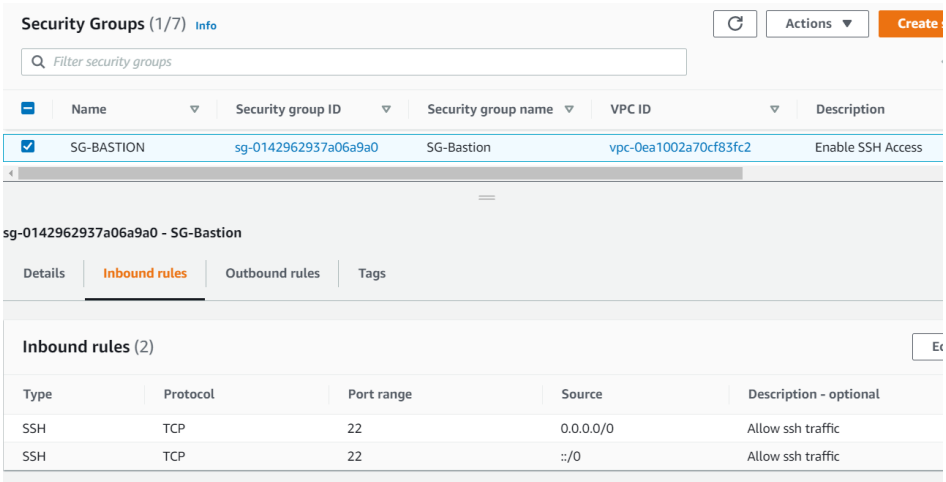


Ilustración 17 Grupo de seguridad del Bastion Host

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

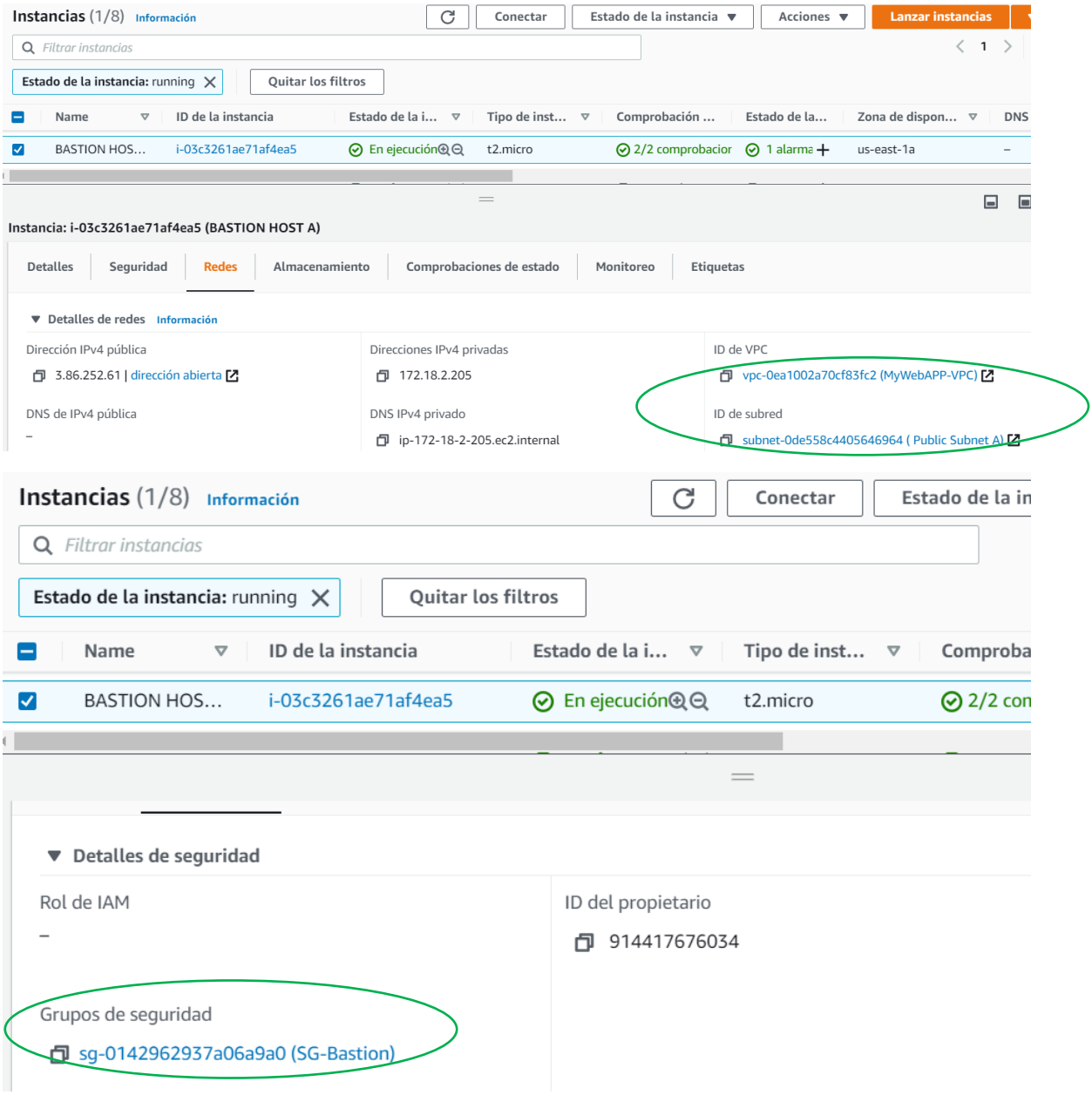


Ilustración 18 Configuración instancia Bastion Host Región A

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).

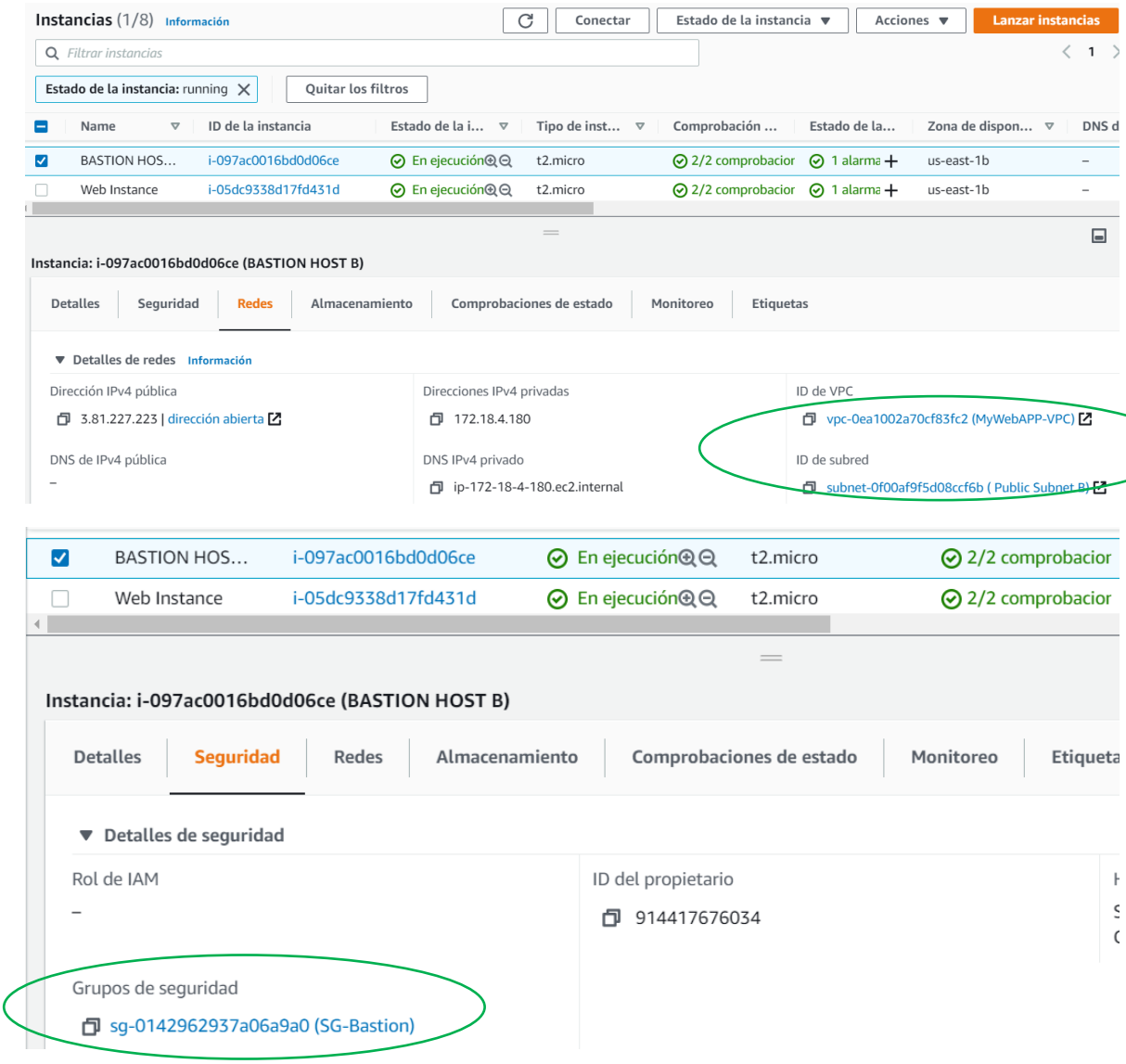


Ilustración 19 Configuración instancia Bastion Host Región B

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.

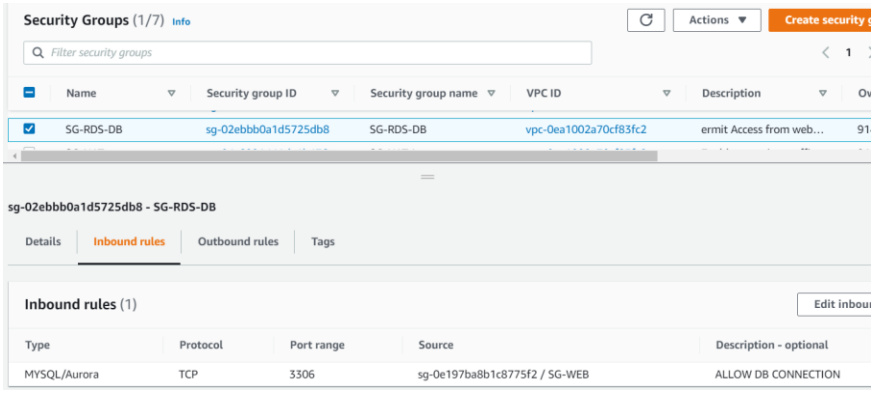


Ilustración 20 Grupo de seguridad para la base de datos

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.

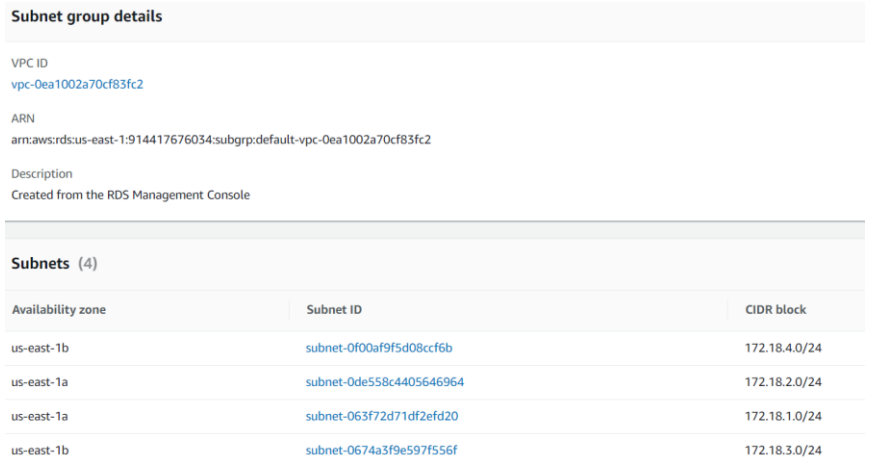


Ilustración 22 Subnets asociadas al grupo de Subnet de la base de datos

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

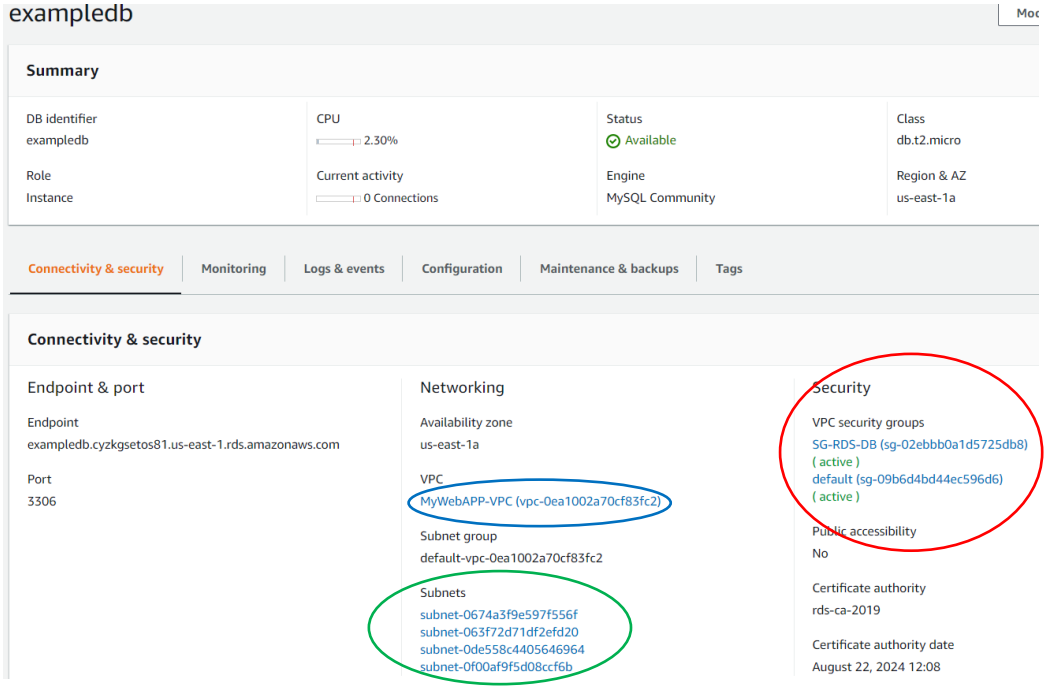
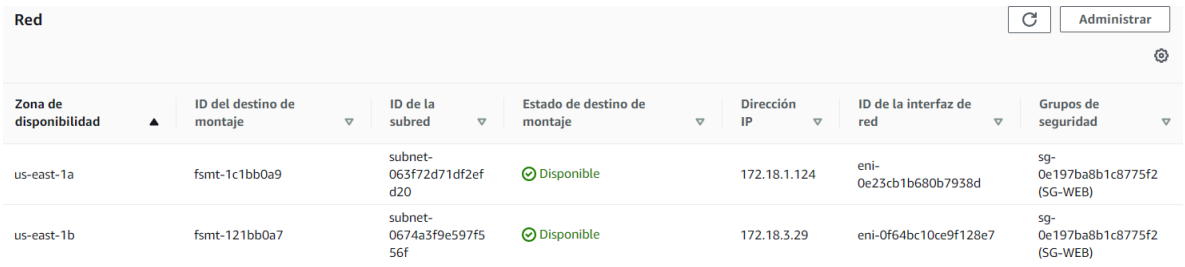


Ilustración 23 Base de datos en MySQL

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-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 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.

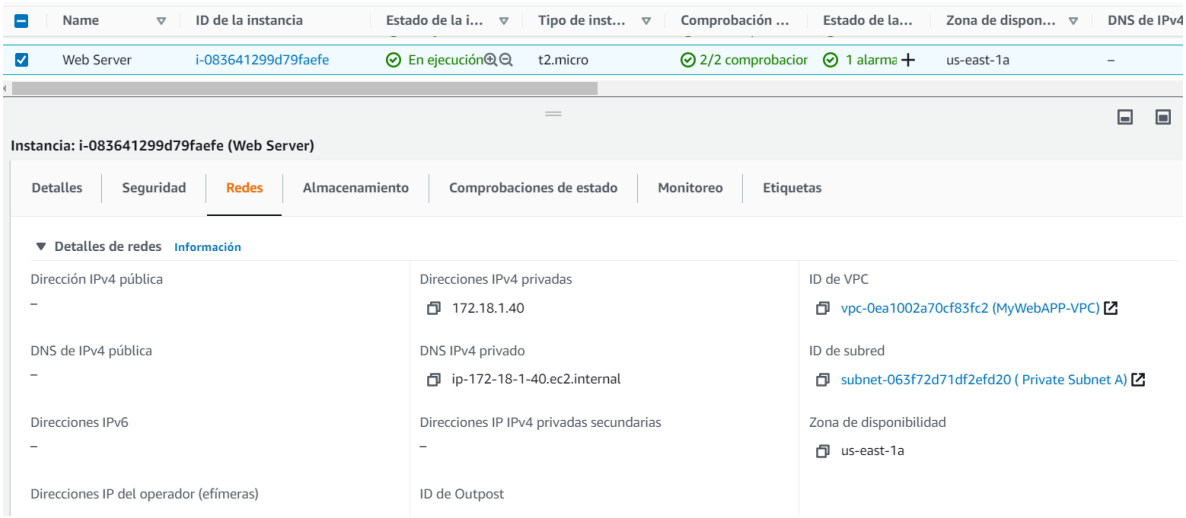


Ilustración 25 Instancia del webserver

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.

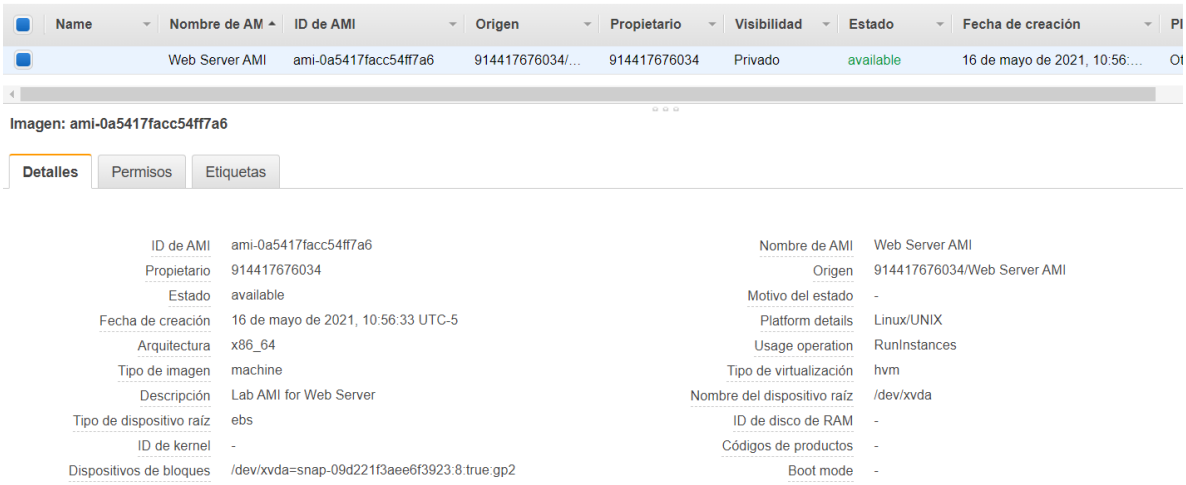


Ilustración 26 Imagen AMI para el servicio de Auto Scaling

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.

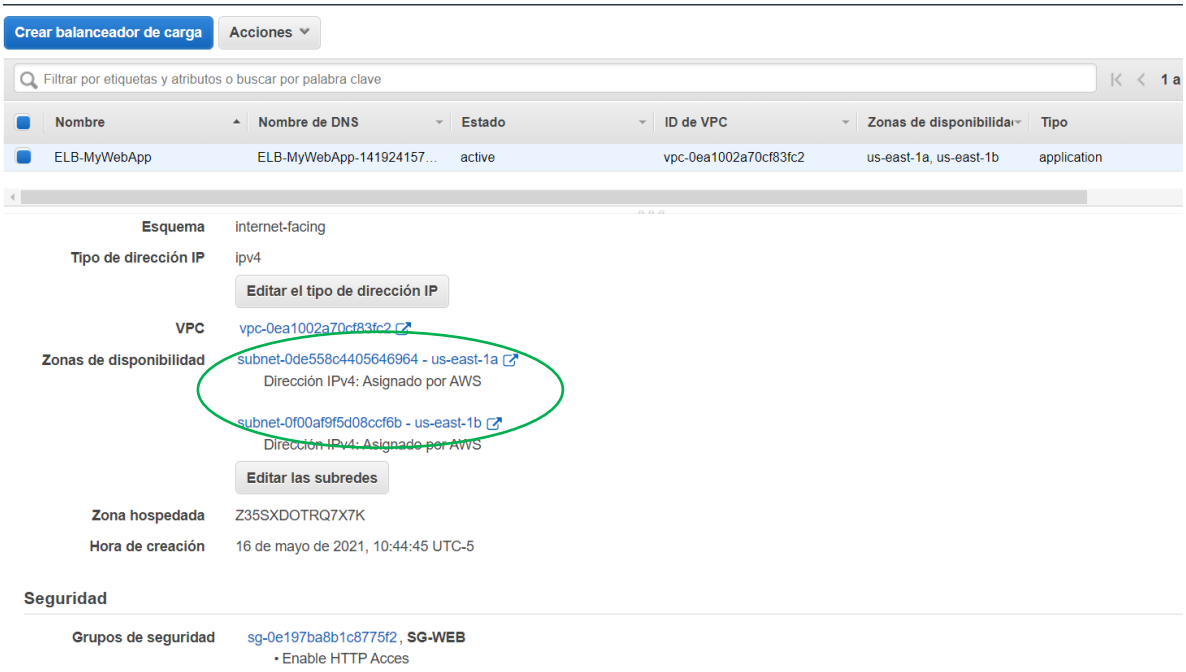


Ilustración 27 Balanceador de carga

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.

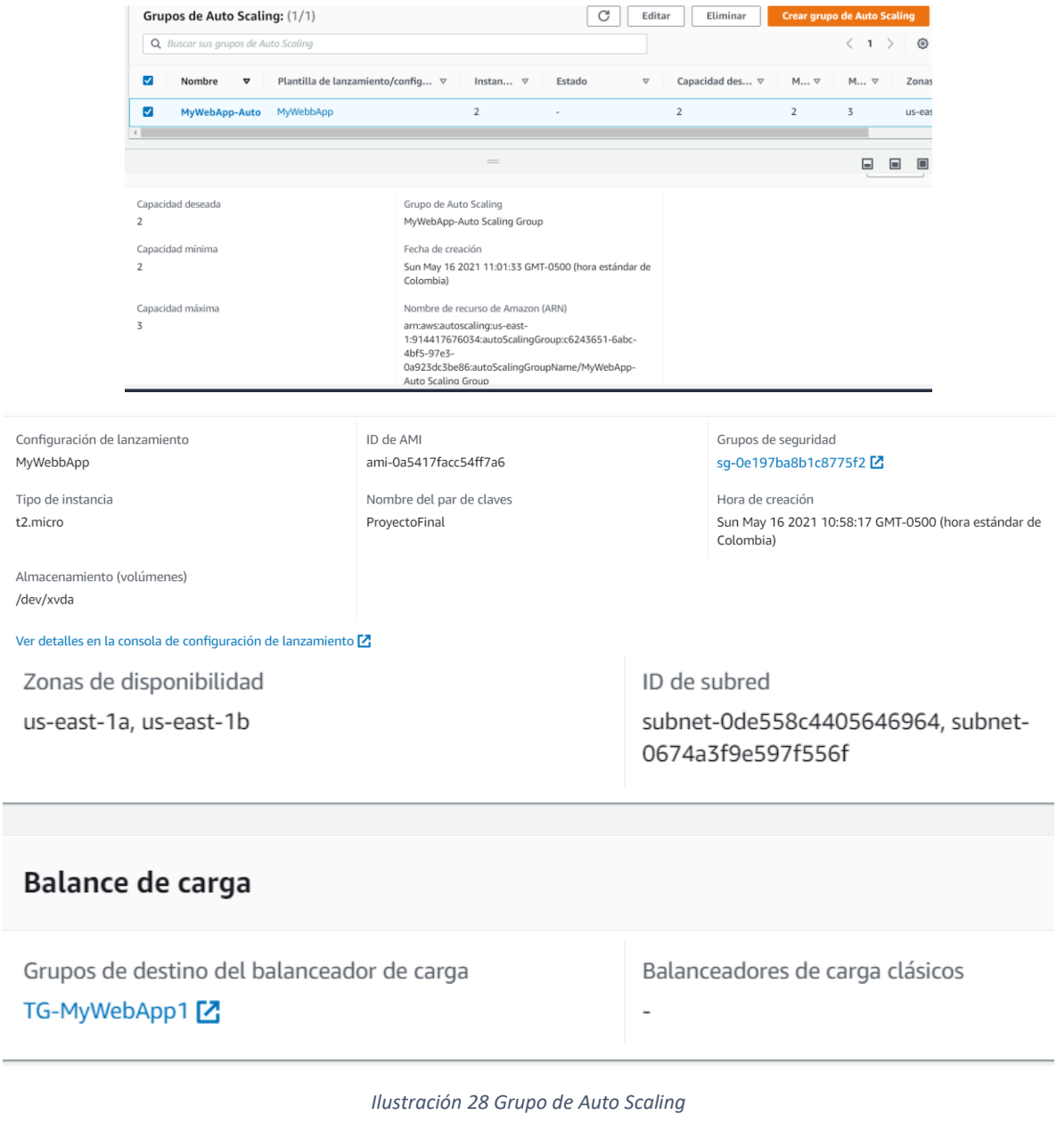


Ilustración 28 Grupo de Auto Scaling

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.

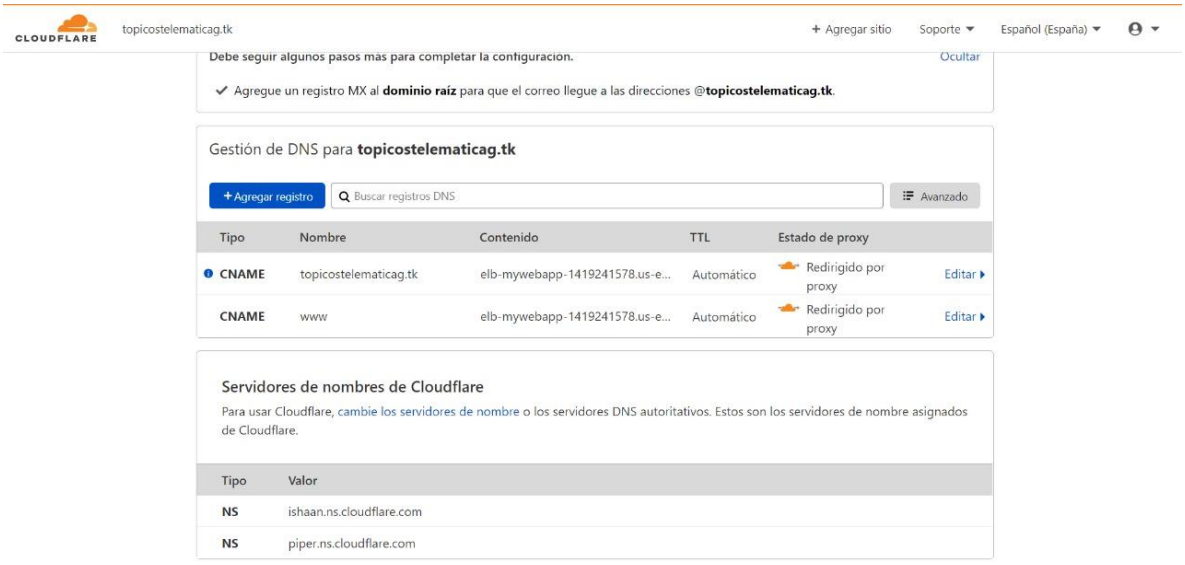


Ilustración 29 Delegación del DNS a CloudFlare

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

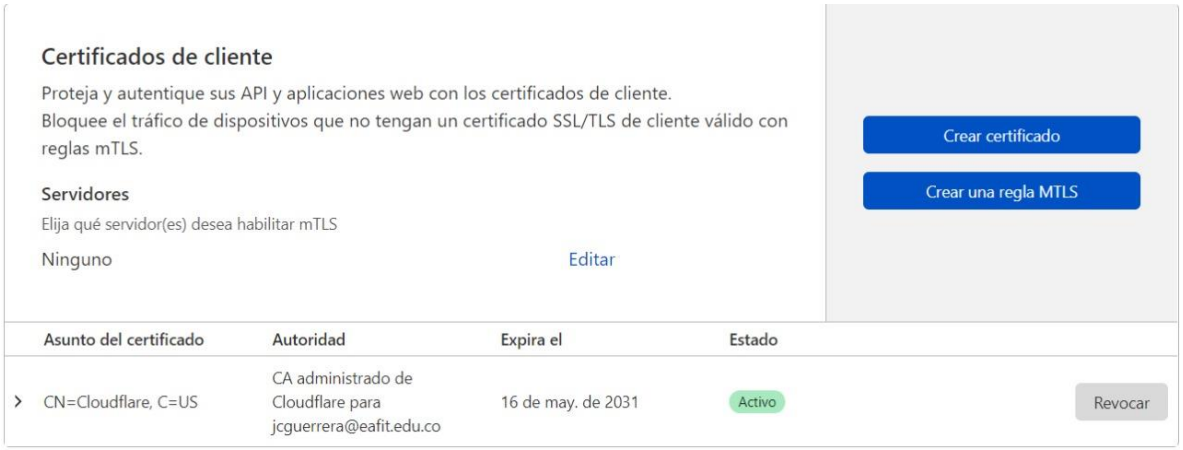


Ilustración 30 Generación de certificados de seguridad

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.

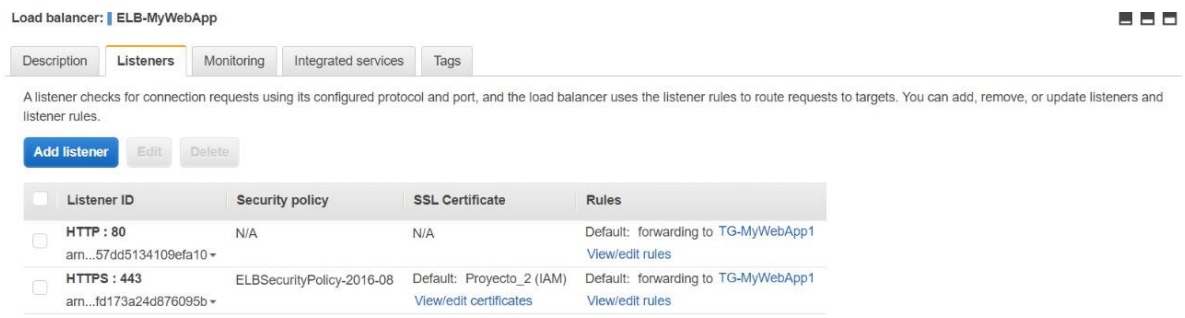


Ilustración 31 Configuración del balanceador de carga con el certificado de seguridad

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

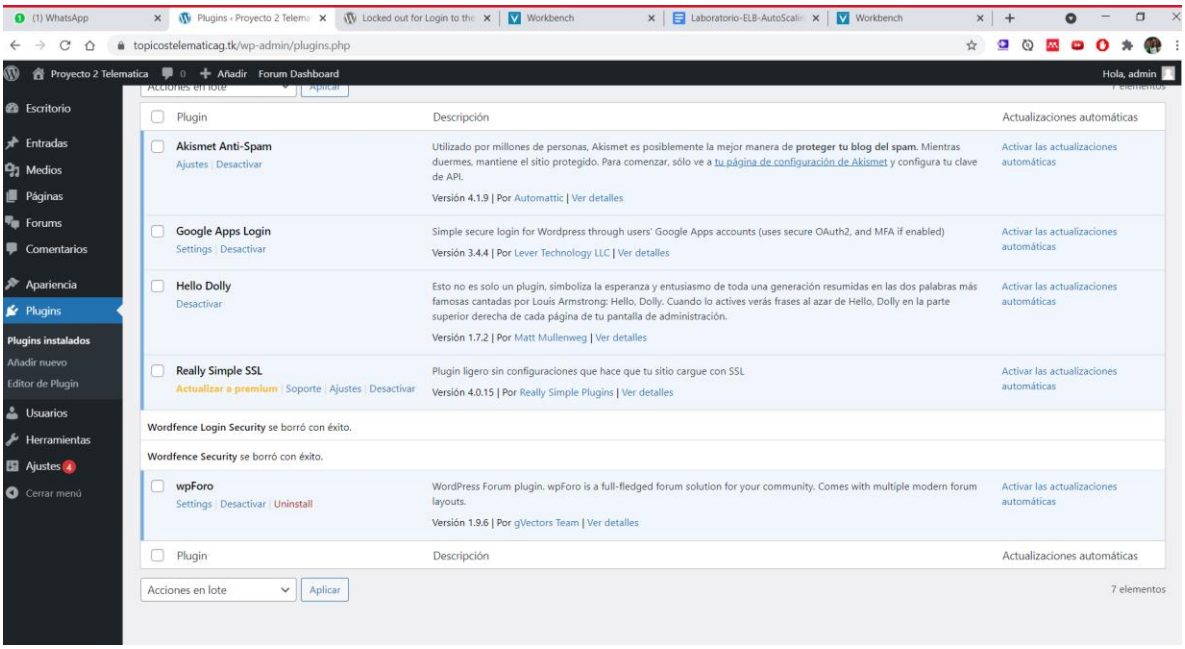


Ilustración 32 Plugin de autenticación por 2 factores