DOCUMENTACIÓN TÉCNICA DEL PROCESO DE INSTALACIÓN, SOLICITUD DE LOS SERVICIOS DE TERCEROS Y PRODUCCIÓN

Por:

- Yhoan Alejandro Guzmán García
- Juan Sebastián Pérez Salazar
- Daniel Felipe Gómez Martínez

Profesor:

Edwin Nelson Montoya Munera

17/05/2021

Universidad EAFIT

VPC

Para el alojamiento de nuestro proyecto se creó una VPC con una dirección privada personalizada (172.24.0.0/16). Con esta VPC además de tener todos los recursos y herramientas concentradas en una sola parte nos brinda seguridad, privacidad y control.

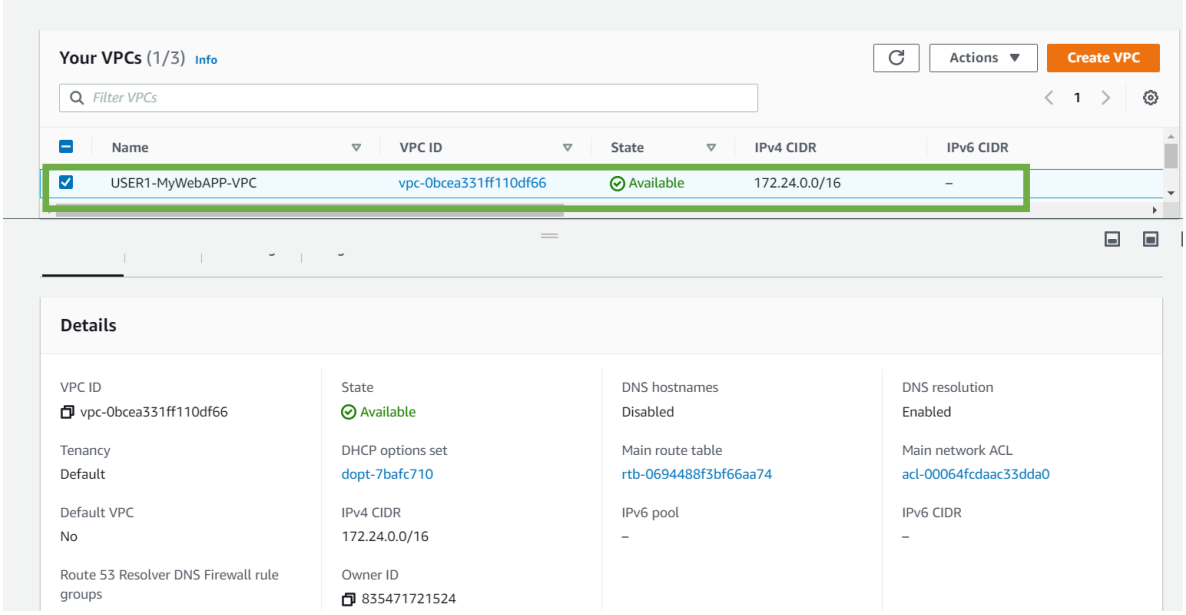

Imagen 1 – VPC creada y configurada

Subnets

En estas 2 subredes que se ven en la siguiente imagen se dividen en dos zonas una en (us-east-2a y us-east-2b) y en cada una de estas zonas se creó una subred privada y una pública.

Para la primera zona us-east-2a (Ohio) se utilizaron las direcciones 172.24.1.0/24 (para la subred privada) y 172.24.2.0/24 (para la subred publica).

Para la primera zona us-east-2b (Ohio) se utilizaron las direcciones 172.24.3.0/24 (para la subred privada) y 172.24.4.0/24 (para la subred publica).

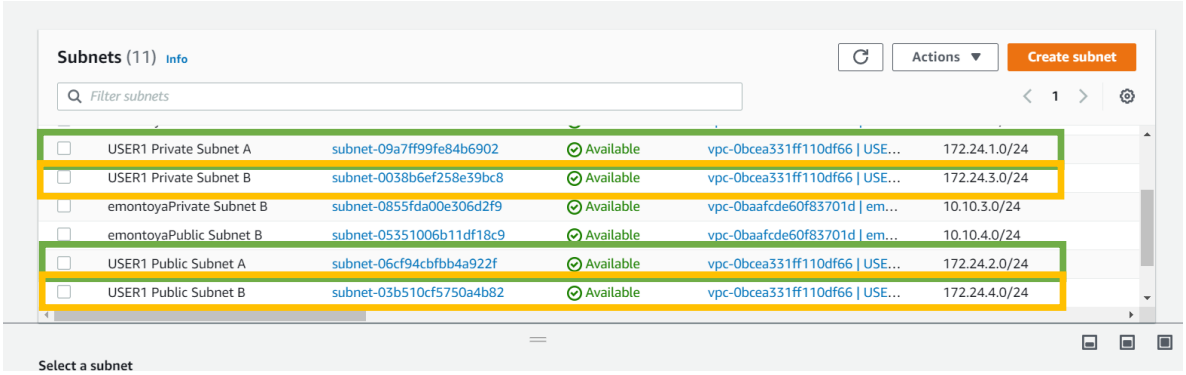

Imagen 2 – Subredes públicas y privadas creadas para la zona A (recuadro verde) y la zona B (recuadro naranja)

Internet Gateway

Para tener la entrada internet solo necesita que se le asigne a nuestra VPC creada, la cual va a ser utilizada para comunicarse y tener acceso a la web, por ende, hace que las instancias puedan desplegar el WordPress.

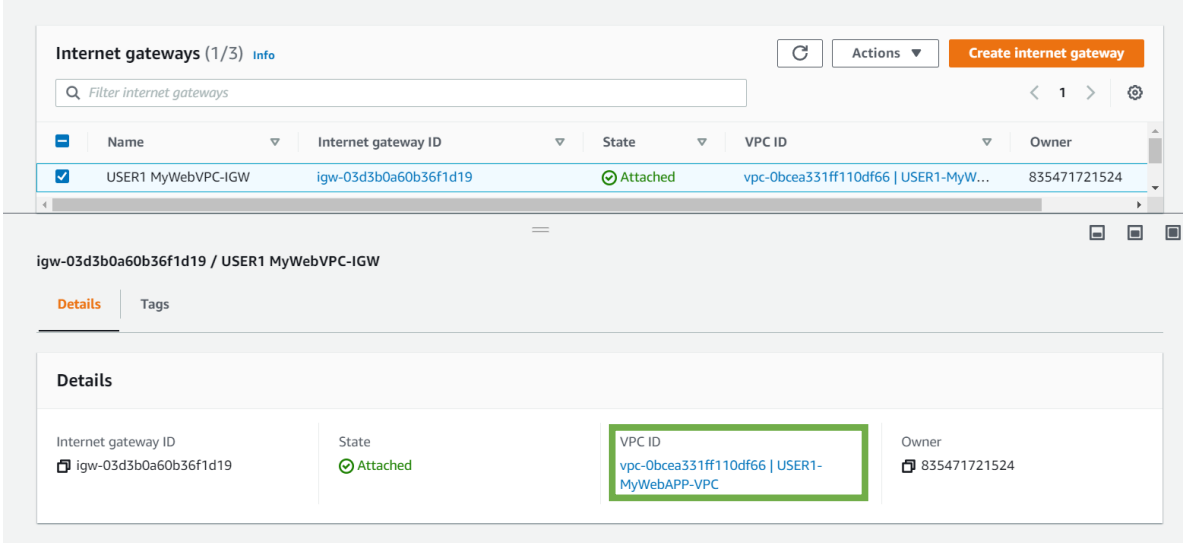

Imagen 3 – Conexión del internet Gateway con la VPC del proyecto

Además de solo crear la entrada a internet, tambien le creamos un grupo de seguridad donde se van a habilitar los puertos de entrada y salida.

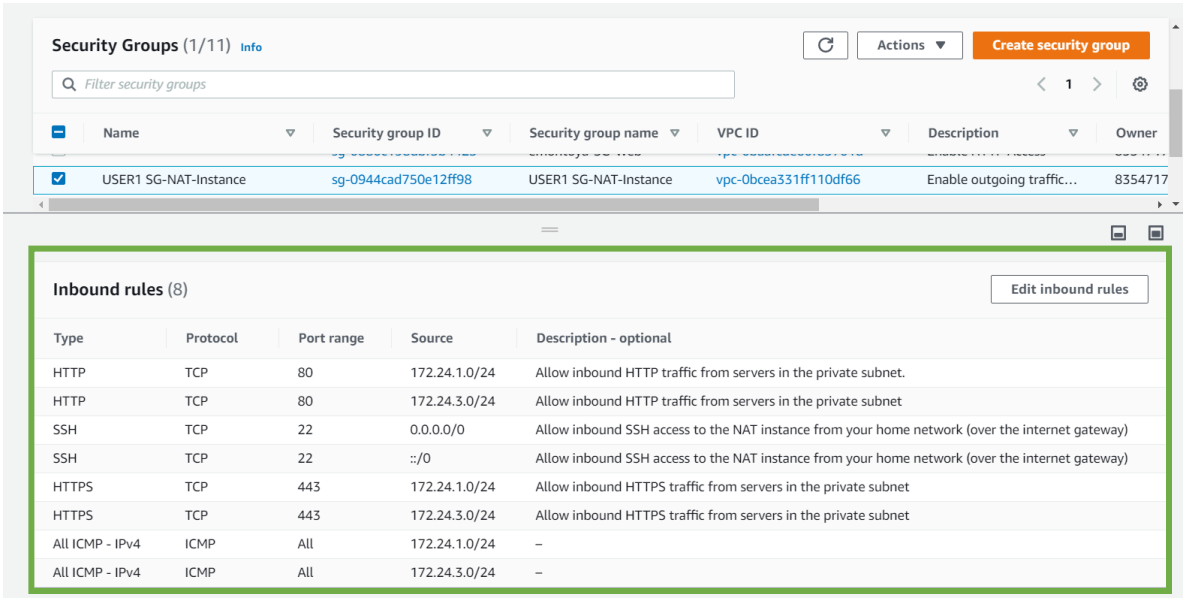

Imagen 4 – Puertos de acceso y comunicación con el internet Gateway

Instancias NAT

A través de las dos instancias NAT una por cada zona (porque estas solo se van a conectar a las subredes públicas), se les va a dar salida a las redes privadas de nuestro proyecto a la web.

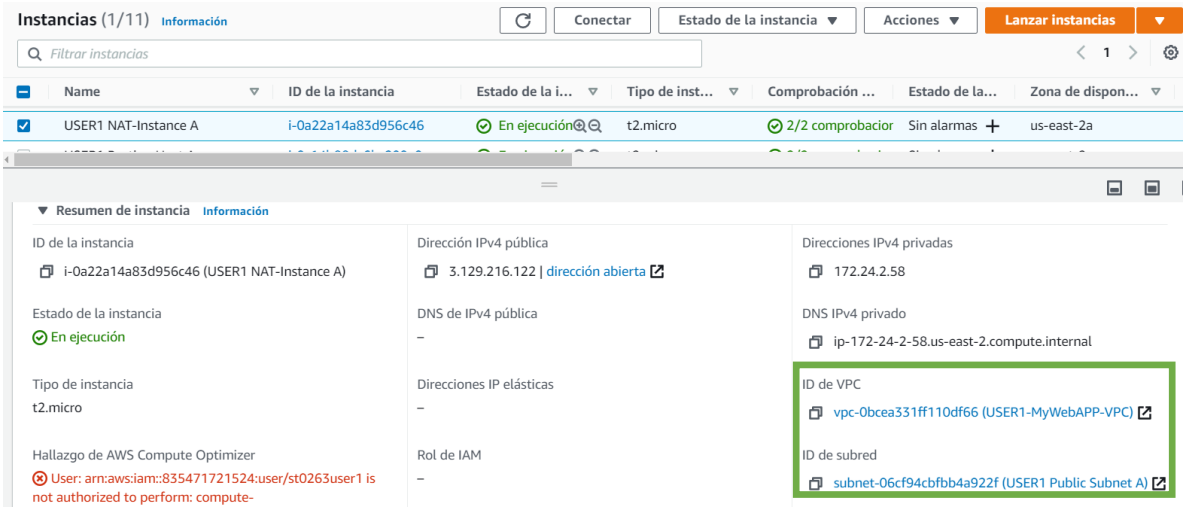

Imagen 5 – Conexión de la instancia NAT de la zona A con la VPC y la subred publica de la zona A

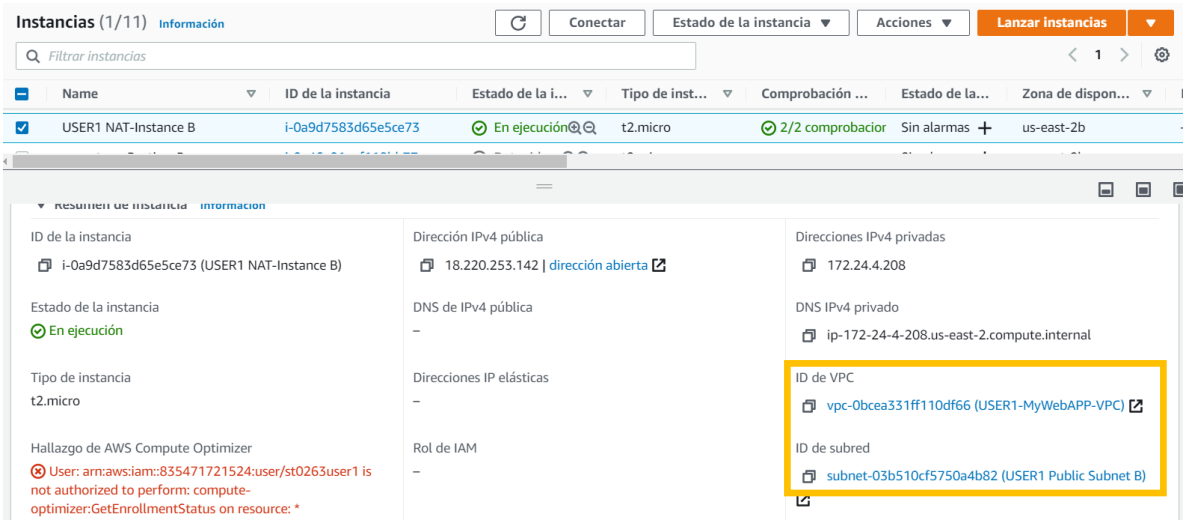

Imagen 6 - Conexión de la instancia NAT de la zona B con la VPC y la subred publica de la zona B

Tablas de ruta

A través de esta esta configuración de las tablas de rutas se van a asignar los flujos de acceso y respuesta de las subredes públicas y privadas a la web.

Name	Route Table ID	Explicit subnet associatior	Edge associations	Main	VPC ID
	rtb-4d451a26	-	-	Yes	vpc-c03daaab | default
emontoyaPrivate Route Table B	rtb-0ddbb42366a76ad26	subnet-0855fda00e306d2f9	-	No	vpc-0baafcde60f83701d | …
USER1 Private Route Table A	rtb-0c8f0bc69080b6718	subnet-09a7ff99fe84b6902	-	No	vpc-0bcea331ff110df66 | …
emontoyaPublic Route Table B	rtb-0baa49d6a8ff1d62a	subnet-05351006b11df18c9	-	No	vpc-0baafcde60f83701d | …
emontoyaPublic Route Table A	rtb-07b054896ae27018d	subnet-0e1aa5818b5eb3db5	-	No	vpc-0baafcde60f83701d | …
	rtb-0694488f3bf66aa74	-	-	Yes	vpc-0bcea331ff110df66 | …
USER1 Public Route Table A	rtb-03afa55c7eaaa382c	subnet-06cf94cbfbb4a922f	-	No	vpc-0bcea331ff110df66 | …
USER1 Public Route Table B	rtb-01c0071d071d7463c	subnet-03b510cf5750a4b82	-	No	vpc-0bcea331ff110df66 | …
USER1 Private Route Table B	rtb-00a046fb6f539ad39	subnet-0038b6ef258e39bc8	-	No	vpc-0bcea331ff110df66 | …
emontoyaPrivate Route Table A	rtb-0059a3937212a84e9	subnet-0f35ac4e9e9c41984	-	No	vpc-0baafcde60f83701d | …

Imagen 7 – Tabla de rutas para cada subred en la zona A (recuadro verde) y zona B (recuadro naranja)

- Para la tabla de rutas públicas de la zona A y de la zona B, deben ser conectadas a sus respectivas subredes, las cuales apuntan directamente al internet Gateway.
    - Para el caso de la tabla de rutas publica de la zona A:

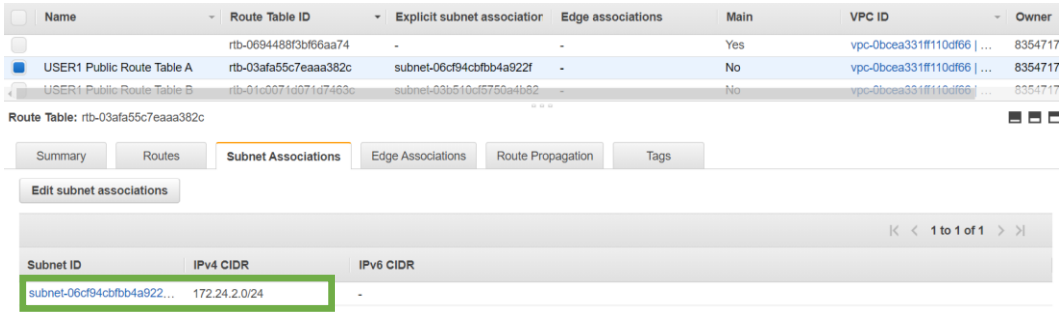

Imagen 8 – Conexión de la tabla de rutas publica en la zona A con la subred publica en la zona A

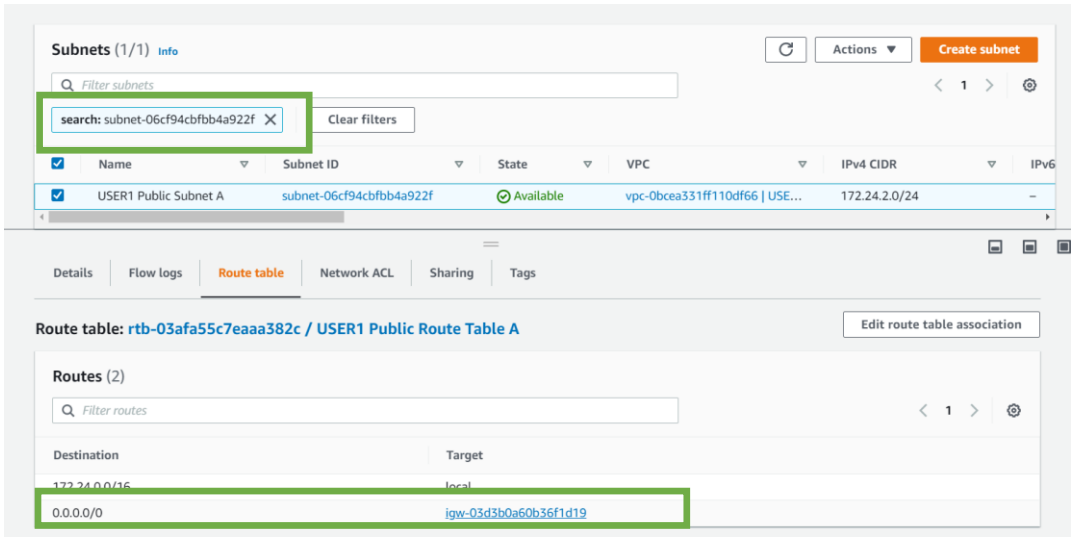

Imagen 9 – conexión de la subred publica en la zona A con el internet Gateway

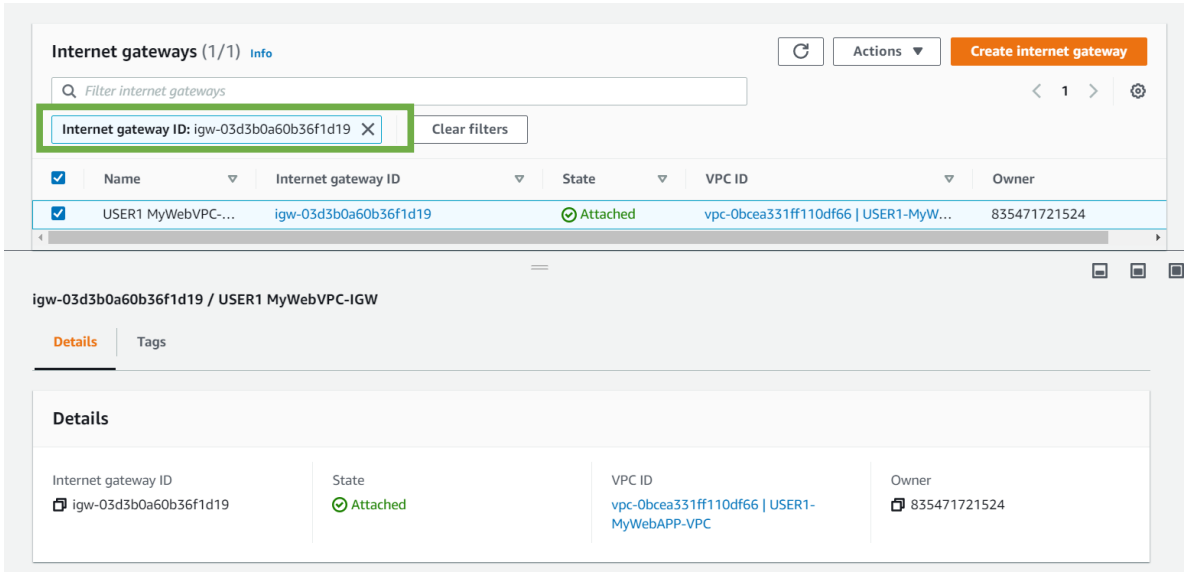

Imagen 10 – Internet Gateway del sistema

- Para el caso de la tabla de rutas publica de la zona B:

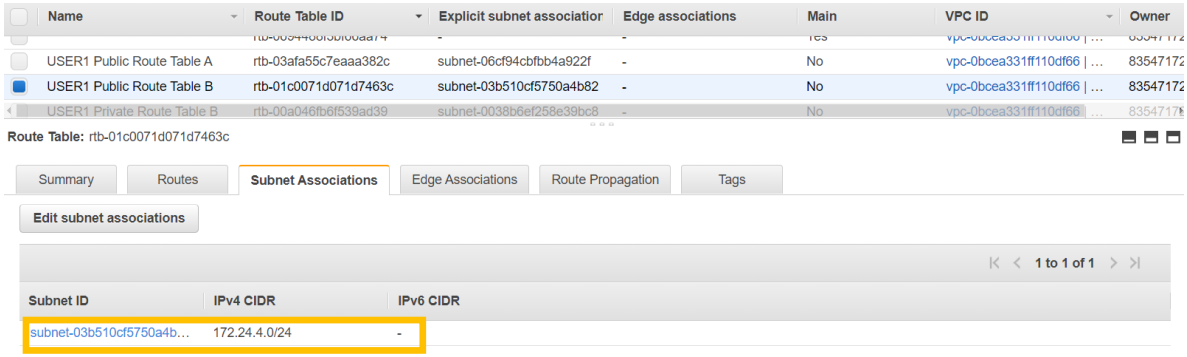

Imagen 11 - Conexión de la tabla de rutas publica en la zona B con la subred publica en la zona B

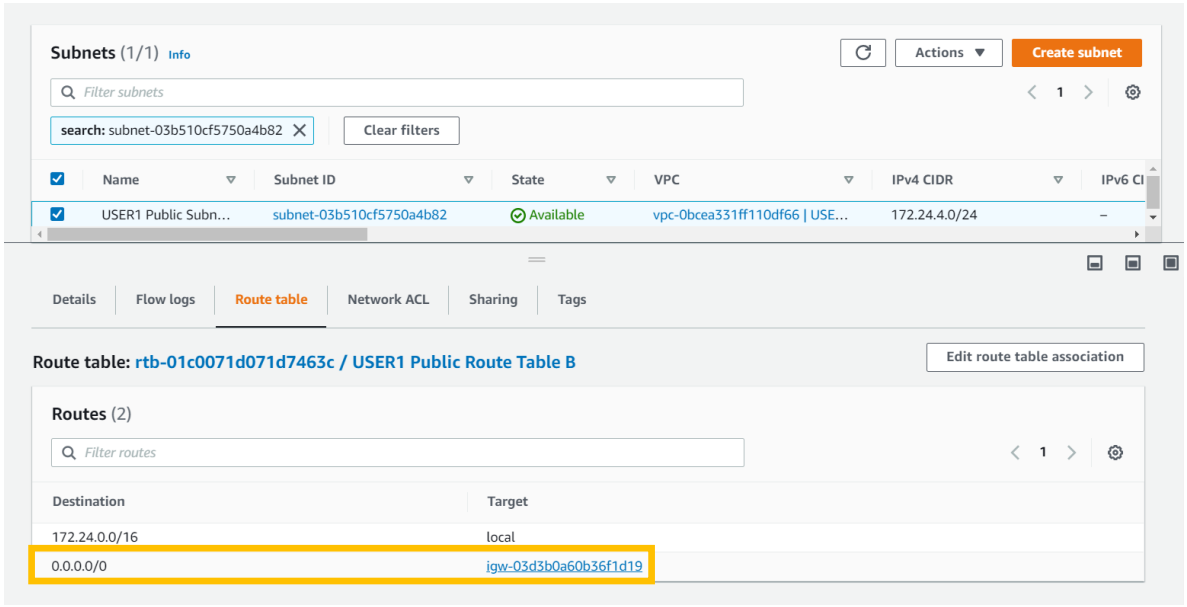

Imagen 12 - conexión de la subred publica en la zona B con el internet Gateway

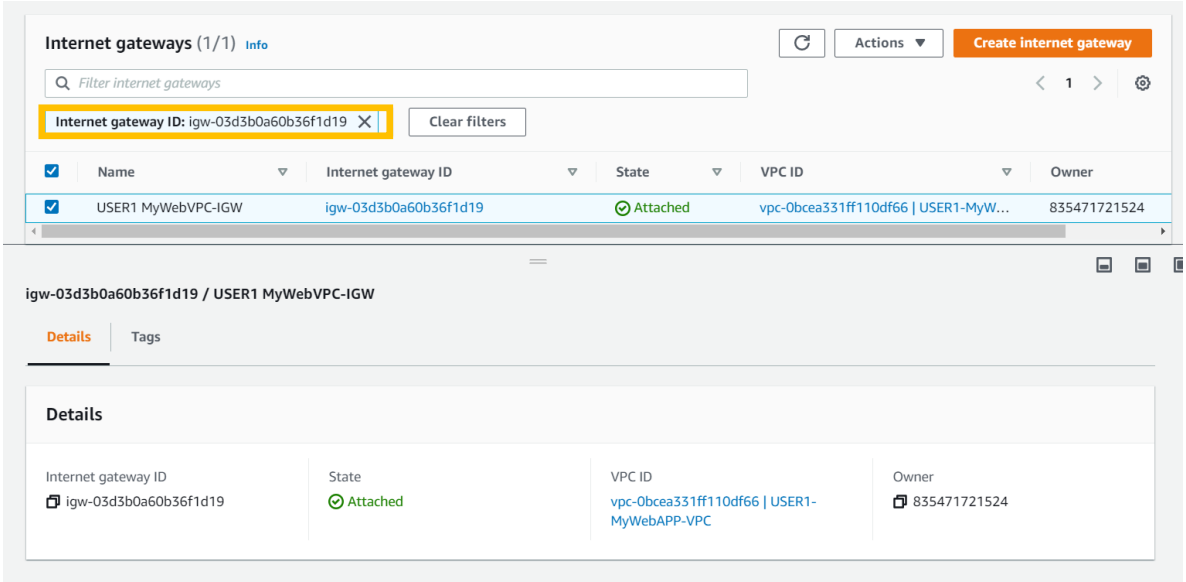

Imagen 13 – Internet Gateway del sistema

Nota: Mire que ambas subredes apuntan directamente al internet Gateway del sistema.

- Para la tabla de rutas privadas de la zona A y zona B, la conexión es distinta porque esta no va directamente conectada al internet Gateway, sino que estas deben apuntar a las respectivas instancias NAT creadas en el punto anterior.
    - Para el caso de la tabla de ruta privada A:

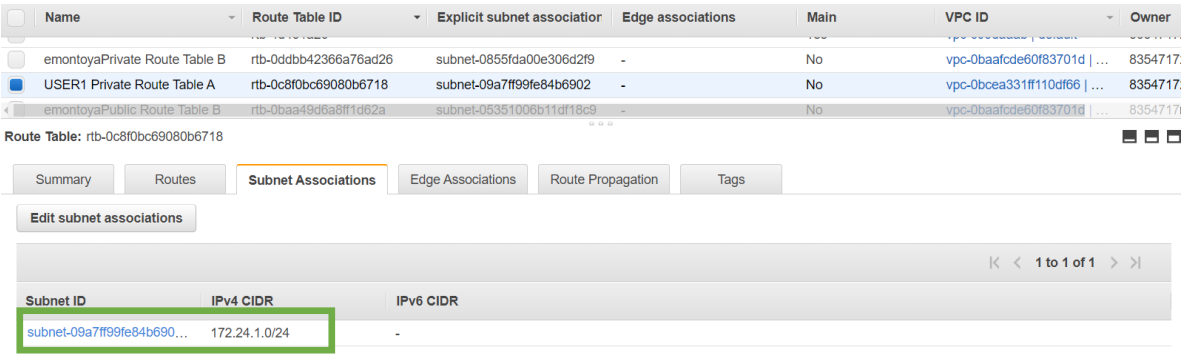

Imagen 14 - Conexión de la tabla de rutas privada en la zona A con la subred privada en la zona A

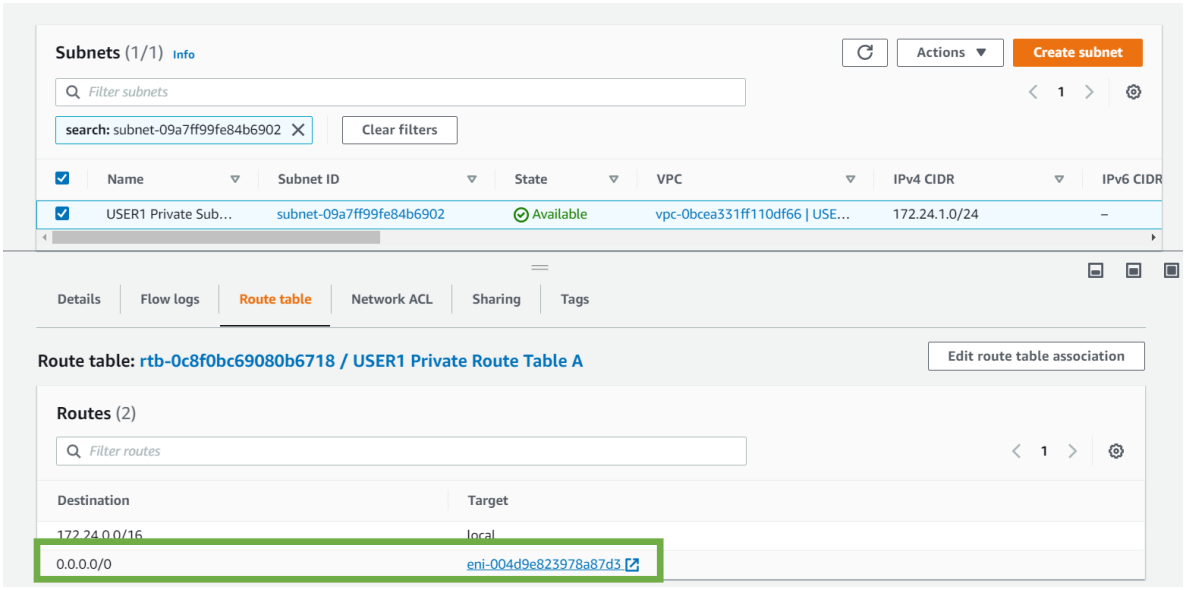

Imagen 15 – Conexión de la subred privada A con la instancia NAT de la zona A

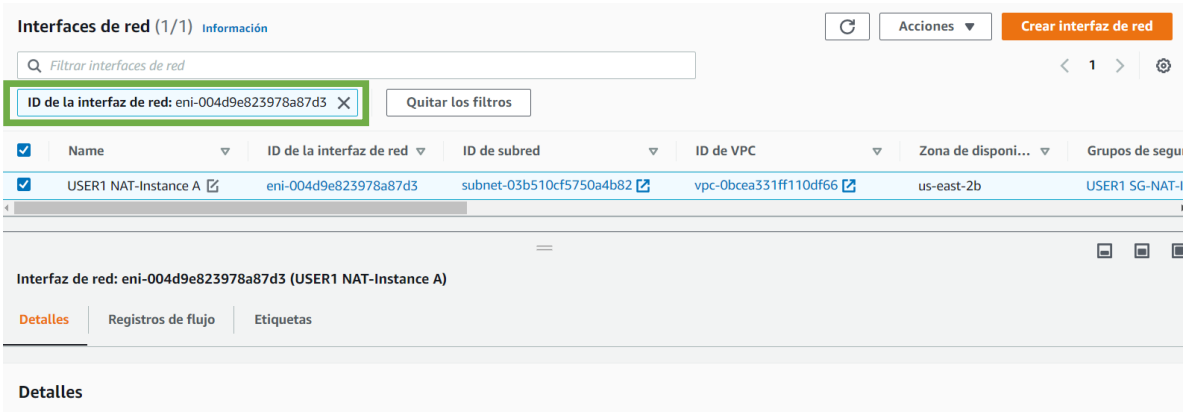

Imagen 16 – Instancia NAT de la zona A

- Para el caso de la tabla de ruta privada B:

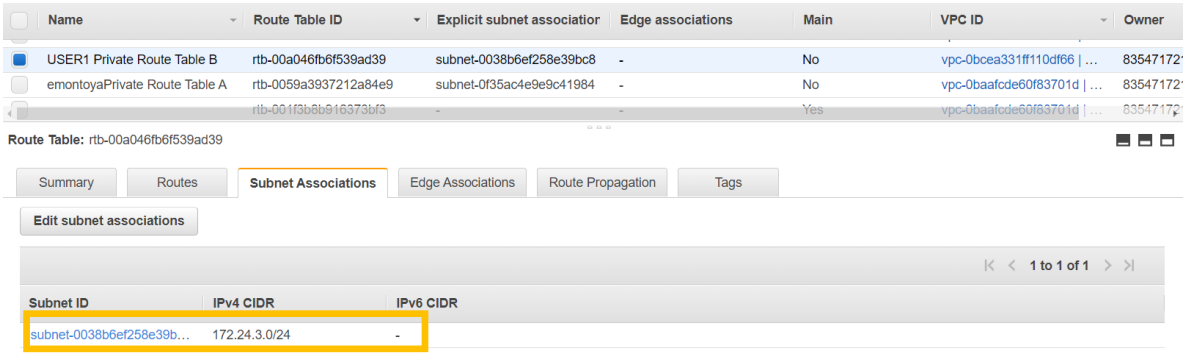

Imagen 17 - Conexión de la tabla de rutas privada en la zona B con la subred privada en la zona B

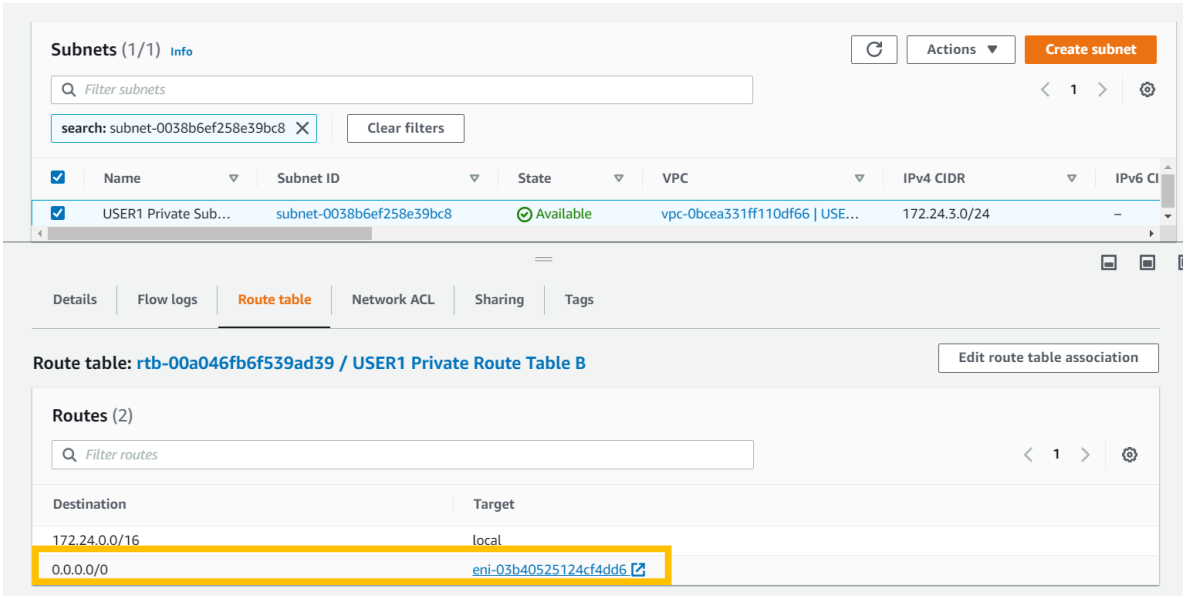

Imagen 18 - Conexión de la subred privada B con la instancia NAT de la zona B

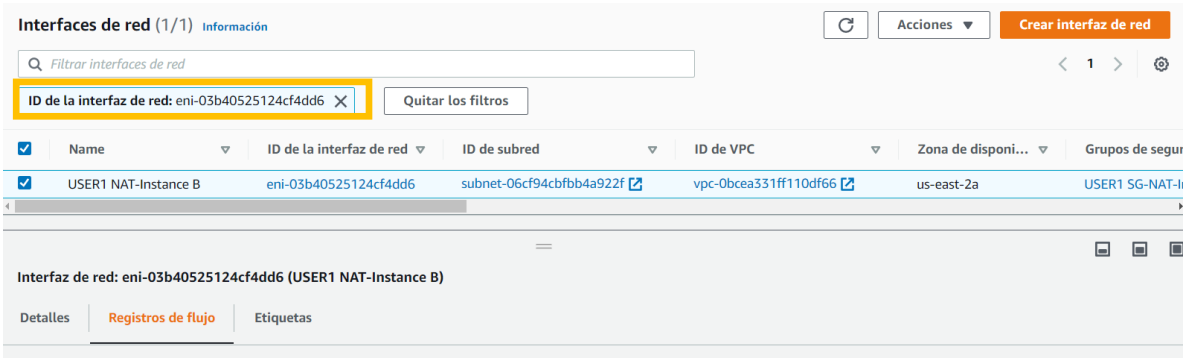

Imagen 19 - Instancia NAT de la zona A

Bastion host

El Bastion Host nos proporciona acceso seguro a las instancias ubicadas tanto en las subredes públicas como privadas, por lo que se van a crear dos instancias EC2 para configurar el Bastion Host una en de cada zona (A y B).

- Instancia Bastion host para la zona A:

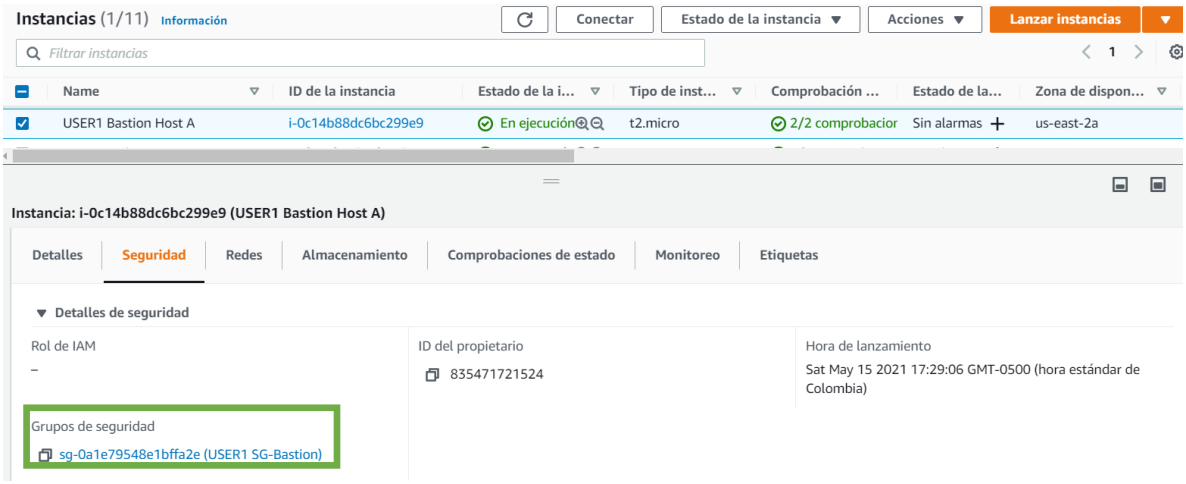

Imagen 20 – Grupo de seguridad del Bastion Host en la instancia creada para la zona A

- Instancia Bastion host para la zona B:

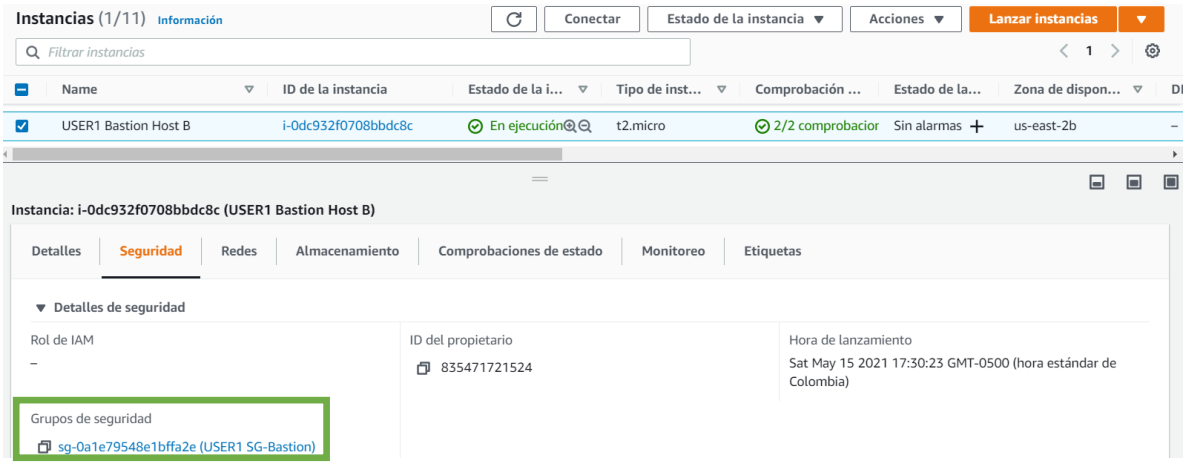

Imagen 21- Grupo de seguridad del Bastion Host en la instancia creada para la zona A

Nota: Ambas instancias tiene el mismo grupo de seguridad (USER1 SG-Bastion). El grupo de seguridad del Bastion Host solo tiene abierto el puerto 22 (SSH):

Imagen 22 - Grupo de seguridad para las instancias del Bastion Host

Grupo de seguridad de la página web

Antes de crear las instancias en las cuales se van a desplegar los WordPress se deben configurar los puertos de entrada y salida de las instancias, sin duda alguna uno de los puertos más importantes son el HTTP y el HTTPS ya que en estos dos puertos se van a recibir peticiones del WordPress y en el caso del HTTPS se tendrá el certificado SSL.

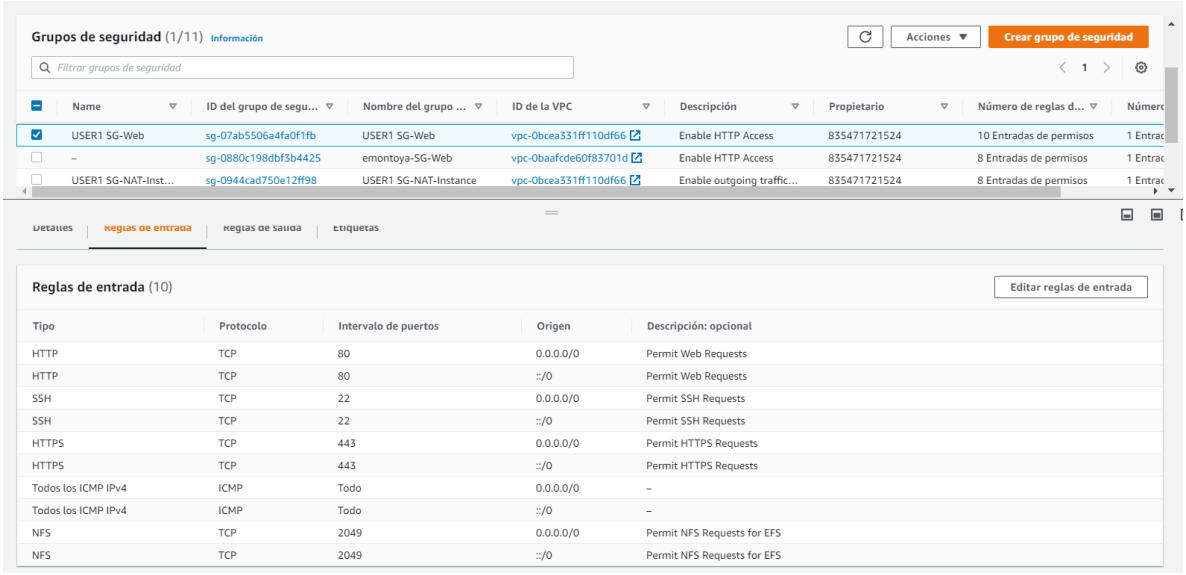

Imagen 23 - Puertos de entrada y salida del grupo de seguridad para la instancia de la web

Grupo de seguridad de la base de datos

En este grupo de seguridad solo se abrirá el puerto 3306 el cual es el predefinido para la base de datos MYSQL/Aurora.

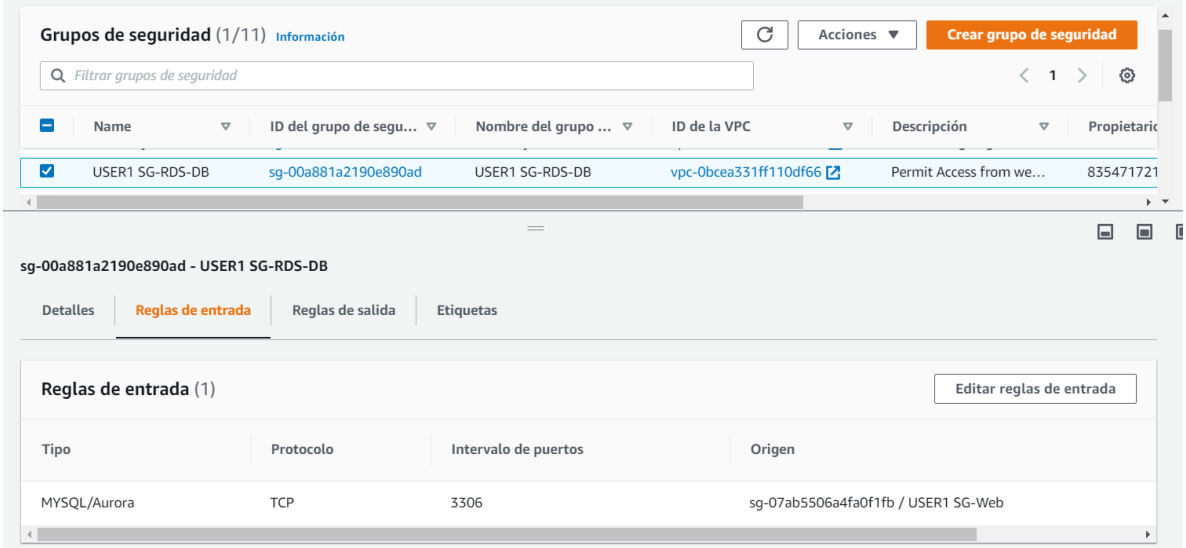

Imagen 24 – Grupo de seguridad de la base de datos

Grupo de seguridad del RDS

Este grupo de seguridad se crea con el fin de indicarle al servicio RDS las subredes que tienen acceso a esta. En nuestro caso solo las subredes privadas de cada zona (A y B) van a tener acceso a este servicio.

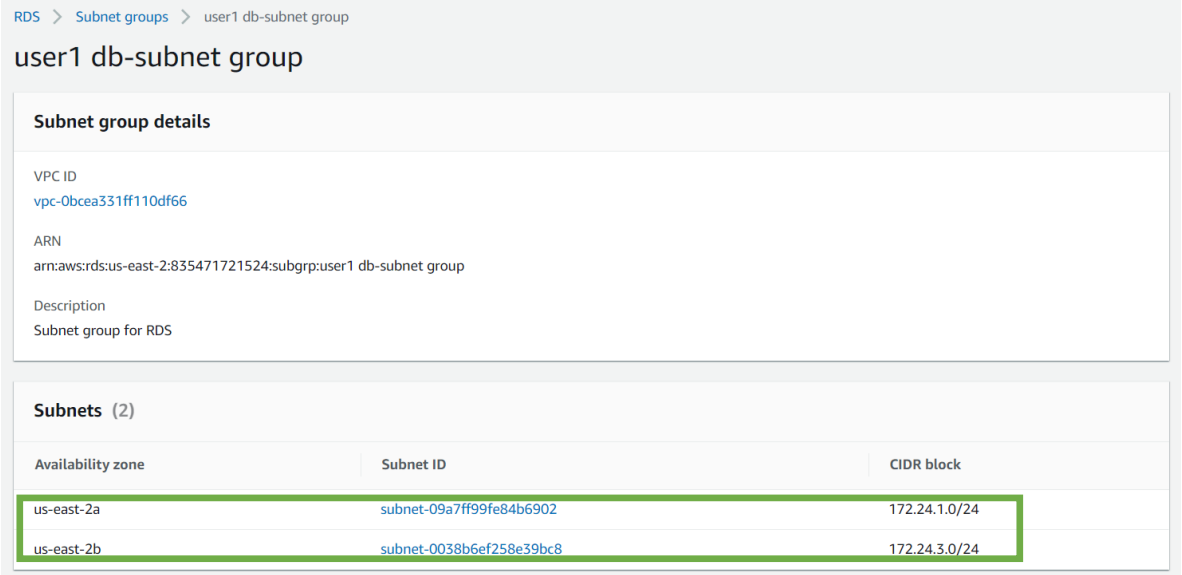

Imagen 25 – Subredes que tienen acceso al servicio de RDS creado

Base de datos RDS

Para la creación de la base de datos se deben de tener en cuenta dos aspectos importantes, uno de ellos es agregar el grupo de seguridad creado en el punto anterior (rectángulo negro). Y el otro punto es ser muy conscientes del nombre de la base de datos (rectángulo azul), porque este nombre será utilizado en el despliegue del WordPress.

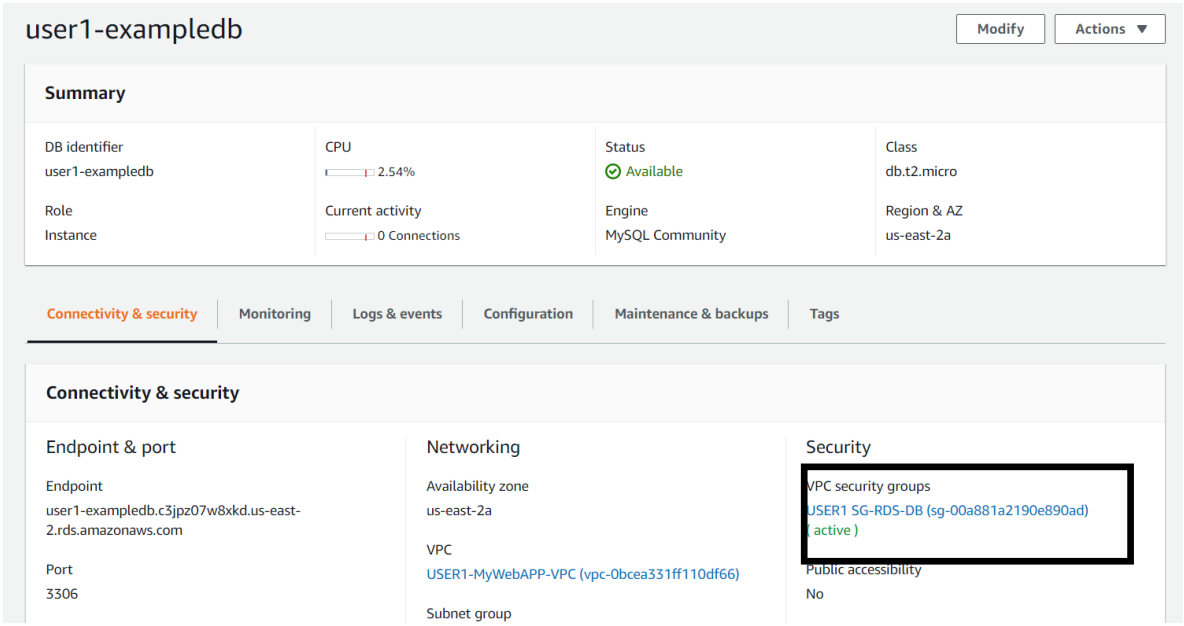

Imagen 26 – Grupo de seguridad de la base de datos

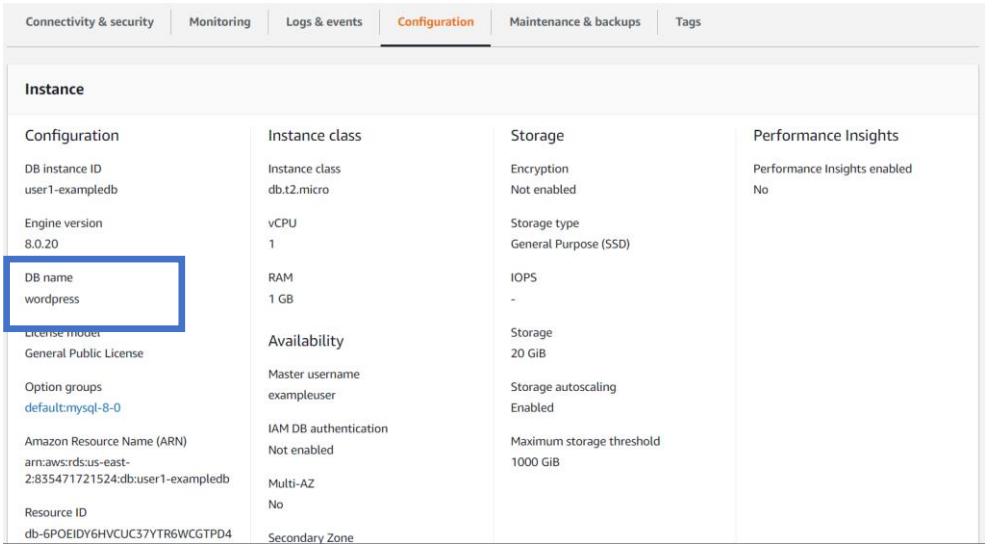

Imagen 27 – Nombre de la base de datos

EFS

Se crea una EFS (Elastic file system) con el fin de tener un sistema elástico y sencillo para compartir datos de archivos. Lo que nos va a permitir compartir todos los archivos de la aplicación WordPress y archivos estáticos como los que gestiona el servicio CMS (sistema de gestión de contenidos) entre las instancias creadas.

En esta imagen se ven las dos subredes privadas de cada zona:

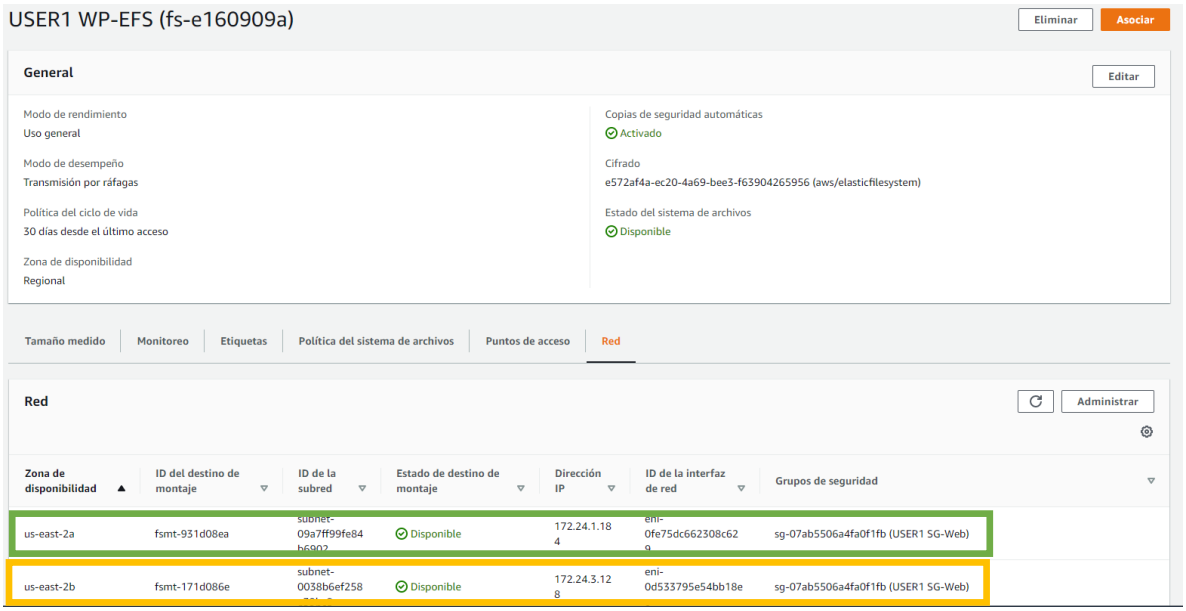

Imagen 28 – Subredes privadas de cada zona que tiene acceso al EFS

Instancia de la página Web

Para la instancia de la página web es importante abrir los puertos de 80 (HTTP), 443 (HTTPS) y 22 (SSH), los cuales van a servir para el despliegue y el montaje del WordPress.

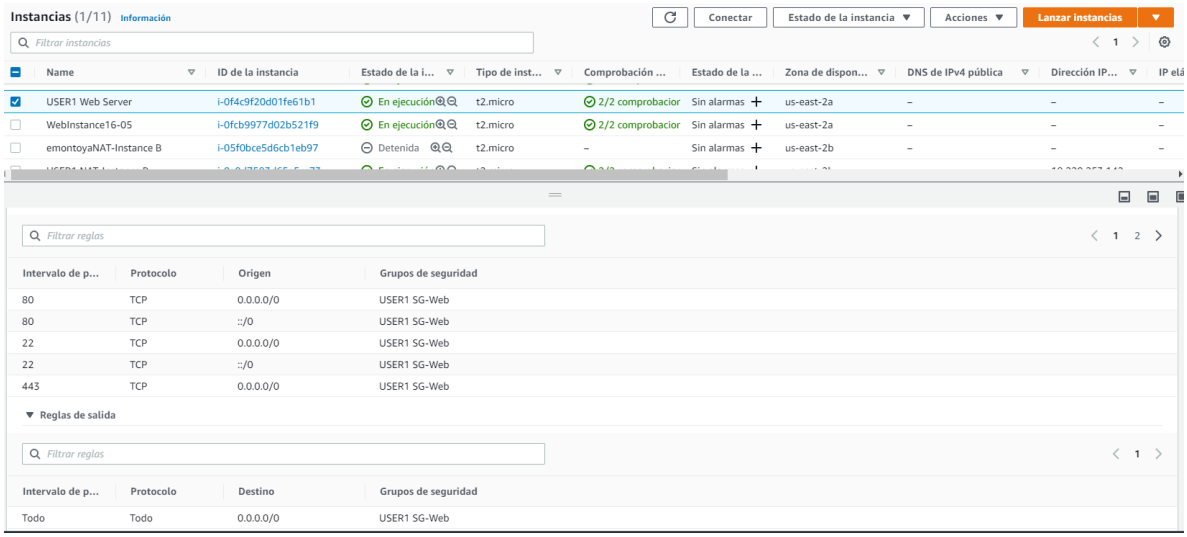

Imagen 29 – Grupo de seguridad de las instancias web

Nota: Una vez que tenga la instancia lanzada se puede crear el Docker compouser para la instalación de WordPress y la base de datos.

Imagen en la instancia web

Una vez creada la instancia de la página web para poder implementar el servicio de auto scaling group, se debe crear una imagen (AMI) la cual va a ser la plantilla con la cual se crearán las nuevas instancias las cuales se van a desplegar con un contenido idéntico.

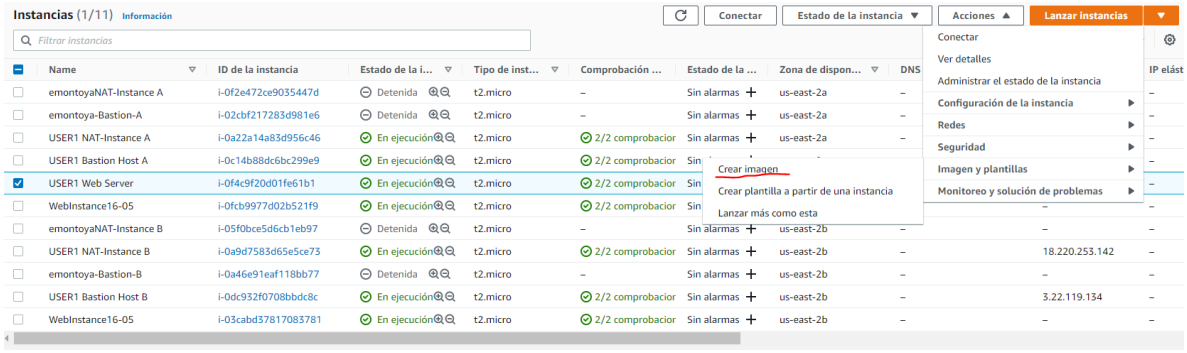

Imagen 30 – Creación de la imagen AMI para replicar las instancias

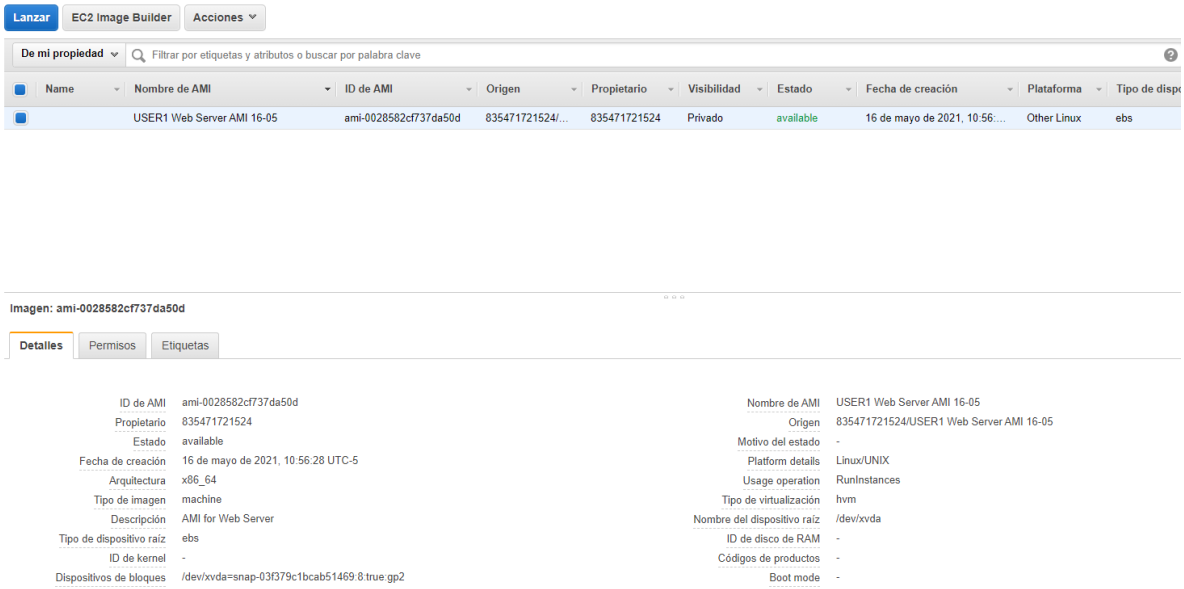

Imagen 31 – Imagen AMI creada y lista par ser utilizada en el auto scaling goup

Load Balancer

Para crear el balanceador de carga se utilizará el servicio administrado de AWS, en el momento de la configuración se deben de tener dos aspectos fundamentales para su configuración. El primero de ellos es la selección de las subredes ya que estas deben ser las subredes públicas de cada zona (recuadro rojo); y el segundo aspecto es configurar un listener el cual apunte al puerto 80 (recuadro amarrillo) porque este va a ser el puerto por el cual va a escuchar las peticiones que se le hagan a la página web.

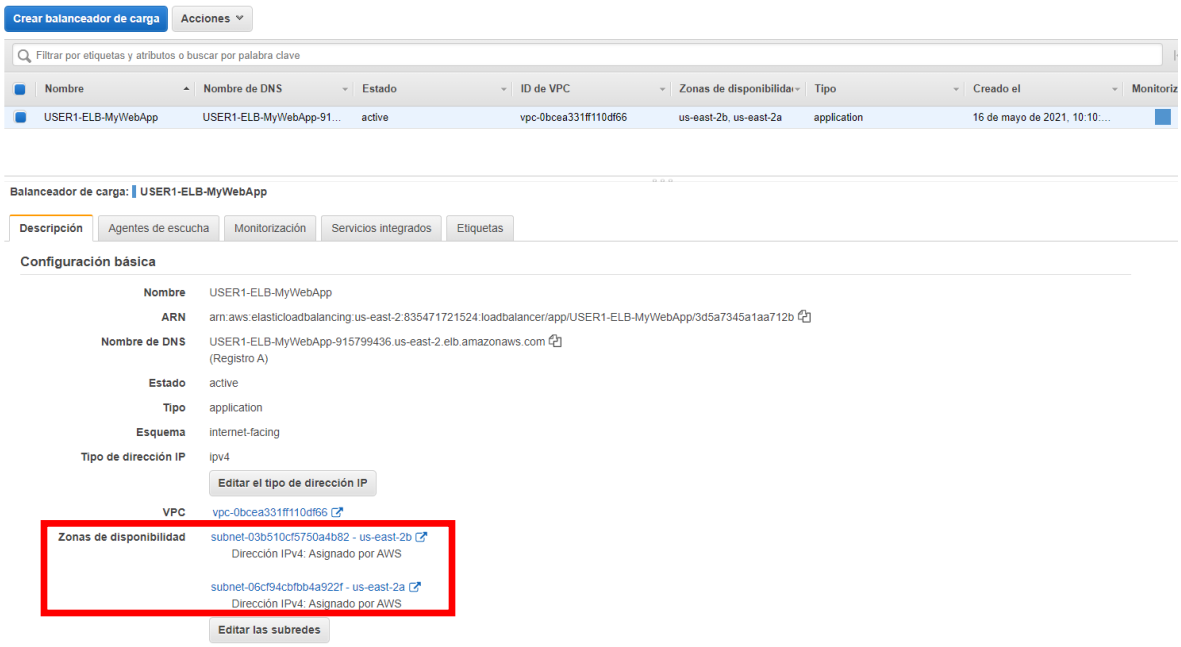

Imagen 32 – Subredes públicas de cada zona

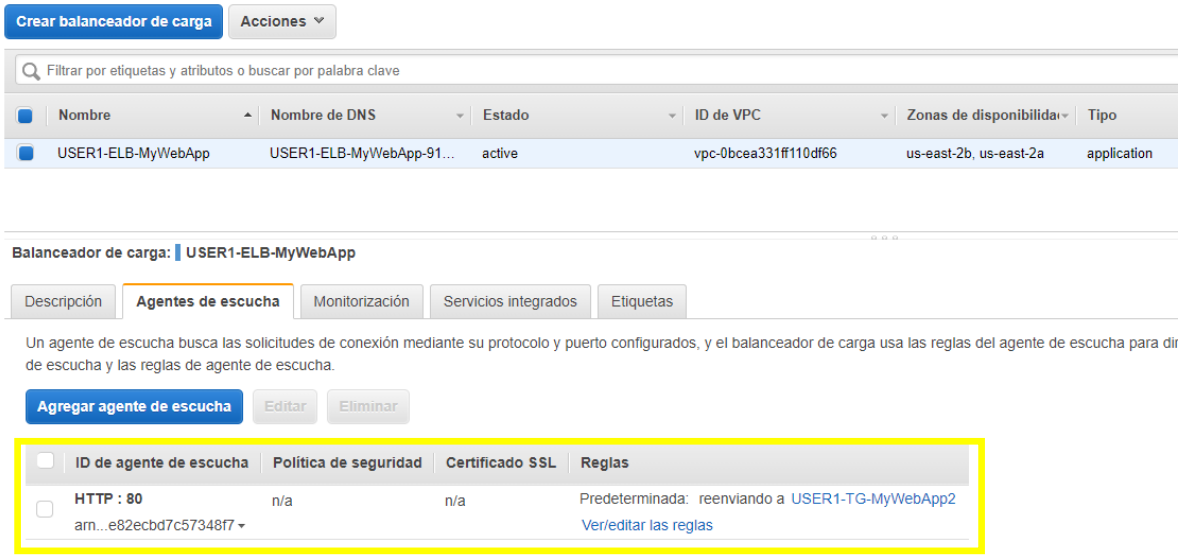

Imagen 33 – Listener por el puerto 80

Auto scaling group

Por ultimo se utilizó otro servicio administrado de AWS el cual es el Auto sclaing group, el cual se encarga de aumentar o disminuir la cantidad de instancias en el sistema a medida que disminuye o aumenta las solicitudes de la pagina web, este nos permite conservar unos tiempos de respuesta estándar para nuestra página web.

Para configurar este servicio se necesita configurar dos cosas de suma importancia, una de estas es configurar el lugar donde se van a crear las nuevas instancias por lo que es fundamental alojarlas en las subredes privadas de cada zona (recuadro morado); y por ultimo se deben especificar la cantidad máxima y mínima de instancias a desplegar.

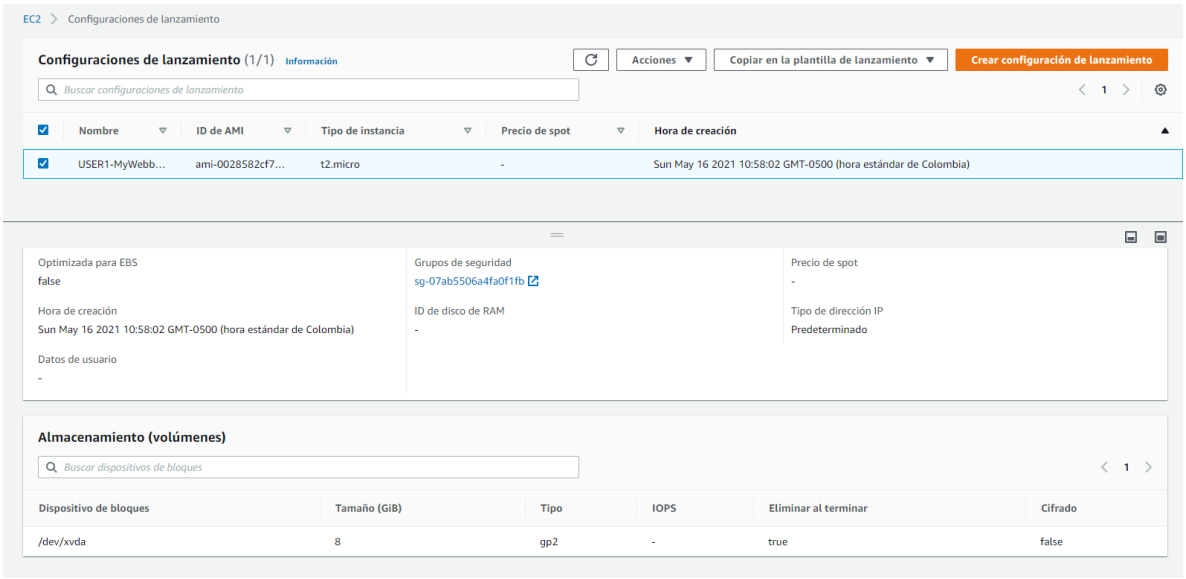

Imagen 34 – Configuración del auto scaling

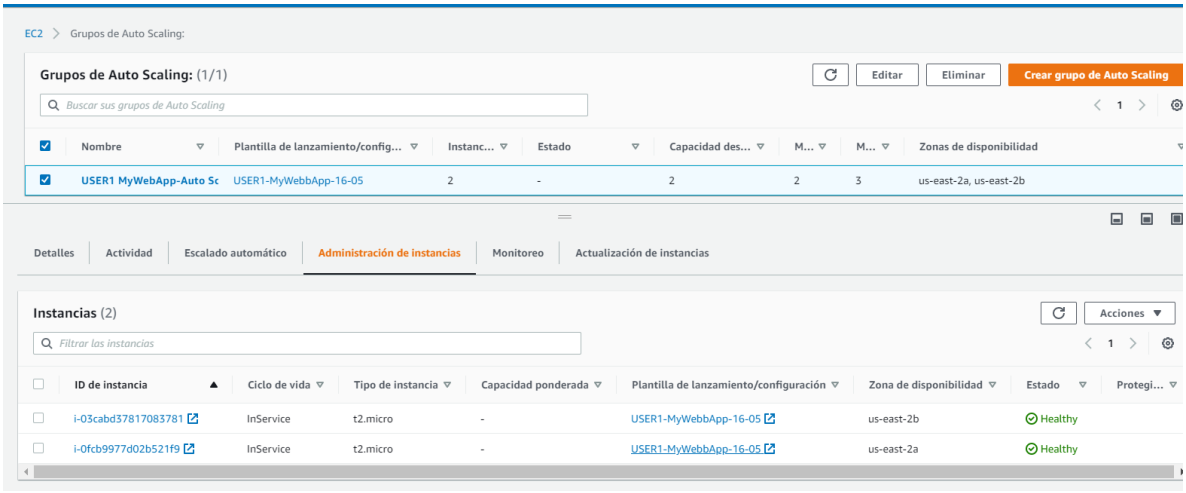

Imagen 35 – Grupo de auto scaling desplegado

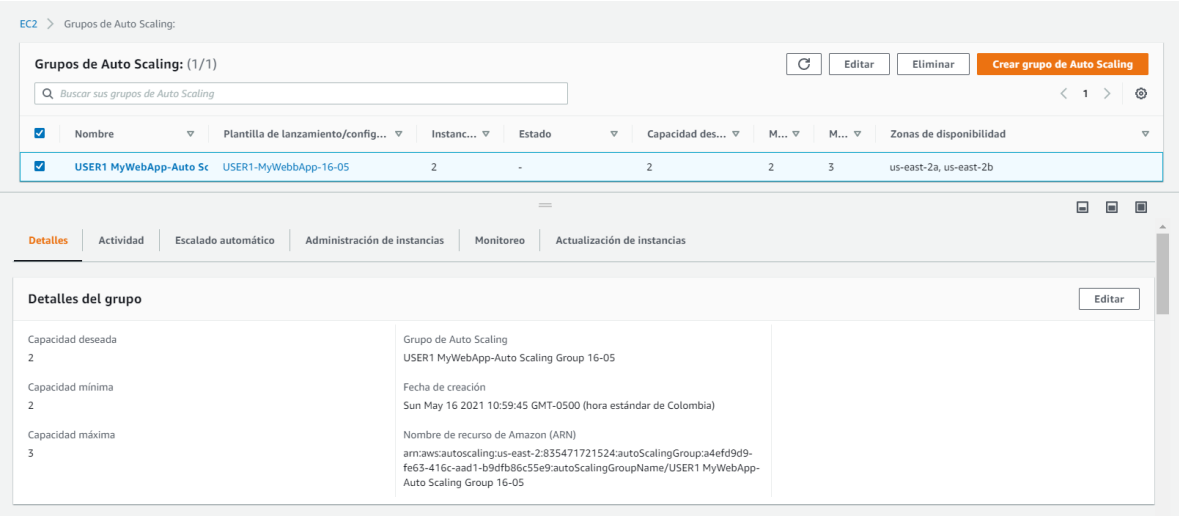

Imagen 36 - Cantidad de instancias mínimas y máximas que puede desplegar al auto scaling group

Generación del certificado SSL

El certificado SSL se genera al nombre del dominio para garantizar al usuario final que su conexión a dicha pagina es segura. Lo primero que se realiza es la reserva de un nombre para el dominio en freenom. En este caso el elegido fue sadteamproyecto2.tk.

Imagen 37 - Nombre del dominio

Posteriormente se delega el manejo del dominio a Cloudflare para desde esta plataforma generar el certificado SSL, para hacer esto se cambian los nombres de servidores en freenom y se ponen los DNS de Cloudflare para delegarle el dominio.

Imagen 38 - Delegando el dominio a Cloudflare

Luego en Cloudflare se añaden los registros necesarios para que el certificado se asocie de manera correcta.

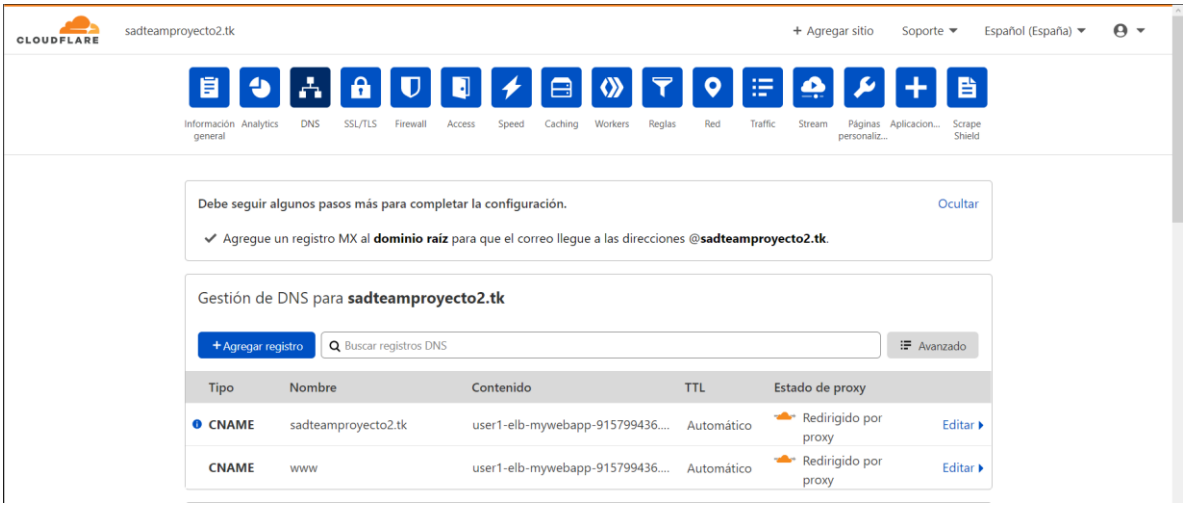

Imagen 39 - Añadiendo registros en Cloudflare

Una vez se haya realizado esto procederemos a generar el certificado desde Cloudflare, para posteriormente asociar la key y el cuerpo que este nos genere a un listener en el load balancer.

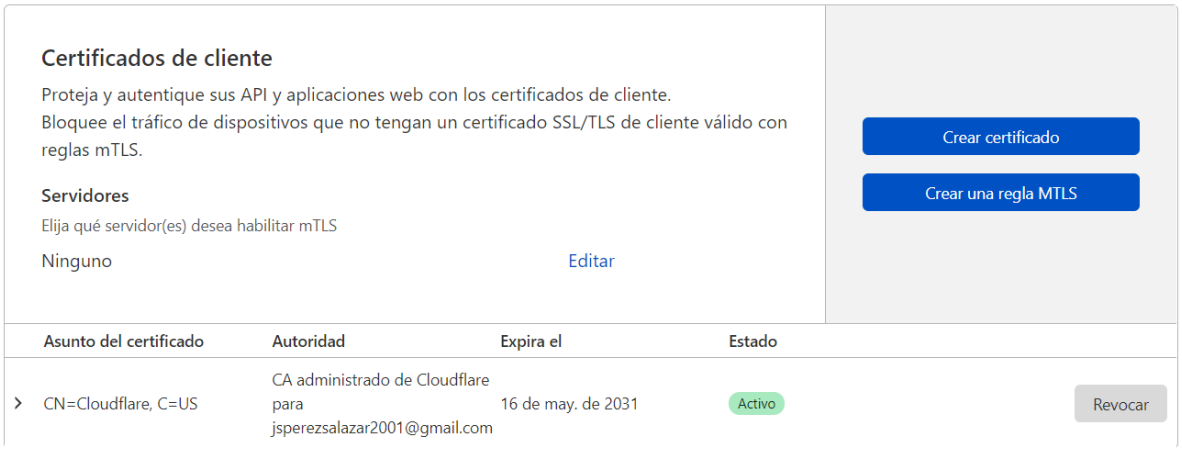

Imagen 40 - Generación del certificado SSL

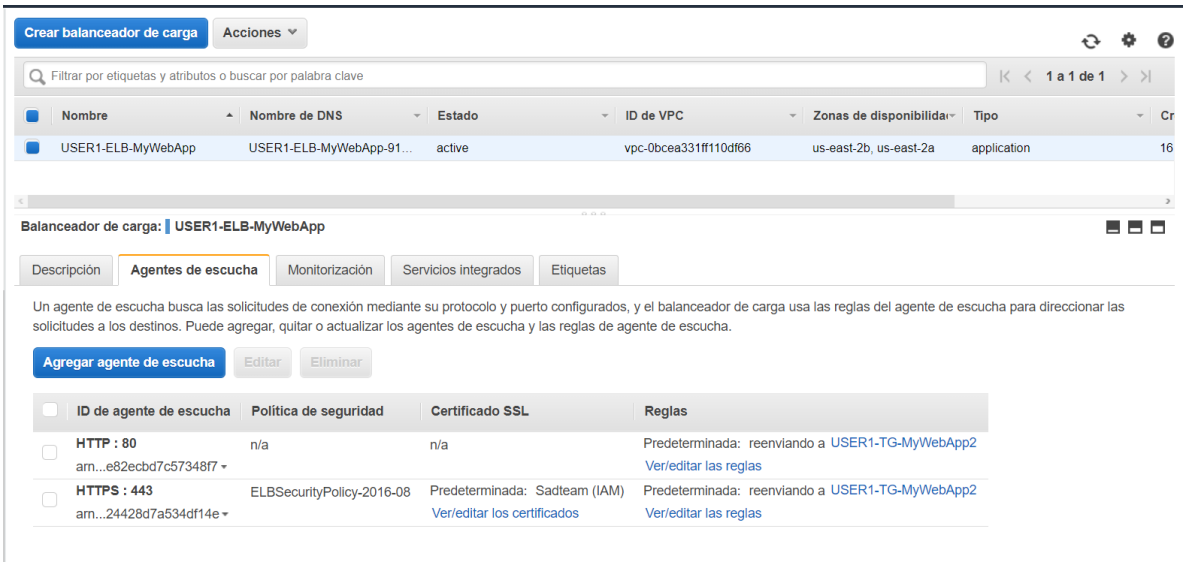

Imagen 41 - Asociando el certificado SSL a un listener en el LoadBalancer

Como se puede ver en la imagen anterior, el certificado que se generó desde Cloudflare se ha asociado mediante https a el load balancer por el puerto 443. Sin embargo, en este momento la pagina carga sin estilos, puesto que aún falta realizar configuraciones en la instancia del wordpress. Por lo tanto, lo primero que se debe realizar es ingresar al wordpress como administrador y en la pestaña settings, cambiar los atributos Wordpress Address (URL) y Site Address (URL) que contienen el DNS del loadbalancer por nuestro dominio “sadteamproyecto2.tk”.

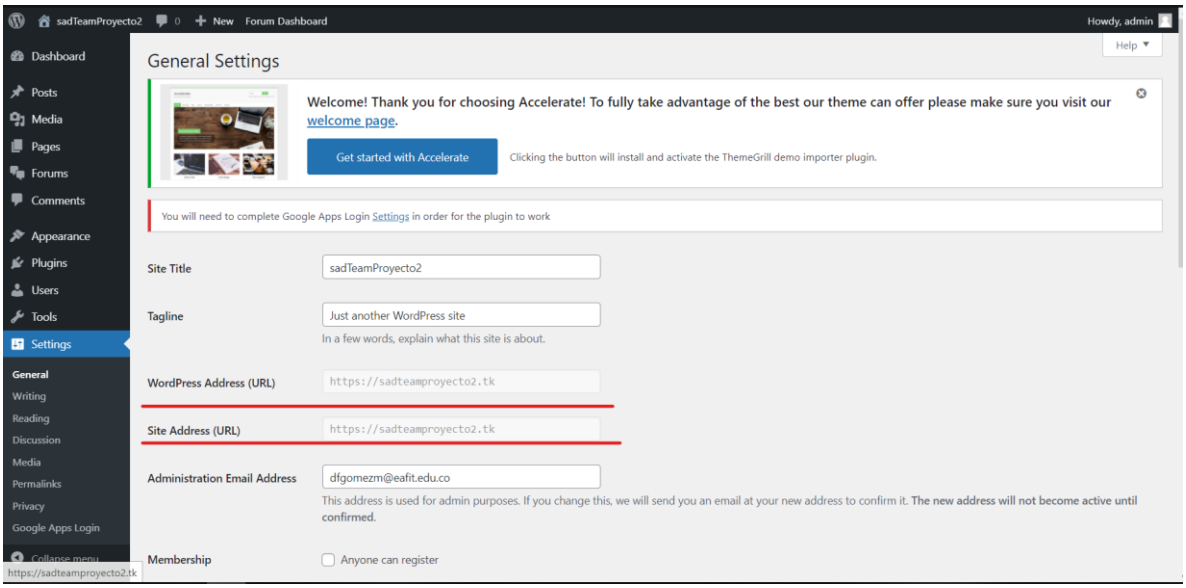

Imagen 42 - Cambiando los atributos para ponerles el nombre del dominio

Posterior a esto, se debe cambiar el archivo /mnt/efs/wordpress/wp-settings.php para inscribir allí los atributos que se cambian en la interfaz gráfica, para ellos agregamos las siguientes líneas en el archivo.

```
*/
define( 'WPINC', 'wp-includes' );
define( 'WP_HOME', 'https://sadteamproyecto2.tk');
define( 'WP_SITEURL', 'https://sadteamproyecto2.tk');
$_SERVER['HTTPS'] = 'on';
/**
```

Imagen 43 - Añadiendo lineas al archivo wp-settings.php para registrar el dominio

Una vez realizado todo este proceso ya se tiene un certificado para el dominio de forma tal que se garantice que la conexión a nuestro aplicativo web es segura.

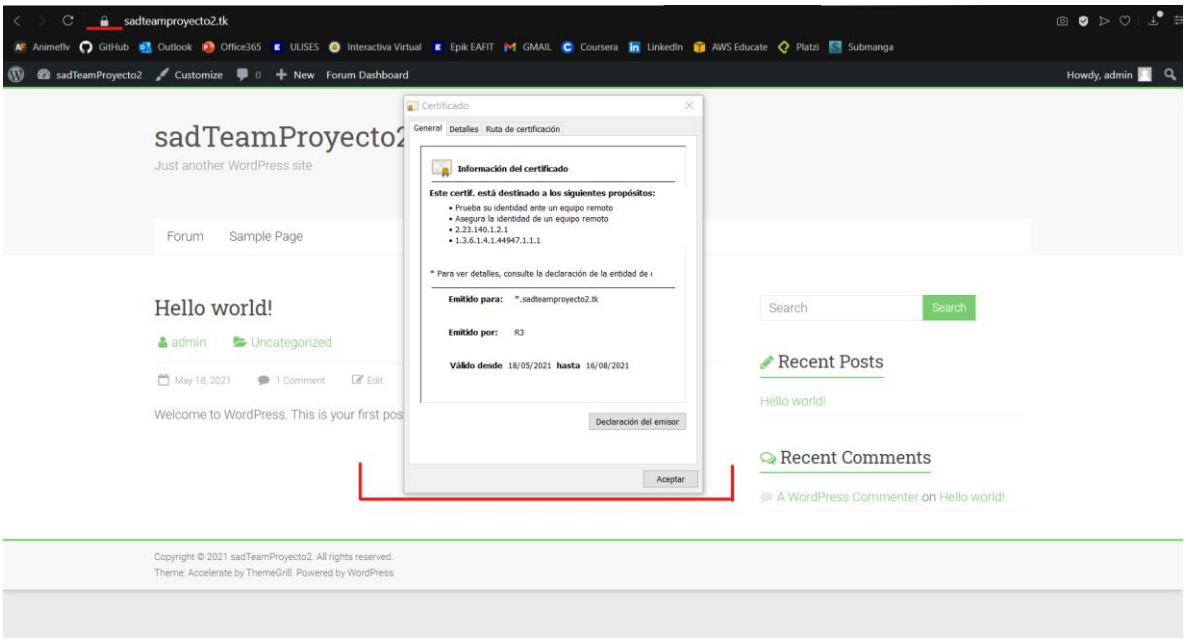

Imagen 44 - Certificado generado y asociado de manera exitosa para el aplicativo web