Desafío #4

Fecha de entrega: 23/10/2024

Objetivo:

El objetivo de este trabajo es poner en práctica todo lo aprendido sobre EC2, VPC y RDS.

Escenario:

Nuestra organización nos ha solicitado crear un nuevo entorno de desarrollo para un nuevo proyecto y debemos generar toda la documentación necesaria para que luego el equipo de implementación lo pueda crear en Staging y producción.

Requisitos:

Amazon RDS es el servicio que facilita la configuración, funcionamiento y escalado de las BD relacionales en AWS. Con éste el BD Admin evita tener que administrar todos los componentes relacionados con este tipo de BD (S.O. del servidor, almacenamiento, copia de seguridad, alta disponibilidad, …).

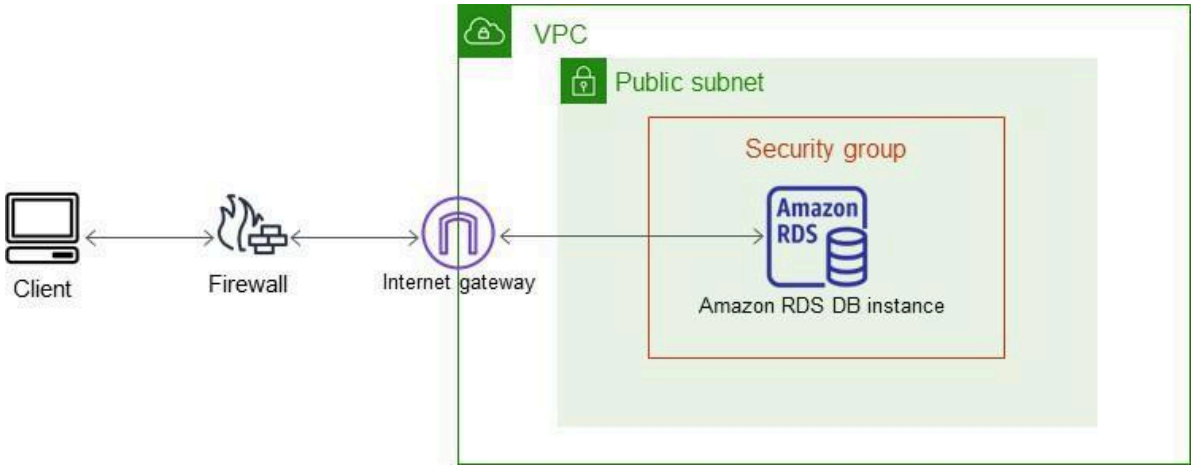
Antes de crear la instancia de la BD, se nos pide realizar una serie de acciones:

1. Crear un usuario IAM con permisos de administrador. Será con este usuario con el que realicemos el resto del tutorial. Amazon aconseja no usar nunca el usuario raíz, salvo ocasiones puntuales, y guardar en lugar seguro sus credenciales.

2. La instancia de BD se creará en una VPC (Virtual Private Cloud). Por lo tanto, también será necesario definir las reglas de grupo de seguridad para tener acceso a esta VPC, (que seguramente será del tipo EC2-VPC).

3. Aquí debe consultar la configuración necesaria para el escenario elegido para el acceso a una instancia de BD situada en una VPC.

4. Para el caso que nos ocupa elegiremos el escenario con la instancia de BD en una VPC y una aplicación cliente a través de Internet.



SOLUCIÓN

[JORGE: Dado que el planteo del desafío incluye los pasos a seguir a detalle no voy a reescribir el documento. Adjunto las capturas de completitud de la tarea asignada en cada paso y prueba de conectividad.]

Crear la VPC

Ahora deberá crear una VPC para utilizarla con una instancia de base de datos, con la configuración descrita en el punto anterior:

- Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
- En la esquina superior derecha de la Consola de administración de AWS, elija la región en la que desea crear la VPC.
- En la esquina superior izquierda, elija VPC Dashboard. Para comenzar a crear una VPC, elija Launch VPC Wizard (Lanzar asistente de VPC).

a. En la página Step 1: Select a VPC Configuration, elija VPC with a Single Public Subnet y, a continuación, elija Select.

b. En la página Step 2: VPC with Public Subnet, establezca estos valores:

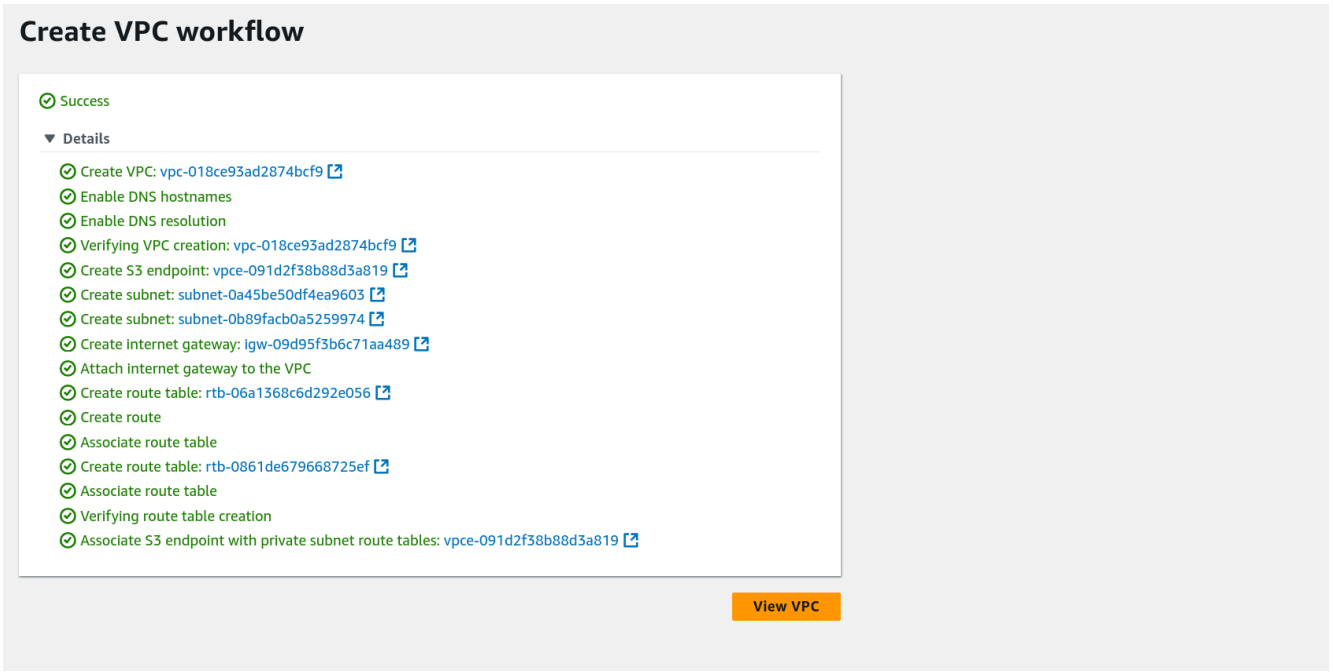
- IPv4 CIDR block: 10.0.0.0/16
- IPv6 CIDR block: No IPv6 CIDR Block
- VPC name: tutorial-vpc
- Public subnet's IPv4 CIDR: 10.0.0.0/24
- Availability Zone: No preference
- Public subnet name: Tutorial public

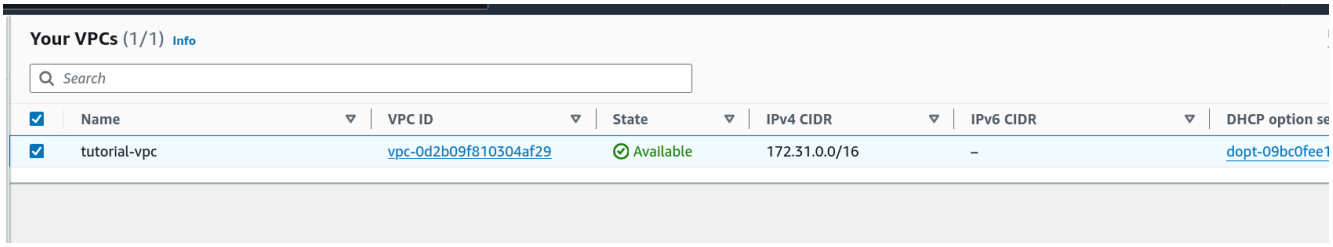
c. Cuando haya terminado, elija Create VPC.

Al ejecutar el *wizard* se crean los siguientes objetos:

- VPC
- Subnet
- Route Tables
- Internet Gateway
- Network ACL
- Security Group

[JORGE: VPC Setup]





Configurar el Security Group

Vaya al apartado **Security Groups** y seleccione el grupo que ha creado (asociado al nuevo VPC). Después seleccione **Inbound rules** del grupo. Le aparecerá con este tipo de configuración:

Type	Protocol	Port range	Source
All traffic	All	All	sg-d57b5896 (default)

La configuración por defecto sólo permite la conexión al VPC desde componentes que usen el mismo *Security Group*. Como queremos conectarnos a la BD desde cualquier punto de Internet deberemos modificar el valor de la propiedad *Source*:

a. Edite **Inbound rules**.

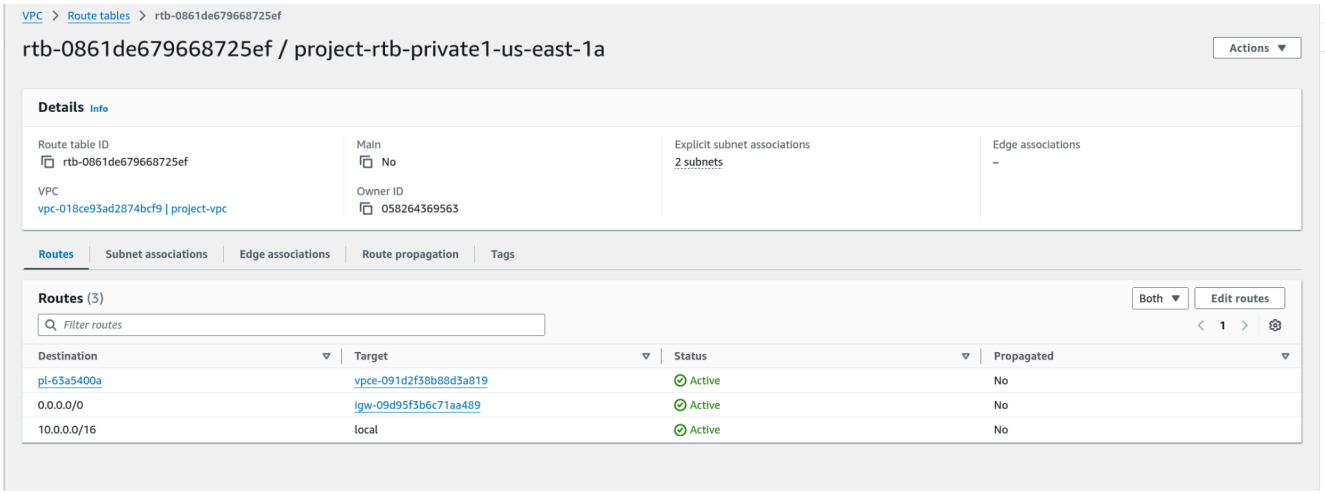
b. En el campo *Source* seleccione la opción 0.0.0.0/0.

c. Pulse el botón **Save rules**.

Si quisiera limitar la conexión a la BD sólo a su equipo u otros de confianza, debería poner en el campo *Source* las IP de estos equipos. De esta forma la configuración quedaría asi:

Type	Protocol	Port range	Source
MYSQL/Aurora	TCP	3306	56.176.2.108/32

[JORGE: Diagrama final RouteTable]



Crear las subredes adicionales

Debe tener dos subredes privadas o dos subredes públicas disponibles para crear un grupo de subredes de base de datos para que lo utilice una instancia de base de datos en una VPC. Debido a que la instancia de base de datos de este tutorial es pública, debe añadir una segunda subred pública a la VPC:

- Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

- Para añadir la segunda subred privada a la VPC, elija VPC Dashboard (Panel VPC), seguido de Subnets (Subredes) y, por último, Create Subnet (Crear subred).

- En la página Create Subnet (Crear subred), defina estos valores:

- Name tag: **Tutorial private 2**
- VPC: elija la VPC que creó anteriormente, por ejemplo: **vpc-identifier (10.0.0.0/16) - tutorial-vpc**.
- Availability Zone: **us-west-2b**

  Elija una zona de disponibilidad que sea distinta de la que eligió para la primera subred pública.

- IPv4 CIDR block: **10.0.2.0/24**

- Cuando haya terminado, elija Create (Crear). A continuación, seleccione Close (Cerrar) en la página de confirmación.

- Para asegurarse de que la segunda subred privada utiliza la misma tabla de enrutamiento que la primera subred privada, realice los pasos que se muestran a continuación:

a. Elija Panel de VPC, elija Subredes y, a continuación, elija la primera subred privada que creó para la VPC, Tutorial private 1.

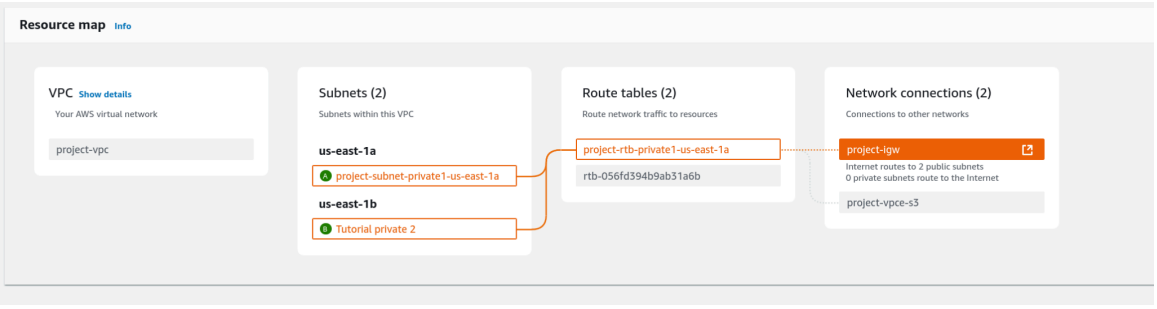
b. Debajo de la lista de subredes, elija la pestaña Route Table (Tabla de enrutamiento) y anote el valor de Route Table (Tabla de enrutamiento), por ejemplo: **rtb-98b613fd**.

c. En la lista de subredes, anule la selección de la primera subred privada.

d. En la lista de subredes, elija la segunda subred privada Tutorial private 2 y elija la pestaña Tablas de ruteo.

e. Si la tabla de ruteo actual no es la misma que la tabla de ruteo de la primera subred privada, seleccione Edit route table association (Editar asociación de tabla de ruteo). En Route Table ID (ID de tabla de ruteo), elija la tabla de enrutamiento que anotó anteriormente, por ejemplo: **rtb-98b613fd**. A continuación, para guardar lo que ha seleccionado, elija Save (Guardar).

[JORGE: Diagrama final VPC/Subnet/IGW]



Crear un grupo de subredes de base de datos

Un grupo de subredes de base de datos es una colección de subredes que se crean en una VPC y que después se asignan a las instancias de bases de datos. Un grupo de subredes de base de datos le permite especificar una VPC específica al crear instancias de bases de datos.

Para crear un grupo de subredes de base de datos Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.

> Asegúrese de conectarse a la consola de Amazon RDS, no a la consola de Amazon VPC.

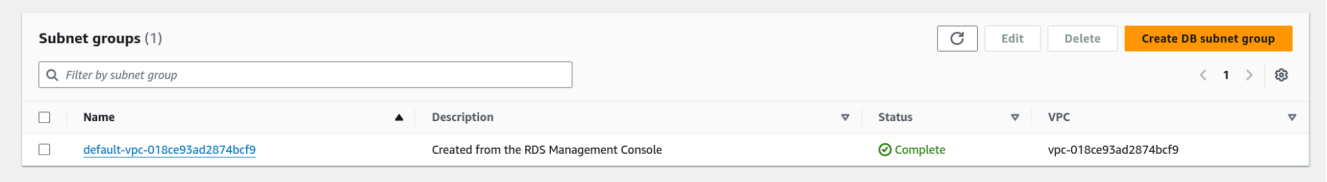
- En el panel de navegación, elija **Subnet groups**.
- Elija **Create DB Subnet Group**.
- En la página Create DB subnet group (Crear grupo de subredes de base de datos), establezca estos valores en Subnet group details (Detalles del grupo de subredes):

- Name: tutorial-db-subnet-group
- Description: Tutorial DB Subnet Group
- VPC: tutorial-vpc (vpc-identifier)

- En la sección Agregar subredes elija las Zonas de disponibilidad y Subredes.
- En este tutorial, elija **us-west-2a y us-west-2b** para las Zonas de disponibilidad. A continuación, elija todas las subredes para Subredes.

  Si ha habilitado una zona local, puede elegir un grupo de zonas de disponibilidad en la página Create DB subnet group (Crear grupo de subredes de base de datos). En este caso, elija Availability Zone group (Grupo de zonas de disponibilidad), Availability Zones (Zonas de disponibilidad)y Subnets (Subredes).

- Seleccione Create. El nuevo grupo de subredes de base de datos aparece en la lista de grupos de subredes de base de datos de la consola de RDS.



Crear la instancia de base de datos en la VPC

1. Abra la consola de Amazon RDS en https://console.aws.amazon.com/rds/.
2. Seleccionamos la región en la que queremos crear la instancia de BD (esquina superior derecha). Esta región deberá ser la misma en la que se creó la VPC.

3. Seleccione **Databases**.

4. Pulsamos el botón **Create database**.

5. Usaremos la opción **Standard Create**, que permite seleccionar la VPC, además de configuraciones como disponibilidad, seguridad, copias de seguridad y mantenimiento. La opción **Easy Create** siempre utilizará la VPC por defecto, por lo que en nuestro caso no nos sirve.

6. Engine Type: Seleccionamos el motor de BD que vayamos a utilizar en esta instancia. En nuestro caso **MariaDB**. Si quisiera instalar una instancia de BD **MySql** debería seleccionar ésta en vez de MariaDB.

7. DB instance size: Seleccionamos **Free tier** para economizar gastos.

8. Indicamos un nombre para la instancia de BD y el nombre del usuario administrador de la BD.

9. Pulsamos en **Auto generate a password**. Cuando creemos la BD nos mostrará en ese único momento la contraseña, que deberemos guardar. Si desea indicar manualmente una contraseña desmarque esta opción.

10. Las siguientes opciones las dejaremos como aparecen por defecto.

11. En **Connectivity** seleccionamos la VPC que hemos creado en el apartado anterior. Y desplegamos **Additional connectivity configuration**.

12. Seleccionamos el **Subnet group** que hemos creado anteriormente.

13. En **Public access** seleccionamos **Yes** para que podamos acceder a la BD desde cualquier equipo en Internet.

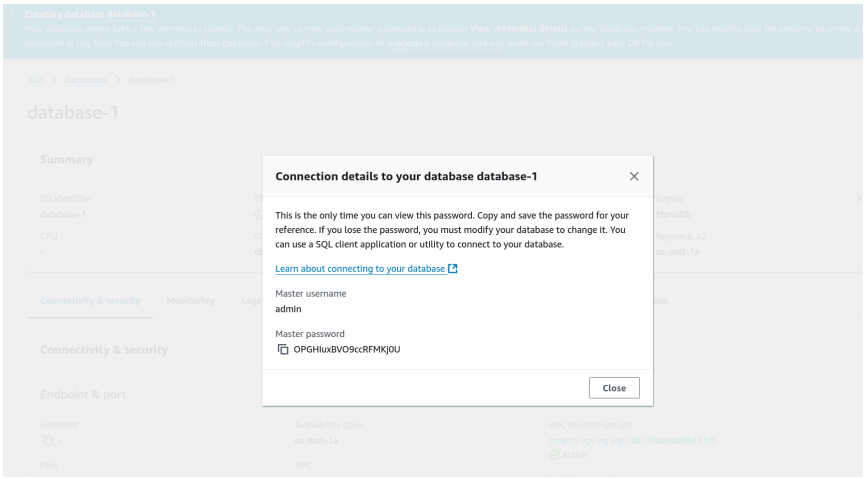
14. Las siguientes opciones las dejaremos como aparecen por defecto.

15. Pulsamos el botón **Create database** al final de la página.

16. Pulsamos el botón **View credential details**. Se abrirá una ventana para ver:

- La contraseña creada para el usuario administrador.
- La dirección (*Endpoint*) de la instancia a la que nos conectaremos con nuestro cliente.

[JORGE: Mensaje final del alta de RDS (la base de datos ya ha sido desprovisionada las credenciales no funcionarán)]



Comprobar el acceso a la instancia

Una vez creada la instancia, podremos comprobar que accedemos a ella mediante cualquier cliente instalado en nuestra máquina. Por ejemplo mediante el comando **mariadb** de la consola:

> Suponemos que el *Endpoint* que nos ha creado es **mariadbinstancia.skdimeitllwst.us-west-1.rds.amazonaws.com**

$ mariadb -h mariadbinstancia.skdimeitllwst.us-west-1.rds.amazonaws.com -u username -p password

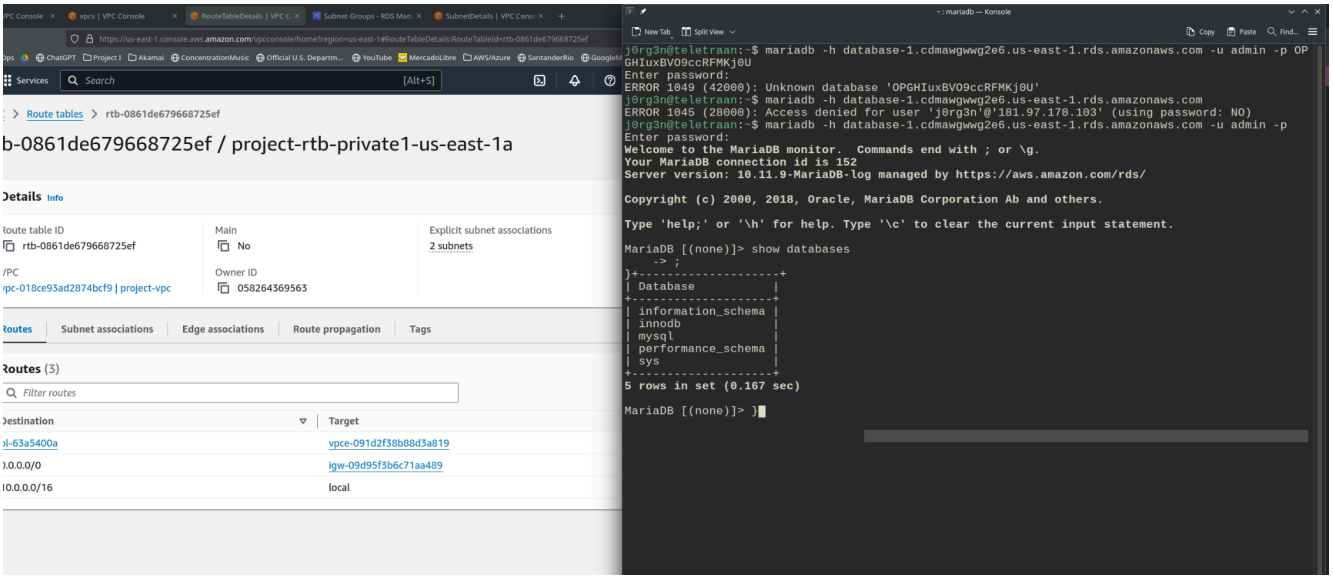
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 60

Server version: 10.1.34-MariaDB MariaDB Server
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement. MariaDB [(none)]> show databases;

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| innodb             |
| mysql              |
| performance_schema |
+--------------------+
4 rows in set (0.05 sec)

MariaDB [(none)]>
```

[JORGE: Prueba de conexion]



Posibles problemas

Route Tables

Desde AWS VPC, vaya a **Route Tables** y compruebe que la *Route table* asociada a la VPC de la BD tiene asociadas las dos *Subnets* creadas, y en *Main* indica **Yes**.

Otros errores

Si ha tenido otros problemas para conectarse a la instancia, en esta página puede consultar algunas soluciones propuestas por AWS.

Mejorar la seguridad

En este tutorial hemos sugerido el uso del *Security Group* como *firewall* para limitar la conexión a la IP de nuestro equipo. Sin embargo, si la BD sólo necesitará estar expuesta a otro componente dentro de AWS (p.e. un servidor HTTP), es posible aumentar su seguridad utilizando una *subnet* privada y un servidor SSH dentro de la misma VPC para acceder a la BD a través de éste.

Entregables:

1. Un documento con los pasos necesarios para resolver el desafío (puede documentar usando los comandos de AWS CLI).
2. Realizar un diagrama detallado de toda la solución y cada uno de sus componentes.

Evaluación:

- Entrega en fecha.
- Redactar documentación legible y que sea comprendida por terceros.
- Añade material de soporte adicional.
    - Ejemplo: Diagrama de alto nivel.
- Cumple con las consignas solicitadas.
- El entregable es funcional.
    - Ejemplo: el script bash al ejecutarse funciona sin errores y realiza lo solicitado.