

## Desafío #4

### 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.

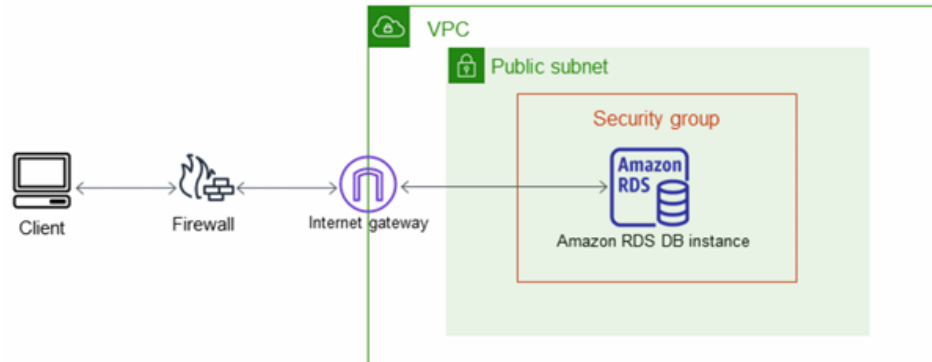
### Requisitos:

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.



## Paso 1: Creación de VPC;

###

### 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:

- 1- Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
- 2- En la esquina superior derecha de la Consola de administración de AWS, elija la región en la que desea crear la VPC.
- 3- 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:
    - IPv4CIDRblock: 10.0.0.0/16

- IPv6CIDRblock: No IPv6 CIDR Block
- VPCname: 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
- RouteTables
- Internet Gateway
- Network ACL
- Security Group

###

*Valores establecidos;*

*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*

## Flujo de trabajo de creación de VPC

✔ Correcto

### ▼ Detalles

- ✔ Crear VPC: [vpc-024000b1731e11aea](#)
- ✔ Habilitar nombres de host DNS
- ✔ Habilitar la resolución de DNS
- ✔ Verificar la creación de una VPC: [vpc-024000b1731e11aea](#)
- ✔ Crear punto de enlace de S3: [vpce-0de2866dd84d23f6f](#)
- ✔ Crear subred: [subnet-065e4e9548f263d70](#)
- ✔ Crear subred: [subnet-0a8c1a6c2e1526a17](#)
- ✔ Crear una gateway de Internet: [igw-0f316b2b121874b8f](#)
- ✔ Adjuntar gateway de Internet a la VPC
- ✔ Crear tabla de enrutamiento: [rtb-03a434c71ae968863](#)
- ✔ Crear ruta
- ✔ Asociar tabla de enrutamiento
- ✔ Crear tabla de enrutamiento: [rtb-09bed50c23a18c391](#)
- ✔ Asociar tabla de enrutamiento
- ✔ Verificando la creación de la tabla de enrutamiento
- ✔ Asociar el punto de conexión de S3 con tablas de enrutamiento de subred privada: [vpce-0de2866dd84d23f6f](#)

## Paso 2: Configurar 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; All Traffic - Protocol; All - Port Range; All - Source; 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:

- Edite Inbound rules.
- En el campo Source seleccione la opción 0.0.0.0/0.
- 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.

###

*Configuración utilizada;*

*Type; All traffic*

*Protocol; All*

*Port Range; All*

*Source; 0.0.0.0/0*

Reglas de entrada (1)									
<input type="text" value="Buscar"/>									
<input type="checkbox"/>	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen		Descripción
<input type="checkbox"/>	-	sgp-04f91decc635432af	IPv4	Todo el tráfico	Todo	Todo	0.0.0.0/0		-

## Paso 3: Creación de subred;

###

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.

- IPv4CIDRblock: 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).

###

*\*Aclaración; Se utilizó el name tag "Tutorial private 2" dado que así indicaban los valores a definir, pero el objetivo de este paso era generar una subnet pública.*

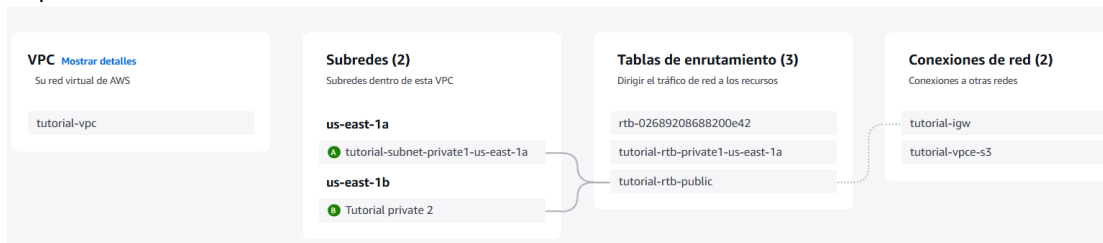
*Valores;*

*Name tag; Tutorial Private 2*

*VPC: tutorial-vpc*

*Availability Zone: us-east-2b*

*IPv4 CIDR Block: 10.0.2.0/24*



## Paso 4: Creación de DB Subnet Group

###

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.

● Enestetutorial, 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.

###

#### tutorial-db-subnet-group

##### Detalles del grupo de subredes

ID de VPC

[vpc-024000b1731e11aea](#) 

ARN

[arn:aws:rds:us-east-1:038462755082:subgrp:tutorial-db-subnet-group](#)

Tipos de red compatibles

IPv4

Descripción

Tutorial DB Subnet Group

##### Subredes (2)

Zona de disponibilidad	Nombre de subred	ID de subred	Bloque de CIDR
us-east-1b	Tutorial private 2	<a href="#">subnet-0a02fa11f7a95d050</a> 	10.0.2.0/24
us-east-1a	tutorial-subnet-private1-us-east-1a	<a href="#">subnet-0a8c1a6c2e1526a17</a> 	10.0.128.0/20

## Paso 5; Creación 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. DBinstance 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.

###

Bases de datos (1)							
<input type="text" value="Filtrar por bases de datos"/>							
<input type="checkbox"/> Identificador de base de datos	Estado	Rol	Motor	Región ...	Tamaño	Recomend	
<input type="radio"/> <a href="#">database-1</a>	🟢 Disponible	Instancia	MariaDB	us-east-1a	db.t4g.micro		

## Paso 6; Comprobación de 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.sktimeitllwst.us-west-1.rds.amazonaws.com

```
$ mariadb-h mariadbinstancia.sktimeitllwst.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.

###

*Comandos utilizados;*

*\$ mariadb -h database-1.c5is6qskcsb.us-east-1.rds.amazonaws.com -P 3306 -u admin -p {password}*

*Dentro de la DB;*

*\$ MariaDB [(none)]> show databases;*

The screenshot displays the AWS RDS console interface on the left and a terminal window on the right. The console shows the 'Conectividad y seguridad' (Connectivity and security) tab for an RDS instance. It lists the endpoint as 'database-1.c5is6qskcsb.us-east-1.rds.amazonaws.com' and the port as '3306'. The 'Redes' (Network) section shows the instance is in 'us-east-1a' availability zone, using 'tutorial-vpc (vpc-024...)' and 'tutorial-db-subnet-gr...' subnets. The terminal window on the right shows a user running the command 'mariadb -h database-1.c5is6qskcsb.us-east-1.rds.amazonaws.com -P 3306 -u admin -p {password}'. The terminal output shows a successful connection to the MariaDB instance, displaying the MariaDB monitor welcome message and the server version '11.4.4-MariaDB-Log managed by https://aws.amazon.com/rds/'. The user then enters 'show databases;' and the output shows 'Database' with a list of databases: 'information\_schema', 'innodb', 'mysql', 'performance\_schema', and 'sys'.

## 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