



## DESAFIO 4

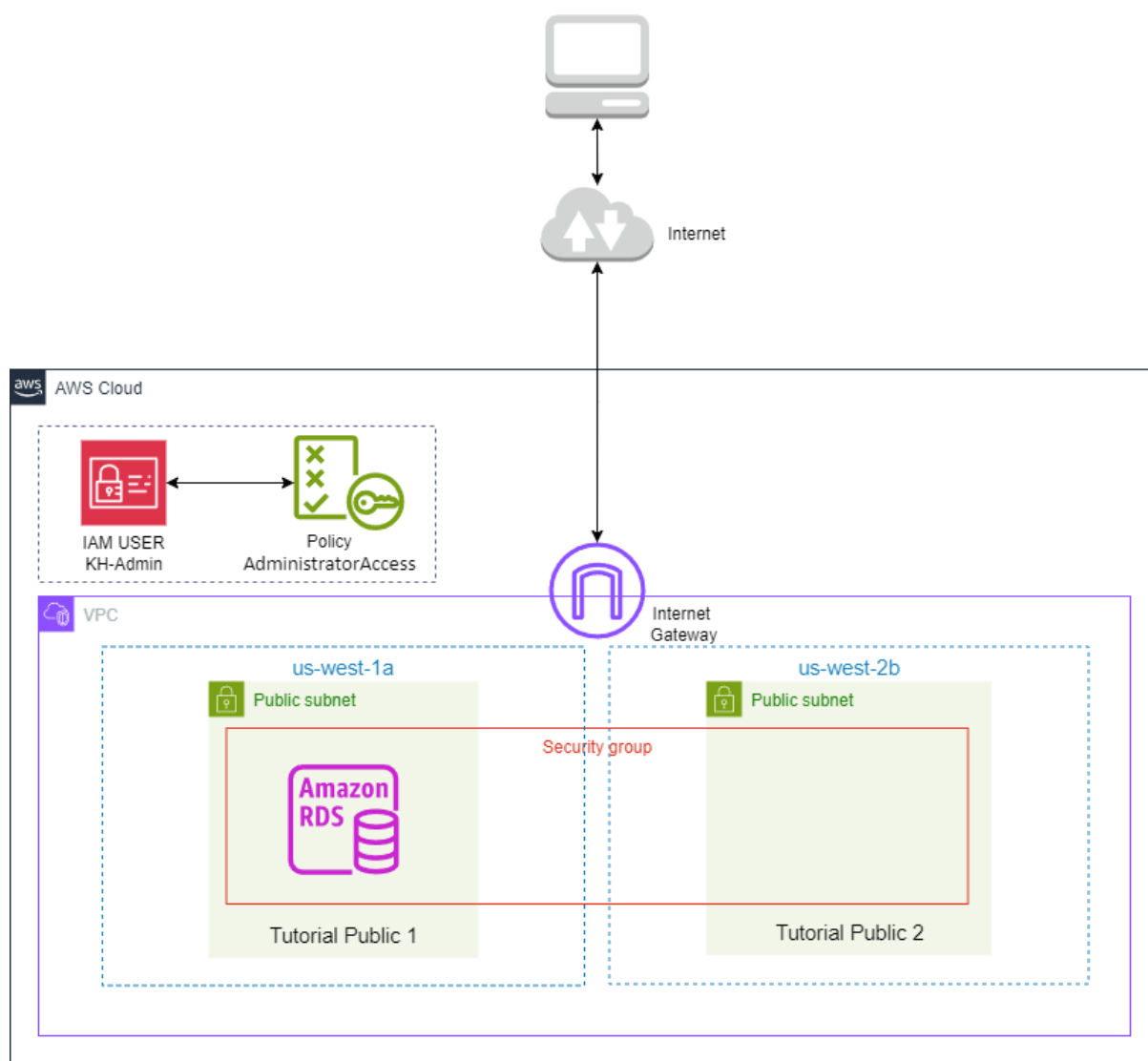
Kevin Damian Hidalgo – 99405

<b>1. Introducción.....</b>	<b>3</b>
<b>2. Crear un usuario IAM con permisos de administrador.....</b>	<b>4</b>
<b>3. Crear una VPC para la instancia de la base de datos .....</b>	<b>6</b>
<b>4. Configurar el grupo de seguridad (Security Group) .....</b>	<b>7</b>
<b>5. Crear subredes adicionales .....</b>	<b>8</b>
<b>6. Crear el grupo de subredes de base de datos .....</b>	<b>8</b>
<b>7. Crear la instancia de base de datos .....</b>	<b>9</b>
<b>8. Comprobar el acceso a la instancia .....</b>	<b>10</b>
<b>9. Mejoras sobre la arquitectura para mayor seguridad.....</b>	<b>10</b>
<b>9.1. Creación de Grupos de Trabajo (IAM Role) .....</b>	<b>11</b>
<b>9.2. Creación de Subnet Pública y Privada .....</b>	<b>11</b>
<b>9.2.1. Crear la VPC .....</b>	<b>12</b>
<b>9.2.2. Crear subredes adicionales.....</b>	<b>12</b>
<b>9.2.3. Configurar las tablas de enrutamiento (Route Tables).....</b>	<b>13</b>
<b>9.2.4. Configurar el Security Group para la instancia EC2 .....</b>	<b>13</b>
<b>9.2.5. Configurar el Security Group para RDS .....</b>	<b>14</b>
<b>9.2.6. Crear la instancia RDS en la Subnet Privada .....</b>	<b>14</b>
<b>9.2.7. Probar la conectividad.....</b>	<b>14</b>

# 1. Introducción

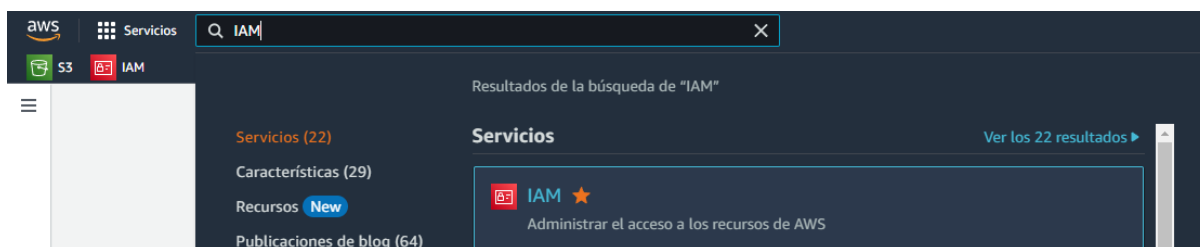
Este documento describe el proceso detallado para la creación de un entorno de base de datos relacional en Amazon Web Services (AWS) utilizando Amazon RDS (Relational Database Service) y otros componentes de AWS como VPC (Virtual Private Cloud), Subnets, y Security Groups.

El ejercicio cubre la configuración de una base de datos MariaDB dentro de un entorno aislado en una VPC personalizada, garantizando conectividad segura y controlada a través de un grupo de seguridad y subredes. Además, se asegura que la instancia de base de datos esté disponible para acceso público de acuerdo con los requisitos de desarrollo y pruebas. El proceso es aplicable a entornos de desarrollo y preparación para producción, donde la automatización y el control de recursos en la nube son esenciales para la escalabilidad y seguridad de las aplicaciones.

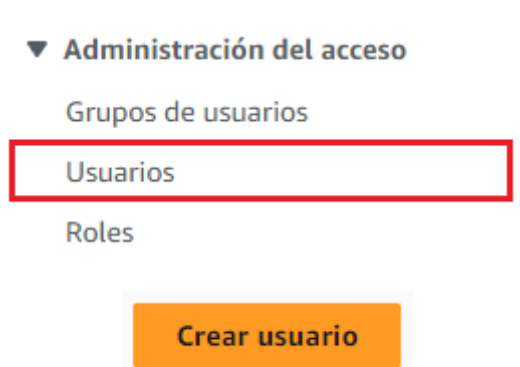


## 2. Crear un usuario IAM con permisos de administrador

En la barra de búsqueda escribe IAM y accede a la búsqueda correspondiente



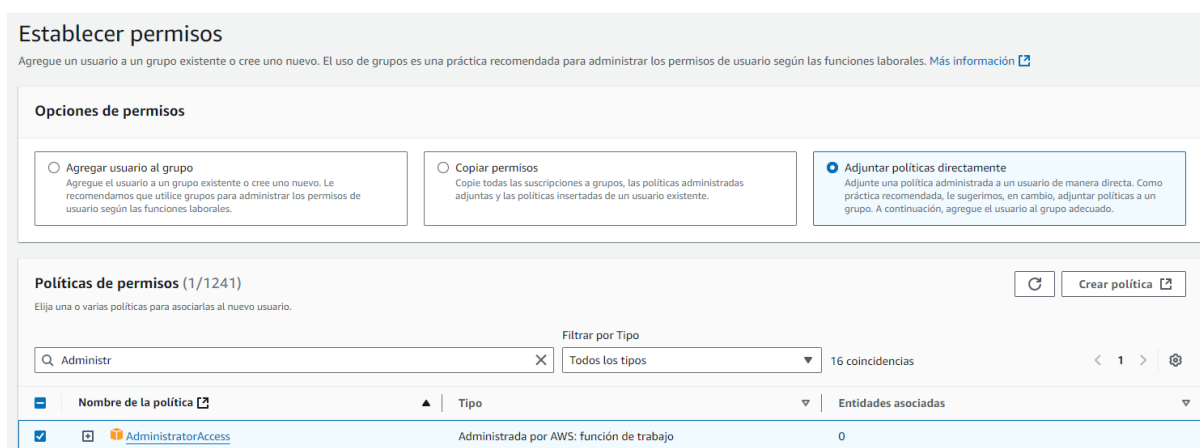
En el panel izquierdo de IAM, seleccione "Usuarios" y luego haga clic en "Crear usuario".



Ingresa **KH-Admin** como nombre de usuario.

Puede marcar la casilla **Acceso a la consola de administración de AWS** por si desea darle permisos de acceso a AWS CLI (es Opcional).

En **Establecer permisos**, elija **Adjuntar políticas directamente**, luego busque y seleccione la casilla de **AdministratorAccess**.



Una vez presionado Continuar te dará un detalle de cómo está configurado el Usuario previo a la creación.

Presiona **Crear** una vez validado que este correcto.

**Usuarios (1)** Información

Un usuario de IAM es una identidad con credenciales válidas a largo plazo que se utiliza para interactuar con AWS en una cuenta.

<input type="checkbox"/>	Nombre de usuario ▲	Ruta ▼	Grupo! ▼	Última actividad ▼
<input type="checkbox"/>	<a href="#">KH-Admin</a>	/	0	-

Una vez creado el usuario, se debe acceder al usuario creado y hacer clic en la opción **Crear clave de Acceso** ya que dicho usuario no posee credenciales para ser utilizado.

Clave de acceso 1

[Crear clave de acceso](#)

Se tendrá que seleccionar el tipo de **Prácticas recomendadas y alternativas para la clave de acceso** para las credenciales que se crearán.

En nuestro caso se le permitirá acceso a **Aplicación ejecutada en un servicio de computación de AWS**.

☒ Aplicación ejecutada en un servicio de computación de AWS

Tiene previsto utilizar esta clave de acceso para permitir que el código de aplicación que se ejecuta en un servicio de computación de AWS como Amazon EC2, Amazon ECS o AWS Lambda obtenga acceso a su cuenta de AWS.

Se presionara Siguiente, y te dará como opcional cargar **Establecer el valor de etiqueta de descripción** del objetivo de dicha clave de acceso.

En mi caso le colocare la siguiente descripción.

Crear clave de acceso

Valor de etiqueta de descripción

Describe el objetivo de esta clave de acceso y dónde se utilizará. Una buena descripción lo ayudará a rotar esta clave de acceso con confianza más adelante.

Máximo de 256 caracteres. Los caracteres permitidos son letras, números, espacios representables en UTF-8 y: \_ . : / = + - @

Hacer Clic en el botón **Crear Clave de Acceso**

Se generara unas credenciales las cuales se deben resguardar en algún lugar seguro, ya que serán necesarias para realizar los próximos pasos, se pueden descargar en un archivo CSV.

## Recuperar claves de acceso [Información](#)

**Clave de acceso**  
Si pierde u olvida la clave de acceso secreta, no podrá recuperarla. En su lugar, cree una nueva clave de acceso y deje inactiva la antigua.

Clave de acceso	Clave de acceso secreta
-----------------	-------------------------

Una vez presionado Listo, se finalizara la creación de las credenciales y se podrá visualizar en la pestaña **Credenciales de Seguridad** dicha credencial creada.

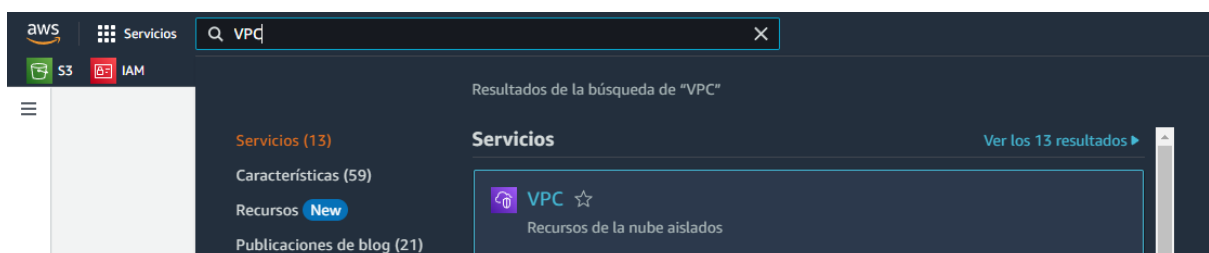
Claves de acceso (1) <a href="#">Crear clave de acceso</a>	
Utilice las claves de acceso para enviar llamadas mediante programación a AWS desde AWS CLI, Herramientas de AWS para PowerShell, AWS SDK o llamadas directas a la API de AWS. Puede tener un máximo de dos claves de acceso (activas o inactivas) a la vez. <a href="#">Más información</a>	
<b>AKIAYM7POCWYLOXP64IJ</b> Descripción Usuario Admin creado para administrar el Desafío 4 Último uso Ninguno Última región utilizada N/A	<b>Estado</b> Active <b>Creado</b> hace 2 minutos <b>Último servicio utilizado</b> N/A

### 3. Crear una VPC para la instancia de la base de datos

Se creara una VPC (Virtual Private Cloud) la cual contendrá una Base de Datos de tipo RDS (Relational Database Service).

Para esto se deberán realizar los siguientes pasos:

En la barra de búsqueda escribe VPC y accede a la búsqueda correspondiente.



Una vez ingresado, haz clic en la opción **Create VPC** (Crear VPC).

**Crear VPC**

De los 2 tipos de VPC, elige la opción **VPC y más** y define:

- **IPv4 CIDR block:** 10.0.0.0/16

#### Bloque de CIDR IPv4 [Información](#)

Determine la IP inicial y el tamaño de la VPC mediante la notación CIDR.

10.0.0.0/16	65,536 IPs
-------------	------------

El tamaño del bloque CIDR debe estar entre /16 y /28.

- **Subnet IPv4 CIDR:** 10.0.0.0/24

### ▼ Personalizar bloques de CIDR de subredes

Bloque de CIDR de la subred pública en us-west-2a

10.0.0.0/24

256 IPs

- **Nombre de la VPC:** tutorial-vpc  
Se puede definir en **Generación automática de etiquetas de nombre** (este establece un formato de nombre para el resto de los componentes a crear) o crear una etiqueta Name = tutorial-vpc.
- **Nombre de la Subnet pública:** Tutorial public  
Si no está marcado la opción **Generar automáticamente** se puede setear el valor correspondiente, de lo contrario se puede editar una vez creada.

Una vez configurado todo, hacer clic en **Create** (Crear).

Esta configuración creará automáticamente:

- Una VPC
- Una subred
- Un Internet Gateway (IGW)
- Tablas de enrutamiento, ACLs de red, y un Security Group.

## 4. Configurar el grupo de seguridad (Security Group)

En la interfaz de VPC, accede a la opción **Security Group** (Grupo de Seguridad) que se encuentra en la sección **Security** (Seguridad) del menú izquierdo asociado a la VPC.

### ▼ Seguridad

ACL de red

Grupos de seguridad

Modifica las reglas Inbound (entrante):

Editar reglas de entrada

Cambia la propiedad Source a 0.0.0.0/0 si deseas permitir el acceso desde cualquier lugar por Internet.

Reglas de entrada (1)									
<input type="text" value="Buscar"/>									
<input type="checkbox"/>	Name	ID de la regla del gru...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen		Descr...
<input type="checkbox"/>	-	sgr-0634dc54756b9bd8c	IPv4	Todo el tráfico	Todo	Todo	0.0.0.0/0		-

Si te retorna un mensaje de error al setear el origen en 0.0.0.0/0 la forma de solucionarlo es ir a EC2, acceder a **Security Group** (Grupos de Seguridad) en la sección de **Red y Seguridad**, seleccionar el grupo a modificar y acceder a la pestaña **Reglas de Entrada** para **Editar Reglas de Entrada**.

Tendrás que eliminar la regla que existe y crear una nueva especificando El origen deseado.

## 5. Crear subredes adicionales

Añade una segunda subred para alta disponibilidad:

En la consola de VPC, selecciona **Create Subnet** (Crear Subred).

Define:

- Nombre: Tutorial public 2
- Pv4 CIDR: 10.0.2.0/24
- Zona de disponibilidad: us-west-1b

Subredes (2) Información										
Find resources by attribute or tag										
<input type="checkbox"/>	Name	ID de subred	Estado	VPC	CIDR IPv4	CIDR...	ID d...	Direccio...	Zona de disponibilidad	
<input type="checkbox"/>	Tutorial public 2	<a href="#">subnet-082f20e6ae967b8ea</a>	Available	<a href="#">vpc-0355ac4f69ebb2e41</a>   <a href="#">tutorial-vpc</a>	10.0.2.0/24	-	-	250	us-west-2b	
<input type="checkbox"/>	Tutorial public	<a href="#">subnet-0acc80f40388abc7c</a>	Available	<a href="#">vpc-0355ac4f69ebb2e41</a>   <a href="#">tutorial-vpc</a>	10.0.0.0/24	-	-	250	us-west-2a	

Asegúrate de asociar la misma tabla de enrutamiento que la primera subred para mantener la consistencia.


En el caso de que no te permita seleccionar la tabla de enrutamiento, seleccionando la subred y haciendo clic en la pestaña Tabla de Enrutamiento, puedes editarla.

[Editar la asociación de la tabla de enrutamiento](#)

Seleccione la tabla de enrutamiento que desea utilizar (la misma que en la subnet anterior).

### Configuración de la tabla de enrutamiento de subred

ID de subred

 subnet-082f20e6ae967b8ea

ID de tabla de enrutamiento

rtb-0b136f833974f6b28 (tutorial-rtb-public) ▲

Q |

rtb-0cf92b582ec63d9f5  
Tabla de enrutamiento principal

rtb-0b136f833974f6b28 (tutorial-rtb-public)  
Asociada

✓

Confirma los cambios.

## 6. Crear el grupo de subredes de base de datos

En la barra de búsqueda escribe RDS y accede a la búsqueda correspondiente





En la consola de Amazon RDS, selecciona la opción **Subnet Group** (Grupo de subredes) y presionar el boton **Create DB Subnet Group**.

**Crear grupo de subredes de base de datos**

Define los siguientes valores:

- **Nombre:** tutorial-db-subnet-group
- **Descripcion:** Tutorial DB Subnet Group
- **VPC:** tutorial-vpc
- **Subredes:** Asigna las dos subredes públicas creadas en los pasos anteriores.  
Deberás seleccionar las **Zonas de disponibilidad** en las que se encuentran las subredes para poder seleccionar las ya creadas.

## 7. Crear la instancia de base de datos

En la consola de **Amazon RDS**, selecciona **Create Database** (Crear base de Datos).

**Crear base de datos**

Se usara la opción Standard Create y se seleccionara las siguientes configuraciones:

- **Motor de base de datos:** MariaDB.
- **DB Name:** a elección, en mi caso **Tutorial-DB**
- **DB instance size:** Free tier (no genera costo).
- **Usuario administrador:** Indica un nombre (en mi caso **bdtutorial**) y generar una contraseña manualmente.
- **VPC:** Selecciona **tutorial-vpc**.
- **Subnet Group:** Selecciona el grupo de subredes creado anteriormente.
- **Public access:** Yes (para acceso público).

Una vez creada la instancia, guarda las credenciales del usuario administrador.

Bases de datos (1)							
<input type="text" value="Filtrar por bases de datos"/>							
Identificador de base de datos	Estado	Rol	Motor	Región ...	Tamaño	Re	
<a href="#">tutorial-db</a>	Disponible	Instancia	MariaDB	us-west-2a	db.t3.micro		

## 8. Comprobar el acceso a la instancia

Usa un cliente compatible (como mariadb) para conectarte a la base de datos utilizando el endpoint generado.

El Formato del comando es:

```
mysql -h <ID-DataBase> -P <Puerto> -u <Usuario> -p
```

Ejemplo:

```
mysql -h tutorial-db.cpcis2i8ud2b.us-west-1.rds.amazonaws.com -P 3306 -u dbtutorial -p
```

```
[cloudshell-user@ip-10-134-50-65 ~]$ mysql -h tutorial-db.cpcis2i8ud2b.us-west-1.rds.amazonaws.com -p 3306 -u dbtutorial -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 105
Server version: 10.11.9-MariaDB-log managed by https://aws.amazon.com/rds/

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)]> █
```

Una vez ingresado si todos los pasos realizados están bien realizados se debe realizar el comando:

```
SHOW DATABASES;
```

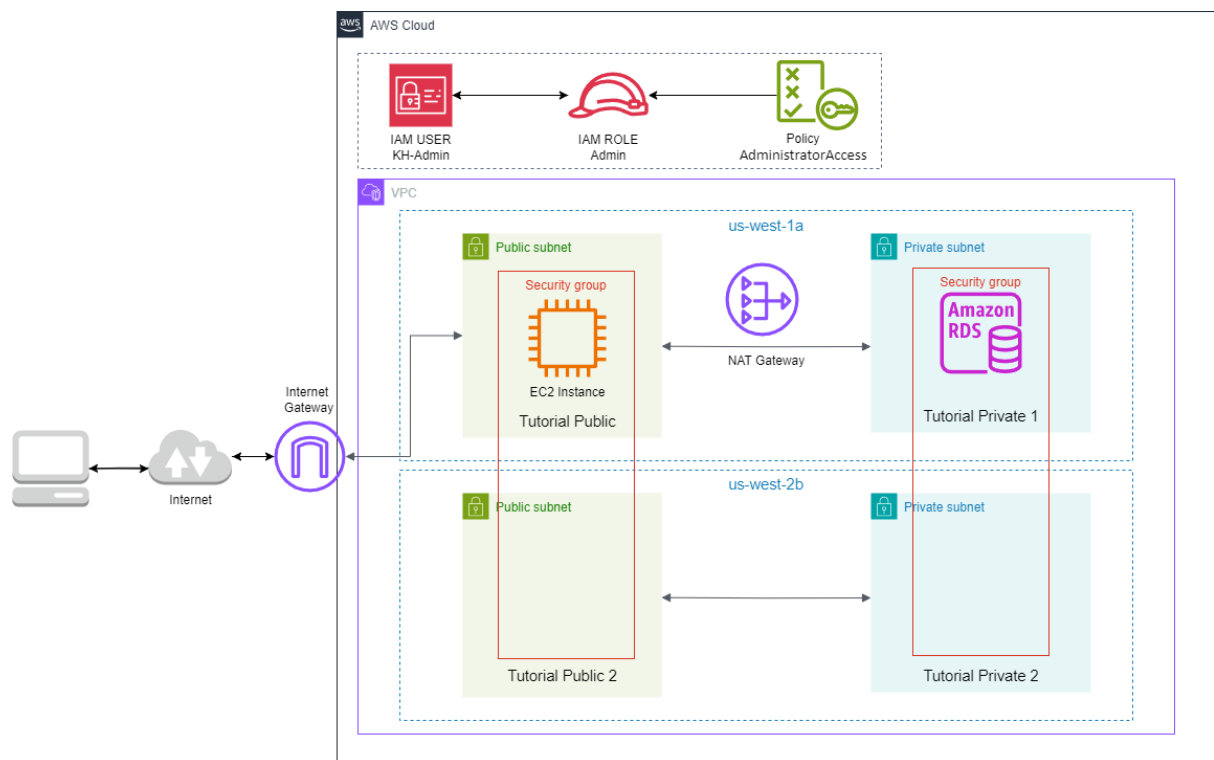
```
MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| innodb      |
| mysql      |
| performance_schema |
| sys        |
+-----+
5 rows in set (0.003 sec)

MariaDB [(none)]> █
```

El cual retornara las tablas existentes en la base de datos (las creadas por defecto).

## 9. Mejoras sobre la arquitectura para mayor seguridad

Se describirá algunas mejoras necesarias para reforzar la seguridad de la arquitectura en AWS del ejercicio propuesto. Se implementarán **Roles de IAM** para gestionar los permisos y accesos de los recursos y usuarios de manera granular. Adicionalmente, se configurará una **subred pública** con una instancia EC2 expuesta mediante un **Internet Gateway**, y una **subred privada** dedicada al alojamiento seguro de una base de datos en **Amazon RDS**, garantizando así un entorno segmentado y seguro.



## 9.1. Creación de Grupos de Trabajo (IAM Role)

Para mejorar la seguridad de la arquitectura en AWS, se recomienda crear un IAM Role para gestionar de forma centralizada los permisos. En lugar de asignar permisos directamente a usuarios individuales, como el usuario **KH-Admin**, se sugiere incluirlo en un grupo de trabajo con permisos de administrador mediante la política **AdministratorAccess**. Esto facilita la gestión de futuros usuarios, ya que podrán heredar los permisos del grupo. Antes de finalizar la creación de los usuarios y asignarles las políticas correspondientes, es recomendable revisar que las mejores prácticas de seguridad estén aplicadas, como la activación de **MFA** (Multi-Factor Authentication) y el uso de contraseñas fuertes.

## 9.2. Creación de Subnet Pública y Privada

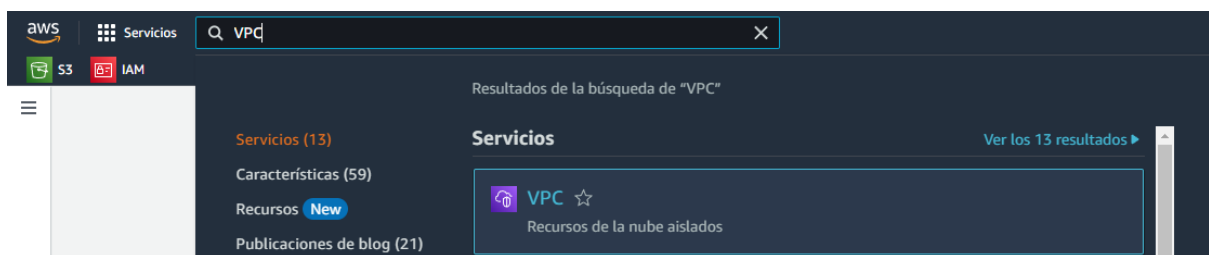
Se determinó que alojar una instancia de Amazon RDS en una subnet pública no es seguro debido a la exposición directa a internet. Como alternativa, se recomienda una arquitectura más óptima, donde se expone una instancia EC2 en una subnet pública para recibir las solicitudes a través de un Internet Gateway. La base de datos de Amazon RDS se alojará en una subnet privada, y gestionará las solicitudes mediante un NAT Gateway, lo que proporciona un mayor nivel de seguridad al restringir el acceso directo a la base de datos desde internet, permitiendo solo el tráfico controlado desde el EC2.

Para aplicar los cambios mencionados se tendrían que modificar las secciones:

- 3. Crear una VPC para la instancia de la base de datos
- 4. Configurar el grupo de seguridad (Security Group)
- 5. Crear subredes adicionales
- 6. Crear el grupo de subredes de base de datos
- 7. Crear la instancia de base de datos

### 9.2.1. Crear la VPC

En la barra de búsqueda escribe VPC y accede a la búsqueda correspondiente.



Una vez ingresado, haz clic en la opción **Create VPC** (Crear VPC).

**Crear VPC**

Elige la opción **VPC y mas** (VPC with Public and Private Subnets).

Configura los siguientes valores:

- **IPv4 CIDR Block:** 10.0.0.0/16 (esto puede variar, pero asegúrate de que sea grande).
- **Nombre de la VPC:** tutorial-vpc.
- **IPv6 CIDR:** No (opcional).
- **Nombre de la Subnet Pública:** Tutorial public 1
- **CIDR Block de la Subnet Pública:** 10.0.1.0/24.
- **Nombre de la Subnet Privada:** Tutorial private 1
- **CIDR Block de la Subnet Privada:** 10.0.2.0/24.

Habilita NAT Gateway para que los recursos de la subnet privada puedan acceder a Internet (salida).

Al completar estos pasos, AWS creará automáticamente una VPC con:

- Una subnet pública con acceso a Internet (para la instancia EC2).
- Una subnet privada sin acceso directo a Internet (para la base de datos RDS).
- Una Internet Gateway y un NAT Gateway.

### 9.2.2. Crear subredes adicionales

Añade una segunda subred para alta disponibilidad tanto para la subred pública como para la privada:

En la consola de VPC, selecciona **Create Subnet** (Crear Subred).

Define:

- **Nombre:** Tutorial public 2
- **Pv4 CIDR:** 10.0.3.0/24
- **Zona de disponibilidad:** us-west-2b

Asegúrate de asociar la misma tabla de enrutamiento que utilizaste en la subred publica anterior (**Tutorial public 1**) para mantener la consistencia.

En el caso de que no te permita seleccionar la tabla de enrutamiento, seleccionando la subred y haciendo clic en la pestaña Tabla de Enrutamiento, puedes editarla.

Realizar los mismos pasos para la creación de la segunda subred privada.

- **Nombre:** Tutorial private 2
- **Pv4 CIDR:** 10.0.4.0/24
- **Zona de disponibilidad:** us-west-2b

### 9.2.3. Configurar las tablas de enrutamiento (Route Tables)

Configurar tabla de enrutamiento de la subnet pública:

- Selecciona la tabla de enrutamiento asociada a la subnet pública.
- Asegúrate de que el tráfico a 0.0.0.0/0 esté dirigido al Internet Gateway (IGW).

Configurar tabla de enrutamiento de la subnet privada:

- Selecciona la tabla de enrutamiento de la subnet privada.
- Dirige el tráfico saliente (0.0.0.0/0) al NAT Gateway para permitir que la base de datos acceda a servicios externos (por ejemplo, para actualizaciones).

### 9.2.4. Configurar el Security Group para la instancia EC2

En la consola de EC2, selecciona Security Groups (Grupos de Seguridad).

Crea un nuevo grupo de seguridad llamado **tutorial-ec2-public**.

Configura las reglas inbound (entrantes):

- **Tipo:** HTTP
- **Protocolo:** TCP
- **Puerto:** 80
- **Fuente:** 0.0.0.0/0 (acceso desde cualquier parte de Internet).
- Agrega otra regla para permitir SSH (puerto 22) solo desde tu dirección IP.

Configura las reglas outbound (salientes) para permitir todo el tráfico.

### 9.2.5. Configurar el Security Group para RDS

En la consola de RDS, selecciona Security Groups.

Crea un nuevo grupo de seguridad llamado **tutorial-rds-private**.

Configura las reglas inbound (entrantes):

- **Tipo:** MySQL\Aurora o el puerto de tu motor de base de datos (por ejemplo, 3306 para MySQL).
- **Protocolo:** TCP.
- **Fuente:** selecciona el ID del grupo de seguridad de la instancia EC2 (**tutorial-ec2-public**) para que solo la instancia EC2 pueda acceder a la base de datos.

Configura las reglas outbound para permitir todo el tráfico dentro de la VPC.

### 9.2.6. Crear la instancia RDS en la Subnet Privada

En la consola de RDS, selecciona **Create Database** (Crear Base de Datos).

Elige las siguientes opciones:

- **Tipo de base de datos:** MariaDB.
- **Método de creación:** Standard Create.
- **DB Name:** a elección, en mi caso **Tutorial-DB**
- **DB instance size:** Free tier (no genera costo).
- **Usuario administrador:** Indica un nombre (en mi caso **bdtutorial**) y generar una contraseña manualmente.
- **VPC:** Selecciona la VPC creada (**tutorial-vpc**).
- **Grupo de Subnet de la base de datos:** Selecciona el grupo de subnets de la VPC, el cual incluirá las subnets privadas.
- **Acceso público:** Selecciona **No**, ya que esta base de datos no debe ser accesible directamente desde Internet.
- **Security Group:** Selecciona **tutorial-rds-private** para asegurar que solo la instancia EC2 pueda comunicarse con la base de datos.

Configura el resto de las opciones y crea la instancia RDS.

### 9.2.7. Probar la conectividad

Una vez que tengas el Endpoint, el nombre de usuario y la contraseña, puedes conectarte a la base de datos desde la terminal de la siguiente manera:

```
mariadb -h <endpoint> -u <username> -p
```

- **-h:** Se usa para especificar el Endpoint de tu base de datos (por ejemplo: **mariadbinstancia.skdimetllwst.us-west-1.rds.amazonaws.com**).
- **-u:** El nombre de usuario que configuraste o que se generó automáticamente al crear la base de datos.
- **-p:** Esta opción solicita la contraseña del usuario que proporcionaste en el paso anterior. Al ingresar el comando, te pedirá que la ingreses de manera segura.

Después de ingresar estos detalles, deberías estar conectado a tu base de datos en Amazon RDS y verás el prompt de MariaDB:

***MariaDB [(none)]>***

Una vez dentro de la consola de MariaDB, puedes ejecutar el siguiente comando para listar todas las bases de datos disponibles:

***SHOW DATABASES;***

Verás una lista de las bases de datos disponibles, incluidas las predeterminadas y las que hayas creado.