

Desafio numero 5

AWS Identity and Access Management (AWS IAM) es un servicio web que permite a los clientes de Amazon Web Services (AWS) administrar los usuarios y los permisos de usuario en AWS. Con IAM, puede administrar de forma centralizada los usuarios, las credenciales de seguridad, como las claves de acceso, y los permisos que controlan a qué recursos de AWS pueden acceder los usuarios.

AWS Identity and Access Management

AWS Identity and Access Management (AWS IAM) se puede utilizar para:

- **Administrar usuarios de IAM** y su acceso: puede crear usuarios y asignarles credenciales de seguridad individuales (claves de acceso, contraseñas y dispositivos con autenticación multifactor). Puede administrar los permisos para controlar qué operaciones puede realizar cada usuario.
- **Administrar roles de IAM** y sus permisos: un rol de IAM es similar a un usuario, ya que es una AWS Identity con políticas de permisos que establecen lo que puede y no puede hacer la identidad en AWS. Sin embargo, en lugar de estar asociado solo a una persona, el objetivo es que cualquiera que necesite el rol pueda asumirlo.
- Administrar usuarios federados y sus permisos: puede habilitar la identidad federada a fin de permitir que los usuarios existentes de su empresa puedan acceder a la Consola de administración de AWS, llamar a las API de AWS y acceder a los recursos sin necesidad de crear un usuario de IAM para cada identidad.

Creación de usuario administrador:

Paso 1: Se Inicio Sesión en AWS

1. Luego nos dirigimos a ([AWS Management Console](#).)
 2. se inicia se Inicia sesión con el **usuario raíz** (solo por esta vez).
-

Paso 2: Crear un Usuario admisntrador IAM

1. En la consola de AWS, se busca **IAM** en la barra de búsqueda y selecciona **Identity and Access Management (IAM)**.
2. En el menú lateral, se hace clic en **Usuarios > Agregar usuario**.
3. Ingresa un nombre para el usuario, por ejemplo: **Admin_Hernan**.
4. En **Tipo de credenciales**, marca:
Acceso a la Consola de Administración de AWS (para usar la interfaz web).
Generar una contraseña y configúrala o permite que AWS la genere automáticamente, en este caso se creo una contraseña. (Personal).

5. Se habilito MFA.
6. Se creo contraseñas y accesos para la consola CLI

Paso 3: Se asigno Permisos de Administrador

1. En la sección **Permisos**, seleccionar "**Adjuntar directamente políticas existentes**".
2. Buscar la política llamada **AdministratorAccess**.
3. Seleccionarla y hacer clic en **Siguiente**.

Paso 4: Revisar y Crear el Usuario

1. Verificar los detalles y hacer clic en **Crear usuario**.
2. AWS genera las credenciales (usuario y contraseña).
3. Descarga el archivo **CSV** con las credenciales o cópialas y guárdalas en un lugar seguro.

Paso 5: Probar el Nuevo Usuario IAM

1. Cerrar sesión del usuario raíz.
2. Iniciar sesión en la **consola de AWS** con el nuevo usuario IAM.
3. Verificar que tienes permisos administrativos accediendo a **IAM** y comprobando las configuraciones.


¡**Listo!** Ahora de puede usar este usuario para realizar todas las configuraciones sin riesgos de seguridad.

Admin_Hernan [Info](#)

Delete

Summary

ARN

 arn:aws:iam::207567791252:user/Admin_Hernan


Created

February 14, 2025, 09:32 (UTC-03:00)

Console access


Enabled with MFA

Last console sign-in

 Today

Access key 1

AKIATAVABESKI5V3LORH - Active

 Never used. Created today.

Access key 2

Create access key

Permissions

Groups
(1)

Tags
(1)

Security credentials

Last Accessed

Permissions policies (2)

Remove

Add permissions

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type

All types

< 1 >

⚙️

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Group Admin_HernanAcosta

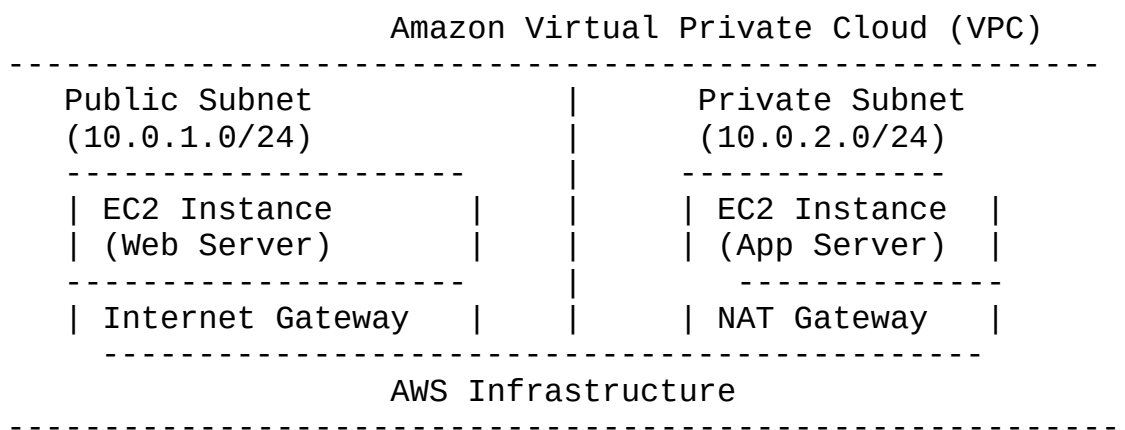
Creación VPC

Amazon Virtual Private Cloud (Amazon VPC)

Amazon VPC permite crear una red virtual en la nube de AWS, similar a una red tradicional en un centro de datos local, con los beneficios de la escalabilidad de AWS. Con VPC, puedes definir un espacio de direcciones IP privadas, dividir la red en subredes y controlar el tráfico entrante y saliente mediante reglas de seguridad.

Diagrama de Amazon VPC

Aquí presntamos un diagrama conceptual que muestra la estructura de una VPC con subredes públicas y privadas (pero en unetro caso para el laboratorio solo utilizaremos dos subnet publicas)de ejemplo:



Explicación del diagrama:

- La **subred pública** contiene servidores accesibles desde Internet (como servidores web).
- La **subred privada** aloja servidores internos (como bases de datos o aplicaciones) que no tienen acceso directo a Internet.
- Una **Internet Gateway** permite que las instancias en la subred pública se comuniquen con Internet.
- Un **NAT Gateway** permite que las instancias en la subred privada inicien conexiones a Internet, pero sin ser accesibles desde afuera.

Details [Info](#)

VPC ID  vpc-030c985080ad4edc7	State  Available	Block Public Access  Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-0dc0ef2ff66170bfe	Main route table rtb-04545229a66bcdcb
Main network ACL acl-0f7c2a65b56c0e632	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID  207567791252

[Resource map](#)[CIDRs](#)[Flow logs](#)[Tags](#)[Integrations](#)Resource map [Info](#)

configuracion de security groups

- Acceder al Security Group - Navega a Security Groups en la consola de AWS.
 - Selecciona el grupo de seguridad asociado al VPC.
- Editar Inbound Rules - Selecciona la pestaña Inbound Rules.
 - Observa la configuración predeterminada:
 - Type: All traffic
 - Protocol: All
 - Port Range: All
 - Source: sg-d57b5896 (default)
- Modificar el Campo Source - Edita las reglas de entrada.
 - Cambia el campo Source según tus necesidades:
 - Para acceso desde cualquier punto de Internet: 0.0.0.0/0
 - Para acceso desde IPs específicas: Ej. 56.176.2.108/32
- Guardar los Cambios - Haz clic en Save rules para aplicar los cambios.

Ejemplo de Configuración para Acceso desde una IP Específica

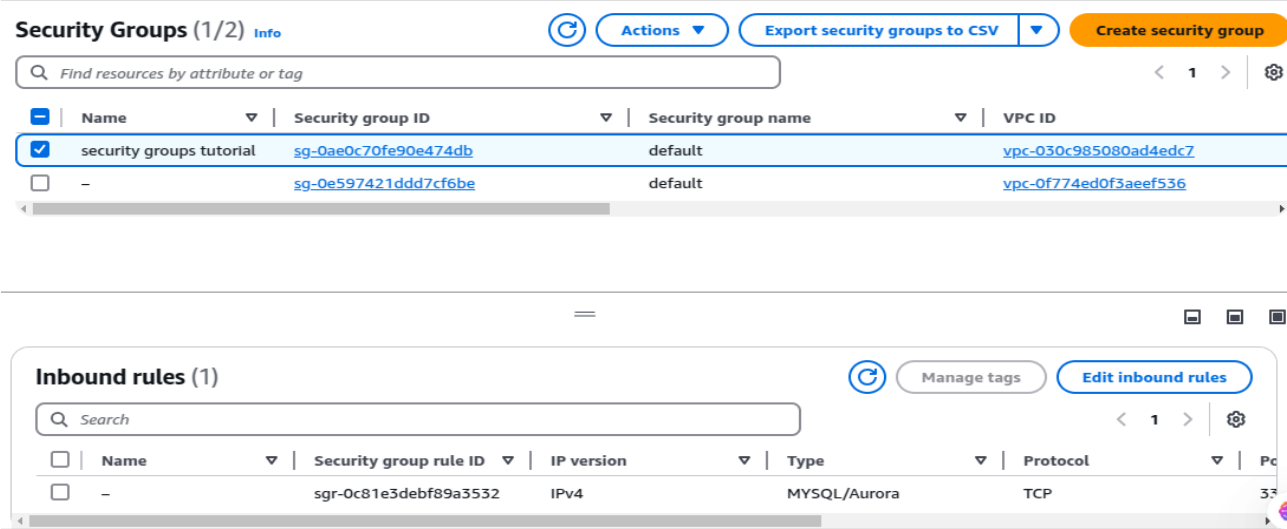
Type	Protocol	Port Range	Source
MYSQL/Aurora	TCP	3306	56.176.2.108/32

Notas Importantes

0.0.0.0/0: Permite el acceso desde cualquier dirección IP en Internet. No es recomendable para entornos de producción debido a riesgos de seguridad.

IP específica: Limita el acceso a una dirección IP o rango de IPs específicas, lo cual es más seguro.

Puerto 3306: Es el puerto predeterminado para MySQL/Aurora. Asegúrate de abrir el puerto correcto según el tipo de base de datos que estás utilizando.



Crear las subredes adicionales

Paso	Detalle
1. Acceder a la Consola de VPC	- Inicia sesión en AWS. - Navega al servicio VPC .
2. Identificar el VPC Existente	- Localiza el VPC en el que trabajarás. - Anota el CIDR block del VPC.
3. Crear las Subredes	- Ve a Subnets y haz clic en Create subnet . - Selecciona el VPC y asigna un CIDR block para la subred. - Selecciona la Availability Zone (AZ) para la subred. - Repite el proceso para todas las subredes adicionales.
4. Configurar como Públicas	- Asocia un Internet Gateway al VPC si no existe. - Crea una Route Table para las subredes públicas. - Agrega una ruta en la Route Table : 0.0.0.0/0 -> igw-id. - Asocia las subredes públicas a esta Route Table .
5. Verificar la Configuración	- Habilita Auto-assign public IPv4 address en las subredes. - Verifica el acceso a Internet desde instancias en las subredes públicas.

Ejemplo de Configuración de Subredes Públicas

Subred	CIDR Block	Availability Zone	Route Table	Internet Gateway
Subnet 1	10.0.1.0/24	us-east-1a	Public-Route-Table	igw-12345678
Subnet 2	10.0.2.0/24	us-east-1b	Public-Route-Table	igw-12345678
Subnet 3	10.0.3.0/24	us-east-1c	Public-Route-Table	igw-12345678

Subnets (6) [Info](#)

Last u
1 mini

Find resources by attribute or tag

<input type="checkbox"/>	Name ▾	Subnet ID ▾	State ▾
<input type="checkbox"/>	tutorial-vpc-subnet-public2-us-west-2b	subnet-0055534b673f166dc	✓ Available
<input type="checkbox"/>	-	subnet-0ba991d142c31e653	✓ Available
<input type="checkbox"/>	-	subnet-0af392630ecd6bf65	✓ Available
<input type="checkbox"/>	-	subnet-03c4737ce3bbfde0f	✓ Available
<input type="checkbox"/>	tutorial-vpc-subnet-public1-us-west-2a	subnet-0f73e26559b1ea5e8	✓ Available

Crear Grupo de Subredes

de Base de Datos

1. Abrir la consola de Amazon RDS

- Ir a: <https://console.aws.amazon.com/rds/>
- Asegurarse de estar en Amazon RDS

2. Navegar al Panel de Navegación

- Elegir "Subnet groups"

3. Crear Grupo de Subredes de Base de Datos

- Elegir "Create DB Subnet Group"

4. Detalles del Grupo de Subredes

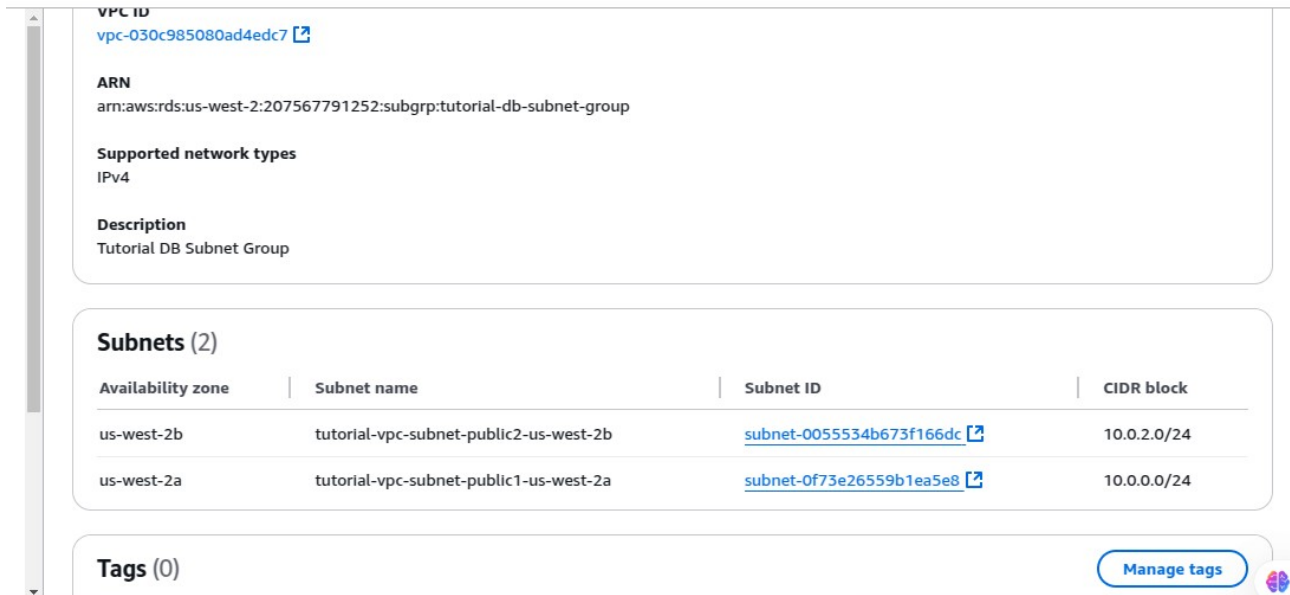
- Name: tutorial-db-subnet-group
- Description: Tutorial DB Subnet Group
- VPC: tutorial-vpc (vpc-identifier)

5. Agregar Subredes

- Elegir Zonas de Disponibilidad
 - * us-west-2a
 - * us-west-2b
- Elegir todas las subredes
- Si hay zona local, elegir:
 - * Grupo de Zonas de Disponibilidad
 - * Zonas de Disponibilidad
 - * Subredes

6. Crear Grupo

- Seleccionar "Create"
- Verificar en la lista de Grupos de Subredes de la consola de RDS



Crear Instancia de Base de Datos

en la VPC de Amazon RDS

1. Abrir la consola de Amazon RDS
 - Ir a: <https://console.aws.amazon.com/rds/>
2. Seleccionar región
 - Elegir la región en la esquina superior derecha
 - Debe coincidir con la región de la VPC
3. Seleccionar "Databases"
4. Pulsar el botón "Create database"
5. Elegir opción de creación
 - Seleccionar "Standard Create"
 - * Permite elegir VPC y configuraciones adicionales
 - * No usar "Easy Create"
6. Seleccionar "Engine Type"
 - Elegir motor de base de datos
 - * Ejemplo: MariaDB (o MySQL si se desea)
7. Seleccionar tamaño de instancia

- Elegir "Free tier" para economizar gastos
- 8. Indicar nombre de la instancia y usuario admin.
- 9. Pulsar "Auto generate a password"
 - La contraseña se mostrará una vez en la creación
 - Opcional: desmarcar para indicar manualmente
- 10. Dejar opciones predeterminadas
- 11. Conectividad
 - Seleccionar la VPC creada anteriormente
 - Desplegar "Additional connectivity configuration"
- 12. Seleccionar el Subnet group creado
- 13. Configurar acceso público
 - En "Public access" seleccionar "Yes"
- 14. Dejar opciones predeterminadas
- 15. Pulsar "Create database" al final de la página
- 16. Pulsar "View credential details"
 - Se mostrará:
 - * Contraseña del usuario administrador
 - * Endpoint de la instancia

The screenshot displays the AWS RDS console interface. At the top, a 'Summary' card provides key details: DB identifier 'database-1', CPU usage at 3.92%, Status 'Available', Class 'db.t4g.micro', Role 'Instance', Current activity '0 Connections', Engine 'MariaDB', and Region & AZ 'us-west-2b'. Below this is a navigation bar with tabs: 'Connectivity & security' (selected), 'Monitoring', 'Logs & events', 'Configuration', 'Maintenance & backups', and 'Data migration'. The main content area is titled 'Connectivity & security' and is divided into three sections: 'Endpoint & port' showing the endpoint 'database-1.c728cuoy6dkg.us-west-2.rds.amazonaws.com' and port '3306'; 'Networking' showing 'Availability Zone' as 'us-west-2b' and 'VPC' as 'tutorial-vpc-vpc'; and 'Security' showing 'VPC security groups' as 'default (sg-0ae0c70fe90e474db)' with an 'Active' status and 'Publicly accessible' checked.

Comprobar Acceso a la Instancia

de Base de Datos en Amazon RDS

1. Verificar que la instancia de base de datos está creada y en estado disponible
2. Obtener el Endpoint de la instancia
 - Ejemplo: mariadbinstancia.skdimetllwst.us-west-1.rds.amazonaws.com
3. Abrir una consola o terminal en su máquina
4. En la consola, utilizar el comando mariadb
 - Estructura del comando:
`$ mariadb -h <Endpoint> -u <username> -p <password>`
 - Ejemplo:
`$ mariadb -h mariadbinstancia.skdimetllwst.us-west-1.rds.amazonaws.com -u username -p password`
5. Introducir la contraseña cuando se solicite
6. Confirmar el acceso
 - Mensaje de bienvenida: "Welcome to the MariaDB monitor."
 - Confirmar que se ve el ID de conexión de MariaDB:
"Your MariaDB connection id is 60"

```
Bye
herman@andres:~$ mariadb -h database-1.c728cuoy6dkg.us-west-2.rds.amazonaws.com -uadmin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 72
Server version: 11.4.4-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)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| innodb |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0,217 sec)

MariaDB [(none)]> 
```

