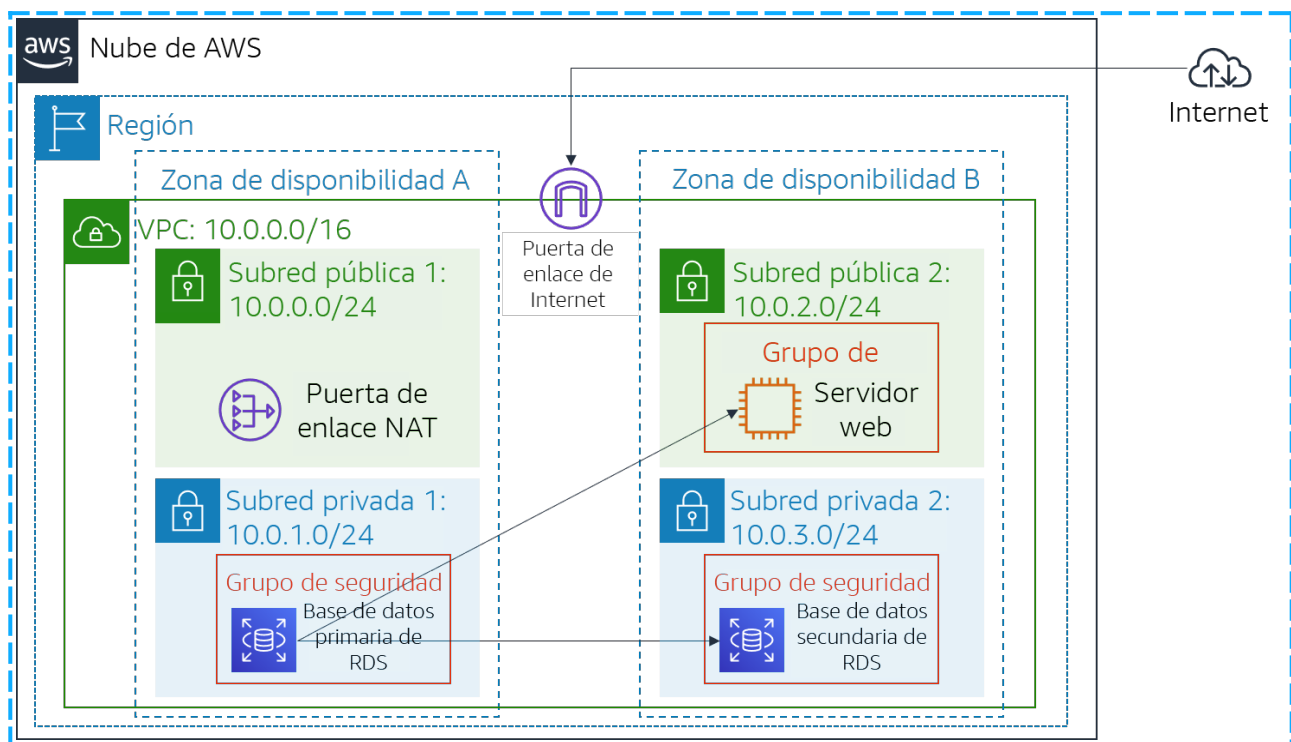


Creación de un servidor de base de datos e interacción con la base de datos mediante una aplicación



Sumario

1. Crear un grupo de seguridad para la instancia de base de datos de RDS.....	3
1.1 Datos básicos.....	4
1.2 Reglas de entrada.....	4
2. Crear un grupo de subredes de base de datos.....	5
2.1 Datos básicos.....	5
2.2 Zonas y subredes.....	6
3. Crear una instancia de base de datos de Amazon RDS.....	7
3.1. Motor.....	7
3.2 Zona Multi-AZ.....	7
3.3 Datos básicos.....	8
3.4 Almacenamiento y tipo de base de datos.....	8
3.5 Conectividad.....	9
3.6 Monitoreo.....	9
3.7 Configuraciones adicionales.....	10

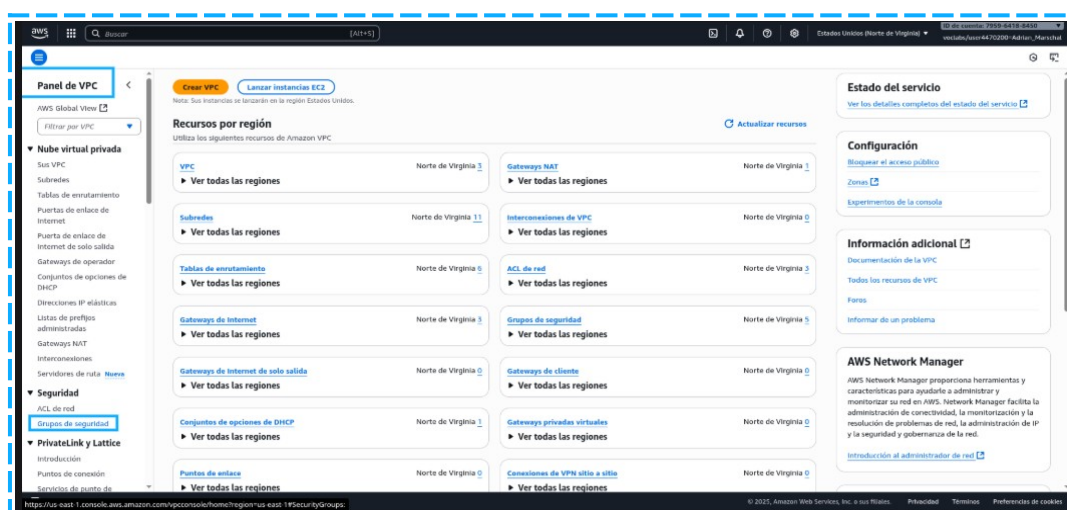
1. Crear un grupo de seguridad para la instancia de base de datos de RDS

En el caso de hoy deberemos crear EC2(Elastic Cloud Compute) como máquina virtual y relacionarla con un RDS(Relational Database Service) dentro de un mismo grupo de seguridad en subredes diferentes.

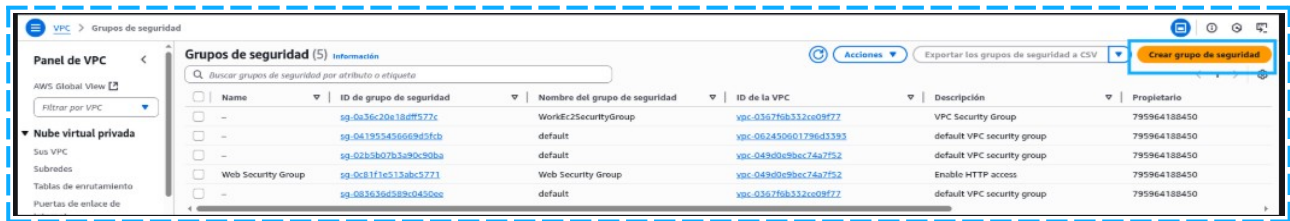
Para ello, deberemos usar una VPC(Virtual Private Cloud) para gestionar el grupo de seguridad:



Dentro del servicio deberemos dirigirnos al apartado



Entramos, y pulsamos



1.1 Datos básicos

Empezaremos con la sección de datos (Nombre, Descripción, VPC relacionada...) y introduciremos los datos que nos piden:

Crear grupo de seguridad Información

Un grupo de seguridad actúa como un firewall virtual para que la instancia controle el tráfico de entrada y salida. Para crear un nuevo grupo de seguridad, complete los campos siguientes.

Detalles básicos

Nombre del grupo de seguridad Información

Web Security Group

El nombre no se puede editar después de su creación.

Descripción Información

Permite acceso a DB Security Group

VPC Información

vpc-049d0e9bec74a7f52 (Lab VPC)

1.2 Reglas de entrada

Al ser un grupo de protección que actúa como firewall podemos aplicarle reglas de entrada, en nuestro caso queremos que se permita la entrada desde el grupo que vamos a crear:

Reglas de entrada Información

Tipo Información: MySQL/Aurora

Protocolo Información: TCP

Intervalo de puertos Información: 3306

Origen Información: Persona...

Descripción: opcional Información

Agregar regla

Utilizar: "sg"

Bloques de CIDR

Grupos de seguridad

default | sg-02b5b07b3a90c90ba

Web Security Group | sg-0c81f1e513abc5771

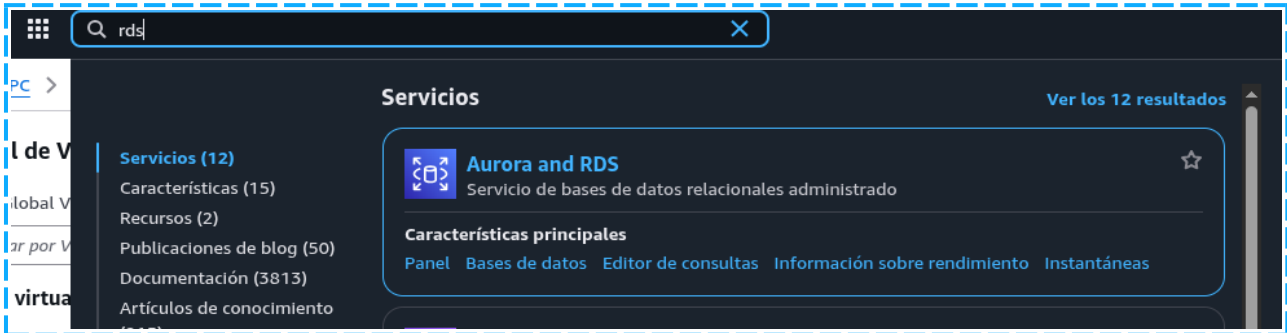
Web Security Group

Finalizamos pulsando
mensaje de función exitosa.

y te saldrá un

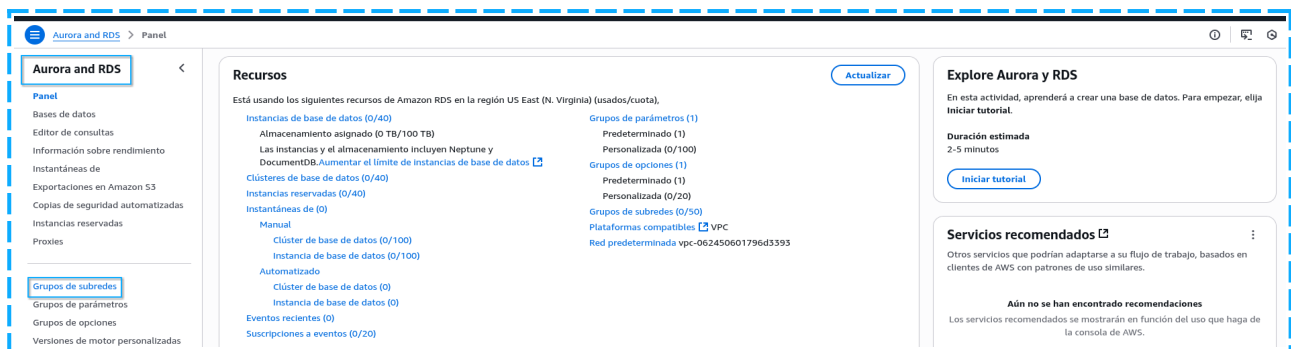
2. Crear un grupo de subredes de base de datos.

A continuación vamos a crear ambas subredes que van a alojar por un lado la instancia y por la otra la base de datos. Para ello vamos a acceder dentro de RDS:



Dentro de este servicio accedemos a

:



2.1 Datos básicos

Pulsamos en

y vuelve a demandar los

datos básicos:

Crear grupo de subredes de base de datos

Para crear un nuevo grupo de subredes, asígnele un nombre y una descripción, y elija una VPC existente. A continuación, podrá agregar subredes relacionadas con dicha VPC.

Detalles del grupo de subredes

Nombre
No podrá modificar el nombre una vez creado el grupo de subredes de base de datos.

Descripción

VPC
Elija un identificador de VPC que se corresponda con las subredes que desea utilizar para el grupo de subredes de base de datos. No podrá elegir otro identificador de VPC una vez creado el grupo de subredes.

2.2 Zonas y subredes

Ahora deberemos determinar las zonas de disponibilidad. Debemos utilizar En estas zonas seleccionadas
elegimos las subredes 10.0.0.1/24 y la 10.0.0.3/24:

Agregar subredes

Zonas de disponibilidad
Elija las zonas de disponibilidad que incluyen las subredes que desea agregar.

Elegir una zona de disponibilidad

us-east-1a X us-east-1b X

Subredes
Elija las subredes que desea agregar. La lista incluye las subredes de las zonas de disponibilidad seleccionadas.

Seleccionar subredes

Q |

☒ us-east-1b

☒ Private Subnet 2
Subnet ID: subnet-01586ca094ad7c792 CIDR: 10.0.3.0/24

☐ Public Subnet 2
Subnet ID: subnet-0ceacb224a3c23e66 CIDR: 10.0.2.0/24

☒ us-east-1a

☒ Private Subnet 1
Subnet ID: subnet-0019ab1a262475be4 CIDR: 10.0.1.0/24

☐ Public Subnet 1
Subnet ID: subnet-015b5af89add05b09 CIDR: 10.0.0.0/24

Bloque de CIDR

10.0.3.0/24

10.0.1.0/24

Pulsamos en y si todo sale bien nos volverá a sacar el
mensaje de confirmación:

DB-Subnet-Group se ha creado correctamente. Ver grupo de subredes

Grupos de subredes (1)

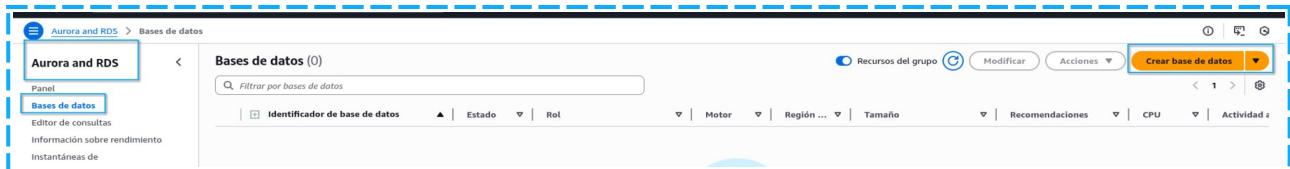
Editar Eliminar Crear grupo de subredes de base de datos

Filtrar por grupo de subredes

Nombre	Descripción	Estado	VPC
db-subnet-group	DB Subnet Group	Completado	vpc-049d0e9bec74a7f52

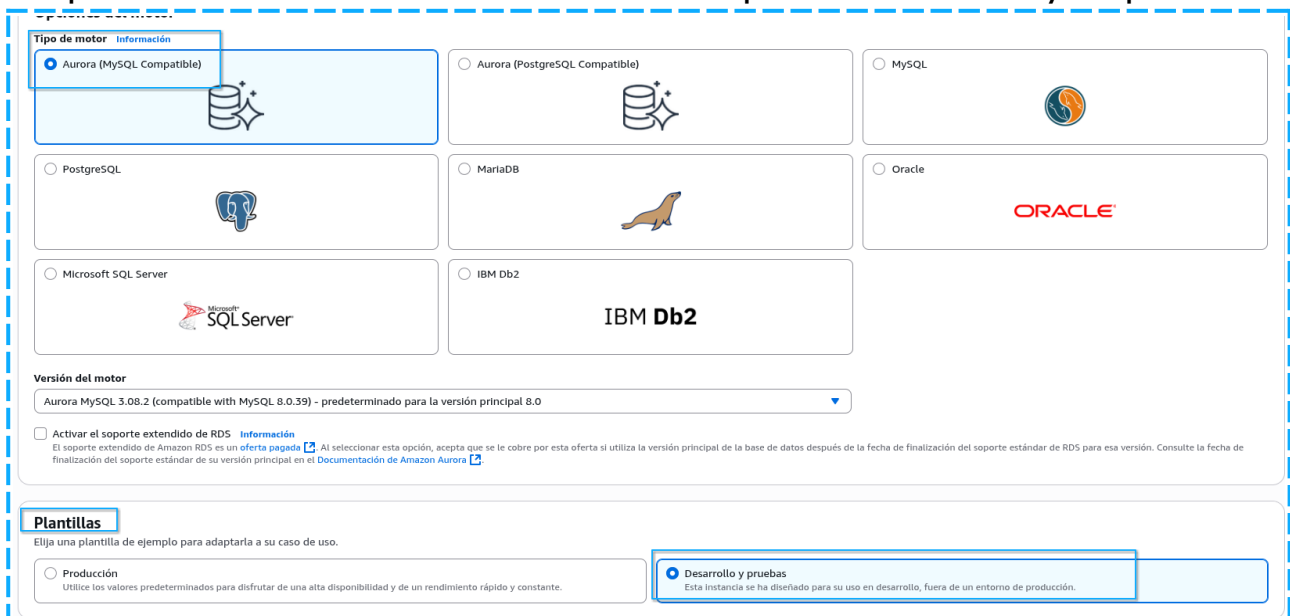
3. Crear una instancia de base de datos de Amazon RDS

A continuación deberemos crear la base de datos asociada a la instancia, para ello navegaremos al apartado de **Bases de datos** y pulsaremos en **Crear base de datos**



3.1. Motor

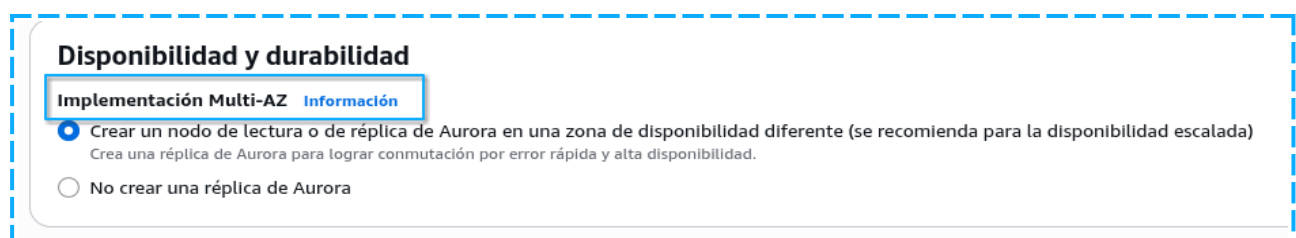
Empezaremos seleccionando el motor que va a utilizar y la plantilla:



3.2 Zona Multi-AZ

Deberemos seleccionar la utilización de el nodo Multi-AZ(Ability Zone):

Al aprovisionar con este nodo se crea una instancia activa y otra instancia en espera de duplicado en una zona distinta



3.3 Datos básicos

A continuación rellenamos los datos clave de la base de datos(nombre, contraseña...):

Es importante añadir un identificador único por que pueden haber varias bases de datos de la misma zona con el mismo nombre

Configuración

Identificador del clúster de base de datos Información
Ingrese un nombre para el clúster de base de datos. El nombre debe ser único entre todos los clústeres de base de datos de la cuenta de AWS de la región de AWS actual.
lab-db

El identificador del clúster de base de datos no distingue entre mayúsculas y minúsculas, pero se almacena todo en minúsculas (por ejemplo, "mydbcluster"). Restricciones: de 1 a 63 caracteres alfanuméricos o guiones. El primer carácter debe ser una letra. No puede contener dos guiones consecutivos. No puede terminar con un guión.

▼ Configuración de credenciales

Nombre de usuario maestro Información
Escriba un ID de inicio de sesión para el usuario maestro de la instancia de base de datos.
main

1 a 34 caracteres alfanuméricos. El primer carácter debe ser una letra.

Administración de credenciales
Puede usar AWS Secrets Manager o administrar sus credenciales de usuario maestro.

☐ Administrado en AWS Secrets Manager - *más seguro*
RDS genera una contraseña y la administra durante todo su ciclo de vida mediante AWS Secrets Manager.

☒ Autoadministrado
Cree su propia contraseña o pida a RDS que cree una contraseña para que pueda administrarla.

☐ Generar contraseña automáticamente
Amazon RDS puede generar una contraseña en su nombre, o bien puede especificar su propia contraseña.

Contraseña maestra Información

Password strength Neutral
Restricciones mínimas: al menos 8 caracteres ASCII imprimibles. No puede contener ninguno de los siguientes símbolos: / " * @

Confirmar la contraseña maestra Información

3.4 Almacenamiento y tipo de base de datos

Una vez rellenado los datos nos encontramos con el tipo de almacenamiento de la base de datos, seleccionamos Aurora Estándar y por el motor de base de datos seleccionado anteriormente(MySQL) existen diferentes clases a la cual escogeremos la clase t3.medium:

Configuración del almacenamiento en clúster Información
Elija la configuración de almacenamiento para el clúster de base de datos de Aurora que mejor se adapte a las necesidades de previsibilidad y rendimiento de precios de la aplicación.

Opciones de configuración
Los cargos por instancia de base de datos, almacenamiento y operaciones de E/S varían en función de la configuración. [Más información](#)

☐ Aurora optimizado para las operaciones de E/S

- Precios previsible para todas las aplicaciones. Mejor rendimiento de precios para las aplicaciones que requieren un uso intensivo de E/S (costos de E/S >25 % de los costos totales de la base de datos).
- Sin cargos adicionales por operaciones de E/S de lectura/escritura. Los precios de instancia de base de datos y del almacenamiento incluyen el uso de E/S.

☒ Aurora Estándar

- Precios rentables para numerosas aplicaciones con un uso moderado de operaciones de E/S (costos de E/S <25% of total database costs).
- Se aplican cargos de E/S de pago por solicitud. Los precios de instancia de base de datos y almacenamiento no incluyen el uso de E/S.

Configuración de la instancia
Las opciones de configuración de la instancia de base de datos que aparecen a continuación están limitadas a las que admite el motor que ha seleccionado anteriormente.

Clase de instancia de base de datos Información

▼ Ocultar filtros

☒ Incluir clases de generación anterior

☐ Sin servidor v2

☐ Clases optimizadas para memoria (incluye clases r)

☒ Clases ampliables (incluye clases t)

db.t3.medium
2 vCPUs 4 GiB RAM Red: hasta 2085 Mbps Network: Up to 5 Gbps

3.5 Conectividad

En este apartado deberemos seleccionar el grupo de seguridad que hemos creado al inicio. Este fue creado en el VPC del Lab por lo que debemos seleccionar el mismo:

Conectividad Información

Recurso de computación
Seleccione si desea configurar una conexión a un recurso de computación para esta base de datos. Al establecer una conexión, se cambiará automáticamente la configuración de conectividad para que el recurso de computación se pueda conectar a esta base de datos.

☒ No se conecte a un recurso informático EC2
No configure una conexión a un recurso informático para esta base de datos. Puede configurar manualmente una conexión a un recurso informático más adelante.

☐ Conectarse a un recurso informático de EC2
Configure una conexión a un recurso informático EC2 para esta base de datos.

Nube privada virtual (VPC) Información
Elija la VPC. La VPC define el entorno de red virtual para este clúster de DB.

Lab VPC (vpc-087b376f3d3e94687)
4 Subredes, 2 Zonas de disponibilidad

Solo se muestran las VPC con grupos de subredes de base de datos correspondientes.

Después de crear una base de datos, no puede cambiar su VPC.

Grupo de subredes de la base de datos Información
Elija el grupo de subredes de DB. El grupo de subredes de DB que define las subredes e intervalos de IP que puede usar el clúster de base de datos en la VPC seleccionada.

Crear un nuevo grupo de subredes de base de datos.

Acceso público Información
☐ Sí
RDS asigna una dirección IP pública al clúster. Las instancias de Amazon EC2 y otros recursos fuera de la VPC pueden conectarse al clúster. Los recursos dentro de la VPC también pueden conectarse al clúster. Elija uno o varios grupos de seguridad de VPC que especifiquen qué recursos pueden conectarse al clúster.

☒ No
RDS no asigna una dirección IP pública al clúster. Solo las instancias de Amazon EC2 y otros recursos dentro de la VPC pueden conectarse al clúster. Elija uno o varios grupos de seguridad de VPC que especifiquen qué recursos pueden conectarse al clúster.

Grupo de seguridad de VPC (firewall) Información
Elija uno o varios grupos de seguridad de VPC para permitir el acceso a su base de datos. Asegúrese de que las reglas del grupo de seguridad permitan el tráfico entrante adecuado.

☒ Elegir existente
Elija grupos de seguridad de VPC existentes

☐ Crear nuevo
Crear un grupo de seguridad nuevo de VPC

Grupos de seguridad de VPC existentes
Elegir una o más opciones

Web Security Group X

3.6 Monitoreo

Como se trata de una base de datos simple no requerimos de un control muy específico por lo que deshabilitaremos la opción:

Supervisión Información
Elija herramientas de supervisión para esta base de datos. Database Insights ofrece una visión combinada de la información sobre el rendimiento y la supervisión mejorada para la flota de bases de datos. Los precios de información de base de datos son independientes de las estimaciones mensuales de RDS. Consulte Precios de Amazon CloudWatch.

☐ Database Insights: avanzado
• Retiene 15 meses de historial de rendimiento
• Monitorización a nivel de flota
• Integración con CloudWatch Application Signals

☒ Database Insights: estándar

Ajustes de monitorización adicional
Monitorización mejorada, registros de CloudWatch y DevOps Guru

Monitorización mejorada
☐ Habilitar la monitorización mejorada
Activar las métricas de monitorización mejorada es útil cuando desea ver cómo diferentes procesos o subprocesos usan la CPU.

Exportaciones de registros
Seleccione los tipos de registros que desea publicar en Amazon CloudWatch Logs.

☐ Registro de auditoría
☐ Registro de errores
☐ Registro general
☐ Registro de iam-db-auth-error
☐ Registro de instance
☐ Registro de consultas lentas

Rol de IAM
El siguiente rol vinculado al servicio se usa para publicar registros en Registros de CloudWatch.

Rol vinculado a servicio de RDS

3.7 Configuraciones adicionales

Para finalizar deberemos indicar el nombre de la base de datos y deshabilitar el cifrado por el mismo motivo anterior, al ser una base de datos de prueba podemos quitar esos complementos actualmente innecesarios:

Finalmente pulsamos en **Crear instancia** y se crearía automáticamente. En mi caso necesito permisos de mis superiores para autorizar la creación por lo que por resultado obtengo: