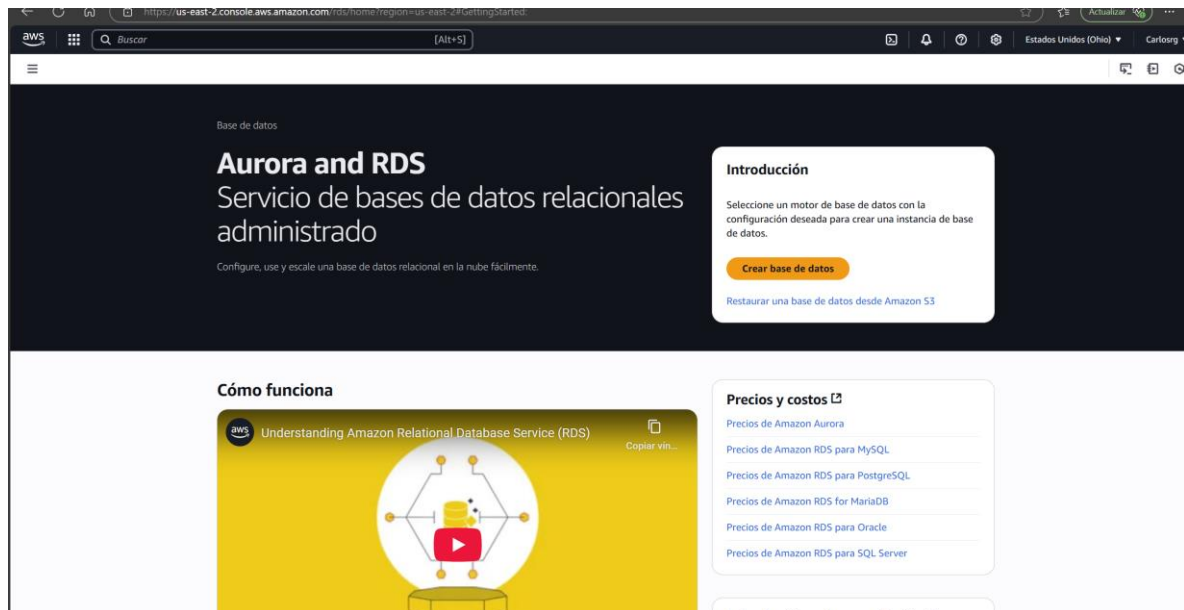


Generar las reglas en AWS para conexión remota a MySQL

Para este mini proyecto, debemos tener una cuenta en la pagina de AWS [Capa gratuita de AWS | Cloud computing gratis | AWS.](#)

Una vez creada la cuenta, procederemos a crear una base datos de mysql

En el buscador de la parte superior izquierda escribimos RDS y nos saldrá la opción de Aurora and RDS, damos click en esa opción.



Una vez dentro, damos click en crear una base de datos y empezamos a configurar nuestra db

Seleccionamos MySQL

Opciones del motor

Tipo de motor [Información](#)

<input type="radio"/> Aurora (MySQL Compatible)	<input type="radio"/> Aurora (PostgreSQL Compatible)
<input checked="" type="radio"/> MySQL	<input type="radio"/> PostgreSQL
<input type="radio"/> MariaDB	<input type="radio"/> Oracle
<input type="radio"/> Microsoft SQL Server	<input type="radio"/> IBM Db2

En la plantilla seleccionamos la capa gratuita de esta forma evitar pagos

Plantillas
Elija una plantilla de ejemplo para adaptarla a su caso de uso.

☐ **Producción**
Utilice los valores predeterminados para disfrutar de una alta disponibilidad y de un rendimiento rápido y constante.

☐ **Desarrollo y pruebas**
Esta instancia se ha diseñado para su uso en desarrollo, fuera de un entorno de producción.

☒ **Capa gratuita**
Utilice el nivel gratuito de RDS para desarrollar nuevas aplicaciones, probar aplicaciones existentes o adquirir experiencia práctica con Amazon RDS. [Información](#)

Disponibilidad y durabilidad
Opciones de implementación [Información](#)
Elija la opción de implementación que proporcione la disponibilidad y durabilidad necesarias en función del caso de uso. AWS se compromete a un determinado nivel de tiempo de actividad según la opción de implementación que elija. Obtenga más información en el [Acuerdo de nivel de servicios \(SLA\) de Amazon RDS](#).

☐ **Implementación de clúster de base de datos multi-AZ (3 instancias)**
Crea una instancia de base de datos principal con dos en espera legibles en zonas de disponibilidad separadas. Esta configuración proporciona:

- Tiempo de actividad del 99,95 %
- Redundancia entre zonas de disponibilidad
- Mayor capacidad de lectura
- Menor latencia de escritura



☐ **Implementación de instancias de base de datos multi-AZ (2 instancias)**
Crea una instancia de base de datos principal con una instancia en espera no legible en una zona de disponibilidad independiente. Esta configuración proporciona:

- Tiempo de actividad del 99,95 %
- Redundancia entre zonas de disponibilidad



☒ **Implementación de una instancia de base de datos de zona de disponibilidad única (1 instancia)**
Crea una única instancia de base de datos sin instancias en espera. Esta configuración proporciona:

- Tiempo de actividad del 99,5 %
- Sin redundancia de datos



Para tener una mayor seguridad seleccionamos la opción para que AWS cree la contraseña.

▼ 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.

1 a 16 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.

[Puede ver sus credenciales después de crear la base de datos. Haga clic en Ver detalles de credenciales en el encabezado de creación de la base de datos para ver la contraseña.](#)

También seleccionamos que sea de acceso publico debido a que usaremos mysql para conectarnos

Acceso público [Información](#)
☒ **Sí**
RDS asigna una dirección IP pública a la base de datos. Las instancias de Amazon EC2 y otros recursos fuera de la VPC pueden conectarse a la base de datos. Los recursos de la VPC también pueden conectarse a la base de datos. Elija uno o varios grupos de seguridad de VPC que especifiquen qué recursos pueden conectarse a la base de datos.

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

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**
Elegir grupos de seguridad de VPC existentes

☐ **Crear nuevo**
Crear un grupo de seguridad nuevo de VPC

Grupos de seguridad de VPC existentes

En opciones adicionales, deshabilitamos los backups automatizados

▼ **Configuración adicional**
Opciones de base de datos, cifrado activado, copia de seguridad desactivado, retroceder desactivado, mantenimiento, Registros de CloudWatch, eliminar protección desactivado.

Opciones de base de datos

Nombre de base de datos inicial [Información](#)

Grupo de parámetros de base de datos [Información](#)

Grupo de opciones [Información](#)

Copia de seguridad

☐ Habilitar las copias de seguridad automatizadas.
Crea una instantánea de un momento dado de su base de datos

Cifrado

Y listo procedemos a crearla. Una vez dentro nos aparecerá una interfaz así

Aurora and RDS

Panel

[Bases de datos](#)

[Editor de consultas](#)

[Información sobre rendimiento](#)

[Instantáneas de](#)

[Exportaciones en Amazon S3](#)

[Copias de seguridad automatizadas](#)

[Instancias reservadas](#)

[Proxies](#)

[Grupos de subredes](#)

[Grupos de parámetros](#)

[Grupos de opciones](#)

infraestructura1

[Modificar](#) [Acciones](#)

Resumen

Identificador de base de datos: infraestructura1

Estado: Disponible

Rol: Instancia

Motor: MySQL Community

CPU: 2.59%

Clase: db.t4g.micro

Actividad actual: 0 Conexiones

Región y AZ: us-east-2b

[Conectividad y seguridad](#) [Supervisión](#) [Registros y eventos](#) [Configuración](#) [Integraciones sin extracción, transformación y carga \(ETL\)](#) [Mantenimiento](#)

Conectividad y seguridad

Punto de enlace y puerto

Redes

Seguridad

Punto de enlace

Zona de disponibilidad

Grupos de seguridad de la VPC

Donde podemos jugar con algunos paramentros de conexión así mismo obtener los datos necesarios para conectarnos de forma remota.

Por ejemplo, habilitamos la conexión en el puerto 3306 ipv4 para conectarnos desde la herramienta de MySQL workbench

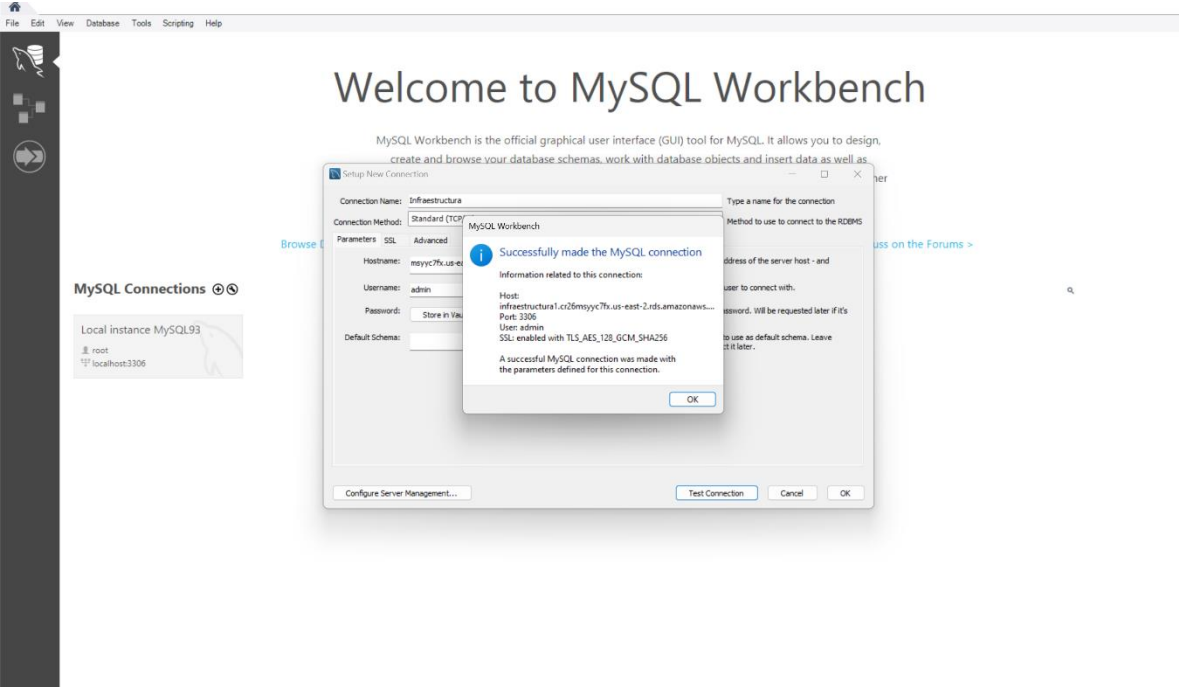
Reglas de entrada (2)

[Administrar etiquetas](#) [Edit](#)

Buscar

	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos
<input type="checkbox"/>	-	sgr-0598dd158fc61cb42	IPv4	MYSQL/Aurora	TCP	3306
<input type="checkbox"/>	-	sgr-08938e6d0bfbdd8c8	-	Todo el tráfico	Todo	Todo

Conexión con MySQL workbench



En la opción de las reglas de entrada podemos configurar mas de ellas. Algo que debemos tener en cuenta es que la selección incorrecta de reglas puede dejar nuestra base de datos vulnerable a ataques no deseados, por ejemplo tener mas puertos abiertos, incrementa la posibilidad de que algún intruso se conecte y comprometa la información que tenemos.

Reglas de entrada (6)							
<div>Buscar</div>							
1 gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción	
37f7e17	-	RDP	TCP	3389	sg-0c636b7b8604b027d / default	-	
34d36d0	IPv4	Todos los ICMP IPv4	ICMP	Todo	0.0.0.0/0	-	
9eb888	IPv6	Todos los ICMP IPv6	ICMP IPv6	Todo	:::0	-	
:61cb42	IPv4	MYSQL/Aurora	TCP	3306	0.0.0.0/0	-	
b48bb1	IPv6	MYSQL/Aurora	TCP	3306	:::0	-	
fbdd8c8	-	Todo el tráfico	Todo	Todo	sg-0c636b7b8604b027d / default	-	

Protocolo	Puerto	Descripción	Estado Actual	Riesgo de Seguridad
Todos	Todos	Permite cualquier tipo de tráfico desde cualquier IP	Activo (IPv4 y IPv6)	Muy riesgoso: puerta abierta total
TCP	443	HTTPS (conexiones seguras web)	Activo (IPv4 y IPv6)	Normal si usas servicios web
TCP	3389	RDP (Remote Desktop)	Limitado a grupo SG	Riesgo medio: depende del acceso

Para mejorar la seguridad se podría deshabilitar las reglas que permiten todo el tráfico. ya que permiten que cualquier persona en Internet acceda a todos los puertos de tu servidor. Es una puerta completamente abierta.

Todo el tráfico – Todo – 0.0.0.0/0 (IPv4)

Todo el tráfico – Todo – ::/0 (IPv6)

Si estamos usando MySQL podríamos habilitar solo el puerto 3306 con el origen de nuestra IP

Puerto: 3306

Origen: Tu dirección IP pública (por ejemplo, 189.144.23.51/32)

Esto significa que solo nuestra IP podrá conectarse a la base de datos.

Si usamos una web app se podría mantener el puerto 443:

Puerto: 443

Origen: 0.0.0.0/0 o solo tu país si es una app privada

Si la app web es pública, puedes dejar este puerto abierto globalmente.

El puerto 3389 RDP, se debería restringir:

RDP es un blanco frecuente de ataques automáticos (bots) que prueban combinaciones de usuario/contraseña.

Muchas filtraciones y ransomware (como el famoso ataque a hospitales) empezaron con acceso por RDP mal asegurado.