Base de datos y Buckets

Configuración de la Base de Datos MySQL y Buckets

Este documento describe la configuración de la base de datos y los buckets y por qué de estas.

**1. Selección del Motor de Base de Datos:**

* **Motor:** MySQL
* **Edición:** Comunidad de MySQL
* **Versión del motor:** MySQL 8.0.41

**Justificación:** Se eligió MySQL por su ecosistema maduro, buen rendimiento, compatibilidad y costo-efectividad, especialmente en el contexto de su fácil gestión a través de Amazon RDS, La versión 8.0.41 ofrece las últimas funcionalidades y mejoras de seguridad.

**2. Configuración de la Instancia:**

* **Plantilla:** Producción

**Justificación:** Se seleccionó la plantilla de "Producción" para aplicar configuraciones predeterminadas optimizadas para la alta disponibilidad y el rendimiento constante, cruciales para un entorno robusto.

* **Clase de instancia:** db.t4g.micro

**Justificación:** Se eligió una instancia de la familia t4g (instancias ampliables con procesadores ARM Graviton2) de tamaño micro para comenzar con un costo optimizado durante las fases iniciales. Esta instancia proporciona recursos suficientes para desarrollo y pruebas. Para producción, se deberá escalar según la carga real.

* **Almacenamiento:**
  + **Tipo de almacenamiento:** SSD de uso general (gp2)
  + **Almacenamiento asignado:** 20 GiB

**Justificación:** El almacenamiento SSD de uso general (gp2) ofrece un equilibrio adecuado entre costo y rendimiento para cargas de trabajo generales. Se asignaron 20 GiB como tamaño inicial, con la posibilidad de escalar verticalmente en el futuro si es necesario.

**3. Disponibilidad y Durabilidad:**

* **Opción de implementación:** Implementación de instancia de base de datos Multi-AZ (2 instancias)

**Justificación:** Se habilitó la implementación Multi-AZ para garantizar la alta disponibilidad. Esto crea una instancia primaria y una réplica de standby en diferentes Zonas de Disponibilidad dentro de la región de AWS. En caso de falla de la instancia primaria, RDS realiza un failover automático a la réplica, minimizando el tiempo de inactividad.

* **Identificador de instancias de base de datos:** Devops-basedata

**Justificación:** Se asignó un nombre único y descriptivo para identificar fácilmente esta instancia de base de datos dentro de la cuenta de AWS.

**4. Configuración de Credenciales:**

* **Nombre de usuario maestro:** admin
* **Administración de credenciales:** Autoadministrado
* **Contraseña maestra:** proyectodevops

**Justificación:** Se configuró un nombre de usuario maestro para la administración inicial de la base de datos. Se optó por la administración autoadministrada para tener control directo sobre la contraseña, la cual se definió siguiendo las recomendaciones de seguridad.

**5. Conectividad:**

* **Recurso de computación:** No se conecte a un recurso informático EC2

**Justificación:** Se seleccionó esta opción para configurar el acceso a la base de datos a través de los grupos de seguridad de la VPC, lo que proporciona un control de acceso más granular y seguro.

* **Tipo de red:** IPv4

**Justificación:** Se seleccionó IPv4 como el protocolo de red principal para la conectividad.

* **Nube privada virtual (VPC):** vpc-0b104fb4d01883cc3

**Justificación:** La base de datos se creó dentro de la VPC principal de la infraestructura, lo que garantiza el aislamiento de la red y la comunicación segura con otros recursos dentro de la misma VPC.

* **Grupo de subredes de base de datos:** (Subgrupo de subredes asociado a las subredes privadas para RDS)

**Justificación:** Se seleccionó un subgrupo de subredes que abarca las subredes privadas designadas para las bases de datos en las diferentes Zonas de Disponibilidad, lo que es un requisito para la implementación Multi-AZ.

* **Acceso público:** No

**Justificación:** Se deshabilitó el acceso público directo a la base de datos para mejorar la seguridad, asegurando que solo los recursos dentro de la VPC puedan acceder a ella.

* **Grupo de seguridad de VPC (firewall):** Elegir existente: db-sg

**Justificación:** Se seleccionó un grupo de seguridad existente llamado db-sg para controlar el tráfico entrante y saliente de la base de datos. **Es crucial que las reglas de entrada de este grupo de seguridad estén configuradas para permitir el tráfico TCP en el puerto 3306 (el puerto predeterminado de MySQL) desde el grupo de seguridad asociado a las instancias de la capa de aplicación.**

**6. Opciones Adicionales (Configuración Predeterminada o según sea necesario):**

* Puerto de la base de datos: 3306 (predeterminado para MySQL)
* Grupo de parámetros: (Predeterminado o personalizado según necesidades específicas)
* Copia de seguridad automática: Habilitada (con un período de retención a definir según la política de retención de datos)
* Mantenimiento: (Ventana de mantenimiento preferida para actualizaciones)

Configuración del Bucket:

**1. Configuración General:**

* **Nombre del bucket:** [cubetadevops](https://us-east-1.console.aws.amazon.com/s3/buckets/cubetadevops?region=us-east-1)

**Justificación:** Se eligió este nombre para identificar claramente el propósito del bucket dentro del proyecto. **Es importante recordar que los nombres de los buckets S3 deben ser únicos a nivel global en AWS.**

**2. Propiedad de Objetos:**

* **ACL deshabilitadas (**

**Justificación:** Se desactivaron las Listas de Control de Acceso (ACL) siguiendo las recomendaciones de AWS. La gestión de permisos se realizará principalmente a través de políticas de bucket y políticas de IAM, lo que proporciona un modelo de control de acceso más robusto y centralizado.

**3. Configuración de Bloqueo de Acceso Público:**

* **Bloquear todo el acceso público:** Activado

**Justificación:** Se activó el bloqueo de todo el acceso público para garantizar la seguridad del bucket y sus objetos, evitando exposiciones accidentales de datos a internet. El acceso a los objetos se gestionará de forma controlada a través de políticas específicas.

**4. Control de Versiones de Buckets:**

* **Control de versiones:** Desactivar

**Justificación:** Se desactivó el control de versiones. En este momento, no se considera necesario mantener un historial de las versiones de los objetos almacenados en el bucket. Si en el futuro se requiere esta funcionalidad para la recuperación ante errores o el seguimiento de cambios, se podrá habilitar posteriormente.

**5. Cifrado Predeterminado:**

* **Tipo de cifrado:** Cifrado del servidor con claves administradas de Amazon S3 (SSE-S3)

**Justificación:** Se seleccionó el cifrado gestionado por S3 (SSE-S3) como una solución de cifrado en reposo sencilla y segura. AWS gestiona las claves de cifrado, lo que simplifica la configuración y garantiza la protección de los datos almacenados en el bucket sin costos adicionales directos de gestión de claves.

* **Clave de bucket:** Desactivar

**Justificación:** Se desactivó la clave de bucket, utilizando la clave de cifrado predeterminada de S3 para el cifrado de los objetos.

Capturas sobre configuración de la DB y Bucket.

DB:

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Una captura de pantalla de una computadora

El contenido generado por IA puede ser incorrecto.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

Captura de pantalla de computadora

El contenido generado por IA puede ser incorrecto.

Bucket:

Una captura de pantalla de una computadora

El contenido generado por IA puede ser incorrecto.

Captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.