[Publish] - 3. Las bases de datos de AWS RDS deben estar cifradas usando Llaves Gestionadas por el Cliente (CMKs)

El hallazgo de seguridad **"Las bases de datos de AWS RDS deben estar cifradas usando Llaves Gestionadas por el Cliente (CMKs) de KMS"** se enfoca en elevar el estándar de protección para tus datos más sensibles. Por defecto, AWS RDS cifra los datos en reposo utilizando llaves gestionadas por AWS. Si bien esto proporciona una capa base de seguridad, el uso de **Llaves Gestionadas por el Cliente (CMKs)** te otorga un control mucho más granular y auditable sobre quién puede acceder a tus datos y bajo qué condiciones.

Las ventajas clave de usar CMKs incluyen:

- **Control de Acceso Centralizado:** Gestionas las políticas de acceso a la llave de cifrado directamente en KMS, separando la gestión de la llave de la gestión de la base de datos.
- **Rotación de Llaves:** Puedes definir y controlar el ciclo de vida de la llave, incluyendo la rotación automática, para cumplir con estrictos requisitos de cumplimiento.
- **Auditoría Detallada:** Cada uso de tu CMK (para cifrar o descifrar) se registra en CloudTrail, proporcionando una pista de auditoría completa sobre el acceso a tus datos.
- **Posibilidad de Revocar Acceso:** Si es necesario, puedes deshabilitar la llave en KMS, haciendo que los datos en la base de datos sean criptográficamente inaccesibles, incluso para los administradores de RDS.

Análisis de las Bases de Datos Reportadas

Las siguientes instancias de bases de datos RDS han sido identificadas por no utilizar una Llave Gestionada por el Cliente (CMK) para su cifrado.

Tipo	Nombre de la Instancia	Número de Cuenta
Rds	bdcarti2	890342916428
Rds	bdcartidev	890342916428
Rds	bdmoodle	002670977573
Rds	biometricos	002670977573
Rds	cotiza	890342916428
Rds	devappdomicilio	002670977573

Rds	devappdomreplica	002670977573
Rds	istimev4	002670977573
Rds	qascarti	890342916428

Preguntas para tu Equipo (Acción Requerida)

La remediación de este hallazgo no es trivial, ya que **no se puede cambiar la llave de cifrado de una instancia de RDS existente**. El proceso requiere crear una nueva instancia a partir de una snapshot. Por favor, coordina con los dueños de las aplicaciones y bases de datos para planificar lo siguiente:

1. **Ventana de Mantenimiento:** ¿Cuándo podrán programar una ventana de mantenimiento para cada una de estas bases de datos? El proceso implicará detener la instancia, tomar una snapshot, restaurarla como una nueva instancia cifrada con una CMK y finalmente, actualizar las aplicaciones para que apunten al nuevo endpoint de la base de datos.
2. **Creación de CMK:** ¿Ya existe una CMK apropiada en KMS para cada aplicación/entorno, o necesitan crear nuevas llaves? Es una buena práctica tener llaves separadas para diferentes aplicaciones o entornos (producción vs. no producción).

Consideraciones de Costo

Cambiar de una llave gestionada por AWS a una CMK introduce un nuevo costo.

- **Llaves Gestionadas por AWS:** El uso de estas llaves para el cifrado de RDS es **gratuito**.
- **Llaves Gestionadas por el Cliente (CMKs):**
  - **Costo de Almacenamiento de la Llave:** Cada CMK tiene un costo de **$1 USD al mes**.
  - **Costo de Solicitudes a la API:** Se te cobrará por las solicitudes que RDS y otras aplicaciones hagan a KMS para usar la llave (ej. para cifrar/descifrar datos). Este costo es generalmente bajo, alrededor de **$0.03 USD por cada 10,000 solicitudes**.

Conclusión sobre Costos:

Adoptar CMKs para RDS introduce un costo mensual fijo por cada llave y un costo variable muy pequeño por su uso. Este es el precio de obtener un control de seguridad superior, una auditoría detallada y la capacidad de gestionar centralizadamente el acceso a los datos cifrados.

Cómo Solucionarlo: Migración a una Instancia Cifrada con CMK

Como se mencionó, no se puede cambiar la llave de una base de datos en funcionamiento. El proceso correcto es el siguiente:

1. **Crear una CMK en KMS:** Si aún no tienes una, ve al servicio de KMS y crea una nueva llave simétrica. Asegúrate de definir una política de llave que otorgue los permisos necesarios a los usuarios y roles que la administrarán.
2. **Tomar una snapshot:**
   - Navega a la consola de **RDS**.
   - Selecciona la instancia de base de datos que deseas migrar.
   - En el menú **Acciones**, elige **Tomar snapshot**.
3. **Copiar la snapshot con la Nueva Llave:**
   - Una vez que el snapshot esté completo, selecciónalo.
   - En el menú **Acciones**, elige **Copiar snapshot**.
   - En la pantalla de copia, en la sección **Cifrado**, selecciona **Habilitar cifrado**.
   - En la lista desplegable **Clave Maestra de AWS KMS**, elige la CMK que creaste en el paso 1.
   - Inicia la copia.
4. **Restaurar el Nueva snapshot Cifrado:**
   - Una vez que la copia del snapshot esté completa, selecciónala.
   - En el menú **Acciones**, elige **Restaurar snapshot**.
   - Configura la nueva instancia de base de datos (tamaño, grupo de seguridad, etc.) como lo necesites. Confirma que la sección de cifrado muestra que se está utilizando tu CMK.
   - Inicia la restauración.
5. **Actualizar Aplicaciones y Desmantelar la Antigua Instancia:**
   - Una vez que la nueva instancia esté disponible, actualiza las cadenas de conexión en tus aplicaciones para que apunten al nuevo endpoint de la base de datos.
   - Después de verificar que todo funciona correctamente, puedes eliminar la instancia de base de datos original para evitar costos innecesarios.

Recomendación

Se recomienda que planifiquen la migración de estas bases de datos para que utilicen Llaves Gestionadas por el Cliente (CMKs). Este es un estándar de la industria para proteger datos sensibles y es un requisito común para muchos marcos de cumplimiento. Prioriza las bases de datos de producción y las que contienen la información más crítica.

Referencias

Encrypting Amazon RDS resources - Amazon Relational Database Service