[Publish] - 5. Los volúmenes de EBS deben estar cifrados

El hallazgo de seguridad **"Los volúmenes de EBS deben estar cifrados"** se enfoca en la protección de tus "discos duros virtuales". Un volumen de EBS es el almacenamiento a nivel de bloque para tus instancias EC2. Si un volumen no está cifrado, los datos en reposo son vulnerables. En el caso de un acceso no autorizado al sistema de almacenamiento subyacente de AWS, o si un snapshot de este volumen se comparte incorrectamente, los datos podrían ser leídos.

El cifrado de volúmenes de EBS es una práctica de seguridad fundamental que:

- **Protege los Datos Sensibles:** Asegura que los datos en tus discos duros virtuales sean ilegibles sin la clave de cifrado.
- **Cumple con Normativas:** Es un requisito común para estándares de cumplimiento como PCI DSS, HIPAA y GDPR.
- **Habilita el Cifrado de Extremo a Extremo:** Al cifrar el volumen (datos en reposo) y usar HTTPS (datos en tránsito), se logra una protección integral de los datos.

Análisis de los Volúmenes Reportados

Los siguientes volúmenes de EBS han sido identificados por no tener el cifrado habilitado, lo que representa un riesgo para los datos que almacenan.

Ver archivo adjunto “5. Los volúmenes de EBS deben estar cifrados.csv“

Preguntas para tu Equipo (Acción Requerida)

La remediación de este hallazgo es un proceso delicado, ya que **no se puede cifrar un volumen de EBS existente mientras está en uso**. El proceso requiere reemplazar el volumen, lo que implica una **ventana de mantenimiento y tiempo de inactividad (downtime)** para la instancia EC2 asociada.

1. **Identificar Dependencias:** ¿A qué instancia EC2 está adjunto cada uno de estos volúmenes y cuál es la función de esa instancia (producción, desarrollo, etc.)?
2. **Programar Ventana de Mantenimiento:** ¿Cuándo se puede programar una ventana de mantenimiento para cada instancia afectada? Es crucial planificar esto para minimizar el impacto en las operaciones.
3. **Selección de Clave KMS:** ¿Se utilizará la clave gestionada por AWS por defecto para EBS (`aws/ebs`) o existe una Llave Gestionada por el Cliente (CMK) específica que debamos usar?

Consideraciones de Costo

- **Costo del Volumen:** No hay diferencia de precio entre un volumen de EBS cifrado y uno no cifrado.
- **Rendimiento:** El cifrado de EBS tiene un impacto mínimo y casi imperceptible en el rendimiento.
- **Uso de Claves KMS:** Si utilizas la clave gestionada por AWS (`aws/ebs`), no hay costo adicional. Si decides usar una Llave Gestionada por el Cliente (CMK), se aplicará el costo estándar de **$1 USD al mes por la llave**.

Conclusión sobre Costos:

El proceso de migración no tiene un costo significativo más allá del almacenamiento temporal de los snapshots. El costo operativo de mantener un volumen cifrado es prácticamente idéntico al de uno no cifrado.

Cómo Solucionarlo: Migrar a un Volumen Cifrado

Este proceso debe realizarse durante una ventana de mantenimiento planificada.

1. **Detener la Instancia EC2:** Para garantizar la consistencia de los datos, detén la instancia a la que está adjunto el volumen.
2. **Crear un Snapshot:** Crea un snapshot del volumen sin cifrar.
3. **Copiar el Snapshot (Habilitando el Cifrado):**
   - Una vez que el snapshot esté completo, selecciónalo.
   - En el menú **Acciones**, elige **Copiar snapshot**.
   - En la pantalla de copia, marca la casilla **Cifrar este snapshot**.
   - Selecciona la **Clave de KMS** que deseas utilizar (`aws/ebs` o una CMK).
   - Inicia la copia.
4. **Crear un Nuevo Volumen Cifrado:**
   - A partir del **snapshot recién copiado y cifrado**, crea un nuevo volumen. Asegúrate de crearlo en la misma Zona de Disponibilidad que tu instancia EC2.
5. **Reemplazar el Volumen:**
   - En la configuración de la instancia EC2, **desmonta (detach)** el volumen original sin cifrar. Anota el punto de montaje (ej. `/dev/sda1`).
   - **Monta (attach)** el nuevo volumen cifrado a la instancia, asegurándote de usar el mismo punto de montaje que tenía el original.
6. **Reiniciar y Validar:**
   - Inicia la instancia EC2.

- Valida que el sistema operativo se inicie correctamente y que todas las aplicaciones funcionen como se espera.

7. **Limpieza:**
   - Una vez que hayas confirmado que todo funciona, puedes eliminar de forma segura el **volumen original sin cifrar** y los **snapshots temporales** que creaste durante el proceso.

Recomendación

1. **Remediación:** Se recomienda que se planifique y ejecute la migración de todos los volúmenes no cifrados a volúmenes cifrados, comenzando por los entornos de producción y aquellos que contienen los datos más sensibles.
2. **Prevención Definitiva:** La mejor manera de evitar este problema en el futuro es habilitando el **cifrado de EBS por defecto** en la configuración de EC2 para cada región de AWS. Al activar esta opción, todos los nuevos volúmenes de EBS creados en esa región se cifrarán automáticamente, eliminando la posibilidad de error humano y estableciendo una base de seguridad sólida.

Referencias

Amazon EBS encryption - Amazon EBS