


[Publish] - 4. Los snapshots de EBS deben estar cifrados

El hallazgo de seguridad "**Los snapshots de EBS deben estar cifrados**" se enfoca en una capa fundamental de la estrategia de defensa en profundidad: la protección de datos en reposo. Un snapshot de EBS es una copia de seguridad de un volumen de disco en un momento específico. Si este snapshot no está cifrado, cualquier persona que obtenga acceso no autorizado a él (ya sea por un error de permisos o por una brecha de seguridad) podría crear un volumen a partir de él y leer todos los datos contenidos.

Cifrar los snapshots asegura que, incluso si el archivo del snapshot es accedido, los datos subyacentes permanezcan ilegibles sin la clave de cifrado correspondiente. Esta es una medida de seguridad crucial para proteger datos sensibles, propiedad intelectual y cumplir con diversas normativas de cumplimiento.

Análisis de los Snapshots Reportados

 Hay **2329** Snapshots reportados. Ver el archivo adjunto "4. Los Snapshots de EBS deben estar cifrados.csv"

Preguntas para tu Equipo (Acción Requerida)

La remediación implica crear una copia cifrada de cada snapshot. Antes de proceder, es importante coordinar con los equipos de infraestructura.

1. **¿Estos snapshots todavía son necesarios?** Es posible que algunos sean antiguos y ya no se requieran. Eliminar snapshots innecesarios es una buena práctica de higiene y ahorro de costos.
2. **¿Qué clave de KMS se debe usar?** ¿Se utilizará la clave gestionada por AWS por defecto para EBS (`aws/ebs`) o existe una Llave Gestionada por el Cliente (CMK) específica que se deba usar para estos recursos?

Consideraciones de Costo

- **Proceso de Cifrado:** No hay un costo directo por la operación de copiar un snapshot para cifrarlo.
- **Almacenamiento del Snapshot:** Se te cobrará por el almacenamiento tanto del snapshot original sin cifrar como de la nueva copia cifrada. Una vez que hayas validado la copia cifrada, puedes eliminar la original para evitar costos duplicados.
- **Uso de Claves KMS:** Si utilizas una Llave Gestionada por el Cliente (CMK), incurrirás en el costo estándar de **\$1 USD al mes por la llave**. El uso de la llave gestionada por AWS

(**aws/ebs**) no tiene costo de almacenamiento.

Conclusión sobre Costos:

El costo principal a considerar es el de eliminar snapshots que ya no sean necesarios. Una vez cifrados, el costo de almacenamieto será el mismo que tenerlos sin cifrar.

Cómo Solucionarlo: Crear una Copia Cifrada

No se puede cifrar un snapshot existente directamente. El proceso correcto es crear una copia cifrada del mismo.

1. Navegar a la Sección de Snapshots:

- Ve a la consola de **EC2**.
- En el panel de navegación izquierdo, en **Elastic Block Store**, elige **Snapshots**.

2. Copiar el Snapshot:

- Selecciona uno de los snapshots sin cifrar de la lista.
- Haz clic en el menú **Acciones** y selecciona **Copiar snapshot**.

3. Habilitar el Cifrado en la Copia:

- En la pantalla de copia, desplázate hacia abajo hasta la sección **Cifrado (Encryption)**.
- Marca la casilla **Cifrar este snapshot (Encrypt this snapshot)**.
- En la lista desplegable **Clave de KMS (KMS key)**, selecciona la clave de cifrado que desees utilizar. Puedes elegir la clave predeterminada (**aws/ebs**) o una CMK que hayas creado.
- Haz clic en **Copiar snapshot**.

4. Verificar y Limpiar:

- El proceso de copia comenzará. Una vez completado, tendrás un nuevo snapshot con un ID diferente que estará cifrado.
- Después de verificar que la copia cifrada es válida y que cualquier proceso que dependa de ella ha sido actualizado, puedes proceder a **eliminar el snapshot original sin cifrar** para evitar costos innecesarios.

5. Repetir: Realiza este proceso para todos los snapshots sin cifrar identificados.

Recomendación

1. Eliminar snapshot innecesarios. Esto ayudará a reducir costos de almacenamiento.
2. **Remediación:** Se recomienda que se inicie el proceso de copiar y cifrar todos los snapshots listados, y luego eliminar las versiones originales sin cifrar.

3. **Prevención:** La mejor manera de prevenir este problema es habilitando el **cifrado de EBS por defecto** en cada región de AWS. Esta configuración a nivel de cuenta asegura que todos los nuevos volúmenes de EBS y, por lo tanto, todos los snapshots creados a partir de ellos, se cifren automáticamente desde el momento de su creación. Esto elimina la posibilidad de error humano y garantiza una postura de seguridad de cifrado por defecto.

Referencias

 [Amazon EBS encryption - Amazon EBS](#)