[Publish] - 6. Cifrar Imágenes de Amazon (AMIs)

El hallazgo de seguridad **"Cifrar Imágenes de Amazon (AMIs)"** se enfoca en la protección de las plantillas base que utilizas para lanzar tus instancias EC2. Una AMI es esencialmente una "fotografía" de un servidor configurado, que incluye el sistema operativo, las aplicaciones y los datos.

Una AMI no cifrada se basa en snapshots de EBS que tampoco están cifrados. Esto representa un riesgo de seguridad significativo:

- **Exposición si se Comparte Accidentalmente:** Si una AMI no cifrada se comparte públicamente por error, cualquier persona podría lanzar una instancia a partir de ella y obtener acceso completo a la configuración de tu sistema y a cualquier dato o credencial que estuviera en la imagen.
- **Datos en Reposo Vulnerables:** Los datos dentro de los snapshots subyacentes no están protegidos criptográficamente en reposo.

Cifrar una AMI asegura que tanto la imagen como sus snapshots asociados estén cifrados, protegiendo así la propiedad intelectual, las configuraciones seguras y cualquier dato sensible contenido en tus plantillas de servidor.

Análisis de las AMIs Reportadas

Las siguientes Imágenes de Máquina de Amazon (AMIs) han sido identificadas por no estar cifradas.

Ver archivo adjunto “6. Cifrar Imágenes de Amazon (AMIs).csv”

Preguntas para tu Equipo (Acción Requerida)

Para remediar este hallazgo, es necesario crear una copia cifrada de cada AMI. Por favor, coordina con los equipos de infraestructura y desarrollo para responder lo siguiente:

1. **¿Estas AMIs todavía están en uso?** Es importante hacer un inventario y determinar si algunas de estas imágenes son antiguas y pueden ser dadas de baja (deregistradas) en lugar de ser migradas.
2. **¿Qué clave de KMS se utilizará para el cifrado?** ¿Se usará la clave gestionada por AWS por defecto (`aws/ebs`) o existe una Llave Gestionada por el Cliente (CMK) específica para estas aplicaciones o entornos?

Consideraciones de Costo

- **Proceso de Cifrado:** No hay un costo directo por la operación de copiar una AMI para cifrarla.
- **Almacenamiento de la AMI:** Se te cobrará por el almacenamiento de los snapshots subyacentes tanto para la AMI original sin cifrar como para la nueva copia cifrada. Una vez que la nueva AMI cifrada esté validada y en uso, puedes dar de baja (deregistrar) la original para evitar costos duplicados.
- **Uso de Claves KMS:** Si utilizas una Llave Gestionada por el Cliente (CMK), se aplicará 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 de llave.

Conclusión sobre Costos:

El costo principal a considerar es el almacenamiento duplicado durante el proceso de migración. Una vez que se elimina la AMI original, el costo de almacenamiento será el mismo que antes.

Cómo Solucionarlo: Crear una Copia Cifrada de una AMI

No se puede cifrar una AMI existente directamente. El proceso implica crear una copia cifrada.

1. **Navegar a la Sección de AMIs:**
   - Ve a la consola de **EC2**.
   - En el panel de navegación izquierdo, en **Imágenes**, elige **AMIs**.
2. **Copiar la AMI:**
   - Selecciona una de las AMIs sin cifrar de la lista.
   - Haz clic en el menú **Acciones** y selecciona **Copiar AMI**.
3. **Habilitar el Cifrado en la Copia:**
   - En la pantalla de copia, en la sección **Cifrado (Encryption)**, marca la casilla **Cifrar snapshots de EBS de destino**.
   - En la lista desplegable **Clave Maestra**, selecciona la clave de KMS que deseas utilizar (la predeterminada `aws/ebs` o una CMK).
   - Haz clic en **Copiar AMI**.
4. **Verificar y Limpiar:**
   - El proceso de copia comenzará. Una vez completado, tendrás una nueva AMI con un ID diferente que estará cifrada.
   - Actualiza tus plantillas de lanzamiento (Launch Templates) o procesos de despliegue para usar la nueva AMI cifrada.

- Después de verificar que las nuevas instancias se lanzan correctamente desde la AMI cifrada, puedes **dar de baja (deregister)** la AMI original sin cifrar para evitar confusiones y costos innecesarios.

5. **Repetir:** Realiza este proceso para todas las AMIs sin cifrar que necesiten ser conservadas.

Recomendación

1. **Remediación:** Se recomienda que se inicie un inventario de las AMIs listadas para dar de baja las que ya no se necesiten. Para las AMIs que sigan siendo necesarias, ejecuten el proceso de copia y cifrado.
2. **Prevención:** La mejor práctica es asegurarse de que todos los volúmenes de EBS base a partir de los cuales se crean las AMIs estén cifrados. Habilitar el **cifrado de EBS por defecto** en cada región es la forma más efectiva de garantizar que todas las futuras AMIs y sus snapshots subyacentes se creen cifrados desde el principio.

Referencias

Use encryption with EBS-backed AMIs - Amazon Elastic Compute Cloud