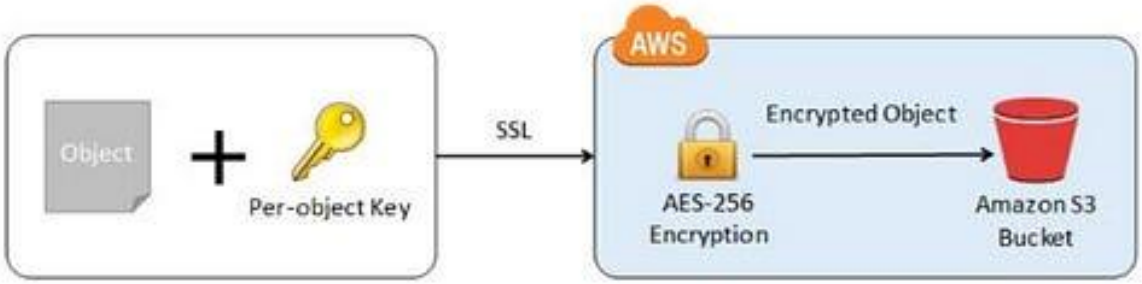
CloudOps Guild

Together, towards mastery in Cloud and DevOps

Cómo activar el cifrado en un bucket de S3



Server-Side Encryption with Customer-Provided Keys — SSE-C

Si quieres proteger tu información en AWS, activar el cifrado es una excelente práctica. Aquí te explico **paso a paso** cómo habilitar el cifrado en un bucket de S3 y un volumen EBS, junto con algunas recomendaciones, observaciones importantes, y recursos adicionales.

Realizado por Mario R. Serrano Pineda

CloudOps Guild
Together, towards mastery in Cloud and DevOps

Nota importante: A partir de enero del 2023, AWS obliga a encriptar la información de todo bucket que se crea en AWS, por eso en este articulo se muestran las dos opciones, activar cifrado para buckets creados antes de esta fecha y la opción de crear un bucket nuevo con la opción de cifrado ya habilitada por defecto.

Conceptos

Cifrado de datos

El cifrado de datos es un proceso diseñado para proteger la información mediante su codificación. Esto se logra a través del uso de contraseñas o claves de cifrado junto con algoritmos especializados. Los datos cifrados solo pueden ser descifrados y accesibles mediante la contraseña o clave adecuada. Este método es esencial para mantener la confidencialidad de los

datos digitales, incluso si personas no autorizadas logran acceder a ellos, ya sea de forma lógica o física. Sin la clave o contraseña correspondiente, los datos permanecen ilegibles. Los algoritmos modernos de cifrado dificultan enormemente, e incluso hacen casi imposible, descifrar claves largas o contraseñas complejas. Algunos de los algoritmos más comunes incluyen AES, 3DES, RSA y Blowfish, entre otros. Los tipos principales de criptografía son la de clave simétrica y la de clave asimétrica.

Recomendación de Amazon sobre cifrado en S3

Amazon sugiere utilizar el cifrado en S3 para almacenar datos en sus buckets, principalmente por razones de seguridad. Este enfoque mejora la privacidad y la protección de los datos almacenados. Además, existe otra razón clave para cifrar los

datos en la nube: la jurisdicción internacional. Amazon almacena información de clientes de distintos países, y en ocasiones, un gobierno puede solicitar acceso a los datos como parte de una investigación legal. Sin embargo, Amazon debe equilibrar estas solicitudes con el cumplimiento de acuerdos de licencia y leyes de otros países involucrados, lo que podría generar conflictos.

Cifrado del lado del servidor (SSE)

El cifrado del lado del servidor (SSE) es una solución sencilla para proteger datos en AWS. En este modelo, los datos se envían a AWS en su forma original (sin cifrar) y luego se cifran automáticamente al ser almacenados en la nube. Cuando los datos son recuperados, AWS se encarga de descifrarlos y los envía al usuario en su forma original. Este proceso es completamente transparente para el usuario final.

CloudOps Guild

Together, towards mastery in Cloud and DevOps

Métodos de cifrado SSE

1. **SSE-S3**:

   Este método es el más simple. AWS gestiona por completo las claves utilizadas para cifrar los datos, las cuales no están disponibles para el cliente. Se utiliza el algoritmo AES-256, un estándar de cifrado simétrico con claves de 256 bits. Si confías plenamente en AWS para gestionar las claves, este método es una opción adecuada.

2. **SSE-KMS**:

   Con SSE-KMS, el servicio AWS Key Management Service (KMS) gestiona el cifrado de los datos. Aunque AWS administra las claves de datos, el cliente controla la clave maestra (CMK) en el servicio KMS. Este método ofrece mayor control al usuario, además de proporcionar una pista de auditoría para mayor transparencia.

3. **SSE-C**:

   Este método permite al cliente proporcionar y gestionar sus propias claves de cifrado. AWS no almacena estas claves, sino que las utiliza temporalmente para las solicitudes de cifrado y descifrado. El usuario es responsable de mantener la seguridad de estas claves. Es importante destacar que este método solo funciona mediante conexiones HTTPS, garantizando una mayor seguridad durante las transferencias de datos.

4. **Cifrado de Doble Capa del Servidor con claves de AWS Key Management Service (DSSE-KMS)**

   Es una característica avanzada de seguridad ofrecida por AWS para proteger los datos almacenados en servicios como Amazon S3. Este mecanismo utiliza

dos capas independientes de cifrado para proporcionar una protección adicional a los datos.

El cifrado del lado del servidor es una herramienta esencial para asegurar la privacidad y la integridad de los datos almacenados en la nube de AWS.

Pasos para activar cifrado.

Parte 1: Activar cifrado en un bucket de S3

El cifrado en Amazon S3 garantiza que los datos se almacenan de forma segura en AWS.

Paso a paso:

1. **Accede a la consola de AWS**

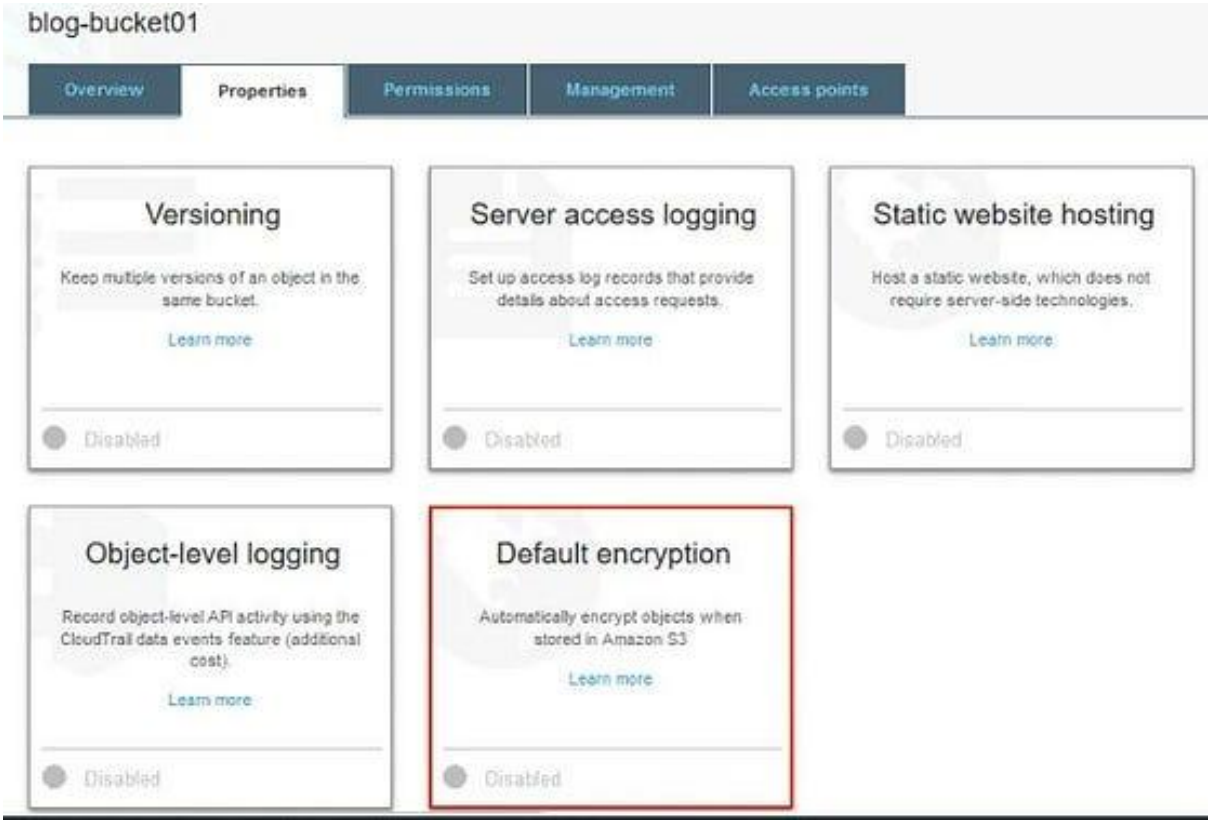
   Ve a Consola de AWS.

2. Busca el servicio de S3

3. Si es un bucket creado antes del 2023

Selecciona el bucket e ingresa menu propiedades

- En la lista de buckets, haz clic en el nombre del bucket al que quieres habilitar el cifrado e ingresa menú propiedades



Activar encriptación en bucket antiguo

Configura el cifrado

En la pestaña *Propiedades* del bucket, busca la sección *Default Encryption* (Cifrado predeterminado).

Haz clic en **Edit** (Editar).

Selecciona el tipo de cifrado y da en guardar.

4. Si es un bucket nuevo que estas creando, llena la información de nombre y baja a la opción de **cifrado predetrminado** y selecciona el metodo de cifrado que quieras y luego en crear bucket.

Elige el tipo de cifrado:

a. **AWS Key Management Service (SSE-KMS)**: Más control sobre las claves.

b. **Amazon S3-Managed Keys (SSE-S3)**: AWS gestiona las claves.

- Si seleccionas **SSE-KMS**, elige una clave gestionada por AWS (default key) o una clave personalizada (CMK).

c. **Cifrado de Doble Capa del Servidor con claves de AWS Key Management Service (DSSE-KMS)**

Recomendaciones para S3:

- **Usa SSE-KMS para datos sensibles**: Esto te permite controlar las claves y realizar auditorías.
- **Habilita el versionado del bucket**: Así proteges contra la pérdida o corrupción accidental de datos.
- **Activa los registros de acceso a S3**: Para monitorear las solicitudes y posibles actividades sospechosas.
- **Verifica el cumplimiento de cifrado**: Usa herramientas como **AWS Config** para asegurarte de que los buckets no cifrados sean marcados.

CloudOps Guild
Together, towards mastery in Cloud and DevOps

Observaciones importantes:

1. **Cargos adicionales**: El uso de claves personalizadas (CMK) con KMS puede generar costos adicionales.
2. **Restricciones de cifrado**: Algunos servicios o regiones pueden no soportar ciertos métodos de cifrado.

Recursos oficiales:

- Documentación sobre cifrado en S3
- AWS Key Management Service (KMS)
- **Video explicativo en youtube**

Con estos pasos y recomendaciones, estarás mejor preparado para proteger tu información en AWS. **¿Listo para activar el cifrado?** 👨‍💻