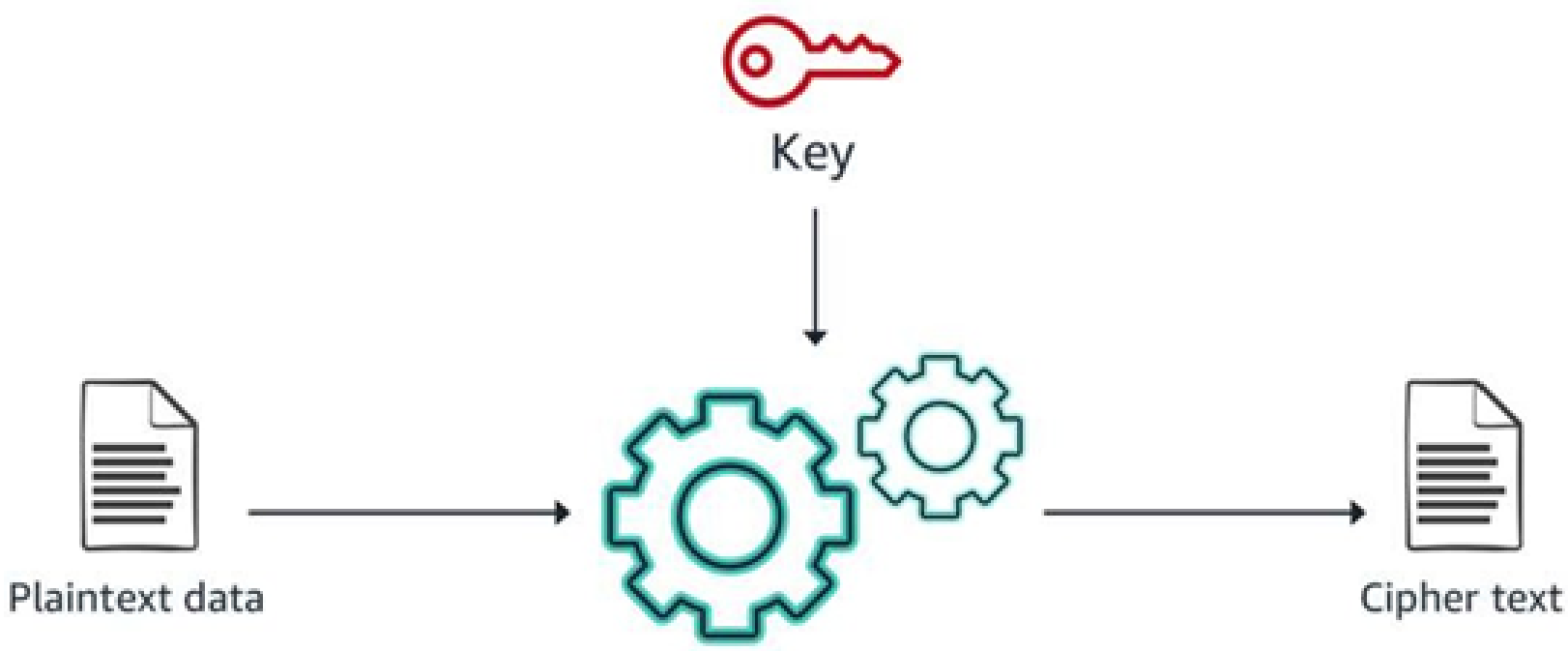
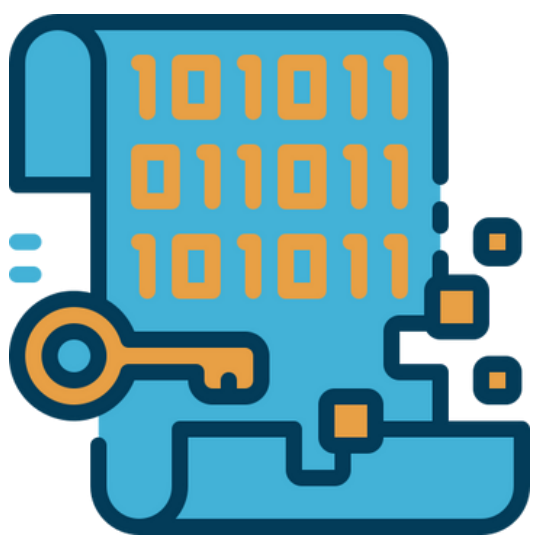
LECCIÓN 3: PROTECCIÓN MEDIANTE CIFRADO

CIFRADO: QUÉ, CÓMO Y POR QUÉ



El cifrado funciona utilizando un algoritmo con una clave para convertir datos de texto sin formato en datos ilegibles (texto cifrado) que solo pueden leerse de nuevo con la clave correcta. Por ejemplo, una frase simple como “¡Hola, mundo!” puede verse como 1c28df2b595b4e30b7b07500963dc7c” cuando se cifra.



Existen varios algoritmos de cifrado diferentes; todos usan diferentes tipos de claves. Un algoritmo de cifrado fuerte se basa en propiedades matemáticas para producir un texto cifrado que no puede descifrarse utilizando cualquier cantidad de potencia de cálculo prácticamente disponible sin tener también la clave necesaria. Por lo tanto, proteger y administrar las claves se convierte en una parte crítica de cualquier solución de cifrado.

COMPARACIÓN DEL CIFRADO DEL LADO DEL SERVIDOR Y DEL LADO DEL CLIENTE

Comparación del cifrado del lado del servidor y del lado del cliente	CIFRADO DEL LADO DEL SERVIDOR (SSE)
• Su aplicación cifra los datos antes de enviarlos a AWS.	• AWS cifra los datos por usted después de que los recibe.
• Los datos se almacenan en su estado cifrado.	• El proceso es transparente para el usuario.
• Solo usted conoce las claves y los algoritmos.	

Según sus requisitos de seguridad, puede utilizar el cifrado del lado del servidor (SSE) o el cifrado del lado del cliente (CSE) para cifrar sus datos. Estos enfoques difieren en cuándo, dónde y quién cifra y descifra los datos. El enfoque no define necesariamente cómo se cifran los datos. Además, los enfoques no son exclusivos:
a menudo puede usar CSE y SSE en los mismos datos para obtener un perfil de seguridad mejorado. Cada enfoque tiene ventajas.

Con el cifrado del lado del cliente (CSE), sus aplicaciones cifran los datos a nivel local antes de enviarlos a AWS y los descifran después de recibirlos de AWS. Puede crear y administrar sus propias claves de cifrado. Los datos se almacenan en forma cifrada, con claves y algoritmos que solo usted conoce.

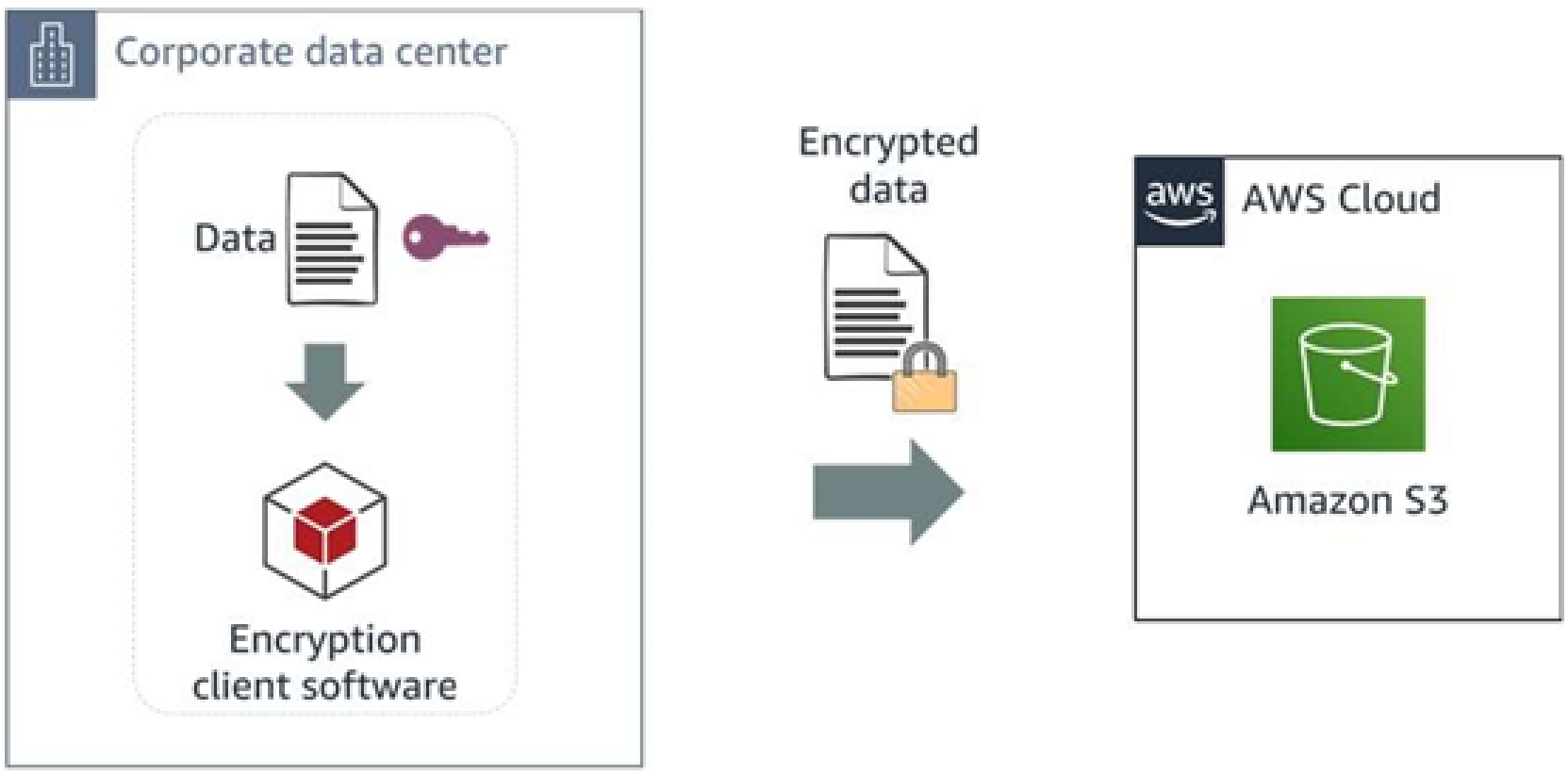
Con el cifrado del lado del servidor (SSE), la aplicación o el servicio que reciben los datos los cifran en su destino. Por ejemplo, si usa SSE con Amazon S3, el servicio cifra los datos a nivel de objeto mientras escribe en los discos en los centros de datos de AWS y los descifra cuando usted accede a ellos. El proceso de cifrado es transparente para el usuario.

AWS es compatible con el CSE y el SSE. La mayoría de los servicios de AWS que almacenan o administran datos de clientes ofrecen una opción de SSE o realizan el SSE en sus datos de forma predeterminada. Estos servicios cifran de forma transparente los datos antes de escribirlos en el disco y los descifran de forma transparente cuando accede a ellos. La mayoría de los servicios de AWS que admiten el SSE se integran con AWS KMS para mantener seguras las claves de cifrado que protegen sus datos. Aprenderá más sobre AWS KMS más adelante en este módulo.

Para más información, consulte “Protecting Data Using Encryption (Protección de los datos con cifrado)” en la Guía del usuario de Amazon Simple Storage Service en:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html

CIFRADO DEL LADO DEL CLIENTE

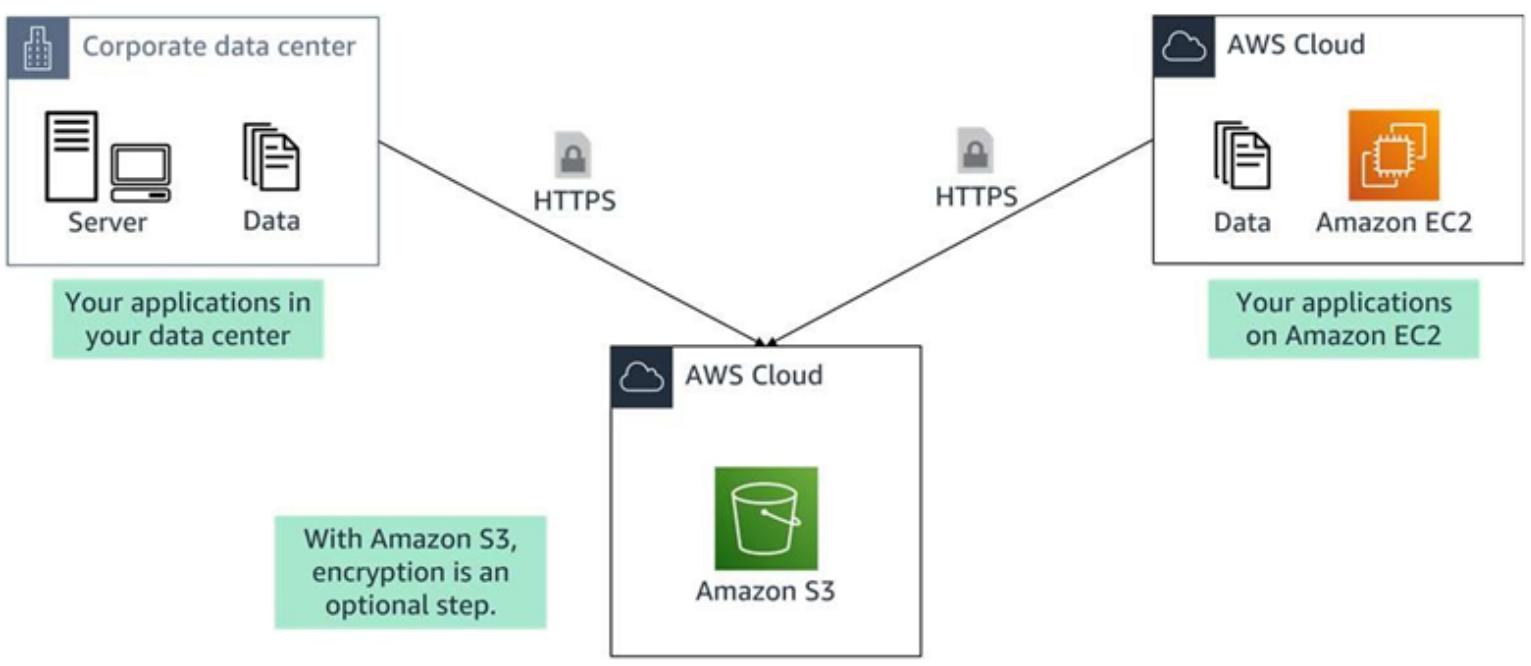


El cifrado del lado del cliente se lleva a cabo antes de que los datos se envíen a AWS y el descifrado se realiza después de recuperar los datos de AWS. Amazon S3 recibe los datos cifrados, pero no desempeña un rol en su cifrado o descifrado.

Para habilitar el cifrado del lado del cliente, puede usar una clave almacenada en AWS KMS o que usted almacene dentro de su aplicación.

AWS admite bibliotecas de cifrado del lado del cliente, como el SDK de cifrado de AWS, el cliente de cifrado de Amazon DynamoDB y los clientes de cifrado de Amazon S3.

CIFRADO DEL LADO DEL SERVIDOR DE AWS



El cifrado del lado del servidor es el cifrado de los datos en su destino por parte de la aplicación o el servicio que los recibe. Con el cifrado del lado del servidor de AWS, sus datos de origen provienen de sistemas de su centro de datos o una instancia de EC2. Puede cargar esos datos a través de una conexión HTTPS a cualquiera de los servicios de AWS que admitan el cifrado automático del lado del servidor. El punto de enlace de servicio se encargará de los procesos de cifrado y administración de la clave por usted.

Con Amazon S3, el cifrado es un paso opcional que usted especifica cuando carga sus datos en el servicio.

TIPOS DE CIFRADO DEL LADO DEL SERVIDOR DE AMAZON S3

SSE-C

• Usted conserva el control de las claves.

• Amazon S3 no almacena las claves de cifrado que usted proporciona,

SSE-S3

• AWS administra las claves.

• Las claves y los datos cifrados se almacenan en hosts separados,

SSE - KMS

• AWS administra las claves.

• Se utiliza una clave de sobre para mayor protección.

Para el cifrado del lado del servidor en Amazon S3, dispone de tres opciones que se excluyen mutuamente, según cómo elija administrar las claves de cifrado:

SSE con claves proporcionadas por el cliente (SSE-C)

Con el cifrado del lado del servidor con claves proporcionadas por el cliente (SSE-C), administra las claves de cifrado. Con la clave de cifrado que proporcione como parte de la solicitud, Amazon S3 administra tanto el cifrado, al escribir en los discos, como el descifrado, al obtener acceso a los objetos. No mantiene el código para realizar el cifrado y el descifrado de los datos, solo las claves.

Amazon S3 no almacena la clave de cifrado que usted proporciona. En cambio, se almacena un valor de código de autenticación de mensajes basado en un hash (HMAC) “salted” de forma aleatoria de la clave de cifrado para validar futuras solicitudes. El valor de HMAC “salted” no se puede usar para derivar el valor de la clave de cifrado ni para descifrar los contenidos del objeto cifrado. Esto implica que, si pierde la clave de cifrado, habrá perdido el objeto.

SSE con claves administradas por Amazon S3 (SSE-S3)

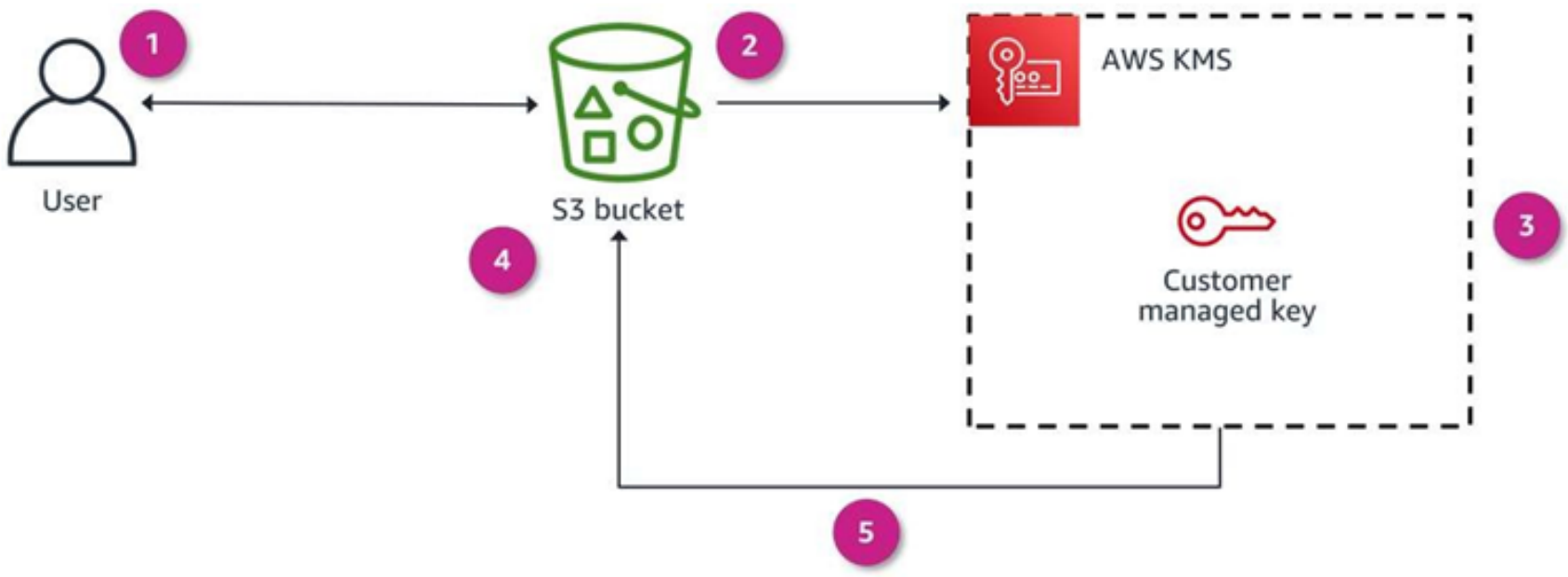
Cuando se usa el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3), cada objeto se cifra con una clave exclusiva. Como medida de seguridad adicional, Amazon S3 cifra la propia clave con una clave que el servicio rota de forma periódica. El SSE-S3 utiliza uno de los métodos de cifrado de bloques más potentes en el sector, el estándar de cifrado avanzado de 256 bits (AES-256), para cifrar los datos.

SSE con claves de AWS KMS (SSE-KMS)

El cifrado del lado del servidor con claves de AWS KMS (SSE-KMS) es similar al SSE-S3, pero con algunos beneficios adicionales y cargos por usar el servicio. Hay permisos independientes para el uso de una clave de KMS que ofrece protección agregada contra el acceso no autorizado de los objetos en Amazon S3. El SSE-KMS también le proporciona una pista de auditoría que muestra cuándo se utilizó la clave de KMS y quién lo hizo. Además, puede crear y administrar claves administradas por el cliente o utilizar claves de KMS administradas por AWS que sean únicas para usted, su servicio y su región. AWS KMS utiliza el cifrado de sobre para proteger aún más los datos. El cifrado de sobre es la práctica de cifrar datos de texto sin formato con una clave de datos y, a continuación, cifrar esa clave de datos con una clave raíz.

Para más información acerca de las opciones de cifrado del lado del servidor en Amazon S3, consulte “Protecting Data Using Server-Side Encryption (Proteger los datos con el cifrado del lado del servidor)” en la Guía del usuario de Amazon Simple Storage Service en https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html

INFORMACIÓN GENERAL SOBRE EL CIFRADO



En este escenario, AMS KMS se utiliza para cifrar datos en reposo (SSE-KMS). El usuario crea una clave de KMS y la utiliza para cifrar objetos almacenados en Amazon S3.

Este diagrama explica cómo ocurre el cifrado al cargar un archivo en Amazon S3:

1. Usted solicita cargar un archivo y almacenarlo como un objeto cifrado en un bucket de S3.

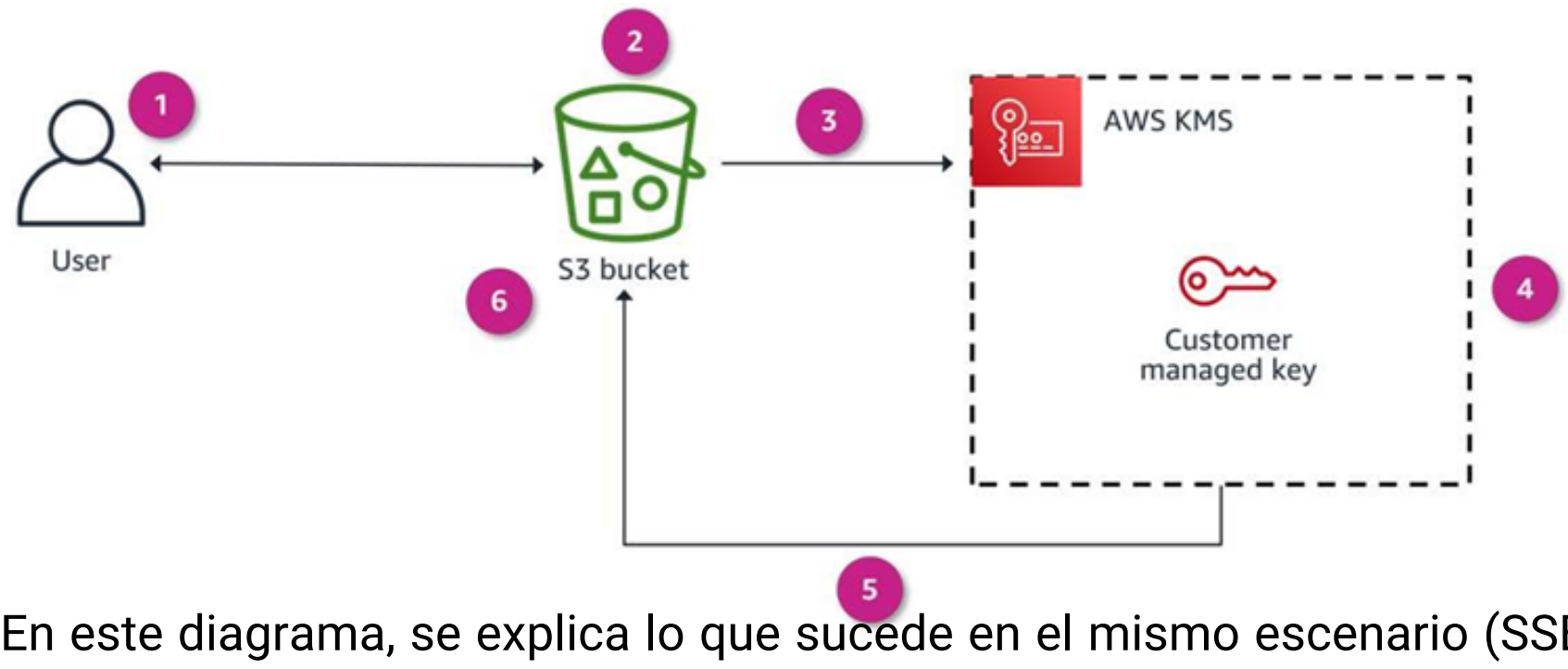
2. Amazon S3 solicita una clave de datos de AWS KMS a fin de utilizarla para cifrar el archivo.

3. AWS KMS genera una clave de datos de texto sin formato y cifra la clave de datos con la clave administrada por el cliente.

4. AWS KMS envía ambas copias de la clave de datos a Amazon S3.

5. Amazon S3 cifra el objeto utilizando la clave de datos de texto sin formato, almacena el objeto y luego elimina dicha clave. La clave cifrada se mantiene en los metadatos del objeto.

INFORMACIÓN GENERAL SOBRE EL DESCIFRADO



En este diagrama, se explica lo que sucede en el mismo escenario (SSE-KMS) cuando el usuario solicita abrir un objeto cifrado que se almacena en Amazon S3:

1. Usted solicita abrir el objeto.

2. Amazon S3 advierte que el objeto solicitado está cifrado.

3. Amazon S3 envía la copia cifrada de la clave de datos con la que se cifra el objeto a AWS KMS. A continuación, AWS KMS descifra la clave de datos con la clave administrada por el cliente (que nunca deja el servicio AWS KMS).

4. AWS KMS luego envía la clave de datos de texto sin formato a Amazon S3.

5. Finalmente, Amazon S3 descifra el texto cifrado del objeto de datos, le permite abrir el objeto y elimina la copia de texto sin formato de la clave de datos.

AWS KEY MANAGEMENT SERVICE (AWS KMS)

• Brinda la capacidad de crear y administrar claves criptográficas.

• Utiliza módulos de seguridad de hardware (HSM) para proteger las claves.

• Se integra en otros servicios de AWS.

• Brinda la capacidad de establecer políticas de uso para determinar qué usuarios pueden utilizar las claves.

AWS KMS es un servicio administrado que brinda la capacidad de crear y controlar las claves que se utilizan para cifrar sus datos. Puede crear claves de datos con alias y descripciones únicos para una mejor administración, rotar automáticamente sus claves de forma programada y desactivar o eliminar claves para que nadie pueda usarlas. También puede importar sus propias claves en lugar de usar claves generadas por AWS.

El servicio utiliza módulos de seguridad de hardware (HSM) validados por FIPS 140-2 para proteger las claves. AWS KMS está integrado en otros servicios de AWS para ayudarlo a proteger los datos que almacena en ellos. Los servicios integrados de AWS utilizan el cifrado de sobre para ayudar a proteger sus claves de cifrado.

Con AWS KMS, puede centrarse en la administración y el almacenamiento seguro de sus claves. Puede utilizar las claves desde las aplicaciones y los servicios de la nube de AWS compatibles para proteger los datos sin que la clave salga de AWS KMS. Esto reduce el riesgo de que se vulnere la clave de datos. Los datos se envían a AWS KMS para que las claves que controla los cifren o descifren.

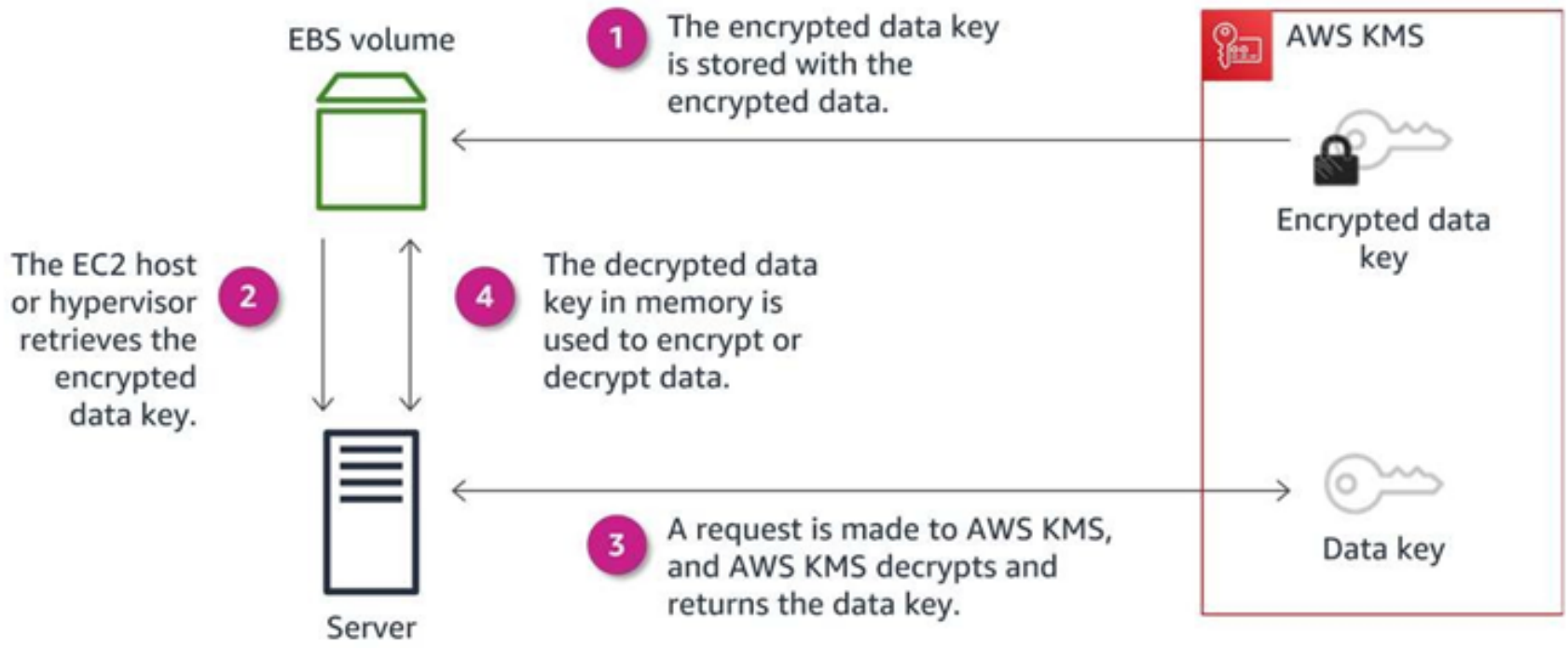
Puede establecer políticas de uso en estas claves para determinar qué usuarios pueden utilizarlas. Todas las solicitudes de uso de estas claves se registran en AWS CloudTrail para que pueda conocer quién usó qué clave y cuándo. CloudTrail registra todas las operaciones de AWS KMS, incluidas las operaciones de solo lectura, las que administran claves de KMS y las criptográficas.

Para más información, consulte los siguientes recursos:

- AWS Key Management Service (AWS KMS) en https://aws.amazon.com/kms/
- “How AWS Services Use AWS KMS” (Cómo usan AWS KMS los servicios de AWS) en la Guía para desarrolladores de AWS Key Management Service en

https://docs.aws.amazon.com/kms/latest/developerguide/service-integration.html

EJEMPLO DE AWS KMS CON AMAZON EBS



El cifrado de Amazon Elastic Block Store (Amazon EBS) es una solución de cifrado sencilla para los recursos de EBS que están asociados con las instancias de EC2. Con el cifrado de Amazon EBS, no debe crear, mantener ni asegurar la infraestructura de administración de claves.

El cifrado de Amazon EBS utiliza claves de KMS al crear volúmenes e instantáneas cifrados. Cada volumen se cifra con AES-256-XTS. Esto requiere dos claves de 256 bits, que puede pensar como una sola clave de 512 bits. La clave de datos se cifra bajo una clave de KMS en su cuenta. Para que Amazon EBS cifre un volumen por usted, debe tener acceso a una clave administrada por el cliente en la cuenta. Para ello, otorga un permiso para que Amazon EBS acceda a la clave administrada por el cliente a fin de crear claves de datos, y cifrar y descifrar dichas claves.

A continuación, se mencionan los pasos básicos para cifrar y descifrar datos de volumen de EBS:

1. Amazon EBS obtiene una clave de datos cifrada bajo una clave administrada por el cliente a través de AWS KMS y almacena la clave cifrada con los datos cifrados.

2. Los servidores que alojan instancias de EC2 recuperan la clave de datos cifrada del almacenamiento.

3. Se hace una llamada a AWS KMS por TLS para descifrar la clave de datos cifrada. AWS KMS identifica la clave de KMS, realiza una solicitud interna a un HSM de la flota para descifrar la clave de datos y devuelve la clave al cliente a través de la sesión TLS.

4. La clave de datos descifrada se almacena en la memoria y se utiliza para cifrar y descifrar todos los datos que ingresan en el volumen de EBS adjunto, o que salen de él. Amazon EBS conserva la clave de datos cifrada para usarla más adelante en caso de que la clave de datos en memoria ya no esté disponible.

En este laboratorio, utilizará AMS KMS para cifrar datos en reposo. Creará una clave de KMS y la usará para cifrar objetos almacenados en Amazon S3 y volúmenes de EBS. También verá cómo CloudTrail brinda un registro de auditoría del uso de la clave de KMS y cómo la desactivación de la clave afecta el acceso a los datos.

En este laboratorio, realizará las siguientes tareas:

1. Creación de una clave de AWS KMS
2. Almacenamiento de un objeto cifrado en un bucket de S3
3. Intento de acceso público al objeto cifrado
4. Intento de acceso firmado al objeto cifrado
5. Supervisión de la actividad de AWS KMS mediante CloudTrail
6. Cifrado del volumen raíz de una instancia de EC2 existente
7. Deshabilitación de la clave de cifrado y sus efectos