AWS Key Management Service mejores prácticas

AWS Orientación prescriptiva

AWS Orientación prescriptiva: AWS Key Management Service mejores prácticas

Table of Contents

AWS Key Management Service mejores prácticas

Amazon Web Services (colaboradores)

Marzo de 2025 (historial del documento)

AWS Key Management Service (AWS KMS) es un servicio administrado que le facilita la creación y el control de las claves criptográficas que se utilizan para proteger los datos. Esta guía describe cómo usarlo de manera efectiva AWS KMS y proporciona las mejores prácticas. Le ayuda a comparar las opciones de configuración y a elegir el conjunto que mejor se adapte a sus necesidades.

Esta guía incluye recomendaciones sobre cómo su organización puede utilizar AWS KMS para proteger la información confidencial e implementar la firma en varios casos de uso. Considera las recomendaciones actuales que utilizan las siguientes dimensiones:

- Administración de claves: opciones de delegación para las opciones de administración y almacenamiento de claves
- Protección de datos: cifrar los datos dentro de sus propias aplicaciones en lugar de Servicios de AWS hacerlo en su nombre
- Gestión del acceso: utilizar políticas AWS KMS clave y políticas AWS Identity and Access Management (IAM) para implementar el control de acceso basado en roles (RBAC) o el control de acceso basado en atributos (ABAC).
- Arquitectura multicuenta y multiregión: recomendaciones para despliegues a gran escala.
- Administración de costos y facturación: conozca sus costos y su uso, y recomiende formas de reducir los costos.
- Controles de Detective: supervisan el estado de las claves KMS, la configuración de cifrado y los datos cifrados.
- Respuesta a incidentes: corregir los errores de configuración que provocan el incumplimiento de las políticas de protección de datos.

Resultados empresariales específicos

Sus datos son un activo fundamental y confidencial para su empresa. Con AWS KMSél, usted administra las claves criptográficas que se utilizan para proteger y verificar sus datos. Usted controla cómo se utilizan sus datos, quién tiene acceso a ellos y cómo se cifran. El objetivo de esta guía

es ayudar a los desarrolladores, administradores de sistemas y profesionales de la seguridad a implementar las mejores prácticas de cifrado que ayuden a proteger los datos confidenciales que se almacenan o se transmiten a través de ellos Servicios de AWS. Si comprende e implementa las recomendaciones de esta guía, podrá promover la confidencialidad e integridad de los datos en todo su AWS entorno. Puede cumplir con sus requisitos de protección de datos, tanto si dichos requisitos se formulan internamente como si tiene requisitos específicos para un programa de conformidad o validación. Para obtener más información sobre cómo AWS KMS puede ayudarle a proteger los datos de su AWS entorno, consulte Uso del AWS KMS cifrado Servicios de AWS en la AWS KMS documentación.

Acerca AWS KMS keys

AWS Key Management Service (AWS KMS) le permite crear claves criptográficas que se pueden utilizar en los datos que se transfieran al servicio. El tipo de recurso principal es la clave KMS, de la que hay tres tipos:

- Claves simétricas del estándar de cifrado avanzado (AES): son claves de 256 bits que se utilizan en el modo Galois Counter Mode (GCM) del AES. Estas claves proporcionan cifrado y descifrado autenticados de datos con un tamaño inferior a 4 KB. Este es el tipo de clave más común. Se utiliza para proteger otras claves de datos, como las que se utilizan en sus aplicaciones, o las Servicios de AWS que cifran los datos en su nombre.
- Claves asimétricas RSA o de curva elíptica: estas claves están disponibles en varios tamaños y admiten muchos algoritmos. Según el algoritmo, se pueden usar para cifrar y descifrar y para operaciones de firma y verificación.
- Claves simétricas para realizar operaciones con códigos de autenticación de mensajes (HMAC) basadas en hash: estas claves son claves de 256 bits que se utilizan para las operaciones de firma y verificación.

Las claves KMS no se pueden exportar desde el servicio en texto sin formato. Las generan los módulos de seguridad de hardware (HSMs) utilizados por el servicio y solo se pueden usar dentro de ellos. Esta es una propiedad de seguridad fundamental AWS KMS para evitar que las claves se vean comprometidas. En las regiones de China (Beijing) y China (Ningxia), HSMs están certificadas por la OSCCA. En todas las demás regiones, las HSMs utilizadas se AWS KMS validan según el programa FIPS 140 del NIST con un nivel de seguridad 3. Para obtener más información sobre el diseño y los controles AWS KMS que ayudan a proteger sus claves, consulte Detalles AWS Key Management Service criptográficos.

Puede enviar datos AWS KMS mediante varios tipos de criptografía APIs para realizar operaciones de cifrado, descifrado, firma o verificación con claves KMS. También puede elegir que una clave KMS actúe como clave de cifrado, lo que protege un tipo de clave denominado clave de datos. Puede exportar una clave de datos AWS KMS para utilizarla en su aplicación local o desde una Servicio de AWS que proteja los datos en su nombre. El uso de claves de datos es común en todos los sistemas de administración de claves y, a menudo, se denomina cifrado sobre. El cifrado de sobres permite utilizar una clave de datos en el sistema remoto que gestiona los datos confidenciales, en lugar de tener que enviarlos al sistema remoto AWS KMS para su cifrado directamente con una clave KMS.

Para obtener más información, consulte AWS KMS keyslos aspectos básicos de AWS KMS la criptografía en la AWS KMS documentación.

Mejores prácticas de administración clave para AWS KMS

Cuando AWS Key Management Service utilices (AWS KMS), debes tomar algunas decisiones fundamentales de diseño. Estas incluyen si se debe utilizar un modelo centralizado o descentralizado para la administración y el acceso a las claves, el tipo de claves que se deben utilizar y el tipo de almacén de claves que se van a utilizar. Las siguientes secciones le ayudan a tomar las decisiones adecuadas para su organización y sus casos de uso. Esta sección concluye con consideraciones importantes para deshabilitar y eliminar las claves de KMS, incluidas las medidas que debe tomar para ayudar a proteger sus datos y claves.

Esta sección contiene los siguientes temas:

- Elegir un modelo centralizado o descentralizado
- Elegir claves administradas por el cliente, claves AWS administradas o claves AWS propias
- Elegir un almacén de AWS KMS claves
- Eliminar y deshabilitar las claves de KMS

Elegir un modelo centralizado o descentralizado

AWS recomienda utilizar varias cuentas Cuentas de AWS y administrarlas como una sola organización en AWS Organizations. Existen dos enfoques generales para la administración AWS KMS keys en entornos de múltiples cuentas.

El primer enfoque es un enfoque descentralizado, en el que se crean claves en cada cuenta que utilice esas claves. Al almacenar las claves de KMS en las mismas cuentas que los recursos que protegen, resulta más fácil delegar los permisos a los administradores locales, que conocen los requisitos de acceso de sus AWS entidades principales y claves. Puede autorizar el uso de claves utilizando solo una política clave, o puede combinar una política clave y políticas basadas en la identidad AWS Identity and Access Management (IAM).

El segundo enfoque es un enfoque centralizado, en el que se mantienen las claves de KMS en una o varias designadas. Cuentas de AWS Permites que otras cuentas solo usen las claves para operaciones criptográficas. Usted administra las claves, su ciclo de vida y sus permisos desde la cuenta centralizada. Permites Cuentas de AWS que otros usen la clave, pero no permites otros permisos. Las cuentas externas no pueden administrar nada relacionado con el ciclo de vida de la clave ni con los permisos de acceso. Este modelo centralizado puede ayudar a minimizar el riesgo

de que los administradores o usuarios delegados eliminen las claves de forma no intencionada o aumenten sus privilegios.

La opción que elija depende de varios factores. Tenga en cuenta lo siguiente al elegir un enfoque:

1. ¿Tiene un proceso automatizado o manual para aprovisionar el acceso a las claves y los recursos? Esto incluye recursos como los procesos de implementación y las plantillas de infraestructura como código (IaC). Estas herramientas pueden ayudarlo a implementar y administrar recursos (como las claves de KMS, las políticas clave, las funciones de IAM y las políticas de IAM) en muchos casos. Cuentas de AWS Si no cuenta con estas herramientas de implementación, un enfoque centralizado de la administración de claves podría ser más fácil de administrar para su empresa.
2. ¿Tiene control administrativo sobre todos los recursos Cuentas de AWS que contienen claves de KMS? Si es así, un modelo centralizado puede simplificar la administración y eliminar la necesidad de cambiar Cuentas de AWS para administrar las claves. Sin embargo, tenga en cuenta que las funciones de IAM y los permisos de usuario para usar las claves aún deben administrarse por cuenta.
3. ¿Necesitas ofrecer acceso para usar tus claves de KMS a los clientes o socios que tengan sus propios Cuentas de AWS recursos? En el caso de estas claves, un enfoque centralizado puede reducir la carga administrativa de sus clientes y socios.
4. ¿Tiene requisitos de autorización para acceder a AWS los recursos que se resuelven mejor con un enfoque de acceso centralizado o local? Por ejemplo, si diferentes aplicaciones o unidades de negocio son responsables de administrar la seguridad de sus propios datos, es mejor adoptar un enfoque descentralizado de la administración de claves.
5. ¿Está excediendo las cuotas de recursos de servicio AWS KMS? Como estas cuotas se establecen por separado Cuenta de AWS, un modelo descentralizado distribuye la carga entre las cuentas, lo que multiplica de manera efectiva las cuotas de servicio.

> **Note**
>
> El modelo de administración de claves es irrelevante a la hora de considerar las cuotas de solicitud, ya que estas cuotas se aplican al director de la cuenta que hace una solicitud en relación con la clave, no a la cuenta que posee o administra la clave.

En general, le recomendamos que comience con un enfoque descentralizado, a menos que pueda explicar la necesidad de un modelo de claves KMS centralizado.

Elegir claves administradas por el cliente, claves AWS administradas o claves AWS propias

Las claves de KMS que crea y administra para usarlas en sus propias aplicaciones criptográficas se conocen como claves administradas por el cliente. Servicios de AWS puede usar claves administradas por el cliente para cifrar los datos que el servicio almacena en su nombre. Se recomiendan las claves administradas por el cliente si quieres tener un control total sobre el ciclo de vida y el uso de tus claves. Disponer de una clave administrada por el cliente en su cuenta tiene asociado un coste mensual. Además, las solicitudes de uso o administración de la clave conllevan un coste de uso. Para más información, consulte Precios de AWS KMS.

Si quiere cifrar sus datos, pero no quiere asumir los gastos generales o los costes que supone gestionar las claves, puede utilizar una clave AWS gestionada. Servicio de AWS Este tipo de clave existe en tu cuenta, pero solo se puede usar en determinadas circunstancias. Solo se puede usar en el contexto en el Servicio de AWS que operas y solo la pueden usar los directores de la cuenta que contiene la clave. No puedes gestionar nada relacionado con el ciclo de vida ni los permisos de estas claves. Algunas Servicios de AWS usan claves AWS administradas. El formato de un alias de clave AWS administrada es`aws/<service code>`. Por ejemplo, una `aws/ebs` clave solo se puede usar para cifrar los volúmenes de Amazon Elastic Block Store (Amazon EBS) en la misma cuenta que la clave y solo la pueden usar los directores de IAM de esa cuenta. Solo los usuarios de esa cuenta y para los recursos de esa cuenta pueden usar una clave AWS administrada. No puedes compartir recursos cifrados con una clave AWS gestionada con otras cuentas. Si esta es una limitación para su caso de uso, le recomendamos que utilice en su lugar una clave gestionada por el cliente; puede compartir el uso de esa clave con cualquier otra cuenta. No se te cobrará por la existencia de una clave AWS gestionada en tu cuenta, pero sí por cualquier uso de este tipo de clave por parte de la Servicio de AWS persona que esté asignada a la clave.

Una clave AWS gestionada es un tipo de clave heredada que dejará de crearse para nuevas a Servicios de AWS partir de 2021. En su lugar, las nuevas (y las antiguas) Servicios de AWS utilizan AWS una clave propia para cifrar los datos de forma predeterminada. AWS las claves propias son un conjunto de claves de KMS que una persona Servicio de AWS posee y administra para utilizarlas en múltiples Cuentas de AWS ocasiones. Si bien estas claves no están en sus manos Cuenta de AWS, Servicio de AWS puede usarlas para proteger los recursos de su cuenta.

Le recomendamos que utilice claves gestionadas por el cliente cuando lo más importante sea el control detallado y que utilice claves AWS propias cuando la comodidad sea lo más importante.

En la siguiente tabla se describen las principales diferencias de política, registro, administración y precios entre cada tipo de clave. Para obtener más información sobre los tipos de claves, consulte AWS KMS conceptos.

Consideración	Claves administradas por el cliente	AWS claves administradas	AWS claves propias
Política de claves	Controlada exclusivamente por el cliente	Controlada por el servicio; visible por el cliente	Controladas exclusivamente y solo visibles por quien Servicio de AWS cifra sus datos
Registro	AWS CloudTrail almacén de datos de eventos o registros de clientes	CloudTrail almacén de datos de eventos o seguimiento de clientes	No visible por el cliente
Gestión del ciclo de vida	El cliente gestiona la rotación, la eliminación y Región de AWS	Servicio de AWS gestiona la rotación (anual), la eliminación y la región	Servicio de AWS gestiona la rotación (anual), la eliminación y la región
Precios	Tarifa mensual por la existencia de la clave (prorrateada por hora); se cobra a la persona que llama por el uso de la API	La existencia de la clave es gratuita; se cobra a la persona que llama por el uso de la API	Sin cargos para el cliente

Elegir un almacén de AWS KMS claves

Un almacén de claves es un lugar seguro para almacenar y utilizar material de claves criptográficas. La mejor práctica del sector para los almacenes de claves es utilizar un dispositivo conocido como módulo de seguridad de hardware (HSM) que haya sido validado según el Programa de Validación de Módulos Criptográficos 140 de la Norma Federal de Procesamiento de Información (FIPS) del NIST con un nivel de seguridad 3. Existen otros programas para ayudar a los almacenes de llaves

que se utilizan para procesar los pagos. AWS Payment Cryptographyes un servicio que puede utilizar para proteger los datos relacionados con sus cargas de trabajo de pago.

AWS KMS admite varios tipos de almacenes de claves para ayudar a proteger el material de claves cuando se utiliza AWS KMS para crear y gestionar las claves de cifrado. Todas las opciones de almacenamiento de claves que ofrece se AWS KMS validan continuamente según la norma FIPS 140 en el nivel de seguridad 3. Están diseñados para evitar que cualquier persona, incluidos AWS los operadores, acceda a sus claves en texto plano o las utilice sin su permiso. Para obtener más información sobre los tipos de almacenes de claves disponibles, consulte los almacenes de claves en la AWS KMS documentación.

El almacén de claves AWS KMS estándar es la mejor opción para la mayoría de las cargas de trabajo. Si necesita elegir un tipo de almacén de claves diferente, considere detenidamente si los requisitos reglamentarios o de otro tipo (por ejemplo, internos) obligan a tomar esta decisión y evalúe cuidadosamente los costos y beneficios.

Eliminar y deshabilitar las claves de KMS

La eliminación de una clave KMS puede tener un impacto significativo. Antes de eliminar una clave de KMS que ya no vaya a utilizar, considere si es adecuado establecer el estado de la clave en Desactivado. Mientras una clave esté deshabilitada, no se puede usar para operaciones criptográficas. Todavía existe en AWS, y puede volver a habilitarlo en el futuro si es necesario. Las llaves deshabilitadas siguen incurriendo en gastos de almacenamiento. Le recomendamos que desactive las claves en lugar de eliminarlas hasta que esté seguro de que la clave no protege ningún dato o clave de datos.

> **Important**
>
> La eliminación de una clave debe planificarse cuidadosamente. Los datos no se pueden descifrar si se ha eliminado la clave correspondiente. AWS no tiene medios para recuperar una clave eliminada después de haberla eliminado. Al igual que con otras operaciones críticas AWS, debe aplicar una política que limite quién puede programar la eliminación de las claves y exija la autenticación multifactor (MFA) para la eliminación de las claves.

Para evitar la eliminación accidental de las claves, se AWS KMS aplica un período de espera mínimo predeterminado de siete días después de la ejecución de una `DeleteKey` llamada antes de que se elimine la clave. Puede establecer el período de espera en un valor máximo de 30 días. Durante el

período de espera, la clave sigue guardada AWS KMS en un estado de eliminación pendiente. No se puede utilizar para operaciones de cifrado o descifrado. Se registra cualquier intento de utilizar una clave que esté en estado de eliminación pendiente para el cifrado o el descifrado. AWS CloudTrail Puedes configurar una CloudWatch alarma de Amazon para estos eventos en tus CloudTrail registros. Si recibe alarmas sobre estos eventos, puede optar por cancelar el proceso de eliminación si es necesario. Hasta que el período de espera haya expirado, puede recuperar la clave del estado de eliminación pendiente y restaurarla al estado Desactivado o Activado.

Para eliminar una clave multiregional, es necesario eliminar las réplicas antes que la copia original. Para obtener más información, consulte Eliminar claves multirregionales.

Si utiliza una clave con material clave importado, puede eliminar el material clave importado inmediatamente. Esto es diferente de eliminar una clave de KMS en varios aspectos. Al realizar la `DeleteImportedKeyMaterial` acción, AWS KMS elimina el material clave y el estado de la clave cambia a Pendiente de importación. Tras eliminar el material clave, la clave queda inutilizable inmediatamente. No hay ningún período de espera. Para volver a permitir el uso de la clave, debe volver a importar el mismo material clave. El período de espera para eliminar las claves de KMS también se aplica a las claves de KMS con material de claves importado.

Si las claves de datos están protegidas por una clave de KMS y se utilizan activamente Servicios de AWS, no se ven afectadas de forma inmediata si la clave de KMS asociada está deshabilitada o si se elimina el material de clave importado. Por ejemplo, supongamos que se utilizó una clave con material importado para cifrar un objeto con SSE-KMS. Está cargando el objeto en un bucket de Amazon Simple Storage Service (Amazon S3). Antes de subir el objeto al depósito, debe importar el material a su clave. Una vez cargado el objeto, eliminas el material clave importado de esa clave. El objeto permanece en el depósito en un estado cifrado, pero nadie puede acceder al objeto hasta que el material clave eliminado se vuelva a importar a la clave. Si bien este flujo requiere una automatización precisa para importar y eliminar el material clave de una clave, puede proporcionar un nivel adicional de control dentro de un entorno.

AWS ofrece una guía prescriptiva para ayudarle a supervisar y corregir (si es necesario) la eliminación programada de las claves de KMS. Para obtener más información, consulte Supervisar y corregir la eliminación programada de claves. AWS KMS

Mejores prácticas de protección de datos para AWS KMS

Esta sección le ayuda a tomar decisiones sobre el uso de AWS Key Management Service (AWS KMS) claves para la protección de datos, por ejemplo, qué claves usar para cada tipo de datos. También proporciona ejemplos específicos del uso AWS KMS con diferentes Servicios de AWS. Estas recomendaciones y ejemplos le ayudan a comprender cuántas claves puede necesitar y qué entidades principales requieren permisos para utilizarlas.

En la sección también se analiza la rotación de claves. La rotación de claves es la práctica de reemplazar una clave KMS existente por una nueva clave o reemplazar el material criptográfico asociado a una clave KMS existente por material nuevo. Esta guía proporciona ejemplos e instrucciones sobre cómo rotar las claves KMS para las de uso Servicios de AWS común. Las recomendaciones y los ejemplos están diseñados para ayudarle a tomar decisiones informadas sobre su estrategia de rotación clave.

Por último, en esta sección se ofrecen recomendaciones sobre cómo utilizar la AWS Encryption SDK herramienta para implementar el cifrado del lado del cliente en sus aplicaciones. En esta sección se incluyen las opciones de diseño que puede realizar en función del conjunto de funciones y las capacidades del. AWS Encryption SDK

En esta sección se tratan los siguientes temas de cifrado:

- Cifrado con AWS KMS
- Rotación clave AWS KMS y alcance del impacto
- Recomendaciones para usar el AWS Encryption SDK

Cifrado con AWS KMS

El cifrado es una práctica recomendada general para proteger la confidencialidad e integridad de la información confidencial. Debe utilizar los niveles de clasificación de datos existentes y tener al menos una AWS Key Management Service (AWS KMS) clave por nivel. Por ejemplo, puede definir una clave KMS para los datos clasificados como confidenciales, otra para los de uso interno y otra para los confidenciales. Esto le ayuda a asegurarse de que solo los usuarios autorizados tienen permisos para usar las claves asociadas a cada nivel de clasificación.

> **Note**
>
> Se puede usar una única clave KMS administrada por el cliente en cualquier combinación de aplicaciones Servicios de AWS o en sus propias aplicaciones que almacenen datos de una clasificación determinada. El factor que limita el uso de una clave en varias cargas de trabajo Servicios de AWS es la complejidad que deben tener los permisos de uso para controlar el acceso a los datos de un conjunto de usuarios. El documento JSON de la política AWS KMS clave debe tener menos de 32 KB. Si esta restricción de tamaño se convierte en una limitación, considere la posibilidad de utilizar AWS KMS concesiones o crear varias claves para minimizar el tamaño del documento de política clave.

En lugar de confiar únicamente en la clasificación de los datos para particionar la clave de KMS, también puede optar por asignar una clave de KMS para utilizarla en una clasificación de datos dentro de una sola Servicio de AWS. Por ejemplo, todos los datos etiquetados `Sensitive` en Amazon Simple Storage Service (Amazon S3) deben cifrarse con una clave KMS que tenga un nombre similar. `S3-Sensitive` Además, puede distribuir sus datos entre varias claves de KMS dentro de la clasificación de datos Servicio de AWS o aplicación que haya definido. Por ejemplo, es posible que pueda eliminar algunos conjuntos de datos en un período de tiempo específico y eliminar otros conjuntos de datos en un período de tiempo diferente. Puede usar etiquetas de recursos para identificar y ordenar los datos cifrados con claves de KMS específicas.

Si elige un modelo de administración descentralizado para las claves de KMS, debe aplicar medidas de protección para garantizar la creación de nuevos recursos con una clasificación determinada y utilizar las claves de KMS esperadas con los permisos adecuados. Para obtener más información sobre cómo aplicar, detectar y administrar la configuración de los recursos mediante la automatización, consulte la Detección y monitoreo sección de esta guía.

En esta sección se analizan los siguientes temas de cifrado:

- Cifrado de datos de registro con AWS KMS
- Cifrado de forma predeterminada
- Cifrado de bases de datos AWS KMS
- Cifrado de datos PCI DSS con AWS KMS
- Uso de claves KMS con Amazon EC2 Auto Scaling

Cifrado de datos de registro con AWS KMS

Muchos Servicios de AWS, como Amazon GuardDuty y AWS CloudTrail, ofrecen opciones para cifrar los datos de registro que se envían a Amazon S3. Al exportar los resultados desde GuardDuty Amazon S3, debe utilizar una clave de KMS. Le recomendamos cifrar todos los datos de registro y conceder el acceso de descifrado únicamente a las personas autorizadas, como los equipos de seguridad, el personal de respuesta a incidentes y los auditores.

La arquitectura AWS de referencia de seguridad recomienda crear una central de registro. Cuenta de AWS Al hacerlo, también puede reducir la sobrecarga de administración de claves. Por ejemplo, con CloudTrail, puede crear un registro de la organización o un almacén de datos de eventos para registrar los eventos en toda su organización. Al configurar el registro organizativo o el almacén de datos de eventos, puede especificar un único bucket de Amazon S3 y una clave de KMS en la cuenta de registro designada. Esta configuración se aplica a todas las cuentas de los miembros de la organización. A continuación, todas las cuentas envían sus CloudTrail registros al bucket de Amazon S3 de la cuenta de registro y los datos de registro se cifran con la clave de KMS especificada. Debe actualizar la política de claves de esta clave de KMS para conceder CloudTrail los permisos necesarios para utilizarla. Para obtener más información, consulte Configurar las políticas AWS KMS clave CloudTrail en la CloudTrail documentación.

Para ayudar a proteger los CloudTrail registros GuardDuty y, el bucket de Amazon S3 y la clave de KMS deben estar en el mismo lugar Región de AWS. La arquitectura AWS de referencia de seguridad también proporciona orientación sobre las arquitecturas de registro y de cuentas múltiples. Al agregar registros de varias regiones y cuentas, consulta la sección Cómo crear un registro para una organización en la CloudTrail documentación para obtener más información sobre las regiones con las que se ha optado y asegurarte de que el registro centralizado funciona según lo diseñado.

Cifrado de forma predeterminada

Servicios de AWS Las que almacenan o procesan datos suelen ofrecer cifrado en reposo. Esta función de seguridad ayuda a proteger sus datos al cifrarlos cuando no están en uso. Los usuarios autorizados pueden seguir accediendo a ellos cuando lo necesiten.

Las opciones de implementación y cifrado varían entre sí Servicios de AWS. Muchas ofrecen cifrado de forma predeterminada. Es importante entender cómo funciona el cifrado para cada servicio que utilices. A continuación se muestran algunos ejemplos:

- Amazon Elastic Block Store (Amazon EBS): al habilitar el cifrado de forma predeterminada, se cifran todos los volúmenes y copias instantáneas nuevos de Amazon EBS. AWS Identity and

Access Management (IAM) o los usuarios no pueden lanzar instancias con volúmenes no cifrados o volúmenes que no admitan el cifrado. Esta función contribuye a la seguridad, el cumplimiento y la auditoría al garantizar que todos los datos almacenados en los volúmenes de Amazon EBS estén cifrados. Para obtener más información sobre el cifrado en este servicio, consulte el cifrado de Amazon EBS en la documentación de Amazon EBS.

- Amazon Simple Storage Service (Amazon S3): todos los objetos nuevos se cifran de forma predeterminada. Amazon S3 aplica automáticamente el cifrado del lado del servidor con claves administradas de Amazon S3 (SSE-S3) para cada objeto nuevo, a menos que especifique una opción de cifrado diferente. Los directores de IAM pueden seguir cargando objetos no cifrados en Amazon S3 indicándolo de forma explícita en la llamada a la API. En Amazon S3, para aplicar el cifrado SSE-KMS, debe usar una política de bucket con condiciones que requieran el cifrado. Para ver un ejemplo de política, consulte Requerir SSE-KMS para todos los objetos escritos en un bucket en la documentación de Amazon S3. Algunos buckets de Amazon S3 reciben y sirven una gran cantidad de objetos. Si esos objetos se cifran con claves de KMS, un gran número de operaciones de Amazon S3 se traduce en un gran número de `Decrypt` llamadas `GenerateDataKey` y llamadas AWS KMS. Esto puede aumentar los cargos en los que incurra por su AWS KMS uso. Puede configurar las claves de bucket de Amazon S3, lo que puede reducir considerablemente sus AWS KMS costes. Para obtener más información sobre el cifrado en este servicio, consulte Protección de datos con cifrado en la documentación de Amazon S3.
- Amazon DynamoDB: DynamoDB es un servicio de base de datos NoSQL totalmente gestionado que permite el cifrado en reposo del lado del servidor de forma predeterminada y no se puede deshabilitar. Se recomienda utilizar una clave gestionada por el cliente para cifrar las tablas de DynamoDB. Este enfoque le ayuda a implementar los privilegios mínimos con permisos detallados y una separación de funciones al centrarse en usuarios y roles específicos de IAM en sus políticas clave. AWS KMS También puede elegir claves AWS administradas o AWS propias al configurar los ajustes de cifrado para las tablas de DynamoDB. Para los datos que requieren un alto grado de protección (donde los datos solo deben estar visibles como texto sin cifrar para el cliente), considere la posibilidad de utilizar el cifrado del lado del cliente con el SDK de cifrado de bases de datos.AWS Para obtener más información sobre el cifrado en este servicio, consulte Protección de datos en la documentación de DynamoDB.

Cifrado de bases de datos AWS KMS

El nivel en el que se implementa el cifrado afecta a la funcionalidad de la base de datos. Las ventajas y desventajas que debe tener en cuenta son las siguientes:

- Si solo utiliza el AWS KMS cifrado, el almacenamiento que respalda las tablas se cifra para DynamoDB y Amazon Relational Database Service (Amazon RDS). Esto significa que el sistema operativo que ejecuta la base de datos ve el contenido del almacenamiento como texto sin cifrar. Todas las funciones de la base de datos, incluida la generación de índices y otras funciones de orden superior que requieren acceso a los datos de texto sin formato, siguen funcionando según lo previsto.
- Amazon RDS se basa en cifrado de Amazon Elastic Block Store (Amazon EBS) para proporcionar cifrado de disco completo para los volúmenes de base de datos. Cuando crea una instancia de base de datos cifrada con Amazon RDS, Amazon RDS crea un volumen de Amazon EBS cifrado en su nombre para almacenar la base de datos. Los datos almacenados en reposo en el volumen, las instantáneas de la base de datos, las copias de seguridad automatizadas y las réplicas de lectura se cifran con la clave KMS que especificó al crear la instancia de base de datos.
- Amazon Redshift se integra AWS KMS y crea una jerarquía de claves de cuatro niveles que se utilizan para cifrar desde el nivel del clúster hasta el nivel de los datos. Al lanzar el clúster, puede optar por utilizar el cifrado. AWS KMS Solo la aplicación Amazon Redshift y los usuarios con los permisos adecuados pueden ver el texto sin cifrar al abrir (y descifrar) las tablas en la memoria. En términos generales, esto es análogo a las funciones de cifrado de datos transparente o basado en tablas (TDE) que están disponibles en algunas bases de datos comerciales. Esto significa que todas las funciones de la base de datos, incluidas la generación de índices y otras funciones de orden superior que requieren acceso a los datos de texto sin formato, siguen funcionando según lo previsto.
- El cifrado a nivel de datos del lado del cliente implementado mediante el SDK de cifrado de AWS bases de datos (y herramientas similares) significa que tanto el sistema operativo como la base de datos solo ven el texto cifrado. Los usuarios solo pueden ver el texto sin formato si acceden a la base de datos desde un cliente que tenga instalado el SDK de cifrado de AWS bases de datos y tengan acceso a la clave correspondiente. Las funciones de bases de datos de orden superior que requieren acceso a texto sin formato para funcionar según lo previsto (como la generación de índices) no funcionarán si se indica que funcionan en campos cifrados. Si decide utilizar el cifrado del lado del cliente, asegúrese de utilizar un mecanismo de cifrado sólido que ayude a prevenir los ataques habituales contra los datos cifrados. Esto incluye el uso de un algoritmo de cifrado sólido y las técnicas adecuadas, como la sal, para ayudar a mitigar los ataques de texto cifrado.

Recomendamos utilizar las capacidades de cifrado AWS KMS integradas para los servicios de AWS bases de datos. Para las cargas de trabajo que procesan datos confidenciales, se debe considerar el cifrado del lado del cliente para los campos de datos confidenciales. Al utilizar el cifrado del lado

del cliente, debe tener en cuenta el impacto en el acceso a la base de datos, como las uniones en consultas SQL o la creación de índices.

Cifrado de datos PCI DSS con AWS KMS

Los controles de seguridad y calidad se AWS KMS han validado y certificado para cumplir con los requisitos del estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS). Esto significa que puede cifrar los datos del número de cuenta principal (PAN) con una clave KMS. El uso de una clave KMS para cifrar datos elimina parte de la carga que supone administrar las bibliotecas de cifrado. Además, las claves KMS no se pueden exportar desde AWS KMS, lo que reduce la preocupación de que las claves de cifrado se almacenen de forma no segura.

Existen otras formas que puede utilizar AWS KMS para cumplir con los requisitos de PCI DSS. Por ejemplo, si lo utiliza AWS KMS con Amazon S3, puede almacenar datos PAN en Amazon S3 porque el mecanismo de control de acceso de cada servicio es distinto del otro.

Como siempre, al revisar sus requisitos de conformidad, asegúrese de obtener el asesoramiento de personas debidamente experimentadas, cualificadas y verificadas. Tenga en cuenta las cuotas de AWS KMS solicitud cuando diseñe aplicaciones que utilicen la clave directamente para proteger los datos de las transacciones con tarjetas incluidas en el ámbito de aplicación de la PCI DSS.

Como todas las AWS KMS solicitudes se registran AWS CloudTrail, puede auditar el uso de las claves revisando los CloudTrail registros. Sin embargo, si utiliza claves de bucket de Amazon S3, no habrá ninguna entrada que corresponda a cada acción de Amazon S3. Esto se debe a que la clave de bucket cifra las claves de datos que se utilizan para cifrar los objetos en Amazon S3. Si bien el uso de una clave de bucket no elimina todas las llamadas a la API AWS KMS, reduce su número. Como resultado, ya no hay one-to-one coincidencia entre los intentos de acceso a objetos de Amazon S3 y las llamadas a la API a AWS KMS.

Uso de claves KMS con Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling es un servicio recomendado para automatizar el escalado de las instancias de Amazon EC2. Le ayuda a asegurarse de que dispone del número correcto de instancias para gestionar la carga de su aplicación. Amazon EC2 Auto Scaling utiliza un rol vinculado a un servicio que proporciona los permisos adecuados al servicio y autoriza sus actividades en su cuenta. Para usar claves de KMS con Amazon EC2 Auto Scaling, AWS KMS sus políticas clave deben permitir que el rol vinculado al servicio utilice su clave de KMS con algunas operaciones de API, por ejemplo`Decrypt`, para que la automatización sea útil. Si la política AWS KMS clave no autoriza al responsable de IAM que está realizando la operación a realizar una acción, se denegará

dicha acción. Para obtener más información sobre cómo aplicar correctamente los permisos en la política clave para permitir el acceso, consulte Protección de datos en Amazon EC2 Auto Scaling en la documentación de Amazon EC2 Auto Scaling.

Rotación clave AWS KMS y alcance del impacto

No recomendamos la rotación de claves AWS Key Management Service (AWS KMS), a menos que sea necesario rotar las claves por motivos de conformidad con la normativa. Por ejemplo, es posible que tengas que rotar tus claves de KMS debido a políticas empresariales, normas contractuales o normativas gubernamentales. El diseño reduce AWS KMS significativamente los tipos de riesgo que la rotación de claves suele utilizarse para mitigar. Si debe girar las claves KMS, le recomendamos que utilice la rotación de clave automática y la rotación de clave manual solo si no se admite la rotación automática de claves.

En esta sección se tratan los siguientes temas clave sobre la rotación:

- AWS KMS rotación clave simétrica
- Rotación de claves para los volúmenes de Amazon EBS
- Rotación de claves para Amazon RDS
- Rotación de claves para Amazon S3 y replicación en la misma región
- Rotación de claves KMS con material importado

AWS KMS rotación clave simétrica

AWS KMS admite la rotación automática de claves solo para claves KMS de cifrado simétrico con el material de clave que AWS KMS crea. La rotación automática es opcional para las claves KMS administradas por el cliente. Anualmente, AWS KMS rota el material clave de las claves de KMS AWS administradas. AWS KMS guarda todas las versiones anteriores del material criptográfico a perpetuidad, de modo que puede descifrar cualquier dato que esté cifrado con esa clave KMS. AWS KMS no elimina ningún material de clave girada hasta que elimine la clave KMS. Además, al descifrar un objeto mediante el uso AWS KMS, el servicio determina el material de soporte correcto que se debe utilizar en la operación de descifrado; no es necesario proporcionar parámetros de entrada adicionales.

Como AWS KMS conserva las versiones anteriores del material de claves criptográficas y se puede utilizar ese material para descifrar datos, la rotación de claves no ofrece ninguna ventaja de seguridad adicional. El mecanismo de rotación de claves existe para facilitar la rotación de claves si

se trabaja con una carga de trabajo en un contexto en el que lo exigen los requisitos reglamentarios o de otro tipo.

Rotación de claves para los volúmenes de Amazon EBS

Puede rotar las claves de datos de Amazon Elastic Block Store (Amazon EBS) mediante uno de los siguientes enfoques. El enfoque depende de los flujos de trabajo, los métodos de implementación y la arquitectura de la aplicación. Es posible que desee hacerlo al cambiar de una clave AWS administrada a una clave administrada por el cliente.

Utilizar las herramientas del sistema operativo para copiar los datos de un volumen a otro

1. Cree la nueva clave KMS. Para obtener instrucciones, consulte Crear una clave KMS.
2. Cree un nuevo volumen de Amazon EBS que sea del mismo tamaño o mayor que el original. Para el cifrado, especifique la clave KMS que creó. Para obtener instrucciones, consulte Crear un volumen de Amazon EBS.
3. Monte el nuevo volumen en la misma instancia o contenedor que el volumen original. Para obtener instrucciones, consulte Adjuntar un volumen de Amazon EBS a una instancia de Amazon EC2.
4. Con la herramienta de sistema operativo que prefiera, copie los datos del volumen existente al nuevo volumen.
5. Cuando se complete la sincronización, durante un período de mantenimiento programado previamente, detenga el tráfico a la instancia. Para obtener instrucciones, consulta Cómo detener e iniciar las instancias manualmente.
6. Desmonte el volumen original. Para obtener instrucciones, consulte Separar un volumen de Amazon EBS de una instancia de Amazon EC2.
7. Monte el nuevo volumen en el punto de montaje original.
8. Compruebe que el nuevo volumen funciona correctamente.
9. Elimine el volumen original. Para obtener instrucciones, consulte Eliminar un volumen de Amazon EBS.

Para usar una instantánea de Amazon EBS para copiar los datos de un volumen a otro

1. Cree la nueva clave KMS. Para obtener instrucciones, consulte Crear una clave KMS.
2. Cree una instantánea del volumen original en Amazon EBS. Para obtener instrucciones, consulte Crear instantáneas de Amazon EBS.

3. Cree un nuevo volumen a partir de la instantánea. Para el cifrado, especifique la nueva clave de KMS que creó. Para obtener instrucciones, consulte Crear un volumen de Amazon EBS.

   > **Note**
   >
   > En función de su carga de trabajo, es posible que desee utilizar la restauración rápida de instantáneas de Amazon EBS para minimizar la latencia inicial del volumen.

4. Cree una nueva instancia de Amazon EC2. Para obtener instrucciones, consulte Lanzar una instancia de Amazon EC2.
5. Adjunte el volumen que creó a la instancia de Amazon EC2. Para obtener instrucciones, consulte Adjuntar un volumen de Amazon EBS a una instancia de Amazon EC2.
6. Transfiera la nueva instancia a producción.
7. Gire la instancia original para sacarla de producción y elimínela. Para obtener instrucciones, consulte Eliminar un volumen de Amazon EBS.

> **Note**
>
> Es posible copiar instantáneas y modificar la clave de cifrado utilizada para la copia de destino. Tras copiar la instantánea y cifrarla con las claves de KMS que prefieras, también puedes crear una Amazon Machine Image (AMI) a partir de las instantáneas. Para obtener más información, consulte el cifrado de Amazon EBS en la documentación de Amazon EC2.

Rotación de claves para Amazon RDS

En el caso de algunos servicios, como Amazon Relational Database Service (Amazon RDS), el cifrado de datos se realiza dentro del servicio y lo proporciona. AWS KMS Siga las instrucciones siguientes para rotar una clave de una instancia de base de datos de Amazon RDS.

Para rotar una clave de KMS para una base de datos de Amazon RDS

1. Cree una instantánea de la base de datos cifrada original. Para obtener instrucciones, consulte Administrar copias de seguridad manuales en la documentación de Amazon RDS.
2. Copie la instantánea en una nueva instantánea. Para el cifrado, especifique la nueva clave KMS. Para obtener instrucciones, consulte Copiar una instantánea de base de datos para Amazon RDS.

3. Utilice la nueva instantánea para crear un nuevo clúster de Amazon RDS. Para obtener instrucciones, consulte Restauración en una instancia de base de datos en la documentación de Amazon RDS. De forma predeterminada, el clúster usa la nueva clave de KMS.
4. Compruebe el funcionamiento de la nueva base de datos y los datos que contiene.
5. Pase la nueva base de datos a producción.
6. Haga que la base de datos antigua deje de estar en producción y elimínela. Para obtener instrucciones, consulte Eliminar una instancia de base de datos.

Rotación de claves para Amazon S3 y replicación en la misma región

En el caso de Amazon Simple Storage Service (Amazon S3), para cambiar la clave de cifrado de un objeto, debe leer y volver a escribir el objeto. Al reescribir el objeto, se especifica de forma explícita la nueva clave de cifrado en la operación de escritura. Para hacer esto con muchos objetos, puede utilizar Amazon S3 Batch Operations. En la configuración del trabajo, especifique la nueva configuración de cifrado para la operación de copia. Por ejemplo, puede elegir SSE-KMS e introducir el KeyID.

Como alternativa, puede usar Amazon S3 Same Region Replication (SRR). SSR puede volver a cifrar los objetos en tránsito.

Rotación de claves KMS con material importado

AWS KMS no recupera ni rota el material clave importado. Para girar una clave KMS con material clave importado, debe girar la clave manualmente.

Recomendaciones para usar el AWS Encryption SDK

AWS Encryption SDKEs una herramienta poderosa para implementar el cifrado del lado del cliente en sus aplicaciones. Hay bibliotecas disponibles para Java JavaScript, C, Python y otros lenguajes de programación. Se integra con AWS Key Management Service (AWS KMS). También puede usarlo como un SDK independiente sin hacer referencia a las claves de KMS.

Las prácticas recomendadas para utilizar esta herramienta incluyen considerar detenidamente los requisitos de la aplicación. Equilibre esos requisitos con los riesgos que pueden presentar determinadas configuraciones, como la introducción del almacenamiento en caché de claves en su aplicación. Para obtener más información sobre el almacenamiento en caché de claves de datos, consulte Almacenamiento en caché de claves de datos en la documentación. AWS Encryption SDK

Tenga en cuenta las siguientes preguntas a la hora de decidir si se debe utilizar: AWS Encryption SDK

- ¿Existe algún requisito de cifrado del lado del cliente que no pueda cumplirse con el cifrado del lado del servidor con servicios que se integren? AWS KMS
- ¿Puede proteger adecuadamente las claves que se utilizan para cifrar los datos en el lado del cliente y cómo lo hará?
- ¿Existen otras bibliotecas de fit-for-purpose cifrado que se adapten mejor a su caso de uso? Considere AWS ofertas alternativas, como el cifrado del lado del cliente de Amazon S3 y el SDK de cifrado de AWS bases de datos.

Para obtener más información sobre cómo elegir el servicio adecuado para su caso de uso, consulte la documentación de AWS Crypto Tools.

Mejores prácticas de gestión de identidades y accesos para AWS KMS

Para usar AWS Key Management Service (AWS KMS), debe tener credenciales que AWS pueda usar para autenticar y autorizar sus solicitudes. Ningún AWS director tiene permisos para acceder a una clave de KMS a menos que dicho permiso se otorgue de forma explícita y nunca se deniegue. No hay permisos implícitos o automáticos para usar o administrar una clave de KMS. En los temas de esta sección se definen las prácticas recomendadas de seguridad para ayudarle a determinar qué controles de administración de AWS KMS acceso debe utilizar para proteger su infraestructura.

En esta sección se analizan los siguientes temas de administración de identidades y accesos:

- AWS KMS políticas clave y políticas de IAM
- Permisos con privilegios mínimos para AWS KMS
- Control de acceso basado en roles para AWS KMS
- Control de acceso basado en atributos para AWS KMS
- Contexto de cifrado para AWS KMS
- Solución de problemas de AWS KMS permisos

AWS KMS políticas clave y políticas de IAM

La forma principal de gestionar el acceso a AWS KMS los recursos es mediante políticas. Las políticas son documentos que describen qué entidades principales pueden acceder a qué recursos. Las políticas asociadas a una identidad AWS Identity and Access Management (IAM) (usuarios, grupos de usuarios o funciones) se denominan políticas basadas en la identidad. Las políticas de IAM que se asocian a los recursos se denominan políticas basadas en recursos. AWS KMS las políticas de recursos para las claves de KMS se denominan políticas clave. Además de las políticas de IAM y las políticas AWS KMS clave, AWS KMS apoya las subvenciones. Las concesiones proporcionan una forma flexible y eficaz de delegar permisos. Puede utilizar las subvenciones para conceder claves de acceso KMS con un límite de tiempo limitado a los directores de IAM en su Cuenta de AWS país o en otros países. Cuentas de AWS

Todas las claves KMS tienen una política de claves. Si no proporciona una, AWS KMS crea una para usted. La política de claves predeterminada que se AWS KMS utiliza varía en función de si se crea la clave mediante la AWS KMS consola o si se utiliza la AWS KMS API. Le recomendamos que edite

la política de claves predeterminada para adaptarla a los requisitos de su organización en materia de permisos con privilegios mínimos. Esto también debería ajustarse a su estrategia de uso de las políticas de IAM junto con las políticas clave. Para obtener más recomendaciones sobre el uso de las políticas de IAM con AWS KMS, consulte las prácticas recomendadas para las políticas de IAM en la documentación. AWS KMS

Puede utilizar la política clave para delegar la autorización de un director de IAM en la política basada en la identidad. También puede usar la política clave para refinar la autorización junto con la política basada en la identidad. En cualquier caso, tanto la política clave como la política basada en la identidad determinan el acceso, junto con cualquier otra política aplicable que abarque el acceso, como las políticas de control de servicios (), las políticas de control de recursos (SCPs)o los límites de los RCPs permisos. Si el principal está en una cuenta diferente a la clave de KMS, básicamente, solo se admiten las acciones criptográficas y de concesión. Para obtener más información sobre este escenario de cuentas múltiples, consulte Permitir que los usuarios de otras cuentas usen una clave KMS en la AWS KMS documentación.

Debe usar políticas de IAM basadas en la identidad en combinación con políticas clave para controlar el acceso a sus claves de KMS. Las subvenciones también se pueden utilizar en combinación con estas políticas para controlar el acceso a una clave de KMS. Para utilizar una política basada en la identidad para controlar el acceso a una clave de KMS, la política de claves debe permitir que la cuenta utilice políticas basadas en la identidad. Puede especificar una declaración de política de claves que habilite las políticas de IAM o puede especificar explícitamente la entidad principal permitida en la política de claves.

Al redactar políticas, asegúrese de contar con controles estrictos que restrinjan quién puede realizar las siguientes acciones:

- Actualice, cree y elimine las políticas de IAM y las políticas clave de KMS
- Adjunte y separe las políticas basadas en la identidad de los usuarios, roles y grupos
- Adjunte y separe las políticas clave de las AWS KMS claves de KMS
- Cree concesiones para sus claves de KMS: ya sea que controle el acceso a sus claves de KMS exclusivamente con políticas clave o que combine las políticas clave con las políticas de IAM, debe restringir la capacidad de modificar las políticas. Implemente un proceso de aprobación para cambiar cualquier política existente. Un proceso de aprobación puede ayudar a evitar lo siguiente:
  - Pérdida accidental de los permisos principales de IAM: es posible realizar cambios que impidan que los responsables de IAM puedan gestionar la clave o utilizarla en operaciones criptográficas. En situaciones extremas, es posible revocar los permisos de administración de claves de

todos los usuarios. Si esto ocurre, debes ponerte en contacto con nosotros AWS Supportpara recuperar el acceso a la clave.

- Cambios no aprobados en las políticas clave de KMS: si un usuario no autorizado obtiene acceso a la política clave, podría modificarla para delegar los permisos a una persona no autorizada Cuenta de AWS o principal.
- Cambios no aprobados en las políticas de IAM: si un usuario no autorizado obtiene un conjunto de credenciales con permisos para administrar la membresía de un grupo, podría aumentar sus propios permisos y realizar cambios en sus políticas de IAM, políticas clave, configuración de claves de KMS u otras configuraciones de recursos. AWS

Revise detenidamente las funciones y los usuarios de IAM asociados a los directores de IAM designados como sus administradores clave de KMS. Esto puede ayudar a evitar eliminaciones o cambios no autorizados. Si necesita cambiar los principales que tienen acceso a sus claves de KMS, compruebe que los nuevos directores de administrador se agreguen a todas las políticas clave obligatorias. Pruebe sus permisos antes de eliminar el principal administrador anterior. Recomendamos encarecidamente seguir todas las prácticas recomendadas de seguridad de IAM y utilizar credenciales temporales en lugar de credenciales de larga duración.

Te recomendamos conceder permisos de acceso con plazos determinados mediante subvenciones si no conoces los nombres de los directores en el momento de crear las políticas o si los directores que requieren acceso cambian con frecuencia. El principal beneficiario puede estar en la misma cuenta que la clave de KMS o en una cuenta diferente. Si la clave principal y la clave de KMS están en cuentas diferentes, debe especificar una política basada en la identidad además de la concesión. Las concesiones requieren una administración adicional, ya que debe llamar a una API para crear la concesión y para retirarla o revocarla cuando ya no sea necesaria.

Ningún responsable AWS , ni siquiera el usuario raíz de la cuenta o el creador de la clave, tiene permisos para acceder a una clave de KMS, a menos que se les permita de forma explícita y no se les deniegue explícitamente en una política de claves, una política de IAM o una concesión. Por extensión, debes tener en cuenta qué pasaría si un usuario obtuviera acceso no deseado para usar una clave de KMS y cuál sería el impacto. Para mitigar este riesgo, tenga en cuenta lo siguiente:

- Puede mantener diferentes claves de KMS para diferentes categorías de datos. Esto le ayuda a separar las claves y a mantener políticas clave más concisas que contienen declaraciones de políticas que se refieren específicamente al acceso principal a esa categoría de datos. También significa que, si se accede a las credenciales de IAM pertinentes de forma no intencionada, la

identidad vinculada a ese acceso solo tendrá acceso a las claves especificadas en la política de IAM y solo si la política de claves permite el acceso a ese principal.

- Puede evaluar si un usuario con acceso no deseado a la clave puede acceder a los datos. Por ejemplo, con Amazon Simple Storage Service (Amazon S3), el usuario también debe tener los permisos adecuados para acceder a los objetos cifrados en Amazon S3. Como alternativa, si un usuario tiene acceso no deseado (mediante RDP o SSH) a una EC2 instancia de Amazon que tiene un volumen cifrado con una clave de KMS, el usuario puede acceder a los datos mediante las herramientas del sistema operativo.

> **Note**
>
> Servicios de AWS ese uso AWS KMS no expone el texto cifrado a los usuarios (la mayoría de los enfoques actuales de criptoanálisis requieren el acceso al texto cifrado). Además, el texto cifrado no está disponible para su examen físico fuera de un centro de AWS datos porque todos los soportes de almacenamiento se destruyen físicamente cuando se retiran del servicio, de acuerdo con los requisitos del NIST 00-88. SP8

Permisos con privilegios mínimos para AWS KMS

Dado que sus claves KMS protegen la información confidencial, le recomendamos que siga el principio del acceso con menos privilegios. Cuando defina las políticas de claves, delegue los permisos mínimos necesarios para realizar una tarea. Permita todas las acciones (`kms:*`) de una política de claves de KMS solo si planea restringir aún más los permisos con políticas adicionales basadas en la identidad. Si planea administrar los permisos con políticas basadas en la identidad, limite quién tiene la capacidad de crear y adjuntar políticas de IAM a las entidades principales de IAM y supervise los cambios en las políticas.

Si permites todas las acciones (`kms:*`) tanto en la política clave como en la política basada en la identidad, el responsable tiene permisos administrativos y de uso para la clave de KMS. Como práctica recomendada de seguridad, recomendamos delegar estos permisos únicamente a directores específicos. Considere cómo asignar los permisos a los directores que administrarán sus claves y a los principales que usarán sus claves. Puede hacerlo nombrando explícitamente al principal en la política de claves o limitando a qué principios se asocia la política basada en la identidad. También puede usar claves de condición para restringir los permisos. Por ejemplo, puedes usar aws:

PrincipalTag para permitir todas las acciones si el director que realiza la llamada a la API tiene la etiqueta especificada en la regla de condición.

Para entender cómo se evalúan las declaraciones de políticas AWS, consulte la lógica de evaluación de políticas en la documentación de IAM. Recomendamos revisar este tema antes de redactar políticas para ayudar a reducir la posibilidad de que su política tenga efectos no deseados, como proporcionar acceso a directores que no deberían tener acceso.

> **Tip**
>
> Cuando pruebe una aplicación en un entorno que no sea de producción, utilice AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) como ayuda para aplicar los permisos con privilegios mínimos en sus políticas de IAM.

Si utiliza usuarios de IAM en lugar de funciones de IAM, le recomendamos encarecidamente que utilice la autenticación AWS multifactor (MFA) para mitigar la vulnerabilidad de las credenciales a largo plazo. Puede utilizar la MFA para hacer lo siguiente:

- Requerir que los usuarios validen sus credenciales con MFA antes de realizar acciones privilegiadas, como programar la eliminación de claves.
- Dividir la propiedad de una contraseña de cuenta de administrador y el dispositivo de MFA entre varias personas para implementar la autorización dividida.

Para ver ejemplos de políticas que pueden ayudarle a configurar los permisos con privilegios mínimos, consulte los ejemplos de políticas de IAM en la documentación. AWS KMS

Control de acceso basado en roles para AWS KMS

El control de acceso basado en roles (RBAC) es una estrategia de autorización que proporciona a los usuarios solo los permisos necesarios para realizar sus tareas laborales, y nada más. Es un enfoque que puede ayudarlo a implementar el principio del privilegio mínimo.

AWS KMS es compatible con RBAC. Le permite controlar el acceso a sus claves especificando permisos detallados dentro de las políticas clave. Las políticas de claves especifican un recurso, una acción, un efecto, una entidad principal y unas condiciones opcionales para conceder el acceso a las claves. Para implementar el RBAC en AWS KMS, recomendamos separar los permisos de los usuarios clave de los administradores clave.

Para los usuarios clave, asigne solo los permisos que el usuario necesite. Usa las siguientes preguntas para ayudarte a refinar aún más los permisos:

- ¿Qué directores de IAM necesitan acceder a la clave?
- ¿Qué acciones debe realizar cada entidad principal con la clave? Por ejemplo, ¿el director solo necesita permisos`Encrypt`? `Sign`
- ¿A qué recursos necesita acceder el director?
- ¿La entidad es un ser humano o un Servicio de AWS? Si se trata de un servicio, puedes usar la clave kms: ViaService condition para restringir el uso de la clave a un servicio específico.

En el caso de los administradores clave, asigne solo los permisos que el administrador necesite. Por ejemplo, los permisos de un administrador pueden variar en función de si la clave se utiliza en entornos de prueba o de producción. Si utiliza permisos menos restrictivos en determinados entornos que no son de producción, implemente un proceso para probar las políticas antes de ponerlas en producción.

Para ver ejemplos de políticas que pueden ayudarle a configurar el control de acceso basado en roles para los principales usuarios y administradores, consulte RBAC para. AWS KMS

Control de acceso basado en atributos para AWS KMS

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. Al igual que el RBAC, es un enfoque que puede ayudarlo a implementar el principio del privilegio mínimo.

AWS KMS es compatible con ABAC, ya que permite definir los permisos en función de las etiquetas asociadas al recurso de destino, como una clave de KMS, y de las etiquetas asociadas a la persona que realiza la llamada a la API. En AWS KMS, puedes usar etiquetas y alias para controlar el acceso a las claves gestionadas por tus clientes. Por ejemplo, puede definir políticas de IAM que utilicen claves de condición de etiqueta para permitir operaciones cuando la etiqueta del principal coincida con la etiqueta asociada a la clave de KMS. Para ver un tutorial, consulte Definir los permisos de acceso a AWS los recursos en función de las etiquetas en la AWS KMS documentación.

Como práctica recomendada, utilice las estrategias de ABAC para simplificar la gestión de las políticas de IAM. Con ABAC, los administradores pueden usar etiquetas para permitir el acceso a nuevos recursos en lugar de actualizar las políticas existentes. ABAC requiere menos políticas porque no es necesario crear políticas diferentes para diferentes funciones laborales. Para

obtener más información, consulte Comparación del ABAC con el modelo RBAC tradicional en la documentación de IAM.

Aplique la mejor práctica de permisos con privilegios mínimos al modelo ABAC. Proporcione a los directores de IAM solo los permisos que necesitan para realizar sus tareas. Controle cuidadosamente el acceso al etiquetado para APIs que los usuarios puedan modificar las etiquetas de las funciones y los recursos. Si utilizas claves de condición de alias clave como soporte para ABAC AWS KMS, asegúrate de disponer también de controles estrictos que restrinjan quién puede crear claves y modificar los alias.

También puedes usar etiquetas para vincular una clave específica a una categoría empresarial y comprobar que se está utilizando la clave correcta para una acción determinada. Por ejemplo, puedes usar AWS CloudTrail los registros para comprobar que la clave utilizada para realizar una AWS KMS acción específica pertenece a la misma categoría empresarial que el recurso en el que se está utilizando.

> **Warning**
>
> No incluya información confidencial en la clave ni en el valor de la etiqueta. Las etiquetas no están cifradas. Son accesibles para muchos Servicios de AWS, incluida la facturación.

Antes de implementar un enfoque ABAC en su control de acceso, considere si los demás servicios que utiliza admiten este enfoque. Si necesita ayuda para determinar qué servicios son compatibles con ABAC, consulte quéServicios de AWS servicios funcionan con IAM en la documentación de IAM.

Para obtener más información sobre la implementación de ABAC AWS KMS y las claves de condiciones que pueden ayudarle a configurar las políticas, consulte ABAC for. AWS KMS

Contexto de cifrado para AWS KMS

Todas las operaciones AWS KMS criptográficas con claves KMS de cifrado simétrico aceptan un contexto de cifrado. El contexto de cifrado es un conjunto opcional de pares clave-valor no secretos que pueden contener información contextual adicional sobre los datos. Como práctica recomendada, puede insertar el contexto de cifrado en `Encrypt` las operaciones AWS KMS para mejorar la autorización y la auditabilidad de las llamadas a la API de descifrado. AWS KMS AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales (AAD) para respaldar el cifrado autenticado. El contexto de cifrado se vincula criptográficamente al texto cifrado, de tal forma que se requiera el mismo contexto de cifrado para descifrar los datos.

El contexto de cifrado no es secreto y no está cifrado. Aparece en texto plano en AWS CloudTrail los registros para que pueda usarlo para identificar y clasificar sus operaciones criptográficas. Como el contexto de cifrado no es secreto, debe permitir que solo las personas autorizadas accedan a sus datos de registro. CloudTrail

También puede usar las EncryptionContextKeys claves condicionales kms ::context-key EncryptionContext y kms: para controlar el acceso a una clave KMS de cifrado simétrico en función del contexto de cifrado. También puede usar estas claves de condición para exigir que los contextos de cifrado se utilicen en las operaciones criptográficas. Para estas claves de condición, consulte las instrucciones sobre el uso `ForAnyValue` o `ForAllValues` configuración de operadores para asegurarse de que sus políticas reflejen los permisos previstos.

Solución de problemas de AWS KMS permisos

Cuando redacte políticas de control de acceso para una clave de KMS, tenga en cuenta cómo funcionan juntas la política de IAM y la política clave. Los permisos efectivos de un principal son los permisos que todas las políticas vigentes conceden (y no deniegan de forma explícita). Dentro de una cuenta, los permisos de una clave de KMS pueden verse afectados por las políticas de IAM basadas en la identidad, las políticas clave, los límites de los permisos, las políticas de control de servicios o las políticas de sesión. Por ejemplo, si utilizas políticas clave y basadas en la identidad para controlar el acceso a la clave de KMS, se evalúan todas las políticas relacionadas con el principal y el recurso para determinar la autorización del principal para realizar una acción determinada. Para obtener más información, consulte Lógica de evaluación de políticas en la documentación de IAM.

Para obtener información detallada y un diagrama de flujo para solucionar problemas de acceso a claves, consulte Solución de problemas de acceso a claves en la documentación. AWS KMS

Para solucionar un mensaje de error de acceso denegado

1. Confirme que las políticas basadas en la identidad de IAM y las políticas clave de KMS permiten el acceso.
2. Confirme que un límite de permisos en IAM no restrinja el acceso.
3. Confirme que una política de control de servicios (SCP) o una política de control de recursos (RCP) no restrinja AWS Organizations el acceso.
4. Si utiliza puntos de enlace de VPC, confirme que las políticas de puntos de enlace sean correctas.

5. En las políticas basadas en la identidad y en las políticas clave, elimine cualquier condición o referencia a recursos que restrinja el acceso a la clave. Tras eliminar estas restricciones, confirme que el director puede llamar correctamente a la API en la que se produjo el error anterior. Si tiene éxito, vuelva a aplicar las condiciones y las referencias a los recursos una por una y, después de cada una, compruebe que el principal sigue teniendo acceso. Esto le ayuda a identificar la condición o la referencia de recurso que está causando el error.

Para obtener más información, consulte Solución de problemas de mensajes de error de acceso denegado en la documentación de IAM.

Mejores prácticas de detección y monitoreo para AWS KMS

La detección y el monitoreo son una parte importante para comprender la disponibilidad, el estado y el uso de sus AWS Key Management Service (AWS KMS) claves. La supervisión ayuda a mantener la seguridad, la confiabilidad, la disponibilidad y el rendimiento de sus AWS soluciones. AWS proporciona varias herramientas para monitorear sus claves y AWS KMS operaciones de KMS. En esta sección, se describe cómo configurar y utilizar estas herramientas para obtener una mayor visibilidad del entorno y supervisar el uso de las claves de KMS.

En esta sección se analizan los siguientes temas de detección y supervisión:

- Supervise AWS KMS las operaciones con AWS CloudTrail
- Supervisión del acceso a las claves de KMS con IAM Access Analyzer
- Monitorear la configuración de cifrado de otros Servicios de AWS con AWS Config
- Supervisión de claves de KMS con CloudWatch alarmas de Amazon
- Automatizar las respuestas con Amazon EventBridge

Supervise AWS KMS las operaciones con AWS CloudTrail

AWS KMS está integrado con AWS CloudTrailun servicio que puede grabar todas las llamadas realizadas AWS KMS por los usuarios, los roles y otros Servicios de AWS. CloudTrail captura todas las llamadas a la API AWS KMS como eventos, incluidas las llamadas desde la AWS KMS consola AWS KMS APIs AWS CloudFormation,,, AWS Command Line Interface (AWS CLI) y Herramientas de AWS para PowerShell.

CloudTrail registra todas AWS KMS las operaciones, incluidas las de solo lectura, como `ListAliases` y. `GetKeyRotationStatus` También registra las operaciones que administran las claves de KMS, como `CreateKey` y`PutKeyPolicy, and cryptographic operations, such as GenerateDataKey`. `Decrypt` También registra las operaciones internas AWS KMS que lo requieran, como`DeleteExpiredKeyMaterial`, `DeleteKeySynchronizeMultiRegionKey`, y`RotateKey`.

CloudTrail está activado en tu Cuenta de AWS dispositivo cuando lo creas. De forma predeterminada, el historial de eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de actividad registrada en la API de eventos de gestión en un. Región de AWSPara supervisar o auditar el uso de tus claves de KMS más allá de los 90 días, te recomendamos crear un registro para ti. CloudTrail Cuenta de AWS Si ha creado una organización

en AWS Organizations, puede crear un registro de la organización o un almacén de datos de eventos que registre los eventos de todos los Cuentas de AWS miembros de esa organización.

Una vez que hayas establecido un registro para tu cuenta u organización, puedes usar otro Servicios de AWS para almacenar, analizar y responder automáticamente a los eventos que se registran en el registro. Por ejemplo, puede hacer lo siguiente:

- Puedes configurar CloudWatch alarmas de Amazon que te notifiquen ciertos eventos en la ruta. Para obtener más información, consulte la sección Supervisión de claves de KMS con CloudWatch alarmas de Amazon de esta guía.
- Puedes crear EventBridge reglas de Amazon que realicen automáticamente una acción cuando se produzca un evento en la ruta. Para obtener más información, consulta Automatizar las respuestas con Amazon EventBridge en esta guía.
- Puede usar Amazon Security Lake para recopilar y almacenar registros de varios Servicios de AWS, incluidos CloudTrail. Para obtener más información, consulte Recopilación de datos desde Servicios de AWS Security Lake en la documentación de Amazon Security Lake.
- Para mejorar el análisis de la actividad operativa, puede consultar CloudTrail los registros con Amazon Athena. Para obtener más información, consulte AWS CloudTrail los registros de consultas en la documentación de Amazon Athena.

Para obtener más información sobre la supervisión de AWS KMS las operaciones con CloudTrail, consulte lo siguiente:

- Registrar llamadas a la AWS KMS API con AWS CloudTrail
- Ejemplos de entradas de AWS KMS registro
- Supervise las claves de KMS con Amazon EventBridge
- CloudTrail integración con Amazon EventBridge

Supervisión del acceso a las claves de KMS con IAM Access Analyzer

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) le ayuda a identificar los recursos de su organización y las cuentas (como las claves de KMS) que se comparten con una entidad externa. Este servicio puede ayudarlo a identificar el acceso no intencionado o demasiado amplio a sus recursos y datos, lo que constituye un riesgo para la seguridad. IAM Access Analyzer

identifica los recursos que se comparten con entidades externas mediante un razonamiento basado en la lógica para analizar las políticas basadas en los recursos de su entorno. AWS

Puede utilizar IAM Access Analyzer para identificar qué entidades externas tienen acceso a sus claves de KMS. Al activar IAM Access Analyzer, se crea un analizador para toda la organización o para una cuenta de destino. La organización o cuenta que elija se conoce como zona de confianza del analizador. El analizador supervisa los recursos compatibles dentro de la zona de confianza. Cualquier acceso a los recursos por parte de los directores dentro de la zona de confianza se considera de confianza.

En el caso de las claves KMS, IAM Access Analyzer analiza las políticas y concesiones clave que se aplican a una clave. Determina si una política o concesión clave permite a una entidad externa acceder a la clave. Utilice el analizador de acceso de IAM para determinar si las entidades externas tienen acceso a sus claves de KMS y, a continuación, compruebe si esas entidades deberían tener acceso.

Para obtener más información sobre el uso del analizador de acceso de IAM para supervisar el acceso a las claves de KMS, consulte lo siguiente:

- Uso de AWS Identity and Access Management Access Analyzer
- Tipos de recursos de IAM Access Analyzer para acceso externo
- Tipos de recursos de IAM Access Analyzer: AWS KMS keys
- Hallazgos relacionados con el acceso externo y no utilizado

Monitorear la configuración de cifrado de otros Servicios de AWS con AWS Config

AWS Configproporciona una vista detallada de la configuración de AWS los recursos de su Cuenta de AWS. Puede utilizarlo AWS Config para comprobar que los Servicios de AWS que utilizan sus claves de KMS tienen sus ajustes de cifrado configurados adecuadamente. Por ejemplo, puede usar la AWS Config regla de volúmenes cifrados para validar que los volúmenes de Amazon Elastic Block Store (Amazon EBS) estén cifrados.

AWS Config incluye reglas administradas que le ayudan a elegir rápidamente las reglas con las que evaluar sus recursos. Compruebe AWS Config si las reglas gestionadas que necesita son compatibles en esa región. Regiones de AWS Las reglas gestionadas disponibles incluyen las comprobaciones de configuración de las instantáneas del Amazon Relational Database Service

(Amazon RDS), el cifrado de pistas CloudTrail , el cifrado predeterminado para los depósitos de Amazon Simple Storage Service (Amazon S3), el cifrado de tablas de Amazon DynamoDB y mucho más.

También puede crear reglas personalizadas y aplicar su lógica empresarial para determinar si sus recursos cumplen con sus requisitos. El código fuente abierto de muchas reglas administradas está disponible en el repositorio de AWS Config reglas en GitHub. Estos pueden ser un punto de partida útil para desarrollar tus propias reglas personalizadas.

Cuando un recurso no cumple con una regla, puede iniciar acciones de respuesta. AWS Config incluye las acciones de corrección que lleva a cabo AWS Systems Manager Automation. Por ejemplo, si ha aplicado la cloud-trail-encryption-enabledregla y la regla arroja un `NON_COMPLIANT` resultado, AWS Config puede iniciar un documento de automatización que solucione el problema cifrando los CloudTrail registros por usted.

AWS Config le permite comprobar de forma proactiva el cumplimiento de AWS Config las reglas antes de aprovisionar los recursos. La aplicación de reglas en modo proactivo le ayuda a evaluar las configuraciones de los recursos de la nube antes de crearlos o actualizarlos. La aplicación de reglas en modo proactivo como parte de su proceso de implementación le permite probar las configuraciones de los recursos antes de desplegarlos.

También puede implementar AWS Config reglas como controles AWS Security Hub CSPM. Security Hub CSPM ofrece estándares de seguridad que puede aplicar a su. Cuentas de AWS Estos estándares le ayudan a evaluar su entorno en función de las prácticas recomendadas. El estándar de prácticas recomendadas de seguridad AWS fundamentales incluye controles dentro de la categoría de control de protección para comprobar que el cifrado en reposo está configurado y que las políticas de claves de KMS siguen las prácticas recomendadas.

Para obtener más información sobre AWS Config cómo supervisar la configuración de cifrado en Servicios de AWS, consulte lo siguiente:

- Introducción a AWS Config
- AWS Config reglas gestionadas
- AWS Config custom rules
- Corregir los recursos no conformes con AWS Config

Supervisión de claves de KMS con CloudWatch alarmas de Amazon

Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede utilizarlas CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir.

La caducidad del material clave importado, o la eliminación de una clave, son eventos potencialmente catastróficos si no son intencionados o no se planifican adecuadamente. Le recomendamos que configure CloudWatch las alarmas para que le avisen de estos eventos antes de que se produzcan. También le recomendamos que configure políticas AWS Identity and Access Management (de IAM) o políticas de control de AWS Organizations servicios (SCPs) para evitar la eliminación de claves importantes.

CloudWatch las alarmas le ayudan a tomar medidas correctivas, como cancelar la eliminación de claves, o tomar medidas correctivas, como volver a importar el material clave eliminado o caducado.

Automatizar las respuestas con Amazon EventBridge

También puede usar Amazon EventBridge para notificarle eventos importantes que afecten a sus claves de KMS. EventBridge es una Servicio de AWS que ofrece un flujo casi en tiempo real de los eventos del sistema que describen los cambios en los AWS recursos. EventBridgerecibe automáticamente los eventos del CloudTrail Security Hub CSPM. En EventBridge, puede crear reglas que respondan a los eventos registrados por. CloudTrail

AWS KMS entre los eventos se incluyen los siguientes:

- El material clave de una clave de KMS se rotaba automáticamente
- El material clave importado en una clave de KMS ha caducado
- Se eliminó una clave de KMS cuya eliminación estaba programada

Estos eventos pueden iniciar acciones adicionales en su Cuenta de AWS. Estas acciones son diferentes de las CloudWatch alarmas descritas en la sección anterior porque solo se pueden activar después de que se produzca el evento. Por ejemplo, es posible que desee eliminar los recursos que están conectados a una clave específica después de que se haya eliminado esa clave, o puede que desee informar a un equipo de cumplimiento o auditoría de que la clave se ha eliminado.

También puede filtrar cualquier otro evento de la API en el que se haya iniciado sesión CloudTrail mediante EventBridge. Esto significa que si las acciones clave de la API relacionadas con las políticas son motivo de preocupación específica, puedes filtrarlas. Por ejemplo, puedes filtrar la acción de EventBridge la `PutKeyPolicy` API. En términos más generales, puedes filtrar cualquier acción de la API que comience con `Disable*` o `Delete*` inicie respuestas automatizadas.

Con EventBridge ella, puede monitorizar (que es un control de detección) e investigar y responder (que son controles de respuesta) ante eventos inesperados o seleccionados. Por ejemplo, puede alertar a los equipos de seguridad y tomar medidas específicas si se crea un usuario o un rol de IAM, cuando se crea una clave de KMS o cuando se cambia una política clave. Puedes crear una regla de EventBridge eventos que filtre las acciones de la API que especifiques y, a continuación, asociar los objetivos a la regla. Los objetivos de ejemplo incluyen AWS Lambda funciones, notificaciones del Amazon Simple Notification Service (Amazon SNS), colas de Amazon Simple Queue Service (Amazon SQS) y más. Para obtener más información sobre el envío de eventos a los objetivos, consulta los destinos de Event Bus en Amazon EventBridge.

Para obtener más información sobre la supervisión AWS KMS EventBridge y la automatización de las respuestas, consulte Supervisar las claves de KMS con Amazon EventBridge en la AWS KMS documentación.

Mejores prácticas de administración de costos y facturación para AWS KMS

Gracias a su amplitud y profundidad, Servicios de AWS ofrezca la flexibilidad necesaria para gestionar sus costes y, al mismo tiempo, cumplir con los requisitos empresariales. En esta sección se describen los precios del almacenamiento de claves en AWS Key Management Service (AWS KMS) y se ofrecen recomendaciones para reducir los costes, por ejemplo, mediante el almacenamiento en caché de claves. También puedes revisar el uso de las claves de KMS para determinar si existen oportunidades adicionales para reducir los costos.

En esta sección se analizan los siguientes temas de administración de costos y facturación:

- AWS KMS precios del almacenamiento de claves
- Claves de bucket de Amazon S3 con cifrado predeterminado
- Almacenar en caché las claves de datos mediante AWS Encryption SDK
- Alternativas al almacenamiento en caché de claves y a las claves de bucket de Amazon S3
- Administrar los costos de registro para el uso de claves de KMS

AWS KMS precios del almacenamiento de claves

Cada uno de los AWS KMS key que cree AWS KMS tiene un coste. El cargo mensual es el mismo para las claves simétricas, las claves asimétricas, las claves HMAC, las claves multirregionales (cada clave principal y cada réplica de una clave multirregional), las claves con material de clave importado y las claves KMS con un origen de clave de un almacén de claves externo o AWS CloudHSM de uno externo.

En el caso de las claves KMS que se rotan automáticamente o a pedido, la primera y la segunda rotación de la clave añaden un coste mensual adicional (prorrateado por hora). Tras la segunda rotación, no se facturarán las rotaciones posteriores de ese mes. Consulte los AWS KMS precios para obtener la información más reciente sobre precios.

Se puede utilizar AWS Budgetspara configurar un presupuesto de uso. AWS Budgets puede avisarte cuando el gasto de tu cuenta supere determinados umbrales. En cuanto a los costes correspondientes AWS KMS, puedes crear un presupuesto de uso para enviar alertas en función de las claves o solicitudes del KMS. Esto puede mejorar la visibilidad de los costes de almacenamiento y uso de las AWS KMS claves.

Claves de bucket de Amazon S3 con cifrado predeterminado

En algunos casos de uso, las cargas de trabajo que acceden o generan un gran número de objetos en Amazon Simple Storage Service (Amazon S3) pueden generar grandes volúmenes de solicitudes, lo que AWS KMS aumenta los costes. La configuración de las claves de bucket de Amazon S3 puede ayudarle a reducir los costes hasta en un 99%. Esta es una alternativa recomendada a la desactivación del cifrado para ayudar a reducir los costes asociados AWS KMS a él.

Almacenar en caché las claves de datos mediante AWS Encryption SDK

Cuando se utiliza AWS Encryption SDKpara realizar el cifrado del lado del cliente, el almacenamiento en caché de las claves de datos puede ayudar a mejorar el rendimiento de la aplicación, reducir el riesgo de que las solicitudes de la aplicación AWS KMS se vean limitadas y ayudarle a reducir los costes. Para obtener más información sobre cómo empezar, consulte Cómo utilizar el almacenamiento en caché de claves de datos.

Alternativas al almacenamiento en caché de claves y a las claves de bucket de Amazon S3

Si el almacenamiento en caché de claves no es una opción para usted debido a sus requisitos de manejo de datos, también puede solicitar aumentos de AWS KMS cuota mediante la API Service Quotas Consola de administración de AWS o la API Service Quotas. Ten en cuenta el volumen de llamadas a la API que podrías realizar. La cantidad de llamadas a la API que realices es un factor importante a la hora de AWS KMS fijar los precios. Si aumentas la cuota de solicitudes para aumentar tu rendimiento, el aumento del número de solicitudes generará costes AWS KMS adicionales.

Administrar los costos de registro para el uso de claves de KMS

Todas las llamadas a la AWS KMS API se registran en AWS CloudTrail. Las aplicaciones y los servicios pueden generar grandes volúmenes de llamadas a la AWS KMS API (por ejemplo, para operaciones criptográficas, incluidas las de cifrado y descifrado). Revisar los CloudTrail registros sin una herramienta que te ayude a organizar esos datos, investigar las tendencias y buscar actividad anómala en las API puede resultar difícil. Amazon Athena proporciona estructuras de

datos predefinidas que pueden ayudarle a configurar rápidamente tablas para CloudTrail registros y empezar a analizar sus datos de registro. Resulta especialmente útil para realizar análisis puntuales o realizar investigaciones adicionales durante la respuesta a un incidente. Para obtener más información, consulte AWS CloudTrail los registros de consultas en la documentación de Athena.

Como pagas por consulta por Athena, puedes configurar tus mesas por adelantado sin coste alguno. No se cobran cargos por las declaraciones en el lenguaje de definición de datos. Cuando responde a un incidente, esto le ayuda a asegurarse de que ya se cumplen muchos requisitos previos. Para ayudarle a prepararse, se recomienda escribir las consultas después de crear la tabla, probarlas y asegurarse de que producen los resultados que desea. Puede guardar sus consultas en Athena para usarlas en el futuro. Para obtener más información sobre cómo empezar a utilizar Athena, consulte Introducción a Amazon Athena.

Los eventos de datos proporcionan visibilidad de las operaciones que se realizan en un recurso o dentro de él. Se denominan también operaciones del plano de datos. Algunos ejemplos son los `PutObject` eventos de Amazon S3 o las llamadas a la API de operaciones de funciones de Lambda. Los eventos de datos suelen ser actividades de gran volumen y se le cobrará por registrarlos. Para ayudar a controlar el volumen de eventos de datos que se registran en las rutas o en los almacenes de datos de eventos CloudTrail, puede optimizar el registro para CloudTrail reducir los costes y configurar Amazon S3 mediante la configuración de selectores de eventos avanzados para limitar los eventos de datos en CloudTrail los que iniciar sesión. AWS KMS Para obtener más información, consulte Cómo optimizar AWS CloudTrail los costes mediante el uso de selectores de eventos avanzados (entrada del AWS blog).

Recursos

AWS Key Management Service (AWS KMS) documentación

- AWS KMS Guía para desarrolladores
- Referencia de la API de AWS KMS
- AWS KMS en la AWS CLI Referencia

Herramientas

- AWS Encryption SDK

AWS Guía prescriptiva

Estrategias

- Crear una estrategia de cifrado para los datos en reposo

Guías

- Características y prácticas recomendadas de cifrado para Servicios de AWS
- AWS Arquitectura de referencia de privacidad (AWS PRA)

Patrones

- Cifre automáticamente los volúmenes de Amazon EBS
- Automatically remediate unencrypted Amazon RDS DB instances and clusters
- Supervise y corrija la eliminación programada de AWS KMS keys

Colaboradores

Creación

- Frank Phillis, arquitecto sénior de soluciones especializado en GTM, AWS
- Ken Beer, director de bibliotecas AWS KMS criptográficas, AWS
- Michael Miller, arquitecto sénior de soluciones, AWS
- Jeremy Stieglitz, director principal de productos, AWS
- Zach Miller, arquitecto principal de soluciones, AWS
- Peter M. O'Donnell, arquitecto principal de soluciones, AWS
- Patrick Palmer, arquitecto principal de soluciones, AWS
- Dave Walker, arquitecto principal de soluciones, AWS

Revisando

- Manigandan Shri, consultora sénior de entregas, AWS

Redacción técnica

- Lilly AbouHarb, redactora técnica sénior, AWS
- Kimberly Garmoe, redactora técnica sénior, AWS

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Publicación inicial	—	24 de marzo de 2025

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.