Guía para desarrolladores

AWS Key Management Service

AWS Key Management Service: Guía para desarrolladores

Table of Contents

AWS Key Management Service

AWS Key Management Service (AWS KMS) es un servicio administrado que le permite crear y controlar fácilmente las claves de cifrado que se utilizan para proteger sus datos. AWS KMS utiliza módulos de seguridad de hardware (HSM) para proteger y validar su AWS KMS keys según el Programa de validación de módulos criptográficos FIPS 140-2. Las regiones China (Pekín) y China (Ningxia) no admiten el programa de validación del módulo criptográfico FIPS 140-2. AWS KMS utiliza los HSM certificados por OSCCA para proteger las claves de KMS en las regiones de China.

AWS KMS está integrado con la mayoría de los demás servicios de AWS que cifran sus datos. AWS KMS también está integrado con AWS CloudTrail para registrar el uso de sus claves KMS para las necesidades de auditoría, regulación y cumplimiento.

Puede utilizar la API AWS KMS para crear y administrar claves KMS y funciones especiales, como almacenes de claves personalizadas y utilizar claves KMS en operaciones criptográficas. Para obtener más detalles, consulte la Referencia de API de la AWS Key Management Service.

Puede crear y administrar su AWS KMS keys:

- Crear, editar y ver claves KMS simétricas y asimétricas, incluidas las claves HMAS.
- Controle el acceso a las claves KMS mediante políticas de claves, políticas de IAM y concesiones. AWS KMS es compatible con el control de acceso basado en atributos (ABAC). También puede refinar políticas mediante claves de condición.
- Crear, eliminar, enumerar y actualizar alias, que son nombres descriptivos para sus claves KMS. También puede utilizar alias para controlar el acceso a sus claves KMS.
- Etiquete sus claves KMS para identificación, automatización y seguimiento de costos. También puede usar etiquetas para controlar el acceso a sus claves KMS.
- Habilitar y desactivar claves KMS.
- Habilitar y desactivar la rotación automática del material criptográfico en una clave KMS.
- Elimine las claves KMS para completar el ciclo de vida de las claves.

Puede usar sus claves KMS en operaciones criptográficas. Para ver ejemplos, consulte Programación de la API de AWS KMS.

- Cifrar, descifrar y volver a cifrar datos con claves KMS simétricas o asimétricas.

- Firmar y verificar mensajes con claves KMS asimétricas.
- Genere claves de datos simétricas exportables y pares de claves de datos asimétricos.
- Generar y verificar códigos HMAC.
- Genere números aleatorios adecuados para las aplicaciones de cifrado.

Puede utilizar las características avanzadas de AWS KMS

- Crear claves de varias regiones, que actúan como copias de la misma clave KMS en diferentes Regiones de AWS.
- Importar material criptográfico a una clave de KMS.
- Cree claves de KMS en su propio almacén de claves de AWS CloudHSM respaldado por su clúster de AWS CloudHSM.
- Cree claves de KMS en un almacén de claves externo respaldado por sus claves criptográficas ajenas a AWS.
- Conectarse directamente a AWS KMS a través de un punto de conexión privado en su VPC.
- Utilice el TLS híbrido postcuántico para proporcionar cifrado prospectivo en tránsito para los datos que envíe a AWS KMS

Con AWS KMS obtiene más control sobre el acceso a los datos que cifra. Puede utilizar las características criptográficas y administración de claves directamente en sus aplicaciones o a través de los servicios de AWS que están integrados con AWS KMS. Tanto si escribe aplicaciones para AWS como si usa los servicios de AWS, AWS KMS le permite mantener el control sobre quién puede usar sus AWS KMS keys y obtener acceso a sus datos cifrados.

AWS KMS se integra con AWS CloudTrail, un servicio que envía los archivos de registro al bucket de Amazon S3 designado. Al usarlo CloudTrail , puede monitorear e investigar cómo y cuándo se usaron sus claves KMS y quién las usó.

AWS KMS en Regiones de AWS

Las Regiones de AWS en las que se admite AWS KMS se mencionan en Cuotas y puntos de conexión de AWS Key Management Service. Si una característica de AWS KMS no se admite en una Región de AWS que admite AWS KMS, la diferencia regional se describe en el tema acerca de la característica.

Precios de AWS KMS

Al igual que con otros productos AWS, el uso de AWS KMS no requiere contratos o compras mínimas. Para obtener más información sobre los precios de AWS KMS, consulte Precios de AWS Key Management Service.

Acuerdo de nivel de servicios

AWS Key Management Service está respaldado por un acuerdo de nivel de servicios que define nuestra política de disponibilidad del servicio.

Más información

- Para obtener más información sobre los términos y conceptos utilizados en AWS KMS, consulte Conceptos de AWS KMS.
- Para obtener más información sobre la API de AWS KMS, consulte la referencia de la API de AWS Key Management Service. Para ver ejemplos en diferentes lenguajes de programación, consulte Programación de la API de AWS KMS.
- Para obtener información sobre cómo utilizar plantillas de AWS CloudFormation para crear y administrar claves de y alias, consulte Creación de AWS KMS recursos con AWS CloudFormation y la referencia de tipos de recursos de AWS Key Management Service en la Guía del usuario de AWS CloudFormation.
- Para obtener información técnica detallada sobre cómo utiliza AWS KMS la criptografía y protege las claves KMS, consulte el documento técnico Detalles criptográficos de AWS Key Management Service. La documentación de Detalles criptográficos no describe cómo AWS KMStrabaja en las regiones China (Pekín) y China (Ningxia).
- Para obtener una lista de puntos de conexión de AWS KMS, incluidos los puntos de conexión FIPS, en cada Región de AWS, consulte Service endpoints en el tema AWS Key Management Service de la Referencia general de AWS.
- Para obtener ayuda sobre preguntas acerca de AWS KMS, consulte el Foro de discusión de AWS Key Management Service.

AWS KMS en los SDK de AWS

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby

Conceptos de AWS KMS

Conozca los términos y conceptos básicos que se usan en AWS Key Management Service (AWS KMS) y cómo funcionan conjuntamente para proteger sus datos.

Temas

- AWS KMS keys
- Claves de cliente y claves de AWS
- Claves KMS de cifrado simétricas
- Claves de KMS asimétricas
- Claves KMS HMAC
- Claves de datos
- Pares de claves de datos
- Alias
- Almacenes de claves personalizados
- Operaciones criptográficas
- Identificadores clave () KeyId
- Material de claves
- Origen del material de claves
- Especificación de clave
- Uso de claves
- Cifrado de sobre
- Contexto de cifrado
- Política de claves

- Concesión
- Auditoría del uso de claves KMS
- Infraestructura de administración de claves

AWS KMS keys

AWS KMS keys (claves KMS) son el recurso principal en AWS KMS. Puede utilizar una clave KMS para cifrar, descifrar y volver a cifrar datos. También puede generar claves de datos que puede usar fuera deAWS KMS. Normalmente, utilizará claves KMS de cifrado simétricas, pero puede crear y utilizar claves KMS asimétricas para el cifrado o la firma y crear y utilizar claves KMS HMAC para generar y verificar etiquetas HMAC.

> **Note**
>
> AWS KMS está reemplazando el término clave maestra del cliente (CMK) por AWS KMS key y Clave KMS. El concepto no ha cambiado. Para evitar que se produzcan cambios bruscos, AWS KMS está manteniendo algunas variaciones de este término.

Una AWS KMS key es una representación lógica de una clave criptográfica. Una clave KMS contiene metadatos, como el ID de clave, especificación de clave, uso de claves, fecha de creación, descripción y estado de claves. Lo más importante es que contiene una referencia al material de claves que se utiliza cuando ejecuta operaciones criptográficas con la clave de KMS.

Puede crear una clave de KMS con material de clave criptográfico generado en módulos de seguridad de hardware validados por FIPS de AWS KMS. El material de clave para las claves de KMS simétricas y para las claves privadas de KMS asimétricas nunca sale de AWS KMS sin cifrar. Para usar o administrar las claves KMS, debe usar AWS KMS. Para obtener información acerca de cómo crear y administrar claves KMS, consulte Administración de claves. Para obtener más información sobre el uso de las claves KMS, consulte la referencia de la API de la AWS Key Management Service.

De forma predeterminada, AWS KMS crea el material de claves para una clave KMS. No puede extraer, exportar, ver ni administrar este material de claves. La única excepción es la clave pública de un par de claves asimétricas, que puede exportar para utilizarla fuera de AWS. Además, no puede eliminar este material de claves; debe eliminar la clave KMS. Sin embargo, puede importar su propio material de clave a una clave de KMS o utilizar un almacén de claves personalizado para crear

claves de KMS que usen material de clave en su clúster de AWS CloudHSM o en un administrador de claves externo que administre fuera de AWS y del cual sea propietario.

AWS KMS también permite usar claves de varias regiones, que le permiten cifrar datos en una Región de AWS y descifrarlo en otra Región de AWS.

Para obtener información acerca de cómo crear y administrar claves KMS, consulte Administración de claves. Para obtener más información sobre el uso de las claves KMS, consulte la referencia de la API de la AWS Key Management Service.

Claves de cliente y claves de AWS

Las claves KMS que usted crea son claves administradas por el cliente. Los Servicios de AWS que utilizan claves KMS para cifrar los recursos de servicio a menudo crean claves para usted. Las claves KMS que los Servicios de AWS crean en su cuenta de AWS son Claves administradas por AWS. Las claves KMS que los Servicios de AWS crean en una cuenta de servicio son Claves propiedad de AWS.

Tipo de clave KMS	Puede ver los metadatos clave KMS	Puede administrar la clave KMS	Usada solo para mi Cuenta de AWS	Rotación automática	Precios
Clave administrada por clientes	Sí	Sí	Sí	Opcional. Cada año (aproxima damente 365 días)	Cuota mensual (prorrateada por hora) Tarifa por uso
Clave administrada de AWS	Sí	No	Sí	Obligatorio. Cada año (aproxima damente 365 días)	Sin cuota mensual Tarifa por uso (algunos Servicios de AWS pagan esta tarifa por usted)

Tipo de clave KMS	Puede ver los metadatos clave KMS	Puede administrar la clave KMS	Usada solo para mi Cuenta de AWS	Rotación automática	Precios
Clave propiedad de AWS	No	No	No	Varía	Sin cuotas

Los servicios de AWS que se integran con AWS KMS difieren en el respaldo de las claves KMS. Algunos servicios de AWS cifran los datos de forma predeterminada con una Clave propiedad de AWS o una Clave administrada de AWS. Algunos servicios de AWS admiten claves administradas por el cliente. Otros servicios de AWS admiten todos los tipos de claves KMS para permitirle la sencillez de una Clave propiedad de AWS, la visibilidad de una Clave administrada de AWS o el control de una clave administrada por el cliente. Para obtener información detallada sobre las opciones de cifrado que ofrece un servicio de AWS, consulte el tema Cifrado en reposo en la guía del usuario o en la guía para desarrolladores del servicio.

Claves administradas por el cliente

Las claves KMS que usted crea son claves administradas por el cliente. Las claves administradas por el cliente son claves KMS de su Cuenta de AWS, que usted ha creado, posee y administra. Puede controlar por completo estas claves KMS, incluido el establecimiento y el mantenimiento de sus políticas de claves, políticas de IAM y concesiones, su habilitación y deshabilitación, la rotación de su material criptográfico, la adición de etiquetas, la creación de alias que hacen referencia a la clave KMS y la programación de las claves KMS para su eliminación.

Las claves administradas por el cliente aparecen en la página Customer managed keys (Claves administradas por el cliente) de la AWS Management Console de AWS KMS. Para identificar definitivamente una clave administrada por el cliente, utilice la operación DescribeKey. En el caso de las claves administradas por el cliente, el valor del campo `KeyManager` de la respuesta `DescribeKey` es `CUSTOMER`.

Puede usar su clave administrada por el cliente en operaciones criptográficas y auditar su uso en los registros de AWS CloudTrail. Además, muchos servicios de AWS integrados con AWS KMS le permiten especificar una clave administrada por el cliente para proteger los datos que almacenan y administran para usted.

Las claves administradas por el cliente tienen una tarifa mensual y una tarifa por uso excesivo del nivel gratuito. Se cuentan contra las cuotas de AWS KMS para su cuenta. Consulte los Precios de AWS Key Management Service y Cuotas para obtener más información.

Claves administradas por AWS

Las Claves administradas por AWS son claves de KMS de su cuenta que se crean, administran y utilizan en su nombre por un servicio de AWS integrado con AWS KMS.

Algunos de los servicios de AWS le permiten elegir una Clave administrada de AWS o una clave administrada por el cliente para proteger sus recursos en ese servicio. En general, a menos que se le pida que controle la clave de cifrado que protege sus recursos, una Clave administrada de AWS es una buena opción. No tiene que crear ni mantener la clave o su política de claves, y nunca hay una tarifa mensual por una Clave administrada de AWS.

Puede ver las Claves administradas por AWS en su cuenta, ver sus políticas de claves y auditar su uso en los registros de AWS CloudTrail. Sin embargo, no puede cambiar ninguna propiedad de Claves administradas por AWS, rotarlas, cambiar sus políticas de claves o programar su eliminación. No puede usar las Claves administradas por AWS en operaciones criptográficas directamente. El servicio que las crea las usa en su nombre.

Claves administradas por AWS aparece en la página Claves administradas por AWS de la AWS Management Console para AWS KMS. También puede identificar Claves administradas por AWS a través de sus alias, que tienen el formato `aws/`*`service-name`*; por ejemplo, `aws/redshift`. Para identificar definitivamente unClaves administradas por AWS, utilice la DescribeKeyoperación. En el caso de Claves administradas por AWS, el valor del campo `KeyManager` de la respuesta `DescribeKey` es `AWS`.

Todas las Claves administradas por AWS rotan cada año de forma automática. No puede cambiar esta programación de rotación.

> **Note**
>
> En mayo de 2022, AWS KMS ha cambiado la programación de rotación para Claves administradas por AWS de cada tres años (aproximadamente 1095 días) hasta cada año (aproximadamente 365 días).
> Las nuevas Claves administradas por AWS rotan automáticamente un año después de su creación y, aproximadamente, cada año a partir de entonces.

> Las Claves administradas por AWS existentes rotan automáticamente un año después de su rotación más reciente y cada año a partir de entonces.

No hay cuota mensual por Claves administradas por AWS. Pueden estar sujetas a tarifas por uso excesivo de la capa gratuita, pero algunos servicios de AWS cubren estos costos por usted. Para obtener más detalles, consulte el tema Cifrado en reposo en la Guía del usuario o en la Guía para desarrolladores del servicio. Consulte los Precios de AWS Key Management Service para obtener más información.

Las Claves administradas por AWS no se contabilizan en las cuotas de recursos correspondientes al número de claves KMS en cada región de su cuenta. Sin embargo, cuando se utilizan en nombre de una entidad principal en su cuenta, estas claves KMS se contabilizan en las cuotas de solicitud. Para obtener más detalles, consulte Cuotas.

Claves propiedad de AWS

Las Claves propiedad de AWS son una colección de clave KMS que un servicio de AWS posee y administra para su uso en varias cuentas de Cuentas de AWS. Aunque las Claves propiedad de AWS no están en su Cuenta de AWS, un servicio de AWS puede usar una Clave propiedad de AWS para proteger los recursos de su cuenta.

Algunos servicios de AWS le permiten elegir una Clave propiedad de AWS o una clave administrada por el cliente. En general, a menos que se le pida que audite o controle la clave de cifrado que protege sus recursos, una Clave propiedad de AWS es una buena opción. Las Claves propiedad de AWS son completamente gratuitas (sin cuotas mensuales ni tarifas de uso), no se tienen en cuenta para las cuotas de AWS KMS para su cuenta y son fáciles de usar. No es necesario crear ni mantener la clave ni su política de claves.

La rotación de Claves propiedad de AWS varía según los servicios. Para obtener información acerca de la rotación de un Clave propiedad de AWS en particular, consulte el tema Cifrado en reposo en la guía del usuario o la guía para desarrolladores del servicio.

Claves KMS de cifrado simétricas

Cuando crea una AWS KMS key, de forma predeterminada, obtiene una clave KMS de cifrado simétrica. Este es el tipo básico y más utilizado de clave KMS.

En AWS KMS, una clave KMS de cifrado simétrico representa una clave de cifrado AES-GCM de 256 bits, excepto en las regiones de China, donde representa una clave de cifrado SM4 de 128 bits.

El material de claves simétrica nunca deja AWS KMS sin cifrar. Para utilizar una clave KMS de cifrado simétrica, tiene que llamar a AWS KMS. Las claves de cifrado simétricas se utilizan en el cifrado simétrico, donde se utiliza la misma clave para cifrar y descifrar. A menos que la tarea requiera de forma explícita un cifrado asimétrico, las claves KMS de cifrado simétricas, que nunca dejan AWS KMS sin cifrar, son una buena opción.

Los servicios de AWS que se integran con AWS KMS utilizan solo claves KMS de cifrado simétricas para cifrar sus datos. Estos servicios no admiten cifrado con claves de KMS asimétricas. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Técnicamente, la especificación de clave de una clave simétrica es SYMMETRIC_DEFAULT, el uso de clave es ENCRYPT_DECRYPT y el algoritmo de cifrado es SYMMETRIC_DEFAULT. Para obtener más detalles, consulte Especificación de clave SYMMETRIC_DEFAULT.

Puede utilizar una clave KMS de cifrado simétrica en AWS KMS para cifrar, descifrar y volver a cifrar datos, generar claves de datos y pares de claves de datos. Puede crear claves KMS de cifrado simétricas de varias regiones, importar su propio material de claves en una clave KMS de cifrado simétrica y crear claves KMS de cifrado simétricas en almacenes de claves personalizadas. Para obtener una tabla en la que se comparan las operaciones que puede realizar con claves KMS de diferentes tipos, consulte Referencia de tipos de claves.

Claves de KMS asimétricas

Puede crear claves KMS asimétricas en AWS KMS. Una clave KMS asimétrica representa un par de claves privadas y públicas relacionadas matemáticamente. La clave privada nunca deja AWS KMS sin cifrar. Para utilizar la clave privada, tiene que llamar a AWS KMS. Puede utilizar la clave pública en AWS KMS llamando a las operaciones de la API de AWS KMS o al descargar la clave pública y utilizarla fuera de AWS KMS. También puede crear claves KMS asimétricas de varias regiones.

Puede crear claves KMS asimétricas que representen pares de claves RSA o pares de claves SM2 (solo en regiones de China) para el cifrado de claves públicas o para la firma y verificación, o pares de claves de curva elíptica para la firma y verificación.

Para obtener más información acerca de cómo crear y utilizar claves KMS asimétricas, consulte Claves asimétricas en AWS KMS.

Claves KMS HMAC

Una clave KMS HMAC representa una clave simétrica de longitud variable que se utiliza para generar y verificar códigos de autenticación de mensajes basados en hash (HMAC). El material de claves de una clave HMAC nunca deja AWS KMS sin cifrar. Para utilizar una clave HMAC, llame a las operaciones de API de `GenerateMac` o `VerifyMac`.

También puede crear claves KMS HMAS de varias regiones.

Para obtener más información acerca de cómo crear y utilizar claves KMS HMAC, consulte Claves HMAC en AWS KMS.

Claves de datos

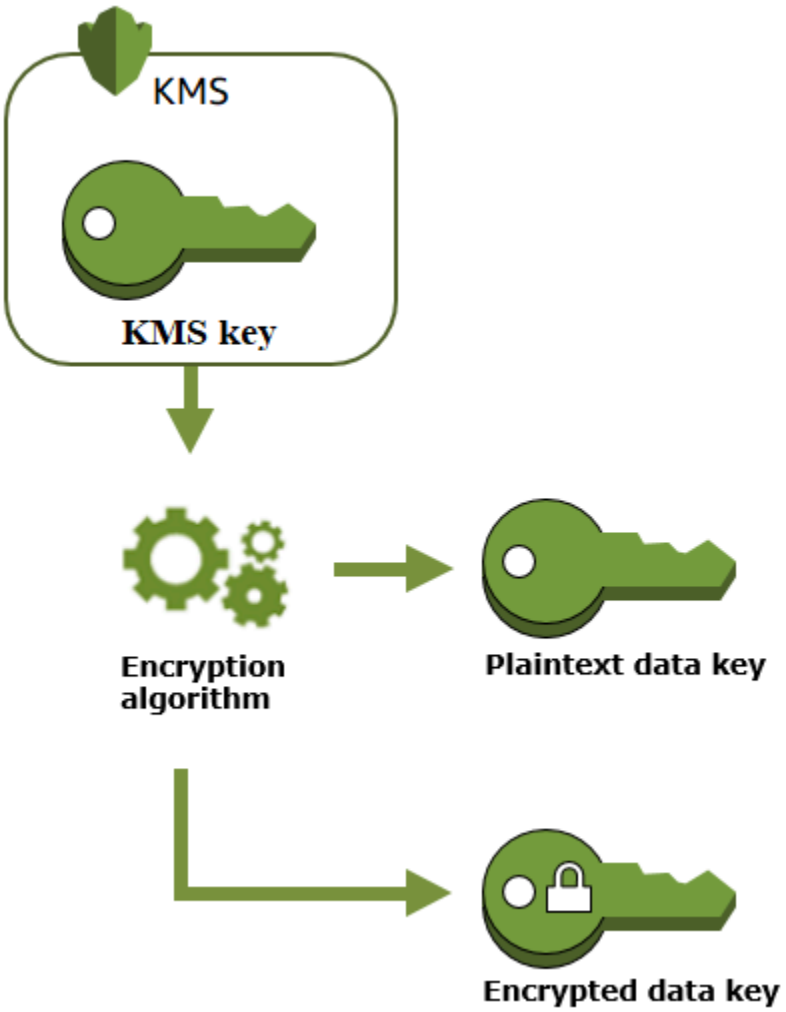
Las claves de datos son las claves simétricas que puede utilizar para cifrar los datos, incluidas grandes cantidades de datos y otras claves de cifrado de datos. A diferencia de las claves KMS simétricas, que no se pueden descargar, las claves de datos se le devuelven para su uso fuera de AWS KMS.

Cuando AWS KMS genera claves de datos, devuelve una clave de datos de texto no cifrado para su uso inmediato (opcional) y una copia cifrada de la clave de datos que puede almacenar de forma segura con los datos. Cuando esté listo para descifrar los datos, primero pídale a AWS KMS que descifre la clave de datos cifrada.

Los AWS KMS generan, cifran y descifran claves de datos. Sin embargo, AWS KMS no almacena, administra o realiza el seguimiento de las claves de datos, ni realiza operaciones criptográficas con claves de datos. Debe utilizar y administrar claves de datos fuera de AWS KMS. Para obtener ayuda para utilizar las claves de datos de forma segura, consulte el AWS Encryption SDK.

Crear una clave de datos

Para crear una clave de datos, llame a la GenerateDataKeyoperación. AWS KMSgenera la clave de datos. Luego, cifra una copia de la clave de datos en una clave KMS de cifrado simétrica que especifique. Esta operación devuelve una copia de texto no cifrado de la clave de datos y una copia de la clave de datos que está cifrada con la clave KMS. En la imagen siguiente, se muestra esta operación.

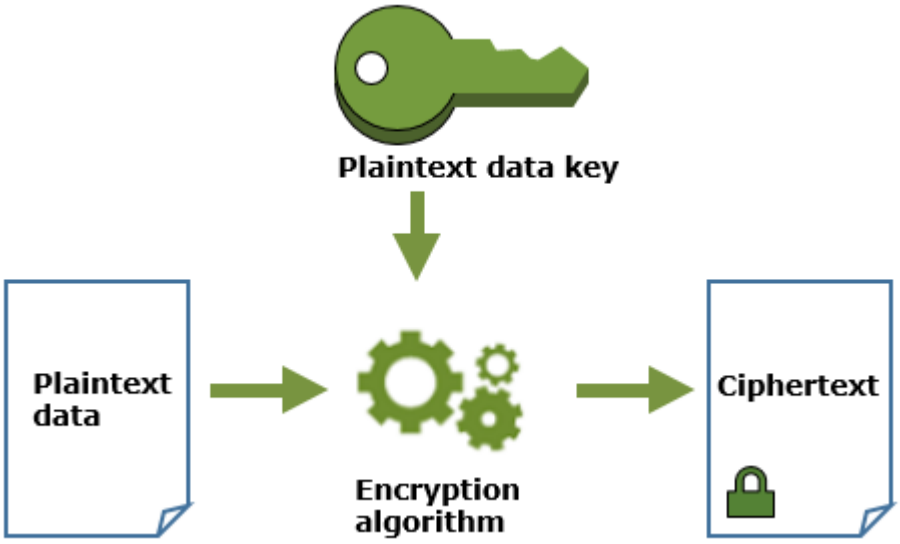


AWS KMStambién admite la GenerateDataKeyWithoutPlaintextoperación, que devuelve solo una clave de datos cifrada. Cuando tenga que utilizar la clave de datos, solicite a AWS KMS que la descifre.

Cifrar los datos con una clave de datos

AWS KMS no puede utilizar una clave de datos para cifrar los datos. Sin embargo, la clave de datos puede utilizarse fuera de AWS KMS; por ejemplo, con OpenSSL o una biblioteca criptográfica, como AWS Encryption SDK.

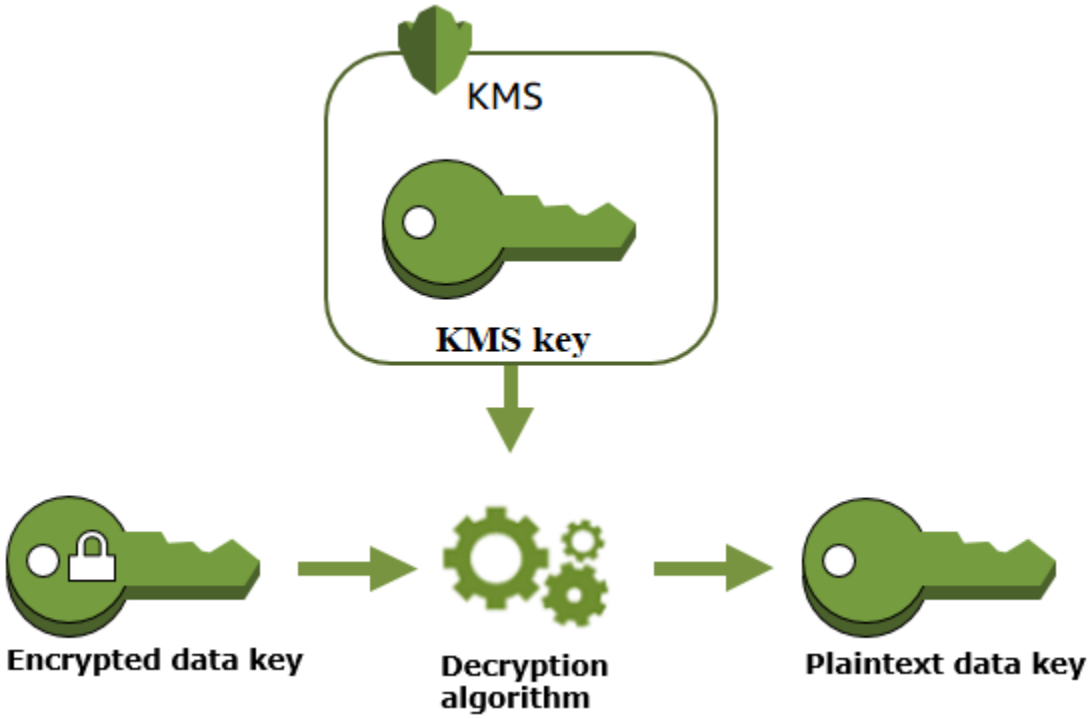
Después de utilizar la clave de datos en texto no cifrado para cifrar los datos, elimínela de la memoria tan pronto como sea posible. Puede almacenar de forma segura la clave de datos cifrada con los datos cifrados para que esté disponible para descifrar los datos.



Descifrar los datos con una clave de datos

Para descifrar los datos, pase la clave de datos cifrada a la operación Decrypt. AWS KMS utiliza la clave KMS para descifrar la clave de datos y, a continuación, devuelve la clave en texto sin cifrar. Utilice la clave de datos de texto no cifrado para descifrar los datos y, a continuación, elimine la clave de datos de texto no cifrado de la memoria tan pronto como sea posible.

En el siguiente diagrama, se muestra cómo se utiliza la operación `Decrypt` para descifrar una clave de datos cifrada.



Cómo afectan las claves de KMS obsoletas a las claves de datos

Cuando una clave de KMS queda obsoleta, el efecto es casi inmediato (sujeto a la posible coherencia). El estado de clave de la clave de KMS cambia para reflejar su nueva condición y todas las solicitudes para utilizar la clave de KMS en operaciones criptográficas fallan.

Sin embargo, el efecto en las claves de datos cifradas por la clave de KMS, y en los datos cifrados por la clave de datos, se retrasa hasta que se vuelva a utilizar la clave de KMS. Por ejemplo, para descifrar la clave de datos.

Las claves de KMS pueden quedar obsoletas por varios motivos. Entre ellos, se incluyen las siguientes acciones que puede realizar.

- Desactivar la clave de KMS
- Programar la clave de KMS para eliminarla
- Eliminar el material de clave de una clave de KMS con material de clave importado o permitir que el material de clave importado caduque.
- Desconectar el almacén de claves de AWS CloudHSM que aloja la clave de KMS o eliminar la clave del clúster de AWS CloudHSM que sirve como material para la clave de KMS.

- Desconectar el almacén de claves externo que aloja la clave de KMS o realizar cualquier otra acción que interfiera con las solicitudes de cifrado y descifrado al proxy del almacén de claves externo, incluida la eliminación de la clave externa de su administrador de claves externo.

Este efecto es particularmente importante para muchos Servicios de AWS que utilizan claves de datos para proteger los recursos que administra el servicio. En el ejemplo siguiente se utiliza Amazon Elastic Block Store (Amazon EBS) y Amazon Elastic Compute Cloud (Amazon EC2). Los diferentes Servicios de AWS utilizan las claves de datos de distintas formas. Para obtener más información, consulte la sección de Protección de datos del capítulo de Seguridad del Servicio de AWS.

Por ejemplo, considere esta situación:

1. Usted crea un volumen de EBS cifrado y especifica una clave de KMS para protegerlo. Amazon EBS solicita a AWS KMS que utilice su clave KMS para generar una clave de datos cifrada para el volumen. Amazon EBS almacena la clave de datos cifrada con los metadatos del volumen.
2. Cuando adjunta el volumen de EBS a una instancia EC2, Amazon EC2 utiliza su clave de KMS para descifrar la clave de datos cifrados del volumen de EBS. Amazon EC2 utiliza la clave de datos del hardware Nitro, que se encarga de cifrar todas las E/S del disco en el volumen de EBS. La clave de datos persiste en el hardware de Nitro mientras el volumen de EBS esté asociado a la instancia de EC2.
3. Usted realiza una acción que deja a la clave de KMS obsoleta. Esto no tiene un efecto inmediato sobre la instancia EC2 ni el volumen de EBS. Amazon EC2 utiliza la clave de datos, no la clave de KMS, para cifrar todas las E/S de disco mientras el volumen esté asociado a la instancia.
4. Sin embargo, cuando el volumen de EBS cifrado se separa de la instancia de EC2, Amazon EBS elimina la clave de datos del hardware de Nitro. La próxima vez que el volumen EBS cifrado se asocia a una instancia EC2, el accesorio devuelve un error, dado que Amazon EBS no puede utilizar la clave KMS para descifrar la clave de datos cifrada del volumen. Para volver a usar el volumen de EBS, debe hacer que la clave de KMS se pueda utilizar de nuevo.

Pares de claves de datos

Los pares de claves de datos son claves de datos asimétricos que constan de una clave privada y una clave pública relacionadas matemáticamente. Están diseñados para ser utilizados para el cifrado y descifrado del cliente o la firma y la verificación fuera de AWS KMS.

A diferencia de los pares de claves de datos que generan herramientas como OpenSSL, AWS KMS protege la clave privada en cada par de claves de datos en una clave KMS de cifrado simétrica

en el AWS KMS que especifique. Sin embargo, AWS KMS no almacena, administra o realiza el seguimiento de los pares de claves de datos, ni realiza operaciones criptográficas con pares de claves de datos. Debe utilizar y administrar pares de claves de datos fuera de AWS KMS.

AWS KMS admite los siguientes tipos de pares de claves de datos:

- Pares de claves RSA: RSA_2048, RSA_3072 y RSA_4096
- Pares de claves de curva elíptica: ECC_NIST_P256, ECC_NIST_P384, ECC_NIST_P521 y ECC_SECG_P256K1
- Pares de claves SM (solo en las regiones de China): SM2

El tipo de par de claves de datos que por lo general depende de su caso de uso o de los requisitos reglamentarios. La mayoría de los certificados precisan claves RSA. Las claves de curva elíptica se utilizan a menudo para firmas digitales. Las claves ECC_SECG_P256K1 se utilizan comúnmente para criptomonedas. AWS KMS recomienda utilizar pares de claves ECC para la firma y el uso de pares de claves RSA para el cifrado o la firma, pero no ambos. Sin embargo, AWS KMS no puede aplicar ninguna restricción al uso de pares de claves de datos fuera de AWS KMS.

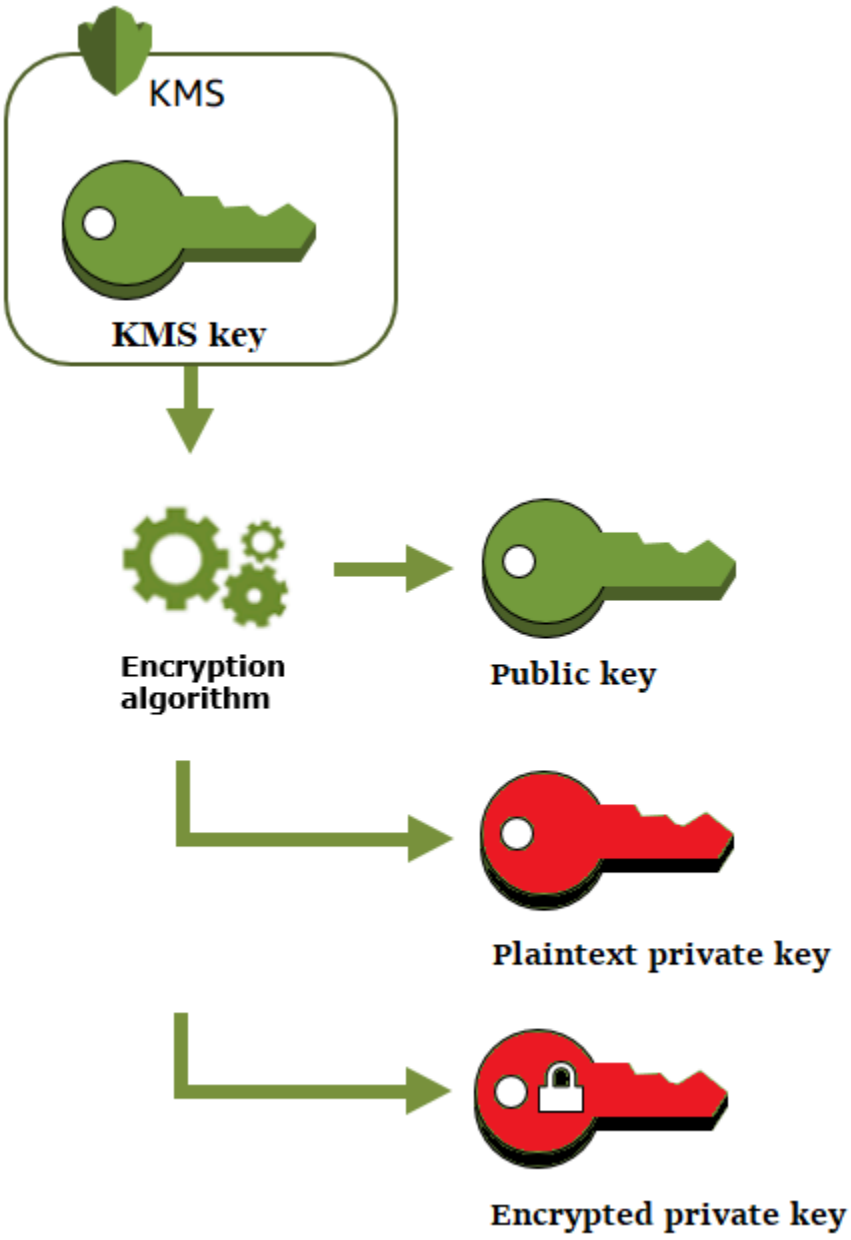
Crear un par de clave de datos

Para crear un par de claves de datos, llame a las GenerateDataKeyPairWithoutPlaintextoperaciones GenerateDataKeyPairo. Especifique la clave KMS de cifrado simétrica que desea utilizar para cifrar la clave privada.

`GenerateDataKeyPair` devuelve una clave pública de texto no cifrado, una clave pública de texto no cifrado y una clave privada cifrada. Utilice esta operación cuando necesite una clave privada de texto no cifrado inmediatamente, por ejemplo, para generar una firma digital.

`GenerateDataKeyPairWithoutPlaintext` devuelve una clave pública de texto no cifrado y una clave privada de texto cifrado, pero no una clave privada de texto no cifrado. Utilice esta operación cuando no necesite una clave privada de texto no cifrado inmediatamente, por ejemplo, cuando esté cifrando con una clave pública. Más tarde, cuando necesite una clave privada de texto no cifrado para descifrar los datos, puede llamar a la operación Decrypt.

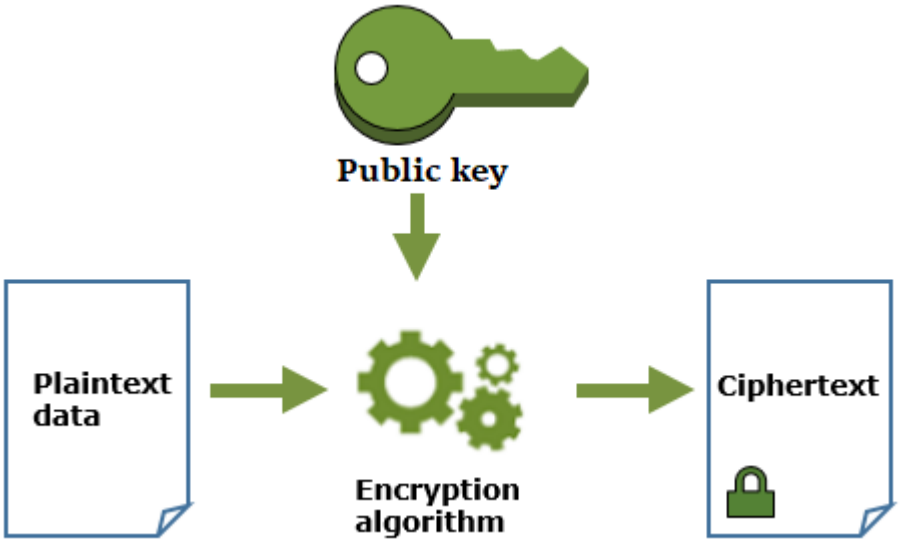
En la imagen siguiente, se muestra la operación `GenerateDataKeyPair`. La operación `GenerateDataKeyPairWithoutPlaintext` omite la clave privada de texto no cifrado.



Cifrar los datos con un par de claves de datos

Cuando cifra con un par de claves de datos, utiliza la clave pública del par para cifrar los datos y la clave privada del mismo par para descifrar los datos. Normalmente, los pares de claves de datos se utilizan cuando muchas partes necesitan cifrar datos que solo la parte que posee la clave privada puede descifrar.

Las partes con la clave pública utilizan esa clave para cifrar datos, como se muestra en el siguiente diagrama.

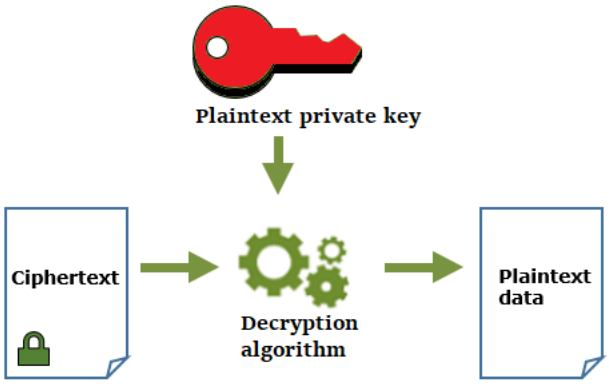


Descifrar los datos con un par de claves de datos

Para descifrar los datos, utilice la clave privada en el par de claves de datos. Para que la operación tenga éxito, las claves públicas y las privadas deben pertenecer al mismo par de claves de datos y debe utilizar el mismo algoritmo de cifrado.

Para descifrar la clave privada cifrada, pásala a la operación Decrypt . Utilice la clave privada de texto no cifrado para descifrar los datos. A continuación, elimina la clave privada de texto no cifrado de la memoria lo antes posible.

El siguiente diagrama muestra cómo utilizar la clave privada en un par de claves de datos para descifrar el texto cifrado.



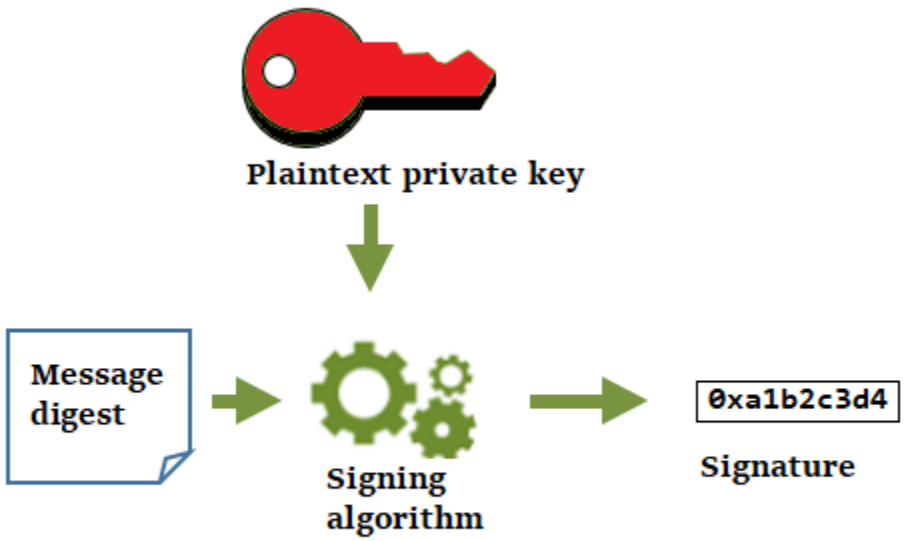
Firmar los mensajes con un par de claves de datos

Para generar una firma criptográfica para un mensaje, utilice la clave privada en el par de claves de datos. Cualquier persona con clave pública puede utilizarla para verificar que el mensaje se firmase con su clave privada y que no haya cambiado desde entonces.

Si su clave privada está cifrada, pase la clave privada cifrada a la operación Decrypt. AWS KMS utiliza su clave KMS para descifrar la clave de datos y después devuelve la clave privada de texto no cifrado. Utilice la clave privada de texto no cifrado para generar la firma. A continuación, elimina la clave privada de texto no cifrado de la memoria lo antes posible.

Para firmar un mensaje, cree un resumen de mensaje con una función hash criptográfica, como el comando `dgst` en OpenSSL. Después, pase su clave privada no cifrada al algoritmo de firma. El resultado es una firma que representa los contenidos del mensaje. (Es posible que pueda firmar mensajes más cortos sin crear primero un resumen. El tamaño máximo del mensaje varía según la herramienta de firma que utilice).

El siguiente diagrama muestra cómo utilizar la clave privada en un par de claves de datos para firmar un mensaje.



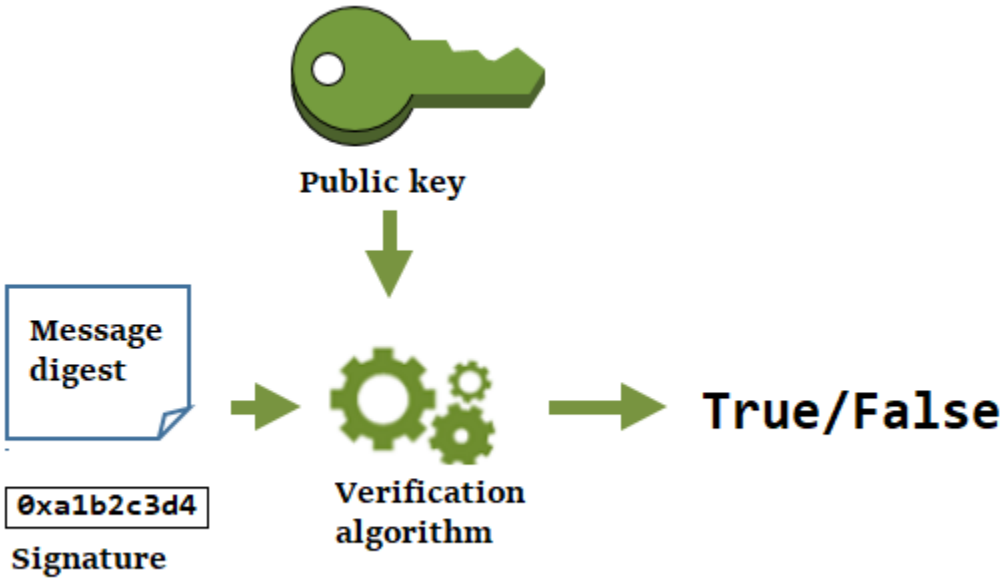
Verificar una firma con un par de claves de datos

Cualquier persona que tenga la clave pública en su par de claves de datos puede utilizarla para verificar la firma que generó con su clave privada. La verificación confirma que un usuario autorizado

firmó el mensaje con el algoritmo de firma y la clave privada especificada y el mensaje no ha cambiado desde entonces.

Para tener éxito, la parte que verifique la firma debe generar el mismo tipo de resumen, utilizar el mismo algoritmo y utilizar la clave pública que se corresponde con la clave privada utilizada para firmar el mensaje.

El siguiente diagrama muestra cómo utilizar la clave pública en un par de claves de datos para verificar la firma de un mensaje.



Alias

Utilice un alias como un nombre fácil de usar para una clave KMS. Por ejemplo, puede referirse a una clave KMS como clave de prueba en lugar de 1234abcd-12ab-34cd-56ef-1234567890ab.

Los alias facilitan la identificación de una clave KMS en el AWS Management Console. Puede utilizar un alias para identificar una clave KMS en algunas operaciones AWS KMS, incluyendo operaciones criptográficas. En las aplicaciones, puede usar un solo alias para hacer referencia a diferentes claves KMS en cada Región de AWS.

También puede permitir y denegar el acceso a claves KMS en función de sus alias sin editar políticas ni administrar concesiones. Esta característica forma parte de la compatibilidad de AWS KMS con el control de acceso basado en atributos (ABAC). Para obtener más detalles, consulte ABAC para AWS KMS.

En AWS KMS, los alias son recursos independientes, no propiedades de una clave KMS. Como tal, puede agregar, cambiar y eliminar un alias sin afectar a la clave KMS asociada.

> **Important**
>
> No incluya información confidencial en un nombre de alias. Los alias pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

Más información:

- Para obtener información más detallada acerca de los alias, consulte Uso de alias.
- Para obtener información sobre los formatos de los identificadores clave, incluidos los alias, consulte Identificadores clave () KeyId.
- Para obtener ayuda para encontrar los alias asociados a una clave KMS, consulte Buscar el nombre del alias y el ARN de alias
- Para obtener ejemplos de cómo crear y administrar alias en varios lenguajes de programación, consulte Trabajar con alias.

Almacenes de claves personalizados

Un almacén de claves personalizado es un recurso de AWS KMS respaldado por un administrador de claves ajeno al AWS KMS que usted posee y administra. Al utilizar una clave de KMS en un almacén de claves personalizado para una operación criptográfica, la operación en realidad se realiza en su administrador de claves con sus claves criptográficas.

AWS KMS admite los almacenes de claves de AWS CloudHSM respaldados por un clúster de AWS CloudHSM y los almacenes de claves externos que están respaldados por un administrador de claves externo ajeno a AWS.

Para obtener más información, consulte Almacenes de claves personalizados.

Operaciones criptográficas

En AWS KMS, las operaciones criptográficas son operaciones de la API que utilizan las claves KMS para proteger los datos. Debido a que las claves KMS permanecen dentro de AWS KMS, debe llamar a AWS KMS para usar una clave KMS en una operación criptográfica.

Para realizar operaciones criptográficas con las claves KMS, utilice los SDK de AWS, la AWS Command Line Interface (AWS CLI) o el AWS Tools for PowerShell. No puede realizar operaciones criptográficas en la consola de AWS KMS. Para ver ejemplos de cómo llamar a las operaciones criptográficas en varios lenguajes de programación, consulte Programación de la API de AWS KMS.

En la siguiente tabla se muestran las operaciones criptográficas de AWS KMS. También se muestra el tipo de clave y los requisitos de uso de clave para las claves KMS utilizadas en la operación.

Operación	Tipo de clave	Uso de claves
Decrypt	Simétrico o asimétrico	`ENCRYPT_DECRYPT`
Encrypt	Simétrico o asimétrico	`ENCRYPT_DECRYPT`
GenerateDataKey	Simétrica	`ENCRYPT_DECRYPT`
GenerateDataKeyPair	Simétrica [1] No es compatible con claves KMS en almacenes de claves personalizados.	`ENCRYPT_DECRYPT`
GenerateDataKeyPairWithoutPlaintext	Simétrica [1] No es compatible con claves KMS en almacenes de claves personalizados.	`ENCRYPT_DECRYPT`
GenerateDataKeyWithoutPlaintext	Simétrica	`ENCRYPT_DECRYPT`
GenerateMac	HMAC	`GENERATE_VERIFY_MAC`
GenerateRandom	N/A. Esta operación no utiliza una clave KMS.	N/A
ReEncrypt	Simétrico o asimétrico	`ENCRYPT_DECRYPT`

Operación	Tipo de clave	Uso de claves
Sign	Asimétrica	`SIGN_VERIFY`
Verificar	Asimétrica	`SIGN_VERIFY`
VerifyMac	HMAC	`GENERATE_VERIFY_MAC`

[1] Genera un par de claves de datos asimétricas protegido por una clave de KMS de cifrado simétrico.

Para obtener información acerca de los permisos para operaciones criptográficas, consulte the section called “Referencia de permisos”.

Para que AWS KMS tenga capacidad de respuesta y sea altamente funcional para todos los usuarios, AWS KMS establece cuotas en el número de operaciones criptográficas que se pueden llamar en cada segundo. Para obtener más detalles, consulte the section called “Cuotas compartidas para operaciones criptográficas”.

Identificadores clave () KeyId

Los identificadores de clave actúan como nombres para las claves KMS. Le ayudan a reconocer sus claves KMS en la consola. Se utilizan para indicar qué claves KMS desea utilizar en operaciones de la API de AWS KMS, políticas de claves, políticas de IAM y concesiones. Los valores del identificador de clave no están relacionados en absoluto con el material de clave asociado a la clave KMS.

AWS KMS define varios identificadores de clave. Al crear una clave KMS, AWS KMS genera un ARN de clave y un ID de clave, que son propiedades de la clave KMS. Al crear un alias, AWS KMS genera un ARN de alias basado en el nombre de alias que defina. Puede ver los identificadores de clave y alias en la AWS Management Console y en la API de AWS KMS.

En la consola de AWS KMS, puede ver y filtrar las claves KMS por su ARN de clave, ID de clave o nombre de alias, y ordenarlas por ID de clave y nombre de alias. Para obtener ayuda para encontrar los identificadores clave en la consola, consulte the section called “Búsqueda del ID y el ARN de la clave”.

En la API de AWS KMS, los parámetros que se utilizan para identificar una clave KMS se denominan `KeyId` o una variación, como `TargetKeyId` o `DestinationKeyId`. Sin embargo, los valores de

esos parámetros no se limitan a los ID de clave. Algunos pueden tomar cualquier identificador de clave válido. Para obtener información sobre los valores de cada parámetro, consulte la descripción del parámetro en la Referencia de la API de AWS Key Management Service.

> **Note**
>
> Cuando utilice la API de AWS KMS, preste especial atención al identificador de clave que utilice. Las diferentes API requieren identificadores de clave distintos. En general, utilice el identificador de clave más completo que sea práctico para su tarea.

AWS KMS admite los siguientes identificadores de clave.

ARN de clave

El ARN de clave es el nombre de recurso de Amazon (ARN) de una clave KMS. Es un identificador único y completo para la clave KMS. Un ARN de clave incluye la Cuenta de AWS, la región y el ID de clave. Para obtener ayuda para encontrar el ARN de clave de una clave KMS, consulte the section called “Búsqueda del ID y el ARN de la clave”.

El formato de un ARN de clave es el siguiente:

```
arn:<partition>:kms:<region>:<account-id>:key/<key-id>
```

A continuación, se muestra un ARN de clave para una clave KMS de región única.

```
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

El elemento *key-id* de los ARN de claves de las claves de varias regiones comienza con el prefijo `mrk-`. A continuación, se muestra un ARN de clave de ejemplo para una clave de múltiples regiones.

```
arn:aws:kms:us-west-2:111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab
```

ID de clave

El ID de clave identifica de forma inequívoca una clave KMS dentro de una cuenta y región. Para obtener ayuda para encontrar el ID de clave de una clave KMS, consulte the section called “Búsqueda del ID y el ARN de la clave”.

A continuación, se muestra un ID de clave de ejemplo para una clave KMS de región única.

```
1234abcd-12ab-34cd-56ef-1234567890ab
```

Los ID de clave de claves de múltiples regiones comienzan con el prefijo `mrk-`. A continuación, se muestra un ID de clave de ejemplo para una clave de múltiples regiones.

```
mrk-1234abcd12ab34cd56ef1234567890ab
```

ARN de alias

El ARN de alias es el nombre de recurso de Amazon (ARN) de un alias de AWS KMS. Es un identificador único y completamente calificado para el alias, y para la clave KMS que representa. Un ARN de alias incluye la Cuenta de AWS, la región y el nombre del alias.

En cualquier momento dado, un ARN de alias identifica una clave KMS en particular. Sin embargo, dado que puede cambiar la clave KMS asociada con el alias, el ARN de alias puede identificar diferentes claves KMS en diferentes momentos. Para obtener ayuda para encontrar el ARN de alias de una clave KMS, consulte Buscar el nombre del alias y el ARN de alias.

El formato de un ARN de alias es el siguiente:

```
arn:<partition>:kms:<region>:<account-id>:alias/<alias-name>
```

A continuación, se muestra el ARN de alias de un `ExampleAlias` ficticio.

```
arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias
```

Nombre del alias

El nombre de alias es una cadena de hasta 256 caracteres. Identifica de forma inequívoca una clave KMS asociada dentro de una cuenta y región. En la API de AWS KMS, los nombres de alias siempre comienzan por `alias/`. Para obtener ayuda para encontrar el nombre de alias de una clave KMS, consulte Buscar el nombre del alias y el ARN de alias.

El formato de un nombre de alias es el siguiente:

```
alias/<alias-name>
```

Por ejemplo:

```
alias/ExampleAlias
```

El prefijo `aws/` de un nombre de alias está reservado para Claves administradas por AWS. No se puede crear un alias con este prefijo. Por ejemplo, el nombre de alias de la Clave administrada de AWS para Amazon Simple Storage Service (Amazon S3) es el siguiente.

```
alias/aws/s3
```

Material de claves

El material de clave es la cadena de bits utilizada en un algoritmo criptográfico. El material de clave secreta debe mantenerse en secreto para proteger las operaciones criptográficas que lo utilizan. El material de clave pública está diseñado para compartirse.

Cada clave KMS incluye una referencia al material de clave en los metadatos. El origen del material de claves de cifrado simétrico, las claves KMS pueden variar. Puede utilizar el material clave que genera AWS KMS, material clave que se genera en el clúster AWS CloudHSM de un almacén de claves personalizado, o bien importar su propio material de claves. Si usa material de claves de AWS KMS para su clave KMS de cifrado simétrica, puede habilitar la rotación automática de su material de claves.

De forma predeterminada, cada clave KMS tiene un material de claves único. Sin embargo, puede crear un conjunto de claves de varias regiones con el mismo material de claves.

Origen del material de claves

El origen del material de claves es una propiedad de la clave KMS que identifica el origen del material de claves en la clave KMS. Usted elija el origen del material de claves cuando crea la clave KMS y no se puede cambiar. La fuente del material de clave afecta a las características de seguridad, durabilidad, disponibilidad, latencia y rendimiento de la clave de KMS.

Para encontrar el origen material de una clave de KMS, utilice la DescribeKeyoperación o consulte el valor de origen en la pestaña de configuración criptográfica de la página de detalles de una clave de KMS en la AWS KMS consola. Para obtener ayuda, consulte Visualización de claves.

Las claves KMS pueden tener uno de los siguientes valores de origen de material de claves.

`AWS_KMS`

AWS KMS crea y administra el material de claves de la clave KMS en su propio almacén de claves. Este es el valor predeterminado y el valor recomendado para la mayoría de las claves KMS.

Para obtener ayuda para crear claves con material de claves de AWS KMS, consulte Crear claves.

`EXTERNAL (Import key material)`

La clave KMS tiene material de claves importado. Cuando se crea una clave KMS con un origen de material de claves `External`, la clave KMS no tiene material de claves. Más adelante, puede importar material de claves en la clave KMS. Cuando utilice material de claves importado, debe proteger y administrar ese material de claves fuera de AWS KMS, incluido reemplazar el material de claves si caduca. Para obtener más detalles, consulte Acerca de material de claves importado.

Para obtener ayuda con la creación de una clave KMS para material de claves importado, consulte Paso 1: Crear una clave KMS sin material de claves.

`AWS_CLOUDHSM`

AWS KMS crea el material de clave en el clúster de AWS CloudHSM para su almacén de claves de AWS CloudHSM.

Para obtener ayuda con la creación de una clave de KMS en un almacén de claves de AWS CloudHSM, consulte Crear claves de KMS en un almacén de claves de AWS CloudHSM.

`EXTERNAL_KEY_STORE`

El material de clave es una clave criptográfica en un administrador de claves externo ajeno a AWS. Este origen solo es compatible con las claves de KMS en un almacén de claves externo.

Para obtener ayuda con la creación de una clave de KMS en un almacén de claves externo, consulte Crear claves de KMS en un almacén de claves externo.

Especificación de clave

La especificación de clave es una propiedad que representa la configuración criptográfica de la clave. El significado de la especificación de clave difiere con el tipo de clave.

- Claves de AWS KMS: la especificación de claves determina si la clave KMS es simétrica o asimétrica. También determina el tipo de su material de clave y los algoritmos que admite.

Se selecciona la especificación de clave al crear la clave KMS y no se puede cambiar. La especificación de clave predeterminada, SYMMETRIC_DEFAULT, representa una clave de cifrado simétrico de 256 bits.

> **Note**
>
> La `KeySpec` para una clave KMS se conocía como `CustomerMasterKeySpec`. El `CustomerMasterKeySpec` parámetro de la CreateKeyoperación está obsoleto. En su lugar, utilice el parámetro `KeySpec`, que funciona de la misma manera. Para evitar cambios importantes, la respuesta de las DescribeKeyoperaciones `CreateKey` y ahora incluye `CustomerMasterKeySpec` los miembros `KeySpec` y con los mismos valores.

Para obtener una lista de especificaciones de clave y ayuda para elegir una especificación de clave, consulte Seleccionar la especificación de clave. Para encontrar la especificación clave de una clave de KMS, utilice la DescribeKeyoperación o consulte la pestaña de configuración criptográfica de la página de detalles de una clave de KMS en la AWS KMS consola. Para obtener ayuda, consulte Visualización de claves.

Para limitar las especificaciones clave que los directores pueden utilizar al crear claves de KMS, utilice la clave de condición kms: KeySpec. También puede utilizar la clave de condición `kms:KeySpec` para permitir que las entidades principales llamen a las operaciones de AWS KMS para una clave KMS con una especificación de clave determinada. Por ejemplo, puede denegar permiso para programar la eliminación de cualquier clave KMS con una especificación de clave `RSA_4096`.

- Claves de datos (GenerateDataKey): la especificación clave determina la longitud de una clave de datos AES.
- Pares de claves de datos (GenerateDataKeyPair): la especificación del par de claves determina el tipo de material clave del par de claves de datos.

Uso de claves

El uso de la clave es una propiedad que determina las operaciones criptográficas que esta admite. Las claves de KMS pueden tener los siguientes usos de clave: `ENCRYPT_DECRYPT`, `SIGN_VERIFY` o `GENERATE_VERIFY_MAC`. Cada clave de KMS solo puede tener un uso. El uso de una clave KMS

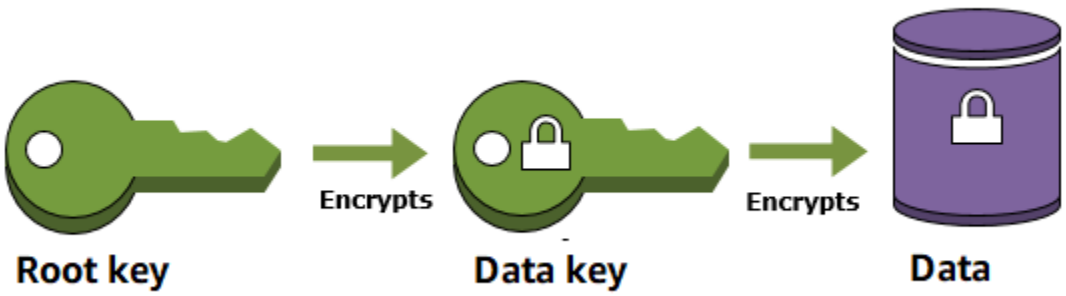
para más de un tipo de operaciones hace que el producto de ambas operaciones sea más vulnerable a ataques.

Para obtener ayuda para elegir el uso de clave para su clave KMS, consulte Seleccionar el uso de la clave. Para averiguar el uso de claves de una clave de KMS, utilice la DescribeKeyoperación o seleccione la pestaña de configuración criptográfica de la página de detalles de una clave de KMS en la AWS KMS consola. Para obtener ayuda, consulte Visualización de claves.

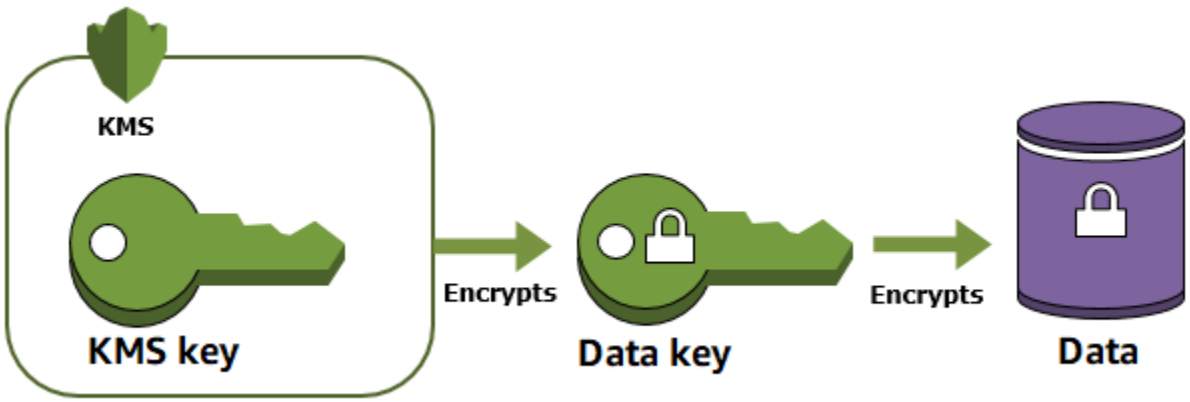
Cifrado de sobre

Al cifrar sus datos, los datos están protegidos, pero tiene que proteger su clave de cifrado. Una estrategia consiste en cifrarla. El cifrado de sobres es la práctica de cifrar los datos en texto no cifrado con una clave de datos y, a continuación, cifrar la clave de datos con otra clave.

Incluso puede cifrar la clave de cifrado de datos con otra clave de cifrado y cifrar dicha clave de cifrado con otra clave de cifrado. Sin embargo, finalmente, una clave debe permanecer en texto no cifrado para que pueda descifrar las claves y los datos. Esta clave de cifrado de clave de texto no cifrado de nivel superior se conoce como clave raíz.



AWS KMS le ayuda a proteger sus claves cifradas almacenándolas y administrándolas de forma segura. Las claves raíz almacenadas en AWS KMS, conocidas como AWS KMS keys, nunca salen de los módulos de seguridad de hardware validados por FIPS de AWS KMS sin cifrar. Para utilizar una clave KMS, tiene que llamar a AWS KMS.



El cifrado de sobre ofrece varios beneficios:

- Protección de las claves de datos

  Al cifrar una clave de datos, no tiene que preocuparse del almacenamiento la clave de datos cifrada, porque la clave de datos está intrínsecamente protegida por el cifrado. Puede almacenar de forma segura la clave de datos cifrada junto con los datos cifrados.
- Cifrado de los mismos datos con varias claves múltiples

  Las operaciones de cifrado pueden tardar mucho tiempo, en concreto cuando los datos que se cifran son objetos grandes. En vez de volver a cifrar los datos sin procesar varias veces con claves distintas, puede volver a cifrar solo las claves de datos que protegen los datos sin procesar.
- Combinación de los puntos fuertes de varios algoritmos

  En general, los algoritmos de clave simétrica son más rápidos y producen textos cifrados más pequeños que los algoritmos de clave pública. Sin embargo, los algoritmos de clave pública proporcionan una separación inherente entre las funciones y facilitan la administración de las claves. El cifrado de sobre le permite combinar los puntos fuertes de cada estrategia.

Contexto de cifrado

Todas las operaciones criptográficas de AWS KMS con claves de KMS de cifrado simétricas aceptan un contexto de cifrado, un conjunto opcional de pares clave-valor no secretos que pueden contener información contextual adicional sobre los datos. AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales (AAD) para permitir el cifrado autenticado.

Cuando incluye un contexto de cifrado en una solicitud de cifrado, este se vincula criptográficamente al texto cifrado de forma que sea necesario utilizar el mismo contexto de cifrado para descifrar (o descifrar y volver a cifrar) los datos. Si el contexto de cifrado proporcionado en la solicitud de descifrado no es una coincidencia exacta, incluido el uso de mayúsculas y minúsculas, la solicitud de descifrado producirá un error. Solo puede variar el orden de los pares clave-valor en el contexto de cifrado.

> **Note**
>
> No puede especificar un contexto de cifrado en una operación criptográfica con una clave KMS asimétrica o una clave KMS HMAC. Los algoritmos asimétricos y los algoritmos MAC no son compatibles con un contexto de cifrado.

El contexto de cifrado no es secreto y no está cifrado. Aparece en texto no cifrado en los registros de AWS CloudTrail para que pueda utilizarlo para identificar y clasificar las operaciones criptográficas. El contexto de cifrado no debe incluir información confidencial. Le recomendamos que el contexto de cifrado describa los datos que se van a cifrar o descifrar. Por ejemplo, cuando cifre un archivo, puede usar parte de la ruta del archivo como contexto de cifrado.

```
"encryptionContext": {
    "department": "10103.0"
}
```

Por ejemplo, al cifrar volúmenes e instantáneas creados con la operación Amazon Elastic Block Store (Amazon EBS) CreateSnapshot, Amazon EBS utiliza el ID del volumen como valor de contexto de cifrado.

```
"encryptionContext": {
  "aws:ebs:id": "vol-abcde12345abc1234"
}
```

También se puede utilizar el contexto de cifrado para ajustar o limitar el acceso a AWS KMS keys de su cuenta. Puede utilizar el contexto de cifrado como una restricción en concesiones y como una condición en declaraciones de política.

Para obtener información sobre cómo utilizar el contexto de cifrado para proteger la integridad de los datos cifrados, consulte la publicación Cómo proteger la integridad de sus datos cifrados mediante el uso AWS Key Management Service y EncryptionContext en el blog sobre seguridad. AWS

Más información sobre el contexto de cifrado.

Reglas de contexto de cifrado

AWS KMS aplica las siguientes reglas para las claves de contexto y los valores de cifrado.

- La clave y el valor de un par de contexto de cifrado deben ser cadenas literales simples. Si utiliza un tipo diferente, como un número entero o flotante, AWS KMS lo interpretará como una cadena.
- Las claves y los valores de un contexto de cifrado pueden incluir caracteres Unicode. Si un contexto de cifrado incluye caracteres que no están permitidos en las políticas clave o en las políticas de IAM, no podrá especificar el contexto de cifrado en las claves de condición de la política, como `kms:EncryptionContext:context-key` y `kms:EncryptionContextKeys`. Para obtener más información sobre las reglas clave de los documentos de política de claves, consulte Formato de la política de claves. Para obtener más información sobre las reglas de documentos de políticas de IAM, consulte Requisitos de nombres de IAM en la Guía del usuario de IAM.

Contexto de cifrado de las políticas

El contexto de cifrado se utiliza principalmente para verificar la integridad y la autenticidad. Sin embargo, también puede utilizar el contexto de cifrado para controlar el acceso a AWS KMS keys de cifrado simétricas en las políticas de claves y las políticas de IAM.

Las claves EncryptionContextKeyscondicionales kmsEncryptionContext:: y kms: permiten (o deniegan) un permiso solo cuando la solicitud incluye claves de contexto de cifrado o pares clave-valor determinados.

Por ejemplo, la siguiente declaración de política de claves permite al rol `RoleForExampleApp` utilizar la KMS en operaciones `Decrypt`. Utiliza la clave de condición `kms:EncryptionContext:context-key` para conceder este permiso solo cuando el contexto de cifrado de la solicitud incluye un par de contexto de cifrado `AppName:ExampleApp`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
```

```
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
}
```

Para obtener más información sobre estas claves de condición de contexto de cifrado, consulte Claves de estado para AWS KMS.

Contexto de cifrado de las concesiones

Cuando crea una concesión, puede incluir restricciones de concesiones que establecen las condiciones para los permisos de concesión. AWS KMS apoya dos restricciones de concesiones, `EncryptionContextEquals` y `EncryptionContextSubset`, las cuales implican el contexto de cifrado en una solicitud de una operación criptográfica. Al utilizar estas restricciones de concesión, los permisos de la concesión solo son efectivos cuando el contexto de cifrado de la solicitud de la operación criptográfica cumple los requisitos de las restricciones de concesión.

Por ejemplo, puede añadir una restricción de `EncryptionContextEquals` concesión a una concesión que permita la operación. GenerateDataKey Con esta restricción, la concesión solo permite la operación cuando el contexto de cifrado de la solicitud coincide con mayúsculas y minúsculas con el contexto de cifrado de la restricción de concesión.

```
$ aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:user/exampleUser \
    --retiring-principal arn:aws:iam::111122223333:role/adminRole \
    --operations GenerateDataKey \
    --constraints EncryptionContextEquals={Purpose=Test}
```

Una solicitud como la siguiente del principal beneficiario satisfaría la restricción de `EncryptionContextEquals`.

```
$ aws kms generate-data-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --key-spec AES_256 \
    --encryption-context Purpose=Test
```

Para obtener más detalles sobre las restricciones de concesiones y , consulte Uso de restricciones de concesiones. Para obtener información detallada sobre las concesiones, consulte the section called “Concesiones”.

Registrar el contexto de cifrado

AWS KMS usa AWS CloudTrail para registrar el contexto de cifrado de modo que pueda determinar a qué clave KMS y datos se ha tenido acceso. La entrada de registro muestra exactamente qué clave KMS se ha usado para cifrar o descifrar los datos específicos a los que hace referencia el contexto de cifrado en la entrada de registro.

> **Important**
>
> Como el contexto de cifrado se ha registrado, no debe contener información confidencial.

Almacenar el contexto de cifrado

Para simplificar el uso de cualquier contexto de cifrado al llamar a las operaciones `Decrypt` o `ReEncrypt`, puede almacenar el contexto de cifrado junto con los datos cifrados. Es recomendable que almacene solo la parte suficiente del contexto de cifrado para crear todo el contexto cuando sea necesario para el cifrado o el descifrado.

Por ejemplo, si el contexto de cifrado es la ruta completa a un archivo, almacene solo parte de esa ruta con el contenido del archivo cifrado. A continuación, cuando necesite todo el contexto de cifrado, reconstrúyalo a partir del fragmento almacenado. Si alguien intenta manipular el archivo (por ejemplo, cambiarlo de nombre o moverlo a otra ubicación), el valor de contexto de cifrado cambia y la solicitud de descifrado produce un error.

Política de claves

Cuando crea una clave KMS, determina quién puede usar y administrar esa clave KMS. Estos permisos se encuentran en un documento denominado la política de claves. Puede utilizar la política de claves para agregar, eliminar o cambiar permisos en una clave administrada por el cliente en cualquier momento. Sin embargo, no puede modificar la política de claves de Claves administradas por AWS. Para obtener más información, consulte Políticas clave en AWS KMS.

Concesión

A concesión es un instrumento de política que permite que las entidades principales de AWS usen AWS KMS keys en operaciones criptográficas. También puede permitirles ver una clave KMS (DescribeKey) y crear y administrar concesiones. Al autorizar el acceso a una clave KMS, se consideran concesiones junto con políticas de claves y políticas de IAM. Las concesiones se utilizan

a menudo para permisos temporales, ya que puede crear uno, utilizar sus permisos y eliminarlo sin cambiar las políticas de claves o las políticas de IAM. Como las concesiones pueden ser muy específicas y son fáciles de crear y revocar, a menudo se utilizan para proporcionar permisos temporales o permisos más detallados.

Para obtener información detallada sobre las concesiones, incluida la terminología de las concesiones, consulte Concesiones en AWS KMS.

Auditoría del uso de claves KMS

Se puede utilizar AWS CloudTrail para auditar el uso de claves. CloudTrail crea archivos de registro que contienen un historial de llamadas a la AWS API y eventos relacionados para tu cuenta. Estos archivos de registro contienen todas las solicitudes de AWS KMS de la API realizadas con la consola de administración de AWS, los SDK de AWS y las herramientas de línea de comandos. Los archivos de registro también contienen las solicitudes dirigidas a AWS KMS que los servicios de AWS realizan en su nombre. Puede utilizar estos archivos de registro para buscar información importante, como cuándo se utilizó la clave KMS, la operación solicitada, la identidad del solicitante y la dirección IP de origen. Para obtener más información, consulte Iniciar sesión con AWS CloudTrail y la Guía del usuario de AWS CloudTrail.

Infraestructura de administración de claves

Una práctica habitual en criptografía es cifrar y descifrar con un algoritmo público y revisado por homólogos, como AES (Advanced Encryption Standard), y una clave secreta. Uno de los principales problemas con la criptografía es que es muy difícil mantener una clave secreta. Este suele ser el trabajo de una infraestructura de administración de claves (KMI). AWS KMS opera la infraestructura clave automáticamente. AWS KMS crea y almacena de forma segura las claves raíz, denominadas AWS KMS keys. Para obtener más información sobre cómo opera AWS KMS, consulte Detalles criptográficos de AWS Key Management Service.

Administración de claves

Para comenzar con AWS KMS, cree una AWS KMS key.

En los temas de esta sección se explica cómo administrar una clave KMS básica, una clave KMS de cifrado simétrico, desde su creación hasta su eliminación. Incluye temas sobre edición y visualización de claves, etiquetado de claves, activación y desactivación de claves, rotación de material clave y uso de herramientas y servicios de AWS para monitorear el uso de las claves KMS. También incluye información sobre el uso de AWS CloudFormation para crear y administrar sus claves KMS y una referencia de estado claveque muestra el estado de clave necesario para cada operación de AWS KMS.

Para obtener información acerca de cómo crear, usar y administrar otros tipos de claves KMS, consulte Llaves para fines especiales.

Temas

Crear claves

Puede crear AWS KMS keys enAWS Management Console, o mediante la CreateKeyoperación o una AWS CloudFormationplantilla. Durante este proceso, elija el tipo de clave KMS, la regionalidad (una única región o varias regiones) y el origen del material de claves (de manera predeterminada, AWS KMS crea el material de clave). No puede cambiar estas propiedades después de que se cree

la clave de KMS. También establece la política de claves para la clave KMS, que puede cambiar en cualquier momento.

En este tema se explica cómo crear la clave KMS básica, una clave KMS de cifrado simétrica para una única región con material de claves de AWS KMS. Puede utilizar esta clave KMS para proteger sus recursos en un Servicio de AWS. Para obtener información detallada acerca de las claves KMS de cifrado simétricas, consulte Especificación de clave SYMMETRIC_DEFAULT. Para obtener ayuda para crear otros tipos de claves, consulte Llaves para fines especiales.

Si crea una clave KMS para cifrar los datos que almacena o administra en un servicio AWS, cree una clave KMS de cifrade simétrica. Los servicios de AWS que se integran con AWS KMS utilizan solo claves KMS de cifrado simétricas para cifrar los datos. Estos servicios no admiten cifrado con claves de KMS asimétricas. Para obtener ayuda para decidir qué tipo de clave KMS crear, consulte Elección de un tipo de clave KMS.

> **Note**
>
> Claves KMS simétricas ahora se denominan claves KMS de cifrado simétricas. AWS KMS admite dos tipos de claves KMS simétricas, claves KMS de cifrado simétricas (el tipo predeterminado) y claves KMS HMAC, que también son claves simétricas.

Cuando crea una clave KMS en la consola AWS KMS, debe darle un alias (nombre descriptivo). La operación `CreateKey` no crea un alias para la nueva clave KMS. Para crear un alias para una clave KMS nueva o existente, utilice la CreateAliasoperación. Para obtener información detallada sobre los alias de AWS KMS, consulte Uso de alias.

En este tema se explica cómo crear una clave KMS de cifrado simétrica. Use la siguiente tabla para encontrar instrucciones para crear claves de KMS de diferentes tipos.

Instrucciones para crear una clave de KMS

Tipo de clave KMS	Instrucciones
Clave de cifrado simétrica (SYMMETRIC_DEFAULT)	the section called “Creación de claves KMS de cifrado simétricas”
Claves asimétricas	the section called “Creación de claves KMS asimétricas”

Tipo de clave KMS	Instrucciones
Clave HMAC	the section called “Creación de claves HMAC”
Clave de varias regiones (de cualquier tipo)	the section called “Crear una clave principal con material de claves importado” the section called “Creación de una clave de réplica con material de claves importado”
Material de claves importado (“Traiga su propia llave: BYOK”)	the section called “Paso 1: Crear una clave KMS sin material de claves”
Almacén de claves de AWS CloudHSM	the section called “Crear claves de KMS en un almacén de claves de AWS CloudHSM”
Almacén de claves externo (“Mantenga su propia clave: HYOK”)	the section called “Crear claves de KMS en un almacén de claves externo”

Más información:

- Para crear claves de datos para el cifrado del lado del cliente, utilice la GenerateDataKeyoperación.
- Para crear una clave KMS asimétrica para cifrado o firma, consulteCreación de claves KMS asimétricas.
- Para crear una clave KMS HMAC, consulte Creación de claves KMS HMAC.
- Para crear una clave KMS con material de claves importado (“traiga su propia clave”), consulte Paso 1 de la importación de material de claves: Crear una AWS KMS keysin material de claves.
- Para crear una clave principal de varias regiones o una clave de réplica, consulte Creación de claves de varias regiones.
- Para crear una clave KMS en un almacén de claves personalizado (origen del material de claves es Custom Key Store [CloudHSM]), consulte Crear claves de KMS en un almacén de claves de AWS CloudHSM.
- Para usar una AWS CloudFormation plantilla para crear una clave KMS, consulte la AWS::KMS::KeyGuía del AWS CloudFormationusuario.

- Para determinar si una clave KMS existente es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.
- Para usar la clave KMS mediante programación y en las operaciones de la interfaz de línea de comandos, necesita un ID de clave o un ARN de clave. Para obtener instrucciones detalladas, consulte Búsqueda del ID y el ARN de la clave.
- Para obtener información acerca de las cuotas que se aplican a las claves KMS, consulte Cuotas.

Temas

- Permisos para crear claves KMS
- Creación de claves KMS de cifrado simétricas

Permisos para crear claves KMS

Para crear una clave KMS en la consola o mediante las API, debe tener el permiso siguiente en una política de IAM. Siempre que sea posible, use claves de condición para limitar los permisos. Por ejemplo, puede usar la clave de KeySpec condición kms: en una política de IAM para permitir que los principales creen solo claves de cifrado simétricas.

Para obtener un ejemplo de una política de IAM para las principales entidades que crean claves, consulte Permitir a un usuario crear claves KMS.

> **Note**
>
> Tenga cuidado al dar permiso a las entidades principales para administrar etiquetas y alias. El cambio de etiqueta o alias puede permitir o denegar permiso a la clave administrada por el cliente. Para obtener más detalles, consulte ABAC para AWS KMS.

- kms: CreateKey es obligatorio.
- kms: CreateAlias es necesario para crear una clave KMS en la consola, donde se requiere un alias para cada nueva clave KMS.
- kms: TagResource es necesario añadir etiquetas al crear la clave KMS.
- iam: CreateServiceLinkedRole es necesario para crear claves principales multirregionales. Para obtener más detalles, consulte Control del acceso a claves de varias regiones.

El PutKeyPolicy permiso kms: no es necesario para crear la clave KMS. El permiso `kms:CreateKey` incluye permiso para establecer la política de clave inicial. Pero debe agregar este permiso a la política de clave mientras crea la clave KMS para asegurarse de que puede controlar el acceso a la clave KMS. La alternativa es utilizar el BypassLockoutSafetyCheckparámetro, lo cual no se recomienda.

Las claves KMS pertenecen a la cuenta de AWS en la que se crearon. El usuario de IAM que crea una clave KMS no se considera el propietario de la clave y no tiene permiso automáticamente para usar o administrar la clave KMS que creó. Al igual que cualquier otra entidad principal, el creador de la clave necesita obtener permiso a través de una política de claves, una política de IAM o una concesión. Sin embargo, las entidades principales que tienen el permiso de `kms:CreateKey` pueden establecer la política de clave inicial y darse permiso a ellas mismas para usar o administrar la clave.

Creación de claves KMS de cifrado simétricas

Puede crear claves KMS en la AWS Management Console o utilizando la API de AWS KMS.

En este tema se explica cómo crear la clave KMS básica, una clave KMS de cifrado simétrica para una única región con material de claves de AWS KMS. Puede utilizar esta clave KMS para proteger sus recursos en un Servicio de AWS. Para obtener ayuda para crear otros tipos de claves, consulte Llaves para fines especiales.

Creación de claves KMS de cifrado simétricas (consola)

Puede utilizar la AWS Management Console para crear AWS KMS keys (claves KMS).

> **Important**
>
> No incluya información confidencial en el alias, la descripción ni las etiquetas. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.

4. Elija Create key.
5. Para crear una clave KMS de cifrado simétrica, para Key type (Tipo de clave) seleccione Symmetric (Simétrica).

   Para obtener información acerca de cómo crear una clave KMS asimétrica en la consola de AWS KMS, consulte Creación de claves KMS asimétricas (consola).
6. En Key usage (Uso de claves), se selecciona la opción Encrypt and decrypt (Cifrar y descifrar) para usted.

   Para obtener información acerca de cómo crear claves KMS que generan y verifican códigos MAC, consulte Creación de claves KMS HMAC.
7. Elija Siguiente.

   Para obtener más información acerca de las Opciones avanzadas, consulte Llaves para fines especiales.
8. Escriba un alias para la clave KMS. El nombre del alias no puede empezar por **`aws/`**. El prefijo **`aws/`** está reservado para Amazon Web Services y representa las Claves administradas por AWS de su cuenta.

   > **Note**
   >
   > Agregar, eliminar o actualizar un alias puede permitir o denegar el permiso a la clave KMS. Para más detalles, consulte ABAC para AWS KMS y Usar alias para controlar el acceso a las claves KMS.

   Un alias es un nombre de visualización que puede usar para identificar a una clave KMS. Le recomendamos que elija un alias que indique el tipo de datos que piensa proteger o la aplicación que piensa usar con la clave KMS.

   Los alias son necesarios para crear una clave KMS en la AWS Management Console. Son opcionales cuando se utiliza la CreateKeyoperación.
9. (Opcional) Escriba una descripción de la clave KMS.

   Puede agregar una descripción ahora o actualizarla en cualquier momento, a menos que el estado de la clave sea `Pending Deletion` o `Pending Replica Deletion`. Para añadir, cambiar o eliminar la descripción de una clave gestionada por el cliente

existente, edite la descripción en la operación AWS Management Console o utilice la UpdateKeyDescriptionoperación.

10. (Opcional) Escriba una clave de etiqueta y un valor de etiqueta opcional. Para agregar más de una etiqueta a la clave KMS, elija Add tag (Agregar etiqueta).

    > **Note**
    >
    > Etiquetar o quitar las etiquetas de la clave KMS puede permitir o denegar permiso a la clave KMS. Para más detalles, consulte ABAC para AWS KMS y Uso de etiquetas para controlar el acceso a las claves KMS.

    Cuando se agregan etiquetas a los recursos de AWS, AWS genera un informe de asignación de costos con el uso y los costos agregados por etiquetas. Las etiquetas también pueden utilizarse para controlar el acceso a una clave KMS. Para obtener información acerca del etiquetado de claves KMS, consulte Etiquetado de claves y ABAC para AWS KMS.

11. Elija Siguiente.
12. Seleccione los usuarios y roles de IAM que pueden administrar la clave de KMS.

    > **Note**
    >
    > Esta política de claves proporciona a la Cuenta de AWS control total de esta clave KMS. Permite a los administradores de cuentas utilizar las políticas de IAM para dar permiso a otras entidades principales para administrar la clave KMS. Para obtener más detalles, consulte the section called “Política de claves predeterminada”.
    >
    > Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

13. (Opcional) Para evitar que los usuarios y los roles de IAM seleccionados eliminen esta clave de KMS, en la sección Eliminación de claves situada en la parte inferior de la página, desactive la casilla Permitir que los administradores de claves eliminen esta clave.
14. Elija Siguiente.
15. Seleccione los usuarios y roles de IAM que pueden usar la clave en operaciones criptográficas

> **Note**
>
> Esta política de claves proporciona a la Cuenta de AWS control total de esta clave KMS. Permite a los administradores de cuentas utilizar las políticas de IAM para dar permiso a otras entidades principales para utilizar la clave KMS. Para obtener más detalles, consulte the section called “Política de claves predeterminada”.
>
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

16. (Opcional) Puede permitir que otras cuentas de Cuentas de AWS usen esta clave de KMS en operaciones criptográficas. Para ello, en la parte inferior de la página de la sección Other Cuentas de AWS (Otras), elija Add another Cuenta de AWS (Agregar otra) e ingrese el número de identificación de Cuenta de AWS de una cuenta externa. Para agregar varias cuentas externas, repita este paso.

> **Note**
>
> Para permitir que las entidades principales de las cuentas externas usen la clave KMS, los administradores de la cuenta externa también deben crear las políticas de IAM que proporcionan estos permisos. Para obtener más información, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS.

17. Seleccione Siguiente.
18. Revise los ajustes de clave que ha elegido. Aún puede volver atrás y cambiar todos los ajustes.
19. Elija Finalizar para crear la clave de KMS.

Creación de claves KMS de cifrado simétricas (API de AWS KMS)

Puede utilizar la CreateKeyoperación para crear AWS KMS keys de todos los tipos. En estos ejemplos, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

> **Important**
>
> No incluya información confidencial en los campos `Description` o `Tags`. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

La siguiente operación crea la clave KMS más utilizada, una clave de cifrado simétrica en una única región respaldada por material de claves generado por AWS KMS. Esta operación no tiene parámetros obligatorios. Sin embargo, es posible que también desee utilizar el parámetro `Policy` para especificar una política de claves. Puede cambiar la política clave (PutKeyPolicy) y añadir elementos opcionales, como una descripción y etiquetas, en cualquier momento. También puede crear claves asimétricas, claves de varias regiones, claves con material de claves importado, y claves en almacenes de claves personalizados.

La `CreateKey` operación no le permite especificar un alias, pero puede usar la CreateAliasoperación para crear un alias para la nueva clave de KMS.

A continuación se muestra un ejemplo de una llamada a la operación `CreateKey` sin parámetros. Este comando utiliza todos los valores predeterminados. Crea una clave KMS de cifrado simétrica para con material de claves generado por AWS KMS.

```
$ aws kms create-key
{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
        "Enabled": true,
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
        "CreationDate": 1502910355.475,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "MultiRegion": false
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
```

```
    }
}
```

Si no especifica una política de claves para su nueva clave KMS, la política de claves predeterminada que aplica `CreateKey` es diferente de la política de claves predeterminada que aplica la consola cuando se utiliza para crear una nueva clave KMS.

Por ejemplo, esta llamada a la GetKeyPolicyoperación devuelve la política clave que `CreateKey` se aplica. Le da el acceso de Cuenta de AWS a la clave KMS y le permite crear políticas AWS Identity and Access Management (IAM) para la clave KMS. Para obtener información detallada sobre las políticas de IAM y las políticas de claves para claves KMS, consulte Autenticación y control de acceso de AWS KMS

```
$ aws kms get-key-policy --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --policy-name
 default --output text
{
  "Version" : "2012-10-17",
  "Id" : "key-default-1",
  "Statement" : [ {
    "Sid" : "Enable IAM User Permissions",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

Uso de alias

Un alias es un nombre fácil de recordar para un AWS KMS key. Por ejemplo, un alias le permite referirse a una clave KMS como `test-key` en lugar de `1234abcd-12ab-34cd-56ef-1234567890ab`.

Puede usar un alias para identificar una clave KMS en la AWS KMS consola, en la DescribeKeyoperación y en las operaciones criptográficas, como Cifrar y. GenerateDataKey Los alias también facilitan el reconocimiento de un Clave administrada de AWS. Los alias de estas claves KMS siempre tienen la forma `aws/<service-name>`. Por ejemplo, el alias para Clave administrada de

AWS para Amazon DynamoDB es `aws/dynamodb`. Puede establecer estándares de alias similares para sus proyectos, como anteponer los alias con el nombre de un proyecto o categoría.

También puede permitir y denegar el acceso a claves KMS en función de sus alias sin editar políticas ni administrar concesiones. Esta característica forma parte de la compatibilidad de AWS KMS para el control de acceso basado en atributos (ABAC). Para obtener más detalles, consulte Usar alias para controlar el acceso a las claves KMS.

Gran parte de la potencia de los alias proviene de su capacidad de cambiar la clave KMS asociada a un alias en cualquier momento. Los alias pueden hacer que su código sea más fácil de escribir y mantener. Por ejemplo, supongamos que utiliza un alias para hacer referencia a una clave KMS concreta y desea cambiar la clave KMS. En ese caso, simplemente asocie el alias con una clave KMS diferente. No es necesario realizar cambios en el código.

Los alias también facilitan la reutilización del mismo código en diferentes Regiones de AWS. Cree alias con el mismo nombre en varias regiones y asocie cada alias a una clave KMS en su región. Cuando el código se ejecuta en cada región, el alias hace referencia a la clave KMS asociada en esa región. Para ver un ejemplo, consulte Usar alias en las aplicaciones.

Puede crear un alias para una clave de KMS en la AWS KMS consola, mediante la CreateAliasAPI o mediante una AWS CloudFormation plantilla.

La API de AWS KMS proporciona un control total de los alias en cada cuenta y región. La API incluye operaciones para crear un alias (CreateAlias), ver los nombres y los ARN de los alias (ListAliases), cambiar la clave de KMS asociada a un alias (UpdateAlias) y eliminar un alias (DeleteAlias). Para ver ejemplos de administración de alias en varios lenguajes de programación, consulte the section called “Trabajar con alias”.

Los siguientes recursos pueden ayudarle a obtener más información:

- Para obtener información acerca de los identificadores de clave KMS, incluidos los alias, consulte Identificadores clave () KeyId.
- Para obtener ayuda sobre el uso AWS CloudFormation de una plantilla para crear un alias para una clave de KMS, consulta AWS::KMS::Aliasla Guía del AWS CloudFormation usuario.
- Para obtener ayuda para encontrar los alias asociados a una clave KMS, consulte Buscar el nombre del alias y el ARN de alias
- Para obtener información acerca de las cuotas de recursos para alias y las cuotas de tasa para operaciones de API relacionadas con alias, consulte Cuotas.

- Para obtener ejemplos de creación y administración de alias en varios lenguajes de programación, consulte Trabajar con alias.

Temas

Acerca de los alias

Obtenga información sobre cómo funcionan los alias en AWS KMS.

Un alias es un recurso AWS independiente.

Un alias no es propiedad de una clave KMS. Las acciones que realice en el alias no afectan a su clave KMS asociada. Puede crear un alias para una clave KMS y, a continuación, actualizar el alias para que esté asociado a una clave KMS diferente. Incluso puede eliminar el alias sin ningún efecto en la clave KMS asociada. Sin embargo, si elimina una clave KMS, se eliminan todos los alias asociados a esa clave KMS.

Si especifica un alias como recurso en una política de IAM, la política hace referencia al alias, no a la clave KMS asociada.

Cada alias tiene dos formatos

Cuando se crea un alias, hay que especificar el nombre del alias. AWS KMS crea el alias ARN por usted.

- Un ARN de alias es un nombre de recurso de Amazon (ARN) que identifica de forma exclusiva el alias.

```
# Alias ARN
arn:aws:kms:us-west-2:111122223333:alias/<alias-name>
```

- El nombre de alias debe ser único en la cuenta y la región. En API de AWS KMS, el nombre del alias siempre tiene el prefijo de `alias/`. Ese prefijo se omite en la consola AWS KMS.

```
# Alias name
alias/<alias-name>
```

Los alias no son secretos

Los alias pueden mostrarse en texto plano en CloudTrail los registros y otros resultados. No incluya información confidencial en el nombre del alias.

Cada alias está asociado a una clave KMS a la vez

El alias y la clave KMS deben estar en la misma cuenta y región.

Puede asociar un alias con cualquier clave administrada por el cliente en la misma Cuenta de AWS y región. Sin embargo, no tiene permiso para asociar un alias con una Clave administrada de AWS.

Por ejemplo, este ListAliasesresultado muestra que el `test-key` alias está asociado exactamente a una clave KMS de destino, que se representa mediante la `TargetKeyId` propiedad.

```
{
     "AliasName": "alias/test-key",
     "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
     "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
     "CreationDate": 1593622000.191,
     "LastUpdatedDate": 1593622000.191
}
```

Se pueden asociar varios alias con la misma clave KMS

Por ejemplo, puede asociar los alias `test-key` y `project-key` con la misma clave KMS.

```
{
     "AliasName": "alias/test-key",
     "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
     "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
     "CreationDate": 1593622000.191,
     "LastUpdatedDate": 1593622000.191
},
{
     "AliasName": "alias/project-key",
```

```
    "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/project-key",
    "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": 1516435200.399,
    "LastUpdatedDate": 1516435200.399
}
```

El alias debe ser único en la cuenta y región.

Por ejemplo, solo puede tener un alias `test-key` en cada cuenta y región. Los alias distinguen entre mayúsculas y minúsculas, pero los alias que solo difieren en sus mayúsculas son muy propensos a errores. No puede cambiar un nombre de alias. Sin embargo, puede eliminar el alias y crear un nuevo alias con el nombre deseado.

Puede crear alias con el mismo nombre en diferentes regiones

Por ejemplo, puede tener un alias `finance-key` en EE. UU. Este (Norte de Virginia) y un alias `finance-key` en Europa (Fráncfort). Cada alias se asociaría a una clave KMS en su región. Si su código se refiere a un nombre de alias como `alias/finance-key`, puede ejecutarlo en varias regiones. En cada región, utiliza una clave KMS diferente. Para obtener más detalles, consulte Usar alias en las aplicaciones.

Puede cambiar la clave KMS asociada a un alias

Puede utilizar la UpdateAliasoperación para asociar un alias a una clave de KMS diferente. Por ejemplo, si el alias `finance-key` está asociado con la clave KMS `1234abcd-12ab-34cd-56ef-1234567890ab`, puede actualizarla para que esté asociada con la clave KMS `0987dcba-09fe-87dc-65ba-ab0987654321`.

Sin embargo, la clave de KMS actual y la nueva deben ser del mismo tipo (ambas simétricas o ambas asimétricas o ambas HMAC) y deben tener el mismo uso de clave (ENCRYPT_DECRYPT o SIGN_VERIFY o GENERATE_VERIFY_MAC). Esta restricción evita errores en el código que utiliza alias. Si debe asociar un alias a otro tipo de clave y ha mitigado los riesgos, puede eliminar el alias y volver a crearlo.

Algunas claves KMS no tienen alias

Cuando crea una clave KMS en la consola AWS KMS, debe darle un alias nuevo. Sin embargo, no se requiere un alias cuando se utiliza la CreateKeyoperación para crear una clave de KMS. Además, puede utilizar la UpdateAliasoperación para cambiar la clave de KMS asociada a un alias y la DeleteAliasoperación para eliminar un alias. Como resultado, algunas claves KMS pueden tener varios alias, y algunas podrían tener ninguno.

AWS crea alias en tu cuenta

AWS crea alias en tu cuenta para Claves administradas por AWS. Estos alias tienen nombres del formulario `alias/aws/<service-name>`, como, por ejemplo, `alias/aws/s3`.

Alguno alias de AWS no tienen clave KMS. Estos alias predefinidos generalmente se asocian con una Clave administrada de AWScuando empieza a utilizar el servicio.

Usar alias para identificar claves KMS

Puede usar un nombre de alias o un ARN de alias para identificar una clave de KMS en las operaciones criptográficas, y DescribeKey. GetPublicKey (Si la clave KMS está en una Cuenta de AWS diferente, debe usar su ARN de clave o ARN de alias). Los alias no son identificadores válidos para las claves KMS en otras operaciones de AWS KMS. Para obtener información acerca de identificadores clave válidos para cada operación de la API de AWS KMS, consulte las descripciones de los parámetros `KeyId` en la Referencia de la API de AWS Key Management Service.

No puede utilizar un nombre de alias ni un ARN de alias para identificar una clave KMS en una política de IAM. Para controlar el acceso a una clave KMS en función de sus alias, utilice las claves condicionales kms: RequestAlias o kms: ResourceAliases. Para obtener más detalles, consulte ABAC para AWS KMS.

Administración de alias

Los usuarios autorizados pueden crear, ver y eliminar alias. También puede actualizar un alias, es decir, asociar un alias existente con una clave KMS distinta.

Temas

- Crear un alias
- Visualización de alias
- Actualización de alias
- Eliminar un alias

Crear un alias

Puede crear alias en la consola AWS KMS o mediante operaciones de la API de AWS KMS.

El alias debe ser una cadena de 1-256 caracteres. Solo puede contener caracteres alfanuméricos, barras (/), guiones bajos (_) y guiones (-). El nombre de alias de un clave administrada por el cliente no puede comenzar con `alias/aws/`. El prefijo `alias/aws/` se reserva para el uso de Clave administrada de AWS.

Puede crear un alias para una nueva clave KMS o para una clave KMS existente. Puede agregar un alias para que se utilice una clave KMS concreta en un proyecto o aplicación.

Creación de un alias (consola)

Cuando crea una clave KMS en la consola AWS KMS, debe crear un alias para la nueva clave KMS. Para crear un alias para una clave KMS existente, utilice la pestaña Aliases (Alias) en la página de detalles de la clave KMS.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente. No puede administrar alias para Claves administradas por AWS ni para Claves propiedad de AWS.
4. En la tabla, elija el ID de clave o el alias de la clave KMS. A continuación, en la página de detalles de la clave KMS, elija la pestaña Aliases (Alias).

   Si una clave KMS tiene varios alias, la columna Aliases (Alias) de la tabla muestra un alias y un resumen de alias, como (+n más). Al elegir el resumen de alias, se le llevará directamente a la pestaña Aliases (Alias) en la página de detalles de la clave KMS.
5. En la pestaña Aliases (Alias), elija Create alias (Creación de alias). Introduzca un nombre de alias y elija Create alias (Creación de alias).

   > **Important**
   >
   > No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.

> **Note**
>
> No agregue el prefijo `alias/`. La consola lo agrega automáticamente. Si ingresa`alias/ExampleAlias`, el nombre de alias real será `alias/alias/ExampleAlias`.

Creación de un alias (API de AWS KMS)

Para crear un alias, utilice la CreateAliasoperación. A diferencia del proceso de creación de claves de KMS en la consola, la CreateKeyoperación no crea un alias para una clave de KMS nueva.

> **Important**
>
> No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.

Puede utilizar la operación `CreateAlias` para crear un alias para una nueva clave KMS sin alias. También puede utilizar la operación `CreateAlias` para agregar un alias a cualquier clave KMS existente o para volver a crear un alias que se eliminó accidentalmente.

En las operaciones de la API de AWS KMS, cada nombre de alias debe comenzar por `alias/` seguido de un nombre, como, por ejemplo `alias/ExampleAlias`. El alias debe ser único en la cuenta y en la región de . Para buscar los nombres de alias que ya están en uso, utilice la ListAliasesoperación. El nombre del alias distingue entre mayúsculas y minúsculas.

La `TargetKeyId` puede ser cualquier clave administrada por el cliente en la misma Región de AWS. Para identificar la clave KMS, utilice su ID de clave o su ARN de clave. No puede usar otro alias.

En el ejemplo siguiente, se crea el alias `example-key` y lo asocia con la clave KMS especificada. Estos ejemplos utilizan la AWS Command Line Interface (AWS CLI). Para ver ejemplos en varios lenguajes de programación, consulte Trabajar con alias.

```
$ aws kms create-alias \
    --alias-name alias/example-key \
    --target-key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

`CreateAlias` no devuelve ningún resultado. Para ver el nuevo alias, utilice la operación `ListAliases`. Para obtener más detalles, consulte Visualización de alias (API de AWS KMS).

Visualización de alias

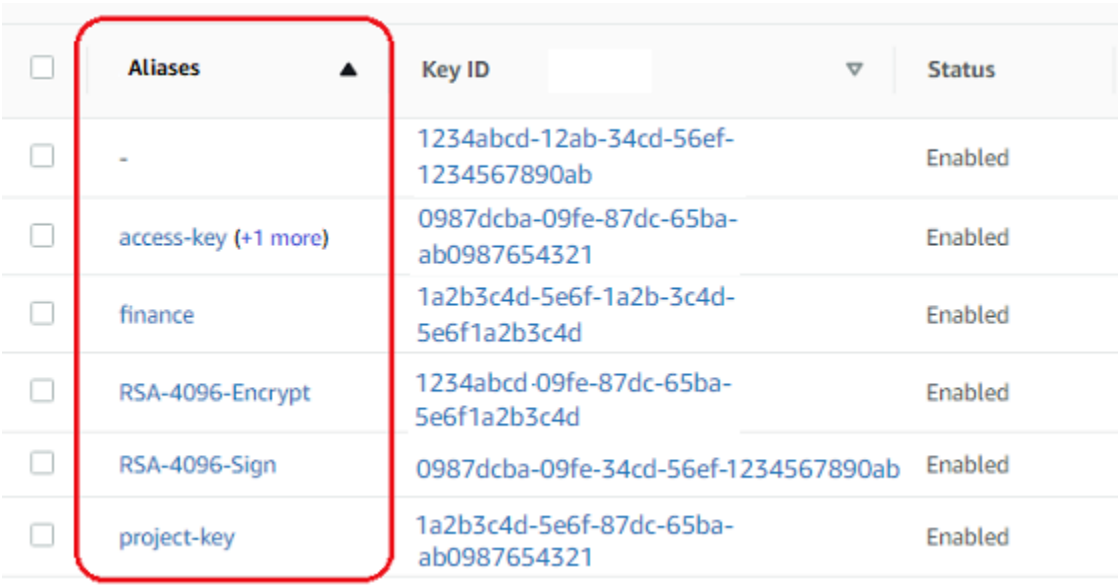
Los alias facilitan el reconocimiento de claves KMS en la consola de AWS KMS. Puede ver los alias de una clave KMS en la AWS KMS consola o mediante la ListAliasesoperación. La DescribeKeyoperación, que devuelve las propiedades de una clave KMS, no incluye los alias.

Visualización de alias (consola)

Las claves administradas por el cliente y las páginas Claves administradas por AWS de la consola de AWS KMS muestran el alias asociado a cada clave KMS. También puede buscar, ordenar y filtrar claves KMS basadas en sus alias.

La siguiente imagen de la consola de AWS KMS muestra los alias en la página Customer managed keys (Claves administradas por el cliente) de una cuenta de ejemplo. Como se muestra en la imagen, algunas claves de KMS no tienen un alias.

Cuando una clave KMS tiene varios alias, la columna Aliases (Alias) muestra un alias y un alias summary (resumen de alias) (+n más). El resumen de alias muestra cuántos alias adicionales están asociados a la clave KMS y los vínculos a la visualización de todos los alias de la clave KMS en la pestaña Aliases (Alias).

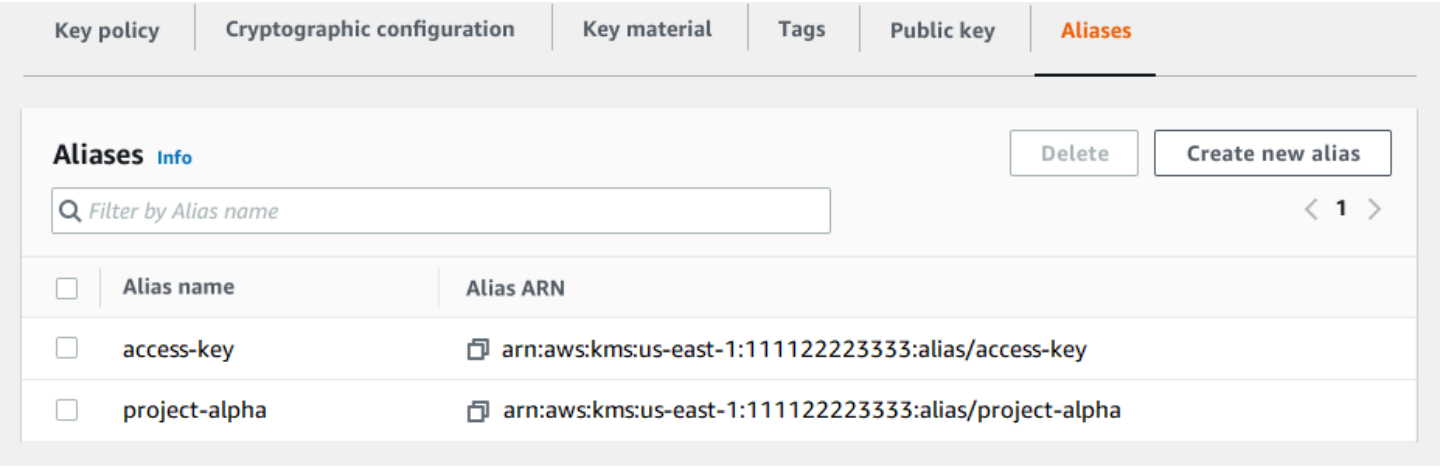


La pestaña Aliases (Alias) de la página de detalles de cada clave KMS muestra el nombre de alias y el ARN de alias de todos los alias de la clave KMS en la Cuenta de AWSy región. También puede utilizar la pestaña Aliases (Alias) para crear alias y para eliminar alias.

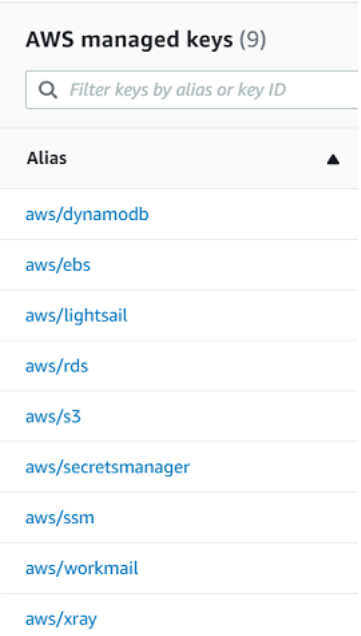
Para buscar el nombre de alias y el ARN de alias de todos los alias de la clave KMS, utilice la pestaña Aliases (Alias).

- Para ir directamente a la pestaña Aliases (Alias), en la columna Aliases (Alias), elija el resumen de alias (+n más). Un resumen de alias sólo aparece si la clave KMS tiene más de un alias.
- O bien, elija el alias o el ID de clave de la clave KMS (que abre la página de detalles de la clave KMS) y, a continuación, elija la pestaña Aliases (Alias). Las pestañas se encuentran debajo de la sección General configuration (Configuración general).

En la siguiente imagen se muestra la pestaña Aliases (Alias) para obtener una clave KMS de ejemplo.



Puede usar el alias para reconocer una Clave administrada de AWS, como se muestra en esta página de Claves administradas por AWS de ejemplo. Los alias de Claves administradas por AWS siempre tienen el formato: `aws/<service-name>`. Por ejemplo, el alias para Clave administrada de AWS para Amazon DynamoDB es `aws/dynamodb`.



Visualización de alias (API de AWS KMS)

La ListAliasesoperación devuelve el nombre del alias y el ARN del alias de la cuenta y la región. La salida incluye alias para Claves administradas por AWS y para claves administradas por el cliente. Los alias de Claves administradas por AWS deben tener el formatoaws/*<service-name>*, como, por ejemplo,`aws/dynamodb`.

La respuesta también podría incluir los alias que no tienen el campo `TargetKeyId`. Estos son los alias predefinidos que AWS ha creado, pero aún no se han asociado con una clave KMS.

```
$ aws kms list-aliases
{
    "Aliases": [
        {
            "AliasName": "alias/access-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1516435200.399,
            "LastUpdatedDate": 1516435200.399
        },
        {
            "AliasName": "alias/ECC-P521-Sign",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ECC-P521-Sign",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1693622000.704,
            "LastUpdatedDate": 1693622000.704
```

```
        },
        {
            "AliasName": "alias/ImportedKey",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ImportedKey",
            "TargetKeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "CreationDate": 1493622000.704,
            "LastUpdatedDate": 1521097200.235
        },
        {
            "AliasName": "alias/finance-project",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/finance-project",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1604958290.014,
            "LastUpdatedDate": 1604958290.014
        },
        {
            "AliasName": "alias/aws/dynamodb",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/dynamodb",
            "TargetKeyId": "0987ab65-43cd-21ef-09ab-87654321cdef",
            "CreationDate": 1521097200.454,
            "LastUpdatedDate": 1521097200.454
        },
        {
            "AliasName": "alias/aws/ebs",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/ebs",
            "TargetKeyId": "abcd1234-09fe-ef90-09fe-ab0987654321",
            "CreationDate": 1466518990.200,
            "LastUpdatedDate": 1466518990.200
        }
    ]
}
```

Para obtener todos los alias que están asociados con una determinada clave KMS, utilice el parámetro `KeyId` de la operación `ListAliases`. El parámetro `KeyId` toma el ID de clave o el ARN de clave de la clave KMS.

En este ejemplo se obtienen todos los alias asociados con el`0987dcba-09fe-87dc-65ba-ab0987654321` de la clave KMS.

```
$ aws kms list-aliases --key-id 0987dcba-09fe-87dc-65ba-ab0987654321
{
    "Aliases": [
        {
```

```
            "AliasName": "alias/access-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": "2018-01-20T15:23:10.194000-07:00",
            "LastUpdatedDate": "2018-01-20T15:23:10.194000-07:00"
        },
        {
            "AliasName": "alias/finance-project",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/finance-project",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1604958290.014,
            "LastUpdatedDate": 1604958290.014
        }
    ]
}
```

El parámetro `KeyId` no toma caracteres comodín, pero puede usar las características de su lenguaje de programación para filtrar la respuesta.

Por ejemplo, el siguiente comando AWS CLI obtiene solo los alias de Claves administradas por AWS.

```
$ aws kms list-aliases --query 'Aliases[?starts_with(AliasName, `alias/aws/`)]'
```

El siguiente comando obtiene sólo el alias de `access-key`. El nombre del alias distingue entre mayúsculas y minúsculas.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/access-key`]'
[
    {
        "AliasName": "alias/access-key",
        "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
        "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "CreationDate": "2018-01-20T15:23:10.194000-07:00",
        "LastUpdatedDate": "2018-01-20T15:23:10.194000-07:00"
    }
]
```

Actualización de alias

Dado que un alias es un recurso independiente, puede cambiar la clave KMS asociada a un alias. Por ejemplo, si el `test-key` alias está asociado a una clave de KMS, puede utilizar la

UpdateAliasoperación para asociarlo a una clave de KMS diferente. Esta es una de las varias maneras de girar manualmente una clave KMS sin cambiar su material clave. También puede actualizar una clave KMS para que una aplicación que estaba utilizando una clave KMS para nuevos recursos utilice ahora una clave KMS diferente.

No puede actualizar un alias en la consola de AWS KMS. Además, no puede utilizar `UpdateAlias` (o cualquier otra operación) para cambiar un nombre de alias. Para cambiar un nombre de alias, elimine el alias actual y, a continuación, cree un alias nuevo para la clave KMS.

Al actualizar un alias, la clave de KMS actual y la nueva clave de KMS deben ser del mismo tipo (ambas simétricas o asimétricas o HMAC). También deben tener el mismo uso de claves (`ENCRYPT_DECRYPT` o `SIGN_VERIFY` o GENERATE_VERIFY_MAC). Esta restricción evita errores criptográficos en el código que utiliza alias.

El siguiente ejemplo comienza con la ListAliasesoperación para mostrar que el `test-key` alias está asociado actualmente a la clave de KMS`1234abcd-12ab-34cd-56ef-1234567890ab`.

```
$ aws kms list-aliases --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "Aliases": [
        {
            "AliasName": "alias/test-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1593622000.191,
            "LastUpdatedDate": 1593622000.191
        }
    ]
}
```

A continuación, utiliza la operación `UpdateAlias` para cambiar la clave KMS que está asociada con el alias `test-key` a la clave KMS `0987dcba-09fe-87dc-65ba-ab0987654321`. No es necesario especificar la clave KMS asociada actualmente, solo la nueva («destino») clave KMS. El nombre del alias distingue entre mayúsculas y minúsculas.

```
$ aws kms update-alias --alias-name 'alias/test-key' --target-key-id
 0987dcba-09fe-87dc-65ba-ab0987654321
```

Para comprobar que el alias se asocia ahora con la clave KMS de destino, utilice la operación `ListAliases` de nuevo. Este comando AWS CLI utiliza el parámetro `--query` para obtener solo el alias de `test-key`. Los campos `TargetKeyId` y `LastUpdatedDate` se actualizan.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/test-key`]'
[
    {
        "AliasName": "alias/test-key",
        "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/test-key",
        "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "CreationDate": 1593622000.191,
        "LastUpdatedDate": 1604958290.154
    }
]
```

Eliminar un alias

Puede eliminar un alias en la AWS KMS consola o mediante la DeleteAliasoperación. Antes de eliminar un alias, asegúrese de que no esté en uso. Aunque eliminar un alias no afecta a la clave KMS asociada, puede crear problemas para cualquier aplicación que utilice el alias. Si elimina un alias por error, puede crear un nuevo alias con el mismo nombre y asociarlo a la misma clave KMS o a otra.

Si elimina una clave KMS, se eliminan todos los alias asociados a esa clave KMS.

Eliminar alias (consola)

Para eliminar un alias en la consola de AWS KMS, utilice la pestaña Aliases (Alias) en la página de detalles de la clave KMS. Puede eliminar varios alias para una clave KMS a la vez.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente. No puede administrar alias para Claves administradas por AWS ni para Claves propiedad de AWS.
4. En la tabla, elija el ID de clave o el alias de la clave KMS. A continuación, en la página de detalles de la clave KMS, elija la pestaña Aliases (Alias).

Si una clave KMS tiene varios alias, la columna Aliases (Alias) de la tabla muestra un alias y un resumen de alias, como (+n más). Al elegir el resumen de alias, se le llevará directamente a la pestaña Aliases (Alias) en la página de detalles de la clave KMS.

5. En la pestaña Aliases (Alias), seleccione la casilla de verificación situada junto a los alias que desea eliminar. A continuación, elija Eliminar.

Eliminar un alias (API de AWS KMS)

Para eliminar un alias, utilice la DeleteAliasoperación. Esta operación elimina un alias a la vez. El nombre del alias distingue entre mayúsculas y minúsculas y debe estar precedido por el prefijo `alias/`.

Por ejemplo, el siguiente comando elimina el alias `test-key`. El comando no devuelve ningún resultado.

```
$ aws kms delete-alias --alias-name alias/test-key
```

Para comprobar que se ha eliminado el alias, utilice la ListAliasesoperación. El siguiente comando utiliza el parámetro `--query` en la AWS CLI para obtener solo el alias de `test-key`. Los corchetes vacíos en la respuesta indican que la respuesta `ListAliases` no incluyó un alias `test-key`. Para eliminar los corchetes, utilice el parámetro y valor `--output text`.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/test-key`]'
[]
```

Usar alias en las aplicaciones

Puede utilizar un alias para representar una clave KMS en el código de la aplicación. El `KeyId` parámetro en las operaciones AWS KMS criptográficas y GetPublicKeyacepta un nombre de alias o un ARN de alias. DescribeKey

Por ejemplo, el siguiente comando `GenerateDataKey` utiliza un nombre de alias (`alias/finance`) para identificar una clave KMS. El nombre del alias es el valor del parámetro `KeyId`.

```
$ aws kms generate-data-key --key-id alias/finance --key-spec AES_256
```

Si la clave KMS está en una Cuenta de AWS diferente, en estas operaciones, debe usar un ARN de clave o ARN de alias. Cuando utilice un alias ARN, recuerde que el alias de una clave KMS se

define en la cuenta que posee la clave KMS y puede diferir en cada región. Para obtener ayuda para encontrar el ARN de alias, consulte Buscar el nombre del alias y el ARN de alias.

Por ejemplo, el siguiente comando `GenerateDataKey` utiliza una clave KMS que no está en la cuenta de la persona que llama. El alias `ExampleAlias` está asociado a la clave KMS en la cuenta y región especificadas.

```
$ aws kms generate-data-key --key-id arn:aws:kms:us-west-2:444455556666:alias/
ExampleAlias --key-spec AES_256
```

Uno de los usos más potentes de los alias es en aplicaciones que se ejecutan en múltiples Regiones de AWS. Por ejemplo, puede tener una aplicación global que utiliza un RSA clave KMS asimétrica para la firma y la verificación.

- En EE.UU. Oeste (Oregón) (us-west-2), desea usar `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`.
- En Europa (Fráncfort) (eu-central-1), desea usar `arn:aws:kms:eu-central-1:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321`
- En Asia Pacífico (Singapur) (ap-southeast-1), desea usar `arn:aws:kms:ap-southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d`.

Puede crear una versión diferente de su aplicación en cada región o utilizar un diccionario o una declaración switch para seleccionar la clave KMS correcta para cada región. Pero es mucho más fácil crear un alias con el mismo nombre de alias en cada región. El nombre del alias distingue entre mayúsculas y minúsculas.

```
aws --region us-west-2 kms create-alias \
    --alias-name alias/new-app \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

aws --region eu-central-1 kms create-alias \
    --alias-name alias/new-app \
    --key-id arn:aws:kms:eu-central-1:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321

aws --region ap-southeast-1 kms create-alias \
    --alias-name alias/new-app \
```

```
    --key-id arn:aws:kms:ap-
southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d
```

A continuación, usa el alias en tu código. Cuando el código se ejecuta en cada región, el alias hará referencia a su clave KMS asociada en esa región. Por ejemplo, este código llama a la operación Sign (Firmar) con un nombre de alias.

```
aws kms sign --key-id alias/new-app \
    --message $message \
    --message-type RAW \
    --signing-algorithm RSASSA_PSS_SHA_384
```

Sin embargo, existe el riesgo de que el alias se elimine o actualice para que se asocie a una clave KMS diferente. En ese caso, los intentos de la aplicación de verificar firmas utilizando el nombre de alias fallarán y es posible que deba volver a crearlo o actualizarlo.

Para mitigar este riesgo, tenga cuidado al conceder permiso a las entidades principales para administrar los alias que utiliza en la aplicación. Para obtener más detalles, consulte Control del acceso a alias.

Hay varias otras soluciones para aplicaciones que cifran datos en múltiples Regiones de AWS, incluido el AWS Encryption SDK.

Control del acceso a alias

Al crear o cambiar un alias, afectará al alias y a su clave KMS asociada. Por lo tanto, las entidades principales que administran alias deben tener permiso para llamar a la operación de alias en el alias y en todas las claves KMS afectadas. Puede proporcionar estos permisos utilizando políticas de claves, políticas de IAM y concesiones.

> **Note**
>
> Tenga cuidado al dar permiso a las entidades principales para administrar etiquetas y alias. El cambio de etiqueta o alias puede permitir o denegar permiso a la clave administrada por el cliente. Para más detalles, consulte ABAC para AWS KMS y Usar alias para controlar el acceso a las claves KMS.

Para obtener más información sobre cómo controlar el acceso a todas las operaciones de AWS KMS, consulte Referencia de permisos.

Los permisos para crear y administrar alias funcionan de la siguiente manera.

kms: CreateAlias

Para crear un alias, la entidad principal necesita los siguientes permisos tanto para el alias como para la clave KMS asociada.

- `kms:CreateAlias` para el alias. Proporcione este permiso en una política de IAM adjunta a la entidad principal que tiene permiso para crear el alias.

  En la siguiente declaración de política de ejemplo se especifica un alias en particular en un elemento `Resource`. Pero puede enumerar varios ARN de alias o especificar un patrón de alias, como "test*". También puede especificar un valor `Resource` de `"*"` para permitir que la entidad principal cree cualquier alias en la cuenta y región. El permiso para crear un alias también se puede incluir en un permiso `kms:Create*` para todos los recursos de una cuenta y región.

```
{
  "Sid": "IAMPolicyForAnAlias",
  "Effect": "Allow",
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"
}
```

- `kms:CreateAlias` para la clave KMS. Este permiso debe proporcionarse en una política de claves o en una política de IAM que se delega desde la política de claves.

```
{
  "Sid": "Key policy for 1234abcd-12ab-34cd-56ef-1234567890ab",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"},
  "Action": [
    "kms:CreateAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Puede utilizar claves de condición para limitar las claves KMS que puede asociar a un alias. Por ejemplo, puede usar la clave de KeySpec condición kms: para permitir que el director cree alias únicamente en claves KMS asimétricas. Para obtener una lista completa de las claves de condiciones que puede utilizar para limitar los permisos `kms:CreateAlias` en recursos de clave KMS, consulteAWS KMS permisos.

kms: ListAliases

Para enumerar los alias de la cuenta y la región, la entidad principal debe tener el permiso `kms:ListAliases` en una política de IAM. Dado que esta política no está relacionada con ninguna clave o recurso de alias KMS en particular, el valor del elemento de recurso de la política debe ser `"*"`.

Por ejemplo, la siguiente declaración de política de IAM otorga el permiso a la entidad principal para enumerar todas las claves y alias KMS en la cuenta y la región.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource": "*"
  }
}
```

km: UpdateAlias

Para cambiar la clave KMS asociada a un alias, la entidad principal necesita tres elementos de permiso: uno para el alias, uno para la clave KMS actual y otro para la nueva clave KMS.

Por ejemplo, suponga que desea cambiar el alias `test-key` de la clave KMS con el ID de clave 1234abcd-12ab-34cd-56ef-1234567890ab a la clave KMS con el ID de clave 0987dcba-09fe-87dc-65ba-ab0987654321. En ese caso, incluya declaraciones de política similares a las de los ejemplos de esta sección.

- `kms:UpdateAlias` para el alias. Puede proporcionar este permiso en una política de IAM que se asocia a la entidad principal. La siguiente política de IAM especifica un alias concreto. Pero puede

enumerar varios ARN de alias o especificar un patrón de alias, como `"test*"`. También puede especificar un valor `Resource` de `"*"` para permitir que la entidad principal actualice cualquier alias en la cuenta y región.

```
{
  "Sid": "IAMPolicyForAnAlias",
  "Effect": "Allow",
  "Action": [
    "kms:UpdateAlias",
    "kms:ListAliases",
    "kms:ListKeys"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"
}
```

- `kms:UpdateAlias` para la clave KMS que está actualmente asociada con el alias. Este permiso debe proporcionarse en una política de claves o en una política de IAM que se delega desde la política de claves.

```
{
  "Sid": "Key policy for 1234abcd-12ab-34cd-56ef-1234567890ab",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"},
  "Action": [
    "kms:UpdateAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

- `kms:UpdateAlias` para la clave KMS que la operación asocia con el alias. Este permiso debe proporcionarse en una política de claves o en una política de IAM que se delega desde la política de claves.

```
{
  "Sid": "Key policy for 0987dcba-09fe-87dc-65ba-ab0987654321",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"},
  "Action": [
    "kms:UpdateAlias",
    "kms:DescribeKey"
  ],
```

```
  "Resource": "*"
}
```

Puede usar claves de condición para limitar una o ambas claves KMS en una operación `UpdateAlias`. Por ejemplo, puede usar una clave de ResourceAliases condición kms: para permitir que el director actualice los alias solo cuando la clave KMS de destino ya tenga un alias concreto. Para obtener una lista completa de las claves de condiciones que puede utilizar para limitar el permiso `kms:UpdateAlias` en un recurso de clave KMS, consulte AWS KMS permisos.

kms: DeleteAlias

Para eliminar un alias, la entidad principal necesita permiso para el alias y para la clave KMS asociada.

Como siempre, debe tener precaución al dar permiso a las entidades principales para eliminar un recurso. Sin embargo, eliminar un alias no afecta a la clave KMS asociada. Aunque puede causar un error en una aplicación que se basa en el alias, si elimina un alias por error, puede volver a crearlo.

- `kms:DeleteAlias` para el alias. Proporcione este permiso en una política de IAM adjunta la entidad principal que tiene permiso para eliminar el alias.

  En la siguiente declaración de política de ejemplo se especifica el alias de un elemento `Resource`. Pero puede enumerar varios ARN de alias o especificar un patrón de alias, como `"test*"`. También puede especificar un valor `Resource` de `"*"` para permitir que la entidad principal elimine cualquier alias en la cuenta y región.

  ```
  {
    "Sid": "IAMPolicyForAnAlias",
    "Effect": "Allow",
    "Action": [
      "kms:CreateAlias",
      "kms:UpdateAlias",
      "kms:DeleteAlias"
    ],
    "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"
  }
  ```

- `kms:DeleteAlias` para la clave KMS asociada. Este permiso debe proporcionarse en una política de claves o en una política de IAM que se delega desde la política de claves.

```
{
  "Sid": "Key policy for 1234abcd-12ab-34cd-56ef-1234567890ab",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/KMSAdminUser"
  },
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

Limitar los permisos de alias

Puede utilizar claves de condición para limitar los permisos de alias cuando el recurso es una clave KMS. Por ejemplo, la siguiente política de IAM permite operaciones de alias en claves KMS en una cuenta y región concretas. Sin embargo, utiliza la clave de KeyOrigin condición kms: para limitar aún más los permisos a las claves de KMS con material clave deAWS KMS.

Para obtener una lista completa de las claves de condiciones que puede utilizar para limitar el permiso de alias en un recurso de clave KMS, consulte AWS KMS permisos.

```
{
  "Sid": "IAMPolicyKeyPermissions",
  "Effect": "Allow",
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "AWS_KMS"
    }
  }
}
```

No puede usar claves de condición en una declaración de política donde el recurso es un alias. Para limitar los alias que una entidad principal puede administrar, utilice el valor del elemento `Resource` de la declaración de política de IAM que controla el acceso al alias. Por ejemplo, las siguientes declaraciones de política permiten que la entidad principal cree, actualice o elimine cualquier alias en el Cuenta de AWS y región a menos que el alias comience con `Restricted`.

```
{
  "Sid": "IAMPolicyForAnAliasAllow",
  "Effect": "Allow",
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/*"
},
{
  "Sid": "IAMPolicyForAnAliasDeny",
  "Effect": "Deny",
  "Action": [
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/Restricted*"
}
```

Usar alias para controlar el acceso a las claves KMS

Puede controlar el acceso a las claves KMS basándose en los alias asociados a la clave KMS. Para ello, utilice las claves de ResourceAliases condición kms: RequestAlias y kms:. Esta característica forma parte de la compatibilidad de AWS KMS para el control de acceso basado en atributos (ABAC).

La clave de condición `kms:RequestAlias` permite o deniega el acceso a una clave KMS basándose en el alias de una solicitud. La clave de condición `kms:ResourceAliases` permite o deniega el acceso a una clave KMS en función de los alias asociados a la clave KMS.

Estas características no le permiten identificar una clave KMS utilizando un alias en el elemento `resource` de una declaración de política. Cuando un alias es el valor de un elemento `resource`, la política se aplica al recurso de alias, no a ninguna clave KMS que pueda estar asociada con él.

> **Note**
>
> Puede que transcurran cinco minutos hasta que los cambios de etiqueta y alias afecten a la autorización de clave KMS. Los cambios recientes pueden ser visibles en las operaciones de API antes de que afecten a la autorización.

Cuando utilice alias para controlar el acceso a las claves KMS, tenga en cuenta lo siguiente:

- Utilice alias para reforzar las prácticas recomendadas de acceso con privilegio mínimo. Dar a las entidades principales de IAM sólo los permisos que necesitan para las claves KMS que deben usar o administrar. Por ejemplo, utilice alias para identificar las claves KMS utilizadas en un proyecto. A continuación, dé permiso al equipo del proyecto para usar solo claves KMS con los alias del proyecto.
- Tenga cuidado al dar a las entidades principales los permisos `kms:CreateAlias`, `kms:UpdateAlias`, o `kms:DeleteAlias` que les permiten agregar, editar y eliminar alias. Cuando utiliza alias para controlar el acceso a las claves KMS, cambiar un alias puede dar permiso a las entidades principales para usar claves KMS que de otro modo no tenían permiso para usar. También puede denegar el acceso a las claves KMS que otras entidades principales requieren para realizar sus trabajos.
- Revise las entidades principales de su Cuenta de AWS que actualmente tienen permiso para administrar alias y ajustar los permisos, si es necesario. Los administradores de claves que no tienen permiso para cambiar políticas de claves o crear concesiones pueden controlar el acceso a claves KMS si tienen permiso para administrar alias.

  Por ejemplo, la consola default key policy for key administrators (política de claves predeterminada para administradores de claves) incluye los permisos `kms:CreateAlias`, `kms:DeleteAlias`, y `kms:UpdateAlias`. Las políticas de IAM pueden dar permisos de alias para todas las claves KMS de su Cuenta de AWS. Por ejemplo, la política AWSKeyManagementServicePowerUseradministrada permite a los directores crear, eliminar y enumerar los alias de todas las claves de KMS, pero no actualizarlos.
- Antes de establecer una política que dependa de un alias, revise los alias de las claves KMS de su Cuenta de AWS. Asegúrese de que la política sólo se aplica a los alias que desea incluir. Usa CloudTrail registros y CloudWatch alarmas para avisarte de los cambios de alias que puedan afectar al acceso a tus claves de KMS. Además, la ListAliasesrespuesta incluye la fecha de creación y la fecha de la última actualización de cada alias.

- Las condiciones de política de alias utilizan la coincidencia de patrones; no están vinculadas a una instancia concreta de un alias. Una política que utiliza claves de condición basadas en alias afecta a todos los alias nuevos y existentes que coincidan con el patrón. Si elimina y vuelve a crear un alias que coincida con una condición de política, la condición se aplica al nuevo alias, tal como lo hizo con el anterior.

La clave de condición `kms:RequestAlias` se basa en el alias especificado explícitamente en una solicitud de operación. La clave de condición `kms:ResourceAliases` depende de los alias asociados a una clave KMS, aunque no aparezcan en la solicitud.

km: RequestAlias

Permitir o denegar el acceso a una clave KMS basada en el alias que identifica la clave KMS en una solicitud. Puede utilizar la clave de RequestAlias condición kms: en una política clave o en una política de IAM. Se aplica a las operaciones que utilizan un alias para identificar una clave de KMS en una solicitud, es decir, las operaciones criptográficas DescribeKey, y. GetPublicKey No es válido para operaciones de alias, como CreateAliaso DeleteAlias.

En la clave de condición, especifique un nombre de alias o patrón de nombre de alias. No puede especificar un ARN de alias.

Por ejemplo, la siguiente declaración de política permite a la entidad principal utilizar las operaciones especificadas en la clave KMS. El permiso solo será efectivo cuando la solicitud utiliza un alias que incluye `alpha` para identificar la clave KMS.

```
{
  "Sid": "Key policy using a request alias condition",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/alpha-developer"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:RequestAlias": "alias/*alpha*"
```

```
    }
  }
}
```

La siguiente solicitud de ejemplo de una entidad principal autorizada cumpliría la condición. Sin embargo, una solicitud que utilizó un ID de clave, unARN de clave, o un alias diferente no cumpliría la condición, incluso si estos valores identificaban la misma clave KMS.

```
$ aws kms describe-key --key-id "arn:aws:kms:us-west-2:111122223333:alias/project-
alpha"
```

kms: ResourceAliases

Permitir o denegar el acceso a una clave KMS basándose en los alias asociados a la clave KMS, incluso si el alias no se utiliza en una solicitud. La clave de ResourceAliases condición kms: le permite especificar un alias o un patrón de alias, por ejemplo`alias/test*`, para poder utilizarlos en una política de IAM para controlar el acceso a varias claves de KMS en la misma región. Es válido para cualquier operación AWS KMS que utiliza una clave KMS.

Por ejemplo, la siguiente política de IAM permite a las entidades principales administrar la rotación automática de claves en las claves KMS en dos Cuentas de AWS. Sin embargo, el permiso sólo se aplica a las claves KMS asociadas con alias que comienzan con `restricted`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AliasBasedIAMPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:EnableKeyRotation",
        "kms:DisableKeyRotation",
        "kms:GetKeyRotationStatus"
      ],
      "Resource": [
        "arn:aws:kms:*:111122223333:key/*",
        "arn:aws:kms:*:444455556666:key/*"
      ],
      "Condition": {
        "ForAnyValue:StringLike": {
          "kms:ResourceAliases": "alias/restricted*"
```

```
        }
      }
    }
  ]
}
```

La condición `kms:ResourceAliases` es una condición del recurso, no de la solicitud. Como tal, una solicitud que no especifique el alias puede cumplir la condición.

La siguiente solicitud de ejemplo, que especifica un alias coincidente, satisface la condición.

```
$ aws kms enable-key-rotation --key-id "alias/restricted-project"
```

Sin embargo, la solicitud de ejemplo siguiente también satisface la condición, siempre que la clave KMS especificada tenga un alias que comience con `restricted`, incluso si ese alias no se usa en la solicitud.

```
$ aws kms enable-key-rotation --key-id "1234abcd-12ab-34cd-56ef-1234567890ab"
```

Búsqueda de alias en registros de AWS CloudTrail

Puede usar un alias para representar un AWS KMS key en una operación de la API de AWS KMS. Cuando lo haga, el alias y la clave ARN de la clave KMS se registran en la entrada de registro AWS CloudTrail del evento. El alias aparece en el campo `requestParameters`. El ARN de clave aparece en el campo `resources`. Esto es así incluso cuando un servicio AWS utiliza un Clave administrada de AWS en su cuenta.

Por ejemplo, la siguiente GenerateDataKeysolicitud utiliza el `project-key` alias para representar una clave de KMS.

```
$ aws kms generate-data-key --key-id alias/project-key --key-spec AES_256
```

Cuando esta solicitud se registra en el CloudTrail registro, la entrada del registro incluye el alias y la clave ARN de la clave KMS real que se utilizó.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDE",
```

```
        "arn": "arn:aws:iam::111122223333:role/ProjectDev",
        "accountId": "111122223333",
        "accessKeyId": "FFHIJ",
        "userName": "example-dev"
    },
    "eventTime": "2020-06-29T23:36:41Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.205.123.000",
    "userAgent": "aws-cli/1.18.89 Python/3.6.10
 Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.12",
    "requestParameters": {
        "keyId": "alias/project-key",
        "keySpec": "AES_256"
    },
    "responseElements": null,
    "requestID": "d93f57f5-d4c5-4bab-8139-5a1f7824a363",
    "eventID": "d63001e2-dbc6-4aae-90cb-e5370aca7125",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


Para obtener más información sobre AWS KMS las operaciones de registro en CloudTrail los registros, consulteRegistrar llamadas a la AWS KMS API con AWS CloudTrail.

Consultar claves

Puede utilizar la AWS Management Console o la API de AWS Key Management Service (AWS KMS) para ver AWS KMS keys en cada cuenta y región, incluidas las claves KMS que administra y las claves KMS administradas por AWS.

Temas

Visualización de las claves KMS en la consola

En la AWS Management Console, puede ver las listas de las claves KMS y detalles sobre cada una de ellas.

> **Note**
>
> La consola de AWS KMS muestra las claves KMS que tiene permitido ver en la cuenta y en la región. Las claves KMS en otras Cuentas de AWS no aparecen en la consola, incluso si tiene permiso para verlas, administrarlas y usarlas. Para ver las claves de KMS en otras cuentas, utilice la DescribeKeyoperación.

Temas

Navegar hasta las tablas de claves

Las AWS KMS keys de cada cuenta y región se muestran en tablas. Hay tablas separadas para las claves KMS que crea y las claves KMS que los servicios de AWS crean para usted.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.

3. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente). Si desea ver las claves de su cuenta que AWS crea y administra, en el panel de navegación, elija claves administradas por AWS. Para obtener información sobre los distintos tipos de claves KMS, consulte AWS KMS keys.

> **Tip**
>
> Para ver Claves administradas por AWS a las que les falta un alias, utilice la página Customer managed keys (Claves administradas por el cliente).
> La consola de AWS KMS también muestra los almacenes de claves personalizadas de la cuenta y la región. Las claves KMS que crea en los almacenes de claves personalizadas aparecen en la página Customer managed keys (Claves administradas por el cliente). Para obtener información acerca de los almacenes de claves personalizadas, consulte Almacenes de claves personalizados.

Navegar a los detalles de la clave

Hay una página de detalles para cada AWS KMS key en la cuenta y la región. La página de detalles muestra la sección Configuración general para la clave KMS e incluye pestañas que permiten a los usuarios autorizados ver y administrar la Configuración criptográfica y la Política de claves para la clave. En función del tipo de clave, la página de detalles también puede incluir las pestañas Alias, Material de claves, Rotación de claves, Clave pública, Regionalidad y Etiquetas.

Navegar a la página de detalles de clave de una clave KMS.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente). Si desea ver las claves de su cuenta que AWS crea y administra, en el panel de navegación, elija claves administradas por AWS. Para obtener información sobre los distintos tipos de claves KMS, consulte AWS KMS key.
4. Para abrir la página de detalles de clave, elija el ID de clave o el alias de la clave KMS.

Si la clave KMS tiene varios alias, un resumen de alias (+n más) aparece junto al nombre de uno de los alias. Elegir el resumen de alias le llevará directamente a la pestaña Alias en la página de detalles de clave.

Ordenar y filtrar las claves KMS

Para facilitar la búsqueda de las claves KMS en la consola, puede ordenarlas y filtrarlas.

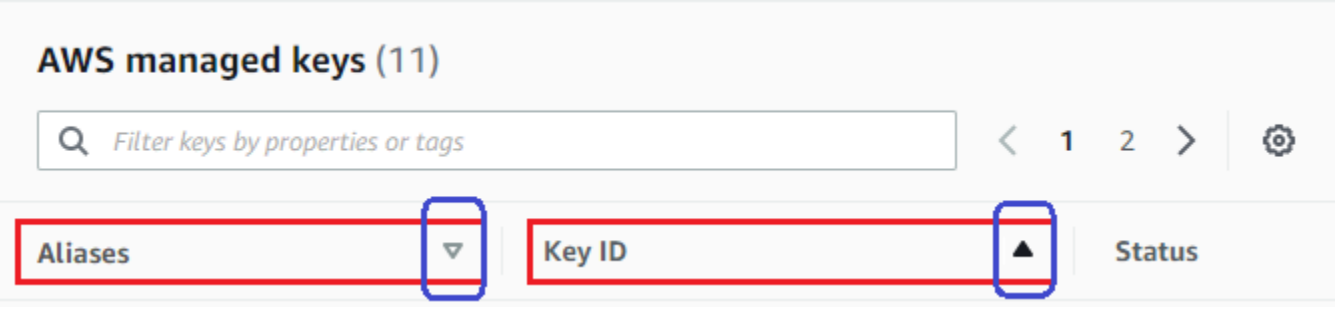
Ordenar

Puede ordenar las claves KMS administradas por el cliente en orden ascendente o descendente por sus valores de columna. Esta función ordena todas las claves KMS de la tabla, aunque no aparezcan en la página de la tabla actual.

Las columnas que se pueden ordenar aparecen indicadas con una flecha que aparece junto al nombre de la columna. En la página Claves administradas por AWS, puede ordenar por Alias o ID de clave. En la página Customer managed keys (Claves administradas por el cliente), puede ordenar por Alias, Key ID (ID de clave) o Key type (Tipo de clave).

Para ordenar en orden ascendente, seleccione el encabezado de la columna hasta que la flecha apunte hacia arriba. Para ordenar en orden descendente, seleccione el encabezado de la columna hasta que la flecha apunte hacia abajo. Puede ordenar solo por una columna cada vez.

Por ejemplo, puede ordenar las claves KMS en orden ascendente por ID de clave en lugar de por alias, que es el valor predeterminado.



Cuando ordena las claves KMS en la página Customer managed keys (Claves administradas por cliente) en orden ascendente por Key type (Tipo de clave), todas las claves asimétricas se muestran antes que todas las claves simétricas.

Filtro

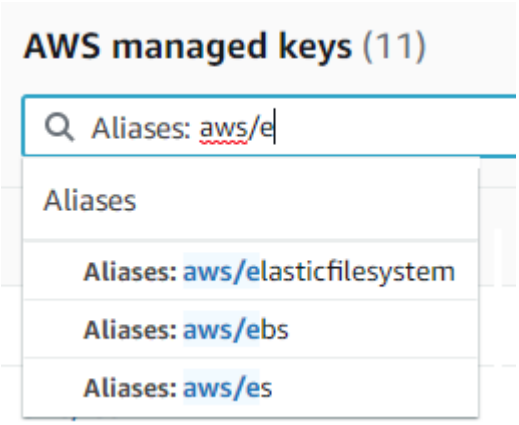
Puede filtrar las claves KMS por sus valores de propiedad o etiquetas. El filtro se aplica a todas las claves KMS de la tabla, aunque no aparezcan en la página de la tabla actual. El filtro no distingue entre mayúsculas y minúsculas.

Las propiedades que se pueden filtrar se enumeran en el cuadro de filtro. En la página Claves administradas por AWS , puede filtrar por alias e ID de clave. En la página Customer managed keys (Claves administradas por el cliente), puede filtrar por las propiedades de alias, ID de clave, tipo de clave y por etiquetas.

- En la página Claves administradas por AWS, puede filtrar por alias e ID de clave.
- En la página Customer managed keys (Claves administradas por el cliente), puede filtrar por etiquetas o por las propiedades de alias, ID de clave, tipo de clave o regionalidad.

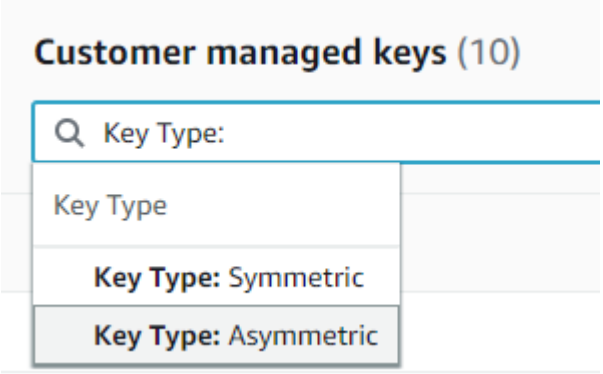
Para filtrar por un valor de propiedad, elija el filtro, seleccione el nombre de propiedad y, a continuación, selecciónelo de la lista de valores de propiedad reales. Para filtrar por una etiqueta, elija la clave de etiqueta y, a continuación, elija de la lista de valores reales de etiqueta. Después de seleccionar una clave de propiedad o de etiqueta, también puede introducir una parte o el valor de la propiedad completo. Verá una vista previa de los resultados antes de tomar su decisión.

Por ejemplo, para mostrar las claves KMS con un nombre de alias que contenga `aws/e`, seleccione el cuadro de filtro, seleccione Alias, introduzca `aws/e` y, a continuación, pulse `Enter` o `Return` para agregar el filtro.

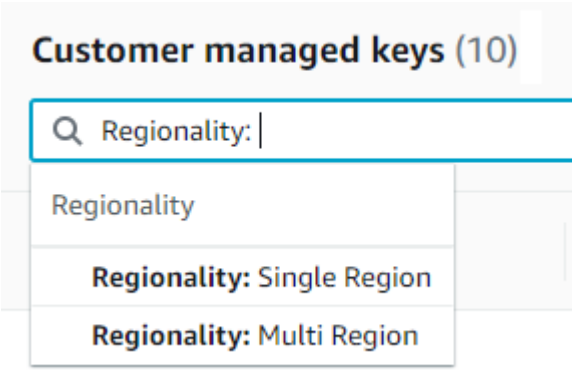


Para mostrar solo las clave KMS asimétricas en la página Customer managed keys (Claves administradas por cliente), haga clic en el cuadro de filtro, elija Key type (Tipo de clave) y, a continuación, elija Key type: Asymmetric (Tipo de clave: Asimétrica). La opción Asymmetric (Asimétrica) solo aparece cuando tiene claves KMS asimétricas en la tabla. Para obtener más

información acerca de cómo identificar claves KMS asimétricas, consulte Identificación de claves KMS asimétricas.



Para mostrar solo las claves de varias regiones, en la página Customer managed keys (Claves adminsitradas por el cliente), elija el cuadro de filtro, seleccione Regionality (Regionalidad) y luego elija Regionality: Multi-Region (Regionalidad: varias regiones). La opción Multi-Region (Varias regiones) solo aparece cuando tiene claves de varias regiones en la tabla. Para obtener más información acerca de cómo identificar las claves de varias regiones, consulte Visualización de claves de varias regiones.

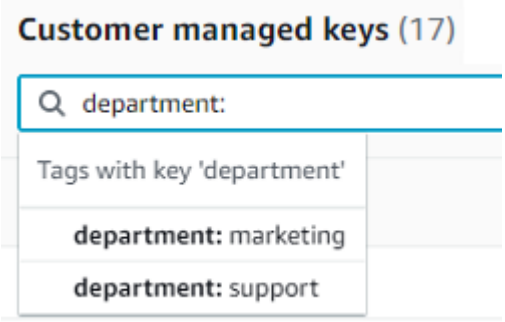


El filtrado de etiquetas es un poco diferente. Para mostrar solo las claves KMS con una etiqueta concreta, elija el cuadro de filtro, elija la clave de etiqueta y, a continuación, elija entre los valores de etiqueta reales. También puede introducir una parte o el valor de la etiqueta completo.

La tabla resultante muestra todas las claves KMS con la etiqueta elegida. Sin embargo, no muestra la etiqueta. Para ver la etiqueta, elija el ID de clave o alias de la clave KMS y, en su página de detalles, elija la pestaña Tags (Etiquetas). Las pestañas aparecen debajo de la sección General configuration (Configuración general).

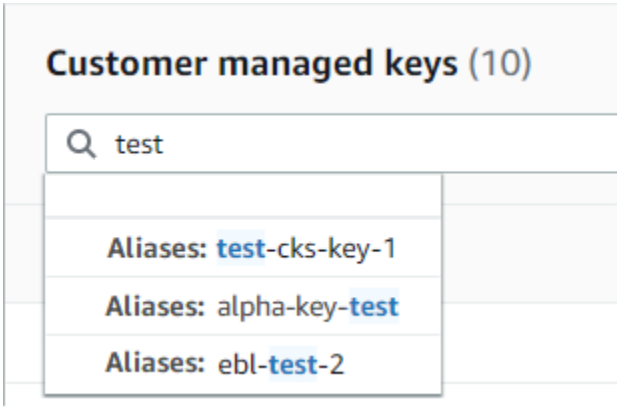
Este filtro requiere la clave y el valor de la etiqueta. No encontrará claves KMS escribiendo solo la clave de etiqueta o solo su valor. Para filtrar las etiquetas por la totalidad o parte de la clave

o el valor de la etiqueta, utilice la ListResourceTagsoperación para obtener las claves de KMS etiquetadas y, a continuación, utilice las funciones de filtrado de su lenguaje de programación. Para ver un ejemplo, consulte ListResourceTags: Obtenga las etiquetas de las claves de KMS.

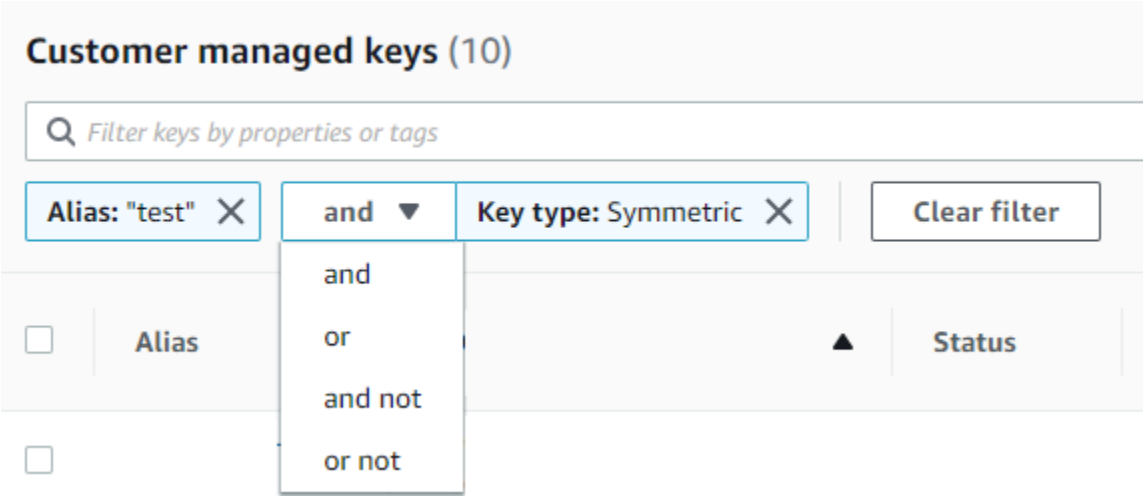


Para buscar texto, introduzca una parte o todo el alias, el ID de clave, el tipo de clave o la clave de etiqueta en el cuadro de filtro. (Después de seleccionar la clave de etiqueta, puede buscar un valor de etiqueta). Verá una vista previa de los resultados antes de tomar su decisión.

Por ejemplo, para mostrar claves KMS con `test` en sus claves de etiqueta o propiedades filtrables, escriba `test` en el cuadro de filtro. La vista previa muestra las claves KMS que seleccionará el filtro. En este caso, `test` solo aparece en la propiedad Alias.



Puede usar varios filtros al mismo tiempo. Cuando agrega filtros adicionales, también puede seleccionar un operador lógico.

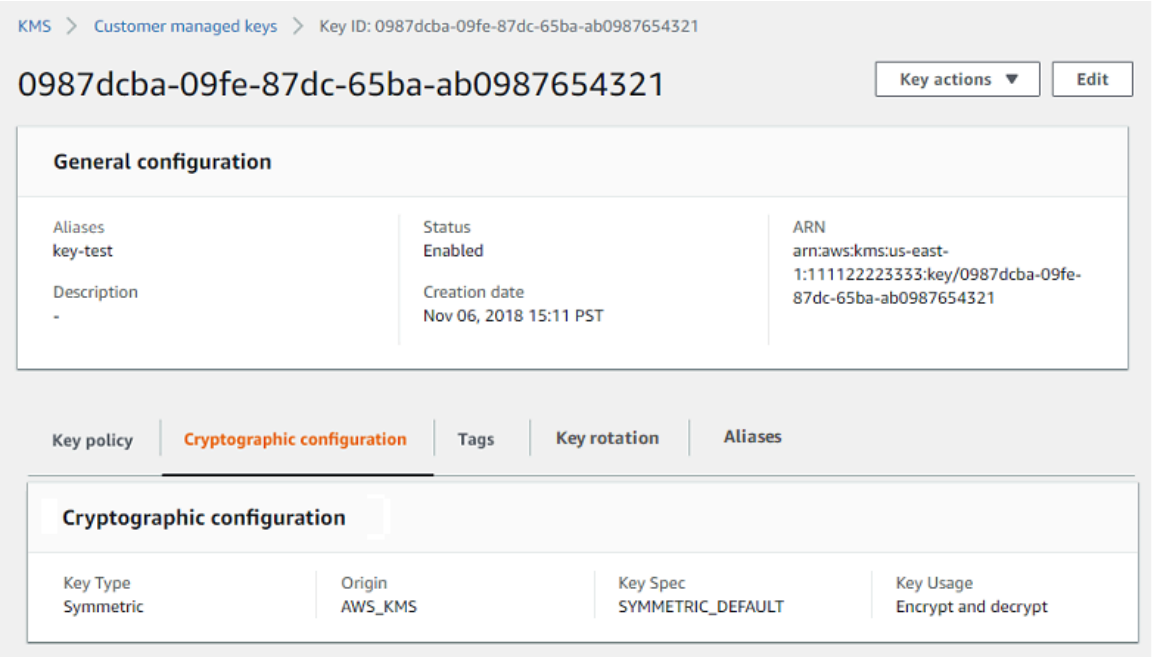


Mostrar detalles de clave KMS

En la página de detalles de cada clave KMS se muestran las propiedades de la clave KMS. Difiere ligeramente de los diferentes tipos de claves KMS.

Para mostrar información detallada sobre una clave KMS, haga clic en la página Claves administradas por AWS o Customer managed keys (Claves administradas por el cliente), elija el alias o el ID de clave de la clave KMS.

La página de detalles de una clave KMS incluye una Configuración general en la que se muestran las propiedades básicas de la clave KMS. Esto también incluye pestañas en las que puede ver y editar propiedades de la clave KMS, como su política de claves, configuración criptográfica, etiquetas, material de claves (para claves KMS con material de clave importado), rotación de claves (para claves KMS de cifrado simétricas), regionalidad (claves de varias regiones) y su clave pública (para claves KMS asimétricas).



En la siguiente lista se describen los campos de la visualización detallada, incluido el campo de las pestañas. Algunos de estos campos también están disponibles como columnas en la visualización de tabla.

Alias

Dónde: Pestañas de Alias

Un nombre fácil de recordar para la clave KMS. Puede utilizar un alias para identificar la clave KMS en la consola y en algunos API de AWS KMS. Para obtener más detalles, consulte Uso de alias.

La pestaña de Alias muestra todos los alias asociados con la clave KMS en la región y la Cuenta de AWS.

ARN

Dónde: sección de configuración general

El Nombre de recurso de Amazon (ARN) de la clave de cifrado. Este valor únicamente identifica la clave KMS. Puede utilizarlo para identificar la clave KMS en las operaciones de la API de AWS KMS.

Estado de la conexión

Indica si un almacén de claves personalizado está conectado a su almacén de claves de respaldo. Este campo aparece únicamente cuando la clave de KMS se crea en un almacén de claves personalizado.

Para obtener información sobre los valores de este campo, consulta ConnectionStatela referencia de la AWS KMS API.

Fecha de creación

Dónde: sección de configuración general

La fecha y hora en que se creó la clave KMS. Este valor se muestra en la hora local del dispositivo. La zona horaria no varía en función de la región.

A diferencia de Expiration (Vencimiento), la creación se refiere únicamente a la clave KMS, no a su material de claves.

ID del clúster de CloudHSM

Dónde: pestaña de Configuración criptográfica

ID del clúster de AWS CloudHSM que contiene el material de claves de la clave KMS. Este campo aparece únicamente cuando la clave de KMS se crea en un almacén de claves personalizado.

Si elije en el ID del clúster de CloudHSM, se abre la página Clusters (Clústeres) de la consola de AWS CloudHSM.

ID del almacén de claves personalizadas

Dónde: pestaña de Configuración criptográfica

ID del almacén de claves personalizadas que contiene la clave KMS. Este campo aparece únicamente cuando la clave de KMS se crea en un almacén de claves personalizado.

Si hace clic en el ID el almacén de claves personalizadas, se abre la página Custom key stores (Almacenes de claves personalizadas) en la consola de AWS KMS.

Nombre del almacén de claves personalizadas

Dónde: pestaña de Configuración criptográfica

El nombre del almacén de claves personalizadas que contiene la clave KMS. Este campo aparece únicamente cuando la clave de KMS se crea en un almacén de claves personalizado.

Tipo de almacén de claves personalizado

Dónde: pestaña de Configuración criptográfica

Indica si el almacén de claves personalizado es un almacén de claves de AWS CloudHSM o un almacén de claves externo. Este campo aparece únicamente cuando la clave de KMS se crea en un almacén de claves personalizado.

Descripción

Dónde: sección de configuración general

Una descripción breve y opcional de la clave KMS que puede escribir y editar. Para agregar o actualizar la descripción de una clave administrada por el cliente, sobre General Configuration (Configuración general), seleccione Edit (Editar).

Algoritmos de cifrado

Dónde: pestaña de Configuración criptográfica

Enumera los algoritmos de cifrado que se pueden utilizar con la clave KMS en AWS KMS. Este campo aparece únicamente cuando el Key type (Tipo de clave) es Asymmetric (Asimétrico) y cuando el Key usage (Uso de la clave) es Encrypt and decrypt (Cifrar y descifrar). Para obtener información acerca de los algoritmos de cifrado que admite AWS KMS, consulte Especificación de clave SYMMETRIC_DEFAULT y Especificaciones de clave de RSA para el cifrado y el descifrado.

Fecha de vencimiento

Dónde: pestaña de Material de clave

Fecha y hora en la que el material de claves de la clave KMS vence. Este campo aparece únicamente en las claves KMS con material de claves importado, es decir, cuando el Origin (Origen) es External (Externo) y la clave KMS contiene material de claves que vence.

ID de clave externa

Dónde: pestaña de Configuración criptográfica

El ID de la clave externa que está asociado a una clave de KMS en un almacén de claves externo. Este campo solo aparece para las claves de KMS de un almacén de claves externo.

Estado de clave externa

Dónde: pestaña de Configuración criptográfica

El estado más reciente que el proxy del almacén de claves externo informó para la clave externa asociada a la clave de KMS. Este campo solo aparece para las claves de KMS de un almacén de claves externo.

Uso de clave externa

Dónde: pestaña de Configuración criptográfica

Las operaciones criptográficas que están habilitadas en la clave externa asociada a la clave de KMS. Este campo solo aparece para las claves de KMS de un almacén de claves externo.

Política de claves

Dónde: pestaña de Política de clave

Controla el acceso a la clave KMS junto con las políticas de IAM y las concesiones. Cada clave KMS tiene una política de claves. Es el único elemento de autorización obligatorio. Para cambiar la política de claves de una clave administrada por el cliente, en la pestaña Key policy (Política de claves), seleccione Edit (Editar). Para obtener más detalles, consulte the section called “Políticas de claves”.

Rotación de claves

Dónde: pestaña de Rotación de claves

Habilita y desactiva la rotación automática del material de claves en una clave KMS administrada por el cliente. Para cambiar el estado de la rotación de claves de una clave administrada por el cliente, utilice la casilla de verificación que se encuentra en la pestaña Key rotation (Rotación de claves).

No puede habilitar ni desactivar la rotación del material de claves en una Clave administrada de AWS. Las Claves administradas por AWS rotan automáticamente cada año.

Especificación de clave

Dónde: pestaña de Configuración criptográfica

El tipo de material de claves de la clave KMS. AWS KMS admite las claves KMS de cifrado simétricas (SYMMETRIC_DEFAULT), claves KMS HMAC de diferentes longitudes, claves KMS

para claves RSA de diferentes largos, y claves de curva elíptica con diferentes curvas. Para obtener más detalles, consulte Especificación de clave.

Tipo de clave

Dónde: pestaña de Configuración criptográfica

Indica si la clave KMS es Symmetric (Simétrica) o Asymmetric (Asimétrica).

Uso de claves

Dónde: pestaña de Configuración criptográfica

Indica si una clave KMS se puede utilizar para Encrypt and decrypt (Cifrar y descifrar), Sign and verify (Firmar y verificar) o Generate and verify MAC (Generar y verificar MAC). Para obtener más detalles, consulte Uso de claves.

Origen

Dónde: pestaña de Configuración criptográfica

El origen del material de claves de la clave KMS. Los valores válidos son:

- AWS KMS para material de claves que genera AWS KMS
- AWS CloudHSM para claves de KMS en el almacén de claves de AWS CloudHSM
- Externo para material de claves importado (BYOK)
- Almacén de claves externo para claves de KMS en un almacén de claves externo

Algoritmos de MAC

Dónde: pestaña de Configuración criptográfica

Enumera los algoritmos MAC que se pueden utilizar con una clave KMS HMAC en AWS KMS. Este campo aparece únicamente cuando la Especificación de la clave es una especificación de la clave HMAC (HMAC_*). Para obtener información acerca de los algoritmos MAC de firma que admite AWS KMS, consulte Especificaciones de la clave para las claves KMS HMAC.

Clave principal

Dónde: pestaña de Regionalidad

Indica que esta clave KMS es una clave principal de varias regiones. Los usuarios autorizados pueden utilizar esta sección para cambiar la clave principal a una clave de varias regiones

relacionada diferente. Este campo aparece únicamente cuando la clave KMS es una clave principal de varias regiones.

Clave pública

Dónde: pestaña de Clave pública

Muestra la clave pública de una clave KMS asimétrica. Los usuarios autorizados pueden utilizar esta pestaña para copiar y descargar la clave pública.

Regionalidad

Dónde: pestañas Sección de configuración general y Regionalidad

Indica si una clave KMS es una clave de una sola región, una clave principal de varias regiones o una clave de réplica de varias regiones. Este campo aparece únicamente cuando la clave KMS es una clave de varias regiones.

Claves de varias regiones relacionadas

Dónde: pestaña de Regionalidad

Muestra todas las claves de réplica y primaria de varias regiones relacionadas, excepto la clave KMS actual. Este campo aparece únicamente cuando la clave KMS es una clave de varias regiones.

En la sección Claves de varias regiones relacionadas de una clave principal, los usuarios autorizados pueden crear nuevas claves de réplica.

Clave de réplica

Dónde: pestaña de Regionalidad

Indica que esta clave KMS es una clave de réplica de varias regiones. Este campo aparece únicamente cuando la clave KMS es una clave de réplica de varias regiones.

Algoritmos de firma

Dónde: pestaña de Configuración criptográfica

Enumera los algoritmos de firma que se pueden utilizar con la clave KMS en AWS KMS. Este campo aparece únicamente cuando el Key type (Tipo de clave) es Asymmetric (Asimétrico) y cuando el Key usage (Uso de la clave) es Sign and verify (Firmar y verificar). Para obtener

información acerca de los algoritmos de firma que admite AWS KMS, consulte Especificaciones de clave de RSA para la firma y la verificación y Especificaciones de clave de curva elíptica.

Status

Dónde: sección de configuración general

El estado de la clave KMS. Puede utilizar la clave KMS en operaciones criptográficas solo cuando el estado es Enabled (Habilitado). Para obtener una descripción detallada de cada estado de clave KMS y su impacto en las operaciones que puede ejecutar en la clave KMS, consulte Estados clave de AWS KMS las claves.

Etiquetas

Dónde: pestaña Etiquetas

Pares clave-valor opcionales que describen la clave KMS. Para agregar o cambiar las etiquetas de una clave KMS, en la pestaña Tags (Etiquetas), seleccione Edit (Editar).

Cuando se agregan etiquetas a los recursos de AWS, AWS genera un informe de asignación de costos con el uso y los costos agregados por etiquetas. Las etiquetas también pueden utilizarse para controlar el acceso a una clave KMS. Para obtener información acerca del etiquetado de claves KMS, consulte Etiquetado de claves y ABAC para AWS KMS.

Personalización de las tablas clave KMS

Puede personalizar las tablas que aparecen en las páginas Claves administradas por AWS y Claves administradas por el cliente en la AWS Management Console para adaptarlo a sus necesidades. Puede seleccionar las columnas de la tabla, el número de AWS KMS keys de cada página (Page size [Tamaño de página]) y el ajuste de texto. La configuración que seleccione se guarda cuando la confirma y se vuelve a aplicar cuando abre las páginas.

Personalización de las tablas clave KMS

1. En la página Claves administradas por AWS o Claves administradas por el cliente, elija el icono de configuración
   ()
   en la parte superior derecha de la página.
2. En la página Preferences (Preferencias), elija su configuración preferida y, a continuación, Confirm (Confirmar).

Considere utilizar la configuración Page size (Tamaño de página) para aumentar el número de clave KMS que se muestran en cada página, especialmente si suele utilizar un dispositivo que es fácil de desplazar.

Las columnas de datos que muestra pueden variar en función de la tabla, el rol de trabajo y los tipos de claves KMS de la cuenta y la región. En la siguiente tabla aparecen algunas sugerencias de configuración. Para obtener descripciones de las columnas, consulte Mostrar detalles de clave KMS.

Configuraciones de tabla clave KMS sugeridas

Puede personalizar las columnas que aparecen en la tabla de claves KMS para mostrar la información que necesita sobre sus claves KMS.

Claves administradas por AWS

De forma predeterminada, la tabla Clave administrada de AWS muestra las columnas Aliases (Alias), Key ID (ID de clave) y Status (Estado). Estas columnas son ideales para la mayoría de casos de uso.

Claves KMS de cifrado simétricas

Si utiliza únicamente las claves KMS de cifrado simétricas con el material de claves que genera AWS KMS, es probable que las columnas Aliases (Alias), Key ID (ID de clave), Status (Estado) y Creation date (Fecha de creación) sean las más útiles.

Claves KMS asimétricas

Si utiliza claves KMS asimétricas, además de las columnas Aliases (Alias), Key ID (ID de clave) y Status (Estado), debe considerar la adición de las columnas Key type (Tipo de clave), Key spec (Especificación de clave) y Key usage (Uso de clave). Estas columnas le mostrarán si una clave KMS es simétrica o asimétrica, el tipo de material de claves y si la clave KMS se puede utilizar para el cifrado o la firma.

Claves KMS HMAC

Si utiliza claves KMS HMAC, además de las columnas Aliases (Alias), Key ID (ID de clave) y Status (Estado), debe considerar la adición de las columnas Key spec (Especificación de clave) y Key usage (Uso de clave). Estas columnas le mostrarán si una clave KMS es una clave HMAC. Debido a que no puede ordenar las claves KMS por especificación de la clave o uso de claves, use alias y etiquetas para identificar sus claves HMAC y, a continuación, use las características de filtro de la consola de AWS KMS para filtrar por alias o etiquetas.

Material de claves importado

Si tiene claves KMS con material de claves importado, considere agregar las columnas Origen (Origen) y Expiration date (Fecha de vencimiento). Estas columnas le mostrarán si el material de claves de una clave KMS se importa o lo genera AWS KMS y cuándo vence el material de claves, si se da el caso. El campo Creation date (Fecha de creación) muestra la fecha en la que se creó la clave KMS (sin el material de claves). No refleja ninguna característica del material de claves.

Claves de los almacenes de claves personalizadas

Si tiene claves de KMS en almacenes de claves personalizados, considere agregar las columnas Origin (Origen) y Custom key store ID (ID del almacén de claves personalizado). Estas columnas muestran que la clave de KMS se encuentra en un almacén de claves personalizado, indican qué tipo de almacén es y lo identifican.

Claves para varias regiones

Si tiene claves para varias regiones, considere agregar la columna Regionality (Regionalidad). Esto muestra si una clave KMS es una clave de una sola región, una clave principal de varias regiones o una clave de réplica de varias regiones.

Visualización de claves KMS con la API

Puede utilizar la API de AWS Key Management Service (AWS KMS) para ver sus claves KMS. En esta sección se muestran varias operaciones que devuelven información detallada sobre las claves KMS existentes. En estos ejemplos se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Temas

- ListKeys: Obtenga el ID y el ARN de todas las claves de KMS
- DescribeKey: Obtenga información detallada sobre una clave de KMS
- GetKeyPolicy: Adjunte la política de claves a una clave de KMS
- ListAliases: Obtenga los nombres de alias y los ARN de las claves de KMS
- ListResourceTags: Obtenga las etiquetas de las claves de KMS

ListKeys: Obtenga el ID y el ARN de todas las claves de KMS

La ListKeysoperación devuelve el ID y el nombre de recurso de Amazon (ARN) de todas las claves de KMS de la cuenta y la región.

Por ejemplo, esta llamada a la operación `ListKeys` devuelve el ID y el ARN de todas las claves KMS de esta cuenta ficticia. Para ver ejemplos en varios lenguajes de programación, consulte Obtener ID de clave y ARN clave de claves KMS.

```
$ aws kms list-keys

{
  "Keys": [
    {
      "KeyArn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "KeyArn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
      "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321"
    },
    {
      "KeyArn": "arn:aws:kms:us-
east-2:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
      "KeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    }
}
```

DescribeKey: Obtenga información detallada sobre una clave de KMS

La DescribeKeyoperación devuelve detalles sobre la clave de KMS especificada. Para identificar la clave KMS, utilice el ID de la clave, ARN de la clave, nombre de alias o ARN del alias.

A diferencia de la ListKeysoperación, que muestra solo las claves KMS de la cuenta y región de la persona que llama, los usuarios autorizados pueden usar la `DescribeKey` operación para obtener detalles sobre las claves KMS de otras cuentas.

> **Note**
>
> La respuesta `DescribeKey` incluye tanto `KeySpec` como `CustomerMasterKeySpec` con los mismos valores. Este miembro `CustomerMasterKeySpec` está obsoleto.

Por ejemplo, esta llamada a `DescribeKey` devuelve información acerca de una clave KMS de cifrado simétrica. Los campos de la respuesta varían según la especificación de la AWS KMS key, el estado de la clave y el origen del material de la clave. Para ver ejemplos en varios lenguajes de programación, consulte Ver un AWS KMS key.

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
        "Enabled": true,
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
        "CreationDate": 1499988169.234,
        "MultiRegion": false,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

Este ejemplo llama a la operación `DescribeKey` en una clave KMS asimétrica utilizada para la firma y la verificación. La respuesta incluye los algoritmos de firma que AWS KMS admite para esta clave KMS.

```
$ aws kms describe-key --key-id 0987dcba-09fe-87dc-65ba-ab0987654321

{
    "KeyMetadata": {
        "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "Origin": "AWS_KMS",
        "Arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "KeyState": "Enabled",
```

```
        "KeyUsage": "SIGN_VERIFY",
        "CreationDate": 1569973196.214,
        "Description": "",
        "KeySpec": "ECC_NIST_P521",
        "CustomerMasterKeySpec": "ECC_NIST_P521",
        "AWSAccountId": "111122223333",
        "Enabled": true,
        "MultiRegion": false,
        "KeyManager": "CUSTOMER",
        "SigningAlgorithms": [
            "ECDSA_SHA_512"
        ]
    }
}
```

GetKeyPolicy: Adjunte la política de claves a una clave de KMS

La GetKeyPolicyoperación obtiene la política clave que se adjunta a la clave de KMS. Para identificar la clave KMS, utilice su ID o ARN de clave. Asimismo, debe especificar el nombre de política, que siempre es `default`. (Si la salida es difícil de leer, agregue la opción `--output text` al comando). `GetKeyPolicy` funciona solo en claves KMS de la cuenta y región de la persona que llama.

Para ver ejemplos en varios lenguajes de programación, consulte Obtener una política de claves.

```
$ aws kms get-key-policy --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --policy-name
 default

{
  "Version" : "2012-10-17",
  "Id" : "key-default-1",
  "Statement" : [ {
    "Sid" : "Enable IAM User Permissions",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

ListAliases: Obtenga los nombres de alias y los ARN de las claves de KMS

La ListAliasesoperación devuelve los alias de la cuenta y la región. El `TargetKeyId` en la respuesta muestra la ID de clave de la clave KMS a la que se refiere el alias, si la hay.

De forma predeterminada el comando ListAliases devuelve todos los alias de la cuenta y la región. Esto incluye los alias que ha creado y asociado a sus claves administradas por el cliente y los alias que AWS ha creado y asociado con Clave administrada de AWS en su cuenta. Puede reconocer los alias de AWS porque sus nombres tienen el formato `aws/<service-name>`, como `aws/dynamodb`.

La respuesta también podría incluir los alias sin el campo `TargetKeyId`, como, por ejemplo, el alias `aws/redshift` en este ejemplo. Estos son los alias predefinidos que AWS ha creado, pero aún no se han asociado con una clave KMS.

Para ver ejemplos en varios lenguajes de programación, consulte Mostrar alias.

```
$ aws kms list-aliases

{
    "Aliases": [
        {
            "AliasName": "alias/access-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1516435200.399,
            "LastUpdatedDate": 1516435200.399
        },
        {
            "AliasName": "alias/financeKey",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/financeKey",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1604958290.014,
            "LastUpdatedDate": 1604958290.014
        },
        {
            "AliasName": "alias/ECC-P521-Sign",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ECC-P521-Sign",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1693622000.704,
            "LastUpdatedDate": 1693622000.704
        },
        {
```

```
            "AliasName": "alias/ImportedKey",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ImportedKey",
            "TargetKeyId": "1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "CreationDate": 1493622000.704,
            "LastUpdatedDate": 1521097200.235
        },
        {
            "AliasName": "alias/aws/dynamodb",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/dynamodb",
            "TargetKeyId": "0987ab65-43cd-21ef-09ab-87654321cdef",
            "CreationDate": 1521097200.454,
            "LastUpdatedDate": 1521097200.454
        },
        {
            "AliasName": "alias/aws/ebs",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/ebs",
            "TargetKeyId": "abcd1234-09fe-ef90-09fe-ab0987654321",
            "CreationDate": 1466518990.200,
            "LastUpdatedDate": 1466518990.200
        },
        {
            "AliasName": "alias/aws/redshift",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/aws/redshift"
        },
    ]
}
```

Para obtener los alias que se refieren a una clave KMS determinada, utilice el parámetro `KeyId`. El valor del parámetro puede ser el ID de la clave o el ARN de la clave. No puede especificar un nombre de alias o ARN de alias.

El comando del siguiente ejemplo obtiene los alias que se refieren a una clave administrada por el cliente. Sin embargo, puede utilizar un comando como este para buscar los alias que se refieren a las Claves administradas por AWS también.

```
$ aws kms list-aliases --key-id arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321
{
    "Aliases": [
        {
            "AliasName": "alias/access-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/access-key",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
```

```
            "CreationDate": 1516435200.399,
            "LastUpdatedDate": 1516435200.399
        },
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/financeKey",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "AliasName": "alias/financeKey",
            "CreationDate": 1604958290.014,
            "LastUpdatedDate": 1604958290.014
        },
    ]
}
```

Para obtener solo los alias de los Claves administradas por AWS, utilice las características del lenguaje de programación para filtrar la respuesta.

```
$ aws kms list-aliases --query 'Aliases[?starts_with(AliasName, `alias/aws/`)]'
```

ListResourceTags: Obtenga las etiquetas de las claves de KMS

La ListResourceTagsoperación devuelve las etiquetas de la clave KMS especificada. La API devuelve etiquetas para una clave KMS, pero puede ejecutar el comando en un bucle para obtener etiquetas para todas las claves KMS de la cuenta y Región, o para un conjunto de claves KMS que seleccione. Esta API devuelve una página a la vez, por lo que si tiene numerosas etiquetas en numerosas claves KMS, es posible que tenga que usar el paginador en su lenguaje de programación para obtener todas las etiquetas que desee.

La operación `ListResourceTags` devuelve etiquetas para todas las claves KMS, pero las Clave administrada de AWS no están etiquetadas. Solo funciona en claves KMS de la cuenta y región de la persona que llama.

Para encontrar las etiquetas de una clave KMS, utilice la operación `ListResourceTags`. El parámetro `KeyId` es obligatorio. Acepta un ID de clave o ARN de clave. Antes de ejecutar este ejemplo, reemplace el ARN de clave de ejemplo por uno válido.

```
$  aws kms list-resource-tags --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
      {
    "Tags": [
        {
```

```
            "TagKey": "Department",
            "TagValue": "IT"
        },
        {
            "TagKey": "Purpose",
            "TagValue": "Test"
        }
    ],
    "Truncated": false
}
```

Es posible que desee utilizar la operación `ListResourceTags` para obtener todas las claves KMS de la cuenta y región con una etiqueta, clave de etiqueta o valor de etiqueta en particular. Para ello, utilice las características de filtrado de su lenguaje de programación.

Por ejemplo, el siguiente script de Bash usa las `ListResourceTags` operaciones ListKeysy para obtener todas las claves de KMS de la cuenta y la región con una clave de `Project` etiqueta. Ambas operaciones obtienen solo la primera página de resultados. Si tiene numerosas claves KMS o numerosas etiquetas, utilice las características de paginación de su idioma para obtener el resultado completo de cada operación. Antes de ejecutar este ejemplo, reemplace los ID de clave de ejemplo por otros válidos.

```
TARGET_TAG_KEY='Project'

for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text); do
  key_tags=$(aws kms list-resource-tags --key-id "$key" --query "Tags[?TagKey==\`
$TARGET_TAG_KEY\`]")
  if [ "$key_tags" != "[]" ]; then
    echo "Key: $key"
    echo "$key_tags"
  fi
done
```

El formato de la salida tendrá un formato semejante al de este ejemplo.

```
Key: 0987dcba-09fe-87dc-65ba-ab0987654321
[
    {
        "TagKey": "Project",
        "TagValue": "Gamma"
    }
```

```
]
Key: 1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d
[
    {
        "TagKey": "Project",
        "TagValue": "Alpha"
    }
]
Key: 0987ab65-43cd-21ef-09ab-87654321cdef
[
    {
        "TagKey": "Project",
        "TagValue": "Alpha"
    }
]
```

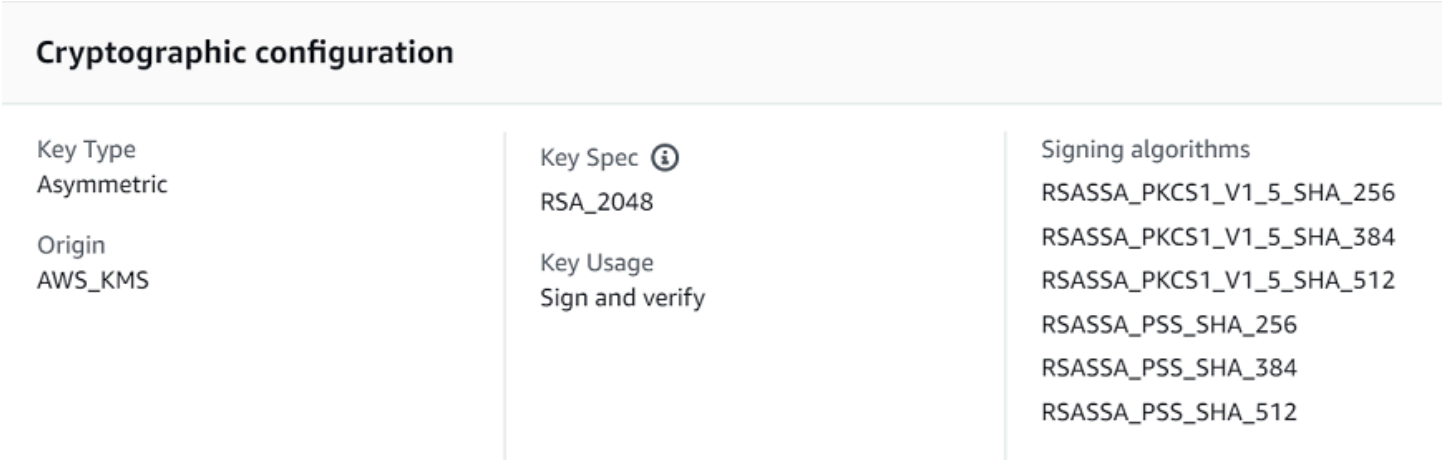
Consultar la configuración criptográfica de las claves KMS

Después de crear la clave KMS, puede ver su configuración criptográfica. No puede cambiar la configuración de una clave KMS después de crearla. Si prefiere utilizar una configuración diferente, elimine la clave KMS y créela de nuevo.

Puede encontrar la configuración criptográfica de las claves KMS, incluida la especificación de clave, el uso de la clave y los algoritmos de firma o cifrado compatibles, en la consola de AWS KMS o mediante la API de AWS KMS. Para obtener más detalles, consulte Identificación de claves KMS asimétricas.

En la consola de AWS KMS, la página de detalles de cada clave KMS incluye la pestaña Cryptographic configuration (Configuración criptográfica), que muestra los detalles criptográficos de las claves KMS. Por ejemplo, en la siguiente imagen se muestra la pestaña Cryptographic configuration (Configuración criptográfica) de una clave KMS de RSA que se utiliza para la firma y la verificación.

La pestaña Cryptographic configuration (Configuración criptográfica) para algunas claves de KMS de uso especial tiene secciones especializadas adicionales. Por ejemplo, la pestaña Cryptographic configuration (Configuración criptográfica) de una clave de KMS en un almacén de claves personalizado tiene una sección de Custom key stores (Almacenes de claves personalizados). La pestaña Cryptographic configuration (Configuración criptográfica) de una clave de KMS en un almacén de claves externo tiene una sección de External key (Clave externa).



En la AWS KMS API, usa la DescribeKeyoperación. La estructura `KeyMetadata` de la respuesta incluye la configuración criptográfica de la clave KMS. Por ejemplo, `DescribeKey` devuelve la siguiente respuesta para una clave KMS de RSA que se utiliza para la firma y la verificación.

```
{
  "KeyMetadata": {

    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "CreationDate": 1571767572.317,
    "CustomerMasterKeySpec": "RSA_2048",
    "Description": "",
    "Enabled": true,
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeyState": "Enabled",
    "MultiRegion": false,
    "Origin": "AWS_KMS",
    "KeySpec": "RSA_2048",
    "KeyUsage": "SIGN_VERIFY",
    "SigningAlgorithms": [
        "RSASSA_PKCS1_V1_5_SHA_256",
        "RSASSA_PKCS1_V1_5_SHA_384",
        "RSASSA_PKCS1_V1_5_SHA_512",
        "RSASSA_PSS_SHA_256",
        "RSASSA_PSS_SHA_384",
        "RSASSA_PSS_SHA_512"
    ]
  }
```

```
}
```

Búsqueda del ID y el ARN de la clave

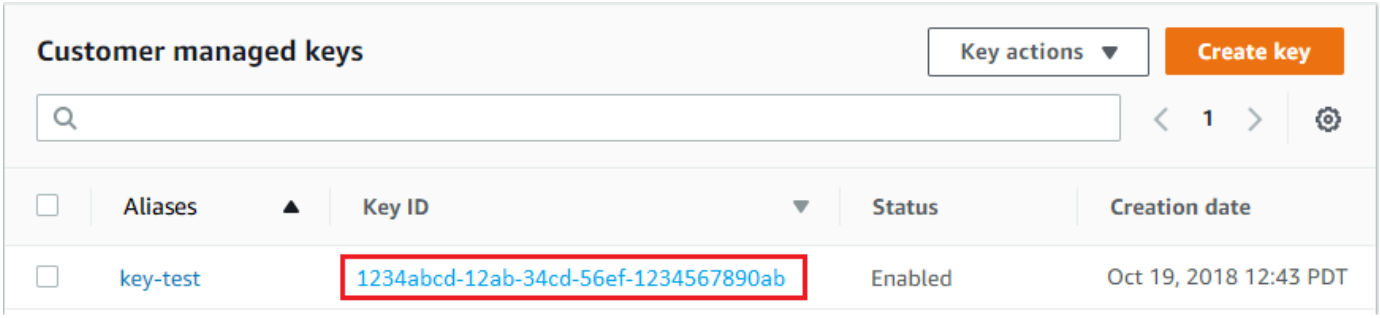
Para identificar un AWS KMS key, puede utilizar su ID de clave o su nombre de recurso de Amazon (ARN de clave). En operaciones criptográficas, también puede utilizar el nombre de alias o el ARN de alias.

Para obtener información detallada sobre los identificadores de clave KMS que admite AWS KMS, consulte Identificadores clave () KeyId. Para obtener ayuda para buscar un nombre de alias y un ARN de alias, consulte Buscar el nombre del alias y el ARN de alias.

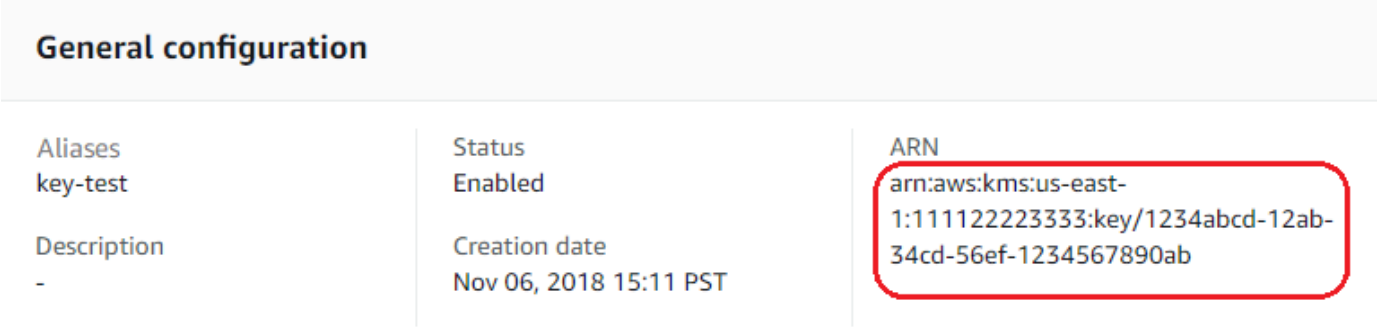
Para encontrar el ID y el ARN de la clave (consola)

1. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente). Si desea ver las claves de su cuenta que AWS crea y administra, en el panel de navegación, elija claves administradas por AWS.
4. Para buscar el ID de clave de una clave KMS, consulte la fila que empieza por el alias de clave KMS.

   La columna Key ID (ID de clave) aparece en las tablas de forma predeterminada. Si la columna Key ID (ID de clave) no aparece en la tabla, utilice el procedimiento que se describe en the section called “Personalización de las tablas clave KMS” para restaurarla. También puede ver el ID de clave de una clave KMS en su página de detalles.



5. Para buscar el nombre de recurso de Amazon (ARN) de la clave KMS, elija el ID o alias de la clave. El ARN de clave aparece en la sección General Configuration (Configuración general).



Para encontrar el ID y el ARN de clave (API de AWS KMS)

Para encontrar el ID de clave y el ARN de clave de unAWS KMS key, utilice la ListKeysoperación. Para obtener ejemplos en varios lenguajes de programación, consulte Obtener ID de clave y ARN y Obtener los ID de clave y ARN.

La respuesta `ListKeys` incluye el ID de clave y el ARN de clave para cada clave KMS en la cuenta y región.

```
$ aws kms list-keys
{
    "Keys": [
        {
            "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "KeyArn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        {
            "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "KeyArn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ]
}
```

Buscar el nombre del alias y el ARN de alias

Un alias es un nombre fácil de recordar para una AWS KMS AWS KMS keys (clave KMS). Puede encontrar el nombre del alias y ARN de alias en la consola de AWS KMS o API de AWS KMS.

Para obtener información detallada sobre los identificadores de claves KMS que admite AWS KMS, consulte Identificadores clave () KeyId. Para obtener ayuda para encontrar el ID de clave y el ARN de clave, consulte Búsqueda del ID y el ARN de la clave.

Temas

Para buscar el nombre del alias y el ARN de alias (consola)

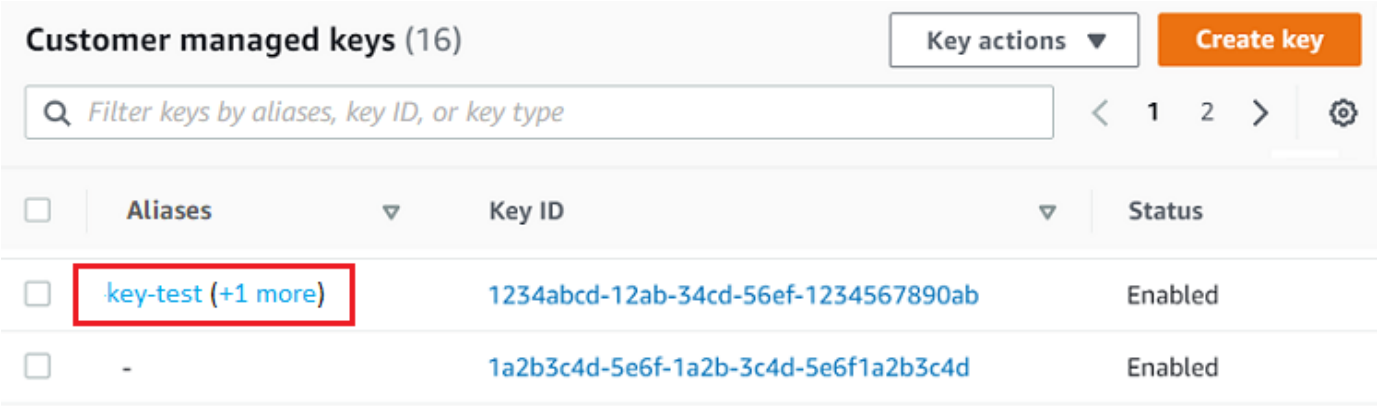
La consola AWS KMS muestra los alias asociados a la clave KMS.

1. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente). Si desea ver las claves de su cuenta que AWS crea y administra, en el panel de navegación, elija claves administradas por AWS.
4. La columna Aliases (Alias) muestra el alias de cada clave KMS. Si una clave KMS no tiene un alias, aparece un guion (-) en la columna Aliases (Alias).

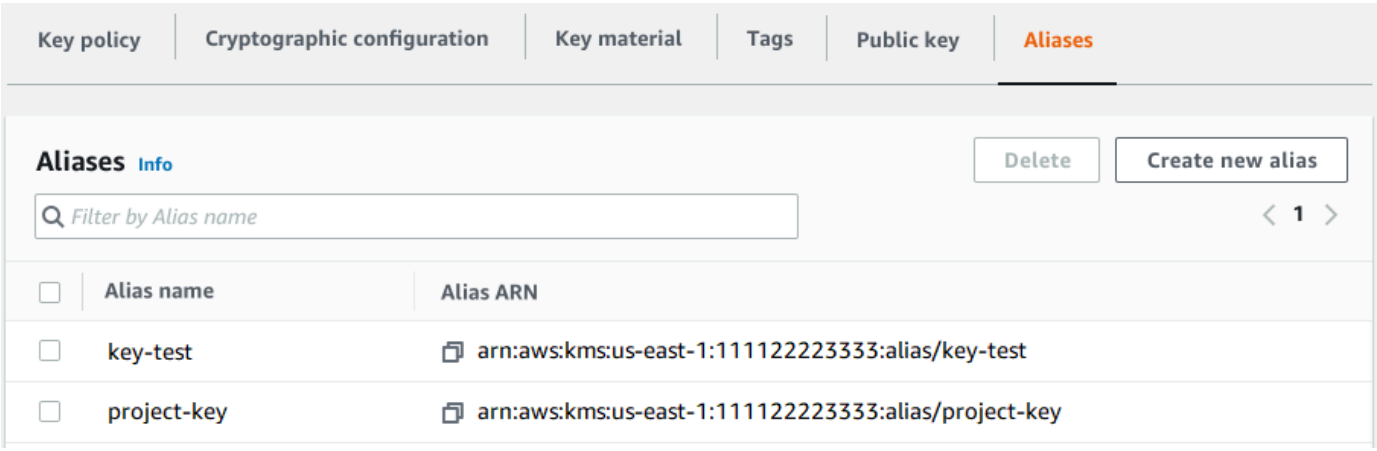
   Si una clave KMS tiene varios alias, la columna Aliases (Alias) también tiene un resumen de alias, como (+n más). Por ejemplo, la siguiente clave KMS tiene dos alias, uno de los cuales es `key-test`.

   Para buscar el nombre del alias y el ARN de alias de la clave KMS, utilice la pestaña Aliases (Alias).

   - Para ir directamente a la pestaña Aliases (Alias), en la columna Aliases (Alias), elija el resumen de alias (+n más). Un resumen de alias sólo aparece si la clave KMS tiene más de un alias.
   - O bien, elija el alias o el ID de clave de la clave KMS (que abre la página de detalles de la clave KMS) y, a continuación, elija la pestaña Aliases (Alias). Las pestañas están debajo de la sección General configuration (Configuración general).



5. La pestaña Aliases (Alias) muestra el nombre del alias y el ARN del alias de todos los alias de una clave KMS. También puede crear y eliminar alias para la clave KMS en esta pestaña.



Buscar el nombre del alias y el ARN de alias (API de AWS KMS)

Para encontrar el nombre del alias y el ARN del alias de unAWS KMS key, utilice la ListAliasesoperación. Para obtener ejemplos en varios lenguajes de programación, consulte Mostrar alias y Obtener nombres de alias y ARN.

De forma predeterminada, la respuesta incluye el nombre de alias y el ARN de alias para cada alias de la cuenta y región. Para obtener solo los alias de una clave KMS en particular, utilice el parámetro `KeyId`.

Por ejemplo, el siguiente comando obtiene solo los alias de una clave KMS de ejemplo con el ID de clave `1234abcd-12ab-34cd-56ef-1234567890ab`.

```
$ aws kms list-aliases --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

```
{
    "Aliases": [
        {
            "AliasName": "alias/key-test",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/key-test",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1593622000.191,
            "LastUpdatedDate": 1593622000.191
        },
        {
            "AliasName": "alias/project-key",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/project-key",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
            "CreationDate": 1516435200.399,
            "LastUpdatedDate": 1516435200.399
        }
    ]
}
```

Editar claves

Puede cambiar las siguientes propiedades de las claves KMS administradas por el cliente en la consola de AWS KMS mediante la API de AWS KMS.

No puede editar ninguna de las propiedades de Claves administradas por AWS ni de Claves propiedad de AWS. Estas claves las administran los servicios de AWS que los crearon.

Descripción

Puede cambiar la descripción de la clave gestionada por el cliente en la página de detalles de la clave KMS o mediante la UpdateKeyDescriptionoperación.

Para editar la descripción de la clave en la consola, en la esquina superior derecha de la página de detalles de la clave KMS, elija Edit (Editar).

Política de claves

Puede cambiar la política clave en la pestaña Política clave de la página de detalles de la clave administrada por el cliente o mediante la PutKeyPolicyoperación.

Para obtener más detalles, consulte Cambiar una política de claves.

Etiquetas

Puede crear y eliminar etiquetas en la página de claves administradas por el cliente de la consola de AWS KMS, o en la pestaña Tags (Etiquetas) de la página de detalles para la clave administrada por el cliente. O puede utilizar las UntagResourceoperaciones TagResourcey.

Para obtener más detalles, consulte Etiquetado de claves.

Habilitar y deshabilitar

Puede habilitar y deshabilitar claves KMS en la página de claves administradas por el cliente de la consola de AWS KMS, o en la página de detalles para la clave administrada por el cliente. O puede usar las DisableKeyoperaciones EnableKeyy.

Para obtener más detalles, consulte Habilitación y deshabilitación de claves.

Rotación automática de claves

Puede activar y desactivar la rotación automática de claves en la pestaña Rotación de claves de la página de detalles de la clave gestionada por el cliente o mediante las DisableKeyRotationoperaciones EnableKeyRotationy.

Para obtener más detalles, consulte Rotativo AWS KMS keys.

Véase también

Actualización de alias

Etiquetado de claves

En AWS KMS puede agregar etiquetas a una clave administrada por el cliente cuando cree la clave KMS, y etiquetar o desetiquetar claves KMS existentes a menos que estén pendientes de eliminación. No puede etiquetar alias, amacenes de claves personalizados, Claves administradas por AWS, Claves propiedad de AWS, o claves KMS en otras Cuentas de AWS. Las etiquetas son opcionales, pero pueden ser muy útiles.

Para obtener más información, consulte Crear claves y Editar claves. Para obtener información general sobre las etiquetas, incluidas las prácticas recomendadas, las estrategias de etiquetado y el formato y la sintaxis de las etiquetas, consulte Etiquetado de recursos de AWS en la Referencia general de Amazon Web Services.

Temas

Acerca de las etiquetas de AWS KMS

Una etiqueta es un elemento de metadatos opcional que usted asigna (o que AWS puede asignar) a un recurso de AWS. Cada etiqueta consta de una clave de etiqueta y a valor de etiqueta, que distinguen entre mayúsculas y minúsculas. El valor de la etiqueta puede ser una cadena vacía (nula). Cada etiqueta de un recurso debe tener una clave de etiqueta diferente, pero puede agregar la misma etiqueta a varios recursos de AWS. Cada recurso puede tener un máximo de 50 etiquetas creadas por el usuario.

No incluya información confidencial en la clave ni en el valor de la etiqueta. Las etiquetas son accesibles para muchos Servicios de AWS, incluida la facturación.

En AWS KMS puede agregar etiquetas a una clave administrada por el cliente cuando cree la clave KMS, y etiquetar o desetiquetar claves KMS existentes a menos que estén pendientes de eliminación. No puede etiquetar alias, amacenes de claves personalizados, Claves administradas por AWS, Claves propiedad de AWS, o claves KMS en otras Cuentas de AWS. Las etiquetas son opcionales, pero pueden ser muy útiles.

Por ejemplo, puede agregar una etiqueta `"Project"="Alpha"` para todas las claves KMS y los buckets de Amazon S3 que utilice para el proyecto Alpha.

```
TagKey   = "Project"
TagValue = "Alpha"
```

Para obtener información general sobre las etiquetas, incluidos el formato y la sintaxis, consulte Etiquetado de recursos de AWS en la Referencia general de Amazon Web Services.

Las etiquetas le ayudan a hacer lo siguiente:

- Identificar y organizar sus recursos de AWS. Muchos servicios de AWS admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los

recursos están relacionados. Por ejemplo, puede asignar la misma etiqueta a una clave KMS y a un volumen de Amazon Elastic Block Store (Amazon EBS) o AWS Secrets Manager secreta. También puede utilizar etiquetas para identificar claves KMS para la automatización.

- Realizar un seguimiento de los costos de AWS. Cuando se agregan etiquetas a los recursos de AWS, AWS genera un informe de asignación de costos con el uso y los costos agregados por etiquetas. Puede utilizar esta característica para realizar un seguimiento de los costos de AWS KMS para un proyecto, aplicación o centro de costos.

  Para obtener más información sobre el uso de etiquetas para la asignación de costos, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing. Para obtener información sobre las reglas que se aplican a las claves y los valores de las etiquetas, consulte Restricciones de las etiquetas definidas por el usuario en la Guía del usuario AWS Billing.
- Controle el acceso a los recursos de AWS. Permitir y denegar el acceso a las claves KMS en función de sus etiquetas es parte de la compatibilidad de AWS KMS para el control de acceso basado en atributos (ABAC). Para obtener más información sobre el control de acceso para AWS KMS keys basado en etiquetas, consulte Uso de etiquetas para controlar el acceso a las claves KMS. Para obtener más información sobre el uso de etiquetas para controlar el acceso a los recursos de AWS, consulte Control de acceso a los recursos de AWS utilizando recursos de etiquetas en la Guía del usuario de IAM.

AWS KMSescribe una entrada en el AWS CloudTrail registro cuando se utilizan las ListResourceTagsoperaciones TagResourceUntagResource, o.

Administración de etiquetas de clave KMS en la consola

Puede agregar etiquetas a una clave KMS al crear la clave KMS en la consola de AWS KMS. También puede utilizar la pestaña Tags (Etiquetas) en la consola para agregar, editar y eliminar etiquetas en claves administradas por el cliente. Para agregar, editar, ver y eliminar etiquetas para una clave KMS, debe tener los permisos necesarios. Para obtener más detalles, consulte Control del acceso a las etiquetas.

Agregar etiquetas al crear una clave KMS

Para agregar etiquetas al crear una clave KMS en la consola debe tener el permiso `kms:TagResource` en una política de IAM, además de los permisos necesarios para crear claves KMS y ver claves KMS en la consola. Como mínimo, el permiso debe cubrir todas las claves KMS de la cuenta y la región.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente. (No puede administrar las etiquetas de una Clave administrada de AWS)
4. Elija el tipo de clave, a continuación, elija Next (Siguiente).
5. Escriba un alias y una descripción opcional.
6. Introduzca una clave de etiqueta y un valor de etiqueta opcional. Para agregar otras etiquetas, elija Add tag (Agregar etiqueta). Para quitar una etiqueta, seleccione Remove (Eliminar). Cuando termine de etiquetar su nueva clave KMS, elija Next (Siguiente).
7. Termine de crear su clave KMS

Ver y administrar etiquetas en claves KMS existentes

Para agregar, ver, editar y eliminar etiquetas en la consola necesita permiso de etiquetado en la clave KMS. Puede obtener este permiso de la política de clave para la clave KMS o, si la política de clave lo permite, de una política de IAM que incluya la clave KMS. Necesita estos permisos además de los permisos para ver las claves KMS en la consola.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente. (No puede administrar las etiquetas de una Clave administrada de AWS)
4. Puede utilizar el filtro de tabla para mostrar sólo claves KMS con etiquetas concretas. Para obtener más detalles, consulte Ordenar y filtrar las claves KMS.
5. Seleccione la casilla de verificación situada junto al alias de una clave KMS.
6. Elija Key actions, Add or edit tags.
7. En la página de detalles de la clave KMS, seleccione la pestaña Tags (Etiquetas).
   - Para crear la primera etiqueta, elija Create tag (Crear etiqueta), escriba el nombre (obligatorio) y el valor (opcional) de la etiqueta y, por último, elija Save (Guardar).

Si deja el valor de etiqueta en blanco, el valor de etiqueta real es una cadena nula o vacía.

- Para agregar una etiqueta, elija Edit (Editar), Add tag (Agregar etiqueta), escriba el nombre y el valor de la etiqueta y, por último, elija Save (Guardar).
- Para modificar el nombre o el valor de una etiqueta, elija Edit (Editar), aplique los cambios y elija Save (Guardar).
- Para eliminar una etiqueta, elija Edit (Editar). En la fila de la etiqueta, elija Remove (Eliminar) y, luego, Save (Guardar).

8. Para guardar los cambios, elija Guardar cambios.

Administración de etiquetas de clave KMS con operaciones de la API

Puede utilizar la API de AWS Key Management Service (AWS KMS) para agregar, eliminar y enumerar etiquetas para las claves KMS que administre. En estos ejemplos, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido. No puede etiquetar Claves administradas por AWS.

Para agregar, editar, ver y eliminar etiquetas de una clave KMS, debe tener los permisos necesarios. Para obtener más detalles, consulte Control del acceso a las etiquetas.

Temas

- CreateKey: añada etiquetas a una nueva clave de KMS
- TagResource: Agregue o cambie las etiquetas de una clave KMS
- ListResourceTags: Obtenga las etiquetas de una clave KMS
- UntagResource: elimina las etiquetas de una clave KMS

CreateKey: añada etiquetas a una nueva clave de KMS

Puede añadir etiquetas al crear una clave gestionada por el cliente. Para especificar las etiquetas, utilice el `Tags` parámetro de la CreateKeyoperación.

Para agregar etiquetas al crear una clave KMS, la persona que llama debe tener el permiso `kms:TagResource` en una política de IAM. Como mínimo, el permiso debe cubrir todas las claves KMS de la cuenta y la región. Para obtener más detalles, consulte Control del acceso a las etiquetas.

El valor del parámetro `Tags` de `CreateKey`es una colección de pares de claves y valores de etiqueta que distinguen mayúsculas y minúsculas. Cada etiqueta de una clave KMS debe tener un nombre de etiqueta diferente. El valor de etiqueta puede ser una cadena vacía o nula.

Por ejemplo, el siguiente comando AWS CLI crea una clave KMS de cifrado simétrica con una etiqueta `Project:Alpha`. Cuando especifique más de un par de clave-valor, utilice un espacio para separar cada par.

```
$ aws kms create-key --tags TagKey=Project,TagValue=Alpha
```

Cuando este comando se ejecuta correctamente, devuelve un objeto `KeyMetadata` con información sobre la nueva clave KMS. Sin embargo, `KeyMetadata` no incluye etiquetas. Para obtener las etiquetas, utilice la ListResourceTagsoperación.

TagResource: Agregue o cambie las etiquetas de una clave KMS

La TagResourceoperación agrega una o más etiquetas a una clave de KMS. No puede usar esta operación para agregar o editar etiquetas en una Cuenta de AWS diferente.

Para agregar una etiqueta, especifique una clave de etiqueta nueva y un valor de la etiqueta. Para editar una etiqueta, especifique una clave de etiqueta existente y un nuevo valor de etiqueta. Cada etiqueta de una clave KMS debe tener una clave de etiqueta distinta. El valor de etiqueta puede ser una cadena vacía o nula.

Por ejemplo, el siguiente comando agrega las etiquetas **`Purpose`** y **`Department`** a una clave KMS de ejemplo.

```
$ aws kms tag-resource \
        --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
        --tags TagKey=Purpose,TagValue=Pretest TagKey=Department,TagValue=Finance
```

Si este comando se realiza correctamente, no devuelve ningún resultado. Para ver las etiquetas de una clave KMS, utilice la ListResourceTagsoperación.

También pueden utilizar TagResource para cambiar los valores de una etiqueta existente. Para sustituir los valores de etiqueta, especifique la misma clave de etiqueta con distintos valores.

Por ejemplo, este comando cambia el valor de la etiqueta `Purpose` de `Pretest` a `Test`.

```
$ aws kms tag-resource \
```

```
        --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
        --tags TagKey=Purpose,TagValue=Test
```

ListResourceTags: Obtenga las etiquetas de una clave KMS

La ListResourceTagsoperación obtiene las etiquetas de una clave KMS. El parámetro `KeyId` es obligatorio. No puede usar esta operación para ver las etiquetas de claves KMS en una Cuenta de AWS diferente.

Por ejemplo, el comando siguiente obtiene las etiquetas para una clave KMS de ejemplo.

```
$ aws kms list-resource-tags --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

  "Truncated": false,
  "Tags": [
      {
        "TagKey": "Project",
        "TagValue": "Alpha"
    },
    {
      "TagKey": "Purpose",
      "TagValue": "Test"
    },
    {
      "TagKey": "Department",
      "TagValue": "Finance"
    }
  ]
}
```

UntagResource: elimina las etiquetas de una clave KMS

La UntagResourceoperación elimina las etiquetas de una clave KMS. Para identificar las etiquetas que desea eliminar, especifique las claves de etiqueta. No puede usar esta operación para eliminar etiquetas de claves KMS una Cuenta de AWS diferente.

Cuando tiene éxito, la operación `UntagResource` no devuelve ningún resultado. Además, si la clave de etiqueta especificada no se encuentra en la clave KMS, no arroja una excepción ni devuelve una respuesta. Para confirmar que la operación ha funcionado, utilice la ListResourceTagsoperación.

Por ejemplo, este comando elimina la etiqueta **`Purpose`** y todos sus valores de la clave KMS especificada.

```
$ aws kms untag-resource --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --tag-keys
 Purpose
```

Control del acceso a las etiquetas

Para agregar, ver y eliminar etiquetas, ya sea en la consola AWS KMS o mediante el uso de la API, las entidades principales necesitan permisos de etiquetado. Puede proporcionar estos permisos en una política de claves. También puede proporcionarlos en las políticas de IAM (incluyendo Políticas de punto de enlace de la VPC), pero solo si la política de claves lo permite. La política AWSKeyManagementServicePowerUseradministrada permite a los directores etiquetar, desetiquetar y enumerar las etiquetas de todas las claves de KMS a las que puede acceder la cuenta.

También puede limitar estos permisos mediante claves de condición globales de AWS. EnAWS KMS, estas condiciones pueden controlar el acceso a las operaciones de etiquetado, como y. TagResourceUntagResource

> **Note**
>
> Tenga cuidado al dar permiso a las entidades principales para administrar etiquetas y alias. El cambio de etiqueta o alias puede permitir o denegar permiso a la clave administrada por el cliente. Para más detalles, consulte ABAC para AWS KMS y Uso de etiquetas para controlar el acceso a las claves KMS.

Para obtener más información y políticas de ejemplo, consulte Control del acceso en función de las claves de etiquetaen la Guía del usuario de IAM.

Los permisos para crear y administrar etiquetas funcionan de la siguiente manera.

km: TagResource

Permite a las entidades principales agregar o editar etiquetas. Para agregar etiquetas al crear una clave KMS, la entidad principal debe tener permiso en una política de IAM que no esté restringida a determinadas claves KMS.

km: ListResourceTags

Permite a las entidades principales ver etiquetas en claves KMS.

km: UntagResource

Permite a las entidades principales eliminar etiquetas de las claves KMS.

Permisos de etiquetas en políticas

Puede proporcionar permisos de etiquetas en una política de claves o una política de IAM. Por ejemplo, la siguiente política de claves de ejemplo ofrece permiso de etiquetar a los usuarios seleccionados en la clave KMS. Da permiso a todos los usuarios que pueden asumir los roles de administrador o desarrollador de ejemplo para ver etiquetas.

```
{
  "Version": "2012-10-17",
  "Id": "example-key-policy",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow all tagging permissions",
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::111122223333:user/LeadAdmin",
        "arn:aws:iam::111122223333:user/SupportLead"
      ]},
      "Action": [
          "kms:TagResource",
          "kms:ListResourceTags",
          "kms:UntagResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow roles to view tags",
      "Effect": "Allow",
      "Principal": {"AWS": [
        "arn:aws:iam::111122223333:role/Administrator",
        "arn:aws:iam::111122223333:role/Developer"
```

```
      ]},
      "Action": "kms:ListResourceTags",
      "Resource": "*"
    }
  ]
}
```

Para conceder permiso de etiquetado de entidades principales en varias claves KMS, puede usar una política de IAM. Para que esta política sea efectiva, la política de claves de cada clave KMS debe permitir a la cuenta utilizar políticas de IAM para controlar el acceso a clave KMS.

Por ejemplo, la siguiente política de IAM permite a las entidades principales crear claves KMS. También les permite crear y administrar etiquetas en todas las claves KMS de la cuenta especificada. Esta combinación permite a los directores utilizar el parámetro Etiquetas de la CreateKeyoperación para añadir etiquetas a una clave de KMS mientras la crean.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyCreateKeys",
      "Effect": "Allow",
      "Action": "kms:CreateKey",
      "Resource": "*"
    },
    {
      "Sid": "IAMPolicyTags",
      "Effect": "Allow",
      "Action": [
        "kms:TagResource",
        "kms:UntagResource",
        "kms:ListResourceTags"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    }
  ]
}
```

Limitar los permisos de etiqueta

Puede limitar los permisos de etiquetado mediante condiciones de política. Las siguientes condiciones de política se pueden aplicar a los permisos `kms:TagResource` y

`kms:UntagResource`. Por ejemplo, puede utilizar la condición `aws:RequestTag/`*`tag-key`* para permitir que una entidad principal agregue solo etiquetas particulares, o impedir que una entidad principal agregue etiquetas con claves de etiqueta concretas. También puede utilizar la condición `kms:KeyOrigin` para evitar que las entidades principales etiqueten o desetiqueten claves KMS con material de claves importado.

- AWS: RequestTag
- aws:ResourceTag/tag-key (solo políticas de IAM)
- AWS: TagKeys
- km: CallerAccount
- km: KeySpec
- km: KeyUsage
- km: KeyOrigin
- km: ViaService

Como práctica recomendada cuando utilice etiquetas para controlar el acceso a claves KMS, utilice la clave de condición `aws:RequestTag/`*`tag-key`* o `aws:TagKeys` para determinar qué etiquetas (o claves de etiqueta) están permitidas.

Por ejemplo, la siguiente política IAM es similar a la anterior. Sin embargo, esta política permite a las entidades principales crear etiquetas (`TagResource`) y eliminar etiquetas `UntagResource` solo para etiquetas con una clave de etiqueta `Project`.

Como `TagResource` las `UntagResource` solicitudes pueden incluir varias etiquetas, debe especificar un operador `ForAllValues` o `ForAnyValue` configurarlo con la TagKeys condición aws:. El operador `ForAnyValue` requiere que al menos una de las claves de etiqueta de la solicitud coincida con una de las claves de etiqueta de la política. El operador `ForAllValues` requiere que todas las claves de etiqueta de la solicitud coincidan con una de las claves de etiqueta de la política. El `ForAllValues` operador también devuelve el `true` mensaje si no hay etiquetas en la solicitud, pero TagResource no lo UntagResource hace si no se especifica ninguna etiqueta. Para obtener información detallada sobre los operadores de conjunto, consulte Usar varias claves y valores en la Guía del usuario de IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Sid": "IAMPolicyCreateKey",
      "Effect": "Allow",
      "Action": "kms:CreateKey",
      "Resource": "*"
    },
    {
      "Sid": "IAMPolicyViewAllTags",
      "Effect": "Allow",
      "Action": "kms:ListResourceTags",
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "IAMPolicyManageTags",
      "Effect": "Allow",
      "Action": [
        "kms:TagResource",
        "kms:UntagResource"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
          "ForAllValues:StringEquals": {"aws:TagKeys": "Project"}
      }
    }
  ]
}
```

Uso de etiquetas para controlar el acceso a las claves KMS

Puede controlar el acceso a AWS KMS keys en función de las etiquetas de la clave KMS. Por ejemplo, puede escribir una política de IAM que permita a las entidades principales habilitar y desactivar solo las claves KMS que tienen una etiqueta concreta. O bien, puede utilizar una política de IAM para evitar que las principales entidades utilicen claves KMS en operaciones criptográficas, a menos que la clave KMS tenga una etiqueta concreta.

Esta característica forma parte de la compatibilidad de AWS KMS para el control de acceso basado en atributos (ABAC). Para obtener más información sobre cómo usar etiquetas para controlar el acceso a los recursos de AWS, consulte ¿Qué es ABAC para AWS? y Control del acceso a recursos de AWS con etiquetas de recursos en la Guía del usuario de IAM. Para obtener ayuda para resolver problemas de acceso relacionados con ABAC, consulte Solución de problemas de ABAC para AWS KMS.

> **Note**
>
> Puede que transcurran cinco minutos hasta que los cambios de etiqueta y alias afecten a la autorización de clave KMS. Los cambios recientes pueden ser visibles en las operaciones de API antes de que afecten a la autorización.

AWS KMSadmite la clave de contexto de condición global aws:ResourceTag/tag-key, que permite controlar el acceso a las claves de KMS en función de las etiquetas de la clave de KMS. Dado que varias claves KMS pueden tener la misma etiqueta, esta función le permite aplicar el permiso a un conjunto seleccionado de claves KMS. También puede cambiar fácilmente las claves KMS del conjunto cambiando sus etiquetas.

En AWS KMS, la clave de condición de `aws:ResourceTag/`*`tag-key`* solo se admite en las políticas de IAM. No se admite en las políticas clave, que solo se aplican a una clave de KMS, ni en las operaciones que no utilizan una clave de KMS concreta, como las operaciones ListKeyso ListAliases.

Controlar el acceso con etiquetas proporciona una forma sencilla, escalable y flexible de administrar los permisos. Sin embargo, si no está diseñado y administrado correctamente, puede permitir o denegar el acceso a sus claves KMS inadvertidamente. Si utiliza etiquetas para controlar el acceso, tenga en cuenta las siguientes prácticas.

- Utilice etiquetas para reforzar la práctica recomendada de acceso menos privilegiado. Proporcione a las entidades principales de IAM solo los permisos que necesitan y únicamente en las claves KMS que deben usar o administrar. Por ejemplo, utilice etiquetas para etiquetar las claves KMS utilizadas en un proyecto. A continuación, dé permiso al equipo del proyecto para usar solo claves KMS con la etiqueta de proyecto.
- Tenga cuidado al dar a las principales entidades los permisos `kms:TagResource` y `kms:UntagResource` que les permiten agregar, editar y eliminar etiquetas. Cuando utiliza etiquetas para controlar el acceso a las claves KMS, cambiar una etiqueta puede dar permiso a las principales entidades para usar claves KMS que de otro modo no tenían permiso para usar. También puede denegar el acceso a las claves KMS que otras entidades principales requieren para realizar sus trabajos. Los administradores de claves que no tienen permiso para cambiar políticas de claves o crear concesiones pueden controlar el acceso a claves KMS si tienen permiso para administrar etiquetas.

Siempre que sea posible, utilice una condición de política, como `aws:RequestTag/tag-key` o `aws:TagKeys` para limitar los permisos de etiquetado de una entidad a determinadas etiquetas o patrones de etiquetas en determinadas claves KMS.

- Revise las entidades principales de su Cuenta de AWS que actualmente tienen permisos para etiquetar y desetiquetar y ajustarlos, si es necesario. Por ejemplo, la consola Política de claves predeterminada para administradores de claves incluye el permiso `kms:TagResource` y `kms:UntagResource` en esa clave KMS. Las políticas de IAM pueden habilitar permisos de etiqueta y desetiqueta en todas las claves KMS. Por ejemplo, la política AWSKeyManagementServicePowerUseradministrada permite a los directores etiquetar, desetiquetar y enumerar las etiquetas de todas las claves de KMS.
- Antes de establecer una política que dependa de una etiqueta, revise las etiquetas de las claves KMS de su Cuenta de AWS. Asegúrese de que su política solo se aplique a las etiquetas que desea incluir. Usa CloudTrail registros y CloudWatch alarmas para avisarte de los cambios en las etiquetas que puedan afectar al acceso a tus claves de KMS.
- Las condiciones de política basadas en etiquetas utilizan la coincidencia de patrones; no están vinculadas a una instancia concreta de una etiqueta. Una política que utiliza claves de condición basadas en etiquetas afecta a todas las etiquetas nuevas y existentes que coincidan con el patrón. Si elimina y vuelve a crear una etiqueta que coincida con una condición de política, la condición se aplica a la nueva etiqueta, igual que a la anterior.

Por ejemplo, tomemos el siguiente ejemplo de política de IAM. Permite a las entidades principales realizar llamadas a las operaciones GenerateDataKeyWithoutPlaintexty descifrar únicamente desde las claves de KMS de tu cuenta que pertenezcan a la región de Asia Pacífico (Singapur) y dispongan de una `"Project"="Alpha"` etiqueta. Puede adjuntar esta política a roles del ejemplo de proyecto Alpha.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:ap-southeast-1:111122223333:key/*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "Alpha"
        }
      }
    }
  ]
}
```

La siguiente política de IAM de ejemplo permite a la entidad principal utilizar la clave KMS en la cuenta para operaciones criptográficas. Pero prohíbe a las principales entidades usar estas operaciones criptográficas en claves KMS con una etiqueta `"Type"="Reserved"` o sin etiqueta `"Type"`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMAllowCryptographicOperations",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "IAMDenyOnTag",
      "Effect": "Deny",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Type": "Reserved"
        }
      }
```

```
    },
    {
      "Sid": "IAMDenyNoTag",
      "Effect": "Deny",
      "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:Decrypt",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/Type": "true"
        }
      }
    }
  ]
}
```

Habilitación y deshabilitación de claves

Puede habilitar y deshabilitar claves administradas por el cliente. Al crear una clave KMS, está habilitada de forma predeterminada. Si desactiva una clave KMS, no se puede utilizar en ninguna operación criptográfica hasta que lo vuelva a habilitar.

Debido a que es temporal y se deshace fácilmente, desactivar una clave KMS es una alternativa segura a eliminar una clave KMS, una acción destructiva e irreversible. Si está pensando en eliminar una clave KMS, deshabilítela primero y configure una CloudWatch alarma o un mecanismo similar para asegurarse de que nunca necesitará usar la clave para descifrar datos cifrados.

Al deshabilitar una clave de KMS, queda inutilizable de inmediato (sujeto a posible coherencia). Sin embargo, los recursos cifrados con claves de datos protegidas por la clave de KMS no se ven afectados hasta que se vuelva a utilizar la clave de KMS, por ejemplo, para descifrar la clave de datos. Este problema afecta a los Servicios de AWS, muchos de los cuales utilizan claves de datos para proteger sus recursos. Para obtener más detalles, consulte Cómo afectan las claves de KMS obsoletas a las claves de datos.

No puede habilitar o desactivar Claves administradas por AWS o Claves propiedad de AWS. Las Claves administradas por AWS están habilitadas de forma permanente para que las usen los

servicios que utilizan AWS KMS. Las Claves propiedad de AWS están administradas exclusivamente por el servicio que les pertenece.

> **Note**
>
> AWS KMS no rota el material de claves de las claves administradas por el cliente mientras están deshabilitadas. Para obtener más información, consulte Cómo funciona la rotación de teclas.

Temas

- Activación y desactivación de claves KMS (consola)
- Habilitar y deshabilitar claves KMS (API de AWS KMS)

Activación y desactivación de claves KMS (consola)

Puede utilizar la consola AWS KMS para habilitar y deshabilitar claves administradas por el cliente.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija la casilla de verificación de las claves de KMS que quiere habilitar o deshabilitar.
5. Para habilitar una clave KMS, elija Key actions (Acciones de claves), Enable (Habilitar). Para deshabilitar una clave KMS, elija Key actions (Acciones de claves), Disable (Deshabilitar).

Habilitar y deshabilitar claves KMS (API de AWS KMS)

La EnableKeyoperación habilita una deshabilitadaAWS KMS key. En estos ejemplos, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido. El parámetro `key-id` es obligatorio.

Esta operación no devuelve ninguna salida. Para ver el estado de la clave, utilice la DescribeKeyoperación.

```
$ aws kms enable-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

La DisableKeyoperación deshabilita una clave KMS habilitada. El parámetro `key-id` es obligatorio.

```
$ aws kms disable-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Esta operación no devuelve ninguna salida. Para ver el estado de la clave, utilice la DescribeKeyoperación y consulte el `Enabled` campo.

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
        "MultiRegion": false,
        "Enabled": false,
        "KeyState": "Disabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "CreationDate": 1502910355.475,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333"
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

Rotativo AWS KMS keys

Para crear nuevo material criptográfico para sus claves administradas por el cliente, puede crear nuevas claves KMS y, a continuación, cambiar sus aplicaciones o alias para que utilicen las claves. O bien, puede rotar el material clave asociado a una clave KMS existente activando la rotación automática de claves o realizando la rotación bajo demanda.

De forma predeterminada, al activar la rotación automática de claves para una clave KMS, se AWS KMS genera nuevo material criptográfico para la clave KMS cada año. También puede especificar una opción personalizada rotation-period para definir el número de días después de activar la rotación automática de claves que AWS KMS rotará el material clave y el número de días que transcurrirán entre cada rotación automática a partir de entonces. Si necesita iniciar inmediatamente la rotación del material clave, puede realizar la rotación bajo demanda, independientemente de si la rotación automática de claves está habilitada o no. Las rotaciones bajo demanda no cambian los programas de rotación automática existentes.

AWS KMS guarda todas las versiones anteriores del material criptográfico a perpetuidad para que pueda descifrar cualquier dato cifrado con esa clave KMS. AWS KMS no elimina ningún material de clave girada hasta que elimine la clave KMS. Puede realizar un seguimiento de la rotación del material clave de sus claves de KMS en Amazon CloudWatch y en la AWS Key Management Service consola. AWS CloudTrail También puede utilizar la GetKeyRotationStatusoperación para comprobar si la rotación automática está habilitada para una clave de KMS e identificar cualquier rotación que se esté realizando bajo demanda. Puede utilizar la ListKeyRotationsoperación para ver los detalles de las rotaciones completadas.

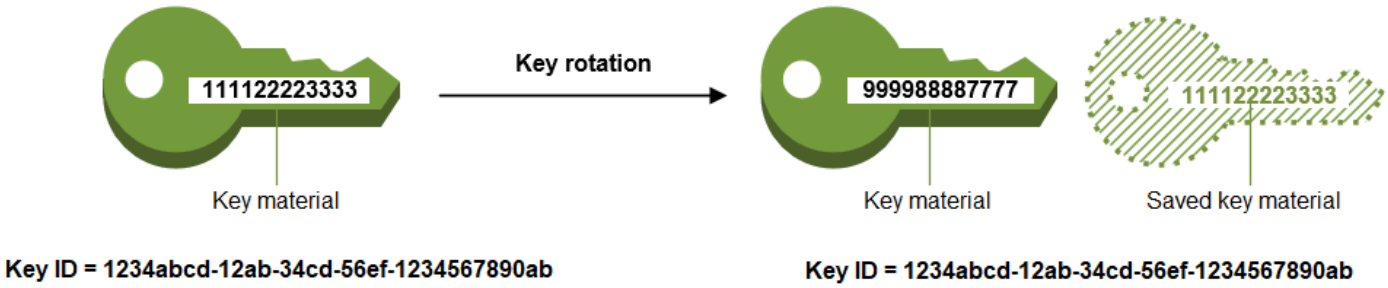
Cuando utiliza una clave KMS girada para cifrar datos, AWS KMS utiliza el material de clave actual. Cuando utiliza la clave KMS girada para descifrar el texto cifrado, AWS KMS utiliza la versión del material clave que se utilizó para cifrarlo. No puede seleccionar una versión concreta del material clave para las operaciones de descifrado, AWS KMS sino que elige automáticamente la versión correcta. Como descifra de AWS KMS forma transparente con el material clave adecuado, puede utilizar de forma segura una clave KMS girada en las aplicaciones y Servicios de AWS sin cambios de código.

Sin embargo, la rotación automática de claves no afecta a los datos que la clave KMS protege. No rota las claves de datos que ha generado la clave KMS ni vuelve a cifrar los datos protegidos por la clave KMS. Además, no mitiga el efecto de una clave de datos comprometida.

AWS KMS admite la rotación de claves automática y bajo demanda solo para claves KMS de cifrado simétrico con el material de clave que crea. AWS KMS La rotación automática es opcional para las claves KMS administradas por el cliente. AWS KMS siempre rota el material de claves para claves KMS administradas de AWS cada año. La rotación de las claves KMS AWS propias la gestiona el AWS servicio propietario de la clave.

> **Note**
>
> El período de rotación Claves administradas por AWS cambió en mayo de 2022. Para obtener más detalles, consulte Claves administradas por AWS.

La rotación de claves cambia únicamente el material de claves, que es el secreto criptográfico que se usa en las operaciones de cifrado. La clave KMS es el mismo recurso lógico, independientemente de si el material de claves cambie o de cuántas veces lo haga. Las propiedades de la clave KMS no cambian, tal y como se muestra en la siguiente imagen.



Podría optar por crear una nueva clave KMS y utilizarla en lugar de la clave KMS original. Esto tiene el mismo efecto que rotar el material de claves de una clave KMS existente, así que a menudo se considera una rotación manual de la clave. La rotación manual es una buena opción si desea rotar claves KMS que no son aptas para la rotación automática de claves, como las claves KMS asimétricas, las claves KMS HMAC, las claves KMS en almacenes de claves personalizados y las claves KMS con material clave importado.

Rotación de claves y precios

AWS KMS cobra una cuota mensual por la primera y la segunda rotación del material clave conservado para tu clave KMS. Este aumento de precio está limitado a la segunda rotación y las rotaciones posteriores no se facturarán. Consulte los Precios de AWS Key Management Service para obtener más información.

> **Note**
>
> Puedes usar AWS Cost Explorer Service para ver un desglose de los cargos por almacenamiento de claves. Por ejemplo, puede filtrar la vista para ver los cargos totales de las claves facturadas como claves de KMS actuales y rotadas especificando `$REGION-KMS-Keys` en Tipo de uso y agrupando los datos por Operación de la API.

Es posible que siga viendo instancias de la operación de la API `Unknown` heredada para fechas antiguas.

Rotación de claves y cuotas

Cada clave KMS cuenta como una clave para el cálculo de las cuotas de recursos clave, independientemente del número de versiones de material de claves rotadas.

Para obtener información detallada sobre el material de claves y la rotación, consulte los Detalles criptográficos de AWS Key Management Service.

Temas

¿Por qué rotar las claves de KMS?

Las mejores prácticas criptográficas desalientan la reutilización extensiva de las claves que cifran los datos directamente, como las claves de datos que se generan. AWS KMS Cuando las claves de datos de 256 bits cifran millones de mensajes, estas pueden fatigarse y empezar a producir texto cifrado con patrones sutiles que los actores inteligentes pueden aprovechar para descubrir los bits de la clave. Para evitar que las claves se fatiguen, lo mejor es utilizar las claves de datos una vez o solo unas cuantas veces, lo que permite rotar el material de la clave de forma eficaz.

Sin embargo, las claves de KMS se utilizan con mayor frecuencia como claves de encapsulamiento, también conocidas como claves de cifrado de claves. En lugar de cifrar los datos, las claves de encapsulamiento cifran las claves de datos que cifran los datos. Por lo tanto, se utilizan con mucha menos frecuencia que las claves de datos y casi nunca se reutilizan lo suficiente como para correr el riesgo de que se fatiguen las claves.

A pesar de que el riesgo de fatiga es muy bajo, es posible que tenga que cambiar sus claves de KMS debido a normas comerciales o contractuales o a normativas gubernamentales. Cuando se vea en la obligación de rotar las claves de KMS, le recomendamos que utilice la rotación automática de claves

cuando se permita y la rotación manual de claves cuando no se admita la rotación automática de claves.

Podría considerar la posibilidad de realizar rotaciones bajo demanda para demostrar las capacidades clave de rotación de materiales o para validar los scripts de automatización. Recomendamos utilizar rotaciones bajo demanda para las rotaciones no planificadas y utilizar la rotación clave automática con un período de rotación personalizado siempre que sea posible.

Cómo funciona la rotación de teclas

La rotación de teclas AWS KMS está diseñada para ser transparente y fácil de usar. AWS KMS admite la rotación de claves automática y bajo demanda opcional solo para las claves administradas por el cliente.

Rotación automática de llaves

AWS KMS gira la clave KMS automáticamente en la siguiente fecha de rotación definida por su período de rotación. No necesita recordar ni programar la actualización.

Rotación bajo demanda

Inicie inmediatamente la rotación del material clave asociado a su clave KMS, independientemente de si la rotación automática de claves está habilitada o no.

Administración de material de claves

AWS KMS conserva todo el material clave de una clave KMS, incluso si la rotación de claves está desactivada. AWS KMS elimina el material clave solo cuando se elimina la clave KMS.

Uso de material de claves

Cuando utiliza una clave KMS girada para cifrar datos, AWS KMS utiliza el material de clave actual. Cuando se utiliza la clave KMS rotada para descifrar el texto cifrado, AWS KMS utiliza la misma versión del material de claves utilizado para cifrarlo. No puede seleccionar una versión concreta del material clave para las operaciones de descifrado, sino que elige AWS KMS automáticamente la versión correcta.

Periodo de rotación

El período de rotación define el número de días después de activar la rotación automática de claves que AWS KMS rotará el material clave y el número de días que transcurrirán entre cada rotación automática de claves a partir de entonces. Si no especifica un valor para

`RotationPeriodInDays` activar la rotación automática de claves, el valor predeterminado es 365 días.

Puede usar la clave de RotationPeriodInDays condición kms: para restringir aún más los valores que los directores pueden especificar en el `RotationPeriodInDays` parámetro.

Fecha de rotación

AWS KMS gira automáticamente la clave KMS en la fecha de rotación definida por el período de rotación. El período de rotación predeterminado es de 365 días.

Claves administradas por el cliente

Como la rotación automática de claves es opcional en las claves administradas por el cliente y se puede habilitar y deshabilitar en cualquier momento, la fecha de rotación depende de la fecha en que se habilitó la rotación por última vez. La fecha puede cambiar si modifica el período de rotación de una clave en la que anteriormente había activado la rotación automática de claves. La fecha de rotación puede cambiar muchas veces a lo largo de la vida útil de la clave.

Por ejemplo, si crea una clave gestionada por el cliente el 1 de enero de 2022 y habilita la rotación automática de claves con el período de rotación predeterminado de 365 días el 15 de marzo de 2022, AWS KMS rota el material clave el 15 de marzo de 2023, el 15 de marzo de 2024 y, a partir de entonces, cada 365 días.

En los ejemplos siguientes se supone que la rotación automática de claves estaba habilitada con el período de rotación predeterminado de 365 días. Estos ejemplos muestran casos especiales que pueden afectar al período de rotación de una clave.

- Deshabilitar la rotación de claves: si deshabilita la rotación automática de claves en cualquier momento, la clave de KMS seguirá utilizando la versión del material de claves que utilizaba cuando la rotación estaba deshabilitada. Si vuelve a activar la rotación automática de claves, AWS KMS gira el material clave en función de la nueva fecha de activación de la rotación.
- Teclas KMS deshabilitadas: mientras una clave KMS esté deshabilitada, AWS KMS no la rota. Sin embargo, el estado de rotación de clave no cambia y no puede cambiarlo mientras la clave KMS esté deshabilitada. Cuando se vuelve a activar la clave KMS, si el material clave ha pasado su última fecha de rotación programada, lo AWS KMS rota inmediatamente. Si el material clave no ha perdido la última fecha de rotación programada, AWS KMS reanuda el programa de rotación clave original.

- Claves de KMS pendientes de eliminación: mientras una clave de KMS esté pendiente de eliminación, AWS KMS no la rota. El estado de rotación de clave se establece en `false` y no puede cambiarla mientras su eliminación está pendiente. Si se cancela la eliminación, se restaura el estado de rotación de clave anterior. Si el material clave ha pasado su última fecha de rotación programada, lo AWS KMS gira inmediatamente. Si el material clave no ha perdido su última fecha de rotación programada, AWS KMS reanuda la programación de rotación clave original.

Claves administradas por AWS

AWS KMS rota automáticamente Claves administradas por AWS cada año (aproximadamente 365 días). No puede habilitar ni desactivar la rotación de claves de Claves administradas por AWS.

El material clave de un objeto Clave administrada de AWS se rota primero un año después de su fecha de creación y, a partir de entonces, todos los años (aproximadamente 365 días a partir de la última rotación).

> **Note**
>
> En mayo de 2022, AWS KMS cambiamos el programa de rotación Claves administradas por AWS de cada tres años (aproximadamente 1095 días) a uno anual (aproximadamente 365 días).
> Claves administradas por AWS Los nuevos se rotan automáticamente un año después de su creación y aproximadamente cada año a partir de entonces.
> Claves administradas por AWS Los existentes se rotan automáticamente un año después de su rotación más reciente y cada año a partir de entonces.

Claves propiedad de AWS

No puede habilitar ni desactivar la rotación de claves de Claves propiedad de AWS. La estrategia de rotación clave de una Clave propiedad de AWS es determinada por el AWS servicio que crea y administra la clave. Para obtener más detalles, consulte el tema Cifrado en reposo en la Guía del usuario o en la Guía para desarrolladores del servicio.

Tipos de claves KMS compatibles

La rotación automática de la clave es compatible únicamente con las claves KMS de cifrado simétricas con material de claves que AWS KMS genera (Origen = AWS_KMS).

La rotación automática de claves no es compatible en los siguientes tipos de claves KMS, pero puede rotar estas claves KMS de forma manual.

- Claves de KMS asimétricas
- Claves KMS HMAC
- Claves KMS en almacenes de claves personalizados
- Claves KMS con material de claves importado

Claves de varias regiones

Puede habilitar y desactivar la rotación automática de claves paraClaves de varias regiones. La propiedad solo se establece en la clave principal. Al AWS KMS sincronizar las claves, copia la configuración de la propiedad de la clave principal a sus claves de réplica. Cuando se gira el material clave de la clave principal, lo copia AWS KMS automáticamente en todas sus réplicas de claves. Para obtener más detalles, consulte Rotación de las claves de varias regiones .

AWS servicios

Puede habilitar la rotación automática de claves en las claves administradas por el cliente que utilice para el cifrado en el lado del servidor en los servicios de AWS . La rotación anual es transparente y compatible con los servicios de AWS .

Supervisión de la rotación de claves

Cuando AWS KMS rota el material clave de una Clave administrada de AWSclave gestionada por el cliente, escribe un `KMS CMK Rotation` evento en Amazon EventBridge y otro RotateKey en tu AWS CloudTrail registro. Puede usar estos registros para comprobar que la clave KMS se ha rotado.

Puede usar la AWS Key Management Service consola para ver el número de rotaciones pendientes bajo demanda y una lista de todas las rotaciones de materiales clave completadas para una clave de KMS.

Puede utilizar la ListKeyRotationsoperación para ver los detalles de las rotaciones completadas.

Consistencia final

La rotación de claves está sujeta a los mismos posibles efectos de coherencia que otras operaciones AWS KMS de gestión. Es posible que haya un ligero retraso antes de que el nuevo material de claves esté disponible en AWS KMS. Sin embargo, la rotación de material clave no causa ninguna interrupción o retraso en las operaciones criptográficas. El material clave actual se utiliza en operaciones criptográficas hasta que el nuevo material de claves esté disponible en

toda la AWS KMS. Cuando el material clave de una clave multirregional se rota automáticamente, AWS KMS utiliza el material clave actual hasta que el nuevo material clave esté disponible en todas las regiones con una clave multirregional relacionada.

Cómo habilitar y desactivar la rotación automática de claves

De forma predeterminada, cuando se habilita la rotación automática de claves para una clave de KMS, se AWS KMS genera nuevo material criptográfico para la clave de KMS cada año. También puede especificar una opción personalizada rotation-period para definir el número de días después de activar la rotación automática de claves que AWS KMS rotará el material clave y el número de días que transcurrirán entre cada rotación automática a partir de entonces.

La rotación automática de claves tiene las siguientes ventajas:

- Las propiedades de la clave KMS, incluido su ID de clave, ARN de clave, región, políticas y permisos, no cambian cuando se rota la clave.
- No necesita cambiar las aplicaciones ni los alias que hacen referencia al ID o ARN de la clave KMS.
- El material de claves de rotación no afecta al uso de la clave KMS en ningún Servicio de AWS.
- Tras activar la rotación de claves, AWS KMS gira la clave KMS automáticamente en la siguiente fecha de rotación definida por el período de rotación. No necesita recordar ni programar la actualización.

Los usuarios autorizados pueden usar la AWS KMS consola y la AWS KMS API para activar y desactivar la rotación automática de claves y ver el estado de la rotación de claves.

Temas

- Activación y desactivación de la rotación automática de claves (consola)
- Habilitar y deshabilitar la rotación automática de claves (API)AWS KMS

Activación y desactivación de la rotación automática de claves (consola)

1. Inicie sesión en la consola AWS Key Management Service (AWS KMS) AWS Management Console y ábrala en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.

3. En el panel de navegación, elija Claves administradas por el cliente. (No puede habilitar o desactivar la rotación de Claves administradas por AWS. Estas rotan cada año de forma automática).
4. Elija el alias o el ID de clave de una clave KMS.
5. Seleccione la pestaña Key Rotation (Rotación de claves).

   La pestaña Rotación de claves solo aparece en la página de detalles de las claves KMS de cifrado simétrico con el material de claves que se AWS KMS generaron (el origen es AWS_KMS), incluidas las claves KMS de cifrado simétrico multirregional.

   No puede rotar de forma automática las claves KMS asimétricas, las claves KMS HMAC, las claves KMS con material de claves importado o las claves KMS en los almacenes de claves personalizados. Sin embargo, puede rotarlas manualmente.
6. En la sección Rotación automática de claves, selecciona Editar.
7. Para la rotación de claves, selecciona Activar.

   > **Note**
   >
   > Si una clave KMS está deshabilitada o pendiente de ser eliminada, AWS KMS no rota el material clave y no se puede actualizar el estado de rotación automática de la clave ni el período de rotación. Active la clave KMS o cancele la eliminación para actualizar la configuración de rotación automática de claves. Para más detalles, consulte Cómo funciona la rotación de teclas y Estados clave de AWS KMS las claves.
8. (Opcional) Escriba un período de rotación de entre 90 y 2560 días. El valor predeterminado es 365 días. Si no especifica un período de rotación personalizado, AWS KMS rotará el material clave cada año.

   Puede usar la clave de RotationPeriodInDays condición kms: para limitar los valores que los directores pueden especificar para el período de rotación.
9. Seleccione Guardar.

Habilitar y deshabilitar la rotación automática de claves (API)AWS KMS

Puedes usar la API AWS Key Management Service (AWS KMS) para activar y desactivar la rotación automática de claves y ver el estado actual de la rotación de cualquier clave gestionada por el

cliente. En estos ejemplos, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

La EnableKeyRotationoperación permite la rotación automática de claves para la clave KMS especificada. La DisableKeyRotationoperación la desactiva. Para identificar la clave KMS en estas operaciones, utilice el ID de la clave o el ARN de la clave. De forma predeterminada, la rotación de claves está desactivada para las claves KMS administradas por el cliente.

Puede usar la clave de RotationPeriodInDays condición kms: para limitar los valores que los principales pueden especificar para el `RotationPeriodInDays` parámetro de una `EnableKeyRotation` solicitud.

El siguiente ejemplo permite la rotación de claves con un período de rotación de 180 días en la clave KMS de cifrado simétrico especificada y utiliza la GetKeyRotationStatusoperación para ver el resultado. A continuación, se desactiva la rotación de claves y, de nuevo, se utiliza GetKeyRotationStatus para ver el cambio.

```
$ aws kms enable-key-rotation \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --rotation-period-in-days 180

$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyRotationEnabled": true,
    "RotationPeriodInDays": 180,
    "NextRotationDate": "2024-02-14T18:14:33.587000+00:00"
}

$ aws kms disable-key-rotation --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyRotationEnabled": false
}
```

¿Cómo realizar la rotación de claves bajo demanda

Puede realizar la rotación bajo demanda del material clave en las claves de KMS gestionadas por el cliente, independientemente de si la rotación automática de claves está habilitada o no. La desactivación de la rotación automática (DisableKeyRotation) no afecta a su capacidad para realizar rotaciones bajo demanda ni cancela ninguna rotación bajo demanda en curso. Las rotaciones bajo demanda no cambian los programas de rotación automática existentes. Por ejemplo, pensemos en una clave KMS que tenga habilitada la rotación automática de claves con un período de rotación de 730 días. Si la clave está programada para rotar automáticamente el 14 de abril de 2024 y usted realiza una rotación bajo demanda el 10 de abril de 2024, la clave rotará automáticamente, según lo programado, el 14 de abril de 2024 y, a partir de entonces, cada 730 días.

Puede realizar la rotación de claves bajo demanda un máximo de 10 veces por clave KMS. Puede utilizar la AWS KMS consola para ver el número de rotaciones bajo demanda restantes disponibles para una clave KMS.

La rotación de claves bajo demanda solo se admite en las claves KMS de cifrado simétrico. No puede realizar la rotación bajo demanda de claves KMS asimétricas, claves KMS HMAC, claves KMS con material de claves importado o claves KMS en un almacén de claves personalizado. Para realizar la rotación bajo demanda de un conjunto de claves multirregionales relacionadas, invoque la rotación bajo demanda en la clave principal.

Los usuarios autorizados pueden usar la AWS KMS consola y la AWS KMS API para iniciar la rotación de claves bajo demanda y ver el estado de la rotación de claves.

Temas

- Iniciar la rotación de claves bajo demanda (consola)
- Iniciar la rotación de claves bajo demanda (API)AWS KMS

Iniciar la rotación de claves bajo demanda (consola)

1. Inicie sesión en la consola AWS Key Management Service (AWS KMS) AWS Management Console y ábrala en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente. (No puede realizar la rotación bajo demanda de. Claves administradas por AWS Se rotan automáticamente cada año.)

4. Elija el alias o el ID de clave de una clave KMS.
5. Seleccione la pestaña Key Rotation (Rotación de claves).

   La pestaña Rotación de claves solo aparece en la página de detalles de las claves KMS de cifrado simétrico con el material de clave que AWS KMS se generaron (el origen es AWS_KMS), incluidas las claves KMS de cifrado simétrico multirregional.

   No puede realizar la rotación bajo demanda de claves KMS asimétricas, claves KMS HMAC, claves KMS con material de claves importado o claves KMS en almacenes de claves personalizados. Sin embargo, puede rotarlas manualmente.
6. En la sección Rotación de claves bajo demanda, selecciona Rotar clave.
7. Lea y tenga en cuenta la advertencia y la información sobre el número de rotaciones bajo demanda restantes de la clave. Si decide que no desea continuar con la rotación bajo demanda, seleccione Cancelar.
8. Seleccione la tecla Rotar para confirmar la rotación bajo demanda.

> **Note**
>
> La rotación bajo demanda está sujeta a los mismos posibles efectos de coherencia que otras operaciones AWS KMS de gestión. Es posible que haya un ligero retraso antes de que el nuevo material de claves esté disponible en AWS KMS. El cartel situado en la parte superior de la consola le avisa cuando se ha completado la rotación bajo demanda.

Iniciar la rotación de claves bajo demanda (API)AWS KMS

Puedes usar la API AWS Key Management Service (AWS KMS) para iniciar la rotación de claves bajo demanda y ver el estado actual de la rotación de cualquier clave gestionada por el cliente. En estos ejemplos, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

La RotateKeyOnDemandoperación inicia inmediatamente la rotación de claves bajo demanda para la clave de KMS especificada. Para identificar la clave KMS en estas operaciones, utilice el ID de la clave o el ARN de la clave.

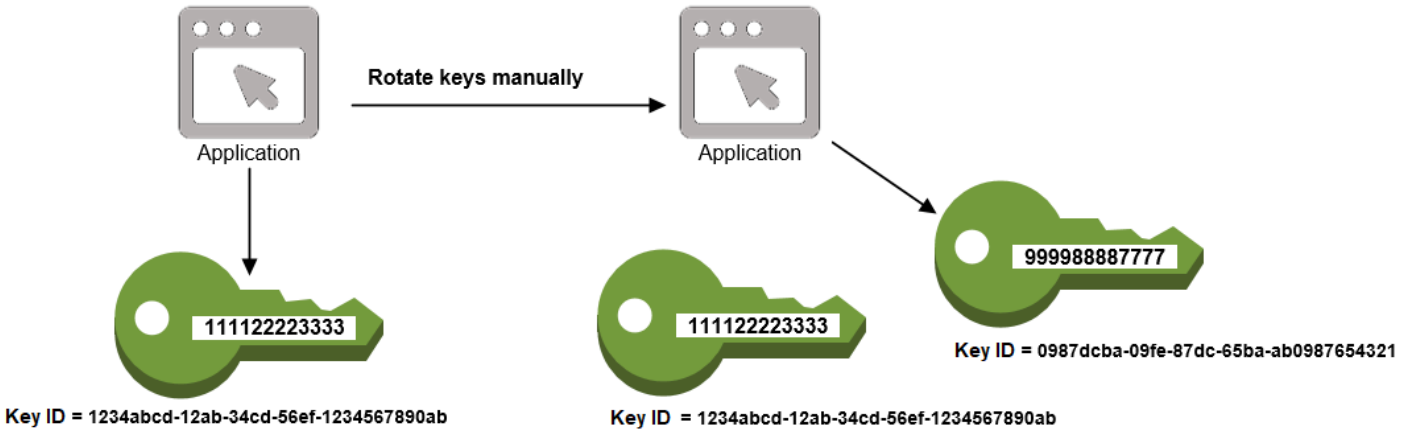
En el siguiente ejemplo, se inicia la rotación de claves bajo demanda en la clave KMS de cifrado simétrico especificada y se utiliza la GetKeyRotationStatusoperación para comprobar

que la rotación bajo demanda está en curso. `OnDemandRotationStartDate`En la `kms:GetKeyRotationStatus` respuesta, se identifica la fecha y la hora en que se inició una rotación bajo demanda en curso.

```
$ aws kms rotate-key-on-demand --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
}

$ aws kms get-key-rotation-status --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyRotationEnabled": true,
    "NextRotationDate": "2024-03-14T18:14:33.587000+00:00",
    "OnDemandRotationStartDate": "2024-02-24T18:44:48.587000+00:00"
    "RotationPeriodInDays": 365
}
```

Rotar manualmente las claves

Es posible que le interese crear una nueva clave KMS y utilizarla en sustitución de una clave KMS actual en lugar de activar la rotación automática de claves. Cuando la nueva clave KMS tiene diferente material criptográfico que la clave KMS actual, el uso de la nueva clave KMS tiene el mismo efecto que cambiar el material de claves de una clave KMS existente. El proceso de sustitución de una clave KMS por otra se denomina rotación manual de claves.



La rotación manual es una buena opción si desea rotar claves de KMS que no son aptas para la rotación automática de claves, como las claves KMS asimétricas, las claves KMS de HMAC, las

claves de KMS en almacenes de claves personalizados y las claves de KMS con material clave importado.

> **Note**
>
> Cuando empiece a usar la nueva clave KMS, asegúrese de mantener habilitada la clave KMS original para AWS KMS poder descifrar los datos cifrados por la clave KMS original.

Cuando rota las claves KMS de forma manual, también debe actualizar las referencias al ID de la clave KMS o al ARN de la clave en sus aplicaciones. Los alias, que asocian un nombre descriptivo a una clave KMS, pueden facilitar este proceso. Utilice un alias para hacer referencia a una clave KMS en sus aplicaciones. Después, cuando desee cambiar la clave KMS que utiliza la aplicación, en lugar editar su código de aplicación, cambie la clave KMS de destino del alias. Para obtener más detalles, consulte Usar alias en las aplicaciones.

> **Note**
>
> Los alias que apuntan a la última versión de una clave KMS girada manualmente son una buena solución para las operaciones de cifrado DescribeKey, GenerateDataKeyGenerateDataKeyPairGenerateMac, y firma. Los alias no están permitidos en las operaciones que administran claves de KMS, como o. DisableKeyScheduleKeyDeletion
> Al realizar la operación de descifrado en claves KMS de cifrado simétrico rotadas manualmente, omita el parámetro en el `KeyId` comando. AWS KMS utiliza automáticamente la clave KMS que cifró el texto cifrado.
> El `KeyId` parámetro es obligatorio cuando se llama `Decrypt` o se verifica con una clave KMS asimétrica, o cuando se llama VerifyMaccon una clave HMAC KMS. Estas solicitudes fallan cuando el valor del parámetro `KeyId` es un alias que ya no apunta a la clave de KMS que realizó la operación criptográfica, por ejemplo, cuando se rota una clave de forma manual. Para evitar este error, debe realizar un seguimiento y especificar la clave de KMS correcta para cada operación.

Para cambiar la clave KMS de destino de un alias, usa la UpdateAliasoperación en la AWS KMS API. Por ejemplo, este comando actualiza el alias `alias/TestKey` para apuntar hacia una nueva clave KMS. Como la operación no devuelve ningún resultado, en el ejemplo se usa la ListAliasesoperación para mostrar que el alias ahora está asociado a una clave de KMS diferente

y que el `LastUpdatedDate` campo está actualizado. Los ListAliases comandos utilizan el [queryparámetro](#) de AWS CLI para obtener únicamente el `alias/TestKey` alias.

```
$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/TestKey`]'
{
    "Aliases": [
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/TestKey",
            "AliasName": "alias/TestKey",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1521097200.123,
            "LastUpdatedDate": 1521097200.123
        },
    ]
}


$ aws kms update-alias --alias-name alias/TestKey --target-key-id
 0987dcba-09fe-87dc-65ba-ab0987654321

$ aws kms list-aliases --query 'Aliases[?AliasName==`alias/TestKey`]'
{
    "Aliases": [
        {
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/TestKey",
            "AliasName": "alias/TestKey",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1521097200.123,
            "LastUpdatedDate": 1604958290.722
        },
    ]
}
```

Supervisión de AWS KMS keys

El monitoreo es una parte importante para entender la disponibilidad, el estado y el uso de su AWS KMS keys en AWS KMS y mantener la fiabilidad, la disponibilidad y el rendimiento de las soluciones de AWS. La recopilación de los datos de monitoreo de todas las partes de su solución de AWS le ayudará a depurar un error que se produce en distintas partes del código, en caso de que ocurra. No obstante, antes de comenzar a monitorizar las claves KMS, debe crear un plan de monitorización que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de monitorización va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando suceda algo?

El siguiente paso es monitorear las claves KMS a lo largo del tiempo para establecer un punto de referencia para el uso normal de AWS KMS y las expectativas en su entorno. A medida que monitorice las claves KMS, almacene los datos de monitorización históricos para que pueda compararlos con los datos actuales, identificar los patrones normales y las anomalías, así como desarrollar métodos para la resolución de problemas.

Por ejemplo, puede monitorear la actividad de la API de AWS KMS y los eventos que afectan a su clave KMS. Cuando los datos están por encima o por debajo de las normas establecidas, es posible que efectuar una investigación o adoptar medidas correctivas.

Para establecer un punto de referencia para los patrones normales, monitorice los elementos siguientes:

- Actividad de la API de AWS KMS para las operaciones de plano de datos. Se trata de operaciones criptográficas que utilizan una clave KMS, como Decrypt, Encrypt y ReEncrypt. GenerateDataKey
- La actividad de la API de AWS KMS para las operaciones de plano de control que considera importantes. Estas operaciones administran una clave de KMS y es posible que desee supervisar las que modifican la disponibilidad de una clave de KMS (por ejemplo ScheduleKeyDeletion,, CancelKeyDeletionDisableKeyEnableKeyImportKeyMaterial, y DeleteImportedKeyMaterial) o cambian el control de acceso de una clave de KMS (por ejemplo, y). PutKeyPolicyRevokeGrant
- Otras métricas AWS KMS (como la cantidad de tiempo restante hasta que venza el material de claves importado) y eventos (como el vencimiento del material de claves importado o la eliminación de la rotación de claves de una clave KMS).

Herramientas de monitoreo

AWS proporciona varias herramientas que puede utilizar para monitorear sus claves KMS. Puede configurar algunas de estas herramientas para que monitoricen por usted, pero otras herramientas

requieren intervención manual. Le recomendamos que automatice las tareas de monitorización en la medida de lo posible.

Herramientas de monitoreo automatizadas

Puede utilizar las siguientes herramientas de monitorización automatizada para monitorizar sus claves KMS e informar cuando haya algún cambio.

- AWS CloudTrailSupervisión de registros: comparta archivos de registro entre cuentas, supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs, cree aplicaciones de procesamiento de registros con la biblioteca de CloudTrail procesamiento y valide que los archivos de registro no hayan cambiado después de su entrega CloudTrail. Para obtener más información, consulte Trabajar con archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.
- Amazon CloudWatch Alarms: observe una sola métrica durante un período de tiempo que especifique y realice una o más acciones en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo. La acción es una notificación enviada a un tema del Servicio de Notificación Simple (Amazon SNS) o a una política de Auto Scaling de Amazon EC2. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener más información, consulte Monitorización con Amazon CloudWatch.
- Amazon EventBridge: haga coincidir los eventos y diríjalos a una o más funciones o transmisiones de destino para capturar información de estado y, si es necesario, realizar cambios o tomar medidas correctivas. Para obtener más información, consulta Monitorización con Amazon EventBridge la Guía del EventBridge usuario de Amazon.
- Amazon CloudWatch Logs: supervise, almacene y acceda a sus archivos de registro desde AWS CloudTrail u otras fuentes. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.

Herramientas de monitoreo manuales

Otra parte importante de la supervisión de las claves de KMS implica la supervisión manual de los elementos que CloudWatch las alarmas y los eventos no cubren. Los AWS paneles AWS KMS CloudWatch,AWS Trusted Advisor, y otros proporcionan una at-a-glance vista del estado de su AWS entorno.

Puede personalizar las Claves administradas por AWS y las páginas Customer Managed Keys (Claves administradas por el cliente) de la consola de AWS KMS para mostrar la siguiente información sobre cada clave KMS:

- ID de clave
- Status
- Fecha de creación
- Fecha de vencimiento (para las claves KMS con material de claves importado)
- Origen
- ID de almacén de claves personalizado (para las claves KMS en almacenes de claves personalizados)

El panel de la consola de CloudWatch muestra lo siguiente:

- Alarmas y estado actual
- Gráficos de alarmas y recursos
- Estado de los servicios

Además, puede utilizarlos CloudWatch para hacer lo siguiente:

- Crear paneles personalizados para monitorizar los servicios que le interesan
- Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias
- Buscar y examinar todas sus métricas de recursos de AWS.
- Crear y editar las alarmas de notificación de problemas

AWS Trusted Advisor puede ayudarlo a monitorear los recursos de AWS para mejorar el rendimiento, la fiabilidad, la seguridad y la rentabilidad. Hay cuatro comprobaciones de Trusted Advisor disponibles para todos los usuarios y hay más de 50 comprobaciones disponibles para usuarios con un plan de soporte Business o Enterprise. Para obtener más información, consulte AWS Trusted Advisor.

Registrar llamadas a la AWS KMS API con AWS CloudTrail

AWS KMS está integrado con AWS CloudTrailun servicio que registra todas las llamadas realizadas AWS KMS por los usuarios, los roles y otros AWS servicios. CloudTrail captura todas las llamadas a

la API AWS KMS como eventos, incluidas las llamadas desde la AWS KMS consola, AWS KMS las API, las AWS CloudFormation plantillas, el AWS Command Line Interface (AWS CLI) y AWS Tools for PowerShell.

CloudTrail registra todas AWS KMS las operaciones, incluidas las operaciones de solo lectura, como ListAliasesy GetKeyRotationStatus, las operaciones que administran las claves de KMS, como CreateKeyy PutKeyPolicy, las operaciones criptográficas, como GenerateDataKeyDecrypt. También registra las operaciones internas que lo AWS KMS requieran, como,, DeleteExpiredKeyMaterialy DeleteKey. SynchronizeMultiRegionKeyRotateKey

CloudTrail registra las operaciones correctas y los intentos de llamadas que han fallado, por ejemplo, cuando se deniega el acceso a un recurso a la persona que llama. Las operaciones que utilizan claves de KMS en otras cuentas se registran tanto en la cuenta del autor de la llamada como en la cuenta del propietario de la clave de KMS. Sin embargo, AWS KMS las solicitudes entre cuentas que se rechazan porque se ha denegado el acceso se registran únicamente en la cuenta de la persona que llama.

Por motivos de seguridad, algunos campos se omiten de las entradas de AWS KMS registro, como el `Plaintext` parámetro de una solicitud de cifrado y la respuesta a GetKeyPolicycualquier operación criptográfica. Para facilitar la búsqueda de entradas de CloudTrail registro para determinadas claves de KMS, AWS KMS agrega el ARN de clave de la clave de KMS afectada al `responseElements` campo de las entradas de registro para algunas operaciones de administración de AWS KMS claves, incluso cuando la operación de API no devuelva el ARN de clave.

Aunque, de forma predeterminada, todas AWS KMS las acciones se registran como CloudTrail eventos, puedes AWS KMS excluirlas de un CloudTrail registro. Para obtener más detalles, consulte Excluir AWS KMS eventos de una ruta.

Más información:

- Para ver ejemplos de CloudTrail registro de AWS KMS las operaciones de un enclave de AWS Nitro, consulteSupervisión de las solicitudes para enclaves de Nitro.

Temas

- Registrar eventos en CloudTrail
- Buscando eventos en CloudTrail
- Excluir AWS KMS eventos de una ruta
- Ejemplos de entradas de AWS KMS registro

Registrar eventos en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS KMS, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos para AWS KMS ti, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen en función de ellos. Para obtener más información, consulte:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario. Para obtener más información acerca de otras formas para monitorear el uso de las claves KMS, consulte Supervisión de AWS KMS keys.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario raíz o credenciales de usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la hizo otra persona Servicio de AWS.

Para obtener más información, consulte el elemento CloudTrail UserIdentity.

Buscando eventos en CloudTrail

Para buscar entradas de CloudTrail registro, utilice la CloudTrail consola o la CloudTrail LookupEventsoperación. CloudTrail admite numerosos valores de atributos para filtrar la búsqueda, incluidos el nombre del evento, el nombre de usuario y la fuente del evento.

Para ayudarle a buscar entradas de AWS KMS registro CloudTrail, AWS KMS rellena los siguientes campos de entrada de CloudTrail registro.

> **Note**
>
> A partir de diciembre de 2022, AWS KMS rellena los atributos Tipo de recurso y Nombre del recurso en todas las operaciones de administración que cambien una clave de KMS concreta. Estos valores de atributo pueden ser nulos en CloudTrail las entradas anteriores para las siguientes operaciones: CreateAliasCreateGrantDeleteAlias, DeleteImportedKeyMaterial, ImportKeyMaterial, ReplicateKey, RetireGrant, RevokeGrantUpdateAlias, y UpdatePrimaryRegion.

Atributo	Valor	Entradas de registro
Fuente del evento (`EventSource`)	`kms.amazonaws.com`	Todas las operaciones.
Tipo de recurso (`ResourceType`)	`AWS::KMS::Key`	Operaciones de administración que cambian una clave de KMS en particular, como `CreateKey` y `EnableKey`, pero no `ListKeys`.
Nombre del recurso (`ResourceName`)	ARN de clave (o ID de clave y ARN de clave)	Operaciones de administración que cambian una clave de KMS en particular, como `CreateKey` y `EnableKey`, pero no `ListKeys`.

Para ayudarle a encontrar entradas de registro para las operaciones de administración en determinadas claves de KMS, AWS KMS registra el ARN de clave de la clave de KMS afectada en el `responseElements.keyId` elemento de la entrada de registro, incluso cuando la operación de AWS KMS API no devuelva el ARN de clave.

Por ejemplo, una llamada correcta a la DisableKeyoperación no devuelve ningún valor en la respuesta, pero en lugar de un valor nulo, el `responseElements.keyId` valor de la entrada de DisableKey registro incluye la clave ARN de la clave KMS deshabilitada.

Esta función se agregó en diciembre de 2022 y afecta a las siguientes entradas de CloudTrail registro: CreateAliasCreateGrantDeleteAlias, DeleteKey, DisableKey, EnableKey, EnableKeyRotation, ImportKeyMaterial, RotateKey, SynchronizeMultiRegionKey, TagResource, UntagResourceUpdateAlias, y UpdatePrimaryRegion.

Excluir AWS KMS eventos de una ruta

Para proporcionar un registro del uso y la administración de sus AWS KMS recursos, la mayoría de AWS KMS los usuarios se basan en los eventos de una CloudTrail ruta. El registro puede ser una fuente de datos valiosa para auditar eventos críticos, como la creación, inhabilitación y eliminación AWS KMS keys, el cambio de la política de claves y el uso de las claves de KMS por parte de AWS los servicios que actúan en su nombre. En algunos casos, los metadatos de una entrada de CloudTrail registro, como el contexto de cifrado de una operación de cifrado, pueden ayudarle a evitar o resolver errores.

Sin embargo, dado que AWS KMS puede generar una gran cantidad de eventos, AWS CloudTrail le permite excluir AWS KMS eventos de un registro. Esta configuración por ruta excluye todos los AWS KMS eventos; no puedes excluir eventos específicos AWS KMS .

> **Warning**
>
> Si se excluyen AWS KMS los eventos de un CloudTrail registro, se pueden ocultar las acciones que utilizan las claves de KMS. Actúe con precaución al conceder a las entidades principales el permiso `cloudtrail:PutEventSelectors` necesario para realizar esta operación.

Para excluir AWS KMS eventos de un registro:

- En la CloudTrail consola, utilice la configuración de eventos del Servicio de administración de claves de registro cuando cree o actualice una ruta. Para obtener instrucciones, consulte Registrar los eventos de administración AWS Management Console en la Guía del AWS CloudTrail usuario.
- En la CloudTrail API, utilice la PutEventSelectorsoperación. Agregue el atributo `ExcludeManagementEventSources` a sus selectores de eventos con un valor de `kms.amazonaws.com`. Para ver un ejemplo, consulte Ejemplo: una ruta que no registra AWS Key Management Service eventos en la Guía del AWS CloudTrail usuario.

Puede desactivar esta exclusión en cualquier momento cambiando la configuración de la consola o los selectores de eventos de un registro de seguimiento. A continuación, el sendero empezará a registrar AWS KMS los eventos. Sin embargo, no puede recuperar AWS KMS los eventos que ocurrieron mientras la exclusión estaba vigente.

Cuando excluyes AWS KMS eventos mediante la consola o la API, la operación de CloudTrail `PutEventSelectors` API resultante también se registra en tus CloudTrail registros. Si AWS KMS los eventos no aparecen en tus CloudTrail registros, busca un `PutEventSelectors` evento con el `ExcludeManagementEventSources` atributo establecido en`kms.amazonaws.com`.

Ejemplos de entradas de AWS KMS registro

AWS KMS escribe entradas en su CloudTrail registro cuando llama a una AWS KMS operación y cuando un AWS servicio llama a una operación en su nombre. AWS KMS también escribe una entrada cuando llama a una operación en tu nombre. Por ejemplo, escribe una entrada cuando elimina una clave KMS programado para su eliminación.

En los temas siguientes se muestran ejemplos de entradas de CloudTrail registro para AWS KMS las operaciones.

Para ver ejemplos de entradas de CloudTrail registro de solicitudes enviadas AWS KMS desde AWS Nitro Enclaves, consulte. Supervisión de las solicitudes para enclaves de Nitro

Temas

- CancelKeyDeletion
- ConnectCustomKeyStore
- CreateAlias
- CreateCustomKeyStore
- CreateGrant

- CreateKey
- Decrypt
- DeleteAlias
- DeleteCustomKeyStore
- DeleteExpiredKeyMaterial
- DeleteImportedKeyMaterial
- DeleteKey
- DescribeCustomKeyStores
- DescribeKey
- DisableKey
- DisableKeyRotation
- DisconnectCustomKeyStore
- EnableKey
- EnableKeyRotation
- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- GenerateRandom
- GetKeyPolicy
- GetKeyRotationStatus
- GetParametersForImport
- ImportKeyMaterial
- ListAliases
- ListGrants
- ListKeyRotations
- PutKeyPolicy
- ReEncrypt

- ReplicateKey
- RetireGrant
- RevokeGrant
- RotateKey
- RotateKeyOnDemand
- ScheduleKeyDeletion
- Sign
- SynchronizeMultiRegionKey
- TagResource
- UntagResource
- UpdateAlias
- UpdateCustomKeyStore
- UpdateKeyDescription
- UpdatePrimaryRegion
- VerifyMac
- Verificar
- Ejemplo uno de Amazon EC2
- Ejemplo dos de Amazon EC2

CancelKeyDeletion

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación CancelKeyDeletion. Para obtener información acerca de cómo eliminar AWS KMS keys, consulte Eliminación de AWS KMS keys.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
```

```
    },
    "eventTime": "2020-07-27T21:53:17Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CancelKeyDeletion",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "e3452e68-d4b0-4ec7-a768-7ae96c23764f",
    "eventID": "d818bf03-6655-48e9-8b26-f279a07075fd",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ConnectCustomKeyStore

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación `ConnectCustomKeyStore`. Para obtener información acerca conectar un almacén de claves personalizadas, consulte Conectar y desconectar un almacén de claves de AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
```

```
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ConnectCustomKeyStore",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreName": "ExampleKeyStore",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

CreateAlias

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la CreateAliasoperación. El elemento `resources` incluye campos para los recursos de alias y clave KMS. Para obtener más información acerca de la creación de alias en AWS KMS, consulte Crear un alias.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
```

```
    },
    "eventTime": "2022-08-14T23:08:31Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateAlias",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "aliasName": "alias/ExampleAlias",
        "targetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "caec1e0c-ce03-419e-bdab-6ab1f7c57c01",
    "eventID": "2dd6e784-8286-46a6-befd-d64e5a02fb28",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:alias/ExampleAlias"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


CreateCustomKeyStore

En el ejemplo siguiente, se muestra una entrada de registro de AWS CloudTrailgenerada llamando a la operación `CreateCustomKeyStore` en un almacén de claves de AWS CloudHSM. Para obtener información acerca de crear los almacenes de claves personalizadas, consulte Crear un almacén de claves de AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateCustomKeyStore",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreName": "ExampleKeyStore",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "responseElements": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

CreateGrant

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la CreateGrantoperación. Para obtener información acerca de cómo crear concesiones en AWS KMS, consulte Concesiones en AWS KMS.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

```
{
```

```
  "eventVersion": "1.02",
  "userIdentity": {
      "type": "IAMUser",
      "principalId": "EX_PRINCIPAL_ID",
      "arn": "arn:aws:iam::111122223333:user/Alice",
      "accountId": "111122223333",
      "accessKeyId": "EXAMPLE_KEY_ID",
      "userName": "Alice"
  },
  "eventTime": "2014-11-04T00:53:12Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "CreateGrant",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "AWS Internal",
  "requestParameters": {
      "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "constraints": {
          "encryptionContextSubset": {
              "ContextKey1": "Value1"
          }
      },
      "operations": ["Encrypt",
      "RetireGrant"],
      "granteePrincipal": "EX_PRINCIPAL_ID"
  },
  "responseElements": {
      "grantId": "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
      "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "requestID": "f3c08808-63bc-11e4-bc2b-4198b6150d5c",
  "eventID": "5d529779-2d27-42b5-92da-91aaea1fc4b5",
  "readOnly": false,
  "resources": [{
      "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

CreateKey

Estos ejemplos muestran las entradas de AWS CloudTrail registro de la CreateKeyoperación.

Una entrada de `CreateKey` registro puede ser el resultado de una `CreateKey` solicitud o de la `CreateKey` operación de una ReplicateKeysolicitud.

El siguiente ejemplo muestra una entrada de CloudTrail registro para una CreateKeyoperación que crea una clave KMS de cifrado simétrico. Para obtener información sobre cómo crear claves KMS, consulte Crear claves.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-08-10T22:38:27Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "description": "",
        "origin": "EXTERNAL",
        "bypassPolicyLockoutSafetyCheck": false,
        "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "keySpec": "SYMMETRIC_DEFAULT",
        "keyUsage": "ENCRYPT_DECRYPT"
    },
    "responseElements": {
        "keyMetadata": {
            "AWSAccountId": "111122223333",
            "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "creationDate": "Aug 10, 2022, 10:38:27 PM",
            "enabled": false,
```

```
            "description": "",
            "keyUsage": "ENCRYPT_DECRYPT",
            "keyState": "PendingImport",
            "origin": "EXTERNAL",
            "keyManager": "CUSTOMER",
            "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
            "keySpec": "SYMMETRIC_DEFAULT",
            "encryptionAlgorithms": [
                "SYMMETRIC_DEFAULT"
            ],
            "multiRegion": false
        }
    },
    "requestID": "1aef6713-0223-4ff7-9a6d-781360521930",
    "eventID": "36327b37-f4f6-40a9-92ab-48064ec905a2",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

El siguiente ejemplo muestra el CloudTrail registro de una `CreateKey` operación que crea una clave KMS de cifrado simétrico en un almacén de AWS CloudHSMclaves.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
```

```
    "eventTime": "2021-10-14T17:39:50Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyUsage": "ENCRYPT_DECRYPT",
        "bypassPolicyLockoutSafetyCheck": false,
        "origin": "AWS_CLOUDHSM",
        "keySpec": "SYMMETRIC_DEFAULT",
        "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "customKeyStoreId": "cks-1234567890abcdef0",
        "description": ""
    },
    "responseElements": {
        "keyMetadata": {
            "aWSAccountId": "111122223333",
            "keyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
            "creationDate": "Oct 14, 2021, 5:39:50 PM",
            "enabled": true,
            "description": "",
            "keyUsage": "ENCRYPT_DECRYPT",
            "keyState": "Enabled",
            "origin": "AWS_CLOUDHSM",
            "customKeyStoreId": "cks-1234567890abcdef0",
            "cloudHsmClusterId": "cluster-1a23b4cdefg",
            "keyManager": "CUSTOMER",
            "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
            "keySpec": "SYMMETRIC_DEFAULT",
            "encryptionAlgorithms": [
                "SYMMETRIC_DEFAULT"
            ],
            "multiRegion": false
        }
    },
    "additionalEventData": {
        "backingKey": "{\"keyHandle\":\"19\",\"backingKeyId\":\"backing-key-id\"}"
    },
    "requestID": "4f0b185c-588c-4767-9e90-c618f7e13cad",
    "eventID": "c73964b8-703d-49e4-bd9e-f773d0ee1e65",
    "readOnly": false,
```

```
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

El siguiente ejemplo muestra el CloudTrail registro de una `CreateKey` operación que crea una clave KMS de cifrado simétrico en un almacén de claves externo.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2022-09-07T22:37:45Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "tags": [],
        "keyUsage": "ENCRYPT_DECRYPT",
        "description": "",
        "origin": "EXTERNAL_KEY_STORE",
        "multiRegion": false,
        "keySpec": "SYMMETRIC_DEFAULT",
        "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "bypassPolicyLockoutSafetyCheck": false,
        "customKeyStoreId": "cks-1234567890abcdef0",
```

```
        "xksKeyId": "bb8562717f809024"
    },
    "responseElements": {
        "keyMetadata": {
            "aWSAccountId": "111122223333",
            "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "creationDate": "Dec 7, 2022, 10:37:45 PM",
            "enabled": true,
            "description": "",
            "keyUsage": "ENCRYPT_DECRYPT",
            "keyState": "Enabled",
            "origin": "EXTERNAL_KEY_STORE",
            "customKeyStoreId": "cks-1234567890abcdef0",
            "keyManager": "CUSTOMER",
            "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
            "keySpec": "SYMMETRIC_DEFAULT",
            "encryptionAlgorithms": [
                "SYMMETRIC_DEFAULT"
            ],
            "multiRegion": false,
            "xksKeyConfiguration": {
                "id": "bb8562717f809024"
            }
        }
    },
    "requestID": "ba197c82-3ac7-487a-8ff4-7736bbeb1316",
    "eventID": "838ad5f4-5fdd-4044-afd7-4dbd88c6af56",
    "readOnly": false,
    "resources": [
        {
            "accountId": "227179770375",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:227179770375:key/39c5eb22-
f37c-4956-92ca-89e8f8b57ab2"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

Estos ejemplos muestran entradas de registro de AWS CloudTrail para la operación Decrypt.

La entrada de CloudTrail registro de una `Decrypt` operación siempre incluye `encryptionAlgorithm` el valor `requestParameters` incluso si el algoritmo de cifrado no se especificó en la solicitud. El texto cifrado de la solicitud y el texto sin formato de la respuesta se omiten.

Temas

- Descifrar con una clave de cifrado simétrica estándar
- Error de descifrado con una clave de cifrado simétrica estándar
- Descifrar con una clave de KMS en un almacén de claves de AWS CloudHSM
- Descifrar con una clave de KMS en un almacén de claves externo
- Error de descifrado con una clave de KMS en un almacén de claves externo

Descifrar con una clave de cifrado simétrica estándar

A continuación se muestra un ejemplo de entrada de CloudTrail registro para una `Decrypt` operación con una clave de cifrado simétrica estándar.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-27T22:58:24Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
```

```
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionContext": {
            "Department": "Engineering",
            "Project": "Alpha"
        }
    },
    "responseElements": null,
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Error de descifrado con una clave de cifrado simétrica estándar

El siguiente ejemplo de entrada de CloudTrail registro registra una `Decrypt` operación fallida con una clave KMS de cifrado simétrico estándar. La excepción (`errorCode`) y el mensaje de error (`errorMessage`) incluidos lo ayudan a resolver el error.

En este caso, la clave de KMS de cifrado simétrica especificada en la solicitud `Decrypt` no era la clave de KMS de cifrado simétrica que se utilizó para cifrar los datos.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-11-24T18:57:43Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "errorCode": "IncorrectKeyException"
    "errorMessage": "The key ID in the request does not identify a CMK that can perform
 this operation.",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionContext": {
            "Department": "Engineering",
            "Project": "Alpha"
        }
    },
    "responseElements": null,
    "requestID": "22345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Descifrar con una clave de KMS en un almacén de claves de AWS CloudHSM

El siguiente ejemplo de entrada de CloudTrail registro registra una `Decrypt` operación con una clave KMS en un almacén de AWS CloudHSM claves. Todas las entradas de registro para operaciones criptográficas con clave KMS en un almacén de claves personalizado incluyen un campo `additionalEventData` con el `customKeyStoreId`. Los `additionalEventData` no están especificados en la solicitud.

```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-26T23:41:27Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionContext": {
            "Department": "Development",
            "Purpose": "Test"
        }
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "requestID": "e1b881f8-2048-41f8-b6cc-382b7857ec61",
    "eventID": "a79603d5-4cde-46fc-819c-a7cf547b9df4",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Descifrar con una clave de KMS en un almacén de claves externo

El siguiente ejemplo de entrada de CloudTrail registro registra una `Decrypt` operación con una clave KMS en un almacén de claves externo. Además de `customKeyStoreId`, el campo `additionalEventData` incluye el ID de clave externa (`XksKeyId`). Los `additionalEventData` no están especificados en la solicitud.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-11-24T00:26:58Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "encryptionContext": {
            "Department": "Engineering",
            "Purpose": "Test"
        }
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreId": "cks-9876543210fedcba9",
        "xksKeyId": "abc01234567890fe"
    },
    "requestID": "f1b881f8-2048-41f8-b6cc-382b7857ec61",
    "eventID": "b79603d5-4cde-46fc-819c-a7cf547b9df4",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Error de descifrado con una clave de KMS en un almacén de claves externo

El siguiente ejemplo de entrada de CloudTrail registro registra una solicitud fallida de una `Decrypt` operación con una clave KMS en un almacén de claves externo. CloudWatch registra las solicitudes que fallan, además de las solicitudes correctas. Al registrar un error, la entrada del CloudTrail registro incluye la excepción (ErrorCode) y el mensaje de error correspondiente (ErrorMessage).

Si la solicitud fallida llegó a su proxy del almacén de claves externo, como en este ejemplo, puede usar el valor `requestId` para asociar la solicitud fallida a la solicitud correspondiente que registre el proxy de su almacén de claves externo, si los proporciona.

Para obtener ayuda con las solicitudes de `Decrypt` en almacenes de claves externos, consulte Errores de descifrado.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-11-24T00:26:58Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "errorCode": "KMSInvalidStateException",
```

```
    "errorMessage": "The external key store proxy rejected the request because the
 specified ciphertext or additional authenticated data is corrupted, missing, or
 otherwise invalid.",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "encryptionContext": {
            "Department": "Engineering",
            "Purpose": "Test"
        }
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreId": "cks-9876543210fedcba9",
        "xksKeyId": "abc01234567890fe"
    },
    "requestID": "f1b881f8-2048-41f8-b6cc-382b7857ec61",
    "eventID": "b79603d5-4cde-46fc-819c-a7cf547b9df4",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


DeleteAlias

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la DeleteAliasoperación. Para obtener información sobre la eliminación de alias, consulte Eliminar un alias.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2014-11-04T00:52:27Z"
            }
        }
    },
    "eventTime": "2014-11-04T00:52:27Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "aliasName": "alias/my_alias"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "d9542792-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "12f48554-bb04-4991-9cfc-e7e85f68eda0",
    "readOnly": false,
    "resources": [{
        "ARN": "arn:aws:kms:us-east-1:111122223333:alias/my_alias",
        "accountId": "111122223333"
    },
    {
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
```

```
}
```

DeleteCustomKeyStore

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación `DeleteCustomKeyStore`. Para obtener información acerca de crear los almacenes de claves personalizadas, consulte Eliminar un almacén de claves de AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteCustomKeyStore",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreName": "ExampleKeyStore",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

DeleteExpiredKeyMaterial

Al importar material clave a una AWS KMS key (clave KMS), puede establecer una fecha y hora de caducidad para ese material clave. AWS KMSregistra una entrada en el CloudTrail registro al importar el material clave (con la configuración de caducidad) y al AWS KMS eliminar el material clave caducado. Para obtener información sobre cómo crear clave KMS con material de claves importado, consulte Importación de material clave para AWS KMS llaves.

En el ejemplo siguiente, se muestra una entrada de registro de AWS CloudTrail generada cuando AWS KMS elimina el material relacionado con claves caducado.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-01-01T16:00:00Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteExpiredKeyMaterial",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "cfa932fd-0d3a-4a76-a8b8-616863a2b547",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    }
}
```

DeleteImportedKeyMaterial

Si importa material clave a una clave KMS, puede eliminar el material clave importado en cualquier momento mediante la DeleteImportedKeyMaterialoperación. Cuando se elimina el material de claves importado de una clave de KMS, el estado de la clave de KMS cambia a `PendingImport` y no se la puede usar en ninguna operación criptográfica. Para obtener más detalles, consulte Eliminar el material de claves importado.

En el ejemplo siguiente, se muestra una entrada de registro de AWS CloudTrail generada para la operación `DeleteImportedKeyMaterial`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-10-04T21:43:33Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteImportedKeyMaterial",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"&example-key-arn-1;"
    },
    "requestID": "dcf0e82f-dad0-4622-a378-a5b964ad42c1",
    "eventID": "2afbb991-c668-4641-8a00-67d62e1fecbd",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DeleteKey

Estos ejemplos muestran la entrada de registro AWS CloudTrail que se genera cuando se elimina una clave KMS. Para eliminar una clave KMS, utilice la ScheduleKeyDeletionoperación. Una vez transcurrido el período de espera especificado, AWS KMS elimina la clave KMS y registra una entrada como la siguiente en el CloudTrail registro para registrar ese evento.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

Para ver un ejemplo de la entrada de CloudTrail registro de la `ScheduleKeyDeletion` operación, consulte. ScheduleKeyDeletion Para obtener más información acerca de cómo eliminar claves KMS, consulte Eliminación de AWS KMS keys.

El siguiente ejemplo de entrada de CloudTrail registro registra una `DeleteKey` operación de una clave de KMS con el material clave incluidoAWS KMS.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2020-07-31T00:07:00Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "b25f9cda-74e1-4458-847b-4972a0bf9668",
    "readOnly": false,
    "resources": [
```

```
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
     "managementEvent": true,
    "eventCategory": "Management"
}
```

La siguiente entrada de CloudTrail registro registra la `DeleteKey` operación de una clave KMS en un almacén de claves AWS CloudHSM personalizado.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-10-26T23:41:27Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "additionalEventData": {
        "customKeyStoreId": "cks-1234567890abcdef0",
        "clusterId": "cluster-1a23b4cdefg",
        "backingKeys": "[{\"keyHandle\":\"01\",\"backingKeyId\":\"backing-key-id\"}]",
        "backingKeysDeletionStatus": "[{\"keyHandle\":\"01\",\"backingKeyId\":
\"backing-key-id\",\"deletionStatus\":\"SUCCESS\"}]"
    },
    "eventID": "1234585c-4b0c-4340-ab11-662414b79239",
    "readOnly": false,
    "resources": [
```

```
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "managementEvent": true,
    "eventCategory": "Management"
}
```

DescribeCustomKeyStores

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación `DescribeCustomKeyStores`. Para obtener información acerca de la visualización de los almacenes de claves personalizadas, consulte Visualización de un almacén de claves de AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeCustomKeyStores",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "responseElements": null,
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "2ea1735f-628d-43e3-b2ee-486d02913a78",
    "readOnly": true,
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

DescribeKey

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la DescribeKeyoperación. AWS KMSregistra una entrada como la siguiente cuando se llama a la `DescribeKey` operación o se ven las claves de KMS en la AWS KMS consola. Esta llamada es el resultado de ver una clave en la consola de administración de AWS KMS.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-26T18:01:36Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
```

```
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

DisableKey

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la DisableKeyoperación. Para obtener más información acerca de cómo habilitar y desactivar AWS KMS keys en AWS KMS, consulte Habilitación y deshabilitación de claves.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:43Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DisableKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": false,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

DisableKeyRotation

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación DisableKeyRotation. Para obtener información acerca de la rotación de claves, consulte Rotativo AWS KMS keys.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T19:31:39Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DisableKeyRotation",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "d6a9351a-ed6e-4581-88d1-2a9a8a538497",
    "eventID": "6313164c-83aa-4cc3-9e1a-b7c426f7a5b1",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DisconnectCustomKeyStore

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación `DisconnectCustomKeyStore`. Para obtener información sobre cómo desconectar un almacén de claves personalizado, consulte Conectar y desconectar un almacén de claves de AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DisconnectCustomKeyStore",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0"
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreName": "ExampleKeyStore",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333"
}
```

EnableKey

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la EnableKeyoperación. Para obtener más información acerca de cómo habilitar y desactivar AWS KMS keys en AWS KMS, consulte Habilitación y deshabilitación de claves.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:20Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "EnableKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "d528a6fb-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "be393928-3629-4370-9634-567f9274d52e",
    "readOnly": false,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
```

```
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

EnableKeyRotation

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro de una llamada a la EnableKeyRotationoperación. Para ver un ejemplo de la entrada de CloudTrail registro que se escribe cuando se gira la clave, consulteRotateKey. Para obtener más información acerca de la rotación AWS KMS keys, consulte Rotativo AWS KMS keys.

> **Note**
>
> rotation-periodEs un parámetro de solicitud opcional. Si no especifica un período de rotación al habilitar la rotación automática de claves, el valor predeterminado es de 365 días.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-25T23:41:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "EnableKeyRotation",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "rotationPeriodInDays": 180
    },
```

```
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "81f5b794-452b-4d6a-932b-68c188165273",
    "eventID": "fefc43a7-8e06-419f-bcab-b3bf18d6a401",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Encrypt

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail para la operación Encrypt.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-07-14T20:17:42Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionContext": {
            "Department": "Engineering"
```

```
        },
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    },
    "responseElements": null,
    "requestID": "f3423043-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "91235988-eb87-476a-ac2c-0cdc244e6dca",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKey

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la GenerateDataKeyoperación.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "keySpec": "AES_256",
        "encryptionContext": {
```

```
            "Department": "Engineering",
            "Project": "Alpha"
        }
    },
    "responseElements": null,
    "requestID": "e0eb83e3-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a9dea4f9-8395-46c0-942c-f509c02c2b71",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKeyPair

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la GenerateDataKeyPairoperación. En este ejemplo se registra una operación que genera un par de claves de RSA cifrado bajo una AWS KMS key de cifrado simétrica.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-27T18:57:57Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyPair",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyPairSpec": "RSA_3072",
        "encryptionContext": {
            "Project": "Alpha"
```

```
        },
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "52fb127b-0fe5-42bb-8e5e-f560febde6b0",
    "eventID": "9b6bd6d2-529d-4890-a949-593b13800ad7",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKeyPairWithoutPlaintext

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la GenerateDataKeyPairWithoutPlaintextoperación. En este ejemplo se registra una operación que genera un par de claves de RSA cifrado bajo un AWS KMS key de cifrado simétrico.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-27T18:57:57Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyPairWithoutPlaintext",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyPairSpec": "RSA_4096",
```

```
        "encryptionContext": {
            "Index": "5"
        },
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "52fb127b-0fe5-42bb-8e5e-f560febde6b0",
    "eventID": "9b6bd6d2-529d-4890-a949-593b13800ad7",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKeyWithoutPlaintext

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la GenerateDataKeyWithoutPlaintextoperación.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyWithoutPlaintext",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "errorCode": "InvalidKeyUsageException",
```

```
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "keySpec": "AES_256",
        "encryptionContext": {
            "Project": "Alpha"
        }
    },
    "responseElements": null,
    "requestID": "d6b8e411-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "f7734272-9ec5-4c80-9f36-528ebbe35e4a",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateMac

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la GenerateMacoperación.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
     },
    "eventTime": "2022-12-23T19:26:54Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateMac",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "macAlgorithm": "HMAC_SHA_512",
```

```
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "e0eb83e3-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a9dea4f9-8395-46c0-942c-f509c02c2b71",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateRandom

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la GenerateRandomoperación. Debido a que esta operación no utiliza una AWS KMS key, el campo `resources` está vacío.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateRandom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "df1e3de6-63bc-11e4-bc2b-4198b6150d5c",
```

```
    "eventID": "239cb9f7-ae05-4c94-9221-6ea30eef0442",
    "readOnly": true,
    "resources": [],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GetKeyPolicy

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la GetKeyPolicyoperación. Para obtener información acerca de cómo ver la política de claves de una clave KMS, consulte Consultar una política de claves.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:50:30Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GetKeyPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "policyName": "default"
    },
    "responseElements": null,
    "requestID": "93746dd6-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "4aa7e4d5-d047-452a-a5a6-2cce282a7e82",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
```

```
    "recipientAccountId": "111122223333"
}
```

GetKeyRotationStatus

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro de la GetKeyRotationStatusoperación. Para obtener información sobre la rotación automática y bajo demanda del material clave de una clave de KMS, consulteRotativo AWS KMS keys.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2024-02-20T19:16:45Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GetKeyRotationStatus",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "12f9b7e8-49b9-4c1c-a7e3-34ac0cdf0467",
    "eventID": "3d082126-9e7d-4167-8372-a6cfcbed4be6",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

```
    "eventCategory": "Management"
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
}
```

GetParametersForImport

En el siguiente ejemplo, se muestra una entrada de AWS CloudTrail registro generada al utilizar la GetParametersForImportoperación. Esta operación devuelve la clave pública y el token de importación que se utiliza al importar material de claves en una clave KMS. La misma CloudTrail entrada se registra cuando se utiliza la `GetParametersForImport` operación o se utiliza la AWS KMS consola para descargar la clave pública y el token de importación.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-25T23:58:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GetParametersForImport",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "wrappingAlgorithm": "RSAES_OAEP_SHA_256",
        "wrappingKeySpec": "RSA_2048"
    },
    "responseElements": null,
    "requestID": "b5786406-e3c7-43d6-8d3c-6d5ef96e2278",
    "eventID": "4023e622-0c3e-4324-bdef-7f58193bba87",
    "readOnly": true,
    "resources": [
        {
```

```
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ImportKeyMaterial

En el siguiente ejemplo, se muestra una entrada de AWS CloudTrail registro generada al utilizar la ImportKeyMaterialoperación. La misma CloudTrail entrada se graba cuando se utiliza la `ImportKeyMaterial` operación o se utiliza la AWS KMS consola para importar material clave a unAWS KMS key.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-26T00:08:00Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ImportKeyMaterial",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "validTo": "Jan 1, 2021 8:00:00 PM",
        "expirationModel": "KEY_MATERIAL_EXPIRES"
    },
    "responseElements": {
```

```
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "89e10ee7-a612-414d-95a2-a128346969fd",
    "eventID": "c7abd205-a5a2-4430-bbfa-fc10f3e2d79f",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ListAliases

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la ListAliasesoperación. Debido a que esta operación no utiliza ningún alias o AWS KMS key en particular, el campo `resources` está vacío. Para obtener información acerca de cómo visualizar los alias en AWS KMS, consulte Visualización de alias.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:51:45Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListAliases",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "limit": 5,
```

```
        "marker":
 "eyJiIjoiYWxpYXMvZTU0Y2MxOTMtYTMwNC00YzEwLTliZWItYTJjZjA3NjA2OTJhIiwiYSI6ImFsaWFzL2U1NGNjMTkzL
    },
    "responseElements": null,
    "requestID": "bfe6c190-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a27dda7b-76f1-4ac3-8b40-42dfba77bcd6",
    "readOnly": true,
    "resources": [],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ListGrants

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la ListGrantoperación. Para obtener más información sobre las concesiones en AWS KMS, consulte Concesiones en AWS KMS.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:49Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListGrants",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "marker":
 "eyJncmFudElkIjoiMWY4M2U2ZmM0YTY2NDgxYjQ2Yzc4MTdhM2Y4YmQwMDFkZDNiYmQ1MGVlYTMyY2RmOWFiNWY1Nzc1N
\u003d\u003d",
        "limit": 10
    },
    "responseElements": null,
    "requestID": "e5c23960-63bc-11e4-bc2b-4198b6150d5c",
```

```
    "eventID": "d24380f5-1b20-4253-8e92-dd0492b3bd3d",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

ListKeyRotations

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro de la ListKeyRotationsoperación. Para obtener información sobre la rotación automática y bajo demanda del material clave de una clave de KMS, consulteRotativo AWS KMS keys.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2024-02-20T19:16:45Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ListKeyRotations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "99c88d32-f2db-455e-8a9a-23855258a452",
    "eventID": "8ce0e74b-b9c7-45a2-96ef-83136d38068e",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
```

```
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
}
```

PutKeyPolicy

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación PutKeyPolicy. Para obtener información sobre cómo actualizar una política de claves, consulte Cambiar una política de claves.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T20:06:16Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "PutKeyPolicy",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "policyName": "default",
        "policy": "{\n  \"Version\" : \"2012-10-17\",\n  \"Id\" : \"key-default-1\",\n
 \"Statement\" : [ {\n    \"Sid\" : \"Enable IAM User Permissions\",\n    \"Effect\" :
```

```
 \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::111122223333:root
\"\n    },\n    \"Action\" : \"kms:*\",\n    \"Resource\" : \"*\"\n  } ]\n}",
        "bypassPolicyLockoutSafetyCheck": false
    },
    "responseElements": null,
    "requestID": "7bb906fa-dc21-4350-b65c-808ff0f72f55",
    "eventID": "c217db1f-903f-4a2f-8f88-9580182d6313",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


ReEncrypt

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la ReEncryptoperación. El campo `resources` en esta entrada de registro especifica dos AWS KMS keys, la clave KMS de origen y la clave KMS de destino, en ese orden.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-27T23:09:13Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ReEncrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "AWS Internal",
    "requestParameters": {
        "sourceEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "sourceEncryptionContext": {
            "Project": "Alpha",
            "Department": "Engineering"
        },
        "destinationKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "destinationEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "destinationEncryptionContext": {
            "Level": "3A"
        }
    },
    "responseElements": null,
    "requestID": "03769fd4-acf9-4b33-adf3-2ab8ca73aadf",
    "eventID": "542d9e04-0e8d-4e05-bf4b-4bdeb032e6ec",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        },
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


ReplicateKey

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación ReplicateKey. Una `ReplicateKey` solicitud da como resultado una `ReplicateKey` operación y una CreateKeyoperación.

Para obtener información acerca de la replicación de claves de varias regiones, consulte Creación de claves de réplica de varias regiones.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-11-18T01:29:18Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ReplicateKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "replicaRegion": "us-west-2",
        "bypassPolicyLockoutSafetyCheck": false,
        "description": ""
    },
    "responseElements": {
        "replicaKeyMetadata": {
            "aWSAccountId": "111122223333",
            "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "creationDate": "Nov 18, 2020, 1:29:18 AM",
            "enabled": false,
            "description": "",
            "keyUsage": "ENCRYPT_DECRYPT",
            "keyState": "Creating",
            "origin": "AWS_KMS",
            "keyManager": "CUSTOMER",
            "keySpec": "SYMMETRIC_DEFAULT",
            "customerMasterKeySpec": "SYMMETRIC_DEFAULT",
            "encryptionAlgorithms": [
                "SYMMETRIC_DEFAULT"
            ],
            "multiRegion": true,
            "multiRegionConfiguration": {
                "multiRegionKeyType": "REPLICA",
```

```
                "primaryKey": {
                    "arn": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                    "region": "us-east-1"
                },
                "replicaKeys": [
                    {
                        "arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                        "region": "us-west-2"
                    }
                ]
            }
        },
        "replicaPolicy": "{\n  \"Version\":\"2012-10-17\",\n  \"Statement\":[{\n
 \"Effect\":\"Allow\",\n    \"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:user/
Alice\"},\n    \"Action\":\"kms:*\",\n    \"Resource\":\"*\"\n  }, {\n    \"Effect
\":\"Allow\",\n    \"Principal\":{\"AWS\":\"arn:aws:iam::012345678901:user/Bob\"},\n
    \"Action\":\"kms:CreateGrant\",\n    \"Resource\":\"*\"\n  }, {\n    \"Effect\":
\"Allow\",\n    \"Principal\":{\"AWS\":\"arn:aws:iam::012345678901:user/Charlie\"},\n
  \"Action\":\"kms:Encrypt\",\n    \"Resource\":\"*\"\n}]\n}",
    },
    "requestID": "abcdef68-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "fedcba44-6773-4f96-8763-1993aec9ae6a",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

RetireGrant

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación RetireGrant. Para obtener más información sobre las concesiones que van a retirarse, consulte Retiro y revocación de concesiones.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T19:39:33Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RetireGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "grantId": "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a"
    },
    "requestID": "1d274d57-5697-462c-a004-f25fcc29fa26",
    "eventID": "0771bcfb-3e24-4332-9ac8-e1c06563eecf",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

RevokeGrant

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación RevokeGrant. Para obtener más información sobre las concesiones que van a retirarse, consulte Retiro y revocación de concesiones.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T19:35:17Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RevokeGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "grantId": "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a"
    },
    "responseElements": null,
    "requestID": "59d94c03-c5b7-428d-ae6e-f2c4b47d2917",
    "eventID": "07a23a39-6526-4ae2-b31e-d35fbe9e24ee",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

RotateKey

Estos ejemplos muestran las entradas de AWS CloudTrail registro de las operaciones que giran AWS KMS keys. Para obtener más información acerca de rotación de claves KMS, consulte Rotativo AWS KMS keys.

El siguiente ejemplo muestra una entrada de CloudTrail registro para la operación que rota una clave KMS de cifrado simétrico en la que está habilitada la rotación automática de claves. Para obtener información sobre cómo activar la rotación automática, consulte. Cómo habilitar y desactivar la rotación automática de claves

Para ver un ejemplo de la entrada de CloudTrail registro que registra la `EnableKeyRotation` operación, consulteEnableKeyRotation.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-01-14T01:41:59Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "rotationType": "AUTOMATIC",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
```

```
    },
    "eventCategory": "Management"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro de una RotateKeyOnDemandoperación. Para obtener información sobre la rotación de claves KMS de cifrado simétrico bajo demanda, consulte¿Cómo realizar la rotación de claves bajo demanda.

Para ver un ejemplo de la entrada de CloudTrail registro que registra la `RotateKeyOnDemand` operación, consulteRotateKeyOnDemand.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-01-14T01:41:59Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "a24b3967-ddad-417f-9b22-2332b918db06",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
        "rotationType": "ON_DEMAND",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "eventCategory": "Management"
```

```
}
```

RotateKeyOnDemand

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro de la RotateKeyOnDemandoperación. Para ver un ejemplo de la entrada de CloudTrail registro que se escribe cuando se gira la clave, consulteRotateKey. Para obtener más información sobre la rotación bajo demanda del material clave de una clave de KMS, consulte¿Cómo realizar la rotación de claves bajo demanda.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2024-02-20T17:41:57Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "RotateKeyOnDemand",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "9e1dee86-eb84-42fd-8f25-e3fc7dbb32c8",
    "eventID": "00a09fbc-20d6-4a58-9b92-7da85984ab77",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
```

```
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES256-GCM-SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
}
```

ScheduleKeyDeletion

En estos ejemplos se muestran las entradas de AWS CloudTrail registro de la ScheduleKeyDeletionoperación.

Para ver un ejemplo de la entrada de CloudTrail registro que se escribe cuando se elimina la clave, consulteDeleteKey. Para obtener información acerca de cómo eliminar AWS KMS keys, consulte Eliminación de AWS KMS keys.

En el siguiente ejemplo se registra una solicitud de `ScheduleKeyDeletion` para una clave KMS de una región.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2021-03-23T18:58:30Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ScheduleKeyDeletion",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "pendingWindowInDays": 20,
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
```

```
    "responseElements": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "keyState": "PendingDeletion",
        "deletionDate": "Apr 12, 2021 18:58:30 PM"
    },
    "requestID": "ee408f36-ea01-422b-ac14-b0f147c68334",
    "eventID": "3c4226b0-1e81-48a8-a333-7fa5f3cbd118",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

En el siguiente ejemplo se registra una solicitud de `ScheduleKeyDeletion` para una clave KMS de varias regiones con claves de réplica.

Porque AWS KMS no eliminará una clave de varias regiones hasta que se eliminen todas sus claves de réplica, en el campo `responseElements`, `keyState` es `PendingReplicaDeletion` y el campo `deletionDate` se omite.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2021-10-28T17:59:05Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ScheduleKeyDeletion",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "AWS Internal",
    "requestParameters": {
        "pendingWindowInDays": 30,
        "keyId": "mrk-1234abcd12ab34cd56ef1234567890ab"
    },
    "responseElements": {
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "keyState": "PendingReplicaDeletion",
        "pendingWindowInDays": 30
    },
    "requestID": "12341411-d846-42a6-a476-b1cbe3011f89",
    "eventID": "abcda5f-396d-494c-9380-0c47860df5f1",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

En el siguiente ejemplo se registra una solicitud de `ScheduleKeyDeletion` para una clave KMS en un almacén de claves personalizado de AWS CloudHSM.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2021-10-26T23:25:25Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "ScheduleKeyDeletion",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "pendingWindowInDays": 30
    },
    "responseElements": {
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "deletionDate": "Nov 2, 2021, 11:25:25 PM",
        "keyState": "PendingDeletion",
        "pendingWindowInDays": 30
    },
    "additionalEventData": {
        "customKeyStoreId": "cks-1234567890abcdef0",
        "clusterId": "cluster-1a23b4cdefg",
        "backingKeys": "[{\"keyHandle\":\"01\",\"backingKeyId\":\"backing-key-id\"}]"
    },
    "requestID": "abcd9f60-2c9c-4a0b-a456-d5d998f7f321",
    "eventID": "ca01996a-01b0-4edd-bbbb-25d7b6d1a6fa",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Sign

Estos ejemplos muestran entradas de registro de AWS CloudTrail para la operación Sign.

El siguiente ejemplo muestra una entrada de CloudTrail registro para una operación de firma que utiliza una clave RSA KMS asimétrica para generar una firma digital para un archivo.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-03-07T22:36:44Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Sign",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "messageType": "RAW",
        "keyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "signingAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256"
    },
    "responseElements": null,
    "requestID": "8d0b35e0-46cf-48b9-be99-bf2ebc9ab9fb",
    "eventID": "107b3cac-b125-4556-9702-12a2b9afcff7",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


SynchronizeMultiRegionKey

En el ejemplo siguiente, se muestra una entrada de registro de AWS CloudTrail generada cuando AWS KMS sincroniza una clave de varias regiones. La sincronización implica llamadas entre

regiones para copiar las propiedades compartidas de una clave principal de varias regiones a sus claves de réplica. AWS KMS sincroniza las claves de varias regiones periódicamente para garantizar que todas las claves de varias regiones relacionadas tengan el mismo material clave.

El `resources` elemento de la entrada de CloudTrail registro incluye la clave ARN de la clave principal multirregional, incluida la suya. Región de AWS Las claves de réplica de varias regiones relacionadas y sus Regiones no se enumeran en esta entrada de registro.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen el ARN clave de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva el ARN de clave.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2020-11-18T02:04:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "SynchronizeMultiRegionKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "12345681-de97-42e9-bed0-b02ae1abd8dc",
    "eventID": "abcdec99-2b5c-4670-9521-ddb8f031e146",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
```

```
    "eventCategory": "Management"
}
```

TagResource

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro de una llamada a la TagResourceoperación para añadir una etiqueta con una clave de etiqueta `Department` y un valor de etiqueta de`IT`.

Para ver un ejemplo de una entrada de `UntagResource` CloudTrail registro que se escribe cuando se gira la clave, consulteUntagResource. Para obtener más información acerca del etiquetado AWS KMS keys, consulte Etiquetado de claves.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-01T21:19:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "tags": [
            {
                "tagKey": "Department",
                "tagValue": "IT"
            }
        ]
    },
    "responseElements": null,
    "requestID": "b942584a-f77d-4787-9feb-b9c5be6e746d",
    "eventID": "0a091b9b-0df5-4cf9-b667-6f2879532b8f",
    "readOnly": false,
```

```
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

UntagResource

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro de una llamada a la UntagResourceoperación para eliminar una etiqueta con una clave de etiqueta de`Dept`.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

Para ver un ejemplo de una entrada de `TagResource` CloudTrail registro, consulte. TagResource Para obtener más información acerca del etiquetado AWS KMS keys, consulte Etiquetado de claves.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-01T21:19:19Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
        "tagKeys": [
            "Dept"
        ]
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "cb1d507b-6015-47f4-812b-179713af8068",
    "eventID": "0b00f4b0-036e-411d-aa75-87eb4a35a4b3",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

UpdateAlias

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la UpdateAliasoperación. El elemento `resources` incluye campos para los recursos de alias y clave KMS. Para obtener más información acerca de la creación de alias en AWS KMS, consulte Crear un alias.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen la clave ARN de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva la clave ARN.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
         "principalId": "EX_PRINCIPAL_ID",
         "arn": "arn:aws:iam::111122223333:user/Alice",
         "accountId": "111122223333",
         "accessKeyId": "EXAMPLE_KEY_ID",
         "userName": "Alice"
    },
```

```
    "eventTime": "2020-11-13T23:18:15Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdateAlias",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "aliasName": "alias/my_alias",
        "targetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "d9472f40-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "f72d3993-864f-48d6-8f16-e26e1ae8dff0",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:alias/my_alias"
        },
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```


UpdateCustomKeyStore

En el siguiente ejemplo, se muestra una entrada de registro de AWS CloudTrail generada llamando a la operación `UpdateCustomKeyStore` para actualizar el ID de clúster de un almacén de claves personalizado. Para obtener información acerca de cómo editar los almacenes de claves personalizadas, consulte Editar la configuración del almacén de claves de AWS CloudHSM.


```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2021-10-21T20:17:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdateCustomKeyStore",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "customKeyStoreId": "cks-1234567890abcdef0",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreName": "ExampleKeyStore",
        "clusterId": "cluster-1a23b4cdefg"
    },
    "requestID": "abcde9e1-f1a3-4460-a423-577fb6e695c9",
    "eventID": "114b61b9-0ea6-47f5-a9d2-4f2bdd0017d5",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
}
```

UpdateKeyDescription

En el ejemplo siguiente, se muestra una entrada de registro AWS CloudTrail generada llamando a la operación UpdateKeyDescription.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
```

```
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-09-01T19:22:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdateKeyDescription",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "description": "New key description"
    },
    "responseElements": null,
    "requestID": "8c3c1f8b-336d-4896-b034-4eb9916bc9b3",
    "eventID": "f5f3d548-2e9e-4658-8427-9dcb5b1ea791",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


UpdatePrimaryRegion

El siguiente ejemplo muestra las entradas de AWS CloudTrail registro que se generan al llamar a la UpdatePrimaryRegionoperación con una clave multirregional.

La `UpdatePrimaryRegion` operación escribe dos entradas de CloudTrail registro: una en la región con la clave principal multirregional que se convierte en una clave de réplica y otra en la región con una clave de réplica multirregional que se convierte en clave principal.

CloudTrail las entradas de registro de esta operación registradas a partir de diciembre de 2022 incluyen el ARN clave de la clave KMS afectada en el `responseElements.keyId` valor, aunque esta operación no devuelva el ARN de clave.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro correspondiente a la región `UpdatePrimaryRegion` en la que la clave multirregional pasó de ser una clave principal a una clave de réplica (us-west-2). El campo `primaryRegion` muestra la región que ahora aloja la clave principal (ap-northeast-1).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2021-03-10T20:23:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdatePrimaryRegion",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "primaryRegion": "ap-northeast-1"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "ee408f36-ea01-422b-ac14-b0f147c68334",
    "eventID": "3c4226b0-1e81-48a8-a333-7fa5f3cbd118",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
```

```
    "recipientAccountId": "111122223333"
}
```

El siguiente ejemplo representa la entrada de CloudTrail registro de la región `UpdatePrimaryRegion` en la que la clave multirregional pasó de ser una clave réplica a una clave principal (ap-northeast-1). Esta entrada de registro no identifica la región principal anterior.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "invokedBy": "kms.amazonaws.com"
    },
    "eventTime": "2021-03-10T20:23:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "UpdatePrimaryRegion",
    "awsRegion": "ap-northeast-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "primaryRegion": "ap-northeast-1"
    },
    "responseElements": {
        "keyId":"arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "ee408f36-ea01-422b-ac14-b0f147c68334",
    "eventID": "091e6be5-737f-43c6-8431-e3679d6d0619",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```

VerifyMac

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro para la VerifyMacoperación.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
     },
    "eventTime": "2022-03-31T19:25:54Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "VerifyMac",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "macAlgorithm": "HMAC_SHA_384",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "requestID": "f35da560-edff-4d6e-9b40-fb306fa9ef1e",
    "eventID": "6b464487-6dea-44cd-84ad-225d7450c975",
    "readOnly": true,
    "resources": [
        {
           "accountId": "111122223333",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Verificar

En estos ejemplos, se muestran entradas de registro de AWS CloudTrail para la operación Verify.

El siguiente ejemplo muestra una entrada de CloudTrail registro para una operación de verificación que usa una clave RSA KMS asimétrica para verificar una firma digital.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2022-03-07T22:50:41Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Verify",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "signingAlgorithm": "RSASSA_PKCS1_V1_5_SHA_256",
        "keyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "messageType": "RAW"
    },
    "responseElements": null,
    "requestID": "c73ab82a-af82-4750-ae2c-b6bb790e9c28",
    "eventID": "3b4331cd-5b7b-4de5-bf5f-82ec22f0dac0",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Ejemplo uno de Amazon EC2

En el siguiente ejemplo registra a una entidad principal de IAM que crea un volumen cifrado con la clave de volumen predeterminada en la consola de administración de Amazon EC2.

El siguiente ejemplo muestra una entrada de CloudTrail registro en la que la usuaria Alice crea un volumen cifrado con una clave de volumen predeterminada en la consola de administración de Amazon EC2. El archivo de registro de EC2 incluye el campo `volumeId` con el valor `"vol-13439757"`. El registro de AWS KMS contiene un campo `encryptionContext` con un valor de `"aws:ebs:id": "vol-13439757"`. Del mismo modo, coinciden `principalId` y `accountId` entre los dos registros. Los registros reflejan el hecho de que crear un volumen cifrado genera una clave de datos que se utiliza para cifrar el contenido del volumen.

```
{
  "Records": [
     {
      "eventVersion": "1.02",
      "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
        },
      "eventTime": "2014-11-05T20:50:18Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "CreateVolume",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "AWS Internal",
      "requestParameters": {
        "size": "10",
        "zone": "us-east-1a",
        "volumeType": "gp2",
        "encrypted": true
      },
      "responseElements": {
        "volumeId": "vol-13439757",
        "size": "10",
        "zone": "us-east-1a",
        "status": "creating",
```

```
        "createTime": 1415220618876,
        "volumeType": "gp2",
        "iops": 30,
        "encrypted": true
      },
      "requestID": "1565210e-73d0-4912-854c-b15ed349e526",
      "eventID": "a3447186-135f-4b00-8424-bc41f1a93b4f",
      "eventType": "AwsApiCall",
      "recipientAccountId": "123456789012"
    },
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
      },
      "eventTime": "2014-11-05T20:50:19Z",
      "eventSource": "kms.amazonaws.com",
      "eventName": "GenerateDataKeyWithoutPlaintext",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "&AWS; Internal",
      "requestParameters": {
        "encryptionContext": {
          "aws:ebs:id": "vol-13439757"
        },
        "numberOfBytes": 64,
        "keyId": "alias/aws/ebs"
      },
      "responseElements": null,
      "requestID": "create-123456789012-758241111-1415220618",
      "eventID": "4bd2a696-d833-48cc-b72c-05e61b608399",
      "readOnly": true,
      "resources": [
        {
          "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "accountId": "111122223333"
        }
      ],
```

```
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Ejemplo dos de Amazon EC2

En el ejemplo siguiente, una entidad principal de IAM que ejecuta una instancia de Amazon EC2 crea y monta un volumen de datos cifrado con una clave KMS. Esta acción genera varios CloudTrail registros.

Cuando se crea el volumen, Amazon EC2, actuando en nombre del cliente, obtiene una clave de datos cifrada de AWS KMS (`GenerateDataKeyWithoutPlaintext`). Luego crea una concesión (`CreateGrant`) que le permite descifrar la clave de datos. Cuando se monta el volumen, Amazon EC2 llama a AWS KMS para descifrar la clave de datos (`Decrypt`).

La `instanceId` de la instancia de Amazon EC2, `"i-81e2f56c"`, aparece en el evento `RunInstances`. El mismo ID de instancia califica el `granteePrincipal` de la concesión que se crea (`"111122223333:aws:ec2-infrastructure:i-81e2f56c"`) y el rol asumido que es la entidad principal en la llamada `Decrypt` (`"arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/i-81e2f56c"`).

El ARN de clave de la clave KMS que protege el volumen de datos `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`, aparece en las tres llamadas de AWS KMS (`CreateGrant`, `GenerateDataKeyWithoutPlaintext` y `Decrypt`).

```
{
  "Records": [
    {
      "eventVersion": "1.02",
      "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
      },
      "eventTime": "2014-11-05T21:35:27Z",
      "eventSource": "ec2.amazonaws.com",
      "eventName": "RunInstances",
```

```
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
      "instancesSet": {
        "items": [
          {
            "imageId": "ami-b66ed3de",
            "minCount": 1,
            "maxCount": 1
          }
        ]
      },
      "groupSet": {
        "items": [
          {
            "groupId": "sg-98b6e0f2"
          }
        ]
      },
      "instanceType": "m3.medium",
      "blockDeviceMapping": {
        "items": [
          {
            "deviceName": "/dev/xvda",
            "ebs": {
              "volumeSize": 8,
              "deleteOnTermination": true,
              "volumeType": "gp2"
            }
          },
          {
            "deviceName": "/dev/sdb",
            "ebs": {
              "volumeSize": 8,
              "deleteOnTermination": false,
              "volumeType": "gp2",
              "encrypted": true
            }
          }
        ]
      },
      "monitoring": {
        "enabled": false
```

```
        },
        "disableApiTermination": false,
        "instanceInitiatedShutdownBehavior": "stop",
        "clientToken": "XdKUT141516171819",
        "ebsOptimized": false
      },
      "responseElements": {
        "reservationId": "r-5ebc9f74",
        "ownerId": "111122223333",
        "groupSet": {
          "items": [
            {
              "groupId": "sg-98b6e0f2",
              "groupName": "launch-wizard-2"
            }
          ]
        },
        "instancesSet": {
          "items": [
            {
              "instanceId": "i-81e2f56c",
              "imageId": "ami-b66ed3de",
              "instanceState": {
                "code": 0,
                "name": "pending"
              },
              "amiLaunchIndex": 0,
              "productCodes": {

              },
              "instanceType": "m3.medium",
              "launchTime": 1415223328000,
              "placement": {
                "availabilityZone": "us-east-1a",
                "tenancy": "default"
              },
              "monitoring": {
                "state": "disabled"
              },
              "stateReason": {
                "code": "pending",
                "message": "pending"
              },
              "architecture": "x86_64",
```

```
            "rootDeviceType": "ebs",
            "rootDeviceName": "/dev/xvda",
            "blockDeviceMapping": {

            },
            "virtualizationType": "hvm",
            "hypervisor": "xen",
            "clientToken": "XdKUT1415223327917",
            "groupSet": {
              "items": [
                {
                  "groupId": "sg-98b6e0f2",
                  "groupName": "launch-wizard-2"
                }
              ]
            },
            "networkInterfaceSet": {

            },
            "ebsOptimized": false
          }
        ]
      }
    },
    "requestID": "41c4b4f7-8bce-4773-bf0e-5ae3bb5cbce2",
    "eventID": "cd75a605-2fee-4fda-b847-9c3d330ebaae",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  },
  {
    "eventVersion": "1.02",
    "userIdentity": {
          "type": "IAMUser",
          "principalId": "EX_PRINCIPAL_ID",
          "arn": "arn:aws:iam::111122223333:user/Alice",
          "accountId": "111122223333",
          "accessKeyId": "EXAMPLE_KEY_ID",
          "userName": "Alice"
    },
    "eventTime": "2014-11-05T21:35:35Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
```

```
      "userAgent": "AWS Internal",
      "requestParameters": {
        "constraints": {
          "encryptionContextSubset": {
            "aws:ebs:id": "vol-f67bafb2"
          }
        },
        "granteePrincipal": "111122223333:aws:ec2-infrastructure:i-81e2f56c",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      },
      "responseElements": {
        "grantId": "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a"
      },
      "requestID": "41c4b4f7-8bce-4773-bf0e-5ae3bb5cbce2",
      "eventID": "c1ad79e3-0d3f-402a-b119-d5c31d7c6a6c",
      "readOnly": false,
      "resources": [
        {
          "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "accountId": "111122223333"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.02",
      "userIdentity": {
          "type": "IAMUser",
          "principalId": "EX_PRINCIPAL_ID",
          "arn": "arn:aws:iam::111122223333:user/Alice",
          "accountId": "111122223333",
          "accessKeyId": "EXAMPLE_KEY_ID",
          "userName": "Alice"
      },
      "eventTime": "2014-11-05T21:35:32Z",
      "eventSource": "kms.amazonaws.com",
      "eventName": "GenerateDataKeyWithoutPlaintext",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "AWS Internal",
      "requestParameters": {
```

```
        "encryptionContext": {
          "aws:ebs:id": "vol-f67bafb2"
        },
        "numberOfBytes": 64,
        "keyId": "alias/aws/ebs"
      },
      "responseElements": null,
      "requestID": "create-111122223333-758247346-1415223332",
      "eventID": "ac3cab10-ce93-4953-9d62-0b6e5cba651d",
      "readOnly": true,
      "resources": [
        {
          "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "accountId": "111122223333"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    },
    {
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "111122223333:aws:ec2-infrastructure:i-81e2f56c",
        "arn": "arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/
i-81e2f56c",
        "accountId": "111122223333",
        "accessKeyId": "",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-11-05T21:35:38Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "111122223333:aws:ec2-infrastructure",
            "arn": "arn:aws:iam::111122223333:role/aws:ec2-infrastructure",
            "accountId": "111122223333",
            "userName": "aws:ec2-infrastructure"
          }
        }
      },
      "eventTime": "2014-11-05T21:35:47Z",
```

```
      "eventSource": "kms.amazonaws.com",
      "eventName": "Decrypt",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "192.0.2.0",
      "requestParameters": {
        "encryptionContext": {
          "aws:ebs:id": "vol-f67bafb2"
        }
      },
      "responseElements": null,
      "requestID": "b4b27883-6533-11e4-b4d9-751f1761e9e5",
      "eventID": "edb65380-0a3e-4123-bbc8-3d1b7cff49b0",
      "readOnly": true,
      "resources": [
        {
          "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
          "accountId": "111122223333"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

Monitorización con Amazon CloudWatch

Puedes monitorizar tu AWS KMS keys uso de Amazon CloudWatch, un AWS servicio que recopila y procesa datos sin procesar para AWS KMS convertirlos en métricas legibles y prácticamente en tiempo real. Estos datos se registran durante un periodo de dos semanas para que pueda obtener acceso a información histórica y conocer mejor el uso de sus claves KMS y sus cambios a lo largo del tiempo.

Puedes usar Amazon CloudWatch para avisarte de eventos importantes, como los siguientes.

- El material clave importado de una clave KMS se acerca a su fecha de vencimiento.
- Se sigue utilizando una clave KMS pendiente de eliminación.
- El material clave de una clave KMS se rotó automáticamente.
- Se ha eliminado una clave KMS.

También puedes crear una CloudWatch alarma de Amazon que te avise cuando tu porcentaje de solicitudes alcance un porcentaje determinado del valor de la cuota. Para obtener más información, consulta Gestiona tus tasas de solicitudes de AWS KMS API mediante Service Quotas y Amazon CloudWatch en el blog AWS de seguridad.

Temas

AWS KMS métricas y dimensiones

AWS KMS predefine CloudWatch las métricas de Amazon para que le resulte más fácil monitorear los datos críticos y crear alarmas. Puedes ver las AWS KMS métricas mediante la API de Amazon AWS Management Console y la CloudWatch API.

En esta sección, se enumeran todas AWS KMS las métricas y las dimensiones de cada una de ellas, y se proporciona una guía básica para crear CloudWatch alarmas en función de estas métricas y dimensiones.

> **Note**
>
> Nombre del grupo de dimensiones:
> Para ver una métrica en la CloudWatch consola de Amazon, en la sección Métricas, selecciona el nombre del grupo de dimensiones. Luego, puede filtrar por Nombre de la métrica. Este tema incluye el nombre de la métrica y el nombre del grupo de dimensiones de cada métrica de AWS KMS .

Temas

- XksProxyLatency

SecondsUntilKeyMaterialExpiration

La cantidad de segundos que quedan hasta que caduque el material de clave importado de una clave de KMS. Esta métrica es válida solo para las claves de KMS con material de clave importado (un origen de material de clave de `EXTERNAL`) y una fecha de caducidad.

Utilice esta métrica para realizar un seguimiento del tiempo que queda hasta que caduque el material de claves importado. Cuando ese tiempo cae por debajo de un umbral que usted define, puede volver a importar el material de clave con una nueva fecha de caducidad. La métrica `SecondsUntilKeyMaterialExpiration` es específica de una clave de KMS. No puede usar esta métrica para supervisar varias claves de KMS o claves de KMS que pueda crear en el futuro. Si necesitas ayuda para crear una CloudWatch alarma para monitorear esta métrica, consultaCrear una CloudWatch alarma por la caducidad del material clave importado.

La estadística más útil para esta métrica es `Minimum`, que le indica la menor cantidad de tiempo restante para todos los puntos de datos en el período estadístico especificado. La única unidad válida para esta métrica es `Seconds`.

Nombre del grupo de dimensiones: Per-Key Metrics

Dimensiones para **`SecondsUntilKeyMaterialExpiration`**

Dimensión	Descripción; relacionada con AWS
KeyId	Valor para cada clave de KMS.

ExternalKeyStoreThrottle

El número de solicitudes de operaciones criptográficas en las claves de KMS de cada almacén de claves externo que se AWS KMS limita (responde con un). `ThrottlingException` Esta métrica se aplica únicamente a los almacenes de claves externos.

La `ExternalKeyStoreThrottle` métrica se aplica solo a las claves KMS de un almacén de claves externo y solo a las solicitudes de operaciones criptográficas y a la operación. DescribeKey AWS KMS limita estas solicitudes cuando la tasa de solicitudes supera la cuota de solicitudes del almacén de claves personalizado del almacén de claves externo. Esta métrica no incluye la limitación por parte del proxy del almacén de claves externo ni del administrador de claves externo.

Usa esta métrica para revisar y ajustar el valor de la cuota de solicitudes de su almacén de claves personalizado. Si esta métrica indica que las solicitudes de estas claves de KMS AWS KMS se limitan con frecuencia, podría considerar la posibilidad de solicitar un aumento del valor de la cuota de solicitudes del almacén de claves personalizado. Para conocer más detalles, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

Si con frecuencia recibe errores `KMSInvalidStateException` con un mensaje que explica que la solicitud fue rechazada “debido a una tasa de solicitudes muy alta” o “debido a que el proxy del almacén de claves externo no respondió a tiempo”, podría indicar que su administrador de claves externo o el proxy de almacén de claves externo no puede seguir el ritmo de la tasa de solicitudes actual. Si es posible, reduzca el porcentaje de solicitudes. También podría considerar solicitar una disminución en el valor de la cuota de solicitudes del almacén de claves personalizado. Reducir este valor de cuota puede aumentar la limitación (y el valor de la `ExternalKeyStoreThrottle` métrica), pero indica que AWS KMS se está rechazando el exceso de solicitudes rápidamente antes de enviarlas al proxy del almacén de claves externo o al administrador de claves externo. Para solicitar una reducción de la cuota, visite el Centro de AWS Support y crea un caso.

Nombre del grupo de dimensiones: Keystore Throttle Metrics

Dimensión	Descripción
CustomKeyStoreId	Valor para cada almacén de claves externo.
KmsOperation	Valor para cada operación de API AWS KMS . Esta métrica se aplica solo a las operaciones criptográficas y a la operación `DescribeKey` en las claves de KMS en un almacén de claves externo.
KeySpec	Valor para cada tipo de clave de KMS. La única especificación de clave admitida para las claves de KMS en un almacén de claves externo es SYMMETRIC_DEFAULT.

XksProxyCertificateDaysToExpire

El número de días que faltan para que venza el certificado TLS del punto de conexión del proxy del almacén de claves externo (`XksProxyUriEndpoint`). Esta métrica se aplica únicamente a los almacenes de claves externos.

Usa esta métrica para crear una CloudWatch alarma que te notifique la próxima caducidad de tu certificado TLS. Cuando el certificado caduque, AWS KMS no podrá comunicarse con el proxy del almacén de claves externo. No se podrá acceder a todos los datos protegidos por las claves de KMS en su almacén de claves externo hasta que renueve el certificado.

Una alarma previene que caduque la certificación que le puede impedir a usted acceder a sus recursos encriptados. Configure la alarma para que su organización tenga tiempo de renovar el certificado antes de que venza.

Nombre del grupo de dimensiones: XKS Proxy Certificate Metrics

Dimensión	Descripción
CustomKeyStoreId	Valor para cada almacén de claves externo.
CertificateName	Nombre del sujeto (CN) en el certificado TLS.

XksProxyCredentialAge

La cantidad de días que transcurrieron desde que la credencial de autenticación del proxy del almacén de claves externo actual (`XksProxyAuthenticationCredential`) se asoció con el almacén de claves externo. Este recuento comienza cuando introduce la credencial de autenticación como parte para crear o actualizar su almacén de claves externo. Esta métrica se aplica únicamente a los almacenes de claves externos.

Este valor está diseñado para recordarle la antigüedad de su credencial de autenticación. Sin embargo, dado que empezamos el recuento cuando asocia la credencial a su almacén de claves externo, no cuando crea su credencial de autenticación en el proxy del almacén de claves externo, es posible que este no sea un indicador preciso de la antigüedad de las credenciales en el proxy.

Utilice esta métrica para crear una CloudWatch alarma que le recuerde que debe cambiar la credencial de autenticación del proxy del almacén de claves externo.

Nombre del grupo de dimensiones: Per-Keystore Metrics

Dimensión	Descripción
CustomKeyStoreId	Valor para cada almacén de claves externo.

XksProxyErrors

El número de excepciones relacionadas con AWS KMS las solicitudes a su proxy de almacén de claves externo. Este recuento incluye las excepciones a las que vuelve el proxy del almacén de claves externo AWS KMS y los errores de tiempo de espera que se producen cuando el proxy del almacén de claves externo no responde AWS KMS dentro del intervalo de tiempo de espera de 250 milisegundos. Esta métrica se aplica únicamente a los almacenes de claves externos.

Puede utilizar esta métrica para realizar un seguimiento del porcentaje de errores de claves de KMS en su almacén de claves externo. Revela los errores más frecuentes, para que pueda priorizar sus esfuerzos de ingeniería. Por ejemplo, las claves de KMS que generan altas tasas de errores no reintentables pueden indicar un problema con la configuración de su almacén de claves externo. Para ver la configuración de su almacén de claves externo, consulte Visualización de un almacén de claves externo. Para editar la configuración de su almacén de claves externo, consulte Edición de propiedades del almacén de claves externo.

Nombre del grupo de dimensiones: XKS Proxy Error Metrics

Dimensión	Descripción
CustomKeyStoreId	Valor para cada almacén de claves externo.
KmsOperation	Valor para cada operación de AWS KMS API que generó una solicitud al proxy XKS.
XksOperation	Valor para cada operación de la API del proxy del almacén de claves externo.
KeySpec	Valor para cada tipo de clave de KMS. La única especificación de clave admitida para las claves de KMS en un almacén de claves externo es SYMMETRIC_DEFAULT.

Dimensión	Descripción
ErrorType	Valores: • Errores que se pueden volver a intentar: es probable que sean transitorios, como los errores de red. • Errores que no se pueden volver a intentar: pueden indicar un problema con la configuración del almacén de claves personalizado o con componentes externos. • N/A: Solicitud exitosa; sin errores
Exception Name	Valores: • Nombre de la excepción • Ninguna: solicitud exitosa; sin errores

XksExternalKeyManagerStates

Un recuento de la cantidad de instancias de un administrador de claves externo en cada uno de los siguientes estados de condición: `Active`, `Degraded` y `Unavailable`. La información de esta métrica proviene del proxy del almacén de claves externo asociado a cada almacén de claves externo. Esta métrica se aplica únicamente a los almacenes de claves externos.

Los siguientes son los estados de condición para las instancias del administrador de claves externo asociadas a un almacén de claves externo. Cada proxy de almacén de claves externo puede utilizar diferentes indicadores para medir el estado de su administrador de claves externo. Para obtener más información, consulte la documentación del proxy del almacén de claves externo.

- `Active`: el administrador de claves externo está en buen estado.
- `Degraded`: el administrador de claves externo no está en buen estado, pero aún puede atender el tráfico.
- `Unavailable`: el administrador de claves externo no puede atender el tráfico.

Usa esta métrica para crear una CloudWatch alarma que te avise de las instancias del administrador de claves externo degradadas y no disponibles. Para determinar en qué estado se encuentra cada instancia del administrador de claves externo, consulte sus registros de proxy del almacén de claves externo.

Nombre del grupo de dimensiones: XKS External Key Manager Metrics

Dimensión	Descripción
CustomKeyStoreId	Valor para cada almacén de claves externo.
XksExternalKeyManagerState	Valor para cada estado de condición.

XksProxyLatency

La cantidad de milisegundos que tarda un proxy del almacén de claves externo en responder a una solicitud de AWS KMS . Si se agotó el tiempo de espera de la solicitud, el valor registrado es un límite de tiempo de espera de 250 milisegundos. Esta métrica se aplica únicamente a los almacenes de claves externos.

Utilice esta métrica para evaluar el rendimiento de su proxy de almacén de claves externo y de su administrador de claves externo. Por ejemplo, si el tiempo del proxy se agota con frecuencia en las operaciones de cifrado y descifrado, consulte a su administrador de proxy externo.

Las respuestas lentas también pueden indicar que su administrador de claves externo no puede gestionar el tráfico de solicitudes actual. AWS KMS recomienda que su administrador de claves externo pueda gestionar hasta 1800 solicitudes de operaciones criptográficas por segundo. Si su administrador de claves externo no puede gestionar la tasa de 1800 solicitudes por segundo, considere solicitar una reducción de su cuota de solicitudes de claves de KMS en un almacén de claves personalizado. Las solicitudes de operaciones criptográficas que utilizan las claves de KMS en su almacén de claves externo van a responder rápido a los errores con una excepción de limitación, en lugar de ser procesadas y luego rechazadas por su proxy del almacén de claves externo o administrador de claves externo.

Nombre del grupo de dimensiones: XKS Proxy Latency Metrics

Dimensión	Descripción
CustomKeyStoreId	Valor para cada almacén de claves externo.

Dimensión	Descripción
KmsOperation	Valor para cada operación de AWS KMS API que generó una solicitud al proxy XKS.
XksOperation	Valor para cada operación de la API del proxy del almacén de claves externo.
KeySpec	Valor para cada tipo de clave de KMS. La única especificación de clave admitida para las claves de KMS en un almacén de claves externo es SYMMETRIC_DEFAULT.

Visualización de métricas AWS KMS

Puedes ver las AWS KMS métricas mediante la API de Amazon AWS Management Console y la CloudWatch API.

Para ver las métricas mediante la CloudWatch consola

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. Si es necesario, cambie la región. En la barra de navegación, seleccione la región donde residen sus recursos de AWS .
3. En el panel de navegación, seleccione Métricas y, a continuación, Todas las métricas.
4. En la pestaña Browse (Examinar), busque `KMS` y, a continuación, seleccione KMS.
5. Elija el nombre del grupo de dimensiones de la métrica que desea ver.

   Por ejemplo, para la métrica `SecondsUntilKeyMaterialExpiration`, elija Per-Key Metrics.
6. Para obtener una gráfica del valor de la métrica, elija el nombre de la métrica y, a continuación, elija `Add to graph`. Para convertir el gráfico de líneas en un valor, elija Line (Línea) y, a continuación, elija Number (Número).

Para ver las métricas mediante la CloudWatch API de Amazon

Para ver AWS KMS las métricas mediante la CloudWatch API, envía una ListMetricssolicitud con el `Namespace` valor establecido en`AWS/KMS`. El siguiente ejemplo muestra cómo hacerlo con la AWS Command Line Interface (AWS CLI).

```
$  aws cloudwatch list-metrics --namespace AWS/KMS

{
    "Metrics": [
        {
            "Namespace": "AWS/KMS",
            "MetricName": "SecondsUntilKeyMaterialExpiration",
            "Dimensions": [
                {
                    "Name": "KeyId",
                    "Value": "1234abcd-12ab-34cd-56ef-1234567890ab"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "ExternalKeyStoreThrottle",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
                {
                    "Name": "KmsOperation",
                    "Value": "Encrypt"
                },
                {
                    "Name": "KeySpec",
                    "Value": "SYMMETRIC_DEFAULT"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyCertificateDaysToExpire",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
                {
                    "Name": "CertificateName",
                    "Value": "myproxy.xks.example.com"
```

```
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyCredentialAge",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyErrors",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
                {
                    "Name": "KmsOperation",
                    "Value": "Decrypt"
                },
                {
                    "Name": "XksOperation",
                    "Value": "Decrypt"
                },
                {
                     "Name": "KeySpec",
                     "Value": "SYMMETRIC_DEFAULT"
                },
                {
                    "Name": "ErrorType",
                    "Value": "Retryable errors"
                },
                {
                     "Name": "ExceptionName",
                     "Value": "KMSInvalidStateException"
                }
            ]
        },
        {
```

```
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyHsmStates",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
                {
                    "Name": "XksProxyHsmState",
                    "Value": "Active"
                }
            ]
        },
        {
            "Namespace": "AWS/KMS",
            "MetricName": "XksProxyLatency",
            "Dimensions": [
                {
                    "Name": "CustomKeyStoreId",
                    "Value": "cks-1234567890abcdef0"
                },
                {
                    "Name": "KmsOperation",
                    "Value": "Decrypt"
                },
                {
                    "Name": "XksOperation",
                    "Value": "Decrypt"
                },
                {
                     "Name": "KeySpec",
                     "Value": "SYMMETRIC_DEFAULT"
                }
            ]
        }
    ]
}
```

Crear CloudWatch alarmas para monitorear las claves de KMS

Puedes crear una CloudWatch alarma de Amazon en función de una AWS KMS métrica. La alarma envía un mensaje de correo electrónico cuando un valor de la métrica supera un umbral especificado en la configuración de la alarma. La alarma puede enviar el mensaje de correo electrónico a un tema

de Amazon Simple Notification Service (Amazon SNS) o a una política de Amazon EC2 Auto Scaling. Para obtener información detallada sobre CloudWatch las alarmas, consulta Uso de CloudWatch las alarmas de Amazon en la Guía del CloudWatch usuario de Amazon

Crear una alarma para el caducidad del material de claves importado

Puede usar la `SecondsUntilKeyMaterialExpiration`métrica para crear una CloudWatch alarma que le notifique cuando el material clave importado en una clave de KMS esté a punto de caducar.

Al importar material de claves en una clave KMS, también puede especificar de manera opcional una fecha y una hora en la que vence el material de claves. Cuando el material clave caduca, lo AWS KMS elimina y la clave KMS queda inutilizable. Para volver a usar la clave KMS, debe volver a importar el material de claves.

Para ver instrucciones, consulte Crear una CloudWatch alarma por la caducidad del material clave importado.

Crear una alarma para el uso de las claves KMS pendientes de eliminación

Al programar una eliminación de claves de una clave KMS, AWS KMS aplica un periodo de espera antes de eliminar la clave KMS. Puede usar el periodo de espera para asegurarse de que no necesita la clave KMS ni ahora ni en el futuro. También puede configurar una CloudWatch alarma para que le avise si una persona o aplicación intenta utilizar la clave KMS en una operación criptográfica durante el período de espera. Si recibe una notificación de una alarma de este tipo, puede cancelar la eliminación de la clave KMS.

Para ver instrucciones, consulte Creación de una alarma que detecte el uso de una eliminación pendiente de una clave KMS.

Cree una alarma para monitorear un almacén de claves externo

Puede crear CloudWatch alarmas en función de las métricas de los almacenes de claves externos y de las claves KMS de los almacenes de claves externos.

Por ejemplo, le recomendamos que configure una CloudWatch alarma para avisarle cuando el certificado TLS de su almacén de claves externo esté a punto de caducar (XksProxyCertificateDaysToExpire), cuando usted y su proxy del almacén de claves externo informen de que las instancias del administrador de claves externo están degradadas o no están disponibles (XksProxyHsmStates).

Para obtener instrucciones, consulte Monitoreo de un almacén de claves externo.

Monitorización con Amazon EventBridge

Puede usar Amazon EventBridge (anteriormente Amazon CloudWatch Events) para que le avise de los siguientes eventos importantes en el ciclo de vida de sus claves de KMS.

- El material clave de una clave KMS se rotó automáticamente.
- El material de clave importado en una clave KMS se ha vencido.
- Se eliminó una clave KMS cuya eliminación estaba programada.

AWS KMSse integra con Amazon EventBridge para notificarle los eventos importantes que afectan a sus claves de KMS. Cada evento se representa en JSON (notación de JavaScript objetos) e incluye el nombre del evento, la fecha y hora en que se produjo el evento y las personas afectadas. Puede recopilar estos eventos y establecer reglas que los dirijan a uno o varios destinos, como funciones de AWS Lambda, temas de Amazon SNS, colas de Amazon SQS, flujos en Amazon Kinesis Data Streams o destinos integrados.

Para obtener más información sobre su uso EventBridge con otros tipos de eventos, incluidos los que se emiten AWS CloudTrail cuando graba una solicitud de API de lectura/escritura, consulta la Guía EventBridge del usuario de Amazon.

En los temas siguientes se describen los EventBridge eventos que AWS KMS se generan.

Rotación de CMK de KMS

AWS KMS es compatible con la rotación automática del material de clave en claves KMS de cifrado simétricas. La rotación anual de materiales de claves es opcional para las claves administradas por el cliente. El material de claves para Claves administradas por AWS se rota cada año de forma automática.

Cada vez que AWS KMS rota el material clave, envía un `KMS CMK Rotation` evento a EventBridge. AWS KMSgenera este evento haciendo el mejor esfuerzo posible.

A continuación se muestra un ejemplo de este evento.

```
{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
```

```
  "detail-type": "KMS CMK Rotation",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

Vencimiento del material de claves importado de KMS

Al importar material de claves en una clave KMS, también puede especificar una hora en la que vence el material de claves. Cuando el material clave caduque, lo AWS KMS elimina y envía el `KMS Imported Key Material Expiration` evento correspondiente a. EventBridge AWS KMSgenera este evento haciendo el mejor esfuerzo posible.

A continuación se muestra un ejemplo de este evento.

```
{
  "version": "0",
  "id": "9da9af57-9253-4406-87cb-7cc400e43465",
  "detail-type": "KMS Imported Key Material Expiration",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

Eliminación de CMK de KMS

Al programar una eliminación de claves de una clave KMS, AWS KMS aplica un periodo de espera antes de eliminar la clave KMS. Una vez finalizado el período de espera, AWS KMS elimina la clave

KMS y envía un `KMS CMK Deletion` evento a. EventBridge AWS KMSgarantiza este EventBridge evento. Debido a los reintentos, puede generar varios eventos en unos segundos que eliminan la misma clave KMS.

A continuación se muestra un ejemplo de este evento.

```
{
  "version": "0",
  "id": "e9ce3425-7d22-412a-a699-e7a5fc3fbc9a",
  "detail-type": "KMS CMK Deletion",
  "source": "aws.kms",
  "account": "111122223333",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  ],
  "detail": {
    "key-id": "1234abcd-12ab-34cd-56ef-1234567890ab"
  }
}
```

Creación de AWS KMS recursos con AWS CloudFormation

AWS Key Management Service está integrado con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Puede crear una plantilla que describa las claves y los alias de KMS, y AWS CloudFormation aprovisiona y configura estos recursos por usted. Para obtener información sobre la AWS KMS compatibilidad con CloudFormation, consulte la referencia sobre los tipos de recursos de KMS en la Guía del AWS CloudFormation usuario.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar AWS KMS los recursos de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos una y otra vez en varias Cuentas de AWS regiones.

Para aprovisionar y configurar recursos AWS KMS y otros AWS servicios, debe conocer AWS CloudFormation las plantillas. Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus AWS CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar AWS CloudFormation Designer para ayudarte a

empezar con AWS CloudFormation las plantillas. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation ? en la Guía del usuario de AWS CloudFormation .

Regiones

AWS KMS CloudFormation los recursos están disponibles en todas las regiones en las que AWS CloudFormation se admite.

AWS KMS recursos en AWS CloudFormation plantillas

AWS KMS admite los siguientes AWS CloudFormation recursos.

- El `AWS::KMS::Key`recurso especifica una clave de KMS AWS Key Management Service. Puede utilizar este recurso para crear claves de KMS de cifrado simétricas, claves de KMS asimétricas para el cifrado o la firma y claves de KMS HMAC simétricas. Se puede utilizar `AWS::KMS::Key` para crear claves principales multirregionales de todos los tipos compatibles. Para crear una clave multirregión, utilice el recurso `AWS::KMS::ReplicaKey`.
- `AWS::KMS::Alias` crea un alias y lo asocia con una clave KMS. La clave KMS se puede definir en la plantilla o crear mediante otro mecanismo.
- `AWS::KMS::ReplicaKey` crea un clave de réplica de varias regiones. Para crear una clave principal de varias regiones, utilice el recurso `AWS::KMS::Key`. No puede utilizar este recurso para replicar claves de varias regiones con material de claves importado. Para obtener más información acerca de las claves de varias regiones, consulte Claves multirregionales en AWS KMS.

> **Important**
>
> Si cambia el valor de propiedad de `KeyUsage`, `KeySpec` o `MultiRegion`, en una clave KMS existente, se programará la clave KMS existente para su eliminación y se crea una clave KMS nueva con el valor especificado.
> Mientras está programada para su eliminación, la clave KMS existente se vuelve inutilizable. Si no cancela la eliminación programada de la clave de KMS existente fuera de AWS CloudFormation, todos los datos cifrados con la clave de KMS existente quedarán irrecuperables cuando se elimine la clave de KMS.

Las claves de KMS que crea la plantilla son recursos reales que tiene. Cuenta de AWS Los directores autorizados pueden usar y administrar las claves de KMS que crea la plantilla, ya sea

mediante la plantilla, la AWS KMS consola o las AWS KMS API. Cuando elimina una clave KMS de la plantilla, la clave KMS está programada para su eliminación utilizando un período de espera que especifique de antemano.

Por ejemplo, puedes usar una AWS CloudFormation plantilla para crear una clave KMS de prueba con la política clave, las especificaciones clave, el uso de claves, los alias y las etiquetas que prefieras. Puede ejecutarlo en el conjunto de pruebas, revisar los resultados y, a continuación, utilizar la plantilla para programar la clave de prueba para su eliminación. Más tarde, puede ejecutar la plantilla de nuevo para crear una clave de prueba con las mismas propiedades.

O bien, puede usar una AWS CloudFormation plantilla para definir una configuración de clave de KMS concreta que satisfaga las normas empresariales y los estándares de seguridad. A continuación, puede usar esa plantilla en cualquier momento que necesite para crear una clave KMS. No tiene que preocuparse por las claves mal configuradas. Si su configuración preferida cambia, puede usar su plantilla para actualizar sus claves KMS. Por ejemplo, la plantilla facilita la activación mediante programación de la rotación automática de claves en todas las claves KMS que define la plantilla.

Para obtener más información sobre AWS KMS los recursos, incluidos ejemplos, consulte la referencia sobre los tipos de recursos de KMS en la Guía del AWS CloudFormation usuario.

Obtenga más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormation Guía del usuario
- AWS CloudFormation Referencia de la API
- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

Eliminación de AWS KMS keys

La eliminación de una AWS KMS key es un proceso destructivo y potencialmente peligroso. Elimina el material de claves y todos los metadatos asociados con la clave KMS. Esta acción es irreversible. Una vez que se elimina una clave KMS, ya no pueden descifrar los datos que se habían cifrado con ella, lo que significa que no se pueden recuperar. (Las únicas excepciones son las claves de réplica de varias regiones y las claves HMAC de KMS y asimétricas con material de claves importado). Este

riesgo es importante en el caso de las claves de KMS asimétricas que se utilizan para el cifrado, ya que, sin previo aviso ni error, los usuarios pueden seguir generando textos cifrados con la clave pública que no se pueden descifrar una vez eliminada la clave privada de AWS KMS.

Debe eliminar una clave KMS solo cuando esté seguro de que ya no necesita usarla. Si no está seguro, considere la posibilidad de desactivar la clave KMS en lugar de eliminarla. Puede volver a habilitar una clave de KMS deshabilitada y cancelar la eliminación programada de una clave de KMS, pero no puede recuperar una clave de KMS eliminada.

Solo puede programar la eliminación de una clave administrada por el cliente. No puede eliminar Claves administradas por AWS ni Claves propiedad de AWS.

Antes de eliminar una clave KMS, es recomendable que averigüe cuántos textos se han cifrado con dicha clave. AWS KMS no almacena esta información ni ninguno de los textos cifrados. Para obtener esta información, debe determinar por su cuenta el uso anterior de una clave KMS. Para obtener ayuda, consulte Determinar el uso anterior de una clave KMS.

AWS KMS nunca elimina las claves KMS a menos que las programe explícitamente para su eliminación y venza el periodo de espera obligatorio.

Sin embargo, puede decidir eliminar una clave KMS por uno o varios de los motivos siguientes:

- Para completar el ciclo de vida de clave de las claves KMS que ya no necesita
- Evitar los gastos generales de administración y los costos asociados con el mantenimiento de las claves KMS no usadas
- Para reducir el número de claves KMS que se contabilizan para su cuota de recursos de clave KMS

> **Note**
>
> Si cierra su Cuenta de AWS, sus claves de KMS dejarán de estar accesibles y no se le facturará por ellas.

AWS KMS registra una entrada en su registro AWS CloudTrail cuando programa la eliminación de la clave de KMS y cuando la clave de KMS se elimina en realidad.

Para obtener información acerca de cómo eliminar claves principales y réplicas de varias regiones, consulte Eliminación de claves de varias regiones.

Temas

Acerca del período de espera

Como la eliminación de una clave KMS es un proceso destructivo y potencialmente peligroso, AWS KMS requiere que establezca un período de espera de 7 a 30 días. El periodo de espera predeterminado es de 30 días.

Sin embargo, el período de espera real puede ser hasta 24 horas más largo que el programado. Para obtener la fecha y la hora reales en las que se eliminará la clave KMS, utilice la DescribeKeyoperación. O en el consola AWS KMS, en la página de detalles para la clave KMS, en la sección Configuración general, consulte la eliminación programada. Asegúrese de anotar la zona horaria.

Durante el periodo de espera, el estado de la clave KMS y el estado de la clave son Pending deletion (Pendiente de eliminación).

- Una clave KMS que está pendiente de eliminación no puede utilizarse en ninguna operación criptográfica.
- AWS KMS no rota el material de clave de las claves KMS que están pendientes de eliminación.

Una vez finalizado el período de espera, AWS KMS elimina la clave KMS, sus alias y todos los metadatos de AWS KMS.

Es posible que programar la eliminación de una clave de KMS no afecte inmediatamente a las claves de datos cifradas por la clave de KMS. Para obtener más detalles, consulte Cómo afectan las claves de KMS obsoletas a las claves de datos.

Use el periodo de espera para asegurarse de que no necesita la clave KMS ahora ni en el futuro. Puedes configurar una CloudWatch alarma de Amazon para que te avise si una persona o aplicación intenta usar la clave KMS durante el período de espera. Para recuperar la clave KMS, puede cancelar la eliminación de claves antes de que finalice el periodo de espera. Una vez que finaliza el periodo de espera, no puede cancelar la eliminación de claves y AWS KMS elimina la clave KMS.

Eliminación de claves KMS asimétricas

Los usuarios autorizados pueden eliminar las claves KMS simétricas y asimétricas. El procedimiento para programar la eliminación de estas claves KMS es el mismo para ambos tipos de claves. Sin embargo, debido a que la clave pública de una clave KMS asimétrica se puede descargar y utilizar fuera de AWS KMS, la operación plantea riesgos adicionales significativos, especialmente para las claves KMS asimétricas utilizadas para el cifrado (el uso de la clave es `ENCRYPT_DECRYPT`).

- Cuando planifica la eliminación de una clave KMS, el estado de la clave de la clave KMS cambia a Pending deletion (Pendiente de eliminación) y la clave KMS no se puede utilizar en operaciones criptográficas. Sin embargo, la eliminación de la programación no tiene ningún efecto en las claves públicas fuera de AWS KMS. Los usuarios que tengan las claves públicas pueden seguir utilizándolas para cifrar mensajes. No reciben ninguna notificación de que se haya cambiado el estado de la clave. A menos que se cancele la eliminación, el texto cifrado creado con la clave pública no se puede descifrar.
- Las alarmas, los registros y otras estrategias que detectan los intentos de uso de la clave KMS que está pendiente de eliminación no pueden detectar el uso de la clave pública fuera de AWS KMS.
- Cuando se elimina la clave KMS, todas las acciones de AWS KMS que involucran a esa clave KMS fallan. Sin embargo, los usuarios que tengan las claves públicas pueden seguir utilizándolas para cifrar mensajes. Estos textos cifrados no se pueden descifrar.

Si debe eliminar una clave KMS asimétrica con un uso de clave igual a`ENCRYPT_DECRYPT`, utilice las entradas de CloudTrail registro para determinar si la clave pública se ha descargado y compartido. Si ha sido así, compruebe que la clave pública no se utilice fuera de AWS KMS. Después, considere la posibilidad de desactivar la clave KMS en lugar de eliminarla.

El riesgo que supone eliminar una clave de KMS asimétrica se mitiga en el caso de las claves de KMS asimétricas con material de claves importado. Para obtener más detalles, consulte Eliminación de una clave de KMS con material de claves importado.

Eliminación de claves de varias regiones

Los usuarios autorizados puede programar la eliminación de claves primarias y réplicas de varias regiones. Sin embargo, AWS KMS no eliminará una clave principal de varias regiones que tenga claves de réplica. Además, siempre y cuando exista su clave principal, puede volver a crear una clave de réplica de varias regiones eliminada. Para obtener más detalles, consulte Eliminación de claves de varias regiones.

Eliminación de claves de KMS con material de claves importado

Los usuarios autorizados pueden programar la eliminación de claves de KMS con material de claves importado. Esta acción elimina de forma permanente la clave de KMS, su material de claves y todos los metadatos asociados con la clave de KMS.

No puede crear una nueva clave de KMS de cifrado simétrico que pueda descifrar los textos cifrados de una clave de cifrado simétrico eliminada con material de claves importado, incluso si tiene una copia de su material de claves. Sin embargo, si tiene el material de claves, puede recrear de manera efectiva una clave de KMS asimétrica o una clave HMAC de KMS con material de claves importado. Para obtener más detalles, consulte Eliminación de una clave de KMS con material de claves importado.

Control del acceso a la eliminación de claves

Si utiliza las políticas de IAM para conceder los permisos de AWS KMS, las identidades que tengan acceso de administrador de AWS (`"Action": "*"`) o acceso completo de AWS KMS (`"Action": "kms:*"`) ya tienen permiso para programar y cancelar la eliminación de claves KMS. Para permitir que los administradores de claves programen y cancelen la eliminación de claves en la política de claves, utilice la consola de AWS KMS o la API de AWS KMS.

Normalmente, solo los administradores de claves tienen permiso para programar o cancelar la eliminación de claves. Sin embargo, puede conceder estos permisos a otras identidades de IAM al agregar los permisos `kms:ScheduleKeyDeletion` y `kms:CancelKeyDeletion` a la política de claves o a una política de IAM. También puede usar la clave de `kms:ScheduleKeyDeletionPendingWindowInDays` condición para restringir aún más los valores que los directores pueden especificar en el `PendingWindowInDays` parámetro de una solicitud. ScheduleKeyDeletion

Permitir a los administradores de claves programar y cancelar la eliminación de claves (consola)

Para otorgar permiso a los administradores de claves para programar y cancelar la eliminación de claves

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija el alias o el ID de clave de la clave KMS cuyos permisos desea cambiar.
5. Seleccione la pestaña key policy (política de claves).
6. El siguiente paso es diferente para la vista predeterminada y la vista de política de su política de claves. La vista predeterminada solo está disponible si utiliza la política de claves de consola predeterminada. De lo contrario, solo está disponible la vista de política.

   Cuando la vista predeterminada está disponible, aparece el botón Switch to policy view (Cambiar a la vista de política) o Switch to default view (Cambiar a la vista predeterminada) en la pestaña Key policy (Política de claves).

   - En la vista predeterminada:
     - En la sección Key deletion (Eliminación de la clave), seleccione Allow key administrators to delete this key (Permitir que los administradores de claves eliminen esta clave).
   - En la vista de la política:
     a. Elija Editar.
     b. En la declaración de política para los administradores de claves, agregue los permisos `kms:ScheduleKeyDeletion` y `kms:CancelKeyDeletion` al elemento `Action`.

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSKeyAdmin"},
  "Action": [
    "kms:Create*",
```

```
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

c. Elija Guardar cambios.

Otorgar permiso a los administradores de claves para programar y cancelar la eliminación (AWS CLI)

Puede utilizar la AWS Command Line Interface para agregar permisos para programar y cancelar la eliminación de claves.

Para agregar permiso para programar y cancelar la eliminación de claves

1. Utilice el comando `aws kms get-key-policy` para recuperar la política de claves existente y, a continuación, guarde el documento de políticas en un archivo.
2. Abra el documento de políticas en el editor de textos que prefiera. En la declaración de política para los administradores de claves, agregue los permisos `kms:ScheduleKeyDeletion` y `kms:CancelKeyDeletion`. El siguiente ejemplo muestra una declaración de política con estos dos permisos:

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:user/KMSKeyAdmin"},
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
```

```
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

3. Utilice el comando `aws kms put-key-policy` para aplicar la política de claves a la clave KMS.

Programación y cancelación de la eliminación de claves

Los siguientes procedimientos describen cómo programar y cancelar la eliminación de claves de una sola región AWS KMS keys (claves KMS) en AWS KMS utilizando la AWS Management Console, la AWS CLI y la AWS SDK for Java.

Para obtener información acerca de cómo programar la eliminación de claves de varias regiones, consulte Eliminación de claves de varias regiones.

> **Warning**
>
> La eliminación de una clave KMS es un proceso destructivo y potencialmente peligroso. Solo debe hacerlo si está seguro de que ya no necesitará la clave KMS y no tendrá que usarla en el futuro. Si no está seguro, debe desactivar la clave KMS en lugar de eliminarla.

Para poder eliminar una clave KMS, debe disponer de permiso para hacerlo. Para obtener información sobre cómo conceder estos permisos a los administradores de claves, consulte Control del acceso a la eliminación de claves. También puede usar la clave de condición `kms:ScheduleKeyDeletionPendingWindowInDays` para restringir aún más el periodo de espera, por ejemplo, para imponer un periodo de espera mínimo.

AWS KMS registra una entrada en su registro AWS CloudTrail cuando programa la eliminación de la clave de KMS y cuando la clave de KMS se elimina en realidad.

Programación y cancelación de eliminación de claves (consola)

En la AWS Management Console, puede programar y cancelar la eliminación de varias claves KMS a la vez.

Para programar la eliminación de claves

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.

   No puede programar la eliminación de Claves administradas por AWS o Claves propiedad de AWS.
4. Seleccione la casilla de verificación situada junto a la clave de KMS que desea eliminar.
5. Elija Key actions (Acciones de claves), Schedule key deletion (Programar la eliminación de claves).
6. Lea y tenga en cuenta la advertencia y la información sobre la cancelación de la eliminación durante el período de espera. Si decide cancelar la eliminación, en la parte inferior de la página, elija Cancel (Cancelar).
7. En Waiting period (in days) [Período de espera (en días)], indique un número de días entre 7 y 30.
8. Revise las claves KMS que está eliminando.
9. Seleccione la casilla de verificación situada junto a Confirm you want to schedule this key for deletion in ***<number of days>*** days (Confirme que quiere programar la eliminación de esta clave para dentro de <número de días> días).
10. Elija Schedule deletion.

El estado de clave KMS cambia a Pending deletion (Eliminación pendiente).

Para cancelar la eliminación de claves

1. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.

3. En el panel de navegación, elija Claves administradas por el cliente.
4. Seleccione la casilla de verificación situada junto a la clave de KMS que desea recuperar.
5. Elija Key actions (Acciones de claves), Cancel key deletion (Cancelar eliminación de la clave).

El estado de clave KMS cambia de Pending deletion (Eliminación pendiente) a Disabled (Deshabilitado). Para utilizar la clave KMS, debe habilitarla.

Programación y cancelación de la eliminación de claves (AWS CLI)

Utilice el comando `aws kms schedule-key-deletion` para programar la eliminación de una clave administrada por el cliente, tal y como se muestra en el siguiente ejemplo.

No puede programar la eliminación de una Clave administrada de AWS o una Clave propiedad de AWS.

```
$ aws kms schedule-key-deletion --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --
pending-window-in-days 10
```

Cuando se utiliza de forma correcta, la AWS CLI devuelve una salida como la que se muestra en el ejemplo siguiente:

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "DeletionDate": 1598304792.0,
    "KeyState": "PendingDeletion",
    "PendingWindowInDays": 10
}
```

Utilice el comando `aws kms cancel-key-deletion` para cancelar la eliminación de claves desde la AWS CLI, tal y como se muestra en el siguiente ejemplo.

```
$ aws kms cancel-key-deletion --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Cuando se utiliza de forma correcta, la AWS CLI devuelve una salida como la que se muestra en el ejemplo siguiente:

```
{
```

```
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

El estado de la clave KMS cambia de Pending Deletion (Eliminación pendiente) a Disabled (Deshabilitada). Para utilizar la clave KMS, debe habilitarla.

Programación y cancelación de la eliminación de claves (AWS SDK for Java)

El siguiente ejemplo muestra cómo programar la eliminación de una clave administrada por el cliente con AWS SDK for Java. Este ejemplo requiere que antes se haya creado una instancia de `AWSKMSClient` como `kms`

```
String KeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

int PendingWindowInDays = 10;

ScheduleKeyDeletionRequest scheduleKeyDeletionRequest =
new
 ScheduleKeyDeletionRequest().withKeyId(KeyId).withPendingWindowInDays(PendingWindowInDays);
kms.scheduleKeyDeletion(scheduleKeyDeletionRequest);
```

El siguiente ejemplo muestra cómo cancelar una eliminación de clave con AWS SDK for Java. Este ejemplo requiere que antes se haya creado una instancia de `AWSKMSClient` como `kms`

```
String KeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

CancelKeyDeletionRequest cancelKeyDeletionRequest =
new CancelKeyDeletionRequest().withKeyId(KeyId);
kms.cancelKeyDeletion(cancelKeyDeletionRequest);
```

El estado de la clave KMS cambia de Pending Deletion (Eliminación pendiente) a Disabled (Deshabilitada). Para utilizar la clave de KMS, debe habilitarla.

Creación de una alarma que detecte el uso de una eliminación pendiente de una clave KMS

Puedes combinar las funciones de AWS CloudTrail Amazon CloudWatch Logs y Amazon Simple Notification Service (Amazon SNS) para crear una alarma de Amazon que te notifique cuando

alguien de tu cuenta intente usar una clave de KMS que está pendiente de ser eliminada. CloudWatch Si recibe esta notificación, puede cancelar la eliminación de la clave KMS y reconsiderar su decisión de eliminarla.

Los siguientes procedimientos crean una alarma que le notifica cada vez que se escribe el mensaje de error *`Key ARN`* `is pending deletion` «» en sus CloudTrail archivos de registro. Este mensaje de error indica que una persona o aplicación ha intentado utilizar la clave KMS en una operación criptográfica. Debido a que la notificación está vinculada al mensaje de error, no se activa cuando se utilizan operaciones de las API permitidas en las clave KMS que están pendientes de eliminación, como por ejemplo `ListKeys`, `CancelKeyDeletion` y `PutKeyPolicy`. Para ver una lista de las operaciones de API de AWS KMS que devuelven este mensaje de error, consulte Estados clave de AWS KMS las claves.

El correo electrónico de notificación que recibe no muestra la clave KMS o la operación criptográfica. Puede encontrar esa información en su registro de CloudTrail. En lugar de ello, el correo electrónico informa de que el estado de la alarma ha cambiado de OK (Correcto) a Alarm (Alarma). Para obtener más información sobre CloudWatch las alarmas y los cambios de estado, consulta Uso de CloudWatch las alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.

> **Warning**
>
> Esta CloudWatch alarma de Amazon no puede detectar el uso de la clave pública de una clave KMS asimétrica fuera deAWS KMS. Para obtener detalles acerca de los riesgos especiales de la eliminación de las claves KMS asimétricas utilizadas para la criptografía de clave pública, incluida la creación de textos cifrados que no se pueden descifrar, consulte Eliminación de claves KMS asimétricas.

Temas

- Requisitos de una alarma CloudWatch
- Crear la CloudWatch alarma

Requisitos de una alarma CloudWatch

Antes de crear una CloudWatch alarma, debe crear una AWS CloudTrail ruta y configurarla CloudTrail para enviar los archivos de CloudTrail registro a Amazon CloudWatch Logs. También necesita un tema de Amazon SNS para la notificación de alarma.

- Crear un registro de seguimiento de CloudTrail.

  CloudTrail se activa automáticamente Cuenta de AWS al crear la cuenta. Sin embargo, para mantener un registro continuo de los eventos de la cuenta, incluidos los eventos de AWS KMS cree un registro de seguimiento.

- Configure CloudTrail para entregar sus archivos de registro (CloudWatch registros).

  Configure la entrega de sus archivos de CloudTrail registro a CloudWatch Logs. Esto permite a CloudWatch Logs supervisar los registros para detectar las solicitudes de AWS KMS API que intenten utilizar una clave de KMS que está pendiente de ser eliminada.

- Cree un tema de Amazon SNS.

  Cuando se activa la alarma, se le notifica mediante el envío de un mensaje a una dirección de correo electrónico de un tema de Amazon Simple Notification Service (Amazon SNS).

Crear la CloudWatch alarma

En este procedimiento, se crea un filtro de métricas de grupos de CloudWatch registros que busca instancias de la excepción de eliminación pendiente. A continuación, crea una CloudWatch alarma basada en la métrica del grupo de registros. Para obtener información sobre los filtros de métricas de grupos de registros, consulte Creación de métricas a partir de eventos de registro mediante filtros en la Guía del usuario de Amazon CloudWatch Logs.

1. Cree un filtro de CloudWatch métricas que analice los CloudTrail registros.

   Siga las instrucciones que se indican en Crear un filtro de métricas para un grupo de registro con los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Patrón de filtro	`{ $.eventSource = kms* && $.errorMessage = "* is pending deletion."}`
Valor de la métrica	1

2. Cree una CloudWatch alarma basada en el filtro de métricas que creó en el paso 1.

Siga las instrucciones de Crear una CloudWatch alarma basada en un filtro métrico de grupos de registros utilizando los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Filtro de métricas	El nombre del filtro de métricas que ha creado en el Paso 1.
Tipo de umbral	Estático
Condiciones	Whenever *metric-name* is Greater than 1 (Siempre que el nombre de la métrica sea mayor que)
Puntos de datos para alarma	1 fuera de 1
Tratamiento de datos que faltan	Treat missing data as good (not breaching threshold) (Tratar los datos que faltan como buenos [dentro del umbral])

Tras completar este procedimiento, recibirá una notificación cada vez que la nueva CloudWatch alarma entre en estado. `ALARM` Si recibe una notificación para esta alarma, puede significar que todavía se necesita una eliminación programada para cifrar o descifrar datos. En ese caso, cancele la eliminación de la clave KMS y reconsidere su decisión de eliminarla.

Determinar el uso anterior de una clave KMS

Antes de eliminar una clave KMS, es recomendable que averigüe cuántos textos se han cifrado con dicha clave. AWS KMS no almacena esta información ni ninguno de los textos cifrados. Saber cómo se ha usado una clave KMS anteriormente puede ayudarle a decidir si la necesitará en el futuro. En este tema se sugieren varias estrategias que pueden ayudarle a determinar el uso anterior de una clave KMS.

> **Warning**
>
> Estas estrategias para determinar el uso anterior y real son efectivas solo para los usuarios de AWS y las operaciones de AWS KMS. No pueden detectar el uso de la clave pública de una clave KMS asimétrica fuera de AWS KMS. Para obtener detalles acerca de los riesgos especiales de la eliminación de las claves KMS asimétricas utilizadas para la criptografía de clave pública, incluida la creación de textos cifrados que no se pueden descifrar, consulte Eliminación de claves KMS asimétricas.

Temas

Examinar los permisos de clave KMS para determinar el ámbito de uso potencial

Determinar quién o qué tiene acceso actualmente a una clave KMS puede ayudarle a determinar el alcance de uso de la clave KMS y si sigue siendo necesaria. Para obtener información sobre cómo determinar quién o qué tiene acceso actualmente a una clave KMS, vaya a Determinar el acceso a AWS KMS keys.

Examinar los registros de AWS CloudTrail para determinar el uso real

Puede utilizar un historial de uso de claves KMS como ayuda para determinar si tiene textos cifrados en una clave KMS concreta.

Toda la actividad de la API de la AWS KMS se registra en los archivos de registro AWS CloudTrail. Si ha creado un registro en CloudTrail la región en la que se encuentra su clave de KMS, puede examinar los archivos de CloudTrail registro para ver un historial de toda la actividad de la AWS KMS API de una clave de KMS concreta. Si no tienes un registro, puedes ver los eventos recientes en tu historial de CloudTrail eventos. Para obtener más información sobre cómo se AWS KMS usa CloudTrail, consulteRegistrar llamadas a la AWS KMS API con AWS CloudTrail.

Los siguientes ejemplos muestran las entradas de CloudTrail registro que se generan cuando se utiliza una clave de KMS para proteger un objeto almacenado en Amazon Simple Storage Service (Amazon S3). En este ejemplo, el objeto se carga en Amazon S3 utilizando Protección de datos mediante cifrado del lado del servidor con claves KMS (SSE-KMS). Al cargar un objeto en Amazon

S3 con SSE-KMS, especifique la clave KMS que se usará para proteger el objeto. Amazon S3 utiliza la AWS KMS GenerateDataKeyoperación para solicitar una clave de datos única para el objeto, y este evento de solicitud se registra CloudTrail con una entrada similar a la siguiente:

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:example-user",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admins/example-user",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2015-09-10T23:12:48Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admins",
        "accountId": "111122223333",
        "userName": "Admins"
      }
    },
    "invokedBy": "internal.amazonaws.com"
  },
  "eventTime": "2015-09-10T23:58:18Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "GenerateDataKey",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {"aws:s3:arn": "arn:aws:s3:::example_bucket/example_object"},
    "keySpec": "AES_256",
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  },
  "responseElements": null,
  "requestID": "cea04450-5817-11e5-85aa-97ce46071236",
  "eventID": "80721262-21a5-49b9-8b63-28740e7ce9c9",
  "readOnly": true,
```

```
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

Cuando posteriormente descargue este objeto de Amazon S3, Amazon S3 envía una solicitud de `Decrypt` de la AWS KMS para descifrar la clave de datos del objeto mediante la clave KMS especificada. Al hacerlo, los archivos de CloudTrail registro incluyen una entrada similar a la siguiente:

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:example-user",
    "arn": "arn:aws:sts::111122223333:assumed-role/Admins/example-user",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2015-09-10T23:12:48Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/Admins",
        "accountId": "111122223333",
        "userName": "Admins"
      }
    },
    "invokedBy": "internal.amazonaws.com"
  },
  "eventTime": "2015-09-10T23:58:39Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
```

```
  "requestParameters": {
    "encryptionContext": {"aws:s3:arn": "arn:aws:s3:::example_bucket/example_object"}},
  "responseElements": null,
  "requestID": "db750745-5817-11e5-93a6-5b87e27d91a0",
  "eventID": "ae551b19-8a09-4cfc-a249-205ddba330e3",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

CloudTrail registra toda la actividad de la API de AWS KMS. Al evaluar estas entradas de registro, puede determinar el uso anterior de una determinada clave KMS y esto puede ayudarle a determinar si desea eliminarla.

Para ver más ejemplos de cómo aparece la actividad de la AWS KMS API en tus archivos de CloudTrail registro, visitaRegistrar llamadas a la AWS KMS API con AWS CloudTrail. Para obtener más información, CloudTrail consulta la Guía AWS CloudTrail del usuario.

Estados clave de AWS KMS las claves

A AWS KMS key siempre tiene un estado clave. Las operaciones en la clave KMS y su entorno pueden cambiar ese estado de clave, ya sea de forma transitoria, o hasta que otra operación cambie su estado clave.

La tabla de esta sección muestra cómo los estados clave afectan a las llamadas a las operaciones de la AWS KMS API. Como resultado de su estado clave, se espera que una operación en una clave KMS tenga éxito (#), falle (X), o tenga éxito solo bajo ciertas condiciones (?). El resultado a menudo difiere en el caso de las claves KMS con material de claves importado.

Esta tabla incluye sólo las operaciones de API que utilizan una clave KMS existente. Se omiten otras operaciones ListKeys, como CreateKeyy.

Temas

- Estados clave y tipos de claves KMS
- Tabla estado de claves

Estados clave y tipos de claves KMS

El tipo de clave KMS determina los estados clave que puede tener.

- Todas las claves KMS pueden estar en los estados `Enabled`, `Disabled` y `PendingDeletion`.
- La mayoría de las claves KMS se crean en el estado `Enabled`. Las claves con material de claves importado se crean en el estado `PendingImport`.
- El estado `PendingImport` solo se aplica a las claves KMS con material de claves importado.
- El estado `Unavailable` se aplica solo a una clave KMS en un almacén de claves personalizado. Una clave KMS en un almacén de AWS CloudHSM claves se produce `Unavailable` cuando el almacén de claves personalizado se desconecta intencionadamente de su AWS CloudHSM clúster. Una clave de KMS en un almacén de claves externo está `Unavailable` cuando el almacén de claves personalizado se desconecta de forma intencionada de su proxy del almacén de claves externo. Puede ver y administrar las claves KMS no disponibles, pero no puede usarlas en operaciones criptográficas.

  El estado de clave de una clave de KMS de un almacén de claves personalizado no se ve afectado por los cambios realizados a su clave de respaldo. Una clave KMS de un almacén de AWS CloudHSM claves no se ve afectada por los cambios en su material de claves asociado en el AWS CloudHSM clúster. Una clave de KMS de un almacén de claves externo no se ve afectada por los cambios en su clave externa en un administrador de claves externo. Si la clave de respaldo está deshabilitada o eliminada, el estado de la clave de KMS no cambia, pero fallan las operaciones criptográficas que utilizan la clave de KMS.
- Los estados clave `Creating`, `Updating` y `PendingReplicaDeletion` solo se aplican a claves de varias regiones.
  - Una clave de réplica de varias regiones está en el estado de clave `Creating` transitorio mientras se está creando. Es posible que este proceso siga en curso cuando se complete la ReplicateKeyoperación. Cuando se completa el proceso de replicación, la clave de réplica se encuentra en el estado `Enabled` o `PendingImport`.
  - Las claves de varias regiones están en el estado clave `Updating` transitorio mientras se actualiza la región principal. Es posible que este proceso siga en curso cuando se complete la UpdatePrimaryRegionoperación. Cuando se completa el proceso de actualización, las claves principal y de réplica reanudan el estado de clave `Enabled`.
  - Cuando se programa la eliminación de una clave principal de varias regiones que tiene claves de réplica, la clave principal se encuentra en el estado `PendingReplicaDeletion` hasta que se eliminen todas sus claves de réplica. A continuación, el estado de clave cambia a

`PendingDeletion`. Para obtener más detalles, consulte Eliminación de claves de varias regiones.

Tabla estado de claves

En la siguiente tabla se muestra cómo el estado de clave de una clave KMS afecta las operaciones de AWS KMS .

Las descripciones de las notas numeradas a pie de página ([n]) se encuentran al final de este tema.

> **Note**
>
> Es posible que tenga que desplazarse horizontal o verticalmente para ver todos los datos de esta tabla.

API	Habilitado	Deshabilitad	Eliminación pendiente Eliminación pendiente de réplica	Importación pendiente	No disponible	Creación	Actualización
CancelKeyDeletion	✗ [4]	✗ [4]	✓	✗ [4]	✗ [4], [13]	✗ [4]	✗ [4]
CreateAlias	✓	✓	✗ [3]	✓	✓	✓	✓
CreateGrant	✓	✗	✗	✗	✓	✗	✓

API	Habilitado	Deshabilitad	Eliminación pendiente Eliminación pendiente de réplica	Importación pendiente	No disponible	Creación	Actualización
		[1]	[2] o [3]	[5]		[14]	
Decrypt	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
DeleteAlias	✓	✓	✓	✓	✓	✓	✓
DeleteImportedKeyMaterial	✓ [9]	✓ [9]	✓ [9]	✓ (sin efecto)	N/A	⊗ [14]	⊗ [15]
DescribeKey	✓	✓	✓	✓	✓	✓	✓
DisableKey	✓	✓	⊗ [3]	⊗ [5]	✓ [12]	⊗ [14]	⊗ [15]
DisableKeyRotation	? [7]	⊗ [1] o [7]	⊗ [3] o [7]	⊗ [6]	⊗ [7]	⊗ [14]	? [7]

API	Habilitado	Deshabilitad	Eliminación pendiente Eliminación pendiente de réplica	Importación pendiente	No disponible	Creación	Actualización
EnableKey	✓	✓	⊗ [3]	⊗ [5]	✓ [12]	⊗ [14]	⊗ [15]
EnableKeyRotation	? [7]	⊗ [1] o [7]	⊗ [3] o [7]	⊗ [6]	⊗ [7]	⊗ [14]	? [7]
Encrypt	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
GenerateDataKey	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
GenerateDataKeyPair	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
GenerateDataKeyPairWithoutPlaintext	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓

API	Habilitado	Deshabilitad	Eliminación pendiente Eliminación pendiente de réplica	Importación pendiente	No disponible	Creación	Actualización
GenerateDataKeyWithoutPlaintext	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
GenerateMac	✓	⊗ [1]	⊗ [2] o [3]	N/A	N/A	⊗ [14]	✓
GetKeyPolicy	✓	✓	✓	✓	✓	✓	✓
GetKeyRotationStatus	? [7]	? [7]	? [7]	⊗ [6]	⊗ [7]	? [7]	? [7]
GetParametersForImport	? [9]	? [9]	⊗ [8] o [9]	✓	⊗ [9]	⊗ [14]	⊗ [15]
GetPublicKey	✓	⊗ [1]	⊗ [2] o [3]	N/A	N/A	⊗ [14]	✓

API	Habilitado	Deshabilitad	Eliminación pendiente Eliminación pendiente de réplica	Importación pendiente	No disponible	Creación	Actualización
ImportKeyMaterial	[9]	[9]	[8] o [9]	✓	[9]	[14]	✓
ListAliases	✓	✓	✓	✓	✓	✓	✓
ListGrants	✓	✓	✓	✓	✓	✓	✓
ListKeyPolicies	✓	✓	✓	✓	✓	✓	✓
ListKeyRotations	[7]	[7]	[7]	[6]	[7]	[7]	[7]
ListResourceTags	✓	✓	✓	✓	✓	✓	✓
PutKeyPolicy	✓	✓	✓	✓	✓	✓	✓
ReEncrypt	✓	[1]	[2] o [3]	[5]	[11]	[14]	✓

API	Habilitado	Deshabilitad	Eliminación pendiente Eliminación pendiente de réplica	Importación pendiente	No disponible	Creación	Actualización
ReplicateKey	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	N/A	⊗ [14]	⊗ [15]
RetireGrant	✓	✓	✓	✓	✓	✓	✓
RevokeGrant	✓	✓	✓	✓	✓	✓	✓
RotateKeyOnDemand	? [7]	⊗ [1] o [7]	⊗ [3] o [7]	⊗ [6]	⊗ [7]	⊗ [14]	? [7]
ScheduleKeyDeletion	✓	✓	⊗ [3]	✓	✓	✓	⊗ [15]
Sign	✓	⊗ [1]	⊗ [2] o [3]	N/A	N/A	⊗ [14]	✓
TagResource	✓	✓	⊗ [3]	✓	✓	✓	✓

API	Habilitado	Deshabilitad	Eliminación pendiente Eliminación pendiente de réplica	Importación pendiente	No disponible	Creación	Actualización
UntagResource	✓	✓	⊗ [3]	✓	✓	✓	✓
UpdateAlias	✓	✓	? [10]	✓	✓	✓	✓
UpdateKeyDescription	✓	✓	⊗ [3]	✓	✓	✓	✓
UpdatePrimaryRegion	✓	⊗ [1]	⊗ [2] o [3]	⊗ [5]	N/A	⊗ [14]	✓
Verificar	✓	⊗ [1]	⊗ [2] o [3]	N/A	N/A	⊗ [14]	✓
VerifyMac	✓	⊗ [1]	⊗ [2] o [3]	N/A	N/A	⊗ [14]	✓

Detalles de la tabla

- [1] `DisabledException: <key ARN> is disabled.`
- [2] `DisabledException: <key ARN> is pending deletion (or pending replica deletion).`
- [3] `KMSInvalidStateException: <key ARN> is pending deletion (or pending replica deletion).`
- [4] `KMSInvalidStateException: <key ARN> is not pending deletion (or pending replica deletion).`
- [5] `KMSInvalidStateException: <key ARN> is pending import.`
- [6] `UnsupportedOperationException: <key ARN> origin is EXTERNAL which is not valid for this operation.`
- [7] Si la clave KMS tiene material de claves importado o está en un almacén de claves personalizado: `UnsupportedOperationException`.
- [8] Si la clave KMS tiene material de claves importado: `KMSInvalidStateException`
- [9] Si la clave KMS no puede tener o no tiene material de claves importado: `UnsupportedOperationException`.
- [10] Si la clave KMS de origen está pendiente de eliminación, el comando se ejecuta satisfactoriamente. Si la clave KMS de destino está pendiente de eliminación, el comando genera el error: `KMSInvalidStateException : <key ARN> is pending deletion.`
- [11] `KMSInvalidStateException: <key ARN> is unavailable.` No puede realizar esta operación en una clave KMS no disponible.
- [12] La operación se ha realizado correctamente pero el estado de clave de la clave KMS no cambiará hasta que esté disponible.
- [13] Mientras una clave KMS en el almacén de claves personalizado esté pendiente de eliminación, su estado de clave seguirá siendo `PendingDeletion` incluso si la clave KMS no está disponible. Esto permite cancelar la eliminación de la clave KMS en cualquier momento durante el período de espera.
- [14] `KMSInvalidStateException: <key ARN> is creating.` AWS KMS lanza esta excepción mientras se replica una clave multirregional ()`ReplicateKey`.
- [15] `KMSInvalidStateException: <key ARN> is updating.` AWS KMS lanza esta excepción mientras se actualiza la región principal de una clave multirregional (). `UpdatePrimaryRegion`

Autenticación y control de acceso de AWS KMS

Para utilizar AWS KMS, debe tener credenciales que AWS pueda utilizar para autenticar las solicitudes. Las credenciales deben incluir permisos para obtener acceso a los recursos de AWS, AWS KMS keys y alias. Ninguna entidad principal de AWS tiene permisos para una clave KMS, a menos que dicho permiso se proporcione explícitamente y nunca se deniegue. No hay permisos implícitos ni automáticos para usar o administrar una clave KMS.

La forma principal de administrar el acceso a sus recursos de AWS KMS es a través de políticas. Las políticas son documentos que describen qué entidades principales pueden acceder a qué recursos. Las políticas adjuntadas a una identidad de IAM se denominan políticas basadas en identidad (o políticas de IAM) y las políticas adjuntadas a otros tipos de recursos se denominan políticas de recursos. Las políticas de recursos de AWS KMS para las claves KMS se denominan políticas de claves. Todas las claves KMS tienen una política de claves.

Para controlar el acceso a sus alias de AWS KMS, utilice las políticas de IAM. Para permitir que las entidades principales creen alias, debe proporcionar el permiso al alias en una política de IAM y el permiso a la clave en una política de claves. Para obtener más detalles, consulte Control del acceso a alias.

Para controlar el acceso a las claves KMS, puede utilizar los siguientes mecanismos de políticas.

- Política de claves: cada clave KMS tiene una política de claves. Es el mecanismo principal para controlar el acceso a una clave KMS. Puede utilizar solo la política de claves para controlar el acceso, lo que significa que el ámbito completo de acceso a la clave KMS se define en un único documento (la política de claves). Para obtener más información sobre el uso de políticas de claves, consulte Políticas de claves.
- Políticas de IAM: puede utilizar políticas de IAM en combinación con la política de claves y subvenciones para controlar el acceso a una clave KMS. Este modo de controlar el acceso le permite administrar todos los permisos de las identidades de IAM en IAM. Para utilizar una política de IAM a fin de permitir el acceso a una clave KMS, la política de claves debe permitirlo explícitamente. Para obtener más información sobre el uso de políticas de IAM, consulte Políticas de IAM.
- Concesiones: puede utilizar concesiones en combinación con la política de claves y políticas de IAM para permitir el acceso a una clave KMS. Con este modo de controlar el acceso, puede permitir el acceso a la clave KMS en la política de claves y permitir que las identidades deleguen

su acceso a otros. Para obtener más información sobre cómo usar concesiones, consulte Concesiones en AWS KMS.

Las claves de KMS pertenecen a la cuenta de AWS en la que se crearon. Sin embargo, ninguna identidad ni entidad principal, incluido el usuario raíz de la cuenta de AWS, tiene permiso para usar o administrar una clave KMS, a menos que ese permiso se proporcione explícitamente en una política de claves, una política de IAM o una concesión. La identidad de IAM que crea una clave KMS no se considera el propietaria de la clave y no tiene permiso automáticamente para usar o administrar la clave KMS que creó. Al igual que cualquier otra identidad, el creador de la clave necesita obtener permiso a través de una política de claves, una política de IAM o una concesión. Sin embargo, las identidades que tienen el permiso de `kms:CreateKey` pueden establecer la política de clave inicial y darse permiso a ellas mismas para usar o administrar la clave.

Los siguientes temas brindan detalles sobre cómo puede utilizar los permisos de AWS Identity and Access Management (IAM) y AWS KMS para ayudar a proteger sus recursos controlando quién puede obtener acceso a ellos.

Temas

- Conceptos sobre el control de acceso de AWS KMS
- Políticas clave en AWS KMS
- Uso de políticas de IAM con AWS KMS
- Concesiones en AWS KMS
- Conectar con AWS KMS a través de un punto de conexión de VPC
- Claves de estado para AWS KMS
- ABAC para AWS KMS
- Permitir a los usuarios de otras cuentas utilizar una clave KMS
- Uso de roles vinculados a servicios de AWS KMS
- Usar el cifrado TLS híbrido postcuántico con AWS KMS
- Determinar el acceso a AWS KMS keys
- AWS KMS permisos
- Prueba de los permisos

Conceptos sobre el control de acceso de AWS KMS

Aprenda los conceptos utilizados en las conversaciones sobre el control de acceso en AWS KMS.

Temas

Autenticación

La autenticación es el proceso de verificación de su identidad. Para enviar una solicitud a AWS KMS, debe iniciar sesión en AWS con sus credenciales de AWS.

Autorización

La autorización proporciona el permiso para enviar solicitudes para crear, administrar o utilizar recursos AWS KMS. Por ejemplo, debe estar autorizado a utilizar una clave KMS en una operación criptográfica.

Use políticas de claves, políticas de IAM y concesiones para controlar el acceso a sus recursos de AWS KMS. Cada clave de KMS debe tener una política de claves. Si la política de claves lo permite, también puede utilizar las políticas y autorizaciones de IAM para conceder acceso a la clave KMS a las entidades principales. Para restringir la autorizaciones, puede utilizar claves de condición que pueden permitir o denegar el acceso solo cuando una solicitud o recurso cumple las condiciones que especifica. También puede permitir el acceso a las entidades principales en las que confía en otras cuentas de Cuentas de AWS.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad de AWS IAM Identity Center. Los usuarios (del

IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso a AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no utiliza las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre el método recomendado para la firma de solicitudes, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Independientemente del método de autenticación que utilice, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidades para acceder a Servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidad web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a Servicios de AWS utilizando credenciales proporcionadas a través de una fuente de identidad. Cuando identidades federadas acceden a las Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones y Cuentas de AWS. Para obtener más información, consulte ¿Qué es el IAM Identity Center? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad en su Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del Usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del Usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad de tu Cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Consolecambiando de roles. Puede asumir un

rol llamando a una operación de AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del Usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del Usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos

para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Rol vinculado al servicio: un rol vinculado al servicio es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de las políticas JSON en la Guía del Usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del rol de la AWS Management Console, la AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidades son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Una política clave AWS KMS es una política basada en recursos que controla el acceso a una clave KMS. Cada clave de KMS debe tener una política de claves. Puede utilizar otro mecanismo de autorizaciones para permitir el acceso a la clave KMS, pero solo si la política de claves lo permite. (Puede utilizar una política de IAM para denegar el acceso a una clave KMS incluso si la política de claves no lo permite explícitamente).

Las políticas basadas en recursos son documentos de política JSON que puede asociar a un recurso, como, por ejemplo, una clave KMS, para controlar el acceso a un recurso específico. Las políticas basadas en recursos definen las acciones que puede realizar una entidad principal en ese recurso y en qué condiciones. No especifica el recurso en una política basada en recursos, pero debe especificar una entidad principal, como cuentas, usuarios, roles, usuarios federados o Servicios

de AWS. Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio que administra el recurso. No puede utilizar políticas de IAM administradas por AWS, como la política administrada de `AWSKeyManagementServicePowerUser` en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para Desarrolladores de Amazon Simple Storage Service.

AWS KMS no es compatible con los ACL.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del Usuario de IAM.
- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de la cuenta de AWS. Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario AWS Organizations.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del Usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS decide si permite o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Recursos de AWS KMS

En AWS KMS, el recurso principal es una AWS KMS key. AWS KMS también permite usar un alias, un recurso independiente que proporciona un nombre descriptivo para una clave de KMS. Algunas operaciones de AWS KMS le permiten utilizar un alias para identificar una clave KMS.

Cada instancia de una clave KMS o alias tiene un único nombre de recurso de Amazon (ARN) con un formato estándar. En los recursos de AWS KMS, el nombre del servicio de AWS es `kms`.

- AWS KMS key

  Formato de ARN:

  `arn:`*`AWS partition name`*`:`*`AWS service name`*`:`*`Región de AWS`*`:`*`Cuenta de AWS ID`*`:key/`*`key ID`*

  Ejemplo de ARN:

  ```
  arn:aws:kms:us-
  west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
  ```

- Alias

  Formato de ARN:

  `arn:`*`AWS partition name`*`:`*`AWS service name`*`:`*`Región de AWS`*`:`*`Cuenta de AWS ID`*`:alias/`*`alias name`*

Ejemplo de ARN:

```
arn:aws:kms:us-west-2:111122223333:alias/example-alias
```

AWS KMS proporciona un conjunto de operaciones de API para trabajar con sus recursos de AWS KMS. Para obtener más información acerca de la identificación de claves KMS en las operaciones de API de la AWS Management Console y AWS KMS, consulte Identificadores clave () KeyId. Para ver una lista de operaciones de AWS KMS, consulte la Referencia de la API de AWS Key Management Service.

Políticas clave en AWS KMS

Una política clave es una política de recursos para un. AWS KMS key Las políticas de claves son la forma principal de controlar el acceso a las claves KMS. Cada clave KMS debe tener exactamente una política de clave. Las declaraciones de políticas de claves determinan quién tiene permiso para usar la clave KMS y cómo debe usar dicho permiso. También puede utilizar políticas de IAM y concesiones para controlar el acceso a la clave KMS, pero cada clave KMS debe tener un documento de política de claves.

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 autorice explícitamente, y nunca se deniegue, en una política de claves, una política de IAM o una concesión.

A menos que la política de claves lo permita explícitamente, no puede utilizar las políticas de IAM para permitir el acceso a una clave KMS. Sin el permiso de la política de claves, las políticas de IAM que conceden permisos no tienen ningún efecto. (Puede utilizar una política de IAM para denegar un permiso a una clave KMS sin el permiso de una política de claves). La política de claves predeterminada habilita las políticas de IAM. Para habilitar las políticas de IAM en la política de claves, agregue la declaración de política descrita en Permite el acceso a la Cuenta de AWS y habilita las políticas de IAM.

A diferencia de las políticas de IAM, que son globales, las políticas de claves son regionales. Una política de claves controla el acceso solo a una clave KMS en la misma región. No tiene ningún efecto sobre las claves KMS de otras regiones.

Temas

- Creación de una política de claves

- Política de claves predeterminada
- Consultar una política de claves
- Cambiar una política de claves
- Permisos para AWS los servicios en las políticas clave

Creación de una política de claves

Puede crear y administrar políticas clave en la AWS KMS consola mediante operaciones de AWS KMS API, como CreateKey, y ReplicateKeyPutKeyPolicy, o mediante una AWS CloudFormation plantilla.

Al crear una clave de KMS en la AWS KMS consola, la consola le explicará los pasos necesarios para crear una política de claves basada en la política de claves predeterminada de la consola. Al utilizar las API `CreateKey` o `ReplicateKey`, si no se especifica una política de claves, estas API aplican la política de claves predeterminada para claves creadas mediante programación. Al usar la API `PutKeyPolicy`, es necesario especificar una política de claves.

Cada documento de política puede tener una o varias declaraciones de política. En el siguiente ejemplo se muestra un documento válido de política de claves con una declaración de política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Describe the policy statement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/Alice"
      },
      "Action": "kms:DescribeKey",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:KeySpec": "SYMMETRIC_DEFAULT"
        }
      }
    }
  ]
}
```

Temas

Formato de la política de claves

Un documento de política de claves debe cumplir las siguientes reglas:

- Pesar hasta 32 kilobytes (32 768 bytes)
- El elemento `Sid` de una declaración de política de claves puede incluir espacios. (Se prohíben los espacios en el elemento `Sid` de un documento de política de IAM).

Un documento de política de claves solo puede incluir los siguientes caracteres:

- Caracteres ASCII imprimibles
- Caracteres imprimibles del conjunto de caracteres Basic Latin y Latin-1 Supplement
- Caracteres especiales como la pestaña (`\u0009`), la fuente de línea (`\u000A`) y retorno de carro (`\u000D`)

Elementos de una política de claves

Un documento de política de claves debe tener los siguientes elementos:

Versión

Especifica la versión del documento de política de claves. Configure la versión en `2012-10-17` (la última versión).

Instrucción

Contiene las declaraciones de la política. Un documento de política de claves debe tener al menos una declaración.

Cada declaración de política de claves consta de hasta seis elementos. Los elementos `Effect`,`Principal`,`Action`, y `Resource` son necesarios.

Sid

(Opcional) El identificador de la declaración (`Sid`) una cadena arbitraria que puede utilizar para describir la declaración. El `Sid` en una política de claves puede incluir espacios. (No puede incluir espacios en un elemento `Sid` de política de IAM).

Efecto

(Obligatorio) Determina si desea permitir o denegar los permisos en la declaración de política. Los valores válidos son `Allow` o `Deny`. Si no permite el acceso de forma explícita a una clave KMS, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a una clave KMS. Puede hacer esto para asegurarse de que un usuario no pueda tener acceso a ella, aunque otra política le permita el acceso.

Entidad principal

(Obligatorio) La entidad principal es la identidad que obtiene los permisos especificados en la declaración de política. Puede especificar Cuentas de AWS los usuarios de IAM, las funciones de IAM y algunos AWS servicios como principales en una política clave. Los grupos de usuarios de IAM no son una entidad principal válida en ningún tipo de política.

Un valor de asterisco, como `"AWS": "*"`, representa todas las identidades de AWS de todas las cuentas.

> **Important**
>
> No establezca la Entidad principal en un asterisco (*) en ninguna declaración de política de claves que permita permisos a menos que utilice condiciones para limitar la política de claves. Un asterisco indica todas las identidades de cada Cuenta de AWS permiso para usar la clave de KMS, a menos que otra declaración de política lo deniegue explícitamente. Los usuarios de otros Cuentas de AWS pueden usar su clave de KMS siempre que tengan los permisos correspondientes en su propia cuenta.

> **Note**
>
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

Cuando la entidad principal en una declaración de política de claves es una entidad principal de Cuenta de AWS se expresa como `arn:aws:iam::111122223333:root"`, la declaración de la política no concede permisos a ninguna entidad principal de IAM. En su lugar, otorga Cuenta de AWS permiso para usar las políticas de IAM para delegar los permisos especificados en la política clave. (Una entidad principal en formato `arn:aws:iam::111122223333:root"` no representa al usuario raíz de la cuenta de AWS, a pesar del uso de "root" en el identificador de la cuenta. Sin embargo, la entidad principal de la cuenta representa a la cuenta y a sus administradores, incluido el usuario raíz de la cuenta).

Cuando el principal es otro Cuenta de AWS o sus directores, los permisos solo entran en vigor cuando la cuenta está habilitada en la región con la clave y la política de claves de KMS. Para obtener información acerca de las regiones que no están habilitadas de forma predeterminada ("Regiones de adhesión"), consulte Administración de Regiones de AWS en la Referencia general de AWS.

Para permitir que otro Cuenta de AWS o sus principales usuarios utilicen una clave de KMS, debes conceder el permiso en una política de claves y en una política de IAM en la otra cuenta. Para obtener más detalles, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS.

Acción

(Obligatorio) Especifique las operaciones de la API que se permitirán o denegarán. Por ejemplo, la `kms:Encrypt` acción corresponde a la operación de AWS KMS cifrado. Puede enumerar varias acciones en una declaración de política. Para obtener más información, consulte Referencia de permisos.

Recurso

(Obligatorio) En una política de claves, el valor del elemento Recurso es `"*"`, que significa "esta clave KMS". El asterisco (`"*"`) identifica la clave KMS a la que se adjunta la política de clave.

> **Note**
>
> Si falta el elemento `Resource` requerido en una declaración de política de claves, la declaración de la política no tiene efecto. Una declaración de política de claves sin un elemento `Resource` no se aplica a ninguna clave KMS.
> Cuando falta un `Resource` elemento en una declaración de política clave, la AWS KMS consola informa correctamente de un error, pero PutKeyPolicylas API

CreateKeyy las API funcionan correctamente, aunque la declaración de política no sea efectiva.

Condición

(Opcional) Las condiciones especifican requisitos que deben cumplirse para que se aplique una política de claves. Con condiciones, AWS puede evaluar el contexto de una solicitud de API para determinar si la declaración de política se aplica o no.

Para especificar las condiciones, se utilizan claves de condición predefinidas. AWS KMS admite claves de condición AWS globales y claves de AWS KMS condición. Para admitir el control de acceso basado en atributos (ABAC), AWS KMS proporciona claves de condición que controlan el acceso a una clave KMS en función de etiquetas y alias. Para obtener más detalles, consulte ABAC para AWS KMS.

El formato de una condición es:

```
"Condition": {"condition operator": {"condition key": "condition value"}}
```

por ejemplo:

```
"Condition": {"StringEquals": {"kms:CallerAccount": "111122223333"}}
```

Para obtener más información sobre la sintaxis de las AWS políticas, consulte la Referencia de políticas de AWS IAM en la Guía del usuario de IAM.

Política de claves de ejemplo

En el siguiente ejemplo se muestra una política de claves completa para una clave KMS de cifrado simétrica. Puede utilizarlo como referencia mientras lee acerca de los conceptos de política de claves de este capítulo. Esta política de claves combina los ejemplos de declaraciones de política de la sección política de claves predeterminada anterior en una sola política de claves que lleva a cabo lo siguiente:

- Permite al ejemplo Cuenta de AWS 111122223333 tener acceso total a la clave KMS. Permite que la cuenta y sus administradores, incluido el usuario raíz de la cuenta (para emergencias), utilicen las políticas de IAM en la cuenta para permitir el acceso a la clave KMS.

- Permite que el rol de IAM `ExampleAdminRole` administre la clave de KMS.
- Permite que el rol de IAM `ExampleUserRole` utilice la clave KMS.

```
{
    "Id": "key-consolepolicy",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow access for Key Administrators",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleAdminRole"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:TagResource",
                "kms:UntagResource",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion",
                "kms:RotateKeyOnDemand"
            ],
            "Resource": "*"
        },
        {
```

```
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleUserRole"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleUserRole"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        }
    ]
}
```

Política de claves predeterminada

Al crear una clave KMS, puede especificar la política de claves para la nueva clave KMS. Si no la proporciona, 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 en la AWS KMS consola o se utiliza la AWS KMS API.

Política de claves predeterminada al crear una clave KMS mediante programación

Cuando se crea una clave de KMS mediante programación con la AWS KMS API (incluso mediante los AWS SDK AWS Tools for PowerShell) y no se especifica una política de claves, AWS KMS se aplica una política de claves predeterminada muy simple. AWS Command Line Interface Esta política de claves predeterminada tiene una declaración de política que otorga al propietario de la Cuenta de AWS clave de KMS permiso para usar las políticas de IAM a fin de permitir el acceso a todas las AWS KMS operaciones de la clave de KMS. Para obtener más información sobre esta declaración de política, consulte Permite el acceso a la Cuenta de AWS y habilita las políticas de IAM.

Política de claves predeterminada al crear una clave KMS con AWS Management Console

Al crear una clave de KMS con la AWS Management Console, la política clave comienza con la declaración de política que permite el acceso a las políticas de IAM Cuenta de AWS y las habilita. A continuación, la consola añade una declaración del administrador clave, una declaración de los usuarios clave y (para la mayoría de los tipos de claves) una declaración que permite a los directores utilizar la clave de KMS con otros AWS servicios. Puede utilizar las funciones de la AWS KMS consola para especificar los usuarios de IAM, los roles de IAM y Cuentas de AWS quiénes son los administradores clave y los usuarios clave (o ambos).

Permisos

- Permite el acceso a la Cuenta de AWS y habilita las políticas de IAM
- Permite que los administradores de claves administren la clave KMS
- Permite a los usuarios de claves utilizar la clave KMS
  - Permite a los usuarios de claves utilizar una clave KMS para las operaciones criptográficas
  - Permite a los usuarios de claves utilizar la clave KMS con los servicios de AWS

Permite el acceso a la Cuenta de AWS y habilita las políticas de IAM

La siguiente declaración de política de claves predeterminada es fundamental.

- Otorga al propietario Cuenta de AWS de la clave KMS acceso completo a la clave KMS.

  A diferencia de otras políticas de AWS recursos, una política AWS KMS clave no otorga automáticamente permisos a la cuenta ni a ninguna de sus identidades. Para conceder permisos a los administradores de cuentas, la política de claves debe incluir una declaración explícita que proporcione este permiso, de forma similar a ésta.
- Permite que la cuenta utilice las políticas de IAM para permitir el acceso a la clave KMS, además de la política de claves.

Sin este permiso, las políticas de IAM que permiten el acceso a la clave son ineficaces, aunque las políticas de IAM que deniegan el acceso a la clave siguen siendo eficaces.

- Reduce el riesgo de que la clave deje de poder administrarse dando permiso de control de acceso a los administradores de la cuenta, incluido el usuario raíz de la cuenta, que no se puede eliminar.

La siguiente declaración de política de claves es toda la política de claves predeterminada para las claves KMS creadas mediante programación. Es la primera declaración de política de la política de claves predeterminada para las claves de KMS creadas en la AWS KMS consola.

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
   },
  "Action": "kms:*",
  "Resource": "*"
}
```

Permite que las políticas de IAM permitan el acceso a la clave KMS.

La declaración de política clave Cuenta de AWS que se muestra arriba otorga al propietario de la clave permiso para usar las políticas de IAM, así como las políticas clave, para permitir todas las acciones (`kms:*`) en la clave de KMS.

La entidad principal en esta declaración de política de claves es la entidad principal de la cuenta, que está representada por un ARN en este formato: `arn:aws:iam::account-id:root`. El principal de la cuenta representa a la AWS cuenta y a sus administradores.

Cuando la entidad principal de una declaración de política de claves es la entidad principal de la cuenta, la declaración de política no concede permisos a ninguna entidad principal de IAM para utilizar la clave KMS. En su lugar, permite que la cuenta utilice las políticas de IAM para delegar los permisos especificados en la declaración de la política. Esta declaración de política de claves predeterminada permite a la cuenta utilizar las políticas de IAM para delegar el permiso para todas las acciones (`kms:*`) en la clave KMS.

reduce el riesgo de que la clave KMS deje de poder administrarse.

A diferencia de otras políticas de AWS recursos, una política AWS KMS clave no otorga automáticamente permisos a la cuenta ni a ninguno de sus directores. Para dar permisos a cualquier entidad principal, incluida la entidad principal de la cuenta, debe utilizar una declaración de política de claves que proporcione los permisos de forma explícita. No es necesario dar a la entidad principal de la cuenta, ni a ninguna entidad principal, acceso a la clave KMS. Sin embargo, dar acceso a la entidad principal de la cuenta le ayuda a evitar que la clave deje de poder administrarse.

Por ejemplo, supongamos que se crea una política de claves que da acceso a la clave KMS a un solo usuario. Si posteriormente elimina ese usuario, la clave deja de poder administrarse y deberá ponerse en contacto con el servicio de asistencia de AWS para recuperar el acceso a la clave KMS.

La declaración de política clave que se muestra arriba permite controlar la clave del principal de la cuenta, que lo representa a él Cuenta de AWS y a sus administradores, incluido el usuario raíz de la cuenta. La cuenta de usuario raíz es la única entidad principal que no se puede eliminar a menos que se elimine la cuenta de Cuenta de AWS. Las prácticas recomendadas de IAM desaconsejan actuar en nombre del usuario raíz de la cuenta, excepto en caso de emergencia. Sin embargo, es posible que tenga que actuar como usuario raíz de la cuenta si elimina todos los demás usuarios y funciones con acceso a la clave KMS.

Permite que los administradores de claves administren la clave KMS

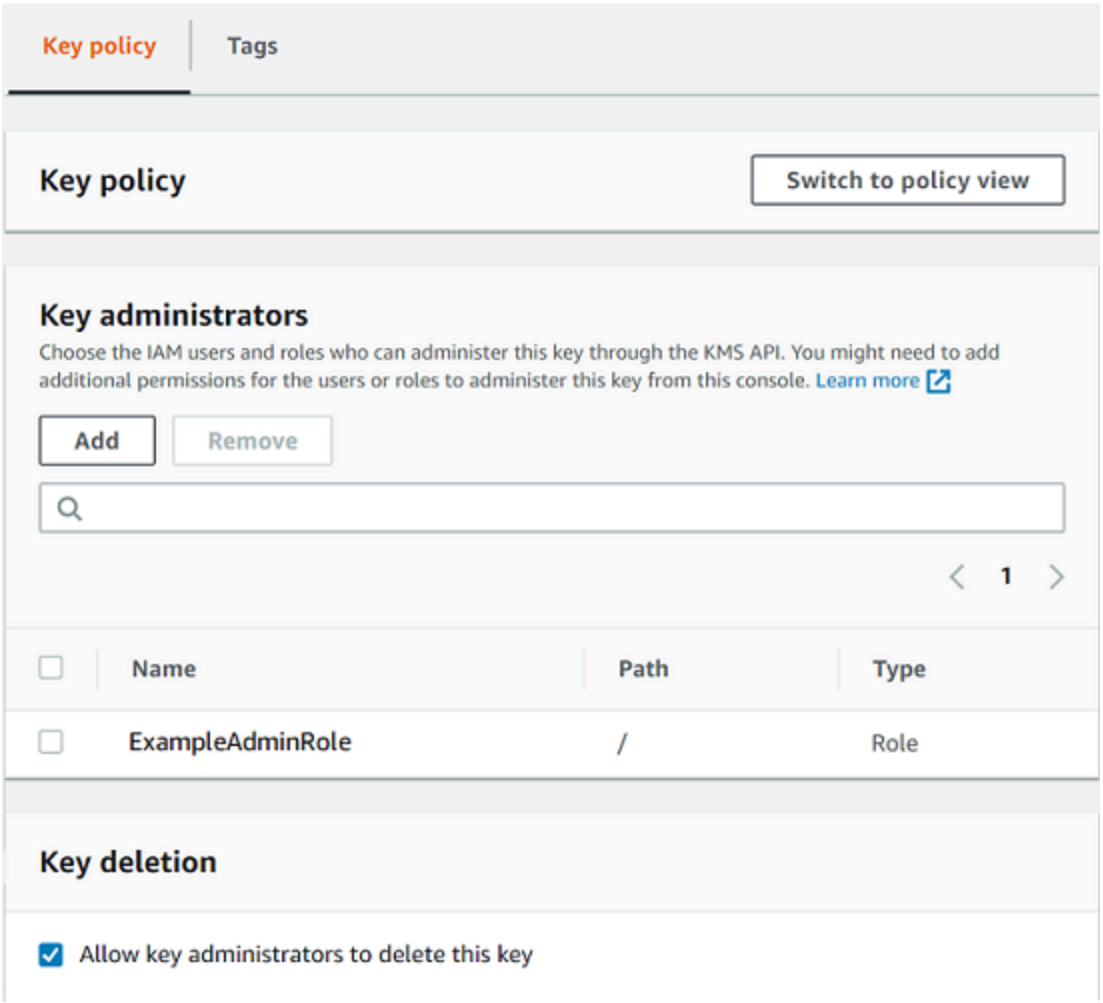
La política de claves predeterminada creada por la consola le permite elegir usuarios y roles de IAM de la cuenta y convertirlos en administradores de claves. Esta declaración se denomina la declaración de los administradores de claves. Los administradores de claves tienen permisos para administrar la clave KMS, pero no para utilizar la clave KMS en operaciones criptográficas. Puede agregar usuarios y roles de IAM a la lista de administradores de claves al crear la clave KMS en la vista predeterminada o en la vista de política.

> **Warning**
>
> Como los administradores de claves tienen permiso para cambiar la política de claves y crear concesiones, pueden concederse a sí mismos y a otras personas AWS KMS permisos no especificados en esta política.

Las entidades principales que tienen permiso para administrar etiquetas y alias también pueden controlar el acceso a una clave KMS. Para obtener más detalles, consulte ABAC para AWS KMS.

> **Note**
>
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

En el siguiente ejemplo se muestra la declaración de los administradores de claves en la vista predeterminada de la consola de AWS KMS .



A continuación se muestra un ejemplo de declaración de los administradores de claves en la vista de política de la consola de AWS KMS . Esta declaración de los administradores de claves es para una clave KMS de cifrado simétrica de una sola región.

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS":"arn:aws:iam::111122223333:role/ExampleAdminRole"},
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:TagResource",
    "kms:UntagResource",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
}
```

La declaración de los administradores de claves predeterminada para la clave KMS más común, una clave KMS de cifrado simétrica de una región única, permite los siguientes permisos. Para obtener información detallada sobre cada permiso, consulte la AWS KMS permisos.

Al usar la AWS KMS consola para crear una clave KMS, la consola agrega los usuarios y roles que especifique al `Principal` elemento en la declaración del administrador clave.

Muchos de estos permisos contienen el carácter comodín (*), que permite todos los permisos que empiezan por el verbo especificado. Como resultado, cuando se AWS KMS añaden nuevas operaciones de API, los administradores de claves pueden utilizarlas automáticamente. No es necesario actualizar las políticas de claves para incluir las nuevas operaciones. Si prefiere limitar sus administradores de claves a un conjunto fijo de operaciones de API, puede cambiar la política de claves.

kms:Create*

Permite kms:CreateAlias y kms:CreateGrant. (El permiso kms:CreateKey solo es válido en una política de IAM).

kms:Describe*

Permite kms:DescribeKey. Se requiere el permiso kms:DescribeKey para ver la página de detalles de clave de una clave KMS en la AWS Management Console.

kms:Enable*

Permite kms:EnableKey. Para las claves KMS de cifrado simétricas, también se permite kms:EnableKeyRotation.

kms:List*

Permite kms:ListGrants, kms:ListKeyPolicies y kms:ListResourceTags. (Los permisos kms:ListAliases y kms:ListKeys, necesarios para ver las claves KMS en la AWS Management Console, solo son válidos en las políticas de IAM.)

kms:Put*

Permite kms:PutKeyPolicy. Este permiso permite a los administradores de claves cambiar la política de claves de esta clave KMS.

kms:Update*

Permite kms:UpdateAlias y kms:UpdateKeyDescription. Para las claves de varias regiones, permite kms:UpdatePrimaryRegion en esta clave KMS.

kms:Revoke*

Permite kms:RevokeGrant, que permite a los administradores de claves eliminar una concesión incluso si no son una entidad principal retirada en la concesión.

kms:Disable*

Permite kms:DisableKey. Para las claves KMS de cifrado simétricas, también se permite kms:DisableKeyRotation.

kms:Get*

Permite kms:GetKeyPolicy y kms:GetKeyRotationStatus. Para claves KMS con material de claves importado, permite kms:GetParametersForImport. Para claves KMS asimétricas, permite kms:GetPublicKey. Se requiere el permiso kms:GetKeyPolicy para ver la política de claves de una clave KMS en la AWS Management Console.

`kms:Delete*`

Permite `kms:DeleteAlias`. Para claves con material de claves importado, permite `kms:DeleteImportedKeyMaterial`. El permiso `kms:Delete*` no permite a los administradores de claves eliminar la clave KMS (`ScheduleKeyDeletion`).

`kms:TagResource`

Permite `kms:TagResource`, que permite a los administradores de claves agregar etiquetas a la clave KMS. Dado que las etiquetas también se pueden utilizar para controlar el acceso a la clave KMS, este permiso permite a los administradores permitir o denegar el acceso a la clave KMS. Para obtener más detalles, consulte ABAC para AWS KMS.

`kms:UntagResource`

Permite `kms:UntagResource`, que permite a los administradores de claves eliminar etiquetas de la clave KMS. Dado que las etiquetas se pueden utilizar para controlar el acceso a la clave, este permiso permite a los administradores permitir o denegar el acceso a la clave KMS. Para obtener más detalles, consulte ABAC para AWS KMS.

`kms:ScheduleKeyDeletion`

Permite `kms:ScheduleKeyDeletion`, que permite a los administradores de claves eliminar esta clave KMS. Para eliminar este permiso, desactive la opción Allow key administrators to delete this key (Permitir a los administradores de claves eliminar esta clave).

`kms:CancelKeyDeletion`

Permite `kms:CancelKeyDeletion`, que permite a los administradores de claves cancelar la eliminación de esta clave KMS. Para eliminar este permiso, desactive la opción Allow key administrators to delete this key (Permitir a los administradores de claves eliminar esta clave).

AWS KMS añade los siguientes permisos a la declaración de administradores de claves predeterminada al crear claves de uso especial.

`kms:ImportKeyMaterial`

El permiso `kms:ImportKeyMaterial` permite a los administradores de claves importar material de claves KMS. Este permiso solo se incluye en la política de claves cuando crea una clave KMS sin material de claves.

`kms:ReplicateKey`

El `kms:ReplicateKey` permiso permite a los administradores de claves crear una réplica de una clave principal multirregional en otra región. AWS Este permiso solo se incluye en la política de claves cuando crea una clave principal o de réplica de varias regiones.

`kms:UpdatePrimaryRegion`

El permiso `kms:UpdatePrimaryRegion` permite a los administradores de claves cambiar una clave de réplica de varias regiones a una clave principal de varias regiones. Este permiso solo se incluye en la política de claves cuando crea una clave principal o de réplica de varias regiones.

Permite a los usuarios de claves utilizar la clave KMS

La política de claves predeterminada que la consola crea para las claves de KMS permite elegir los usuarios y roles de IAM en la cuenta y los externos Cuentas de AWS, y convertirlos en usuarios clave.

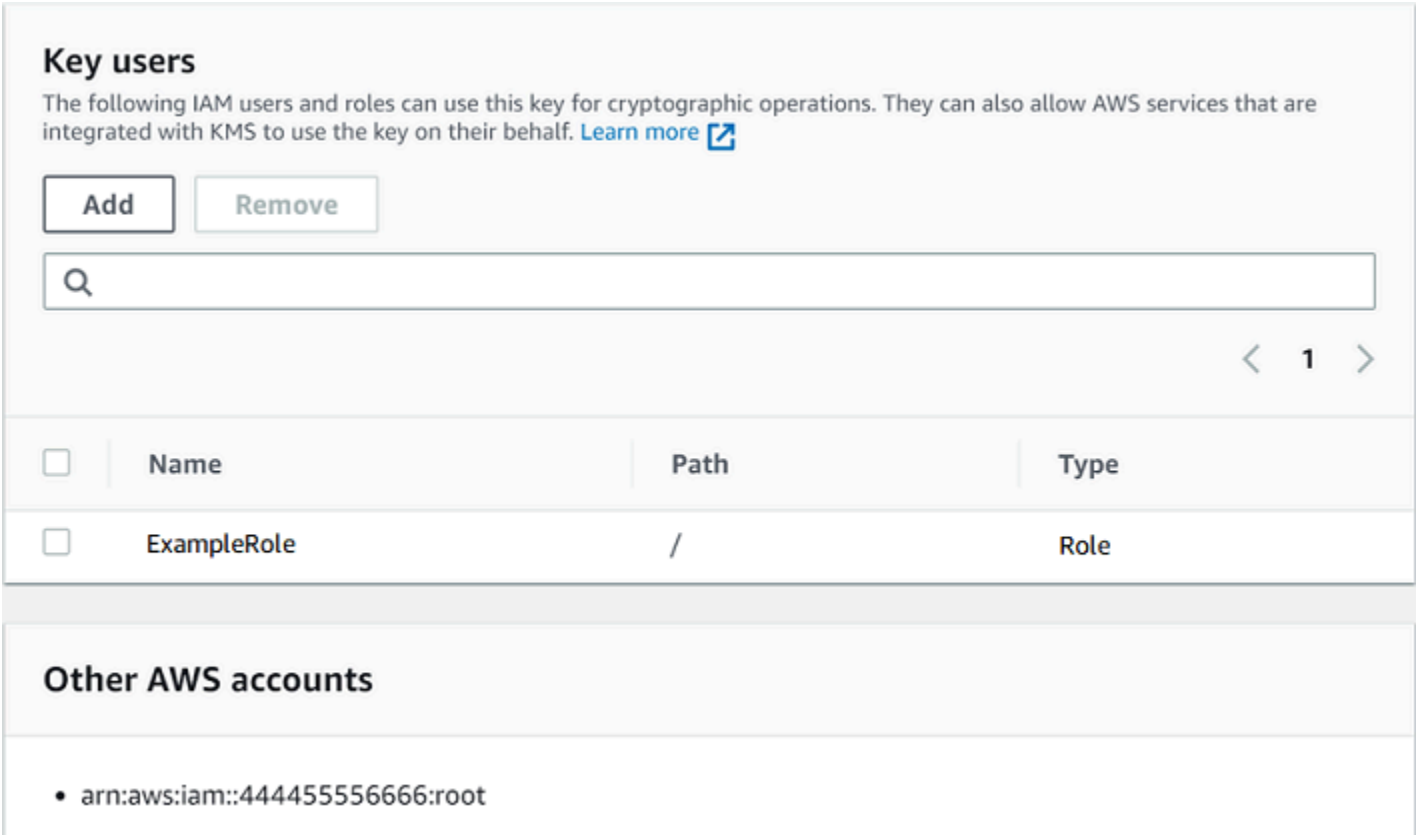
La consola agrega dos declaraciones de política a la política de claves para los usuarios de claves.

- Utilice la clave KMS directamente: la primera declaración de política de claves da a los usuarios de claves permiso para usar la clave KMS directamente para todas las operaciones criptográficas de ese tipo de clave KMS.
- Use la clave de KMS con AWS los servicios: la segunda declaración de política otorga a los usuarios clave permiso para permitir que los AWS servicios que están integrados usen la clave de KMS en su nombre para proteger los recursos, como los buckets de Amazon S3 y las tablas de Amazon DynamoDB. AWS KMS

Puede añadir usuarios de IAM, funciones de IAM y otros Cuentas de AWS a la lista de usuarios clave al crear la clave de KMS. También puede editar la lista con la vista predeterminada de la consola para las políticas de claves, tal como se muestra en la siguiente imagen. La vista predeterminada de las políticas de claves está disponible en la página de detalles de clave. Para obtener más información sobre cómo permitir que los usuarios de otros países Cuentas de AWS usen la clave de KMS, consulte. Permitir a los usuarios de otras cuentas utilizar una clave KMS

> **Note**
>
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan

credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.



Las declaraciones de usuarios de claves predeterminadas para una clave simétrica de región única permite los siguientes permisos. Para obtener información detallada sobre cada permiso, consulte la AWS KMS permisos.

Cuando utiliza la AWS KMS consola para crear una clave KMS, la consola agrega los usuarios y roles que especifique al `Principal` elemento de la declaración de cada usuario clave.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:role/ExampleRole",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:Encrypt",
```

```
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": [
    "arn:aws:iam::111122223333:role/ExampleRole",
    "arn:aws:iam::444455556666:root"
  ]},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

Permite a los usuarios de claves utilizar una clave KMS para las operaciones criptográficas

Los usuarios de claves tienen permiso para usar la clave KMS directamente en todas las operaciones criptográficas admitidas en la clave KMS. También pueden usar la DescribeKeyoperación para obtener información detallada sobre la clave de KMS en la AWS KMS consola o mediante las operaciones de la AWS KMS API.

De forma predeterminada, la AWS KMS consola agrega las declaraciones de los usuarios clave, como las de los ejemplos siguientes, a la política de claves predeterminada. Debido a que son compatibles con diferentes operaciones de la API, las acciones en las declaraciones de la política para las claves KMS de cifrado simétricas, claves KMS HMAC, claves KMS asimétricas para el cifrado de claves público y las claves KMS asimétricas para la firma y la verificación son ligeramente diferentes.

Claves KMS de cifrado simétricas

La consola agrega la siguiente declaración a la política de claves para claves KMS de cifrado simétricas.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:Encrypt",
    "kms:GenerateDataKey*",
    "kms:ReEncrypt*"
  ],
  "Resource": "*"
}
```

Claves KMS HMAC

La consola agrega la siguiente declaración a la política de claves para claves KMS HMAC.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateMac",
    "kms:VerifyMac"
  ],
  "Resource": "*"
}
```

Claves KMS asimétricas para el cifrado de claves públicas

La consola agrega la siguiente declaración a la política de claves para claves KMS asimétricas con un uso de claves de Encrypt and decrypt (Cifrar y descifrar).

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"
  },
  "Action": [
```

```
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:DescribeKey",
    "kms:GetPublicKey"
  ],
  "Resource": "*"
}
```

Claves KMS asimétricas para la firma y la verificación

La consola agrega la siguiente declaración a la política de claves para claves KMS asimétricas con un uso de claves de Sign and verify (Firmar y verificar).

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:DescribeKey",
    "kms:GetPublicKey",
    "kms:Sign",
    "kms:Verify"
  ],
  "Resource": "*"
}
```

Las acciones de estas declaraciones proporcionan a los usuarios de clave los siguientes permisos.

`kms:Encrypt`

Permite a los usuarios de claves cifrar datos con esta clave KMS.

`kms:Decrypt`

Permite a los usuarios de claves descifrar los datos con esta clave KMS.

`kms:DescribeKey`

Permite a los usuarios de claves recuperar información sobre esta clave KMS, incluidos sus identificadores, fecha de creación, estado y mucho más. También permite a los usuarios clave mostrar detalles sobre la clave KMS en la AWS KMS consola.

`kms:GenerateDataKey*`

Permite a los usuarios de claves solicitar una clave de datos simétrica o un par de claves de datos asimétricos para operaciones criptográficas del cliente. La consola utiliza el carácter comodín * para representar el permiso para las siguientes operaciones de API: GenerateDataKey, GenerateDataKeyWithoutPlaintextGenerateDataKeyPair, y GenerateDataKeyPairWithoutPlaintext. Estos permisos solo son válidos en las claves KMS simétricas que cifran las claves de datos.

kms: GenerateMac

Permite a los usuarios de claves utilizar una clave KMS HMAC para generar una etiqueta HMAC.

km: GetPublicKey

Permite a los usuarios de claves descargar la clave pública de la clave KMS asimétrica. Las partes con las que compartes esta clave pública pueden cifrar los datos fuera de AWS KMS. Sin embargo, esos textos cifrados solo se pueden descifrar llamando a la operación Descifrar en AWS KMS.

km: * ReEncrypt

Permite a los usuarios de claves volver a cifrar los datos que se habían cifrado originalmente con esta clave KMS, o utilizar esta clave KMS para volver a cifrar los datos cifrados anteriormente. La ReEncryptoperación requiere acceso a las claves KMS de origen y destino. Para lograr esto, puede habilitar el permiso `kms:ReEncryptFrom` en la clave KMS fuente y el permiso `kms:ReEncryptTo` en la clave KMS de destino. Sin embargo, para simplificar, la consola permite `kms:ReEncrypt*` (con el carácter comodín `*`) en ambas claves KMS.

kms:Sign

Permite a los usuarios de claves firmar mensajes con esta clave KMS.

kms:Verify

Permite a los usuarios de claves verificar las firmas con esta clave KMS.

kms: VerifyMac

Permite a los usuarios de claves utilizar una clave KMS HMAC para verificar una etiqueta HMAC.

Permite a los usuarios de claves utilizar la clave KMS con los servicios de AWS

La política de claves predeterminada de la consola también proporciona a los usuarios clave los permisos de concesión que necesitan para proteger sus datos en AWS los servicios que utilizan concesiones. AWS los servicios suelen utilizar las concesiones para obtener un permiso específico y limitado para usar una clave de KMS.

Esta declaración de política clave permite al usuario clave crear, ver y revocar concesiones en la clave de KMS, pero solo cuando la solicitud de operación de concesión proviene de un AWS servicio integrado en ella. AWS KMS La condición de GrantIsFor AWSResource política kms: no permite al usuario llamar directamente a estas operaciones de concesión. Cuando el usuario clave lo permite, un AWS servicio puede crear una concesión en nombre del usuario que permita al servicio utilizar la clave KMS para proteger los datos del usuario.

Los usuarios de claves requieren estos permisos de concesiones para utilizar la clave KMS con los servicios integrados, pero estos permisos no son suficientes. Los usuarios de claves también necesitan permiso para utilizar los servicios integrados. Para obtener más información sobre cómo dar a los usuarios acceso a un AWS servicio que se integra con él AWS KMS, consulte la documentación del servicio integrado.

```
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
}
```

Por ejemplo, los usuarios de claves pueden utilizar estos permisos en la clave KMS de las siguientes maneras.

- Utilice esta clave KMS con Amazon Elastic Block Store (Amazon EBS) y Amazon Elastic Compute Cloud (Amazon EC2) para adjuntar un volumen de EBS cifrado a una instancia EC2. El usuario de claves concede implícitamente a Amazon EC2 permiso para utilizar la clave KMS con el fin de

asociar el volumen cifrado a la instancia. Para obtener más información, consulte ¿Cómo Amazon Elastic Block Store (Amazon EBS) utiliza AWS KMS?.

- Utilice esta clave KMS con Amazon Redshift para lanzar un clúster cifrado. El usuario de claves concede implícitamente a Amazon Redshift permiso para utilizar la clave KMS con el fin de lanzar el clúster cifrado y crear instantáneas cifradas. Para obtener más información, consulte ¿Cómo Amazon Redshift utiliza AWS KMS?.
- Utilice esta clave KMS con otros servicios de AWS integrados con AWS KMS, que utilizan concesiones, para crear, administrar o usar recursos cifrados con esos servicios.

La política de claves predeterminada permite a los usuarios de claves delegar su permiso de concesión a todos los servicios integrados que utilizan concesiones. Sin embargo, puede crear una política de claves personalizada que restrinja el permiso a AWS servicios específicos. Para obtener más información, consulte la clave de condición kms: ViaService.

Consultar una política de claves

Puedes ver la política de claves de una clave gestionada por el AWS KMS cliente o de una Clave administrada de AWSde tu cuenta mediante la GetKeyPolicyoperación AWS Management Console o de la AWS KMS API. No puede utilizar estas técnicas para ver la política de claves de una clave KMS en una cuenta de Cuenta de AWS distinta.

Para obtener más información sobre las políticas de claves de AWS KMS, consulte Políticas clave en AWS KMS. Para obtener información acerca de cómo determinar qué usuarios y roles tienen acceso a un clave KMS, consulte the section called “Determinar el acceso”.

Temas

- Consultar una política de claves (consola)
- Consultar una política de claves (API de AWS KMS)

Consultar una política de claves (consola)

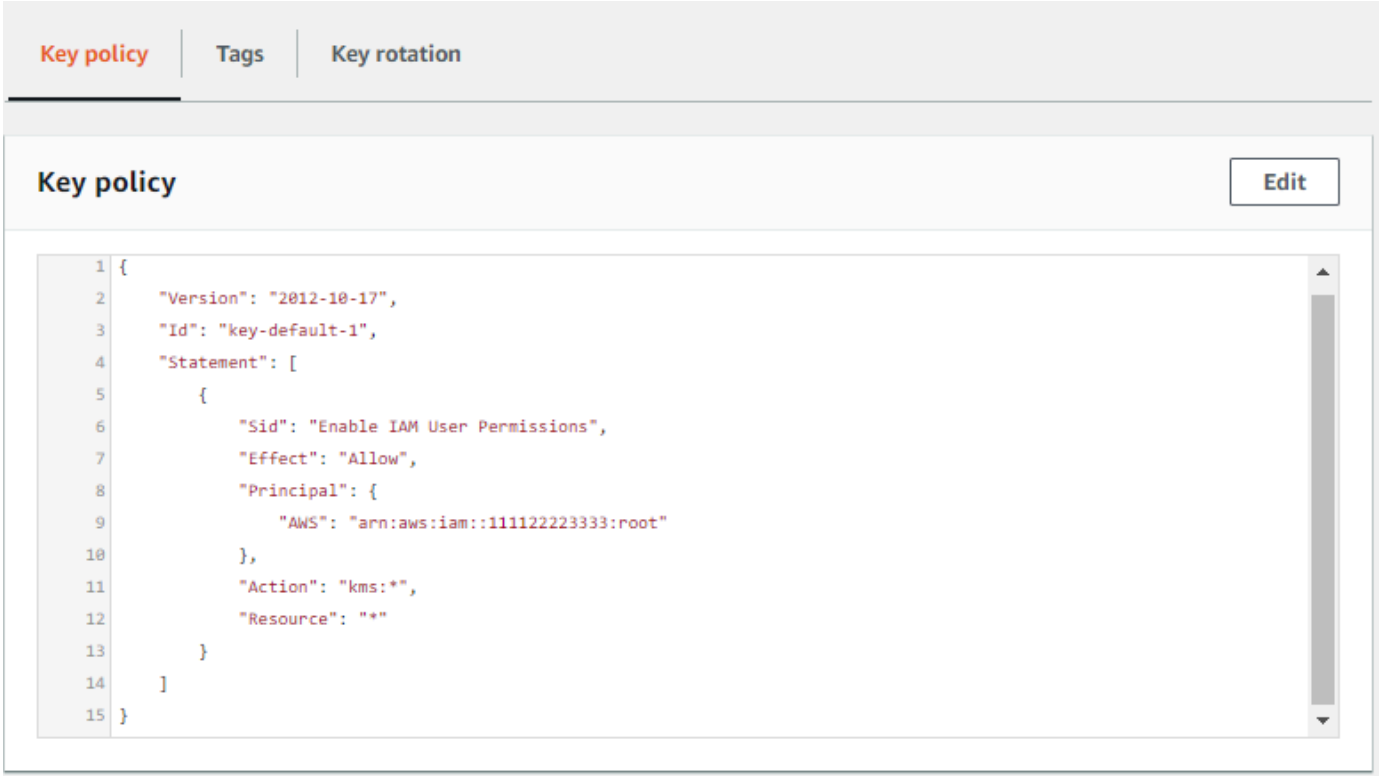
Los usuarios autorizados pueden ver la política de claves para una Clave administrada de AWS o una clave administrada por el cliente en la pestaña Key policy (Política de claves) de la AWS Management Console.

Para ver la política clave de una clave de KMS enAWS Management Console, debes tener los GetKeyPolicy permisos kms: DescribeKey, kms: y kms:. ListAliases

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. Si desea ver las claves de su cuenta que AWS crea y administra, en el panel de navegación, elija claves administradas por AWS. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente).
4. En la lista de claves KMS, elija el alias o ID de clave de la clave KMS que desea examinar.
5. Seleccione la pestaña Key policy (Política de claves).

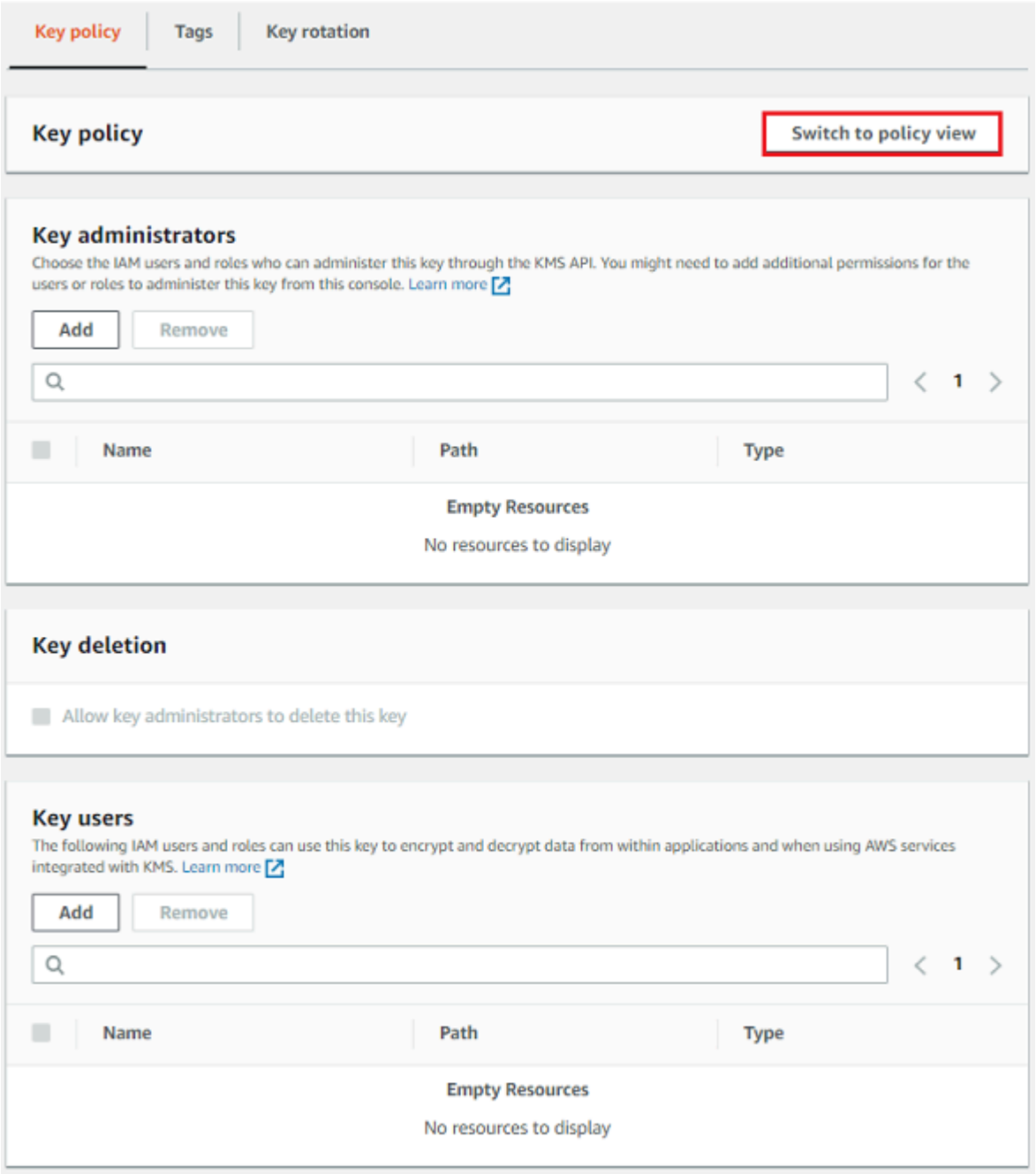
   En la pestaña Key policy (Política de claves), es posible que vea el documento de política de claves. Esta es la vista de política. En las declaraciones de políticas de claves, puede ver las entidades principales a las que la política de claves ha dado acceso a la clave KMS y las acciones que pueden realizar.

   En el ejemplo siguiente se muestra la vista de política de la política de claves predeterminada.



O bien, si ha creado la clave KMS en la AWS Management Console, verá la vista predeterminada con secciones para Key administrators (Administradores de claves), Key deletion (Eliminación de claves) y Key Users (Usuarios de claves). Para ver el documento de políticas de claves, elija Switch to policy view (Cambiar a la vista de política).

En el ejemplo siguiente se muestra la vista predeterminada de la política de claves predeterminada.



Consultar una política de claves (API de AWS KMS)

Para obtener la política clave de una clave de KMS para Cuenta de AWS ti, usa la GetKeyPolicyoperación de la AWS KMS API. No puede utilizar esta operación para ver una política de claves en una cuenta distinta.

En el siguiente ejemplo, se usa el get-key-policycomando de AWS Command Line Interface (AWS CLI), pero puedes usar cualquier AWS SDK para realizar esta solicitud.

Tenga en cuenta que el parámetro `PolicyName` es obligatorio aunque `default` sea su único valor válido. Además, este comando solicita la salida en texto, en lugar de en JSON, para que sea más fácil de ver.

Antes de ejecutar este comando, reemplace el ID de clave de ejemplo por uno válido de su cuenta.

```
$ aws kms get-key-policy --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --policy-name
 default --output text
```

La respuesta debe ser similar a la siguiente, que devuelve la política de claves predeterminada.

```
{
  "Version" : "2012-10-17",
  "Id" : "key-consolepolicy-3",
  "Statement" : [ {
    "Sid" : "Enable IAM User Permissions",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

Cambiar una política de claves

Puede cambiar la política de claves de una clave de KMS suya Cuenta de AWS mediante la PutKeyPolicyoperación AWS Management Console o. No puede utilizar estas técnicas para cambiar la política de claves de una clave KMS en una cuenta de Cuenta de AWS distinta.

Cuando cambie una política de claves, tenga en cuenta las siguientes reglas:

- Puede ver la política de claves para una Clave administrada de AWS o una clave administrada por el cliente, pero solo puede cambiar la política de claves para una clave KMS administrada por el cliente. Las políticas de Claves administradas por AWS se crean y administran mediante el servicio de AWS que creó la clave KMS en su cuenta. No puede ver ni modificar la política de claves de una Clave propiedad de AWS.
- Puede agregar o eliminar usuarios de IAM, roles de IAM y Cuentas de AWS en la política de claves y cambiar las acciones que se permiten o deniegan para dichas entidades principales. Para obtener más información sobre las formas de especificar entidades principales y permisos en una política de claves, consulte Políticas de claves.
- No puede agregar grupos de IAM a una política de claves, aunque puede agregar varios usuarios de IAM y roles de IAM. Para obtener más información, consulte Conceder permiso a varias entidades principales de IAM para acceder a una clave KMS.
- Si agrega Cuentas de AWS externas a una política de claves, también debe usar las políticas de IAM en las cuentas externas para conceder permisos a los usuarios, los grupos o los roles de IAM en dichas cuentas. Para obtener más información, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS.
- El documento de política de claves resultante no puede superar los 32 KB (32 768 bytes).

Temas

- Cómo cambiar una política de claves
- Conceder permiso a varias entidades principales de IAM para acceder a una clave KMS

Cómo cambiar una política de claves

Puede cambiar una política de claves de tres formas diferentes, tal como se explica en las siguientes secciones.

Temas

- Usar la vista predeterminada de la AWS Management Console
- Usar la vista de políticas de la AWS Management Console
- Mediante la API de AWS KMS

Usar la vista predeterminada de la AWS Management Console

Puede utilizar la consola para cambiar una política de claves con una interfaz gráfica denominada la vista predeterminada.

Si estos pasos no se corresponden con lo que aparece en la consola, puede significar que la consola no ha creado esta política de claves. O bien que la política de claves se ha modificado de un modo que no admite la vista predeterminada de la consola. En ese caso, siga los pasos de Usar la vista de políticas de la AWS Management Console o Mediante la API de AWS KMS.

1. Vea la política de claves para una clave administrada por el cliente tal y como se indica en Consultar una política de claves (consola). (Usted no puede cambiar la política claves de Claves administradas por AWS).
2. Decida lo que desea cambiar.

   - Para agregar o eliminar administradores de claves y para permitir o evitar que los administradores de claves eliminen la clave KMS, utilice los controles de la sección Key administrators (Administradores de claves) de la página. Los administradores de claves administran la clave KMS, incluida su activación y desactivación, estableciendo la política de claves y habilitando la rotación de claves.
   - Para agregar o eliminar usuarios de claves y para permitir o no permitir que las cuentas de Cuentas de AWS externas usen la clave KMS, utilice los controles de la sección Key users (Usuarios de claves) de la página. Los usuarios de claves pueden usar la clave KMS en operaciones criptográficas, como cifrar, descifrar, volver a cifrar y generar claves de datos.

Usar la vista de políticas de la AWS Management Console

Puede utilizar la consola para cambiar un documento de política de claves con la vista de políticas de la consola.

1. Vea la política de claves para una clave administrada por el cliente tal y como se indica en Consultar una política de claves (consola). (Usted no puede cambiar la política claves de Claves administradas por AWS).
2. En la sección Política de claves, elija Cambiar a la vista de política.
3. Edite el documento de políticas de claves y, a continuación, elija Save changes (Guardar cambios).

Mediante la API de AWS KMS

Puede utilizar la PutKeyPolicyoperación para cambiar la política de claves de una clave de KMS en suCuenta de AWS. No puede utilizar esta API en una clave KMS en una cuenta de Cuenta de AWS diferente.

1. Utilice la GetKeyPolicyoperación para obtener el documento de política clave existente y, a continuación, guárdelo en un archivo. Para obtener un código de ejemplo en varios lenguajes de programación, consulte Obtener una política de claves.
2. Abra el documento de políticas de claves en el editor de textos que prefiera, edítelo y, a continuación, guarde el archivo.
3. Utilice la PutKeyPolicyoperación para aplicar el documento de política clave actualizado a la clave de KMS. Para obtener un código de ejemplo en varios lenguajes de programación, consulte Configurar una política de claves.

Para ver un ejemplo de cómo copiar una política clave de una clave de KMS a otra, consulte el GetKeyPolicy ejemplo en la Referencia de AWS CLI comandos.

Conceder permiso a varias entidades principales de IAM para acceder a una clave KMS

Los grupos de IAM no son entidades principales válidas en una política de claves. Para permitir que varios usuarios y roles obtengan acceso a una clave KMS, realice una de las acciones siguientes:

- Utilice un rol de IAM como entidad principal en la política clave. Varios usuarios autorizados pueden asumir el rol según sea necesario. Para obtener más información, consulte la sección Roles de IAM en la Guía del usuario de IAM.

  Si bien puede incluir varios usuarios de IAM en una política clave, no se recomienda esta práctica porque requiere que actualice la política clave cada vez que cambia la lista de usuarios autorizados. Además, las mejores prácticas de IAM desaconsejan el uso de usuarios de IAM con credenciales a largo plazo. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.
- Utilice una política de IAM para conceder permisos a un grupo de IAM. Para ello, asegúrese de que la política de claves incluya la declaración que permite a las políticas de IAM permitir el acceso a la clave KMS, cree una política de IAM que permita el acceso a la clave KMS y, a continuación, adjunte dicha política a un grupo de IAM que contenga los usuarios de IAM autorizados. Con este

enfoque, no es necesario cambiar ninguna política cuando cambie la lista de usuarios autorizados. En su lugar, solo debe agregar o eliminar dichos usuarios del grupo de IAM apropiado. Para obtener más información, consulte los grupos de usuarios de IAM en la Guía del usuario de IAM

Para obtener más información sobre cómo funcionan las políticas de AWS KMS y las políticas de IAM de forma conjunta, consulte Solución de problemas de acceso a las claves.

Permisos para AWS los servicios en las políticas clave

Muchos AWS servicios se utilizan AWS KMS keys para proteger los recursos que administran. Cuando un servicio usa Claves propiedad de AWS o Claves administradas por AWS, el servicio establece y mantiene las políticas de claves para estas claves KMS.

Sin embargo, cuando usa una clave administrada personalizada con un servicio de AWS , establece y mantiene la política de claves. Esta política de claves debe permitir al servicio los permisos mínimos que necesita para proteger el recurso en su nombre. Le recomendamos que siga el principio de privilegio mínimo: otorgar al servicio solo los permisos que requiere. Puede hacerlo de manera eficaz aprendiendo qué permisos necesita el servicio y utilizando claves de condición globales de AWS y claves de condición de AWS KMS para refinar los permisos.

Para encontrar los permisos que requiere el servicio en una clave administrada por el cliente, consulte la documentación de cifrado del servicio. Por ejemplo, para obtener información sobre los permisos que requiere Amazon Elastic Block Store (Amazon EBS), consulte Permisos para los usuarios de IAM en la Guía del usuario de Amazon EC2 para instancias de Linux y la Guía del usuario de Amazon EC2 para instancias de Windows. Para obtener los permisos que requiere Secrets Manager, consulte Autorización del uso de la clave KMS en la Guía del usuario de AWS Secrets Manager .

Implementación de permisos de privilegio mínimo

Cuando concedas permiso a un AWS servicio para usar una clave de KMS, asegúrate de que el permiso sea válido solo para los recursos a los que el servicio debe acceder en tu nombre. Esta estrategia de privilegios mínimos ayuda a evitar el uso no autorizado de una clave KMS cuando las solicitudes se transfieren entre AWS servicios.

Para implementar una estrategia de privilegios mínimos, se recomienda utilizar las claves de condición del contexto de AWS KMS cifrado y las claves de condición del ARN de origen global o de la cuenta de origen.

Uso de claves de condición de contexto de cifrado

La forma más eficaz de implementar los permisos con privilegios mínimos cuando se utilizan AWS KMS recursos es incluir las claves kms:EncryptionContext:context-keyo kms:EncryptionContextKeyscondicionales en la política que permite a los directores realizar operaciones AWS KMS criptográficas. Estas claves de condición son especialmente eficaces porque asocian el permiso al contexto de cifrado que está enlazado al texto cifrado cuando el recurso está cifrado.

Utilice las claves de condiciones del contexto de cifrado únicamente cuando la acción de la declaración de política CreateGrantsea una operación criptográfica AWS KMS simétrica que utilice un `EncryptionContext` parámetro, como operaciones como Decrypt. GenerateDataKey (Para ver una lista de las operaciones admitidas, consulte kms:EncryptionContext:context-key o kms:EncryptionContextKeys). Si utiliza estas claves de condición para permitir otras operaciones, por ejemplo DescribeKey, se denegará el permiso.

Establezca el valor en el contexto de cifrado que utiliza el servicio cuando cifra el recurso. Esta información generalmente suele estar disponible en el capítulo Seguridad de la documentación del servicio. Por ejemplo, el contexto de cifrado de AWS Proton identifica el recurso AWS Proton y su plantilla asociada. El contexto de cifrado AWS Secrets Manager identifica el secreto y su versión. El contexto de cifrado para Amazon Location identifica el rastreador o la recopilación.

El siguiente ejemplo de declaración de política de claves permite a Amazon Location Service crear concesiones en nombre de usuarios autorizados. Esta declaración de política limita el permiso mediante el uso de las claves kms: ViaService, kms: CallerAccount y `kms:EncryptionContext:`*`context-key`* condition para vincular el permiso a un recurso de rastreo concreto.

```
{
  "Sid": "Allow Amazon Location to create grants on behalf of authorized users",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/LocationTeam"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "geo.us-west-2.amazonaws.com",
      "kms:CallerAccount": "111122223333",
```

```
      "kms:EncryptionContext:aws:geo:arn": "arn:aws:geo:us-west-2:111122223333:tracker/
SAMPLE-Tracker"
    }
  }
}
```

Uso de claves de condición **`aws:SourceArn`** o **`aws:SourceAccount`**

Cuando la entidad principal de una declaración de política de claves es una entidad principal del servicio de AWS, recomendamos encarecidamente que utilice las claves de condición globales aws:SourceArn o aws:SourceAccount, además de la clave de condición `kms:EncryptionContext:`*`context-key`*. El ARN y los valores de la cuenta se incluyen en el contexto de autorización solo cuando una solicitud proviene AWS KMS de otro AWS servicio. Esta combinación de condiciones implementa los permisos de privilegio mínimo y evita un potencial escenario suplente confuso. Las entidades principales de servicio no suelen utilizarse como entidades principales en una política clave, pero algunos AWS servicios, como AWS CloudTrail por ejemplo, sí lo requieren.

Para utilizar las claves de condición globales `aws:SourceArn` o `aws:SourceAccount`, establezca el valor en el nombre de recurso de Amazon (ARN) o la cuenta del recurso que se está cifrando. Por ejemplo, en una declaración de política de claves que da permiso AWS CloudTrail para cifrar una traza, establezca el valor de `aws:SourceArn` al ARN de la traza. Siempre que sea posible, utilice `aws:SourceArn`, que es más específico. Establezca el valor en el ARN o un patrón ARN con caracteres comodín. Si no conoce el ARN del recurso, utilice `aws:SourceAccount` en su lugar.

> **Note**
>
> Si el ARN de un recurso incluye caracteres que no están permitidos en una política de AWS KMS claves, no puede usar ese ARN de recurso en el valor de la clave de condición. `aws:SourceArn` En cambio, utilice la clave de condición `aws:SourceAccount`. Para obtener más información sobre las reglas del documento de política de claves, consulte Formato de la política de claves.

En el siguiente ejemplo de política de claves, la entidad principal que obtiene los permisos es la entidad principal del servicio AWS CloudTrail , `cloudtrail.amazonaws.com`. Para implementar el privilegio mínimo, esta política utiliza las claves de condición `aws:SourceArn` y `kms:EncryptionContext:`*`context-key`*. La declaración de política permite CloudTrail utilizar

la clave KMS para generar la clave de datos que se utiliza para cifrar un rastro. Las condiciones `aws:SourceArn` y `kms:EncryptionContext:context-key` se evalúan de forma independiente. Cualquier solicitud de uso de la clave KMS para la operación especificada debe cumplir ambas condiciones.

Para restringir el permiso del servicio a la traza `finance` en la cuenta de ejemplo (111122223333) y la región `us-west-2`, esta declaración de política establece la clave de condición `aws:SourceArn` del ARN de una traza concreta. La declaración de condición utiliza el ArnEqualsoperador para garantizar que cada elemento del ARN se evalúe de forma independiente al coincidir. En el ejemplo también se utiliza la clave de condición `kms:EncryptionContext:context-key` para limitar el permiso a las trazas de una cuenta y región en particular.

Antes de utilizar esta política de claves, reemplace el ID de la cuenta de ejemplo, la región y el nombre de traza por valores válidos de su cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow CloudTrail to encrypt logs",
      "Effect": "Allow",
      "Principal": {
        "Service": "cloudtrail.amazonaws.com"
      },
      "Action": "kms:GenerateDataKey",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:cloudtrail:us-west-2:111122223333:trail/finance"
          ]
        },
        "StringLike": {
          "kms:EncryptionContext:aws:cloudtrail:arn": [
            "arn:aws:cloudtrail:*:111122223333:trail/*"
          ]
        }
      }
    }
  ]
}
```

Uso de políticas de IAM con AWS KMS

Puedes usar las políticas de IAM, junto con las políticas clave, las subvenciones y las políticas de puntos finales de VPC, para controlar el acceso a AWS KMS keys tu entrada. AWS KMS

> **Note**
>
> Para utilizar una política de IAM a fin de controlar el acceso a una clave KMS, la política de claves de la clave KMS debe conceder permiso a la cuenta para utilizar políticas de IAM. En concreto, la política de claves debe incluir la declaración de política que habilita las políticas de IAM.
> En esta sección, se explica cómo utilizar las políticas de IAM para controlar el acceso a las operaciones. AWS KMS Para obtener más información sobre IAM, consulte la Guía del usuario de IAM.

Todas las claves KMS deben tener una política de claves. Las políticas de IAM son opcionales. Para utilizar una política de IAM a fin de controlar el acceso a una clave KMS, la política de claves de la clave KMS debe conceder permiso a la cuenta para utilizar políticas de IAM. En concreto, la política de claves debe incluir la declaración de política que habilita las políticas de IAM.

Las políticas de IAM pueden controlar el acceso a cualquier AWS KMS operación. A diferencia de las políticas clave, las políticas de IAM pueden controlar el acceso a varias claves de KMS y proporcionar permisos para las operaciones de varios servicios relacionados AWS . Sin embargo, las políticas de IAM son especialmente útiles para controlar el acceso a las operaciones CreateKey, por ejemplo, que no pueden controlarse mediante una política clave porque no implican ninguna clave de KMS en particular.

Si accede a AWS KMS través de un punto de enlace de Amazon Virtual Private Cloud (Amazon VPC), también puede utilizar una política de punto de enlace de VPC para limitar el acceso a sus AWS KMS recursos cuando utilice el punto de enlace. Por ejemplo, cuando utilices el punto final de la VPC, es posible que solo permitas que los principales de tu cuenta accedan Cuenta de AWS a las claves gestionadas por el cliente. Para obtener más detalles, consulte Control del acceso a un punto de conexión de VPC.

Para obtener ayuda sobre cómo escribir y dar formato a un documento de política JSON, consulte la Referencia de políticas JSON de IAM en la Guía del usuario de IAM.

Temas

Información general de políticas de IAM

Puede las políticas de IAM de las siguientes formas:

- Adjuntar una política de permisos a un rol para federación o permisos en varias cuentas: puede adjuntar una política de IAM a un rol de IAM para habilitar la identidad federada, permitir los permisos en varias cuentas o conceder permisos a las aplicaciones que se ejecutan en instancias EC2. Para obtener más información sobre los diferentes casos de uso para roles de IAM, consulte Roles de IAM en la Guía del usuario de IAM.
- Asociar una política de permisos a un usuario o grupo: puede adjuntar una política que permita a un usuario o grupo de usuarios llamar a las operaciones de AWS KMS . Sin embargo, las prácticas recomendadas de IAM recomiendan utilizar identidades con credenciales temporales, como roles de IAM, siempre que sea posible.

En el siguiente ejemplo, se muestra una política de IAM con permisos. AWS KMS Esta política permite a las identidades de IAM a las que está asociada obtener todas las claves KMS y alias.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource": "*"
  }
}
```

Al igual que todas las políticas de IAM, esta política no tiene ningún elemento `Principal`. Cuando asocia una política de IAM a una identidad de IAM, esa identidad obtiene los permisos especificados en la política.

Para ver una tabla en la que se muestran todas las acciones de la AWS KMS API y los recursos a los que se aplican, consulte laReferencia de permisos.

Prácticas recomendadas para las políticas de IAM

Asegurar el acceso a AWS KMS keys es fundamental para la seguridad de todos sus AWS recursos. Las claves KMS se utilizan para proteger muchos de los recursos más confidenciales de su propiedad Cuenta de AWS. Tómese el tiempo para diseñar las políticas de claves, políticas de IAM, concesiones y políticas de punto de enlace de la VPC que controlan el acceso a sus claves KMS.

En las declaraciones de política de IAM que controlan el acceso a las claves KMS, utilice el principio del menos privilegiado. Proporcione a las entidades principales de IAM solo los permisos que necesitan y únicamente en las claves de KMS que deben usar o administrar.

Las siguientes prácticas recomendadas se aplican a las políticas de IAM que controlan el acceso a AWS KMS las claves y los alias. Para obtener información general sobre las prácticas recomendadas de política de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Use políticas de claves

> Siempre que sea posible, proporcione permisos en las políticas de clave que afecten a una clave KMS, en lugar de en una política de IAM que se pueda aplicar a muchas claves KMS, incluidas las de otras Cuentas de AWS. Esto es especialmente importante para los permisos confidenciales, como kms: PutKeyPolicy y kms: ScheduleKeyDeletion, pero también para las operaciones criptográficas que determinan cómo se protegen los datos.

Limite el permiso CreateKey

> Conceda permiso para crear claves (kms: CreateKey) solo a los directores que lo necesiten. Las principales entidades que crean una clave KMS también establecen su política de claves, de modo que puedan concederse a sí mismos y a otros permisos para usar y administrar las claves KMS que crean. Cuando permita este permiso, considere limitarlo mediante el uso de condiciones de política. Por ejemplo, puede usar la KeySpec condición kms: para limitar el permiso a las claves KMS de cifrado simétrico.

Especifique claves KMS en una política de IAM

Como práctica recomendada, especifique la ARN de clave de cada clave KMS a la que se aplica el permiso en el elemento `Resource`de la declaración de política. Esta práctica restringe el permiso a las claves KMS que requiere la entidad principal. Por ejemplo, este elemento `Resource` muestra solo las claves KMS que la entidad principal necesita usar.

```
"Resource": [
    "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
]
```

Si no es práctico especificar las claves de KMS, utilice un `Resource` valor que Cuenta de AWS limite el acceso a las claves de KMS en una región de confianza, como. `arn:aws:kms:`*`region`*`:`*`account`*`:key/*` O limite el acceso a las claves de KMS en todas las regiones (*) de una región de confianza Cuenta de AWS, por ejemplo. `arn:aws:kms:*:`*`account`*`:key/*`

No puede utilizar un ID de clave, nombre de alias o bien ARN de alias para representar una clave KMS en el campo `Resource` de una política de IAM. Si especifica un alias ARN, la política se aplica al alias, no a la clave KMS. Para obtener información general sobre las políticas de IAM, consulte Control del acceso a alias.

Evite “Recurso”: “*” en una política de IAM

Utilice los caracteres de comodín (*) con juicio. En una política de claves, el carácter de comodín en el elemento `Resource` representa la clave KMS a la que se adjunta la política de clave. Sin embargo, en una política de IAM, un carácter comodín solo en el `Resource` elemento (`"Resource": "*"`) aplica los permisos a todas las claves de KMS en todos los casos en los Cuentas de AWS que la cuenta del principal tenga permiso de uso. Esto puede incluir las claves de KMS en otras cuentas Cuentas de AWS, así como las claves de KMS de la cuenta del principal.

Por ejemplo, para usar una clave de KMS en otra Cuenta de AWS, el principal necesita el permiso de la política de claves de la clave de KMS de la cuenta externa y de una política de IAM de su propia cuenta. Supongamos que una cuenta arbitraria le dio a su Cuenta de AWS el permiso kms:Decrypt en sus claves KMS. Si es así, una política de IAM en su cuenta que le asigne permiso `kms:Decrypt` a un rol en todas las claves KMS (`"Resource": "*"`) satisfaría la parte de IAM del requisito. Como resultado, las principales entidades que pueden asumir

ese rol ahora pueden descifrar textos cifrados utilizando la clave KMS en la cuenta que no es de confianza. Las entradas de sus operaciones aparecen en los CloudTrail registros de ambas cuentas.

En particular, evite usar `"Resource": "*"` en una declaración de política que permita las siguientes operaciones de API. Estas operaciones se pueden realizar en las claves de KMS de otras Cuentas de AWS.

- DescribeKey
- GetKeyRotationStatus
- Operaciones criptográficas (cifrar, descifrar,,,,, GenerateDataKey,, GenerateDataKeyPair, GenerateDataKeyWithoutPlaintext, GenerateDataKeyPairWithoutPlaintext, firmar GetPublicKeyReEncrypt, verificar)
- CreateGrant, ListGrants, ListRetirableGrants, RetireGrant, RevokeGrant

Cuándo usar “Recurso”: “*”

En una política de IAM, utilice un carácter comodín en el elemento `Resource` solo para los permisos que lo requieran. Solo los siguientes permisos requieren el elemento `"Resource": "*"`.

- kilómetros: CreateKey
- km: GenerateRandom
- km: ListAliases
- km: ListKeys
- Permisos para almacenes de claves personalizados, como kms: CreateCustomKeyStore y kms: ConnectCustomKeyStore.

> **Note**
>
> Los permisos para las operaciones de alias (kms: CreateAlias, kms: UpdateAlias, kms: DeleteAlias) deben adjuntarse al alias y a la clave KMS. Puede utilizar `"Resource": "*"` en una política de IAM para representar los alias y las claves KMS, o especificar los alias y las claves KMS en el elemento `Resource`. Para ver ejemplos, consulte Control del acceso a alias.

Los ejemplos de este tema proporcionan más información y orientación para diseñar políticas de IAM para claves KMS. Para obtener una guía general sobre las AWS KMS mejores prácticas, consulte las AWS Key Management Service mejores prácticas (PDF). Para ver las prácticas recomendadas de IAM para todos los AWS recursos, consulte las mejores prácticas de seguridad en IAM en la Guía del usuario de IAM.

Especificación de claves KMS en declaraciones de políticas de IAM

Puede utilizar una política de IAM para permitir que una entidad principal utilice o administre claves KMS. Las claves KMS se especifican en el elemento `Resource` de la declaración de política.

- Para especificar una clave KMS en una declaración de política de IAM, debe utilizar su ARN de clave. No puede utilizar un ID de clave, un nombre de alias ni un ARN de alias para identificar una clave KMS en una declaración de política de IAM.

  Por ejemplo: `"Resource": "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"`

  Para controlar el acceso a una clave de KMS en función de sus alias, utilice las claves de condición kms: RequestAlias o kms:. ResourceAliases Para obtener más detalles, consulte ABAC para AWS KMS.

  Utilice un ARN de alias como recurso solo en una declaración de política que controle el acceso a las operaciones de alias, como CreateAliasUpdateAlias, o. DeleteAlias Para obtener más detalles, consulte Control del acceso a alias.

- Para especificar varias claves KMS en la cuenta y la región, utilice caracteres de comodín (*) en las posiciones de ID de región o recurso del ARN de clave.

  Por ejemplo, para especificar todas las claves KMS de la región EE. UU. Oeste (Oregón) de una cuenta, utilice “`Resource": "arn:aws:kms:us-west-2:111122223333:key/*`”. Para especificar todas las claves KMS en todas las regiones de la cuenta, utilice “`Resource": "arn:aws:kms:*:111122223333:key/*`”.

- Para representar todas las claves KMS, utilice un carácter de comodín solo (`"*"`). Utilice este formato para las operaciones que no utilicen ninguna clave de KMS concreta, es decir CreateKey, GenerateRandomListAliases, y ListKeys.

Al escribir sus declaraciones de política, se trata de una práctica recomendada para especificar solo las claves KMS que la entidad principal necesita usar, en lugar de darles acceso a todas las claves KMS.

Por ejemplo, la siguiente declaración de política de IAM permite al director llamar a las operaciones DescribeKey, GenerateDataKey, Decrypt únicamente con las claves de KMS que figuran en el `Resource` elemento de la declaración de política. La especificación de claves KMS por ARN clave, que es una práctica recomendada, garantiza que los permisos estén limitados únicamente a las claves KMS especificadas.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
    ]
  }
}
```

Para aplicar el permiso a todas las claves de KMS de una entidad de confianza concreta Cuenta de AWS, puede utilizar caracteres comodín (*) en las posiciones de la región y de los ID de las claves. Por ejemplo, la siguiente declaración de política permite a la entidad principal llamar a las operaciones especificadas en cualquier clave KMS de las dos cuenta de ejemplo de confianza.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:DescribeKey",
      "kms:GenerateDataKey",
      "kms:GenerateDataKeyPair"
    ],
    "Resource": [
```

```
      "arn:aws:kms:*:111122223333:key/*",
      "arn:aws:kms:*:444455556666:key/*"
    ]
  }
}
```

También puede utilizar un carácter comodín ("*") solo en el elemento `Resource`. Debido a que permite el acceso a todas las claves KMS que la cuenta tiene permiso para usar, se recomienda principalmente para operaciones sin una clave KMS concreta y declaraciones `Deny`. También puede utilizarlo en declaraciones de política que solo permiten operaciones de solo lectura menos sensibles. Para determinar si una AWS KMS operación implica una clave de KMS determinada, busque el valor de la clave de KMS en la columna Recursos de la tabla de. the section called "Referencia de permisos"

Por ejemplo, la siguiente declaración de política utiliza un efecto `Deny` para prohibir que las principales entidades utilicen las operaciones especificadas en cualquier clave KMS. Utiliza un carácter comodín en el elemento `Resource` para representar todas las claves KMS.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [
      "kms:CreateKey",
      "kms:PutKeyPolicy",
      "kms:CreateGrant",
      "kms:ScheduleKeyDeletion"
    ],
    "Resource": "*"
  }
}
```

La siguiente declaración de política utiliza un carácter comodín solo para representar todas las claves KMS. Pero solo permite operaciones de solo lectura menos sensibles y operaciones que no se aplican a ninguna clave KMS en particular.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
```

```
      "kms:CreateKey",
      "kms:ListKeys",
      "kms:ListAliases",
      "kms:ListResourceTags"
    ],
    "Resource": "*"
  }
}
```

Permisos necesarios para usar la AWS KMS consola

Para trabajar con la AWS KMS consola, los usuarios deben tener un conjunto mínimo de permisos que les permita trabajar con AWS KMS los recursos de la que disponen Cuenta de AWS. Además de estos permisos de AWS KMS , los usuarios también deben disponer de permisos para enumerar usuarios de IAM y los roles de IAM. Si crea una política de IAM que sea más restrictiva que los permisos mínimos requeridos, la AWS KMS consola no funcionará según lo previsto para los usuarios con esa política de IAM.

Para conocer los permisos mínimos necesarios para permitir a un usuario acceso de solo lectura a la consola de AWS KMS , consulte Permita que un usuario vea las claves de KMS en la consola AWS KMS.

Para permitir que los usuarios trabajen con la AWS KMS consola para crear y administrar las claves de KMS, adjunte la política AWSKeyManagementServicePowerUseradministrada al usuario, tal y como se describe en la siguiente sección.

No es necesario que conceda permisos mínimos para la consola a los usuarios que trabajan con la API de AWS KMS a través de las SDK de AWS, AWS Command Line Interface o AWS Tools for PowerShell. Sin embargo, es necesario conceder permiso a estos usuarios para utilizar la API. Para obtener más información, consulte Referencia de permisos.

AWS política gestionada para usuarios avanzados

Puede utilizar la política administrada de `AWSKeyManagementServicePowerUser` para dar a las entidades principales de IAM en su cuenta los permisos de un usuario avanzado. Los usuarios avanzados pueden crear claves KMS, usar y administrar las claves KMS que crean y ver todas las claves KMS e identidades de IAM. Las entidades principales que tienen la política administrada `AWSKeyManagementServicePowerUser` también pueden obtener permisos de otras fuentes, incluidas las políticas de claves, otras políticas de IAM y las concesiones.

`AWSKeyManagementServicePowerUser`es una política de IAM AWS gestionada. Para obtener más información sobre las políticas AWS gestionadas, consulte las políticas AWS gestionadas en la Guía del usuario de IAM.

> **Note**
>
> Los permisos de esta política que son específicos de una clave de KMS, como `kms:TagResource` y`kms:GetKeyRotationStatus`, solo entran en vigor cuando la política clave de esa clave de KMS permite explícitamente el Cuenta de AWS uso de políticas de IAM para controlar el acceso a la clave. Para determinar si un permiso es específico para una clave KMS, consulte AWS KMS permisos y busque un valor de clave KMS en la columna Resources (Recursos).
>
> Esta política proporciona al usuario avanzado permisos sobre cualquier clave KMS con una política de claves que permita la operación. En el caso de los permisos entre cuentas, como `kms:DescribeKey` y `kms:ListGrants`, esto podría incluir las claves KMS en Cuentas de AWS no confiables. Para más detalles, consulte Prácticas recomendadas para las políticas de IAM y Permitir a los usuarios de otras cuentas utilizar una clave KMS. Para determinar si un permiso es válido en las claves KMS de otras cuentas, consulte AWS KMS permisos y busque un valor Yes (Sí) en la columna Cross-account use (Uso entre cuentas).
>
> Para que los directores puedan ver la AWS KMS consola sin errores, el director necesita la etiqueta: GetResources permission, que no está incluida en la `AWSKeyManagementServicePowerUser` política. Puede autorizar este permiso en una política de IAM independiente.

La política de IAM AWSKeyManagementServicePowerUsergestionada incluye los siguientes permisos.

- Permite a las entidades principales crear claves KMS. Dado que este proceso incluye la configuración de la política de claves, los usuarios avanzados pueden concederse a sí mismos y a otros permisos para usar y administrar las claves KMS que crean.
- Permite a las entidades principales crear y eliminar alias y etiquetas en todas las claves KMS. Si cambia una etiqueta o un alias, puede permitir o denegar el permiso para usar y administrar la clave KMS. Para obtener más detalles, consulte ABAC para AWS KMS.
- Permite a las entidades principales obtener información detallada sobre todas las claves KMS, incluyendo su ARN clave, configuración criptográfica, política de claves, alias, etiquetas y estado de rotación.

- Permite a las entidades principales enumerar usuarios, grupos y roles de IAM.
- Esta política no permite a las entidades principales utilizar o administrar claves KMS que no hayan creado. Sin embargo, pueden cambiar los alias y las etiquetas de todas las claves KMS, lo que podría permitirles o denegarles el permiso para utilizar o administrar una clave KMS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateAlias",
                "kms:CreateKey",
                "kms:DeleteAlias",
                "kms:Describe*",
                "kms:GenerateRandom",
                "kms:Get*",
                "kms:List*",
                "kms:TagResource",
                "kms:UntagResource",
                "iam:ListGroups",
                "iam:ListRoles",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplos de políticas de IAM

En esta sección, encontrará ejemplos de políticas de IAM que conceden permisos para varias acciones de AWS KMS .

> **Important**
>
> Algunos de los permisos de las siguientes políticas solo se permiten cuando la política de claves de la clave KMS también los permite. Para obtener más información, consulte Referencia de permisos.

Para obtener ayuda sobre cómo escribir y dar formato a un documento de política JSON, consulte la Referencia de políticas JSON de IAM en la Guía del usuario de IAM.

Ejemplos

- Permita que un usuario vea las claves de KMS en la consola AWS KMS
- Permitir a un usuario crear claves KMS
- Permita que un usuario cifre y descifre con cualquier clave KMS de una determinada Cuenta de AWS
- Permita que un usuario cifre y descifre con cualquier clave de KMS en una región específica Cuenta de AWS
- Permitir a un usuario cifrar y descifrar con claves KMS específicas
- Impedir a un usuario desactivar o eliminar cualquier clave KMS

Permita que un usuario vea las claves de KMS en la consola AWS KMS

La siguiente política de IAM permite a los usuarios el acceso de solo lectura a la consola. AWS KMS Los usuarios con estos permisos pueden ver todas las claves de KMS que contienen Cuenta de AWS, pero no pueden crear ni cambiar ninguna clave de KMS.

Para ver las claves de KMS en las páginas de claves administradas por el cliente Claves administradas por AWSy en las páginas de claves administradas por el clienteListAliases, los directores necesitan GetResources los permisos kms:, kms: y tag:, incluso si las claves no tienen etiquetas ni alias. ListKeys Los permisos restantes, especialmente kms: DescribeKey, son necesarios para ver las columnas y los datos opcionales de la tabla de claves de KMS en las páginas de detalles clave de KMS. Los ListRoles permisos iam: ListUsers e iam: son necesarios para mostrar la política clave en la vista predeterminada sin errores. Para ver los datos de la página de almacenes de claves personalizados y los detalles sobre las claves de KMS en los almacenes de claves personalizados, los directores también necesitan el permiso kms:. DescribeCustomKeyStores

Si limita el acceso de la consola de un usuario a determinadas claves KMS, la consola muestra un error para cada clave KMS que no está visible.

Esta política incluye dos declaraciones de política. El elemento `Resource` en la primera declaración de política permite los permisos especificados en todas las claves KMS en todas las regiones del ejemplo Cuenta de AWS. Los lectores de la consola no necesitan acceso adicional porque la consola AWS KMS muestra solo las claves KMS en la cuenta de la entidad principal. Esto es cierto incluso si tienen permiso para ver las claves de KMS en otros Cuentas de AWS. El resto de los permisos AWS

KMS y los de IAM requieren un `"Resource": "*"` elemento porque no se aplican a ninguna clave de KMS concreta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnlyAccessForAllKMSKeysInAccount",
      "Effect": "Allow",
      "Action": [
        "kms:GetPublicKey",
        "kms:GetKeyRotationStatus",
        "kms:GetKeyPolicy",
        "kms:DescribeKey",
        "kms:ListKeyPolicies",
        "kms:ListResourceTags",
        "tag:GetResources"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "ReadOnlyAccessForOperationsWithNoKMSKey",
      "Effect": "Allow",
      "Action": [
        "kms:ListKeys",
        "kms:ListAliases",
        "iam:ListRoles",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

Permitir a un usuario crear claves KMS

La siguiente política de IAM permite a un usuario crear todos los tipos de claves KMS. El valor del `Resource` elemento se `*` debe a que la `CreateKey` operación no utiliza ningún AWS KMS recurso concreto (claves o alias de KMS).

Para restringir al usuario a determinados tipos de claves de KMS, utilice las claves de KeyOrigin condición kms: KeyUsage, kms: y kms:. KeySpec

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "kms:CreateKey",
    "Resource": "*"
  }
}
```

Es posible que las principales entidades que crean claves necesiten algunos permisos relacionados.

- kms: PutKeyPolicy — Los directores que tengan `kms:CreateKey` permiso pueden establecer la política de claves inicial para la clave de KMS. Sin embargo, la `CreateKey` persona que llama debe tener el PutKeyPolicy permiso kms:, que le permite cambiar la política de claves de KMS, o debe especificar el `BypassPolicyLockoutSafetyCheck` parámetro de`CreateKey`, lo cual no es recomendable. La persona que llama `CreateKey` puede obtener permiso `kms:PutKeyPolicy` para la clave KMS desde una política de IAM o pueden incluir este permiso en la política de claves de la clave KMS que están creando.
- kms: TagResource — Para añadir etiquetas a la clave KMS durante la `CreateKey` operación, la persona que `CreateKey` llama debe tener el TagResource permiso kms: en una política de IAM. Incluir este permiso en la política de claves de la nueva clave KMS no es suficiente. Sin embargo, si la persona que llama a `CreateKey` incluye `kms:TagResource` en la política de clave inicial, pueden agregar etiquetas en una llamada separada después de crear la clave KMS.
- kms: CreateAlias — Los responsables que creen una clave KMS en la AWS KMS consola deben tener el CreateAlias permiso kms: en la clave KMS y en el alias. (La consola realiza dos llamadas; una a `CreateKey` y una a `CreateAlias`). Debe proporcionar el permiso de alias en una política de IAM. Puede proporcionar estos permisos en una política de claves, una política de IAM o una concesión. Para obtener más detalles, consulte Control del acceso a alias.

Además`kms:CreateKey`, la siguiente política de IAM otorga `kms:TagResource` permisos a todas las claves de KMS de la cuenta Cuenta de AWS y `kms:CreateAlias` a todos los alias de la cuenta. También incluye algunos permisos de solo lectura útiles que únicamente se pueden proporcionar en una política de IAM.

Esta política de IAM no incluye permiso `kms:PutKeyPolicy` ni ningún otro permiso que se pueda establecer en una política de clave. Es una práctica recomendada para establecer estos permisos en la política de claves donde se aplican exclusivamente a una clave KMS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPermissionsForParticularKMSKeys",
      "Effect": "Allow",
      "Action": "kms:TagResource",
      "Resource": "arn:aws:kms:*:111122223333:key/*"
    },
    {
      "Sid": "IAMPermissionsForParticularAliases",
      "Effect": "Allow",
      "Action": "kms:CreateAlias",
      "Resource": "arn:aws:kms:*:111122223333:alias/*"
    },
    {
      "Sid": "IAMPermissionsForAllKMSKeys",
      "Effect": "Allow",
      "Action": [
        "kms:CreateKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    }
  ]
}
```

Permita que un usuario cifre y descifre con cualquier clave KMS de una determinada Cuenta de AWS

La siguiente política de IAM permite a los usuarios cifrar y descifrar datos con cualquier clave de KMS en 111122223333. Cuenta de AWS

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
```

```
    "Resource": "arn:aws:kms:*:111122223333:key/*"
  }
}
```

Permita que un usuario cifre y descifre con cualquier clave de KMS en una región específica Cuenta de AWS

La siguiente política de IAM permite a los usuarios cifrar y descifrar datos con cualquier clave KMS Cuenta de AWS 111122223333 en la región EE.UU. Oeste (Oregón).

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/*"
    ]
  }
}
```

Permitir a un usuario cifrar y descifrar con claves KMS específicas

La siguiente política de IAM permite a un usuario cifrar y descifrar datos con las dos claves KMS especificadas en el elemento `Resource`. Al especificar una clave KMS en una declaración de política de IAM, debe utilizar la ARN de clave de la clave KMS.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321"
    ]
```

```
  }
}
```

Impedir a un usuario desactivar o eliminar cualquier clave KMS

La siguiente política de IAM impide que un usuario deshabilite o elimine cualquier clave KMS, aunque otra política de IAM o política de claves conceda estos permisos. Una política que deniega de forma explícita los permisos anula todas las demás políticas, incluso aquellas que hayan permitido explícitamente los mismos permisos. Para obtener más información, consulte Solución de problemas de acceso a las claves.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [
      "kms:DisableKey",
      "kms:ScheduleKeyDeletion"
    ],
    "Resource": "*"
  }
}
```

Concesiones en AWS KMS

Una concesión es un instrumento de política que permite que las principales entidades de AWS usen claves KMS en operaciones criptográficas. También puede permitirles ver una clave KMS (`DescribeKey`) y crear y administrar concesiones. Al autorizar el acceso a una clave KMS, se consideran concesiones junto con políticas de claves y políticas de IAM. Las concesiones se utilizan a menudo para permisos temporales, ya que puede crear uno, utilizar sus permisos y eliminarlo sin cambiar las políticas de claves o las políticas de IAM.

Las concesiones son comúnmente utilizadas por los servicios de AWS que se integran con AWS KMS para cifrar sus datos en reposo. El servicio crea una concesión en nombre de un usuario de la cuenta, utiliza sus permisos y retira la concesión tan pronto como finalice su tarea. Para obtener más detalles sobre los servicios de AWS, consulte Cómo los servicios de AWS usan AWS KMS o el tema Cifrado en reposo en la Guía del usuario o en la Guía para desarrolladores del servicio.

En Trabajar con concesiones puede consultar ejemplos de código que muestran cómo funcionan las concesiones en varios lenguajes de programación.

Temas

Acerca de las concesiones

Las concesiones son un mecanismo de control de acceso muy flexible y útil. Al crear una concesión para una clave de KMS, la concesión permite a las entidades principales beneficiarias llamar a las operaciones de concesión especificadas en la clave de KMS siempre que se cumplan todas las condiciones especificadas en la concesión.

- Cada concesión permite el acceso a exactamente una clave KMS. Puede crear una concesión para una clave KMS en una Cuenta de AWS diferente.
- Una concesión puede permitir el acceso a una clave KMS, pero no denegar el acceso.
- Cada concesión tiene una entidad principal beneficiaria. La entidad principal beneficiaria puede representar una o más identidades en la misma Cuenta de AWS que la clave de KMS o en una cuenta diferente.
- Una concesión solo puede permitir operaciones de concesión. Las operaciones de concesión deben estar respaldadas por la clave KMS de la concesión. Si especificas una operación no admitida, la CreateGrantsolicitud fallará con una `ValidationError` excepción.
- La entidad principal beneficiaria puede utilizar los permisos que la concesión le otorga sin especificar la concesión, tal como lo haría si los permisos procedieran de una política de clave o de una política de IAM. Sin embargo, dado que la API de AWS KMS sigue un modelo de coherencia final, al crear, retirar o revocar una concesión, es posible que haya un breve retraso antes de que el cambio esté disponible a través de AWS KMS. Para utilizar los permisos de una concesión inmediatamente, use un token de concesión.
- Un beneficiario principal autorizado puede eliminar la concesión (retirarla o revocarla). Al eliminar una concesión se eliminan todos los permisos permitidos por la concesión. No es necesario averiguar qué políticas se deben agregar o quitar para deshacer la concesión.
- AWS KMS limita el número de concesiones en cada clave KMS. Para obtener más detalles, consulte Concesiones por clave KMS: 50 000.

Tenga cuidado al crear concesiones y al dar permiso a otros para crear concesiones. El permiso para crear subvenciones tiene implicaciones de seguridad, al igual que permitir el PutKeyPolicy permiso kms: para establecer políticas.

- Los usuarios con permiso para crear concesiones para una clave KMS (`kms:CreateGrant`) puede usar una concesión para permitir a los usuarios y roles, incluyendo los servicios de AWS, para utilizar la clave KMS. Los principales beneficiarios pueden ser identidades en su propia Cuenta de AWS o identidades en una cuenta u organización diferente.
- Las concesiones solo pueden permitir un subconjunto de operaciones de AWS KMS. Puede utilizar concesiones para permitir a los principales beneficiarios ver la clave KMS, utilizarla en operaciones criptográficas y crear y retirar concesiones. Para obtener más información, consulte Operaciones de concesión. También puede utilizar restricciones de la concesión para limitar los permisos de una concesión para una clave de cifrado simétrica.
- Las entidades principales pueden obtener permiso para crear concesiones a partir de una política de claves o de una política de IAM. Las entidades principales que reciben el permiso `kms:CreateGrant` de una política puede crear concesiones para cualquier operación de concesión en la clave KMS. Estas entidades principales no necesitan tener el permiso que conceden en la clave. Cuando se permite permiso `kms:CreateGrant` en una política, puede usar condiciones de política para limitar este permiso.
- Los principales beneficiarios también pueden obtener permiso para crear concesiones a partir de una concesión. Estas principales entidades solo pueden delegar los permisos que se les concedieron, incluso si tienen otros permisos de una política. Para obtener más detalles, consulte Concesión del permiso CreateGrant .

Para obtener ayuda con los conceptos relacionados con las concesiones, consulte Terminología de la concesión.

Conceptos de concesión

Para utilizar las concesiones de manera efectiva, deberá comprender los términos y conceptos que AWS KMS utiliza.

Restricción de concesiones

> Condición que limita los permisos de la concesión. En la actualidad, AWS KMS admite restricciones de concesión basadas en el contexto de cifrado en la solicitud de una operación criptográfica. Para obtener más detalles, consulte Uso de restricciones de concesiones.

ID de concesión

El identificador único de una concesión de una clave KMS. Puedes usar un identificador de concesión, junto con un identificador clave, para identificar una concesión en una RevokeGrantsolicitud RetireGranto solicitud.

Operaciones de concesión

Las operaciones AWS KMS que puede permitir en una concesión. Si especificas otras operaciones, la CreateGrantsolicitud fallará con una `ValidationError` excepción. Estas son también las operaciones que aceptan un token de concesión. Para obtener información detallada sobre estos permisos, consulte la AWS KMS permisos.

Estas operaciones de concesión representan realmente permiso para usar la operación. Por lo tanto, para la operación `ReEncrypt`, puede especificar `ReEncryptFrom`, `ReEncryptTo` o ambos `ReEncrypt*`.

Las operaciones de concesión son:

- Operaciones criptográficas
  - Decrypt
  - Encrypt
  - GenerateDataKey
  - GenerateDataKeyPair
  - GenerateDataKeyPairWithoutPlaintext
  - GenerateDataKeyWithoutPlaintext
  - GenerateMac
  - ReEncryptFrom
  - ReEncryptTo
  - Sign
  - Verificar
  - VerifyMac
- Otras operaciones
  - CreateGrant
  - DescribeKey
  - GetPublicKey

- RetireGrant

Las operaciones de concesión que usted permita deben ser compatibles con la clave KMS de la concesión. Si especificas una operación no admitida, la CreateGrantsolicitud fallará con una `ValidationError` excepción. Por ejemplo, las concesiones para claves KMS de cifrado simétricas no pueden permitir las operaciones Sign (Firmar), Verify (Verificar), `GenerateMac` o `VerifyMac`. Las concesiones para claves CMK asimétricas no pueden permitir operaciones que generen claves de datos o pares de claves de datos.

Token de concesión

La API de AWS KMS sigue un modelo de coherencia final. Al crear una concesión, es posible que haya un breve retraso antes de que el cambio esté disponible a través de AWS KMS. Por lo general, el cambio tarda menos de unos segundos en propagarse por todo el sistema, pero en algunos casos puede tardar varios minutos. Si intenta utilizar una concesión antes de que se propague por completo por el sistema, es posible que obtenga un error de acceso denegado. Un token de concesión le permite hacer referencia a la concesión y utilizar los permisos de concesión inmediatamente.

Un token de concesión es una cadena única, no secreta, de longitud variable, codificada en base64 que representa una concesión. Puede usar el token de concesión para identificar la concesión en cualquier operación de concesión. Sin embargo, debido a que el valor del token es un resumen hash, no revela ningún detalle sobre la concesión.

Un token de concesión está diseñado para utilizarse solo hasta que la concesión se haya propagado por completo a través de AWS KMS. Después de eso, el principal beneficiario puede utilizar el permiso de la concesión sin proporcionar un token de concesión ni cualquier otra prueba de la concesión. Puede usar un token de concesión en cualquier momento, pero una vez que la concesión tenga una consistencia final, AWS KMS utiliza la concesión para determinar los permisos, no el token de concesión.

Por ejemplo, el siguiente comando llama a la GenerateDataKeyoperación. Utiliza un token de concesión para representar la concesión que da a la persona que llama (el principal beneficiario) permiso para llamar a `GenerateDataKey` en la clave KMS especificada.

```
$ aws kms generate-data-key \
        --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
        --key-spec AES_256 \
        --grant-token $token
```

También puede utilizar un token de concesión para identificar una concesión en operaciones que administran concesiones. Por ejemplo, el director que se retira puede usar un token de concesión en una llamada a la RetireGrantoperación.

```
$ aws kms retire-grant \
        --grant-token $token
```

`CreateGrant` es la única operación que devuelve un token de concesión. No puede obtener un token de concesión de ninguna otra AWS KMS operación ni del evento de CloudTrail registro de la CreateGrant operación. Las ListRetirableGrantsoperaciones ListGrantsy devuelven el ID de concesión, pero no un token de concesión.

Para obtener más detalles, consulte Uso de un token de concesión.

Principal beneficiario

Las identidades que obtienen los permisos especificados en la concesión. Cada concesión tiene una entidad principal beneficiaria, pero la entidad principal beneficiaria puede representar varias identidades.

El principal del beneficiario puede ser cualquier entidad principal de AWS, incluida una Cuenta de AWS (raíz), un usuario de IAM, un rol de IAM, un rol o usuario federado o un usuario de rol asumido. El principal del beneficiario puede estar en la misma cuenta que la clave KMS o en una cuenta diferente. Sin embargo, el principal beneficiario no puede ser una entidad principal del servicio, un grupo de IAM o una organización de AWS.

> **Note**
>
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

Retiro (de una concesión)

Termina una concesión. Retire una concesión cuando termine de usar los permisos.

La revocación y el retiro de una concesión eliminan la concesión. Sin embargo, el retiro se realiza por medio de una entidad principal especificada en la concesión. La revocación suele

realizarla un administrador de claves. Para obtener más detalles, consulte Retiro y revocación de concesiones.

Entidad principal que se va a dar de baja

Una entidad principal que puede retirar una concesión. Puede especificar una entidad principal que se va a dar de baja en una concesión, pero no es necesario. Esta entidad principal que se va a dar de baja puede ser cualquier entidad principal de AWS, incluyendo Cuentas de AWS, usuarios de IAM, roles de IAM, usuarios federados y usuarios de rol asumido. La entidad principal que se va a dar de baja puede estar en la misma cuenta de que la clave KMS o en una cuenta diferente.

> **Note**
>
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

Además de la principal entidad que se da de baja especificada en la concesión, la Cuenta de AWS también puede retirar la concesión en la que se creó. El principal beneficiario puede retirar la concesión, si la concesión admite la operación `RetireGrant`. Además, la Cuenta de AWS o una Cuenta de AWS que sea la principal entidad que se retira puede delegar el permiso para retirar una concesión a una entidad principal de IAM en la misma Cuenta de AWS. Para obtener más detalles, consulte Retiro y revocación de concesiones.

Revocación (de una concesión)

Termina una concesión. Puede revocar una concesión para denegar activamente los permisos que permite la concesión.

La revocación y el retiro de una concesión eliminan la concesión. Sin embargo, el retiro se realiza por medio de una entidad principal especificada en la concesión. La revocación suele realizarla un administrador de claves. Para obtener más detalles, consulte Retiro y revocación de concesiones.

Consistencia final (para las concesiones)

La API de AWS KMS sigue un modelo de coherencia final. Al crear, retirar o revocar una concesión, es posible que haya un breve retraso antes de que el cambio esté disponible a través

de AWS KMS. Por lo general, el cambio tarda menos de unos segundos en propagarse por todo el sistema, pero en algunos casos puede tardar varios minutos.

Puede darse cuenta de este breve retraso si recibe errores inesperados. Por ejemplo, si intenta administrar una nueva concesión o utiliza los permisos en una nueva concesión antes de que se conozca la concesión en toda la AWS KMS, puede que obtenga un error de acceso denegado. Si retira o revoca una concesión, es posible que el principal beneficiario pueda seguir utilizando sus permisos durante un breve período hasta que la concesión se elimine por completo. La estrategia típica es volver a intentar la solicitud, y algunas AWS SDK incluyen el respaldo automático y la lógica de reintento.

AWS KMS tiene características para mitigar este breve retraso.

- Para utilizar los permisos de una nueva concesión inmediatamente, utilice un token de concesión. Puede usar un token de concesión para referirse a una concesión en cualquier operación de concesión. Para obtener instrucciones, consulte Uso de un token de concesión.
- La CreateGrantoperación tiene un `Name` parámetro que impide que las operaciones de reintento creen concesiones duplicadas.

> **Note**
>
> Los tokens de concesión reemplazan la validez de la concesión hasta que todos los puntos de conexión del servicio se hayan actualizado con el nuevo estado de concesión. En la mayoría de los casos, la consistencia final se logrará en cinco minutos.

Para obtener más información, consulte Coherencia final de AWS KMS.

Prácticas recomendadas para concesiones de AWS KMS

AWS KMS recomienda las siguientes prácticas recomendadas a la hora de crear, usar y administrar concesiones.

- Limite los permisos de la concesión a los que requiere el principal beneficiario. Utilice el principio de acceso menos privilegiado.
- Utilice un principal beneficiario específico, como un rol de IAM, y otorgue permiso al principal beneficiario para usar solo las operaciones de API que requieran.

- Use el contexto de cifrado de restricciones de concesión para asegurarse de que las personas que llaman utilizan la clave KMS para el propósito previsto. Para obtener más información sobre cómo utilizar el contexto de cifrado en una solicitud para proteger sus datos, consulte Cómo proteger la integridad de los datos cifrados mediante el uso AWS Key Management Service y EncryptionContext en el blog sobre AWS seguridad.

  > **Tip**
  >
  > Utilice la restricción de EncryptionContextEqualconcesión siempre que sea posible. La restricción de EncryptionContextSubsetconcesión es más difícil de usar correctamente. Si necesita usarlo, lea detenidamente la documentación y pruebe la limitación de concesión para asegurarse de que funciona según lo previsto.

- Suprima concesiones duplicadas. Las concesiones duplicadas tienen la misma clave ARN, acciones de API, principal beneficiario, contexto de cifrado y nombre. Si retira o revoca la concesión original pero deja los duplicados, las concesiones duplicadas sobrantes constituyen escaladas no intencionadas de privilegios. Para evitar duplicar concesiones al volver a intentar una solicitud `CreateGrant`, utilice el parámetro `Name`. Para detectar concesiones duplicadas, utilice la ListGrantsoperación. Si crea accidentalmente una concesión duplicada, retírela o revóquela lo antes posible.

  > **Note**
  >
  > Las concesiones para las claves administradas por AWS podrían parecer duplicados, pero tienen diferentes beneficiarios principales.
  > El campo `GranteePrincipal` de la respuesta `ListGrants` generalmente contiene el principal beneficiario de la concesión. Sin embargo, cuando el principal beneficiario de la concesión es un servicio de AWS, el campo `GranteePrincipal` contiene el servicio principal, que puede representar varios beneficiarios principales distintos.

- Recuerde que las concesiones no caducan automáticamente. Retire o revoque la concesiones ni bien el permiso ya no sea necesario. Las concesiones que no se eliminan pueden crear un riesgo de seguridad para los recursos cifrados.

Creación de concesiones

Antes de crear una concesión, obtenga información sobre las opciones para personalizar su concesión. Puede usar restricciones de concesión para limitar los permisos de la concesión. Además, obtenga más información sobre la concesión de permiso `CreateGrant`. Las principales entidades que obtienen permiso para crear concesiones a partir de una concesión están limitadas en las concesiones que pueden crear.

Temas

- Crear una concesión
- Uso de restricciones de concesiones
- Concesión del permiso CreateGrant

Crear una concesión

Para crear una concesión, llame a la CreateGrantoperación. Especifique una clave KMS, un beneficiario principal y una lista de operaciones de concesión permitidas. También puede designar una entidad principal que se retira. Para personalizar la concesión, utilice los parámetros opcionales `Constraints` para definir restricciones de concesión.

Al crear, retirar o revocar una concesión, es posible que haya un breve retraso, normalmente menos de cinco minutos, antes de que el cambio esté disponible a través de AWS KMS. Para obtener más información, consulte Eventual consistency (for grants).

Por ejemplo, el siguiente comando `CreateGrant` crea una concesión que permite a los usuarios que están autorizados a asumir el rol `keyUserRole` para llamar a la operación Decrypt en la clave KMS simétrica especificada. La concesión utiliza el parámetro `RetiringPrincipal` para designar una entidad principal que puede retirar la concesión. También incluye una restricción de concesión que permite el permiso únicamente cuando el contexto de cifrado de la solicitud incluye `"Department": "IT"`.

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --retiring-principal arn:aws:iam::111122223333:role/adminRole \
    --constraints EncryptionContextSubset={Department=IT}
```

Si su código vuelve a intentar la operación `CreateGrant`, o utiliza una AWSSDK que reintenta automáticamente las solicitudes, utilice el parámetro opcional Name (Nombre) para evitar la creación de concesiones duplicadas. Si AWS KMS obtiene una solicitud `CreateGrant` de una concesión con las mismas propiedades que una concesión existente, incluido el nombre, reconoce la solicitud como un reintento y no crea una nueva concesión. No puede usar el valor `Name` para identificar la concesión en cualquier operación de AWS KMS.

> **Important**
>
> No incluya información confidencial en el nombre de la concesión. Puede aparecer en texto plano en CloudTrail los registros y otros resultados.

```
$ aws kms create-grant \
    --name IT-1234abcd-keyUserRole-decrypt \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --retiring-principal arn:aws:iam::111122223333:role/adminRole \
    --constraints EncryptionContextSubset={Department=IT}
```

En Trabajar con concesiones puede consultar ejemplos de código que muestran cómo funcionan las concesiones en varios lenguajes de programación.

Uso de restricciones de concesiones

Las restricciones de concesión establecen condiciones sobre los permisos que la concesión otorga a entidad principal beneficiaria. Las restricciones de concesión sustituyen a las claves de condición en una política de claves o una política de IAM. Cada valor de restricción de concesión puede incluir hasta 8 pares de contexto de cifrado. El valor de contexto de cifrado en cada restricción de concesión no puede superar los 384 caracteres.

> **Important**
>
> No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.

AWS KMS admite dos limitaciones de concesión, `EncryptionContextEquals` y `EncryptionContextSubset`, que establecen los requisitos para el contexto de cifrado en una solicitud de una operación criptográfica.

Las restricciones de concesión de contexto de cifrado están diseñadas para ser utilizadas con operaciones de concesión que tienen un parámetro de contexto de cifrado.

- Las restricciones de contexto de cifrado solo son válidas en una concesión para una clave KMS de cifrado simétrica. Las operaciones criptográficas con otras claves KMS no son compatibles con un contexto de cifrado.
- La restricción de contexto de cifrado se omite para las operaciones `DescribeKey` y `RetireGrant`. `DescribeKey` y `RetireGrant` no tienen un parámetro de contexto de cifrado, pero puede incluir estas operaciones en una concesión que tenga una restricción de contexto de cifrado.
- Puede usar una restricción de contexto de cifrado en una concesión para la operación `CreateGrant`. La restricción de contexto de cifrado requiere que cualquier concesión creada con el permiso `CreateGrant` tenga una restricción de contexto de cifrado igualmente estricta o más estricta.

AWS KMS admite las siguientes restricciones de concesión de contexto de cifrado.

EncryptionContextEquals

Use `EncryptionContextEquals` para especificar el contexto de cifrado exacto para las solicitudes permitidas.

`EncryptionContextEquals` requiere que los pares de contexto de cifrado de la solicitud coincidan exactamente, incluido el uso de mayúsculas y minúsculas, con los pares de contexto de cifrado de la restricción de concesión. Los pares pueden aparecer en cualquier orden, pero las claves y los valores de cada par no pueden variar.

Por ejemplo, si la limitación de la concesión `EncryptionContextEquals` requiere el par de restricción de concesión `"Department": "IT"`, la concesión permite solicitudes del tipo especificado cuando el contexto de cifrado de la solicitud es exactamente `"Department": "IT"`.

EncryptionContextSubset

Use `EncryptionContextSubset` para requerir que las solicitudes incluyan pares de contexto de cifrado particulares.

`EncryptionContextSubset` requiere que la solicitud incluya todos los pares de contexto de cifrado de la restricción de concesión (una coincidencia exacta, incluido el uso de mayúsculas y minúsculas), pero la solicitud también puede tener pares de contexto de cifrado adicionales. Los pares pueden aparecer en cualquier orden, pero las claves y los valores de cada par no pueden variar.

Por ejemplo, si la limitación de la concesión `EncryptionContextSubset` requiere el par de contexto de concesión de `Department=IT`, la concesión permite solicitudes del tipo especificado cuando el contexto de cifrado de la solicitud es `"Department": "IT"`, o incluye `"Department": "IT"` junto con otros pares de contexto de cifrado, como `"Department": "IT","Purpose": "Test"`.

Para especificar una restricción de contexto de cifrado en la concesión de una clave KMS de cifrado simétrico, utilice el `Constraints` parámetro en la operación. CreateGrant La concesión que crea este comando concede a los usuarios autorizados asumir el permiso del rol `keyUserRole` para llamar a la operación Decrypt. Sin embargo, ese permiso solo es efectivo cuando el contexto de cifrado de la solicitud `Decrypt` es un par de contexto de cifrado `"Department": "IT"`.

```
$ aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --retiring-principal arn:aws:iam::111122223333:role/adminRole \
    --constraints EncryptionContextEquals={Department=IT}
```

La concesión resultante se parece a la siguiente. Tenga en cuenta que el permiso concedido al rol `keyUserRole` solo es efectivo cuando la solicitud `Decrypt` utiliza el mismo par de contexto de cifrado especificado en la restricción de concesiones. Para encontrar las concesiones de una clave KMS, utilice la ListGrantsoperación.

```
$ aws kms list-grants --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "Grants": [
        {
```

```
            "Name": "",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "GrantId":
 "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a",
            "Operations": [
                "Decrypt"
            ],
            "GranteePrincipal": "arn:aws:iam::111122223333:role/keyUserRole",
            "Constraints": {
                "EncryptionContextEquals": {
                    "Department": "IT"
                }
            },
            "CreationDate": 1568565290.0,
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "RetiringPrincipal": "arn:aws:iam::111122223333:role/adminRole"
        }
    ]
}
```

Para satisfacer la limitación de concesión `EncryptionContextEquals`, el contexto de cifrado en la solicitud para la operación `Decrypt` debe ser un par `"Department": "IT"`. Una solicitud como la siguiente del principal beneficiario satisfaría la restricción de concesiones `EncryptionContextEquals`.

```
$ aws kms decrypt \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab\
    --ciphertext-blob fileb://encrypted_msg \
    --encryption-context Department=IT
```

Cuando la restricción de concesión es `EncryptionContextSubset`, los pares de contexto de cifrado de la solicitud deben incluir los pares de contexto de cifrado de la restricción de concesión, pero la solicitud también puede incluir otros pares de contexto de cifrado. La siguiente restricción de concesión requiere que uno de los pares de contexto de cifrado en la solicitud sea `"Deparment": "IT"`.

```
"Constraints": {
   "EncryptionContextSubset": {
       "Department": "IT"
```

```
    }
}
```

La siguiente solicitud del principal beneficiario sería capaz de satisfacer tanto las restricciones de concesión `EncryptionContextEqual` y `EncryptionContextSubset` en este ejemplo.

```
$ aws kms decrypt \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --ciphertext-blob fileb://encrypted_msg \
    --encryption-context Department=IT
```

Sin embargo, una solicitud como la siguiente del principal beneficiario podría satisfacer la limitación de concesión `EncryptionContextSubset`, pero se produciría un error en la restricción de concesiones `EncryptionContextEquals`.

```
$ aws kms decrypt \
    --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --ciphertext-blob fileb://encrypted_msg \
    --encryption-context Department=IT,Purpose=Test
```

Los servicios de AWS suelen utilizar restricciones de contexto de cifrado en las concesiones que les dan permiso para utilizar claves KMS en su Cuenta de AWS. Por ejemplo, Amazon DynamoDB utiliza una concesión como la siguiente para obtener permiso para utilizar la Clave administrada de AWS para DynamoDB de su cuenta. La restricción `EncryptionContextSubset` de esta concesión hace que los permisos de la concesión solo sean efectivos cuando el contexto de cifrado de la solicitud contiene pares `"tableName": "Services"` y `"subscriberID": "111122223333"`. Esta restricción de concesión significa que la concesión permite a DynamoDB utilizar la clave KMS especificada solo en una determinada tabla de su Cuenta de AWS.

Para obtener este resultado, ejecute la ListGrantsoperación en DynamoDB de su cuenta. Clave administrada de AWS

```
$ aws kms list-grants --key-id 0987dcba-09fe-87dc-65ba-ab0987654321

{
    "Grants": [
        {
```

```
            "Operations": [
                "Decrypt",
                "Encrypt",
                "GenerateDataKey",
                "ReEncryptFrom",
                "ReEncryptTo",
                "RetireGrant",
                "DescribeKey"
            ],
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "Constraints": {
                "EncryptionContextSubset": {
                    "aws:dynamodb:tableName": "Services",
                    "aws:dynamodb:subscriberId": "111122223333"
                }
            },
            "CreationDate": 1518567315.0,
            "KeyId": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
            "GranteePrincipal": "dynamodb.us-west-2.amazonaws.com",
            "RetiringPrincipal": "dynamodb.us-west-2.amazonaws.com",
            "Name": "8276b9a6-6cf0-46f1-b2f0-7993a7f8c89a",
            "GrantId":
 "1667b97d27cf748cf05b487217dd4179526c949d14fb3903858e25193253fe59"
        }
    ]
}
```

Concesión del permiso CreateGrant

Una concesión puede incluir permiso para llamar a la operación `CreateGrant`. Pero cuando un principal beneficiario obtiene permiso para llamar a `CreateGrant` desde una concesión, en lugar de una política, ese permiso es limitado.

- El principal beneficiario solo puede crear concesiones que permitan algunas o todas las operaciones de la concesión principal.
- Las restricciones de concesión en las concesiones que crean deben ser al menos tan estrictas como las de la concesión principal.

Estas limitaciones no se aplican a las entidades principales que obtienen permito `CreateGrant` de una política, aunque sus permisos pueden estar limitados por condiciones de política.

Por ejemplo, supongamos que existe una concesión que permite a la entidad principal beneficiaria llamar a las operaciones `GenerateDataKey`, `Decrypt` y `CreateGrant`. Llamamos a una concesión que permita un permiso `CreateGrant` una concesión principal.

```
# The original grant in a ListGrants response.
{
    "Grants": [
        {
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1572216195.0,
            "GrantId":
 "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a",
            "Operations": [
                "GenerateDataKey",
                "Decrypt",
                "CreateGrant
            ]
            "RetiringPrincipal": "arn:aws:iam::111122223333:role/adminRole",
            "Name": "",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "GranteePrincipal": "arn:aws:iam::111122223333:role/keyUserRole",
            "Constraints": {
                "EncryptionContextSubset": {
                    "Department": "IT"
                }
            },
        }
    ]
}
```

La entidad principal beneficiaria, exampleUser, puede utilizar este permiso para crear una concesión que incluya cualquier subconjunto de las operaciones especificadas en la concesión principal, como `CreateGrant` y `Decrypt`. La concesión secundaria no puede incluir otras operaciones, como `ScheduleKeyDeletion` o `ReEncrypt`.

Además, las restricciones de concesión de las concesiones secundarias deben ser restrictivas o más restrictivas que las de la concesión principal. Por ejemplo, la concesión secundaria puede agregar pares a una restricción `EncryptionContextSubset` de la concesión principal, pero no puede eliminarlos. La concesión secundaria puede cambiar una restricción `EncryptionContextSubset` por una restricción `EncryptionContextEquals`, pero no al revés.

Por ejemplo, el principal beneficiario puede usar el permiso `CreateGrant` que obtuvo de la concesión principal para crear la siguiente concesión secundaria. Las operaciones del subsidio por hijos son un subconjunto de las operaciones del subsidio parental y las restricciones de la concesión son más restrictivas.

```
# The child grant in a ListGrants response.
{
    "Grants": [
        {
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1572249600.0,
            "GrantId":
 "fedcba9999c1e2e9876abcde6e9d6c9b6a1987650000abcee009abcdef40183f",
            "Operations": [
                "CreateGrant"
                "Decrypt"
            ]
            "RetiringPrincipal": "arn:aws:iam::111122223333:user/exampleUser",
            "Name": "",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "GranteePrincipal": "arn:aws:iam::111122223333:user/anotherUser",
            "Constraints": {
IAM best practices discourage the use of IAM users with long-term credentials. Whenever
                      possible, use IAM roles, which provide temporary credentials. For
 details,
                      see Security best practices in IAM in the IAM User Guide.
        "EncryptionContextEquals": {
                    "Department": "IT"
                }
            },
        }
    ]
}
```

El principal beneficiario en la concesión secundaria, `anotherUser`, puede usar su permiso `CreateGrant` para crear concesiones. Sin embargo, las concesiones que `anotherUser` crea deben incluir las operaciones en su concesión principal o en un subconjunto, y las restricciones de concesión deben ser las mismas o más estrictas.

Administración de las concesiones

Las entidades principales con los permisos necesarios pueden ver, usar y eliminar (retirar o revocar) concesiones. Para refinar los permisos para crear y administrar concesiones, AWS KMS admite varias condiciones de política que puede usar en las políticas de claves y en las políticas de IAM.

Temas

Control del acceso a las concesiones

Puede controlar el acceso a las operaciones que crean y administran concesiones en políticas de claves, políticas de IAM y concesiones. Las principales entidades que reciben el permiso `CreateGrant` de una concesión tienen permisos de concesión más limitados.

Operación de la API	Política de claves o política de IAM	Concesión
CreateGrant	✓	✓
ListGrants	✓	-
ListRetirableGrants	✓	-
Retiro de concesiones	(Limitado. Consulte Retiro y revocación de concesiones)	✓
RevokeGrant	✓	-

Al usar una política de claves o política de IAM para controlar el acceso a las operaciones que crean y administran concesiones, puede usar una o varias condiciones de política para limitar el permiso. AWS KMS admite todas las siguientes claves de condición relacionadas con las concesiones. Para obtener más detalles y ejemplos, consulte AWS KMS claves de condición.

km: GrantConstraintType

Permite a las entidades principales crear una concesión solo cuando la concesión incluye la restricción de concesiones especificada.

km: GrantIsFor AWSResource

Permite a las entidades principales llamar `CreateGrant`, `ListGrants` o `RevokeGrant` o bien solo cuando un servicio de AWS que está integrado con AWS KMS envía la solicitud en nombre del principal.

km: GrantOperations

Permite a las entidades principales crear una concesión, pero limita la concesión a las operaciones especificadas.

km: GranteePrincipal

Permite a las entidades principales crear una concesión solo para el beneficiario principal.

km: RetiringPrincipal

Permite a las entidades principales crear una concesión solo cuando la concesión especifica una entidad principal que se retira en particular.

Visualización de concesiones

Para ver la concesión, utilice la ListGrantsoperación. Debe especificar la clave KMS a la que se aplican las concesiones. También puede filtrar la lista de concesiones por ID de concesión o entidad beneficiaria principal. Para obtener más ejemplos, consulte Consultar una concesión.

Para ver todas las subvenciones de la región Cuenta de AWS y con un principal saliente en particular, utilice ListRetirableGrants. Las respuestas incluyen detalles sobre cada concesión.

> **Note**
>
> El campo `GranteePrincipal` de la respuesta `ListGrants` generalmente contiene el principal beneficiario de la concesión. Sin embargo, cuando el principal beneficiario de la concesión es un servicio de AWS, el campo `GranteePrincipal` contiene el servicio principal, que puede representar varios beneficiarios principales distintos.

Por ejemplo, el siguiente comando muestra todas las concesiones de una clave KMS.

```
$  aws kms list-grants --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "Grants": [
        {
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1572216195.0,
            "GrantId":
 "abcde1237f76e4ba7987489ac329fbfba6ad343d6f7075dbd1ef191f0120514a",
            "Constraints": {
                "EncryptionContextSubset": {
                    "Department": "IT"
                }
            },
            "RetiringPrincipal": "arn:aws:iam::111122223333:role/adminRole",
            "Name": "",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "GranteePrincipal": "arn:aws:iam::111122223333:user/exampleUser",
            "Operations": [
                "Decrypt"
            ]
        }
    ]
}
```

Uso de un token de concesión

La API de AWS KMS sigue un modelo de coherencia final. Al crear una concesión, es posible que la concesión no sea efectiva inmediatamente. Es posible que haya un breve retraso antes de que el cambio esté disponible a través de AWS KMS. Por lo general, el cambio tarda menos de unos segundos en propagarse por todo el sistema, pero en algunos casos puede tardar varios minutos. Una vez que el cambio se haya propagado totalmente a través del sistema, la entidad principal beneficiaria puede utilizar los permisos de la concesión sin especificar el token de concesión ni ninguna prueba de la concesión. Sin embargo, si una concesión es tan nueva que aún no es conocida por todas las AWS KMS, la solicitud puede fallar con un error `AccessDeniedException`.

Para utilizar los permisos de una nueva concesión inmediatamente, utilice el token de concesión para la concesión. Guarda el token de concesión que devuelve la CreateGrantoperación. A continuación, envíe el token de concesión en la solicitud para la operación AWS KMS. Puede enviar un token de concesión a cualquier operación de concesión de AWS KMS y puede enviar varios tokens de concesión en la misma solicitud.

En el siguiente ejemplo, se utiliza la `CreateGrant` operación para crear una concesión que permita las operaciones GenerateDataKeyy Decrypt. Guarda el token de concesión que `CreateGrant` devuelve en la variable `token`. Luego, en una llamada a la operación `GenerateDataKey`, utiliza el token de concesión en la variable `token`.

```
# Create a grant; save the grant token
$ token=$(aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:user/appUser \
    --retiring-principal arn:aws:iam::111122223333:user/acctAdmin \
    --operations GenerateDataKey Decrypt \
    --query GrantToken \
    --output text)

# Use the grant token in a request
$ aws kms generate-data-key \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --key-spec AES_256 \
    --grant-tokens $token
```

Las entidades principales con permiso también pueden usar un token de concesión para retirar una nueva concesión incluso antes de que la concesión esté disponible a través de AWS KMS. (La operación `RevokeGrant` no acepta un token de concesión). Para obtener más detalles, consulte Retiro y revocación de concesiones.

```
# Retire the grant
$ aws kms retire-grant --grant-token $token
```

Retiro y revocación de concesiones

Para eliminar una concesión, retírela o revoquela.

Las RevokeGrantoperaciones RetireGranty son muy similares entre sí. Ambas operaciones eliminan una concesión, lo que elimina los permisos que permite la concesión. La principal diferencia entre estas operaciones es cómo se autorizan.

RevokeGrant

Como la mayoría de las operaciones AWS KMS, el acceso a la operación `RevokeGrant` se controla a través de las políticas de claves y las políticas de IAM. Cualquier director puede

llamar a la RevokeGrantAPI con `kms:RevokeGrant` permiso. Este permiso está incluido en los permisos estándar otorgados a los administradores de claves. Normalmente, los administradores revocan una concesión para denegar los permisos que permite la concesión.

RetireGrant

La concesión determina quién puede retirarla. Este diseño le permite controlar el ciclo de vida de una concesión sin cambiar las políticas de claves o las políticas de IAM. Normalmente, usted retira una concesión cuando ha terminado de usar sus permisos.

Una entidad principal que se retira opcional especificada puede retirar una concesión. La entidad beneficiaria principal también puede retirar la concesión, pero solo si también se trata de una entidad principal que se retira o si la concesión incluye la operación `RetireGrant`. Como copia de seguridad, la Cuenta de AWS en la que se creó la concesión puede retirar la concesión.

Hay un permiso `kms:RetireGrant` que se puede utilizar en las políticas de IAM, pero tiene una utilidad limitada. Las entidades principales especificadas en la concesión pueden retirar una concesión sin el permiso `kms:RetireGrant`. El permiso `kms:RetireGrant` por sí solo no permite a las entidades principales retirar una concesión. El permiso `kms:RetireGrant` no es efectivo en una política de clave.

- Para denegar el permiso de retirar una concesión, puede usar una acción `Deny` con el permiso `kms:RetireGrant`.
- La Cuenta de AWS que posee la clave KMS puede delegar el permiso `kms:RetireGrant` a una entidad principal de IAM de la cuenta.
- Si la entidad principal que se retira es una Cuenta de AWS diferente, los administradores de la otra cuenta pueden usar `kms:RetireGrant` para delegar el permiso para retirar la concesión a una entidad principal de IAM en esa cuenta.

La API de AWS KMS sigue un modelo de coherencia final. Al crear, retirar o revocar una concesión, es posible que haya un breve retraso antes de que el cambio esté disponible a través de AWS KMS. Por lo general, el cambio tarda menos de unos segundos en propagarse por todo el sistema, pero en algunos casos puede tardar varios minutos. Si necesita eliminar una nueva concesión inmediatamente, antes de que esté disponible a través de AWS KMS, use un token de concesión para retirar la concesión. No puede usar un token de concesión para revocar una concesión.

Conectar con AWS KMS a través de un punto de conexión de VPC

Puede conectarse directamente a AWS KMS mediante un punto de conexión de interfaz privada de su nube virtual privada (VPC). Cuando utiliza un punto de conexión de VPC de interfaz, la comunicación entre su VPC y AWS KMS se realiza en su totalidad dentro de la red de AWS.

AWS KMS es compatible con puntos de conexión de Amazon Virtual Private Cloud (Amazon VPC) con tecnología de AWS PrivateLink. Cada punto de conexión de VPC está representado por una o varias Interfaces de red elásticas (ENI) con direcciones IP privadas en las subredes de la VPC.

El punto de conexión de VPC de tipo interfaz conecta directamente la VPC con AWS KMS sin necesidad de gateway de Internet, dispositivos NAT, conexiones de VPN ni conexiones de AWS Direct Connect. Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con AWS KMS.

Regiones

AWS KMS admite los puntos de conexión de VPC y las políticas de puntos de conexión de VPC en todas las Regiones de AWS en las que se admite AWS KMS.

Temas

Consideraciones para los puntos de conexión de VPC de AWS KMS

Antes de configurar un punto de conexión de VPC de interfaz para AWS KMS, revise el tema Propiedades y limitaciones de los puntos de conexión de interfaz en la Guía de AWS PrivateLink.

El soporte de AWS KMS para un punto de conexión de VPC incluye lo siguiente.

- Puede utilizar el punto de conexión de VPC para llamar a todas las operaciones de la API de AWS KMS desde su VPC.

- Puede crear un punto de conexión de VPC de interfaz que se conecte a un punto de conexión de la región de AWS KMS o a un punto de conexión FIPS de AWS KMS.
- También puede utilizar registros de AWS CloudTrail para auditar el uso de las claves de KMS a través del punto de conexión de VPC. Para obtener más detalles, consulte Registro de su punto de conexión de VPC.

Creación de un punto de conexión de VPC para AWS KMS

Puede crear un punto de conexión de VPC para AWS KMS mediante la consola de Amazon VPC o la API de Amazon VPC. Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink.

- Para crear un punto de conexión de VPC para AWS KMS, utilice el siguiente nombre de servicio:

  ```
  com.amazonaws.region.kms
  ```

  Por ejemplo, en la Región EE. UU. Oeste (Oregón) (`us-west-2`), el nombre del servicio sería:

  ```
  com.amazonaws.us-west-2.kms
  ```

- Para crear un punto de conexión de VPC que se conecte a un punto de conexión FIPS de AWS KMS, utilice el siguiente nombre de servicio:

  ```
  com.amazonaws.region.kms-fips
  ```

  Por ejemplo, en la Región EE. UU. Oeste (Oregón) (`us-west-2`), el nombre del servicio sería:

  ```
  com.amazonaws.us-west-2.kms-fips
  ```

Para facilitar el uso del punto de conexión de VPC, puede habilitar un nombre de DNS privado para el punto de conexión de VPC. Si selecciona la opción Enable DNS Name (Habilitar nombre DNS), el nombre del host de DNS de AWS KMS estándar se resuelve en el punto de conexión de VPC. Por ejemplo, `https://kms.us-west-2.amazonaws.com` se resolvería en un punto de conexión de VPC conectado al nombre del servicio `com.amazonaws.us-west-2.kms`.

Esta opción facilita el uso del punto de conexión de VPC. Además, los SDK de la AWS y AWS CLI utilizan el nombre de alojamiento DNS de AWS KMS estándar de forma predeterminada, por lo

que no es necesario especificar la URL del punto de conexión de VPC en las aplicaciones y los comandos.

Para obtener más información, consulte Acceso a un servicio a través de un punto de conexión de interfaz en la Guía de AWS PrivateLink.

Conectar con un punto de conexión de VPC de AWS KMS

Puede conectarse con AWS KMS a través del punto de conexión de VPC mediante el SDK de AWS, la AWS CLI o AWS Tools for PowerShell. Para especificar el punto de conexión de VPC, utilice su nombre de DNS.

Por ejemplo, este comando list-keys utiliza el parámetro `endpoint-url` para especificar el punto de conexión de VPC. Para utilizar un comando de este tipo, sustituya el ID del punto de conexión de VPC del ejemplo por uno de su cuenta.

```
$ aws kms list-keys --endpoint-url https://vpce-1234abcdf5678c90a-09p7654s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com
```

Si ha habilitado los nombres de host privados al crear el punto de conexión de VPC, no es necesario que especifique la URL de este en los comandos de la CLI ni en la configuración de la aplicación. El nombre del host de DNS de AWS KMS estándar se resuelve en el punto de conexión de VPC. La AWS CLI y los SDK utilizan este nombre de host de forma predeterminada, por lo que puede empezar a utilizar el punto de conexión de VPC para conectarse a un punto de conexión de AWS KMS regional sin cambiar nada en los scripts ni en las aplicaciones.

Para utilizar nombres de host privados, se deben establecer los atributos `enableDnsHostnames` y `enableDnsSupport` de la VPC en `true`. Para establecer estos atributos, utilice la ModifyVpcAttributeoperación. Para obtener más información, consulte Ver y actualizar los atributos de DNS de su VPC en la Guía del usuario de Amazon VPC.

Control del acceso a un punto de conexión de VPC

Para controlar el acceso al punto de conexión de VPC paraAWS KMS, adjunte una política de puntos de conexión de VPC a su punto de conexión de VPC. La política de punto de conexión determina si las entidades principales pueden utilizar el punto de conexión de VPC para llamar a operaciones AWS KMS en recursos de AWS KMS.

Puede crear una política de punto de conexión de VPC cuando cree el punto de conexión y puede cambiar la política de punto de conexión de VPC en cualquier momento. Utilice la consola de

administración de VPC o las operaciones CreateVpcEndpointo ModifyVpcEndpoint. También puede crear y cambiar una política de punto de conexión de VPC mediante una plantilla AWS CloudFormation. Para obtener ayuda sobre el uso de la consola de administración de la VPC, consulte Creación de un punto de conexión de interfaz y Modificación de un punto de conexión de interfaz en la Guía de AWS PrivateLink.

> **Note**
>
> AWS KMS admite políticas de puntos de conexión de VPC a partir de julio de 2020. Puntos de conexión de VPC para AWS KMS que se crearon antes de esa fecha tienen la política de puntos de conexión de VPC predeterminada, pero puede cambiarla en cualquier momento.

Para obtener ayuda sobre cómo escribir y dar formato a un documento de política JSON, consulte la Referencia de políticas JSON de IAM en la Guía del usuario de IAM.

Temas

- Uso de políticas de punto de conexión de VPC
- Política de puntos de conexión de VPC predeterminada
- Creación de una política de punto de conexión de VPC
- Visualización de una política de punto de conexión de VPC

Uso de políticas de punto de conexión de VPC

Para una solicitud AWS KMS que utiliza un punto de conexión de VPC para tener éxito, la entidad principal requiere permisos de dos orígenes:

- Una política de claves, política de IAM, o bien concesión debe dar permiso a la entidad principal para llamar a la operación en el recurso (clave KMS o alias).
- Una política de extremo de VPC debe conceder a la entidad principal permiso para utilizar el punto de conexión para realizar la solicitud.

Por ejemplo, una política de clave puede conceder permiso a una entidad principal para llamar a Descifrado en una clave KMS en particular. Sin embargo, es posible que la política de punto de conexión de VPC no permita que la entidad principal llame a `Decrypt` en esa clave KMS mediante el punto de conexión.

O bien, una política de punto final de VPC podría permitir que un principal utilice el punto final para invocar determinadas claves DisableKeyde KMS. Pero si la entidad principal no tiene esos permisos de una política de clave, política de IAM o concesión, se produce un error en la solicitud.

Política de puntos de conexión de VPC predeterminada

Cada punto de conexión de VPC tiene una política de punto de conexión de VPC, pero no es necesario que especifique la política. Si no especifica una política, la política de punto de conexión predeterminada permite todas las operaciones de todas las entidades principales en todos los recursos del punto de conexión.

Sin embargo, para los recursos de AWS KMS, la entidad principal también debe tener permiso para llamar a la operación desde una política de clave, política de IAM, o concesión. Por lo tanto, en la práctica, la política predeterminada dice que si una entidad principal tiene permiso para llamar a una operación en un recurso, también puede llamarla mediante el punto de conexión.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

Para permitir que las entidades principales utilicen el punto de conexión de VPC solo para un subconjunto de sus operaciones permitidas, cree o modifique la política de puntos de conexión de VPC.

Creación de una política de punto de conexión de VPC

Una política de punto de conexión de VPC determina si una entidad principal tiene permiso para utilizar el punto de conexión de VPC para realizar operaciones en un recurso. Para recursos de AWS KMS, la entidad principal también debe tener permiso para realizar las operaciones desde una política de clave,política de IAM, o bien concesión.

Cada declaración de política de puntos de conexión de VPC requiere los siguientes elementos:

- La entidad principal que puede realizar acciones

- Las acciones que se pueden realizar
- Los recursos en los que se pueden llevar a cabo las acciones

La declaración de política no especifica el punto de conexión de VPC. En cambio, se aplica a cualquier punto de conexión de VPC al que esté asociada dicha política. Para obtener más información, consulte Control del acceso a los servicios con puntos de conexión de VPC en la guía del usuario de Amazon VPC.

A continuación, se muestra un ejemplo de una política de un punto de conexión de VPC para AWS KMS. Cuando la política se asocia a un punto de conexión de VPC, permite a `ExampleUser` utilizar el punto de conexión de VPC para llamar a las operaciones especificadas en las claves KMS especificadas. Antes de utilizar una política como esta, sustituya la entidad principal de ejemplo y ARN de clave con valores válidos de tu cuenta.

```
{
   "Statement":[
      {
         "Sid": "AllowDecryptAndView",
         "Principal": {"AWS": "arn:aws:iam::111122223333:user/ExampleUser"},
         "Effect":"Allow",
         "Action": [
             "kms:Decrypt",
             "kms:DescribeKey",
             "kms:ListAliases",
             "kms:ListKeys"
          ],
         "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
      }
   ]
}
```

AWS CloudTrail registra todas las operaciones que utilizan el punto de conexión de VPC. Sin embargo, tus CloudTrail registros no incluyen las operaciones solicitadas por los responsables de otras cuentas ni las operaciones relacionadas con las claves de KMS de otras cuentas.

Como tal, es posible que desee crear una política de punto de conexión de VPC que impida que las entidades principales de cuentas externas utilicen el punto de conexión de VPC para llamar a cualquier operaciones de AWS KMS en cualquier clave de la cuenta local.

En el siguiente ejemplo, se usa la clave de condición PrincipalAccount global aws: para denegar el acceso a todos los principales para todas las operaciones de todas las claves de KMS, a menos que el principal esté en la cuenta local. Antes de utilizar una política como esta, sustituya el ID de la cuenta de ejemplo por uno válido.

```
{
  "Statement": [
    {
      "Sid": "AccessForASpecificAccount",
      "Principal": {"AWS": "*"},
      "Action": "kms:*",
      "Effect": "Deny",
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

Visualización de una política de punto de conexión de VPC

Para ver la política de puntos de conexión de la VPC de un punto final, utilice la consola de administración de la VPC o la operación. DescribeVpcEndpoints

Los siguientes comandos de AWS CLI obtienen la política para el punto de conexión con el ID de punto de conexión de VPC especificado.

Antes de ejecutar este comando, reemplace el ID de punto de conexión de ejemplo por uno válido de su cuenta.

```
$ aws ec2 describe-vpc-endpoints \
--query 'VpcEndpoints[?VpcEndpointId==`vpce-1234abcdf5678c90a`].[PolicyDocument]'
--output text
```

Utilizar un punto de conexión de VPC en una declaración de política

Puede controlar el acceso a recursos y operaciones de AWS KMScuando la solicitud proviene de VPC o utiliza un punto de conexión de VPC. Para ello, utilice una de las siguientes claves de condición global en una política de claves o política de IAM.

- Utilice la clave de condición `aws:sourceVpce` para conceder o restringir el acceso en función del punto de conexión de VPC.
- Utilice la clave de condición `aws:sourceVpc` para conceder o restringir el acceso en función de la VPC que aloja el punto de conexión privado.

> **Note**
>
> Actúe con precaución al crear políticas de IAM y de claves basadas en el punto de conexión de VPC. Si una declaración de política requiere que las solicitudes procedan de una VPC o un punto de conexión de VPC determinados, las solicitudes de los servicios de AWS integrados que utilicen un recurso AWS KMS en su nombre podrían producir un error. Para obtener ayuda, consulte Usar condiciones de punto de conexión de VPC en políticas con permisos de AWS KMS.
>
> Además, la clave de condición `aws:sourceIP` no es efectiva si la solicitud procede de un punto de conexión de Amazon VPC. Para restringir las solicitudes a un punto de conexión de VPC, utilice las claves de condición `aws:sourceVpce` o `aws:sourceVpc`. Para obtener más información, consulte Administración de identidades y accesos para puntos de conexión de VPC y servicios de puntos de conexión de VPC en la Guía de AWS PrivateLink.

Puede usar estas claves de condición globales para controlar el acceso a AWS KMS keys (claves KMS), a los alias y a operaciones como esas CreateKeyque no dependen de ningún recurso en particular.

Por ejemplo, la siguiente política de claves de ejemplo permite a un usuario realizar operaciones de cifrado con una clave KMS solo cuando la solicitud utiliza el punto de conexión de VPC especificado. Cuando un usuario realiza una solicitud a AWS KMS, el ID del punto de conexión de VPC de la solicitud se compara con el valor de la clave de condición `aws:sourceVpce` de la política. Si no coinciden, la solicitud se deniega.

Para utilizar una política como esta, sustituya el ID de la cuenta de Cuenta de AWS del marcador de posición y los ID del punto de conexión de VPC por valores válidos para su cuenta.

```
{
    "Id": "example-key-1",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM policies",
            "Effect": "Allow",
            "Principal": {"AWS":["111122223333"]},
            "Action": ["kms:*"],
            "Resource": "*"
        },
        {
            "Sid": "Restrict usage to my VPC endpoint",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:sourceVpce": "vpce-1234abcdf5678c90a"
                }
            }
        }

    ]
}
```

También puede utilizar la clave de condición `aws:sourceVpc` para restringir el acceso a las claves KMS en función de la VPC en la que reside el punto de conexión.

La siguiente política de claves de ejemplo permite comandos que administran la clave KMS solo cuando proceden de `vpc-12345678`. Además, permite comandos que utilizan la clave KMS para operaciones criptográficas únicamente si proceden de `vpc-2b2b2b2b`. Podría utilizar una política

como esta en caso de que una aplicación se ejecute en una VPC, pero utiliza una segunda VPC aislada para funciones de administración.

Para utilizar una política como esta, sustituya el ID de la cuenta de Cuenta de AWS del marcador de posición y los ID del punto de conexión de VPC por valores válidos para su cuenta.

```
{
    "Id": "example-key-2",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow administrative actions from vpc-12345678",
            "Effect": "Allow",
            "Principal": {"AWS": "111122223333"},
            "Action": [
                "kms:Create*","kms:Enable*","kms:Put*","kms:Update*",
                "kms:Revoke*","kms:Disable*","kms:Delete*",
                "kms:TagResource", "kms:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:sourceVpc": "vpc-12345678"
                }
            }
        },
        {
            "Sid": "Allow key usage from vpc-2b2b2b2b",
            "Effect": "Allow",
            "Principal": {"AWS": "111122223333"},
            "Action": [
                "kms:Encrypt","kms:Decrypt","kms:GenerateDataKey*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:sourceVpc": "vpc-2b2b2b2b"
                }
            }
        },
        {
            "Sid": "Allow read actions from everywhere",
            "Effect": "Allow",
```

```
            "Principal": {"AWS": "111122223333"},
            "Action": [
                "kms:Describe*","kms:List*","kms:Get*"
            ],
            "Resource": "*",
        }
    ]
}
```

Registro de su punto de conexión de VPC

AWS CloudTrail registra todas las operaciones que utilizan el punto de conexión de VPC. Cuando una solicitud a AWS KMS utiliza un punto de conexión de VPC, el ID de este aparece en la entrada de registro de AWS CloudTrail que registra la solicitud. Puede utilizar el ID del punto de conexión para auditar el uso del punto de conexión de VPC de AWS KMS.

Sin embargo, tus CloudTrail registros no incluyen las operaciones solicitadas por los responsables de otras cuentas ni las solicitudes de AWS KMS operaciones con las claves y los alias de KMS de otras cuentas. Además, para proteger su VPC, las solicitudes que son denegadas por una política de puntos de conexión de la VPC, pero de lo contrario se habría permitido, no se registran en AWS CloudTrail.

Por ejemplo, esta entrada de log de ejemplo registra una solicitud GenerateDataKey que ha utilizado el punto de enlace de la VPC. El campo `vpcEndpointId` aparece al final de la entrada de log.

```
{
  "eventVersion":"1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::111122223333:user/Alice",
    "accessKeyId": "EXAMPLE_KEY_ID",
    "accountId": "111122223333",
    "userName": "Alice"
  },
  "eventTime":"2018-01-16T05:46:57Z",
  "eventSource":"kms.amazonaws.com",
  "eventName":"GenerateDataKey",
  "awsRegion":"eu-west-1",
  "sourceIPAddress":"172.01.01.001",
  "userAgent":"aws-cli/1.14.23 Python/2.7.12 Linux/4.9.75-25.55.amzn1.x86_64
 botocore/1.8.27",
```

```
  "requestParameters":{
    "keyId":"1234abcd-12ab-34cd-56ef-1234567890ab",
    "numberOfBytes":128
  },
  "responseElements":null,
  "requestID":"a9fff0bf-fa80-11e7-a13c-afcabff2f04c",
  "eventID":"77274901-88bc-4e3f-9bb6-acf1c16f6a7c",
  "readOnly":true,
  "resources":[{
    "ARN":"arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "accountId":"111122223333",
    "type":"AWS::KMS::Key"
  }],
  "eventType":"AwsApiCall",
  "recipientAccountId":"111122223333",
  "vpcEndpointId": "vpce-1234abcdf5678c90a"
}
```

Claves de estado para AWS KMS

Puede especificar las condiciones en las políticas clave y en las políticas de IAM que controlan el acceso a AWS KMS los recursos. La declaración de política solo será efectiva si se cumplen las condiciones. Por ejemplo, es posible que desee que solo entre en vigor una declaración de política después de una fecha específica. O puede que desee que una declaración de política controle el acceso solo cuando aparezca un valor específico en una solicitud de la API.

Para especificar condiciones, se utilizan claves de condición en el elemento `Condition` de la declaración de una política con operadores de condiciones de IAM. Algunas claves de condición se aplican de forma general AWS; otras son específicas de AWS KMS.

Los valores de las claves de condición deben cumplir las reglas de caracteres y codificación de las políticas AWS KMS clave y las políticas de IAM. Para obtener más información sobre las reglas del documento de política de claves, consulte Formato de la política de claves. Para obtener más información sobre las reglas del documento de política de IAM, consulte Requisitos de nombres de IAM en la Guía del usuario de IAM.

Temas

- AWS claves de condición globales
- AWS KMS claves de condición

- AWS KMS claves de condición para AWS Nitro Enclaves

AWS claves de condición globales

AWS define las claves de condición globales, un conjunto de claves de condiciones de política para todos los AWS servicios que utilizan IAM para el control de acceso. AWS KMS admite todas las claves de condición globales. Puede utilizarlas en políticas AWS KMS clave y políticas de IAM.

Por ejemplo, puede usar la clave de condición PrincipalArn global aws: para permitir el acceso a una AWS KMS key (clave KMS) solo cuando el principal de la solicitud esté representado por el nombre de recurso de Amazon (ARN) en el valor de la clave de condición. Para respaldar el control de acceso basado en atributos (ABAC) AWS KMS, puede utilizar la clave de condición global aws:ResourceTag/tag-key en una política de IAM para permitir el acceso a las claves de KMS con una etiqueta determinada.

Para evitar que un AWS servicio se utilice de forma confusa en una política en la que el director es el director del AWS servicio, puede utilizar las claves de condición o globales. aws:SourceArnaws:SourceAccount Para obtener más detalles, consulte Uso de claves de condición `aws:SourceArn` o `aws:SourceAccount`.

Para obtener información sobre las claves de condición AWS globales, incluidos los tipos de solicitudes en las que están disponibles, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM. Para obtener ejemplos del uso de claves de condición globales en las políticas de IAM, consulte Control del acceso a las solicitudes y Control de claves de etiqueta en la Guía del usuario de IAM.

En los temas siguientes se proporcionan instrucciones especiales para el uso de claves de condición basadas en direcciones IP y puntos de conexión de VPC.

Temas

- Usar la condición de dirección IP en políticas con permisos de AWS KMS
- Usar condiciones de punto de conexión de VPC en políticas con permisos de AWS KMS

Usar la condición de dirección IP en políticas con permisos de AWS KMS

Puede utilizarlas AWS KMS para proteger sus datos en un AWS servicio integrado. Sin embargo, tenga cuidado al especificar la dirección IP, la condición, los operadores o la clave de `aws:SourceIp` condición en la misma declaración de política a la que se permite o deniega el

acceso AWS KMS. Por ejemplo, la política de Denega el acceso en AWSAWS función de la IP de origen restringe AWS las acciones a las solicitudes del rango de IP especificado.

Considere esta situación:

1. Adjunta a una identidad de IAM una política como la que se muestra en AWS: Denega el acceso a una identidad de IAM en AWS función de la IP de origen. A continuación, establece el valor de la clave de condición `aws:SourceIp` en el rango de direcciones IP de la empresa del usuario. Esta identidad de IAM tiene otras políticas adjuntadas que le permiten usar Amazon EBS, Amazon EC2 y AWS KMS.
2. La identidad intenta asociar un volumen de EBS cifrado a una instancia de EC2. Esta acción falla con un error de autorización a pesar de que el usuario tiene permiso para utilizar todos los servicios pertinentes.

El paso 2 falla porque la solicitud AWS KMS para descifrar la clave de datos cifrados del volumen proviene de una dirección IP asociada a la infraestructura de Amazon EC2. Para que la solicitud se realice correctamente, debe provenir de la dirección IP del usuario que la origina. Dado que la política del paso 1 deniega explícitamente todas las solicitudes de las direcciones IP que no sean las especificadas, a Amazon EC2 se le deniega el permiso para descifrar la clave de datos cifrada del volumen de EBS.

Además, la clave de condición `aws:sourceIP` no es efectiva si la solicitud procede de un punto de conexión de Amazon VPC. Para restringir las solicitudes a un punto de conexión de VPC, incluido un punto de conexión de VPC de AWS KMS, utilice las claves de condición `aws:sourceVpce` o `aws:sourceVpc`. Para obtener más información, consulte Puntos de conexión de VPC - Control del uso de los puntos de conexión en la Guía del usuario de Amazon VPC.

Usar condiciones de punto de conexión de VPC en políticas con permisos de AWS KMS

AWS KMS es compatible con los puntos de conexión de Amazon Virtual Private Cloud (Amazon VPC) que funcionan con la tecnología de. AWS PrivateLink Puede usar las siguientes claves de condición globales en las políticas clave y en las políticas de IAM para controlar el acceso a AWS KMS los recursos cuando la solicitud proviene de una VPC o utiliza un punto de enlace de la VPC. Para obtener más detalles, consulte Utilizar un punto de conexión de VPC en una declaración de política.

- `aws:SourceVpc` limita el acceso a las solicitudes procedentes de la VPC especificada.

- `aws:SourceVpce` limita el acceso a las solicitudes procedentes del punto de conexión de VPC especificado.

Si utilizas estas claves de condición para controlar el acceso a las claves de KMS, podrías denegar inadvertidamente el acceso a los AWS servicios que se utilizan en tu nombre. AWS KMS

Procure evita una situación como la del ejemplo de claves de condición de dirección IP. Si restringes las solicitudes de una clave de KMS a una VPC o un punto final de VPC, es posible que se produzcan errores en las llamadas AWS KMS desde un servicio integrado, como Amazon S3 o Amazon EBS. Esto puede ocurrir incluso si la solicitud de origen procede en última instancia de la VPC o del punto de conexión de VPC.

AWS KMS claves de condición

AWS KMS proporciona un conjunto de claves de condición que puede utilizar en las políticas clave y en las políticas de IAM. Estas claves de condición son específicas de. AWS KMS Por ejemplo, puede utilizar la clave de condición `kms:EncryptionContext:`*`context-key`* para exigir un determinado contexto de cifrado al controlar el acceso a una clave KMS de cifrado simétrica.

Condiciones para una solicitud de operación de la API

Muchas claves de AWS KMS condición controlan el acceso a una clave de KMS en función del valor de un parámetro de la solicitud de una AWS KMS operación. Por ejemplo, puede usar la clave de KeySpec condición kms: en una política de IAM para permitir el uso de la CreateKeyoperación solo cuando el valor del `KeySpec` parámetro de la `CreateKey` solicitud sea `RSA_4096` el mismo.

Este tipo de condición funciona incluso cuando el parámetro no aparece en la solicitud, como cuando se utiliza el valor predeterminado del parámetro. Por ejemplo, puede usar la clave de KeySpec condición kms: para permitir que los usuarios usen la `CreateKey` operación solo cuando el valor del `KeySpec` parámetro sea`SYMMETRIC_DEFAULT`, que es el valor predeterminado. Esta condición permite las solicitudes que tienen el parámetro `KeySpec` con el valor `SYMMETRIC_DEFAULT` y las solicitudes que no tienen el parámetro `KeySpec`.

Condiciones para claves KMS utilizadas en operaciones de la API

Algunas claves de AWS KMS condición pueden controlar el acceso a las operaciones en función de una propiedad de la clave KMS que se utiliza en la operación. Por ejemplo, puede usar la KeyOrigin condición kms: para permitir que los directores GenerateDataKeyinvoquen una clave KMS solo

cuando `Origin` la clave KMS lo sea`AWS_KMS`. Para averiguar si una clave de condición se puede utilizar de esta manera, consulte la descripción de la clave de condición.

La operación debe ser una operación de recursos de clave KMS, es decir, una operación que está autorizada para una clave KMS en particular. Para identificar las operaciones de recursos clave de KMS, en la tabla de acciones y recursos, busque un valor de `KMS key` en la columna `Resources` para la operación. Si utiliza este tipo de clave de condición con una operación que no está autorizada para un recurso clave de KMS concreto, por ejemplo ListKeys, el permiso no entra en vigor porque la condición nunca se puede cumplir. No existe ningún recurso de clave KMS involucrado en la autorización de la operación `ListKeys` y tampoco la propiedad `KeySpec`.

En los temas siguientes se describe cada clave de AWS KMS condición e incluyen ejemplos de declaraciones de política que muestran la sintaxis de las políticas.

Uso de operadores de conjuntos con claves de condición

Cuando una condición de política compara dos conjuntos de valores, como el conjunto de etiquetas de una solicitud y el conjunto de etiquetas de una política, es necesario saber AWS cómo comparar los conjuntos. IAM define dos operadores de conjunto, `ForAnyValue` y `ForAllValues` con este fin. Utilice operadores de conjunto solo con claves de condición de varios valores, que los requieren. No utilice operadores de conjunto con claves de condición de un solo valor. Como siempre, pruebe sus declaraciones de políticas minuciosamente antes de usarlas en entornos de producción.

Las claves de condición tienen un valor único o un valor múltiple. Para determinar si una clave de AWS KMS condición es de un solo valor o de varios valores, consulte la columna Tipo de valor en la descripción de la clave de condición.

- Las claves de condiciones Single-valued (Valor único) tienen como máximo un valor en el contexto de autorización (la solicitud o el recurso). Por ejemplo, dado que cada llamada a la API solo puede originarse desde una Cuenta de AWS, kms: CallerAccount es una clave de condición de un solo valor. No utilice un operador de conjunto con una clave de condición de un solo valor.
- Las claves de condición de múltiples valores tienen varios valores en el contexto de autorización (la solicitud o el recurso). Por ejemplo, dado que cada clave de KMS puede tener varios alias, kms: ResourceAliases puede tener varios valores. Las claves de condición de varios valores requieren un operador de conjunto.

Tenga en cuenta que la diferencia entre las claves de condición de un solo valor y de varios valores depende del número de valores en el contexto de autorización, no del número de valores de la condición de política.

> **Warning**
>
> El uso de un operador de conjunto con una clave de condición de un solo valor puede crear una declaración de política excesivamente permisiva (o excesivamente restrictiva). Utilice operadores de conjunto solo con claves de condición de varios valores.
> Si crea o actualiza una política que incluye un operador de `ForAllValues` conjunto con las claves de contexto o `aws:RequestTag/`*`tag-key`* condición kmsEncryptionContext::, AWS KMS devuelve el siguiente mensaje de error:
> `OverlyPermissiveCondition: Using the ForAllValues set operator with a single-valued condition key matches requests without the specified [encryption context or tag] or with an unspecified [encryption context or tag]. To fix, remove ForAllValues.`

Para obtener información detallada acerca de los operadores de conjuntos `ForAnyValue` y `ForAllValues`, consulte Uso de múltiples claves y valores en la Guía del usuario de IAM. Para obtener información sobre el riesgo de utilizar el operador `ForAllValues` set con una condición de un solo valor, consulte Advertencia de seguridad: ForAllValues con clave de un solo valor en la Guía del usuario de IAM.

Temas

- km: BypassPolicyLockoutSafetyCheck
- km: CallerAccount
- kms: CustomerMasterKeySpec (obsoleto)
- kms: CustomerMasterKeyUsage (obsoleto)
- km: DataKeyPairSpec
- km: EncryptionAlgorithm
- kmsEncryptionContext: clave de contexto
- kms: EncryptionContextKeys
- km: ExpirationModel
- kms: GrantConstraintType
- km: GrantIsFor AWSResource
- kms: GrantOperations
- km: GranteePrincipal

- kms: KeyOrigin
- kms: KeySpec
- kms: KeyUsage
- km: MacAlgorithm
- km: MessageType
- km: MultiRegion
- kms: MultiRegionKeyType
- kms: PrimaryRegion
- km: ReEncryptOnSameKey
- kms: RequestAlias
- km: ResourceAliases
- kms: ReplicaRegion
- km: RetiringPrincipal
- km: RotationPeriodInDays
- km: ScheduleKeyDeletionPendingWindowInDays
- km: SigningAlgorithm
- kms: ValidTo
- kms: ViaService
- km: WrappingAlgorithm
- km: WrappingKeySpec

km: BypassPolicyLockoutSafetyCheck

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:BypassPolicyLockoutSafetyCheck`	Booleano	Valor único	`CreateKey` `PutKeyPolicy`	Solo políticas de IAM

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
				Políticas de claves y políticas de IAM

La clave de `kms:BypassPolicyLockoutSafetyCheck` condición controla el acceso a PutKeyPolicylas operaciones CreateKeyy en función del valor del `BypassPolicyLockoutSafetyCheck` parámetro de la solicitud.

En el siguiente ejemplo, la declaración de la política de IAM impide que los usuarios eludan la comprobación de seguridad de bloqueo de la política denegándoles el permiso para crear claves KMS cuando el valor del parámetro `BypassPolicyLockoutSafetyCheck` de la solicitud `CreateKey` es `true`.

```
{
  "Effect": "Deny",
  "Action": [
    "kms:CreateKey",
    "kms:PutKeyPolicy"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
}
```

También puede utilizar la clave de condición `kms:BypassPolicyLockoutSafetyCheck` en una política de IAM o en una política de claves para controlar el acceso a la operación `PutKeyPolicy`. En el ejemplo siguiente, la declaración de una política de claves impide que los usuarios eludan la comprobación de seguridad de bloqueo cuando se modifica la política de una clave KMS.

En lugar de utilizar una operación `Deny` explícita, esta declaración de la política utiliza `Allow` con el operador de condición Null para permitir únicamente el acceso cuando la solicitud no contiene el parámetro `BypassPolicyLockoutSafetyCheck`. Cuando no se utiliza el parámetro, el valor

predeterminado es `false`. Esta declaración de la política es algo más débil y puede anularse en el caso improbable de que sea necesario eludirla.

```
{
  "Effect": "Allow",
  "Action": "kms:PutKeyPolicy",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
}
```

Véase también

- kms: KeySpec
- kms: KeyOrigin
- kms: KeyUsage

km: CallerAccount

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:CallerAccount`	Cadena	Valor único	Operaciones de recursos de claves KMS Operaciones de almacén de claves personalizadas	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para permitir o denegar el acceso a todas las identidades (usuarios y roles) de una Cuenta de AWS. En las políticas de claves, se usa el elemento `Principal`

para especificar las identidades a las que se aplica la declaración de política. La sintaxis del elemento `Principal` no proporciona una forma de especificar todas las identidades en una Cuenta de AWS. Sin embargo, puede lograr este efecto combinando esta clave de condición con un `Principal` elemento que especifique todas AWS las identidades.

Puede usarla para controlar el acceso a cualquier operación de recurso clave de KMS, es decir, cualquier AWS KMS operación que utilice una clave de KMS concreta. Para identificar las operaciones de recursos clave KMS, en laTabla de acciones y recursos, busque un valor de `KMS key` en la columna `Resources` para la operación. También es válido para operaciones que administran almacenes de claves personalizados.

Por ejemplo, la siguiente declaración de política de claves demuestra cómo utilizar la clave de condición `kms:CallerAccount`. Esta declaración de política se encuentra en la política clave Clave administrada de AWS de Amazon EBS. Combina un `Principal` elemento que especifica todas las AWS identidades con la clave de `kms:CallerAccount` condición para permitir el acceso efectivo a todas las identidades en Cuenta de AWS 111122223333. Contiene una clave de AWS KMS condición adicional (`kms:ViaService`) para limitar aún más los permisos al permitir únicamente las solicitudes que llegan a través de Amazon EBS. Para obtener más información, consulte kms: ViaService.

```
{
  "Sid": "Allow access through EBS for all principals in the account that are
 authorized to use EBS",
  "Effect": "Allow",
  "Principal": {"AWS": "*"},
  "Condition": {
    "StringEquals": {
      "kms:CallerAccount": "111122223333",
      "kms:ViaService": "ec2.us-west-2.amazonaws.com"
    }
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:DescribeKey"
  ],
  "Resource": "*"
```

```
}
```

kms: CustomerMasterKeySpec (obsoleto)

La clave de condición `kms:CustomerMasterKeySpec` está obsoleta. En su lugar, utilice la clave de KeySpec condición kms:.

Las claves de condición `kms:CustomerMasterKeySpec` y `kms:KeySpec` funcionan de la misma forma. Solo los nombres difieren. Le recomendamos que utilice `kms:KeySpec`. Sin embargo, para evitar cambios irrelevantes, AWS KMS es compatible con ambas claves de condición.

kms: CustomerMasterKeyUsage (obsoleto)

La clave de condición `kms:CustomerMasterKeyUsage` está obsoleta. En su lugar, utilice la clave de KeyUsage condición kms:.

Las claves de condición `kms:CustomerMasterKeyUsage` y `kms:KeyUsage` funcionan de la misma forma. Solo los nombres difieren. Le recomendamos que utilice `kms:KeyUsage`. Sin embargo, para evitar cambios irrelevantes, AWS KMS es compatible con ambas claves de condición.

km: DataKeyPairSpec

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:DataKeyPairSpec`	Cadena	Valor único	`GenerateDataKeyPair` `GenerateDataKeyPairWithoutPlaintext`	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para controlar el acceso a las GenerateDataKeyPairWithoutPlaintextoperaciones GenerateDataKeyPairy en función del valor del `KeyPairSpec` parámetro de la solicitud. Por ejemplo, puede permitir que un usuario genere solo determinados tipos de pares de claves de datos.

El siguiente ejemplo de declaración de política de claves utiliza la clave de condición `kms:DataKeyPairSpec` para permitir a los usuarios utilizar la clave KMS para generar solo pares de claves de datos RSA.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:GenerateDataKeyPair",
    "kms:GenerateDataKeyPairWithoutPlaintext"
  ],
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:DataKeyPairSpec": "RSA*"
    }
  }
}
```

Véase también

- kms: KeySpec
- the section called “km: EncryptionAlgorithm”
- the section called “kmsEncryptionContext: clave de contexto”
- the section called “kms: EncryptionContextKeys”

km: EncryptionAlgorithm

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:EncryptionAlgorithm`	Cadena	Valor único	`Decrypt` `Encrypt`	Políticas de claves y políticas de IAM

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política

			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateDataKeyPairWithoutPlaintext`
			`GenerateDataKeyWithoutPlaintext`
			`ReEncrypt`	

Puede utilizar la clave de condición `kms:EncryptionAlgorithm` para controlar el acceso a operaciones criptográficas en función del algoritmo de cifrado que se utiliza en la operación. Para las ReEncryptoperaciones de cifrado, descifrado y, por el contrario, controla el acceso en función del valor del EncryptionAlgorithmparámetro de la solicitud. Para operaciones que generan claves de datos y pares de claves de datos, controla el acceso basado en el algoritmo de cifrado que se utiliza para cifrar la clave de datos.

Esta clave de condición no afecta a las operaciones que se realizan fuera de AWS KMS, como el cifrado con la clave pública de un par de claves KMS asimétricas fuera de. AWS KMS

EncryptionAlgorithm parámetro en una solicitud

Para permitir a los usuarios utilizar solo un algoritmo de cifrado determinado con una clave KMS, utilice una declaración de política con un efecto `Deny` y un operador de condición `StringNotEquals`. Por ejemplo, la siguiente declaración de política de claves de ejemplo prohíbe a las entidades principales que pueden asumir el rol `ExampleRole` utilizar esta clave KMS en las

operaciones criptográficas especificadas, a menos que el algoritmo de cifrado de la solicitud sea `RSAES_OAEP_SHA_256`, un algoritmo de cifrado asimétrico que se usa con claves KMS RSA.

A diferencia de una declaración de política que permite a un usuario utilizar un algoritmo de cifrado determinado, una declaración de política con un doble negativo como este impide que otras políticas y concesiones para esta clave KMS permitan que este rol utilice otros algoritmos de cifrado. `Deny` en esta declaración de política tiene prioridad sobre cualquier otra política de claves o política de IAM con un efecto `Allow` y tiene prioridad sobre todas las concesiones para esta clave KMS y sus entidades principales.

```
{
  "Sid": "Allow only one encryption algorithm with this asymmetric KMS key",
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:EncryptionAlgorithm": "RSAES_OAEP_SHA_256"
    }
  }
}
```

Algoritmo de cifrado utilizado para la operación

También puede utilizar la clave de condición `kms:EncryptionAlgorithm` para controlar el acceso a operaciones según el algoritmo de cifrado utilizado en la operación, incluso cuando el algoritmo no se especifica en la solicitud. Esto le permite requerir o prohibir el algoritmo `SYMMETRIC_DEFAULT`, que puede que no se especifique en una solicitud porque es el valor predeterminado.

Esta característica le permite usar la clave de condición `kms:EncryptionAlgorithm` para controlar el acceso a las operaciones que generan claves de datos y pares de claves de datos. Estas operaciones solo utilizan claves KMS de cifrado simétricas y el algoritmo `SYMMETRIC_DEFAULT`.

Por ejemplo, esta política de IAM limita sus entidades principales al cifrado simétrico. Deniega el acceso a cualquier clave KMS en la cuenta de ejemplo para operaciones criptográficas a menos que el algoritmo de cifrado especificado en la solicitud o utilizado en la operación sea SYMMETRIC_DEFAULT. Incluye `GenerateDataKey*` GenerateDataKeyadiciones GenerateDataKeyWithoutPlaintext, GenerateDataKeyPair, y GenerateDataKeyPairWithoutPlaintexta los permisos. La condición no tiene ningún efecto en estas operaciones porque siempre utilizan un algoritmo de cifrado simétrico.

```
{
  "Sid": "AllowOnlySymmetricAlgorithm",
  "Effect": "Deny",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringNotEquals": {
      "kms:EncryptionAlgorithm": "SYMMETRIC_DEFAULT"
    }
  }
}
```

Véase también

- the section called “km: MacAlgorithm”
- km: SigningAlgorithm

kmsEncryptionContext: clave de contexto

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:EncryptionCont`	Cadena	Valor único	`CreateGrant` `Encrypt`	Políticas de claves y políticas de IAM

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política

`ext: context-key`			`Decrypt`
			
			`GenerateDataKey`
			
			`GenerateDataKeyPair`
			
			`GenerateDataKeyPairWithoutPlaintext`
			
			`GenerateDataKeyWithoutPlaintext`
			
			`ReEncrypt`	

Puede usar la clave de condición `kms:EncryptionContext:context-key` para controlar el acceso a una clave KMS de cifrado simétrica en función del contexto de cifrado de una solicitud para una operación criptográfica. Utilice esta clave de condición para evaluar la clave y el valor del par de contexto de cifrado. Para evaluar solo las claves de contexto de cifrado o para requerir un contexto de cifrado independientemente de las claves o los valores, utilice la clave EncryptionContextKeys condicionada kms:.

> **Note**
>
> Los valores de claves de condición deben ajustarse a las reglas de caracteres de políticas de claves y políticas de IAM. Algunos caracteres válidos en un contexto de cifrado no son válidos en las políticas. Es posible que no pueda utilizar esta clave de condición para expresar todos los valores de contexto de cifrado válidos. Para obtener más información sobre las reglas del documento de política de claves, consulte Formato de la política de

claves. Para obtener más información sobre las reglas del documento de política de IAM, consulte Requisitos de nombres de IAM en la Guía del usuario de IAM.

No puede especificar un contexto de cifrado en una operación criptográfica con una clave KMS asimétrica o una clave KMS HMAC. Los algoritmos asimétricos y los algoritmos MAC no son compatibles con un contexto de cifrado.

Para usar la clave de condición de clave de contexto kmsEncryptionContext::, sustituya el marcador de posición de la clave de *contexto por la clave* de contexto de cifrado. Sustituya el marcador de posición *context-value* por el valor de contexto de cifrado.

```
"kms:EncryptionContext:context-key": "context-value"
```

Por ejemplo, la siguiente clave de condición especifica un contexto de cifrado en el que la clave es `AppName` y el valor es `ExampleApp` (`AppName = ExampleApp`).

```
"kms:EncryptionContext:AppName": "ExampleApp"
```

Esta es una clave de condición de un solo valor. La clave de la clave de condición especifica una clave de contexto de cifrado determinada (context-key). Aunque puede incluir varios pares de contexto de cifrado en cada solicitud de la API, el par de contexto de cifrado con el context-key puede tener solo un valor. Por ejemplo, la clave de condición `kms:EncryptionContext:Department` solo se aplica a los pares de contexto de cifrado con una clave `Department`, y cualquier par de contexto de cifrado dado con la clave `Department` solo puede tener un valor.

No utilice un operador de conjunto con la clave de condición `kms:EncryptionContext:`*`context-key`*. Si crea una declaración de política con una acción `Allow`, la clave de condición `kms:EncryptionContext:`*`context-key`* y el operador de conjunto `ForAllValues`, la condición permite solicitudes sin contexto de cifrado y solicitudes con pares de contexto de cifrado que no se especifican en la condición de política.

> **Warning**
>
> No utilice un operador de conjunto `ForAnyValue` o `ForAllValues` con esta clave de condición de un solo valor. Estos operadores de conjunto pueden crear una condición

de política que no requiera valores que pretenda requerir y permite valores que pretende prohibir.
Si crea o actualiza una política que incluye un operador `ForAllValues` set con la clave de contexto kms:EncryptionContext:, devuelve el siguiente mensaje de error: AWS KMS `OverlyPermissiveCondition:EncryptionContext: Using the ForAllValues set operator with a single-valued condition key matches requests without the specified encryption context or with an unspecified encryption context. To fix, remove ForAllValues.`

Para requerir un par de contexto de cifrado concreto, utilice la clave de condición `kms:EncryptionContext:`*`context-key`* con el operador `StringEquals`.

En la siguiente declaración de política de claves de ejemplo se permite a las entidades principales que pueden asumir la función utilizar la clave KMS en una solicitud `GenerateDataKey` solo cuando el contexto de cifrado de la solicitud contiene el par `AppName:ExampleApp`. Se permiten otros pares de contexto de cifrado.

El nombre de las claves distingue entre mayúsculas y minúsculas. La distinción de mayúsculas y minúsculas del valor se determina mediante el operador de condición, como `StringEquals`. Para obtener más detalles, consulte Uso de mayúsculas y minúsculas en las condiciones de contexto de cifrado.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
}
```

Para exigir un par de contextos de cifrado y prohibir todos los demás pares de contextos de cifrado, utilice kms:EncryptionContext: context-key y `kms:EncryptionContextKeys`en la declaración de política. En la siguiente declaración de política de claves se utiliza la

condición `kms:EncryptionContext:AppName` para requerir el par de contexto de cifrado `AppName=ExampleApp` en la solicitud. También utiliza una clave de condición `kms:EncryptionContextKeys` con el operador de conjunto `ForAllValues` para permitir solo la clave de contexto de cifrado `AppName`.

El operador de conjunto `ForAllValues` limita las claves de contexto de cifrado en la solicitud a `AppName`. Si la condición `kms:EncryptionContextKeys` con el operador de conjunto `ForAllValues` se utilizó solo en una declaración de política, este operador de conjunto permitiría solicitudes sin contexto de cifrado. Sin embargo, si la solicitud no tenía contexto de cifrado, la condición `kms:EncryptionContext:AppName` fallaría. Para conocer los detalles sobre el operador de conjunto `ForAllValues`, consulte Uso de múltiples claves y valores en la Guía del usuario de IAM.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/KeyUsers"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    },
    "ForAllValues:StringEquals": {
      "kms:EncryptionContextKeys": [
        "AppName"
      ]
    }
  }
}
```

También puede utilizar esta clave de condición para denegar el acceso a una clave KMS para una operación concreta. En la siguiente declaración de política de claves de ejemplo se utiliza un efecto `Deny` para prohibir a la entidad principal utilizar la clave KMS si el contexto de cifrado de la solicitud contiene un par de contexto de cifrado `Stage=Restricted`. Esta condición permite una solicitud con otros pares de contexto de cifrado, incluidos los pares de contexto de cifrado con la clave `Stage` y otros valores, como `Stage=Test`.

```
{
```

```
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": "Restricted"
    }
  }
}
```

Uso de varios pares de contexto de cifrado

Puede requerir o prohibir varios pares de contexto de cifrado. También puede requerir uno de varios pares de contexto de cifrado. Para conocer los detalles de la lógica utilizada para interpretar estas condiciones, consulte Crear una condición con varias claves o valores en la Guía del usuario de IAM.

> **Note**
>
> Las versiones anteriores de este tema mostraban declaraciones de política que utilizaban los operadores `ForAnyValue` y `ForAllValues` set con la clave de condición kms:EncryptionContext: context-key. Usando un operador de conjunto con una clave de condición de un solo valor puede dar lugar a políticas que permiten solicitudes sin contexto de cifrado y pares de contexto de cifrado no especificados.
> Por ejemplo, una condición de política con el efecto `Allow`, el operador de conjunto `ForAllValues` y la clave de condición `"kms:EncryptionContext:Department": "IT"` no limita el contexto de cifrado al par "Department=IT". Permite solicitudes sin contexto de cifrado y solicitudes con pares de contexto de cifrado no especificados, como `Stage=Restricted`.
> Revise sus políticas y elimine el operador set de cualquier condición con kms:EncryptionContext: context-key. Los intentos de crear o actualizar una política con este formato fallan con una excepción `OverlyPermissiveCondition`. Para resolver el error, elimine el operador de conjunto.

Para requerir varios pares de contexto de cifrado, enumere los pares en la misma condición. En la siguiente declaración de política de claves de ejemplo se requieren dos pares de contexto de

cifrado, `Department=IT` y `Project=Alpha`. Debido a que las condiciones tienen diferentes claves (`kms:EncryptionContext:Department` y `kms:EncryptionContext:Project`), están implícitamente conectados por un operador AND. Otros pares de contexto de cifrado están permitidos, pero no son necesarios.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Department": "IT",
      "kms:EncryptionContext:Project": "Alpha"
    }
  }
}
```

Para requerir un par de contexto de cifrado U otro par, coloque cada clave de condición en una declaración de política independiente. En la siguiente política de claves de ejemplo se requiere `Department=IT` o `Project=Alpha` pares, o ambos. Otros pares de contexto de cifrado están permitidos, pero no son necesarios.

```
{
 "Effect": "Allow",
 "Principal": {
  "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
 },
 "Action": "kms:GenerateDataKey",
 "Resource": "*",
 "Condition": {
  "StringEquals": {
   "kms:EncryptionContext:Department": "IT"
  }
 }
},
{
 "Effect": "Allow",
 "Principal": {
  "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
```

```
 },
 "Action": "kms:GenerateDataKey",
 "Resource": "*",
 "Condition": {
  "StringEquals": {
   "kms:EncryptionContext:Project": "Alpha"
  }
 }
}
```

Para exigir pares de cifrado específicos y excluir todos los demás pares de contextos de cifrado, utilice tanto la clave de contexto kms:EncryptionContext: como la de la declaración de política `kms:EncryptionContextKeys`. La siguiente declaración de política clave utiliza la condición de clave contextual kmsEncryptionContext:: para requerir un contexto de cifrado con ambos pares y. *`Department=IT`* `Project=Alpha` Utiliza una clave de condición `kms:EncryptionContextKeys` con el operador de conjuntos `ForAllValues` para permitir solo las claves de contexto de cifrado `Department` y `Project`.

El operador de conjuntos `ForAllValues` limita las claves de contexto de cifrado en la solicitud a `Department` y `Project`. Si se usara solo en una condición, este operador de conjunto permitiría solicitudes sin contexto de cifrado, pero en esta configuración, la clave de contexto kms:EncryptionContext: en esta condición fallaría.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Department": "IT",
      "kms:EncryptionContext:Project": "Alpha"
    },
    "ForAllValues:StringEquals": {
      "kms:EncryptionContextKeys": [
        "Department",
        "Project"
      ]
    }
  }
```

```
}
```

También puede prohibir varios pares de contexto de cifrado. En la siguiente declaración de política de claves de ejemplo se utiliza un efecto `Deny` para prohibir a la entidad principal utilizar las claves KMS si el contexto de cifrado de la solicitud contiene un par `Stage=Restricted` o `Stage=Production`.

Múltiples valores (`Restricted` y `Production`) para la misma clave (`kms:EncryptionContext:Stage`) están implícitamente conectados por un OR. Para conocer los detalles, consulte la Lógica de evaluación para condiciones con múltiples claves o valores en la Guía del usuario de IAM.

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": [
         "Restricted",
         "Production"
      ]
    }
  }
}
```

Uso de mayúsculas y minúsculas en las condiciones de contexto de cifrado

El contexto de cifrado que se especifica en una operación de descifrado debe coincidir exactamente, incluido el uso de mayúsculas y minúsculas, con el contexto de cifrado que se especifica en la operación de cifrado. Solo puede variar el orden de los pares de un contexto de cifrado con varios pares.

Sin embargo, en las condiciones de políticas, la clave de condición no distingue entre mayúsculas y minúsculas. La distinción de mayúsculas y minúsculas del valor de la condición se determina por el operador de condición de política que utilice, como `StringEquals` o `StringEqualsIgnoreCase`.

Por tanto, la clave de condición, que consta del prefijo `kms:EncryptionContext:` y el valor sustituto de *`context-key`*, no distingue mayúsculas de minúsculas. Una política que utiliza esta condición no comprueba el uso de mayúsculas o minúsculas de ninguno de los elementos de la clave de condición. La distinción de mayúsculas y minúsculas del valor, es decir *`context-value`*, lo determina el operador de la política de condición.

Por ejemplo, la siguiente declaración de política permite la operación cuando el contexto de cifrado incluye una clave `Appname`, independientemente de si está en mayúsculas o minúsculas. La condición `StringEquals` requiere que `ExampleApp` esté en mayúsculas cuando se especifique.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Appname": "ExampleApp"
    }
  }
}
```

Para requerir una clave de contexto de cifrado que distinga entre mayúsculas y minúsculas, utilice la condición kms: EncryptionContextKeys policy con un operador de condición que distinga entre mayúsculas y minúsculas, como. `StringEquals` En esta condición de política, como la clave de contexto de cifrado es el valor de la condición de política, el operador de condición determina si se distingue entre mayúsculas y minúsculas.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
```

```
  }
}
```

Para exigir una evaluación de la clave y el valor del contexto de cifrado que distinga entre mayúsculas y minúsculas, utilice las condiciones de política `kms:EncryptionContextKeys` y la clave de contexto kmsEncryptionContext:: juntas en la misma declaración de política. El operador de condición sensible a mayúsculas y minúsculas (como `StringEquals`) siempre se aplica al valor de la condición. La clave de contexto de cifrado (como `AppName`) es el valor de la condición `kms:EncryptionContextKeys`. El valor del contexto de cifrado (por ejemplo*`ExampleApp`*) es el valor de la condición de clave contextual kms:EncryptionContext:.

Por ejemplo, en la siguiente declaración de política de clave de ejemplo, como el operador `StringEquals` distingue entre mayúsculas y minúsculas, tanto la clave de contexto de cifrado como el valor de contexto de cifrado distinguen entre mayúsculas y minúsculas.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    },
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
}
```

Uso de variables en una condición de contexto de cifrado

La clave y el valor de un par de contexto de cifrado deben ser cadenas literales simples. No pueden ser números enteros ni objetos, ni ningún tipo que no esté totalmente resuelto. Si utiliza un tipo diferente, como un entero o un flotante, lo AWS KMS interpreta como una cadena literal.

```
"encryptionContext": {
    "department": "10103.0"
}
```

Sin embargo, el valor de la clave de condición `kms:EncryptionContext:`*`context-key`* puede ser una variable de política de IAM. Estas variables de política se resuelven en tiempo de ejecución con arreglo a los valores de la solicitud. Por ejemplo, `aws:CurrentTime` se resuelve en la hora de la solicitud y `aws:username` se resuelve en el nombre descriptivo del autor de la llamada.

Puede utilizar estas variables de política para crear una declaración de política con una condición que requiera información muy específica de un contexto de cifrado, como el nombre de usuario del autor de la llamada. Como contiene una variable, puede utilizar la misma declaración de política con todos los usuarios que puedan adoptar ese rol. No tiene que escribir una declaración de política diferente para cada usuario.

Imagine una situación en la que desea que todos los usuarios que puedan adoptar un rol utilicen la misma clave KMS para cifrar y descifrar los datos. Sin embargo, solo quiere que puedan descifrar los datos que ellos han cifrado. Comience por exigir que todas las solicitudes AWS KMS incluyan un contexto de cifrado en el que la clave esté `user` y el valor sea el nombre de AWS usuario de la persona que llama, como el siguiente.

```
"encryptionContext": {
    "user": "bob"
}
```

A continuación, para forzar la aplicación de este requisito, puede utilizar una declaración de política como la del siguiente ejemplo. Esta declaración de política concede al rol `TestTeam` permiso para cifrar y descifrar datos con la clave KMS. Sin embargo, el permiso solo es válido cuando el contexto de cifrado de la solicitud incluye un par `"user": "`*`<username>`*`"`. Para representar el nombre de usuario, la condición utiliza la variable de política `aws:username`.

Cuando se evalúa la solicitud, la variable de condición se sustituye por el nombre de usuario del autor de la llamada. Por tanto, la condición necesita el contexto de cifrado `"user": "bob"` para "bob" y `"user": "alice"` para "alice".

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/TestTeam"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt"
  ],
```

```
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:user": "${aws:username}"
    }
  }
}
```

Puede utilizar una variable de política de IAM únicamente en el valor del par de la clave de condición `kms:EncryptionContext:`*`context-key`*. No puede utilizar una variable en la clave.

También puede utilizar claves de contexto específicas del proveedor en las variables. Estas claves de contexto identifican de forma exclusiva a los usuarios que han iniciado sesión AWS mediante la federación de identidades web.

Al igual que todas las variables, estas solo se pueden utilizar en la condición de política `kms:EncryptionContext:`*`context-key`*, no en el contexto de cifrado real. Y solo se pueden utilizar en el valor de la condición, no en la clave.

Por ejemplo, la siguiente declaración de política de clave es similar a la anterior. Sin embargo, la condición requiere un contexto de cifrado en el que la clave sea `sub` y el valor identifique de forma inequívoca a un usuario que ha iniciado sesión en un grupo de usuarios de Amazon Cognito. Para obtener más información acerca de la identificación de usuarios y roles en Amazon Cognito, consulte Roles de IAMen la Guía para desarrolladores de Amazon Cognito.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/TestTeam"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
       "kms:EncryptionContext:sub": "${cognito-identity.amazonaws.com:sub}"
    }
  }
}
```

Véase también

- the section called “kms: EncryptionContextKeys”
- the section called “kms: GrantConstraintType”

kms: EncryptionContextKeys

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política

`kms:EncryptionContextKeys`	Cadena (lista)	Multivalor	`CreateGrant`
			`Decrypt`
			`Encrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateDataKeyPairWithoutPlaintext`
			`GenerateDataKeyWithoutPlaintext`
			`ReEncrypt`
				Políticas de claves y políticas de IAM

Puede usar la clave de condición `kms:EncryptionContextKeys` para controlar el acceso a una clave KMS de cifrado simétrica en función del contexto de cifrado de una solicitud para una operación criptográfica. Utilice esta clave de condición para evaluar únicamente la clave de cada par

de contexto de cifrado. Utilice esta clave de condición `kms:EncryptionContext:`*`context-key`* para evaluar la clave y el valor del par de contexto de cifrado.

No puede especificar un contexto de cifrado en una operación criptográfica con una clave KMS asimétrica o una clave KMS HMAC. Los algoritmos asimétricos y los algoritmos MAC no son compatibles con un contexto de cifrado.

> **Note**
>
> Los valores de las claves de condición, incluida una clave de contexto de cifrado, deben ajustarse a las reglas de caracteres y codificación de las políticas de AWS KMS claves. Es posible que no pueda utilizar esta clave de condición para expresar todas las claves de contexto de cifrado válidas. Para obtener más información sobre las reglas del documento de política de claves, consulte Formato de la política de claves. Para obtener más información sobre las reglas del documento de política de IAM, consulte Requisitos de nombres de IAM en la Guía del usuario de IAM.

Esta es una clave de condición multivalor. Puede especificar varios pares de contexto de cifrado en cada solicitud de la API. `kms:EncryptionContextKeys` compara las claves de contexto de cifrado de la solicitud con el conjunto de claves de contexto de cifrado de la política. Para determinar cómo se comparan estos conjuntos, debe proporcionar un operador de conjuntos `ForAnyValue` o `ForAllValues` en la condición de política. Para conocer los detalles sobre los operadores de conjuntos, consulte Uso de múltiples claves y valores en la Guía del usuario de IAM.

- `ForAnyValue`: al menos una clave de contexto de cifrado en la solicitud debe coincidir con una clave de contexto de cifrado en la condición de política. Se permiten otras claves de contexto de cifrado. Si la solicitud no tiene contexto de cifrado, la condición no se cumple.
- `ForAllValues`: cada clave de contexto de cifrado de la solicitud debe coincidir con una clave de contexto de cifrado en la condición de política. Este operador de conjunto limita las claves de contexto de cifrado a aquellas en la condición de política. No requiere ninguna clave de contexto de cifrado, pero prohíbe las claves de contexto de cifrado no especificadas.

En la siguiente declaración de política de claves de ejemplo se utiliza la condición `kms:EncryptionContextKeys` con la clave de condición del operador de conjuntos `ForAnyValue`. Esta declaración de la política utiliza la clave KMS para las operaciones

especificadas, pero solamente cuando al menos uno de los pares de contexto de cifrado de la solicitud incluye la clave `AppName`, independientemente de su valor.

Por ejemplo, esta declaración de política de claves permite una solicitud `GenerateDataKey` con dos pares de contexto de cifrado, `AppName=Helper` y `Project=Alpha`, porque el primer par de contexto de cifrado cumple con la condición. Una solicitud con solo `Project=Alpha` o sin contexto de cifrado fallaría.

Como la operación de la StringEqualscondición distingue entre mayúsculas y minúsculas, esta declaración de política exige que la clave de contexto de cifrado esté escrita y escrita en mayúsculas y minúsculas. Sin embargo, puede utilizar un operador de condición que omita el uso de mayúsculas y minúsculas de la clave, como `StringEqualsIgnoreCase`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
  }
}
```

También puede utilizar la clave de condición `kms:EncryptionContextKeys` para solicitar un contexto de cifrado (cualquier contexto de cifrado) en las operaciones criptográficas que utilizan la clave KMS.

La siguiente declaración de política de ejemplo utiliza la clave de condición `kms:EncryptionContextKeys` con el operador de condición Null para permitir el acceso para utilizar una clave KMS de solo cuando el contexto de cifrado de la solicitud de la API no sea nulo. Esta condición no comprueba las claves ni los valores del contexto de cifrado. Solo verifica que existe el contexto de cifrado.

```
{
```

```
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContextKeys": false
    }
  }
}
```

Véase también

- kmsEncryptionContext: clave de contexto
- kms: GrantConstraintType

km: ExpirationModel

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:ExpirationModel`	Cadena	Valor único	`ImportKeyMaterial`	Políticas de claves y políticas de IAM

La clave de `kms:ExpirationModel` condición controla el acceso a la ImportKeyMaterialoperación en función del valor del ExpirationModelparámetro de la solicitud.

`ExpirationModel` es un parámetro opcional que determina si el material de claves importado vence. Los valores válidos son `KEY_MATERIAL_EXPIRES` y `KEY_MATERIAL_DOES_NOT_EXPIRE`. El valor predeterminado es `KEY_MATERIAL_EXPIRES`.

La fecha y la hora de caducidad vienen determinadas por el valor del ValidToparámetro. El parámetro `ValidTo` es necesario a menos que el valor del parámetro `ExpirationModel` sea `KEY_MATERIAL_DOES_NOT_EXPIRE`. También puede usar la clave de ValidTo condición kms: para exigir una fecha de caducidad determinada como condición de acceso.

La siguiente declaración de política de ejemplo utiliza la clave de condición `kms:ExpirationModel` para permitir a los usuarios importar solamente material de claves en una clave KMS cuando la solicitud incluye el parámetro `ExpirationModel` y su valor sea `KEY_MATERIAL_DOES_NOT_EXPIRE`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ExpirationModel": "KEY_MATERIAL_DOES_NOT_EXPIRE"
    }
  }
}
```

También puede utilizar la clave de condición `kms:ExpirationModel` para que un usuario solamente pueda importar material de claves cuando expire el material de claves. En el ejemplo siguiente, la declaración de la política de clave utiliza la clave de condición `kms:ExpirationModel` con el operador de condición Null para que un usuario solamente pueda importar material de claves cuando la solicitud no contenga un parámetro `ExpirationModel`. El valor predeterminado ExpirationModel es`KEY_MATERIAL_EXPIRES`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:ExpirationModel": true
```

```
    }
  }
}
```

Véase también

- kms: ValidTo
- km: WrappingAlgorithm
- km: WrappingKeySpec

kms: GrantConstraintType

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:GrantConstraintType`	Cadena	Valor único	`CreateGrant`	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para controlar el acceso a la CreateGrantoperación en función del tipo de restricción de concesión de la solicitud.

Al crear una concesión, también puede especificar una restricción de concesión para permitir las operaciones que permite la concesión solo cuando esté presente un determinado contexto de cifrado. La restricción de concesión puede ser uno de estos dos tipos: `EncryptionContextEquals` o `EncryptionContextSubset`. Puede usar esta clave de condición para comprobar que la solicitud contiene un tipo u otro.

> **Important**
>
> No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.

En la siguiente declaración de política de clave utiliza la clave de condición `kms:GrantConstraintType` para permitir que un usuario cree concesiones solo cuando la

solicitud incluya una restricción de concesión `EncryptionContextEquals`. En el ejemplo se muestra una declaración de política en una política de claves.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GrantConstraintType": "EncryptionContextEquals"
    }
  }
}
```

Véase también

- kmsEncryptionContext: clave de contexto
- kms: EncryptionContextKeys
- km: GrantIsFor AWSResource
- kms: GrantOperations
- km: GranteePrincipal
- km: RetiringPrincipal

km: GrantIsFor AWSResource

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política

`kms:GrantIsForAWSResource`	Booleano	Valor único	`CreateGrant`
			`ListGrants`
			`RevokeGrant`
				Políticas de claves y políticas de IAM

Permite o deniega el CreateGrantpermiso para RevokeGrantlas operaciones o solo cuando un AWS servicio integrado AWS KMS llama a la operación en nombre del usuario. ListGrants Esta condición de política no permite al usuario realizar estas operaciones de concesión directamente.

La siguiente declaración de política de ejemplo utiliza la clave de condición `kms:GrantIsForAWSResource`. Permite a AWS los servicios integrados AWS KMS, como Amazon EBS, crear concesiones en esta clave de KMS en nombre del principal especificado.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:GrantIsForAWSResource": true
    }
  }
}
```

Véase también

- kms: GrantConstraintType
- kms: GrantOperations
- km: GranteePrincipal
- km: RetiringPrincipal

kms: GrantOperations

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:GrantOperations`	Cadena	Multivalor	`CreateGrant`	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para controlar el acceso a la CreateGrantoperación en función de las operaciones de concesión de la solicitud. Por ejemplo, puede permitir que los usuarios creen concesiones que deleguen el permiso para cifrar pero no para descifrar. Para obtener más información acerca de concesiones, consulte Uso de concesiones.

Esta es una clave de condición de varios valores. `kms:GrantOperations` compara el conjunto de operaciones de concesión en la solicitud `CreateGrant` al conjunto de operaciones de concesión de la política. Para determinar cómo se comparan estos conjuntos, debe proporcionar un operador de conjuntos `ForAnyValue` o `ForAllValues` en la condición de política. Para conocer los detalles sobre los operadores de conjuntos, consulte Uso de múltiples claves y valores en la Guía del usuario de IAM.

- `ForAnyValue`: al menos una operación de concesión en la solicitud debe coincidir con una de las operaciones de concesión en la condición de política. Se permiten otras operaciones de concesión.
- ForAllValues: Cada operación de subvención incluida en la solicitud debe coincidir con una operación de subvención incluida en la condición de la política. Este operador de conjuntos limita las operaciones de concesión a las especificadas en la condición de política. No requiere ninguna operación de concesión, pero prohíbe operaciones de concesión no especificadas.

  ForAllValues también devuelve el valor true cuando no hay operaciones de subvención en la solicitud, pero `CreateGrant` no las permite. Si el parámetro `Operations` falta o tiene un valor nulo, la solicitud `CreateGrant` falla.

La siguiente declaración de política de clave de ejemplo utiliza la clave de condición `kms:GrantOperations` para crear concesiones solo cuando las operaciones de concesión sean `Encrypt`, `ReEncryptTo` o ambas. Si la concesión incluye cualquier otra operación, la solicitud `CreateGrant` falla.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
```

```
        "Encrypt",
        "ReEncryptTo"
      ]
    }
  }
}
```

Si cambia el operador de conjuntos en la condición de política a `ForAnyValue`, la declaración de política requerirá que al menos una de las operaciones de concesión sea `Encrypt` o `ReEncryptTo`, pero permitirá otras operaciones de concesión, como `Decrypt` o `ReEncryptFrom`.

Véase también

- kms: GrantConstraintType
- km: GrantIsFor AWSResource
- km: GranteePrincipal
- km: RetiringPrincipal

km: GranteePrincipal

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:GranteePrincipal`	Cadena	Valor único	`CreateGrant`	Políticas de IAM y de claves

Puede utilizar esta clave de condición para controlar el acceso a la CreateGrantoperación en función del valor del GranteePrincipalparámetro de la solicitud. Por ejemplo, puede crear concesiones para utilizar una clave KMS cuando la entidad principal del beneficiario en la solicitud `CreateGrant` coincida con la entidad principal especificada en la declaración de la condición.

Para especificar el principal beneficiario, utilice el nombre de recurso de Amazon (ARN) de un principal. AWS Entre los principales válidos se incluyen los usuarios de IAM Cuentas de AWS, los roles de IAM, los usuarios federados y los usuarios con roles asumidos. Para obtener ayuda con la sintaxis del ARN de un principal, consulte los ARN de IAM en la Guía del usuario de IAM.

En el ejemplo siguiente, la declaración de la política de claves utiliza la clave de condición `kms:GranteePrincipal` para crear concesiones de una clave KMS cuando la entidad principal del beneficiario de la concesión sea `LimitedAdminRole`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/LimitedAdminRole"
    }
  }
}
```

Véase también

- kms: GrantConstraintType
- km: GrantIsFor AWSResource
- kms: GrantOperations
- km: RetiringPrincipal

kms: KeyOrigin

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:KeyOrigin`	Cadena	Valor único	`CreateKey` Operaciones de recursos de claves KMS	Políticas de IAM Políticas de claves y políticas de IAM

La clave de condición `kms:KeyOrigin` controla el acceso a las operaciones en función del valor de la propiedad `Origin` de clave KMS creada por la operación o utilizada en ella. Funciona como una condición de recurso o una condición de solicitud.

Puede utilizar esta clave de condición para controlar el acceso a la CreateKeyoperación en función del valor del parámetro Origin de la solicitud. Los valores válidos para `Origin` son `AWS_KMS`, `AWS_CLOUDHSM` y `EXTERNAL`.

Por ejemplo, puede crear una clave KMS solo cuando el material clave se genere en AWS KMS (`AWS_KMS`), solo cuando el material clave se genere en un AWS CloudHSM clúster asociado a un almacén de claves personalizado (`AWS_CLOUDHSM`) o solo cuando el material clave se importe de una fuente externa (`EXTERNAL`).

El siguiente ejemplo de declaración de política clave utiliza la clave de `kms:KeyOrigin` condición para crear una clave de KMS solo cuando se AWS KMS crea el material clave.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
      },
      "Action": "kms:CreateKey",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:KeyOrigin": "AWS_KMS"
        }
      }
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
```

```
        "kms:GenerateDataKeyPair",
        "kms:GenerateDataKeyPairWithoutPlaintext",
        "kms:ReEncrypt*"
      ],
      "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "kms:KeyOrigin": "AWS_CLOUDHSM"
        }
      }
    }
  ]
}
```

También puede utilizar la clave de condición `kms:KeyOrigin` para controlar el acceso a las operaciones que utilizan o administran una clave de KMS en función de la propiedad `Origin` de la clave de KMS utilizada para la operación. La operación debe ser una operación de recursos de clave KMS, es decir, una operación que está autorizada para una clave KMS en particular. Para identificar las operaciones de recursos clave KMS, en laTabla de acciones y recursos, busque un valor de `KMS key` en la columna `Resources` para la operación.

Por ejemplo, la siguiente política de IAM permite a las entidades principales realizar las operaciones de recursos de clave KMS especificadas, pero solo con las claves KMS de la cuenta que se crearon en un almacén de claves personalizado.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyWithoutPlaintext",
    "kms:GenerateDataKeyPair",
    "kms:GenerateDataKeyPairWithoutPlaintext",
    "kms:ReEncrypt*"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "AWS_CLOUDHSM"
    }
  }
```

```
}
```

Véase también

- km: BypassPolicyLockoutSafetyCheck
- kms: KeySpec
- kms: KeyUsage

kms: KeySpec

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:KeySpec`	Cadena	Valor único	`CreateKey` Operaciones de recursos de claves KMS	Políticas de IAM Políticas de claves y políticas de IAM

La clave de condición `kms:KeySpec` controla el acceso a las operaciones en función del valor de la propiedad `KeySpec` de clave KMS creada por la operación o utilizada en ella.

Puede utilizar esta clave de condición en una política de IAM para controlar el acceso a la CreateKeyoperación en función del valor del KeySpecparámetro de una `CreateKey` solicitud. Por ejemplo, puede utilizar esta condición para permitir a los usuarios crear solo claves KMS de cifrado simétricas o solo claves KMS HMAC.

El siguiente ejemplo la declaración de política de IAM utiliza la clave de condición `kms:KeySpec` para permitir a las entidades principales crear solo claves KMS asimétricas RSA. El permiso solo es válido cuando el `KeySpec` en la solicitud comienza con `RSA_`.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
```

```
    "StringLike": {
      "kms:KeySpec": "RSA_*"
    }
  }
}
```

También puede utilizar la clave de condición `kms:KeySpec` para controlar el acceso a las operaciones que utilizan o administran una clave de KMS en función de la propiedad `KeySpec` de la clave de KMS utilizada para la operación. La operación debe ser una operación de recursos de clave KMS, es decir, una operación que está autorizada para una clave KMS en particular. Para identificar las operaciones de recursos clave de KMS, en la tabla de acciones y recursos, busque un valor de `KMS key` en la columna `Resources` para la operación.

Por ejemplo, la siguiente política de IAM permite a las entidades principales realizar las operaciones de recursos de clave KMS especificadas, pero solo con las claves KMS de cifrado simétricas de la cuenta.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:KeySpec": "SYMMETRIC_DEFAULT"
    }
  }
}
```

Véase también

- km: BypassPolicyLockoutSafetyCheck
- kms: CustomerMasterKeySpec (obsoleto)
- km: DataKeyPairSpec
- kms: KeyOrigin
- kms: KeyUsage

kms: KeyUsage

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:KeyUsage`	Cadena	Valor único	`CreateKey` Operaciones de recursos de claves KMS	Políticas de IAM Políticas de claves y políticas de IAM

La clave de condición `kms:KeyUsage` controla el acceso a las operaciones en función del valor de la propiedad `KeyUsage` de clave KMS creada por la operación o utilizada en ella.

Puede utilizar esta clave de condición para controlar el acceso a la CreateKeyoperación en función del valor del KeyUsageparámetro de la solicitud. Los valores válidos para `KeyUsage` son `ENCRYPT_DECRYPT`, `SIGN_VERIFY` y `GENERATE_VERIFY_MAC`.

Por ejemplo, puede crear una clave KMS solo cuando `KeyUsage` sea `ENCRYPT_DECRYPT` o denegar un permiso de usuario cuando `KeyUsage` sea `SIGN_VERIFY`.

En el siguiente ejemplo la declaración de política de IAM utiliza la clave de condición `kms:KeyUsage` para crear una clave KMS solo cuando `KeyUsage` sea `ENCRYPT_DECRYPT`.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:KeyUsage": "ENCRYPT_DECRYPT"
    }
  }
}
```

También puede utilizar la clave de condición `kms:KeyUsage` para controlar el acceso a las operaciones que utilizan o administran una clave KMS en función de la propiedad `KeyUsage` de la clave KMS utilizada para la operación. La operación debe ser una operación de recursos de clave

KMS, es decir, una operación que está autorizada para una clave KMS en particular. Para identificar las operaciones de recursos clave KMS, en laTabla de acciones y recursos, busque un valor de `KMS key` en la columna `Resources` para la operación.

Por ejemplo, la siguiente política de IAM permite a las entidades principales realizar las operaciones de recursos de clave KMS especificadas, pero solo con las claves KMS de la cuenta que se utilizan para la firma y la verificación.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey",
    "kms:GetPublicKey",
    "kms:ScheduleKeyDeletion"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:KeyUsage": "SIGN_VERIFY"
    }
  }
}
```

Véase también

- km: BypassPolicyLockoutSafetyCheck
- kms: CustomerMasterKeyUsage (obsoleto)
- kms: KeyOrigin
- kms: KeySpec

km: MacAlgorithm

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:MacAlgorithm`	Cadena	Valor único	`GenerateMac` `VerifyMac`	Políticas de claves y políticas de IAM

Puede utilizar la clave de `kms:MacAlgorithm` condición para controlar el acceso a las VerifyMacoperaciones GenerateMacy en función del valor del `MacAlgorithm` parámetro de la solicitud.

El siguiente ejemplo de política de claves permite a los usuarios que pueden asumir el rol de `testers` utilizar la clave KMS HMAC para generar y verificar etiquetas HMAC solo cuando el algoritmo MAC de la solicitud es `HMAC_SHA_384` o `HMAC_SHA_512`. Esta política utiliza dos declaraciones de políticas independientes, cada una con su propia condición. Si especifica más de un algoritmo MAC en una única declaración de condición, la condición requiere ambos algoritmos, en lugar de uno u otro.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/testers"
      },
      "Action": [
        "kms:GenerateMac",
        "kms:VerifyMac"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:MacAlgorithm": "HMAC_SHA_384"
        }
      }
```

```
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/testers"
      },
      "Action": [
        "kms:GenerateMac",
        "kms:VerifyMac"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:MacAlgorithm": "HMAC_SHA_512"
        }
      }
    }
  ]
}
```

Véase también

- the section called “km: EncryptionAlgorithm”
- km: SigningAlgorithm

km: MessageType

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:MessageType`	Cadena	Valor único	`Sign` `Verify`	Políticas de claves y políticas de IAM

La clave de condición `kms:MessageType` controla el acceso a las operaciones Sign y Verify en función del valor del parámetro `MessageType` de la solicitud. Los valores válidos para `MessageType` son `RAW` y `DIGEST`.

Por ejemplo, la siguiente declaración de política de claves utiliza la clave de condición `kms:MessageType` para utilizar una clave KMS asimétrica para firmar un mensaje, pero no un resumen de mensajes.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:Sign",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:MessageType": "RAW"
    }
  }
}
```

Véase también

- the section called “km: SigningAlgorithm”

km: MultiRegion

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:MultiRegion`	Booleano	Valor único	`CreateKey` Operaciones de recursos de claves KMS	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para permitir operaciones solo en claves de una región o solo en claves de varias regiones. La clave de `kms:MultiRegion` condición controla el acceso a AWS KMS las operaciones en las claves de KMS y a la CreateKeyoperación en función del valor de la

`MultiRegion` propiedad de la clave de KMS. Los valores válidos son `true` (de varias regiones) y `false` (de una sola región). Todas las claves KMS tienen una propiedad `MultiRegion`.

El siguiente ejemplo la declaración de política de IAM utiliza la clave de condición `kms:MultiRegion` para permitir a las entidades principales crear solo claves de una sola región.

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:MultiRegion": false
    }
  }
}
```

kms: MultiRegionKeyType

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:MultiRegionKeyType`	Cadena	Valor único	`CreateKey` Operaciones de recursos de claves KMS	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para permitir operaciones solo en claves principales de varias regiones o solo en claves de réplicas de varias regiones. La clave de `kms:MultiRegionKeyType` condición controla el acceso a AWS KMS las operaciones en las claves de KMS y la CreateKeyoperación en función de la `MultiRegionKeyType` propiedad de la clave de KMS. Los valores válidos son `PRIMARY` y `REPLICA`. Solo las claves de varias regiones tienen una propiedad `MultiRegionKeyType`.

Normalmente, utilice la clave de condición `kms:MultiRegionKeyType` en una política de IAM para controlar el acceso a varias claves KMS. Sin embargo, dado que una clave de varias regiones puede cambiar a principal o réplica, es posible que desee utilizar esta condición en una política de clave

para permitir una operación solo cuando la clave de varias regiones concreta sea una clave principal o de réplica.

Por ejemplo, la siguiente declaración de política de IAM utiliza la clave de condición `kms:MultiRegionKeyType` para permitir que las principales entidades programen y cancelen la eliminación de claves solo en claves de réplica de varias regiones en la Cuenta de AWS especificada.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "arn:aws:kms:*:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:MultiRegionKeyType": "REPLICA"
    }
  }
}
```

Para permitir o denegar el acceso a todas las claves de varias regiones, puede usar ambos valores o un valor nulo con `kms:MultiRegionKeyType`. Sin embargo, se recomienda utilizar la clave de MultiRegion condición kms: para ello.

kms: PrimaryRegion

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:PrimaryRegion`	Cadena (lista)	Valor único	`UpdatePrimaryRegion`	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para limitar las regiones de destino de una UpdatePrimaryRegionoperación. Estas son las Regiones de AWS que pueden alojar las claves principales de varias regiones.

La clave de `kms:PrimaryRegion` condición controla el acceso a la UpdatePrimaryRegionoperación en función del valor del `PrimaryRegion` parámetro. El `PrimaryRegion` parámetro especifica la clave Región de AWS de réplica multirregional que se va a convertir en principal. El valor de la condición es uno o más Región de AWS nombres, como `us-east-1` o`ap-southeast-2`, o patrones de nombres de regiones, como `eu-*`

Por ejemplo, la siguiente declaración de política utiliza la clave de condición `kms:PrimaryRegion` para permitir que las entidades principales actualicen la región principal de una clave de varias regiones a una de las cuatro regiones especificadas.

```
{
  "Effect": "Allow",
  "Action": "kms:UpdatePrimaryRegion",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Developer"
  },
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:PrimaryRegion": [
         "us-east-1",
         "us-west-2",
         "eu-west-3",
         "ap-southeast-2"
      ]
    }
  }
}
```

km: ReEncryptOnSameKey

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:ReEncryptOnSameKey`	Booleano	Valor único	`ReEncrypt`	Políticas de claves y políticas de IAM

Puede usar esta clave de condición para controlar el acceso a la ReEncryptoperación en función de si la solicitud especifica una clave KMS de destino que sea la misma que se utilizó para el cifrado original.

Por ejemplo, la siguiente declaración de política de clave utiliza la clave de condición `kms:ReEncryptOnSameKey` para volver a cifrar únicamente cuando la clave KMS de destino sea la misma que se utilizó para el cifrado original.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:ReEncrypt*",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:ReEncryptOnSameKey": true
    }
  }
}
```

kms: RequestAlias

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:RequestAlias`	Cadena (lista)	Valor único	Operaciones criptográficas DescribeKey GetPublicKey	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para permitir una operación solo cuando la solicitud utiliza un alias determinado para identificar la clave KMS. La clave de condición `kms:RequestAlias` controla el acceso a una clave KMS utilizada en una operación criptográfica, `GetPublicKey`, o bien `DescribeKey` en función del alias que identifica esa clave KMS en la solicitud. (Esta condición de

política no afecta a la GenerateRandomoperación porque la operación no utiliza una clave o alias de KMS).

Esta condición admite el control de acceso basado en atributos (ABAC) AWS KMS, que permite controlar el acceso a las claves de KMS en función de las etiquetas y los alias de una clave de KMS. Puede utilizar etiquetas y alias para permitir o denegar el acceso a una clave KMS sin cambiar las políticas o las concesiones. Para obtener más detalles, consulte ABAC para AWS KMS.

Para especificar el alias en esta condición de política, utilice un nombre del alias, como, por ejemplo, `alias/project-alpha`, o un patrón de nombre de alias, como `alias/*test*`. No puede especificar una ARN de alias en el valor de esta clave de condición.

Para satisfacer esta condición, el valor del parámetro `KeyId` de la solicitud debe tener un nombre de alias o ARN de alias coincidente. Si la solicitud utiliza un identificador de clave diferente, no cumple con la condición, incluso si identifica la misma clave KMS.

Por ejemplo, la siguiente declaración de política clave permite al director llamar a la GenerateDataKeyoperación mediante la clave KMS. Sin embargo, esto solo está permitido cuando el valor del parámetro `KeyId` de la solicitud es `alias/finance-key` o un ARN de alias con ese nombre de alias, como por ejemplo `arn:aws:kms:us-west-2:111122223333:alias/finance-key`.

```
{
  "Sid": "Key policy using a request alias condition",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/developer"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:RequestAlias": "alias/finance-key"
    }
  }
}
```

No puede usar esta clave de condición para controlar el acceso a las operaciones de alias, como CreateAliaso DeleteAlias. Para obtener más información sobre cómo controlar el acceso a operaciones de alias, consulte Control del acceso a alias.

km: ResourceAliases

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:ResourceAliases`	Cadena (lista)	Multivalor	Operaciones de recursos de claves KMS	Solo políticas de IAM

Utilice esta clave de condición para controlar el acceso a una clave KMS según los alias que estén asociados a la clave KMS. La operación debe ser una operación de recursos de clave KMS, es decir, una operación que está autorizada para una clave KMS en particular. Para identificar las operaciones de recursos clave de KMS, en la tabla de acciones y recursos, busque un valor de `KMS key` en la columna `Resources` para la operación.

Esta condición admite el control de acceso basado en atributos (ABAC) en AWS KMS. Con ABAC, puede controlar el acceso a las claves KMS en función de las etiquetas asignadas a una clave KMS y los alias asociados a una clave KMS. Puede utilizar etiquetas y alias para permitir o denegar el acceso a una clave KMS sin cambiar las políticas o las concesiones. Para obtener más detalles, consulte ABAC para AWS KMS.

El alias debe ser único en una región Cuenta de AWS y, pero esta condición le permite controlar el acceso a varias claves de KMS de la misma región (mediante el operador de `StringLike` comparación) o a varias claves Regiones de AWS de KMS en distintas cuentas.

> **Note**
>
> La ResourceAliases condición kms: solo entra en vigor cuando la clave KMS se ajusta a la cuota de alias por clave de KMS. Si una clave KMS supera esta cuota, las entidades principales que están autorizadas a usar la clave KMS mediante la condición `kms:ResourceAliases` se deniega el acceso a la clave KMS.

Para especificar el alias en esta condición de política, utilice un nombre del alias, como, por ejemplo, `alias/project-alpha`, o un patrón de nombre de alias, como `alias/*test*`. No puede especificar una ARN de alias en el valor de esta clave de condición. Para satisfacer la condición, la

clave KMS utilizada en la operación debe tener el alias especificado. No importa si la clave KMS se identifica o cómo se identifica en la solicitud de la operación.

Se trata de una clave de condición multivalor que compara el conjunto de alias asociado a una clave KMS con el conjunto de alias de la política. Para determinar cómo se comparan estos conjuntos, debe proporcionar un operador de conjuntos `ForAnyValue` o `ForAllValues` en la condición de política. Para conocer los detalles sobre los operadores de conjuntos, consulte Uso de múltiples claves y valores en la Guía del usuario de IAM.

- ForAnyValue: Al menos un alias asociado a la clave de KMS debe coincidir con un alias de la condición de la política. Se permiten otros alias. Si la clave KMS no tiene alias, la condición no se cumple.
- ForAllValues: Todos los alias asociados a la clave de KMS deben coincidir con un alias de la política. Este operador de conjuntos limita los alias asociados con la clave KMS a los que se encuentran en la condición de política. No requiere ningún alias, pero prohíbe los alias no especificados.

Por ejemplo, la siguiente declaración de política de IAM permite al director llamar a la GenerateDataKeyoperación desde cualquier clave de KMS especificada Cuenta de AWS que esté asociada al `finance-key` alias. (Las políticas de clave de las claves KMS afectadas también deben permitir que la cuenta de la entidad principal las utilice para esta operación.) Para indicar que la condición se cumple cuando uno de los muchos alias que podrían estar asociados con la clave KMS es `alias/finance-key`, la condición utiliza el operador de conjuntos `ForAnyValue`.

Ya que la condición `kms:ResourceAliases` se basa en el recurso, no en la solicitud, se realiza con éxito una llamada a `GenerateDataKey` para cualquier clave KMS asociada con el alias `finance-key`, incluso si la solicitud utiliza un ID de clave o ARN de clave para identificar la clave KMS.

```
{
  "Sid": "AliasBasedIAMPolicy",
  "Effect": "Allow",
  "Action": "kms:GenerateDataKey",
  "Resource": [
    "arn:aws:kms:*:111122223333:key/*",
    "arn:aws:kms:*:444455556666:key/*"
  ],
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:ResourceAliases": "alias/finance-key"
```

```
    }
  }
}
```

El siguiente ejemplo de declaración de política de IAM permite que la principal entidad habilite y deshabilite las claves KMS, pero solo cuando todos los alias de las claves KMS incluyen “`Test`“. Esta declaración de política utiliza dos condiciones. La condición con el operador de conjuntos `ForAllValues` requiere que todos los alias asociados con la clave KMS incluyan “Test” (Prueba). La condición con el operador de conjuntos `ForAnyValue` requiere que la clave KMS tenga al menos un alias con “Test” (Prueba). Sin la condición `ForAnyValue`, esta declaración de política habría permitido a la entidad principal utilizar claves KMS que no tenían alias.

```
{
  "Sid": "AliasBasedIAMPolicy",
  "Effect": "Allow",
  "Action": [
    "kms:EnableKey",
    "kms:DisableKey"
  ],
  "Resource": "arn:aws:kms:*:111122223333:key/*",
  "Condition": {
    "ForAllValues:StringLike": {
      "kms:ResourceAliases": [
        "alias/*Test*"
      ]
    },
    "ForAnyValue:StringLike": {
      "kms:ResourceAliases": [
        "alias/*Test*"
      ]
    }
  }
}
```

kms: ReplicaRegion

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:ReplicaRegion`	Cadena (lista)	Valor único	`ReplicateKey`	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para limitar el número de Regiones de AWS veces que un principal puede replicar una clave multirregional. La clave de `kms:ReplicaRegion` condición controla el acceso a la ReplicateKeyoperación en función del valor del ReplicaRegionparámetro de la solicitud. Este parámetro especifica la Región de AWS para la nueva clave de réplica.

El valor de la condición es uno o más Región de AWS nombres, como `us-east-1` o`ap-southeast-2`, o patrones de nombres, como`eu-*`. Para obtener una lista de los nombres de Regiones de AWS esos AWS KMS soportes, consulte los AWS Key Management Service puntos finales y las cuotas en. Referencia general de AWS

Por ejemplo, la siguiente declaración de política clave utiliza la clave de `kms:ReplicaRegion` condición para permitir que los directores llamen a la ReplicateKeyoperación solo cuando el valor del `ReplicaRegion` parámetro es una de las regiones especificadas.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Administrator"
  },
  "Action": "kms:ReplicateKey"
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ReplicaRegion": [
         "us-east-1",
         "eu-west-3",
         "ap-southeast-2"
      ]
    }
```

```
  }
}
```

Esta clave de condición controla el acceso únicamente a la ReplicateKeyoperación. Para controlar el acceso a la UpdatePrimaryRegionoperación, utilice la clave de PrimaryRegion condición kms:.

km: RetiringPrincipal

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:RetiringPrincipal`	Cadena (lista)	Valor único	`CreateGrant`	Políticas de claves y políticas de IAM

Puede utilizar esta clave de condición para controlar el acceso a la CreateGrantoperación en función del valor del RetiringPrincipalparámetro de la solicitud. Por ejemplo, puede crear concesiones para utilizar una clave KMS cuando el `RetiringPrincipal` de la solicitud `CreateGrant` coincida con el `RetiringPrincipal` de la declaración de la condición.

Para especificar el principal que se retira, utilice el nombre de recurso de Amazon (ARN) de AWS un principal. Entre los principales válidos se incluyen los usuarios de IAM Cuentas de AWS, los roles de IAM, los usuarios federados y los usuarios con roles asumidos. Para obtener ayuda con la sintaxis del ARN de un principal, consulte los ARN de IAM en la Guía del usuario de IAM.

El siguiente ejemplo de declaración de política clave permite a un usuario crear concesiones para la clave de KMS. La clave de `kms:RetiringPrincipal` condición restringe el permiso a `CreateGrant` las solicitudes en las que el principal de la concesión que se retira es el. `LimitedAdminRole`

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
```

```
    "StringEquals": {
      "kms:RetiringPrincipal": "arn:aws:iam::111122223333:role/LimitedAdminRole"
    }
  }
}
```

Véase también

- kms: GrantConstraintType
- km: GrantIsFor AWSResource
- kms: GrantOperations
- km: GranteePrincipal

km: RotationPeriodInDays

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:RotationPeriodInDays`	Numérico	Valor único	`EnableKeyRotation`	Políticas de claves y políticas de IAM

Puede usar esta clave de condición para limitar los valores que los directores pueden especificar en el `RotationPeriodInDays` parámetro de una EnableKeyRotationsolicitud.

`RotationPeriodInDays`Especifica el número de días entre cada fecha de rotación automática de claves. AWS KMS permite especificar un período de rotación de entre 90 y 2560 días, pero puede utilizar la clave de `kms:RotationPeriodInDays` condición para restringir aún más el período de rotación, por ejemplo, imponiendo un período de rotación mínimo dentro del rango válido.

Por ejemplo, la siguiente declaración de política clave utiliza la clave de `kms:RotationPeriodInDays` condición para impedir que los directores habiliten la rotación de claves si el período de rotación es inferior o igual a 180 días.

```
{
  "Effect": "Deny",
```

```
  "Action": "kms:EnableKeyRotation",
  "Principal": "*",
  "Resource": "*",
  "Condition" : {
      "NumericLessThanEquals" : {
        "kms:RotationPeriodInDays" : "180"
      }
  }
}
```

km: ScheduleKeyDeletionPendingWindowInDays

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:ScheduleKeyDeletionPendingWindowInDays`	Numérico	Valor único	`ScheduleKeyDeletion`	Políticas de claves y políticas de IAM

Puede usar esta clave de condición para limitar los valores que los directores pueden especificar en el `PendingWindowInDays` parámetro de una ScheduleKeyDeletionsolicitud.

`PendingWindowInDays`Especifica el número de días que deben AWS KMS transcurrir antes de eliminar una clave. AWS KMS permite especificar un período de espera de entre 7 y 30 días, pero puede usar la clave de `kms:ScheduleKeyDeletionPendingWindowInDays` condición para restringir aún más el período de espera, por ejemplo, imponiendo un período de espera mínimo dentro del rango válido.

Por ejemplo, la siguiente declaración de política de claves utiliza la clave de condición `kms:ScheduleKeyDeletionPendingWindowInDays` para impedir que las entidades principales programen la eliminación de claves si el periodo de espera es inferior o igual a 21 días.

```
{
  "Effect": "Deny",
  "Action": "kms:ScheduleKeyDeletion",
  "Principal": "*",
```

```
  "Resource": "*",
  "Condition" : {
      "NumericLessThanEquals" : {
        "kms:ScheduleKeyDeletionPendingWindowInDays" : "21"
      }
  }
}
```

km: SigningAlgorithm

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:SigningAlgorithm`	Cadena	Valor único	`Sign` `Verify`	Políticas de claves y políticas de IAM

Puede usar la clave de `kms:SigningAlgorithm` condición para controlar el acceso a las operaciones de firma y verificación en función del valor del SigningAlgorithmparámetro de la solicitud. Esta clave de condición no afecta a las operaciones realizadas fuera de AWS KMS, como la verificación de firmas con la clave pública en un par de claves KMS asimétricas fuera de. AWS KMS

La siguiente política de claves de ejemplo permite a los usuarios que puedan asumir el rol `testers` utilizar la clave KMS para firmar mensajes solo cuando el algoritmo de firma utilizado para la solicitud sea un algoritmo RSASSA_PSS, como `RSASSA_PSS_SHA512`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/testers"
  },
  "Action": "kms:Sign",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:SigningAlgorithm": "RSASSA_PSS*"
    }
  }
```

```
}
```

Véase también

- km: EncryptionAlgorithm
- the section called “km: MacAlgorithm”
- the section called “km: MessageType”

kms: ValidTo

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:ValidTo`	Timestamp	Valor único	`ImportKeyMaterial`	Políticas de claves y políticas de IAM

La clave de `kms:ValidTo` condición controla el acceso a la ImportKeyMaterialoperación en función del valor del ValidToparámetro de la solicitud, que determina cuándo caduca el material clave importado. El valor se expresa en tiempo Unix.

De forma predeterminada, el parámetro `ValidTo` es obligatorio en las solicitudes `ImportKeyMaterial`. Sin embargo, si el valor del ExpirationModelparámetro es`KEY_MATERIAL_DOES_NOT_EXPIRE`, no es válido. `ValidTo` También puede usar la clave de ExpirationModel condición kms: para requerir el `ExpirationModel` parámetro o un valor de parámetro específico.

La siguiente declaración de política de ejemplo permite a un usuario importar material de claves en una clave KMS. La clave de condición `kms:ValidTo` limita el permiso a las solicitudes `ImportKeyMaterial` en las que el valor `ValidTo` sea menor o igual que `1546257599.0` (31 de diciembre de 2018 11:59:59 p. m.).

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
```

```
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "NumericLessThanEquals": {
      "kms:ValidTo": "1546257599.0"
    }
  }
}
```

Véase también

- km: ExpirationModel
- km: WrappingAlgorithm
- km: WrappingKeySpec

kms: ViaService

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:ViaService`	Cadena	Valor único	Operaciones de recursos de claves KMS	Políticas de claves y políticas de IAM

La clave de `kms:ViaService` condición limita el uso de una clave KMS a las solicitudes de AWS servicios específicos. Puede especificar uno o varios servicios en cada clave de condición `kms:ViaService`. La operación debe ser una operación de recursos de clave KMS, es decir, una operación que está autorizada para una clave KMS en particular. Para identificar las operaciones de recursos clave KMS, en laTabla de acciones y recursos, busque un valor de `KMS key` en la columna `Resources` para la operación.

Por ejemplo, la siguiente declaración de una política de claves utiliza la clave de condición `kms:ViaService` para permitir que se use una clave administrada por el cliente para las acciones especificadas solo cuando la solicitud provenga de Amazon EC2 o Amazon RDS en la región EE. UU. Oeste (Oregón) en nombre de `ExampleRole`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": [
        "ec2.us-west-2.amazonaws.com",
        "rds.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

También puede utilizar un clave de condición `kms:ViaService` para denegar permisos para usar una clave KMS cuando la solicitud provenga de determinados servicios. Por ejemplo, la siguiente declaración de una política de claves utiliza una clave de condición `kms:ViaService` para impedir que se utilice una clave administrada por el cliente para las operaciones `Encrypt` cuando la solicitud provenga de AWS Lambda en nombre de `ExampleRole`.

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
```

```
      "kms:ViaService": [
          "lambda.us-west-2.amazonaws.com"
      ]
    }
  }
}
```

> **Important**
>
> Cuando se utiliza la clave de condición `kms:ViaService`, el servicio realiza la solicitud en nombre de una entidad principal de la Cuenta de AWS. Estas entidades principales deben tener los siguientes permisos:
>
> - Permiso para usar la clave KMS. La entidad principal debe conceder estos permisos al servicio integrado para que pueda utilizar la clave administrada por el cliente en nombre de la entidad principal. Para obtener más información, consulte Cómo los servicios de AWS usan AWS KMS.
> - Permiso para utilizar el servicio integrado. Para obtener más información sobre cómo dar a los usuarios acceso a un AWS servicio que se integra con él AWS KMS, consulte la documentación del servicio integrado.

Todas las Claves administradas por AWS utilizan una clave de condición `kms:ViaService` incluida en su documento de política de claves. Esta condición permite que solo se utilice la clave KMS para las solicitudes que proceden del servicio que ha creado la clave KMS. Para ver la política clave de un Clave administrada de AWS, utilice la GetKeyPolicyoperación.

La clave de condición `kms:ViaService` es válida en IAM y las declaraciones de políticas de clave. Los servicios que especifique deben estar integrados con AWS KMS y admitir la clave de condición `kms:ViaService`.

Servicios que admiten la clave de condición **`kms:ViaService`**

En la siguiente tabla se enumeran AWS los servicios que están integrados con la clave de `kms:ViaService` condición en las claves administradas por el cliente AWS KMS y que permiten su uso. Es posible que los servicios de esta tabla no estén disponibles en todas las regiones. Utilice el `.amazonaws.com` sufijo del AWS KMS ViaService nombre en todas las AWS particiones.

> **Note**
>
> Es posible que deba desplazarse horizontal o verticalmente para ver todos los datos de esta tabla.

Nombre del servicio	AWS KMS ViaService nombre
AWS App Runner	`apprunner.` *`AWS_region`* `.amazonaws.com`
AWS AppFabric	`appfabric.` *`AWS_region`* `.amazonaws.com`
Amazon AppFlow	`appflow.`*`AWS_region`* `.amazonaws.com`
AWS Application Migration Service	`mgn.`*`AWS_region`* `.amazonaws.com`
Amazon Athena	`athena.`*`AWS_region`* `.amazonaws.com`
AWS Audit Manager	`auditmanager.` *`AWS_region`* `.amazonaws.com`
Amazon Aurora	`rds.`*`AWS_region`* `.amazonaws.com`
AWS Backup	`backup.`*`AWS_region`* `.amazonaws.com`
AWS Backup Gateway	`backup-gateway.` *`AWS_region`* `.amazonaws.com`
Amazon Chime SDK	`chimevoiceconnector.` *`AWS_region`* `.amazonaws.com`
AWS CodeArtifact	`codeartifact.` *`AWS_region`* `.amazonaws.com`
CodeGuru Revisor de Amazon	`codeguru-reviewer.` *`AWS_region`* `.amazonaws.com`

Nombre del servicio	AWS KMS ViaService nombre
Amazon Comprehend	`comprehend.` *`AWS_region`* `.amazonaws.com`
Amazon Connect	`connect.`*`AWS_region`* `.amazonaws.com`
Perfiles de clientes de Amazon Connect	`profile.`*`AWS_region`* `.amazonaws.com`
Amazon Q in Connect	`wisdom.`*`AWS_region`* `.amazonaws.com`
AWS Database Migration Service (AWS DMS)	`dms.`*`AWS_region`* `.amazonaws.com`
AWS Directory Service	`directoryservice.` *`AWS_region`* `.amazonaws.com`
Amazon DynamoDB	`dynamodb.` *`AWS_region`* `.amazonaws.com`
Amazon DocumentDB	`docdb-elastic.` *`AWS_region`* `.amazonaws.com`
Amazon EC2 Systems Manager (SSM)	`ssm.`*`AWS_region`* `.amazonaws.com`
Amazon Elastic Block Store (Amazon EBS)	`ec2.`*`AWS_region`* `.amazonaws.com` (EBS solo)
Amazon Elastic Container Registry (Amazon ECR)	`ecr.`*`AWS_region`* `.amazonaws.com`
Amazon Elastic File System (Amazon EFS)	`elasticfilesystem.` *`AWS_region`* `.amazonaws.com`
Amazon ElastiCache	Incluye ambos ViaService nombres en el valor de la clave de condición: • `elasticache.` *`AWS_region`* `.amazonaws.com` • `dax.`*`AWS_region`* `.amazonaws.com`

Nombre del servicio	AWS KMS ViaService nombre
AWS Elemental MediaTailor	mediatailor. *AWS_region* .amazonaws.com
AWS Resolución de la entidad	entityresolution. *AWS_region* .amazonaws.com
Amazon FinSpace	finspace. *AWS_region* .amazonaws.com
Amazon Forecast	forecast. *AWS_region* .amazonaws.com
Amazon FSx	fsx.*AWS_region* .amazonaws.com
AWS Glue	glue.*AWS_region* .amazonaws.com
AWS Ground Station	groundstation. *AWS_region* .amazonaws.com
Amazon GuardDuty	malware-protection. *AWS_region* .amazonaws.com
AWS HealthLake	healthlake. *AWS_region* .amazonaws.com
AWS IoT SiteWise	iotsitewise. *AWS_region* .amazonaws.com
Amazon Kendra	kendra.*AWS_region* .amazonaws.com
Amazon Keyspaces (para Apache Cassandra)	cassandra. *AWS_region* .amazonaws.com
Amazon Kinesis	kinesis.*AWS_region* .amazonaws.com
Amazon Data Firehose	firehose. *AWS_region* .amazonaws.com

Nombre del servicio	AWS KMS ViaService nombre
Amazon Kinesis Video Streams	kinesisvideo. *AWS_region* .amazonaws.com
AWS Lambda	lambda.*AWS_region* .amazonaws.com
Amazon Lex	lex.*AWS_region* .amazonaws.com
AWS License Manager	license-manager. *AWS_region* .amazonaws.com
Amazon Location Service	geo.*AWS_region* .amazonaws.com
Amazon Lookout for Equipment	lookoutequipment. *AWS_region* .amazonaws.com
Amazon Lookout for Metrics	lookoutmetrics. *AWS_region* .amazonaws.com
Amazon Lookout for Vision	lookoutvision. *AWS_region* .amazonaws.com
Amazon Macie	macie.*AWS_region* .amazonaws.com
AWS Mainframe Modernization	m2.*AWS_region* .amazonaws.com
Amazon Managed Blockchain	managedblockchain. *AWS_region* .amazonaws.com
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	kafka.*AWS_region* .amazonaws.com
Flujos de trabajo administrados por Amazon Managed Workflows for Apache Airflow (MWAA)	airflow.*AWS_region* .amazonaws.com
Amazon MemoryDB para Redis	memorydb. *AWS_region* .amazonaws.com

Nombre del servicio	AWS KMS ViaService nombre
Amazon Monitron	monitron. *AWS_region* .amazonaws.com
Amazon MQ	mq.*AWS_region* .amazonaws.com
Amazon Neptune	rds.*AWS_region* .amazonaws.com
Amazon Nimble Studio	nimble.*AWS_region* .amazonaws.com
AWS HealthOmics	omics.*AWS_region* .amazonaws.com
OpenSearch Servicio Amazon	es.*AWS_region* .amazonaws.com , aoss.*AWS_region* .amazonaws.com
AWS Proton	proton.*AWS_region* .amazonaws.com
Amazon Quantum Ledger Database (Amazon QLDB)	qldb.*AWS_region* .amazonaws.com
Amazon RDS Performance Insights	rds.*AWS_region* .amazonaws.com
Amazon Redshift	redshift. *AWS_region* .amazonaws.com
Editor de consultas de Amazon Redshift V2	sqlworkbench. *AWS_region* .amazonaws.com
Amazon Redshift Serverless	redshift-serverless. *AWS_region* .amazonaws.com
Amazon Rekognition	rekognition. *AWS_region* .amazonaws.com
Amazon Relational Database Service (Amazon RDS)	rds.*AWS_region* .amazonaws.com
Almacén de datos replicados de Amazon	ards.*AWS_region* .amazonaws.com

Nombre del servicio	AWS KMS ViaService nombre
Amazon SageMaker	`sagemaker.` *`AWS_region`* `.amazonaws.com`
AWS Secrets Manager	`secretsmanager.` *`AWS_region`* `.amazonaws.com`
Amazon Security Lake	`securitylake.` *`AWS_region`* `.amazonaws.com`
Amazon Simple Email Service (Amazon SES)	`ses.`*`AWS_region`* `.amazonaws.com`
Amazon Simple Notification Service (Amazon SNS)	`sns.`*`AWS_region`* `.amazonaws.com`
Amazon Simple Queue Service (Amazon SQS)	`sqs.`*`AWS_region`* `.amazonaws.com`
Amazon Simple Storage Service (Amazon S3)	`s3.`*`AWS_region`* `.amazonaws.com`
AWS Snowball	`importexport.` *`AWS_region`* `.amazonaws.com`
AWS Storage Gateway	`storagegateway.` *`AWS_region`* `.amazonaws.com`
AWS Systems Manager Incident Manager	`ssm-incidents.` *`AWS_region`* `.amazonaws.com`
AWS Systems Manager Incident Manager Contactos	`ssm-contacts.` *`AWS_region`* `.amazonaws.com`
Amazon Timestream	`timestream.` *`AWS_region`* `.amazonaws.com`
Amazon Translate	`translate.` *`AWS_region`* `.amazonaws.com`
Acceso verificado de AWS	`verified-access.` *`AWS_region`* `.amazonaws.com`

Nombre del servicio	AWS KMS ViaService nombre
Amazon WorkMail	`workmail.` *`AWS_region`* `.amazonaws.com`
Amazon WorkSpaces	`workspaces.` *`AWS_region`* `.amazonaws.com`
Amazon WorkSpaces Thin Client	`thinclient.` *`AWS_region`* `.amazonaws.com`
Amazon WorkSpaces Web	`workspaces-web.` *`AWS_region`* `.amazonaws.com`
AWS X-Ray	`xray.`*`AWS_region`* `.amazonaws.com`

km: WrappingAlgorithm

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:WrappingAlgorithm`	Cadena	Valor único	`GetParametersForImport`	Políticas de claves y políticas de IAM

Esta clave de condición controla el acceso a la GetParametersForImportoperación en función del valor del WrappingAlgorithmparámetro de la solicitud. Puede utilizar esta condición para exigir que las entidades principales usen un algoritmo para cifrar el material durante el proceso de importación. Las solicitudes de la clave pública y el token de importación necesarios no se realizan cuando especifican un algoritmo de encapsulamiento diferente.

La siguiente declaración de política de clave de ejemplo utiliza la clave de condición `kms:WrappingAlgorithm` para conceder al usuario de ejemplo permiso para llamar a la operación `GetParametersForImport`, pero le impide utilizar el algoritmo de encapsulamiento `RSAES_OAEP_SHA_1`. Cuando `WrappingAlgorithm` en la solicitud `GetParametersForImport` es `RSAES_OAEP_SHA_1`, se produce un error en la operación.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:GetParametersForImport",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:WrappingAlgorithm": "RSAES_OAEP_SHA_1"
    }
  }
}
```

Véase también

- km: ExpirationModel
- kms: ValidTo
- km: WrappingKeySpec

km: WrappingKeySpec

AWS KMS claves de condición	Tipo de condición	Tipo de valor	Operaciones de la API	Tipo de política
`kms:WrappingKeySpec`	Cadena	Valor único	`GetParametersForImport`	Políticas de claves y políticas de IAM

Esta clave de condición controla el acceso a la GetParametersForImportoperación en función del valor del WrappingKeySpecparámetro de la solicitud. Puede utilizar esta condición para exigir que las entidades principales usen un determinado tipo de clave pública durante el proceso de importación. Si la solicitud especifica un tipo de clave diferente, produce un error.

Como el único valor válido del parámetro `WrappingKeySpec` es `RSA_2048`, al impedir que los usuarios utilicen este valor, se evita que utilicen la operación `GetParametersForImport`.

En el ejemplo siguiente, la declaración de la política utiliza la clave de condición `kms:WrappingAlgorithm` para requerir que el parámetro `WrappingKeySpec` de la solicitud sea `RSA_4096`.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:GetParametersForImport",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:WrappingKeySpec": "RSA_4096"
    }
  }
}
```

Véase también

- km: ExpirationModel
- kms: ValidTo
- km: WrappingAlgorithm

AWS KMS claves de condición para AWS Nitro Enclaves

AWS Nitro Enclaves es una funcionalidad de Amazon EC2 que le permite crear entornos informáticos aislados denominados enclaves para proteger y procesar datos altamente confidenciales. AWS KMS proporciona claves de condición para admitir Nitro Enclaves. AWS Estas claves de condiciones solo son válidas para las solicitudes de un AWS KMS Nitro Enclave.

Al llamar a las operaciones de descifrado GenerateDataKeyGenerateDataKeyPair, o GenerateRandomAPI con el documento de certificación firmado desde un enclave, estas API cifran el texto sin formato de la respuesta con la clave pública del documento de certificación y devuelven texto cifrado en lugar de texto sin formato. Este texto cifrado solo se puede descifrar con la clave privada del enclave. Para obtener más información, consulte ¿Cómo AWS Nitro Enclaves utiliza AWS KMS?.

Las siguientes claves de condición permiten limitar los permisos para estas operaciones en función del contenido del documento de conformidad firmado. Antes de permitir una operación, AWS KMS compara el documento de certificación del enclave con los valores de estas claves de condición. AWS KMS

km: 384 RecipientAttestation ImageSha

AWS KMS Claves de estado	Tipo de condición	Tipo de valor	Operaciones de API	Tipo de política

`kms:RecipientAttestation:ImageSha384`	Cadena	Valor único	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Políticas de claves y políticas de IAM

La clave de condición `kms:RecipientAttestation:ImageSha384` controla el acceso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` y `GenerateRandom` con una clave de KMS cuando el resumen de la imagen del documento de certificación firmado de la solicitud coincide con el valor de la clave de condición. El valor `ImageSha384` corresponde a PCR0 en el documento de certificación. Esta clave de condición solo entra en vigor cuando el `Recipient` parámetro de la solicitud especifica un documento de certificación firmado para un enclave de AWS Nitro.

Este valor también se incluye en los CloudTraileventos relacionados con las solicitudes de enclaves de AWS KMS Nitro.

> **Note**
>
> Esta clave de condición es válida en las declaraciones de política de claves y en las declaraciones de política de IAM aunque no aparezca en la consola de IAM ni en la Referencia de autorizaciones de servicio de IAM.

Por ejemplo, la siguiente declaración de política clave permite al `data-processing` rol usar la clave KMS para las operaciones de descifrado GenerateDataKeyGenerateDataKeyPair, y. GenerateRandom La clave de condición `kms:RecipientAttestation:ImageSha384` permite las operaciones solo cuando el valor de resumen de imagen (PCR0) del documento de certificación en la solicitud coincida con el valor de resumen de imagen de la condición. Esta clave de condición solo entra en vigor cuando el `Recipient` parámetro de la solicitud especifica un documento de certificación firmado para un AWS enclave de Nitro.

Si la solicitud no incluye un documento de certificación válido de un enclave de AWS Nitro, se deniega el permiso porque no se cumple esta condición.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyPair",
    "kms:GenerateRandom"
  ],
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:ImageSha384":
 "9fedcba8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdef2abcdef3a
    }
  }
}
```

kms ::PCR RecipientAttestation <PCR_ID>

AWS KMS Claves de condición	Tipo de condición	Tipo de valor	Operaciones de API	Tipo de política

`kms:RecipientAttestation:PCR<PCR_ID>`	Cadena	Valor único	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Políticas de claves y políticas de IAM

La clave de condición `kms:RecipientAttestation:PCR<PCR_ID>` controla el acceso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` y `GenerateRandom` con una clave de KMS solo cuando los registros de configuración de la plataforma (PCR) del documento de certificación firmado en la solicitud coincidan con el valor de la clave de condición. Esta clave de condición solo entra en vigor cuando el `Recipient` parámetro de la solicitud especifica un documento de certificación firmado desde un enclave de AWS Nitro.

Este valor también se incluye en los CloudTraileventos que representan solicitudes de acceso a AWS KMS enclaves de Nitro.

> **Note**
>
> Esta clave de condición es válida en las declaraciones de política de claves y en las declaraciones de política de IAM aunque no aparezca en la consola de IAM ni en la Referencia de autorizaciones de servicio de IAM.

Para especificar un valor de PCR, utilice el siguiente formato. Concatene el ID de PCR con el nombre de la clave de condición. El valor de PCR debe ser una cadena hexadecimal en minúsculas de hasta 96 bytes.

```
"kms:RecipientAttestation:PCRPCR_ID": "PCR_value"
```

Por ejemplo, la siguiente clave de condición especifica un valor particular para PCR1, que corresponde al hash del kernel utilizado para el enclave y el proceso de arranque.

```
kms:RecipientAttestation:PCR1:
 "0x1abcdef2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef
```

Por ejemplo, la siguiente declaración de política de claves permite al rol `data-processing` utilizar la clave de KMS para la operación Decrypt.

La clave de condición `kms:RecipientAttestation:PCR` en esta declaración permite la operación solo cuando el valor PCR1 del documento de conformidad firmado en la solicitud coincide con el valor `kms:RecipientAttestation:PCR1` de la condición. Use el operador de política `StringEqualsIgnoreCase` para requerir una comparación entre mayúsculas y minúsculas de los valores de PCR.

Si la solicitud no incluye un documento de certificación, se deniega el permiso porque esta condición no se cumple.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": "kms:Decrypt",
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:PCR1":
 "0x1de4f2dcf774f6e3b679f62e5f120065b2e408dcea327bd1c9dddaea6664e7af79355814748447674530 82c6f15
    }
  }
}
```

ABAC para AWS KMS

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos basados en atributos. AWS KMS admite ABAC al permitirle controlar el acceso a las claves

administradas por el cliente en función de las etiquetas y alias asociados con las claves KMS. Las claves de condición de etiqueta y alias que habilitan ABAC en AWS KMS proporcionan una forma potente y flexible de autorizar a las principales entidades a utilizar claves KMS sin editar políticas ni administrar concesiones. Pero debe usar esta característica con cuidado para que a las principales entidades no se les permita o se les deniegue el acceso inadvertidamente.

Si utiliza ABAC, tenga en cuenta que el permiso para administrar etiquetas y alias es ahora un permiso de control de acceso. Asegúrese de conocer las etiquetas y alias existentes en todas las claves KMS antes de implementar una política que dependa de etiquetas o alias. Tome las precauciones razonables al agregar, eliminar y actualizar alias, y al etiquetar y desetiquetar claves. Otorgue permisos para administrar etiquetas y alias solo a las principales entidades que los necesiten y limite las etiquetas y alias que puedan administrar.

> **Notas**
>
> Cuando se utiliza ABAC para AWS KMS, tenga cuidado al dar permiso a las principales entidades para administrar etiquetas y alias. Cambiar una etiqueta o alias podría permitir o denegar el permiso a una clave KMS. Los administradores de claves que no tienen permiso para cambiar políticas de claves o crear concesiones pueden controlar el acceso a claves KMS si tienen permiso para administrar etiquetas o alias.
>
> Puede que transcurran cinco minutos hasta que los cambios de etiqueta y alias afecten a la autorización de clave KMS. Los cambios recientes pueden ser visibles en las operaciones de API antes de que afecten a la autorización.
>
> Para controlar el acceso a una clave KMS basándose en su alias, debe utilizar una clave de condición. No puede utilizar un alias para representar una clave KMS en el elemento `Resource` de una declaración de política. Cuando aparece un alias en el elemento `Resource`, la declaración de política se aplica al alias, no a la clave KMS asociada.

Más información

- Para conocer detalles sobre la compatibilidad de AWS KMS con ABAC, incluidos ejemplos, consulte Usar alias para controlar el acceso a las claves KMS y Uso de etiquetas para controlar el acceso a las claves KMS.
- Para obtener más información general acerca de cómo utilizar etiquetas para controlar el acceso a AWS, consulte ¿Qué es ABAC para AWS? y Control del acceso a recursos de AWS que utilizan etiquetas de recursos en la Guía del usuario de IAM.

Claves de condición de ABAC para AWS KMS

Para autorizar el acceso a claves KMS en función de sus etiquetas y alias, utilice las siguientes claves de condición en una política de claves o política de IAM.

Clave de condición de ABAC	Descripción	Tipo de política	Operaciones de AWS KMS
leyes: ResourceTag	La etiqueta (clave y valor) en la clave KMS coincide con la etiqueta (clave y valor) o el patrón de etiqueta en la política	Política de IAM únicamente	Operaciones de recursos clave KMS [2]
aws:RequestTag/tag-key	La etiqueta (clave y valor) en la solicitud coincide con la etiqueta (clave y valor) o el patrón de etiqueta en la política	Políticas de claves y políticas de IAM[1]	TagResource, UntagResource
leyes: TagKeys	Las claves de etiqueta de la solicitud coinciden con las claves de etiqueta de la política.	Políticas de claves y políticas de IAM[1]	TagResource, UntagResource
km: ResourceAliases	Los alias asociados a la clave KMS coinciden con los alias o patrones de alias de la política	Política de IAM únicamente	Operaciones de recursos clave KMS [2]
km: RequestAlias	El alias que represent a la clave KMS en la solicitud coincide con	Políticas de clavessss y políticas de IAM[1]	Operaciones criptográficas, DescribeKeyGetPublicKey

Clave de condición de ABAC	Descripción	Tipo de política	Operaciones de AWS KMS
	los patrones de alias o alias de la política.		

[1]Cualquier clave de condición que se pueda utilizar en una política de clave también se puede utilizar en una política de IAM, pero solo si la política de claves lo permite.

[2]Una operación de recursos de clave KMS es una operación autorizada para una clave KMS en particular. Para identificar las operaciones de recursos clave KMS, en la tabla de permisos AWS KMS, busque un valor de la clave KMS en la columna `Resources` para la operación.

Por ejemplo, puede utilizar estas claves de condición para crear las siguientes políticas.

- Una política de IAM con `kms:ResourceAliases` que habilita el permiso para usar claves KMS con un alias o patrón de alias en particular. Esto es un poco diferente de las políticas que se basan en etiquetas: aunque puede usar patrones de alias en una política, cada alias debe ser único en una Cuenta de AWS y región. Esto le permite aplicar una política a un conjunto seleccionado de claves KMS sin enumerar los ARN clave de las claves KMS en la declaración de política. Para agregar o quitar claves KMS del conjunto, cambie el alias de la clave KMS.
- Una política de claves con `kms:RequestAlias` que permite a las principales entidades usar una clave KMS en una operación `Encrypt`, pero solo cuando la solicitud `Encrypt` utiliza ese alias para identificar la clave KMS.
- Una política de IAM con `aws:ResourceTag/`*`tag-key`* que deniega permiso para utilizar claves KMS con una clave de etiqueta y un valor de etiqueta en concreto. Esto le permite aplicar una política a un conjunto seleccionado de claves KMS sin enumerar los ARN clave de las claves KMS en la declaración de política. Para agregar o quitar claves KMS del conjunto, etiqueta o desmarca de la clave KMS.
- Una política de IAM con `aws:RequestTag/`*`tag-key`* que permite a las principales entidades eliminar solo etiquetas de claves KMS de `"Purpose"="Test"`
- Una política de IAM con `aws:TagKeys` que deniega el permiso para etiquetar o desetiquetar una clave KMS con una clave de etiqueta `Restricted`.

ABAC hace que la administración de accesos sea flexible y escalable. Por ejemplo, puede utilizar la clave de condición `aws:ResourceTag/`*`tag-key`* para crear una política de IAM que permita a las

principales entidades utilizar una clave KMS para operaciones especificadas solo cuando la clave KMS tenga una etiqueta `Purpose=Test`. La política se aplica a todas las claves KMS de todas las regiones de la Cuenta de AWS.

Cuando se adjunta a un usuario o rol, la siguiente política de IAM permite a las principales entidades utilizar todas las claves KMS existentes con una etiqueta `Purpose=Test` para las operaciones especificadas. Para proporcionar este acceso a claves KMS nuevas o existentes, no es necesario cambiar la política. Solo tiene que adjuntar la etiqueta `Purpose=Test` a las claves KMS. Del mismo modo, para eliminar este acceso de las claves KMS con una etiqueta `Purpose=Test`, edite o elimine la etiqueta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AliasBasedIAMPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Test"
        }
      }
    }
  ]
}
```

Sin embargo, si utiliza esta función, tenga cuidado al administrar etiquetas y alias. Agregar, cambiar o eliminar una etiqueta o alias puede permitir o denegar inadvertidamente el acceso a una clave KMS. Los administradores de claves que no tienen permiso para cambiar políticas de claves o crear concesiones pueden controlar el acceso a claves KMS si tienen permiso para administrar etiquetas y alias. Para mitigar este riesgo, considere limitar permisos para administrar etiquetas y alias. Por ejemplo, es posible que exija solo las principales entidades administren etiquetas `Purpose=Test`.

Para más detalles, consulte Usar alias para controlar el acceso a las claves KMS y Uso de etiquetas para controlar el acceso a las claves KMS.

¿Etiquetas o alias?

AWS KMS admite ABAC con etiquetas y alias. Ambas opciones proporcionan una estrategia de control de acceso flexible y escalable, pero son ligeramente diferentes entre sí.

Es posible que decida usar etiquetas o alias en función de sus patrones de uso de AWS particulares. Por ejemplo, si ya ha otorgado permisos de etiquetado a la mayoría de los administradores, podría ser más fácil controlar una estrategia de autorización basada en alias. O bien, si está cerca de la cuota de alias por clave KMS, es posible que prefiera una estrategia de autorización basada en etiquetas.

Los siguientes beneficios son de interés general.

Beneficios del control de acceso basado en etiquetas

- Mismo mecanismo de autorización para diferentes tipos de recursos de AWS.

  Puede utilizar la misma etiqueta o clave de etiqueta para controlar el acceso a varios tipos de recursos, como un clúster de Amazon Relational Database Service (Amazon RDS), un volumen de Amazon Elastic Block Store (Amazon EBS) y una clave KMS. Esta función permite varios modelos de autorización diferentes que son más flexibles que el control de acceso basado en roles tradicional.
- Autorizar el acceso a un grupo de claves KMS.

  Puede utilizar etiquetas para administrar el acceso a un grupo de claves KMS en la misma región y Cuenta de AWS. Asigne la misma etiqueta o clave de etiqueta a las claves KMS que elija. A continuación, cree una declaración easy-to-maintain de política sencilla que se base en la etiqueta o la clave de la etiqueta. Para agregar o quitar una clave KMS de su grupo de autorización, agregue o elimine la etiqueta; no necesita editar la política.

Beneficios del control de acceso basado en alias

- Autorizar el acceso a operaciones criptográficas basadas en alias.

  La mayoría de las condiciones políticas de atributos basadas en solicitudes, incluida aws:RequestTag/tag-key, solo afectan a las operaciones que agregan, editan o eliminan el atributo. Sin embargo, la clave de RequestAlias condición kms: controla el acceso a las

operaciones criptográficas en función del alias utilizado para identificar la clave KMS de la solicitud. Por ejemplo, puede concederle permiso a una entidad principal para usar una clave KMS en una operación `Encrypt` pero solo cuando el valor del parámetro `KeyId` sea `alias/restricted-key-1`. Para satisfacer esta condición se requiere todo lo siguiente:

- La clave KMS debe estar asociada a ese alias.
- La solicitud debe utilizar el alias para identificar la clave KMS.
- La entidad principal debe tener permiso para utilizar la clave KMS en función de la condición `kms:RequestAlias`.

Esto resulta especialmente útil si las aplicaciones utilizan comúnmente nombres de alias o ARN de alias para hacer referencia a claves KMS.

- Proporcione permisos muy limitados.

  Un alias debe ser único en una región y Cuenta de AWS. Como resultado, dar acceso a las principales entidades a una clave KMS basada en un alias puede ser mucho más restrictivo que darles acceso basado en una etiqueta. A diferencia de los alias, las etiquetas se pueden asignar a varias claves KMS de la misma cuenta y región. Si lo desea, puede usar un patrón de alias, como `alias/test*`, para dar acceso a las entidades principales a un grupo de claves KMS en la misma cuenta y Región. Sin embargo, permitir o denegar acceso a un alias en concreto permite un control muy estricto de claves KMS.

Solución de problemas de ABAC para AWS KMS

Controlar el acceso a las claves KMS en función de sus etiquetas y alias es conveniente y potente. Sin embargo, es propenso a algunos errores predecibles que querrá evitar.

Acceso cambiado debido al cambio de etiqueta

Si se elimina una etiqueta o se cambia su valor, se denegará el acceso a la clave KMS a las principales entidades que tengan acceso a una clave KMS basada únicamente en esa etiqueta. Esto también puede ocurrir cuando una etiqueta incluida en una declaración de política de denegación se agrega a una clave KMS. Agregar una etiqueta relacionada con la política a una clave KMS puede permitir el acceso a entidades principales a las que se debe denegar el acceso a una clave KMS.

Por ejemplo, supongamos que una entidad principal tiene acceso a una clave KMS basada en la etiqueta `Project=Alpha`, como el permiso proporcionado por la siguiente declaración de política de IAM de ejemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMPolicyWithResourceTag",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:ap-southeast-1:111122223333:key/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "Alpha"
        }
      }
    }
  ]
}
```

Si se elimina la etiqueta de esa clave KMS o se cambia el valor de la etiqueta, la entidad principal ya no tiene permiso para usar la clave KMS para las operaciones especificadas. Esto puede resultar evidente cuando el director intenta leer o escribir datos en un AWS servicio que utiliza una clave gestionada por el cliente. Para rastrear el cambio de etiqueta, revise CloudTrail los registros TagResourceo UntagResource las entradas.

Para restaurar el acceso sin actualizar la política, cambie las etiquetas de la clave KMS. Esta acción tiene un impacto mínimo aparte de un breve período de tiempo mientras está surtiendo efecto a lo largo de AWS KMS. Para evitar un error como este, otorgue permisos de etiquetado y desetiquetado solo a las principales entidades que lo necesiten ylimite sus permisos de etiquetado a las etiquetas que necesitan administrar. Antes de cambiar una etiqueta, busque políticas para detectar el acceso que depende de la etiqueta y obtenga claves KMS en todas las regiones que tengan la etiqueta. Podrías considerar la posibilidad de crear una CloudWatch alarma de Amazon cuando cambies determinadas etiquetas.

Cambio de acceso debido al cambio de alias

Si se elimina un alias o se asocia a una clave KMS diferente, se denegará el acceso a la clave KMS a las principales entidades que tengan acceso a la clave KMS basándose únicamente en ese alias. Esto también puede ocurrir cuando se incluye un alias asociado con una clave KMS en una

declaración de política de denegación. Agregar un alias relacionado con la política a una clave KMS también puede permitir el acceso a entidades principales a las que se debe denegar el acceso a una clave KMS.

Por ejemplo, la siguiente declaración de política de IAM utiliza la clave de ResourceAliases condición kms: para permitir el acceso a las claves de KMS en distintas regiones de la cuenta con cualquiera de los alias especificados.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AliasBasedIAMPolicy",
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:Describe*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "kms:ResourceAliases": [
            "alias/ProjectAlpha",
            "alias/ProjectAlpha_Test",
            "alias/ProjectAlpha_Dev"
          ]
        }
      }
    }
  ]
}
```

Para rastrear el cambio de alias, revise CloudTrail los registros y DeleteAliaslas CreateAliasUpdateAliasentradas.

Para restaurar el acceso sin actualizar la política, cambie el alias asociado con la clave KMS. Dado que cada alias se puede asociar a una sola clave KMS en una cuenta y región, administrar alias es un poco más difícil que administrar etiquetas. Restaurar el acceso a algunas entidades principales en una clave KMS puede denegar el acceso a la misma u otras entidades principales a una clave KMS diferente.

Para evitar este error, otorgue permisos de administración de alias solo a las principales entidades que lo necesiten y limite sus permisos de administración de alias a los alias que necesitan administrar. Antes de actualizar o eliminar un alias, busque políticas para detectar el acceso que depende del alias y busque claves KMS en todas las regiones asociadas al alias.

Acceso denegado debido a la cuota de alias

Los usuarios que estén autorizados a usar una clave de KMS con una ResourceAliases condición de kms: recibirán una `AccessDenied` excepción si la clave de KMS supera los alias predeterminados por cuota de claves de KMS para esa cuenta y región.

Para restaurar el acceso, elimine los alias asociados a la clave KMS para que cumpla con la cuota. O utilice un mecanismo alternativo para dar a los usuarios acceso a la clave KMS.

Cambio de autorización retrasado

Los cambios que realice en las etiquetas y alias pueden tardar hasta cinco minutos en afectar a la autorización de claves KMS. Como resultado, un cambio de etiqueta o alias podría reflejarse en las respuestas de las operaciones de API antes de que afecten a la autorización. Es probable que este retraso sea más largo que el breve retraso de consistencia final que afecta a la mayoría de las operaciones de AWS KMS.

Por ejemplo, puede que tenga una política de IAM que permita a ciertas entidades principales utilizar cualquier clave KMS con una etiqueta `"Purpose"="Test"`. Luego, agrega la etiqueta `"Purpose"="Test"` de una clave KMS. Aunque la TagResourceoperación se complete y la ListResourceTagsrespuesta confirme que la etiqueta está asignada a la clave de KMS, es posible que las entidades principales no tengan acceso a la clave de KMS durante un máximo de cinco minutos.

Para evitar errores, construya este retraso esperado en su código.

Solicitudes fallidas debido a actualizaciones de alias

Cuando se actualiza un alias, se asocia un alias existente con una clave KMS diferente.

El descifrado y ReEncryptlas solicitudes que especifican el nombre del alias o el ARN del alias pueden fallar porque el alias ahora está asociado a una clave KMS que no cifró el texto cifrado. Esta situación normalmente devuelve un `IncorrectKeyException` o `NotFoundException`. O si la solicitud no tiene parámetro `KeyId` o `DestinationKeyId`, la operación puede fallar con la

excepción `AccessDenied` dado que la persona que llama ya no tiene acceso a la clave KMS que cifró el texto cifrado.

Puede rastrear el cambio consultando los CloudTrail registros y las entradas de CreateAliasregistro. UpdateAliasDeleteAlias También puede usar el valor del `LastUpdatedDate` campo en la ListAliasesrespuesta para detectar un cambio.

Por ejemplo, en el siguiente ListAliasesejemplo de respuesta se muestra que se actualizó el `ProjectAlpha_Test` alias de la `kms:ResourceAliases` condición. Como resultado, las principales entidades que tienen acceso basado en el alias pierden el acceso a la clave KMS previamente asociada. En su lugar, tienen acceso a la clave KMS recién asociada.

```
$ aws kms list-aliases --query 'Aliases[?starts_with(AliasName, `alias/ProjectAlpha`)]'

{
    "Aliases": [
        {
            "AliasName": "alias/ProjectAlpha_Test",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/ProjectAlpha_Test",
            "TargetKeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
            "CreationDate": 1566518783.394,
            "LastUpdatedDate": 1605308931.903
        },
        {
            "AliasName": "alias/ProjectAlpha_Restricted",
            "AliasArn": "arn:aws:kms:us-west-2:111122223333:alias/
ProjectAlpha_Restricted",
            "TargetKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
            "CreationDate": 1553410800.010,
            "LastUpdatedDate": 1553410800.010
        }
    ]
}
```

La solución para este cambio no es simple. Puede actualizar el alias nuevamente para asociarlo a la clave KMS original. Sin embargo, antes de actuar, debe considerar el efecto de ese cambio en la clave KMS asociada actualmente. Si las principales entidades utilizan la última clave KMS en operaciones criptográficas, es posible que necesiten acceso continuo a ella. En este caso, es posible que desee actualizar la política para asegurarse de que las principales entidades tienen permiso para usar ambas claves KMS.

Puede evitar un error como el siguiente: antes de actualizar un alias, busque políticas para detectar el acceso que depende del alias. A continuación, obtenga claves KMS en todas las regiones asociadas con el alias. De permisos de administración de alias solo a las principales entidades que lo necesiten y limite sus permisos de administración de alias a los alias que necesitan administrar.

Permitir a los usuarios de otras cuentas utilizar una clave KMS

Puede permitir que los usuarios o roles de una Cuenta de AWS usen una clave KMS en su cuenta. El acceso entre cuentas requiere permiso en la política de claves de la clave KMS y en una política de IAM en la cuenta del usuario externo.

El permiso entre cuentas solo es efectivo para las siguientes operaciones:

- Operaciones criptográficas
- CreateGrant
- DescribeKey
- GetKeyRotationStatus
- GetPublicKey
- ListGrants
- RetireGrant
- RevokeGrant

Si concede a un usuario de otra cuenta permiso para otras operaciones, esos permisos no surten efecto. Por ejemplo, si concedes al principal de una cuenta diferente el ListKeys permiso kms: en una política de IAM, o el ScheduleKeyDeletion permiso kms: en una clave de KMS en una política clave, los intentos del usuario de realizar esas operaciones en tus recursos seguirán fallando.

Para obtener más información sobre el uso de claves KMS en diferentes cuentas para las operaciones AWS KMS, consulte la columna Cross-account use (Uso entre cuentas) en AWS KMS permisos y Uso de claves KMS en otras cuentas. También hay una sección Cross-account use (Uso entre cuentas) en cada descripción de la API en la Referencia de la API de AWS Key Management Service.

> **Warning**
>
> Tenga cuidado al conceder permisos a las principales entidades para usar las claves KMS. Siempre que sea posible, siga el principio del mínimo privilegio. Proporcione a los usuarios acceso solo a las claves KMS que necesitan para las operaciones que requieren.
> Además, tenga cuidado con el uso de cualquier clave KMS desconocida, especialmente una clave KMS en una cuenta diferente. Es posible que los usuarios malintencionados le den permisos para usar su clave KMS para obtener información sobre usted o su cuenta.
> Para obtener más información sobre el uso de políticas de para proteger los recursos de su cuenta, consulte Prácticas recomendadas para las políticas de IAM.

Para conceder a permiso para utilizar una clave KMS a los usuarios y roles de otra cuenta, debe utilizar dos tipos diferentes de políticas:

- La política de claves de la clave KMS debe conceder a la cuenta externa (o a los usuarios y roles de la cuenta externa) permiso para utilizar la clave KMS. La política de claves está en la cuenta propietaria de la clave KMS.
- Las políticas de IAM de la cuenta externa debe delegar los permisos de política de claves de a sus usuarios y roles. Estas políticas se establecen en la cuenta externa y otorgan permisos para los usuarios y roles de esa cuenta.

La política de claves determina quién puede tener acceso a la clave KMS. La política de IAM determina quién sí tiene acceso a la clave KMS. Ni la política de claves ni la política de IAM solas son suficientes, debe cambiar ambas.

Para editar la política clave, puedes usar la vista de políticas en las AWS Management Console PutKeyPolicyoperaciones CreateKeyo. Para obtener ayuda sobre la configuración de la política de claves al crear una clave KMS, consulte Crear claves KMS que otras cuentas pueden utilizar.

Para obtener ayuda con la edición de políticas de IAM, consulte Uso de políticas de IAM con AWS KMS.

Para ver un ejemplo que muestra cómo la política de claves y las políticas de IAM se combinan para permitir el uso de una clave KMS en una cuenta diferente, consulte Ejemplo 2: El usuario asume un rol con permiso para utilizar una clave KMS en una Cuenta de AWS diferente.

Puede ver las resultantes operaciones de AWS KMS entre cuentas en la clave KMS de sus registros de AWS CloudTrail. Las operaciones que utilizan claves KMS en otras cuentas se registran tanto en la cuenta del autor de la llamada como en la cuenta del propietario de la clave KMS.

Temas

> **Note**
>
> En los ejemplos de este tema, se muestra cómo utilizar juntas una política de claves y una política de IAM para proporcionar y limitar el acceso a una clave KMS. Estos ejemplos genéricos no pretenden representar los permisos que ningún Servicio de AWS particular requiere en una clave KMS. Para obtener más información acerca de los permisos que requiere un Servicio de AWS, consulte el tema de cifrado en la documentación del servicio.

Paso 1: Agregar una declaración de política de claves en la cuenta local

La política de claves de una clave KMS es el principal determinante de quién puede obtener acceso a la clave KMS y qué operaciones puede realizar. La política de claves siempre se define en la cuenta propietaria de la clave KMS. A diferencia de las políticas de IAM, las políticas de claves no especifican ningún recurso. El recurso es la clave KMS asociada a la política de claves. Al proporcionar permiso entre cuentas, la política de claves de la clave KMS debe conceder a la cuenta externa (o a los usuarios y roles de la cuenta externa) permiso para utilizar la clave KMS.

Para conceder a una cuenta externa permiso para utilizar la clave KMS, agregue una declaración a la política de claves que especifique la cuenta externa. En el elemento `Principal` de la política de claves, escriba el nombre de recurso de Amazon (ARN) de la cuenta externa.

Al especificar una cuenta externa en una política de claves, los administradores de IAM de la cuenta externa pueden utilizar políticas de IAM para delegar esos permisos a cualquier usuario y rol de la cuenta externa. También pueden decidir qué acciones especificadas en la política de claves pueden realizar los usuarios y roles.

Los permisos otorgados a la cuenta externa y sus entidades principales solo son efectivos si la cuenta externa está habilitada en la región que aloja la clave KMS y su política de clave. Para obtener información acerca de las regiones que no están habilitadas de forma predeterminada ("Regiones de adhesión"), consulte Administración de Regiones de AWS en la Referencia general de AWS.

Por ejemplo, suponga que desea permitir que la cuenta `444455556666` utilice una clave KMS de cifrado simétrica en la cuenta `111122223333`. Para ello, agregue una declaración de política como la del siguiente ejemplo a la política de claves de la clave KMS de la cuenta `111122223333`. Esta declaración de política concede a la cuenta externa, `444455556666`, permiso para utilizar la clave KMS en operaciones criptográficas para claves KMS de cifrado simétricas.

> **Note**
>
> El siguiente ejemplo representa un ejemplo de política de claves para compartir una clave KMS con otra cuenta. Sustituya los valores de `Sid`, `Principal` y `Action` de ejemplo por valores válidos para el uso previsto de su clave KMS.

```
{
    "Sid": "Allow an external account to use this KMS key",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::444455556666:root"
        ]
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

En lugar de conceder permiso a la cuenta externa, puede especificar usuarios y roles externos concretos en la política de claves. Sin embargo, esos usuarios y roles de no pueden utilizar la clave KMS hasta que los administradores de IAM de la cuenta externa asocien las políticas de

IAM adecuadas a sus identidades. Las políticas de IAM pueden conceder permiso a todos o a un subconjunto de los usuarios y roles externos que se especifican en la política de claves. Y pueden permitir todas o un subconjunto de las acciones especificadas en la política de claves.

Especificar identidades en una política de claves restringe los permisos que los administradores de IAM de la cuenta externa pueden proporcionar. Sin embargo, hace que la administración de políticas con dos cuentas sea más compleja. Por ejemplo, suponga que necesita agregar un usuario o rol. Debe agregar dicha identidad a la política de claves en la cuenta propietaria de la clave KMS y crear políticas de IAM en la cuenta de la identidad.

Para especificar usuarios o roles externos concretos en una política de claves, en el elemento `Principal`, escriba el nombre de recurso de Amazon (ARN) de un usuario o rol en la cuenta externa.

Por ejemplo, la siguiente declaración de política de claves de ejemplo permite a `ExampleRole` de la cuenta `444455556666` utilizar una clave KMS en la cuenta `111122223333`. Esta declaración de política de claves concede a la cuenta externa, `444455556666`, permiso para utilizar la clave KMS en operaciones criptográficas para claves KMS de cifrado simétricas.

> **Note**
>
> El siguiente ejemplo representa un ejemplo de política de claves para compartir una clave KMS con otra cuenta. Sustituya los valores de `Sid`, `Principal` y `Action` de ejemplo por valores válidos para el uso previsto de su clave KMS.

```
{
    "Sid": "Allow an external account to use this KMS key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::444455556666:role/ExampleRole"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
```

```
}
```

> **Note**
>
> No establezca la Entidad principal en un asterisco (*) en ninguna declaración de política de claves que permita permisos a menos que utilice condiciones para limitar la política de claves. Un asterisco da cada identidad en cada permiso de Cuenta de AWS para utilizar la clave de KMS, a menos que otra declaración de política lo deniegue explícitamente. Los usuarios de otras Cuentas de AWS pueden usar la clave de KMS siempre que tengan los permisos correspondientes en sus propias cuentas.

También debe decidir qué permisos desea conceder a la cuenta externa. Para obtener una lista de permisos en las claves KMS, consulte AWS KMS permisos.

Puede conceder a la cuenta externa permiso para utilizar la clave KMS en operaciones criptográficas y utilizar la clave KMS con servicios de AWS integrados con AWS KMS. Para ello, utilice la sección Key Users (Usuarios de claves) de la AWS Management Console. Para obtener más detalles, consulte Crear claves KMS que otras cuentas pueden utilizar.

Para especificar otros permisos en las políticas de claves, edite el documento de política de claves. Por ejemplo, es posible que desee conceder a los usuarios permiso para descifrar pero no cifrar, o permiso para ver la clave KMS pero no utilizarla. Para editar el documento de política clave, puede utilizar la vista de políticas en las AWS Management Console PutKeyPolicyoperaciones CreateKeyo.

Paso 2: Agregar políticas de IAM a la cuenta externa

La política de claves de la cuenta propietaria de la clave KMS establece el rango válido de permisos. Sin embargo, los usuarios y roles de la cuenta externa no pueden utilizar la clave KMS hasta que adjunte políticas de IAM que deleguen esos permisos o utilice concesiones para administrar el acceso a la clave KMS. Las políticas de IAM se establecen en la cuenta externa.

Si la política de claves concede permiso a la cuenta externa, puede asociar políticas de IAM a cualquier usuario o rol de la cuenta. Sin embargo, si la política de claves concede permiso a usuarios o roles especificados, la política de IAM solo puede conceder esos permisos a todos o a un subconjunto de los usuarios y roles especificados. Si una política de IAM concede a la clave KMS acceso a otros usuarios o roles externos, no tiene ningún efecto.

La política de claves también limita las acciones de la política de IAM. La política de IAM puede delegar todas o un subconjunto de las acciones especificadas en la política de claves. Si la política de IAM enumera acciones que no se especifican en la política de claves, esos permisos no son efectivos.

La siguiente política de IAM de ejemplo permite a la entidad principal utilizar la clave KMS en la cuenta de `111122223333` para operaciones criptográficas. Para conceder este permiso a los usuarios y roles de la cuenta `444455556666`, asocie la política a los usuarios o roles de la cuenta `444455556666`.

> **Note**
>
> El siguiente ejemplo representa un ejemplo de política de IAM para compartir una clave KMS con otra cuenta. Sustituya los valores de `Sid`, `Resource` y `Action` de ejemplo por valores válidos para el uso previsto de su clave KMS.

```
{
    "Sid": "AllowUseOfKeyInAccount111122223333",
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
}
```

Tenga en cuenta los siguientes detalles sobre esta política:

- A diferencia de las políticas de claves, las declaraciones de política de IAM no contienen el elemento `Principal`. En las políticas de IAM, la entidad principal es la identidad a la que está asociada la política.
- El elemento de `Resource` de la política de IAM identifica la clave KMS que la entidad principal puede utilizar. Para especificar una clave KMS, agregue el ARN de la clave al elemento `Resource`.

- Puede especificar más de una clave KMS en el elemento `Resource`. Sin embargo, si no especifica determinadas claves KMS en el elemento `Resource`, es posible que conceda acceso de forma inadvertida a más clave KMS de las que pretendía.
- Para permitir al usuario externo utilizar la clave KMS con servicios de AWS que se integran con AWS KMS, es posible que tenga que agregar permisos a la política de claves o a la política de IAM. Para obtener más detalles, consulte Permitir el uso de claves KMS externas con Servicios de AWS.

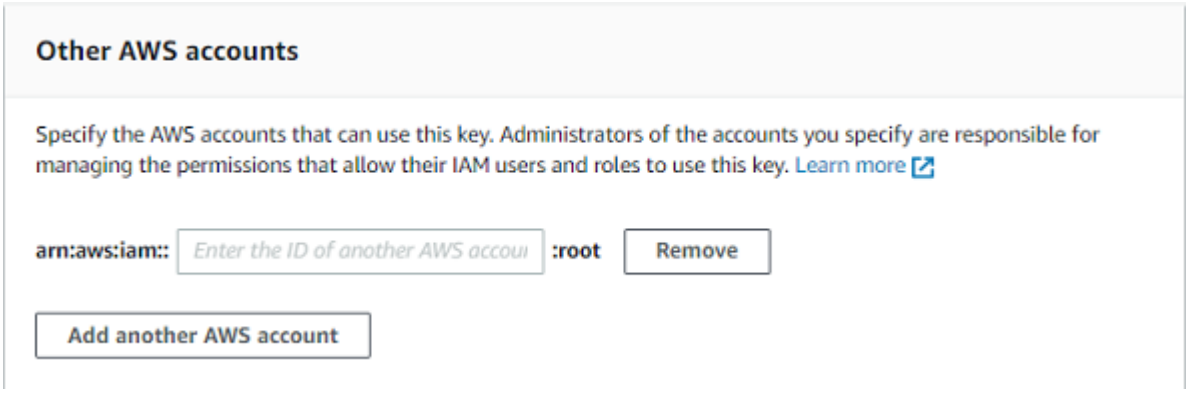
Para obtener más información sobre el uso de las políticas de IAM, consulte Políticas de IAM.

Crear claves KMS que otras cuentas pueden utilizar

Al usar la CreateKeyoperación para crear una clave de KMS, puede usar su `Policy` parámetro para especificar una política de claves que conceda permiso a una cuenta externa, o a usuarios y roles externos, para usar la clave de KMS. También debe agregar políticas de IAM en la cuenta externa que deleguen estos permisos a los usuarios y roles de la cuenta, incluso cuando los usuarios y roles estén especificados en la política de claves. Puede cambiar la política clave en cualquier momento mediante la PutKeyPolicyoperación.

Al crear una clave KMS en la AWS Management Console, también debe crear su política de claves. Al seleccionar identidades en las secciones Key Administrators (Administradores de claves) y Key Users (Usuarios de claves), AWS KMS agrega declaraciones de política para esas identidades a la política de claves de la clave KMS.

La sección Key Users (Usuarios de claves) también le permite agregar cuentas externas como usuarios de claves.



Al escribir el ID de cuenta de una cuenta externa, AWS KMS agrega dos declaraciones a la política de claves. Esta acción solo afecta a la política de claves. Los usuarios y roles de la cuenta externa

no pueden utilizar la clave KMS hasta que se asocien políticas de IAM para concederles algunos o todos estos permisos.

La primera declaración de la política de claves concede a la cuenta externa permiso para utilizar la clave KMS en operaciones criptográficas.

> **Note**
>
> Los siguientes ejemplos representan un ejemplo de política de claves para compartir una clave KMS con otra cuenta. Sustituya los valores de `Sid`, `Principal` y `Action` de ejemplo por valores válidos para el uso previsto de su clave KMS.

```
{
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::444455556666:root"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

La segunda declaración de la política de claves permite a la cuenta externa crear, ver y revocar concesiones en la clave KMS, pero solo cuando la solicitud proviene de un servicio de AWS integrado con AWS KMS. Estos permisos permiten que otros servicios de AWS que cifran datos de usuario utilicen la clave KMS.

Estos permisos están diseñados para claves de KMS que cifran los datos de los usuarios en AWS servicios, como Amazon WorkMail. Estos servicios suelen utilizar concesiones para obtener los permisos que necesitan para utilizar la clave KMS en nombre del usuario. Para obtener más detalles, consulte Permitir el uso de claves KMS externas con Servicios de AWS.

```
{
```

```
    "Sid": "Allow attachment of persistent resources",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::444455556666:root"
    },
    "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource": "*",
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
}
```

Si estos permisos no se ajustan a sus necesidades, puede editarlos en la vista de políticas de la consola o mediante la PutKeyPolicyoperación. Puede especificar usuarios y roles externos concretos en lugar de conceder permiso a la cuenta externa. Puede cambiar las acciones que especifica la política. Además, puede utilizar condiciones globales y de políticas de AWS KMS para refinar los permisos.

Permitir el uso de claves KMS externas con Servicios de AWS

Puede conceder a un usuario de otra cuenta permiso para utilizar su clave KMS con un servicio integrado con AWS KMS. Por ejemplo, un usuario de una cuenta externa puede utilizar su clave KMS para cifrar los objetos en un bucket de Amazon S3 o para cifrar los secretos que almacenan en AWS Secrets Manager.

La política de claves debe conceder al usuario externo o a la cuenta del usuario externo permiso para utilizar la clave KMS. Además, debe asociar políticas de IAM a la identidad que concede al usuario permiso para utilizar el Servicio de AWS. Además, el servicio podría requerir que los usuarios tengan permisos adicionales en la política de claves o política de IAM. Para obtener una lista de permisos que Servicio de AWS requiere una clave administrada por el cliente, consulte el tema Protección de datos en el capítulo de Seguridad de la guía del usuario o la guía para desarrolladores del servicio.

Uso de claves KMS en otras cuentas

Si tiene permiso para usar una clave KMS en un Cuenta de AWS diferente, puede usar la clave KMS en la AWS Management Console, las SDK de AWS, AWS CLI y AWS Tools for PowerShell.

Para identificar una clave KMS en una cuenta diferente en un comando de shell o solicitud de la API, utilice los siguientes identificadores clave.

- Para las operaciones criptográficas DescribeKey, y GetPublicKey, utilice la clave ARN o el alias ARN de la clave KMS.
- Para CreateGrant, GetKeyRotationStatusListGrants, y RevokeGrant, utilice la clave ARN de la clave KMS.

Si solo introduce un ID de clave o un nombre de alias, AWS supone que la clave KMS está en su cuenta.

La consola AWS KMS no muestra claves KMS en otras cuentas, incluso si tiene permiso para usarlas. Además, las listas de claves KMS mostradas en las consolas de otros servicios de AWS no incluyen claves KMS en otras cuentas.

Para especificar una clave KMS en una cuenta diferente de la consola de un servicio de AWS, debe introducir la clave ARN o el alias ARN de la clave KMS. El identificador de clave requerido varía según el servicio y podría diferir entre la consola de servicio y sus operaciones de API. Para conocer detalles, consulte la documentación del servicio.

Uso de roles vinculados a servicios de AWS KMS

AWS Key Management Service utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a AWS KMS. Los roles vinculados a un servicio están definidos por AWS KMS e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Con un rol vinculado a servicios, resulta más sencillo configurar AWS KMS, porque no es preciso agregar los permisos necesarios manualmente. AWS KMS define los permisos de los roles vinculados con su propio servicio y, a menos que esté definido de otra manera, solo AWS KMS puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar un rol vinculado a servicios después de eliminar los recursos relacionados. De esta forma, se protegen los recursos de AWS KMS, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a un servicio para almacenes de claves personalizadas de AWS KMS

AWS KMSutiliza un rol vinculado a un servicio denominado AWSServiceRoleForKeyManagementServiceCustomKeyStorespara admitir almacenes de claves personalizados. Este rol vinculado a un servicio otorga permiso de AWS KMS para ver sus clústeres AWS CloudHSM y crear la infraestructura de red para admitir una conexión entre el almacén de claves personalizado y su clúster AWS CloudHSM,AWS KMS crea este rol solo cuando se crea un almacén de claves personalizadas. No puede crear este rol vinculado a un servicio directamente.

El rol vinculado a un servicio AWSServiceRoleForKeyManagementServiceCustomKeyStores confía en que `cks.kms.amazonaws.com` asumirá el rol. En consecuencia, solo AWS KMS puede asumir este rol vinculado a un servicio.

Los permisos del rol están limitados a las acciones que ejecuta AWS KMS para conectar un almacén de claves personalizado con un clúster de AWS CloudHSM. No concede permisos adicionales a AWS KMS. Por ejemplo, AWS KMS no dispone de permiso para crear, administrar o eliminar los clústeres de AWS CloudHSM, los HSM o las copias de seguridad.

Para obtener más información acerca del rol AWSServiceRoleForKeyManagementServiceCustomKeyStores, incluida la lista de permisos y las instrucciones sobre cómo ver el rol, editar la descripción del rol, eliminar el rol y hacer que AWS KMS vuelva a crearlo, consulte Autorizar a AWS KMS para administrar AWS CloudHSM y recursos de Amazon EC2.

Permisos de roles vinculados a un servicio para claves de AWS KMS de varias regiones

AWS KMSutiliza un rol vinculado a un servicio denominado AWSServiceRoleForKeyManagementServiceMultiRegionKeyspara admitir claves multirregionales.

El rol vinculado a un servicio le otorga permiso a AWS KMS para sincronizar los cambios realizados en el material de clave de una clave principal de varias regiones con las claves de réplica. AWS KMS crea este rol solo cuando se crea una clave principal de varias regiones. No puede crear este rol vinculado a un servicio directamente.

El rol vinculado a un servicio AWSServiceRoleForKeyManagementServiceMultiRegionKeys confía en que `mrk.kms.amazonaws.com` asumirá el rol. En consecuencia, solo AWS KMS puede asumir este rol vinculado a un servicio. Los permisos del rol están limitados a las acciones que AWS KMS realiza para mantener sincronizado el material clave de las claves de varias regiones relacionadas. No concede permisos adicionales a AWS KMS.

Para obtener más información acerca del rol AWSServiceRoleForKeyManagementServiceMultiRegionKeys, incluida la lista de permisos y las instrucciones sobre cómo ver el rol, editar la descripción del rol, eliminar el rol y hacer que AWS KMS vuelva a crearlo, consulte Autorización de AWS KMS para la sincronización de claves de varias regiones.

Actualizaciones de AWS KMS a las políticas administradas de AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas de AWS para AWS KMS debido a que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de AWS KMS Historial de documentos.

Cambio	Descripción	Fecha
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy: actualización de una política actual	AWS KMSagregó los `ec2:DescribeNetworkInterfaces` permisos `ec2:DescribeVpcs` `ec2:DescribeNetworkAcls` , y para monitorear los cambios en la VPC que contiene el AWS CloudHSM clúster, de modo que AWS KMS puedan proporcionar mensajes de error claros en caso de fallas.	10 de noviembre de 2023

Cambio	Descripción	Fecha
AWS KMS comenzó el seguimiento de los cambios	AWS KMS comenzó el seguimiento de los cambios de las políticas administradas de AWS.	10 de noviembre de 2023

Usar el cifrado TLS híbrido postcuántico con AWS KMS

AWS Key Management Service (AWS KMS) admite una opción de intercambio híbrido postcuántico de claves para el protocolo de cifrado de red de seguridad de la capa de transporte (TLS). Puede utilizar esta opción de TLS cuando se conecte a los puntos de conexión de la API de AWS KMS. Estamos ofreciendo esta característica antes de que se estandaricen los algoritmos postcuánticos para que pueda comenzar a probar el efecto de estos protocolos de intercambio de claves en las llamadas a AWS KMS. Estas características opcionales de intercambio híbrido postcuántico de claves son al menos tan seguras como el cifrado TLS que utilizamos hoy en día y es muy probable que aporten beneficios de seguridad adicionales. Sin embargo, afectan a la latencia y a la velocidad si las comparamos con los protocolos clásicos de intercambio de claves que se utilizan hoy en día.

Los datos que envía a AWS Key Management Service (AWS KMS) están protegidos en tránsito por el cifrado proporcionado por una conexión de seguridad de la capa de transporte (TLS). Los conjuntos de cifrado clásicos que AWS KMS admite para las sesiones de TLS convierten en inviables los ataques de fuerza bruta en los mecanismos de intercambio de claves con la tecnología actual. Sin embargo, si la informática cuántica a gran escala tiene efectos prácticos en el futuro, los conjuntos de cifrado clásicos utilizados en los mecanismos de intercambio de claves TLS serán susceptibles a estos ataques. Si va a desarrollar aplicaciones que dependen de la confidencialidad a largo plazo de los datos transmitidos a través de una conexión TLS, debe considerar un plan para migrar a la criptografía postcuántica antes de que los equipos cuánticos a gran escala estén disponibles para su uso. AWS está trabajando para prepararse para este futuro y queremos que usted también esté bien preparado.

Para proteger los datos cifrados hoy frente a posibles ataques futuros, AWS trabaja con la comunidad criptográfica en el desarrollo de algoritmos resistentes a la informática cuántica o postcuánticos. Hemos implementado conjuntos de cifrado híbridos de intercambios de claves postcuánticos AWS KMS, que combinan elementos clásicos y postcuánticos para garantizar que su conexión TLS sea al menos tan segura como con los conjuntos cifrado clásicos.

Estos conjuntos de cifrado híbridos están disponibles para su uso en las cargas de trabajo de producción en la mayoría de las Regiones de AWS. Sin embargo, dado que las características de rendimiento y los requisitos de ancho de banda de los conjuntos de cifrado híbridos son diferentes de los mecanismos clásicos de intercambio de claves, le recomendamos que los pruebe en las llamadas a la API de AWS KMS en condiciones diferentes.

Comentarios

Como siempre, agradecemos sus comentarios y su participación en nuestros repositorios de código abierto. Nos gustaría especialmente saber cómo interactúa su infraestructura con esta nueva variante del tráfico TLS.

- Para proporcionar comentarios sobre este tema, utilice el enlace Feedback (Comentarios) situado en la esquina superior derecha de esta página.
- Estamos desarrollando estas suites de cifrado híbridas en código abierto en el s2n-tlsrepositorio de. GitHub Para proporcionar comentarios sobre la usabilidad de los conjuntos de cifrado, o para compartir nuevas condiciones o resultados de pruebas, abra una incidencia en el repositorio s2n-tls.
- Estamos escribiendo ejemplos de código para usar el TLS poscuántico híbrido AWS KMS en el repositorio. aws-kms-pq-tls-example GitHub Para hacer preguntas o compartir ideas acerca de cómo configurar su cliente HTTP o el cliente de AWS KMS para utilizar los conjuntos de cifrado híbridos, abra una incidencia en el repositorio aws-kms-pq-tls-example.

Regiones de AWS soportadas

La TLS postcuántica para AWS KMS está disponible en todas las Regiones de AWS que AWS KMS admite, excepto para China (Pekín) y China (Ningxia).

> **Note**
>
> AWS KMS no admite la TLS poscuántica híbrida para los puntos de conexión FIPS en AWS GovCloud (US).

Para obtener una lista de todos los puntos de conexión de AWS KMS de cada Región de AWS, consulte AWS Key Management Service endpoints and quotas en la Referencia general de Amazon Web Services. Para obtener más información acerca de los puntos de conexión FIPS, consulte FIPS endpoints en la Referencia general de Amazon Web Services.

Acerca del intercambio de claves postcuántico híbrido en TLS

AWS KMS admite conjuntos de cifrado de intercambio híbrido postcuántico de claves. Puede utilizar el tiempo de ejecución común de AWS SDK for Java 2.x y AWS en sistemas Linux para configurar un cliente HTTP y usar estos conjuntos de cifrado. Entonces, cada vez que se conecte a un punto de conexión de AWS KMS con su cliente HTTP, se utilizarán los conjuntos de cifrado híbridos.

Este cliente HTTP utiliza s2n-tls, que es una implementación de código abierto del protocolo TLS. Los conjuntos de cifrado híbridos que utiliza s2n-tls se implementan solo para el intercambio de claves, no para el cifrado de datos directo. Durante el intercambio de claves, el cliente y el servidor calculan la clave que utilizarán para cifrar y descifrar los datos en la red.

Los algoritmos que s2n-tls utiliza son un híbrido que combina la curva elíptica de Diffie-Hellman (ECDH), un algoritmo clásico de intercambio de claves que se utiliza hoy en día en TLS, con Kyber, un algoritmo de cifrado de claves públicas y establecimiento de claves que el Instituto Nacional de Estándares y Tecnología (NIST) ha designado como su primer algoritmo de acuerdo de claves postcuántico estándar. Este híbrido utiliza cada uno de los algoritmos de forma independiente para generar una clave. Luego combina las dos claves criptográficamente. Con s2n-tls, puede configurar un cliente HTTP con una preferencia por TLS postcuántico, que coloca a ECDH con Kyber en primer lugar en la lista de preferencias. Los algoritmos clásicos de intercambio de claves se incluyen en la lista de preferencias para garantizar la compatibilidad, pero están en una posición inferior en esta lista.

Si la investigación en curso revela que el algoritmo Kyber carece de la seguridad postcuántica prevista, la clave híbrida seguirá siendo al menos tan segura como la clave ECDH actualmente en uso. Hasta que la investigación en algoritmos poscuánticos esté completa, recomendamos usar algoritmos híbridos, en lugar de usar solo algoritmos postcuánticos.

Usar el cifrado TLS híbrido postcuántico con AWS KMS

Puede usar el cifrado TLS híbrido postcuántico para sus llamadas a AWS KMS. Cuando configure el entorno de prueba del cliente HTTP, tenga en cuenta la siguiente información:

Cifrado en tránsito

Los conjuntos de cifrado híbridos de s2n-tls se utilizan únicamente para el cifrado en tránsito. Protegen los datos mientras viajan desde su cliente hasta el punto de conexión de AWS KMS. AWS KMS no utiliza estos conjuntos de cifrado para cifrar datos en AWS KMS keys.

En cambio, cuando AWS KMS cifra sus datos con claves KMS, utiliza criptografía simétrica con claves de 256 bits y el algoritmo Advanced Encryption Standard in Galois Counter Mode (AES-GCM), que ya es resistente a la informática cuántica. Los futuros e hipotéticos ataques de informática cuántica a gran escala a textos cifrados creados con claves AES-GCM de 256 bits reducen la seguridad nominal de la clave a 128 bits. Este nivel de seguridad es suficiente para hacer inviables los ataques de fuerza bruta contra textos cifrados de AWS KMS.

Sistemas compatibles

El uso de los conjuntos de cifrado híbridos de s2n-tls solo es compatible actualmente con sistemas Linux. Además, estos conjuntos de cifrado solo se admiten en los SDK compatibles con el tiempo de ejecución común de AWS, como AWS SDK for Java 2.x. Para ver un ejemplo, consulte Cómo configurar el cifrado TLS postcuántico híbrido.

Puntos de conexión de AWS KMS

Cuando utilice los conjuntos de cifrado híbridos, use el punto de conexión de AWS KMS estándar. Los conjuntos de cifrado híbridos de s2n-tls no son compatibles con los puntos de conexión validados por FIPS 140-2 de AWS KMS.

Cuando configura un cliente HTTP con la preferencia de conexiones de TLS postcuántico en s2n-tls, los mecanismos de cifrado postcuántico son los primeros en la lista de preferencias de cifrado. Sin embargo, la lista de preferencias incluye los cifrados clásicos no híbridos en una posición inferior en el orden de prioridad por motivos de compatibilidad. Cuando se configura un cliente HTTP para que prefiera el TLS postcuántico con un punto de conexión validado por un FIPS 140-2 AWS KMS, s2n-tls negocia un cifrado de intercambio de claves clásico no híbrido.

Para obtener una lista de todos los puntos de conexión de AWS KMS de cada Región de AWS, consulte AWS Key Management Service endpoints and quotas en la Referencia general de Amazon Web Services. Para obtener más información acerca de los puntos de conexión FIPS, consulte FIPS endpoints en la Referencia general de Amazon Web Services.

Rendimiento previsto

Nuestras primeras pruebas de referencia muestran que los conjuntos de cifrado híbridos de s2n-tls son más lentos que los conjuntos de cifrado TLS clásicos. El efecto varía según el perfil de red, la velocidad de la CPU, el número de núcleos y la frecuencia de llamadas. Para obtener resultados de pruebas de rendimiento, consulteCómo ajustar TLS para el cifrado poscuántico híbrido con Kyber.

Cómo configurar el cifrado TLS postcuántico híbrido

En este procedimiento, agregue una dependencia de Maven para el cliente HTTP en tiempo de ejecución común de AWS. A continuación, configure un cliente HTTP que prefiera el TLS postcuántico. A continuación, cree un cliente de AWS KMS que utilice el cliente HTTP.

Para ver ejemplos completos y funcionales de cómo configurar y usar el cifrado TLS híbrido postcuántico con AWS KMS, consulte el repositorio aws-kms-pq-tls-example.

> **Note**
>
> El cliente HTTP de en tiempo de ejecución común de AWS, que estaba disponible como versión preliminar, pasó a estar disponible en febrero de 2023. En esa versión, la clase `tlsCipherPreference` y el parámetro del método `tlsCipherPreference()` se sustituyen por el parámetro del método `postQuantumTlsEnabled()`. Si utilizó este ejemplo durante la vista previa, debe actualizar el código.

1. Agregue el cliente del tiempo de ejecución común de AWS a sus dependencias de Maven. Le recomendamos que utilice la última versión disponible.

   Por ejemplo, esta declaración agrega la versión `2.20.0` del cliente del tiempo de ejecución común de AWS a sus dependencias de Maven.

   ```
   <dependency>
       <groupId>software.amazon.awssdk</groupId>
       <artifactId>aws-crt-client</artifactId>
       <version>2.20.0</version>
   </dependency>
   ```

2. Para habilitar los conjuntos de cifrado híbrido postcuántico, agregue AWS SDK for Java 2.x a su proyecto e inícielo. Luego habilite los conjuntos de cifrado postcuántico híbrido en su cliente HTTP como se muestra en el siguiente ejemplo.

   Este código usa el parámetro del método `postQuantumTlsEnabled()` para configurar un cliente HTTP de AWS en tiempo de ejecución común que prefiera el conjunto de cifrado poscuántico híbrido recomendado, ECDH con Kyber. A continuación, utiliza el cliente HTTP configurado para crear una instancia del cliente de AWS KMS asincrónico, `KmsAsyncClient`.

Cuando se complete este código, todas las solicitudes de la API de AWS KMS de la instancia `KmsAsyncClient` utilizarán un TLS poscuántico híbrido.

```
// Configure HTTP client
SdkAsyncHttpClient awsCrtHttpClient = AwsCrtAsyncHttpClient.builder()
          .postQuantumTlsEnabled(true)
          .build();

// Create the AWS KMS async client
KmsAsyncClient kmsAsync = KmsAsyncClient.builder()
         .httpClient(awsCrtHttpClient)
         .build();
```

3. Pruebe sus llamadas a AWS KMS con TLS postcuántico híbrido.

   Cuando llama a operaciones de la API de AWS KMS en el cliente de AWS KMS configurado, sus llamadas se transmiten al punto de conexión de AWS KMS mediante TLS híbrido postcuántico. Para probar la configuración, ejecute una llamada a la API de AWS KMS, como `ListKeys`.

   ```
   ListKeysReponse keys = kmsAsync.listKeys().get();
   ```

Probar el cifrado TLS postcuántico híbrido con AWS KMS

Considere la posibilidad de ejecutar las siguientes pruebas con conjuntos de cifrado híbridos en las aplicaciones que llaman a AWS KMS.

- Ejecute pruebas de carga y pruebas de rendimiento. Los conjuntos de cifrado híbridos funcionan de manera diferente que los algoritmos tradicionales de intercambio de claves. Es posible que tenga que ajustar los tiempos de espera de conexión para permitir tiempos de negociación más prolongados. Si la ejecución se realiza dentro de una función AWS Lambda, amplíe la configuración del tiempo de espera de ejecución.
- Intente conectarse desde diferentes ubicaciones. En función de la ruta de red que tome la solicitud, es posible que descubra que hosts intermedios, proxies o firewalls con inspección profunda de paquetes (DPI) bloquean la solicitud. Esto puede deberse al uso de los nuevos conjuntos de cifrado como ClientHelloparte del protocolo de enlace de TLS o a los mensajes de intercambio de claves más amplios. Si le resulta difícil resolver estos problemas, trabaje con su equipo de

seguridad o con los administradores de TI para actualizar la configuración pertinente y desbloquear los nuevos conjuntos de cifrado TLS.

Obtenga más información sobre el cifrado TLS postcuántico en AWS KMS

Para obtener más información acerca del uso de TLS híbrido poscuántico en AWS KMS, consulte los siguientes recursos.

- Para obtener más información sobre la criptografía poscuántica en AWS, incluidos enlaces a publicaciones de blogs y artículos de investigación, consulte Criptografía poscuántica.
- Para obtener información acerca de s2n-tls, consulte Presentación de s2n-tls, una nueva implementación de TLS de código abierto y Uso de s2n-tls.
- Para obtener información sobre el cliente HTTP de AWS de tiempo de ejecución común, consulte Configuración del cliente HTTP de AWS basado en CRT en la Guía para AWS SDK for Java 2.x desarrolladores.
- Para obtener información sobre el proyecto de criptografía postcuántica del Instituto Nacional de Estándares y Tecnología (NIST), consulte Post-Quantum Cryptography.
- Para obtener información sobre la estandarización de la criptografía poscuántica del NIST, consulte Estandarización de la criptografía poscuántica.

Determinar el acceso a AWS KMS keys

Para determinar el alcance máximo de quién o qué tiene acceso actualmente a una AWS KMS key, debe examinar la política de claves de la clave KMS, todas las concesiones que se aplican a la clave KMS y, posiblemente, todas las políticas de AWS Identity and Access Management (IAM). Puede hacerlo para determinar el ámbito del uso potencial de una clave KMS o como ayuda para cumplir los requisitos de conformidad o auditoría. Los siguientes temas pueden ayudarle a generar una lista completa de las entidades principales de AWS (identidades) que actualmente tienen acceso a una clave KMS.

Temas

- Examinar la política de claves
- Examen de las políticas de IAM
- Examinar concesiones
- Solución de problemas de acceso a las claves

Examinar la política de claves

Las políticas de claves son la forma principal de controlar el acceso a las claves KMS. Cada clave KMS tiene exactamente una política de claves.

Cuando una política de claves consta de la política de claves predeterminada o la incluye, la política de claves permite a los administradores de IAM de la cuenta utilizar políticas de IAM para controlar el acceso a la clave KMS. Además, si la política de claves da permiso a otra Cuenta de AWS para que utilice la clave KMS, los administradores de IAM de la cuenta externa pueden utilizar políticas de IAM para delegar dichos permisos. Para determinar la lista completa de entidades principales que pueden obtener acceso a la clave KMS, examine las políticas de IAM.

Para ver la política de claves de una clave gestionada por Clave administrada de AWSel AWS KMS cliente o de tu cuenta, utiliza la GetKeyPolicyoperación AWS Management Console o de la AWS KMS API. Para ver la política de claves, debe tener permisos `kms:GetKeyPolicy` para la clave KMS. Para obtener declaraciones acerca de cómo ver la política de claves para una clave KMS, consulte the section called “Consultar una política de claves”.

Examine el documento de políticas de claves y anote todas las entidades principales especificadas en el elemento `Principal` de cada declaración de política. En una declaración de política con un efecto `Allow`, los usuarios de IAM, los roles de IAM y las Cuentas de AWS en el elemento `Principal` tienen acceso a esta clave KMS.

> **Note**
>
> No establezca la Entidad principal en un asterisco (*) en ninguna declaración de política de claves que permita permisos a menos que utilice condiciones para limitar la política de claves. Un asterisco da cada identidad en cada permiso de Cuenta de AWS para utilizar la clave de KMS, a menos que otra declaración de política lo deniegue explícitamente. Los usuarios de otras Cuentas de AWS pueden usar la clave de KMS siempre que tengan los permisos correspondientes en sus propias cuentas.

En los siguientes ejemplos se utilizan las declaraciones de política existentes en la política de claves predeterminada para demostrar cómo hacerlo.

Example Declaración de política 1

```
{
```

```
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
  "Action": "kms:*",
  "Resource": "*"
}
```

En la declaración de política 1, `arn:aws:iam::111122223333:root` es una cuenta de AWS de entidad principal que hace referencia a la Cuenta de AWS 111122223333. (No es el usuario raíz de la cuenta). De forma predeterminada, una declaración de política como esta se incluye en el documento de políticas de claves al crear una clave KMS nueva con la AWS Management Console, o al crear una KMS nueva mediante programación, pero no proporcionan una política de claves.

Un documento de políticas de claves con una declaración que permita el acceso a la Cuenta de AWS habilita las políticas de IAM en la cuenta para permitir el acceso a la clave KMS. Esto significa que los usuarios y las roles de la cuenta podrían tener acceso a la clave KMS aunque no se indiquen explícitamente como entidades principales en el documento de políticas de claves. Examine todas las políticas de IAM en todas las Cuentas de AWS mencionadas como entidades principales para determinar si permiten el acceso a esta clave KMS.

Example Declaración de política 2

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/KMSKeyAdmins"},
  "Action": [
    "kms:Describe*",
    "kms:Put*",
    "kms:Create*",
    "kms:Update*",
    "kms:Enable*",
    "kms:Revoke*",
    "kms:List*",
    "kms:Disable*",
    "kms:Get*",
    "kms:Delete*",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
```

```
}
```

En la declaración de política 2, `arn:aws:iam::111122223333:role/KMSKeyAdmins` hace referencia a la función de IAM denominada KMS KeyAdmins en Cuenta de AWS 111122223333. Los usuarios que están autorizados a asumir este rol pueden realizar las acciones enumeradas en la declaración de política, que son las acciones administrativas para administrar una clave KMS.

Example Declaración de política 3

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/EncryptionApp"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateDataKey*",
    "kms:Encrypt",
    "kms:ReEncrypt*",
    "kms:Decrypt"
  ],
  "Resource": "*"
}
```

En la declaración de política 3, `arn:aws:iam::111122223333:role/EncryptionApp` hace referencia a la función de IAM nombrada en 111122223333. EncryptionApp Cuenta de AWS Las entidades principales que están autorizadas a asumir este rol tienen permiso para realizar las acciones enumeradas en la declaración de política, que incluyen las operaciones criptográficas para una clave KMS de cifrado simétrico.

Example Declaración de política 4

```
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/EncryptionApp"},
  "Action": [
    "kms:ListGrants",
    "kms:CreateGrant",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}
```

```
}
```

En la declaración de política 4, `arn:aws:iam::111122223333:role/EncryptionApp` hace referencia a la función de IAM nombrada en 111122223333. EncryptionApp Cuenta de AWS Las entidades principales que están autorizadas a asumir este rol tienen permiso para realizar las acciones enumeradas en la declaración de política. Estas acciones, cuando se combinan con las acciones permitidas en Ejemplo de declaración de política 3, son las necesarias para delegar el uso de la clave KMS a la mayoría de los servicios de AWS que se integran con AWS KMS, específicamente los servicios que usan concesiones. El GrantIsFor AWSResource valor kms: del `Condition` elemento garantiza que la delegación solo esté permitida cuando el delegado sea un AWS servicio que se integre con las concesiones de autorización AWS KMS y las utilice.

Para conocer las distintas formas en las que puede especificar una entidad principal en un documento de políticas de claves, consulte Especificación de un elemento principal en la Guía del usuario de IAM.

Para obtener más información sobre las políticas de claves de AWS KMS, consulte Políticas clave en AWS KMS.

Examen de las políticas de IAM

Además de la política de claves y concesiones, también puede utilizar políticas de IAM para permitir el acceso a una clave KMS. Para obtener más información sobre cómo funcionan las políticas de IAM y las políticas de claves de forma conjunta, consulte Solución de problemas de acceso a las claves.

Para determinar qué entidades principales tienen acceso a una clave KMS a través de las políticas de IAM, puede utilizar la herramienta del simulador de políticas de IAM o puede realizar solicitudes a la API de IAM.

Formas de examinar las políticas de IAM

- Examen de las políticas de IAM con el simulador de políticas de IAM
- Examen de políticas de IAM con la API de IAM

Examen de las políticas de IAM con el simulador de políticas de IAM

El simulador de políticas de IAM puede ayudarle a saber qué entidades principales tienen acceso a una clave KMS mediante una política de IAM.

Para utilizar el simulador de políticas de IAM para determinar el acceso a una clave KMS

1. Inicie sesión en la AWS Management Console y abra el simulador de políticas de IAM en https://policysim.aws.amazon.com/.
2. En el panel Users, Groups, and Roles, elija el usuario, grupo o rol cuyas políticas desee simular.
3. (Opcional) Desactive la casilla de verificación situada junto a la política que desee omitir en la simulación. Para simular todas las políticas, deje todas las políticas seleccionadas.
4. En el panel Policy Simulator, haga lo siguiente:
   a. En Select service, elija Key Management Service.
   b. Para simular acciones de AWS KMS específicas, en Select actions, elija las acciones que desea simular. Para simular todas las acciones de AWS KMS, elija Select All (Seleccionar todo).
5. (Opcional) El simulador de políticas simula el acceso a todas las claves KMS de forma predeterminada. Para simular el acceso a una clave KMS específica, elija Simulation Settings (Configuraciones de simulación) y, a continuación, escriba el nombre de recurso de Amazon (ARN) de la clave KMS que se simulará.
6. Elija Run Simulation (Ejecutar la simulación).

Puede ver los resultados de la simulación en la sección Results. Repita los pasos del 2 al 6 por cada usuario, grupo y rol de la Cuenta de AWS.

Examen de políticas de IAM con la API de IAM

Puede utilizar la API de IAM para examinar políticas de IAM mediante programación. En los pasos siguientes se ofrece información general sobre cómo hacerlo:

1. Utilice las ListRolesoperaciones y de la API de IAM para obtener todos los usuarios ListUsersy funciones de la AWScuenta para cada uno de los principales que Cuenta de AWS figuran como principales en la política clave (es decir, cada principal de cuenta especificado en este formato:`"Principal": {"AWS": "arn:aws:iam::111122223333:root"}`).
2. Para cada usuario y rol de la lista, usa la SimulatePrincipalPolicyoperación en la API de IAM e introduce los siguientes parámetros:
   - Para `PolicySourceArn`, especifique el nombre de recurso de Amazon (ARN) de un usuario o rol de la lista. Puede especificar solo un `PolicySourceArn` para cada solicitud

`SimulatePrincipalPolicy`, de modo que debe llamar a esta operación varias veces, una vez por cada usuario y rol de la lista.

- Para la lista `ActionNames`, especifique cada acción de API de AWS KMS que se simulará. Para simular todas las acciones de la API de AWS KMS utilice `kms:*`. Para probar las acciones de la API de AWS KMS individuales, anteponga a cada acción de la API "`kms:`", por ejemplo, "`kms:ListKeys`". Si desea ver una lista completa de las acciones de la API de AWS KMS, consulte Acciones en la Referencia de la API de AWS Key Management Service.
- (Opcional) Para determinar si los usuarios o roles de tienen acceso a determinadas claves KMS, use el parámetro `ResourceArns` para especificar una lista de los nombres de recurso de Amazon (ARN) de las claves KMS. Para determinar si los usuarios o roles tienen acceso a cualquier clave KMS, no use el parámetro `ResourceArns`.

IAM responde a cada solicitud de `SimulatePrincipalPolicy` con una decisión de evaluación: `allowed`, `explicitDeny` o `implicitDeny`. Por cada respuesta que contenga una decisión de evaluación del tipo `allowed`, la respuesta incluye el nombre de la operación de API de AWS KMS específica permitida. También incluye el ARN de la clave KMS utilizado en la evaluación, si se ha realizado.

Examinar concesiones

Las concesiones son mecanismos avanzados para especificar permisos que el usuario o un servicio de AWS integrado con AWS KMS pueden usar para especificar el modo y el momento en que se puede usar una clave KMS. Las concesiones están asociadas a una clave KMS, y cada concesión contiene la entidad principal que recibe el permiso de usar la clave KMS y una lista de las operaciones permitidas. Las concesiones son una alternativa a la política de claves, y son útiles para casos de uso específicos. Para obtener más información, consulte Concesiones en AWS KMS.

Para obtener una lista de las concesiones de una clave de KMS, utilice la AWS KMS ListGrantsoperación. Puede examinar las concesiones de una clave KMS para determinar quién o qué tiene acceso actualmente para utilizar la clave KMS a través de dichas concesiones. Por ejemplo, a continuación se ofrece una representación JSON de una concesión que se ha obtenido del comando list-grants en la AWS CLI.

```
{"Grants": [{
  "Operations": ["Decrypt"],
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
  "Name": "0d8aa621-43ef-4657-b29c-3752c41dc132",
  "RetiringPrincipal": "arn:aws:iam::123456789012:root",
  "GranteePrincipal": "arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/
i-5d476fab",
  "GrantId": "dc716f53c93acacf291b1540de3e5a232b76256c83b2ecb22cdefa26576a2d3e",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "CreationDate": 1.444151834E9,
  "Constraints": {"EncryptionContextSubset": {"aws:ebs:id": "vol-5cccfb4e"}}
}]}
```

Para averiguar quién o qué tiene acceso para utilizar la clave KMS, busque el elemento `"GranteePrincipal"`. En el ejemplo anterior, la entidad principal beneficiaria es un usuario de rol asumido que está asociado con la instancia EC2 i-5d476fab, que la infraestructura de EC2 usa para asociar el volumen de EBS cifrado vol-5cccfb4e a la instancia. En este caso, el rol de infraestructura EC2 tiene permiso para usar la clave KMS porque anteriormente ha creado un volumen de EBS cifrado que está protegido por esta clave KMS y, después, ha asociado el volumen a una instancia EC2.

A continuación, se ofrece otro ejemplo de una representación JSON de una concesión que se ha obtenido del comando list-grants en la AWS CLI. En el siguiente ejemplo, la entidad principal beneficiaria es otra Cuenta de AWS.

```
{"Grants": [{
  "Operations": ["Encrypt"],
  "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
  "Name": "",
  "GranteePrincipal": "arn:aws:iam::444455556666:root",
  "GrantId": "f271e8328717f8bde5d03f4981f06a6b3fc18bcae2da12ac38bd9186e7925d11",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "CreationDate": 1.444151269E9
}]}
```

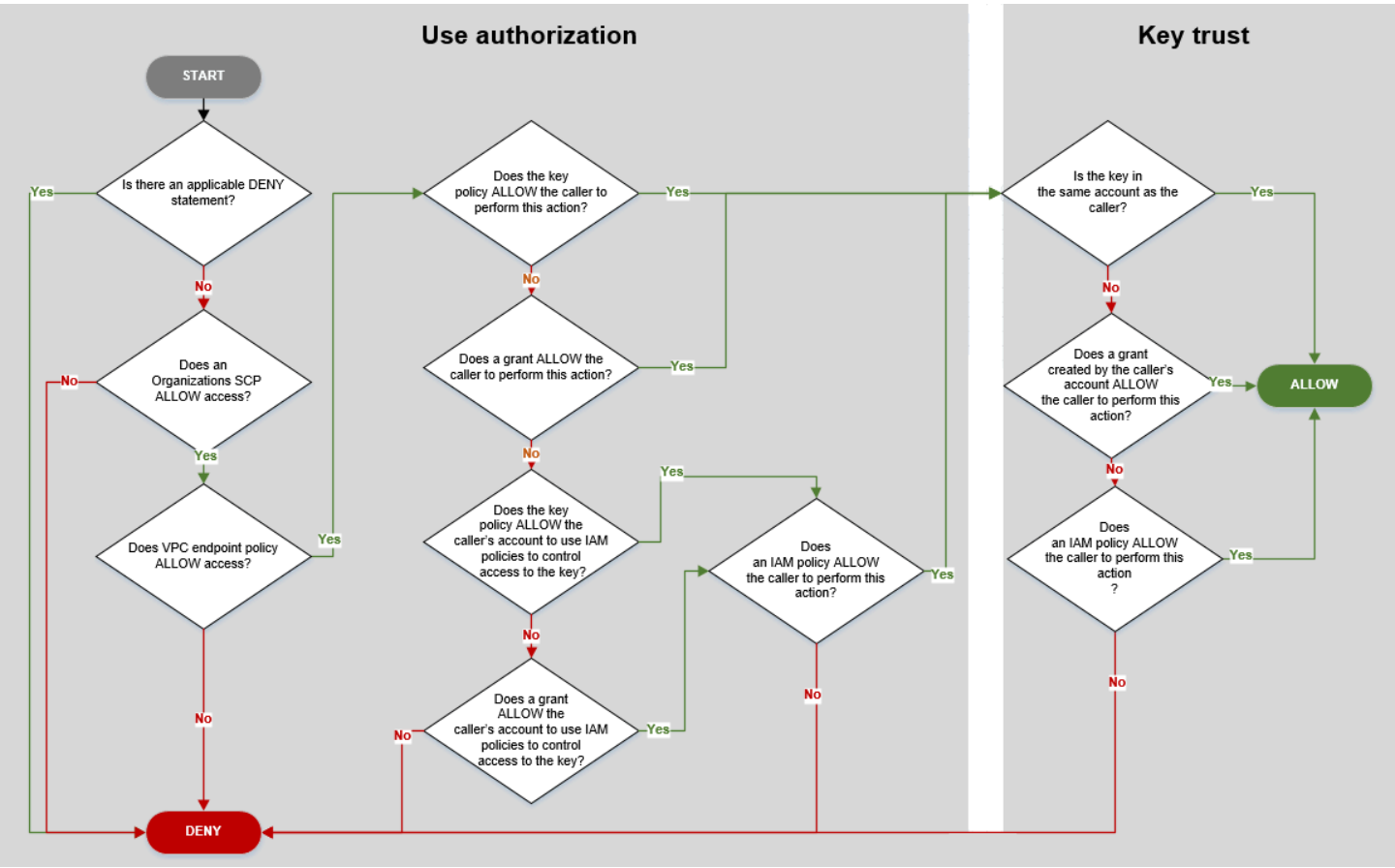
Solución de problemas de acceso a las claves

Al autorizar el acceso a una clave KMS, AWS KMS evalúa lo siguiente:

- La política de claves asociada a la clave KMS. La política de claves siempre se define en la región y la Cuenta de AWS propietaria de la clave KMS.

- Todas las políticas de IAM asociadas al usuario o rol que realiza la solicitud. Las políticas de IAM que rigen el uso de una clave KMS por una entidad principal siempre se definen en la Cuenta de AWS.
- Todas las concesiones que afectan a la clave KMS.
- Otros tipos de políticas que podrían aplicarse a la solicitud de usar la clave KMS, como Políticas de control de servicios de AWS Organizations y Políticas de punto de enlace de la VPC. Estas políticas son opcionales y permiten todas las acciones de forma predeterminada, pero puede usarlas para restringir los permisos otorgados a las entidades principales.

AWS KMS evalúa estos mecanismos de política juntos para determinar si se permite o se deniega el acceso a la clave KMS. Para ello, AWS KMS utiliza un proceso similar al representado en el siguiente diagrama de flujo. El siguiente diagrama de flujo ofrece una representación visual del proceso de evaluación de las políticas.



Este diagrama de flujo se divide en dos partes. Las partes parecen secuenciales, pero se suelen evaluar al mismo tiempo.

- El use de la autorización determina si puede utilizar una clave KMS en función de su política de claves, sus políticas de IAM, sus concesiones y otras políticas aplicables.
- La confianza en la clave determina si debe confiar en una clave KMS que se le ha permitido utilizar. En general, puede confiar en los recursos de su Cuenta de AWS. Sin embargo, puede estar tranquilo a la hora de utilizar las claves KMS de una Cuenta de AWS diferente si una concesión o política de IAM de su cuenta le permite utilizar la clave KMS.

Puede utilizar este diagrama de flujo para saber por qué se ha permitido o denegado que un intermediario utilice una clave KMS. También puede utilizarlo para evaluar sus políticas y concesiones. Por ejemplo, el diagrama de flujo muestra que se puede negar el acceso a un intermediario mediante una declaración `DENY` explícita, o por la ausencia de una declaración `ALLOW` explícita, en la política de claves, la política de IAM o la concesión.

El diagrama de flujo puede explicar algunos escenarios comunes de permisos.

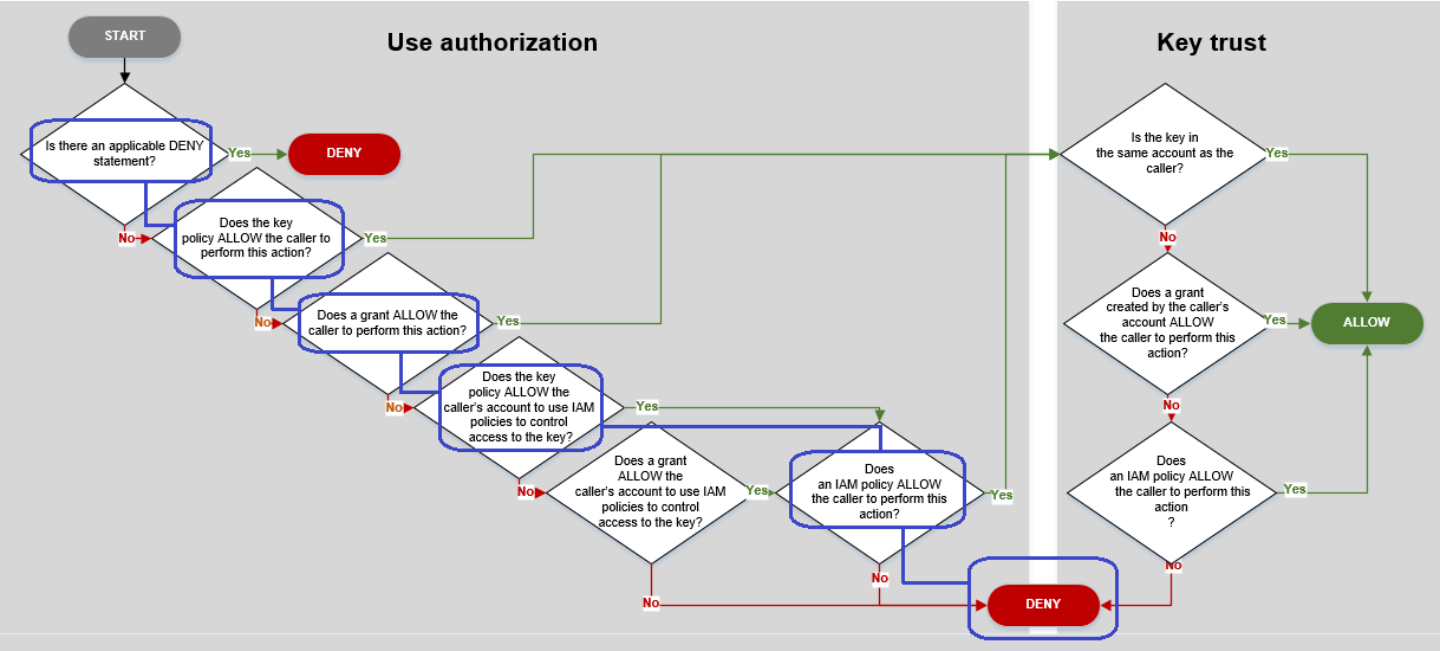
Ejemplos de permisos

- Ejemplo 1: Se deniega el acceso al usuario a una clave KMS en su Cuenta de AWS
- Ejemplo 2: El usuario asume un rol con permiso para utilizar una clave KMS en una Cuenta de AWS diferente

Ejemplo 1: Se deniega el acceso al usuario a una clave KMS en su Cuenta de AWS

Alice es una usuaria de IAM en la Cuenta de AWS 111122223333. Se le ha denegado al acceso a una clave KMS en la misma Cuenta de AWS. ¿Por qué no puede utilizar Alice la clave KMS?

En este caso, se le deniega el acceso a Alice a la clave KMS porque no hay ninguna política de claves, política de IAM o concesión que proporcione los permisos necesarios. La política de la clave KMS permite que la Cuenta de AWS utilice políticas de IAM para controlar el acceso a la clave KMS, pero ninguna política de IAM concede a Alice permiso para usar la clave KMS.



Considere las políticas relevantes para este ejemplo.

- La clave KMS que Alice quiere utilizar tiene la política de claves predeterminada. Esta política permite que la Cuenta de AWS que posee la clave KMS para utilizar políticas de IAM para controlar el acceso a la clave KMS. Esta política de claves satisface la condición ¿PERMITE la política de claves que la cuenta de los intermediarios utilice políticas de IAM para controlar el acceso a clave? del diagrama de flujo.

```
{
  "Version" : "2012-10-17",
  "Id" : "key-test-1",
  "Statement" : [ {
    "Sid" : "Delegate to IAM policies",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : "kms:*",
    "Resource" : "*"
  } ]
}
```

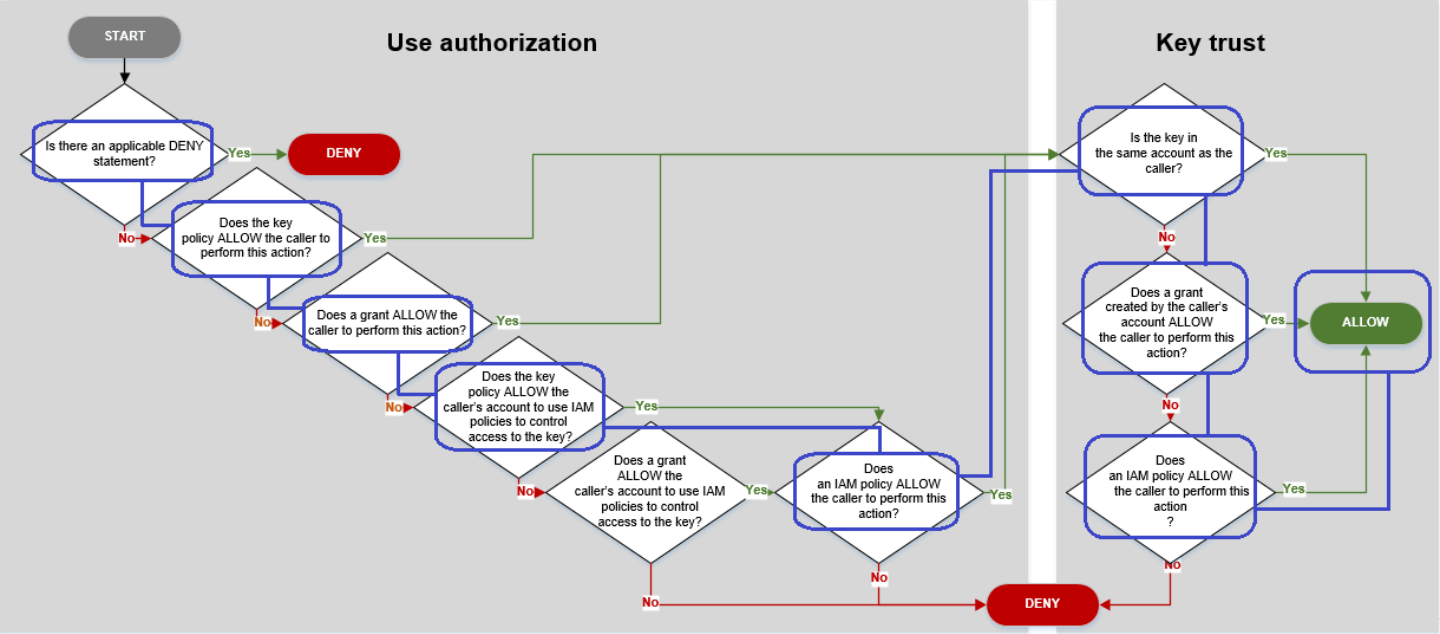
- Sin embargo, no hay ninguna política de claves, política de IAM ni concesión que conceda a Alice permiso para usar la clave KMS. Por lo tanto, se deniega a Alice el permiso para utilizar la clave KMS.

Ejemplo 2: El usuario asume un rol con permiso para utilizar una clave KMS en una Cuenta de AWS diferente

Roberto es un usuario de la cuenta 1 (111122223333). Se le permite usar una clave KMS en la cuenta 2 (444455556666) en operaciones criptográficas. ¿Cómo es posible?

> **Tip**
>
> Al evaluar los permisos entre cuentas, recuerde que la política de claves se especifica en la cuenta de la clave KMS. La política de IAM se especifica en la cuenta del intermediario, incluso cuando el intermediario está en una cuenta diferente. Para obtener más detalles sobre cómo proporcionar acceso entre cuentas a claves KMS, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS.

- La política de claves de la clave KMS de la cuenta 2 permite que la cuenta 2 utilice políticas de IAM para controlar el acceso a la clave KMS.
- La política de claves de la clave KMS de la cuenta 2 permite que la cuenta 1 utilice la clave KMS en operaciones criptográficas. Sin embargo, la cuenta 1 debe utilizar políticas de IAM para conceder acceso a la clave KMS a sus entidades principales.
- Una política de IAM de la cuenta 1 permite al rol `Engineering` utilizar la clave KMS de la cuenta 2 para las operaciones criptográficas.
- Roberto, un usuario de la cuenta 1, tiene permiso para asumir el rol `Engineering`.
- Roberto confía en esta clave KMS, porque, aunque no se encuentre en su cuenta, una política de IAM de su cuenta le otorga permiso explícito para utilizar esta clave KMS.



Considere las políticas que permiten a Roberto, un usuario de la cuenta 1, utilizar la clave KMS de la cuenta 2.

- La política de claves de la clave KMS permite que la cuenta 2 (444455556666, la cuenta propietaria de la clave KMS) utilice políticas de IAM para controlar el acceso a la clave KMS. Esta política de claves permite también que la cuenta 1 (111122223333) utilice la clave KMS en operaciones criptográficas (especificado en el elemento `Action` de la declaración de política). Sin embargo, ninguna persona de la cuenta 1 puede usar la clave KMS de la cuenta 2 hasta que la cuenta 1 defina políticas de IAM que concedan a las entidades principales acceso a la clave KMS.

  En el diagrama de flujo, esta política de claves de la cuenta 2 satisface la condición ¿PERMITE la política de claves que la cuenta de los intermediarios utilice políticas de IAM para controlar el acceso a la clave?

```
{
    "Id": "key-policy-acct-2",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Permission to use IAM policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:root"
            },
            "Action": "kms:*",
```

```
            "Resource": "*"
        },
        {
            "Sid": "Allow account 1 to use this KMS key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        }
    ]
}
```

- Una política de IAM de la cuenta de Cuenta de AWS del intermediario (cuenta 1, 111122223333) concede al rol de la cuenta 1 permiso para realizar operaciones criptográficas mediante la clave KMS de la cuenta 2 (444455556666). El elemento `Action` delega a la entidad principal los mismos permisos que la política de claves de la cuenta 2 concedió a la cuenta 1. Para conceder estos permisos al rol `Engineering` en la cuenta 1, esta política en línea está incrustada en el rol `Engineering`.

  Las políticas de IAM entre cuentas como esta son eficaces solo cuando la política de claves de la clave KMS de la cuenta 2 concede a la cuenta 1 permiso para utilizar la clave KMS. Además, la cuenta 1 solo puede conceder permiso a sus entidades principales para realizar las acciones que la política de claves concedió a la cuenta.

  En el diagrama de flujo, esto satisface la condición ¿Permite una política de IAM que el intermediario realice esta acción?

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-
west-2:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab"
            ]
        }
    ]
}
```

- El último elemento necesario es la definición del rol `Engineering` en la cuenta 1. El elemento `AssumeRolePolicyDocument` del rol permite a Roberto asumir el rol `Engineering`.

```
{
    "Role": {
        "Arn": "arn:aws:iam::111122223333:role/Engineering",
        "CreateDate": "2019-05-16T00:09:25Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": {
                "Principal": {
                    "AWS": "arn:aws:iam::111122223333:user/bob"
                },
                "Effect": "Allow",
                "Action": "sts:AssumeRole"
            }
        },
        "Path": "/",
        "RoleName": "Engineering",
        "RoleId": "AROA4KJY2TU23Y7NK62MV"
    }
}
```

AWS KMS permisos

Esta tabla está diseñada para ayudarle a entender AWS KMS los permisos para que pueda controlar el acceso a sus AWS KMS recursos. Las definiciones de los títulos de las columnas aparecen bajo la tabla.

También puede obtener información sobre AWS KMS los permisos en las claves de acciones, recursos y condición del AWS Key Management Service tema de la Referencia de autorización de servicios. Sin embargo, ese tema no enumera todas las claves de condición que puede utilizar para limitar cada permiso.

> **Note**
>
> Es posible que tenga que desplazarse en forma horizontal o vertical para ver todos los datos de la tabla.

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
CancelKeyDeletion `kms:CancelKeyDeletion`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
				aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService
ConnectCustomKeyStore `kms:ConnectCustomKeyStore`	Política de IAM	No	*	km: CallerAccount

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
CreateAlias `kms:CreateAlias` Para utilizar esta operación, el intermediario necesita permiso `kms:CreateAlias` en dos recursos: • El alias (en una política de IAM) • La clave KMS (en una política de clave) Para obtener más detalles, consulte Control del acceso a alias.	Política de IAM (para el alias)	No	Alias	Ninguno (cuando se controla el acceso al alias)
	Política de claves (para la clave KMS)	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService
CreateCustomKeyStore `kms:CreateCustomKeyStore`	Política de IAM	No	*	km: CallerAccount

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
CreateGrant `kms:CreateGrant`	Política de claves	Sí	Clave KMS	Condiciones de contexto de cifrado: kmsEncryptionContext: clave de contexto kms: EncryptionContextKeys Condiciones de concesión: km: GrantConstraintType km: GranteePrincipal km: GrantIsFor AWSResource km: GrantOperations km: RetiringPrincipal Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
				km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
CreateKey `kms:CreateKey`	Política de IAM	No	*	km: BypassPolicyLockoutSafetyCheck km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ViaService aws:RequestTag/tag-key (clave de condición AWS global) aws:ResourceTag/tag-key (clave de condición global)AWS aws: TagKeys (clave de condición AWS global)

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
Decrypt `kms:Decrypt`	Política de claves	Sí	Clave KMS	Condiciones para operaciones criptográficas kms: EncryptionAlgorithm km: RequestAlias Condiciones de contexto de cifrado: kmsEncryptionContext: clave de contexto kms: EncryptionContextKeys Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
				aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService
DeleteAlias `kms:DeleteAlias` Para utilizar esta operación, el intermediario necesita permiso `kms:DeleteAlias` en dos recursos: • El alias (en una política de IAM) • La clave KMS (en una política de clave) Para obtener más detalles, consulte Control del acceso a alias.	Política de IAM (para el alias)	No	Alias	Ninguno (cuando se controla el acceso al alias)
	Política de claves (para la clave KMS)	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
DeleteCustomKeyStore `kms:DeleteCustomKeyStore`	Política de IAM	No	*	km: CallerAccount
DeleteImportedKeyMaterial `kms:DeleteImportedKeyMaterial`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService
DescribeCustomKeyStores `kms:DescribeCustomKeyStores`	Política de IAM	No	*	km: CallerAccount

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
DescribeKey `kms:DescribeKey`	Política de claves	Sí	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Otras condiciones: km: RequestAlias

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
DisableKey `kms:DisableKey`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
DisableKeyRotation `kms:DisableKeyRotation`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService
DisconnectCustomKeyStore `kms:DisconnectCustomKeyStore`	Política de IAM	No	*	km: CallerAccount

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
EnableKey `kms:EnableKey`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
EnableKeyRotation `kms:EnableKeyRotation`	Política de claves	No	Clave KMS (solo simétrica)	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Condiciones de rotación automática de las teclas: km: RotationPeriodInDays

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
Encrypt `kms:Encrypt`	Política de claves	Sí	Clave KMS	Condiciones para operaciones criptográficas km: EncryptionAlgorithm km: RequestAlias Condiciones de contexto de cifrado: kmsEncryptionContext: clave de contexto kms: EncryptionContextKeys Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
				aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
GenerateDataKey `kms:GenerateDataKey`	Política de claves	Sí	Clave KMS (solo simétrica)	Condiciones para operaciones criptográficas km: EncryptionAlgorithm km: RequestAlias Condiciones de contexto de cifrado: kmsEncryptionContext: clave de contexto kms: EncryptionContextKeys Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
				aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
GenerateDataKeyPair `kms:GenerateDataKeyPair`	Política de claves	Sí	Clave KMS (solo simétrica) Genera un par de claves de datos asimétricos protegido por una clave de KMS de cifrado simétrica.	Condiciones para pares de claves de datos: km: DataKeyPairSpec Condiciones para operaciones criptográficas km: EncryptionAlgorithm km: RequestAlias Condiciones de contexto de cifrado: kmsEncryptionContext: clave de contexto kms: EncryptionContextKeys Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
				km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
GenerateDataKeyPairWithoutPlaintext `kms:GenerateDataKeyPairWithoutPlaintext`	Política de claves	Sí	Clave KMS (solo simétrica) Genera un par de claves de datos asimétricos protegido por una clave de KMS de cifrado simétrica.	Condiciones para pares de claves de datos: km: DataKeyPairSpec Condiciones para operaciones criptográficas km: EncryptionAlgorithm km: RequestAlias Condiciones de contexto de cifrado: kmsEncryptionContext: clave de contexto kms: EncryptionContextKeys Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
				km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
GenerateDataKeyWithoutPlaintext `kms:GenerateDataKeyWithoutPlaintext`	Política de claves	Sí	Clave KMS (solo simétrica)	Condiciones para operaciones criptográficas km: EncryptionAlgorithm km: RequestAlias Condiciones de contexto de cifrado: kmsEncryptionContext: clave de contexto kms: EncryptionContextKeys Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
				aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService
GenerateMac `kms:GenerateMac`	Política de claves	Sí	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Condiciones para operaciones criptográficas: km: MacAlgorithm km: RequestAlias

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
GenerateRandom `kms:GenerateRandom`	Política de IAM	N/A	*	Ninguna
GetKeyPolicy `kms:GetKeyPolicy`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
GetKeyRotationStatus `kms:GetKeyRotationStatus`	Política de claves	Sí	Clave KMS (solo simétrica)	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
GetParametersForImport `kms:GetParametersForImport`	Política de claves	No	Clave KMS	km: WrappingAlgorithm km: WrappingKeySpec Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
GetPublicKey `kms:GetPublicKey`	Política de claves	Sí	Clave KMS (solo asimétrica)	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Otras condiciones: km: RequestAlias

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
ImportKeyMaterial `kms:ImportKeyMaterial`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Otras condiciones: km: ExpirationModel km: ValidTo
ListAliases `kms:ListAliases`	Política de IAM	No	*	Ninguna

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
ListGrants `kms:ListGrants`	Política de claves	Sí	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Otras condiciones: km: GrantIsFor AWSResource

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
ListKeyPolicies `kms:ListKeyPolicies`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
ListKeyRotations `kms:ListKeyRotations`	Política de claves	No	Clave KMS (solo simétrica)	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService
ListKeys `kms:ListKeys`	Política de IAM	No	*	Ninguna

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
ListResourceTags `kms:ListResourceTags`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
ListRetirableGrants `kms:ListRetirableGrants`	Política de IAM	La principal entidad especificada debe estar en la cuenta local, pero la operación devuelve concesiones en todas las cuentas.	*	Ninguna

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
PutKeyPolicy `kms:PutKeyPolicy`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Otras condiciones: km: BypassPolicyLockoutSafetyCheck

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición

ReEncrypt
 	
`kms:ReEncryptFrom`
 	
`kms:ReEncryptTo`
 	
Para utilizar esta operación, la persona que llama necesita permiso en dos claves KMS:
 	
• `kms:ReEncryptFrom` en la clave KMS utilizada para descifrar
• `kms:ReEncryptTo` en la clave KMS utilizada para cifrar
	Política de claves	Sí	Clave KMS	Condiciones para operaciones criptográficas
				
				km: EncryptionAlgorithm
				
				km: RequestAlias
				
				Condiciones de contexto de cifrado:
				
				kmsEncryptionContext: clave de contexto
				
				kms: EncryptionContextKeys
				
				Condiciones para las operaciones clave KMS:
				
				km: CallerAccount
				
				km: KeySpec
				
				km: KeyUsage
				
				km: KeyOrigin
				
				km: MultiRegion
				
				km: MultiRegionKeyType
				
				km: ResourceAliases

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
				aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Otras condiciones: km: ReEncrypt OnSameKey

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
ReplicateKey `kms:ReplicateKey` Para utilizar esta operación, la persona que llama necesita estos permisos: • `kms:ReplicateKey` en la clave principal de varias regiones • `kms:CreateKey` en una política de IAM en la región de réplica	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Otras condiciones: km: ReplicaRegion

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
RetireGrant `kms:RetireGrant` El permiso para retirar una concesión se determina principalmente por la concesión. Una política por sí sola no puede permitir el acceso a esta operación. Para obtener más informaci ón, consulte Retiro y revocación de concesion es.	Política de IAM (Este permiso no es efectivo en una política de clave.)	Sí	Clave de KMS	km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global)

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
RevokeGrant `kms:RevokeGrant`	Política de claves	Sí	Clave KMS	Condiciones para las operaciones clave KMS: kms: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Otras condiciones: km: GrantIsFor AWSResource

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
RotateKeyOnDemand `kms:RotateKeyOnDemand`	Política de claves	No	Clave KMS (solo simétrica)	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
ScheduleKeyDeletion `kms:ScheduleKeyDeletion`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
Sign `kms:Sign`	Política de claves	Sí	Clave KMS (solo asimétrica)	Condiciones para la firma y la verificación: km: MessageType km: RequestAlias km: SigningAlgorithm Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
TagResource `kms:TagResource`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Condiciones para el etiquetado: aws:RequestTag/tag-key (clave de condición AWS global) aws: TagKeys (clave de condición AWS global)

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
UntagResource `kms:UntagResource`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: kms: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Condiciones para el etiquetado: aws:RequestTag/tag-key (clave de condición AWS global) aws: TagKeys (clave de condición AWS global)

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
UpdateAlias `kms:UpdateAlias` Para utilizar esta operación, el intermediario necesita permiso `kms:UpdateAlias` en tres recursos: • El alias • La clave KMS asociada actualmente • La clave KMS recién asociada Para obtener más detalles, consulte Control del acceso a alias.	Política de IAM (para el alias)	No	Alias	Ninguno (cuando se controla el acceso al alias)
	Política de claves (para las claves KMS)	No	Clave KMS	Condiciones para las operaciones clave KMS: kms: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService
UpdateCustomKeyStore `kms:UpdateCustomKeyStore`	Política de IAM	No	*	km: CallerAccount

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
UpdateKeyDescription `kms:UpdateKeyDescription`	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
UpdatePrimaryRegion `kms:UpdatePrimaryRegion` Para utilizar esta operación, la persona que llama necesita permiso `kms:UpdatePrimaryRegion` tanto en la clave principal de varias regiones que se convertirá en una clave de réplica como en la clave de réplica de varias regiones que se convertirá en la clave principal.	Política de claves	No	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Otras condiciones km: PrimaryRegion

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
Verificar `kms:Verify`	Política de claves	Sí	Clave KMS (solo asimétrica)	Condiciones para la firma y la verificación: km: MessageType km: RequestAlias km: SigningAlgorithm Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService

Acciones y permisos	Tipo de política	Uso entre cuentas	Recursos (para políticas de IAM)	AWS KMS claves de condición
VerifyMac `kms:VerifyMac`	Política de claves	Sí	Clave KMS	Condiciones para las operaciones clave KMS: km: CallerAccount km: KeySpec km: KeyUsage km: KeyOrigin km: MultiRegion km: MultiRegionKeyType km: ResourceAliases aws:ResourceTag/tag-key (clave de condición AWS global) kms: ViaService Condiciones para operaciones criptográficas: km: MacAlgorithm km: RequestAlias

Descripciones de las columnas

Las columnas de esta tabla proporcionan la siguiente información:

- Acciones y permisos muestra cada operación de la AWS KMS API y el permiso que permite la operación. Especifique la operación en el elemento `Action` de una declaración de política.
- Tipo de política indica si el permiso se puede utilizar en una política de claves o en una política de IAM.

  Política de claves significa que puede especificar el permiso en la política de claves. Cuando la política de claves contiene la declaración de política que permite las políticas de IAM, puede especificar el permiso en una política de IAM.

  La política de IAM significa que puede especificar el permiso solo en la política de IAM.
- Uso entre cuentas muestra las operaciones que los usuarios autorizados pueden realizar en recursos de una Cuenta de AWS diferente.

  Un valor de Yes (Sí) significa que las entidades principales pueden realizar la operación en los recursos en una Cuenta de AWS diferente.

  Un valor de No significa que las principales entidades pueden realizar la operación solo en recursos en sus propios Cuenta de AWS.

  Si otorga a una entidad principal de una cuenta diferente un permiso que no se puede utilizar en un recurso entre cuentas, el permiso no será efectivo. Por ejemplo, si le das TagResource permiso a un director de una cuenta diferente para usar una clave de KMS en tu cuenta, sus intentos de etiquetar la clave de KMS en tu cuenta fallarán.
- Recursos muestra los AWS KMS recursos a los que se aplican los permisos. AWS KMS admite dos tipos de recursos: una clave KMS y un alias. En una política de claves, el valor del elemento `Resource` es siempre `*`, lo que indica la clave KMS a la que está asociada la política de claves.

  Utilice los siguientes valores para representar un AWS KMS recurso en una política de IAM.

  Clave de KMS

  Cuando el recurso sea una clave KMS, utilice su ARN de clave. Para obtener ayuda, consulte the section called “Búsqueda del ID y el ARN de la clave”.

  `arn:`*`AWS_partition_name`*`:kms:`*`AWS_Region`*`:`*`AWS_account_ID`*`:key/`*`key_ID`*

  Por ejemplo:

  arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab

Alias

Cuando el recurso sea un alias, utilice su ARN de alias. Para obtener ayuda, consulte the section called “Buscar el nombre del alias y el ARN de alias”.

`arn:AWS_partition_name:kms:AWS_region:AWS_account_ID:alias/alias_name`

Por ejemplo:

arn:aws:kms:us-west- 2:111122223333:alias/ ExampleAlias

***** (asterisco)

Cuando el permiso no se aplique a un recurso determinado (clave KMS o alias), utilice un asterisco (`*`).

En una política de IAM para un AWS KMS permiso, un asterisco en el elemento indica todos los recursos (claves y alias de KMS). `Resource` AWS KMS También puedes usar un asterisco en el `Resource` elemento cuando el AWS KMS permiso no se aplique a ninguna clave o alias de KMS en concreto. Por ejemplo, al permitir o denegar el permiso `kms:CreateKey` o `kms:ListKeys`, puede establecer el elemento `Resource` en `*` o en una variación específica de la cuenta, como `arn:AWS_partition_name:kms:AWS_region:AWS_account_ID:*`.

- AWS KMS las claves de condición enumeran las claves de AWS KMS condición que puede usar para controlar el acceso a la operación. Las condiciones se especifican en un elemento `Condition` de la política. Para obtener más información, consulte AWS KMS claves de condición. Esta columna también incluye las claves de condición AWS globales que son compatibles con todos los AWS servicios AWS KMS, pero no con todos ellos.

Prueba de los permisos

Para utilizar AWS KMS, debe tener credenciales que AWS pueda utilizar para autenticar las solicitudes a la API. Las credenciales deben incluir permisos para obtener acceso a las claves de KMS y alias. Los permisos vienen determinados por las políticas de claves, las políticas de IAM, las concesiones y los controles de acceso entre cuentas. Además de controlar el acceso a las claves de KMS, puede controlar el acceso a su CloudHSM y a los almacenes de claves personalizados.

Puede especificar el parámetro `DryRun` de la API para comprobar que dispone de los permisos necesarios para utilizar las claves de AWS KMS. También puede utilizar `DryRun` para comprobar

que los parámetros de solicitud de una llamada a la API de AWS KMS estén especificados correctamente.

Temas

¿Cuál es el DryRun parámetro?

`DryRun` es un parámetro de API opcional que se especifica para comprobar que las llamadas a la API de AWS KMS se realizan correctamente. Use `DryRun` para probar la llamada a la API antes de hacer una llamada a AWS KMS. Puede comprobar lo siguiente:

- Que cuenta con los permisos necesarios para utilizar las claves de AWS KMS.
- Que ha especificado correctamente los parámetros de la llamada.

AWS KMS admite el uso del parámetro `DryRun` en determinadas acciones de la API:

- CreateGrant
- Decrypt
- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- ReEncrypt
- RetireGrant
- RevokeGrant
- Sign
- Verificar
- VerifyMac

El uso del parámetro `DryRun` generará cargos y se facturará como una solicitud a la API estándar. Para obtener más información sobre los precios de AWS KMS, consulte Precios de AWS Key Management Service.

Todas las solicitudes a la API que utilizan el parámetro `DryRun` se aplican a la cuota de solicitudes a la API y pueden dar lugar a una excepción de limitación si se supera una cuota de solicitudes a la API. Por ejemplo, llamar a Decrypt con `DryRun` o sin `DryRun` cuenta para la misma cuota de operaciones criptográficas. Consulte Limitar las solicitudes AWS KMS para obtener más información.

Cada llamada a una operación de la API de AWS KMS se captura como un evento y se incluye en un registro de AWS CloudTrail. El resultado de cualquier operación que especifique el `DryRun` parámetro aparece en el CloudTrail registro. Para obtener más información, consulte Registrar llamadas a la AWS KMS API con AWS CloudTrail.

Especificar DryRun con la API

Para usar `DryRun`, especifique el parámetro `–dry-run` en los comandos de la AWS CLI y las llamadas a la API de AWS KMS que admiten el parámetro. Cuando lo haga, AWS KMS comprobará si la llamada se ha realizado correctamente. Las llamadas a AWS KMS que utilicen `DryRun` siempre fallarán y devolverán un mensaje con información sobre el motivo por el que se produjo el error en la llamada. El mensaje puede incluir las siguientes excepciones:

- `DryRunOperationException`: la solicitud se realizaría correctamente si `DryRun` no se especificara.
- `ValidationException`: se produjo un error en la solicitud al especificar un parámetro de API incorrecto.
- `AccessDeniedException`: no tiene permisos para realizar la acción de API especificada en el recurso de KMS.

Por ejemplo, el siguiente comando usa la CreateGrantoperación y crea una concesión que permite a los usuarios autorizados a asumir la `keyUserRole` función llamar a la operación de descifrado en una clave KMS simétrica específica. Se especifica el parámetro `DryRun`.

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --dry-run
```

Llaves para fines especiales

AWS Key Management Service (AWS KMS) admite varios tipos de claves diferentes para diferentes usos.

Cuando crea una AWS KMS key, de forma predeterminada, obtiene una clave de KMS de cifrado simétrica. En AWS KMS, una clave KMS de cifrado simétrico representa una clave de cifrado AES-GCM de 256 bits, excepto en las regiones de China, donde representa una clave de cifrado de 128 bits que utiliza cifrado SM4. El material de claves simétrica nunca deja AWS KMS sin cifrar. A menos que la tarea requiera de forma explícita un cifrado asimétrico o claves HMAC, las claves KMS de cifrado simétricas, que nunca dejan AWS KMS sin cifrar, son una buena opción. Además, los servicios de AWS que se integran con AWS KMS utilizan solo claves KMS de cifrado simétricas para cifrar sus datos. Estos servicios no admiten cifrado con claves de KMS asimétricas.

Puede utilizar una clave KMS de cifrado simétrica en AWS KMS para cifrar, descifrar y volver a cifrar datos, generar claves de datos y pares de claves de datos y generar cadenas de bytes aleatorias. Puede importar su propio material de claves en una clave KMS de cifrado simétrica y crear claves KMS de cifrado simétricas en almacenes de claves personalizadas. Para obtener una tabla en la que se comparan las operaciones que puede realizar en las claves KMS simétricas y asimétricas, consulte Referencia de tipos de claves.

AWS KMS también admite los siguientes tipos de claves KMS para fines especiales:

- Claves RSA asimétricas para criptografía de clave pública
- Claves RSA y ECC asimétricas para la firma y la verificación
- Claves SM2 asimétricas(solo en las regiones de China) para cifrado de clave pública o firma y verificación
- Claves HMAC para generar y verificar códigos de autenticación de mensajes basados en hash
- Claves de varias regiones (simétrica y asimétrica) que funcionan como copias de la misma clave en diferentes Regiones de AWS
- Claves con material de claves importado que usted proporciona
- Claves de un almacén de claves personalizado que está respaldado por un clúster de AWS CloudHSM o un administrador de claves externo ajeno a AWS.

Elección de un tipo de clave KMS

AWS KMS admite varios tipos de claves KMS: claves de cifrado simétricas, claves HMAC simétricas, claves de cifrado asimétricas y claves de firma asimétricas.

Las claves KMS difieren porque contienen material de claves criptográfico diferente.

- Clave de KMS de cifrado simétrica: representa una única clave de cifrado AES-GCM de 256 bits, excepto en las regiones de China, donde representa una clave de cifrado SM4 de 128 bits. El material de claves simétrica nunca deja AWS KMS sin cifrar. Para utilizar la clave KMS de cifrado simétrica, debe llamar a AWS KMS.

  Las claves de cifrado simétricas, que son las claves KMS predeterminadas, son ideales para la mayoría de los usos. Si necesita una clave KMS para proteger sus datos en un Servicio de AWS, utilice una clave de cifrado simétrica a menos que se le indique que utilice otro tipo de clave.
- Clave KMS asimétrica: representa un par de claves privadas y públicas relacionadas de forma matemática que puede utilizar para cifrar y descifrar o para firmar y verificar, pero no para ambas acciones. La clave privada nunca deja AWS KMS sin cifrar. Puede utilizar la clave pública en AWS KMS llamando a las operaciones de la API de AWS KMS o al descargar la clave pública y utilizarla fuera de AWS KMS.
- Clave KMS HMAC (simétrica): representa una clave simétrica de longitud variable que se utiliza para generar y verificar códigos de autenticación de mensajes basados en hash. El material de claves en una clave KMS HMAC nunca deja AWS KMS sin cifrar. Para utilizar su clave KMS HMAC, tiene que llamar a AWS KMS.

El tipo de clave KMS que crea varía en gran medida en función de cómo tiene pensado utilizar la clave KMS, los requisitos de seguridad y los requisitos de autorización. Al crear su clave KMS, recuerde que la configuración criptográfica de la clave KMS, incluido el uso de la clave y la especificación de la clave, se establecen cuando crea la clave KMS y no se puede cambiar.

Utilice las siguientes directrices para determinar qué tipo de clave KMS necesita en función de su caso de uso.

Cifrar y descifrar datos

Utilice una clave KMS simétrica para la mayoría de los casos de uso que requieren cifrar y descifrar datos. El algoritmo de cifrado simétrico que utiliza AWS KMS es rápido, eficaz y asegura la confidencialidad y la autenticidad de los datos. Admite el cifrado autenticado con datos

autenticados adicionales (AAD), definidos como un contexto de cifrado. Este tipo de clave KMS requiere que tanto el remitente como el destinatario de los datos cifrados tengan las credenciales válidas de AWS para llamar a AWS KMS.

Si su caso de uso requiere que los usuarios que no pueden llamar a AWS KMS realicen el cifrado fuera de AWS, las claves KMS asimétricas son una buena opción. Puede distribuir la parte pública de la clave KMS asimétrica para permitir que estos usuarios cifren los datos. Las aplicaciones que necesitan descifrar estos datos pueden utilizar la parte privada de la clave KMS asimétrica en AWS KMS.

Firmar mensajes y verificar firmas

Para firmar mensajes y verificar firmas, tiene que utilizar una clave KMS asimétrica. Puede utilizar una clave KMS con una especificación de clave que representa un par de claves de RSA, un par de claves de curva elíptica (ECC) o un par de claves SM2 (solo en las regiones de China). La especificación de clave que seleccione la determina el algoritmo de firma que desea utilizar. Se recomiendan los algoritmos de firma ECDSA que admiten los pares de claves ECC en lugar de los algoritmos de firma RSA. Sin embargo, es posible que necesite utilizar una especificación clave y un algoritmo de firma específicos para ayudar a los usuarios a verificar las firmas fuera de AWS.

Realizar el cifrado de clave pública

Para realizar el cifrado de clave pública, tiene que utilizar una clave KMS asimétrica con una especificación de clave de RSA, o una especificación de clave SM2 (solo en las regiones de China). Para cifrar los datos de AWS KMS con la clave pública de un par de claves KMS, utilice la operación Encrypt (Cifrar). También puede descargar la clave pública y compartirla con las partes que necesitan cifrar los datos fuera de AWS KMS.

Cuando descarga la clave pública de una clave KMS asimétrica, puede utilizarla fuera de AWS KMS. No obstante, ya no está sujeto a los controles de seguridad que protegen la clave KMS en AWS KMS. Por ejemplo, no puede utilizar las concesiones o las políticas de claves AWS KMS para controlar el uso de la clave pública. Tampoco puede controlar si la clave se utiliza únicamente para el cifrado y descifrado mediante los algoritmos de cifrado que admite AWS KMS. Para obtener más información, consulte Consideraciones especiales para la descarga de claves públicas.

Para descifrar los datos que se han cifrado con la clave pública fuera de AWS KMS, llame a la operación Decrypt (Descifrar). La operación `Decrypt` falla si los datos se cifran con una clave pública de una clave KMS con un uso de la clave de `SIGN_VERIFY`. También fallará si

se cifran mediante un algoritmo que AWS KMS no admite para las especificaciones de clave que se seleccionaron. Para obtener más información sobre las especificaciones de claves y los algoritmos compatibles, consulte Especificaciones de claves asimétricas.

Para evitar estos errores, cualquier persona que utilice una clave pública fuera de AWS KMS debe almacenar la configuración de la clave. La AWS KMS consola y la GetPublicKeyrespuesta proporcionan la información que debe incluir cuando comparte la clave pública.

Generación y verificación de códigos HMAC

Para generar y verificar códigos de autenticación de mensajes basados en hash, utilice una clave KMS HMAC. Al crear una clave HMAC en AWS KMS, AWS KMS crea y protege el material clave y se asegura de que se utilicen los algoritmos MAC correctos para su clave. Los códigos HMAC también se pueden utilizar como números pseudoaleatorios y, en ciertos escenarios, para la firma simétrica y la tokenización.

Las claves KMS HMAC son claves simétricas. Al crear una clave KMS HMAC en la consola de AWS KMS, elija el tipo de clave `Symmetric`.

Uso con servicios de AWS

Para crear una clave KMS para utilizarla con un servicios de AWS que está integrado con AWS KMS, consulte la documentación correspondiente al servicio. Los servicios de AWS que cifran sus datos requieren una clave KMS de cifrado simétrica..

Además de estas consideraciones, las operaciones criptográficas en las claves KMS con diferentes especificaciones de clave tienen diferentes precios y diferentes cuotas de solicitud. Para obtener más información acerca de los precios de AWS KMS, consulte Precios de AWS Key Management Service. Para obtener más información acerca de las cuotas de solicitud, consulte Cuotas de solicitudes.

Seleccionar el uso de la clave

El uso de la clave de una clave KMS determina si la clave KMS se utiliza para el cifrado y el descifrado o para la firma y la verificación de firmas, o para la generación y la verificación de etiquetas HMAC. Cada clave KMS tiene solo un uso de claves. El uso de una clave KMS para más de un tipo de operaciones hace que el producto de todas las operaciones sea más vulnerable a ataques.

Como se muestra en la siguiente tabla, las claves KMS de cifrado simétricas se pueden utilizar solo para cifrar y descifrar. Las claves KMS HMAC solo se pueden utilizar para generar y verificar códigos HMAC. Las claves KMS de curva elíptica (ECC) se pueden utilizar únicamente para firmar y verificar. Tiene que tomar una decisión de uso de claves solo para las claves KMS RSA.

Usos de la clave válidos para los tipos de claves KMS

Tipo de clave KMS	Cifrar y descifrar ENCRYPT_DECRYPT	Firmar y verificar SIGN_VERIFY	Generar y verificar MAC GENERATE_VERIFY_MAC
Claves KMS de cifrado simétricas	✓	⊗	⊗
Claves KMS HMAC (simétricas)	⊗	⊗	✓
Claves KMS asimétricas con pares de claves de RSA	✓	✓	⊗
Claves KMS asimétricas con pares de claves de ECC	⊗	✓	⊗
Claves de KMS asimétricas con pares de claves SM2 (solo en regiones de China)	✓	✓	⊗

En la consola de AWS KMS, primero debe seleccionar el tipo de clave (simétrica o asimétrica) y luego el uso de la clave. El tipo de clave que elija determina qué opciones de uso de clave se muestran. El uso de la clave que elija determina qué especificaciones de clave se muestran, si hay alguno.

Para seleccionar el uso de la clave en la consola de AWS KMS:

- Para las claves KMS de cifrado simétricas (predeterminada), elija Cifrado y descifrado.
- Para las claves KMS HMAC, elija Generate and verify MAC (Generar y verificar MAC).
- Para las claves KMS asimétricas con el material de claves de curva elíptica (ECC), elija Sign and verify (Firmar y verificar).
- Para las claves KMS asimétricas con el material de claves de RSA, elija Encrypt and decrypt (Cifrar y descifrar) o Sign and verify (Firmar y verificar).
- Para las claves KMS asimétricas con el material de claves SM2, elija Encrypt and decrypt (Cifrar y descifrar) o Sign and verify (Firmar y verificar). La especificación de clave SM2 solo está disponible en las regiones de China.

Para permitir que los principales creen claves de KMS solo para un uso de clave determinado, utilice la clave de KeyUsage condición kms:. También puede utilizar la clave de condición `kms:KeyUsage` para permitir que las entidades principales llamen a las operaciones de la API para una clave KMS basada en su uso de claves. Por ejemplo, puede permitir un permiso que deshabilite una clave KMS solo si su uso de clave es SIGN_VERIFY.

Seleccionar la especificación de clave

Cuando crea una clave KMS asimétrica o una clave KMS HMAC, seleccione su especificación de clave. La especificación de clave, que es una propiedad de cada AWS KMS key, representa la configuración criptográfica de su clave KMS. Se selecciona la especificación de clave al crear la clave KMS y no se puede cambiar. Si ha seleccionado una especificación de clave errónea, elimine la clave KMS y cree una nueva.

> **Note**
>
> La especificación de clave para una clave KMS se conocía como “especificación de clave maestra del cliente”. El `CustomerMasterKeySpec` parámetro de la CreateKeyoperación está obsoleto. En su lugar, utilice el parámetro `KeySpec`. La respuesta de las DescribeKeyoperaciones `CreateKey` y incluye un `CustomerMasterKeySpec` elemento `KeySpec` and con el mismo valor.

La especificación de clave determina si la clave KMS es simétrica o asimétrica, el tipo de material de claves de la clave KMS y los algoritmos de cifrado, algoritmos de firma o algoritmos de código

de autenticación de mensajes (MAC) que AWS KMS admite para la clave KMS. La especificación de clave que seleccione suele estar determinada por el caso de uso y los requisitos normativos. Sin embargo, las operaciones criptográficas en las claves KMS con diferentes especificaciones de clave tienen un precio diferente y están sujetas a diferentes cuotas de solicitud. Para obtener más información sobre precios, consulte precios de AWS Key Management Service. Para obtener más información acerca de las cuotas de solicitud, consulte Cuotas de solicitudes.

Para determinar las especificaciones clave que los directores de tu cuenta pueden usar para las claves de KMS, usa la clave de KeySpec condición kms:.

AWS KMS admite las siguientes especificaciones de clave para las claves KMS:

Especificaciones de la clave de cifrado simétricas (predeterminado)

- SYMMETRIC_DEFAULT

Especificaciones de la clave HMAC

- HMAC_224
- HMAC_256
- HMAC_384
- HMAC_512

Especificaciones de clave de RSA (cifrado y descifrado o firma y verificación)

- RSA_2048
- RSA_3072
- RSA_4096

Especificaciones de clave de curva elíptica

- Pares de claves de curva elíptica asimétricas recomendadas por NIST (firma y verificación)
  - ECC_NIST_P256 (secp256r1)
  - ECC_NIST_P384 (secp384r1)
  - ECC_NIST_P521 (secp521r1)
- Otros pares de claves de curva elíptica asimétricas (firma y verificación)
  - ECC_SECG_P256K1 (secp256k1), que se suele utilizar para las criptomonedas.

Especificaciones de clave SM2 (cifrado y descifrado o firma y verificación)

- SM2 (solo en regiones de China)

Claves asimétricas en AWS KMS

AWS KMS admite claves KMS asimétricas que representan un par de claves públicas y privadas de RSA, de curva elíptica (ECC), o un par de claves públicas y privadas de SM2 (solo en las regiones de China) relacionado matemáticamente. Estos pares de claves se generan en módulos de seguridad de hardware certificados de AWS KMS con el Programa de validación de módulos criptográficos FIPS 140-2, excepto en las regiones China (Pekín) y China (Ningxia). La clave privada nunca deja las HSM de AWS KMS sin cifrar. También puede descargar la clave pública para distribución y utilizarla fuera de AWS. Puede crear las claves KMS asimétricas para el cifrado y el descifrado o para la firma y la verificación, pero no para ambas acciones.

Puede crear y administrar las claves KMS asimétricas de su Cuenta de AWS, incluida la configuración de políticas de claves, políticas de IAM y concesiones que controlan el acceso a las claves, habilitando y deshabilitando las claves KMS, creando etiquetas y alias, y eliminando las claves KMS. Además, puede auditar todas las operaciones que utilizan o administran sus claves KMS asimétricas dentro de AWS en los registros de AWS CloudTrail.

AWS KMS también ofrece pares de claves de datos asimétricas diseñados para su uso en una criptografía del lado del cliente fuera de AWS KMS. La clave privada de una clave de datos asimétrica se encuentra protegida por una clave de KMS de cifrado simétrica en AWS KMS.

En este tema se explica cómo funcionan las claves de KMS asimétricas, en qué difieren de otras claves de KMS y cómo decidir qué tipo de clave de KMS necesita para proteger sus datos. También se explica cómo funcionan los pares de claves de datos asimétricos y cómo se pueden utilizar fuera de AWS KMS.

Regiones

Las claves KMS asimétricas y los pares de claves de datos asimétricas se admiten en todas las Regiones de AWS que admite AWS KMS.

Más información

- Para crear claves KMS asimétricas, consulte Creación de claves KMS asimétricas. Para crear claves KMS de cifrado simétricas, consulte Crear claves.
- Para crear claves KMS asimétricas de varias regiones, consulte Creación de claves de varias regiones.
- Para averiguar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

- Para obtener una tabla que compara las operaciones de la API de AWS KMS que se aplican a cada tipo de KMS, consulte the section called “Referencia de tipos de claves”.
- Para controlar el acceso a las especificaciones de clave, el uso de la clave, los algoritmos de cifrado y los algoritmos de firma que las entidades principales de la cuenta pueden utilizar en las claves KMS, consulte the section called “AWS KMS claves de condición”.
- Para obtener información acerca de las cuotas que se aplican a los diferentes tipos de claves KMS, consulte the section called “Cuotas de solicitudes”.
- Para aprender a firmar mensajes y verificar firmas con las claves KMS asimétricas, consulte Firma digital con la nueva función de claves asimétricas de AWS KMS en el Blog de seguridad de AWS.

Temas

Claves de KMS asimétricas

Puede crear una clave KMS asimétrica en AWS KMS. Una clave KMS asimétrica representa un par de claves privadas y públicas relacionadas matemáticamente. Puede entregar la clave pública a cualquiera, aunque no sea de confianza, pero la clave privada debe ser secreta.

En una clave KMS asimétrica, la clave privada se crea en AWS KMS y nunca deja AWS KMS sin cifrar. Para utilizar la clave privada, tiene que llamar a AWS KMS. Puede utilizar la clave pública en AWS KMS llamando a las operaciones de la API de AWS KMS. También puede descargar la clave pública y utilizarla fuera de AWS KMS.

Si su caso de uso requiere que los usuarios que no pueden llamar a AWS KMS realicen el cifrado fuera de AWS, las claves KMS asimétricas son una buena opción. Sin embargo, si crea una clave KMS para cifrar los datos que almacena o administra en un servicio de AWS, utilice una clave KMS de cifrado simétrica. Los servicios de AWS que se están integrados con AWS KMS utilizan solo claves KMS de cifrado simétricas para cifrar sus datos. Estos servicios no admiten cifrado con claves de KMS asimétricas.

AWS KMS es compatible con tres tipos de claves KMS asimétricas.

- Claves de KMS RSA: una clave KMS con un par de claves RSA para cifrar y descifrar o para firmar y verificar (pero no para ambas opciones). AWS KMS admite diferentes longitudes de claves para diferentes requisitos de seguridad.
- Claves KMS de curva elíptica (ECC): una clave KMS con un par de claves de curva elíptica para firmar y verificar. AWS KMS admite diferentes curvas utilizadas habitualmente.
- Claves SM2 KMS (solo en las regiones de China): una clave KMS con un par de claves SM2 para cifrar y descifrar o para firmar y verificar (pero no para ambas acciones).

Para obtener ayuda para elegir la configuración de clave asimétrica, consulte Elección de un tipo de clave KMS. Para obtener detalles técnicos acerca de los algoritmos de cifrado y firma que admite AWS KMS para las claves KMS de RSA, consulte Especificaciones de clave de RSA. Para obtener detalles técnicos acerca de los algoritmos de firma que admite AWS KMS para las claves KMS de ECC, consulte Especificaciones de clave de curva elíptica. Para obtener detalles técnicos acerca de los algoritmos de cifrado y firma que admite AWS KMS para las claves KMS de SM2 (solo en las regiones de China), consulte las Especificaciones de clave SM2.

Para obtener una tabla en la que se comparan las operaciones que puede realizar en las claves KMS simétricas y asimétricas, consulte Comparación de claves KMS simétricas y asimétricas. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Regiones

Las claves de KMS asimétricas y los pares de claves de datos asimétricas se admiten en todas las Regiones de AWS que admite AWS KMS.

Creación de claves KMS asimétricas

Puede crear claves KMS asimétricas en la AWS KMS consola, mediante la CreateKeyAPI o mediante una AWS CloudFormationplantilla. Una clave KMS asimétrica representa un par de claves pública y privada que se puede utilizar para el cifrado o la firma. La clave privada se mantiene dentro de la AWS KMS. Para descargar la clave pública para utilizarla fuera de AWS KMS, consulte Descargar claves públicas.

Si va a crear una clave KMS para cifrar los datos que almacena o administra en un servicio de AWS, utilice una clave KMS de cifrado simétrica. Los servicios de AWS que se integran con AWS KMS no admiten clave KMS asimétricas. Para obtener ayuda para decidir si crear una clave KMS simétrica o asimétrica, consulte Elección de un tipo de clave KMS.

Para obtener información sobre los permisos necesarios para crear claves de KMS, consulte Permisos para crear claves KMS.

Temas

- Creación de claves KMS asimétricas (consola)
- Creación de claves KMS asimétricas (API de AWS KMS)

Creación de claves KMS asimétricas (consola)

Puede utilizar la AWS Management Console para crear AWS KMS keys asimétricas (claves KMS). Cada clave KMS asimétrica representa un par de claves públicas y privadas.

> **Important**
>
> No incluya información confidencial en el alias, la descripción ni las etiquetas. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija Create key.
5. Para crear una clave KMS asimétrica, en Key Type (Tipo de clave), seleccione Asymmetric (Asimétrica).

   Para obtener información acerca de cómo crear una clave KMS de cifrado simétrica en la consola de AWS KMS, consulte Creación de claves KMS de cifrado simétricas (consola).
6. Para crear una clave KMS asimétrica para el cifrado de claves públicas, en Key Usage (Uso de claves), elija Encrypt and decrypt (Cifrar y descifrar). O bien, para crear una clave KMS asimétrica para firmar mensajes y verificar firmas, en Key Usage (Uso de claves), elija Sign and verify (Firmar y verificar).

   Para obtener ayuda sobre cómo elegir un valor de uso de clave, consulte Seleccionar el uso de la clave.

7. Seleccione una especificación (Key spec [Especificación de clave]) para su clave KMS asimétrica.

   A menudo, la especificación de clave que seleccione está determinada por requisitos normativos, de seguridad o empresariales. También puede estar influenciado por el tamaño de los mensajes que necesita cifrar o firmar. En general, las claves de cifrado más largas son más resistentes a los ataques de fuerza bruta.

   Para obtener ayuda para elegir una especificación de clave, consulte Seleccionar la especificación de clave.

8. Elija Siguiente.

9. Escriba un alias para la clave KMS El nombre del alias no puede empezar por **`aws/`**. El prefijo **`aws/`** está reservado para Amazon Web Services y representa las Claves administradas por AWS de su cuenta.

   Un alias es un nombre sencillo que puede utilizar para identificar la clave KMS en la consola y en algunos API de AWS KMS. Le recomendamos que elija un alias que indique el tipo de datos que piensa proteger o la aplicación que piensa usar con la clave KMS.

   Los alias son necesarios para crear una clave KMS en la AWS Management Console. No puede especificar un alias al usar la CreateKeyoperación, pero puede usar la consola o la CreateAliasoperación para crear un alias para una clave de KMS existente. Para obtener más detalles, consulte Uso de alias.

10. (Opcional) Escriba una descripción de la clave KMS.

    Escriba una descripción que explique el tipo de datos que piensa proteger o la aplicación que piensa usar con la clave KMS.

    Puede agregar una descripción ahora o actualizarla en cualquier momento, a menos que el estado de la clave sea `Pending Deletion` o `Pending Replica Deletion`. Para añadir, cambiar o eliminar la descripción de una clave gestionada por el cliente existente, edite la descripción en la operación AWS Management Console o utilice esta UpdateKeyDescriptionoperación.

11. (Opcional) Escriba una clave de etiqueta y un valor de etiqueta opcional. Para agregar más de una etiqueta a la clave KMS, elija Add tag (Agregar etiqueta).

    Cuando se agregan etiquetas a los recursos de AWS, AWS genera un informe de asignación de costos con el uso y los costos agregados por etiquetas. Las etiquetas también pueden utilizarse

para controlar el acceso a una clave KMS. Para obtener información acerca del etiquetado de claves KMS, consulte Etiquetado de claves y ABAC para AWS KMS.

12. Elija Siguiente.
13. Seleccione los usuarios y roles de IAM que pueden administrar la clave de KMS.

> **Note**
>
> Esta política de claves proporciona a la Cuenta de AWS control total de esta clave KMS. Permite a los administradores de cuentas utilizar las políticas de IAM para dar permiso a otras entidades principales para administrar la clave KMS. Para obtener más detalles, consulte the section called “Política de claves predeterminada”.
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

14. (Opcional) Para evitar que los usuarios y los roles de IAM seleccionados eliminen esta clave de KMS, en la sección Eliminación de claves situada en la parte inferior de la página, desactive la casilla Permitir que los administradores de claves eliminen esta clave.
15. Elija Siguiente.
16. Seleccione los usuarios y roles de IAM que pueden usar la clave de KMS en operaciones criptográficas.

> **Note**
>
> Esta política de claves proporciona a la Cuenta de AWS control total de esta clave KMS. Permite a los administradores de cuentas utilizar las políticas de IAM para dar permiso a otras entidades principales para utilizar la clave KMS. Para obtener más detalles, consulte the section called “Política de claves predeterminada”.
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

17. (Opcional) Puede permitir que otras cuentas de Cuentas de AWS usen esta clave de KMS en operaciones criptográficas. Para ello, en la parte inferior de la página de la sección Other Cuentas de AWS (Otras), elija Add another Cuenta de AWS (Agregar otra) e ingrese el número

de identificación de Cuenta de AWS de una cuenta externa. Para agregar varias cuentas externas, repita este paso.

> **Note**
>
> Para permitir que las entidades principales de las cuentas externas usen la clave KMS, los administradores de la cuenta externa también deben crear las políticas de IAM que proporcionan estos permisos. Para obtener más información, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS.

18. Seleccione Siguiente.
19. Revise los ajustes de clave que ha elegido. Aún puede volver atrás y cambiar todos los ajustes.
20. Elija Finish (Finalizar) para crear la clave KMS.

Creación de claves KMS asimétricas (API de AWS KMS)

Puede utilizar la CreateKeyoperación para crear una asimétricaAWS KMS key. En estos ejemplos, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Al crear una clave KMS asimétrica, debe especificar el parámetro `KeySpec`, que determina el tipo de claves que cree. Además, debe especificar un valor `KeyUsage` de ENCRYPT_DECRYPT o SIGN_VERIFY. No puede cambiar estas propiedades después de que se cree la clave de KMS.

La `CreateKey` operación no le permite especificar un alias, pero puede utilizarla para crear un alias para la CreateAliasnueva clave de KMS.

> **Important**
>
> No incluya información confidencial en los campos `Description` o `Tags`. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

En el siguiente ejemplo se utiliza la operación `CreateKey` para crear una clave KMS asimétrica de claves RSA de 4096 bits diseñadas para el cifrado de claves públicas.

```
$ aws kms create-key --key-spec RSA_4096 --key-usage ENCRYPT_DECRYPT
{
    "KeyMetadata": {
```

```
        "KeyState": "Enabled",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "Description": "",
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "CreationDate": 1569973196.214,
        "MultiRegion": false,
        "KeySpec": "RSA_4096",
        "CustomerMasterKeySpec": "RSA_4096",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "EncryptionAlgorithms": [
            "RSAES_OAEP_SHA_1",
            "RSAES_OAEP_SHA_256"
        ],
        "AWSAccountId": "111122223333",
        "Origin": "AWS_KMS",
        "Enabled": true
    }
}
```

El comando del siguiente ejemplo crea una clave KMS asimétrica que representa un par de claves ECDSA utilizadas para la firma y verificación. No se puede crear un par de claves de curva elíptica para el cifrado y el descifrado.

```
$ aws kms create-key --key-spec ECC_NIST_P521 --key-usage SIGN_VERIFY
{
    "KeyMetadata": {
        "KeyState": "Enabled",
        "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
        "CreationDate": 1570824817.837,
        "Origin": "AWS_KMS",
        "SigningAlgorithms": [
            "ECDSA_SHA_512"
        ],
        "Arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
        "AWSAccountId": "111122223333",
        "KeySpec": "ECC_NIST_P521",
        "CustomerMasterKeySpec": "ECC_NIST_P521",
        "KeyManager": "CUSTOMER",
        "Description": "",
        "Enabled": true,
```

```
        "MultiRegion": false,
        "KeyUsage": "SIGN_VERIFY"
    }
}
```

Descargar claves públicas

Puede ver, copiar y descargar la clave pública de un par de claves KMS asimétricas al utilizar la AWS Management Console o la API de AWS KMS. Debe tener el permiso `kms:GetPublicKey` en la clave KMS asimétrica.

Cada par de claves KMS asimétricas consta de una clave privada que nunca deja AWS KMS sin cifrar y una clave pública que puede descargar y compartir.

Puede compartir una clave pública para permitir que otros cifren datos fuera de AWS KMS que puede descifrar solo con su clave privada. O bien, para permitir que otros verifiquen una firma digital fuera del AWS KMS que haya generado con su clave privada.

Cuando utiliza la clave pública en su clave KMS asimétrica dentro de AWS KMS, se beneficia de la autenticación, autorización y registro que forman parte de cada operación de AWS KMS. También reduce el riesgo de cifrar datos que no se pueden descifrar. Estas características no son efectivas fuera de AWS KMS. Para obtener más detalles, consulte Consideraciones especiales para descargar claves públicas.

> **Tip**
>
> ¿Busca claves de datos o claves SSH? En este tema se explica cómo administrar claves asimétricas en AWS Key Management Service, donde la clave privada no es exportable. Para ver los pares de claves de datos exportables en los que la clave privada está protegida por una clave KMS de cifrado simétrico, consulte. GenerateDataKeyPair Para obtener ayuda sobre la descarga de la clave pública asociada a una instancia de Amazon EC2, consulte Recuperar la clave pública en la Guía del usuario de Amazon EC2 para instancias de Linux y Guía del usuario de Amazon EC2 para instancias de Windows.

Temas

- Consideraciones especiales para descargar claves públicas
- Descargar una clave pública (consola)
- Descargar una clave pública (API de AWS KMS)

Consideraciones especiales para descargar claves públicas

Para proteger sus claves KMS, AWS KMS proporciona controles de acceso, cifrado autenticado y registros detallados de cada operación. AWS KMS también le permite evitar el uso de claves KMS, temporal o permanentemente. Finalmente, las operaciones de AWS KMS están diseñadas para minimizar el riesgo de cifrar datos que no se pueden descifrar. Estas características no están disponibles cuando utiliza claves públicas descargadas fuera de AWS KMS.

Autorización

Las políticas de claves y las políticas de IAM que controlan el acceso a la clave KMS dentro de AWS KMS no tienen efecto en las operaciones realizadas fuera de AWS. Cualquier usuario que pueda obtener la clave pública puede utilizarla fuera de AWS KMS aunque no tenga permiso para cifrar datos o verificar firmas con la clave KMS.

Restricciones de uso de las claves

Las restricciones de uso de las claves no son efectivas fuera de AWS KMS. Si llama a la operación Encrypt (Cifrado) con una clave KMS que tiene `KeyUsage` de `SIGN_VERIFY`, la operación de AWS KMS falla. Sin embargo, si cifra datos fuera de AWS KMS con una clave pública de una clave KMS con un `KeyUsage` de `SIGN_VERIFY`, los datos no se pueden descifrar.

Restricciones del algoritmo

Las restricciones a los algoritmos de cifrado y firma compatibles con AWS KMS no son efectivas fuera de AWS KMS. Si cifra los datos con la clave pública de una clave KMS fuera de AWS KMS y utiliza un algoritmo de cifrado que no es compatible con AWS KMS, no se pueden descifrar los datos.

Desactivar y eliminar claves KMS

Las acciones que puede tomar para evitar el uso de la clave KMS en una operación criptográfica en AWS KMS no evitan que nadie utilice la clave privada fuera de AWS KMS. Por ejemplo, desactivar una clave KMS, programar la eliminación de una clave KMS, eliminar una clave KMS o eliminar el material de claves de una clave KMS no tienen ningún efecto en una clave pública fuera de AWS KMS. Si elimina una clave KMS asimétrica o elimina o pierde su material de claves, los datos que cifra con una clave pública fuera de AWS KMS son irrecuperables.

Registro

Registros de AWS CloudTrail que registran cada operación de AWS KMS, incluida la solicitud, la respuesta, la fecha, el tiempo y el usuario autorizado, no registran el uso de la clave pública fuera de AWS KMS.

Verificación sin conexión con pares de claves SM2 (solo en las regiones de China)

Para verificar una firma fuera de AWS KMS con una clave pública SM2, debe especificar el identificador distintivo. Por defecto, AWS KMS utiliza 1234567812345678 como identificador distintivo. Para más información, consulte Verificación sin conexión con pares de claves SM2 (solo en las regiones de China)

Descargar una clave pública (consola)

Puede utilizar la AWS Management Console para ver, copiar y descargar la clave pública en una clave KMS asimétrica en su cuenta de Cuenta de AWS. Para descargar la clave pública de una clave KMS asimétrica en una cuenta de Cuenta de AWS diferente, utilice la API de AWS KMS.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija el alias o el ID de clave de una clave KMS asimétrica.
5. Elija la pestaña Cryptographic configuration (Configuración criptográfica). Registre los valores de los campos Key spec (Especificación de clave), Key usage (Uso de claves) y Encryption algorithms (Algoritmos de cifrado) o Signing Algorithms (Algoritmos de firma). Tendrá que utilizar estos valores para utilizar la clave pública fuera de AWS KMS. Asegúrese de compartir esta información cuando comparta la clave pública.
6. Seleccione la pestaña Public key (Clave pública).
7. Para copiar la clave pública al portapapeles, elija Copy (Copiar). Para descargar la clave pública en un archivo, elija Download (Descargar).

Descargar una clave pública (API de AWS KMS)

La GetPublicKeyoperación devuelve la clave pública en una clave KMS asimétrica. También devuelve información crítica que necesita para utilizar la clave pública correctamente fuera de AWS KMS, incluido el uso de claves y algoritmos de cifrado. Asegúrese de guardar estos valores y compartirlos siempre que comparta la clave pública.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Para especificar una clave KMS, utilice el ID de la clave, ARN de la clave, nombre de alias o ARN del alias. Cuando utilice un nombre del alias, utilice el prefijo alias/. Para especificar una clave KMS en una cuenta de Cuenta de AWS diferente, debe utilizar su clave de ARN o su alias de ARN.

Antes de ejecutar este comando, sustituya el nombre del alias de ejemplo por un identificador válido para la clave KMS. Para ejecutar este comando, debe tener permisos de `kms:GetPublicKey` en la clave KMS.

```
$ aws kms get-public-key --key-id alias/example_RSA_3072

{
    "KeySpec": "RSA_3072",
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "EncryptionAlgorithms": [
        "RSAES_OAEP_SHA_1",
        "RSAES_OAEP_SHA_256"
    ],
    "PublicKey": "MIIBojANBgkqhkiG..."
}
```

Identificación de claves KMS asimétricas

Para determinar si una clave KMS concreta es una clave KMS asimétrica, busque su tipo de clave o especificación de clave. Puede utilizar la consola de AWS KMS o la API de AWS KMS.

Algunos de estos métodos también le muestran otros aspectos de la configuración criptográfica de una clave KMS, incluido su uso de claves y los algoritmos de cifrado o de firma que admite la clave KMS. Puede ver la configuración criptográfica de una clave KMS existente, pero no puede cambiarla.

Para obtener información general sobre cómo ver las clave KMS, como ordenar, filtrar y elegir columnas para la pantalla de la consola, consulte Visualización de las claves KMS en la consola.

Temas

- Buscar el tipo de clave en la tabla de claves KMS
- Buscar el tipo de clave en la página de detalles

- Buscar la especificación de clave mediante la API de AWS KMS

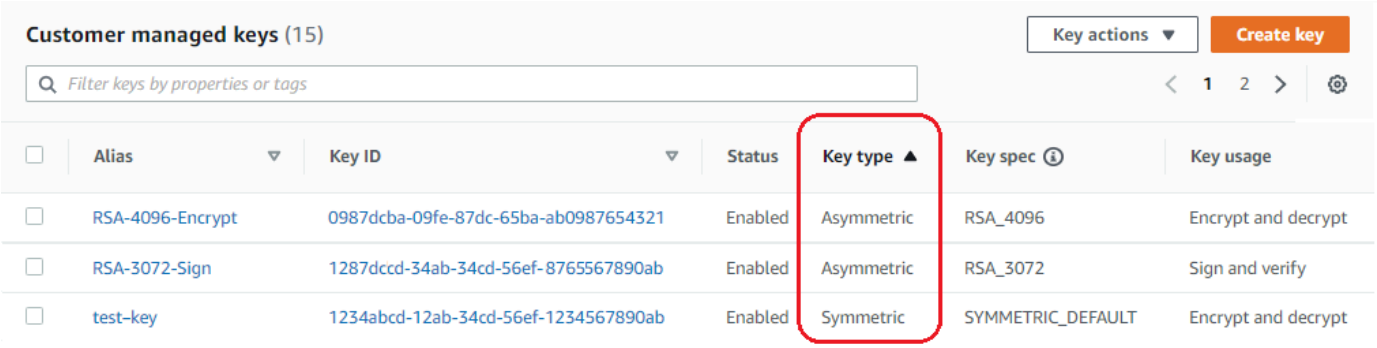
Buscar el tipo de clave en la tabla de claves KMS

En la consola de AWS KMS, la columna Key type (Tipo de clave) muestra si cada clave KMS es simétrica o asimétrica. Puede agregar una columna Key type (Tipo de clave) a la tabla de clave KMS en las páginas Customer managed keys (Claves administradas por el cliente) o Claves administradas por AWS en la consola.

Para identificar claves KMS simétricas y asimétricas en la tabla de clave KMS, utilice el procedimiento siguiente.

1. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente). Si desea ver las claves de su cuenta que AWS crea y administra, en el panel de navegación, elija claves administradas por AWS.
4. Las columnas Key type (Tipo de clave) muestran si cada clave KMS es simétrica o asimétrica. También puede ordenar y filtrar por el valor Key type (Tipo de clave).

   Si la columna Key type (Tipo de clave) no aparece en la tabla de clave KMS, elija el icono de engranaje en la esquina superior derecha de la página, elija Key type (Tipo de clave), y, a continuación, elija Confirm (Confirmar). También puede agregar las columnas Key spec (Especificación de clave) y Key usage (Uso de clave).



Buscar el tipo de clave en la página de detalles

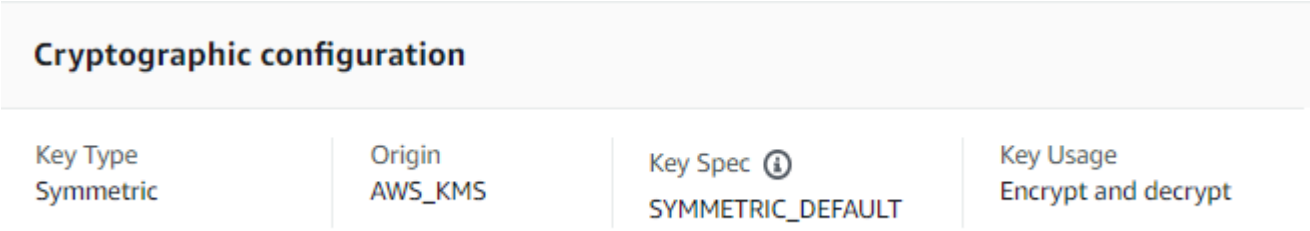
En la consola de AWS KMS, la página de detalles de cada clave KMS incluye una pestaña Cryptographic Configuration (Configuración criptográfica) que muestra el tipo de clave (simétrica o asimétrica) y otros detalles criptográficos sobre la clave KMS.

Para identificar claves KMS simétricas y asimétricas en la página de detalles de una clave KMS, utilice el procedimiento siguiente.

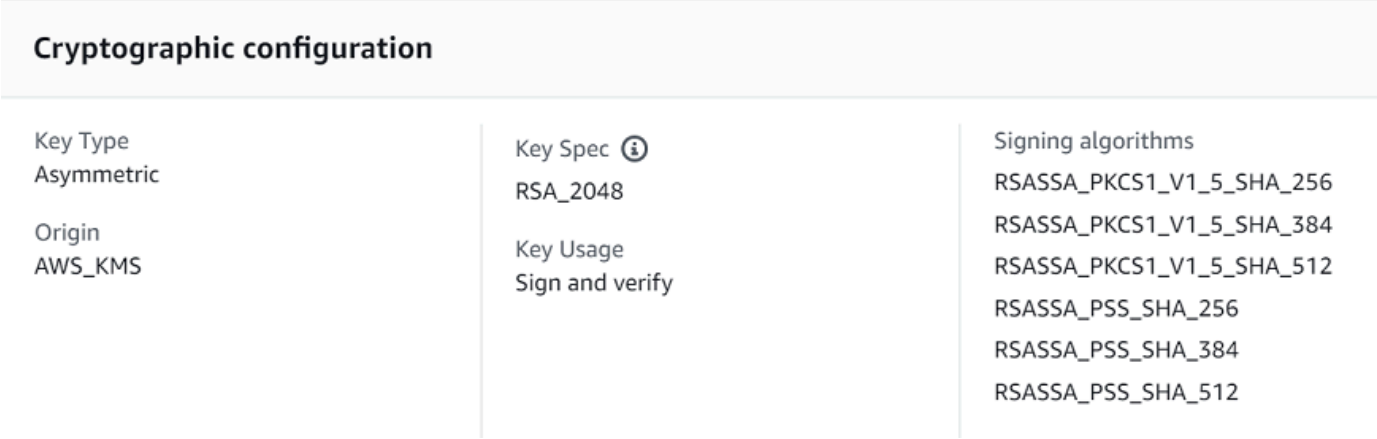
1. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. Si desea ver las claves de la cuenta que usted crea y administra, en el panel de navegación, elija Customer managed keys (Claves administradas por el cliente). Si desea ver las claves de su cuenta que AWS crea y administra, en el panel de navegación, elija claves administradas por AWS.
4. Elija el alias o el ID de clave de una clave KMS.
5. Elija la pestaña Configuración criptográfica. Las pestañas están debajo de la sección General configuration (Configuración general).

   La pestaña de Cryptographic configuration (Configuración criptográfica) incluye el Key type (Tipo de clave), que indica si es simétrica o asimétrica. También muestra otros detalles sobre la clave KMS, incluido el Key Usage (Uso de claves), que indica si una clave KMS se puede utilizar para cifrar y descifrar o para firmar y verificar. Para claves KMS asimétricos, muestra los algoritmos de cifrado o algoritmos de firma que admite la clave KMS.

   Por ejemplo, la siguiente es una pestaña de Cryptographic configuration (Configuración criptográfica) de ejemplo para una clave KMS de cifrado simétrica.



   A continuación se muestra un ejemplo de la pestaña de Cryptographic configuration (Configuración criptográfica) para una clave KMS asimétrica de RSA que se utiliza para la firma y la verificación.



Buscar la especificación de clave mediante la API de AWS KMS

Para determinar si una clave KMS es simétrica o asimétrica, utilice la DescribeKeyoperación. El campo `KeySpec` de la respuesta contiene la especificación de clave de la clave KMS. Para una clave KMS de cifrado simétrica, el valor de `KeySpec` es `SYMMETRIC_DEFAULT`. Otros valores indican una clave KMS asimétrica o una clave KMS HMAC.

> **Note**
>
> Este miembro `CustomerMasterKeySpec` está obsoleto. En su lugar, utilice `KeySpec`. Para evitar que se produzcan cambios, la respuesta `DescribeKey` incluye los miembros `KeySpec` y `CustomerMasterKeySpec` con el mismo valor.

Por ejemplo, `DescribeKey` devuelve la siguiente respuesta para una clave KMS de cifrado simétrica. El valor de `KeySpec` es `SYMMETRIC_DEFAULT`.

```
{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "KeyId": "0987dcba-09fe-87dc-65ba-ab0987654321",
    "Arn": "arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321",
    "CreationDate": 1496966810.831,
    "Enabled": true,
    "Description": "",
    "KeyState": "Enabled",
    "Origin": "AWS_KMS",
```

```
    "KeyManager": "CUSTOMER",
    "MultiRegion": false,
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "EncryptionAlgorithms": [
        "SYMMETRIC_DEFAULT"
    ]
  }
}
```

La respuesta `DescribeKey` para una clave KMS asimétrica de RSA utilizada en la firma y verificación es similar a este ejemplo. El valor `KeySpec` es RSA_2048 y el `KeyUsage` es `SIGN_VERIFY`. El elemento `SigningAlgorithms` indica los algoritmos de firma válidos para la clave KMS.

```
{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": 1571767572.317,
    "CustomerMasterKeySpec": "RSA_2048",
    "Enabled": false,
    "Description": "",
    "KeyState": "Disabled",
    "Origin": "AWS_KMS",
    "MultiRegion": false,
    "KeyManager": "CUSTOMER",
    "KeySpec": "RSA_2048",
    "KeyUsage": "SIGN_VERIFY",
    "SigningAlgorithms": [
        "RSASSA_PKCS1_V1_5_SHA_256",
        "RSASSA_PKCS1_V1_5_SHA_384",
        "RSASSA_PKCS1_V1_5_SHA_512",
        "RSASSA_PSS_SHA_256",
        "RSASSA_PSS_SHA_384",
        "RSASSA_PSS_SHA_512"
    ]
  }
}
```

Especificaciones de claves asimétricas

En los siguientes temas se incluye información técnica acerca de las especificaciones de clave que AWS KMS admite para las claves KMS asimétricas. Se incluye información sobre la especificación de la clave SYMMETRIC_DEFAULT para claves de cifrado simétricas para comparar.

Temas

Especificaciones de clave de RSA

Cuando utiliza una especificación de clave de RSA, AWS KMS crea una clave KMS asimétrica con un par de claves de RSA. La clave privada nunca deja AWS KMS sin cifrar. Puede utilizar la clave pública en AWS KMS o descargarla para utilizarla fuera de AWS KMS.

> **Warning**
>
> Cuando cifre datos fuera de AWS KMS, asegúrese de que puede descifrar el texto cifrado. Si utiliza la clave pública de una clave KMS que se ha eliminado de AWS KMS, la clave pública de una clave KMS configurada para firma y verificación o un algoritmo de cifrado que no es compatible con la clave KMS, los datos son irrecuperables.

En AWS KMS, puede utilizar las claves KMS asimétricas con pares de claves de RSA para el cifrado y el descifrado o para la firma y la verificación, pero no para ambas acciones. Esta propiedad, conocida como uso de la clave, se determina independientemente de la especificación de clave, pero tiene que tomar esta decisión antes de seleccionar una especificación de clave.

AWS KMS admite las siguientes especificaciones de clave de RSA para el cifrado y el descifrado o para la firma y la verificación:

- RSA_2048
- RSA_3072

- RSA_4096

Las especificaciones de clave de RSA varían en la longitud de la clave de RSA en bits. La especificación de clave de RSA que seleccione puede estar determinada por las normas de seguridad o los requisitos de la tarea. Por regla general, utilice la clave más grande que sea práctica y asequible para la tarea. Las operaciones criptográficas en claves KMS con diferentes especificaciones de clave de RSA tienen un precio diferente. Para obtener información acerca de los precios de AWS KMS, consulte Precios del servicio de gestión de claves de AWS. Para obtener más información acerca de las cuotas de solicitud, consulte Cuotas de solicitudes.

Especificaciones de clave de RSA para el cifrado y el descifrado

Cuando se utiliza una clave KMS asimétrica de RSA para el cifrado y el descifrado, se cifra con la clave pública y se descifra con la clave privada. Cuando llama a la operación `Encrypt` en AWS KMS para una clave KMS de RSA, AWS KMS utiliza la clave pública del par de claves de RSA y el algoritmo de cifrado que especifique para cifrar los datos. Para descifrar el texto cifrado, llame a la operación `Decrypt` y especifique la misma clave KMS y el mismo algoritmo de cifrado. AWS KMS utiliza la clave privada del par de claves de RSA para descifrar los datos.

También puede descargar la clave pública y utilizarla para cifrar los datos fuera de AWS KMS. Asegúrese de utilizar un algoritmo de cifrado que AWS KMS admita para las claves KMS de RSA. Para descifrar el texto cifrado, llame a la función `Decrypt` con la misma clave KMS y el mismo algoritmo de cifrado.

AWS KMS admite dos algoritmos de cifrado para las claves KMS con especificaciones de clave de RSA. Estos algoritmos, que se definen en PKCS #1 v2.2, difieren en la función hash que utilizan de forma interna. En AWS KMS, los algoritmos RSAES_OAEP siempre utilizan la misma función hash para los fines de hash y para la función de generación de máscaras (MGF1). Tiene que especificar un algoritmo de cifrado cuando llame a las operaciones Encrypt y Decrypt. Puede elegir un algoritmo diferente para cada solicitud.

Algoritmos de cifrado compatibles con las especificaciones de clave de RSA

Algoritmo de cifrado	Descripción del algoritmo
RSAES_OAEP_SHA_1	PKCS #1 v2.2, sección 7.1. Cifrado de RSA con relleno OAEP mediante SHA-1 para la función de generación de máscaras MGF1 y hash, junto con una etiqueta vacía.

Algoritmo de cifrado	Descripción del algoritmo
RSAES_OAEP_SHA_256	PKCS #1, sección 7.1. Cifrado de RSA con relleno OAEP mediante SHA-256 para la función de generación de máscaras MGF1 y hash, junto con una etiqueta vacía.

No puede configurar una clave KMS para utilizar un algoritmo de cifrado específico. Sin embargo, puede usar la condición kms: EncryptionAlgorithm policy para especificar los algoritmos de cifrado que los principales pueden usar con la clave KMS.

Para obtener los algoritmos de cifrado de una clave KMS, consulte la configuración criptográfica de la clave KMS en la AWS KMS consola o utilice la DescribeKeyoperación. AWS KMStambién proporciona las especificaciones clave y los algoritmos de cifrado al descargar la clave pública, ya sea en la AWS KMS consola o mediante la GetPublicKeyoperación.

Puede elegir una especificación de clave de RSA en función de la longitud de los datos de texto no cifrado que puede cifrar en cada solicitud. En la siguiente tabla se muestra el tamaño máximo, en bytes, del texto no cifrado que puede cifrar en una única llamada a la operación Encrypt. Los valores varían en función de la especificación de clave y el algoritmo de cifrado. Para realizar una comparación, puede utilizar una clave KMS de cifrado simétrica para cifrar hasta 4096 bytes a la vez.

Para calcular la longitud de texto no cifrado máxima en bytes para estos algoritmos, utilice la siguiente fórmula: (*key_size_in_bits* / 8) - (2 * *hash_length_in_bits*/8) - 2. Por ejemplo, para RSA_2048 con SHA-256, el tamaño máximo de texto no cifrado en bytes es (2048/8) - (2 * 256/8) -2 = 190.

Tamaño máximo de texto no cifrado (en bytes) en una operación de cifrado

	Algoritmo de cifrado	
Especificación de clave	RSAES_OAEP_SHA_1	RSAES_OAEP_SHA_256
RSA_2048	214	190
RSA_3072	342	318
RSA_4096	470	446

Especificaciones de clave de RSA para la firma y la verificación

Cuando se utiliza una clave KMS asimétrica de RSA para la firma y la verificación, genera la firma para un mensaje con la clave privada y verifica la firma con la clave pública.

Cuando llama a la operación `Sign` en AWS KMS para una clave KMS asimétrica, AWS KMS utiliza la clave privada del par de claves de RSA, el mensaje y el algoritmo de firma que especifique para generar una firma. Para verificar la firma, llame a la operación Verify. Especifique la firma, la misma clave KMS, el mismo mensaje y el mismo algoritmo de firma. A continuación, AWS KMS utiliza la clave pública del par de claves de RSA para verificar la firma. También puede descargar la clave pública y utilizarla para verificar la firma fuera de AWS KMS.

AWS KMS admite los siguientes algoritmos de firma para todas las claves KMS con una especificación de clave de RSA. Tiene que especificar un algoritmo de firma cuando llame a las operaciones Sign y Verify. Puede elegir un algoritmo diferente para cada solicitud. Al firmar con pares de claves de RSA, se prefieren los algoritmos RSASSA-PSS. Incluimos los algoritmos RSASSA-PKCS1-v1_5 para garantizar la compatibilidad con las aplicaciones existentes.

Algoritmos de firma compatibles con las especificaciones de clave de RSA

Algoritmo de firma	Descripción del algoritmo
RSASSA_PSS_SHA_256	PKCS #1 v2.2, sección 8.1, firma de RSA con relleno PSS mediante SHA-256 para la función de generación de máscaras MGF1 y resumen de mensaje, junto con una sal de 256 bits.
RSASSA_PSS_SHA_384	PKCS #1 v2.2, sección 8.1, firma de RSA con relleno PSS mediante SHA-384 para la función de generación de máscaras MGF1 y resumen de mensaje, junto con una sal de 384 bits.
RSASSA_PSS_SHA_512	PKCS #1 v2.2, sección 8.1, firma de RSA con relleno PSS mediante SHA-512 para la función de generación de máscaras MGF1 y resumen de mensaje, junto con una sal de 512 bits.
RSASSA_PKCS1_V1_5_SHA_256	PKCS #1 v2.2, sección 8.2, firma de RSA con relleno PKCS #1 v1.5 y SHA-256

Algoritmo de firma	Descripción del algoritmo
RSASSA_PKCS1_V1_5_SHA_384	PKCS #1 v2.2, sección 8.2, firma de RSA con relleno PKCS #1 v1.5 y SHA-384
RSASSA_PKCS1_V1_5_SHA_512	PKCS #1 v2.2, sección 8.2, firma de RSA con relleno PKCS #1 v1.5 y SHA-512

No puede configurar una clave de KMS para utilizar algoritmos de firma específicos. Sin embargo, puedes usar la condición de SigningAlgorithm política kms: para especificar los algoritmos de firma que los principales pueden usar con la clave KMS.

Para obtener los algoritmos de firma de una clave KMS, consulte la configuración criptográfica de la clave KMS en la AWS KMS consola o utilice la DescribeKeyoperación. AWS KMStambién proporciona las especificaciones clave y los algoritmos de firma al descargar la clave pública, ya sea en la AWS KMS consola o mediante la GetPublicKeyoperación.

Especificaciones de clave de curva elíptica

Cuando utiliza una especificación de clave de curva elíptica (ECC), AWS KMS crea una clave KMS asimétrica con un par de claves de ECC para la firma y la verificación. La clave privada que genera la firma nunca deja AWS KMS sin cifrar. Puede utilizar la clave pública para verificar firmas en AWS KMS o descargar la clave pública para utilizarla fuera de AWS KMS.

AWS KMS es compatible con las siguientes especificaciones de clave de ECC para las clave KMS asimétricas.

- Pares de claves de curva elíptica asimétricas recomendadas por NIST (firma y verificación)
  - ECC_NIST_P256 (secp256r1)
  - ECC_NIST_P384 (secp384r1)
  - ECC_NIST_P521 (secp521r1)
- Otros pares de claves de curva elíptica asimétricas (firma y verificación)
  - ECC_SECG_P256K1 (secp256k1), que se suele utilizar para las criptomonedas.

La especificación de clave de ECC que selecciona puede estar determinada por las normas de seguridad o los requisitos de la tarea. Por regla general, utilice la curva con más puntos que sea práctica y asequible para la tarea.

Si va a crear una clave KMS asimétrica para utilizarla con criptomonedas, utilice la especificación de clave ECC_SECG_P256K1. También puede utilizar esta especificación de clave para otros fines, pero es obligatoria para Bitcoin y otras criptomonedas.

Las claves KMS con diferentes especificaciones de clave de ECC tienen un precio diferente y están sujetas a diferentes cuotas de solicitud. Para obtener más información acerca de los precios de AWS KMS, consulte Precios de AWS Key Management Service. Para obtener más información acerca de las cuotas de solicitud, consulte Cuotas de solicitudes.

En la siguiente tabla se muestran los algoritmos de firma que AWS KMS admite para cada especificación de clave de ECC. No puede configurar una clave de KMS para utilizar algoritmos de firma específicos. Sin embargo, puedes usar la condición de SigningAlgorithm política kms: para especificar los algoritmos de firma que los directores pueden usar con la clave KMS.

Algoritmos de firma compatibles con las especificaciones de clave de ECC

Especificación de clave	Algoritmo de firma	Descripción del algoritmo
ECC_NIST_P256	ECDSA_SHA_256	NIST FIPS 186-4, sección 6.4, firma de ECDSA mediante la curva que especifican la clave y SHA-256 para el resumen de mensaje.
ECC_NIST_P384	ECDSA_SHA_384	NIST FIPS 186-4, sección 6.4, firma de ECDSA mediante la curva que especifican la clave y SHA-384 para el resumen de mensaje.
ECC_NIST_P521	ECDSA_SHA_512	NIST FIPS 186-4, sección 6.4, firma de ECDSA mediante la curva que especifican la clave y SHA-512 para el resumen de mensaje.

Especificación de clave	Algoritmo de firma	Descripción del algoritmo
ECC_SECG_P256K1	ECDSA_SHA_256	NIST FIPS 186-4, sección 6.4, firma de ECDSA mediante la curva que especifican la clave y SHA-256 para el resumen de mensaje.

Especificación de clave SM2 (solo en las regiones de China)

La especificación de clave SM2 es una especificación clave de curva elíptica definida dentro de la serie de especificaciones GM/T publicada por la Oficina de Administración Estatal de Criptografía Comercial de China (OSCCA). La especificación de clave SM2 solo está disponible en las regiones de China. Cuando utiliza una especificación de clave SM2, AWS KMS crea una clave KMS asimétrica con un par de claves SM2. Puede utilizar la clave pública en AWS KMS o descargarla para utilizarla fuera de AWS KMS.

A diferencia de la especificación de clave ECC, puede utilizar una clave SM2 de KMS para la firma y la verificación, o el cifrado y descifrado. Debe especificar el uso de claves al crear la clave KMS y no se la puede cambiar una vez creada.

AWS KMS admite los siguientes algoritmos de cifrado y firma SM2:

- Algoritmo de cifrado SM2PKE

  SM2PKE es un algoritmo de cifrado basado en curvas elípticas definido por OSCCA en GM/T 0003.4-2012.

- Algoritmo de firma SM2DSA

  SM2DSA es un algoritmo de cifrado basado en curvas elípticas definido por OSCCA en GM/T 0003.2-2012. SM2DSA requiere un identificador distintivo que se cifra con hash con el algoritmo hash SM3 y, a continuación, se combina con el mensaje, o resumen del mensaje, que se pasa a AWS KMS. A continuación, este valor concatenado es cifrado con hash y firmado por AWS KMS.

Operaciones fuera de línea con SM2 (solo en las regiones de China)

Puede descargar la clave pública del par de claves SM2 para uso en operaciones fuera de línea, es decir, operaciones fuera de AWS KMS. Sin embargo, cuando utilice su clave pública de SM2 sin conexión, es posible que tenga que realizar conversiones y cálculos adicionales de forma manual. Las operaciones de SM2DSA pueden requerir que proporcione un identificador distintivo o que calcule un resumen del mensaje. Las operaciones de cifrado SM2PKE pueden requerir que convierta la salida de texto cifrado sin procesar a un formato que AWS KMS puede aceptar.

Para ayudarle con estas operaciones, la clase de `SM2OfflineOperationHelper` para Java tiene métodos que realizan las tareas por usted. Puede usar esta clase auxiliar como modelo para otros proveedores de cifrado.

> **Important**
>
> El código de referencia `SM2OfflineOperationHelper` está diseñado para ser compatible con Bouncy Castle versión 1.68. Para obtener ayuda con otras versiones, póngase en contacto con bouncycastle.org.

Verificación sin conexión con pares de claves SM2 (solo en las regiones de China)

Para verificar una firma fuera de AWS KMS con una clave pública SM2, debe especificar el identificador distintivo. Cuando pasa un mensaje sin formato, `MessageType:RAW`, a la API Sign, AWS KMS utiliza el identificador distintivo predeterminado, `1234567812345678`, definido por la OSCCA en GM/T 0009-2012. No puede especificar su propio identificador distintivo en AWS KMS.

Sin embargo, si está generando un resumen de mensajes fuera de AWS, puede especificar su propio identificador distintivo y, a continuación, pasar el resumen del mensaje, `MessageType:DIGEST`, a AWS KMS para su firma. Para ello, cambie el valor `DEFAULT_DISTINGUISHING_ID` en la clase `SM2OfflineOperationHelper`. El identificador distintivo que especifique puede ser cualquier cadena de hasta 8192 caracteres. Después de que AWS KMS firma el resumen del mensaje, necesita el resumen del mensaje o el mensaje y el identificador distintivo utilizados para calcular el resumen y verificarlo sin conexión.

Classe **`SM2OfflineOperationHelper`**

Dentro de AWS KMS, las conversiones de texto cifrado sin procesar y los cálculos de resumen de mensajes SM2DSA se producen automáticamente. No todos los proveedores de cifrado

implementan SM2 de la misma manera. Algunas bibliotecas, como OpenSSL versiones 1.1.1 y posteriores, realizan estas acciones de forma automática. AWS KMS confirmó este comportamiento en pruebas con OpenSSL versión 3.0. Utilice la siguiente clase de `SM2OfflineOperationHelper` con bibliotecas, como Bouncy Castle, que requieren que realice estas conversiones y cálculos manualmente.

La clase `SM2OfflineOperationHelper` proporciona métodos para las siguientes operaciones fuera de línea:

- Cálculo del resumen del mensaje

  Para generar un resumen de mensajes sin conexión que pueda usar para la verificación sin conexión o que pueda pasar a AWS KMS para su firma, utilice el método `calculateSM2Digest`. El método `calculateSM2Digest` genera un resumen de mensajes con el algoritmo hash SM3. La GetPublicKeyAPI devuelve la clave pública en formato binario. Debe analizar la clave binaria para convertirla en una versión Java PublicKey. Proporcione la clave pública analizada con el mensaje. El método combina automáticamente el mensaje con el identificador distintivo predeterminado, `1234567812345678`, pero puede establecer su propio identificador distintivo cambiando el valor `DEFAULT_DISTINGUISHING_ID`.

- Verificar

  Para verificar una firma sin conexión, utilice el método `offlineSM2DSAVerify`. El método `offlineSM2DSAVerify` utiliza el resumen del mensaje calculado a partir del identificador distintivo especificado y el mensaje original que proporciona para verificar la firma digital. La GetPublicKeyAPI devuelve la clave pública en formato binario. Debe analizar la clave binaria para convertirla en una versión Java PublicKey. Proporcione la clave pública analizada con el mensaje original y la firma que desea verificar. Para obtener más información, consulte Verificación sin conexión con pares de claves SM2.

- Encrypt

  Para cifrar texto sin formato sin conexión, utilice el método `offlineSM2PKEEncrypt`. Este método garantiza que el texto cifrado esté en un formato que AWS KMS puede descifrar. El método `offlineSM2PKEEncrypt` cifra el texto sin formato y, a continuación, convierte el texto cifrado sin procesar producido por SM2PKE al formato ASN.1. La GetPublicKeyAPI devuelve la clave pública en formato binario. Debe analizar la clave binaria para convertirla en una versión Java PublicKey. Proporcione la clave pública analizada con el texto sin formato que desea cifrar.

Si no está seguro de si necesita realizar la conversión, utilice la siguiente operación de OpenSSL para probar el formato del texto cifrado. Si la operación falla, debe convertir el texto cifrado al formato ASN.1.

```
openssl asn1parse -inform DER -in ciphertext.der
```

De forma predeterminada, la clase `SM2OfflineOperationHelper` usa el identificador distintivo predeterminado, `1234567812345678`, al generar resúmenes de mensajes para operaciones SM2DSA.

```
package com.amazon.kms.utils;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.NoSuchPaddingException;
import java.io.IOException;
import java.math.BigInteger;
import java.nio.ByteBuffer;
import java.nio.charset.StandardCharsets;
import java.security.InvalidKeyException;
import java.security.MessageDigest;
import java.security.NoSuchAlgorithmException;
import java.security.NoSuchProviderException;
import java.security.PrivateKey;
import java.security.PublicKey;

import org.bouncycastle.crypto.CryptoException;
import org.bouncycastle.jce.interfaces.ECPublicKey;

import java.util.Arrays;

import org.bouncycastle.asn1.ASN1EncodableVector;
import org.bouncycastle.asn1.ASN1Integer;
import org.bouncycastle.asn1.DEROctetString;
import org.bouncycastle.asn1.DERSequence;
import org.bouncycastle.asn1.gm.GMNamedCurves;
import org.bouncycastle.asn1.x9.X9ECParameters;
import org.bouncycastle.crypto.CipherParameters;
import org.bouncycastle.crypto.params.ParametersWithID;
```

```
import org.bouncycastle.crypto.params.ParametersWithRandom;
import org.bouncycastle.crypto.signers.SM2Signer;
import org.bouncycastle.jcajce.provider.asymmetric.util.ECUtil;

public class SM2OfflineOperationHelper {
    // You can change the DEFAULT_DISTINGUISHING_ID value to set your own
 distinguishing ID,
    // the DEFAULT_DISTINGUISHING_ID can be any string up to 8,192 characters long.
    private static final byte[] DEFAULT_DISTINGUISHING_ID =
 "1234567812345678".getBytes(StandardCharsets.UTF_8);
    private static final X9ECParameters SM2_X9EC_PARAMETERS =
 GMNamedCurves.getByName("sm2p256v1");

    // ***calculateSM2Digest***
    // Calculate message digest
    public static byte[] calculateSM2Digest(final PublicKey publicKey, final byte[]
 message) throws
            NoSuchProviderException, NoSuchAlgorithmException {
        final ECPublicKey ecPublicKey = (ECPublicKey) publicKey;

        // Generate SM3 hash of default distinguishing ID, 1234567812345678
        final int entlenA = DEFAULT_DISTINGUISHING_ID.length * 8;
        final byte [] entla = new byte[] { (byte) (entlenA & 0xFF00), (byte) (entlenA &
 0x00FF) };
        final byte [] a = SM2_X9EC_PARAMETERS.getCurve().getA().getEncoded();
        final byte [] b = SM2_X9EC_PARAMETERS.getCurve().getB().getEncoded();
        final byte [] xg = SM2_X9EC_PARAMETERS.getG().getXCoord().getEncoded();
        final byte [] yg = SM2_X9EC_PARAMETERS.getG().getYCoord().getEncoded();
        final byte[] xa = ecPublicKey.getQ().getXCoord().getEncoded();
        final byte[] ya = ecPublicKey.getQ().getYCoord().getEncoded();
        final byte[] za = MessageDigest.getInstance("SM3", "BC")
                .digest(ByteBuffer.allocate(entla.length +
 DEFAULT_DISTINGUISHING_ID.length + a.length + b.length + xg.length + yg.length +
                        xa.length +
 ya.length).put(entla).put(DEFAULT_DISTINGUISHING_ID).put(a).put(b).put(xg).put(yg).put(xa).put
                        .array());

        // Combine hashed distinguishing ID with original message to generate final
 digest
        return MessageDigest.getInstance("SM3", "BC")
                .digest(ByteBuffer.allocate(za.length +
 message.length).put(za).put(message)
                        .array());
    }
```

```
   // ***offlineSM2DSAVerify***
   // Verify digital signature with SM2 public key
   public static boolean offlineSM2DSAVerify(final PublicKey publicKey, final byte []
message,
           final byte [] signature) throws InvalidKeyException {
       final SM2Signer signer = new SM2Signer();
       CipherParameters cipherParameters =
ECUtil.generatePublicKeyParameter(publicKey);
       cipherParameters = new ParametersWithID(cipherParameters,
DEFAULT_DISTINGUISHING_ID);
       signer.init(false, cipherParameters);
       signer.update(message, 0, message.length);
       return signer.verifySignature(signature);
   }

   // ***offlineSM2PKEEncrypt***
   // Encrypt data with SM2 public key
   public static byte[] offlineSM2PKEEncrypt(final PublicKey publicKey, final byte []
plaintext) throws
           NoSuchPaddingException, NoSuchAlgorithmException, NoSuchProviderException,
InvalidKeyException,
           BadPaddingException, IllegalBlockSizeException, IOException {
       final Cipher sm2Cipher = Cipher.getInstance("SM2", "BC");
       sm2Cipher.init(Cipher.ENCRYPT_MODE, publicKey);

       // By default, Bouncy Castle returns raw ciphertext in the c1c2c3 format
       final byte [] cipherText = sm2Cipher.doFinal(plaintext);

       // Convert the raw ciphertext to the ASN.1 format before passing it to AWS KMS
       final ASN1EncodableVector asn1EncodableVector = new ASN1EncodableVector();
       final int coordinateLength = (SM2_X9EC_PARAMETERS.getCurve().getFieldSize() +
7) / 8 * 2 + 1;
       final int sm3HashLength = 32;
       final int xCoordinateInCipherText = 33;
       final int yCoordinateInCipherText = 65;
       byte[] coords = new byte[coordinateLength];
       byte[] sm3Hash = new byte[sm3HashLength];
       byte[] remainingCipherText = new byte[cipherText.length - coordinateLength -
sm3HashLength];

       // Split components out of the ciphertext
       System.arraycopy(cipherText, 0, coords, 0, coordinateLength);
```

```
        System.arraycopy(cipherText, cipherText.length - sm3HashLength, sm3Hash, 0,
 sm3HashLength);
        System.arraycopy(cipherText, coordinateLength, remainingCipherText,
 0,cipherText.length - coordinateLength - sm3HashLength);

        // Build standard SM2PKE ASN.1 ciphertext vector
        asn1EncodableVector.add(new ASN1Integer(new BigInteger(1,
 Arrays.copyOfRange(coords, 1, xCoordinateInCipherText))));
        asn1EncodableVector.add(new ASN1Integer(new BigInteger(1,
 Arrays.copyOfRange(coords, xCoordinateInCipherText, yCoordinateInCipherText))));
        asn1EncodableVector.add(new DEROctetString(sm3Hash));
        asn1EncodableVector.add(new DEROctetString(remainingCipherText));

        return new DERSequence(asn1EncodableVector).getEncoded("DER");
    }
}
```

Especificación de clave SYMMETRIC_DEFAULT

La especificación de clave predeterminada, SYMMETRIC_DEFAULT, es la especificación de clave para las claves KMS de cifrado simétricas. Cuando selecciona el tipo de clave Symmetric (Simétrica) y Encrypt and decrypt (Cifrar y descifrar) en la consola de AWS KMS, esta selecciona la especificación de clave `SYMMETRIC_DEFAULT`. En la CreateKeyoperación, si no especifica ningún `KeySpec` valor, se selecciona SYMMETRIC_DEFAULT. Si no tiene un motivo para utilizar una especificación de clave diferente, SYMMETRIC_DEFAULT es una buena opción.

SYMMETRIC_DEFAULT actualmente representa AES-256-GCM, un algoritmo simétrico basado en el estándar de cifrado avanzado (AES) en el modo de contador Galois (GCM) con claves de 256 bits, un estándar del sector para conseguir un cifrado seguro. El texto cifrado que este algoritmo genera admite datos autenticados adicionales (AAD), como un contexto de cifrado, y GCM ofrece una comprobación de integridad adicional en el texto cifrado. Para obtener más detalles, consulte.Detalles criptográficos de AWS Key Management Service.

Los datos cifrados con AES-256-GCM están protegidos ahora y en el futuro. Los criptógrafos consideran que este algoritmo es resistente a la informática cuántica. Los futuros e hipotéticos ataques de informática cuántica a gran escala a textos cifrados creados con claves AES-GCM de 256 bits reducen la seguridad nominal de la clave a 128 bits. No obstante, este nivel de seguridad es suficiente para hacer inviables los ataques de fuerza bruta en los textos cifrados de AWS KMS.

La única excepción es en las regiones de China, donde SYMMETRIC_DEFAULT representa una clave simétrica de 128 bits que utiliza el cifrado SM4. Solo puede crear una clave SM4 de 128 bits

dentro de las regiones de China. No puede crear una clave KMS con cifrado AES-GCM de 256 bits en las regiones de China.

Puede utilizar una clave de KMS de cifrado simétrica en AWS KMS para cifrar, descifrar y volver a cifrar los datos y para proteger claves de datos y pares de claves de datos generados. Los servicios de AWS que están integrados con AWS KMS utilizan claves de KMS de cifrado simétricas para cifrar los datos en reposo. Puede importar su propio material de claves en una clave KMS de cifrado simétrica y crear claves KMS de cifrado simétricas en almacenes de claves personalizadas. Para obtener una tabla en la que se comparan las operaciones que puede realizar en las claves de KMS simétricas y asimétricas, consulte Comparación de claves de KMS simétricas y asimétricas.

Para obtener más información técnica sobre AWS KMS y claves de cifrado simétricas, consulte Información criptográfica de AWS Key Management Service.

Claves HMAC en AWS KMS

Las claves KMS del código de autenticación de mensajes basado en hash (HMAC) son claves simétricas que se utilizan para generar y verificar HMAC en AWS KMS. El material de claves exclusivo de cada clave HMAC de KMS proporciona la clave secreta que requieren los algoritmos HMAC. Puede utilizar una clave KMS HMAC con las operaciones `GenerateMac` y `VerifyMac` para verificar la integridad y autenticidad de los datos dentro de AWS KMS.

Los algoritmos HMAC combinan una función hash criptográfica y una clave secreta compartida. Toman un mensaje y una clave secreta, como el material clave de una clave KMS HMAC, y devuelven un código o una etiquetaúnicos de tamaño fijo. Si cambia incluso un carácter del mensaje, o si la clave secreta no es idéntica, la etiqueta resultante es totalmente diferente. Al requerir una clave secreta, HMAC también proporciona autenticación; es imposible generar una etiqueta HMAC idéntica sin la clave secreta. Los HMAC a veces se llaman firmas simétricas, porque funcionan como firmas digitales, pero utilizan una única clave para la firma y la verificación.

Las claves KMS HMAC y los algoritmos HMAC que AWS KMS usa se ajustan a los estándares del sector definidos en RFC 2104. La AWS KMS GenerateMacoperación genera etiquetas HMAC estándar. Las claves KMS HMAC se generan en módulos de seguridad de hardware de certificados de AWS KMS con el Programa de validación de módulos criptográficos FIPS 140-2, (excepto en las regiones China [Pekín] y China [Ningxia]) y nunca dejan AWS KMS sin cifrar. Para utilizar una clave KMS HMAC, tiene que llamar a AWS KMS.

Puede utilizar claves KMS HMAC para determinar la autenticidad de un mensaje, como un token web JSON (JWT), información de tarjeta de crédito tokenizada o una contraseña enviada. También se

pueden utilizar como funciones de derivación clave seguras (KDF), especialmente en aplicaciones que requieren claves deterministas.

Las claves KMS HMAC proporcionan una ventaja sobre los HMAC del software de aplicación porque el material de claves se genera y utiliza íntegramente en AWS KMS, sujeto a los controles de acceso que haya establecido en la clave.

> **Tip**
>
> Las prácticas recomendadas indican limitar el tiempo durante el cual cualquier mecanismo de firma, incluido un HMAC, es efectivo. Esto impide un ataque en el que el actor utiliza un mensaje firmado para establecer la validez repetidamente o mucho después de que se sustituya el mensaje. Las etiquetas del HMAC no incluyen una marca de hora, pero puede incluir una marca de hora en el token o mensaje para ayudarlo a detectar cuándo es hora de actualizar el HMAC.

Los usuarios autorizados pueden crear, administrar y utilizar las claves HMAC de KMS en su cuenta de AWS. Esto incluye habilitar y deshabilitar claves, configurar y cambiar alias y etiquetas, y borrar programación de claves KMS HMAC. También puede controlar el acceso a las claves KMS HMAC usando políticas clave, políticas de IAM y concesiones. Además, puede auditar todas las operaciones que utilizan o administran sus claves KMS HMAC dentro de AWS en los registros de AWS CloudTrail. Puede crear claves HMAC de KMS con material de claves importado. También puede crear claves KMS de varias regiones HMAC que se comportan como copias de la misma clave KMS HMAC en múltiples Regiones de AWS.

Las claves KMS HMAC solo admiten las operaciones criptográficas `GenerateMac` y `VerifyMac`. No puede utilizar claves KMS HMAC para cifrar datos o firmar mensajes, ni utilizar ningún otro tipo de clave KMS en las operaciones de HMAC. Cuando utiliza la operación `GenerateMac`, proporciona un mensaje de hasta 4096 bytes, una clave KMS HMAC y el algoritmo MAC compatible con la especificación de clave HMAC, y `GenerateMac` computa la etiqueta HMAC. Para verificar una etiqueta HMAC, debe proporcionar la etiqueta HMAC y el mismo mensaje, clave KMS HMAC y algoritmo MAC que `GenerateMac` utilizó para computar la etiqueta HMAC original. La operación `VerifyMac` computa la etiqueta HMAC y verifica que es idéntica a la etiqueta HMAC suministrada. Si la entrada y las etiquetas HMAC calculadas no son idénticas, la verificación falla.

Las claves HMAC de KMS no admiten rotación automática de claves y no se puede crear una clave de KMS HMAC en un almacén de claves personalizado.

Si va a crear una clave KMS para cifrar los datos de un servicio de AWS, utilice una clave de cifrado simétrica. No puede utilizar una clave KMS HMAC.

Regiones

Las claves HMAC de KMS son compatibles en todas las Regiones de AWS que AWS KMS admite.

Más información

- Para obtener ayuda sobre cómo elegir un tipo de clave KMS, consulte Elección de un tipo de clave KMS.
- Para obtener una tabla que compara las operaciones de la API de AWS KMS que admite cada tipo de clave KMS, consulte Referencia de tipos de claves.
- Para obtener información sobre cómo crear claves KMS HMAC de varias regiones, consulte Claves multirregionales en AWS KMS.
- Para analizar las diferencias de la política de claves predeterminada que establece la consola de AWS KMS para las claves KMS HMAC, consulte the section called “Permite a los usuarios de claves utilizar la clave KMS con los servicios de AWS”.
- Para obtener más información acerca de los precios de las claves KMS HMAC, consulte Precios de AWS Key Management Service.
- Para obtener información acerca de las cuotas que se aplican a las claves KMS HMAC, consulte Cuotas de recursos y Cuotas de solicitudes.
- Para obtener más información acerca de cómo eliminar claves KMS HMAC, consulte Eliminación de AWS KMS keys.
- Para obtener más información sobre el uso de HMAC para crear tokens web JSON, consulte Cómo proteger los HMAC en el interior del AWS KMS en el Blog de seguridad de AWS.
- Escuche un podcast: Presentación de las HMAC para AWS Key Management Service en The Official AWS Podcast.

Temas

Especificaciones de la clave para las claves KMS HMAC

AWS KMS admite claves HMAC simétricas de diferentes longitudes. La especificación de clave que seleccione puede depender de sus requisitos normativos, de seguridad o empresariales. La longitud de la clave determina el algoritmo MAC que se utiliza en VerifyMaclas operaciones GenerateMacy. En general, las claves más largas son más seguras. Utilice la clave más larga que sea práctica para su caso de uso.

Especificación de la clave HMAC	Algoritmo MAC
HMAC_224	HMAC_SHA_224
HMAC_256	HMAC_SHA_256
HMAC_384	HMAC_SHA_384
HMAC_512	HMAC_SHA_512

Creación de claves KMS HMAC

Puede crear claves KMS HMAC en la consola de AWS KMS, mediante la API CreateKey o mediante una plantilla de AWS CloudFormation.

AWS KMS admite múltiples especificaciones de la clave para claves KMS HMAC. La especificación de clave que seleccione podría estar determinada por requisitos normativos, de seguridad o empresariales. En general, las claves más largas son más resistentes a los ataques de fuerza bruta.

> **Important**
>
> No incluya información confidencial en el alias, la descripción ni las etiquetas. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

Si va a crear una clave KMS para cifrar los datos de un servicio de AWS, utilice una clave de cifrado KMS simétrica. Los servicios de AWS que se integran con AWS KMS no admiten claves KMS asimétricas ni claves KMS HMAC. Para obtener ayuda a la hora de crear una clave KMS de cifrado simétrica, consulte Crear claves.

Más información

- Para determinar qué tipo de clave KMS crear, consulte Elección de un tipo de clave KMS.
- Puede utilizar los procedimientos descritos en este tema para crear una clave KMS HMAC primaria de varias regiones. Para replicar una clave HMAC de varias regiones, consulte the section called "Creación de claves de réplica".
- Para obtener información sobre los permisos necesarios para crear claves de KMS, consulte Permisos para crear claves KMS.
- Para obtener información sobre el uso de una AWS CloudFormation plantilla para crear una clave HMAC KMS, consulte AWS::KMS::Keyla Guía del AWS CloudFormation usuario.

Temas

- Creación de claves KMS HMAC (consola)
- Creación de claves KMS HMAC (API de AWS KMS)

Creación de claves KMS HMAC (consola)

Puede utilizar la AWS Management Console para crear claves KMS HMAC. Las claves KMS HMAC son claves simétricas con un uso de claves de Generate and verify MAC (Generar y verificar MAC). También puede crear claves HMAC de varias regiones.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija Create key.
5. En Key type (Tipo de clave), elija Symmetric (Simétrica).

   Las claves KMS HMAC son simétricas. Utilice la misma clave para generar y verificar etiquetas HMAC.
6. Para Key usage (Uso de claves), elija Generate and verify MAC (Generar y verificar MAC).

   Generar y verificar que MAC es el único uso de clave válido para las claves KMS HMAC.

> **Note**
>
> Key usage (Uso de claves) se muestra para las claves simétricas solo cuando las claves KMS HMAC son compatibles en la región seleccionada.

7. Seleccione una especificación (Key spec [Especificación de clave]) para su clave KMS HMAC.

   La especificación de clave que seleccione se puede determinar mediante requisitos normativos, de seguridad o empresariales. En general, las claves más largas son más seguras.

8. Para crear una clave HMAC de varias regiones primaria, en Advanced options (Opciones avanzadas), elija Multi-Region key (Clave de varias regiones). Las propiedades compartidas que defina para esta clave KMS, como su tipo de clave y uso de claves, se compartirán con sus claves de réplica. Para obtener más detalles, consulte Creación de claves de varias regiones.

   No puede utilizar este procedimiento para crear una clave de réplica. Para crear una clave HMAC réplica de varias regiones, siga las instrucciones para crear una clave de réplica.

9. Elija Siguiente.

10. Ingrese un alias para la clave KMS El nombre del alias no puede empezar por **`aws/`**. El prefijo **`aws/`** está reservado para Amazon Web Services y representa las Claves administradas por AWS de su cuenta.

    Le recomendamos que utilice un alias que identifique la clave KMS como clave HMAC, como `HMAC/test-key`. Esto le facilitará la identificación de claves HMAC en la consola AWS KMS en la que puede ordenar y filtrar claves por etiquetas y alias, pero no por especificación de la clave o uso de claves.

    Los alias son necesarios para crear una clave de KMS en la AWS Management Console. No puede especificar un alias al usar la CreateKeyoperación, pero puede usar la consola o la CreateAliasoperación para crear un alias para una clave de KMS existente. Para obtener más detalles, consulte Uso de alias.

11. (Opcional) Ingrese una descripción de la clave KMS.

    Escriba una descripción que explique el tipo de datos que piensa proteger o la aplicación que piensa usar con la clave de KMS.

    Puede agregar una descripción ahora o actualizarla en cualquier momento, a menos que el estado de la clave sea `Pending Deletion` o `Pending Replica Deletion`.

Para añadir, cambiar o eliminar la descripción de una clave gestionada por el cliente existente, edite la descripción en la operación AWS Management Console o utilice esta UpdateKeyDescriptionoperación.

12. (Opcional) Ingrese una clave de etiqueta y un value de etiqueta opcional. Para agregar más de una etiqueta a la clave de KMS, elija Agregar etiqueta.

    Considere agregar una etiqueta que identifique la clave como una clave HMAC, por ejemplo `Type=HMAC`. Esto le facilitará la identificación de claves HMAC en la consola AWS KMS en la que puede ordenar y filtrar claves por etiquetas y alias, pero no por especificación de clave o uso de claves.

    Cuando se agregan etiquetas a los recursos de AWS, AWS genera un informe de asignación de costos con el uso y los costos agregados por etiquetas. Las etiquetas también pueden utilizarse para controlar el acceso a una clave KMS. Para obtener información acerca del etiquetado de claves KMS, consulte Etiquetado de claves y ABAC para AWS KMS.

13. Elija Siguiente.

14. Seleccione los usuarios y roles de IAM que pueden administrar la clave de KMS.

    > **Note**
    >
    > Esta política de claves proporciona a la Cuenta de AWS control total de esta clave KMS. Permite a los administradores de cuentas utilizar las políticas de IAM para dar permiso a otras entidades principales para administrar la clave KMS. Para obtener más detalles, consulte the section called “Política de claves predeterminada”.
    > Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

15. (Opcional) Para evitar que los usuarios y los roles de IAM seleccionados eliminen esta clave de KMS, en la sección Eliminación de claves situada en la parte inferior de la página, desactive la casilla Permitir que los administradores de claves eliminen esta clave.

16. Elija Siguiente.

17. Seleccione los usuarios y roles de IAM que pueden usar la clave de KMS en operaciones criptográficas.

> **Note**
>
> Esta política de claves proporciona a la Cuenta de AWS control total de esta clave KMS. Permite a los administradores de cuentas utilizar las políticas de IAM para dar permiso a otras entidades principales para utilizar la clave KMS. Para obtener más detalles, consulte the section called “Política de claves predeterminada”.
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

18. (Opcional) Puede permitir que otras cuentas de Cuentas de AWS usen esta clave de KMS en operaciones criptográficas. Para ello, en la parte inferior de la página de la sección Other Cuentas de AWS (Otras), elija Add another Cuenta de AWS (Agregar otra) e ingrese el número de identificación de Cuenta de AWS de una cuenta externa. Para agregar varias cuentas externas, repita este paso.

> **Note**
>
> Para permitir que las entidades principales de las cuentas externas usen la clave KMS, los administradores de la cuenta externa también deben crear las políticas de IAM que proporcionan estos permisos. Para obtener más información, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS.

19. Seleccione Siguiente.
20. Revise los ajustes de clave que ha elegido. Aún puede volver atrás y cambiar todos los ajustes.
21. Elija Finish (Finalizar) para crear la clave KMS HMAC.

Creación de claves KMS HMAC (API de AWS KMS)

Puede utilizar la CreateKeyoperación para crear una clave HMAC KMS. En estos ejemplos, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Al crear una clave KMS HMAC, debe especificar el parámetro `KeySpec`, que determina el tipo de clave KMS. Además, debe especificar un valor `KeyUsage` de GENERATE_VERIFY_MAC, aunque

sea el único valor de uso de claves válido para claves HMAC. Para crear una clave KMS HMAC de múltiples regiones, agregue el parámetro `MultiRegion` con un valor de `true`. No puede cambiar estas propiedades después de que se cree la clave de KMS.

La `CreateKey` operación no le permite especificar un alias, pero puede utilizarla para crear un alias para la CreateAliasnueva clave KMS. Le recomendamos que utilice un alias que identifique la clave KMS como clave HMAC, como `HMAC/test-key`. Esto le facilitará la identificación de claves HMAC en la consola de AWS KMS en la que puede ordenar y filtrar claves por alias, pero no por especificación de la clave o uso de claves.

Si intenta crear una clave de KMS HMAC en una Región de AWS en la que no se admiten claves HMAC, la operación `CreateKey` devuelve una `UnsupportedOperationException`.

El siguiente ejemplo utiliza la operación `CreateKey` para crear una clave KMS HMAC de 512 bits.

```
$ aws kms create-key --key-spec HMAC_512 --key-usage GENERATE_VERIFY_MAC
{
    "KeyMetadata": {
        "KeyState": "Enabled",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "KeyManager": "CUSTOMER",
        "Description": "",
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "CreationDate": 1669973196.214,
        "MultiRegion": false,
        "KeySpec": "HMAC_512",
        "CustomerMasterKeySpec": "HMAC_512",
        "KeyUsage": "GENERATE_VERIFY_MAC",
        "MacAlgorithms": [
            "HMAC_SHA_512"
        ],
        "AWSAccountId": "111122223333",
        "Origin": "AWS_KMS",
        "Enabled": true
    }
}
```

Control del acceso a las claves KMS HMAC

Para controlar el acceso a una clave KMS HMAC, utilice una política de claves, necesaria para cada clave KMS. También puede utilizar políticas de IAM y concesiones.

La política de claves predeterminada para claves HMAC creadas en la consola AWS KMS da permiso a los usuarios de claves para llamar a `GenerateMac` y `VerifyMac`. Sin embargo, no incluye la declaración de política de claves diseñada para utilizar concesiones con servicios de AWS. Si crea claves HMAC mediante la operación `CreateKey`, debe especificar estos permisos en la política de claves o en una política de IAM.

Puede usar claves de condición globales de AWS y claves de condición de AWS KMS para refinar y limitar los permisos a las claves HMAC. Por ejemplo, puede utilizar la clave de condición `kms:ResourceAliases` para controlar el acceso a las operaciones de AWS KMS basadas en los alias asociados a una clave HMAC. Las siguientes condiciones de política de AWS KMS son útiles para las políticas de claves HMAC.

- Use una clave de condición `kms:MacAlgorithm` para limitar los algoritmos que las entidades principales pueden solicitar cuando llaman al `GenerateMac` y `VerifyMac`. Por ejemplo, puede permitir a las entidades principales llamar a las operaciones `GenerateMac` pero solo cuando el algoritmo MAC de la solicitud es `HMAC_SHA_384`.
- Use una clave de condición `kms:KeySpec` para permitir o impedir que las entidades principales creen ciertos tipos de claves HMAC. Por ejemplo, para permitir que los directores creen solo claves HMAC, puede permitir la CreateKeyoperación, pero usar la `kms:KeySpec` condición para permitir solo claves con una especificación `HMAC_384` clave.

  También puede utilizar la clave de condición `kms:KeySpec` para controlar el acceso a otras operaciones de una clave KMS en función de la especificación de la clave. Por ejemplo, puede permitir que las entidades principales programen y cancelen la eliminación de claves solo en claves KMS con una especificación de la clave `HMAC_256`.
- Use la clave de condición `kms:KeyUsage` para permitir o impedir que las entidades principales creen claves HMAC. Por ejemplo, para permitir que los directores creen solo claves HMAC, puede permitir la CreateKeyoperación, pero usar la `kms:KeyUsage` condición para permitir solo las claves con un uso de clave. `GENERATE_VERIFY_MAC`

  También puede utilizar la clave de condición `kms:KeyUsage` para controlar el acceso a las operaciones de una clave KMS en función del uso de la clave. Por ejemplo, puede permitir a las entidades principales habilitar y desactivar solo en claves KMS con un uso de claves `GENERATE_VERIFY_MAC`.

También puede crear concesiones para operaciones `GenerateMac` y `VerifyMac`, que son operaciones de concesión. Sin embargo, no puede utilizar las restricciones de concesiones de

contexto de cifrado en una concesión para una clave HMAC. El formato de etiqueta HMAC no admite valores de contexto de cifrado.

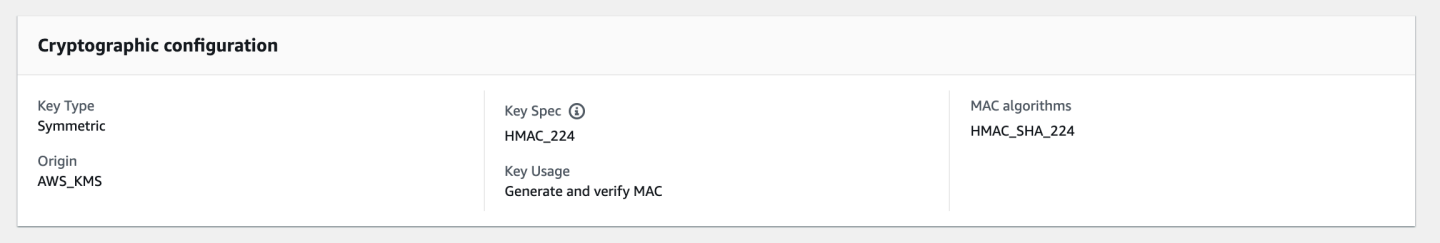
Visualización de las claves KMS HMAC

Puede ver las claves KMS HMAC en la consola de AWS KMS o utilizando la API DescribeKey. Puede supervisar el uso de sus claves HMAC KMS en AWS CloudTraillos registros y en Amazon CloudWatch. Para obtener instrucciones básicas sobre cómo ver las claves KMS, consulte Consultar claves.

Puede distinguir las claves KMS HMAC de otros tipos de claves KMS por sus especificaciones de clave, que comienza con `HMAC`, o su uso clave, que siempre es Generate and verify MAC (Generar y verificar MAC) (`GENERATE_VERIFY_MAC`).

Las claves KMS HMAC se incluyen en la tabla de la página Customer managed keys (Claves administradas por el cliente) de la consola de AWS KMS. Sin embargo, no puede ordenar ni filtrar las claves KMS por especificación de la clave o uso de claves. Para facilitar la búsqueda de las claves HMAC, asígneles un alias o una etiqueta distintiva. A continuación, puede ordenar o filtrar por el alias o la etiqueta.

En la página de detalles clave para una clave KMS HMAC, puede encontrar los detalles de configuración en la pestaña Configuración criptográfica.



Claves multirregionales en AWS KMS

AWS KMS admite claves multirregionales, que son AWS KMS keys diferentes Regiones de AWS y se pueden usar indistintamente, como si tuvieras la misma clave en varias regiones. Cada conjunto de claves multirregionales relacionadas tiene el mismo material de clave y el mismo identificador de clave, por lo que puede cifrar los datos en uno Región de AWS y descifrarlos en otro diferente Región de AWS sin necesidad de volver a cifrarlos ni de realizar llamadas entre regiones. AWS KMS

Como todas las claves de KMS, las claves multirregionales nunca se quedan sin cifrar. AWS KMS Puede crear claves multirregionales simétricas o asimétricas para el cifrado o la firma, crear claves

multirregionales HMAC para generar y verificar las etiquetas HMAC y crear claves multirregionales con material clave importado o material clave que genere. AWS KMS Debe administrar cada clave de varias regiones de forma independiente, incluida la creación de alias y etiquetas, el establecimiento de sus políticas y concesiones clave, y la habilitación y deshabilitación selectivas. Puede utilizar claves de varias regiones en todas las operaciones criptográficas que puede realizar con claves de una sola región.

Las claves de varias regiones son una solución flexible y potente para muchos escenarios comunes de seguridad de datos.

Recuperación de desastres

En una arquitectura de copia de seguridad y recuperación, las claves multirregionales permiten procesar datos cifrados sin interrupciones, incluso en caso de que se produzca una interrupción. Región de AWS Los datos mantenidos en las regiones de copia de seguridad se pueden descifrar en la región de copia de seguridad, y los datos recién cifrados en la región de copia de seguridad se pueden descifrar en la región principal cuando se restaura esa región.

Administración de datos global

Las empresas que operan en todo el mundo necesitan datos distribuidos globalmente que estén disponibles de manera consistente en Regiones de AWS. Puede crear claves de varias regiones en todas las regiones donde residen los datos y, a continuación, utilizar las claves como si fueran una clave de una sola región sin la latencia de una llamada entre regiones o el costo de volver a cifrar datos bajo una clave diferente en cada región.

Aplicaciones de firma distribuidas

Las aplicaciones que requieren capacidades de firma entre regiones pueden utilizar claves de firma asimétricas de varias regiones para generar firmas digitales idénticas de forma consistente y repetida en diferentes Regiones de AWS.

Si utiliza el encadenamiento de certificado con un único almacén de confianza global (para una entidad de certificado [CA] de raíz única y las CA intermedias regionales firmadas por la CA raíz) no necesita claves de varias regiones. Sin embargo, si el sistema no admite CA intermedias, como la firma de aplicaciones, puede usar claves de varias regiones para dar coherencia a las certificaciones regionales.

Aplicaciones activa-activa que abarcan varias regiones

Algunas cargas de trabajo y aplicaciones pueden abarcar varias regiones en arquitecturas activa-activa. Para estas aplicaciones, las claves de varias regiones pueden reducir la complejidad al

proporcionar el mismo material clave para operaciones simultáneas de cifrado y descifrado en datos que podrían estar moviéndose a través de los límites de la región.

Puede utilizar claves de varias regiones con bibliotecas de cifrado del cliente, como la AWS Encryption SDK, el Cliente de cifrado de DynamoDB y el Cifrado del cliente de Amazon S3. Para ver un ejemplo del uso de claves de varias regiones con las tablas globales de Amazon DynamoDB y el cliente de cifrado de DynamoDB, consulte Cifrar datos globales del lado del cliente con claves de varias regiones en el blog de seguridad. AWS KMS AWS

AWS Los servicios que se integran AWS KMS para el cifrado en reposo o las firmas digitales actualmente tratan las claves multirregionales como si fueran claves de una sola región. Es posible que vuelvan a envolver o cifrar los datos que se mueven entre regiones. Por ejemplo, la replicación entre regiones de Amazon S3 descifra y vuelve a cifrar datos bajo una clave KMS en la región de destino, incluso cuando se replican objetos protegidos por una clave de varias regiones.

Las claves de varias regiones no son globales. Cree una clave principal de varias regiones y, a continuación, replíquela en las regiones que seleccione dentro de una partición de AWS. Luego, administre la clave de varias regiones en cada región de forma independiente. Tampoco crea AWS ni AWS KMS replica automáticamente claves multirregionales en ninguna región en tu nombre. Claves administradas por AWS, las claves de KMS que AWS los servicios crean en su cuenta para usted, son siempre claves de una sola región.

No puede convertir una clave de región única existente en una clave de varias regiones. Este diseño garantiza que todos los datos protegidos con claves de una sola región existentes mantengan las mismas propiedades de residencia y soberanía de datos.

Para la mayoría de las necesidades de seguridad de los datos, el aislamiento regional y la tolerancia a errores de los recursos regionales hacen que las claves de una AWS KMS sola región estándar sean la solución más adecuada. Sin embargo, cuando necesite cifrar o firmar datos en aplicaciones del cliente en varias regiones, es posible que las claves de varias regiones sean la solución.

Regiones

Las claves multirregionales son compatibles con todos los Regiones de AWS AWS KMS soportes, excepto en China (Pekín) y China (Ningxia).

Precios y cuotas

Cada clave de un conjunto de claves de varias regiones relacionadas cuenta como una clave KMS para precios y cuotas. Las cuotas de AWS KMS se calculan por separado por cada región de una cuenta. El uso y la administración de las claves de varias regiones en cada Región cuenta para las cuotas de dicha Región.

Tipos de claves KMS compatibles

Puede crear los siguientes tipos de claves KMS para varias regiones:

- Claves de KMS de cifrado simétrico
- Claves de KMS asimétricas
- Claves KMS HMAC
- Claves KMS con material de claves importado

No puede crear claves de varias regiones en un almacén de claves personalizado.

Temas

- Control del acceso a claves de varias regiones
- Creación de claves de varias regiones
- Visualización de claves de varias regiones
- Administración de claves de varias regiones
- Importación de material clave en claves de varias regiones
- Eliminación de claves de varias regiones

Consideraciones sobre seguridad para claves de varias regiones

Usa una clave AWS KMS multirregional solo cuando la necesites. Las claves de varias regiones proporcionan una solución flexible y escalable para cargas de trabajo que mueven datos cifrados entre Regiones de AWS o necesitan acceso entre regiones. Considere una clave de varias regiones si debe compartir, mover o hacer una copia de seguridad de datos protegidos entre regiones o necesita crear firmas digitales idénticas de aplicaciones que operan en regiones diferentes.

Sin embargo, el proceso de creación de una clave de varias regiones mueve el material clave a través de límites Región de AWS dentro de AWS KMS. El texto cifrado generado por una clave de varias regiones se puede descifrar potencialmente mediante varias claves relacionadas en varias ubicaciones geográficas. También se ofrecen importantes beneficios para los servicios y los recursos

aislados a nivel regional. Cada Región de AWS es independiente y está aislada de las demás regiones. Las regiones proporcionar tolerancia a errores, estabilidad y resistencia, y también pueden reducir la latencia. Le permiten crear recursos redundantes que sigan estando disponibles y no resulten afectados por una interrupción en otra región. En AWS KMS, también se aseguran de que cada texto cifrado se pueda descifrar con una sola clave.

Las claves de varias regiones también plantean nuevas consideraciones de seguridad:

- Controlar el acceso y aplicar la política de seguridad de datos es más complejo con las claves de varias regiones. Debe asegurarse de que la política se auditará de forma coherente en clave en varias regiones aisladas. Y debe usar la política para imponer límites, en lugar de depender de claves separadas.

  Por ejemplo, debe establecer condiciones de política en los datos para evitar que los equipos de nómina de una Región puedan leer los datos de nómina de una Región diferente. Además, debe usar el control de acceso para evitar un escenario en el que una clave de varias regiones en una región proteja los datos de un inquilino y una clave de varias regiones relacionada en otra región proteja los datos de un inquilino diferente.
- La auditoría de claves entre regiones también es más compleja. Con las claves de varias regiones, debe examinar y conciliar las actividades de auditoría en varias regiones para obtener una comprensión completa de las actividades clave en los datos protegidos.
- La conformidad de los mandatos de residencia de datos puede ser más complejo. Con Regiones aisladas, puede garantizar la residencia de datos y la conformidad de la soberanía de datos. Las claves KMS de una región determinada solo pueden descifrar información confidencial en esa región. Los datos cifrados en una región pueden permanecer completamente protegidos e inaccesibles en cualquier otra región.

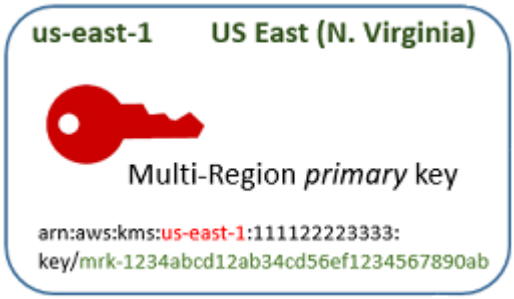
  Para verificar la residencia y la soberanía de los datos con claves multirregionales, debe implementar políticas de acceso y compilar AWS CloudTrail eventos en varias regiones.

Para facilitar la administración del control de acceso de las claves multirregionales, el permiso para replicar una clave multirregional (kms: ReplicateKey) es independiente del permiso estándar para crear claves (kms:). CreateKey Además, AWS KMS admite varias condiciones políticas para las claves multirregionales`kms:MultiRegion`, como permitir o denegar el permiso para crear, usar o administrar claves multirregionales y `kms:ReplicaRegion` restringir las regiones en las que se puede replicar una clave multiregional. Para obtener más detalles, consulte Control del acceso a claves de varias regiones.

Funcionamiento de las claves de varias regiones

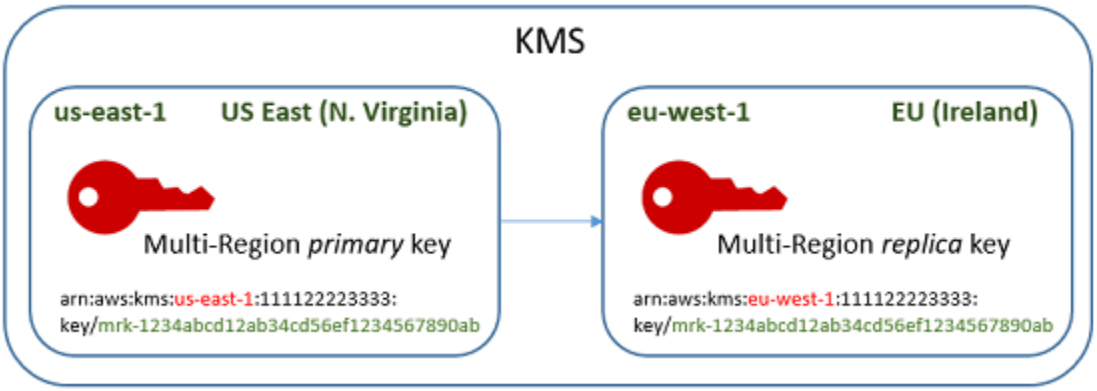
Se empieza por crear una clave principal multirregional simétrica o asimétrica en una Región de AWS que AWS KMS sea compatible, como US East (Virginia del Norte). Usted decide si una clave es de una región o de varias regiones únicamente cuando la crea; no puede cambiar esta propiedad más adelante. Al igual que con cualquier clave KMS, debe establecer una política de clave para la clave de varias regiones, y se pueden crear concesiones y agregar alias y etiquetas para la categorización y autorización. (Estas son propiedades independientes que no están compartidas ni sincronizadas con otras claves). Puede utilizar la clave principal de varias regiones en operaciones criptográficas para el cifrado o la firma.

Puede crear una clave principal multirregional en la AWS KMS consola o mediante la CreateKeyAPI con el `MultiRegion` parámetro establecido en. `true` Observe que las claves de varias regiones tienen un ID de clave distintivo que comienza con `mrk-`. Puede utilizar el prefijo `mrk-` para identificar los MRK mediante programación.



Si lo desea, puede replicar la clave principal multirregional en una o más unidades diferentes Regiones de AWS de la misma AWS partición, como Europa (Irlanda). Al hacerlo, AWS KMS crea una clave de réplica en la región especificada con el mismo ID de clave y otras propiedades compartidas que la clave principal. Luego transporta de forma segura el material clave a través del límite de la región y lo asocia con la nueva clave KMS en la región de destino, todo dentro de AWS KMS. El resultado son dos claves de varias regiones relacionadas (una clave principal y una clave de réplica) que se pueden utilizar de forma intercambiable.

Puede crear una clave de réplica multirregional en la AWS KMS consola o mediante la ReplicateKeyAPI.



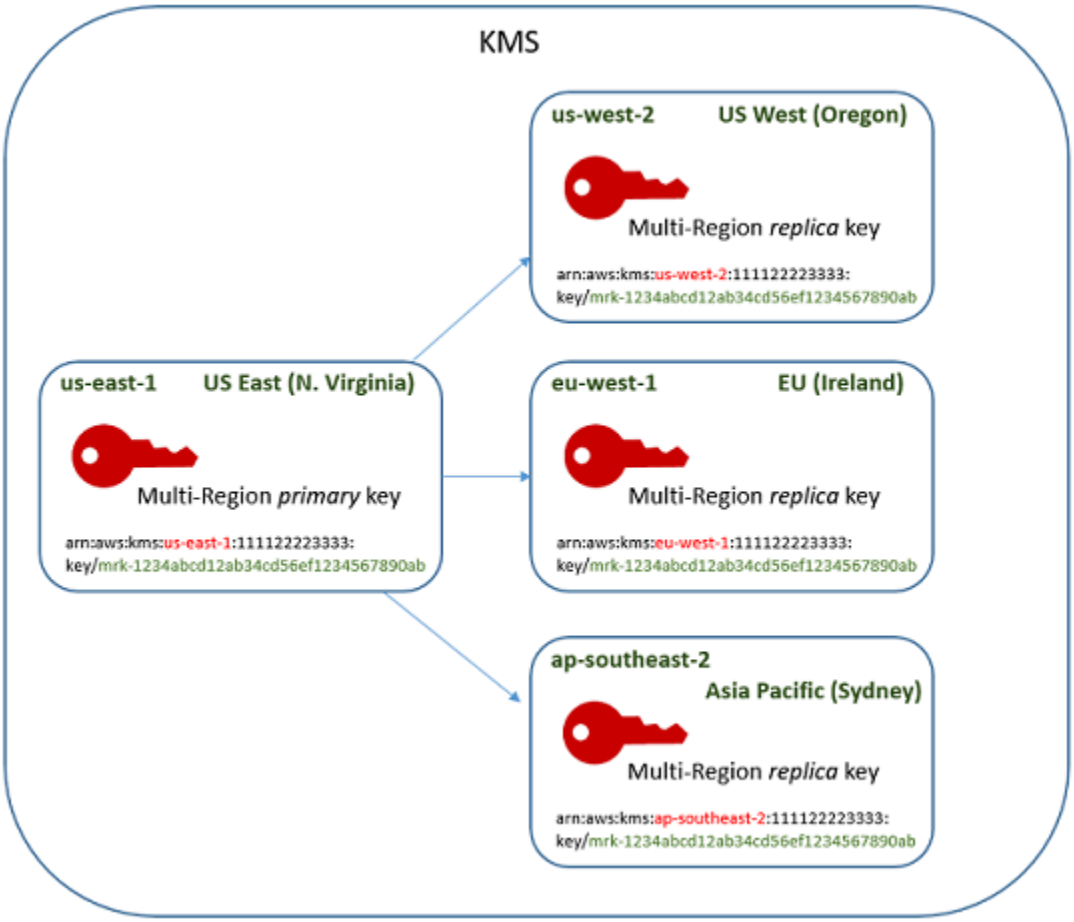
El resultado de la clave de réplica de varias regiones es una clave KMS completamente funcional con las mismas propiedades compartidas que la clave principal. En todos los demás aspectos, es una clave KMS independiente con su propia descripción, política de clave, concesiones, alias y etiquetas. La habilitación o deshabilitación de una clave de varias regiones no tiene ningún efecto en las claves de varias regiones relacionadas. Puede utilizar las claves principal y de réplica de forma independiente en operaciones criptográficas o coordinar su uso. Por ejemplo, puede cifrar datos con la clave principal en la región EE .UU. Este (Norte de Virginia), mover los datos a la región Europa (Irlanda) y usar la clave de réplica para descifrar los datos.

Las claves de varias regiones relacionadas tienen el mismo ID de clave. Sus ARN (nombres de recursos de Amazon) clave solo difieren en el campo Región. Por ejemplo, la clave principal de varias regiones y las claves de réplica pueden tener los siguientes ARN de clave de ejemplo. El ID de clave, que es el último elemento de la clave ARN, es idéntico. Ambas claves tienen el ID de clave distintivo de las claves de varias regiones, que comienza con mrk-.

```
Primary key: arn:aws:kms:us-
east-1:111122223333:key/mrk-1234abcd12ab34cd56ef12345678990ab
Replica key: arn:aws:kms:eu-
west-1:111122223333:key/mrk-1234abcd12ab34cd56ef12345678990ab
```

Se requiere tener el mismo ID de clave para lograr interoperabilidad. Al cifrar, AWS KMS vincula el ID de clave de la clave KMS al texto cifrado para que el texto cifrado solo se pueda descifrar con esa clave KMS o con una clave KMS con el mismo ID de clave. Esta característica también facilita el reconocimiento de las claves de varias regiones relacionadas y facilita su uso de forma intercambiable. Por ejemplo, cuando se utilizan en una aplicación, puede hacer referencia a las claves de varias regiones relacionadas por su ID de clave compartida. A continuación, si es necesario, especifique la Región o ARN para distinguirlos.

A medida que cambien sus necesidades de datos, puede replicar la clave principal Regiones de AWS en otra de la misma partición, como EE. UU. oeste (Oregón) y Asia Pacífico (Sídney). El resultado son cuatro claves de varias regiones relacionadas con el mismo material de claves y los mismos ID de claves, tal y como se muestra en el siguiente diagrama. Administra las claves de forma independiente. Puede usarlas de forma independiente o coordinada. Por ejemplo, puede cifrar datos con la clave de réplica en Asia-Pacífico (Sídney), mover los datos a EE. UU. Oeste (Oregón) y descifrarlos con la clave de réplica en EE. UU. Oeste (Oregón).



Otras consideraciones para las claves de varias regiones son las siguientes.

Sincronización de propiedades compartidas: si una propiedad compartida de las claves multirregionales cambia, sincroniza AWS KMS automáticamente el cambio de la clave principal con todas sus claves de réplica. No puede solicitar ni forzar la sincronización de las propiedades compartidas. AWS KMS detecta y sincroniza todos los cambios por usted. Sin embargo, puede auditar la sincronización utilizando el SynchronizeMultiRegionKeyevento en los CloudTrail registros.

Por ejemplo, si habilita la rotación automática de claves en una clave principal simétrica multirregional, AWS KMS copia esa configuración en todas sus claves de réplica. Cuando se gira el

material clave, la rotación se sincroniza entre todas las claves de varias regiones relacionadas, de modo que sigan teniendo el mismo material clave actual y acceso a todas las versiones anteriores del material clave. Si crea una nueva clave de réplica, tiene el mismo material de clave actual de todas las claves de varias regiones relacionadas y acceso a todas las versiones anteriores del material claves. Para obtener más detalles, consulte Rotación de las claves de varias regiones .

Cambio de la clave principal: cada conjunto de claves de varias regiones debe tener exactamente una clave principal. La clave principal es la única clave que se puede replicar. También es el origen de las propiedades compartidas de sus claves de réplica. Sin embargo, puede cambiar la clave principal a una réplica y promover una de las claves de réplica a primaria. Puede hacerlo para eliminar una clave principal de varias regiones de una región determinada o ubicar la clave principal en una región más cercana a los administradores del proyecto. Para obtener más detalles, consulte Actualización de la región principal.

Eliminar claves multirregionales: al igual que todas las claves de KMS, debe programar la eliminación de claves multirregionales antes de eliminarlas. AWS KMS Mientras la clave está pendiente de eliminación, no puede utilizarla en ninguna operación criptográfica. Sin embargo, no AWS KMS eliminará una clave principal multirregional hasta que se eliminen todas sus claves de réplica. Para obtener más detalles, consulte Eliminación de claves de varias regiones.

Conceptos

Los siguientes términos y conceptos se utilizan con claves de varias regiones.

Clave de varias regiones

Una clave de varias regiones es una de un conjunto de claves KMS con el mismo ID de clave y material de claves (y otras propiedades compartidas) en diferentes Regiones de AWS. Cada clave de varias regiones es una clave KMS que funciona completamente que se puede utilizar independientemente de sus claves de varias regiones relacionadas. Como todas las claves multirregionales relacionadas tienen el mismo identificador de clave y material clave, son interoperables, es decir, cualquier clave multirregional relacionada de una misma Región de AWS puede descifrar el texto cifrado por cualquier otra clave multirregional relacionada.

Usted configura la propiedad de varias regiones de una clave KMS cuando la crea. No se puede cambiar esta propiedad de varias regiones en una clave existente. No se puede convertir una clave de región única en clave de varias regiones ni convertir una clave de varias regiones en una clave de región única. Para mover cargas de trabajo existentes a escenarios de varias regiones, debe volver a cifrar los datos o crear nuevas firmas con nuevas claves de varias regiones.

Una clave multirregional puede ser simétrica o asimétrica y puede utilizar material clave o material clave importado. AWS KMS No puede crear claves de varias regiones en un almacén de claves personalizado.

En un conjunto de claves de varias regiones relacionadas, hay exactamente una clave principal en cualquier momento. Puede crear claves de réplica de esa clave principal en otras Regiones de AWS. También puede actualizar la región principal, que cambia la clave principal a una clave de réplica y cambia una clave de réplica especificada a la clave principal. Sin embargo, solo puede mantener una clave principal o una clave de réplica en cada una. Región de AWS Todas las regiones deben estar en la misma partición de AWS.

Puede tener varios conjuntos de claves de varias regiones relacionadas en la misma o diferentes Regiones de AWS. Aunque las claves de varias regiones relacionadas son interoperables, las claves de varias regiones no relacionadas no son interoperables.

Clave principal

Una clave principal multirregional es una clave de KMS que se puede replicar Regiones de AWS en otra de la misma partición. Cada conjunto de claves de varias regiones tiene una sola clave principal.

Una clave principal difiere de una clave de réplica en las siguientes formas:

- Solo se puede replicar una clave principal.
- La clave principal es el origen de propiedades compartidas de su claves de réplica, incluido el material de la clave y el ID de la clave.
- Puede habilitar y desactivar la rotación automática de claves solo en una clave principal.
- Puede programar la eliminación de una clave principal en cualquier momento. Sin embargo, no AWS KMS eliminará una clave principal hasta que se eliminen todas sus claves de réplica.

Sin embargo, las claves primarias y de réplica no difieren en ninguna propiedad criptográfica. Puede utilizar una clave principal y sus claves de réplica de forma intercambiable.

No es necesario replicar una clave principal. Puede usarla como lo haría con cualquier clave KMS y replicarla cuando sea útil. Sin embargo, dado que las claves de varias regiones tienen propiedades de seguridad diferentes a las claves de una sola región, se recomienda crear una clave de varias regiones solo cuando planee replicarla.

Clave de réplica

Una clave de réplica de varias regiones es una clave KMS que tiene el mismo ID de clave y material de claves que su clave principal y las claves de réplica relacionadas, pero existe en una Región de AWS diferente.

Una clave de réplica es una clave KMS completamente funcional con su propia política de clave, concesiones, alias, etiquetas y otras propiedades. No es una copia ni un puntero a la clave principal ni a ninguna otra clave. Puede utilizar una clave de réplica incluso si su clave principal y todas las claves de réplica relacionadas están deshabilitadas. También puede convertir una clave de réplica en una clave principal y una clave principal en una clave de réplica. Una vez creada, una clave de réplica se basa en su clave principal solo para la rotación de claves y la actualización de la región principal.

Las claves principales y de réplica no difieren en ninguna propiedad criptográfica. Puede utilizar una clave principal y sus claves de réplica de forma intercambiable. Los datos cifrados por una clave principal o de réplica se pueden descifrar con la misma clave o mediante cualquier clave principal o de réplica relacionada.

Replicación

Puede replicar una clave principal multirregional Región de AWS en otra diferente de la misma partición. Al hacerlo, AWS KMS crea una clave de réplica multirregional en la región especificada con el mismo ID de clave y otras propiedades compartidas que su clave principal. Luego transporta de forma segura el material clave a través del límite de la región y lo asocia con la nueva clave de réplica, todo dentro de AWS KMS.

Propiedades compartidas

Las propiedades compartidas son propiedades de una clave principal multirregional que se comparten con sus claves de réplica. AWS KMS crea las claves de réplica con los mismos valores de propiedad compartidos que los de la clave principal. A continuación, sincroniza periódicamente los valores de propiedad compartida de la clave principal con sus claves de réplica. No puede establecer estas propiedades en una clave de réplica.

Las siguientes son las propiedades compartidas de claves de varias regiones.

- ID de clave: (el elemento de la `Region` del ARN de clave difiere).
- Material de claves

- Origen del material de claves
- Especificación de clave y algoritmos de cifrado
- Uso de claves
- Rotación automática de claves: solo puede habilitar y desactivar la rotación automática de claves en la clave principal. Las nuevas claves de réplica se crean con todas las versiones del material de claves compartido. Para obtener más detalles, consulte Rotación de las claves de varias regiones .
- Rotación bajo demanda: solo puede realizar la rotación bajo demanda en la clave principal. Las nuevas claves de réplica se crean con todas las versiones del material de claves compartido. Para obtener más detalles, consulte Rotación de las claves de varias regiones .

También puede pensar en las designaciones primarias y de réplica de claves de varias regiones relacionadas como propiedades compartidas. Al crear nuevas claves de réplica o actualizar la clave principal, AWS KMS sincroniza el cambio con todas las claves multirregionales relacionadas. Cuando se completan estos cambios, todas las claves de varias regiones relacionadas muestran su clave principal y las claves de réplica con precisión.

Todas las demás propiedades de las claves de varias regiones sonpropiedades independientes, incluida la descripción, la política de claves, las concesiones, los estados clave habilitados y deshabilitados, los alias y las etiquetas. Puede establecer los mismos valores para estas propiedades en todas las claves de varias regiones relacionadas, pero si cambia el valor de una propiedad independiente, AWS KMS no lo sincroniza.

Puede realizar un seguimiento de la sincronización de las propiedades compartidas de las claves de varias regiones. Busca el evento en tu AWS CloudTrail registro. SynchronizeMultiRegionKey

Control del acceso a claves de varias regiones

Puede usar claves de varias regiones en escenarios de conformidad, recuperación de desastres y copia de seguridad que serían más complejos con claves de una sola región. Sin embargo, dado que las propiedades de seguridad de las claves de varias regiones son significativamente diferentes de las de las claves de una sola región, recomendamos tener precaución al autorizar la creación, la administración y el uso de claves de varias regiones.

> **Note**
>
> Las declaraciones de la política de IAM existentes con caracteres comodín en el campo `Resource` ahora se aplican a las claves de una sola región y de varias regiones. Para

restringirlas a claves KMS de una sola región o claves de varias regiones, utilice la clave de MultiRegion condición kms:.

Utilice las herramientas de autorización para evitar la creación y el uso de claves de varias regiones en cualquier escenario en el que una sola región sea suficiente. Permita a las entidades principales replicar una clave de varias regiones solo en las Regiones de AWS que las requieran. De permiso para las claves de varias regiones solo a las entidades principales que las necesiten y solo para las tareas que las requieran.

Puede usar políticas de clave, políticas de IAM y concesiones para permitir que las entidades principales de IAM administren y usen claves de varias regiones en su Cuenta de AWS. Cada clave de varias regiones es un recurso independiente con un ARN clave única y una política clave. Debe establecer y mantener una política clave para cada clave y asegurarse de que las políticas de IAM nuevas y existentes implementen su estrategia de autorización.

Temas

- Conceptos básicos de autorización para claves de varias regiones
- Autorización de administradores y usuarios clave de varias regiones
- Autorización de AWS KMS para la sincronización de claves de varias regiones

Conceptos básicos de autorización para claves de varias regiones

Al diseñar políticas de claves y políticas de IAM para claves de varias regiones, tenga en cuenta los siguientes principios.

- Política de claves: cada clave de varias regiones es un recurso clave KMS independiente con su propia política de claves. Puede aplicar la misma política de clave o una política de clave diferente para cada clave del conjunto de claves de varias regiones relacionadas. Las políticas de claves no son propiedades compartidas de claves de varias regiones. AWS KMS no copia ni sincroniza las políticas clave entre las claves de varias regiones relacionadas.

  Cuando se crea una clave de réplica en la consola de AWS KMS, la consola muestra la política de clave actual de la clave principal como conveniencia. Puede utilizar esta política de claves, editarla o eliminarla y reemplazarla. Pero incluso si acepta la política de clave principal sin cambios, AWS KMSno sincroniza las políticas. Por ejemplo, si cambia la política de clave de la clave principal, la política de clave de la clave de réplica sigue siendo la misma.

- Política de claves predeterminada: al crear claves multirregionales mediante las `ReplicateKey` operaciones CreateKeyy, se aplica la política de claves predeterminada, a menos que especifique una política de claves en la solicitud. Esta es la misma política de clave predeterminada que se aplica a las claves de una sola región.
- Políticas de IAM: al igual que con todas las claves KMS, puede usar políticas de IAM para controlar el acceso a las claves de varias regiones solo cuando la política clave lo permite. Las políticas de IAM se aplican a todas las Regiones de AWS de forma predeterminada. Sin embargo, puede utilizar claves de condición, como aws: RequestedRegion, para limitar los permisos a una región concreta.

  Para crear claves primarias y de réplica, las entidades principales deben tener permiso `kms:CreateKey` en una política de IAM que se aplica a la región donde se crea la clave.
- Concesiones:AWS KMS las concesiones son regionales. Cada concesión da permisos para una clave KMS. Puede utilizar concesiones para dar permisos a una clave principal de varias regiones o clave de réplica. Sin embargo, no puede utilizar una sola concesión para dar permisos a varias claves KMS, incluso si se trata de claves de varias regiones relacionadas.
- ARN de clave: cada clave de varias regiones tiene un ARN de clave única. Los ARN clave de las claves de varias regiones relacionadas tienen la misma partición, cuenta e ID de clave, pero diferentes regiones.

  Para aplicar una declaración de política de IAM a una clave concreta de varias regiones, utilice su ARN clave o un patrón ARN clave que incluya la región. Para aplicar una declaración de política de IAM a todas las claves de varias regiones, utilice un comodín (*) en el elemento Región del ARN, como se muestra en el siguiente ejemplo.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Describe*",
    "kms:List*"
  ],
  "Resource": {
      "arn:aws:kms:*::111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab"
  }
}
```

Para aplicar una declaración de política a todas las claves multirregionales de su Cuenta de AWS país, puede utilizar la condición de MultiRegion política kms: o un patrón de identificador de clave que incluya el `mrk-` prefijo distintivo.

- Función vinculada al servicio: los directores que crean claves principales multirregionales deben tener el permiso iam:. CreateServiceLinkedRole

  Para sincronizar las propiedades compartidas de claves de varias regiones relacionadas, AWS KMS asume un rol vinculado al servicio de de IAM. AWS KMS crea el rol vinculado a un servicio en la Cuenta de AWS cuando crea una clave principal de varias regiones. (Si la función existe, AWS KMS lo recrea, que no tiene ningún efecto nocivo). El rol es válido en todas las regiones. Para poder crear (o volver AWS KMS a crear) el rol vinculado al servicio, los directores que creen claves principales multirregionales deben tener el permiso iam:. CreateServiceLinkedRole

Autorización de administradores y usuarios clave de varias regiones

Las entidades principales que crean y administran claves de varias regiones necesitan los siguientes permisos en las regiones principal y de réplica:

- `kms:CreateKey`
- `kms:ReplicateKey`
- `kms:UpdatePrimaryRegion`
- `iam:CreateServiceLinkedRole`

Creación de una clave principal

Para crear una clave principal multirregional, el director necesita CreateServiceLinkedRole permisos kms: CreateKey e iam: en una política de IAM que sea efectiva en la región de la clave principal. Las entidades principales que tienen estos permisos pueden crear claves de una sola región y de varias regiones a menos que restrinja sus permisos.

El `iam:CreateServiceLinkedRole` permiso permite crear el AWSServiceRoleForKeyManagementServiceMultiRegionKeysrol AWS KMS para sincronizar las propiedades compartidas de las claves multirregionales relacionadas.

Por ejemplo, esta política de IAM permite a una entidad de seguridad crear cualquier tipo de clave KMS.

```
{
  "Version": "2012-10-17",
  "Statement":{
      "Action": [
        "kms:CreateKey",
        "iam:CreateServiceLinkedRole"
      ],
      "Effect":"Allow",
      "Resource":"*"
  }
}
```

Para permitir o denegar el permiso para crear claves principales multirregionales, utilice la clave de condición kms: MultiRegion. Los valores válidos son `true` (clave de varias regiones) o `false` (clave de una sola región). Por ejemplo, la siguiente declaración de política de IAM utiliza una acción `Deny` con la clave de condición `kms:MultiRegion` para evitar que las entidades principales creen claves de varias regiones.

```
{
  "Version": "2012-10-17",
  "Statement":{
      "Action":"kms:CreateKey",
      "Effect":"Deny",
      "Resource":"*",
      "Condition": {
          "Bool": "kms:MultiRegion": true
      }
  }
}
```

Claves de replicación

Para crear una clave de réplica de varias regiones, la entidad principal necesita los siguientes permisos:

- kms: ReplicateKey permiso en la política de claves de la clave principal.
- kms: CreateKey permiso en una política de IAM que está en vigor en la región de claves réplicas.

Tenga cuidado al permitir estos permisos. Permiten a las entidades principales crear claves KMS y las políticas de claves que autorizan su uso. El permiso `kms:ReplicateKey` también autoriza la transferencia de material clave a través de los límites de la región dentro de AWS KMS.

Para restringir los campos Regiones de AWS en los que se puede replicar una clave multirregional, utilice la clave de condición kms: ReplicaRegion. Limita solo el permiso `kms:ReplicateKey`. De lo contrario, no tiene ningún efecto. Por ejemplo, la siguiente política de claves permite a la entidad principal replicar esta clave principal, pero solo en las regiones especificadas.

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Administrator"
  },
  "Action": "kms:ReplicateKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:ReplicaRegion": [
         "us-east-1",
         "eu-west-3",
         "ap-southeast-2"
      ]
    }
  }
}
```

Actualización de la región principal

Las entidades principales autorizadas pueden convertir una clave de réplica en una clave principal, lo que cambia la clave principal anterior en una réplica. Esta acción se denomina actualización de la región principal. Para actualizar la región principal, el director necesita el UpdatePrimaryRegion permiso kms: en ambas regiones. Puede proporcionar estos permisos en una política de claves o una política de IAM.

- `kms:UpdatePrimaryRegion` en la clave principal. Este permiso debe ser efectivo en la región de clave principal.
- `kms:UpdatePrimaryRegion` en la clave de réplica. Este permiso debe ser efectivo en la región clave de réplica.

Por ejemplo, la siguiente política de clave otorga a los usuarios que pueden asumir el permiso de rol de Administrador para actualizar la región principal de la clave KMS. Esta clave KMS puede ser la clave principal o una clave de réplica en esta operación.

```
{
  "Effect": "Allow",
  "Resource": "*",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/Administrator"
  },
  "Action": "kms:UpdatePrimaryRegion"
}
```

Para restringir Regiones de AWS lo que puede alojar una clave principal, utilice la clave de PrimaryRegion condición kms:. Por ejemplo, la siguiente declaración de política de IAM permite que las entidades principales actualicen la región principal de las claves de varias regiones en la Cuenta de AWS, pero solo cuando la nueva Región principal es una de las Regiones especificadas.

```
{
  "Effect": "Allow",
  "Action": "kms:UpdatePrimaryRegion",
  "Resource": {
      "arn:aws:kms:*:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": {
      "kms:PrimaryRegion": [
         "us-west-2",
         "sa-east-1",
         "ap-southeast-1"
      ]
    }
  }
}
```

Uso y administración de claves de varias regiones

De forma predeterminada, las principales entidades que tienen permiso para usar y administrar claves KMS en una Cuenta de AWS y Región también tienen permiso para usar y administrar claves de varias regiones. Sin embargo, puede usar la clave de MultiRegion condición kms: para permitir solo claves de una sola región o solo claves de varias regiones. O bien, utilice la clave de

MultiRegionKeyType condición kms: para permitir solo las claves principales de varias regiones o solo las claves de réplica. Ambas claves de condición controlan el acceso a la CreateKeyoperación y a cualquier operación que utilice una clave KMS existente, como Encrypt o. EnableKey

En el siguiente ejemplo de declaración de política de IAM se utiliza la clave de condición `kms:MultiRegion` para evitar que las entidades principales utilicen o administren cualquier clave de varias regiones.

```
{
  "Effect": "Deny",
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "Bool": "kms:MultiRegion": true
  }
}
```

Esta declaración de política de IAM de ejemplo utiliza la condición `kms:MultiRegionKeyType` para permitir que las entidades principales programen y cancelen la eliminación de claves, pero solo en las claves de réplica de varias regiones.

```
{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": {
      "arn:aws:kms:us-west-2:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": "kms:MultiRegionKeyType": "REPLICA"
  }
}
```

Autorización de AWS KMS para la sincronización de claves de varias regiones

Para apoyar las claves de varias regiones, AWS KMS utiliza una función vinculada al servicio de IAM. Este rol le da a AWS KMS los permisos que necesita para sincronizar propiedades compartidas. Puede ver el SynchronizeMultiRegionKey CloudTrail evento que registra la AWS KMS sincronización de propiedades compartidas en sus AWS CloudTrail registros.

Acerca del rol vinculado a un servicio para claves de varias regiones

Un rol vinculado a un servicio es un rol de IAM que otorga permiso a un servicio de AWS para llamar a otros servicios de AWS en su nombre. Se ha diseñado para facilitar el uso de las características de múltiples servicios de AWS integrados sin tener que crear ni actualizar políticas de IAM complejas.

En el caso de las claves multirregionales, AWS KMS crea el rol AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculado al servicio con la política. AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy Esta política le confiere al rol el permiso `kms:SynchronizeMultiRegionKey`, que le permite sincronizar las propiedades compartidas de claves de varias regiones.

Como el rol AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculado al servicio es únicamente de confianza`mrk.kms.amazonaws.com`, solo AWS KMS puede asumir este rol vinculado al servicio. Este rol se limita a las operaciones que AWS KMS necesita para sincronizar las propiedades compartidas de varias regiones. No concede permisos adicionales a AWS KMS. Por ejemplo, AWS KMS no tiene permiso para crear, replicar o eliminar claves KMS.

Para obtener más información acerca de cómo los servicios de AWS utilizan los roles vinculados con el servicio, consulte Uso de roles vinculados a servicios en la Guía del usuario de IAM.

Creación del rol vinculado a servicios

AWS KMScrea automáticamente el rol AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculado al servicio en usted Cuenta de AWS al crear una clave multirregional, si el rol aún no existe. No puede crear o volver a crear este rol vinculado a un servicio directamente.

Editar la descripción del rol vinculado a un servicio

No puede editar el nombre del rol ni las declaraciones de política del rol AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculado al servicio, pero sí puede editar la descripción del rol. Para obtener más información, consulte Editar un rol vinculado a un servicio en la Guía del usuario de IAM.

Eliminar el rol vinculado a servicios

AWS KMSno elimina el rol AWSServiceRoleForKeyManagementServiceMultiRegionKeysvinculado al servicio de su cuenta Cuenta de AWS y usted no puede eliminarlo. Sin embargo, AWS KMS no asume el AWSServiceRoleForKeyManagementServiceMultiRegionKeysrol ni usa ninguno de sus permisos a menos que tenga claves multirregionales en su Cuenta de AWS región.

Creación de claves de varias regiones

Puede crear claves de varias regiones en la consola o mediante la API de AWS KMS.

La propiedad de varias regiones establecida en este procedimiento es inmutable. No se puede convertir una clave de región única en clave de varias regiones ni convertir una clave de varias regiones en una clave de región única.

Temas

- Creación de claves primarias de varias regiones
- Creación de claves de réplica de varias regiones

Creación de claves primarias de varias regiones

Puede crear una clave principal de varias regiones en la consola de AWS KMS o mediante la API de AWS KMS. Puede crear la clave principal en cualquier Región de AWS donde AWS KMS admite claves de varias regiones.

Para crear una clave principal multirregional, el director necesita los mismos permisos que necesita para crear cualquier clave de KMS, incluido el CreateKey permiso kms: en una política de IAM. El director también necesita el permiso iam:. CreateServiceLinkedRole Puede usar la clave de MultiRegionKeyType condición kms: para permitir o denegar el permiso para crear claves principales multirregionales.

Estas declaraciones crean una clave principal de varias regiones con material de claves que AWS KMS genera. Para crear una clave principal de varias regiones con material de claves importado, consulte Crear una clave principal con material de claves importado.

Temas

- Creación de una clave principal de varias regiones (consola)
- Creación de una clave principal de varias regiones (API de AWS KMS)

Creación de una clave principal de varias regiones (consola)

Para crear una clave principal de varias regiones en la consola AWS KMS, utilice el mismo proceso que usaría para crear cualquier clave KMS. Seleccione una clave de varias regiones en Advanced options (Opciones avanzadas). Para obtener instrucciones completas, consulte Crear claves.

> **Important**
>
> No incluya información confidencial en el alias, la descripción ni las etiquetas. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija Create key.
5. Seleccione un tipo de clave simétrica o asimétrica. Las claves simétricas son las predeterminadas.

   Puede crear claves simétricas y asimétricas de varias regiones, incluidas las claves de KMS HMAC de varias regiones, que son simétricas.
6. Seleccione el uso de claves. Encrypt and decrypt (Cifrar y descifrar) es el valor predeterminado.

   Para obtener ayuda, consulte the section called “Crear claves”, the section called “Creación de claves KMS asimétricas” o the section called “Creación de claves HMAC”.
7. Expanda Advanced options (Opciones avanzadas).
8. En Key material origin (Origen del material de claves), para hacer que AWS KMS genere el material clave que compartirán sus claves principales y de réplica, elija KMS. Si importa material de claves en las claves principal y de réplica, elija External (Import key material) Externo (material de claves importado).
9. En Key material origin (Replicación de varias regiones), elija Allow this key to be replicated into other Regions (Permitir que esta clave se replique en otras regiones).

   No puede cambiar esta configuración después de crear la clave KMS.
10. Escriba un alias para la clave principal.

    Los alias no son una propiedad compartida de claves de varias regiones. Puede asignar a su clave principal de varias regiones y sus réplicas el mismo alias o alias diferentes. AWS KMS no sincroniza los alias de las claves de varias regiones.

> **Note**
>
> Agregar, eliminar o actualizar un alias puede permitir o denegar el permiso a la clave KMS. Para más detalles, consulte ABAC para AWS KMS y Usar alias para controlar el acceso a las claves KMS.

11. (Opcional) Escriba una descripción de la clave primaria.

    Las descripciones no son una propiedad compartida de las claves de varias regiones. Puede dar a su clave principal de varias regiones y sus réplicas la misma descripción o descripciones diferentes. AWS KMS no sincroniza las descripciones de las claves de varias regiones.

12. (Opcional) Escriba una clave de etiqueta y un valor de etiqueta opcional. Para asignar más de una etiqueta a la clave principal, elija Add tag (Agregar etiqueta).

    Las etiquetas no son una propiedad compartida de las claves de varias regiones. Puede asignar a su clave principal de varias regiones y sus réplicas las mismas etiquetas o etiquetas diferentes. AWS KMS no sincroniza las etiquetas de las claves de varias regiones. Puede cambiar las etiquetas de las claves KMS en cualquier momento.

> **Note**
>
> Etiquetar o quitar las etiquetas de la clave KMS puede permitir o denegar permiso a la clave KMS. Para más detalles, consulte ABAC para AWS KMS y Uso de etiquetas para controlar el acceso a las claves KMS.

13. Seleccione los usuarios y roles de IAM que pueden administrar la clave principal.

> **Note**
>
> Las políticas de IAM pueden otorgar permisos para que usuarios y roles de IAM administren la clave KMS.
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

Este paso inicia el proceso de creación de una política de claves para la clave principal. Las políticas de clave no son una propiedad compartida de las claves de varias regiones. Puede asignar a su clave principal de varias regiones y sus réplicas la misma política de claves o políticas de claves diferentes. AWS KMS no sincroniza las políticas de claves de varias regiones. Puede cambiar la política de claves de una clave KMS en cualquier momento.

14. Complete los pasos para crear la política de claves, incluida la selección de usuarios de claves. Después de revisar la política de claves, elija Finish (Finalizar) para crear la clave KMS

Creación de una clave principal de varias regiones (API de AWS KMS)

Para crear una clave principal multirregional, utilice la CreateKeyoperación. Utilice el parámetro `MultiRegion` con un valor de `True`.

Por ejemplo, el siguiente comando crea una clave principal de varias regiones en la Región de AWS de la persona que llama (us-east-1). Acepta valores predeterminados para todas las demás propiedades, incluida la política de claves. Los valores predeterminados para las claves principales de varias regiones son los mismos que los valores predeterminados para todas las demás claves KMS, incluida la política de claves predeterminada. Este procedimiento crea una clave de cifrado simétrica, la clave KMS predeterminada.

La respuesta incluye el elemento `MultiRegion` y el elemento `MultiRegionConfiguration` con subelementos y valores típicos para una clave principal de varias regiones sin claves de réplica. La ID de clave de una clave de varias regiones siempre comienza con `mrk-`.

Important

No incluya información confidencial en los campos `Description` o `Tags`. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

```
$ aws kms create-key --multi-region
{
    "KeyMetadata": {
        "Origin": "AWS_KMS",
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "Description": "",
        "KeyManager": "CUSTOMER",
```

```
        "Enabled": true,
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
        "CreationDate": 1606329032.475,
        "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "AWSAccountId": "111122223333",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegion": true,
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-east-1"
            },
            "ReplicaKeys": [ ]
      }
    }
}
```

Creación de claves de réplica de varias regiones

Puede crear una clave de réplica multirregional en la AWS KMS consola, mediante la ReplicateKeyoperación o mediante una AWS CloudFormationplantilla. No puede utilizar la CreateKeyoperación para crear una clave de réplica.

Puede utilizar estos procedimientos para replicar cualquier clave principal de varias regiones, incluida una clave simétrica de KMS de cifrado, una clave asimétrica de KMS o una clave KMS HMAC.

Cuando se completa esta operación, la nueva clave de réplica tiene un valor transitorio de estado clave de `Creating`. Este estado de clave cambia a `Enabled` (o PendingImport) después de unos segundos cuando se completa el proceso de creación de la nueva clave de réplica. Mientras el estado de la clave es `Creating`, puede administrar las claves, pero aún no puede usarlas en operaciones criptográficas. Si va a crear y utilizar la clave de réplica mediante programación, vuelva a intentarlo `KMSInvalidStateException` o llame DescribeKeypara comprobar su `KeyState` valor antes de utilizarla.

En caso de que elimine por error una clave de réplica, puede utilizar este procedimiento para volver a crearla. En caso de que replique la misma clave primaria en la misma región, la nueva clave de réplica que cree tendrá las mismas propiedades compartidas que la clave de réplica original.

> **Important**
>
> No incluya información confidencial en el alias, la descripción ni las etiquetas. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

Más información

- Para crear una clave de réplica de varias regiones con material de claves importado, consulte Creación de una clave de réplica con material de claves importado.
- Para usar una AWS CloudFormation plantilla para crear una clave de réplica, consulte AWS::KMS::ReplicaKeyla Guía del AWS CloudFormation usuario.

Temas

- Regiones de réplica
- Creación de claves de réplica (consola)
- Crear una clave de réplica (API de AWS KMS)

Regiones de réplica

Normalmente, opta por replicar una clave de varias regiones en una Región de AWS en función de su modelo de negocio y los requisitos reglamentarios. Por ejemplo, puede replicar una clave en Regiones donde guarda sus recursos. O bien, para cumplir con un requisito de recuperación de desastres, puede replicar una clave en regiones geográficamente distantes.

Los siguientes son los requisitos de AWS KMS para las regiones de réplica. Si la región que eliges no cumple con estos requisitos, se producirá un error en los intentos de replicar una clave.

- Una clave de varias regiones relacionada por región: no se puede crear una clave de réplica en la misma Región que su clave principal, o en la misma Región que otra réplica de la clave principal.

  En caso de que intente replicar una clave primaria en una región que ya tiene una réplica de esa clave primaria, el intento producirá un error. En caso de que la clave de réplica actual de la región

se encuentre en el estado de clave `PendingDeletion`, puede cancelar la eliminación de la clave de réplica o esperar hasta que se elimine.

- Múltiples claves de varias regiones no relacionadas en la misma región: puede tener varias claves de varias regiones no relacionadas en la misma región. Por ejemplo, puede tener dos claves principales de varias regiones en la región `us-east-1`. Cada una de las claves principales puede tener una clave de réplica en la región `us-west-2`.
- Regiones en la misma partición: la región de la clave de réplica debe estar en la misma partición de AWS que la región de claves principal.
- La región debe estar habilitada: si una región está deshabilitada de forma predeterminada, no puede crear ningún recurso en esa región hasta que esté habilitado para su Cuenta de AWS.

Creación de claves de réplica (consola)

En la consola de AWS KMS, puede crear una o varias réplicas de una clave principal de varias regiones en la misma operación.

Este procedimiento es similar a la creación de una clave KMS de una sola región estándar en la consola. Sin embargo, dado que una clave de réplica se basa en la clave principal, no se seleccionan valores para propiedades compartidas, como la especificación de la clave (simétrica o asimétrica), el uso de la clave u origen de la clave.

Se especifican propiedades que no se comparten, como un alias, etiquetas, una descripción y una política de clave. Como conveniencia, la consola muestra los valores de propiedad actuales de la clave principal, pero puede cambiarlos. Incluso si mantiene los valores de la clave principal, AWS KMS no mantiene estos valores sincronizados.

> **Important**
>
> No incluya información confidencial en el alias, la descripción ni las etiquetas. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.

4. Seleccione el alias o el ID de clave de una clave principal de varias regiones. Se abrirá la página de detalles de clave de la clave KMS.

   Para identificar una clave principal de varias regiones, utilice el icono de herramienta situado en la esquina superior derecha para agregar la columna Regionality (Regionalidad) de la tabla.
5. Elija la pestaña Regionality (Regionalidad).
6. En la sección Related multi-Region keys (Claves de varias regiones relacionadas), elija Create new replica keys (Crear nuevas claves de réplica).

   La sección Related multi-Region keys (Claves de varias regiones relacionadas) muestra la región de la clave principal y sus claves de réplica. Puede utilizar esta pantalla para ayudarle a elegir la región para su nueva clave de réplica.
7. Seleccione una o más Regiones de AWS. Este procedimiento crea una clave de réplica en cada una de las regiones seleccionadas.

   El menú incluye solo Regiones en la misma partición AWS que la clave principal. Las regiones que ya tienen una clave de varias regiones relacionadas se muestran, pero no se pueden seleccionar. Es posible que no tenga permiso para replicar una clave en todas las regiones del menú.

   Cuando haya terminado de elegir Regiones, cierre el menú. Aparecerán las regiones elegidas. Para cancelar la replicación en una región, seleccione la Xque está junto al nombre de la región.
8. Escriba un alias para la clave de réplica.

   La consola muestra uno de los alias actuales de la clave principal, pero puede cambiarlo. Puede asignar a su clave principal de varias regiones y sus réplicas el mismo alias o a alias diferentes. Los alias no son una propiedad compartida de claves de varias regiones. AWS KMS no sincroniza los alias de las claves de varias regiones.

   Agregar, eliminar o actualizar un alias puede permitir o denegar el permiso a la clave KMS. Para más detalles, consulte ABAC para AWS KMS y Usar alias para controlar el acceso a las claves KMS.
9. (Opcional) Escriba una descripción de la clave de réplica.

   La consola muestra la descripción actual de la clave principal, pero puede cambiarla. Las descripciones no son una propiedad compartida de las claves de varias regiones. Puede dar a su clave principal de varias regiones y sus réplicas la misma descripción o descripciones diferentes. AWS KMS no sincroniza las descripciones de las claves de varias regiones.

10. (Opcional) Escriba una clave de etiqueta y un valor de etiqueta opcional. Para asignar más de una etiqueta a la clave de réplica, elija Add tag (Agregar etiqueta).

    La consola muestra las etiquetas actualmente conectadas a la clave principal, pero puede cambiarlas. Las etiquetas no son una propiedad compartida de las claves de varias regiones. Puede asignar a su clave principal de varias regiones y sus réplicas las mismas etiquetas o etiquetas diferentes. AWS KMS no sincroniza las etiquetas de las claves de varias regiones.

    Etiquetar o quitar las etiquetas de la clave KMS puede permitir o denegar permiso a la clave KMS. Para más detalles, consulte ABAC para AWS KMS y Uso de etiquetas para controlar el acceso a las claves KMS.

11. Seleccione los usuarios y roles de IAM que pueden administrar la clave de réplica.

    > **Note**
    >
    > Las políticas de IAM pueden otorgar permisos para que los usuarios y roles de IAM administren las claves de réplica.
    > Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

    Este paso comienza el proceso de creación de una política de claves para la clave de réplica. La consola muestra la política de clave actual de la clave principal, pero puede cambiarla. Las políticas de clave no son una propiedad compartida de las claves de varias regiones. Puede asignar a su clave principal de varias regiones y sus réplicas la misma política de claves o políticas de claves diferentes. AWS KMS no sincroniza las políticas de claves. Puede cambiar la política de claves de cualquier clave KMS en cualquier momento.

12. Complete los pasos para crear la política de claves, incluida la selección de usuarios de claves. Después de revisar la política de claves, elija Finish (Finalizar) para crear la clave de réplica.

Crear una clave de réplica (API de AWS KMS)

Para crear una clave de réplica multirregional, utilice la ReplicateKeyoperación. No puede utilizar la CreateKeyoperación para crear una clave de réplica. Esta operación crea las claves de réplica de

una en una. La región que especifique debe cumplir con los Requisitos de región para las claves de réplica.

Cuando utiliza la operación `ReplicateKey`, no especifique valores para ninguna propiedad compartida de claves de varias regiones. Los valores de propiedad compartida se copian de la clave principal y se mantienen sincronizados. Sin embargo, puede especificar valores para las propiedades que no se comparten. De lo contrario, AWS KMS aplica los valores predeterminados estándar para las claves KMS, no los valores de la clave principal.

> **Note**
>
> Si no especifica valores para los parámetros `Description`, `KeyPolicy` o `Tags`, AWS KMS crea la clave de réplica sin etiquetas con una descripción de cadena vacía y la política de claves predeterminada.
> No incluya información confidencial en los campos `Description` o `Tags`. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

Por ejemplo, el comando siguiente crea una clave de réplica de varias regiones en la región Asia Pacífico (Sídney) (ap-southeast-2). Esta clave de réplica está modelada en la clave principal de la región EE. UU. Este (Norte de Virginia) (us-east-1), que se identifica mediante el valor del parámetro `KeyId`. En este ejemplo se aceptan valores predeterminados para todas las demás propiedades, incluida la política de claves.

La respuesta describe la nueva clave de réplica. Incluye campos para propiedades compartidas, como el `KeyId`, `KeySpec`, `KeyUsage` y el origen del material clave (`Origin`). También incluye propiedades que son independientes de la clave principal, como la `Description`, la política de claves (`ReplicaKeyPolicy`), y las etiquetas (`ReplicaTags`).

La respuesta también incluye el ARN clave y la región de la clave principal y todas sus claves de réplica, incluida la que se acaba de crear en la región ap-southeast-2. En este ejemplo, el elemento `ReplicaKey` muestra que esta clave principal ya se replicó en la región Europa (Irlanda) (eu-west-1).

```
$ aws kms replicate-key \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \
    --replica-region ap-southeast-2
{
```

```
    "ReplicaKeyMetadata": {
        "MultiRegion": true,
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "REPLICA",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-east-1"
            },
            "ReplicaKeys": [
                {
                    "Arn": "arn:aws:kms:ap-southeast-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "ap-southeast-2"
                },
                {
                    "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "eu-west-1"
                }
            ]
        },
        "AWSAccountId": "111122223333",
        "Arn": "arn:aws:kms:ap-southeast-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "CreationDate": 1607472987.918,
        "Description": "",
        "Enabled": true,
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    },
    "ReplicaKeyPolicy": "{\n  \"Version\" : \"2012-10-17\",\n  \"Id\" : \"key-
default-1\",...,
    "ReplicaTags": []
}
```

Visualización de claves de varias regiones

Puede ver las claves de una sola región y de varias regiones en la consola AWS KMS y mediante las operaciones de la API de AWS KMS.

Temas

- Visualización de las claves de varias regiones en la consola
- Visualización de claves de varias regiones en la API

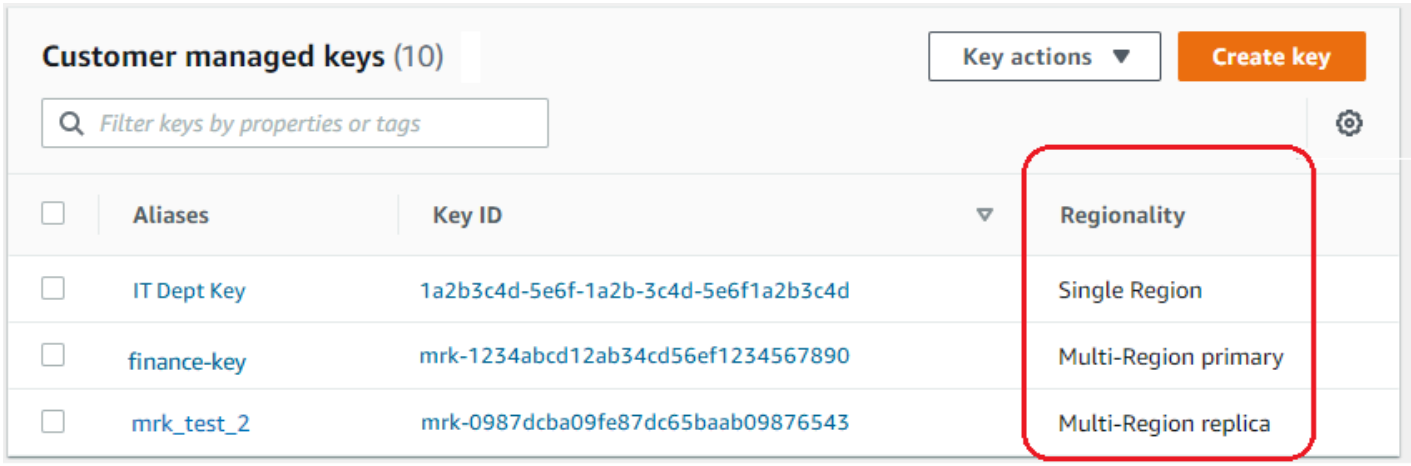
Visualización de las claves de varias regiones en la consola

En la consola de AWS KMS, puede ver las claves KMS en la región seleccionada. Sin embargo, si tiene una clave de varias regiones, puede ver sus claves de varias regiones relacionadas en otras Regiones de AWS.

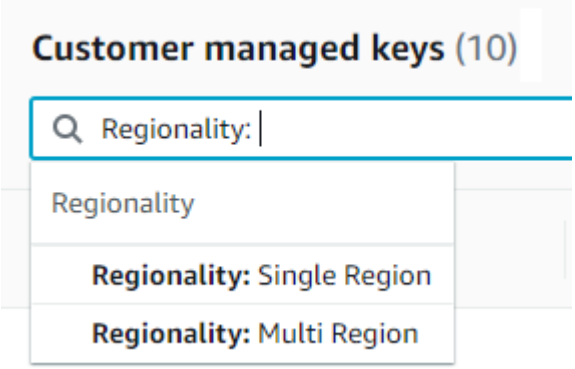
La tabla de Customer managed keys (Claves administradas por clientes) en la consola de AWS KMS muestra solo las claves KMS en la región seleccionada. Puede ver las claves principales y de réplica de varias regiones en la región seleccionada. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.

La tabla Claves administradas por AWS no tiene las características de regionalidad dado que las Claves administradas por AWS son siempre claves de una sola región.

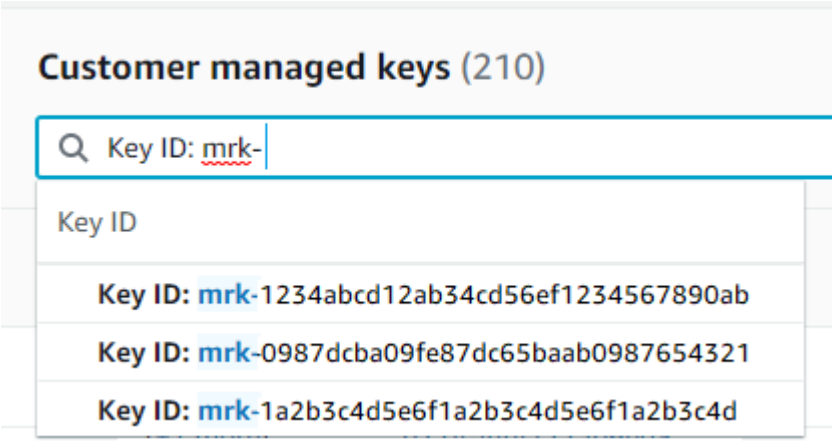
- Para facilitar la identificación de las claves de varias regiones, agregue la columna Regionality (Regionalidad) a la tabla de claves. Para obtener ayuda, consulte Personalización de las tablas clave KMS.



- Para mostrar solo las claves de una sola región o solo las claves de varias regiones en la tabla de claves, filtre las claves por la propiedad Regionality (Regionalidad) de cada clave. Para obtener ayuda, consulte Ordenar y filtrar las claves KMS.



- También puede ordenar y filtrar su tabla Customer managed keys (Claves administradas por el cliente) para el prefijo distintivo de ID de clave mrk-.

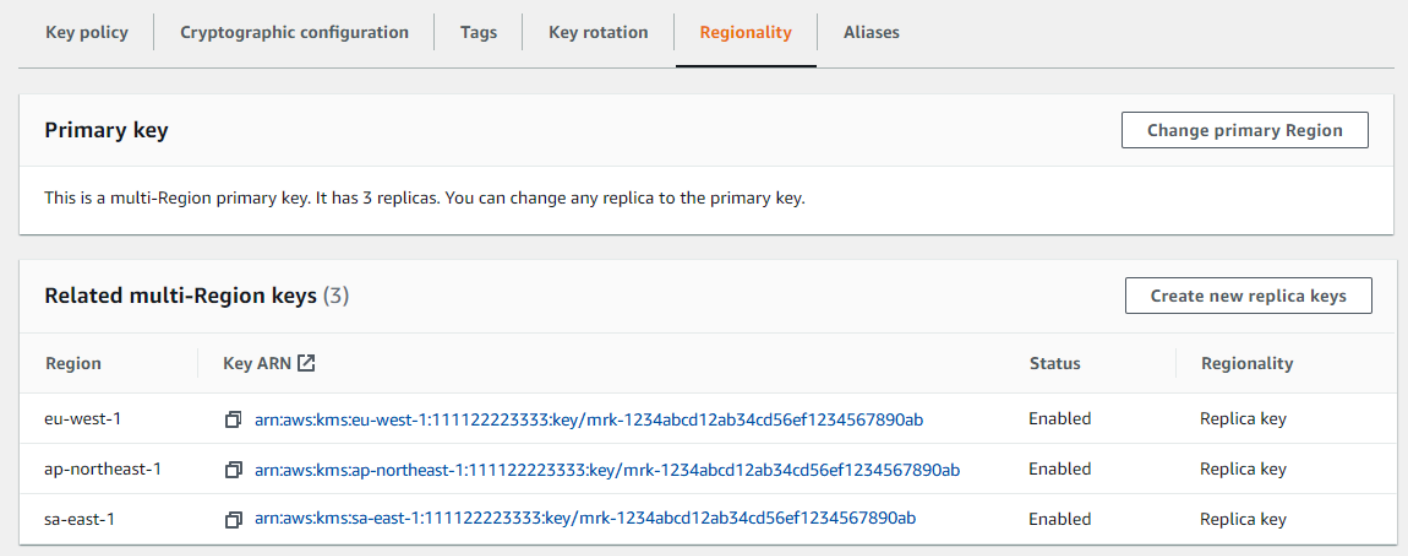


- Para obtener más información acerca de una clave principal de varias regiones o una clave de réplica, vaya a la página de detalles para la clave y elija la pestaña Regionality (Regionalidad).

  La pestaña Regionality (Regionalidad) de una clave principal incluye los botones Change primary Region (Cambiar región principal) y Create new replica keys (Crear nuevas claves de réplica). (La pestaña Regionality (Regionalidad) de una clave de réplica no tiene ningún botón). La sección Related multi-Region keys (Claves de varias regiones relacionadas) enumera todas las claves de varias regiones relacionadas con la actual. Si la clave actual es una clave de réplica, esta lista incluye la clave principal.

  Si elige una clave de varias regiones relacionada de la tabla Related multi-Region keys (Claves de varias regiones relacionadas), la tabla de la consola AWS KMS cambia a la región de la clave seleccionada y abre la página de detalles de la clave. Por ejemplo, si elige la clave de réplica en

la región `sa-east-1` de la sección de ejemplo Related multi-Region keys (Claves multde varias regiones relacionadas) que aparece a continuación, la consola AWS KMS cambia a la región `sa-east-1` para mostrar la página de detalles de esa clave de réplica. Puede hacer esto para ver el alias o la política de clave de la clave de réplica. Para cambiar la región nuevamente, utilice el selector de regiones en la esquina superior derecha de la página.



Visualización de claves de varias regiones en la API

Para ver las claves de varias regiones en la AWS KMS API, usa la DescribeKeyoperación. Muestra la clave especificada y todas sus claves de varias regiones relacionadas.

Al igual que la consola AWS KMS, las operaciones de la API de AWS KMS son regionales. Por ejemplo, cuando llamas a las ListAliasesoperaciones ListKeyso, solo devuelven los recursos de la región actual o especificada. Pero cuando se llama a la operación `DescribeKey` en una clave de varias regiones, la respuesta incluye todas las claves de varias regiones relacionadas en otras Regiones de AWS.

Por ejemplo, la siguiente expresión solicitud de `DescribeKey` obtiene detalles acerca de una clave de réplica de varias regiones en la región de Asia Pacífico (Tokio) (`ap-northeast-1`).

```
$ aws kms describe-key \
        --key-id arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \
        --region ap-northeast-1
```

La mayor parte de la `KeyMetadata` de la respuesta describe la clave de réplica en la región de Asia Pacífico (Tokio) que es el tema de la solicitud. Sin embargo, el elemento `MultiRegionConfiguration` describe la clave principal en la región EE. UU. Oeste (Oregón) (us-west-2) y sus claves de réplica en otras Regiones de AWS, incluida la réplica en la región Asia Pacífico (Tokio). `DescribeKey` devuelve el mismo valor `MultiRegionConfiguration` para todas las claves de varias regiones relacionadas.

```
{
    "KeyMetadata": {
        "MultiRegion": true,
        "AWSAccountId": "111122223333",
        "Arn": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "CreationDate": 1586329200.918,
        "Description": "",
        "Enabled": true,
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "KeyManager": "CUSTOMER",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-west-2"
            },
            "ReplicaKeys": [
                {
                    "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "eu-west-1"
                },
                {
                    "Arn": "arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "ap-northeast-1"
                },
```

```
                {
                    "Arn": "arn:aws:kms:sa-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "sa-east-1"
                }
            ]
        }
    }
}
```

Administración de claves de varias regiones

Para la mayoría de las acciones, administra las claves de varias regiones de la misma manera que usa y administra las claves de una sola región. Puede habilitar y desactivar las claves, establecer y actualizar alias, políticas de clave, concesiones y etiquetas. Sin embargo, la administración de claves de varias regiones difiere en las siguientes formas.

- Puede.actualizar la región principal. Esto cambia una de las claves de réplica a una clave principal y la clave principal actual a una réplica.
- Usted administra la rotación automática de claves solo en la clave principal.
- Puede obtener la clave pública para una clave de varias regiones asimétrica de cualquiera de las claves principales o de réplica relacionadas.

La propiedad de varias regiones que usted establece cuando crea una clave KMS es inmutable. No se puede convertir una clave de región única en clave de varias regiones ni convertir una clave de varias regiones en una clave de región única.

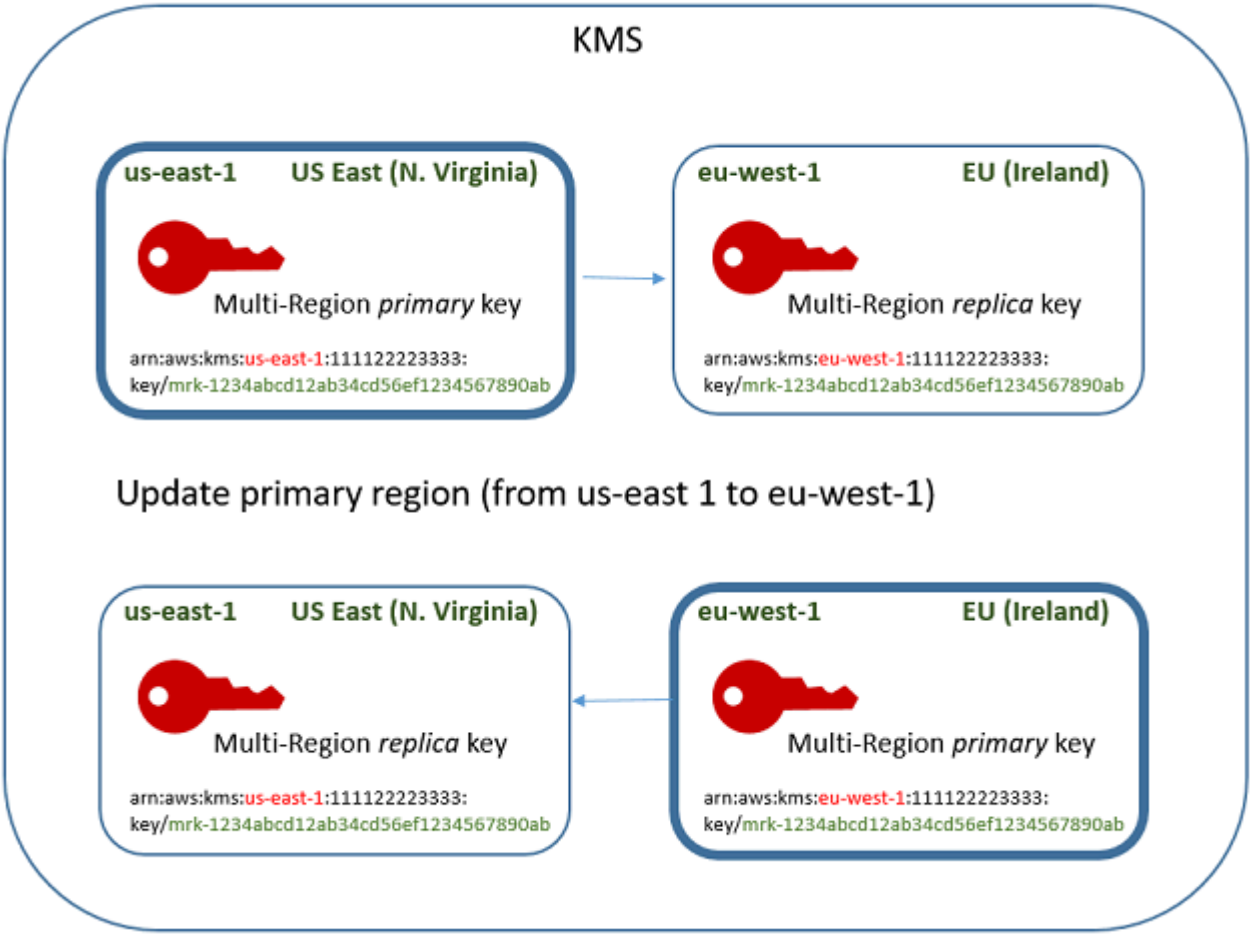
Actualización de la región principal

Cada conjunto de claves de varias regiones relacionadas debe contar con una clave principal. Pero puede cambiar la clave principal. Esta acción, conocida como actualización de la región principal, convierte la clave principal actual en una clave de réplica y convierte una de las claves de réplica relacionadas en la clave principal. Puede hacerlo si necesita eliminar la clave principal actual mientras mantiene las claves de réplica, o para ubicar la clave principal en la misma región que los administradores de claves.

Puede seleccionar cualquier clave de réplica relacionada para que sea la nueva clave principal. Tanto la clave principal como la clave de réplica deben estar en el estado clave `Enabled` Cuando se inicia la operación.

Incluso después de completar esta operación, es posible que el proceso de actualización de la región principal siga en curso durante unos segundos más. Durante este tiempo, las claves principales antiguas y nuevas tienen un estado de clave transitoria de Updating (Actualizando). Mientras que el estado de clave es `Updating`, puede usar las claves en operaciones criptográficas, pero no puede replicar la nueva clave principal ni realizar determinadas operaciones de administración, como habilitar o desactivar estas claves. Operaciones como la DescribeKeypueden mostrar las claves principales antiguas y nuevas como réplicas. El estado de clave `Enabled` se restaura cuando se haya completado la actualización.

Suponga que tiene una clave principal en EE. UU. Este (Norte de Virginia) (us-east-1) y una réplica de claves en Europa (Irlanda) (eu-west-1). Puede utilizar la función de actualización para cambiar la clave principal en EE. UU. Este (Norte de Virginia) (us-east-1) a una clave de réplica y cambiar la clave de réplica en Europa (Irlanda) (eu-west-1) a la clave principal.



Cuando se completa el proceso de actualización, la clave de varias regiones en la región Europa (Irlanda) (eu-west-1) es una clave principal de varias regiones y la clave en la región EE. UU. Este (Norte de Virginia) (us-east-1) es su clave de réplica. Si hay otras claves de réplica relacionadas,

se convierten en réplicas de la nueva clave principal. La próxima vez que AWS KMS sincronice las propiedades compartidas de las claves multirregionales, obtendrá las propiedades compartidas de la nueva clave principal y las copiará en sus claves de réplica, incluida la clave principal anterior.

La operación de actualización no modifica el ARN de clave de ninguna clave de varias regiones. Tampoco afecta a las propiedades compartidas, como el material clave, ni a las propiedades independientes, como la política de claves. Sin embargo, es posible que desee actualice la política de claves de la nueva clave principal. Por ejemplo, es posible que desee añadir el ReplicateKey permiso kms: para entidades de confianza a la nueva clave principal y eliminarlo de la nueva clave de réplica.

El estado clave de **`Updating`**

El proceso de actualización de una región principal tarda un poco más que el breve retraso de coherencia que puede producirse en la mayoría de AWS KMS las operaciones. Es posible que el proceso aún esté en curso después de que la operación `UpdatePrimaryRegion` regrese o que usted haya completado el procedimiento de actualización en la consola. Operaciones como esta DescribeKeypueden mostrar las claves principales antiguas y nuevas como réplicas hasta que se complete el proceso.

Durante el proceso de actualización de la Región principal, la clave principal antigua y la nueva clave primaria se encuentran en el estado de clave `Updating`. Cuando el proceso de actualización se completa correctamente, ambas claves vuelven al estado de clave `Enabled`. Mientras está en el estado `Updating`, ciertas operaciones de administración, como habilitar y desactivar las claves, no están disponibles. Sin embargo, puede continuar usando ambas claves en operaciones de cifrado sin interrupción. Para obtener información acerca del efecto del estado de clave `Updating`, consulte Estados clave de AWS KMS las claves.

Actualización de una región principal (consola)

Puede actualizar la clave principal en la AWS KMS consola. Comience con la página de detalles de clave de la clave principal actual.

1. Inicia sesión en la consola AWS Key Management Service (AWS KMS) AWS Management Console y ábrela en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.

4. Seleccione el alias o el ID de clave de la clave principal de varias regiones. Esto abre la página de detalles de clave de la clave principal.

   Para identificar una clave principal de varias regiones, utilice el icono de herramienta situado en la esquina superior derecha para agregar la columna Regionality (Regionalidad) de la tabla.
5. Elija la pestaña Regionality (Regionalidad).
6. En la sección Primary key (Clave principal), seleccione Change primary Region (Cambiar de región principal).
7. Elija la región de la nueva clave principal. Solo puede elegir una región del menú.

   El menú Change primary Regions (Cambiar las regiones principales) incluye solo Regiones que tienen una clave de varias regiones relacionada. Es posible que no tenga permiso para actualizar la región principal en todas las regiones del menú.
8. Seleccione Change primary Region (Cambiar región principal).

Actualización de una región principal (API)AWS KMS

Para cambiar la clave principal de un conjunto de claves multirregionales relacionadas, utilice la UpdatePrimaryRegionoperación.

Use el parámetro `KeyId` para identificar la clave principal actual. Utilice el `PrimaryRegion` parámetro para indicar Región de AWS la nueva clave principal. Si la clave principal aún no tiene una réplica en la nueva región principal, se produce un error en la operación.

En el ejemplo siguiente se cambia la clave principal de la clave de varias regiones en la región `us-west-2` a su réplica en la región `eu-west-1`. El parámetro `KeyId` identifica la clave principal actual en la región `us-west-2`. El `PrimaryRegion` parámetro especifica Región de AWS la nueva clave principal,`eu-west-1`.

```
$ aws kms update-primary-region \
      --key-id arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \
      --primary-region eu-west-1
```

Cuando se realiza correctamente, esta operación no devuelve ningún resultado; solo el código de estado HTTP. Para ver el efecto, ejecute la DescribeKeyoperación en cualquiera de las claves multirregionales. Es posible que desee esperar hasta que el estado de la clave vuelva a `Enabled`.

Mientras que el estado de clave es Updating (Actualizando), los valores de la clave aún pueden estar en flujo.

Por ejemplo, la siguiente llamada `DescribeKey` obtiene los detalles acerca de la clave de varias regiones en la región `eu-west-1`. La salida muestra que la clave de varias regiones de la región `eu-west-1` es ahora la clave principal. La clave de varias regiones relacionada (mismo ID de clave) en la región `us-west-2` es ahora una clave de réplica.

```
$ aws kms describe-key \
      --key-id arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \

{
    "KeyMetadata": {
        "AWSAccountId": "111122223333",
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "CreationDate": 1609193147.831,
        "Enabled": true,
        "Description": "multi-region-key",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "Enabled",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS",
        "KeyManager": "CUSTOMER",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegion": true,
        "MultiRegionConfiguration": {
           "MultiRegionKeyType": "PRIMARY",
           "PrimaryKey": {
              "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
              "Region": "eu-west-1"
           },
           "ReplicaKeys": [
              {
                 "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                 "Region": "us-west-2"
```

```
                }
            ]
        }
    }
}
```

Rotación de las claves de varias regiones

Puede activar y desactivar la rotación automática y realizar la rotación bajo demanda del material clave en claves multirregionales. La rotación de claves es una propiedad compartida de las claves multirregionales.

Solo habilita y deshabilita la rotación automática de claves en la clave principal. La rotación bajo demanda solo se inicia en la clave principal.

- Al AWS KMS sincronizar las claves multirregionales, copia el valor de la propiedad de rotación de claves de la clave principal a todas las claves de réplica relacionadas.
- Al AWS KMS girar el material clave, crea un nuevo material clave para la clave principal y, a continuación, lo copia más allá de los límites de la región en todas las réplicas de claves relacionadas. El material clave nunca se queda AWS KMS sin cifrar. Este paso se controla cuidadosamente para garantizar que el material clave esté completamente sincronizado antes de utilizar cualquier clave en una operación criptográfica.
- AWS KMS no cifra ningún dato con el nuevo material clave hasta que dicho material clave esté disponible en la clave principal y en cada una de sus réplicas.
- Cuando se replica una clave principal que se ha rotado, la nueva clave de réplica tiene el material de clave actual y todas las versiones anteriores del material clave para sus claves de varias regiones relacionadas.

Este patrón garantiza que las claves de varias regiones relacionadas sean totalmente interoperables. Cualquier clave de varias regiones puede descifrar cualquier texto cifrado mediante una clave de varias regiones relacionada, incluso si el texto cifrado se cifró antes de que se creara la clave.

La rotación automática de claves no es compatible con las claves KMS asimétricas o las claves KMS con el material de claves importado. Para obtener información sobre la rotación de claves automática y bajo demanda, consulteRotativo AWS KMS keys.

Descargar claves públicas

Al crear una clave KMS asimétrica multirregión, AWS KMS crea un par de claves RSA o de curva elíptica (ECC) para la clave principal. Luego copia ese par de claves en cada réplica de la clave principal. Como resultado, puede descargar la clave pública desde la clave principal o cualquiera de sus claves de réplica. Siempre obtendrá el mismo material clave.

Para obtener información sobre la descarga y el uso de claves públicas fuera de, consulte. AWS KMSConsideraciones especiales para descargar claves públicas Para obtener instrucciones, consulte Descargar claves públicas.

Importación de material clave en claves de varias regiones

Puede importar su propio material de claves en una clave de KMS de varias regiones. Las claves de varias regiones que cree con su propio material clave son interoperables. Puede cifrar datos en una región y descifrarlos en cualquier otra región con una clave de varias regiones relacionada.

Sin embargo, debe administrar el material clave.

- AWS KMS no copia ni sincroniza el material claves de una clave principal con el material de clave importado en sus claves de réplica. Debe importar el mismo material de claves en claves principales y de réplica relacionadas.
- El modelo de caducidad y las fechas de vencimiento de cada clave se establecen de forma independiente al importar el material clave. Puede configurar el mismo modelo o un modelo de vencimiento y fechas de vencimiento diferentes para las claves de varias regiones relacionadas. Si el material clave se acerca a su fecha de caducidad, debe volver a importar el material clave en la clave de varias regiones afectada.

  Los estados de claves relacionadas con varias regiones son independientes entre sí. Por ejemplo, si el material de claves de la clave principal vence, sus claves de réplica no se verán afectadas.

Los mismos Requisitos de región para claves de réplica se aplican a claves de varias regiones con material de claves importado. Si importa el mismo material clave en claves de una sola región o claves de varias regiones no relacionadas, estas claves KMS son no interoperable.

Puede crear claves de varias regiones con material importado de claves simétricas, asimétricas o HMAC. AWS KMS no admite material de claves importado en almacenes de claves personalizados. Además, no puede habilitar la rotación automática de claves de ninguna clave KMS con material de claves importado.

Aparte de sus características de varias regiones, las claves de varias regiones con material clave importado son las mismas que otras claves KMS con material clave importado. Para obtener información detallada sobre cómo crear y configurar claves de una región con material de claves importado, consulte Acerca de material de claves importado.

Temas

- ¿Por qué no son interoperables todas las claves KMS con material de claves importado?
- Crear una clave principal con material de claves importado
- Creación de una clave de réplica con material de claves importado

¿Por qué no son interoperables todas las claves KMS con material de claves importado?

Las claves KMS de una sola región con material clave importado no son interoperables, incluso cuando tienen el mismo material clave. Cuando AWS KMS utiliza una clave KMS para cifrar datos, enlaza criptográficamente algunos de los metadatos clave al texto cifrado. Esto asegura el texto cifrado para que solo la clave KMS que los datos cifrados puedan descifrar esos datos.

Las claves de varias regiones están diseñadas para ser interoperables. Además de tener el mismo material clave, tienen el mismo ID de clave y otros metadatos. Por lo tanto, los textos cifrados que generan pueden ser descifrados por cualquier clave de varias regiones relacionada. Como resultado, las propiedades de confianza de las claves de varias regiones son diferentes de las de las claves de una sola región. Pero para algunos clientes, el beneficio de descifrar en varias regiones supera el valor de seguridad de un texto cifrado que depende de una sola clave KMS en una sola Región de AWS.

Crear una clave principal con material de claves importado

Para crear una clave principal con material importado de claves, comience con la creación de una clave de KMS sin material de claves. Al crear la clave principal sin material clave, debe indicar la especificación de la clave que refleje el tipo de material de claves que planea importar. A continuación, importará el material de claves a la clave principal.

El procedimiento para crear una clave principal de varias regiones sin material clave es casi el mismo que el procedimiento para crear una clave de una sola región sin material clave. La única diferencia es que debe especificar que la clave es una clave de varias regiones.

Los permisos para crear una clave principal multirregional con material clave importado son los mismos que los necesarios para crear una clave principal multirregional con material AWS KMS clave, incluidos los CreateServiceLinkedRole permisos kms: CreateKey e iam: de una política de IAM. Puede usar las claves KeyOrigin condicionales kms: MultiRegionKeyType y kms: para conceder o denegar el permiso para crear claves principales multirregionales con material clave importado.

Al crear una clave principal con material clave importado en la consola de AWS KMS, utilice la configuración de la sección Opciones avanzadas. No puede cambiar estas propiedades después de que se cree la clave de KMS.

- Defina el origen del material clave como Externo (Importar material clave).
- Establezca Multi-Region replication (Replicación de varias regiones) en Allow this key to be replicated into other Regions (Permitir que esta clave se replique en otras regiones).

Cuando utilice la CreateKeyoperación para crear una clave principal con material clave importado, utilice los `MultiRegion` parámetros `Origin` y, a continuación, especifique los parámetros `KeySpec` y. `KeyUsage` En el siguiente ejemplo, se crea una clave de KMS `EXTERNAL` que puede importar material de claves `ECC_NIST_P384`.

```
$ aws kms create-key --origin EXTERNAL --key-spec ECC_NIST_P384 --key-usage SIGN_VERIFY
 --multi-region
```

El resultado es una clave principal de varias regiones sin material clave y un estado clave de `PendingImport`.

Para habilitar esta clave KMS, debe descargar una clave pública y un token de importación, utilizar la clave pública para cifrar el material de claves y, a continuación, importar el material de claves. Para obtener instrucciones, consulte Importación de material clave para AWS KMS llaves.

Creación de una clave de réplica con material de claves importado

Puede crear una clave de réplica de varias regiones en la consola AWS KMS o mediante las operaciones de la API de AWS KMS. Para replicar una clave principal de varias regiones con material de claves importado, utilice el mismo procedimiento que utiliza paracrear una clave de réplica con material de claves de AWS KMS. Sin embargo, el resultado es diferente. En lugar de devolver una clave de réplica con el mismo material de clave que la clave principal, el proceso de replicación devuelve una clave de réplica sin material de claves y un estado de clave de

`PendingImport`. Para habilitar la clave de réplica, debe importar el mismo material de claves en la clave de réplica que importó a su clave principal.

Aunque no replica el material de claves, AWS KMS crea la clave de réplica con el mismo ID de clave, especificación de claves, uso de claves y origen del material de claves como clave principal. También garantiza que el material clave importado en la clave de réplica sea idéntico al material de claves importado en la clave principal.

Para crear una clave de réplica con material de claves importado:

1. Creación de una clave principal de varias regiones con material de claves importado.
2. Aplique alguna de las siguientes acciones.

   En la consola AWS KMS, elija una clave principal de varias regiones con material de claves importado. Luego, en su pestaña Regionality (Regionalidad), elija Create new replica keys (Crear nuevas claves de réplica). Para obtener instrucciones, consulte Creación de claves de réplica (consola).

   O utilice la ReplicateKeyoperación. Para el parámetro `KeyId`, introduzca el ID de clave o ARN de clave de una clave principal de varias regiones con material de claves importado. Para obtener instrucciones, consulte Crear una clave de réplica (API de AWS KMS).
3. Para cada nueva clave de réplica, siga los pasos para descargar una clave pública y un token de importación. Utilice la clave pública para cifrar el material de claves de la clave principal y, a continuación, importe el material de claves de la clave principal en la clave de réplica. Necesita una clave pública diferente y un token de importación para cada clave de réplica.

   Si el material de claves que intenta importar a la clave de réplica no es el mismo que su clave principal, se produce un error en la operación. AWS KMS no requiere que el modelo de caducidad y las fechas de caducidad estén coordinadas, pero es posible que establezca reglas de negocio para las claves de varias regiones. Para obtener instrucciones, consulte Importación de material clave para AWS KMS llaves.

Permisos para replicar claves con materiales clave importados

Para crear una clave de réplica con material de claves importado, debe tener los siguientes permisos.

En la región de claves principal:

- kms: ReplicateKey en la clave principal (en la región de la clave principal). Incluya este permiso en la política de clave de la clave principal o en una política de IAM.

En la región clave de réplica:

- kms: CreateKey en una política de IAM.
- kms: GetParametersForImport. Puede incluir este permiso en la política de clave de la clave de réplica o en una política de IAM.
- kilómetros: ImportKeyMaterial. Puede incluir este permiso en la política de clave de la clave de réplica o en una política de IAM.
- kms: TagResource se requiere para asignar etiquetas al replicar. Incluya este permiso en una política de IAM en la región de réplica.
- kms: CreateAlias es necesario para replicar una clave en la AWS KMS consola. Para obtener más información, consulte Control del acceso a alias.

Eliminación de claves de varias regiones

Si ya no utiliza una clave principal o una clave de réplica de varias regiones, puede programar su eliminación.

Aunque la eliminación de claves KMS siempre debe hacerse con precaución, eliminar una réplica de una clave de varias regiones es menos arriesgada, siempre que la clave principal siga existiendo en AWS KMS. Si elimina una clave de réplica de su Región, pero descubre el texto cifrado que se cifró bajo la clave eliminada, puede descifrar ese texto cifrado con cualquier clave de varias regiones relacionada. También puede volver a crear la clave de réplica replicando la clave principal de nuevo en la región de clave de réplica.

Sin embargo, eliminar una clave principal y toda su clave de réplica es una operación muy peligrosa, equivalente a eliminar una clave de región única.

> **Warning**
>
> La eliminación de una clave KMS es un proceso destructivo y potencialmente peligroso. Solo debe hacerlo si está seguro de que ya no necesitará la clave KMS y no tendrá que usarla en el futuro. Si no está seguro, debe desactivar la clave KMS en lugar de eliminarla.

Para eliminar una clave principal, primero debe eliminar todas sus claves de réplica. Si debe eliminar una clave principal de una región concreta sin eliminar sus claves de réplica, cambie la clave principal por una clave de réplica mediante actualización de la región principal.

Antes de programar la eliminación de cualquier clave de KMS, revise las precauciones del Eliminación de AWS KMS keys tema y los temas que explican cómo determinar el uso anterior de una clave de KMS y cómo configurar una CloudWatch alarma que le avise del uso de la clave de KMS durante el período de espera. Antes de eliminar la clave principal de una clave de varias regiones asimétrica, revise el tema Eliminar claves asimétricas.

Temas

- Permisos para eliminar claves de varias regiones
- Cómo eliminar una clave de réplica
- Cómo eliminar una clave principal

Permisos para eliminar claves de varias regiones

Para programar la eliminación de una clave de varias regiones, solo necesita el permiso siguiente.

- kms: ScheduleKeyDeletion — para programar la eliminación de la clave multirregional y establecer su período de espera.

También recomendamos encarecidamente que tenga los siguientes permisos relacionados.

- kms: CancelKeyDeletion — para cancelar la eliminación programada de la clave multirregional.
- kms: DescribeKey — para ver el estado de la clave multirregional y la lista de claves multirregionales relacionadas.
- kms: DisableKey — para darte la opción de deshabilitar una clave multirregional en lugar de eliminarla.
- kms: EnableKey — para restaurar la funcionalidad de una clave multirregional tras cancelar su eliminación.

También puede incluir permisos para replicar la clave principal y cambiar la clave principal.

- kms: ReplicateKey
- km: UpdateReplicaRegion

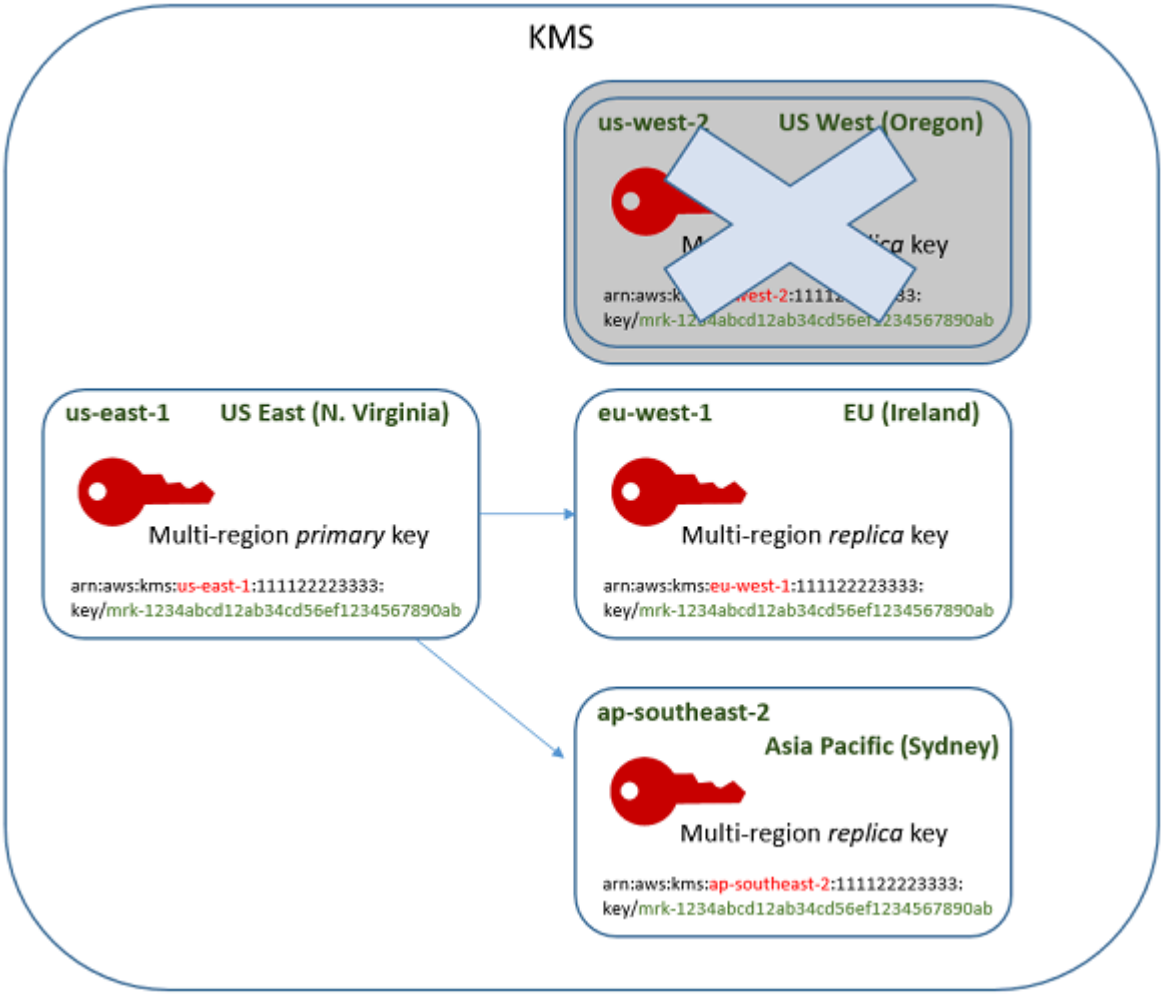
Puede incluir estos permisos en una política de IAM, pero es recomendable colocarlos en una política clave en la que solo se aplican a la clave KMS que necesita administrar.

Cómo eliminar una clave de réplica

Puede utilizar la consola de AWS KMS o la API de AWS KMS para eliminar un conjunto de reglas de réplica. Puede eliminar una clave réplica en cualquier momento. No depende del estado de la clave de ninguna otra clave KMS.

Si elimina por error una clave de réplica, puede volver a crearla replicando la misma clave primaria en la misma región. La nueva clave de réplica que cree tendrá las mismas propiedades compartidas que la clave de réplica original.

El procedimiento para eliminar una clave de réplica de varias regiones es el mismo que eliminar una clave de región única.



1. Programe la eliminación de la clave de réplica. Seleccione un período de espera de 7 a 30 días. El periodo de espera predeterminado es de 30 días.
2. Durante el periodo de espera, el estado clave de la clave de réplica cambia a `Pending deletion` (`PendingDeletion`) y no puede usarlo en operaciones criptográficas.
3. Puede cancelar la eliminación programada de la clave de réplica en cualquier momento del período de espera. El estado de la clave cambia a `Disabled`, pero puede volver a habilitar la clave KMS.
4. Cuando finaliza el periodo de espera, AWS KMS elimina la clave de réplica.

Puede ver un registro de sus acciones en su registro de AWS CloudTrail. AWS KMS registra las operaciones que programan la eliminación de la clave KMS y la acción que borra la clave KMS.

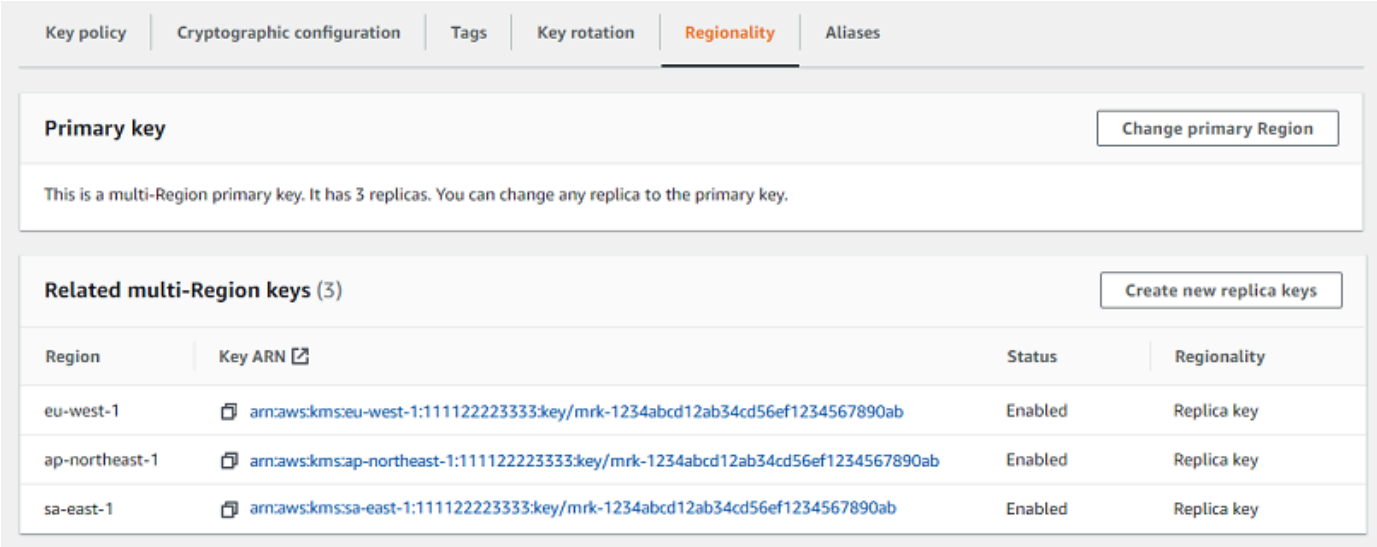
Eliminación de una clave de réplica (consola)

Para programar la eliminación de una clave de réplica de varias regiones, utilice el mismo procedimiento que se utiliza para programar la eliminación de una clave de una sola región.

Debido a que las claves de réplica relacionadas están en diferentes Regiones de AWS, no puede programar la eliminación de más de una clave de réplica a la vez. Para eliminar todas las claves de réplica relacionadas, utilice un patrón similar al siguiente.

Para programar la eliminación de todas las claves de réplica relacionadas

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. En el panel de navegación, elija Claves administradas por el cliente.
3. Utilice el selector de regiones en la esquina superior derecha para elegir la región de la clave principal de varias regiones.
4. Elija el alias o el ID de clave de la clave principal.
5. Elija la pestaña Regionality (Regionalidad).



6. En la sección Claves de varias regiones relacionadas, elija la clave ARN de una clave de réplica.

   Esta acción abre la página de detalles de clave de la clave de réplica en una nueva pestaña del navegador. La consola se establece en la clave de réplica Región.

7. En el menú Key actions (Acciones de claves), elija Schedule key deletion (Programar la eliminación de claves).

   Esta acción inicia el proceso de programación de eliminación de la clave. Complete el proceso de eliminación de claves de programación. Para obtener más detalles, consulte Programación y cancelación de eliminación de claves (consola).

8. Volver a la pestaña del navegador que muestra la pestaña de Regionality (Regionalidad) de la clave principal. (Es posible que tenga que actualizar la página para ver el estado actualizado de las claves de réplica). Elija la clave ARN de otra clave de réplica y repita el proceso de programación de eliminación de la clave de réplica.

Eliminar una clave de réplica (API de AWS KMS)

Para programar la eliminación de una clave de réplica multirregional, utilice la ScheduleKeyDeletionoperación. Para especificar la clave KMS, utilice su ID clave o ARN de clave. Al trabajar con claves de varias regiones, puede reducir la incidencia de errores utilizando la clave ARN con su valor de región explícito.

Por ejemplo, este comando elimina una clave de réplica de la región us-west-2 (EE. UU. Oeste (Oregón)). Dado que el comando no especifica un período de espera, el período de espera se establece en el valor predeterminado de 30 días.

```
$ aws kms schedule-key-deletion \
    --region us-west-2 \
    --key-id arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

Cuando el comando se ejecuta correctamente, devuelve ARN (`KeyId`), el período de espera (`PendingWindowInDays`), la fecha de eliminación (`DeletionDate`), y el estado actual de la clave (`KeyState`), que se espera `PendingDeletion`.

Al eliminar una clave de réplica de varias regiones, asegúrese de verificar que los valores de ID de clave y Región en el ARN clave son los que espera.

```
{
    "KeyId": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "DeletionDate": 1599523200.0,
    "KeyState": "PendingDeletion",
    "PendingWindowInDays": 30
}
```

Para eliminar todas las réplicas de una clave principal de varias regiones mediante programación, cree una lista de las Regiones que contienen claves de réplica. A continuación, para cada región de la lista, llame a la operación `ScheduleKeyDeletion`, como se muestra arriba.

A diferencia de una clave de región única que se elimina permanentemente, puede restaurar una clave de réplica al replicar la clave principal en la región donde se encontraba la clave de réplica eliminada.

Para comprobar el estado de la clave de réplica y ver la clave principal y las claves de réplica de una clave multirregional, utilice la DescribeKeyoperación.

Cómo eliminar una clave principal

Puede programar la eliminación de una clave principal de varias regiones en cualquier momento. Sin embargo, AWS KMS no eliminará una clave principal de varias regiones que tenga claves de réplica, incluso si están programadas para su eliminación.

Para eliminar una clave principal, debe programar la eliminación de todas sus claves de réplica y esperar a que se eliminen las claves de réplica. El período de espera necesario para eliminar una

clave principal comienza cuando se elimina la última de sus claves de réplica. Si debe eliminar una clave principal de una región concreta sin eliminar sus claves de réplica, cambie la clave principal por una clave de réplica mediante actualización de la región principal.

Si una clave principal no tiene claves de réplica, el proceso es idéntico a eliminar una clave de réplica o eliminar cualquier clave KMS regional.

Aunque una clave principal está programada para eliminación, no puede utilizarla en operaciones criptográficas y no puede replicarla. Sin embargo, a menos que también estén programadas para su eliminación, sus claves de réplica no se verán afectadas.

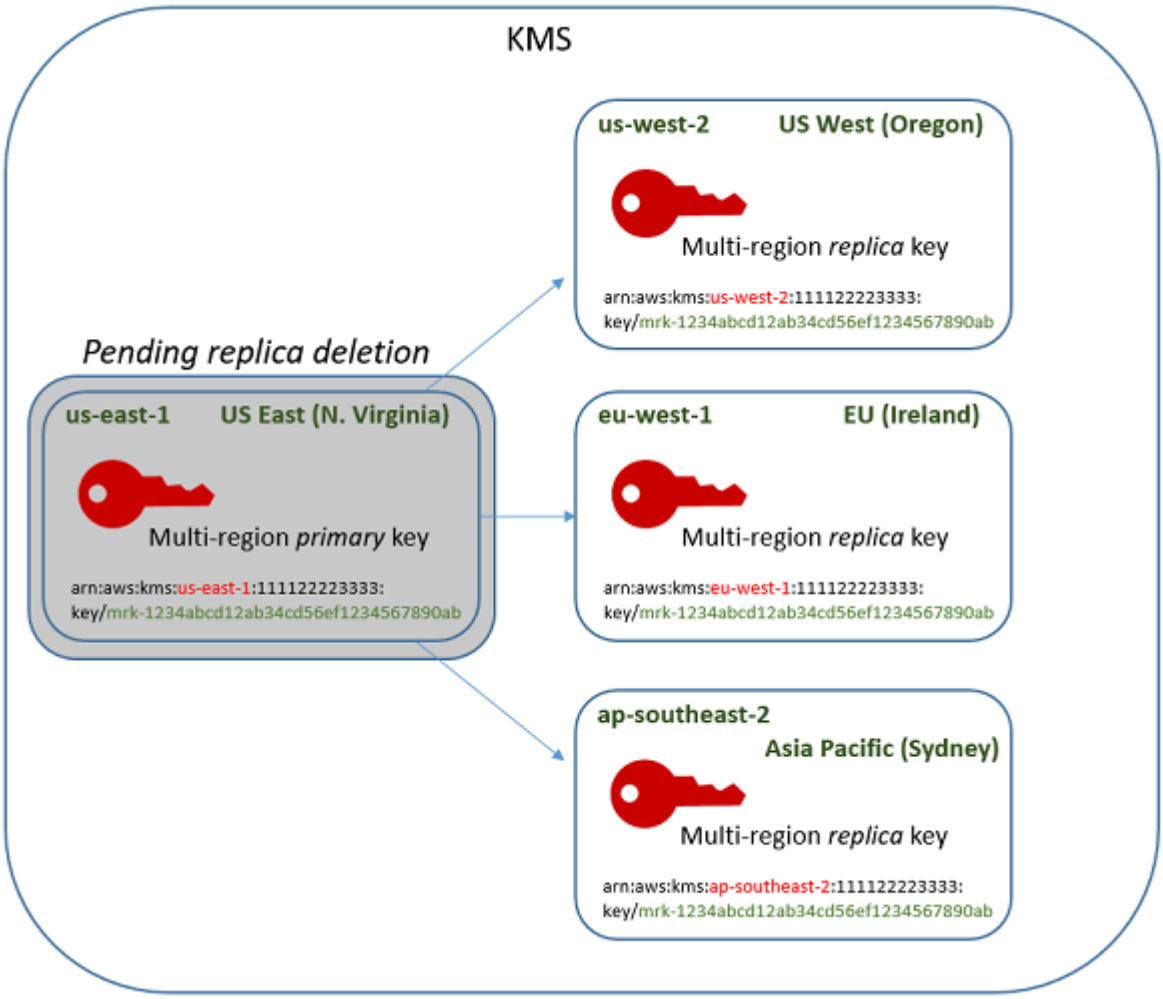
Puede utilizar la consola AWS KMS o la API de AWS KMS para programar la eliminación de claves primarias y de réplica. Puede programar la eliminación de la clave principal antes, después o al mismo tiempo que programe la eliminación de las claves de réplica. El proceso podría tener un aspecto similar al siguiente.

1. Programe la eliminación de la clave principal. Seleccione un período de espera de 7 a 30 días. El periodo de espera predeterminado es de 30 días. Sin embargo, el período de espera para la clave principal no comienza hasta que se eliminen todas las claves de réplica.

   Si aún existe alguna clave de réplica, el estado clave de la clave principal cambia a `Pending replica deletion` (`PendingReplicaDeletion`). De lo contrario, cambia a `Pending deletion` (`PendingDeletion`). En cualquier caso, no puede usar la clave principal en operaciones criptográficas y no puede replicarla.

   La programación de la eliminación de una clave principal no afecta a las claves de réplica. Su estado de clave permanece habilitado y puede utilizarlos en operaciones criptográficas. Si no se eliminan las claves de réplica, el estado de `Pending replica deletion` de la clave principal puede persistir indefinidamente.

```
KMS key:                    Key state:
Primary (us-east-1)           Pending replica deletion (waiting period 30 days -- not
 started)
Replica (us-west-2)           Enabled
Replica (eu-west-1)           Enabled
Replica (ap-southeast-2)      Enabled
```



2. Programe la eliminación de cada clave de réplica. Seleccione un período de espera de 7 a 30 días. El periodo de espera predeterminado es de 30 días. Puede eliminar varias claves de réplica al mismo tiempo. Sus períodos de espera se ejecutan al mismo tiempo. Durante el periodo de espera, el estado clave de las claves de réplica cambia a `Pending deletion` (`PendingDeletion`) y no puede usar estas claves KMS en operaciones criptográficas.

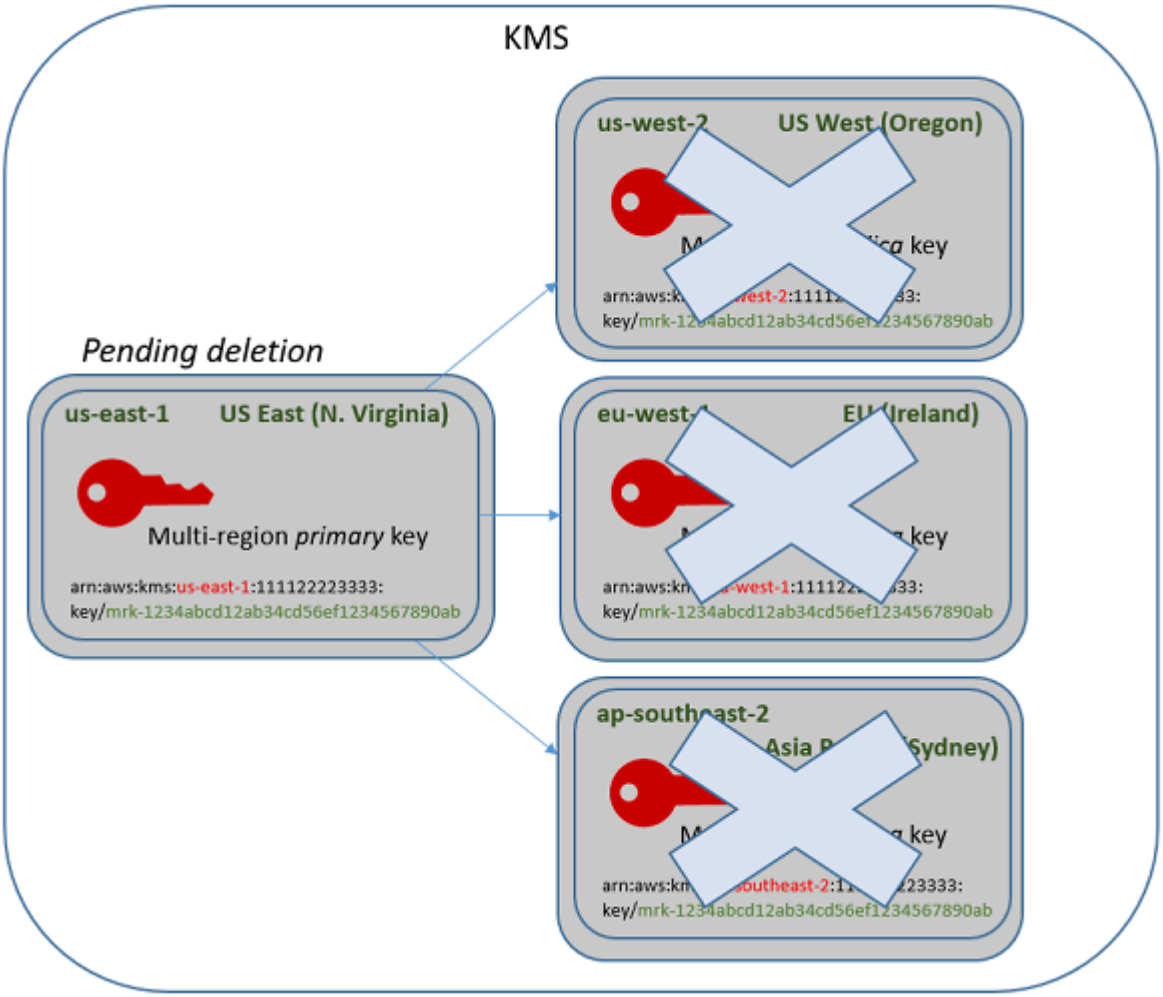
   Por ejemplo, si tiene tres claves de réplica, puede programar la eliminación de las tres al mismo tiempo. Pueden tener los mismos o diferentes períodos de espera. Observe que el período de espera en la clave principal aún no ha comenzado. Su estado clave es `PendingReplicaDeletion` porque tiene claves de réplica existentes.

```
KMS key:                    Key state:
Primary key (us-east-1)       Pending replica deletion (waiting period 30 days -- not
 started)
Replica (us-west-2)           Pending deletion (7 days)
```

```
Replica (eu-west-1)           Pending deletion (7 days)
Replica (ap-southeast-2)      Pending deletion (30 days)
```

3. Puede cancelar la eliminación programada de la clave principal o de cualquier clave de réplica hasta que se elimine. El estado de la clave cambia a `Disabled`, pero puede volver a habilitar la clave KMS.
4. Cuando caduque el período de espera de la última clave de réplica, AWS KMS elimina la última clave de réplica. El estado clave de la clave principal cambia de `Pending replica deletion` (`PendingReplicaDeletion`) a `Pending deletion` (`PendingDeletion`) y comienza el período de espera de 7 a 30 días para la clave principal.

```
KMS key:                    Key state:
Primary key (us-east-1)       Pending deletion (waiting period 30 days)
```



5. Cuando expire su período de espera, AWS KMS borra la clave principal.

El tiempo mínimo para eliminar una clave principal con réplicas es de 14 días.

Si programa la eliminación de claves de la clave principal y todas las claves de réplica con un período de espera de 7 días, las claves de réplica se eliminarán después de 7 días. La clave principal se elimina el día 14.

- Día 1: programe la eliminación de las claves principal y de réplica con el período de espera mínimo de 7 días. Se inician los períodos de espera de eliminación de 7 días para las claves de réplica. El período de espera de eliminación de la clave principal aún no se inicia.
- Día 7: finalizan los períodos de espera de eliminación de las claves de réplica. AWS KMS elimina todas las claves de réplica. Cuando se elimina la última clave de réplica, se inicia el período de espera de eliminación de 7 días para la clave principal.
- Día 14: finaliza el período de espera de eliminación de la clave principal. AWS KMS borra la clave principal.

Puede ver un registro de sus acciones en su registro AWS CloudTrail. AWS KMS registra las operaciones que programan eliminación de cada clave KMS y la acción que borra la clave KMS.

Eliminación de una clave principal (consola)

Para eliminar una clave principal de varias regiones, utilice el siguiente procedimiento.

Para programar la eliminación de claves

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Seleccione la casilla de verificación situada junto a la clave que desea eliminar. También puede seleccionar una o más claves KMS, incluidas las réplicas de esta clave principal.
5. Elija Key actions (Acciones de claves), Schedule key deletion (Programar la eliminación de claves).
6. Lea y tenga en cuenta la advertencia y la información sobre la cancelación de la eliminación durante el período de espera. Si decide cancelar la eliminación, elija Cancel (Cancelar).
7. En Waiting period (in days) [Período de espera (en días)], indique un número de días entre 7 y 30. Si ha seleccionado varias claves KMS, el período de espera que elija se aplicará a todas

las claves KMS seleccionadas. El período de espera para las claves de réplica se ejecuta simultáneamente, pero el período de espera para la clave principal no comienza hasta que AWS KMS elimina la última de las claves de réplica.

8. Seleccione la casilla de verificación situada junto a Confirm you want to schedule this key for deletion in ***<number of days>*** days (Confirme que quiere programar esta clave durante <número de días> días).
9. Elija Schedule deletion.

Para comprobar el estado de eliminación de las claves KMS, en la página de detalles para la clave principal, consulte la sección General configuration (Configuración general). El estado de la clave aparece en el campo Status (Estado). Cuando el estado de clave de la clave principal cambia a `Pending deletion`, aparece la Fecha de eliminación programada.

También puede comprobar el estado de clave (Estado) de todas las claves principales y de réplica en la pestaña Regionality (Regionalidad) de la página de detalles de cualquier clave de varias regiones. Para obtener más detalles, consulte Visualización de claves de varias regiones.

Eliminar una clave principal (API de AWS KMS)

Para eliminar una clave de réplica multirregional, utilice la ScheduleKeyDeletionoperación. Para especificar la clave KMS, utilice su ID clave o ARN de clave. Al trabajar con claves de varias regiones, puede reducir la incidencia de errores utilizando la clave ARN con su valor de región explícito.

Por ejemplo, este comando elimina una clave principal de la región us-east-1 (EE. UU. Este (Norte de Virginia)). Dado que el comando no especifica un período de espera, el período de espera se establece en el valor predeterminado de 30 días.

```
$ aws kms schedule-key-deletion \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

Cuando el comando se ejecuta correctamente, devuelve ARN de clave, el estado de clave resultante y el periodo de espera (`PendingWindowInDays`).

Si la clave principal no tiene réplicas, el estado de la clave principal es `PendingDeletion` y la salida incluye el campo `DeletionDate`. Si persiste alguna clave de réplica, el estado de la clave principal es `PendingReplicaDeletion` y `DeletionDate` se omite porque es incierto. Incluso

si las claves de réplica también están programadas para su eliminación, es posible que cancele la eliminación programada.

Al eliminar una clave principal de varias regiones, asegúrese de verificar que los valores de ID de clave y Región en el ARN clave son los que espera.

```
{
    "KeyId": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "KeyState": "PendingReplicaDeletion",
    "PendingWindowInDays": 30
}
```

Para comprobar el estado de eliminación de las claves de KMS, utilice la DescribeKeyoperación con la clave principal o con las claves de réplica restantes. El reloj de período de espera para la clave principal no se inicia hasta que se elimina la última réplica y el estado de la clave cambia a`PendingDeletion`.

Para calcular la fecha de eliminación esperada de la clave principal, recorra los ARN de clave de réplica en la respuesta, ejecute `DescribeKey` en cada una de ellas, obtenga el último valor `DeletionDate` y, a continuación, agregue el valor `PendingDeletionWindowInDays` para la clave principal. Los períodos de espera para las claves de réplica se ejecutan simultáneamente.

En el siguiente ejemplo, la clave KMS es una clave principal de varias regiones con claves de réplica existentes. Debido a que el estado de clave es `PendingReplicaDeletion`, la respuesta incluye el período de espera (`PendingWindowInDays`), pero no el `DeletionDate`. La fecha de eliminación real de la clave principal depende de cuándo se eliminan las claves de réplica.

```
$ aws kms describe-key \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab

{
    "KeyMetadata": {
        "AWSAccountId": "111122223333",
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
        "CreationDate": 1597902361.481,
        "Enabled": false,
        "Description": "",
```

```
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "PendingReplicaDeletion",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "Origin": "AWS_KMS",
        "KeyManager": "CUSTOMER",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegion": true,
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-east-1"
            },
            "ReplicaKeys": [
                {
                    "Arn": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "us-west-2"
                },
{
                    "Arn": "arn:aws:kms:eu-west-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "eu-west-1"
                },
                {
                    "Arn": "arn:aws:kms:ap-southeast-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                    "Region": "ap-southeast-2"
                }
            ]
        },
        "PendingDeletionWindowInDays": 30
    }
}
```

Cuando se eliminan todas las réplicas, el resultado de `DescribeKey` muestra la clave principal restante con un estado de clave de `PendingDeletion`. Mientras que el estado de clave es `PendingDeletion`, el campo `DeletionDate` aparece en lugar del campo `PendingWindowInDays`.

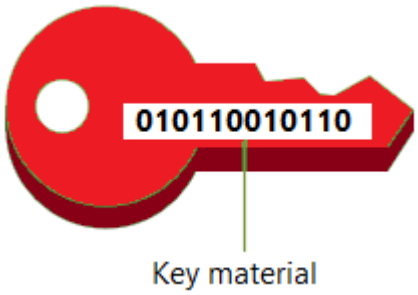
```
$ aws kms describe-key \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab

{
    "KeyMetadata": {
        "AWSAccountId": "111122223333",
        "KeyId": "mrk-1234abcd12ab34cd56ef1234567890ab",
        "Arn": "",
        "CreationDate": 1597902361.481,
        "Enabled": false,
        "Description": "",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "KeyState": "PendingDeletion",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "DeletionDate": 1597968000.0,
        "Origin": "AWS_KMS",
        "KeyManager": "CUSTOMER",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ],
        "MultiRegion": true,
        "MultiRegionConfiguration": {
            "MultiRegionKeyType": "PRIMARY",
            "PrimaryKey": {
                "Arn": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
                "Region": "us-east-1"
            },
            "ReplicaKeys": []
        }
    }
}
```

Importación de material clave para AWS KMS llaves

Puede crear una AWS KMS keys (clave de KMS) con el material de claves que usted suministra.

Una clave KMS es una representación lógica de una clave de cifrado. Los metadatos de una clave KMS incluyen el ID del material de claves que se utiliza para cifrar y descifrar datos. Al crear una clave KMS, AWS KMS genera de forma predeterminada el material de claves de dicha clave KMS.

Pero puede crear una clave KMS sin material de claves y, a continuación, importar su propio material de claves en esa clave KMS, una característica que se conoce a menudo como "bring your own key" (BYOK) ("utilice su propia clave").



> **Note**
>
> AWS KMS no admite el descifrado de ningún AWS KMS texto cifrado ajeno a AWS KMS, incluso si el texto cifrado se ha cifrado con una clave KMS con material clave importado. AWS KMS no publica el formato de texto cifrado que requiere esta tarea y el formato puede cambiar sin previo aviso.

El material de claves importado se admite en todos los tipos de claves de KMS, excepto en las claves de KMS de los almacenes de claves personalizados.

Cuando utiliza material clave importado, sigue siendo responsable del material clave y permite AWS KMS utilizar una copia del mismo. Puede hacerlo por uno o varios de los motivos siguientes:

- Para demostrar que ha generado el material de claves con un origen de entropía que cumple sus requisitos.
- Para utilizar el material clave de su propia infraestructura con AWS los servicios y AWS KMS para gestionar el ciclo de vida de ese material clave interno AWS.
- Para utilizar claves existentes y bien establecidas, como las claves para la firma de código AWS KMS, la firma de certificados de PKI y las aplicaciones con certificados anclados
- Para establecer una fecha de caducidad para el material clave AWS y eliminarlo manualmente, pero también para que vuelva a estar disponible en el futuro. Por el contrario, programar la eliminación de claves requiere un periodo de espera de 7 a 30 días, transcurrido el cual no puede recuperar la clave KMS eliminada.

- Ser propietario de la copia original del material clave y mantenerla fuera de ella AWS para garantizar una mayor durabilidad y recuperación ante desastres durante todo el ciclo de vida del material clave.
- En el caso de las claves asimétricas y las claves HMAC, la importación crea claves compatibles e interoperables que funcionan dentro y fuera de ellas. AWS

Puede auditar y supervisar el uso y la administración de una clave KMS con material clave importado. AWS KMS registra un evento en el AWS CloudTrail registro al crear la clave KMS, descargar la clave pública empaquetadora y el token de importación e importar el material de la clave. AWS KMS también registra un evento cuando se elimina manualmente el material clave importado o cuando se AWS KMS elimina el material clave caducado.

Para obtener información sobre las diferencias importantes entre las claves de KMS con material clave importado y aquellas con material clave generado por AWS KMS, consulteAcerca de material de claves importado.

Claves de KMS compatibles

AWS KMS admite material clave importado para los siguientes tipos de claves de KMS. No puede importar material de claves a una clave de KMS de almacenes de claves personalizados.

- Claves de KMS de cifrado simétrico
- Claves de KMS RSA asimétricas (para cifrado o firma, pero no para ambas opciones)
- Claves de KMS de curva elíptica asimétrica (ECC) (solo para firma)
- Claves KMS SM2 asimétricas: solo para regiones de China (para cifrar o firmar, pero no para ambos)
- Claves KMS HMAC
- Claves de varias regiones de todos los tipos compatibles.

Regiones

El material clave importado es compatible con todos los soportes Regiones de AWS . AWS KMS

En las regiones de China, los requisitos de material clave para las claves KMS de cifrado simétrico difieren de los de otras regiones. Para obtener más detalles, consulte Paso 3 de la importación de material de claves: Cifrar el material de claves.

Temas

Planificación de la importación del material de claves

El material clave importado te permite proteger tus AWS recursos con las claves criptográficas que generes. El material de claves que importa está asociado a una clave de KMS concreta. Puede volver a importar el mismo material clave a la misma clave de KMS, pero no puede importar material de clave diferente a la clave de KMS y no puede convertir una clave de KMS diseñada para el material de clave importado en una clave de KMS con material AWS KMS clave.

Más información:

- the section called “Selección de una especificación de clave pública de encapsulamiento”
- the section called “Seleccionar un algoritmo de encapsulamiento”

Temas

Acerca de material de claves importado

Antes de decidir importar material clave a AWS KMS, debe conocer las siguientes características del material clave importado.

Generar el material de clave

> Es su responsabilidad generar el material de claves con una fuente de aleatoriedad que cumpla sus requisitos de seguridad.

Puede eliminar el material de clave

Puede eliminar el material de claves importado de una clave de KMS, al inutilizar inmediatamente la clave de KMS. Además, al importar material de claves en una clave de KMS, puede determinar si la clave vence y establecer su fecha de vencimiento. Cuando llegue el momento de caducidad, AWS KMS elimina el material clave. Sin material de claves, la clave KMS no puede utilizarse en ninguna operación criptográfica. Para restaurar la clave, debe volver a importar el mismo material en la clave.

No puede cambiar el material de claves

Al importar el material de claves en una clave de KMS, la clave de KMS se asocia de forma permanente a dicho material de claves. Puede volver a importar el mismo material de claves, pero no puede importar material de claves diferente en esa clave KMS. Además, no puede habilitar la rotación automática de claves para una clave KMS con material de claves importado. Sin embargo, puede rotar manualmente una clave KMS con material de claves importado.

No puede cambiar el origen del material de claves

Las claves KMS diseñadas para el material de claves importado tienen un valor de origen de `EXTERNAL` que no se puede cambiar. No puede convertir una clave KMS para material clave importado para utilizar material clave de ninguna otra fuente, ni siquiera. AWS KMS Del mismo modo, no puede convertir una clave KMS con material AWS KMS clave en una diseñada para material clave importado.

No puede exportar el material de claves

No puede exportar ningún material clave que haya importado. AWS KMS no puede devolverle el material clave importado de ninguna forma. Debe conservar una copia del material clave importado fuera de AWS, preferiblemente, en un administrador de claves, como un módulo de seguridad de hardware (HSM), de modo que pueda volver a importar el material clave si lo elimina o si caduca.

Puede crear claves de varias regiones con material de claves importado

Las múltiples regiones con material de claves importado tienen las características de las claves de KMS con material de claves importado y pueden interoperar entre Regiones de AWS. Para crear una clave de varias regiones con material de claves importado, debe importar el mismo material de claves en la clave de KMS principal y en cada clave de réplica. Para obtener más detalles, consulte Importación de material clave en claves de varias regiones.

Las claves asimétricas y las claves HMAC son portátiles e interoperables

Puede utilizar el material de clave asimétrico y el material de clave HMAC de forma externa AWS para interoperar con AWS KMS llaves con el mismo material de clave importado.

A diferencia del texto cifrado AWS KMS simétrico, que está inextricablemente vinculado a la clave KMS utilizada en el algoritmo, AWS KMS utiliza formatos HMAC estándar y asimétricos para el cifrado, la firma y la generación de MAC. Como resultado, las claves son portátiles y admiten los escenarios tradicionales de claves de depósito de garantía.

Si su clave KMS tiene material clave importado, puede usar el material clave importado fuera de él para realizar las siguientes operaciones. AWS

- Claves HMAC: puede verificar una etiqueta HMAC generada por la clave HMAC de KMS con material de claves importado. También puede usar la clave HMAC KMS con el material clave importado para verificar una etiqueta HMAC que se haya generado fuera del material clave. AWS
- Claves de cifrado asimétricas: puede utilizar su clave de cifrado asimétrica privada AWS para descifrar un texto cifrado mediante la clave KMS con la clave pública correspondiente. También puedes usar tu clave KMS asimétrica para descifrar un texto cifrado asimétrico que se haya generado fuera de. AWS
- Claves de firma asimétrica: puedes usar tu clave KMS de firma asimétrica con material clave importado para verificar las firmas digitales generadas por tu clave de firma privada fuera de. AWS También puedes usar tu clave de firma pública asimétrica fuera de ella AWS para verificar las firmas generadas por tu clave KMS asimétrica.

Si importa el mismo material de claves en claves de KMS diferentes de la misma Región de AWS, esas claves son también interoperables. Para crear claves KMS interoperables en diferentes regiones Regiones de AWS, cree una clave multirregional con material clave importado.

Las claves de cifrado simétricas no son portátiles ni interoperables

Los textos cifrados simétricos que se AWS KMS producen no son portátiles ni interoperables. AWS KMS no publica el formato de texto cifrado simétrico que requiere la portabilidad y el formato puede cambiar sin previo aviso.

- AWS KMS no puede descifrar los textos cifrados simétricos que no estén cifrados AWS, incluso si utiliza material clave que ha importado.
- AWS KMS no admite el descifrado de ningún texto cifrado AWS KMS simétrico que no sea AWS KMS, incluso si el texto cifrado se ha cifrado con una clave KMS con material clave importado.

- Las claves de KMS con el mismo material de claves importado no son interoperables. El texto cifrado simétrico que AWS KMS genera el texto cifrado específico de cada clave KMS. Este formato de texto cifrado garantiza que solo la clave de KMS que cifró los datos pueda descifrarlos.

  Además, no puede utilizar ninguna AWS herramienta, como el cifrado del lado del cliente AWS Encryption SDKo Amazon S3, para descifrar AWS KMS textos cifrados simétricos.

  Por lo tanto, no puede utilizar claves con material clave importado para respaldar acuerdos de custodia de claves, en los que un tercero autorizado con acceso condicional al material clave puede descifrar determinados textos cifrados fuera de él. AWS KMS Para admitir el depósito de claves, utilice AWS Encryption SDK para cifrar su mensaje bajo una clave que es independiente de AWS KMS.

Usted es responsable de la disponibilidad y durabilidad

AWS KMS está diseñado para mantener una alta disponibilidad del material clave importado. Sin embargo, AWS KMS no mantiene la durabilidad del material clave importado al mismo nivel que el material clave que se AWS KMS genera. Para obtener más detalles, consulte Protección del material de claves importado.

Protección del material de claves importado

El material de claves que importa está protegido en tránsito y en reposo. Antes de importar el material clave, cifra (o «envuelve») el material clave con la clave pública de un par de claves RSA generado en módulos de seguridad de AWS KMS hardware (HSM) validados según el programa de validación de módulos criptográficos FIPS 140-2. Puede cifrar el material de claves directamente con la clave pública que envuelve o cifrar el material de claves con una clave simétrica AES y, a continuación, cifrar la clave simétrica AES con la clave pública RSA.

Al recibirlo, AWS KMS descifra el material de claves con la clave privada correspondiente en un AWS KMS HSM y lo vuelve a cifrar con una clave simétrica AES que solo existe en la memoria volátil del HSM. El material de claves nunca sale del HSM en texto sin formato. Solo se descifra mientras está en uso y solo dentro de los HSM. AWS KMS

El uso de la clave de KMS con el material de claves importado viene determinado únicamente por las políticas de control de acceso que se establezcan en la clave de KMS. Además, puede usar alias y etiquetas para identificar y controlar el acceso a la clave de KMS. Puede habilitar y deshabilitar la clave, ver y editar sus propiedades y supervisarla mediante servicios como AWS CloudTrail.

Sin embargo, usted conserva la única copia de seguridad de su material de claves. A cambio de esta medida de control adicional, usted es responsable de la durabilidad y la disponibilidad general del material clave importado. AWS KMS está diseñado para mantener una alta disponibilidad del material clave importado. Sin embargo, AWS KMS no mantiene la durabilidad del material clave importado al mismo nivel que el material clave que se AWS KMS genera.

Esta diferencia relativa a la durabilidad es importante en los casos siguientes:

- Al establecer una fecha de caducidad para el material clave importado, AWS KMS elimina el material clave una vez que caduque. AWS KMS no elimina la clave KMS ni sus metadatos. Puedes crear una CloudWatch alarma de Amazon que te notifique cuando el material clave importado se acerca a su fecha de caducidad.

  No puede eliminar el material clave que se AWS KMS genera para una clave de KMS ni puede configurar el material AWS KMS clave para que caduque, aunque puede rotarlo.
- Al eliminar manualmente el material clave importado, AWS KMS elimina el material clave pero no elimina la clave KMS ni sus metadatos. Por el contrario, programar la eliminación de claves requiere un periodo de espera de 7 a 30 días, después de lo cual AWS KMS elimina permanentemente la clave KMS, sus metadatos y su material de claves.
- En el improbable caso de que se produzcan algunos fallos en toda la región AWS KMS (por ejemplo, una pérdida total de energía), AWS KMS no podrá restaurar automáticamente el material clave importado. Sin embargo, AWS KMS puede restaurar la clave KMS y sus metadatos.

Debe conservar una copia del material clave importado fuera del AWS sistema que controle. Se recomienda almacenar una copia exportable del material de claves importado en un sistema de administración de claves, como un HSM. Si el material de claves importado se elimina o vence, la clave de KMS asociada quedará inutilizable hasta que vuelva a importar el mismo material de claves. Si el material de claves importado se pierde de forma permanente, cualquier texto cifrado con la clave de KMS será irrecuperable.

Permisos para importar material de clave

Para crear y administrar claves KMS con material de claves importado, el usuario necesita permiso para las operaciones de este proceso. Puede proporcionar los permisos `kms:GetParametersForImport`, `kms:ImportKeyMaterial`, y `kms:DeleteImportedKeyMaterial` en la política de claves al crear la clave KMS. En la AWS KMS consola, estos permisos se añaden automáticamente a los administradores de claves al crear una clave con un origen de material clave externo.

Para crear claves KMS con material de claves importado, la entidad principal necesita los siguientes permisos.

- kms: CreateKey (política de IAM)
  - Para limitar este permiso a las claves de KMS con material clave importado, utilice la condición kms: KeyOrigin policy con un valor de`EXTERNAL`.

```
{
  "Sid": "CreateKMSKeysWithoutKeyMaterial",
  "Effect": "Allow",
  "Resource": "*",
  "Action": "kms:CreateKey",
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "EXTERNAL"
    }
  }
}
```

- kms: GetParametersForImport (política clave o política de IAM)
  - Para limitar este permiso a las solicitudes que utilizan un algoritmo de empaquetado y una especificación clave de empaquetado determinados, usa las condiciones de la WrappingKeySpec política kms: WrappingAlgorithm y kms:.
- kms: ImportKeyMaterial (política clave o política de IAM)
  - Para permitir o prohibir que el material clave caduque y controlar la fecha de caducidad, utilice las condiciones de la ValidTo política kms: ExpirationModel y kms:.

Para volver a importar el material clave importado, el director necesita los ImportKeyMaterial permisos kms: GetParametersForImport y kms:.

Para eliminar el material clave importado, el director necesita el DeleteImportedKeyMaterial permiso kms:.

Por ejemplo, para dar permiso `KMSAdminRole` al ejemplo y que pueda administrar todos los aspectos de una clave KMS con material de claves importado, incluya una declaración de política clave como la siguiente en la política clave de la clave KMS.

```
{
  "Sid": "Manage KMS keys with imported key material",
```

```
  "Effect": "Allow",
  "Resource": "*",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/KMSAdminRole"
  },
  "Action": [
    "kms:GetParametersForImport",
    "kms:ImportKeyMaterial",
    "kms:DeleteImportedKeyMaterial"
  ]
}
```

Requisitos para el material de claves importado

El material de claves que importa debe ser compatible con la especificación de clave de la clave de KMS asociada. Para los pares de claves asimétricas, importe solo la clave privada del par. AWS KMS deriva la clave pública de la clave privada.

AWS KMS admite las siguientes especificaciones clave para las claves de KMS con material de claves importado.

Especificación de clave de la clave de KMS	Requisitos del material de claves
Claves de cifrado simétricas SYMMETRIC_DEFAULT	256 bits (32 bytes) de datos binarios En las regiones de China, debe ser un dato binario de 128 bits (16 bytes).
Claves HMAC HMAC_224 HMAC_256 HMAC_384 HMAC_512	El material de claves HMAC debe cumplir con la RFC 2104. La longitud de la clave debe coincidir con la longitud especificada en la especificación de la clave.
Clave privada asimétrica RSA RSA_2048	La clave privada asimétrica RSA que importe debe formar parte de un par de claves que cumpla con la RFC 3447.

Especificación de clave de la clave de KMS	Requisitos del material de claves
RSA_3072 RSA_4096	Módulo: 2048 bits, 3072 bits o 4096 bits Número de números primos: 2 (no se admiten claves RSA de varios números primos) El material de clave asimétrica debe estar codificado en BER o DER en el formato de los estándares de criptografía de clave pública (PKCS) #8 que cumpla con la RFC 5208.
Clave privada asimétrica de curva elíptica ECC_NIST_P256 (secp256r1) ECC_NIST_P384 (secp384r1) ECC_NIST_P521 (secp521r1) ECC_SECG_P256K1 (secp256k1)	La clave privada asimétrica ECC que importe debe formar parte de un par de claves que cumpla con la RFC 5915. Curva: NIST P-256, NIST P-384, NIST P-521 o Secp256k1 Parámetros: solo curvas con nombre (se rechazan las claves ECC con parámetros explícitos) Coordenadas de puntos públicos: pueden estar comprimidas, descomprimidas o ser proyectivas El material de clave asimétrica debe estar codificado en BER o DER en el formato #8 de los estándares de criptografía de clave pública (PKCS) que cumple con la RFC 5208.

Especificación de clave de la clave de KMS	Requisitos del material de claves
Clave privada asimétrica SM2 (solo para las regiones de China)	La clave privada asimétrica SM2 que importe debe formar parte de un par de claves que cumpla con la norma GM/T 0003. Curva: SM2 Parámetros: solo curva con nombre (se rechazan las claves SM2 con parámetros explícitos) Coordenadas de puntos públicos: pueden estar comprimidas, descomprimidas o ser proyectivas El material de clave asimétrica debe estar codificado en BER o DER en el formato #8 de los estándares de criptografía de clave pública (PKCS) que cumple con la RFC 5208.

Administración de material de claves importado

En estos temas se explica cómo importar y volver a importar material de claves a una clave de KMS y cómo crear material de claves importado que venza automáticamente.

Temas

- Descripción de la importación de material de claves
- Nueva importación del material de claves
- Identificación de claves de KMS con material de claves importado
- Crear una CloudWatch alarma por la caducidad del material clave importado
- Eliminar el material de claves importado
- Eliminación de una clave de KMS con material de claves importado

Descripción de la importación de material de claves

En la siguiente información general se explica cómo importar el material de claves en AWS KMS. Para obtener más información sobre cada paso del proceso, consulte el tema correspondiente.

1. Cree una clave de KMS sin material de claves: el origen debe ser `EXTERNAL`. Un origen de clave de `EXTERNAL` indica que la clave está diseñada para material clave importado y evita AWS KMS que se genere material clave para la clave KMS. En un paso posterior importará su propio material de claves en esta clave KMS.

   El material clave que importe debe ser compatible con la especificación clave de la clave asociada AWS KMS . Para obtener más información sobre la compatibilidad, consulte the section called “Requisitos para el material de claves importado”.

2. Descargar la clave pública de encapsulamiento y el token de importación: después de completar el paso 1, descargue una clave pública de encapsulamiento y un token de importación. Estos elementos protegen el material clave mientras se importa a. AWS KMS

   En este paso, elige el tipo (“especificación de clave”) de la clave de encapsulamiento RSA y el algoritmo de encapsulamiento que utilizará para cifrar los datos en tránsito en AWS KMS. Puede elegir una especificación de clave de encapsulamiento y un algoritmo de clave de encapsulamiento diferentes cada vez que importe o vuelva a importar el mismo material de claves.

3. Cifrar el material de claves: utilice la clave pública de encapsulamiento que ha descargado en el paso 2 para cifrar el material de claves que ha creado en su propio sistema.

4. Importar el material de claves: cargue el material de claves cifrado que ha creado en el paso 3 y el token de importación que ha descargado en el paso 2.

   En esta etapa, puede establecer una fecha de vencimiento opcional. Cuando el material clave importado caduca, lo AWS KMS elimina y la clave KMS queda inutilizable. Para seguir usando la clave de KMS, debe volver a importar el mismo material de claves.

   Cuando la operación de importación se completa de manera correcta, el estado de la clave KMS cambia de `PendingImport` a `Enabled`. Ahora puede usar la clave KMS en operaciones criptográficas.

AWS KMS registra una entrada en el AWS CloudTrail registro al crear la clave KMS, descargar la clave pública empaquetadora y el token de importación e importar el material clave. AWS KMS

también registra una entrada cuando se elimina el material clave importado o cuando se AWS KMS elimina el material clave caducado.

Nueva importación del material de claves

Si administra una clave KMS con material de clave importado, es posible que tenga que reimportar el material de clave. Puede volver a importar el material de claves para reemplazar el material de claves vencido o eliminado o para cambiar el modelo de vencimiento o la fecha de vencimiento del material de claves.

Al importar el material de claves en una clave de KMS, la clave de KMS se asocia de forma permanente a dicho material de claves. Puede volver a importar el mismo material de claves, pero no puede importar material de claves diferente en esa clave KMS. No puede rotar el material de claves y AWS KMS no puede crear material de claves para una clave de KMS con material de claves importado.

Puede volver a importar material de claves en cualquier momento y en cualquier horario que cumpla con sus requisitos de seguridad. No tiene que esperar hasta que el material de claves esté en su fecha de vencimiento o cerca de ella.

Para volver a importar material de claves nuevo o existente, utilice el mismo procedimiento que utilizó para importar el material de claves la primera vez, con las siguientes excepciones.

- Utilice una clave KMS existente en lugar de crear una nueva clave KMS. Puede omitir el paso 1 del procedimiento de importación.
- Al volver a importar el material de clave, puede cambiar el modelo de vencimiento y la fecha de vencimiento.

Cada vez que se importa material de claves en una clave KMS, es necesario descargar y utilizar una nueva clave de encapsulamiento y un nuevo token de importación para la clave KMS. El procedimiento de encapsulamiento no afecta al contenido del material de claves, por lo que puede utilizar distintas claves públicas de encapsulamiento y diferentes algoritmos de encapsulamiento para importar el mismo material de claves.

Identificación de claves de KMS con material de claves importado

Cuando se crea una clave KMS sin material de claves, el valor de la propiedad `Origin` de la clave KMS es `EXTERNAL` y no se puede modificar. A diferencia del estado de claves, el valor `Origin` no depende de la presencia o ausencia del material de claves.

Puede utilizar el valor de origen `EXTERNAL` para identificar claves KMS diseñadas para material de claves importado. Puede encontrar el origen de la clave en la AWS KMS consola o mediante la DescribeKeyoperación. También puede ver las propiedades del material de claves, por ejemplo, si vence y cuándo mediante la consola o las API.

Para identificar claves KMS con material de claves importado (consola)

1. Abra la AWS KMS consola en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. Utilice una de las siguientes técnicas para ver la propiedad `Origin` de las claves KMS.
   - Para agregar una columna Origin (Origen) a la tabla de clave KMS, elija el icono Settings (Configuración) de la esquina superior derecha. Elija Origin (Origen) y Confirm (Confirmar). La columna Origen facilita la identificación de las claves de KMS que tienen un valor de propiedad de origen Externo (Importar material de claves).
   - Para buscar el valor de la propiedad `Origin` de una clave KMS determinada, elija el ID o alias de la clave KMS. A continuación, elija la pestaña Cryptographic configuration (Configuración criptográfica). Las pestañas están debajo de la sección General configuration (Configuración general).
4. Para ver información detallada sobre el material de claves, elija la pestaña Key material (Material de claves). Esta pestaña sólo aparece en la página de detalles para claves KMS con material de claves importado.

Para identificar las claves de KMS con material clave importado (API)AWS KMS

Utilice la DescribeKeyoperación. La respuesta incluye la propiedad `Origin` de la clave KMS, el modelo de caducidad y la fecha de caducidad, como se muestra en el siguiente ejemplo.

```
$  aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
{
    "KeyMetadata": {
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Origin": "EXTERNAL",
        "ExpirationModel": "KEY_MATERIAL_EXPIRES"
        "ValidTo": 2023-06-05T12:00:00+00:00,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
        "AWSAccountId": "111122223333",
        "CreationDate": 2018-06-09T00:06:50.831000+00:00,
        "Enabled": false,
        "MultiRegion": false,
        "Description": "",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "PendingImport",
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```


Crear una CloudWatch alarma por la caducidad del material clave importado

Puede crear una CloudWatch alarma que le notifique cuando el material clave importado en una clave de KMS se acerca a su fecha de caducidad. Por ejemplo, la alarma puede avisarle cuando el plazo de caducidad esté a menos de 30 días.

Al importar material de claves en una clave KMS, también puede especificar de manera opcional una fecha y una hora en la que vence el material de claves. Cuando el material clave caduca, lo AWS KMS elimina y la clave KMS queda inutilizable. Para volver a usar la clave KMS, debe volver a importar el material de claves. Sin embargo, si vuelve a importar el material de claves antes de que caduque, puede evitar interrumpir los procesos que utilizan esa clave de KMS.

Esta alarma utiliza la `SecondsUntilKeyMaterialExpires`métrica que se AWS KMS publica en el caso de las claves CloudWatch de KMS cuyo material clave importado caduque. Cada alarma usa esta métrica para supervisar el material de claves importado para una clave de KMS en particular. No puede crear una sola alarma para todas las claves de KMS con material de claves que caduque ni una alarma para las claves de KMS que pueda crear en el futuro.

Requisitos

Se necesitan los siguientes recursos para una CloudWatch alarma que supervise la caducidad del material clave importado.

- Una clave KMS con material de claves importado que caduca. Para obtener ayuda, consulte Identificación de claves de KMS con material de claves importado.

- Un tema de Amazon SNS. Para obtener más información, consulte el tema Creación de un Amazon SNS en la Guía CloudWatch del usuario de Amazon.

Crear la alarma

Siga las instrucciones de Cómo crear una CloudWatch alarma basada en un umbral estático utilizando los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Seleccionar métrica	Elija KMS y, a continuación, seleccione Per-Key Metrics (Métricas por clave). Seleccione la fila con la clave de KMS y la métrica `SecondsUntilKeyMaterialExpires` . A continuación, elija Select metric (Seleccionar métrica). La lista Metrics (Métricas) muestra la métrica `SecondsUntilKeyMaterialExpires` solo para claves KMS con material de claves importado que caduca. Si no tiene claves de KMS con estas propiedades en la cuenta y la región, esta lista está vacía.
Estadística	Mínimo
Período	1 minuto
Tipo de umbral	Estático
Whenever…	Whenever *`metric-name`* is Greater than 1 (Siempre que el nombre de la métrica sea mayor que)

Eliminar el material de claves importado

Puede eliminar el material de claves importado desde una clave de KMS en cualquier momento. Además, cuando el material clave importado con fecha de caducidad caduca, lo AWS KMS elimina. En cualquier caso, cuando se elimina el material de claves, el estado de la clave de KMS cambia a importación pendiente y la clave de KMS no puede utilizarse en ninguna operación criptográfica hasta que vuelva a importar el mismo material de claves. (No puede importar ningún otro material de claves en una clave de KMS).

Además de deshabilitar la clave de KMS y retirar los permisos, la eliminación del material de claves se puede utilizar como estrategia para detener el uso de la clave de KMS de forma rápida, pero temporal. Por el contrario, si se programa la eliminación de una clave de KMS con material de claves importado, también se detiene rápidamente el uso de la clave de KMS. Sin embargo, si la eliminación no se cancela durante el periodo de espera, la clave de KMS, el material de claves y todos los metadatos clave se eliminan de forma permanente. Para obtener más detalles, consulte the section called “Eliminación de una clave de KMS con material de claves importado”.

Para eliminar el material clave, puede utilizar la AWS KMS consola o la operación de la DeleteImportedKeyMaterialAPI. AWS KMS registra una entrada en su AWS CloudTrail registro cuando elimina el material clave importado y cuando AWS KMS elimina el material clave caducado.

Temas

- Cómo afecta AWS a los servicios la eliminación de material clave
- Eliminar el material de claves (console)
- Elimine el material clave (API)AWS KMS

Cómo afecta AWS a los servicios la eliminación de material clave

Cuando se elimina el material de claves, la clave de KMS sin material de claves se vuelve inutilizable de forma inmediata (sujeto a posible coherencia). Sin embargo, los recursos cifrados con claves de datos protegidas por la clave de KMS no se ven afectados hasta que se vuelva a utilizar la clave de KMS, por ejemplo, para descifrar la clave de datos. Este problema afecta a Servicios de AWS muchos de los cuales utilizan claves de datos para proteger sus recursos. Para obtener más detalles, consulte Cómo afectan las claves de KMS obsoletas a las claves de datos.

Eliminar el material de claves (console)

Puede utilizarla AWS Management Console para eliminar material clave.

1. Inicie sesión en la consola AWS Key Management Service (AWS KMS) AWS Management Console y ábrala en https://console.aws.amazon.com/kms.
2. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Realice una de las siguientes acciones siguientes:

- Seleccione la casilla de verificación de una clave KMS con material de claves importado. Elija Key actions, Delete key material.
- Elija el alias o el ID de clave de una clave KMS con material de claves importado. Elija la pestaña Key material (Material de claves) y, a continuación, seleccione Delete key material (Eliminar el material de claves).

5. Confirme que desea eliminar el material de claves y, a continuación, seleccione Delete key material. El estado de la clave KMS, que corresponde a su estado de clave, cambia a Pending import (Importación pendiente).

Elimine el material clave (API)AWS KMS

Para usar la AWS KMS API para eliminar material clave, envía una DeleteImportedKeyMaterialsolicitud. El siguiente ejemplo muestra cómo hacerlo con la AWS CLI.

Sustituya *1234abcd-12ab-34cd-56ef-1234567890ab* por el ID de clave de la clave KMS cuyo material de claves desea eliminar. Puede usar el ID de clave o el ARN de la clave KMS, pero no puede usar un alias para esta operación.

```
$ aws kms delete-imported-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

Eliminación de una clave de KMS con material de claves importado

Eliminar el material de claves de una clave de KMS con material de claves importado es temporal y reversible. Para restaurar la clave, vuelva a importar su material de claves.

Por el contrario, eliminar una clave KMS es irreversible. Si programa la eliminación de claves y vence el período de espera requerido, eliminará de AWS KMS forma permanente e irreversible la clave de KMS, su material clave y todos los metadatos asociados a la clave de KMS.

Sin embargo, el riesgo y las consecuencias de eliminar una clave de KMS con material de claves importado dependen del tipo (“especificación de clave”) de la clave de KMS.

- Claves de cifrado simétrico: si elimina una clave de KMS de cifrado simétrico, no se podrán recuperar los textos cifrados restantes cifrados con esa clave. No puede crear una nueva clave de KMS de cifrado simétrico que pueda descifrar los textos cifrados de una clave de KMS de cifrado simétrico eliminada, incluso si tiene el mismo material de claves. Los metadatos exclusivos de cada clave de KMS están enlazados criptográficamente a cada texto cifrado simétrico. Esta

característica de seguridad garantiza que solo la clave de KMS que cifró el texto cifrado simétrico pueda descifrarlo, pero le impide volver a crear una clave de KMS equivalente.

- Claves asimétricas y HMAC: si dispone del material clave original, puede crear una nueva clave KMS con las mismas propiedades criptográficas que una clave KMS asimétrica o HMAC que se haya eliminado. AWS KMS genera firmas y textos cifrados RSA estándar, firmas ECC y etiquetas HMAC, que no incluyen ninguna característica de seguridad exclusiva. Además, puede utilizar una clave HMAC o la clave privada de un par de claves asimétricas fuera de AWS.

  Una clave de KMS nueva que cree con el mismo material de clave asimétrica o HMAC tendrá un identificador de clave diferente. Tendrá que crear una nueva política de claves, volver a crear los alias y actualizar las políticas y concesiones de IAM existentes para hacer referencia a la nueva clave.

Paso 1 de la importación de material de claves: Crear una AWS KMS keysin material de claves

De forma predeterminada, AWS KMS crea el material de claves automáticamente al crear una clave de KMS. Para importar su propio material de claves, comience con la creación de una clave de KMS sin material de claves. Después, importe el material de claves. Para crear una clave KMS sin material clave, utilice la AWS KMS consola o la CreateKeyoperación.

Para crear una clave sin material de claves, especifique un origen de `EXTERNAL`. La propiedad de origen de una clave de KMS es inmutable. Una vez creada, no podrá convertir una clave de KMS diseñada para material de claves importado en una clave de KMS con material de claves de AWS KMS o cualquier otro origen.

El estado de claves de una clave de KMS con un origen `EXTERNAL` y ningún material de claves es `PendingImport`. Una clave de KMS puede permanecer en estado `PendingImport` indefinidamente. Sin embargo, no puede utilizar una clave de KMS en estado `PendingImport` en operaciones criptográficas. Cuando importa material de claves, el estado de la clave de KMS cambia a `Enabled` y puede usar la clave de KMS en operaciones criptográficas.

AWS KMSregistra un evento en el AWS CloudTrail registro al crear la clave KMS, descargar la clave pública y el token de importación e importar el material clave. AWS KMStambién registra un CloudTrail evento cuando se elimina el material clave importado o cuando se AWS KMS elimina el material clave caducado.

Para obtener información sobre cómo crear claves de varias regiones con material de claves importado, consulte Importación de material clave en claves de varias regiones.

Temas

- Crear una clave KMS sin material de claves (consola)
- Crear una clave KMS sin material de claves (API de AWS KMS)

Crear una clave KMS sin material de claves (consola)

Solo tiene que crear una clave de KMS para el material de claves importado una vez. Puede importar y volver a importar el mismo material de claves en la clave de KMS existente siempre que lo necesite, pero no puede importar material de claves diferente en una clave de KMS. Para obtener más detalles, consulte Paso 2: descargar la clave pública de encapsulamiento y el token de importación.

Para encontrar las claves de KMS existentes con material de claves importado en la tabla de claves gestionadas por el cliente, utilice el icono con forma de engranaje situado en la esquina superior derecha para mostrar la columna Origen de la lista de claves de KMS. Las claves importadas tienen el valor Origen de Externo (Importar material de claves).

Para crear una clave de KMS con material de claves importado, comience por seguir las instrucciones básicas para crear una clave de KMS del tipo de clave que prefiera, con la siguiente excepción.

Después de elegir el uso de la clave, haga lo siguiente:

1. Expanda Advanced options (Opciones avanzadas).
2. En Origen del material de claves, elija Externo (Material de claves importado).
3. Elija la casilla de verificación situada junto a Entiendo las implicaciones de seguridad y durabilidad del uso de una clave importada para indicarnos que entiende las implicaciones de utilizar material de claves importado. Para leer más información acerca de estas implicaciones, consulte Protección del material de claves importado.
4. Vuelva a las instrucciones básicas. Los pasos restantes del procedimiento básico son los mismos para todas las claves de KMS de ese tipo.

Al elegir Finalizar, habrá creado una clave de KMS sin material de claves y con un estado (estado de la clave) de Pendiente de importación.

Sin embargo, en lugar de volver a la tabla de claves administradas por el cliente, la consola muestra una página en la que puede descargar la clave pública y el token de importación que necesita para importar el material de claves. Puede continuar con el paso de descarga ahora o seleccionar Cancelar para detenerse en este momento. Puede volver a este paso de descarga en cualquier momento.

Siguiente: Paso 2: descargar la clave pública de encapsulamiento y el token de importación.

Crear una clave KMS sin material de claves (API de AWS KMS)

Para usar la AWS KMSAPI para crear una clave KMS de cifrado simétrico sin material clave, envía una CreateKeysolicitud con el `Origin` parámetro establecido en. `EXTERNAL` El siguiente ejemplo muestra cómo hacerlo con la AWS Command Line Interface (AWS CLI).

```
$ aws kms create-key --origin EXTERNAL
```

Si el comando se ejecuta correctamente, verá un resultado parecido al siguiente. El `Origin` de la clave de AWS KMS es `EXTERNAL` y su `KeyState` es `PendingImport`.

> **Tip**
>
> Si el comando no se ejecuta correctamente, es posible que aparezca `KMSInvalidStateException` o `NotFoundException`. Puede reintentar la solicitud.

```
{
    "KeyMetadata": {
        "Origin": "EXTERNAL",
        "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "Description": "",
        "Enabled": false,
        "MultiRegion": false,
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "PendingImport",
        "CreationDate": 1568289600.0,
        "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "AWSAccountId": "111122223333",
        "KeyManager": "CUSTOMER",
        "KeySpec": "SYMMETRIC_DEFAULT",
```

```
        "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
        "EncryptionAlgorithms": [
            "SYMMETRIC_DEFAULT"
        ]
    }
}
```

Copie el valor `KeyId` del resultado del comando para usarlo en pasos posteriores y, a continuación, vaya a Paso 2: descargar la clave pública de encapsulamiento y el token de importación.

> **Note**
>
> Este comando crea una clave de KMS de cifrado simétrico con una `KeySpec` de `SYMMETRIC_DEFAULT` y un `KeyUsage` de `ENCRYPT_DECRYPT`. Puede usar los parámetros opcionales `--key-spec` y `--key-usage` crear una clave de KMS asimétrica o HMAC. Para obtener más información, consulte la operación CreateKey.

Paso 2 de la importación de material de claves: descargar la clave pública de encapsulamiento y el token de importación

Después de crear un material AWS KMS key sin clave, descargue una clave pública empaquetadora y un token de importación para esa clave de KMS mediante la AWS KMS consola o la GetParametersForImportAPI. La clave pública de encapsulamiento y el token de importación son un conjunto indivisible que deben usarse juntos.

Utilizará la clave pública de encapsulamiento para cifrar el material de claves para su transferencia. Antes de descargar un par de claves de empaquetado RSA, seleccione la longitud (especificación de clave) del par de claves de empaquetado RSA y el algoritmo de empaquetado que utilizará para cifrar el material clave importado para su transporte en el paso 3. AWS KMS también es compatible con la especificación de claves de empaquetado SM2 (solo para regiones de China).

Cada conjunto de claves públicas de encapsulamiento y token de importación es válido durante 24 horas. Si no los utiliza para importar material de claves en un plazo de 24 horas después de descargarlos, debe descargar un nuevo conjunto. Puede descargar nuevos conjuntos de claves públicas de encapsulamiento y tokens de importación en cualquier momento. Esto le permite cambiar la longitud de la clave de encapsulamiento RSA (“especificación de clave”) o sustituir un conjunto perdido.

También puede descargar un conjunto de claves públicas de encapsulamiento y un conjunto de tokens de importación para volver a importar el mismo material de claves en una clave de KMS. Puede hacerlo para establecer o cambiar el tiempo de vencimiento del material de claves o para restaurar el material de claves vencidas o eliminadas. Debe descargar y volver a cifrar el material clave cada vez que lo importe a. AWS KMS

Uso de la clave pública de encapsulamiento

La descarga incluye una clave pública exclusiva para usted Cuenta de AWS, también denominada clave pública empaquetadora.

Antes de importar el material clave, cifra el material clave con la clave de empaquetado pública y, a AWS KMS continuación, carga el material clave cifrado en. Cuando AWS KMS recibe el material clave cifrado, lo descifra con la clave privada correspondiente y, a continuación, lo vuelve a cifrar con una clave simétrica AES, todo ello dentro de un módulo de seguridad de AWS KMS hardware (HSM).

Uso del token de importación

La descarga incluye un token de importación que contiene metadatos para garantizar que el material de claves se importa correctamente. Al cargar el material de claves cifradas en AWS KMS, debe cargar el mismo token de importación que descargó en este paso.

Selección de una especificación de clave pública de encapsulamiento

Para proteger el material clave durante la importación, debes cifrarlo mediante la clave pública de empaquetado desde AWS KMS la que lo descargaste y un algoritmo de empaquetado compatible. Debe seleccionar una especificación de claves antes de descargar la clave pública de encapsulamiento y el token de importación. Todos los pares de claves de empaquetado se generan en módulos AWS KMS de seguridad de hardware (HSM). La clave privada nunca sale del HSM en texto sin formato.

Especificaciones clave del empaquetado RSA

La especificación de clave de la clave pública de encapsulamiento determina la longitud de las claves del par de claves RSA que protege el material de la clave durante su transferencia a AWS KMS. En general, se recomienda utilizar la clave pública de encapsulamiento más larga que resulte práctica. Ofrecemos varias especificaciones de encapsulamiento de claves públicas para admitir una variedad de HSM y administradores de claves.

AWS KMS admite las siguientes especificaciones clave para las claves de embalaje RSA que se utilizan para importar material clave de todo tipo, excepto cuando se indica lo contrario.

- RSA_4096 (preferido)
- RSA_3072
- RSA_2048

> **Note**
>
> NO se admite la siguiente combinación: material de claves ECC_NIST_P521, la especificación de clave pública de encapsulamiento RSA_2048 y un algoritmo de encapsulamiento RSAES_OAEP_SHA_*.
> No se puede encapsular directamente el material de claves ECC_NIST_P521 con una clave pública de encapsulamiento RSA_2048. Utilice una clave de encapsulamiento más grande o un algoritmo de encapsulamiento RSA_AES_KEY_WRAP_SHA_*.

Especificaciones clave del embalaje SM2 (solo en las regiones de China)

AWS KMS admite las siguientes especificaciones clave para las claves de embalaje SM2 que se utilizan para importar material de clave asimétrico.

- SM2

Seleccionar un algoritmo de encapsulamiento

Para proteger su material de claves durante la importación, deberá cifrarlo con la clave pública de encapsulamiento descargada y un algoritmo de encapsulamiento admitido.

AWS KMS admite varios algoritmos de empaquetado RSA estándar y un algoritmo de empaquetado híbrido de dos pasos. En general, se recomienda utilizar el algoritmo de encapsulamiento más seguro que sea compatible con el material de claves y la especificación de clave de encapsulamiento importados. Normalmente, se elige un algoritmo admitido por el módulo de seguridad de hardware (HSM) o el sistema de administración de claves que protege el material de claves.

En la siguiente tabla se muestran los algoritmos de encapsulamiento compatibles con cada tipo de material de claves y clave de KMS. Los algoritmos se muestran en el orden de preferencia.

Material de claves	Algoritmo y especificaciones de encapsula miento compatibles
Clave de cifrado simétrica Clave AES de 256 bits Clave SM4 de 128 bits (solo en las regiones de China)	Algoritmos de encapsulamiento: RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 Algoritmos de encapsulamiento obsoletos: RSAES_PKCS1_V1 **Note** A partir del 10 de octubre de 2023, AWS KMS no es compatible con el algoritmo de empaquetado RSAES_PKCS1_V1_5. Especificaciones de claves de encapsula miento: RSA_2048 RSA_3072 RSA_4096
Clave privada RSA asimétrica	Algoritmos de encapsulamiento: RSA_AES_KEY_WRAP_SHA_256 RSA_AES_KEY_WRAP_SHA_1 SM2PKE (solo para regiones de China) Especificaciones de claves de encapsula miento: RSA_2048

Material de claves	Algoritmo y especificaciones de encapsula miento compatibles
	RSA_3072 RSA_4096 SM2 (solo en regiones de China)
Clave privada de curva elíptica asimétrica (ECC) No puede utilizar los algoritmos de encapsula miento RSAES_OAEP_SHA_* con la especific ación de clave de encapsulamiento RSA_2048 para encapsular el material de claves ECC_NIST_P521.	Algoritmos de encapsulamiento: RSA_AES_KEY_WRAP_SHA_256 RSA_AES_KEY_WRAP_SHA_1 RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 SM2PKE (solo regiones de China) Especificaciones de claves de encapsula miento: RSA_2048 RSA_3072 RSA_4096 SM2 (solo en regiones de China)

Material de claves	Algoritmo y especificaciones de encapsula miento compatibles
Clave privada SM2 asimétrica (solo para regiones de China)	Algoritmos de encapsulamiento: RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 SM2PKE (solo para regiones de China) Especificaciones de claves de encapsula miento: RSA_2048 RSA_3072 RSA_4096 SM2 (solo en regiones de China)
Clave HMAC	Algoritmos de encapsulamiento: RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 Especificaciones de claves de encapsula miento: RSA_2048 RSA_3072 RSA_4096

> **Note**
>
> Los algoritmos `RSA_AES_KEY_WRAP_SHA_256` y `RSA_AES_KEY_WRAP_SHA_1` empaquetado no son compatibles en las regiones de China.

- `RSA_AES_KEY_WRAP_SHA_256`: un algoritmo de encapsulamiento híbrido de dos pasos que combina el cifrado del material de claves con una clave simétrica AES que el usuario genere con el cifrado posterior de la clave simétrica AES con la clave de encapsulamiento pública RSA descargada y el algoritmo de encapsulamiento RSAES_OAEP_SHA_256.

  Se requiere un algoritmo de `RSA_AES_KEY_WRAP_SHA_*` empaquetado para empaquetar el material de clave privada de RSA, excepto en las regiones de China, donde debe usarse el algoritmo de `SM2PKE` empaquetado.
- `RSA_AES_KEY_WRAP_SHA_1`: un algoritmo de encapsulamiento híbrido de dos pasos que combina el cifrado del material de claves con una clave simétrica AES que el usuario genere con el cifrado posterior de la clave simétrica AES con la clave de encapsulamiento pública RSA descargada y el algoritmo de encapsulamiento RSAES_OAEP_SHA_1.

  Se requiere un algoritmo de `RSA_AES_KEY_WRAP_SHA_*` empaquetado para empaquetar el material de clave privada de RSA, excepto en las regiones de China, donde debe usarse el algoritmo de `SM2PKE` empaquetado.
- `RSAES_OAEP_SHA_256`: algoritmo de cifrado RSA con relleno óptimo de cifrado asimétrico (OAEP) con la función hash SHA-256.
- `RSAES_OAEP_SHA_1`: algoritmo de cifrado RSA con relleno óptimo de cifrado asimétrico (OAEP) con la función hash SHA-1.
- `RSAES_PKCS1_V1_5`(En desuso; desde el 10 de octubre de 2023, AWS KMS no es compatible con el algoritmo de empaquetado RSAES_PKCS1_V1_5): el algoritmo de cifrado RSA con el formato de relleno definido en la versión 1.5 del PKCS #1.
- `SM2PKE`(Solo para regiones de China): algoritmo de cifrado basado en curvas elípticas definido por la OSCCA en el documento GM/T 0003.4-2012.

Temas

Descarga de la clave pública de encapsulamiento y el token de importación (consola)

Puede usar la AWS KMS consola para descargar la clave pública de empaquetado y el token de importación.

1. Si acaba de completar los pasos para crear una clave KMS sin material de claves y se encuentra en la página Download wrapping key and import token (Descargar la clave de encapsulamiento y el token de importación), pase a Step 9.
2. Inicie sesión en la consola AWS Key Management Service (AWS KMS) AWS Management Console y ábrala en https://console.aws.amazon.com/kms.
3. Para cambiarla Región de AWS, usa el selector de regiones en la esquina superior derecha de la página.
4. En el panel de navegación, elija Claves administradas por el cliente.

   > **Tip**
   >
   > Solo puede importar el material de claves a una clave de KMS con un Origen de Externo (importar material de claves). Esto indica que la clave KMS se ha creado sin material de claves. Para agregar la columna Origin (Origen) a la tabla, en la esquina superior derecha de la página, elija el icono de configuración (). Active Origin (Origen) y, a continuación, elija Confirm (Confirmar).

5. Elija el alias o el ID de clave de la clave KMS que está pendiente de importación.
6. Elija la pestaña Cryptographic configuration (Configuración criptográfica) y vea sus valores. Las pestañas están debajo de la sección General configuration (Configuración general).

   Solo se puede importar material de claves a claves de KMS con un Origen de Externo (importar material de claves). Para obtener información acerca de cómo crear claves KMS con material de claves importado, consulte Importación de material clave para AWS KMS llaves.
7. Elija la pestaña Material de claves y, a continuación, seleccione Importar material de claves.

   La pestaña Material de claves aparece solo para las claves de KMS con un Origen de Externo (importar material de claves).
8. En Seleccionar especificación de la clave de encapsulamiento, elija la configuración de su clave de KMS. Después de crear esta clave, no puede cambiar las especificaciones de clave.
9. En Select wrapping algorithm, elija la opción que usará para cifrar el material de claves. Para obtener más información acerca de estas opciones, consulte Seleccionar un algoritmo de encapsulamiento.

10. Elija Descargar clave de encapsulamiento y token de importación y, a continuación, guarde el archivo.

    Si dispone de la opción Next (Siguiente) para continuar con el proceso ahora, elija Next (Siguiente). Para continuar más adelante, elija Cancel (Cancelar).

11. Descomprima el archivo `.zip` que ha guardado en el paso anterior (`Import_Parameters_<key_id>_<timestamp>`).

    La carpeta contiene los siguientes archivos:

    - Una clave pública envolvente en un archivo llamado. `WrappingPublicKey.bin`
    - Un token de importación en un archivo llamado `ImportToken.bin`.
    - Un archivo de texto denominado README.txt. Este archivo contiene información sobre la clave pública de encapsulamiento, el algoritmo de encapsulamiento que se usará para cifrar el material de claves y la fecha y hora en que vencen la clave pública de encapsulamiento y el token de importación.

12. Para continuar el proceso, consulte cifrar el material de claves.

Descargar la clave pública empaquetadora y el token de importación (AWS KMS API)

Para descargar la clave pública y el token de importación, usa la GetParametersForImportAPI. Especifique la clave de KMS que se asociará al material de claves importado. Esta clave de KMS debe tener un valor para Origin de `EXTERNAL`.

En este ejemplo se especifica el algoritmo de encapsulamiento `RSA_AES_KEY_WRAP_SHA_256`, la especificación de clave pública de encapsulamiento RSA_3072 y un ID de clave de ejemplo. Sustituya estos valores de ejemplo por valores válidos para la descarga. En el ID de la clave puede usar el ID de la clave o el ARN de la clave, pero no puede usar un nombre de alias ni un ARN de alias en esta operación.

```
$ aws kms get-parameters-for-import \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --wrapping-algorithm RSA_AES_KEY_WRAP_SHA_256 \
    --wrapping-key-spec RSA_3072
```

Si el comando se ejecuta correctamente, verá un resultado parecido al siguiente:

```
{
```

```
    "ParametersValidTo": 1568290320.0,
    "PublicKey": "public key (base64 encoded)",
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "ImportToken": "import token (base64 encoded)"
}
```

Para preparar los datos para el siguiente paso, base64 decodifica la clave pública e importa el token y guarda los valores decodificados en los archivos.

Para decodificar en base64 la clave pública y el token de importación:

1. Copie los datos codificados en base64 de la clave pública (representados por la *clave pública [codificada en base64]* en el resultado de ejemplo), péguelos en un archivo nuevo y, a continuación, guarde el archivo. Póngale al archivo un nombre descriptivo, como por ejemplo `PublicKey.b64`.
2. Utilice OpenSSL para decodificar en base64 el contenido del archivo y guarde los datos descodificados en un nuevo archivo. El siguiente ejemplo descodifica los datos del archivo que ha guardado en el paso anterior (`PublicKey.b64`) y guarda el resultado en un nuevo archivo denominado `WrappingPublicKey.bin`.

   ```
   $ openssl enc -d -base64 -A -in PublicKey.b64 -out WrappingPublicKey.bin
   ```
3. Copie el token importado codificado en base64 (representado por el *token de importación [codificado en base64]* en el resultado de ejemplo), péguelo en un archivo nuevo y, a continuación, guarde el archivo. Asigne un nombre descriptivo al archivo, por ejemplo, `importtoken.b64`.
4. Utilice OpenSSL para decodificar en base64 el contenido del archivo y guarde los datos descodificados en un nuevo archivo. El siguiente ejemplo descodifica los datos del archivo que ha guardado en el paso anterior (`ImportToken.b64`) y guarda el resultado en un nuevo archivo denominado `ImportToken.bin`.

   ```
   $ openssl enc -d -base64 -A -in importtoken.b64 -out ImportToken.bin
   ```

Continúe en Paso 3: Cifrar el material de claves.

Paso 3 de la importación de material de claves: Cifrar el material de claves

Después de descargar la clave pública y el token de importación, cifre el material de claves con la clave pública que descargó y el algoritmo de encapsulamiento que especificó. Si necesita reemplazar la clave pública o el token de importación, o cambiar el algoritmo de encapsulamiento, debe descargar una nueva clave pública y un token de importación. Para obtener información sobre las claves públicas y los algoritmos de empaquetado AWS KMS compatibles, consulte Selección de una especificación de clave pública de encapsulamiento ySeleccionar un algoritmo de encapsulamiento.

El material de claves debe estar en formato binario. Para obtener información detallada, consulte Requisitos para el material de claves importado.

> **Note**
>
> Para los pares de claves asimétricas, cifra e importa solo la clave privada. AWS KMS deriva la clave pública de la clave privada.
> NO se admite la siguiente combinación: material de claves ECC_NIST_P521, la especificación de clave pública de encapsulamiento RSA_2048 y un algoritmo de encapsulamiento RSAES_OAEP_SHA_*.
> No se puede encapsular directamente el material de claves ECC_NIST_P521 con una clave pública de encapsulamiento RSA_2048. Utilice una clave de encapsulamiento más grande o un algoritmo de encapsulamiento RSA_AES_KEY_WRAP_SHA_*.
> Los algoritmos de empaquetado RSA_AES_KEY_WRAP_SHA_256 y RSA_AES_KEY_WRAP_SHA_1 no se admiten en las regiones de China.

Normalmente, el material de claves se cifra al exportarlo desde el módulo de seguridad de hardware (HSM) o el sistema de administración de claves. Para obtener información sobre cómo exportar el material de claves en formato binario, consulte la documentación de su HSM o sistema de administración de claves. También puede consultar la siguiente sección que proporciona una demostración de prueba de concepto con OpenSSL.

Al cifrar el material de claves, utilice el mismo algoritmo de encapsulamiento que especificó al descargar la clave pública y el token de importación. Para encontrar el algoritmo de empaquetado que especificó, consulte el evento de registro de la solicitud asociada. CloudTrail GetParametersForImport

Generación de material de claves para realizar pruebas

Los siguientes comandos de OpenSSL generan material de claves de cada tipo compatible para realizar pruebas. Estos ejemplos se proporcionan únicamente para pruebas y proof-of-concept demostraciones. En el caso de los sistemas de producción, utilice un método más seguro para generar el material de claves, como un módulo de seguridad de hardware o un sistema de administración de claves.

Para convertir las claves privadas de los pares de claves asimétricas a un formato cifrado en DER, transfiera el comando de generación de material de claves al siguiente comando `openssl pkcs8`. El parámetro `topk8` indica a OpenSSL que tome una clave privada como entrada y devuelva una clave con formato PKCS #8. (El comportamiento predeterminado es el contrario).

```
openssl pkcs8 -topk8 -outform der -nocrypt
```

Los siguientes comandos generan material de claves de prueba para cada uno de los tipos de clave compatibles.

- Clave de cifrado simétrica (32 bytes)

  Este comando genera una clave simétrica de 256 bits (cadena aleatoria de 32 bytes) y la guarda en el archivo `PlaintextKeyMaterial.bin`. No es necesario cifrar este material de claves.

  ```
  openssl rand -out PlaintextKeyMaterial.bin 32
  ```

  Solo en las regiones de China, debe generar una clave simétrica de 128 bits (cadena aleatoria de 16 bytes).

  ```
  openssl rand -out PlaintextKeyMaterial.bin 16
  ```

- Claves HMAC

  Este comando genera una cadena de bytes aleatorios del tamaño especificado. No es necesario cifrar este material de claves.

  La longitud de la clave HMAC debe coincidir con la longitud definida en la especificación de clave de la clave de KMS. Por ejemplo, si la clave de KMS es HMAC_384, debe importar una clave de 384 bits (48 bytes).

```
openssl rand -out HMAC_224_PlaintextKey.bin 28

openssl rand -out HMAC_256_PlaintextKey.bin 32

openssl rand -out HMAC_384_PlaintextKey.bin 48

openssl rand -out HMAC_512_PlaintextKey.bin 64
```

- Claves privadas RSA

```
openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:2048 | openssl pkcs8 -topk8 -
outform der -nocrypt > RSA_2048_PrivateKey.der

openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:3072 | openssl pkcs8 -topk8 -
outform der -nocrypt > RSA_3072_PrivateKey.der

openssl genpkey -algorithm rsa -pkeyopt rsa_keygen_bits:4096 | openssl pkcs8 -topk8 -
outform der -nocrypt > RSA_4096_PrivateKey.der
```

- Claves privadas ECC

```
openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:P-256 | openssl pkcs8 -topk8
 -outform der -nocrypt > ECC_NIST_P256_PrivateKey.der

openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:P-384 | openssl pkcs8 -topk8
 -outform der -nocrypt > ECC_NIST_P384_PrivateKey.der

openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:P-521 | openssl pkcs8 -topk8
 -outform der -nocrypt > ECC_NIST_P521_PrivateKey.der

openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:secp256k1 | openssl pkcs8 -
topk8 -outform der -nocrypt > ECC_SECG_P256K1_PrivateKey.der
```

- Claves privadas SM2 (solo para regiones de China)

```
openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:sm2 | openssl pkcs8 -topk8 -
outform der -nocrypt > SM2_PrivateKey.der
```

Ejemplos de cifrado de material de claves con OpenSSL

Los siguientes ejemplos muestran cómo utilizar OpenSSL para cifrar el material de claves con la clave pública que ha descargado. Para cifrar el material de su clave con una clave pública SM2 (solo para las regiones de China), utilice la clase. `SM2OfflineOperationHelper`

> **Important**
>
> Estos ejemplos son solo una demostración de la prueba de concepto. En el caso de los sistemas de producción, utilice un método más seguro (como un HSM o un sistema de administración de claves comercial) para generar y almacenar el material de claves.
> NO se admite la siguiente combinación: material de claves ECC_NIST_P521, la especificación de clave pública de encapsulamiento RSA_2048 y un algoritmo de encapsulamiento RSAES_OAEP_SHA_*.
> No se puede encapsular directamente el material de claves ECC_NIST_P521 con una clave pública de encapsulamiento RSA_2048. Utilice una clave de encapsulamiento más grande o un algoritmo de encapsulamiento RSA_AES_KEY_WRAP_SHA_*.

RSAES_OAEP_SHA_1

AWS KMS admite la RSAES_OAEP_SHA_1 para claves de cifrado simétricas (SYMMETRIC_DEFAULT), claves privadas de curva elíptica (ECC), claves privadas SM2 y claves HMAC.

RSAES_OAEP_SHA_1 no es compatible con las claves privadas RSA. Además, no puede usar una clave de encapsulamiento pública RSA_2048 con ningún algoritmo de encapsulamiento RSAES_OAEP_SHA_* para encapsular una clave privada ECC_NIST_P521 (secp521r1). Debe usar una clave de pública de encapsulamiento más grande o un algoritmo de encapsulamiento RSA_AES_KEY_WRAP.

El siguiente ejemplo cifra el material de claves con la clave pública que ha descargado y el algoritmo de encapsulamiento RSAES_OAEP_SHA_1, y lo guarda en el archivo `EncryptedKeyMaterial.bin`.

En este ejemplo:

- *`WrappingPublicKey.bin`* es el archivo que contiene la clave pública de encapsulamiento descargada.

- *PlaintextKeyMaterial.bin* es el archivo que contiene el material de claves que está cifrando, como `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin` o `ECC_NIST_P521_PrivateKey.der`.

```
$ openssl pkeyutl \
    -encrypt \
    -in PlaintextKeyMaterial.bin \
    -out EncryptedKeyMaterial.bin \
    -inkey WrappingPublicKey.bin \
    -keyform DER \
    -pubin \
    -pkeyopt rsa_padding_mode:oaep \
    -pkeyopt rsa_oaep_md:sha1
```

RSAES_OAEP_SHA_256

AWS KMS admite el RSAES_OAEP_SHA_256 para claves de cifrado simétricas (SYMMETRIC_DEFAULT), claves privadas de curva elíptica (ECC), claves privadas SM2 y claves HMAC.

RSAES_OAEP_SHA_256 no es compatible con las claves privadas RSA. Además, no puede usar una clave de encapsulamiento pública RSA_2048 con ningún algoritmo de encapsulamiento RSAES_OAEP_SHA_* para encapsular una clave privada ECC_NIST_P521 (secp521r1). Debe usar una clave pública más grande o un algoritmo de encapsulamiento RSA_AES_KEY_WRAP.

El siguiente ejemplo cifra el material de claves con la clave pública que ha descargado y el algoritmo de encapsulamiento RSAES_OAEP_SHA_256, y lo guarda en el archivo `EncryptedKeyMaterial.bin`.

En este ejemplo:

- *WrappingPublicKey.bin* es el archivo que contiene la clave de encapsulamiento pública descargada. Si ha descargado la clave pública desde la consola, este archivo se denomina `wrappingKey_`*KMS key_key_ID_timestamp* (por ejemplo, `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).
- *PlaintextKeyMaterial.bin* es el archivo que contiene el material de claves que está cifrando, como `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin` o `ECC_NIST_P521_PrivateKey.der`.

```
$ openssl pkeyutl \
    -encrypt \
    -in PlaintextKeyMaterial.bin \
    -out EncryptedKeyMaterial.bin \
    -inkey WrappingPublicKey.bin \
    -keyform DER \
    -pubin \
    -pkeyopt rsa_padding_mode:oaep \
    -pkeyopt rsa_oaep_md:sha256 \
    -pkeyopt rsa_mgf1_md:sha256
```

RSA_AES_KEY_WRAP_SHA_1

El algoritmo de encapsulamiento RSA_AES_KEY_WRAP_SHA_1 implica dos operaciones de cifrado.

1. Cifre el material de claves con una clave simétrica AES que genere y un algoritmo de cifrado simétrico AES.
2. Cifre la clave simétrica AES que utilizó con la clave pública que descargó y el algoritmo de encapsulamiento RSAES_OAEP_SHA_1.

AWS KMS admite los algoritmos de empaquetado RSA_AES_KEY_WRAP_SHA_* para todos los tipos de material de claves importadas admitidos y todas las especificaciones de claves públicas compatibles. Los algoritmos RSA_AES_KEY_WRAP_SHA_* son los únicos algoritmos de encapsulamiento compatibles para encapsular material de claves RSA.

El algoritmo de encapsulamiento RSA_AES_KEY_WRAP_SHA_1 requiere la versión 3.x de OpenSSL o posterior.

1. Generación de una clave de cifrado simétrica AES de 256 bits

   Este comando genera una clave de cifrado simétrica AES que consta de 256 bits aleatorios y la guarda en el archivo `aes-key.bin`

   ```
   # Generate a 32-byte AES symmetric encryption key
   $ openssl rand -out aes-key.bin 32
   ```

2. Cifrado del material de claves con la clave de cifrado simétrica AES

   Este comando cifra el material de claves con la clave de cifrado simétrica AES y guarda el material de claves cifrado en el archivo `key-material-wrapped.bin`.

   En este comando de ejemplo:

   - *`PlaintextKeyMaterial.bin`* es el archivo que contiene el material de claves que está importando, como `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin`, `RSA_3072_PrivateKey.der` o `ECC_NIST_P521_PrivateKey.der`.
   - *`aes-key.bin`* es el archivo que contiene la clave de cifrado simétrica AES de 256 bits que generó en el comando anterior.

```
# Encrypt your key material with the AES symmetric encryption key
$ openssl enc -id-aes256-wrap-pad \
        -K "$(xxd -p < aes-key.bin | tr -d '\n')" \
        -iv A65959A6 \
        -in PlaintextKeyMaterial.bin\
        -out key-material-wrapped.bin
```

3. Cifrado de la clave de cifrado simétrica AES con la clave pública

   Este comando cifra la clave de cifrado simétrica AES con la clave pública que ha descargado y el algoritmo de encapsulamiento RSAES_OAEP_SHA_1, la cifra en DER y la guarda en el archivo `aes-key-wrapped.bin`.

   En este comando de ejemplo:

   - *`WrappingPublicKey.bin`* es el archivo que contiene la clave de encapsulamiento pública descargada. Si ha descargado la clave pública desde la consola, este archivo se denomina `wrappingKey_`*`KMS key_key_ID_timestamp`* (por ejemplo, `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).
   - *`aes-key.bin`* es el archivo que contiene la clave de cifrado simétrica AES de 256 bits que generó en el primer comando de esta secuencia de ejemplo.

```
# Encrypt your AES symmetric encryption key with the downloaded public key
$ openssl pkeyutl \
    -encrypt \
```

```
    -in aes-key.bin \
    -out aes-key-wrapped.bin \
    -inkey WrappingPublicKey.bin \
    -keyform DER \
    -pubin \
    -pkeyopt rsa_padding_mode:oaep \
    -pkeyopt rsa_oaep_md:sha1 \
    -pkeyopt rsa_mgf1_md:sha1
```

4. Generación del archivo que se va a importar

   Concatene el archivo con el material de la clave cifrada y el archivo con la clave AES cifrada. Guárdelos en el archivo `EncryptedKeyMaterial.bin`, que es el archivo que va a importar en Paso 4: Importar el material de claves.

   En este comando de ejemplo:

   - *`key-material-wrapped.bin`* es el archivo que contiene el material de claves cifrado.
   - *`aes-key-wrapped.bin`* es el archivo que contiene la clave de cifrado AES cifrada.

```
# Combine the encrypted AES key and encrypted key material in a file
$ cat aes-key-wrapped.bin key-material-wrapped.bin > EncryptedKeyMaterial.bin
```

RSA_AES_KEY_WRAP_SHA_256

El algoritmo de encapsulamiento RSA_AES_KEY_WRAP_SHA_256 implica dos operaciones de cifrado.

1. Cifre el material de claves con una clave simétrica AES que genere y un algoritmo de cifrado simétrico AES.
2. Cifre la clave simétrica AES que utilizó con la clave pública que descargó y el algoritmo de encapsulamiento RSAES_OAEP_SHA_256.

AWS KMS admite los algoritmos de empaquetado RSA_AES_KEY_WRAP_SHA_* para todos los tipos de material clave importado y todas las especificaciones de clave pública compatibles. Los algoritmos RSA_AES_KEY_WRAP_SHA_* son los únicos algoritmos de encapsulamiento compatibles para encapsular material de claves RSA.

El algoritmo de encapsulamiento RSA_AES_KEY_WRAP_SHA_256 requiere la versión 3.x de OpenSSL o posterior.

1. Generación de una clave de cifrado simétrica AES de 256 bits

   Este comando genera una clave de cifrado simétrica AES que consta de 256 bits aleatorios y la guarda en el archivo `aes-key.bin`

   ```
   # Generate a 32-byte AES symmetric encryption key
   $ openssl rand -out aes-key.bin 32
   ```

2. Cifrado del material de claves con la clave de cifrado simétrica AES

   Este comando cifra el material de claves con la clave de cifrado simétrica AES y guarda el material de claves cifrado en el archivo `key-material-wrapped.bin`.

   En este comando de ejemplo:

   - *`PlaintextKeyMaterial.bin`* es el archivo que contiene el material de claves que está importando, como `PlaintextKeyMaterial.bin`, `HMAC_384_PlaintextKey.bin`, `RSA_3072_PrivateKey.der` o `ECC_NIST_P521_PrivateKey.der`.
   - *`aes-key.bin`* es el archivo que contiene la clave de cifrado simétrica AES de 256 bits que generó en el comando anterior.

   ```
   # Encrypt your key material with the AES symmetric encryption key
   $ openssl enc -id-aes256-wrap-pad \
           -K "$(xxd -p < aes-key.bin | tr -d '\n')" \
           -iv A65959A6 \
           -in PlaintextKeyMaterial.bin\
           -out key-material-wrapped.bin
   ```

3. Cifrado de la clave de cifrado simétrica AES con la clave pública

   Este comando cifra la clave de cifrado simétrica AES con la clave pública que ha descargado y el algoritmo de encapsulamiento RSAES_OAEP_SHA_256, la cifra en DER y la guarda en el archivo `aes-key-wrapped.bin`.

   En este comando de ejemplo:

- *WrappingPublicKey.bin* es el archivo que contiene la clave de encapsulamiento pública descargada. Si ha descargado la clave pública desde la consola, este archivo se denomina `wrappingKey_`*KMS key_key_ID_timestamp* (por ejemplo, `wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909`).
- *aes-key.bin* es el archivo que contiene la clave de cifrado simétrica AES de 256 bits que generó en el primer comando de esta secuencia de ejemplo.

```
# Encrypt your AES symmetric encryption key with the downloaded public key
$ openssl pkeyutl \
    -encrypt \
    -in aes-key.bin \
    -out aes-key-wrapped.bin \
    -inkey WrappingPublicKey.bin \
    -keyform DER \
    -pubin \
    -pkeyopt rsa_padding_mode:oaep \
    -pkeyopt rsa_oaep_md:sha256 \
    -pkeyopt rsa_mgf1_md:sha256
```

4. Generación del archivo que se va a importar

   Concatene el archivo con el material de la clave cifrada y el archivo con la clave AES cifrada. Guárdelos en el archivo `EncryptedKeyMaterial.bin`, que es el archivo que va a importar en Paso 4: Importar el material de claves.

   En este comando de ejemplo:

   - *key-material-wrapped.bin* es el archivo que contiene el material de claves cifrado.
   - *aes-key-wrapped.bin* es el archivo que contiene la clave de cifrado AES cifrada.

```
# Combine the encrypted AES key and encrypted key material in a file
$ cat aes-key-wrapped.bin key-material-wrapped.bin > EncryptedKeyMaterial.bin
```

Continúe en Paso 4: Importar el material de claves.

Paso 4 de la importación de material de claves: Importar el material de claves

Después de cifrar el material de claves, puede importar el material de claves para usarlo con una AWS KMS key. Para importar el material de claves, debe cargar el material de claves cifrado desde Paso 3: Cifrar el material de claves y el token de importación que ha descargado en Paso 2: descargar la clave pública de encapsulamiento y el token de importación. Debe importar material de claves en la misma clave KMS que ha especificado al descargar la clave pública y el token de importación. Cuando se importa el material de claves, el estado de la clave de KMS cambia a `Enabled`. Puede usar la clave de KMS en operaciones criptográficas.

Al importar el material de claves de importación, puede establecer una fecha de vencimiento opcional para el material de claves. Cuando vence el material de claves, AWS KMS lo elimina y ya no se puede utilizar la clave KMS. Para volver a usar la clave KMS en operaciones criptográfica, debe volver a importar el mismo material de claves. Después de importar el material de claves, no puede establecer, cambiar ni cancelar la fecha de caducidad de la importación actual. Para cambiar estos valores, debe eliminar y volver a importar el mismo material de claves.

Para importar material clave, puede usar la AWS KMS consola o la ImportKeyMaterialAPI. Puede utilizar la API directamente efectuando solicitudes HTTP o mediante un SDK deAWS, AWS Command Line Interface o AWS Tools for PowerShell.

Al importar el material clave, se añade una ImportKeyMaterialentrada al AWS CloudTrail registro para registrar la `ImportKeyMaterial` operación. La CloudTrail entrada es la misma tanto si se utiliza la AWS KMS consola como si se utiliza la AWS KMS API.

Configuración de una fecha de vencimiento (opcional)

Al importar el material de claves para su clave de KMS, puede establecer una fecha y hora de vencimiento opcionales para el material de claves de hasta 365 días a partir de la fecha de importación. Cuando el material clave importado vence, AWS KMS lo borra. Esta acción cambia el estado de clave de la clave de KMS a `PendingImport`, lo que evita que se la utilice en operaciones criptográficas. Para usar la clave de KMS, debe volver a importar una copia del material de claves original.

Garantizar que el material de claves importado venza con frecuencia puede ayudarlo a cumplir con los requisitos normativos, pero supone un riesgo adicional para los datos cifrados con la clave de KMS. Hasta que no se vuelva a importar una copia del material de claves original, no se podrá utilizar una clave de KMS con material de claves vencido y no se podrá acceder a los datos cifrados con la

clave de KMS. Si no vuelve a importar el material de claves por cualquier motivo, incluida la pérdida de la copia del material de claves original, la clave de KMS quedará inutilizable de forma permanente y los datos cifrados con la clave de KMS no se podrán recuperar.

Para mitigar este riesgo, asegúrese de que su copia del material de claves importado esté accesible y diseñe un sistema para eliminar y volver a importar el material de claves antes de que venza e interrumpa su carga de trabajo en AWS. Le recomendamos que active una alarma que le indique el vencimiento del material de claves importado para que tenga tiempo suficiente para volver a importarlo antes de que venza. También puede utilizar sus CloudTrail registros para auditar las operaciones de importación (y reimportación) de material clave y eliminar material clave importado, así como la AWS KMS operación de eliminación del material clave caducado.

No puede importar material de claves diferente a la clave de KMS y AWS KMS no puede restaurar, recuperar ni reproducir el material de claves eliminado. En lugar de establecer una fecha de vencimiento, puede eliminar y volver a importar periódicamente el material de claves importado mediante programación, pero los requisitos para retener una copia del material de claves original son los mismos.

Usted determina si el material de claves importado vence y cuándo lo hace cuando importa el material de claves. Sin embargo, puede activar y desactivar el vencimiento o establecer una nueva fecha de vencimiento eliminando y volviendo a importar el material de claves. Utilice el `ExpirationModel` parámetro ImportKeyMaterialpara activar (`KEY_MATERIAL_EXPIRES`) y desactivar la caducidad (`KEY_MATERIAL_DOES_NOT_EXPIRE`) y el `ValidTo` parámetro para establecer la hora de caducidad. El tiempo máximo es de 365 días a partir de los datos de importación; no hay un mínimo, pero la fecha debe ser en el futuro.

Importar el material de claves (consola)

Puede usar la AWS Management Console para importar el material de claves.

1. Si se encuentra en la página Cargar material de claves encapsulado, vaya a Step 8.
2. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
3. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
4. En el panel de navegación, elija Claves administradas por el cliente.
5. Elija el ID de clave o el alias de la clave KMS para los que ha descargado la clave pública y el token de importación.

6. Elija la pestaña Cryptographic configuration (Configuración criptográfica) y vea sus valores. Las pestañas se encuentran en la página de detalles de una clave KMS debajo de la sección General configuration (Configuración general).

   Solo se puede importar material de claves a claves de KMS con un Origen de Externo (importar material de claves). Para obtener información sobre cómo crear claves KMS con material de claves importado, consulte Importación de material clave para AWS KMS llaves.

7. Elija la pestaña Material de claves y, a continuación, seleccione Importar material de claves. La pestaña Material de claves aparece solo para las claves de KMS con un Origen de Externo (importar material de claves).

   Si descargó el material de claves, importó el token y cifró el material de claves, seleccione Siguiente.

8. En la sección Token de importación y material de claves cifrado, haga lo siguiente:

   a. En Material de claves encapsulado, seleccione Elegir archivo. A continuación, especifique el archivo que contiene el material de claves encapsulado (cifrado).

   b. En Token de importación, seleccione Elegir archivo. Suba el archivo que contenga el token de importación que ha descargado.

9. En la sección Expiration option (Opción de vencimiento), determina si vence el material de claves. Para establecer una fecha y una hora de vencimiento, elija El material de claves caduca, y seleccione una fecha y una hora en el calendario. Puede especificar una fecha de hasta 365 días a partir de la hora y fecha actuales.

10. Elija Cargar material de claves.

Importar material de claves (API de AWS KMS)

Para importar material clave, utilice la ImportKeyMaterialoperación. Los ejemplos siguientes utilizan la AWS CLI, pero puede usar cualquier lenguaje de programación admitido.

Para usar este ejemplo:

1. Sustituya *1234abcd-12ab-34cd-56ef-1234567890ab* por un ID de clave de la clave KMS que usó cuando descargó la clave pública y el token de importación. Para identificar la clave KMS, utilice su ID de clave o su ARN de clave. No puede utilizar un nombre de alias o un ARN de alias para esta operación.

2. Sustituya *EncryptedKeyMaterial.bin* por el nombre del archivo que contiene el material de claves cifradas.
3. Sustituya *ImportToken.bin* por el nombre del archivo que contiene el token de importación.
4. Si desea que el material de claves importado caduque, defina el valor del parámetro `expiration-model` a su valor predeterminado, `KEY_MATERIAL_EXPIRES`, u omita el parámetro `expiration-model`. A continuación, sustituya el valor del parámetro `valid-to` con la fecha y la hora en que desea que caduque el material de claves. La fecha y la hora pueden ser hasta 365 días a partir del momento de la solicitud.

```
$ aws kms import-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --encrypted-key-material fileb://EncryptedKeyMaterial.bin \
    --import-token fileb://ImportToken.bin \
    --expiration-model KEY_MATERIAL_EXPIRES \
    --valid-to 2023-06-17T12:00:00-08:00
```

Si no desea que el material de claves importado caduque, defina el valor del parámetro `expiration-model` a `KEY_MATERIAL_DOES_NOT_EXPIRE` y omita el parámetro `valid-to` del comando.

```
$ aws kms import-key-material --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --encrypted-key-material fileb://EncryptedKeyMaterial.bin \
    --import-token fileb://ImportToken.bin \
    --expiration-model KEY_MATERIAL_DOES_NOT_EXPIRE
```

> **Tip**
>
> Si el comando no se ejecuta correctamente, es posible que aparezca `KMSInvalidStateException` o `NotFoundException`. Puede reintentar la solicitud.

Almacenes de claves personalizados

Un almacén de claves es una ubicación segura para almacenar claves criptográficas. El almacén de claves predeterminado en AWS KMS también admite métodos para generar y administrar las claves que almacena. De forma predeterminada, el material de claves criptográficas para las AWS KMS keys que crea en AWS KMS son generadas y están protegidas por módulos de seguridad de

hardware (HSM) que son módulos criptográficos validados mediante FIPS 140-2. El material de claves para sus claves de KMS nunca sale de los HSM sin cifrar.

Sin embargo, si necesita un mayor control de los HSM, puede crear un almacén de claves personalizado.

Un almacén de claves personalizado es un almacén de claves lógico en AWS KMS que está respaldado por un administrador de claves externo a AWS KMS que usted posee y administra. Los almacenes de claves personalizados combinan la interfaz de administración de claves integral y simple de AWS KMS con la capacidad de poseer y controlar el material de claves y las operaciones criptográficas. Al utilizar una clave de KMS en un almacén de claves personalizado, el administrador de claves realiza las operaciones criptográficas usando sus claves criptográficas. Como resultado, usted asume una mayor responsabilidad por la disponibilidad y la durabilidad de las claves criptográficas y por el funcionamiento de los HSM.

AWS KMS es compatible con dos tipos de almacenes de claves personalizados.

- Un almacén de claves de AWS CloudHSM es un almacén de claves de AWS KMS personalizado respaldado por un clúster de AWS CloudHSM. Al crear una clave de KMS en el almacén de claves de AWS CloudHSM, AWS KMS genera una clave simétrica Advanced Encryption Standard (AES) de 256 bits, persistente y no exportable en el clúster de AWS CloudHSM asociado. Este material de claves nunca sale de sus clústeres de AWS CloudHSM sin cifrar. Al utilizar una clave de KMS en el almacén de claves de AWS CloudHSM, las operaciones criptográficas se realizan en los HSM del clúster. Los clústeres de AWS CloudHSM están respaldados por módulos de seguridad de hardware (HSM) que tienen el certificado FIPS 140-2 nivel 3.
- Un almacén de claves externo es un almacén de claves personalizado de AWS KMS respaldado por un administrador de claves externo ajeno a AWS que usted posee y controla. Cuando usa una clave de KMS en su almacén de claves externo, el administrador de claves externo realiza todas las operaciones de cifrado y descifrado mediante sus claves criptográficas. Los almacenes de claves externos están diseñados para ser compatibles con una variedad de administradores de claves externos de diferentes proveedores.

  AWS KMS nunca ve, accede ni interactúa directamente con su administrador de claves externo o sus claves criptográficas. Al cifrar o descifrar con una clave de KMS en un almacén de claves externo, el administrador de claves externo realiza la operación utilizando sus claves externas. Puede mantener el control total sobre sus claves criptográficas, incluida la posibilidad de rechazar o detener una operación criptográfica sin interactuar con AWS. Sin embargo, debido a la distancia y al procesamiento adicional, las claves de KMS de un almacén de claves externo pueden tener

una latencia y un rendimiento más bajos y pueden tener características de disponibilidad diferentes a las de las claves de KMS que contienen material de claves en AWS KMS. Para obtener más información sobre los administradores de claves compatibles con la característica de almacén de claves externos de AWS KMS, consulte ¿Qué proveedores externos son compatibles con la especificación del proxy del XKS? en las Preguntas frecuentes de AWS Key Management Service.

Estos dos tipos de almacenes de claves personalizados son muy diferentes del almacén de claves de AWS KMS estándar y entre sí. Sus modelos de seguridad, la asignación de responsabilidad, el rendimiento, el precio y los casos de uso también son muy diferentes. Antes de seleccionar un almacén de claves personalizado, lea la documentación relacionada y confirme que la responsabilidad adicional de configuración y mantenimiento es una buena compensación por el control adicional. Sin embargo, si las normas y reglamentos bajo los que opera requieren un control directo del material de claves, un almacén de claves personalizado podría ser una buena opción para usted.

Características no admitidas

AWS KMS no es compatible con las siguientes características en almacenes de claves personalizado.

- Claves de KMS asimétricas
- Pares de claves de datos asimétricas
- Claves KMS HMAC
- Claves KMS con material de claves importado
- Rotación automática de claves
- Claves de varias regiones

Temas

- AWS CloudHSM tiendas clave
- Almacenes de claves externos

AWS CloudHSM tiendas clave

Un almacén de AWS CloudHSM claves es un almacén de claves personalizado respaldado por un AWS CloudHSM clúster. Al crear uno AWS KMS keyen un almacén de claves personalizado,

AWS KMS genera y almacena material de claves no extraíble para la clave de KMS en un AWS CloudHSM clúster que es de su propiedad y que administra. Al utilizar una clave KMS en un almacén de claves personalizado, las operaciones criptográficas se realizan en los HSM del clúster. Esta función combina la comodidad y la amplia integración AWS KMS con el control adicional de un AWS CloudHSM clúster en el suyo. Cuenta de AWS

AWS KMS proporciona soporte completo de consola y API para crear, usar y administrar sus almacenes de claves personalizados. Puede usar las claves KMS de su almacén de claves personalizado de la misma manera que usa cualquier clave KMS. Por ejemplo, puede usar las claves KMS para generar claves de datos y para cifrar datos. También puede usar las claves de KMS en su almacén de claves personalizado con AWS servicios que admitan las claves administradas por el cliente.

¿Necesito un almacén de claves personalizado?

Para la mayoría de los usuarios, el almacén de AWS KMS claves predeterminado, que está protegido por módulos criptográficos validados por el FIPS 140-2, cumple sus requisitos de seguridad. No es necesario agregar una capa extra de responsabilidad de mantenimiento o una dependencia de un servicio adicional.

Sin embargo, puede plantearse crear un almacén de claves personalizado si su organización cumple alguno de los siguientes requisitos:

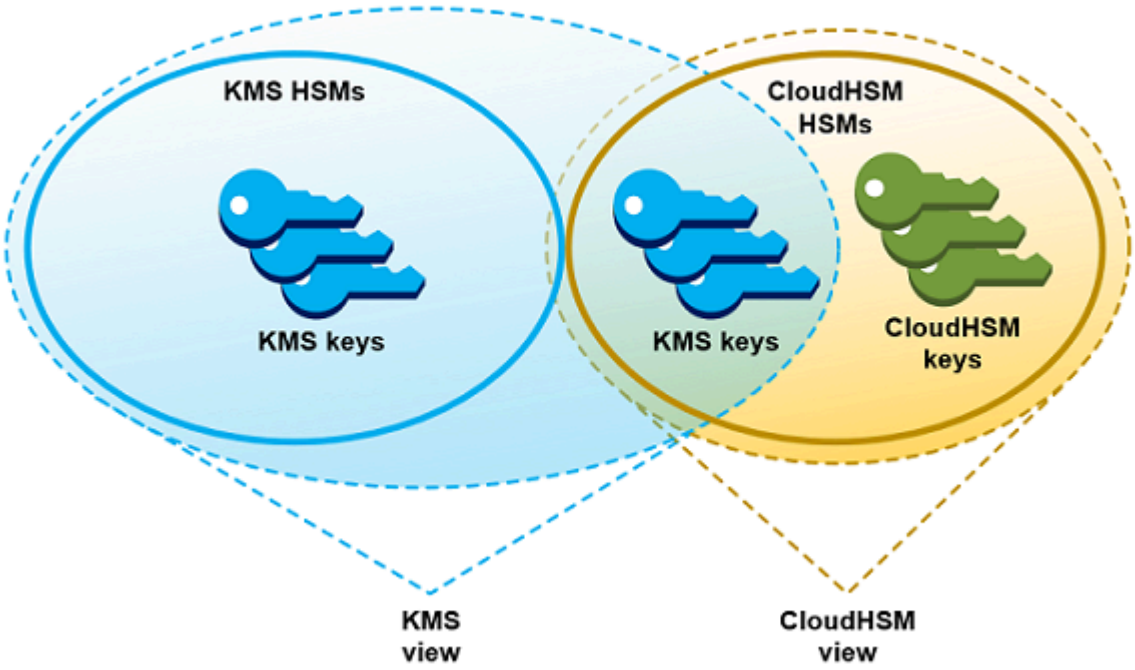
- Tiene claves que deben protegerse de forma explícita en un HSM de un solo inquilino o en un HSM sobre el que tiene control directo.
- Necesita la capacidad de eliminar inmediatamente el material clave de. AWS KMS
- Debe poder auditar todo el uso de sus claves de forma independiente AWS KMS o AWS CloudTrail.

¿Cómo funcionan los almacenes de claves personalizados?

Cada almacén de claves personalizado está asociado a un AWS CloudHSM clúster de su Cuenta de AWS. Al conectar el almacén de claves personalizado a su clúster, AWS KMS crea la infraestructura de red necesaria para respaldar la conexión. A continuación, inicia sesión en el AWS CloudHSM cliente de claves del clúster con las credenciales de un usuario criptográfico dedicado del clúster.

Puede crear y administrar sus almacenes de claves personalizados AWS KMS y crear y administrar sus clústeres de HSM en AWS CloudHSM. Al crear AWS KMS keys en un almacén de claves AWS

KMS personalizado, puede ver y administrar las claves de KMS en AWS KMSél. Sin embargo, también puede ver y administrar su material clave en él AWS CloudHSM, tal como lo haría con otras claves del clúster.



Puede crear claves KMS de cifrado simétrico con el material de claves generado AWS KMS en su almacén de claves personalizado. A continuación, utilice las mismas técnicas para ver y administrar las claves de KMS del almacén de claves personalizado que utiliza para las claves de KMS del almacén de AWS KMS claves. Puede controlar el acceso con políticas de claves y de IAM, crear etiquetas y alias, habilitar y desactivar las claves KMS y programar la eliminación de claves. Puede usar las claves de KMS para operaciones criptográficas y utilizarlas con AWS servicios que se integren con AWS KMS ellas.

Además, tiene el control total del AWS CloudHSM clúster, lo que incluye la creación y eliminación de los HSM y la gestión de las copias de seguridad. Puede usar el AWS CloudHSM cliente y las bibliotecas de software compatibles para ver, auditar y administrar el material clave de sus claves de KMS. Mientras el almacén de claves personalizadas esté desconectado, AWS KMS no podrá acceder a él y los usuarios no podrán utilizar las claves de KMS del almacén de claves personalizadas para operaciones criptográficas. Esta capa de control agregada convierte a los almacenes de claves personalizados en una solución potente para las organizaciones que la necesitan.

¿Por dónde empiezo?

Para crear y administrar un almacén de AWS CloudHSM claves, utilice las funciones de AWS KMS y AWS CloudHSM.

1. Comience en AWS CloudHSM. Cree un clúster de AWS CloudHSM activo o seleccione uno existente. El clúster debe tener al menos dos HSM activos en distintas zonas de disponibilidad. A continuación, cree una cuenta de usuario de criptografía (CU) dedicado en dicho clúster para AWS KMS.
2. En AWS KMS, cree un almacén de claves personalizado que esté asociado al AWS CloudHSM clúster seleccionado. AWS KMS proporciona una interfaz de administración completa que le permite crear, ver, editar y eliminar sus almacenes de claves personalizados.
3. Cuando esté listo para usar su almacén de claves personalizado, conéctelo al AWS CloudHSM clúster asociado. AWS KMS crea la infraestructura de red que necesita para soportar la conexión. A continuación, se registra en el clúster con las credenciales de la cuenta de usuario de criptografía dedicado para que pueda generar y administrar material de claves en el clúster.
4. Ahora, puede crear claves KMS de cifrado simétricas en su almacén de claves personalizado. Únicamente debe especificar el almacén de claves personalizado al crear la clave KMS.

Si se queda bloqueado en algún momento, puede buscar ayuda en el tema Resolver problemas de un almacén de claves personalizado. Si su pregunta no tiene respuesta, utilice el enlace de comentarios en la parte inferior de cada página de esta guía o escriba en el Foro de discusión de AWS Key Management Service.

Cuotas

AWS KMS permite hasta 10 almacenes de claves personalizados en cada Cuenta de AWS región, incluidos los almacenes de AWS CloudHSM claves y los almacenes de claves externos, independientemente del estado de conexión. Además, hay cuotas de AWS KMS solicitud para el uso de claves KMS en un almacén de AWS CloudHSM claves.

Precios

Para obtener información sobre el costo de los almacenes de claves AWS KMS personalizados y las claves administradas por el cliente en un almacén de claves personalizado, consulte AWS Key Management Service los precios. Para obtener información sobre el costo de AWS CloudHSM los clústeres y los HSM, consulte AWS CloudHSM los precios.

Regiones

AWS KMS admite tiendas AWS CloudHSM clave en todos los Regiones de AWS lugares donde AWS KMS sea compatible, excepto en Asia Pacífico (Melbourne), China (Pekín), China (Ningxia) y Europa (España).

Características no admitidas

AWS KMS no admite las siguientes funciones en los almacenes de claves personalizadas.

- Claves de KMS asimétricas
- Pares de claves de datos asimétricas
- Claves KMS HMAC
- Claves KMS con material de claves importado
- Rotación automática de claves
- Claves de varias regiones

Temas

Conceptos del almacén de claves de AWS CloudHSM

En este tema se explican algunos de los conceptos empleados en los almacenes de claves de AWS CloudHSM.

Almacén de claves de AWS CloudHSM

Un almacén de claves de AWS CloudHSM es un almacén de claves personalizado asociado a un clúster de AWS CloudHSM que usted posee y administra. Los clústeres de AWS CloudHSM están respaldados por módulos de seguridad de hardware (HSM) que tienen el certificado FIPS 140-2 nivel 3.

Al crear una clave de KMS en el almacén de claves de AWS CloudHSM, AWS KMS genera una clave simétrica Advanced Encryption Standard (AES) de 256 bits, persistente y no exportable

en el clúster de AWS CloudHSM asociado. Este material de claves nunca sale de los HSM sin cifrar. Al utilizar una clave de KMS en un almacén de claves de AWS CloudHSM, las operaciones criptográficas se realizan en los HSM del clúster.

Los almacenes de claves de AWS CloudHSM combinan la interfaz de administración de claves integral y simple de AWS KMS con controles adicionales proporcionados por un clúster de AWS CloudHSM en su Cuenta de AWS. Esta característica integrada le permite crear, administrar y usar claves KMS en AWS KMS a la vez que controla por completo los HSM que almacenan su material de claves, incluida la administración de clústers, HSM y copias de seguridad. Puede usar la consola de AWS KMS y las API para administrar un almacén de claves de AWS CloudHSM y sus claves de KMS. También puede utilizar la consola de AWS CloudHSM, las API, el software de cliente y las bibliotecas de software asociadas para administrar el clúster asociado.

Puede ver y administrar su almacén de claves de AWS CloudHSM, editar sus propiedades y conectar y desconectarlo de su clúster de AWS CloudHSM asociado. Si tiene que eliminar un almacén de claves de AWS CloudHSM, primero deberá eliminar las claves de KMS del almacén de claves de AWS CloudHSM programando su eliminación y esperando a que venza el periodo de gracia. Al eliminar el almacén de claves de AWS CloudHSM, desaparece el recurso de AWS KMS, pero no afecta a su clúster de AWS CloudHSM.

AWS CloudHSMClúster de

Cada almacén de claves de AWS CloudHSM está asociado a un clúster de AWS CloudHSM. Al crear una AWS KMS key en el almacén de claves de AWS CloudHSM, AWS KMS crea su material de claves en el clúster asociado. Al utilizar una clave de KMS en el almacén de claves de AWS CloudHSM, la operación criptográfica se realiza en el clúster asociado.

Cada clúster de AWS CloudHSM solo puede asociarse a un almacén de claves de AWS CloudHSM. El clúster que elija no podrá asociarse con ningún otro almacén de claves de AWS CloudHSM o compartir un historial de copias de seguridad con un clúster asociado a otro almacén de claves de AWS CloudHSM. El clúster debe inicializarse y estar activo y estar en la misma Cuenta de AWS y región que el almacén de claves de AWS CloudHSM. Puede crear un clúster nuevo o utilizar uno existente. AWS KMS no requiere un uso exclusivo del clúster. Para crear las claves de KMS en el almacén de claves de AWS CloudHSM, su clúster asociado debe incluir al menos dos HSM activos. El resto de operaciones solo precisan un HSM.

Debe especificar el clúster de AWS CloudHSM al crear el almacén de claves de AWS CloudHSM y no lo puede cambiar. Sin embargo, puede sustituir cualquier clúster que comparta un historial de copias de seguridad con el clúster original. De este modo podrá eliminar el clúster, en caso

necesario, y reemplazarlo por uno creado a partir de una de sus copias de seguridad. Mantendrá todo el control del clúster de AWS CloudHSM asociado, por lo que podrá administrar usuarios y claves, crear y eliminar HSM, y usar y administrar copias de seguridad.

Cuando esté listo para usar el almacén de claves de AWS CloudHSM, deberá conectarlo a su clúster de AWS CloudHSM asociado. Puede conectar y desconectar su almacén de claves personalizado en cualquier momento. Cuando el almacén de claves personalizado está conectado, se pueden crear y utilizar sus claves KMS. Cuando está desconectado, puede ver y administrar el almacén de claves de AWS CloudHSM y sus claves de KMS. Pero no podrá crear claves de KMS nuevas ni usar las claves de KMS en el almacén de claves de AWS CloudHSM en operaciones criptográficas.

Usuario de criptografía de **`kmsuser`**

Para crear y administrar material de claves en el clúster de AWS CloudHSM asociado en su nombre, AWS KMS utiliza un usuario de criptografía (CU) de AWS CloudHSM dedicado en el clúster denominado `kmsuser`. El CU `kmsuser` es una cuenta de CU estándar que se sincroniza de forma automática con todos los HSM del clúster y se guarda en copias de seguridad del clúster.

Antes de crear el almacén de claves de AWS CloudHSM, cree una cuenta de CU `kmsuser` en el clúster de AWS CloudHSM con el comando createUser en cloudhsm_mgmt_util. Luego, cuando cree el almacén de claves de AWS CloudHSM, deberá proporcionar la contraseña de la cuenta de `kmsuser` a AWS KMS. Al conectar el almacén de claves personalizado, AWS KMS inicia sesión en el clúster con el CU `kmsuser` y rota su contraseña. AWS KMS cifra su contraseña de `kmsuser` antes de que se almacene de manera segura. Cuando se gira la contraseña, la nueva contraseña se cifra y se almacena de la misma manera.

AWS KMS conserva la sesión como `kmsuser` siempre y cuando el almacén de claves de AWS CloudHSM esté conectado. No debería usar esta cuenta de CU para otros fines. Sin embargo, conservará el control total de la cuenta del CU `kmsuser`. Podrá buscar los identificadores de las claves propiedad de `kmsuser` en todo momento. Si es necesario, puede desconectar el almacén de claves personalizado, cambiar la contraseña de `kmsuser`, iniciar sesión en el clúster como `kmsuser`, y ver y administrar las claves propiedad de `kmsuser`.

Para obtener instrucciones sobre cómo crear la cuenta del CU `kmsuser`, consulte Crear el usuario de criptografía `kmsuser`.

Claves de KMS en un almacén de claves de AWS CloudHSM

Puede utilizar la AWS KMS o la API de AWS KMS para crear un AWS KMS keys en un almacén de claves de AWS CloudHSM. Utilice la misma técnica que utilizaría en cualquier clave KMS. La

única diferencia es que debe identificar el almacén de claves de AWS CloudHSM y especificar que el origen del material de claves es el clúster de AWS CloudHSM.

Al crear una clave de KMS en un almacén de claves de AWS CloudHSM, AWS KMS crea una clave de KMS en AWS KMS y genera un material de claves simétrico Advanced Encryption Standard (AES) de 256 bits, persistente y no exportable en su clúster asociado. Cuando utiliza la clave de AWS KMS en una operación criptográfica, la operación se realiza en el clúster de AWS CloudHSM mediante la clave de AES basada en el clúster. Aunque AWS CloudHSM es compatible con claves simétricas y asimétricas de distintos tipos, los almacenes de claves de AWS CloudHSM solo admiten claves de cifrado simétrico AES.

Puede ver las claves de KMS en un almacén de claves de AWS CloudHSM en la consola de AWS KMS y usar las opciones de la consola para visualizar el ID del almacén de claves personalizado. También puede usar la DescribeKeyoperación para buscar el ID del almacén de AWS CloudHSM claves y el ID del AWS CloudHSM clúster.

Las claves de KMS de un almacén de claves de AWS CloudHSM funcionan igual que las claves de KMS en AWS KMS. Los usuarios autorizados necesitan los permisos para usar y administrar las claves KMS. Utilice los mismos procedimientos de consola y operaciones de la API para ver y administrar las claves de KMS en un almacén de claves de AWS CloudHSM. Puede habilitar y desactivar claves KMS, crear y usar etiquetas y alias, y configurar y cambiar las políticas de claves y de IAM. Puede utilizar las claves de KMS en un almacén de claves de AWS CloudHSM en operaciones criptográficas y usarlas con servicios integrados de AWS que sean compatibles con el uso de claves administradas por el cliente. Sin embargo, no puede habilitar la rotación automática de claves o importar material de claves en una clave de KMS de un almacén de claves de AWS CloudHSM.

También puede usar el mismo proceso para programar la eliminación de una clave de KMS de un almacén de claves de AWS CloudHSM. Cuando finaliza el periodo de espera, AWS KMS elimina la clave KMS de KMS. Y se esfuerza por eliminar el material de claves para la clave KMS del clúster de AWS CloudHSM asociado. Sin embargo, es posible que deba eliminar el material de claves huérfano manualmente del clúster y de sus copias de seguridad.

Controlar el acceso al almacén de claves de AWS CloudHSM

Utilice las políticas de IAM para controlar el acceso al almacén de claves de AWS CloudHSM y al clúster de AWS CloudHSM. Puede usar las políticas de claves y las políticas de IAM y concesiones para controlar el acceso a las AWS KMS keys en su almacén de claves de AWS CloudHSM. Le

recomendamos que únicamente otorgue a los usuarios, grupos y roles los permisos necesarios para las tareas que es probable que se vayan a realizar.

Temas

- Autorizar a administradores y usuarios del almacén de claves de AWS CloudHSM
- Autorizar a AWS KMS para administrar AWS CloudHSM y recursos de Amazon EC2

Autorizar a administradores y usuarios del almacén de claves de AWS CloudHSM

Al diseñar el almacén de claves de AWS CloudHSM, asegúrese de que las entidades principales que usan y administran el almacén dispongan únicamente de los permisos que necesitan. En la siguiente lista se describen los permisos mínimos necesarios para los administradores y usuarios del almacén de claves de AWS CloudHSM.

- Las entidades principales que crean y administran el almacén de claves de AWS CloudHSM requieren el siguiente permiso para utilizar las operaciones de API del almacén de claves de AWS CloudHSM.
  - `cloudhsm:DescribeClusters`
  - `kms:CreateCustomKeyStore`
  - `kms:ConnectCustomKeyStore`
  - `kms:DeleteCustomKeyStore`
  - `kms:DescribeCustomKeyStores`
  - `kms:DisconnectCustomKeyStore`
  - `kms:UpdateCustomKeyStore`
  - `iam:CreateServiceLinkedRole`
- Las entidades principales que crean y administran el clúster de AWS CloudHSM asociado al almacén de claves de AWS CloudHSM requieren permiso para crear e inicializar un clúster de AWS CloudHSM. Este permiso también les permite crear o utilizar una nube privada virtual (VPC), crear subredes y crear una instancia de Amazon EC2. También es posible que deban crear y eliminar HSM, y administrar copias de seguridad. Para obtener una lista de los permisos necesarios, consulte Administración de identidades y accesos para AWS CloudHSM en la Guía del usuario de AWS CloudHSM.
- Las entidades principales que crean y administran AWS KMS keys del almacén de claves de AWS CloudHSM necesitan los mismos permisos que aquellas que crean y administran las claves de KMS en AWS KMS. La política de claves predeterminada para claves de KMS en un almacén de

claves de AWS CloudHSM es idéntica a la política de claves predeterminada para claves de KMS en AWS KMS. El control de acceso basado en atributos (ABAC), que utiliza etiquetas y alias para controlar el acceso a las claves de KMS, también es efectivo en claves de KMS de almacenes de claves de AWS CloudHSM.

- Las entidades principales que usan las claves de KMS en el almacén de claves de AWS CloudHSM para operaciones criptográficas requieren permiso para realizar la operación criptográfica con la clave de KMS, por ejemplo, kms:Decrypt. Puede proporcionar estos permisos en una política de claves o una política de IAM. Sin embargo, no necesitan más permisos para utilizar una clave de KMS en un almacén de claves de AWS CloudHSM.

Autorizar a AWS KMS para administrar AWS CloudHSM y recursos de Amazon EC2

Para dar soporte a los almacenes de claves de AWS CloudHSM, AWS KMS necesita permiso para obtener información de los clústeres de AWS CloudHSM. También necesita permiso para crear la infraestructura de red que conecta el almacén de claves de AWS CloudHSM con su clúster de AWS CloudHSM. Para obtener estos permisos, AWS KMS crea el rol AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculado al servicio en su. Cuenta de AWS Los usuarios que crean almacenes de claves de AWS CloudHSM deben tener el permiso `iam:CreateServiceLinkedRole` que les permite crear roles vinculados a un servicio.

Temas

- Acerca del rol vinculado a un servicio de AWS KMS
- Creación del rol vinculado a servicios
- Editar la descripción del rol vinculado a un servicio
- Eliminar el rol vinculado a servicios

Acerca del rol vinculado a un servicio de AWS KMS

Un rol vinculado a un servicio es un rol de IAM que otorga permiso a un servicio de AWS para llamar a otros servicios de AWS en su nombre. Se ha diseñado para facilitar el uso de las características de múltiples servicios de AWS integrados sin tener que crear ni actualizar políticas de IAM complejas. Para obtener más información, consulte Uso de roles vinculados a servicios de AWS KMS.

En el AWS CloudHSM caso de los almacenes de claves, AWS KMS crea el rol AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculado al servicio con la política. AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy Esta política concede los siguientes permisos al rol:

- CloudHSM:Describe*: detecta los cambios en el AWS CloudHSM clúster adjunto a su almacén de claves personalizado.
- ec2: CreateSecurityGroup — se utiliza cuando se conecta un almacén de AWS CloudHSM claves para crear el grupo de seguridad que permite el flujo de tráfico de red entre el clúster y el clúster. AWS KMS AWS CloudHSM
- ec2: AuthorizeSecurityGroupIngress — se utiliza cuando se conecta un almacén de AWS CloudHSM claves para permitir el acceso a la red desde AWS KMS la VPC que contiene AWS CloudHSM el clúster.
- ec2: CreateNetworkInterface — se utiliza cuando se conecta un almacén de AWS CloudHSM claves para crear la interfaz de red que se utiliza para la comunicación entre el clúster AWS KMS y el clúster. AWS CloudHSM
- ec2: RevokeSecurityGroupEgress — se utiliza cuando se conecta un almacén de AWS CloudHSM claves para eliminar todas las reglas de salida del grupo de seguridad que lo creó. AWS KMS
- ec2: DeleteSecurityGroup — se utiliza cuando se desconecta un almacén de AWS CloudHSM claves para eliminar los grupos de seguridad que se crearon al conectar el AWS CloudHSM almacén de claves.
- ec2: DescribeSecurityGroups — se usa para monitorear los cambios en el grupo de seguridad que se AWS KMS creó en la VPC que contiene AWS CloudHSM el clúster, de modo AWS KMS que pueda proporcionar mensajes de error claros en caso de fallas.
- ec2: DescribeVpcs — se usa para monitorear los cambios en la VPC que contiene AWS CloudHSM el clúster, de modo AWS KMS que pueda proporcionar mensajes de error claros en caso de fallas.
- ec2: DescribeNetworkAcls — se utiliza para supervisar los cambios en las ACL de la red de la VPC que contiene el AWS CloudHSM clúster, de modo que AWS KMS pueda proporcionar mensajes de error claros en caso de errores.
- ec2: DescribeNetworkInterfaces — se utiliza para supervisar los cambios en las interfaces de red que se AWS KMS crearon en la VPC que contiene AWS CloudHSM el clúster, de modo AWS KMS que puedan proporcionar mensajes de error claros en caso de errores.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "cloudhsm:Describe*",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeVpcs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    }
  ]
}
```

Como el rol AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculado al servicio solo es de confianza`cks.kms.amazonaws.com`, solo AWS KMS puede asumir este rol vinculado al servicio. Este rol está limitado a las operaciones que necesita AWS KMS para ver los clústeres de AWS CloudHSM y para conectar un almacén de claves de AWS CloudHSM con su clúster de AWS CloudHSM asociado. No concede permisos adicionales a AWS KMS. Por ejemplo, AWS KMS no dispone de permiso para crear, administrar o eliminar los clústeres de AWS CloudHSM, los HSM o las copias de seguridad.

Regiones

Al igual que la función de almacenes de AWS CloudHSM claves, el AWSServiceRoleForKeyManagementServiceCustomKeyStoresrol se admite en todas Regiones de AWS partes AWS KMS y está disponible. AWS CloudHSM Para obtener una lista de las Regiones de AWS que admiten cada servicio, consulte AWS Key Management Service Endpoints and Quotas y AWS CloudHSM endpoints and quotas en la Referencia general de Amazon Web Services.

Para obtener más información acerca de cómo los servicios de AWS utilizan los roles vinculados con el servicio, consulte Uso de roles vinculados a servicios en la Guía del usuario de IAM.

Creación del rol vinculado a servicios

AWS KMScrea automáticamente el rol AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculado al servicio en su cuenta Cuenta de AWS al crear un almacén de AWS CloudHSM claves, si el rol aún no existe. No puede crear o volver a crear este rol vinculado a un servicio directamente.

Editar la descripción del rol vinculado a un servicio

No puede editar el nombre del rol o las instrucciones de la política en el rol vinculado a un servicio AWSServiceRoleForKeyManagementServiceCustomKeyStores, aunque sí puede editar la descripción del rol. Para obtener más información, consulte Editar un rol vinculado a un servicio en la Guía del usuario de IAM.

Eliminar el rol vinculado a servicios

AWS KMSno elimina el rol AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculado al servicio de su cuenta, Cuenta de AWS incluso si ha eliminado todos sus almacenes de claves. AWS CloudHSM Aunque actualmente no existe ningún procedimiento para eliminar la función AWSServiceRoleForKeyManagementServiceCustomKeyStoresvinculada al servicio, AWS KMS no la asume ni utiliza sus permisos a menos que tenga almacenes de claves activos. AWS CloudHSM

Administrar un almacén de claves personalizado de CloudHSM

Puede administrar un almacén de claves personalizado desde la AWS Management Console y la API de AWS KMS. Por ejemplo, puede ver un almacén de claves personalizado, editar sus propiedades, conectarlo y desconectarlo de su clúster de AWS CloudHSM asociado y eliminar el almacén de claves personalizado.

Temas

- Crear un almacén de claves de AWS CloudHSM
- Visualización de un almacén de claves de AWS CloudHSM
- Editar la configuración del almacén de claves de AWS CloudHSM
- Conectar y desconectar un almacén de claves de AWS CloudHSM
- Eliminar un almacén de claves de AWS CloudHSM

Crear un almacén de claves de AWS CloudHSM

Puede crear uno o varios almacenes de claves de AWS CloudHSM en la cuenta. Cada almacén de claves de AWS CloudHSM está asociado a un clúster de AWS CloudHSM en la misma Cuenta de AWS y región. Antes de crear un almacén de claves de AWS CloudHSM, debe cumplir los requisitos previos. A continuación, antes de usar el almacén de claves de AWS CloudHSM, deberá conectarlo a su clúster de AWS CloudHSM.

> **Note**
>
> Si intenta crear un almacén de claves de AWS CloudHSM con los mismos valores de propiedad que un almacén de claves de AWS CloudHSM desconectado existente, AWS KMS no crea un nuevo almacén de claves de AWS CloudHSM y no genera ninguna excepción ni muestra ningún error. En cambio, AWS KMS reconoce el duplicado como consecuencia probable de un reintento y devuelve el ID del almacén de claves de AWS CloudHSM existente.

> **Tip**
>
> No tiene que conectar el almacén de claves de AWS CloudHSM inmediatamente. Puede dejarlo desconectado hasta que lo necesite. Sin embargo, para comprobar que se ha configurado correctamente, debería conectarlo, ver su estado de conexión y, a continuación, desconectarlo.

Temas

Cumplir los requisitos previos

Cada almacén de claves de AWS CloudHSM está respaldado por un clúster de AWS CloudHSM. Para crear en un almacén de claves de AWS CloudHSM, especifique un clúster de AWS CloudHSM activo que no esté asociado a otro almacén de claves. También deberá crear un usuario de criptografía (CU) dedicado en los HSM del clúster que AWS KMS podrá utilizar para crear y administrar claves en su nombre.

Antes de crear un almacén de claves de AWS CloudHSM, haga lo siguiente:

Seleccionar un clúster de AWS CloudHSM

Cada almacén de claves de AWS CloudHSM está asociado a exactamente un clúster de AWS CloudHSM. Al crear una AWS KMS keys en el almacén de claves de AWS CloudHSM, AWS KMS

crea los metadatos de la clave de KMS, como el ID y el Nombre de recurso de Amazon (ARN), en AWS KMS. A continuación, crea el material de claves en los HSM del clúster asociado. Puede crear un clúster de AWS CloudHSM nuevo o utilizar uno existente. AWS KMS no requiere acceso exclusivo al clúster.

El clúster de AWS CloudHSM que seleccione estará asociado de forma permanente al almacén de claves de AWS CloudHSM. Después de crear un almacén de claves de AWS CloudHSM, puede cambiar el ID del clúster asociado, pero el clúster que especifique debe compartir un historial de copias de seguridad con el clúster original. Para usar un clúster sin relación, debe crear un almacén de claves de AWS CloudHSM nuevo.

El clúster de AWS CloudHSM que seleccione debe tener las siguientes características:

- El clúster debe estar activo.

  Debe crear el clúster, inicializarlo, instalar el software del cliente de AWS CloudHSM para su plataforma y, a continuación, activarlo. Para obtener instrucciones, consulte Introducción a AWS CloudHSM en la Guía del usuario de AWS CloudHSM.
- El clúster debe estar en la misma cuenta y región que el almacén de claves de AWS CloudHSM. No puede asociar un almacén de claves de AWS CloudHSM en una región con un clúster en otra región. Para crear una infraestructura de claves en varias regiones, debe crear almacenes de claves de AWS CloudHSM y clústeres en cada región.
- El clúster no puede estar asociado con otro almacén de claves personalizado en la misma cuenta y región. Cada almacén de claves de AWS CloudHSM de la cuenta y la región debe estar asociado a un clúster de AWS CloudHSM diferente. No puede especificar un clúster que ya esté asociado a un almacén de claves personalizado o a un clúster que comparte historial de copias de seguridad con un clúster asociado. Los clústers que comparten un historial de copias de seguridad deben tener el mismo certificado del clúster. Para ver el certificado de clúster de un clúster, utilice la AWS CloudHSM consola o la DescribeClustersoperación.

  Si la copia de seguridad de un clúster de AWS CloudHSM en una región diferente, se considera un clúster diferente y puede asociar la copia de seguridad a un almacén de claves personalizado en su región. Sin embargo, las claves KMS de los dos almacenes de claves personalizados no son interoperables, incluso si tienen la misma clave de respaldo. AWS KMS vincula metadatos al texto cifrado para que solo se pueda descifrar mediante la clave KMS que lo cifró.
- El clúster debe configurarse con subredes privadas en al menos dos zonas de disponibilidad de la región. Puesto que AWS CloudHSM no es compatible en todas las zonas de disponibilidad,

le recomendamos que cree subredes privadas en todas las zonas de disponibilidad de la región. No puede volver a configurar las subredes para un clúster existente, pero puede crear un clúster a partir de una copia de seguridad con subredes distintas en la configuración del clúster.

> **Important**
>
> Después de crear el almacén de claves de AWS CloudHSM, no elimine ninguna de las subredes privadas configuradas para su clúster de AWS CloudHSM. Si AWS KMS no puede encontrar todas las subredes de la configuración del clúster, los intentos de conectarse al almacén de claves personalizado producen el error de conexión `SUBNET_NOT_FOUND`. Para obtener más detalles, consulte Cómo arreglar un error de conexión.

- El grupo de seguridad para el clúster (`cloudhsm-cluster-<cluster-id>-sg`) debe incluir las reglas entrantes y salientes que permiten el tráfico TCP en los puertos 2223-2225. El origen de las reglas de entrada y el destino de las reglas de salida deben coincidir con el ID del grupo de seguridad. Estas reglas se establecen de forma predeterminada al crear el clúster. No las elimine ni las cambie.
- El clúster debe tener al menos dos HSM activos en distintas zonas de disponibilidad. Para comprobar la cantidad de HSM, utilice la AWS CloudHSM consola o la DescribeClustersoperación. Si es necesario, puede agregar un HSM.

Buscar el certificado de anclaje de confianza

Al crear un almacén de claves personalizado, deberá cargar un certificado de anclaje de confianza para el clúster de AWS CloudHSM en AWS KMS. AWS KMS necesita dicho certificado para conectar el almacén de claves de AWS CloudHSM al clúster de AWS CloudHSM asociado.

Cada clúster de AWS CloudHSM activo tiene un certificado de anclaje de confianza. Al inicializar el clúster, se genera el certificado. Guárdelo en el archivo `customerCA.crt` y cópielo en alojamientos que se conecten con el clúster.

Crear el usuario de criptografía **`kmsuser`** para AWS KMS

Para administrar el almacén de claves de AWS CloudHSM, AWS KMS inicia sesión en la cuenta del usuario de criptografía `kmsuser` (CU) en el clúster seleccionado. Antes de crear un almacén de claves de AWS CloudHSM, debe crear el CU `kmsuser`. Luego, cuando cree el almacén de claves de AWS CloudHSM, deberá proporcionar la contraseña de `kmsuser` a AWS KMS. Al

conectar el almacén de claves de AWS CloudHSM a su clúster de AWS CloudHSM asociado, AWS KMS inicia sesión como `kmsuser` y rota la contraseña de `kmsuser`.

> **Important**
>
> No especifique la opción `2FA` al crear el CU `kmsuser`. Si lo hace, AWS KMS no podrá iniciar sesión y el almacén de claves de AWS CloudHSM no podrá conectarse a su clúster de AWS CloudHSM. Después de especificar 2FA, ya no podrá deshacer dicha acción. En su lugar, deberá eliminar el CU y crearlo de nuevo.

Para crear el CU `kmsuser`, use el siguiente procedimiento.

1. Inicie cloudhsm_mgmt_util tal como se describe en el tema Getting started with CloudHSM Management Utility (CMU) (Introducción a la Utilidad de administración (CMU) de CloudHSM) de la Guía del usuario de AWS CloudHSM.
2. Utilice el comandocreateUser en cloudhsm_mgmt_util para crear un CU llamado `kmsuser`. La contraseña debe contener entre 7 y 32 caracteres alfanuméricos, distingue entre mayúsculas y minúsculas, y no puede tener caracteres especiales.

   Por ejemplo, el siguiente comando de ejemplo crea un CU `kmsuser` con una contraseña `kmsPswd`.

   ```
   aws-cloudhsm> createUser CU kmsuser kmsPswd
   ```

Creación de un almacén de claves de AWS CloudHSM (consola)

Al crear un almacén de claves de AWS CloudHSM en la AWS Management Console, puede agregar y crear los requisitos previos como parte del flujo de trabajo. Sin embargo, el proceso es más rápido si los compila previamente.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Almacenes de claves personalizados, Almacenes de claves de AWS CloudHSM.

4. Seleccione Crear un almacén de claves.
5. Escriba un nombre fácil de recordar para el almacén de claves personalizado. El nombre debe ser único entre todos los almacenes de claves personalizados de su cuenta.

   > **Important**
   >
   > No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.

6. Seleccione un clúster de AWS CloudHSM para el almacén de claves de AWS CloudHSM. O para crear un clúster de AWS CloudHSM nuevo, elija el enlace Create an AWS CloudHSM cluster (Crear un clúster de).

   El menú muestra los clústeres de AWS CloudHSM de la cuenta y la región no asociados todavía con un almacén de claves de AWS CloudHSM. El clúster debe cumplir los requisitos de asociación con un almacén de claves personalizado.
7. Elija Choose file (Elegir archivo) y cargue el certificado de anclaje de confianza para el clúster de AWS CloudHSM que elija. Este es el archivo `customerCA.crt` que creó al inicializar el clúster.
8. Escriba la contraseña del `kmsuser` usuario de criptografía (CU) que creó en el clúster seleccionado.
9. Seleccione Crear.

Si el proceso se ejecuta correctamente, el nuevo almacén de claves de AWS CloudHSM aparecerá en la lista de almacenes de claves de AWS CloudHSM de la cuenta y la región. Si el procedimiento da error, aparecerá un mensaje de error donde se describe el problema y se explica cómo resolverlo. Si necesita más ayuda, consulte Resolver problemas de un almacén de claves personalizado.

Si intenta crear un almacén de claves de AWS CloudHSM con los mismos valores de propiedad que un almacén de claves de AWS CloudHSM desconectado existente, AWS KMS no crea un nuevo almacén de claves de AWS CloudHSM y no genera ninguna excepción ni muestra ningún error. En cambio, AWS KMS reconoce el duplicado como consecuencia probable de un reintento y devuelve el ID del almacén de claves de AWS CloudHSM existente.

Siguiente: los nuevos almacenes de claves de AWS CloudHSM no se conectan de forma automática. Antes de crear AWS KMS keys en el almacén de claves de AWS CloudHSM, debe conectar el almacén de claves personalizado a su clúster de AWS CloudHSM asociado.

Creación de un almacén de claves de AWS CloudHSM (API)

Puede utilizar la CreateCustomKeyStoreoperación para crear un nuevo almacén de AWS CloudHSM claves asociado a un AWS CloudHSM clúster de la cuenta y la región. En estos ejemplos se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

La operación `CreateCustomKeyStore` requiere los siguientes valores de parámetro.

- CustomKeyStoreName — Un nombre descriptivo para el almacén de claves personalizado que es único en la cuenta.

  > **Important**
  >
  > No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.

- CloudHsmClusterId — El ID de clúster de un AWS CloudHSM clúster que cumple los requisitos de un almacén de AWS CloudHSM claves.
- KeyStorePassword — La contraseña de la cuenta `kmsuser` CU del clúster especificado.
- TrustAnchorCertificate — El contenido del `customerCA.crt` archivo que creó al inicializar el clúster.

En el siguiente ejemplo se usa un ID de clúster ficticio. Antes de ejecutar el comando, reemplácelo por un ID de clúster válido.

```
$ aws kms create-custom-key-store
        --custom-key-store-name ExampleCloudHSMKeyStore \
        --cloud-hsm-cluster-id cluster-1a23b4cdefg \
        --key-store-password kmsPswd \
        --trust-anchor-certificate <certificate-goes-here>
```

Si utiliza la AWS CLI, puede especificar un archivo de certificado de anclaje de confianza en lugar de su contenido. En el siguiente ejemplo, el archivo `customerCA.crt` se encuentra en el directorio raíz.

```
$ aws kms create-custom-key-store
        --custom-key-store-name ExampleCloudHSMKeyStore \
```

```
        --cloud-hsm-cluster-id cluster-1a23b4cdefg \
        --key-store-password kmsPswd \
        --trust-anchor-certificate file://customerCA.crt
```

Si la operación se ejecuta correctamente, `CreateCustomKeyStore` devolverá el ID del almacén de claves personalizado, tal y como se muestra en la siguiente respuesta de ejemplo.

```
{
    "CustomKeyStoreId": cks-1234567890abcdef0
}
```

Si la operación falla, corrija el error que indica la excepción e inténtelo de nuevo. Para obtener ayuda adicional, consulte Resolver problemas de un almacén de claves personalizado.

Si intenta crear un almacén de claves de AWS CloudHSM con los mismos valores de propiedad que un almacén de claves de AWS CloudHSM desconectado existente, AWS KMS no crea un nuevo almacén de claves de AWS CloudHSM y no genera ninguna excepción ni muestra ningún error. En cambio, AWS KMS reconoce el duplicado como consecuencia probable de un reintento y devuelve el ID del almacén de claves de AWS CloudHSM existente.

Siguiente: para usar el almacén de claves de AWS CloudHSM, conéctelo a su clúster de AWS CloudHSM.

Visualización de un almacén de claves de AWS CloudHSM

Puede ver los almacenes de AWS CloudHSM claves de cada cuenta y región mediante la AWS KMS consola o la DescribeCustomKeyStoresoperación.

Véase también:

- Visualización de un almacén de claves externo
- Consultar las claves de KMS en un almacén de claves de AWS CloudHSM
- Registrar llamadas a la AWS KMS API con AWS CloudTrail

Temas

- Visualización de un almacén de claves de AWS CloudHSM (consola)
- Visualización de un almacén de claves de AWS CloudHSM (API)

Visualización de un almacén de claves de AWS CloudHSM (consola)

Al consultar los almacenes de claves de AWS CloudHSM en la AWS Management Console, verá lo siguiente:

- El nombre y el ID del almacén de claves personalizado
- El ID del clúster de AWS CloudHSM asociado
- El número de HSM en el clúster
- El estado de conexión actual

El valor (Status) del estado de conexión Disconnected (Desconectado) indica que el almacén de claves personalizado es nuevo y que no se ha conectado nunca, o que se ha desconectado de su clúster de AWS CloudHSM de forma intencional. Sin embargo, si los intentos de usar una clave KMS en un almacén de claves personalizado no son fructíferos, puede deberse a un problema con el almacén de claves personalizado o su clúster de AWS CloudHSM. Para obtener ayuda, consulte ¿Cómo arreglar una clave KMS que produce error?.

Para ver los almacenes de claves de AWS CloudHSM de una cuenta y región determinados, use el siguiente procedimiento.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Almacenes de claves personalizados, Almacenes de claves de AWS CloudHSM.

Para personalizar la pantalla, haga clic en el icono de engranaje que aparece por debajo del botón Create key store (Crear almacén de claves).

Visualización de un almacén de claves de AWS CloudHSM (API)

Para ver sus almacenes de AWS CloudHSM claves, utilice la DescribeCustomKeyStoresoperación. De forma predeterminada, esta operación devuelve los almacenes de claves personalizados de la cuenta y región. Pero puede usar el parámetro `CustomKeyStoreId` o `CustomKeyStoreName` (pero no ambos) para limitar el resultado de un almacén de claves personalizado determinado. Para los almacenes de claves de AWS CloudHSM, el resultado consta de un ID y nombre del almacén

de claves personalizado, el tipo del almacén de claves personalizado, el ID del clúster de AWS CloudHSM asociado y el estado de conexión. Si el estado de conexión indica un error, el resultado también incluirá un código de error que describe el motivo del error.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Por ejemplo, el siguiente comando devuelve todos los almacenes de claves personalizados de la cuenta y la región. Puede usar los parámetros `Limit` y `Marker` para desplazarse por los almacenes de claves personalizados del resultado.

```
$ aws kms describe-custom-key-stores
```

El siguiente comando de ejemplo usa el parámetro `CustomKeyStoreName` para obtener únicamente el almacén de claves personalizado con el nombre fácil de recordar `ExampleCloudHSMKeyStore`. Puede usar el parámetro `CustomKeyStoreName` o `CustomKeyStoreId` (pero no ambos) en cada comando.

El siguiente resultado de ejemplo muestra un almacén de claves de AWS CloudHSM conectado a su clúster de AWS CloudHSM.

> **Note**
>
> El campo `CustomKeyStoreType` se agregó a la respuesta `DescribeCustomKeyStores` para distinguir los almacenes de claves de AWS CloudHSM de los almacenes de claves externos.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleCloudHSMKeyStore
{
   "CustomKeyStores": [
      {
         "CloudHsmClusterId": "cluster-1a23b4cdefg",
         "ConnectionState": "CONNECTED",
         "CreationDate": "1.499288695918E9",
         "CustomKeyStoreId": "cks-1234567890abcdef0",
         "CustomKeyStoreName": "ExampleCloudHSMKeyStore",
         "CustomKeyStoreType": "AWS_CLOUDHSM",
         "TrustAnchorCertificate": "<certificate appears here>"
      }
```

```
    ]
}
```

Un `ConnectionState` `Disconnected` indica que no se ha conectado nunca un almacén de claves personalizado o que se ha desconectado de su clúster de AWS CloudHSM de forma intencionada. Sin embargo, si los intentos de usar una clave de KMS en un almacén de claves de AWS CloudHSM conectado no son fructíferos, puede deberse a un problema con el almacén de claves de AWS CloudHSM o su clúster de AWS CloudHSM. Para obtener ayuda, consulte ¿Cómo arreglar una clave KMS que produce error?.

Si el `ConnectionState` del almacén de claves personalizado es `FAILED`, la respuesta `DescribeCustomKeyStores` incluirá un elemento `ConnectionErrorCode` que explica el motivo del error.

Por ejemplo, en el resultado siguiente, el valor `INVALID_CREDENTIALS` indica que la conexión del almacén de claves personalizado ha fallado porque la contraseña de `kmsuser` no es válida. Para obtener ayuda con esto y los errores de conexión, consulte Resolver problemas de un almacén de claves personalizado.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      {
         "CloudHsmClusterId": "cluster-1a23b4cdefg",
         "ConnectionErrorCode": "INVALID_CREDENTIALS",
         "ConnectionState": "FAILED",
         "CustomKeyStoreId": "cks-1234567890abcdef0",
         "CustomKeyStoreName": "ExampleCloudHSMKeyStore",
         "CustomKeyStoreType": "AWS_CLOUDHSM",
         "CreationDate": "1.499288695918E9",
         "TrustAnchorCertificate": "<certificate appears here>"
      }
   ]
}
```

Editar la configuración del almacén de claves de AWS CloudHSM

Puede modificar la configuración de un almacén de claves de AWS CloudHSM existente. El almacén de claves personalizado debe estar desconectado de su clúster de AWS CloudHSM.

Para editar la configuración del almacén de claves de AWS CloudHSM:

1. Desconecte el almacén de claves personalizado de su clúster de AWS CloudHSM. Mientras el almacén de claves personalizado esté desconectado, no podrá crear AWS KMS keys (claves KMS) en el almacén de claves personalizado y no podrán usar las claves KMS que contiene en operaciones criptográficas.
2. Edite una o más de las configuraciones del almacén de claves de AWS CloudHSM.
3. Vuelva a conectar el almacén de claves personalizado a su clúster de AWS CloudHSM.

Puede editar la siguiente configuración en un almacén de claves personalizado:

El nombre fácil de recordar del almacén de claves personalizado.

Escriba un nuevo nombre fácil de recordar. El nuevo nombre debe ser único entre todos los almacenes de claves personalizados de su Cuenta de AWS.

> **Important**
>
> No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.

El ID del clúster de AWS CloudHSM asociado.

Edite este valor para sustituir un clúster de AWS CloudHSM relacionado por el original. Puede utilizar esta característica para reparar un almacén de claves personalizado si se daña o elimina su clúster de AWS CloudHSM.

Especifique un clúster de AWS CloudHSM que comparta un historial de copias de seguridad con el clúster original y cumpla los requisitos de asociación con un almacén de claves personalizado, incluidos dos HSM activos en zonas de disponibilidad distintas. Los clústers que comparten un historial de copias de seguridad deben tener el mismo certificado del clúster. Para ver el certificado de clúster de un clúster, utilice la DescribeClustersoperación. No puede usar la característica de edición para asociar el almacén de claves personalizado con un clúster de AWS CloudHSM sin relación.

La contraseña actual del **`kmsuser`** usuario de criptografía (CU).

Le indica a AWS KMS la contraseña actual del CU `kmsuser` en el clúster de AWS CloudHSM. Esta acción no cambia la contraseña del CU `kmsuser` en el clúster de AWS CloudHSM.

Si cambia la contraseña del CU `kmsuser` en el clúster de AWS CloudHSM, use esta característica para comunicarle a AWS KMS la nueva contraseña de `kmsuser`. De lo contrario, AWS KMS no podrá iniciar sesión en el clúster y todos los intentos de conexión del almacén de claves personalizado al clúster darán error.

Temas

Editar un almacén de claves de AWS CloudHSM (consola)

Al editar un almacén de claves de AWS CloudHSM, puede cambiar cualquiera de los valores configurables.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Almacenes de claves personalizados, Almacenes de claves de AWS CloudHSM.
4. Elija la fila del almacén de claves de AWS CloudHSM que quiere editar.

   Si el valor de la columna Estado de conexión no está desconectado, debe desconectar el almacén de claves personalizado antes de poder editarlo. [En el menú Key store actions (Acciones del almacén de claves), seleccione Disconnect (Desconectar)].

   Mientras un almacén de claves de AWS CloudHSM esté desconectado, podrá administrar el almacén de claves de AWS CloudHSM y sus claves de KMS, pero no podrá crear ni usar las claves de KMS en el almacén de claves de AWS CloudHSM.
5. Desde el menú Key store actions (Acciones del almacén de claves), seleccione Edit (Editar).
6. Realice una o más de las siguientes acciones.

   - Escriba un nuevo nombre fácil de recordar para el almacén de claves personalizado.
   - Escriba el ID del clúster de un clúster de AWS CloudHSM relacionado.
   - Escriba la contraseña actual del usuario de criptografía `kmsuser` en el clúster de AWS CloudHSM asociado.

7. Seleccione Guardar.

   Si el procedimiento se ejecuta correctamente, aparecerá un mensaje donde se describe la configuración que ha editado. Si el procedimiento da error, aparecerá un mensaje de error donde se describe el problema y se explica cómo resolverlo. Si necesita más ayuda, consulte Resolver problemas de un almacén de claves personalizado.
8. Vuelva a conectar el almacén de claves personalizado.

   Para utilizar el almacén de claves de AWS CloudHSM deberá volverlo a conectar después de editarlo. Puede dejar el almacén de claves de AWS CloudHSM desconectado. Pero mientras esté desconectado, no podrá crear las claves de KMS en el almacén de claves de AWS CloudHSM ni usar las claves de KMS del almacén de claves de AWS CloudHSM en operaciones criptográficas.

Editar un almacén de claves de AWS CloudHSM (API)

Para cambiar las propiedades de un almacén de AWS CloudHSM claves, utilice la UpdateCustomKeyStoreoperación. Puede cambiar varias propiedades de un almacén de claves personalizado en el mismo comando. Si la operación se realiza correctamente, AWS KMS devuelve una respuesta HTTP 200 y un objeto JSON sin propiedades. Para comprobar que los cambios son efectivos, utilice la DescribeCustomKeyStoresoperación.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Comience por DisconnectCustomKeyStoredesconectar el almacén de claves personalizado de su AWS CloudHSM clúster. Reemplace el ID del almacén de claves personalizado de ejemplo, cks-1234567890abcdef0, por un ID real.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

En el primer ejemplo, UpdateCustomKeyStorese utiliza para cambiar el nombre descriptivo del almacén de AWS CloudHSM claves a`DevelopmentKeys`. El comando utiliza el parámetro `CustomKeyStoreId` para especificar el almacén de claves de AWS CloudHSM y `CustomKeyStoreName` para especificar el nuevo nombre del almacén de claves personalizado.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-
custom-key-store-name DevelopmentKeys
```

El siguiente ejemplo cambia el clúster asociado con el almacén de claves de AWS CloudHSM por otra copia de seguridad del mismo clúster. El comando utiliza el parámetro `CustomKeyStoreId` para identificar el almacén de claves de AWS CloudHSM y el parámetro `CloudHsmClusterId` para especificar el nuevo ID del clúster.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --cloud-hsm-cluster-id cluster-1a23b4cdefg
```

El siguiente ejemplo indica a AWS KMS que la contraseña actual de `kmsuser` es `ExamplePassword`. El comando utiliza el parámetro `CustomKeyStoreId` para identificar el almacén de claves de AWS CloudHSM y el parámetro `KeyStorePassword` para especificar la contraseña actual.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --key-store-password ExamplePassword
```

El comando final vuelve a conectar el almacén de claves de AWS CloudHSM a su clúster de AWS CloudHSM. Puede dejar el almacén de claves personalizado desconectado, pero deberá conectarlo antes de crear claves KMS nuevas o para utilizar las claves KMS existentes para operaciones criptográficas. Reemplace el ID del almacén de claves personalizado de ejemplo por un ID real.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Conectar y desconectar un almacén de claves de AWS CloudHSM

Los nuevos almacenes de claves de AWS CloudHSM no están conectados. Antes de crear y utilizar AWS KMS keys en el almacén de claves de AWS CloudHSM, debe conectarlo a su clúster de AWS CloudHSM asociado. Puede conectar y desconectar su almacén de claves de AWS CloudHSM en cualquier momento y ver su estado de conexión.

No es obligatorio conectar el almacén de claves de AWS CloudHSM. Puede dejar un almacén de claves de AWS CloudHSM desconectado de forma indefinida y conectarlo únicamente cuando tenga que usarlo. Sin embargo, le recomendamos que compruebe la conexión de forma periódica para verificar que la configuración es correcta y que se puede conectar.

> **Note**
>
> Los almacenes de claves de AWS CloudHSM tienen un estado de conexión `DISCONNECTED` solo cuando el almacén de claves nunca se ha conectado o lo desconecta explícitamente.

Si el estado de conexión del almacén de claves de AWS CloudHSM es `CONNECTED`, pero tiene problemas para usarlo, asegúrese de que su clúster de AWS CloudHSM asociado está activo y contiene al menos un HSM activo. Si desea ayuda con las conexiones que dan error, consulte the section called “Resolver problemas de un almacén de claves personalizado”.

Temas

Conectar un almacén de claves de AWS CloudHSM

Al conectar un almacén de claves de AWS CloudHSM, AWS KMS busca el clúster de AWS CloudHSM asociado, lo conecta al clúster, inicia sesión en el cliente de AWS CloudHSM como usuario de criptografía `kmsuser` (CU) y rota la contraseña `kmsuser`. AWS KMS mantiene iniciada la sesión en el cliente de AWS CloudHSM siempre y cuando el almacén de claves de AWS CloudHSM esté conectado.

Para establecer la conexión, AWS KMS crea un grupo de seguridad llamado `kms-<custom key store ID>` en la nube virtual privada (VPC) del clúster. El grupo de seguridad tiene una única regla que permite el tráfico de entrada desde el grupo de seguridad del clúster. AWS KMS también crea una interfaz de red elástica (ENI) en cada zona de disponibilidad de la subred privada para el clúster. AWS KMS agrega las ENI al grupo de seguridad `kms-<cluster ID>` y al grupo de seguridad del clúster. La descripción de cada ENI es `KMS managed ENI for cluster <cluster-ID>`.

El proceso de conexión puede tardar bastante en completarse, unos 20 minutos.

Antes de conectar el almacén de claves de AWS CloudHSM, compruebe que cumple los requisitos.

- Su clúster de AWS CloudHSM asociado debe incluir al menos un HSM activo. Para encontrar el número de HSM en el clúster, visualice el clúster en la AWS CloudHSM consola o utilice la DescribeClustersoperación. Si es necesario, puede agregar un HSM.

- El clúster debe tener una cuenta de usuario de criptografía `kmsuser` (CU), pero ese CU no se puede registrar en el clúster cuando conecta el almacén de claves de AWS CloudHSM. Para obtener ayuda con el cierre de sesión, consulte Cómo cerrar sesión y volver a conectar.
- El estado de conexión del almacén de claves de AWS CloudHSM no puede ser `DISCONNECTING` ni `FAILED`. Para ver el estado de la conexión, utilice la AWS KMS consola o la DescribeCustomKeyStoresrespuesta. Si el estado de conexión es `FAILED`, desconecte el almacén de claves personalizado, resuelva el problema y conéctelo de nuevo.

Si desea ayuda con las conexiones que dan error, consulte Cómo arreglar un error de conexión.

Cuando el almacén de claves de AWS CloudHSM esté conectado, puede crear las claves de KMS en él y usar las claves de KMS existentes en operaciones criptográficas.

Desconectar un almacén de claves de AWS CloudHSM

Al desconectar un almacén de claves de AWS CloudHSM, AWS KMS cierra sesión en el cliente de AWS CloudHSM, se desconecta del clúster de AWS CloudHSM asociado y elimina la infraestructura de red creada para respaldar la conexión.

Mientras un almacén de claves de AWS CloudHSM esté desconectado, podrá administrar el almacén de claves de AWS CloudHSM y sus claves de KMS, pero no podrá crear ni usar las claves de KMS en el almacén de claves de AWS CloudHSM. El estado de conexión del almacén de claves es `DISCONNECTED` y el estado de clave de las claves de KMS en el almacén de claves personalizado es `Unavailable`, a menos que sean `PendingDeletion`. Puede volver a conectar el almacén de claves de AWS CloudHSM en cualquier momento.

Al desconectar un almacén de claves personalizado, las claves de KMS del almacén de claves quedan inutilizables de inmediato (sujeto a posible coherencia). Sin embargo, los recursos cifrados con claves de datos protegidas por la clave de KMS no se ven afectados hasta que se vuelva a utilizar la clave de KMS, por ejemplo, para descifrar la clave de datos. Este problema afecta a los Servicios de AWS, muchos de los cuales utilizan claves de datos para proteger sus recursos. Para obtener más detalles, consulte Cómo afectan las claves de KMS obsoletas a las claves de datos.

> **Note**
>
> Mientras un almacén de claves personalizado esté desconectado, todos los intentos de crear claves KMS en el almacén de claves personalizado o de usar claves KMS existentes en

operaciones criptográficas fallarán. Esta acción puede impedir que los usuarios almacenen y accedan a datos confidenciales.

Para realizar una mejor estimación del efecto de desconectar el almacén de claves personalizado, identifique las claves de KMS en el almacén de claves personalizado y determine su uso en el pasado.

Puede desconectar el almacén de claves de AWS CloudHSM por los siguientes motivos:

- Para rotar la contraseña **`kmsuser`**. AWS KMS cambia la contraseña de `kmsuser` cada vez que se conecta al clúster de AWS CloudHSM. Para forzar la rotación de contraseñas, desconecte y vuelva a conectar.
- Para auditar el material de claves para las claves KMS en el clúster de AWS CloudHSM. Al desconectar el almacén de claves personalizado, AWS KMS cierra la sesión de la cuenta del `kmsuser` usuario de criptografía en el cliente de AWS CloudHSM. Esto le permite iniciar sesión en el clúster con el CU `kmsuser` y auditar y administrar el material de claves para la clave KMS.
- Para desactivar de inmediato todas las claves de KMS en un almacén de claves de AWS CloudHSM Puede deshabilitar y volver a habilitar las claves KMS en un almacén de AWS CloudHSM claves mediante la DisableKeyoperación AWS Management Console o. Estas operaciones se completan rápidamente, pero actúan en una clave KMS cada vez. La desconexión inmediata del almacén de claves de AWS CloudHSM cambia el estado de clave de todas las claves de KMS del almacén de claves de AWS CloudHSM a `Unavailable`, lo que evita que se utilicen en operaciones criptográficas.
- Para reparar un error en la conexión. Si el intento de conexión al almacén de claves de AWS CloudHSM falla (el estado de la conexión del almacén de claves personalizado es `FAILED`), deberá desconectar el almacén de claves de AWS CloudHSM antes de intentar conectarlo de nuevo.

Conectar un almacén de claves de AWS CloudHSM (consola)

Para conectar un almacén de claves de AWS CloudHSM en la AWS Management Console, primero deberá seleccionar el almacén de datos de AWS CloudHSM en la página Custom key stores (Almacenes de claves personalizados). El proceso de conexión puede tardar hasta 20 minutos en completarse.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Almacenes de claves personalizados, Almacenes de claves de AWS CloudHSM.
4. Elija la fila del almacén de claves de AWS CloudHSM que quiere conectar.

   Si el estado de conexión del almacén de AWS CloudHSM claves es Fallido, debe desconectar el almacén de claves personalizado antes de conectarlo.
5. En el menú Key store actions (Acciones del almacén de claves), seleccione Connect (Conectar).

AWS KMS empieza el proceso de conexión del almacén de claves personalizado. Encuentra el clúster del AWS CloudHSM asociado, genera la infraestructura de red necesaria, se conecta a él, inicia sesión en el clúster de AWS CloudHSM con el CU `kmsuser` y rota la contraseña `kmsuser`. Cuando se complete la operación, el estado de la conexión cambiará a Conectado.

Si la operación falla, aparecerá un mensaje de error que describe el motivo del error. Antes de intentar conectarse de nuevo, vea el estado de conexión del almacén de claves de AWS CloudHSM. Si se produce un error, debe desconectar el almacén de claves personalizado antes de volver a conectarlo. Si necesita más ayuda, consulte Resolver problemas de un almacén de claves personalizado.

Siguiente: the section called “Crear claves de KMS en un almacén de claves de AWS CloudHSM”.

Conectar un almacén de claves personalizado (API)

Para conectar un almacén de AWS CloudHSM claves desconectado, utilice la ConnectCustomKeyStoreoperación. El clúster de AWS CloudHSM asociado debe incluir al menos un HSM activo y su estado de conexión no puede ser `FAILED`.

El proceso de conexión puede tardar bastante en completarse, unos 20 minutos. A menos que el error sea rápido, la operación devuelve una respuesta HTTP 200 y un objeto JSON sin propiedades. Sin embargo, esta respuesta inicial no indica que la conexión se haya realizado correctamente. Para determinar el estado de conexión del almacén de claves personalizado, consulte la DescribeCustomKeyStoresrespuesta.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Para identificar el almacén de claves de AWS CloudHSM, use el ID del almacén de claves personalizado. Puede encontrar el ID en la página de almacenes de claves personalizados de la consola o mediante la DescribeCustomKeyStoresoperación sin parámetros. Antes de ejecutar este ejemplo, reemplace el ID de ejemplo por uno válido.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Para comprobar que el almacén de AWS CloudHSM claves está conectado, utilice la DescribeCustomKeyStoresoperación. De forma predeterminada, esta operación devuelve los almacenes de claves personalizados de su cuenta y región. Pero puede usar el parámetro `CustomKeyStoreId` o `CustomKeyStoreName` (pero no ambos) para limitar la respuesta a almacenes de claves personalizados determinados. El valor `ConnectionState` de `CONNECTED` indica que el almacén de claves personalizado está conectado a su clúster de AWS CloudHSM.

> **Note**
>
> El campo `CustomKeyStoreType` se agregó a la respuesta `DescribeCustomKeyStores` para distinguir los almacenes de claves de AWS CloudHSM de los almacenes de claves externos.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleCloudHSMKeyStore",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "CustomKeyStoreType": "AWS_CLOUDHSM",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "CONNECTED"
   ],
}
```

Si el valor `ConnectionState` da error, el elemento `ConnectionErrorCode` indicará el motivo del error. En este caso, AWS KMS no ha encontrado ningún clúster de AWS CloudHSM en la cuenta

con el ID de clúster `cluster-1a23b4cdefg`. Si ha eliminado el clúster, puede restaurarlo a partir de una copia de seguridad del clúster original y, a continuación, editar el ID del clúster para el almacén de claves personalizado. Para obtener ayuda sobre cómo responder a un código de error de conexión, consulte Cómo arreglar un error de conexión.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "CustomKeyStoreType": "AWS_CLOUDHSM",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "FAILED"
      "ConnectionErrorCode": "CLUSTER_NOT_FOUND"
   ],
}
```

Siguiente: Crear claves de KMS en un almacén de claves de AWS CloudHSM.

Desconectar un almacén de claves de AWS CloudHSM (consola)

Para desconectar un almacén de claves de AWS CloudHSM conectado en la AWS Management Console, primero deberá seleccionar el almacén de claves de AWS CloudHSM en la página Custom Key Stores (Almacenes de claves personalizados).

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Almacenes de claves personalizados, Almacenes de claves de AWS CloudHSM.
4. Elija la fila del almacén de claves externo que desee desconectar.
5. En el menú Key store actions (Acciones del almacén de claves), seleccione Disconnect (Desconectar).

Cuando se complete la operación, el estado de la conexión cambiará de Desconectada a Desconectada. Si la operación da error, aparecerá un mensaje de error donde se describe el

problema y se explica cómo resolverlo. Si necesita más ayuda, consulte Resolver problemas de un almacén de claves personalizado.

Desconectar un almacén de claves de AWS CloudHSM (API)

Para desconectar un almacén de AWS CloudHSM claves conectado, utilice la DisconnectCustomKeyStoreoperación. Si la operación se realiza correctamente, AWS KMS devuelve una respuesta HTTP 200 y un objeto JSON sin propiedades.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Este ejemplo desconecta un almacén de claves de AWS CloudHSM. Antes de ejecutar este ejemplo, reemplace el ID de ejemplo por uno válido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Para comprobar que el almacén de AWS CloudHSM claves está desconectado, utilice la DescribeCustomKeyStoresoperación. De forma predeterminada, esta operación devuelve los almacenes de claves personalizados de su cuenta y región. Pero puede usar el parámetro `CustomKeyStoreId` o `CustomKeyStoreName` (pero no ambos) para limitar la respuesta a almacenes de claves personalizados determinados. El valor `ConnectionState` de `DISCONNECTED` indica que el almacén de claves de AWS CloudHSM no está conectado a su clúster de AWS CloudHSM.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionState": "DISCONNECTED",
      "CreationDate": "1.499288695918E9",
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "CustomKeyStoreType": "AWS_CLOUDHSM",
      "TrustAnchorCertificate": "<certificate string appears here>"
   ],
}
```

Eliminar un almacén de claves de AWS CloudHSM

Al eliminar un almacén de claves de AWS CloudHSM, AWS KMS elimina de KMS todos los metadatos del almacén de claves de AWS CloudHSM, incluida información sobre su asociación con un clúster de AWS CloudHSM. Esta operación no afecta al clúster de AWS CloudHSM, sus HSM o sus usuarios. Puede crear un nuevo almacén de claves de AWS CloudHSM asociado al mismo clúster de AWS CloudHSM, pero no se puede deshacer la operación de eliminación.

Solo puede eliminar un almacén de claves de AWS CloudHSM desconectado de su clúster de AWS CloudHSM y que no incluye AWS KMS keys. Antes de eliminar un almacén de claves personalizado, haga lo siguiente.

- Compruebe que no necesitará nunca utilizar ninguna de las claves KMS del almacén de claves para ninguna operación criptográfica. A continuación, programe la eliminación de todas las claves KMS del almacén de claves. Para obtener ayuda en la búsqueda de las claves de KMS en un almacén de claves de AWS CloudHSM, consulte Buscar las claves de KMS en un almacén de claves de AWS CloudHSM.
- Confirme que se han eliminado todas las claves KMS. Para ver las claves de KMS de un almacén de claves de AWS CloudHSM, consulte Consultar las claves de KMS en un almacén de claves de AWS CloudHSM.
- Desconecte el almacén de claves de AWS CloudHSM de su clúster de AWS CloudHSM.

En lugar de eliminar el almacén de claves de AWS CloudHSM, considere desconectarlo del clúster de AWS CloudHSM que tiene asociado. Mientras un almacén de claves de AWS CloudHSM esté desconectado, puede administrar el almacén de claves de AWS CloudHSM y sus AWS KMS keys. Pero no puede crear ni usar claves de KMS en el almacén de claves de AWS CloudHSM. Puede volver a conectar el almacén de claves de AWS CloudHSM en cualquier momento.

Temas

- Eliminar un almacén de claves de AWS CloudHSM (consola)
- Eliminar un almacén de claves de AWS CloudHSM (API)

Eliminar un almacén de claves de AWS CloudHSM (consola)

Para eliminar un almacén de claves de AWS CloudHSM en la AWS Management Console, primero deberá seleccionar dicho almacén de claves de AWS CloudHSM en la página Custom key stores (Almacenes de claves personalizados).

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Almacenes de claves personalizados, Almacenes de claves de AWS CloudHSM.
4. Busque la fila que representa el almacén de claves de AWS CloudHSM que quiere eliminar. Si el estado de conexión del almacén de AWS CloudHSM claves no es Desconectado, debe desconectar el almacén de AWS CloudHSM claves antes de eliminarlo.
5. En el menú Key store actions (Acciones del almacén de claves), seleccione Delete (Eliminar).

Cuando la operación finalice, aparecerá un mensaje de confirmación y el almacén de claves de AWS CloudHSM ya no aparecerá en la lista de almacenes de claves. Si la operación da error, aparecerá un mensaje de error donde se describe el problema y se explica cómo resolverlo. Si necesita más ayuda, consulte Resolver problemas de un almacén de claves personalizado.

Eliminar un almacén de claves de AWS CloudHSM (API)

Para eliminar un almacén de AWS CloudHSM claves, utilice la DeleteCustomKeyStoreoperación. Si la operación se realiza correctamente, AWS KMS devuelve una respuesta HTTP 200 y un objeto JSON sin propiedades.

Para empezar, compruebe que el almacén de claves de AWS CloudHSM no contenga AWS KMS keys. No puede eliminar un almacén de claves personalizado que contenga claves KMS. El primer comando de ejemplo utiliza ListKeysy DescribeKeybusca AWS KMS keys en el almacén de claves con el identificador de almacén de AWS CloudHSM claves personalizado *cks-1234567890abcdef0*. En ese caso, el comando no devuelve ninguna clave KMS. Si es así, utilice la ScheduleKeyDeletionoperación para programar la eliminación de cada una de las claves del KMS.

Bash

```
for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text) ;
do aws kms describe-key --key-id $key |
grep '"CustomKeyStoreId": "cks-1234567890abcdef0"' --context 100; done
```

PowerShell

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreId -eq
 'cks-1234567890abcdef0'
```

A continuación, desconecte el almacén de claves de AWS CloudHSM. Este comando de ejemplo utiliza la DisconnectCustomKeyStoreoperación para desconectar un almacén de AWS CloudHSM claves de su AWS CloudHSM clúster. Antes de ejecutar este comando, reemplace el ID del almacén de claves personalizado de ejemplo por uno válido.

Bash

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Disconnect-KMSCustomKeyStore -CustomKeyStoreId cks-1234567890abcdef0
```

Una vez desconectado el almacén de claves personalizado, puede utilizar la DeleteCustomKeyStoreoperación para eliminarlo.

Bash

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Remove-KMSCustomKeyStore -CustomKeyStoreId cks-1234567890abcdef0
```

Administrar claves de KMS en un almacén de claves de CloudHSM

Puede crear, ver, administrar, usar y programar la eliminación de AWS KMS keys en un almacén de claves de AWS CloudHSM. Los procedimientos son muy similares a los que usaría para otras claves de KMS. La única diferencia es que debe especificar un almacén de claves de AWS CloudHSM al crear la clave de KMS. A continuación, AWS KMS crea un material de claves no extraíble para la clave de KMS en el clúster de AWS CloudHSM que está asociado al almacén de claves de

AWS CloudHSM. Al utilizar una clave de KMS en un almacén de claves de AWS CloudHSM, las operaciones criptográficas se realizan en los HSM del clúster.

Características admitidas

Además de los procedimientos tratados en esta sección, puede hacer lo siguiente con las claves de KMS en un almacén de claves de AWS CloudHSM:

- Utilice políticas de claves, políticas de IAM y concesiones para autorizar el acceso a las claves de KMS.
- Habilite y deshabilite las claves de KMS.
- Asigne etiquetas, cree alias y utilice el control de acceso basado en atributos (ABAC) para autorizar el acceso a las claves de KMS.
- Use las claves KMS en operaciones criptográficas, incluido cifrar, descifrar, volver a cifrar y generar claves de datos.
- Utilice las claves de KMS con servicios de AWS que se integran con AWS KMS y que admiten las claves administradas por el cliente.
- Realice un seguimiento del uso de sus claves de KMS en AWS CloudTraillos registros y en las herramientas CloudWatch de supervisión de Amazon.

Características no admitidas

- Los almacenes de claves personalizados de AWS CloudHSM solo admiten claves de KMS de cifrado simétrico. No puede crear claves de KMS con HMAC, claves de KMS asimétricas ni pares de claves de datos asimétricas en un almacén de claves de AWS CloudHSM.
- No se puede importar material de claves a una clave de KMS en un almacén de claves de AWS CloudHSM. AWS KMS genera el material de claves para la clave de KMS en el clúster de AWS CloudHSM.
- No puede habilitar ni deshabilitar la rotación automática del material clave para una clave de KMS en un almacén de claves de AWS CloudHSM.

Temas

- Crear claves de KMS en un almacén de claves de AWS CloudHSM
- Consultar las claves de KMS en un almacén de claves de AWS CloudHSM
- Usar las claves KMS en un almacén de claves de AWS CloudHSM

- Buscar las claves KMS y material de claves
- Programar la eliminación de claves de KMS de un almacén de claves de AWS CloudHSM

Crear claves de KMS en un almacén de claves de AWS CloudHSM

Después de crear un almacén de claves de AWS CloudHSM, puede crear AWS KMS keys en su almacén de claves. Deben ser claves KMS de cifrado simétricas con el material de claves que AWS KMS genera. No puede crear claves KMS asimétricas, claves KMS HMAC ni claves KMS con material clave importado en un almacén de claves personalizado. Además, no puede utilizar claves KMS de cifrado simétricas en un almacén de claves personalizado para generar pares de claves de datos asimétricos.

Para crear una clave de KMS en un almacén de claves de AWS CloudHSM, dicho almacén de AWS CloudHSM debe estar conectado a su clúster de AWS CloudHSM asociado y el clúster debe contener al menos dos HSM activos en zonas de disponibilidad distintas. Para buscar el estado de conexión y el número de HSM, consulte la página de almacenes de claves de AWS CloudHSM en la AWS Management Console. Cuando utilice las operaciones de la API, utilice la DescribeCustomKeyStoresoperación para comprobar que el almacén de AWS CloudHSM claves esté conectado. Para comprobar la cantidad de HSM activos en el clúster y sus zonas de disponibilidad, utilice la AWS CloudHSM DescribeClustersoperación.

Al crear una clave de KMS en su almacén de claves de AWS CloudHSM, AWS KMS crea la clave de KMS en AWS KMS. Pero crea el material de claves para la clave KMS en el clúster de AWS CloudHSM asociado. En concreto, AWS KMS inicia sesión en el clúster con el `kmsuser` CU que creó. A continuación crea una clave simétrica Advanced Encryption Standard (AES) de 256 bits, no extraíble y persistente en el clúster. AWS KMS establece el valor del atributo de la etiqueta de claves, que solo es visible en el clúster, en el Nombre de recurso de Amazon (ARN) de la clave KMS.

Cuando el comando se ejecuta correctamente, el estado de clave de la nueva clave KMS es `Enabled` y su origen es `AWS_CLOUDHSM`. No se puede cambiar el origen de ninguna clave KMS después de crearla. Al ver una clave de KMS en un almacén de AWS CloudHSM claves de la AWS KMS consola o mediante la DescribeKeyoperación, puede ver las propiedades típicas, como su ID de clave, estado de clave y fecha de creación. Pero también puede ver el ID del almacén de claves personalizado y (de forma opcional) el ID del clúster de AWS CloudHSM. Para obtener más detalles, consulte Consultar las claves de KMS en un almacén de claves de AWS CloudHSM.

Si intenta crear una clave de KMS en su almacén de claves de AWS CloudHSM sin éxito, utilice el mensaje de error para ayudar a determinar la causa. Puede indicar que el almacén de claves

de AWS CloudHSM no esté conectado (`CustomKeyStoreInvalidStateException`) o que el clúster de AWS CloudHSM asociado no tiene los dos HSM activos necesarios para esta operación (`CloudHsmClusterInvalidConfigurationException`). Para obtener ayuda, consulte Resolver problemas de un almacén de claves personalizado.

Para ver un ejemplo del registro de AWS CloudTrail de la operación que crea una clave de KMS en un almacén de claves de AWS CloudHSM, consulte CreateKey.

Temas

- Crear una clave de KMS en un almacén de claves de AWS CloudHSM (consola)
- Crear una clave de KMS en un almacén de claves de AWS CloudHSM (API)

Crear una clave de KMS en un almacén de claves de AWS CloudHSM (consola)

Utilice el siguiente procedimiento para crear una clave de KMS de cifrado simétrica en un almacén de claves de AWS CloudHSM.

> **Note**
>
> No incluya información confidencial en el alias, la descripción ni las etiquetas. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija Create key.
5. Seleccione Symmetric (Simétrica).
6. En Key usage (Uso de claves), se selecciona la opción Encrypt and decrypt (Cifrar y descifrar) para usted. No la cambie.
7. Elija Advanced options (Opciones avanzadas).
8. En Origen del material de claves, elija Almacén de claves de AWS CloudHSM.

   No puede crear claves de varias regiones en un almacén de claves de AWS CloudHSM.

9. Elija Siguiente.
10. Seleccione un almacén de claves de AWS CloudHSM para su nueva clave de KMS. Para crear un almacén de claves de AWS CloudHSM, seleccione Create custom key store (Crear almacén de claves personalizado).

    El almacén de AWS CloudHSM claves que seleccione debe tener el estado Conectado. El clúster de AWS CloudHSM que tiene asociado debe estar activo y tener al menos dos HSM activos en distintas zonas de disponibilidad.

    Para obtener ayuda para conectarse a un almacén de claves de AWS CloudHSM, consulte Conectar y desconectar un almacén de claves de AWS CloudHSM. Para obtener ayuda para agregar HSM, consulte Agregar un HSM en la Guía del usuario de AWS CloudHSM.
11. Elija Siguiente.
12. Escriba un alias y, si lo desea, una descripción para la clave KMS.
13. (Opcional). En la página agregar etiquetas, añada etiquetas que identifiquen o categoricen la clave KMS.

    Cuando se agregan etiquetas a los recursos de AWS, AWS genera un informe de asignación de costos con el uso y los costos agregados por etiquetas. Las etiquetas también pueden utilizarse para controlar el acceso a una clave KMS. Para obtener información acerca del etiquetado de claves KMS, consulte Etiquetado de claves y ABAC para AWS KMS.
14. Elija Siguiente.
15. En la sección administradores de claves, seleccione los usuarios y roles de IAM que pueden administrar la clave KMS. Para obtener más información, consulte Permite que los administradores de claves administren la clave de KMS.

> **Note**
>
> Las políticas de IAM pueden otorgar permisos para usar la clave KMS a otros usuarios y roles de IAM.
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

16. (Opcional) Para evitar que estos administradores de claves eliminen esta clave KMS, desactive la casilla Allow key administrators to delete this key (Permitir que los administradores de claves eliminen esta clave) situada en la parte inferior de la página.
17. Elija Siguiente.
18. En la sección This account (Esta cuenta), seleccione los usuarios y roles de IAM de esta Cuenta de AWS que pueden usar la clave KMS en operaciones criptográficas. Para obtener más información, consulte Permite a los usuarios de claves utilizar la clave de KMS.

> **Note**
>
> Las políticas de IAM pueden otorgar permisos para usar la clave KMS a otros usuarios y roles de IAM.
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

19. (Opcional) Puede permitir que otras cuentas de Cuentas de AWS usen esta clave de KMS en operaciones criptográficas. Para ello, en la parte inferior de la página de la sección Other Cuentas de AWS (Otra) elija Add another Cuenta de AWS (Agregar otra) e ingrese el ID de Cuenta de AWS de una cuenta externa. Para agregar varias cuentas externas, repita este paso.

> **Note**
>
> Los administradores de las otras cuentas de Cuentas de AWS también deben permitir el acceso a la clave KMS mediante la creación de políticas de IAM para sus usuarios. Para obtener más información, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS.

20. Seleccione Siguiente.
21. Revise los ajustes de clave que ha elegido. Aún puede volver atrás y cambiar todos los ajustes.
22. Cuando haya acabado, elija Finish (Finalizar) para crear la clave.

Si el procedimiento se realiza correctamente, la pantalla mostrará la nueva clave de KMS en el almacén de claves de AWS CloudHSM de su elección. Al elegir el nombre o alias de la nueva clave de KMS, la pestaña Cryptographic configuration (Configuración criptográfica) en su pantalla

de detalle mostrará el origen de la clave de KMS (AWS CloudHSM), el nombre, el ID y el tipo del almacén de claves personalizado, y el ID del clúster de AWS CloudHSM. Si el procedimiento falla, aparecerá un mensaje de error que describe el motivo del error.

> **Tip**
>
> Para facilitar la identificación de las claves KMS en un almacén de claves personalizado, en la página Customer managed keys (Claves administradas por el cliente) agregue la columna Custom key store ID (ID del almacén de claves personalizado). Haga clic en el icono de engranaje en la esquina superior derecha y, a continuación, seleccione Custom key store ID (ID del almacén de claves personalizado). Para obtener más detalles, consulte Personalización de las tablas clave KMS.

Crear una clave de KMS en un almacén de claves de AWS CloudHSM (API)

Para crear una nueva AWS KMS key(clave KMS) en su almacén de AWS CloudHSM claves, utilice la CreateKeyoperación. Use el parámetro `CustomKeyStoreId` para identificar su almacén de claves personalizado y en el valor `Origin` especifique `AWS_CLOUDHSM`.

Es posible que también desee utilizar el parámetro `Policy` para especificar una política de claves. Puede cambiar la política de claves (PutKeyPolicy) y añadir elementos opcionales, como una descripción y etiquetas, en cualquier momento.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

El siguiente ejemplo comienza con una llamada a la DescribeCustomKeyStoresoperación para comprobar que el almacén de AWS CloudHSM claves está conectado al AWS CloudHSM clúster asociado. De forma predeterminada, esta operación devuelve los almacenes de claves personalizados de su cuenta y región. Para describir únicamente un almacén de claves de AWS CloudHSM determinado, utilice el parámetro `CustomKeyStoreId` o `CustomKeyStoreName` (pero no ambos).

Antes de ejecutar este comando, reemplace el ID del almacén de claves personalizado de ejemplo por un ID válido.

> **Note**
>
> No incluya información confidencial en los campos `Description` o `Tags`. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0
{
   "CustomKeyStores": [
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "CustomKeyStoreType": "AWS CloudHSM key store",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "CONNECTED"
   ],
}
```

El siguiente comando de ejemplo utiliza la DescribeClustersoperación para comprobar que el AWS CloudHSM clúster asociado al `ExampleKeyStore` (cluster-1a23b4cdefg) tiene al menos dos HSM activos. Si el clúster tiene menos de dos HSM, la operación `CreateKey` dará error.

```
$ aws cloudhsmv2 describe-clusters
{
    "Clusters": [
        {
            "SubnetMapping": {
               ...
            },
            "CreateTimestamp": 1507133412.351,
            "ClusterId": "cluster-1a23b4cdefg",
            "SecurityGroup": "sg-865af2fb",
            "HsmType": "hsm1.medium",
            "VpcId": "vpc-1a2b3c4d",
            "BackupPolicy": "DEFAULT",
            "Certificates": {
                "ClusterCertificate": "-----BEGIN CERTIFICATE-----\...\n-----END
 CERTIFICATE-----\n"
            },
            "Hsms": [
```

```
                {
                    "AvailabilityZone": "us-west-2a",
                    "EniIp": "10.0.1.11",
                    "ClusterId": "cluster-1a23b4cdefg",
                    "EniId": "eni-ea8647e1",
                    "StateMessage": "HSM created.",
                    "SubnetId": "subnet-a6b10bd1",
                    "HsmId": "hsm-abcdefghijk",
                    "State": "ACTIVE"
                },
                {
                    "AvailabilityZone": "us-west-2b",
                    "EniIp": "10.0.0.2",
                    "ClusterId": "cluster-1a23b4cdefg",
                    "EniId": "eni-ea8647e1",
                    "StateMessage": "HSM created.",
                    "SubnetId": "subnet-b6b10bd2",
                    "HsmId": "hsm-zyxwvutsrqp",
                    "State": "ACTIVE"
                },
            ],
            "State": "ACTIVE"
        }
    ]
}
```

Este comando de ejemplo usa la CreateKeyoperación para crear una clave KMS en un almacén de claves. AWS CloudHSM Para crear una clave de KMS en un almacén de claves de AWS CloudHSM, debe proporcionar el ID del nombre del almacén de claves de AWS CloudHSM y especificar un valor `Origin` de `AWS_CLOUDHSM`.

La respuesta contiene los ID del almacén de claves personalizado y el clúster de AWS CloudHSM.

Antes de ejecutar este comando, reemplace el ID del almacén de claves personalizado de ejemplo por un ID válido.

```
$ aws kms create-key --origin AWS_CLOUDHSM --custom-key-store-id cks-1234567890abcdef0
{
  "KeyMetadata": {
    "AWSAccountId": "111122223333",
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "CreationDate": 1.499288695918E9,
```

```
    "Description": "Example key",
    "Enabled": true,
    "MultiRegion": false,
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "Origin": "AWS_CLOUDHSM"
    "CloudHsmClusterId": "cluster-1a23b4cdefg",
    "CustomKeyStoreId": "cks-1234567890abcdef0"
    "KeySpec": "SYMMETRIC_DEFAULT",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "EncryptionAlgorithms": [
        "SYMMETRIC_DEFAULT"
    ]
  }
}
```

Consultar las claves de KMS en un almacén de claves de AWS CloudHSM

Para ver las AWS KMS keys en un almacén de claves de AWS CloudHSM, use las mismas técnicas que usaría para ver cualquier clave administrada por el cliente de AWS KMS. Para conocer la información básica, consulte Consultar claves. Para identificar las claves de su clúster de AWS CloudHSM que actúa como material de claves para su clave KMS, consulte Buscar las claves KMS y material de claves. Para obtener información acerca de cómo ver los registros AWS CloudTrail que registran todas las operaciones de la API en un almacén de claves personalizado, consulte Registrar llamadas a la AWS KMS API con AWS CloudTrail.

En la consola de AWS KMS, las claves de KMS del almacén de claves personalizado se muestran en la página de las claves administradas por el cliente, junto con las otras claves administradas por el cliente de su región y Cuenta de AWS.

Sin embargo, los siguientes valores son específicos de las claves de KMS de un almacén de claves de AWS CloudHSM.

- El nombre y el ID del almacén de claves de AWS CloudHSM que almacena la clave de KMS.
- El ID clúster de AWS CloudHSM asociado que contiene su material de claves.
- Un valor `Origin` de `AWS CloudHSM` en la consola de AWS KMS o `AWS_CLOUDHSM` en las respuestas de la API.

- El valor del estado de clave puede ser `Unavailable`. Para ayudar a resolver el estado, consulte ¿Cómo arreglar las claves KMS no disponibles?.

Para ver las claves de KMS de un almacén de claves de AWS CloudHSM (consola)

1. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. En la esquina superior derecha, seleccione el icono de engranaje, elija Custom key store ID (ID del almacén de claves personalizado) y Origin (Origen), y, por último, Confirm (Confirmar).
5. Para identificar las claves de KMS en cualquier almacén de claves de AWS CloudHSM, busque las claves de KMS con el valor de Origin (Origen) establecido en AWS CloudHSM. Para identificar las claves de KMS en un almacén de claves de AWS CloudHSM determinado, consulte los valores de la columna Custom key store ID (ID del almacén de claves personalizado).
6. Elija el alias o el ID de clave de una clave de KMS en un almacén de claves de AWS CloudHSM.

   Esta página muestra información detallada sobre la clave KMS, incluido su Nombre de recurso de Amazon (ARN), su política claves y sus etiquetas.
7. Elija la pestaña Cryptographic configuration (Configuración criptográfica). Las pestañas están debajo de la sección General configuration (Configuración general).

   Esta sección incluye información acerca del almacén de claves de AWS CloudHSM y del clúster de AWS CloudHSM asociado a la clave de KMS.

Para ver las claves de KMS en un almacén de claves personalizado (API)

Utiliza las mismas operaciones de AWS KMS API para ver las claves de KMS en un almacén de AWS CloudHSM claves que usaría para cualquier clave de KMS ListKeys, incluidas DescribeKey, y GetKeyPolicy. Por ejemplo, la siguiente operación `describe-key` en la AWS CLI muestra los campos especiales de una clave de KMS en un almacén de claves de AWS CloudHSM. Antes de ejecutar un comando de este tipo, reemplace el ID de la clave KMS de ejemplo por un valor válido.

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab

{
```

```
   "KeyMetadata": {
      "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
      "AWSAccountId": "111122223333",
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "CreationDate": 1537582718.431,
      "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "Description": "Key in custom key store",
      "Enabled": true,
      "EncryptionAlgorithms": [
         "SYMMETRIC_DEFAULT"
      ],
      "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
      "KeyManager": "CUSTOMER",
      "KeySpec": "SYMMETRIC_DEFAULT",
      "KeyState": "Enabled",
      "KeyUsage": "ENCRYPT_DECRYPT",
      "MultiRegion": false,
      "Origin": "AWS_CLOUDHSM"
   }
}
```

Para obtener información sobre cómo buscar las claves de KMS en un almacén de claves de AWS CloudHSM o cómo identificar las claves en el clúster de AWS CloudHSM que actúa como material de claves para la clave de KMS, consulte Buscar las claves KMS y material de claves.

Usar las claves KMS en un almacén de claves de AWS CloudHSM

Después de crear una clave de KMS de cifrado simétrico en un almacén de claves de AWS CloudHSM, puede usarla para las siguientes operaciones criptográficas:

- Encrypt
- Decrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt

Las operaciones que generan pares de claves de datos asimétricos GenerateDataKeyPairy GenerateDataKeyPairWithoutPlaintextno se admiten en los almacenes de claves personalizados.

Cuando utilice la clave de KMS en una solicitud, identifique la clave de KMS por su ID o alias. No es necesario especificar el almacén de claves de AWS CloudHSM ni el clúster de AWS CloudHSM. La respuesta incluye los mismos campos que se devuelven para cualquier clave KMS de cifrado simétrica.

Sin embargo, cuando se utiliza una clave de KMS en un almacén de claves de AWS CloudHSM, la operación criptográfica se realiza completamente dentro del clúster de AWS CloudHSM asociado con el almacén de claves de AWS CloudHSM. La operación utiliza el material de claves del clúster asociado con la clave KMS elegida.

Para ello, se deben cumplir las siguientes condiciones.

- El estado de clave de la clave KMS debe ser `Enabled`. Para encontrar el estado de la clave, utilice el campo Estado de la AWS KMSconsola o el `KeyState` campo de la DescribeKeyrespuesta.
- El almacén de claves de AWS CloudHSM debe estar conectado a su clúster de AWS CloudHSM. Su estado en la AWS KMSconsola o `ConnectionState` en la DescribeCustomKeyStoresrespuesta debe ser`CONNECTED`.
- El clúster de AWS CloudHSM asociado al almacén de claves personalizado debe incluir al menos un HSM activo. Para averiguar el número de HSM activos en el clúster, utilice la AWS KMSconsola, la AWS CloudHSM consola o la DescribeClustersoperación.
- El clúster de AWS CloudHSM debe incluir el material de claves para la clave KMS. Si se ha eliminado el material de claves del clúster, o se ha creado un HSM a partir de una copia de seguridad que no incluía el material de claves, la operación criptográfica dará error.

Si no se cumplen estas condiciones, la operación criptográfica dará error y AWS KMS devolverá una excepción `KMSInvalidStateException`. Normalmente, bastará con que vuelva a conectar el almacén de claves de AWS CloudHSM. Para obtener ayuda adicional, consulte ¿Cómo arreglar una clave KMS que produce error?.

Cuando utilice las claves de KMS en un almacén de claves de AWS CloudHSM, tenga en cuenta que las claves de KMS de cada almacén de claves de AWS CloudHSM comparten una cuota de solicitudes del almacén de claves personalizado para operaciones criptográficas. Si supera la cuota, AWS KMS devuelve una `ThrottlingException`. Si el clúster de AWS CloudHSM que está asociado al almacén de claves de AWS CloudHSM procesa numerosos comandos, incluidos los no relacionados con el almacén de claves de AWS CloudHSM, es posible que obtenga una `ThrottlingException` a un velocidad aún inferior. Si recibe una excepción `ThrottlingException` para cualquier solicitud, baje la velocidad de solicitud e intente ejecutar

los comandos de nuevo. Para obtener más información sobre la cuota de solicitudes del almacén de claves personalizado, consulte Cuotas de solicitudes del almacén de claves personalizado.

Buscar las claves KMS y material de claves

Si administra un almacén de claves de AWS CloudHSM, es posible que tenga que identificar las claves de KMS en cada almacén de claves de AWS CloudHSM. Por ejemplo, es probable que deba realizar algunas de las siguientes tareas.

- Realizar el seguimiento de las claves de KMS en un almacén de claves de AWS CloudHSM en registros de AWS CloudTrail.
- Predecir qué efecto tendrá sobre las claves de KMS desconectar un almacén de claves de AWS CloudHSM.
- Programar la eliminación de claves de KMS antes de eliminar un almacén de claves de AWS CloudHSM.

Además, debería identificar las claves de su clúster de AWS CloudHSM que actúa como material de claves para sus claves KMS. Aunque AWS KMS administra las claves KMS y su material de claves, sigue controlando y es responsable de la administración de su clúster de AWS CloudHSM, sus HSM y las copias de seguridad, y las claves en los HSM. Es probable que deba identificar las claves para poder auditar el material de claves, protegerlo de ser eliminado por error o eliminarlo de los HSM y de las copias de seguridad del clúster tras eliminar la clave KMS.

Todo el material de claves para las claves de KMS en su almacén de claves de AWS CloudHSM es propiedad del usuario de criptografía `kmsuser` (CU). AWS KMS establece el atributo de la etiqueta de claves, que solo puede verse en AWS CloudHSM, en el Nombre de recurso de Amazon (ARN) de la clave de KMS.

Para buscar las claves KMS y el material de claves, puede utilizar cualquiera de las técnicas siguientes.

- Buscar las claves de KMS en un almacén de claves de AWS CloudHSM: cómo identificar las claves de KMS en uno o todos sus almacenes de claves de AWS CloudHSM.
- Buscar todas las claves para un almacén de claves de AWS CloudHSM: cómo encontrar todas las claves en su clúster que actúan como material de claves para las claves de KMS en su almacén de claves de AWS CloudHSM.

- Buscar la clave de AWS CloudHSM de una clave de KMS: cómo encontrar la clave en el clúster que actúa como material de claves para una clave de KMS en particular en su almacén de claves de AWS CloudHSM.
- Buscar la clave de KMS para una clave de AWS CloudHSM: Cómo encontrar la clave KMS para una clave concreta en su clúster.

Buscar las claves de KMS en un almacén de claves de AWS CloudHSM

Si administra un almacén de claves de AWS CloudHSM, es posible que tenga que identificar las claves de KMS en cada almacén de claves de AWS CloudHSM. Puede utilizar esta información para realizar el seguimiento de las operaciones de las claves de KMS en registros de AWS CloudTrail, predecir qué efecto tendrá sobre las claves de KMS la desconexión de un almacén de claves personalizado o programar la eliminación de las claves de KMS antes de eliminar un almacén de claves de AWS CloudHSM.

Para buscar las claves de KMS en un almacén de claves de AWS CloudHSM (consola)

Para buscar las claves de KMS en un almacén de claves de AWS CloudHSM determinado, en la página Customer managed keys (Claves administradas por el cliente) consulte los valores de los campos Custom Key Store Name (Nombre del almacén de claves personalizado) o Custom Key Store ID (ID del almacén de claves personalizado). Para identificar las claves de KMS en cualquier almacén de claves de AWS CloudHSM, busque las claves de KMS con el valor de Origin (Origen) establecido en AWS CloudHSM. Para agregar columnas opcionales a la pantalla, elija el icono de engranaje en la esquina superior derecha de la página.

Para buscar las claves de KMS en un almacén de claves de AWS CloudHSM (API)

Para buscar las claves de KMS en un almacén de AWS CloudHSM claves, utilice las DescribeKeyoperaciones ListKeysy y, a continuación, filtre por `CustomKeyStoreId` valor. Antes de ejecutar los ejemplos, reemplace los valores ficticios del ID del almacén de claves personalizado por un ID válido.

Bash

Para buscar las claves de KMS en un almacén de claves de AWS CloudHSM en particular, recopile todas las claves de KMS de la cuenta y la región. A continuación, filtre por el ID del almacén de claves personalizado.

```
for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text) ;
```

```
do aws kms describe-key --key-id $key |
grep '"CustomKeyStoreId": "cks-1234567890abcdef0"' --context 100; done
```

Para obtener una clave de KMS en cualquier almacén de claves de AWS CloudHSM en la cuenta y región, busque `CustomKeyStoreType` con valores de `AWS_CloudHSM`.

```
for key in $(aws kms list-keys --query 'Keys[*].KeyId' --output text) ;
do aws kms describe-key --key-id $key |
grep '"CustomKeyStoreType": "AWS_CloudHSM"' --context 100; done
```

PowerShell

Para buscar las claves de KMS en un almacén de AWS CloudHSM claves concreto, utilice los KmsKey cmdlets Get KmsKeyList y Get para obtener todas las claves de KMS de la cuenta y la región. A continuación, filtre por el ID del almacén de claves personalizado.

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreId -eq
 'cks-1234567890abcdef0'
```

Para obtener las claves de KMS en cualquier almacén de AWS CloudHSM claves de la cuenta y la región, filtra por el CustomKeyStoreType valor de. `AWS_CLOUDHSM`

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreType -eq 'AWS_CLOUDHSM'
```

Buscar todas las claves para un almacén de claves de AWS CloudHSM

Puede identificar las claves en su clúster de AWS CloudHSM que actúan como material de claves para su almacén de claves de AWS CloudHSM. Para ello, usa el findAllKeyscomando de cloudhsm_mgmt_util para encontrar los identificadores de todas las claves que posean o compartan. `kmsuser` A menos que haya iniciado sesión como `kmsuser` y haya creado claves fuera de AWS KMS, todas las claves que posee `kmsuser` representan material de claves para las claves de KMS.

Cualquier responsable de criptografía del clúster puede ejecutar este comando sin desconectar el almacén de claves de AWS CloudHSM.

1. Inicie cloudhsm_mgmt_util mediante el procedimiento descrito en el tema Getting started with CloudHSM Management Utility (CMU) (Introducción a la utilidad de administración (CMU) de CloudHSM).

2. Inicie sesión en cloudhsm_mgmt_util con la cuenta del responsable de criptografía (CO).
3. Use el comando listUsers para buscar el ID del usuario de criptografía `kmsuser`.

   En este ejemplo, `kmsuser` tiene el ID de usuario 3.

```
aws-cloudhsm> listUsers
Users on server 0(10.0.0.1):
Number of users found:3

    User Id              User Type       User Name            MofnPubKey
 LoginFailureCnt          2FA
         1               PCO             admin                     NO
 0               NO
         2               AU              app_user                  NO
 0               NO
         3               CU              kmsuser                   NO
 0               NO
```

4. Usa el findAllKeyscomando para buscar los identificadores de todas las claves que posean o compartan. `kmsuser` Reemplace el ID (3) de usuario de ejemplo por el ID de usuario real de `kmsuser` en su clúster.

   El resultado del ejemplo muestra que `kmsuser` es propietario de claves con los identificadores de claves 8, 9 y 262162 en ambos HSM del clúster.

```
aws-cloudhsm> findAllKeys 3 0
Keys on server 0(10.0.0.1):
Number of keys found 3
number of keys matched from start index 0::6
8,9,262162
findAllKeys success on server 0(10.0.0.1)

Keys on server 1(10.0.0.2):
Number of keys found 6
number of keys matched from start index 0::6
8,9,262162
findAllKeys success on server 1(10.0.0.2)
```

Buscar la clave de KMS para una clave de AWS CloudHSM

Si conoce el identificador de clave de una clave que es propiedad de `kmsuser` en el clúster, puede utilizar la etiqueta de claves para identificar la clave de KMS asociada en su almacén de claves de AWS CloudHSM.

Cuando AWS KMS crea el material de claves para una clave KMS en su clúster de AWS CloudHSM, este escribe el Nombre de recurso de Amazon (ARN) de la clave KMS en la etiqueta de la clave. A menos que haya cambiado el valor de la etiqueta, puede utilizar el comando getAttribute en key_mgmt_util o cloudhsm_mgmt_util para asociar la clave con su clave KMS.

Para ejecutar este procedimiento, debe desconectar temporalmente el almacén de claves de AWS CloudHSM para poder iniciar sesión como el CU `kmsuser`.

> **Note**
>
> Mientras un almacén de claves personalizado esté desconectado, todos los intentos de crear claves KMS en el almacén de claves personalizado o de usar claves KMS existentes en operaciones criptográficas fallarán. Esta acción puede impedir que los usuarios almacenen y accedan a datos confidenciales.

1. Desconecte el almacén de claves de AWS CloudHSM, si no lo está todavía, e inicie sesión en key_mgmt_util como `kmsuser`, tal como se explica en Cómo desconectar e iniciar sesión.
2. Use el comando `getAttribute` en key_mgmt_util o cloudhsm_mgmt_util para obtener el atributo de la etiqueta (`OBJ_ATTR_LABEL`, atributo `3`) para un identificador de claves determinado.

   Por ejemplo, este comando utiliza `getAttribute` en cloudhsm_mgmt_util para obtener el atributo de la etiqueta (atributo `3`) de la clave con el identificador de claves `262162`. El resultado muestra que la clave `262162` actúa como material de claves para la clave KMS con el ARN `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`. Antes de ejecutar este comando, reemplace el identificador de claves de ejemplo por uno válido.

   Para obtener una lista de los atributos de clave, use el comando listAttributes o consulte el tema Referencia de los atributos de claves en la Guía del usuario de AWS CloudHSM.

   ```
   aws-cloudhsm> getAttribute 262162 3
   ```

```
Attribute Value on server 0(10.0.1.10):
OBJ_ATTR_LABEL
arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

3. Cierre la sesión de key_mgmt_util o cloudhsm_mgmt_util y vuelva a conectar el almacén de claves de AWS CloudHSM tal como se explica en Cómo cerrar sesión y volver a conectar.

Buscar la clave de AWS CloudHSM de una clave de KMS

Puede utilizar el ID de una clave de KMS en un almacén de claves de AWS CloudHSM para identificar la clave del clúster de AWS CloudHSM que actúa como su material de claves. A continuación, puede usar su clave para identificar la clave en otros comandos del cliente AWS CloudHSM.

Cuando AWS KMS crea el material de claves para una clave KMS en su clúster de AWS CloudHSM, este escribe el Nombre de recurso de Amazon (ARN) de la clave KMS en la etiqueta de la clave. A menos que haya cambiado el valor de la etiqueta, puede usar el comando findKey en key_mgmt_util para obtener el identificador de claves del material de claves para la clave KMS. Para ejecutar este procedimiento, debe desconectar temporalmente el almacén de claves de AWS CloudHSM para poder iniciar sesión como el CU `kmsuser`.

> **Note**
>
> Mientras un almacén de claves personalizado esté desconectado, todos los intentos de crear claves KMS en el almacén de claves personalizado o de usar claves KMS existentes en operaciones criptográficas fallarán. Esta acción puede impedir que los usuarios almacenen y accedan a datos confidenciales.

1. Desconecte el almacén de claves de AWS CloudHSM, si no lo está todavía, e inicie sesión en key_mgmt_util como `kmsuser`, tal como se explica en Cómo desconectar e iniciar sesión.
2. Use el comando findKey en key_mgmt_util para buscar una clave con una etiqueta que coincida con el ARN de la clave de KMS de su almacén de claves de AWS CloudHSM. Reemplace el ARN de la clave KMS de ejemplo en el valor del parámetro `-l` (L en minúscula por "label") por un ARN de la clave KMS válido.

   Por ejemplo, este comando encuentra la clave con una etiqueta que coincide con el ARN de la clave KMS de ejemplo, `arn:aws:kms:us-`

`west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`. El resultado del ejemplo muestra que la clave con el identificador de clave 262162 tiene el ARN de la clave KMS especificado en su etiqueta. Ahora puede utilizar este identificador de claves en otros comandos key_mgmt_util.

```
Command: findKey -l arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
Total number of keys present 1

 number of keys matched from start index 0::1
262162

        Cluster Error Status
        Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
        Node id 0 and err state 0x00000000 : HSM Return: SUCCESS

        Cfm3FindKey returned: 0x00 : HSM Return: SUCCESS
```

3. Cierre la sesión de key_mgmt_util y vuelva a conectar el almacén de claves personalizado tal como se explica en Cómo cerrar sesión y volver a conectar.

Programar la eliminación de claves de KMS de un almacén de claves de AWS CloudHSM

Si está seguro de que no necesitará una AWS KMS key para ninguna operación criptográfica, puede programar la eliminación de la clave KMS. Puede usar el mismo procedimiento que utilizaría para programar la eliminación de una clave KMS de AWS KMS. Además, debe mantener el almacén de claves de AWS CloudHSM conectado para que AWS KMS pueda eliminar el material de claves correspondiente del clúster de AWS CloudHSM asociado cuando venza el periodo de espera.

Puede monitorear la programación, la cancelación y la eliminación de la clave de KMS en sus registros de AWS CloudTrail.

> **Warning**
>
> Eliminar una clave de KMS es una operación destructiva y potencialmente peligrosa que evita que recupere todo el cifrado de datos con la clave de KMS. Antes de programar la eliminación de la clave de KMS, examine el uso anterior de la clave de KMS y cree una CloudWatch alarma de Amazon que le avise cuando alguien intente usar la clave de KMS

mientras está pendiente de ser eliminada. Es preferible, siempre que sea posible, desactivar la clave KMS a eliminarla.

Si programa la eliminación de una clave de KMS de un almacén de claves de AWS CloudHSM, su estado de clave cambiará a Pending deletion (Eliminación pendiente). La clave de KMS conservará el estado Pending deletion (Eliminación pendiente) durante todo el periodo de espera, incluso si la clave de KMS deja de estar disponible porque ha desconectado el almacén de claves personalizado. Esto permite cancelar la eliminación de la clave KMS en cualquier momento durante el período de espera.

Cuando finaliza el periodo de espera, AWS KMS elimina la clave KMS de AWS KMS. AWS KMS hará lo posible por eliminar el material de claves del clúster de AWS CloudHSM asociado. Si AWS KMS no puede eliminar el material de claves, como, por ejemplo, cuando el almacén de claves está desconectado de AWS KMS, es probable que tenga que eliminar el material de claves huérfano manualmente del clúster.

AWS KMS no elimina el material de claves de las copias de seguridad del clúster. Incluso si elimina la clave KMS de AWS KMS y borra su material de claves de su clúster de AWS CloudHSM, los clústers creados a partir de copias de seguridad podrían incluir material de claves eliminado. Para eliminar el material de claves de forma permanente, consulte la fecha de creación de la clave KMS. A continuación, elimine todas las copias de seguridad del clúster que puedan contener el material de claves.

Al programar la eliminación de una clave de KMS de un almacén de claves de AWS CloudHSM, la clave de KMS queda inutilizable de inmediato (sujeto a la posible coherencia). Sin embargo, los recursos cifrados con claves de datos protegidas por la clave de KMS no se ven afectados hasta que se vuelva a utilizar la clave de KMS, por ejemplo, para descifrar la clave de datos. Este problema afecta a los Servicios de AWS, muchos de los cuales utilizan claves de datos para proteger sus recursos. Para obtener más información, consulte Cómo afectan las claves de KMS obsoletas a las claves de datos.

Resolver problemas de un almacén de claves personalizado

Los almacenes de claves de AWS CloudHSM están diseñados para ofrecer disponibilidad y larga duración. Sin embargo, pueden surgir algunas condiciones de error que deberá reparar para mantener operativo su almacén de claves de AWS CloudHSM.

Temas

- ¿Cómo arreglar las claves KMS no disponibles?
- ¿Cómo arreglar una clave KMS que produce error?
- Cómo arreglar un error de conexión
- Cómo responder ante un error de operación criptográfica
- Cómo arreglar las credenciales de kmsuser no válidas
- Cómo eliminar material de claves huérfano
- ¿Cómo recuperar el material de claves eliminado de una clave KMS?
- Cómo iniciar sesión como kmsuser

¿Cómo arreglar las claves KMS no disponibles?

El estado de clave de AWS KMS keys en un almacén de claves de AWS CloudHSM normalmente es `Enabled`. De igual modo que todas las claves de KMS, el estado de clave cambia al deshabilitar las claves de KMS en un almacén de claves de AWS CloudHSM o al programar su eliminación. Sin embargo, a diferencia de otras claves KMS, las claves KMS de un almacén de claves personalizado también pueden tener el estado de clave `Unavailable`.

El estado de clave `Unavailable` indica que la clave de KMS está en un almacén de claves personalizado que se ha desconectado de forma intencional y que los intentos de conectarlo de nuevo han fallado. Mientras una clave KMS no esté disponible, puede consultarla y administrarla, pero no puede usarla en operaciones criptográficas.

Para buscar el estado de clave de una clave KMS en la página Customer managed keys (Claves administradas por el cliente) consulte el campo Status (Estado) de la clave KMS. O bien, utilice la DescribeKeyoperación y visualice el `KeyState` elemento en la respuesta. Para obtener más detalles, consulte Consultar claves.

Las claves KMS en un almacén de claves personalizado desconectado tendrá el estado de clave `Unavailable` o `PendingDeletion`. Las claves de KMS programadas para su eliminación de un almacén de claves personalizado tienen el estado de clave `Pending Deletion`, incluso si el almacén de claves personalizado está desconectado. Esto permite cancelar la eliminación programada de la clave sin volver a conectar el almacén de claves personalizado.

Para arreglar una clave KMS no disponible, vuelva a conectar el almacén de claves personalizado. Después de volver a conectar el almacén de claves personalizado, el estado de clave de las claves KMS en el almacén de claves personalizado se restaura automáticamente al estado anterior, como

`Enabled` o `Disabled`. Las claves KMS pendientes de eliminación seguirán teniendo el estado `PendingDeletion`. Sin embargo, si el problema persiste, habilitar y desactivar una clave KMS no disponible no cambia su estado de clave. La acción de habilitar o desactivar solo será efectiva cuando la clave esté disponible.

Si desea ayuda con las conexiones que dan error, consulte Cómo arreglar un error de conexión.

¿Cómo arreglar una clave KMS que produce error?

Los problemas para crear y utilizar claves de KMS en almacenes de claves de AWS CloudHSM pueden deberse a un problema con el almacén de claves de AWS CloudHSM, su clúster de AWS CloudHSM asociado, la clave de KMS o su material de claves.

Cuando un almacén de claves de AWS CloudHSM se desconecta de su clúster de AWS CloudHSM, el estado de clave de las claves de KMS en el almacén de claves personalizado es `Unavailable`. Todas las solicitudes para crear claves de KMS en un almacén de claves de AWS CloudHSM desconectado devuelven una excepción `CustomKeyStoreInvalidStateException`. Todas las solicitudes para cifrar, descifrar, volver a cifrar o generar claves de datos devuelve una excepción `KMSInvalidStateException`. Para solucionar el problema, vuelva a conectar el almacén de claves de AWS CloudHSM.

Sin embargo, los intentos de usar una clave de KMS de un almacén de claves de AWS CloudHSM para operaciones criptográficas pueden no ser fructíferos incluso cuando el estado de clave es `Enabled` y el estado de conexión del almacén de claves de AWS CloudHSM es `Connected`. Esto puede deberse a una de las siguientes condiciones.

- Puede que se haya eliminado el material de claves para la clave KMS del clúster de AWS CloudHSM asociado. Para investigar, busque el identificador de claves del material de claves para una clave KMS y, si es necesario, intente recuperar el material de claves.
- Se eliminaron todos los HSM del clúster de AWS CloudHSM asociado al almacén de claves de AWS CloudHSM. Para utilizar una clave de KMS en un almacén de claves de AWS CloudHSM en una operación criptográfica, su clúster de AWS CloudHSM debe contener al menos un HSM activo. Para comprobar el número y el estado de los HSM de un AWS CloudHSM clúster, utilice la AWS CloudHSM consola o la DescribeClustersoperación. Para añadir un HSM al clúster, utilice la AWS CloudHSM consola o la CreateHsmoperación.
- Se eliminó el clúster de AWS CloudHSM asociado al almacén de claves de AWS CloudHSM. Para resolver el problema, cree un clúster a partir de una copia de seguridad relacionada con el clúster original, como una copia de seguridad de un clúster original o una copia de seguridad utilizada

para crear el clúster original. A continuación, edite el ID del clúster en la configuración del almacén de claves personalizado. Para obtener instrucciones, consulte ¿Cómo recuperar el material de claves eliminado de una clave KMS?.

- El clúster de AWS CloudHSM asociado al almacén de claves personalizado no tenía ninguna sesión de PKCS#11 disponible. Esto ocurre, por lo general, cuando se producen períodos de ráfagas de tráfico elevado, en los que se necesitan sesiones adicionales para dar servicio al tráfico. Para responder a una `KMSInternalException` con un mensaje de error sobre las sesiones de PKCS#11, regrese y vuelva a intentar la solicitud.

Cómo arreglar un error de conexión

Si intenta conectar un almacén de claves de AWS CloudHSM a su clúster de AWS CloudHSM, pero la operación falla, el estado de conexión del almacén de claves de AWS CloudHSM cambiará a `FAILED`. Para encontrar el estado de conexión de un almacén de AWS CloudHSM claves, utilice la AWS KMS consola o la DescribeCustomKeyStoresoperación.

Algunos intentos de conexión producen un error rápidamente debido a errores de configuración del clúster detectados fácilmente. En este caso, el estado de la conexión aún es `DISCONNECTED`. Estos errores devuelven un mensaje de error o unaexcepción que explica por qué el intento produjo un error. Revise la descripción de la excepción y los requisitos del clúster, solucione el problema, actualice el almacén de claves de AWS CloudHSM, si es necesario, e intente conectarse de nuevo.

Cuando el estado de la conexión seaFAILED, ejecute la DescribeCustomKeyStoresoperación y observe el `ConnectionErrorCode` elemento en la respuesta.

> **Note**
>
> Cuando el estado de conexión de un almacén de claves de AWS CloudHSM es `FAILED`, deberá desconectar el almacén de claves de AWS CloudHSM antes de conectarlo de nuevo. No puede conectar un almacén de claves de AWS CloudHSM que tenga el estado de conexión `FAILED`.

- `CLUSTER_NOT_FOUND` indica que AWS KMS no ha encontrado ningún clúster de AWS CloudHSM con el ID de clúster especificado. Esto puede deberse a que se ha proporcionado un ID de clúster erróneo a una operación de API o que se ha eliminado el clúster y no se ha reemplazado. Para corregir este error, compruebe el ID del clúster, por ejemplo, mediante la AWS CloudHSM consola o la DescribeClustersoperación. Si se ha eliminado el clúster, cree un clúster a partir de una copia

de seguridad reciente del original. A continuación, desconecte el almacén de claves de AWS CloudHSM, edite la configuración del ID del clúster del almacén de claves deAWS CloudHSM y vuelva a conectar el almacén de claves de AWS CloudHSM al clúster.

- `INSUFFICIENT_CLOUDHSM_HSMS` indica que el clúster de AWS CloudHSM asociado no contiene ningún HSM. Para conectarse, el clúster debe tener al menos un HSM. Para encontrar el número de HSM en el clúster, utilice la DescribeClustersoperación. Para solucionar este error, agregue al menos un HSM al clúster. Si aagrega diversos HSM, recomendamos crearlos en diferentes zonas de disponibilidad.
- `INSUFFICIENT_FREE_ADDRESSES_IN_SUBNET` indica que AWS KMS no se pudo conectar el almacén de claves de AWS CloudHSM a su clúster de AWS CloudHSM porque al menos una subred privada asociada al clúster no dispone de direcciones IP. Una conexión de almacén de claves de AWS CloudHSM requiere una dirección IP libre en cada una de las subredes privadas asociadas, si bien se prefieren dos.

  No se pueden añadir direcciones IP (bloques CIDR) a una subred existente. Si es posible, se deben mover o eliminar otros recursos que estén utilizando las direcciones IP de la subred, como instancias de EC2 no utilizadas o interfaces de red elásticas. De lo contrario, cree un clúster a partir de una copia de seguridad reciente del clúster AWS CloudHSM con subredes privadas nuevas o existentes que tienen más espacio de direcciones gratuito. A continuación, para asociar el clúster nuevo con el almacén de claves de AWS CloudHSM, desconecte el almacén de claves personalizado, cambie el ID del clúster del almacén de claves de AWS CloudHSM por el ID del clúster nuevo e intente conectarse de nuevo.

  > **Tip**
  >
  > Para evitar restablecer la contraseña `kmsuser`, utilice la copia de seguridad más reciente del clúster de AWS CloudHSM.

- `INTERNAL_ERROR` indica que AWS KMS pudo completar la solicitud debido a un error interno. Intente realizar de nuevo la solicitud . Para las solicitudes `ConnectCustomKeyStore`, desconecte el almacén de claves de AWS CloudHSM antes de intentar conectarlo de nuevo.
- `INVALID_CREDENTIALS` indica que AWS KMS no puede iniciar sesión en el clúster de AWS CloudHSM porque no se ha introducido la contraseña de la cuenta `kmsuser` correcta. Si desea ayuda para solucionar este error, consulte Cómo arreglar las credenciales de `kmsuser` no válidas.
- `NETWORK_ERRORS` suele hacer referencia a problemas temporales de red. Desconecte el almacén de claves de AWS CloudHSM, espere unos minutos, e intente conectarlo de nuevo.

- `SUBNET_NOT_FOUND` indica que se ha eliminado al menos una subred de la configuración del clúster de AWS CloudHSM. Si AWS KMS no puede encontrar todas las subredes de la configuración del clúster, se producirá un error al intentar conectar el almacén de claves de AWS CloudHSM al clúster de AWS CloudHSM.

  Para corregir este error, cree un clúster a partir de una copia de seguridad reciente del mismo clúster de AWS CloudHSM. (Este proceso crea una nueva configuración de clúster con una VPC y subredes privadas). Compruebe que el nuevo clúster cumple los requisitos de un almacén de claves personalizado y anote el nuevo ID del clúster. A continuación, para asociar el clúster nuevo con el almacén de claves de AWS CloudHSM, desconecte el almacén de claves personalizado, cambie el ID del clúster del almacén de claves de AWS CloudHSM por el ID del clúster nuevo e intente conectarse de nuevo.

  > **Tip**
  >
  > Para evitar restablecer la contraseña `kmsuser`, utilice la copia de seguridad más reciente del clúster de AWS CloudHSM.

- `USER_LOCKED_OUT` indica que la cuenta del usuario de criptografía (CU) `kmsuser` está bloqueada del clúster de AWS CloudHSM asociado porque se han realizado demasiados intentos fallidos de introducción de contraseña. Si desea ayuda para solucionar este error, consulte Cómo arreglar las credenciales de `kmsuser` no válidas.

  Para solucionar este error, desconecte el almacén de claves de AWS CloudHSM y use el comando changePswd en cloudhsm_mgmt_util para cambiar la contraseña de la cuenta de `kmsuser`. A continuación, edite la configuración de la contraseña de `kmsuser` para el almacén de claves personalizado e intente conectarlo de nuevo. Para obtener ayuda, utilice el procedimiento descrito en el tema Cómo arreglar las credenciales de `kmsuser` no válidas.

- `USER_LOGGED_IN` indica que la cuenta del CU `kmsuser` ha iniciado sesión en el clúster de AWS CloudHSM asociado. Esto impide a AWS KMS rotar la contraseña de la cuenta `kmsuser` e iniciar sesión en el clúster. Para corregir este error, cierre la sesión del CU `kmsuser` del clúster. Si ha cambiado la contraseña de `kmsuser` para iniciar sesión en el clúster, también debe actualizar el valor de la contraseña del almacén de claves para el almacén de claves de AWS CloudHSM. Para obtener ayuda, consulte Cómo cerrar sesión y volver a conectar.

- `USER_NOT_FOUND` indica que AWS KMS no puede encontrar una cuenta del CU `kmsuser` en el clúster de AWS CloudHSM asociado. Para corregir este error, cree una cuenta de usuario de criptografía (CU) `kmsuser` en el clúster y, a continuación, actualice el valor de contraseña del

almacén de claves para el almacén de claves de AWS CloudHSM. Para obtener ayuda, consulte Cómo arreglar las credenciales de `kmsuser` no válidas.

Cómo responder ante un error de operación criptográfica

Una operación criptográfica que utiliza una clave de KMS en un almacén de claves personalizado puede dar un error `KMSInvalidStateException`. Los siguientes mensajes de error pueden acompañar al error `KMSInvalidStateException`.

KMS no puede comunicarse con el clúster de CloudHSM. Esto puede ser un problema de red transitorio. Si ve este error repetidamente, compruebe que las ACL de red y las reglas del grupo de seguridad de la VPC del clúster del AWS CloudHSM sean correctas.

- Aunque se trata de un error HTTPS 400, puede deberse a problemas de red transitorios. Para responder, comience por volver a intentar la solicitud. Sin embargo, si continúa fallando, examine la configuración de los componentes de red. Este error es probablemente causado por la configuración incorrecta de un componente de red, como una regla de firewall o una regla de grupo de seguridad de VPC que bloquea el tráfico saliente.

KMS no puede comunicarse con el clúster del AWS CloudHSM porque el usuario kmsuser está bloqueado. Si ve este error varias veces, desconecte el almacén de claves del AWS CloudHSM y restablezca la contraseña de la cuenta kmsuser. Actualice la contraseña de kmsuser para el almacén de claves personalizado y pruebe a realizar la solicitud de nuevo.

- Este mensaje de error indica que la cuenta del usuario de criptografía (CU) `kmsuser` está bloqueada del clúster del AWS CloudHSM asociado porque se han realizado demasiados intentos fallidos de introducción de contraseña. Si desea ayuda para solucionar este error, consulte Cómo desconectar e iniciar sesión.

Cómo arreglar las credenciales de **`kmsuser`** no válidas

Al conectar un almacén de claves de AWS CloudHSM, AWS KMS inicia sesión en el clúster de AWS CloudHSM asociado como el usuario de criptografía (CU) `kmsuser`. Conserva la sesión hasta que se desconecte el almacén de claves de AWS CloudHSM. La respuesta DescribeCustomKeyStores

muestra un `ConnectionState` de `FAILED` y un valor de `ConnectionErrorCode` de `INVALID_CREDENTIALS`, como se muestra en el siguiente ejemplo.

Si desconecta el almacén de claves de AWS CloudHSM y cambia la contraseña de `kmsuser`, AWS KMS no podrá iniciar sesión en el clúster de AWS CloudHSM con las credenciales de la cuenta del CU `kmsuser`. En consecuencia, todos los intentos de conectar el almacén de claves de AWS CloudHSM darán error. La respuesta `DescribeCustomKeyStores` muestra un `ConnectionState` de `FAILED` y un valor de `ConnectionErrorCode` de `INVALID_CREDENTIALS`, como se muestra en el siguiente ejemplo.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleKeyStore
{
   "CustomKeyStores": [
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionErrorCode": "INVALID_CREDENTIALS"
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
      "ConnectionState": "FAILED"
   ],
}
```

Además, después de 5 intentos de iniciar sesión en el clúster con una contraseña incorrecta, AWS CloudHSM bloquea la cuenta del usuario. Para iniciar sesión en el clúster, deberá cambiar la contraseña de la cuenta.

Si AWS KMS recibe una respuesta de bloqueo al intentar iniciar sesión en el clúster como el CU `kmsuser`, la solicitud para conectar el almacén de claves de AWS CloudHSM dará error. La DescribeCustomKeyStoresrespuesta incluye un valor `ConnectionState` de `FAILED` y un `ConnectionErrorCode` valor de`USER_LOCKED_OUT`, como se muestra en el siguiente ejemplo.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleKeyStore
{
   "CustomKeyStores": [
      "CloudHsmClusterId": "cluster-1a23b4cdefg",
      "ConnectionErrorCode": "USER_LOCKED_OUT"
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleKeyStore",
      "TrustAnchorCertificate": "<certificate string appears here>",
      "CreationDate": "1.499288695918E9",
```

```
      "ConnectionState": "FAILED"
   ],
}
```

Para reparar cualquiera de estas condiciones use el procedimiento siguiente.

1. Desconecte el almacén de claves de AWS CloudHSM.
2. Ejecute la DescribeCustomKeyStoresoperación y vea el valor del `ConnectionErrorCode` elemento en la respuesta.

   - Si el valor de `ConnectionErrorCode` es `INVALID_CREDENTIALS`, determine la contraseña actual para la cuenta de `kmsuser`. Si es necesario, use el comando changePswd en cloudhsm_mgmt_util para establecer la contraseña con un valor conocido.
   - Si el valor de `ConnectionErrorCode` es `USER_LOCKED_OUT`, deberá usar el comando changePswd en cloudhsm_mgmt_util para modificar la contraseña de `kmsuser`.
3. Edite la configuración de la contraseña de `kmsuser` para que coincida con la contraseña de `kmsuser` del clúster. Esta acción le dice a AWS KMS qué contraseña debe usar para iniciar sesión en el clúster. No cambia la contraseña de `kmsuser` en el clúster.
4. Conecte el almacén de claves personalizado.

Cómo eliminar material de claves huérfano

Después de programar la eliminación de una clave de KMS del almacén de claves de AWS CloudHSM, es probable que deba eliminar manualmente el material de claves correspondiente al clúster de AWS CloudHSM asociado.

Al crear una clave de KMS en un almacén de claves de AWS CloudHSM, AWS KMS crea los metadatos de la clave de KMS en AWS KMS y genera el material de claves en el clúster de AWS CloudHSM asociado. Al programar una eliminación de una clave de KMS en un almacén de claves de AWS CloudHSM, AWS KMS elimina los metadatos de la clave de KMS una vez pasado el periodo de espera. A continuación, AWS KMS hará lo posible por eliminar el material de claves del clúster de AWS CloudHSM. El intento puede fallar si AWS KMS no puede acceder al clúster, por ejemplo, cuando se desconecta del almacén de claves de AWS CloudHSM o cambia la contraseña del `kmsuser`. AWS KMS no intenta eliminar el material de claves de las copias de seguridad del clúster.

AWS KMS informa de los resultados de su intento de eliminar el material de claves del clúster en la entrada del evento `DeleteKey` de su registro de AWS CloudTrail. Aparece en el elemento `backingKeysDeletionStatus` del elemento `additionalEventData`, tal y como se muestra en

la siguiente entrada de ejemplo. La entrada también incluye el ID de la clave KMS, el ID del clúster de AWS CloudHSM y el identificador de claves del material de claves (`backing-key-id`).


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "111122223333",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2021-12-10T14:23:51Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DeleteKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "customKeyStoreId": "cks-1234567890abcdef0",
        "clusterId": "cluster-1a23b4cdefg",
        "backingKeys": "[{\"keyHandle\":\"01\",\"backingKeyId\":\"backing-key-id\"}]",
        "backingKeysDeletionStatus": "[{\"keyHandle\":\"16\",\"backingKeyId\":
\"backing-key-id\",\"deletionStatus\":\"FAILURE\"}]"
    },
    "eventID": "c21f1f47-f52b-4ffe-bff0-6d994403cf40",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "111122223333",
    "managementEvent": true,
    "eventCategory": "Management"
}
```


Para eliminar el material de claves del clúster de AWS CloudHSM asociado, siga un procedimiento similar al siguiente. En este ejemplo se usa la AWS CLI y las herramientas de línea de comandos de AWS CloudHSM, pero puede usar la AWS Management Console en lugar de la CLI.

1. Desconecte el almacén de claves de AWS CloudHSM, si aún no está desconectado, e inicie sesión en key_mgmt_util, tal como se explica en Cómo desconectar e iniciar sesión.
2. Utilice el comando deleteKey de key_mgmt_util para eliminar una clave de los HSM del clúster.

   Por ejemplo, este comando elimina la clave 262162 de los HSM del clúster. El identificador clave aparece en la entrada del CloudTrail registro.

   ```
   Command: deleteKey -k 262162

           Cfm3DeleteKey returned: 0x00 : HSM Return: SUCCESS

           Cluster Error Status
           Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
           Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
           Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
   ```
3. Cierre la sesión de key_mgmt_util y vuelva a conectar el almacén de claves de AWS CloudHSM tal como se describe en Cómo cerrar sesión y volver a conectar.

¿Cómo recuperar el material de claves eliminado de una clave KMS?

Si se elimina el material de claves de una AWS KMS key, la clave KMS no podrá utilizarse y todo el texto cifrado con la clave KMS no podrá descifrarse. Esto puede ocurrir si el material de claves de una clave de KMS en un almacén de claves de AWS CloudHSM se elimina del clúster de AWS CloudHSM asociado. Sin embargo, el material de claves se puede recuperar.

Al crear una AWS KMS key (clave de KMS) en un almacén de claves de AWS CloudHSM, AWS KMS inicia sesión en el clúster de AWS CloudHSM asociado y crea el material de claves para la clave de KMS. También cambia la contraseña por un valor que solo conoce él y mantiene la sesión abierta mientras el almacén de claves de AWS CloudHSM esté conectado. Dado que solo puede eliminar la clave su propietario, es decir, el CU que creó la clave, es poco probable que la clave se elimine de los HSM por accidente.

Sin embargo, si el material de claves para una clave KMS se elimina de los HSM en un clúster, el estado de clave de la clave KMS podría cambiar a `UNAVAILABLE`. Si intenta usar la clave de KMS para una operación criptográfica, la operación da error con una excepción `KMSInvalidStateException`. Lo más importante es que todos los datos cifrados con la clave KMS no pueden descifrarse.

Puede recuperar el material de claves eliminado, bajo determinadas circunstancias, creando un clúster a partir de una copia de seguridad que contenga el material de claves. Esta estrategia funciona únicamente si se creó al menos una copia de seguridad mientras existió la clave y antes de que se eliminara.

Utilice el siguiente proceso para recuperar el material de claves.

1. Busque una copia de seguridad del clúster que incluya el material de claves. La copia de seguridad también debe incluir todos los usuarios y claves necesarios para respaldar el clúster y sus datos cifrados.

   Utilice la DescribeBackupsoperación para enumerar las copias de seguridad de un clúster. A continuación, use la marca temporal de la copia de seguridad para seleccionar una copia de seguridad. Para limitar el resultado al clúster asociado con el almacén de claves de AWS CloudHSM, utilice el parámetro `Filters`, tal como se muestra en el siguiente ejemplo.

   ```
   $ aws cloudhsmv2 describe-backups --filters clusterIds=<cluster ID>
   {
       "Backups": [
           {
               "ClusterId": "cluster-1a23b4cdefg",
               "BackupId": "backup-9g87f6edcba",
               "CreateTimestamp": 1536667238.328,
               "BackupState": "READY"
           },
                ...
       ]
   }
   ```

2. Crear un clúster a partir de la copia de seguridad seleccionada. Compruebe que la copia de seguridad contiene la clave eliminada y otros usuarios y claves necesarios para el clúster.
3. Desconecte el almacén de claves de AWS CloudHSM para poder editar sus propiedades.
4. Edite el ID del clúster del almacén de claves de AWS CloudHSM. Escriba el ID del clúster creado a partir de la copia de seguridad. Puesto que el clúster comparte un historial de copias de seguridad con el clúster original, el nuevo ID del clúster debería ser válido.
5. Vuelva a conectar el almacén de claves de AWS CloudHSM.

Cómo iniciar sesión como **kmsuser**

Para crear y administrar el material de claves en el clúster de AWS CloudHSM para el almacén de claves de AWS CloudHSM, AWS KMS usa la cuenta del usuario de criptografía (CU) kmsuser. Cree la cuenta del CU kmsuser en el clúster y proporcione la contraseña a AWS KMS al crear el almacén de claves de AWS CloudHSM.

En general, AWS KMS administra la cuenta de kmsuser. Sin embargo, para algunas tareas, deberá desconectar el almacén de claves de AWS CloudHSM, iniciar sesión en el clúster con el CU kmsuser y utilizar cloudhsm_mgmt_util y las herramientas de línea de comandos key_mgmt_util.

> **Note**
>
> Mientras un almacén de claves personalizado esté desconectado, todos los intentos de crear claves KMS en el almacén de claves personalizado o de usar claves KMS existentes en operaciones criptográficas fallarán. Esta acción puede impedir que los usuarios almacenen y accedan a datos confidenciales.

En este tema, se explica cómo desconectar el almacén de claves de AWS CloudHSM e iniciar sesión como kmsuser, cómo ejecutar la herramienta de línea de comandos de AWS CloudHSM y cerrar sesión y volver a conectar el almacén de claves de AWS CloudHSM.

Temas

- Cómo desconectar e iniciar sesión
- Cómo cerrar sesión y volver a conectar

Cómo desconectar e iniciar sesión

Siga el siguiente procedimiento cada vez que deba iniciar sesión en un clúster asociado con el CU kmsuser.

1. Desconecte el almacén de claves de AWS CloudHSM, si aún no está desconectado. Puede utilizar la consola de AWS KMS o la API de AWS KMS.

   Mientras la clave AWS CloudHSM esté conectada, AWS KMS conserva la sesión como kmsuser. Esto evita que inicie sesión como kmsuser o que cambie la contraseña de kmsuser.

Por ejemplo, este comando se utiliza DisconnectCustomKeyStorepara desconectar un almacén de claves de ejemplo. Reemplace el ID del almacén de claves de AWS CloudHSM de ejemplo por uno válido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

2. Inicie cloudhsm_mgmt_util. Utilice el procedimiento que se describe en la sección Prepararse para ejecutar cloudhsm_mgmt_util de la Guía de usuario de AWS CloudHSM.
3. Inicie sesión en cloudhsm_mgmt_util en el clúster de AWS CloudHSM como responsable de criptografía (CO).

   Por ejemplo, este comando inicia sesión como un CO denominado admin. Reemplace el nombre de usuario y la contraseña del CO de ejemplo por valores válidos.

```
aws-cloudhsm>loginHSM CO admin <password>
loginHSM success on server 0(10.0.2.9)
loginHSM success on server 1(10.0.3.11)
loginHSM success on server 2(10.0.1.12)
```

4. Use el comando changePswd para cambiar la contraseña de la cuenta de `kmsuser` por una que conozca. (AWS KMS rota la contraseña cuando conecta el almacén de claves de AWS CloudHSM). La contraseña debe contener entre 7 y 32 caracteres alfanuméricos, distingue entre mayúsculas y minúsculas, y no puede tener caracteres especiales.

   Por ejemplo, este comando cambia la contraseña de `kmsuser` a `tempPassword`.

```
aws-cloudhsm>changePswd CU kmsuser tempPassword

************************CAUTION*******************************
This is a CRITICAL operation, should be done on all nodes in the
cluster. Cav server does NOT synchronize these changes with the
nodes on which this operation is not executed or failed, please
ensure this operation is executed on all nodes in the cluster.
**************************************************************

Do you want to continue(y/n)?y
Changing password for kmsuser(CU) on 3 nodes
```

5. Inicie sesión en key_mgmt_util o cloudhsm_mgmt_util como `kmsuser` y use la contraseña que ha establecido. Para obtener instrucciones detalladas, consulte Introducción a

cloudhsm_mgmt_util e Introducción a key_mgmt_util. La herramienta que use dependerá de su tarea.

Por ejemplo, este comando inicia sesión en key_mgmt_util.

```
Command: loginHSM -u CU -s kmsuser -p tempPassword
Cfm3LoginHSM returned: 0x00 : HSM Return: SUCCESS

Cluster Error Status
Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
Node id 2 and err state 0x00000000 : HSM Return: SUCCESS
```

Cómo cerrar sesión y volver a conectar

1. Realice la tarea y, a continuación, cierre la sesión de la herramienta de línea de comandos. Si no cierra la sesión, los intentos de volver a conectar al almacén de claves de AWS CloudHSM darán error.

   ```
   Command:  logoutHSM
   Cfm3LogoutHSM returned: 0x00 : HSM Return: SUCCESS

   Cluster Error Status
   Node id 0 and err state 0x00000000 : HSM Return: SUCCESS
   Node id 1 and err state 0x00000000 : HSM Return: SUCCESS
   ```

2. Edite la configuración de la contraseña de `kmsuser` para el almacén de claves personalizado.

   Esto le indica a AWS KMS la contraseña actual para el `kmsuser` en el clúster. Si se salta este paso, AWS KMS no podrá iniciar sesión en el clúster como `kmsuser` y todos los intentos para volver a conectar el almacén de claves personalizado darán error. Puede utilizar la AWS KMS consola o el `KeyStorePassword` parámetro de la UpdateCustomKeyStoreoperación.

   Por ejemplo, este comando le indica a AWS KMS que la contraseña actual es `tempPassword`. Reemplace la contraseña de ejemplo por una real.

   ```
   $ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --
   key-store-password tempPassword
   ```

3. Vuelva a conectar el almacén de claves de AWS KMS a su clúster de AWS CloudHSM. Reemplace el ID del almacén de claves de AWS CloudHSM de ejemplo por uno válido. Durante el proceso de conexión, AWS KMS cambia la contraseña de `kmsuser` por un valor que solo conoce él.

   La ConnectCustomKeyStoreoperación se restablece rápidamente, pero el proceso de conexión puede llevar un período de tiempo prolongado. La respuesta inicial no indica que el proceso de conexión se haya realizado correctamente.

   ```
   $ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
   ```

4. Utilice la DescribeCustomKeyStoresoperación para comprobar que el almacén de AWS CloudHSM claves está conectado. Reemplace el ID del almacén de claves de AWS CloudHSM de ejemplo por uno válido.

   En este ejemplo, el campo del estado de la conexión muestra que ahora el almacén de claves de AWS CloudHSM está conectado.

   ```
   $ aws kms describe-custom-key-stores --custom-key-store-
   id cks-1234567890abcdef0
   {
      "CustomKeyStores": [
         "CustomKeyStoreId": "cks-1234567890abcdef0",
         "CustomKeyStoreName": "ExampleKeyStore",
         "CloudHsmClusterId": "cluster-1a23b4cdefg",
         "TrustAnchorCertificate": "<certificate string appears here>",
         "CreationDate": "1.499288695918E9",
         "ConnectionState": "CONNECTED"
      ],
   }
   ```

Almacenes de claves externos

Los almacenes de claves externos le permiten proteger sus AWS recursos mediante claves criptográficas externas. AWS Esta función avanzada está diseñada para cargas de trabajo reguladas que debe proteger con claves de cifrado almacenadas en un sistema de administración de claves externo controlado por usted. Los almacenes de claves externos respaldan el compromiso de soberanía AWS digital al otorgarle el control soberano sobre sus datos AWS, incluida la posibilidad de cifrarlos con material clave que le pertenezca y que controle fuera de él. AWS

Un almacén de claves externo es un almacén de claves personalizado respaldado por un administrador de claves externo del que eres propietario y desde el que administras. AWS Su administrador de claves externo puede ser un módulo de seguridad de hardware (HSM) físico o virtual, o cualquier sistema basado en hardware o software capaz de generar y utilizar claves criptográficas. El administrador de claves externo realiza operaciones de cifrado y descifrado que utilizan una clave de KMS en un almacén de claves externo mediante el material de claves criptográficas, una función conocida como guardar sus propias claves (HYOK).

AWS KMS nunca interactúa directamente con su administrador de claves externo y no puede crear, ver, administrar ni eliminar sus claves. En su lugar, solo AWS KMS interactúa con el software de proxy de almacenamiento de claves externo (proxy XKS) que usted proporcione. El proxy del almacén de claves externo interviene en todas las comunicaciones entre AWS KMS y el administrador de claves externo. Transmite todas las solicitudes AWS KMS a su administrador de claves externo y transmite las respuestas de su administrador de claves externo a AWS KMSél. El proxy del almacén de claves externo también traduce las solicitudes genéricas AWS KMS a un formato específico del proveedor que su administrador de claves externo pueda entender, lo que le permite utilizar almacenes de claves externos con administradores de claves de diversos proveedores.

Puede utilizar las claves de KMS en un almacén de claves externo para el cifrado del cliente, incluso con el AWS Encryption SDK. Sin embargo, los almacenes de claves externos son un recurso importante para el cifrado del lado del servidor, ya que le permiten proteger sus AWS recursos en múltiples ubicaciones Servicios de AWS con sus claves criptográficas fuera de ellas. AWS Servicios de AWS que admiten claves administradas por el cliente para el cifrado simétrico también admiten claves KMS en un almacén de claves externo. Para obtener más información sobre el soporte, consulte la Integración de servicios de AWS.

Los almacenes de claves externos permiten utilizarlos AWS KMS para cargas de trabajo reguladas, en las que las claves de cifrado deben almacenarse y utilizarse fuera de ellas. AWS Sin embargo, representan una desviación importante del modelo estándar de responsabilidad compartida y requieren cargas operativas adicionales. Para la mayoría de los clientes, el mayor riesgo para la disponibilidad y la latencia superará los beneficios de seguridad de los almacenes de claves externos.

Los almacenes de claves externos le permiten controlar la raíz de la confianza. Los datos cifrados con las claves de KMS de su almacén de claves externo solo se pueden descifrar mediante el administrador de claves externo que usted controle. Si revoca temporalmente el acceso a su administrador de claves externo, por ejemplo, desconectando el almacén de claves externo o

desconectando su administrador de claves externo del proxy del almacén de claves externo, AWS pierde todo el acceso a sus claves criptográficas hasta que lo restaure. Durante ese intervalo, el texto cifrado encriptado con las claves de KMS no se puede descifrar. Si revoca permanentemente el acceso al administrador de claves externo, todo el texto cifrado encriptado con una clave de KMS en su almacén de claves externo no se podrá recuperar. Las únicas excepciones son los AWS servicios que almacenan en caché brevemente las claves de datos protegidas por las claves de KMS. Estas claves de datos seguirán en funcionamiento hasta que desactive el recurso o caduque la memoria caché. Para obtener más detalles, consulte Cómo afectan las claves de KMS obsoletas a las claves de datos.

Los almacenes de claves externos desbloquean los pocos casos de uso para cargas de trabajo reguladas, en las que las claves de cifrado deben permanecer exclusivamente bajo su control y ser inaccesibles para ellas. AWS Sin embargo, se trata de un cambio importante en la forma en que opera la infraestructura basada en la nube y un cambio significativo en el modelo de responsabilidad compartida. Para la mayoría de las cargas de trabajo, la carga operativa adicional y los mayores riesgos para la disponibilidad y el rendimiento superarán los beneficios de seguridad de los almacenes de claves externos.

Más información:

- Anunciamos el almacén de claves externo de AWS KMS en el blog de noticias de AWS .

¿Necesito un almacén de claves externo?

Para la mayoría de los usuarios, el almacén de AWS KMS claves predeterminado, que está protegido por módulos de seguridad de hardware validados por el FIPS 140-2 de nivel de seguridad 3, cumple con sus requisitos normativos, de seguridad y de control. Los usuarios de almacenes de claves externos incurren en altos costos, cargas de mantenimiento y solución de problemas, además de riesgos para la latencia, la disponibilidad y la fiabilidad.

Al considerar un almacén de claves externo, tómese un tiempo para entender las alternativas. Estas incluyen un almacén de claves de AWS CloudHSM respaldado por un clúster de AWS CloudHSM del que es propietario y administra, y claves de KMS con material de clave importado generado en sus propios HSM y que pueda eliminar de las claves de KMS a pedido. En particular, la importación de material de clave con un intervalo de caducidad muy breve podría proporcionar un nivel de control similar sin los riesgos de rendimiento o disponibilidad.

Un almacén de claves externo puede ser la solución adecuada para su organización si tiene los siguientes requisitos:

- Debe utilizar claves criptográficas en su administrador de claves local o en un administrador de claves fuera de su control. AWS
- Debe demostrar que sus claves criptográficas se conservan únicamente bajo su control fuera de la nube.
- Debe cifrar y descifrar mediante claves criptográficas con autorización independiente.
- El material de claves debe estar sujeto a una ruta de auditoría secundaria e independiente.

Si elige un almacén de claves externo, limite su uso a las cargas de trabajo que requieran protección con claves criptográficas fuera de AWS.

Modelo de responsabilidad compartida

Las claves KMS estándar utilizan material clave que se genera y utiliza en los HSM que AWS KMS poseen y administran. Usted establece las políticas de control de acceso en sus claves de KMS y las configura para Servicios de AWS que usen claves de KMS para proteger sus recursos. AWS KMS asume la responsabilidad de la seguridad, la disponibilidad, la latencia y la durabilidad del material clave de sus claves de KMS.

Las claves de KMS de los almacenes de claves externos se basan en el material de clave y las operaciones de su administrador de claves externo. Como tal, el equilibrio de responsabilidades cambia en su dirección. Usted es responsable de la seguridad, la fiabilidad, la durabilidad y el rendimiento de las claves criptográficas de su administrador de claves externo. AWS KMS es responsable de responder con prontitud a las solicitudes y de comunicarse con el proxy de su almacén de claves externo, así como de mantener nuestros estándares de seguridad. Para garantizar que cada clave externa almacene el texto cifrado al menos con la misma seguridad que el AWS KMS texto cifrado estándar, AWS KMS primero cifra todo el texto sin formato con material AWS KMS clave específico de su clave KMS y, a continuación, lo envía a su administrador de claves externo para que lo cifre con su clave externa, un procedimiento conocido como doble cifrado. Como resultado, ni AWS KMS ni el propietario del material de clave externo pueden descifrar por sí solos el texto cifrado con doble cifrado.

Usted es responsable de mantener un administrador de claves externo que cumpla con sus estándares reglamentarios y de rendimiento. También es responsable de proporcionar y mantener

un proxy del almacén de claves externo que cumpla con la especificación de la API del proxy del almacén de claves externo de AWS KMS y de garantizar la disponibilidad y la durabilidad del material de claves. También debe crear, configurar y mantener un almacén de claves externo. Cuando se produzcan errores causados por componentes que usted mantiene, debe estar preparado para identificarlos y resolverlos, de modo que los AWS servicios puedan acceder a sus recursos sin interrupciones indebidas. AWS KMS proporciona una guía de solución de problemas para ayudarle a determinar la causa de los problemas y las soluciones más probables.

Revisa las CloudWatch métricas y dimensiones de Amazon que AWS KMS registran los almacenes de claves externos. AWS KMS le recomienda encarecidamente que cree CloudWatch alarmas para supervisar su almacén de claves externo, de modo que pueda detectar los primeros signos de problemas operativos y de rendimiento antes de que se produzcan.

¿Qué está cambiando?

Los almacenes de claves externos solo admiten claves de KMS de cifrado simétrico. En su interior AWS KMS, las claves de KMS se utilizan y administran en un almacén de claves externo prácticamente de la misma manera que se administran otras claves administradas por el cliente, lo que incluye la configuración de políticas de control de acceso y la supervisión del uso de las claves. Utiliza las mismas API con los mismos parámetros para solicitar una operación criptográfica con una clave de KMS en un almacén de claves externo que utilice para cualquier clave de KMS. El precio también es el mismo que el de las claves de KMS estándar. Para obtener más información, consulte Precios de AWS Key Management Service, Administrar claves de KMS en un almacén de claves externo y Utilizar claves de KMS en un almacén de claves externo.

Sin embargo, con los almacenes de claves externos cambian los siguientes principios:

- Usted es responsable de la disponibilidad, la durabilidad y la latencia de las operaciones de claves.
- Usted es responsable de todos los costos de desarrollo, compra, operación y licencias de su sistema de administración de claves externo.
- Puede implementar la autorización independiente de todas las solicitudes desde AWS KMS el proxy de su almacén de claves externo.
- Puede supervisar, auditar y registrar todas las operaciones de su proxy de almacén de claves externo y todas las operaciones de su administrador de claves externo relacionadas con AWS KMS las solicitudes.

¿Por dónde empiezo?

Para crear y administrar un almacén de claves externo, debe elegir la opción de conectividad proxy del almacén de claves externo, reunir los requisitos previos y crear y configurar el almacén de claves externo. Para empezar, consulte Planificación de un almacén de claves externo.

Cuotas

AWS KMS permite hasta 10 almacenes de claves personalizados en cada Cuenta de AWS región, incluidos los almacenes de AWS CloudHSM claves y los almacenes de claves externos, independientemente del estado de conexión. Además, hay cuotas de solicitudes de AWS KMS sobre el uso de claves KMS en un almacén de claves externo.

Si elige la conectividad de proxy de VPC para su proxy de almacén de claves externo, es posible que también haya cuotas en los componentes necesarios, como las VPC, las subredes y los equilibradores de carga de red. Para obtener más información sobre estas cuotas, utilice la consola de Service Quotas.

Regiones

Para minimizar la latencia de la red, cree los componentes del almacén de claves externo en la Región de AWS más cercana a su administrador de claves externo. Si es posible, elija una región con un tiempo de ida y vuelta (RTT) de la red de 35 milisegundos o menos.

Los almacenes de claves externos son compatibles Regiones de AWS en todos los AWS KMS países, excepto en China (Pekín) y China (Ningxia).

Características no admitidas

AWS KMS no admite las siguientes funciones en los almacenes de claves personalizadas.

- Claves de KMS asimétricas
- Pares de claves de datos asimétricas
- Claves KMS HMAC
- Claves KMS con material de claves importado
- Rotación automática de claves
- Claves de varias regiones

Temas

Conceptos del almacén de claves externo

En este tema se explican algunos de los conceptos empleados en los almacenes de claves externos.

Temas

Almacén de claves externo

Un almacén de claves externo es un almacén de claves AWS KMS personalizado respaldado por un administrador de claves externo al AWS que usted posee y administra. Cada clave de KMS de un almacén de claves externo está asociada a una clave externa del administrador de claves externo. Cuando utiliza una clave de KMS en un almacén de claves externo para el cifrado o el descifrado, la operación se realiza en el administrador de claves externo mediante su clave externa, una función conocida como Guardar sus propias claves (HYOK). Esta función está diseñada para organizaciones que deben mantener las claves criptográficas en su propio administrador de claves externo.

Los almacenes de claves externos garantizan que las claves criptográficas y las operaciones que protegen sus AWS recursos permanezcan en el administrador de claves externo que está bajo su

control. AWS KMS envía solicitudes a su administrador de claves externo para cifrar y descifrar datos, pero AWS KMS no puede crear, eliminar ni administrar ninguna clave externa. Todas las solicitudes AWS KMS a su administrador de claves externo están mediadas por un componente de software proxy de almacenamiento de claves externo que usted suministra, posee y administra.

AWS Los servicios que admiten claves administradas por el AWS KMS cliente pueden usar las claves KMS de su almacén de claves externo para proteger sus datos. Como resultado, sus datos se protegen en última instancia mediante sus claves mediante las operaciones de cifrado de su administrador de claves externo.

Las claves de KMS de un almacén de claves externo tienen modelos de confianza, acuerdos de responsabilidad compartida y expectativas de rendimiento fundamentalmente diferentes a los de las claves de KMS estándar. Con los almacenes de claves externos, usted es responsable de la seguridad e integridad del material de clave y de las operaciones criptográficas. La disponibilidad y la latencia de las claves de KMS en un almacén de claves externo se ven afectadas por el equipo, el software, los componentes de red y la distancia entre AWS KMS y el administrador de claves externo. También es probable que incurra en costes adicionales para el administrador de claves externo y para la infraestructura de redes y equilibrio de carga que necesita para comunicarse con su administrador de claves externo AWS KMS

Puede utilizar su almacén de claves externo como parte de una estrategia más abarcativa de protección de datos. Para cada AWS recurso que proteja, puede decidir cuáles requieren una clave KMS en un almacén de claves externo y cuáles pueden protegerse mediante una clave KMS estándar. Esto le brinda la flexibilidad de elegir claves de KMS para clasificaciones de datos, aplicaciones o proyectos específicos.

Administrador de claves externo

Un administrador de claves externo es un componente ajeno a AWS que puede generar claves simétricas AES de 256 bits y realizar un cifrado y descifrado simétricos. El administrador de claves externo para un almacén de claves externo puede ser un módulo de seguridad de hardware (HSM) físico, un HSM virtual o un administrador de claves de software con o sin un componente de HSM. Puede estar ubicado en cualquier lugar fuera de AWS, incluso en sus instalaciones, en un centro de datos local o remoto o en cualquier nube. Su almacén de claves externo puede estar respaldado por un único administrador de claves externo o por varias instancias de administrador de claves relacionadas que compartan claves criptográficas, como un clúster de HSM. Los almacenes de claves externos están diseñados para dar soporte a una variedad de administradores externos de diferentes proveedores. Para obtener más información sobre los requisitos del administrador de claves externo, consulte Planificación de un almacén de claves externo.

Clave externa

Cada clave de KMS de un almacén de claves externo está asociada a una clave criptográfica del administrador de claves externo conocida como clave externa. Al cifrar o descifrar con una clave de KMS en su almacén de claves externo, la operación criptográfica se realiza en su administrador de claves externo utilizando su clave externa.

> **Warning**
>
> La clave externa es esencial para el funcionamiento de la clave de KMS. Si se pierde o se elimina la clave externa, el texto cifrado con la clave KMS asociada será irrecuperable.

Para los almacenes de claves externos, la clave externa debe ser una clave AES de 256 bits que esté habilitada y pueda realizar el cifrado y el descifrado. Para obtener información detallada sobre los requisitos de clave externa, consulte Requisitos para una clave de KMS en un almacén de claves externo.

AWS KMS no puede crear, eliminar ni administrar ninguna clave externa. El material de claves criptográficas nunca sale de su administrador de claves externo. Cuando crea una clave de KMS en un almacén de claves externo, proporciona el ID de una clave externa (`XksKeyId`). No puede cambiar el ID de clave externa asociado a una clave de KMS, aunque el administrador de claves externo puede cambiar el material de clave asociado al ID de clave externa.

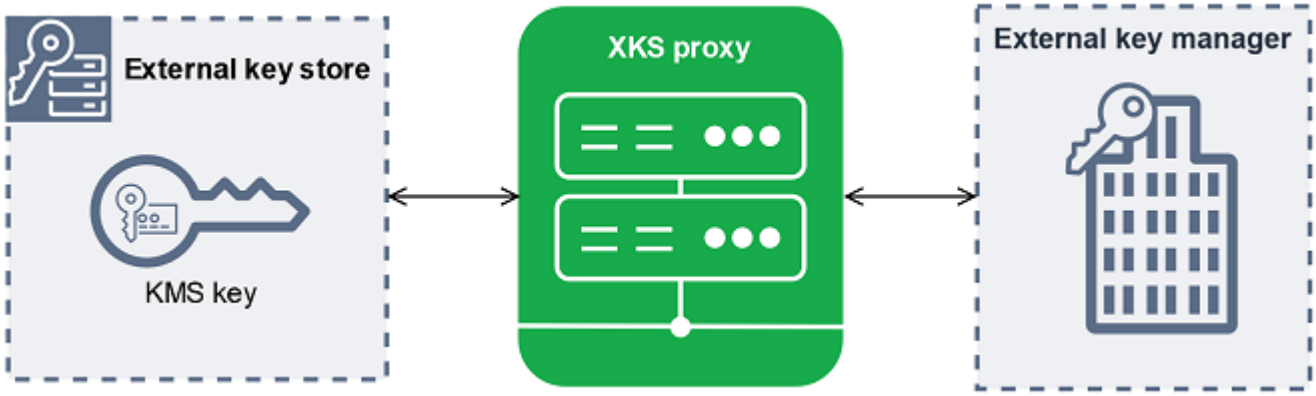
Además de la clave externa, una clave de KMS en un almacén de claves externo también contiene material de clave de AWS KMS . Los datos protegidos por la clave KMS se cifran primero AWS KMS con el material de la AWS KMS clave y, a continuación, mediante el administrador de claves externo con la clave externa. Este proceso de doble cifrado garantiza que el texto cifrado protegido por su clave de KMS esté siempre tan seguro como el texto cifrado protegido solo por AWS KMS.

Muchas claves criptográficas tienen diferentes tipos de identificadores. Al crear una clave de KMS en un almacén de claves externo, proporcione el ID de la clave externa que el proxy del almacén de claves externo utiliza para hacer referencia a la clave externa. Si utiliza un identificador incorrecto, el intento de crear una clave de KMS en su almacén de claves externo no tendrá éxito.

Proxy del almacén de claves externo

El proxy de almacenamiento de claves externo («proxy XKS») es una aplicación de software propiedad y gestionada por el cliente que interviene en todas las comunicaciones entre AWS KMS

el administrador de claves externo y el administrador de claves externo. También traduce AWS KMS las solicitudes genéricas a un formato que el administrador de claves externo específico del proveedor comprenda. Se necesita un proxy del almacén de claves externo para un almacén de claves externo. Cada almacén de claves externo está asociado a un proxy del almacén de claves externo.



AWS KMS no puede crear, eliminar ni administrar ninguna clave externa. El material de claves criptográficas nunca sale de su administrador de claves externo. Toda la comunicación entre su administrador de claves externo AWS KMS y su administrador de claves externo está mediada por el proxy del almacén de claves externo. AWS KMS envía las solicitudes al proxy del almacén de claves externo y recibe las respuestas del proxy del almacén de claves externo. El proxy del almacén de claves externo es responsable de transmitir las solicitudes AWS KMS a su administrador de claves externo y de transmitir las respuestas de su administrador de claves externo a AWS KMS

Usted posee y administra el proxy del almacén de claves externo de su almacén de claves externo, y es responsable de su mantenimiento y funcionamiento. Puede desarrollar su proxy de almacén de claves externo basándose en la especificación de la API de proxy de almacén de claves externo de código abierto que AWS KMS publica o compra una aplicación de proxy a un proveedor. Su proxy del almacén de claves externo puede estar incluido en su administrador de claves externo. Para facilitar el desarrollo de servidores proxy, AWS KMS también proporciona un ejemplo de proxy de almacén de claves externo (aws-kms-xks-proxy) y un cliente de prueba (xks-kms-xksproxy-test-client) que comprueba que el proxy de almacén de claves externo cumple con la especificación.

Para autenticarse, el proxy utiliza certificados AWS KMS TLS del lado del servidor. Para autenticarse en su proxy, AWS KMS firme todas las solicitudes enviadas a su proxy de almacén de claves externo con una credencial de autenticación de proxy SigV4. Si lo desea, su proxy puede habilitar el TLS mutuo (mTLS) para tener la seguridad adicional de que solo acepta solicitudes procedentes de personas. AWS KMS

El proxy del almacén de claves externo debe ser compatible con HTTP/1.1 o posterior y TLS 1.2 o posterior con al menos uno de los siguientes conjuntos de cifrado:

- TLS_AES_256_GCM_SHA384 (TLS 1.3)
- TLS_CHACHA20_POLY1305_SHA256 (TLS 1.3)

> **Note**
>
> AWS GovCloud (US) Region No es compatible con TLS_CHACHA20_POLY1305_SHA256.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (TLS 1.2)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (TLS 1.2)

Para crear y utilizar las claves de KMS en el almacén de claves externo, primero debe conectar el almacén de claves externo a su proxy del almacén de claves externo. También puede desconectar el almacén de claves externo de su proxy cuando lo solicite. Cuando lo haga, todas las claves de KMS del almacén de claves externo dejarán de estar disponibles; no se podrán utilizar en ninguna operación criptográfica.

Conectividad proxy del almacén de claves externo

La conectividad proxy del almacén de claves externo («conectividad proxy XKS») describe el método que se utiliza para comunicarse con el proxy del almacén de claves externo. AWS KMS

Especifica la opción de conectividad de proxy al crear el almacén de claves externo y pasa a ser una propiedad del almacén de claves externo. Puede cambiar la opción de conectividad del proxy al actualizar la propiedad del almacén de claves personalizado, pero debe asegurarse de que el proxy del almacén de claves externo pueda seguir accediendo a las mismas claves externas.

AWS KMS admite las siguientes opciones de conectividad:

- Conectividad de punto final público: AWS KMS envía solicitudes para el proxy de su almacén de claves externo a través de Internet a un punto final público que usted controle. Esta opción es fácil de crear y mantener, pero es posible que no cumpla los requisitos de seguridad de todas las instalaciones.
- Conectividad del servicio de punto final de VPC: AWS KMS envía solicitudes a un servicio de punto final de Amazon Virtual Private Cloud (Amazon VPC) que usted crea y mantiene. Puede alojar su proxy de almacén de claves externo dentro de su Amazon VPC o alojar su proxy de almacén de claves externo fuera AWS y usar la Amazon VPC solo para comunicarse.

Para obtener más información sobre las opciones de conectividad de proxy del almacén de claves externo, consulte Elegir una opción de conectividad del proxy.

Credencial de autenticación de proxy del almacén de claves externo

Para autenticarse en su proxy de almacén de claves externo, AWS KMS firme todas las solicitudes enviadas a su proxy de almacén de claves externo con una credencial de autenticación Signature V4 (SiGv4). Establece y mantiene la credencial de autenticación en el proxy y, a continuación, se la proporciona AWS KMS al crear el almacén externo.

> **Note**
>
> La credencial de SigV4 que se AWS KMS utiliza para firmar las solicitudes al proxy de XKS no tiene relación con ninguna de las credenciales de SigV4 asociadas a los principales de su servidor. AWS Identity and Access Management Cuentas de AWS No reutilice ninguna credencial SigV4 de IAM para su proxy del almacén de claves externo.

Cada credencial de autenticación del proxy tiene dos partes. Debe proporcionar ambas partes al crear un almacén de claves externo o actualizar la credencial de autenticación del almacén de claves externo.

- ID de clave de acceso: identifica la clave de acceso secreta. Puede proporcionar este ID en texto sin formato.
- Clave de acceso secreta: la parte secreta de la credencial. AWS KMS cifra la clave de acceso secreta de la credencial antes de almacenarla.

Puede editar la configuración de la credencial en cualquier momento, por ejemplo, al introducir valores incorrectos, al cambiar la credencial en el proxy o cuando el proxy rota la credencial. Para obtener información técnica sobre la AWS KMS autenticación en el proxy del almacén de claves externo, consulte Autenticación en la especificación de la API del proxy del almacén de claves AWS KMS externo.

Para que pueda cambiar su credencial sin interrumpir las Servicios de AWS que utilizan claves de KMS en su almacén de claves externo, le recomendamos que el proxy del almacén de claves externo admita al menos dos credenciales de autenticación válidas. AWS KMS Esto garantiza que la credencial anterior siga funcionando mientras usted proporciona su nueva credencial a AWS KMS.

Para ayudarlo a realizar un seguimiento de la antigüedad de su credencial de autenticación de proxy, AWS KMS define una CloudWatch métrica de Amazon, XksProxyCredentialAge. Puede usar esta métrica para crear una CloudWatch alarma que le notifique cuando la antigüedad de su credencial alcance el umbral que usted establezca.

Para garantizar aún más la seguridad de que AWS KMS solo responde el proxy de su almacén de claves externo, algunos proxy de claves externos admiten la seguridad mutua de la capa de transporte (mTLS). Para obtener más detalles, consulte Autenticación mTLS (opcional).

API de proxy

Para admitir un almacén de claves AWS KMS externo, un proxy de almacén de claves externo debe implementar las API de proxy requeridas, tal como se describe en la especificación de la API de proxy del almacén de claves AWS KMS externo. Estas solicitudes de API de proxy son las únicas solicitudes que se AWS KMS envían al proxy. Aunque nunca envíe estas solicitudes directamente, conocerlas puede ayudarlo a solucionar cualquier problema que pueda surgir con el almacén de claves externo o el proxy. Por ejemplo, AWS KMS incluye información sobre la latencia y las tasas de éxito de estas llamadas a la API en sus CloudWatch métricas de Amazon para almacenes de claves externos. Para obtener más detalles, consulte Monitoreo de un almacén de claves externo.

En la siguiente tabla se enumeran y describen todas las API de proxy. También incluye las AWS KMS operaciones que desencadenan una llamada a la API de proxy y cualquier excepción de AWS KMS operación relacionada con la API de proxy.

API de proxy	Descripción	AWS KMS Operaciones relacionadas
Decrypt	AWS KMS envía el texto cifrado que se va a descifrar y el identificador de la clave externa que se va a utilizar. El algoritmo de cifrado requerido es AES_GCM.	Descifrar, ReEncrypt
Encrypt	AWS KMS envía los datos que se van a cifrar y el ID de la clave externa que se va a utilizar. El algoritmo de cifrado requerido es AES_GCM.	Cifrar,, GenerateDataKey, GenerateDataKeyWithoutPlaintextReEncrypt

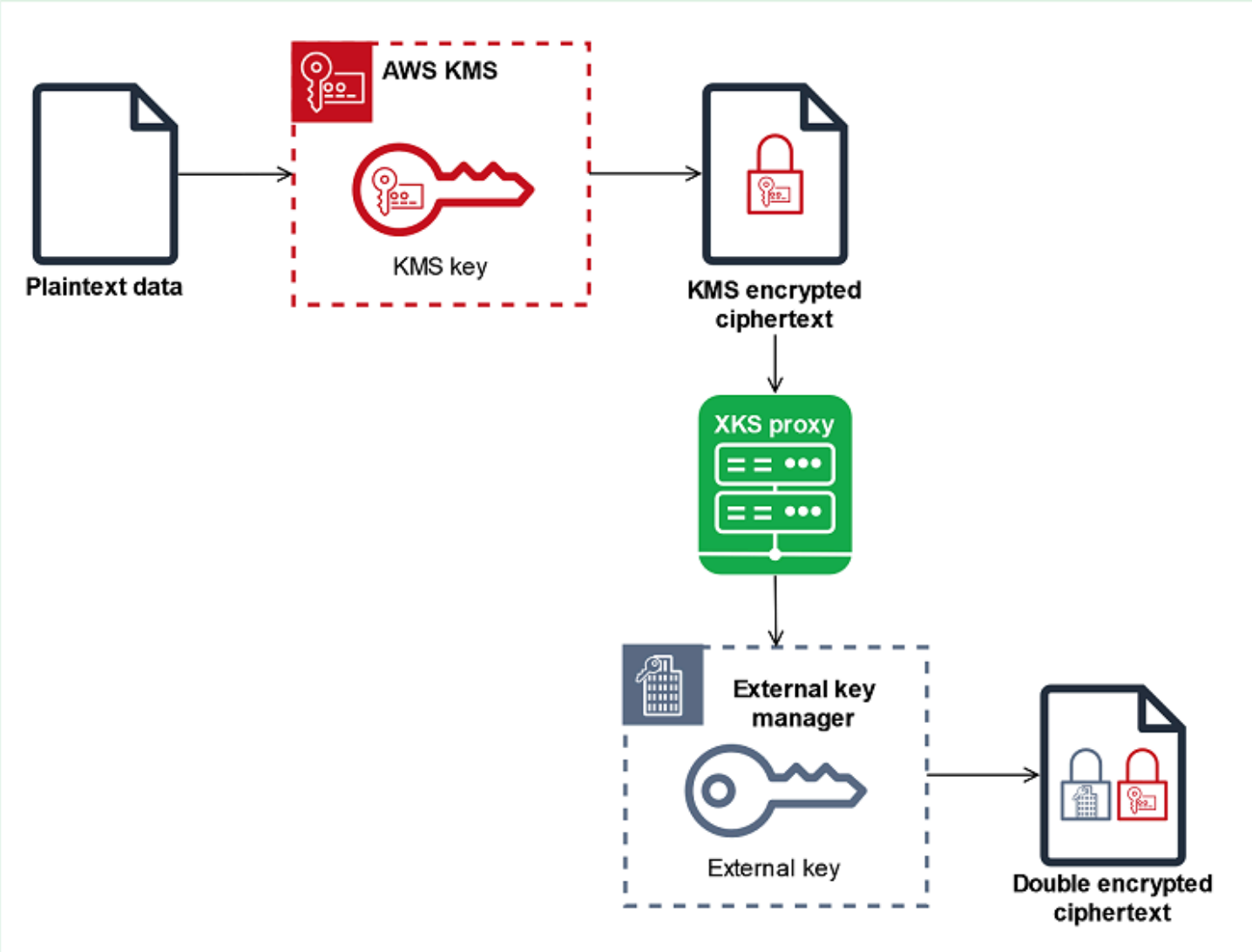
API de proxy	Descripción	AWS KMS Operaciones relacionadas
GetHealthStatus	AWS KMS solicita información sobre el estado del proxy y de su administrador de claves externo. El estado de cada administrador de claves externo puede ser uno de los siguientes. • `Active`: en buen estado; puede servir al tráfico • `Degraded`: en mal estado, pero puede servir al tráfico • `Unavailable` : en mal estado; no sirve para el tráfico	CreateCustomKeyStore(para conectividad de punto final público), ConnectCustomKeyStore(para conectividad de servicio de punto final de VPC) Si todas las instancias del administrador de claves externo tienen estado `Unavailable` , fallan los intentos de crear o conectar el almacén de claves con `XksProxyUriUnreachableException` .
GetKeyMetadata	AWS KMS solicita información sobre la clave externa asociada a una clave de KMS en su almacén de claves externo. La respuesta incluye la especificación de la clave (`AES_256`), el uso de la clave (`[ENCRYPT, DECRYPT]`) y si la clave externa está `ENABLED` o `DISABLED`.	CreateKey Si la especificación de la clave no es `AES_256`, el uso de la clave no es `[ENCRYPT, DECRYPT]` ni el estado es `DISABLED`, la operación de `CreateKey` fallará con `XksKeyInvalidConfigurationException` .

Cifrado doble

Los datos cifrados por una clave de KMS en un almacén de claves externo se cifran dos veces. En primer lugar, AWS KMS cifra los datos con material AWS KMS clave específico de la clave KMS. A continuación, su administrador de claves externo cifra el texto cifrado por AWS KMS con su clave externa. Este proceso se conoce como doble cifrado.

El doble cifrado garantiza que los datos cifrados por una clave de KMS en un almacén de claves externo sean tan seguros como el texto cifrado con una clave de KMS estándar. También protege el texto sin formato en tránsito desde AWS KMS el proxy del almacén de claves externo. Con el

doble cifrado, conserva el control total de sus textos cifrados. Si revoca el acceso de AWS a su clave externa de forma permanente a través de su proxy externo, todo el texto cifrado que quede en AWS se destruirá mediante una operación criptográfica.



Para habilitar el doble cifrado, cada clave de KMS de un almacén de claves externo tiene dos claves de respaldo criptográficas:

- Un material AWS KMS clave exclusivo de la clave KMS. Este material clave se genera y solo se utiliza en los módulos de seguridad de hardware (HSM) certificados por la norma AWS KMS FIPS 140-2 de nivel de seguridad 3.
- Una clave externa de su administrador de claves externo.

El doble cifrado tiene los siguientes efectos:

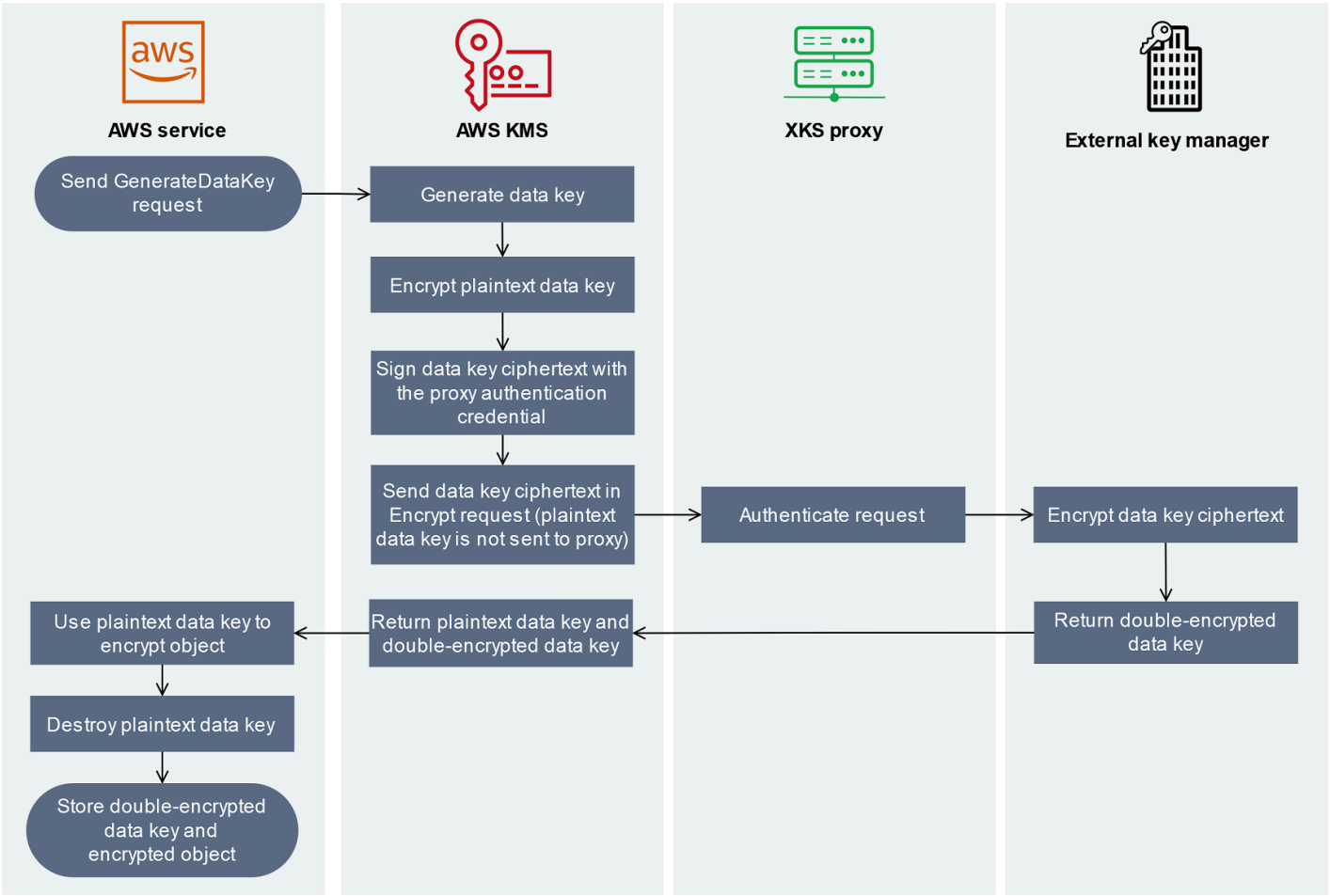
- AWS KMS no puede descifrar ningún texto cifrado mediante una clave KMS en un almacén de claves externo sin acceder a las claves externas a través del proxy del almacén de claves externo.
- No puede descifrar ningún texto cifrado por una clave KMS en un almacén de claves externo externo AWS, incluso si tiene su material de clave externa.
- No puede volver a crear una clave de KMS que se haya eliminado de un almacén de claves externo, aunque disponga de su material de claves externas. Cada clave de KMS tiene metadatos únicos que incluye en el texto cifrado simétrico. Una nueva clave de KMS no podría descifrar el texto cifrado con la clave original, incluso si utilizara el mismo material de clave externa.

Para ver un ejemplo de doble cifrado en la práctica, consulte Cómo funcionan los almacenes de claves externos.

Cómo funcionan los almacenes de claves externos

El almacén de claves externo, el proxy del almacén de claves externo y el administrador de claves externo trabajan en conjunto para proteger los recursos de AWS . El siguiente procedimiento muestra el flujo de trabajo de cifrado típico de Servicio de AWS que cifra cada objeto con una clave de datos única protegida por una clave de KMS. En este caso, ha elegido una clave de KMS en un almacén de claves externo para proteger el objeto. En el ejemplo se muestra cómo se AWS KMS utiliza el doble cifrado para proteger la clave de datos en tránsito y garantizar que el texto cifrado generado por una clave KMS en un almacén de claves externo sea siempre al menos tan seguro como el texto cifrado mediante una clave KMS simétrica estándar con el material clave incluido. AWS KMS

Los métodos de cifrado utilizados por cada entidad que se integra varían. Servicio de AWS AWS KMS Para obtener más información, consulte el tema “Protección de datos” del capítulo Seguridad de la documentación de los Servicio de AWS .



1. Agrega un objeto nuevo a su Servicio de AWS recurso. Para cifrar el objeto, Servicio de AWS envía una GenerateDataKeysolicitud para AWS KMS utilizar una clave KMS en su almacén de claves externo.
2. AWS KMS genera una clave de datos simétrica de 256 bits y se prepara para enviar una copia de la clave de datos en texto plano al administrador de claves externo a través del proxy del almacén de claves externo. AWS KMS inicia el proceso de doble cifrado cifrando la clave de datos en texto plano con el material de clave asociado a la AWS KMS clave KMS en el almacén de claves externo.
3. AWS KMS envía una solicitud de cifrado al proxy del almacén de claves externo asociado al almacén de claves externo. La solicitud incluye el texto cifrado de la clave de datos que se va a cifrar y el ID de la clave externa asociada a la clave KMS. AWS KMS firma la solicitud con la credencial de autenticación del proxy del proxy del almacén de claves externo.

   La copia en texto sin formato de la clave de datos no se envía al proxy del almacén de claves externo.

4. El proxy del almacén de claves externo autentica la solicitud y, a continuación, la pasa a su administrador de claves externo.

   Algunos servidores proxy de almacenes de claves externos también implementan una política de autorización opcional que permite que solo las entidades principales seleccionadas realicen operaciones en condiciones específicas.

5. El administrador de claves externo cifra el texto cifrado de la clave de datos mediante la clave externa especificada. El administrador de claves externo devuelve la clave de datos con doble cifrado al proxy del almacén de claves externo, que la devuelve a AWS KMS.

6. AWS KMS devuelve la clave de datos en texto plano y la copia doblemente cifrada de esa clave de datos al. Servicio de AWS

7. Servicio de AWS Utiliza la clave de datos de texto sin formato para cifrar el objeto de recurso, destruye la clave de datos de texto sin formato y almacena la clave de datos cifrada con el objeto cifrado.

   Algunos Servicios de AWS pueden almacenar en caché la clave de datos de texto sin formato para utilizarla en varios objetos o reutilizarla mientras el recurso está en uso. Para obtener más detalles, consulte Cómo afectan las claves de KMS obsoletas a las claves de datos.

Para descifrar el objeto cifrado, Servicio de AWS deben devolver la clave de datos cifrados a una solicitud AWS KMS de descifrado. Para descifrar la clave de datos cifrada, AWS KMS debe devolverla al proxy del almacén de claves externo con el ID de la clave externa. Si la solicitud de descifrado al proxy del almacén de claves externo falla por algún motivo, AWS KMS no puede descifrar la clave de datos cifrados y Servicio de AWS no puede descifrar el objeto cifrado.

Controlar el acceso al almacén de claves externo

Todas las funciones de control de acceso de AWS KMS (políticas de claves, políticas de IAM y concesiones) que se utilizan con las claves de KMS estándar funcionan de la misma manera con las claves de KMS en un almacén de claves externo. Puede usar las políticas de IAM para controlar el acceso a las operaciones de la API que crean y administran almacenes de claves externos. Usa políticas de IAM y políticas de claves para controlar el acceso a las AWS KMS keys en su almacén de claves externo. También puede usar las políticas de control de servicios de su organización de AWS y las políticas de punto de conexión de VPC para controlar el acceso a las claves de KMS en su almacén de claves externo.

Le recomendamos que únicamente otorgue a los usuarios y roles los permisos necesarios para las tareas que es probable que se vayan a realizar.

Temas

Autorizar a administradores de almacenes de claves externos

Las entidades principales que crean y administran un almacén de claves externo necesitan permisos para las operaciones del almacén de claves personalizado. En la siguiente lista, se describen los permisos mínimos necesarios para los administradores del almacén de claves externo. Como un almacén de claves personalizado no es un recurso de AWS, no puede conceder permisos a un almacén de claves externo para las entidades principales de otras Cuentas de AWS.

- `kms:CreateCustomKeyStore`
- `kms:DescribeCustomKeyStores`
- `kms:ConnectCustomKeyStore`
- `kms:DisconnectCustomKeyStore`
- `kms:UpdateCustomKeyStore`
- `kms:DeleteCustomKeyStore`

Las entidades principales que crean un almacén de claves externo necesitan permiso para crear y configurar los componentes del almacén de claves externo. Las entidades principales pueden crear almacenes de claves externos solo en sus propias cuentas. Para crear un almacén de claves externo con conectividad a los servicios de punto de conexión de VPC, las entidades principales deben tener permiso para crear los siguientes componentes:

- Una VPC de Amazon
- Subredes públicas y privadas
- Un equilibrador de carga de red y grupo de destino
- Un servicio de punto de conexión de VPC

Para obtener más información, consulte Identity and Access Management para Amazon VPC, Identity and Access Management para puntos de conexión de VPC y servicios de puntos de conexión de VPC y Elastic Load Balancing API permissions (Permisos de la API de Elastic Load Balancing).

Autorización de usuarios de claves de KMS en almacenes de claves externos

Las entidades principales que crean y administran AWS KMS keys del almacén de claves externo necesitan los mismos permisos que aquellas que crean y administran las claves de KMS en AWS KMS. La política de claves predeterminada para claves de KMS en un almacén de claves externo es idéntica a la política de claves predeterminada para claves de KMS en AWS KMS. El control de acceso basado en atributos (ABAC), que utiliza etiquetas y alias para controlar el acceso a las claves de KMS, también es efectivo para claves de KMS en almacenes de claves externos.

Las entidades principales que usan las claves KMS en el almacén de claves personalizado para operaciones criptográficas requieren permiso para realizar la operación criptográfica con la clave KMS, por ejemplo, kms:Decrypt. Puede proporcionar estos permisos en una política de IAM o en una política de claves. Sin embargo, no necesitan más permisos para utilizar una clave KMS en un almacén de claves personalizado.

Para establecer un permiso que se aplique solo a las claves de KMS en un almacén de claves externo, utilice la condición de política `kms:KeyOrigin` con un valor de `EXTERNAL_KEY_STORE`. Puede usar esta condición para limitar el permiso kms: o cualquier CreateKey permiso que sea específico de un recurso clave de KMS. Por ejemplo, la siguiente política de IAM permite a la identidad a la que está asociada llamar a las operaciones especificadas en cualquier clave de KMS de la cuenta, siempre que las claves de KMS se encuentren en un almacén de claves externo. Tenga en cuenta que puede limitar el permiso a las claves de KMS de un almacén de claves externo y a las claves de KMS en una Cuenta de AWS, pero no a cualquier almacén de claves externo en particular en la cuenta.

```
{
  "Sid": "AllowKeysInExternalKeyStores",
  "Effect": "Allow",
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:key/*",
```

```
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "EXTERNAL_KEY_STORE"
    }
  }
}
```

Autorización de AWS KMS para la comunicación con su proxy del almacén de claves externo

AWS KMS se comunica con su administrador de claves externo únicamente a través del proxy del almacén de claves externo que usted proporcione. AWS KMS autentica en su proxy firmando sus solicitudes mediante el proceso Signature Version 4 (SigV4) con la credencial de autenticación del proxy del almacén de claves externo que usted especifique. Si utiliza conectividad a un punto de conexión público para su proxy del almacén de claves externo, AWS KMS no requiere ningún permiso adicional.

Sin embargo, si utiliza la conectividad al servicio de punto de conexión de VPC, debe conceder permiso a AWS KMS para crear un punto de conexión de interfaz para su servicio de punto de conexión de VPC de Amazon. Este permiso es necesario independientemente de si el proxy del almacén de claves externo se encuentra en la VPC o si el proxy del almacén de claves externo se encuentra en otro lugar, pero utiliza el servicio del punto de conexión de VPC para comunicarse con AWS KMS.

AWS KMSPara permitir la creación de un punto final de interfaz, utilice la consola de Amazon VPC o la ModifyVpcEndpointServicePermissionsoperación. Conceda permisos para la siguiente entidad principal: `cks.kms.<region>.amazonaws.com`.

Por ejemplo, el siguiente comando de la AWS CLI permite que AWS KMS se conecte al servicio del punto de conexión de VPC especificado en la región Oeste de EE. UU. (Oregón) (us-west-2). Antes de ejecutar este comando, reemplace el ID de servicio de la VPC de Amazon y la Región de AWS con valores válidos para su configuración.

```
modify-vpc-endpoint-service-permissions
--service-id vpce-svc-12abc34567def0987
--add-allowed-principals '["cks.kms.us-west-2.amazonaws.com"]'
```

Para eliminar este permiso, utilice la consola de Amazon VPC o el parámetro ModifyVpcEndpointServicePermissionswith. `RemoveAllowedPrincipals`

Autorización del proxy del almacén de claves externo (opcional)

Algunos proxy del almacén de claves externo implementan requisitos de autorización para el uso de sus claves externas. Se permite, pero no es obligatorio, utilizar un proxy del almacén de claves externo para diseñar e implementar un esquema de autorización que permita a determinados usuarios solicitar ciertas operaciones únicamente en determinadas condiciones. Por ejemplo, un proxy puede configurarse para permitir al usuario A cifrar con una clave externa determinada, pero no descifrar con ella.

La autorización del proxy es independiente de la autenticación del proxy basada en SigV4 que AWS KMS requiere para todos los proxy del almacén de claves externo. También es independiente de las políticas de clave, las políticas de IAM y las concesiones que autorizan el acceso a las operaciones que afectan al almacén de claves externo o a sus claves de KMS.

Para habilitar la autorización por parte del proxy del almacén de claves externo, AWS KMS incluye metadatos en cada solicitud de la API de proxy, incluidos la persona que llama, la clave de KMS, la operación AWS KMS y el Servicio de AWS (si la hubiera). Los metadatos de solicitud para la versión 1 (v1) de la API del proxy de clave externa son los siguientes.

```
"requestMetadata": {
    "awsPrincipalArn": string,
    "awsSourceVpc": string, // optional
    "awsSourceVpce": string, // optional
    "kmsKeyArn": string,
    "kmsOperation": string,
    "kmsRequestId": string,
    "kmsViaService": string // optional
}
```

Por ejemplo, puede configurar su proxy para permitir las solicitudes de una entidad principal específica (`awsPrincipalArn`), pero solo cuando la solicitud la realiza una entidad principal en nombre de un Servicio de AWS (`kmsViaService`) específico.

Si se produce un error en la autorización del proxy, la operación AWS KMS relacionada falla con un mensaje que explica el error. Para obtener más información, consulte Problemas de autorización de proxy.

Autenticación mTLS (opcional)

Para permitir que su proxy del almacén de claves externo autentique solicitudes desde AWS KMS, AWS KMS firma todas las solicitudes en su proxy del almacén de claves externo con una credencial de autenticación del proxy de Signature V4 (SigV4).

Para garantizar aún más que el proxy de su almacén de claves externo solo responda a las solicitudes AWS KMS, algunos proxy de clave externos admiten seguridad mutua de la capa de transporte (mTLS), en la que ambas partes de una transacción utilizan certificados para autenticarse entre sí. mTLS agrega la autenticación del cliente (en la que el servidor del proxy del almacén de claves externo autentica el cliente de AWS KMS) a la autenticación del servidor que proporciona la TLS estándar. En el caso improbable de que su credencial de autenticación de proxy se vea comprometida, mTLS impide que un tercero realice solicitudes de API satisfactorias al proxy del almacén de claves externo.

Para implementar la mTLS, configure su proxy del almacén de claves externo para que solo acepte certificados TLS del cliente con las siguientes propiedades:

- El nombre común del asunto en el certificado TLS debe ser `cks.kms.<Region>.amazonaws.com`, por ejemplo, `cks.kms.eu-west-3.amazonaws.com`.
- El certificado debe estar vinculado a una autoridad de certificación asociada a Amazon Trust Services.

Planificación de un almacén de claves externo

Antes de crear el almacén de claves externo, elija la opción de conectividad que determina la forma en que AWS KMS se comunica con los componentes del almacén de claves externo. La opción de conectividad que elija determina el resto del proceso de planificación.

Más información:

- Revise el proceso de creación de un almacén de claves externo, incluido el ensamblaje de los requisitos previos. Lo ayudará a asegurarse de que dispone de todos los componentes que necesita para crear su almacén de claves externo.
- Aprenda a controlar el acceso a su almacén de claves externo, incluidos los permisos que requieren los administradores y usuarios del almacén de claves externo.
- Obtén información sobre las CloudWatch métricas y dimensiones de Amazon que AWS KMS registran los almacenes clave externos. Le recomendamos encarecidamente que cree alarmas

para monitorear su almacén de claves externo y así poder detectar los primeros signos de problemas operativos y de rendimiento.

Elegir una opción de conectividad del proxy

Si está creando un almacén de claves externo, debe determinar cómo AWS KMS se comunica con su proxy del almacén de claves externo. Esta elección determinará qué componentes necesita y cómo configurarlos. AWS KMS admite las siguientes opciones de conectividad. Elija la opción que se ajuste a sus objetivos de rendimiento y seguridad.

Antes de empezar, confirme que necesita un almacén de claves externo. La mayoría de los clientes pueden usar claves de KMS respaldadas por material de claves de AWS KMS.

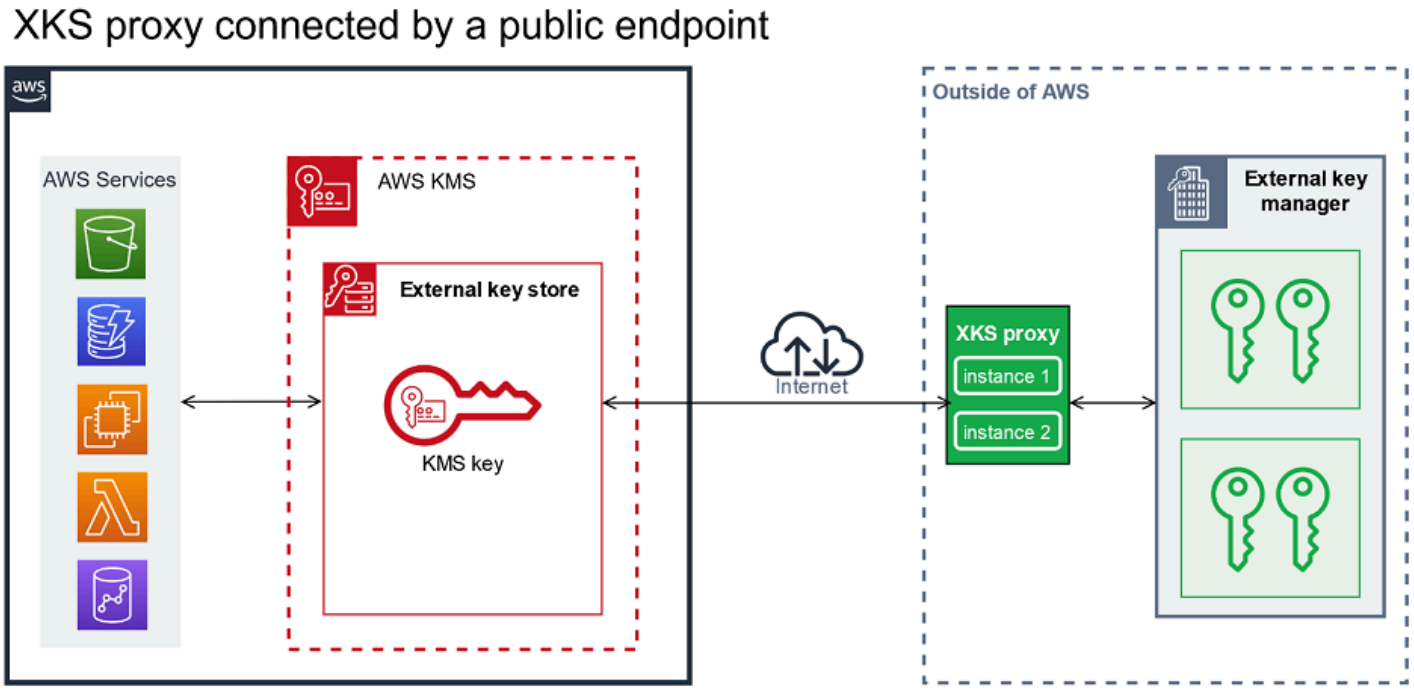
> **Note**
>
> Si el proxy del almacén de claves externo está integrado en el administrador de claves externo, es posible que la conectividad esté predeterminada. Para obtener orientación, consulte la documentación de su administrador de claves externo o proxy del almacén de claves externo.

Puede cambiar la opción de conectividad proxy del almacén de claves externo incluso en un almacén de claves externo en funcionamiento. Sin embargo, el proceso debe planificarse y ejecutarse en detalle para minimizar las interrupciones, evitar errores y garantizar el acceso continuo a las claves criptográficas que cifran los datos.

Conectividad de punto de conexión público

AWS KMS se conecta al proxy del almacén de claves externo (proxy XKS) a través de Internet mediante un punto de conexión público.

Esta opción de conectividad es más fácil de configurar y mantener, y se alinea bien con algunos modelos de administración de claves. Sin embargo, es posible que no cumpla con los requisitos de seguridad de algunas organizaciones.



Requisitos

Si elige la conectividad de punto de conexión público, se requiere lo siguiente.

- El proxy de su almacén de claves externo debe estar accesible en un punto de conexión que se pueda enrutar públicamente.
- Puede utilizar el mismo punto de conexión público para varios almacenes de claves externos, siempre que utilicen valores de ruta URI de proxy diferentes.
- No puede utilizar el mismo punto de conexión para un almacén de claves externo con conectividad de punto de conexión público y ningún almacén de claves externo con conectividad de servicios de punto de conexión de VPC en la misma Región de AWS, incluso si los almacenes de claves se encuentran en diferentes ubicaciones de Cuentas de AWS.
- Debe obtener un certificado TLS emitido por una autoridad de certificación pública compatible con almacenes de claves externos. Para obtener una lista, consulte Autoridades de certificación de confianza.

  El nombre común del sujeto (CN) en el certificado TLS debe coincidir con el nombre de dominio en el punto de conexión URI del proxy para el proxy del almacén de claves externo. Por ejemplo, si el punto de conexión público es `https://myproxy.xks.example.com`, el TLS, el CN del certificado TLS debe ser `myproxy.xks.example.com` o `*.xks.example.com`.

- Asegúrese de que todos los firewalls entre AWS KMS y el proxy del almacén de claves externo permitan el tráfico hacia y desde el puerto 443 del proxy. AWS KMS se comunica en el puerto 443. Este valor no se puede configurar.

Para conocer todos los requisitos de un almacén de claves externo, consulte Ensamblaje de los requisitos previos.

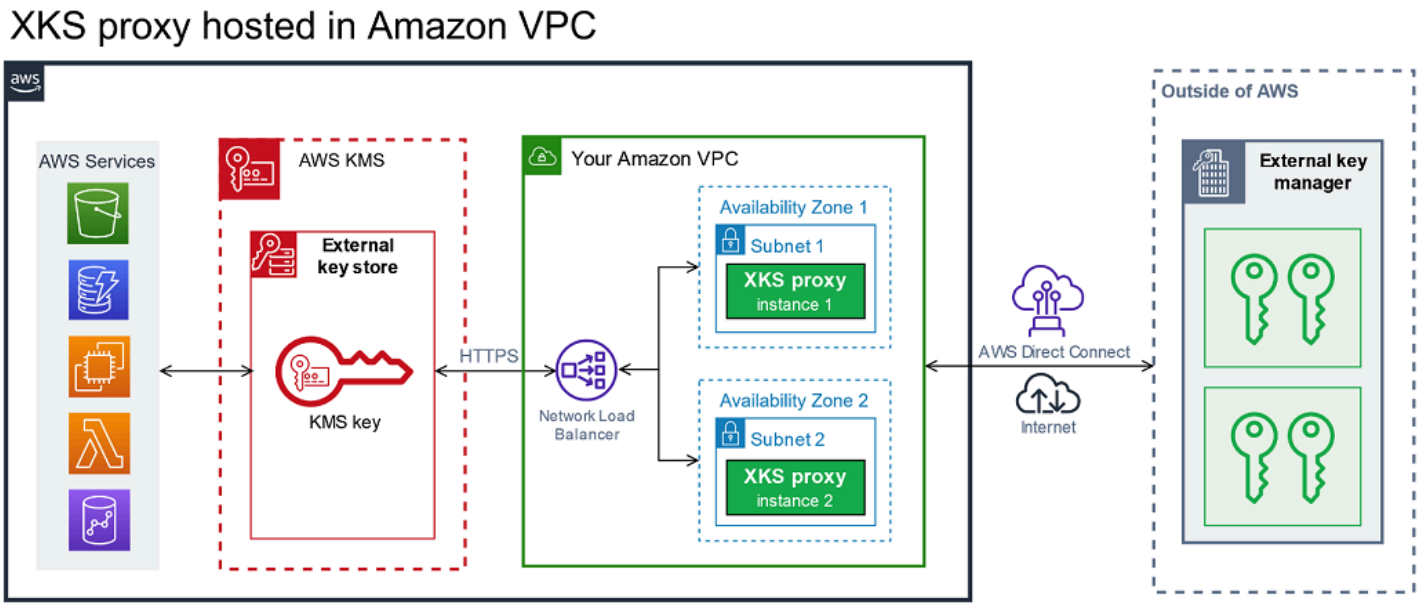
Conectividad del servicio del punto de conexión de VPC

AWS KMS se conecta al proxy del almacén de claves externo (proxy XKS) mediante la creación de un punto de conexión de interfaz para un servicio de punto de conexión de VPC de Amazon que usted cree y configure. Usted es responsable de crear el servicio de punto de conexión de VPC y de conectar la VPC al administrador de claves externo.

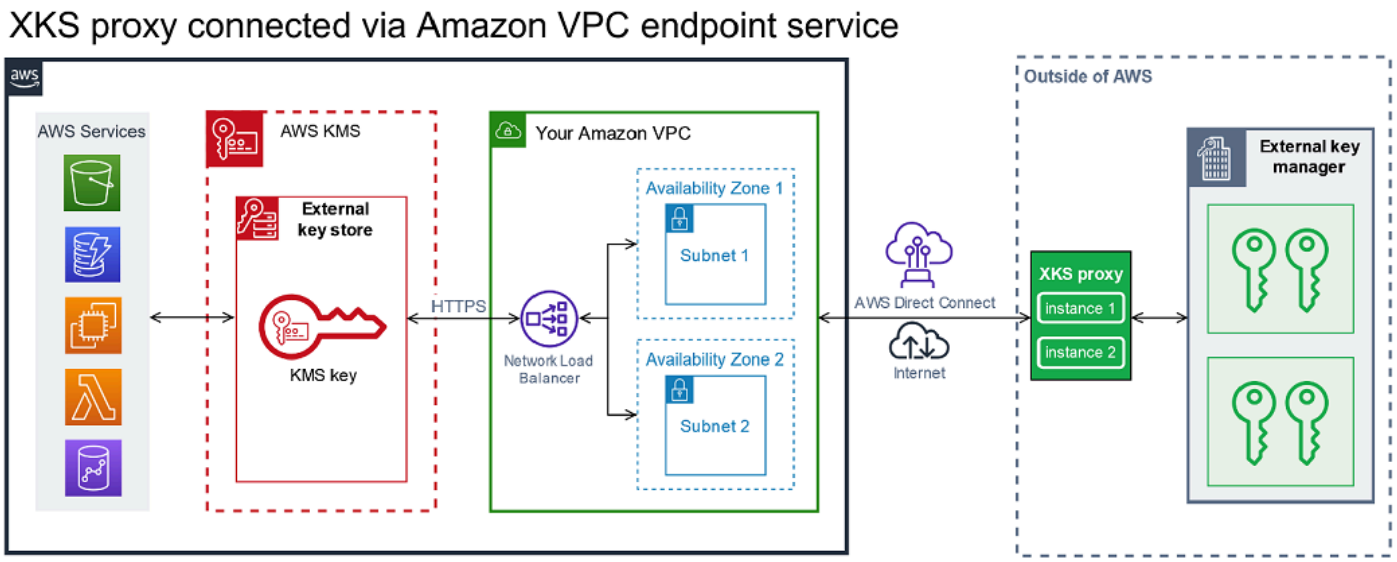
Su servicio de punto de conexión puede usar cualquiera de las opciones compatibles de red a una VPC de Amazon para las comunicaciones, incluidos AWS Direct Connect.

Esta opción de conectividad es más complicada de configurar y mantener. Pero usa un AWS PrivateLink, lo que permite a AWS KMS conectarse de forma privada a su VPC de Amazon y a su proxy del almacén de claves externo sin utilizar la Internet pública.

Puede localizar su proxy del almacén de claves externo en su VPC de Amazon.



O ubique su proxy del almacén de claves externo fuera de AWS y use su servicio de punto de conexión de VPC de Amazon solo para una comunicación segura con AWS KMS.



Configurar la conectividad del servicio de punto de conexión de VPC

Utilice las instrucciones de esta sección para crear y configurar los recursos de AWS y los componentes relacionados que se requieren para un almacén de claves externo que utilice la conectividad de servicios de punto de conexión de VPC. Los recursos que se enumeran para esta opción de conectividad complementan los recursos necesarios para todos los almacenes de claves externos. Después de crear y configurar los recursos necesarios, puede crear su almacén de claves externo.

Puede localizar su proxy de almacén de claves externo en su VPC de Amazon o localizarlo fuera de AWS y utilizar su servicio de punto de conexión de VPC para la comunicación.

Antes de empezar, confirme que necesita un almacén de claves externo. La mayoría de los clientes pueden usar claves de KMS respaldadas por material de claves de AWS KMS.

> **Note**
>
> Es posible que algunos de los elementos necesarios para la conectividad del servicio de punto de conexión de VPC estén incluidos en el administrador de claves externo. Además, es posible que el software tenga requisitos de configuración adicionales. Antes de crear y configurar los recursos de AWS de esta sección, consulte la documentación del proxy y del administrador de claves.

Temas

Requisitos para la conectividad del servicio del punto de conexión de VPC

Si elige la conectividad del servicio de punto de conexión de VPC para su almacén de claves externo, necesitará los siguientes recursos.

Para minimizar la latencia de la red, cree sus componentes de AWS en la Región de AWS compatible que esté más cerca de su administrador de claves externo. Si es posible, elija una región con un tiempo de ida y vuelta (RTT) de la red de 35 milisegundos o menos.

- Una VPC de Amazon que esté conectada a su administrador de claves externo. Debe tener al menos dos subredes privadas en dos zonas de disponibilidad diferentes.

  Puede utilizar una VPC de Amazon existente para su almacén de claves externo, siempre que cumpla los requisitos para su uso con un almacén de claves externo. Varios almacenes de claves externos pueden compartir una VPC de Amazon, pero cada almacén de claves externo debe tener su propio servicio de punto de conexión de VPC y un nombre DNS privado.
- Un servicio de punto de conexión de VPC de Amazon proporcionado por un AWS PrivateLink con un Equilibrador de carga de red y un grupo de destino.

  El servicio de punto de conexión no puede requerir aceptación. Además, debe agregar AWS KMS como entidad principal permitida. Esto permite a AWS KMS crear puntos de conexión de interfaz para que pueda comunicarse con el proxy del almacén de claves externo.
- Un nombre de DNS privado para el servicio de punto de conexión de VPC que es único en su Región de AWS.

  El nombre DNS privado debe ser un subdominio de un dominio público de nivel superior. Por ejemplo, si el nombre DNS privado es `myproxy-private.xks.example.com`, debe ser un subdominio de un dominio público, como `xks.example.com` o `example.com`.

Debe verificar la propiedad del dominio de DNS para el nombre DNS privado.

- Un certificado TLS emitido por una autoridad de certificación pública admitida para su proxy del almacén de claves externo.

  El nombre común del sujeto (CN) en el certificado TLS debe coincidir con el nombre DNS privado. Por ejemplo, si el nombre DNS privado es `myproxy-private.xks.example.com`, el CN del certificado TLS debe ser `myproxy-private.xks.example.com` o `*.xks.example.com`.

Para conocer todos los requisitos de un almacén de claves externo, consulte Ensamblaje de los requisitos previos.

Creación de una VPC de Amazon y de subredes

La conectividad del servicio de punto de conexión de VPC requiere una VPC de Amazon que esté conectada a su administrador de claves externo con al menos dos subredes privadas. Puede crear una VPC de Amazon o utilizar una VPC de Amazon existente que cumpla con los requisitos para los almacenes de claves externos. Para obtener ayuda con la creación de una nueva VPC de Amazon, consulte Crear una VPC en la Guía del usuario de Amazon Virtual Private Cloud.

Requisitos para su VPC de Amazon

Para trabajar con almacenes de claves externos que utilicen la conectividad del servicio de punto de conexión de VPC, la VPC de Amazon debe tener las siguientes propiedades:

- Debe estar en la misma Cuenta de AWS y región admitida que su almacén de claves externo.
- Requiere al menos dos subredes privadas, cada una en una zona de disponibilidad diferente.
- El intervalo de direcciones IP privadas de su VPC de Amazon no debe superponerse con el intervalo de direcciones IP privadas del centro de datos que aloja su administrador de claves externo.
- Todos los componentes deben utilizar IPv4.

Tiene muchas opciones para conectar la VPC de Amazon a su proxy del almacén de claves externo. Elija la opción que se ajuste a sus necesidades de rendimiento y seguridad. Para obtener una lista, consulte Conectar su VPC a otras redes y Opciones de conectividad de red a una VPC de Amazon. Para obtener más detalles, consulte AWS Direct Connect y la Guía del usuario de AWS Site-to-Site VPN.

Creación de una VPC de Amazon para su almacén de claves externo

Use las siguientes instrucciones para crear la VPC de Amazon para su almacén de claves externo. Solo se requiere una VPC de Amazon si elige la opción de conectividad del servicio de punto de conexión de VPC. Puede utilizar una VPC de Amazon existente que cumpla los requisitos para un almacén de claves externo.

Siga las instrucciones que se indican en el tema Crear una VPC, subredes y otros recursos de la VPC con los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
IPv4 CIDR block	Introduzca las direcciones IP de la VPC. El intervalo de direcciones IP privadas de su VPC de Amazon no debe superponerse con el intervalo de direcciones IP privadas del centro de datos que aloja su administrador de claves externo.
Número de zonas de disponibilidad (AZ)	2 o más
Número de subredes públicas	No se requiere ninguna (0)
Número de subredes privadas	Una para cada AZ
Puerta de enlace NAT	No se requiere ninguna.
Puntos de conexión de VPC	No se requiere ninguna.
Enable DNS hostnames	Sí

Campo	Valor
Habilitar la resolución de DNS	Sí

Asegúrese de probar la comunicación de la VPC. Por ejemplo, si su proxy de almacén de claves externo no se encuentra en su VPC de Amazon, cree una instancia de Amazon EC2 en su VPC de Amazon y compruebe que la VPC de Amazon pueda comunicarse con su proxy del almacén de claves externo.

Conexión de la VPC al administrador de claves externo

Conecte la VPC al centro de datos que aloja su administrador de claves externo mediante cualquiera de las opciones de conectividad de red que admite la VPC de Amazon. Asegúrese de que la instancia de Amazon EC2 en la VPC (o el proxy del almacén de claves externo, si está en la VPC) pueda comunicarse con el centro de datos y el administrador de claves externo.

Creación de un grupo de destino

Antes de crear el servicio de punto de conexión de VPC requerido, cree los componentes necesarios, un equilibrador de carga de red (NLB) y un grupo de destino. El equilibrador de carga de red (NLB) distribuye las solicitudes entre varios objetivos en buen estado, cualquiera de los cuales puede atender la solicitud. En este paso, crea un grupo de destino con al menos dos servidores para su proxy del almacén de claves externo y registra sus direcciones IP en el grupo de destino.

Siga las instrucciones que se indican en el tema Configuración de un grupo de destino con los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Tipo de objetivo	Direcciones IP
Protocolo	TCP
Puerto	443

Campo	Valor
Tipo de dirección IP	IPv4
VPC	Elija la VPC en la que va a crear el servicio de punto de conexión de VPC para su almacén de claves externo.
Protocolo y ruta de comprobación de estado	El protocolo y la ruta de comprobación de estado variarán según la configuración del proxy del almacén de claves externo. Consulte la documentación de su administrador de claves externo o proxy del almacén de claves externo. Para obtener información general sobre la configuración de comprobaciones de estado para sus grupos de destino, consulte Comprobaciones de estado para sus grupos de destino en la Guía del usuario del equilibrador de carga elástico para el equilibrador de carga de red.
Network	Otra dirección IP privada
Dirección IPv4	Las direcciones privadas del proxy de su almacén de claves externo
Puertos	443

Creación de un equilibrador de carga de red

El equilibrador de carga de red distribuye el tráfico de la red, incluidas las solicitudes de AWS KMS a su proxy del almacén de claves externo, a los destinos configurados.

Siga las instrucciones del tema Configuración de un equilibrador de carga y un oyente para configurar y agregar un oyente y crear un equilibrador de carga con los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Esquema	Interna
Tipo de dirección IP	IPv4

Campo	Valor
Asignación de redes	Elija la VPC en la que va a crear el servicio de punto de conexión de VPC para su almacén de claves externo.
Correspondencia	Elija las dos zonas de disponibilidad (al menos dos) que configuró para las subredes de VPC. Compruebe los nombres de las subredes y la dirección IP privada.
Protocolo	TCP
Puerto	443
Acción predeterminada: Reenviar a	Elija el grupo de destino para su equilibrador de carga de red.

Creación de un servicio de punto de conexión de VPC

Por lo general, se crea un punto de conexión para un servicio. Sin embargo, cuando crea un servicio de punto de conexión de VPC, usted es el proveedor y AWS KMS crea un punto de conexión para su servicio. Para un almacén de claves externo, cree un servicio de punto de conexión de VPC con el equilibrador de carga de red que creó en el paso anterior. El servicio de punto de conexión de VPC debe estar en la misma Cuenta de AWS y región compatible que su almacén de claves externo.

Varios almacenes de claves externos pueden compartir una VPC de Amazon, pero cada almacén de claves externo debe tener su propio servicio de punto de conexión de VPC y un nombre DNS privado.

Siga las instrucciones del tema Crear un servicio de punto de conexión para crear un servicio de punto de conexión de VPC con los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Tipo de balanceador de carga	Network
Equilibradores de carga disponibles	Elija el equilibrador de carga de red que creó en el paso anterior. Si el nuevo equilibrador de carga no aparece en la lista, compruebe que su estado esté activo. Es posible que el estado del equilibrador de carga tarde unos minutos en cambiar de aprovisionamiento a activo.
Se requiere aceptación	False. Anule la selección de la casilla de verificación. No requieren aceptación. AWS KMS no se puede conectar al servicio de punto de conexión de VPC sin una aceptación manual. Si se requiere la aceptació n, los intentos de crear el almacén de claves externo fallan con una excepción `XksProxyInvalidConfigurationException` .
Habilitación de nombre DNS privado	Asociar un nombre DNS privado con el servicio
Nombre de DNS privado	Introduzca un nombre DNS privado que sea único en su Región de AWS. El nombre DNS privado debe ser un subdominio de un dominio público de nivel superior. Por ejemplo, si el nombre DNS privado es `myproxy-p rivate.xks.example.com` , debe ser un subdominio de un dominio público, como `xks.example.com` o `example.com` . Este nombre DNS privado debe coincidir con el nombre común del asunto (CN) del certificado TLS configurado en el proxy del almacén de claves externo. Por ejemplo, si el nombre DNS privado es `myproxy-private.xk s.example.com` , el CN del certificado TLS debe ser `myproxy-p rivate.xks.example.com` o `*.xks.example.com` . Si el certificado y el nombre DNS privado no coinciden, los intentos de conectar un almacén de claves externo a su proxy del almacén de claves externo fallan con un código de error de conexión de `XKS_PROXY_INVALID_`

Campo	Valor
	`TLS_CONFIGURATION` . Para obtener más detalles, consulte Errores de configuración general.
Tipos de direcciones IP compatibles	IPv4

Verificación del dominio de su nombre DNS privado

Al crear el servicio de punto de conexión de VPC, su estado de verificación de dominio es `pendingVerification`. Antes de utilizar el servicio de punto de conexión de VPC para crear un almacén de claves externo, este estado debe ser `verified`. Para verificar que es el propietario del dominio asociado con su nombre DNS privado, debe crear un registro TXT en un servidor DNS público.

Por ejemplo, si el nombre DNS privado de su servicio de punto de conexión de VPC es `myproxy-private.xks.example.com`, debe crear un registro TXT en un dominio público, como `xks.example.com` o `example.com`, lo que sea público. AWS PrivateLink busca el registro TXT primero en `xks.example.com` y luego en `example.com`.

> **Tip**
>
> Después de agregar un registro TXT, es posible que el estado de verificación del dominio tarde unos minutos en cambiar de `pendingVerification` a `verify`.

Para empezar, busque el estado de verificación de su dominio mediante uno de los siguientes métodos. Los valores válidos son `verified`, `pendingVerification` y `failed`.

- En la consola de VPC de Amazon, seleccione Endpoint services (Servicios de punto de conexión) y elija su servicio de punto de conexión. En el panel de detalles, consulte Estado de verificación del dominio.
- Usa la DescribeVpcEndpointServiceConfigurationsoperación. El valor `State` está en el campo `ServiceConfigurations.PrivateDnsNameConfiguration.State`.

Si el estado de verificación no es `verified`, siga las instrucciones del tema Verificación de la propiedad del dominio para agregar un registro TXT al servidor de DNS de su dominio y comprobar que el registro TXT esté publicado. A continuación, vuelva a comprobar el estado de la verificación.

No es necesario crear un registro A para el nombre de dominio DNS privado. Cuando AWS KMS crea un punto de conexión de interfaz para su servicio de punto de conexión de VPC, AWS PrivateLink crea automáticamente una zona alojada con el registro A requerido para el nombre de dominio privado en la VPC de AWS KMS. Para almacenes de claves externos con conectividad de servicio de punto de conexión de VPC, esto sucede cuando conecta su almacén de claves externo a su proxy de almacén de claves externo.

Autorizar a AWS KMS para que se conecte al servicio de punto de conexión de VPC

Debe agregar AWS KMS a la lista Allow principals (Permitir entidad principal) para su servicio de punto de conexión de VPC. Esto permite a AWS KMS crear puntos de conexión de interfaz para su servicio de punto de conexión de VPC. Si AWS KMS no es una entidad principal permitida, los intentos de crear un almacén de claves externo fallarán con una excepción `XksProxyVpcEndpointServiceNotFoundException`.

Siga las instrucciones del tema Administrar permisos de la Guía de AWS PrivateLink. Use el siguiente valor obligatorio.

Campo	Valor
ARN	`cks.kms.<region>.amazonaws.com` Por ejemplo, `cks.kms.us-east-1.amazonaws.com`

Siguiente: Creación de un almacén de claves externo

Administrar un almacén de claves externo

Puede administrar un almacén de claves externo mediante la consola de AWS KMS o la API de AWS KMS. Puede crear un almacén de claves externo, ver y editar sus propiedades, monitorear su rendimiento y conectarlo y desconectarlo de su proxy del almacén de claves externo y eliminar el almacén de claves externo.

Temas

- Creación de un almacén de claves externo

- Edición de propiedades del almacén de claves externo
- Visualización de un almacén de claves externo
- Monitoreo de un almacén de claves externo
- Conectar y desconectar un almacén de claves externo
- Eliminación de un almacén de claves externo

Creación de un almacén de claves externo

Puede crear uno o varios almacenes de claves externos en cada Cuenta de AWS y región. Cada almacén de claves externo debe estar asociado a un administrador de claves externo fuera de AWS y a un proxy del almacén de claves externo (proxy XKS) que es un mediador de la comunicación entre AWS KMS y su administrador de claves externo. Para obtener más detalles, consulte Planificación de un almacén de claves externo. Antes de empezar, confirme que necesita un almacén de claves externo. La mayoría de los clientes pueden usar claves de KMS respaldadas por material de claves de AWS KMS.

> **Tip**
>
> Algunos administradores de claves externos proporcionan un método más sencillo para crear un almacén de claves externo. Para obtener más detalles, consulte la documentación del administrador de claves externo.

Antes de crear un almacén de claves externo, debe cumplir los requisitos previos. Durante el proceso de creación, usted especifica las propiedades del almacén de claves externo. Lo más importante es que indique si su almacén de claves externo en AWS KMS utiliza un punto de conexión público o un servicio del punto de conexión de VPC para conectarse a su proxy del almacén de claves externo. También especifica los detalles de la conexión, incluido el punto de conexión URI del proxy y la ruta dentro de ese punto de conexión del proxy desde donde AWS KMS envía las solicitudes de API al proxy.

- Si utiliza una conectividad de punto de conexión público, asegúrese de que AWS KMS puede comunicarse con su proxy a través de Internet mediante una conexión HTTPS. Esto incluye configurar TLS en el proxy del almacén de claves externo y garantizar que cualquier firewall entre AWS KMS y el proxy permita el tráfico hacia y desde el puerto 443 del proxy. Al crear un almacén de claves externo con conectividad a un punto de conexión público, AWS KMS prueba la conexión al enviar una solicitud de estado al proxy del almacén de claves externo. Esta prueba comprueba

que se puede acceder al punto de conexión y que el proxy del almacén de claves externo aceptará una solicitud firmada con la credencial de autenticación del proxy del almacén de claves externo. Si se produce un error en esta solicitud de prueba, se produce un error en la operación para crear el almacén de claves externo.

- Si utiliza la conectividad al servicio de punto de conexión de VPC, asegúrese de que el equilibrador de carga de red, el nombre DNS privado y el servicio de punto de conexión de VPC estén configurados correctamente y en funcionamiento. Si el proxy del almacén de claves externo no está en la VPC, debe asegurarse de que el servicio de punto de conexión de VPC pueda comunicarse con el proxy del almacén de claves externo. (AWS KMS prueba la conectividad del servicio del punto de conexión de VPC al conectar el almacén de claves externo a su proxy del almacén de claves externo).

Consideraciones adicionales:

- AWS KMSregistra CloudWatch las métricas y dimensiones de Amazon, especialmente para los almacenes de claves externos. Los gráficos de monitoreo basados en algunas de estas métricas aparecen en la consola de AWS KMS para cada almacén de claves externo. Le recomendamos encarecidamente que utilice estas métricas para crear alarmas que monitoreen su almacén de claves externo. Estas alarmas le avisan de las señales tempranas de problemas operativos y de rendimiento antes de que se produzcan. Para obtener instrucciones, consulte Monitoreo de un almacén de claves externo.
- Los almacenes de claves externos están sujetos a cuotas de recursos. El uso de claves de KMS en un almacén de claves externo está sujeto a las cuotas de solicitud. Revise estas cuotas antes de diseñar la implementación de su almacén de claves externo.

> **Note**
>
> Revise su configuración para ver si hay dependencias circulares que puedan impedir que funcione.
> Por ejemplo, si crea su proxy de almacén de claves externo con recursos de AWS, asegúrese de que el funcionamiento del proxy no requiera la disponibilidad de una clave de KMS en un almacén de claves externo al que se acceda a través de ese proxy.

Todos los nuevos almacenes de claves externos se crean en un estado desconectado. Antes de poder crear claves de KMS en su almacén de claves externo, debe conectarlo a su proxy del

almacén de claves externo. Para cambiar las propiedades del almacén de claves externo, edite la configuración del almacén de claves externo.

Temas

- Cumplir los requisitos previos
- Archivo de configuración del proxy
- Creación de un almacén de claves externo (consola)
- Creación de un almacén de claves externo (API)

Cumplir los requisitos previos

Antes de crear un almacén de claves externo, debe reunir los componentes necesarios, incluido el administrador de claves externo que utilizará para respaldar el almacén de claves externo y el proxy del almacén de claves externo que traduce las solicitudes de AWS KMS a un formato que su administrador de claves externo pueda entender.

Los siguientes componentes son necesarios para todos los almacenes de claves externos. Además de estos componentes, debe proporcionar los componentes que admitan la opción de conectividad al proxy del almacén de claves externo que elija.

> **Tip**
>
> Su administrador de claves externo puede incluir algunos de estos componentes o puede que estén configurados para usted. Para obtener más detalles, consulte la documentación del administrador de claves externo.
> Si está creando su almacén de claves externo en la consola de AWS KMS, tiene la opción de cargar un archivo de configuración del proxy basado en JSON que especifique la ruta URI del proxy y la credencial de autenticación del proxy. Algunos proxy del almacén de claves externos generan este archivo por usted. Para obtener más información, consulte la documentación del proxy del almacén de claves externo o el administrador de claves externo.

Administrador de claves externo

Cada almacén de claves externo requiere al menos una instancia del administrador de claves externo. Puede ser un módulo de seguridad de hardware (HSM) físico o virtual o un software de administración de claves.

Puede usar un único administrador de claves, pero le recomendamos al menos dos instancias del administrador de claves relacionadas que compartan claves criptográficas por motivos de redundancia. El almacén de claves externo no requiere el uso exclusivo del administrador de claves externo. Sin embargo, el administrador de claves externo debe tener la capacidad de administrar la frecuencia esperada de las solicitudes de cifrado y descifrado de los servicios de AWS que utilizan las claves de KMS en el almacén de claves externo para proteger sus recursos. El administrador de claves externo debe configurarse para administrar hasta 1800 solicitudes por segundo y responder dentro del tiempo de espera de 250 milisegundos para cada solicitud. Le recomendamos que ubique el administrador de claves externo cerca de una Región de AWS, de modo que el tiempo de ida y vuelta (RTT) de la red sea de 35 milisegundos o menos.

Si su proxy del almacén de claves externo lo permite, puede cambiar el administrador de claves externo que asocia a su proxy del almacén de claves externo, pero el nuevo administrador de claves externo debe ser una copia de seguridad o una instantánea con el mismo material de claves. Si la clave externa que asocia a una clave de KMS ya no está disponible para su proxy del almacén de claves externo, AWS KMS no podrá descifrar el texto cifrado encriptado con la clave de KMS.

El proxy del almacén de claves externo debe poder acceder al administrador de claves externo. Si la GetHealthStatusrespuesta del proxy indica que todas las instancias del administrador de claves externo lo sonUnavailable, todos los intentos de crear un almacén de claves externo fallan con un `XksProxyUriUnreachableException`.

Proxy del almacén de claves externo

Debe especificar un proxy del almacén de claves externo (proxy XKS) que cumpla con los requisitos de diseño de la especificación de la API de proxy del almacén de claves externo de AWS KMS. Puede desarrollar o comprar un proxy del almacén de claves externo, o utilizar un proxy del almacén de claves externo proporcionado o integrado en su administrador de claves externo. AWS KMS recomienda configurar el proxy del almacén de claves externo para gestionar hasta 1800 solicitudes por segundo y responder dentro del tiempo de espera de 250 milisegundos a cada solicitud. Le recomendamos que ubique el administrador de claves externo cerca de una Región de AWS, de modo que el tiempo de ida y vuelta (RTT) de la red sea de 35 milisegundos o menos.

Puede utilizar un proxy del almacén de claves externo para más de un almacén de claves externo, pero cada almacén de claves externo debe tener un punto de conexión y una ruta de URI únicos dentro del proxy del almacén de claves externo para sus solicitudes.

Si utiliza la conectividad a un servicio de punto de conexión de VPC, puede localizar su proxy del almacén de claves externo en su VPC de Amazon, pero no es obligatorio. Puede localizar su proxy

fuera de AWS, por ejemplo, en su centro de datos privado, y utilizar el servicio de punto de conexión de VPC únicamente para comunicarse con el proxy.

Credencial de autenticación del proxy

Para crear un almacén de claves externo, debe especificar su credencial de autenticación del proxy del almacén de claves externo (`XksProxyAuthenticationCredential`).

Debe establecer una credencial de autenticación (`XksProxyAuthenticationCredential`) para AWS KMS en el proxy de su almacén de claves externo. AWS KMS autentica en su proxy firmando sus solicitudes mediante el proceso Signature Version 4 (SigV4) con la credencial de autenticación del proxy del almacén de claves externo. Debe especificar una credencial de autenticación cuando se crea el almacén de claves externo y se puede cambiar en cualquier momento. Si su proxy rota la credencial, asegúrese de actualizar los valores de la credencial del almacén de claves externo.

La credencial de autenticación del proxy tiene dos partes. Debe proporcionar ambas partes para su almacén de claves externo.

- ID de clave de acceso: identifica la clave de acceso secreta. Puede proporcionar este ID en texto sin formato.
- Clave de acceso secreta: la parte secreta de la credencial. AWS KMS cifra la clave de acceso secreta de la credencial antes de almacenarla.

La credencial SigV4 que utiliza AWS KMS para firmar las solicitudes al proxy del almacén de claves externo no está relacionada con ninguna credencial de SigV4 asociada a las entidades principales de AWS Identity and Access Management de sus cuentas de AWS. No reutilice ninguna credencial SigV4 de IAM para su proxy del almacén de claves externo.

Conectividad de proxy

Para crear un almacén de claves externo, debe especificar su opción de conectividad del proxy del almacén de claves externo (`XksProxyConnectivity`).

AWS KMS puede comunicarse con su proxy del almacén de claves externo mediante un punto de conexión público o un servicio de punto de conexión de Amazon Virtual Private Cloud (Amazon VPC). Si bien un punto de conexión público es más sencillo de configurar y mantener, es posible que no cumpla con los requisitos de seguridad de todas las instalaciones. Si elige la opción de conectividad del servicio de punto de conexión de VPC de Amazon, debe crear y mantener los componentes necesarios, incluida una VPC de Amazon con al menos dos subredes en dos zonas de

disponibilidad diferentes, un servicio del punto de conexión de VPC con un equilibrador de carga de red y un grupo de destino, y un nombre DNS privado para el servicio de punto de conexión de VPC.

Puede cambiar la opción de conectividad del proxy para su almacén de claves externo. Sin embargo, debe asegurar la disponibilidad continua del material de claves asociado a las claves de KMS en su almacén de claves externo. De lo contrario, AWS KMS no podrá descifrar ningún texto cifrado encriptado con esas claves de KMS.

Para obtener ayuda para decidir qué opción de conectividad de proxy es mejor para su almacén de claves externo, consulte Elegir una opción de conectividad del proxy. Para obtener ayuda para crear una configuración de la conectividad del servicio del punto de conexión de VPC, consulte Configurar la conectividad del servicio de punto de conexión de VPC.

Punto de conexión URI del proxy

Para crear un almacén de claves externo, debe especificar el punto de conexión (`XksProxyUriEndpoint`) que AWS KMS se utiliza para enviar las solicitudes al proxy del almacén de claves externo.

El protocolo debe ser HTTPS. AWS KMS se comunica en el puerto 443. No especifique el puerto en el valor del punto de conexión URI del proxy.

- Conectividad al punto de conexión público: especifique el punto de conexión disponible públicamente para su proxy del almacén de claves externo. Se debe poder acceder a este punto de conexión antes de crear el almacén de claves externo.
- Conectividad al servicio de punto de conexión de VPC: especifique `https://` seguido del nombre DNS privado del servicio de punto de conexión de VPC.

El certificado del servidor TLS configurado en el proxy del almacén de claves externo debe coincidir con el nombre de dominio del punto de conexión URI y debe ser emitido por una autoridad de certificación compatible con los almacenes de claves externos. Para obtener una lista, consulte Autoridades de certificación de confianza. La autoridad de certificación exigirá una prueba de la propiedad del dominio antes de emitir el certificado TLS.

El nombre común del sujeto (CN) en el certificado TLS debe coincidir con el nombre DNS privado. Por ejemplo, si el nombre DNS privado es `myproxy-private.xks.example.com`, el CN del certificado TLS debe ser `myproxy-private.xks.example.com` o `*.xks.example.com`.

Puede cambiar el punto de conexión de la URI del proxy, pero asegúrese de que el proxy del almacén de claves externo tenga acceso al material de claves asociado a las claves de KMS de

su almacén de claves externo. De lo contrario, AWS KMS no podrá descifrar ningún texto cifrado encriptado con esas claves de KMS.

Requisitos de singularidad

- El valor combinado del punto de conexión del URI del proxy (`XksProxyUriEndpoint`) y el valor de la ruta URI del proxy (`XksProxyUriPath`) deben ser únicos en la Cuenta de AWS y en la región.
- Los almacenes de claves externos con conectividad al punto de conexión público pueden compartir el mismo punto de conexión URI del proxy, siempre que tengan valores de ruta URI de proxy diferentes.
- Un almacén de claves externo con conectividad al punto de conexión público no puede utilizar el mismo valor de punto de conexión URI de proxy que cualquier almacén de claves externo con conectividad a servicios de punto de conexión de VPC en la misma Región de AWS, incluso si los almacenes de claves se encuentran en diferentes Cuentas de AWS.
- Cada almacén de claves externo con conectividad al punto de conexión de VPC debe tener su propio nombre DNS privado. El punto de conexión URI del proxy (nombre DNS privado) debe ser único en Cuenta de AWS y la región.

Ruta URI del proxy

Para crear un almacén de claves externo, debe especificar la ruta base en su proxy del almacén de claves externo a las API de proxy necesarias. El valor debe empezar con `/` y terminar en /kms/xks/v1, donde `v1` representa la versión de la API de AWS KMS para el proxy del almacén de claves externo. Esta ruta puede incluir un prefijo opcional entre los elementos necesarios, por ejemplo `/example-prefix/kms/xks/v1`. Para encontrar este valor, consulte la documentación de su proxy del almacén de claves externo.

AWS KMS envía las solicitudes de proxy a la dirección especificada mediante la concatenación del punto de conexión de la URI del proxy y la ruta URI del proxy. Por ejemplo, si el punto de conexión de la URI del proxy es `https://myproxy.xks.example.com` y la ruta URI del proxy es `/kms/xks/v1`, AWS KMS envía sus solicitudes de API de proxy a `https://myproxy.xks.example.com/kms/xks/v1`.

Puede cambiar la ruta URI del proxy, pero asegúrese de que el proxy del almacén de claves externo tenga acceso al material de claves asociado a las claves de KMS de su almacén de claves externo. De lo contrario, AWS KMS no podrá descifrar ningún texto cifrado encriptado con esas claves de KMS.

Requisitos de singularidad

- El valor combinado del punto de conexión del URI del proxy (`XksProxyUriEndpoint`) y el valor de la ruta URI del proxy (`XksProxyUriPath`) deben ser únicos en la Cuenta de AWS y en la región.

Servicio de punto de conexión de VPC

Especifica el nombre del servicio de punto de conexión de VPC de Amazon que se utiliza para comunicarse con el proxy del almacén de claves externo. Este componente solo es necesario para los almacenes de claves externos que utilizan la conectividad a servicios de punto de conexión de VPC. Para obtener ayuda para establecer y configurar el servicio de punto de conexión de VPC para un almacén de claves externo, consulte Configurar la conectividad del servicio de punto de conexión de VPC.

El servicio de punto de conexión de VPC debe tener las siguientes propiedades:

- El servicio de punto de conexión de VPC debe estar en la mismaCuenta de AWS y región que el almacén de claves externo.
- Debe tener un equilibrador de carga de red (NLB) conectado a al menos dos subredes, cada una en una zona de disponibilidad diferente.
- La lista de entidades principales permitidas para el servicio de punto de conexión de VPC debe incluir la entidad principal del servicio de AWS KMS de la región: `cks.kms.<region>.amazonaws.com`, por ejemplo `cks.kms.us-east-1.amazonaws.com`.
- No debe requerir la aceptación de las solicitudes de conexión.
- Debe tener un nombre DNS privado dentro de un dominio público de nivel superior. Por ejemplo, podría tener un nombre DNS privado myproxy-private.xks.example.com en el dominio `xks.example.com` público.

  El nombre DNS privado de un almacén de claves externo con conectividad al servicio de punto de conexión de VPC debe ser único en su Región de AWS.
- El estado de verificación de dominio del dominio de su nombre DNS privado debe ser `verified`.
- El certificado de servidor TLS configurado en el proxy del almacén de claves externo debe especificar el nombre de host DNS privado en el que se puede acceder al punto de conexión.

Requisitos de singularidad

- Los almacenes de claves externos con conectividad al punto de conexión de VPC pueden compartir una `Amazon VPC`, pero cada almacén de claves externo debe tener su propio servicio de punto de conexión de VPC y nombre DNS privado.

Archivo de configuración del proxy

Un archivo de configuración del proxy es un archivo opcional basado en JSON que contiene valores para la ruta URI del proxy y las propiedades de las credenciales de autenticación del proxy del almacén de claves externo. Al crear o editar un almacén de claves externo en la consola de AWS KMS, puede cargar un archivo de configuración del proxy para proporcionar los valores de configuración del almacén de claves externo. El uso de este archivo evita errores al escribir y pegar, y garantiza que los valores del almacén de claves externo coincidan con los valores del proxy del almacén de claves externo.

Los archivos de configuración del proxy los genera el proxy del almacén de claves externo. Para saber si su proxy del almacén de claves externo ofrece un archivo de configuración del proxy, consulte la documentación del proxy del almacén de claves externo.

A continuación, se muestra un ejemplo de un archivo de configuración de proxy bien estructurado con valores ficticios.

```
{
  "XksProxyUriPath": "/example-prefix/kms/xks/v1",
  "XksProxyAuthenticationCredential": {
    "AccessKeyId": "ABCDE12345670EXAMPLE",
    "RawSecretAccessKey": "0000EXAMPLEFA5FT0mCc3DrGUe2sti527BitkQ0Zr9MO9+vE="
  }
}
```

Solo puede cargar un archivo de configuración del proxy al crear o editar un almacén de claves externo en la consola de AWS KMS. No puede usarlo con las UpdateCustomKeyStoreoperaciones CreateCustomKeyStoreo, pero puede usar los valores del archivo de configuración del proxy para asegurarse de que los valores de los parámetros son correctos.

Creación de un almacén de claves externo (consola)

Antes de crear un almacén de claves externo, revise el Planificación de un almacén de claves externo, elija el tipo de conectividad de proxy y asegúrese de haber creado y configurado todos los componentes necesarios. Si necesita ayuda para encontrar alguno de los valores

requeridos, consulte la documentación del proxy de su almacén de claves externo o del software de administración de claves.

> **Note**
>
> Al crear un almacén de claves externo en la AWS Management Console, puede cargar un archivo de configuración del proxy basado en JSON con valores para la ruta URI del proxy y la credencial de autenticación del proxy. Algunos proxy generan este archivo por usted. No es obligatorio.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Custom key stores (Almacenes de claves personalizados), External key stores (Almacenes de claves externos).
4. Seleccione Create external key store (Crear almacén de claves externo).
5. Escriba un nombre fácil de recordar para el almacén de claves externo. El nombre debe ser único entre todos los almacenes de claves externos de su cuenta.

   > **Important**
   >
   > No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.

6. Elija el tipo de conectividad del proxy.

   Su elección de conectividad del proxy determina los componentes necesarios para su proxy del almacén de claves externo. Si necesita ayuda para tomar esta decisión, consulte Elegir una opción de conectividad del proxy.

7. Elija o introduzca el nombre del servicio de punto de conexión de VPC para este almacén de claves externo. Este paso solo aparece cuando el tipo de conectividad al proxy del almacén de claves externo es el servicio de punto de conexión de VPC.

El servicio de punto de conexión de VPC y sus VPC deben cumplir los requisitos de un almacén de claves externo. Para obtener más detalles, consulte the section called “Cumplir los requisitos previos”.

8. Introduzca el punto de conexión de la URI de su proxy. El protocolo debe ser HTTPS. AWS KMS se comunica en el puerto 443. No especifique el puerto en el valor del punto de conexión URI del proxy.

   Si AWS KMS reconoce el servicio de punto de conexión de VPC que especificó en el paso anterior, rellena este campo por usted.

   Para la conectividad al punto de conexión público, introduzca una URI de punto de conexión disponible públicamente. Para la conectividad de punto de conexión de VPC, introduzca `https://` seguido del nombre DNS privado del servicio de punto de conexión de VPC.

9. Para introducir los valores del prefijo de ruta URI del proxy y de la credencial de autenticación del proxy, cargue un archivo de configuración de proxy o introduzca los valores manualmente.

   - Si tiene un archivo de configuración de proxy opcional que contiene valores para la ruta URI del proxy y la credencial de autenticación del proxy, elija Upload configuration file (Cargar archivo de configuración). Siga los pasos para cargar el archivo.

     Cuando se carga el archivo, la consola muestra los valores del archivo en campos editables. Puede cambiar los valores ahora o editarlos después de crear el almacén de claves externo.

     Para mostrar el valor de la clave de acceso secreta, seleccione Show secret access key (Mostrar clave de acceso secreta).

   - Si no tiene un archivo de configuración de proxy, puede introducir la ruta URI del proxy y los valores de las credenciales de autenticación del proxy manualmente.

     a. Si no dispone de un archivo de configuración de proxy, puede introducir la URI de proxy manualmente. La consola proporciona el valor /kms/xks/v1 requerido.

        Si la ruta URI de su proxy incluye un prefijo opcional, como el `example-prefix` en `/example-prefix/kms/xks/v1`, introduzca el prefijo en el campo del prefijo de ruta URI del proxy. De lo contrario, deje el campo en blanco.

     b. Si no dispone de un archivo de configuración de proxy, puede introducir su credencial de autenticación del proxy manualmente. Se requieren tanto el ID de clave de acceso como la clave de acceso secreta.

- En Proxy credential: Access key ID (Credencial de proxy: ID de clave de acceso), introduzca el ID de clave de acceso de la credencial de autenticación del proxy. El ID de clave de acceso identifica la clave de acceso secreta.
- En Proxy credential: Secret access key (Credencial de proxy: clave de acceso secreta), introduzca el ID de clave de acceso secreta de la credencial de autenticación del proxy.

Para mostrar el valor de la clave de acceso secreta, seleccione Show secret access key (Mostrar clave de acceso secreta).

Este procedimiento no establece ni cambia la credencial de autenticación que estableció en su proxy del almacén de claves externo. Simplemente asocia estos valores con su almacén de claves externo. Para obtener información sobre la configuración, el cambio y la credencial de autenticación del proxy rotativo, consulte la documentación del proxy del almacén de claves externo o del software de administración de claves.

Si la credencial de autenticación del proxy cambia, edite la configuración de credenciales del almacén de claves externo.

10. Seleccione Create external key store (Crear almacén de claves externo).

Si el proceso se ejecuta correctamente, el nuevo almacén de claves externo aparecerá en la lista de almacenes de claves externos de la cuenta y la región. Si el procedimiento da error, aparecerá un mensaje de error donde se describe el problema y se explica cómo resolverlo. Si necesita más ayuda, consulte CreateKey errores en la clave externa.

Siguiente: los nuevos almacenes de claves externos no se conectan de forma automática. Antes de poder crear AWS KMS keys en su almacén de claves externo, debe conectar el almacén de clave externo a su proxy del almacén de claves externo.

Creación de un almacén de claves externo (API)

Puede utilizar la CreateCustomKeyStoreoperación para crear un nuevo almacén de claves externo. Para obtener ayuda para encontrar los parámetros requeridos, consulte la documentación del proxy de su almacén de claves externo o del software de administración de claves.

> **Tip**
>
> No puede cargar un archivo de configuración de proxy cuando utilice la operación `CreateCustomKeyStore`. Sin embargo, puede utilizar los valores del archivo de configuración del proxy para asegurarse de que los valores de los parámetros son correctos.

Para crear un almacén de claves externo, la operación `CreateCustomKeyStore` requiere los siguientes valores de parámetros.

- `CustomKeyStoreName`: un nombre fácil de recordar para el almacén de claves externo que es exclusivo de la cuenta.

  > **Important**
  >
  > No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.

- `CustomKeyStoreType`: especifique `EXTERNAL_KEY_STORE`.
- `XksProxyConnectivity`: especifique `PUBLIC_ENDPOINT` o `VPC_ENDPOINT_SERVICE`.
- `XksProxyAuthenticationCredential`: especifique el ID de clave de acceso y la clave de acceso secreta.
- `XksProxyUriEndpoint`: el punto de conexión que AWS KMS utiliza para comunicarse con el proxy de su almacén de claves externo.
- `XksProxyUriPath`: la ruta dentro del proxy a las API de proxy.
- `XksProxyVpcEndpointServiceName`: es obligatorio solo cuando su valor `XksProxyConnectivity` es `VPC_ENDPOINT_SERVICE`.

> **Note**
>
> Si usa la versión 1.0 de la AWS CLI, ejecute el siguiente comando antes de especificar un parámetro con un valor HTTP o HTTPS, como el parámetro `XksProxyUriEndpoint`.
>
> ```
> aws configure set cli_follow_urlparam false
> ```

De lo contrario, la versión 1.0 de la AWS CLI sustituye el valor del parámetro por el contenido que se encuentra en esa dirección URI, lo que provoca el siguiente error:

```
Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve
https:// : received non 200 status code of 404
```

En los siguientes ejemplos se utilizan valores ficticios. Antes de ejecutar el comando, sustituya los valores por valores válidos para el almacén de claves externo.

Cree un almacén de claves externo con conectividad a los puntos de conexión públicos.

```
$ aws kms create-custom-key-store
        --custom-key-store-name ExampleExternalKeyStorePublic \
        --custom-key-store-type EXTERNAL_KEY_STORE \
        --xks-proxy-connectivity PUBLIC_ENDPOINT \
        --xks-proxy-uri-endpoint https://myproxy.xks.example.com \
        --xks-proxy-uri-path /kms/xks/v1 \
        --xks-proxy-authentication-credential
 AccessKeyId=<value>,RawSecretAccessKey=<value>
```

Cree un almacén de claves externo con conectividad al servicio de punto de conexión de VPC.

```
$ aws kms create-custom-key-store
        --custom-key-store-name ExampleExternalKeyStoreVPC \
        --custom-key-store-type EXTERNAL_KEY_STORE \
        --xks-proxy-connectivity VPC_ENDPOINT_SERVICE \
        --xks-proxy-vpc-endpoint-service-name com.amazonaws.vpce.us-east-1.vpce-svc-
example \
        --xks-proxy-uri-endpoint https://myproxy-private.xks.example.com \
        --xks-proxy-uri-path /kms/xks/v1 \
        --xks-proxy-authentication-credential
 AccessKeyId=<value>,RawSecretAccessKey=<value>
```

Si la operación se ejecuta correctamente, `CreateCustomKeyStore` devolverá el ID del almacén de claves personalizado, tal y como se muestra en la siguiente respuesta de ejemplo.

```
{
    "CustomKeyStoreId": cks-1234567890abcdef0
}
```

Si la operación falla, corrija el error que indica la excepción e inténtelo de nuevo. Para obtener ayuda adicional, consulte Solución de problemas de almacenes de claves externos.

Siguiente: para usar el almacén de claves externo, conéctelo a su proxy del almacén de claves externo.

Edición de propiedades del almacén de claves externo

Puede editar las propiedades seleccionadas de un almacén de claves externo existente.

Puede editar algunas propiedades mientras el almacén de claves externo esté conectado o desconectado. Para otras propiedades, primero debe desconectar el almacén de claves externo de su proxy del almacén de claves externo. El estado de conexión del almacén de claves externo debe ser `DISCONNECTED`. Mientras su almacén de claves externo esté desconectado, puede administrar el almacén de claves y sus claves de KMS, pero no puede crear ni usar las claves de KMS en el almacén de claves externo. Para encontrar el estado de conexión del almacén de claves externo, utilice la DescribeCustomKeyStoresoperación o consulte la sección Configuración general en la página de detalles del almacén de claves externo.

Antes de actualizar las propiedades del almacén de claves externo, AWS KMS envía una GetHealthStatussolicitud al proxy del almacén de claves externo con los nuevos valores. Si la solicitud se realiza correctamente, indica que puede conectarse y autenticarse en un proxy del almacén de claves externo con los valores de propiedad actualizados. Si la solicitud falla, la operación de edición falla con una excepción que identifica el error.

Cuando finalice la operación de edición, los valores de propiedades actualizados del almacén de claves externo aparecerán en la consola de AWS KMS y en la respuesta `DescribeCustomKeyStores`. No obstante, pueden pasar hasta cinco minutos hasta que los cambios surtan efecto.

Si edita su almacén de claves externo en la consola de AWS KMS, tiene la opción de cargar un archivo de configuración del proxy basado en JSON que especifique la ruta URI del proxy y la credencial de autenticación del proxy. Algunos proxy del almacén de claves externos generan este archivo por usted. Para obtener más información, consulte la documentación del proxy del almacén de claves externo o el administrador de claves externo.

> **Warning**
>
> Los valores actualizados de las propiedades deben conectar el almacén de claves externo a un proxy para el mismo administrador de claves externo que los valores anteriores, o para

obtener una copia de seguridad o una instantánea del administrador de claves externo con las mismas claves criptográficas. Si su almacén de claves externo pierde permanentemente el acceso a las claves externas asociadas a sus claves de KMS, el texto cifrado encriptado con esas claves externas no se podrá recuperar. En particular, cambiar la conectividad del proxy de un almacén de claves externo puede impedir que AWS KMS acceda a las claves externas.

Tip

Algunos administradores de claves externos proporcionan un método más sencillo para editar las propiedades de un almacén de claves externo. Para obtener más detalles, consulte la documentación del administrador de claves externo.

Puede cambiar las siguientes propiedades de un almacén de claves externo.

Propiedades editables del almacén de claves externo	Cualquier estado de conexión	Requerir estado desconectado
Nombre del almacén de claves personalizadas Un nombre fácil de recordar obligatorio para el almacén de claves personalizado. **Important** No incluya información confidencial en este campo. Este campo puede mostrarse en texto plano en CloudTrail los registros y otros resultados.	✓	
Credencial de autenticación proxy () XksProxyAuthenticationCredential	✓	

Propiedades editables del almacén de claves externo	Cualquier estado de conexión	Requerir estado desconectado
(Debe especificar el ID de clave de acceso y la clave de acceso secreta, incluso si cambia solo un elemento).		
Ruta de URI del proxy () XksProxyUriPath	✓	
Conectividad proxy (XksProxyConnectivity) (También debe actualizar el punto de conexión de la URI del proxy. Si va a cambiar a la conectividad al servicio de punto de conexión de VPC, debe especificar un nombre de servicio de punto de conexión de VPC del proxy).		✓
Punto final del URI del proxy (XksProxyUriEndpoint) Si cambia la URI del punto de conexión del proxy, es posible que también tenga que cambiar el certificado TLS asociado.		✓
Nombre del servicio de punto final de VPC proxy () XksProxyVpcEndpointServiceName (Este campo es obligatorio para la conectividad al servicio de punto de conexión de VPC)		✓

Temas

- Edición de un almacén de claves externo (consola)
- Edición de un almacén de claves externo (API)

Edición de un almacén de claves externo (consola)

Al editar un almacén de claves, puede cambiar cualquiera de los valores editables. Algunos cambios requieren que el almacén de claves externo esté desconectado de su proxy del almacén de claves externo.

Si está editando la ruta URI del proxy o la credencial de autenticación del proxy, puede introducir los nuevos valores o cargar un archivo de configuración del proxy del almacén de claves externo que incluya los nuevos valores.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Custom key stores (Almacenes de claves personalizados), External key stores (Almacenes de claves externos).
4. Elija la fila del almacén de claves externo que quiere editar.
5. Si es necesario, desconecte el almacén de claves externo de su proxy del almacén de claves externo. En el menú Key store actions (Acciones del almacén de claves), seleccione Disconnect (Desconectar).
6. Desde el menú Key store actions (Acciones del almacén de claves), seleccione Edit (Editar).
7. Cambie una o más de las propiedades editables del almacén de claves externo. También puede cargar un archivo de configuración del proxy con valores para la ruta URI del proxy y la credencial de autenticación del proxy. Puede utilizar un archivo de configuración de proxy incluso si algunos valores especificados en el archivo no han cambiado.
8. Elija Update external key store (Actualizar el almacén de claves externo).
9. Revise la advertencia y, si decide continuar, confirme la advertencia y, a continuación, seleccione Update external key store (Actualizar almacén de claves externo).

   Si el procedimiento se ejecuta correctamente, aparecerá un mensaje donde se describen las propiedades que ha editado. Si el procedimiento da error, aparecerá un mensaje de error donde se describe el problema y se explica cómo resolverlo.
10. Si es necesario, vuelva a conectar el almacén de claves externo. En el menú Key store actions (Acciones del almacén de claves), seleccione Connect (Conectar).

Puede dejar el almacén de claves externo desconectado. Pero mientras esté desconectado, no podrá crear las claves de KMS en el almacén de claves externo ni usar las claves de KMS del almacén de claves externo en operaciones criptográficas.

Edición de un almacén de claves externo (API)

Para cambiar las propiedades de un almacén de claves externo, utilice la UpdateCustomKeyStoreoperación. Puede cambiar varias propiedades de un almacén de claves externo en la misma operación. Si la operación se realiza correctamente, AWS KMS devuelve una respuesta HTTP 200 y un objeto JSON sin propiedades.

Utilice el parámetro `CustomKeyStoreId` para identificar el almacén de claves externo. Utilice los demás parámetros para cambiar las propiedades. No puede usar un archivo de configuración del proxy con la operación `UpdateCustomKeyStore`. El archivo de configuración del proxy solo es compatible con la consola de AWS KMS. Sin embargo, puede utilizar el archivo de configuración del proxy como ayuda para determinar los valores de los parámetros correctos para el proxy del almacén de claves externo.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Antes de empezar, si es necesario, desconecte el almacén de claves externo de su proxy del almacén de claves externo. Tras la actualización, si es necesario, puede volver a conectar el almacén de claves externo a su proxy del almacén de claves externo. Puede dejar el almacén de claves externo en el estado desconectado, pero deberá volver a conectarlo antes de crear claves de KMS nuevas en el almacén de claves, o para utilizar las claves de KMS existentes en el almacén de claves para operaciones criptográficas.

> **Note**
>
> Si usa la versión 1.0 de la AWS CLI, ejecute el siguiente comando antes de especificar un parámetro con un valor HTTP o HTTPS, como el parámetro `XksProxyUriEndpoint`.
>
> ```
> aws configure set cli_follow_urlparam false
> ```
>
> De lo contrario, la versión 1.0 de la AWS CLI sustituye el valor del parámetro por el contenido que se encuentra en esa dirección URI, lo que provoca el siguiente error:

```
Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve
https:// : received non 200 status code of 404
```

Cambio del nombre del almacén de claves externo

El primer ejemplo utiliza la UpdateCustomKeyStoreoperación para cambiar el nombre descriptivo del almacén de claves externo a`XksKeyStore`. El comando utiliza el parámetro `CustomKeyStoreId` para especificar el almacén de claves personalizado y `CustomKeyStoreName` para especificar el nuevo nombre del almacén de claves personalizado. Sustituya todos los valores de ejemplo por valores reales para su almacén de claves externo.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-
custom-key-store-name XksKeyStore
```

Cambio de la credencial de autenticación del proxy

En el siguiente ejemplo, se actualiza la credencial de autenticación del proxy que AWS KMS utiliza para autenticarse en el proxy del almacén de claves externo. Puede usar un comando como este para actualizar la credencial si está rotada en su proxy.

Primero actualice la credencial del proxy del almacén de claves externo. A continuación, utilice esta función para informar del cambio a AWS KMS. (Su proxy admitirá brevemente tanto la credencial anterior como la nueva para que tenga tiempo de actualizarla en AWS KMS).

Siempre debe especificar el ID de clave de acceso y la clave de acceso secreta en la credencial, incluso si solo se cambia un valor.

Los dos primeros comandos configuran variables para conservar los valores de las credenciales. Las operaciones `UpdateCustomKeyStore` utilizan el parámetro `CustomKeyStoreId` para identificar el almacén de claves externo. Utiliza el parámetro `XksProxyAuthenticationCredential` con sus campos `AccessKeyId` y `RawSecretAccessKey` para especificar la nueva credencial. Sustituya todos los valores de ejemplo por valores reales para su almacén de claves externo.

```
$ accessKeyID=access key id
$ secretAccessKey=secret access key

$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
```

```
        --xks-proxy-authentication-credential \
            AccessKeyId=$accessKeyId,RawSecretAccessKey=$secretAccessKey
```

Cambio de la ruta URI del proxy

El siguiente ejemplo actualiza la ruta URI del proxy (`XksProxyUriPath`). La combinación del punto de conexión de la URI del proxy y la ruta URI del proxy debe ser única en la región y la Cuenta de AWS. Sustituya todos los valores de ejemplo por valores reales para su almacén de claves externo.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
            --xks-proxy-uri-path /kms/xks/v1
```

Cambio a la conectividad del servicio del punto de conexión de VPC

En el siguiente ejemplo, se utiliza la UpdateCustomKeyStoreoperación para cambiar el tipo de conectividad proxy del almacén de claves externo a`VPC_ENDPOINT_SERVICE`. Para realizar este cambio, debe especificar los valores necesarios para la conectividad del servicio de punto de conexión de VPC, incluido el nombre del servicio de punto de conexión de VPC (`XksProxyVpcEndpointServiceName`) y un valor de punto de conexión URI del proxy (`XksProxyUriEndpoint`) que incluya el nombre DNS privado del servicio de punto de conexión de VPC. Sustituya todos los valores de ejemplo por valores reales para su almacén de claves externo.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
            --xks-proxy-connectivity "VPC_ENDPOINT_SERVICE" \
            --xks-proxy-uri-endpoint https://myproxy-private.xks.example.com \
            --xks-proxy-vpc-endpoint-service-name com.amazonaws.vpce.us-east-1.vpce-
svc-example
```

Cambio a la conectividad de puntos de conexión públicos

En el siguiente ejemplo, se cambia el tipo de conectividad del proxy del almacén de claves externo a `PUBLIC_ENDPOINT`. Al realizar este cambio, debe actualizar el valor del punto de conexión URI (`XksProxyUriEndpoint`) del proxy. Sustituya todos los valores de ejemplo por valores reales para su almacén de claves externo.

> **Note**
>
> La conectividad al punto de conexión de VPC proporciona mayor seguridad que la conectividad al punto de conexión público. Antes de cambiar a la conectividad al punto de

conexión público, considere otras opciones, como localizar el proxy del almacén de claves externo en las instalaciones y utilizar la VPC solo para la comunicación.

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
            --xks-proxy-connectivity "PUBLIC_ENDPOINT" \
            --xks-proxy-uri-endpoint https://myproxy.xks.example.com
```

Visualización de un almacén de claves externo

Puede ver los almacenes de claves externos de cada cuenta y región mediante la AWS KMS consola o mediante la DescribeCustomKeyStoresoperación.

Al consultar un almacén de claves externo, puede ver lo siguiente:

- Información básica sobre el almacén de claves, incluido su nombre fácil de recordar, ID, tipo de almacén de claves y fecha de creación.
- Información de configuración para el proxy del almacén de claves externo, incluidos el tipo de conectividad, el punto de conexión URI del proxy y su ruta y el ID de clave de acceso de su credencial de autenticación de proxy actual.
- Si el proxy del almacén de claves externo utiliza la conectividad al servicio de punto de conexión de VPC, la consola muestra el nombre del servicio de punto de conexión de VPC.
- El estado de conexión actual.

  > **Note**
  >
  > Un valor de estado de conexión Disconnected (Desconectado) indica que el almacén de claves externo nunca se ha conectado o que se ha desconectado intencionadamente de su proxy del almacén de claves externo. Sin embargo, si los intentos de usar una clave de KMS en un almacén de claves externo conectado no son fructíferos, puede deberse a un problema con el almacén de claves externo o el proxy. Para obtener ayuda, consulte Errores de conexión del almacén de claves externo.

- Una sección de monitorización con gráficos de CloudWatch las métricas de Amazon diseñada para ayudarte a detectar y resolver problemas con tu almacén de claves externo. Si necesitas ayuda para interpretar los gráficos, utilizarlos en la planificación y la resolución de problemas y crear CloudWatch alarmas en función de las métricas de los gráficos, consultaMonitoreo de un almacén de claves externo.

Véase también:

- Visualización de claves de KMS en un almacén de claves externo
- Registrar llamadas a la AWS KMS API con AWS CloudTrail

Temas

Propiedades del almacén de claves externo

Las siguientes propiedades de un almacén de claves externo están visibles en la AWS KMS consola y en la DescribeCustomKeyStoresrespuesta.

Propiedades del almacén de claves personalizado

Los siguientes valores aparecen en la sección Configuración general de la página de detalles de cada almacén de claves personalizado. Estas propiedades aplican a todos los almacenes de claves personalizados, incluidos los almacenes de claves de AWS CloudHSM y los almacenes de claves externos.

ID del almacén de claves personalizadas

Un ID único que AWS KMS asigna al almacén de claves personalizado.

Nombre del almacén de claves personalizadas

Un nombre fácil de recordar que asigna al almacén de claves personalizado al crearlo. Puede cambiar este valor en cualquier momento.

Tipo de almacén de claves personalizado

El tipo de almacén de claves personalizado. Los valores válidos son AWS CloudHSM (`AWS_CLOUDHSM`) o Almacén de claves externo (`EXTERNAL_KEY_STORE`). No se puede cambiar el tipo después de crear el almacén de claves personalizado.

Fecha de creación

Fecha en la que se creó el almacén de claves personalizado. Este valor se muestra en la hora local de la Región de AWS.

Estado de la conexión

Indica si el almacén de claves personalizado está conectado a su almacén de claves de respaldo. El estado de conexión será `DISCONNECTED` solo si el almacén de claves personalizado nunca se ha conectado al almacén de claves de respaldo o se ha desconectado intencionadamente. Para obtener más detalles, consulte the section called “Estado de la conexión”.

Propiedades de configuración del almacén de claves externo

Los siguientes valores aparecen en la sección de configuración del proxy del almacén de claves externo de la página de detalles de cada almacén de claves externo y en el `XksProxyConfiguration` elemento de la DescribeCustomKeyStoresrespuesta. Para obtener una descripción detallada de cada campo, incluidos los requisitos de exclusividad y ayuda para determinar el valor correcto de cada campo, consulte the section called “Cumplir los requisitos previos” en el tema Creación de un almacén de claves externo.

Conectividad de proxy

Indica si el almacén de claves externo utiliza conectividad de puntos de conexión públicos o conectividad del servicio de punto de conexión de VPC.

Punto de conexión URI del proxy

El punto de conexión que AWS KMS utiliza para conectarse al proxy del almacén de claves externo.

Ruta URI del proxy

La ruta desde el punto de conexión URI del proxy donde AWS KMS envía las solicitudes de API de proxy.

Credencial de proxy: ID de clave de acceso

Parte de la credencial de autenticación de proxy que establece en el proxy de su almacén de claves externo. El ID de clave de acceso identifica la clave de acceso secreta de la credencial.

AWS KMS utiliza el proceso de firma SigV4 y la credencial de autenticación de proxy para firmar sus solicitudes en el proxy de su almacén de claves externo. La credencial de la firma permite al proxy del almacén de claves externo autenticar las solicitudes en su nombre desde AWS KMS.

Nombre del servicio de punto de conexión de VPC

El nombre del servicio de punto de conexión de VPC de Amazon que admite su almacén de claves externo. Este valor solo aparece cuando el almacén de claves externo utiliza la conectividad del servicio de punto de conexión de VPC. Puede localizar su proxy de almacén de claves externo en la VPC o utilizar el servicio de punto de conexión de VPC para comunicarse de forma segura con su proxy de almacén de claves externo.

Visualización de un almacén de claves externo (consola)

Para ver los almacenes de claves externos de una cuenta y región determinados, use el siguiente procedimiento.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Custom key stores (Almacenes de claves personalizados), External key stores (Almacenes de claves externos).
4. Para ver información detallada sobre un almacén de claves externo, elija el nombre de almacén de claves.

Visualización de un almacén de claves externo (API)

Para ver los almacenes de claves externos, utilice la DescribeCustomKeyStoresoperación. De forma predeterminada, esta operación devuelve los almacenes de claves personalizados de la cuenta y región. Pero puede usar el parámetro `CustomKeyStoreId` o `CustomKeyStoreName` (pero no ambos) para limitar el resultado de un almacén de claves personalizado determinado.

Para los almacenes de claves personalizados, el resultado consiste en el ID, el nombre y el tipo del almacén de claves personalizado y el estado de conexión del almacén de claves. Si el estado de conexión es `FAILED`, el resultado también incluirá un `ConnectionErrorCode` que describe el motivo del error. Para obtener ayuda para interpretar el `ConnectionErrorCode` para un almacén de claves externo, consulte Códigos de error de conexión para almacenes de claves externos.

Para los almacenes de claves externos, el resultado también incluye el elemento `XksProxyConfiguration`. Este elemento incluye el tipo de conectividad, el punto de conexión

URI del proxy, la ruta URI del proxy y el ID de clave de acceso de la credencial de autenticación del proxy.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Por ejemplo, el siguiente comando devuelve todos los almacenes de claves personalizados de la cuenta y la región. Puede usar los parámetros `Limit` y `Marker` para desplazarse por los almacenes de claves personalizados del resultado.

```
$ aws kms describe-custom-key-stores
```

El siguiente comando usa el parámetro `CustomKeyStoreName` para obtener únicamente el almacén de claves externo con el nombre fácil de recordar `ExampleXksPublic`. Este ejemplo de almacén de claves utiliza conectividad a puntos de conexión públicos. Está conectado a su proxy del almacén de claves externo.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksPublic
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-1234567890abcdef0",
      "CustomKeyStoreName": "ExampleXksPublic",
      "ConnectionState": "CONNECTED",
      "CreationDate": "2022-12-14T20:17:36.419000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE12345670EXAMPLE",
        "Connectivity": "PUBLIC_ENDPOINT",
        "UriEndpoint": "https://xks.example.com:6443",
        "UriPath": "/example/prefix/kms/xks/v1"
      }
    }
  ]
}
```

El siguiente comando obtiene un ejemplo de almacén de claves externo con conectividad del servicio de punto de conexión de VPC. En este ejemplo, el almacén de claves externo está conectado a su proxy del almacén de claves externo.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
```

```
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "CONNECTED",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Un `ConnectionState` `Disconnected` indica que no se ha conectado nunca un almacén de claves externo o que se ha desconectado de su proxy del almacén de claves externo de forma intencionada. Sin embargo, si los intentos de usar una clave de KMS en un almacén de claves externo conectado no son fructíferos, puede deberse a un problema con el proxy del almacén de claves externo u otros componentes externos.

Si el `ConnectionState` del almacén de claves externo es `FAILED`, la respuesta `DescribeCustomKeyStores` incluirá un elemento `ConnectionErrorCode` que explica el motivo del error.

Por ejemplo, en el siguiente resultado, el valor `XKS_PROXY_TIMED_OUT` indica que AWS KMS se puede conectar al proxy del almacén de claves externo, pero la conexión falló porque el proxy del almacén de claves externo no respondió a AWS KMS durante el tiempo establecido. Si ve este código de error de conexión varias veces, comuníqueselo al proveedor del proxy del almacén de claves externo. Para obtener ayuda con esto y los errores de conexión, consulte Solución de problemas de almacenes de claves externos.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
```

```
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "FAILED",
      "ConnectionErrorCode": "XKS_PROXY_TIMED_OUT",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Monitoreo de un almacén de claves externo

AWS KMSrecopila las métricas de cada interacción con un almacén de claves externo y las publica en su CloudWatch cuenta. Estas métricas se utilizan para generar los gráficos en la sección de seguimiento de la página de detalles para cada almacén de claves externo. El siguiente tema detalla cómo usar los gráficos para identificar y solucionar problemas operativos y de configuración que afectan su almacén de claves externo. Te recomendamos usar las CloudWatch métricas para configurar alarmas que te notifiquen cuando tu almacén de claves externo no funcione como esperabas. Para obtener más información, consulta Monitoring with Amazon CloudWatch.

Temas

- Visualización de los gráficos
- Interpretación de los gráficos
- Configurar las alarmas

Visualización de los gráficos

Puede ver los gráficos en diferentes niveles de detalle. De forma predeterminada, cada gráfico utiliza un intervalo de tiempo de tres horas y un periodo de agregación de cinco minutos. Puede ajustar la vista del gráfico dentro de la consola, pero sus cambios volverán a la configuración predeterminada cuando se cierre la página de detalles del almacén de claves externo o se actualice el navegador. Para obtener ayuda con la CloudWatch terminología de Amazon, consulta CloudWatch Conceptos de Amazon.

Visualización de detalles de puntos de datos

Los datos de cada gráfico se recopilan mediante métricas de AWS KMS. Para ver más información sobre un punto de datos específico, coloque el ratón sobre el punto de datos del gráfico lineal. Esto mostrará una ventana emergente con más información sobre la métrica de la que se derivó el gráfico. Cada elemento de la lista muestra el valor de dimensión registrado en ese punto de datos. La ventana emergente muestra un valor nulo (–) si no hay datos métricos disponibles para el valor de la dimensión en ese punto de datos. Algunos gráficos registran varias dimensiones y valores para un único punto de datos. Otros gráficos, como el gráfico de fiabilidad, utilizan los datos recopilados por la métrica para calcular un valor único. Cada elemento de la lista está asociado con un color de gráfico de líneas diferente.

Modificación del intervalo de tiempo

Para modificar el intervalo de tiempo, seleccione uno de los intervalos de tiempo predefinidos en la esquina superior derecha de la sección de monitoreo. Los intervalos de tiempo predefinidos abarcan de 1 hora a 1 semana (1 h, 3 h, 12 h, 1 día, 3 días o 1 sem.). Esto ajusta el intervalo de tiempo de todos los gráficos. Si quieres ver un gráfico específico en un intervalo de tiempo diferente, o si quieres establecer un intervalo de tiempo personalizado, amplía el gráfico o visualízalo en la CloudWatch consola de Amazon.

Acercar un gráfico

Puede usar la función de zoom del minimapa para enfocarse en secciones de gráficos de líneas y porciones apiladas de los gráficos sin cambiar entre vistas ampliadas y alejadas. Por ejemplo, puede usar la función de zoom del minimapa para enfocarse en un pico en un gráfico, de modo que pueda comparar el pico con otros gráficos en la sección de monitoreo de la misma línea de tiempo.

1. Elija y arrastre el área del gráfico en la que desea centrarse y, a continuación, suéltela.
2. Para restablecer el tamaño del gráfico, elija el icono Reset zoom (Restablecer el zoom) que parece una lupa con un símbolo menos (-) en su interior.

Ampliación de un gráfico

Para ampliar un gráfico, seleccione el icono de menú situado en la esquina superior derecha de un gráfico individual y, a continuación, seleccione Enlarge (Ampliar). También puede seleccionar el icono de ampliación que aparece junto al icono del menú al pasar el ratón sobre un gráfico.

Al ampliar un gráfico, puede modificar aún más la vista de un gráfico especificando un periodo diferente, un intervalo de tiempo personalizado o un intervalo de actualización. Estos cambios volverán a la configuración predeterminada cuando cierre la vista ampliada.

Modificación del periodo

1. Seleccione el menú Period options (Opciones de periodo). De forma predeterminada, este menú muestra el valor: 5 minutos.
2. Elija un periodo, los periodos predefinidos van de 1 segundo a 30 días.

   Por ejemplo, puede elegir una vista de un minuto, que puede ser útil a la hora de solucionar problemas. O bien puede elegir una vista menos detallada de una hora. Esto puede ser útil cuando desee ver un intervalo de tiempo mayor (por ejemplo, tres días) para poder identificar las tendencias a lo largo del tiempo. Para obtener más información, consulta Periodos en la Guía del CloudWatch usuario de Amazon.

Modificación del intervalo de tiempo o la zona horaria

1. Seleccione uno de los intervalos de tiempo predefinidos, que van desde 1 hora hasta 1 semana (1 h, 3 h, 12 h, 1 día, 3 días o 1 semana). También puede elegir Custom (Personalizado) para establecer su propio intervalo de tiempo.
2. Elija Custom (Personalizado).

   a. Intervalo de tiempo: seleccione la pestaña Absolute (Absoluto) en la esquina superior izquierda del cuadro. Utilice el selector de calendario o los cuadros de campos de texto para especificar el intervalo de tiempo.

   b. Zona horaria: elija el menú desplegable ubicado en la esquina superior derecha del cuadro. Puede cambiar la zona horaria a UTC (UTC) o Local time zone (Zona horaria local).
3. Después de especificar un intervalo de tiempo, seleccione Apply (Aplicar).

Modifique la frecuencia con la que se actualizan los datos de su gráfico

1. Elija el menú Refresh options (Opciones de actualización) en la esquina superior derecha.
2. Elija un intervalo de actualización [Off (desactivado), 10 seconds (10 segundos), 1 minute (1 minuto), 2 minutes (2 minutes), 5 minutes (5 minutos) o 15 minutes(15 minutos)].

Ver gráficos en la CloudWatch consola de Amazon

Los gráficos de la sección de monitorización se derivan de métricas predefinidas que se AWS KMS publican en Amazon CloudWatch. Puede abrirlos en la CloudWatch consola y guardarlos en los CloudWatch paneles. Si tiene varios almacenes de claves externos, puede abrir sus gráficos respectivos CloudWatch y guardarlos en un único panel para comparar su estado y uso.

Añadir al CloudWatch panel

Selecciona Añadir al panel en la esquina superior derecha para añadir todos los gráficos a un CloudWatch panel de Amazon. Puede seleccionar un tablero existente o crear uno nuevo. Para obtener información sobre el uso de este panel para crear vistas personalizadas de los gráficos y las alarmas, consulte Uso de los CloudWatch paneles de Amazon en la Guía del CloudWatch usuario de Amazon.

Ver en métricas CloudWatch

Selecciona el icono de menú en la esquina superior derecha de un gráfico individual y selecciona Ver en métricas para ver este gráfico en la CloudWatch consola de Amazon. Desde la CloudWatch consola, puedes añadir este único gráfico a un panel y modificar los rangos de tiempo, los períodos y los intervalos de actualización. Para obtener más información, consulta Cómo graficar métricas en la Guía del CloudWatch usuario de Amazon.

Interpretación de los gráficos

AWS KMS proporciona varios gráficos para monitorear el estado del almacén de claves externo en la consola de AWS KMS. Estos gráficos se configuran automáticamente y se derivan de las métricas de AWS KMS.

Los datos del gráfico se recopilan como parte de las llamadas que realiza a su almacén de claves externo y claves externas. Es posible que vea datos que completan los gráficos durante un intervalo de tiempo en el que no realizó ninguna llamada, estos datos provienen de las llamadas periódicas a `GetHealthStatus` que AWS KMS realiza en su nombre para verificar el estado de su proxy de almacén de claves externo y administrador de claves externo. Si sus gráficos muestran el mensaje No data available (No hay datos disponibles), entonces no hubo llamadas registradas durante ese intervalo de tiempo o su almacén de claves externo está en un estado `DISCONNECTED`. Es posible que pueda identificar la hora en que se desconectó su almacén de claves externo ajustando su vista a un intervalo de tiempo más amplio.

Temas

- Número total de solicitudes
- Fiabilidad
- Latencia
- Las 5 excepciones principales
- Días para el vencimiento del certificado

Número total de solicitudes

El número total de solicitudes de AWS KMS que se reciben para un almacén de claves externo específico durante un intervalo de tiempo determinado. Utilice este gráfico para determinar si corre el riesgo de sufrir una limitación.

AWS KMS recomienda que el administrador de claves externas pueda gestionar hasta 1800 solicitudes de operaciones criptográficas por segundo. Si se acerca a las 540 000 llamadas en un periodo de cinco minutos, corre el riesgo de sufrir una limitación.

Puede monitorear la cantidad de solicitudes de operaciones criptográficas en las claves de KMS de su almacén de claves externo que AWS KMS limita con la métrica ExternalKeyStoreThrottle.

Si recibe errores `KMSInvalidStateException` muy frecuentes con un mensaje que explica que la solicitud fue rechazada “debido a una tasa de solicitudes muy alta”, podría indicar que su administrador de claves externo o el proxy del almacén de claves externo no pueden seguir el ritmo de la tasa de solicitudes actual. Si es posible, reduzca el porcentaje de solicitudes. También podría considerar solicitar una disminución en el valor de la cuota de solicitudes del almacén de claves personalizado. Reducir este valor de cuota puede aumentar la limitación, pero indica que AWS KMS está rechazando rápidamente el exceso de solicitudes antes de enviarlas a su proxy del almacén de claves externo o a un administrador de claves externo. Para solicitar una reducción de la cuota, visite el Centro AWS Support y cree un caso.

El gráfico del total de solicitudes se obtiene de la métrica XksProxyErrors, que recopila datos sobre las respuestas correctas y fallidas que AWS KMS recibe del proxy del almacén de claves externo. Al ver un punto de datos específico, la ventana emergente muestra el valor de la dimensión `CustomKeyStoreId` junto con el número total de solicitudes de AWS KMS registradas en ese punto de datos. El `CustomKeyStoreId` siempre será el mismo.

Fiabilidad

El porcentaje de solicitudes de AWS KMS para las que el proxy del almacén de claves externo devolvió una respuesta correcta o un error reintentable. Utilice este gráfico para evaluar el estado operativo de su proxy del almacén de claves externo.

Cuando el gráfico muestra un valor inferior al 100 %, indica los casos en los que el proxy no respondió o respondió con un error reintentable. Esto puede indicar problemas con la red, lentitud del proxy del almacén de claves externo o del administrador de claves externo, o errores de implementación.

Si la solicitud incluye una credencial incorrecta y su proxy responde con una `AuthenticationFailedException`, el gráfico seguirá indicando una fiabilidad del 100 % porque el proxy identificó un valor incorrecto en la solicitud de la API del proxy del almacén de claves externo y, por lo tanto, es de esperar que se produzca un error. Si el porcentaje del gráfico de fiabilidad es del 100 %, entonces el proxy del almacén de claves externo responde según lo esperado. Si el gráfico muestra un valor inferior al 100 %, el proxy respondió con un error reintentable o se agotó el tiempo de espera. Por ejemplo, si el proxy responde con una respuesta de `ThrottlingException` debido a una tasa de solicitudes muy alta, mostrará un porcentaje de fiabilidad más bajo porque el proxy no pudo identificar un problema específico en la solicitud que provocó el error. Esto se debe a que los errores reintentables son probablemente problemas transitorios que se pueden resolver reintentando la solicitud.

Las siguientes respuestas de error reducirán el porcentaje de fiabilidad. Puede usar el gráfico Las 5 excepciones principales y la métrica XksProxyErrors para controlar con más detalle la frecuencia con la que su proxy devuelve cada error reintentable.

- `InternalException`
- `DependencyTimeoutException`
- `ThrottlingException`
- `XksProxyUnreachableException`

El gráfico de fiabilidad se obtiene de la métrica XksProxyErrors, que recopila datos sobre las respuestas correctas y fallidas que AWS KMS recibe del proxy del almacén de claves externo. El porcentaje de fiabilidad solo disminuirá si la respuesta tiene un valor de `ErrorType` de `Retryable`. Al ver un punto de datos específico, la ventana emergente muestra el valor de la dimensión `CustomKeyStoreId` junto con el porcentaje de fiabilidad de solicitudes de AWS KMS registradas en ese punto de datos. El `CustomKeyStoreId` siempre será el mismo.

Le recomendamos que utilice la XksProxyErrors métrica para crear una CloudWatch alarma que le notifique posibles problemas de red, ya que le avise cuando se registren más de cinco errores reintentables en un período de un minuto. Para obtener más información, consulte Crear una CloudWatch alarma de Amazon para errores reintentables.

Latencia

La cantidad de milisegundos que tarda un proxy del almacén de claves externo en responder a una solicitud de AWS KMS. Utilice este gráfico para evaluar el rendimiento de su proxy del almacén de claves externo y de su administrador de claves externo.

AWS KMS espera que el proxy del almacén de claves externo responda a cada solicitud en 250 milisegundos. En el caso de que se agoten los tiempos de espera de la red, AWS KMS volverá a intentar la solicitud una vez. Si el proxy falla por segunda vez, la latencia registrada es el límite de tiempo de espera combinado para ambos intentos de solicitud y el gráfico mostrará aproximadamente 500 milisegundos. En todos los demás casos en los que el proxy no responde dentro del límite de tiempo de espera de 250 milisegundos, la latencia registrada es de 250 milisegundos. Si el proxy se agota con frecuencia en las operaciones de cifrado y descifrado, consulte a su administrador de proxy externo. Para obtener ayuda con la solución de problemas de latencia, consulte Errores de latencia y tiempo de espera.

Las respuestas lentas también pueden indicar que el administrador de claves externo no puede gestionar el tráfico de solicitudes actual. AWS KMS recomienda que su administrador de claves externo pueda gestionar hasta 1800 solicitudes de operaciones criptográficas por segundo. Si su administrador de claves externo no puede gestionar la tasa de 1800 solicitudes por segundo, considere solicitar una reducción de su cuota de solicitudes de claves de KMS en un almacén de claves personalizado. Las solicitudes de operaciones criptográficas que utilizan las claves de KMS en su almacén de claves externo van a responder rápido a los errores con una excepción de limitación, en lugar de ser procesadas y luego rechazadas por su proxy del almacén de claves externo o administrador de claves externo.

El gráfico de latencia se realiza a partir de la métrica XksProxyLatency. Al consultar un punto de datos específico, la ventana emergente muestra los valores de dimensión `KmsOperation` y `XksOperation` correspondientes junto con la latencia promedio registrada para las operaciones en ese punto de datos. Los elementos de la lista se ordenan de mayor a menor latencia.

Te recomendamos usar la XksProxyLatency métrica para crear una CloudWatch alarma que te notifique cuando la latencia se acerque al límite de tiempo de espera. Para obtener más información, consulte Crear una CloudWatch alarma de Amazon para el tiempo de espera de respuesta.

Las 5 excepciones principales

Las cinco excepciones principales para operaciones criptográficas y de administración fallidas durante un intervalo de tiempo determinado. Utilice este gráfico para realizar un seguimiento de los errores más frecuentes, de modo que pueda priorizar sus esfuerzos de ingeniería.

Este recuento incluye las excepciones que AWS KMS recibió del proxy del almacén de claves externo y la `XksProxyUnreachableException` que AWS KMS devuelve internamente cuando no puede establecer comunicación con el proxy del almacén de claves externo.

Las altas tasas de errores reintentables pueden indicar errores de red, mientras que las altas tasas de errores no reintentables pueden indicar un problema con la configuración del almacén de claves externo. Por ejemplo, un pico en `AuthenticationFailedExceptions` indica una discrepancia entre las credenciales de autenticación configuradas en AWS KMS y el proxy del almacén de claves externo. Para ver la configuración de su almacén de claves externo, consulte Visualización de un almacén de claves externo. Para editar la configuración de su almacén de claves externo, consulte Edición de propiedades del almacén de claves externo.

Las excepciones que recibe AWS KMS del proxy del almacén de claves externo son diferentes de las excepciones que se AWS KMS devuelve cuando se produce un error en una operación. Las operaciones criptográficas de AWS KMS devuelven un `KMSInvalidStateException` para todos los errores relacionados con la configuración externa o el estado de conexión del almacén de claves externo. Para identificar el problema, utilice el texto del mensaje de error adjunto.

La siguiente tabla muestra las excepciones que pueden aparecer en el gráfico de las 5 excepciones principales y las excepciones correspondientes que AWS KMS devuelve.

Tipo de error	Excepción mostrada en el gráfico	Excepción que AWS KMS devolvió
No reintentable	**`AccessDeniedException`** Para obtener ayuda sobre la resolución de problemas, consulte Problemas de autorización de proxy.	**`CustomKeyStoreInvalidStateException`** en respuesta a operaciones `CreateKey` . **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.

Tipo de error	Excepción mostrada en el gráfico	Excepción que AWS KMS devolvió
No reintentable	**`AuthenticationFailedException`** Para obtener ayuda sobre la resolución de problemas, consulte Errores en las credenciales de autenticación.	**`XksProxyIncorrectAuthenticationCredentialException`** en respuesta a operaciones `CreateCustomKeyStore` y `UpdateCustomKeyStore`. **`CustomKeyStoreInvalidStateException`** en respuesta a operaciones `CreateKey`. **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.
Reintentable	**`DependencyTimeoutException`** Para obtener ayuda sobre la resolución de problemas, consulte Errores de latencia y tiempo de espera.	**`XksProxyUriUnreachableException`** en respuesta a operaciones `CreateCustomKeyStore` y `UpdateCustomKeyStore`. **`CustomKeyStoreInvalidStateException`** en respuesta a operaciones `CreateKey`. **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.

Tipo de error	Excepción mostrada en el gráfico	Excepción que AWS KMS devolvió
Reintentable	**`InternalException`** El proxy del almacén de claves externo rechazó la solicitud porque no puede comunicarse con el administrador de claves externo. Compruebe que la configuración del proxy del almacén de claves externo sea correcta y que el administrador de claves externo esté disponible.	**`XksProxyInvalidResponseException`** en respuesta a operaciones `CreateCustomKeyStore` y `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** en respuesta a operaciones `CreateKey` . **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.
No reintentable	**`InvalidCiphertextException`** Para obtener ayuda sobre la resolución de problemas, consulte Errores de descifrado.	**`KMSInvalidStateException`** en respuesta a operaciones criptográficas.
No reintentable	**`InvalidKeyUsageException`** Para obtener ayuda sobre la resolución de problemas, consulte Errores de operación criptográfica para la clave externa.	**`XksKeyInvalidConfigurationException`** en respuesta a operaciones `CreateKey` . **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.

Tipo de error	Excepción mostrada en el gráfico	Excepción que AWS KMS devolvió
No reintentable	**`InvalidStateException`** Para obtener ayuda sobre la resolución de problemas, consulte Errores de operación criptográfica para la clave externa.	**`XksKeyInvalidConfigurationException`** en respuesta a operaciones `CreateKey` . **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.
No reintentable	**`InvalidUriPathException`** Para obtener ayuda sobre la resolución de problemas, consulte Errores de configuración general.	**`XksProxyInvalidConfigurationException`** en respuesta a operaciones `CreateCustomKeyStore` y `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** en respuesta a operaciones `CreateKey` . **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.
No reintentable	**`KeyNotFoundException`** Para obtener ayuda sobre la resolución de problemas , consulte Errores de clave externa.	**`XksKeyNotFoundException`** en respuesta a operaciones `CreateKey` . **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.

Tipo de error	Excepción mostrada en el gráfico	Excepción que AWS KMS devolvió
Reintentable	**`ThrottlingException`** El proxy del almacén de claves externo rechazó la solicitud debido a una tasa de solicitudes muy alta. Reduzca la frecuencia de las llamadas con las claves de KMS en este almacén de claves externo.	**`XksProxyUriUnreachableException`** en respuesta a operaciones `CreateCustomKeyStore` y `UpdateCustomKeyStore` . **`CustomKeyStoreInvalidStateException`** en respuesta a operaciones `CreateKey` . **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.
No reintentable	**`UnsupportedOperationException`** Para obtener ayuda sobre la resolución de problemas, consulte Errores de operación criptográfica para la clave externa.	**`XksKeyInvalidResponseException`** en respuesta a operaciones `CreateKey` . **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.

Tipo de error	Excepción mostrada en el gráfico	Excepción que AWS KMS devolvió
No reintentable	**`ValidationException`** Para obtener ayuda sobre la resolución de problemas, consulte Problemas con el proxy.	**`XksProxyInvalidResponseException`** en respuesta a operaciones `CreateCustomKeyStore` y `UpdateCustomKeyStore`. **`CustomKeyStoreInvalidStateException`** en respuesta a operaciones `CreateKey`. **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.
Reintentable	**`XksProxyUnreachableException`** Si aparece este error varias veces, compruebe que el proxy del almacén de claves externo esté activo y conectado a la red, y que su ruta URI y su nombre de servicio de VPC o URI de punto de conexión sean correctos en su almacén de claves externo.	**`XksProxyUriUnreachableException`** en respuesta a operaciones `CreateCustomKeyStore` y `UpdateCustomKeyStore`. **`CustomKeyStoreInvalidStateException`** en respuesta a operaciones `CreateKey`. **`KMSInvalidStateException`** en respuesta a operaciones criptográficas.

El gráfico de las 5 excepciones principales se deriva de la métrica XksProxyErrors. Al ver un punto de datos específico, la ventana emergente muestra el valor de la dimensión `ExceptionName` junto

con la cantidad de veces que se registró la excepción en ese punto de datos. Los cinco elementos de la lista están ordenados de la excepción más frecuente a la menos frecuente.

Te recomendamos que utilices la XksProxyErrors métrica para crear una CloudWatch alarma que te avise de posibles problemas de configuración y te avise cuando se registren más de cinco errores que no se puedan volver a intentar en un período de un minuto. Para obtener más información, consulte Crear una CloudWatch alarma de Amazon para errores que no se pueden volver a intentar.

Días para el vencimiento del certificado

El número de días que faltan para que venza el certificado TLS del punto de conexión del proxy del almacén de claves externo (`XksProxyUriEndpoint`). Utilice este gráfico para monitorear el próximo vencimiento de su certificado TLS.

Cuando el certificado vence, AWS KMS no se puede comunicar con el proxy del almacén de claves externo. No se podrá acceder a todos los datos protegidos por las claves de KMS en su almacén de claves externo hasta que renueve el certificado.

El gráfico de días para el vencimiento del certificado se deriva de la métrica XksProxyCertificateDaysToExpire. Recomendamos encarecidamente utilizar esta métrica para crear una CloudWatch alarma que notifique la próxima caducidad. El vencimiento del certificado puede impedirle acceder a los recursos cifrados. Configure la alarma para que su organización tenga tiempo de renovar el certificado antes de que venza. Para obtener más información, consulte Crear una CloudWatch alarma de Amazon para la caducidad del certificado.

Configurar las alarmas

Los gráficos de la sección de monitoreo ofrecen una descripción general del estado de los almacenes de claves externos y de las claves de KMS de los almacenes de claves externos durante un periodo determinado. Sin embargo, puedes crear CloudWatch alarmas de Amazon basadas en métricas externas del almacén de claves para que te notifiquen cuando el valor de una métrica supere un umbral que hayas especificado. La alarma puede enviar el mensaje a un tema de Amazon Simple Notification Service (Amazon SNS) o a una política de Amazon EC2 Auto Scaling. Para obtener información detallada sobre CloudWatch las alarmas, consulta Uso de CloudWatch alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.

Antes de crear una CloudWatch alarma de Amazon, necesitas un tema de Amazon SNS. Para obtener más información, consulte el tema Creación de Amazon SNS en la Guía CloudWatch del usuario de Amazon.

Temas

Crear una CloudWatch alarma de Amazon para la caducidad del certificado

Esta alarma utiliza la XksProxyCertificateDaysToExpire métrica que se AWS KMS publica CloudWatch para registrar la caducidad prevista del certificado TLS asociado al punto de conexión proxy del almacén de claves externo. No puede crear una sola alarma para todos los almacenes de claves externos de su cuenta ni una alarma para los almacenes de claves externos que pueda crear en el futuro.

Le recomendamos configurar la alarma para que le avise 10 días antes de que venza su certificado, pero debe establecer el umbral que mejor se adapte a sus necesidades.

Crear la alarma

Siga las instrucciones de Crear una CloudWatch alarma basada en un umbral estático utilizando los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Seleccionar métrica	Elija KMS y, a continuación, elija XKS Proxy Certificate Metrics (Métricas del certificado de proxy XKS). Seleccione la casilla de verificación junto al `XksProxyCertificateName` que desea monitorear. A continuación, elija Select metric (Seleccionar métrica).
Estadística	Mínimo
Período	5 minutos
Tipo de umbral	Estático

Campo	Valor
Whenever…	Siempre que XksProxyCertificateDaysToExpiresea `Lower` que`10`.

Crear una CloudWatch alarma de Amazon para el tiempo de espera de respuesta

Esta alarma utiliza la XksProxyLatency métrica que se AWS KMS publica CloudWatch para registrar el número de milisegundos que tarda un proxy de almacén de claves externo en responder a una AWS KMS solicitud. No puede crear una sola alarma para todos los almacenes de claves externos de su cuenta ni una alarma para los almacenes de claves externos que pueda crear en el futuro.

AWS KMS espera que el proxy del almacén de claves externo responda a cada solicitud en 250 milisegundos. Recomendamos configurar una alarma para que le avise cuando su proxy del almacén de claves externo tarde más de 200 milisegundos en responder, pero debe establecer el umbral que mejor se adapte a sus necesidades.

Crear la alarma

Siga las instrucciones de Crear una CloudWatch alarma basada en un umbral estático utilizando los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Seleccionar métrica	Elija KMS y, a continuación, elija XKS Proxy Latency Metrics (Métricas del certificado de proxy XKS). Seleccione la casilla de verificación junto al `KmsOperation` que desea monitorear. A continuación, elija Select metric (Seleccionar métrica).
Estadística	Media
Período	5 minutos
Tipo de umbral	Estático
Whenever…	Siempre que XksProxyLatencysea `Greater` que`200`.

Crear una CloudWatch alarma de Amazon para errores reintentables

Esta alarma utiliza la XksProxyErrors métrica que se AWS KMS publica CloudWatch para registrar el número de excepciones relacionadas con las AWS KMS solicitudes a tu proxy de almacén de claves externo. No puede crear una sola alarma para todos los almacenes de claves externos de su cuenta ni una alarma para los almacenes de claves externos que pueda crear en el futuro.

Los errores reintentables reducirán el porcentaje de fiabilidad y pueden indicar errores de red. Le recomendamos configurar una alarma para que le avise cuando se registren más de cinco errores reintentables en un periodo de un minuto, pero debe establecer el umbral que mejor se adapte a sus necesidades.

Siga las instrucciones de Crear una CloudWatch alarma basada en un umbral estático utilizando los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Seleccionar métrica	Elija la pestaña Queries (Consultas). Elija `AWS/KMS` para Namespace (Espacio de nombres). Ingrese `SUM(XksProxyErrors)` para Metric name (Nombre de la métrica). Ingrese `ErrorType = Retryable` para Filter by (Filtrar por). Elija Ejecutar. A continuación, elija Select metric (Seleccionar métrica).
Etiqueta	*`Errores reintentables`*
Período	1 minuto
Tipo de umbral	Estático
Whenever…	Siempre que `q1` sea `Greater` que `5`.

Crear una CloudWatch alarma de Amazon para errores que no se pueden volver a intentar

Esta alarma utiliza la XksProxyErrors métrica que se AWS KMS publica CloudWatch para registrar el número de excepciones relacionadas con las AWS KMS solicitudes a tu proxy de almacén de claves

externo. No puede crear una sola alarma para todos los almacenes de claves externos de su cuenta ni una alarma para los almacenes de claves externos que pueda crear en el futuro.

Los errores no reintentables pueden indicar un problema con la configuración del almacén de claves externo. Le recomendamos configurar una alarma para que le avise cuando se registren más de cinco errores no reintentables en un periodo de un minuto, pero debe establecer el umbral que mejor se adapte a sus necesidades.

Siga las instrucciones de Crear una CloudWatch alarma basada en un umbral estático utilizando los siguientes valores obligatorios. Para los demás campos, acepte los valores predeterminados y proporcione los nombres solicitados.

Campo	Valor
Seleccionar métrica	Elija la pestaña Queries (Consultas). Elija `AWS/KMS` para Namespace (Espacio de nombres). Ingrese `SUM(XksProxyErrors)` para Metric name (Nombre de la métrica). Ingrese `ErrorType = Non-retryable` para Filter by (Filtrar por). Elija Ejecutar. A continuación, elija Select metric (Seleccionar métrica).
Etiqueta	*Errores no reintentables*
Período	1 minuto
Tipo de umbral	Estático
Whenever…	Siempre que `q1` sea `Greater` que `5`.

Conectar y desconectar un almacén de claves externo

Los nuevos almacenes de claves externos no están conectados. Para crear y utilizar AWS KMS keys en su almacén de claves externo, debe conectar su almacén de claves externo a su proxy del almacén de claves externo. Puede conectar y desconectar su almacén de claves externo en cualquier momento y ver su estado de conexión.

Mientras el almacén de claves externo esté desconectado, AWS KMS no podrá comunicarse con el proxy del almacén de claves externo. Como resultado, puede ver y administrar su almacén de claves externo y sus claves de KMS existentes. Sin embargo, no puede crear claves de KMS en su almacén de claves externo ni utilizar sus claves de KMS en operaciones criptográficas. Puede que tenga que desconectar el almacén de claves externo en algún momento, por ejemplo, al editar sus propiedades, por lo que debería planificar ante eventualidades. La desconexión del almacén de claves podría interrumpir el funcionamiento de los servicios de AWS que utilizan sus claves de KMS.

No es obligatorio conectar el almacén de claves externo. Puede dejar un almacén de claves externo desconectado de forma indefinida y conectarlo únicamente cuando tenga que usarlo. Sin embargo, le recomendamos que compruebe la conexión de forma periódica para verificar que la configuración es correcta y que se puede conectar.

Al desconectar un almacén de claves personalizado, las claves de KMS del almacén de claves quedan inutilizables de inmediato (sujeto a posible coherencia). Sin embargo, los recursos cifrados con claves de datos protegidas por la clave de KMS no se ven afectados hasta que se vuelva a utilizar la clave de KMS, por ejemplo, para descifrar la clave de datos. Este problema afecta a los Servicios de AWS, muchos de los cuales utilizan claves de datos para proteger sus recursos. Para obtener más detalles, consulte Cómo afectan las claves de KMS obsoletas a las claves de datos.

> **Note**
>
> Los almacenes de claves externos tienen un estado `DISCONNECTED` solo cuando el almacén de claves nunca se ha conectado o lo desconecta explícitamente. Un estado `CONNECTED` no indica que el almacén de claves externo o sus componentes de soporte estén funcionando de manera eficiente. Para obtener información sobre el rendimiento de los componentes del almacén de claves externo, consulte los gráficos de la sección Monitoreo de la página de detalles de cada almacén de claves externo. Para obtener más detalles, consulte Monitoreo de un almacén de claves externo.
>
> El administrador de claves externo puede proporcionar métodos adicionales para detener y reiniciar la comunicación entre el almacén de claves externo de AWS KMS y el proxy del almacén de claves externo, o entre el proxy del almacén de claves externo y el administrador de claves externo. Para obtener más detalles, consulte la documentación del administrador de claves externo.

Temas

- Conexión de un almacén de claves externo

- Desconexión de un almacén de claves externo
- Estado de la conexión
- Conectar un almacén de claves externo (consola)
- Conectar un almacén de claves externo (API)
- Desconectar un almacén de claves externo (consola)
- Desconectar un almacén de claves externo (API)

Conexión de un almacén de claves externo

Cuando el almacén de claves externo esté conectado, puede crear las claves de KMS en él y usar las claves de KMS existentes en operaciones criptográficas.

El proceso que conecta un almacén de claves externo a su proxy del almacén de claves externo difiere en función de la conectividad del almacén de claves externo.

- Cuando conecta un almacén de claves externo con conectividad de punto final público, AWS KMS envía una GetHealthStatus solicitud al proxy del almacén de claves externo para validar el punto final URI del proxy, la ruta URI del proxy y la credencial de autenticación del proxy. Una respuesta correcta del proxy confirma que el punto de conexión de la URI del proxy y la ruta de la URI del proxy son precisos y accesibles, y que el proxy autenticó la solicitud firmada con la credencial de autenticación del proxy para el almacén de claves externo.
- Al conectar un almacén de claves externo con conectividad al servicio de punto de conexión de VPC a su proxy del almacén de claves externo, AWS KMS hace lo siguiente:
  - Confirma que se ha verificado el dominio del nombre DNS privado especificado en el punto de conexión de URI del proxy.
  - Crea un punto de conexión de interfaz desde una VPC de AWS KMS a su servicio del punto de conexión de VPC.
  - Crea una zona alojada privada para el nombre DNS privado especificado en el punto de conexión de URI del proxy
  - Envía una GetHealthStatussolicitud al proxy del almacén de claves externo. Una respuesta correcta del proxy confirma que el punto de conexión de la URI del proxy y la ruta de la URI del proxy son precisos y accesibles, y que el proxy autenticó la solicitud firmada con la credencial de autenticación del proxy para el almacén de claves externo.

La operación de conexión inicia el proceso de conexión del almacén de claves personalizado, pero conectar un almacén de claves externo a su proxy externo tarda aproximadamente cinco minutos. Una respuesta correcta de la operación de conexión no indica que el almacén de claves externo esté conectado. Para confirmar que la conexión se ha realizado correctamente, utilice la AWS KMS consola o la DescribeCustomKeyStoresoperación para ver el estado de la conexión del almacén de claves externo.

Cuando el estado de conexión es `FAILED`, se muestra un código de error de conexión en la consola de AWS KMS y se agrega a la respuesta `DescribeCustomKeyStore`. Para obtener ayuda para interpretar los códigos de error de conexión, consulte Códigos de error de conexión para almacenes de claves externos.

Desconexión de un almacén de claves externo

Al desconectar un almacén de claves externo con conectividad a un servicio de punto de conexión de VPC de su proxy del almacén de claves externo, AWS KMS elimina el punto de conexión de su interfaz al servicio del punto de conexión de VPC y elimina la infraestructura de red que creó para respaldar la conexión. No se requiere ningún proceso equivalente para los almacenes de claves externos con puntos de conexión públicos. Esta acción no afecta al servicio del punto de conexión de VPC ni a ninguno de sus componentes de soporte, ni al proxy del almacén de claves externo ni a ningún componente externo.

Mientras el almacén de claves externo esté desconectado, AWS KMS no envía ninguna solicitud al proxy del almacén de claves externo. El estado de conexión del almacén de claves externo es `DISCONNECTED`. Las claves de KMS del almacén de claves externo desconectado se encuentran en el estado de clave `UNAVAILABLE` (a menos que estén pendientes de eliminación), lo que significa que no se pueden utilizar en operaciones criptográficas. Sin embargo, aún puede ver y administrar su almacén de claves externo y sus claves de KMS existentes.

El estado desconectado está diseñado para ser temporal y reversible. Puede volver a conectar el almacén de claves externo en cualquier momento. Por lo general, no es necesaria ninguna reconfiguración. Sin embargo, si alguna de las propiedades del proxy del almacén de claves externo asociado cambió mientras estaba desconectado, como la rotación de su credencial de autenticación del proxy, debe editar la configuración del almacén de claves externo antes de volver a conectarse.

> **Note**
>
> Mientras un almacén de claves personalizado esté desconectado, todos los intentos de crear claves KMS en el almacén de claves personalizado o de usar claves KMS existentes en

operaciones criptográficas fallarán. Esta acción puede impedir que los usuarios almacenen y accedan a datos confidenciales.

Para realizar una mejor estimación del efecto de desconectar el almacén de claves externo, identifique las claves de KMS en el almacén de claves externo y determine su uso en el pasado.

Puede desconectar el almacén de claves externo por los motivos siguientes:

- Para editar sus propiedades. Puede editar el nombre del almacén de claves personalizado, la ruta URI del proxy y la credencial de autenticación del proxy mientras el almacén de claves externo esté conectado. Sin embargo, para editar el tipo de conectividad del proxy, el punto de conexión URI del proxy o el nombre del servicio de punto de conexión de VPC, primero debe desconectar el almacén de claves externo. Para obtener más detalles, consulte Edición de propiedades del almacén de claves externo.
- Para detener toda comunicación entre el proxy del almacén de claves externo y AWS KMS. También puede detener la comunicación entre su proxy y AWS KMS al desactivar su punto de conexión o servicio del punto de conexión de VPC. Además, el proxy de su almacén de claves externo o el software de administración de claves pueden proporcionar mecanismos adicionales para impedir que AWS KMS se comunique con el proxy o evitar que el proxy acceda a su administrador de claves externo.
- Para deshabilitar todas las claves de KMS en el almacén de claves externo. Puede deshabilitar y volver a habilitar las claves KMS en un almacén de claves externo mediante la AWS KMS consola o la DisableKeyoperación. Estas operaciones se completan rápidamente (sujeto a eventual consistencia), pero actúan en una clave de KMS cada vez. La desconexión del almacén de claves externo cambia el estado de clave de todas las claves de KMS en el almacén de claves externo a `Unavailable`, lo que evita que se utilicen en operaciones criptográficas.
- Para reparar un error en la conexión. Si el intento de conexión al almacén de claves externo falla (el estado de la conexión del almacén de claves externo es `FAILED`), deberá desconectar el almacén de claves externo antes de intentar conectarlo de nuevo.

Estado de la conexión

La conexión y la desconexión cambian el estado de conexión del almacén de claves personalizado. Los valores del estado de conexión son los mismos para los almacenes de claves de AWS CloudHSM y para los almacenes de claves externos.

Para ver el estado de la conexión de su almacén de claves personalizado, utilice la DescribeCustomKeyStoresoperación o la AWS KMS consola. El Connection state (Estado de la conexión) aparece en cada tabla de almacén de claves personalizado, en la sección General configuration (Configuración general), y en la pestaña Cryptographic configuration (Configuración criptográfica) de las claves de KMS de un almacén de claves personalizado. Para más detalles, consulte Visualización de un almacén de claves de AWS CloudHSM y Visualización de un almacén de claves externo.

Un almacén de claves personalizado puede tener uno de los siguientes estados de conexión:

- `CONNECTED`: el almacén de claves personalizado está conectado a su almacén de claves de respaldo. Puede crear y usar claves de KMS en el almacén de claves personalizado.

  El almacén de claves de respaldo de un almacén de claves de AWS CloudHSM es su clúster de AWS CloudHSM asociado. El almacén de claves de respaldo de un almacén de claves externo es el proxy del almacén de claves externo y el administrador de claves externo que admite.

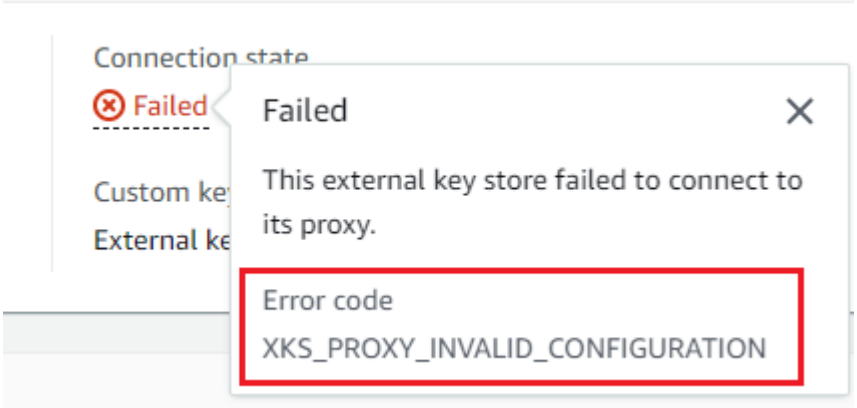
  El estado CONNECTED (CONECTADO) significa que la conexión se ha realizado correctamente y que el almacén de claves personalizado no se ha desconectado intencionadamente. No indica que la conexión funcione correctamente. Para obtener información sobre el estado del AWS CloudHSM clúster asociado a su almacén de AWS CloudHSM claves, consulte Obtener CloudWatch métricas AWS CloudHSM en la Guía del AWS CloudHSM usuario. Para obtener información sobre el estado y el funcionamiento del almacén de claves externo, consulte los gráficos de la sección Monitoreo de la página de detalles de cada almacén de claves externo. Para obtener más detalles, consulte Monitoreo de un almacén de claves externo.
- `CONNECTING`: el proceso de conectar un almacén de claves personalizado está en curso. Este es un estado transitorio.
- `DISCONNECTED`: El almacén de claves personalizado nunca se conectó a su soporte o se desconectó intencionadamente mediante la AWS KMS consola o la DisconnectCustomKeyStoreoperación.
- `DISCONNECTING`: el proceso de desconexión de un almacén de claves personalizado está en curso. Este es un estado transitorio.
- `FAILED`: se produjo un error al intentar conectar el almacén de claves personalizado. Lo que `ConnectionErrorCode` aparece en la DescribeCustomKeyStoresrespuesta indica el problema.

Para conectar un almacén de claves personalizado, su estado de conexión debe ser `DISCONNECTED`. Si el estado de la conexión es `FAILED`, utilice el `ConnectionErrorCode` para

identificar y resolver el problema. Luego, desconecte el almacén de claves personalizado antes de intentar conectarse de nuevo. Si desea ayuda con las conexiones que dan error, consulte Errores de conexión del almacén de claves externo. Para obtener ayuda sobre cómo responder a un código de error de conexión, consulte Códigos de error de conexión para almacenes de claves externos.

Para ver el código de error de conexión:

- En la DescribeCustomKeyStoresrespuesta, vea el valor del `ConnectionErrorCode` elemento. Este elemento aparece en la respuesta `DescribeCustomKeyStores` solo cuando el `ConnectionState` es `FAILED`.
- Para ver el código de error de conexión en la consola de AWS KMS, vaya a la página de detalles del almacén de claves externo y coloque el cursor sobre el valor Failed (Error).



Conectar un almacén de claves externo (consola)

Puede utilizar la consola de AWS KMS para conectar un almacén de claves externo a su proxy del almacén de claves externo.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Custom key stores (Almacenes de claves personalizados), External key stores (Almacenes de claves externos).
4. Elija la fila del almacén de claves externo que desee conectar.

   Si el estado de conexión del almacén de claves externo es FAILED (ERROR), deberá desconectar el almacén de claves externo antes de conectarlo.

5. En el menú Key store actions (Acciones del almacén de claves), seleccione Connect (Conectar).

El proceso de conexión suele tardar unos cinco minutos en completarse. Cuando se completa la operación, el estado de la conexión cambia a CONNECTED (CONECTADO).

Si el estado de conexión es Failed (Error), coloque el cursor sobre el estado de la conexión para ver el código de error de conexión, que explica la causa del error. Para obtener ayuda sobre cómo responder a un código de error de conexión, consulte Códigos de error de conexión para almacenes de claves externos. Para conectar un almacén de claves externo con un estado de conexión Failed (Error), primero debe desconectar el almacén de claves personalizado.

Conectar un almacén de claves externo (API)

Para conectar un almacén de claves externo desconectado, utilice la ConnectCustomKeyStoreoperación.

Antes de realizar la conexión, el estado de conexión del almacén de claves externo debe ser `DISCONNECTED`. Si el estado de conexión actual es `FAILED`, desconecte el almacén de claves externo y conéctelo de nuevo.

El proceso de conexión tarda hasta cinco minutos en completarse. A menos que el error sea rápido, la operación `ConnectCustomKeyStore` devuelve una respuesta HTTP 200 y un objeto JSON sin propiedades. Sin embargo, esta respuesta inicial no indica que la conexión se haya realizado correctamente. Para determinar si el almacén de claves externo está conectado, consulte el estado de la conexión en la DescribeCustomKeyStoresrespuesta.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Para identificar el almacén de claves externo, use el ID del almacén de claves personalizado. Puede encontrar el ID en la página de almacenes de claves personalizados de la consola o mediante la DescribeCustomKeyStoresoperación. Antes de ejecutar este ejemplo, reemplace el ID de ejemplo por uno válido.

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

En cambio, la operación `ConnectCustomKeyStore` no devuelve el `ConnectionState` en su respuesta. Para comprobar que el almacén de claves externo está conectado, utilice la DescribeCustomKeyStoresoperación. De forma predeterminada, esta operación devuelve los almacenes de claves personalizados de su cuenta y región. Pero puede usar el parámetro

`CustomKeyStoreId` o `CustomKeyStoreName` (pero no ambos) para limitar la respuesta a almacenes de claves personalizados determinados. El valor de `ConnectionState` `CONNECTED` indica que el almacén de claves externo está conectado a su proxy del almacén de claves externo.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "CONNECTED",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Si el valor de `ConnectionState` en la respuesta `DescribeCustomKeyStores` es `FAILED`, el elemento `ConnectionErrorCode` indica el motivo del error.

En el siguiente ejemplo, el valor `XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND` para el `ConnectionErrorCode` indica que AWS KMS no puede encontrar el servicio del punto de conexión de VPC que utiliza para comunicarse con el proxy del almacén de claves externo. Compruebe que el `XksProxyVpcEndpointServiceName` es correcto, que la entidad principal del servicio de AWS KMS es una entidad principal permitida en el servicio de punto de conexión de VPC de Amazon y que el servicio del punto de conexión de VPC no requiere la aceptación de las solicitudes de conexión. Para obtener ayuda sobre cómo responder a un código de error de conexión, consulte Códigos de error de conexión para almacenes de claves externos.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
```

```
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "FAILED",
      "ConnectionErrorCode": "XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Desconectar un almacén de claves externo (consola)

Puede utilizar la consola de AWS KMS para conectar un almacén de claves externo a su proxy del almacén de claves externo. Este proceso tarda alrededor de 5 minutos en completarse.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Custom key stores (Almacenes de claves personalizados), External key stores (Almacenes de claves externos).
4. Elija la fila del almacén de claves externo que desee desconectar.
5. En el menú Key store actions (Acciones del almacén de claves), seleccione Disconnect (Desconectar).

Cuando la operación finalizada, el estado de conexión cambia de DISCONNECTING (DESCONECTANDO) a DISCONNECTED (DESCONECTADO). Si la operación da error, aparecerá un mensaje de error donde se describe el problema y se explica cómo resolverlo. Si necesita más ayuda, consulte Errores de conexión del almacén de claves externo.

Desconectar un almacén de claves externo (API)

Para desconectar un almacén de claves externo conectado, utilice la DisconnectCustomKeyStoreoperación. Si la operación se realiza correctamente, AWS KMS devuelve

una respuesta HTTP 200 y un objeto JSON sin propiedades. El proceso tarda hasta cinco minutos en completarse. Para encontrar el estado de conexión del almacén de claves externo, utilice la DescribeCustomKeyStoresoperación.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

En este ejemplo, se desconecta un almacén de claves externo con la conectividad del servicio del punto de conexión de VPC. Antes de ejecutar este ejemplo, reemplace el ID del almacén de claves personalizado de ejemplo por uno válido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Para comprobar que el almacén de claves externo está desconectado, utilice la DescribeCustomKeyStoresoperación. De forma predeterminada, esta operación devuelve los almacenes de claves personalizados de su cuenta y región. Pero puede usar el parámetro `CustomKeyStoreId` o `CustomKeyStoreName` (pero no ambos) para limitar la respuesta a almacenes de claves personalizados determinados. El valor de `ConnectionState` `DISCONNECTED` indica que el almacén de claves externo ya no está conectado a su proxy del almacén de claves externo.

```
$ aws kms describe-custom-key-stores --custom-key-store-name ExampleXksVpc
{
    "CustomKeyStores": [
    {
      "CustomKeyStoreId": "cks-9876543210fedcba9",
      "CustomKeyStoreName": "ExampleXksVpc",
      "ConnectionState": "DISCONNECTED",
      "CreationDate": "2022-12-13T18:34:10.675000+00:00",
      "CustomKeyStoreType": "EXTERNAL_KEY_STORE",
      "XksProxyConfiguration": {
        "AccessKeyId": "ABCDE98765432EXAMPLE",
        "Connectivity": "VPC_ENDPOINT_SERVICE",
        "UriEndpoint": "https://example-proxy-uri-endpoint-vpc",
        "UriPath": "/example/prefix/kms/xks/v1",
        "VpcEndpointServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example"
      }
    }
  ]
}
```

Eliminación de un almacén de claves externo

Al eliminar un almacén de claves externo, AWS KMS elimina todos los metadatos del almacén de claves externo de AWS KMS, incluida la información sobre su proxy del almacén de claves externo. Esta operación no afecta al proxy del almacén de claves externo, al administrador de claves externo, a las claves externas ni a ningún recurso de AWS que haya creado para admitir el almacén de claves externo, como una VPC de Amazon o un servicio de punto de conexión de VPC.

Antes de eliminar un almacén de claves externo, debe eliminar todas las claves de KMS del almacén de claves y desconectar el almacén de claves de su proxy del almacén de claves externo. De lo contrario, fallarán los intentos de eliminar el almacén de claves.

Eliminar un almacén de claves externo es irreversible, pero puede crear un nuevo almacén de claves externo y asociarlo al mismo proxy del almacén de claves externo y al mismo administrador de claves externo. Sin embargo, no puede volver a crear las claves de KMS de cifrado simétrico en el almacén de claves externo, aunque tenga acceso al mismo material de claves externas. AWS KMS incluye metadatos en el texto cifrado simétrico exclusivo de cada clave de KMS. Esta función de seguridad garantiza que solo la clave de KMS que cifró los datos pueda descifrarlos.

En lugar de eliminar el almacén de claves externo, considere la posibilidad de desconectarlo. Mientras el almacén de claves externo esté desconectado, podrá administrar el almacén de claves externo y sus AWS KMS keys, pero no podrá crear ni usar las claves de KMS en el almacén de claves externo. Puede volver a conectar el almacén de claves externo en cualquier momento y reanudar el uso de sus claves de KMS para cifrar y descifrar datos. Un proxy del almacén de claves externo desconectado o sus claves de KMS no disponibles no incurren en ningún costo.

Temas

- Eliminación de un almacén de claves externo (consola)
- Eliminación de un almacén de claves externo (API)

Eliminación de un almacén de claves externo (consola)

Puede utilizar la consola de AWS KMS para eliminar un almacén de claves externo.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.

3. En el panel de navegación, elija Custom key stores (Almacenes de claves personalizados), External key stores (Almacenes de claves externos).
4. Busque la fila que representa el almacén de claves externo que quiere eliminar. Si el estado de conexión del almacén de claves externo no es DISCONNECTED (DESCONECTADO), debe desconectar el almacén de claves externo antes de eliminarlo.
5. En el menú Key store actions (Acciones del almacén de claves), seleccione Delete (Eliminar).

Cuando la operación finalice, aparecerá un mensaje de confirmación y el almacén de claves externo ya no aparecerá en la lista de almacenes de claves. Si la operación da error, aparecerá un mensaje de error donde se describe el problema y se explica cómo resolverlo. Si necesita más ayuda, consulte Solución de problemas de almacenes de claves externos.

Eliminación de un almacén de claves externo (API)

Para eliminar un almacén de claves externo, utilice la DeleteCustomKeyStoreoperación. Si la operación se realiza correctamente, AWS KMS devuelve una respuesta HTTP 200 y un objeto JSON sin propiedades.

Para empezar, desconecte el almacén de claves externo. Antes de ejecutar este comando, reemplace el ID del almacén de claves personalizado de ejemplo por uno válido.

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Una vez desconectado el almacén de claves externo, puede utilizar la DeleteCustomKeyStoreoperación para eliminarlo.

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

Para confirmar que se ha eliminado el almacén de claves externo, utilice la DescribeCustomKeyStoresoperación.

```
$ aws kms describe-custom-key-stores

{
    "CustomKeyStores": []
}
```

Si especifica un nombre o identificador del almacén de claves personalizado que ya no existe, AWS KMS devuelve una excepción `CustomKeyStoreNotFoundException`.

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0

An error occurred (CustomKeyStoreNotFoundException) when calling the
 DescribeCustomKeyStore operation:
```

Administrar claves de KMS en un almacén de claves externo

Para crear, ver, administrar, usar y programar la eliminación de las claves de KMS en un almacén de claves externo, utilice procedimientos que son muy similares a los que usa para otras claves de KMS. Sin embargo, cuando crea una clave de KMS en un almacén de claves externo, especifica un almacén de claves externo y una clave externa. Cuando usa una clave de KMS en un almacén de claves externo, el administrador de claves externo realiza las operaciones de cifrado y descifrado mediante la clave externa especificada.

AWS KMS no puede crear, ver, actualizar ni eliminar ninguna clave criptográfica en su administrador de claves externo. AWS KMS nunca accede directamente a su administrador de claves externo ni a ninguna clave externa. Todas las solicitudes de operaciones criptográficas están mediadas por su proxy del almacén de claves externo. Para usar una clave de KMS en un almacén de claves externo, el almacén de claves externo que aloja la clave de KMS debe estar conectado a su proxy del almacén de claves externo.

Características admitidas

Además de los procedimientos tratados en esta sección, puede hacer lo siguiente con las claves de KMS en un almacén de claves personalizado:

- Utilice políticas de claves, políticas de IAM y concesiones para controlar el acceso a las claves de KMS.
- Habilite y deshabilite las claves de KMS. Estas acciones no afectan a la clave externa del administrador de claves externo.
- Asigne etiquetas, cree alias y utilice el control de acceso basado en atributos (ABAC) para autorizar el acceso a las claves de KMS.
- Utilice las claves de KMS con Servicios de AWS que se integran con AWS KMS y que admiten las claves administradas por el cliente.

Características no admitidas

- Los almacenes de claves externos solo admiten claves de KMS de cifrado simétrico. No puede crear claves de KMS HMAC ni claves de KMS asimétricas en un almacén de claves externo.
- GenerateDataKeyPairy no GenerateDataKeyPairWithoutPlaintextson compatibles con las claves KMS de un almacén de claves externo.
- No puede usar una plantilla de AWS CloudFormation para crear un almacén de claves externo o una clave de KMS en un almacén de claves externo.
- Las claves multirregionales no se admiten en un almacén de claves externo.
- Las claves de KMS con material de clave importado no se admiten en un almacén de claves externo.
- La rotación automática de claves no es compatible con las claves de KMS en un almacén de claves externo.

Temas

- Crear claves de KMS en un almacén de claves externo
- Visualización de claves de KMS en un almacén de claves externo
- Utilizar claves de KMS en un almacén de claves externo
- Programar la eliminación de claves de KMS de un almacén de claves externo

Crear claves de KMS en un almacén de claves externo

Después de crear y conectar el almacén de claves externo, puede crear AWS KMS keys en su almacén de claves. Deben ser claves de KMS de cifrado simétrico con un valor de origen de Almacén de claves externo (`EXTERNAL_KEY_STORE`). No puede crear claves KMS asimétricas, claves KMS HMAC ni claves KMS con material clave importado en un almacén de claves personalizado. Además, no puede utilizar claves KMS de cifrado simétricas en un almacén de claves personalizado para generar pares de claves de datos asimétricos.

Una clave de KMS de un almacén de claves externo puede tener una latencia, durabilidad y disponibilidad más bajas que una clave de KMS estándar porque depende de componentes ubicados fuera de AWS. Antes de crear o utilizar una clave de KMS en un almacén de claves externo, compruebe que necesita una clave con las propiedades del almacén de claves externo.

> **Note**
>
> Algunos administradores de claves externos proporcionan un método más sencillo para crear claves de KMS en un almacén de claves externo. Para obtener más detalles, consulte la documentación del administrador de claves externo.

Para crear una clave de KMS en su almacén de claves externo, especifique lo siguiente:

- El ID de su almacén de claves externo.
- Un origen de material de claves del almacén de claves externo (`EXTERNAL_KEY_STORE`).
- El ID de una clave externa existente en el administrador de claves externo asociado al almacén de claves externo. Esta clave externa sirve como material de claves para la clave de KMS. No se puede cambiar el ID de clave externa después de crear la clave de KMS.

  AWS KMS proporciona el identificador de clave externa al proxy del almacén de claves externo en las solicitudes de operaciones de cifrado y descifrado. AWS KMS no puede acceder directamente a su administrador de claves externo ni a ninguna de sus claves criptográficas.

Además de la clave externa, una clave de KMS en un almacén de claves externo también contiene material de claves de AWS KMS. Todos los datos cifrados con la clave de KMS se cifran primero en AWS KMS con el material de claves de la clave de AWS KMS y, a continuación, mediante su administrador de claves externo con su clave externa. Este proceso de doble cifrado garantiza que el texto cifrado protegido por una clave de KMS en un almacén de claves externo sea tan seguro como el texto cifrado protegido solo por AWS KMS. Para obtener más detalles, consulte Cómo funcionan los almacenes de claves externos.

Cuando la operación `CreateKey` se realiza correctamente, el estado de la clave de la nueva clave de KMS es `Enabled`. Al ver una clave de KMS en un almacén de claves externo, puede ver las propiedades habituales, como el ID de la clave, la especificación de la clave, el uso de la clave, el estado de la clave y la fecha de creación. Sin embargo, también puede ver el ID y el estado de la conexión del almacén de claves externo y el ID de la clave externa.

Si intenta crear una clave de KMS en su almacén de claves externo sin éxito, utilice el mensaje de error para identificar la causa. Puede indicar que el almacén de claves externo no está conectado (`CustomKeyStoreInvalidStateException`), que el proxy del almacén de claves externo no puede encontrar una clave externa con el ID de clave externa especificado

(`XksKeyNotFoundException`) o que la clave externa ya está asociada a una clave de KMS en el mismo almacén de claves externo (`XksKeyAlreadyInUseException`).

.

Para ver un ejemplo del registro de AWS CloudTrail de la operación que crea una clave de KMS en un almacén de claves externo, consulte CreateKey.

Temas

- Requisitos para una clave de KMS en un almacén de claves externo
- Crear una clave de KMS en un almacén de claves externo (consola)
- Crear una clave de KMS en un almacén de claves externo (API de AWS KMS)

Requisitos para una clave de KMS en un almacén de claves externo

Para crear una clave de KMS en un almacén de claves externo, se requieren las siguientes propiedades del almacén de claves externo, la clave de KMS y la clave externa que sirve como material de clave criptográfica externa para la clave de KMS.

Requisitos de almacenes de claves externos

- Debe estar conectado a su proxy del almacén de claves externo.

  Para ver el estado de conexión de un almacén de claves externo, consulte Visualización de un almacén de claves externo. Para conectar su almacén de claves externo, consulte Conectar y desconectar un almacén de claves externo.

Requisitos de la clave de KMS

No puede cambiar estas propiedades después de crear la clave de KMS.

- Especificación de clave: SYMMETRIC_DEFAULT
- Uso de clave: ENCRYPT_DECRYPT
- Origen del material de claves: EXTERNAL_KEY_STORE
- Multirregión: FALSE

Requisitos de clave externa

- Clave criptográfica AES de 256 bits (256 bits aleatorios). El `KeySpec` de la clave externa debe ser `AES_256`.
- Habilitado y disponible para usarse. El `Status` de la clave externa debe ser `ENABLED`.
- Configurado para el cifrado y descifrado. El `KeyUsage` de la clave externa debe incluir `ENCRYPT` y `DECRYPT`.
- Se usa solo con esta clave de KMS. Cada `KMS key` de un almacén de claves externo debe estar asociada a una clave externa diferente.

  AWS KMS también recomienda que la clave externa se utilice exclusivamente para el almacén de claves externo. Esta restricción facilita la identificación y la resolución de problemas con la clave.
- Accesible mediante el proxy del almacén de claves externo para el almacén de claves externo.

  Si el proxy del almacén de claves externo no puede encontrar la clave con el ID de clave externa especificado, se produce un error en la operación `CreateKey`.
- Puede manejar el tráfico anticipado que genera el uso de Servicios de AWS. AWS KMS recomienda que las claves externas estén preparadas para manejar hasta 1800 solicitudes por segundo.

Crear una clave de KMS en un almacén de claves externo (consola)

Hay dos formas de crear una clave de KMS en un almacén de claves externo.

- Método 1 (recomendado): elija un almacén de claves externo y, a continuación, cree una clave de KMS en ese almacén de claves externo.
- Método 2: cree una clave de KMS y, a continuación, indique que está en un almacén de claves externo.

Si usa el método 1, en el que elige su almacén de claves externo antes de crear su clave, AWS KMS selecciona todas las propiedades de claves de KMS necesarias y rellena el ID de su almacén de claves externo. Este método evita los errores que puede cometer al crear la clave de KMS.

> **Note**
>
> No incluya información confidencial en el alias, la descripción ni las etiquetas. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

Método 1 (recomendado): comience en su almacén de claves externo

Para usar este método, elija su almacén de claves externo y, a continuación, cree una clave de KMS. La consola de AWS KMS selecciona todas las propiedades necesarias y rellena el ID de su almacén de claves externo. Este método evita muchos de los errores que puede cometer al crear la clave de KMS.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Custom key stores (Almacenes de claves personalizados), External key stores (Almacenes de claves externos).
4. Elija el nombre del almacén de claves externo.
5. En la esquina superior derecha, seleccione Create a KMS key in this key store (Crear una clave de KMS en este almacén de claves).

   Si el almacén de claves externo no está conectado, se le pedirá que lo conecte. Si el intento de conexión falla, debe resolver el problema y conectar el almacén de claves externo para poder crear una nueva claves de KMS en él.

   Si el almacén de claves externo está conectado, se redirigirá a la página de Customer managed keys (Claves gestionadas por el cliente) para crear una clave. Los valores de Configuración de claves requeridos ya están seleccionados. Además, se rellena el identificador del almacén de claves personalizado de su almacén de claves externo, aunque puede cambiarlo.
6. Introduzca el identificador de clave de una clave externa en su administrador de claves externo. Esta clave externa debe cumplir los requisitos para su uso con una clave de KMS. No puede cambiar este valor después de crear la clave.

   Si la clave externa tiene varios identificadores, introduzca el ID de clave que utiliza el proxy del almacén de claves externo para identificar la clave externa.
7. Confirme que va a crear una clave de KMS en el almacén de claves externo especificado.
8. Elija Siguiente.

   El resto de este procedimiento es el mismo que para crear una clave de KMS estándar.
9. Escriba un alias (requerido) y, una descripción (opcional) para la clave de KMS.

10. (Opcional). En la página agregar etiquetas, añada etiquetas que identifiquen o categoricen la clave KMS.

    Cuando se agregan etiquetas a los recursos de AWS, AWS genera un informe de asignación de costos con el uso y los costos agregados por etiquetas. Las etiquetas también pueden utilizarse para controlar el acceso a una clave KMS. Para obtener información acerca del etiquetado de claves KMS, consulte Etiquetado de claves y ABAC para AWS KMS.

11. Elija Siguiente.

12. En la sección administradores de claves, seleccione los usuarios y roles de IAM que pueden administrar la clave KMS. Para obtener más información, consulte Permite que los administradores de claves administren la clave de KMS.

    > **Note**
    >
    > Las políticas de IAM pueden otorgar permisos para usar la clave KMS a otros usuarios y roles de IAM.
    > Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

13. (Opcional) Para evitar que estos administradores de claves eliminen esta claves de KMS, desactive la casilla Allow key administrators to delete this key (Permitir que los administradores de claves eliminen esta clave).

    Eliminar una clave de KMS es una operación destructiva e irreversible que puede hacer que el texto cifrado sea irrecuperable. No puede volver a crear una clave de KMS simétrica en un almacén de claves externo, aunque disponga del material de claves externas. Sin embargo, eliminar una clave de KMS no afecta a su clave externa asociada. Para obtener información sobre cómo eliminar una clave de KMS de un almacén de claves externo, consulte Programar la eliminación de claves de KMS de un almacén de claves externo.

14. Elija Siguiente.

15. En la sección This account (Esta cuenta), seleccione los usuarios y roles de IAM de esta Cuenta de AWS que pueden usar la clave KMS en operaciones criptográficas. Para obtener más información, consulte Permite a los usuarios de claves utilizar la clave de KMS.

> **Note**
>
> Las políticas de IAM pueden otorgar permisos para usar la clave KMS a otros usuarios y roles de IAM.
> Las prácticas recomendadas de IAM desalientan el uso de usuarios de IAM con credenciales a largo plazo. Siempre que sea posible, utilice los roles de IAM, que proporcionan credenciales temporales. Para obtener más información, consulte la sección Prácticas recomendadas de seguridad de IAM en la Guía del usuario de IAM;.

16. (Opcional) Puede permitir que otras cuentas de Cuentas de AWS usen esta clave de KMS en operaciones criptográficas. Para ello, en la parte inferior de la página de la sección Other Cuentas de AWS (Otra) elija Add another Cuenta de AWS (Agregar otra) e ingrese el ID de Cuenta de AWS de una cuenta externa. Para agregar varias cuentas externas, repita este paso.

> **Note**
>
> Los administradores de las otras cuentas de Cuentas de AWS también deben permitir el acceso a la clave KMS mediante la creación de políticas de IAM para sus usuarios. Para obtener más información, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS.

17. Seleccione Siguiente.
18. Revise los ajustes de clave que ha elegido. Aún puede volver atrás y cambiar todos los ajustes.
19. Cuando haya acabado, elija Finish (Finalizar) para crear la clave.

Método 2: Comience con las claves gestionadas por el cliente

Este procedimiento es el mismo que el procedimiento para crear una clave de cifrado simétrica con material de claves de AWS KMS. Sin embargo, en este procedimiento, se especifica el ID del almacén de claves personalizado del almacén de claves externo y el ID de clave de la clave externa. También debe especificar los valores de propiedad requeridos para una clave de KMS en un almacén de claves externo, como la especificación de la clave y el uso de la clave.

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.

2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija Create key.
5. Seleccione Symmetric (Simétrica).
6. En Key usage (Uso de claves), se selecciona la opción Encrypt and decrypt (Cifrar y descifrar) para usted. No la cambie.
7. Elija Advanced options (Opciones avanzadas).
8. En Key material origin (Origen del material de claves), elija External key store (Almacenes de claves externos).
9. Confirme que va a crear una clave de KMS en el almacén de claves externo especificado.
10. Elija Siguiente.
11. Elija la fila que representa el almacén de claves externo para la nueva clave de KMS.

    No puede elegir un almacén de claves externo desconectado. Para conectar un almacén de claves que está desconectado, elija el nombre del almacén de claves y, a continuación, en Key store actions (Acciones del almacén de claves), elija Connect (Conectar). Para obtener más detalles, consulte Conectar un almacén de claves externo (consola).
12. Introduzca el identificador de clave de una clave externa en su administrador de claves externo. Esta clave externa debe cumplir los requisitos para su uso con una clave de KMS. No puede cambiar este valor después de crear la clave.

    Si la clave externa tiene varios identificadores, introduzca el ID de clave que utiliza el proxy del almacén de claves externo para identificar la clave externa.
13. Elija Siguiente.

    El resto de este procedimiento es el mismo que para crear una clave de KMS estándar.
14. Escriba un alias y, si lo desea, una descripción para la clave KMS.
15. (Opcional). En la página agregar etiquetas, añada etiquetas que identifiquen o categoricen la clave KMS.

    Cuando se agregan etiquetas a los recursos de AWS, AWS genera un informe de asignación de costos con el uso y los costos agregados por etiquetas. Las etiquetas también pueden utilizarse para controlar el acceso a una clave KMS. Para obtener información acerca del etiquetado de claves KMS, consulte Etiquetado de claves y ABAC para AWS KMS.

16. Elija Siguiente.
17. En la sección administradores de claves, seleccione los usuarios y roles de IAM que pueden administrar la clave KMS. Para obtener más información, consulte Permite que los administradores de claves administren la clave de KMS.

    > **Note**
    >
    > Las políticas de IAM pueden otorgar permisos para usar la clave KMS a otros usuarios y roles de IAM.

18. (Opcional) Para evitar que estos administradores de claves eliminen esta claves de KMS, desactive la casilla Allow key administrators to delete this key (Permitir que los administradores de claves eliminen esta clave).

    Eliminar una clave de KMS es una operación destructiva e irreversible que puede hacer que el texto cifrado sea irrecuperable. No puede volver a crear una clave de KMS simétrica en un almacén de claves externo, aunque disponga del material de claves externas. Sin embargo, eliminar una clave de KMS no afecta a su clave externa asociada. Para obtener información sobre cómo eliminar una clave de KMS de un almacén de claves externo, consulte Programar la eliminación de claves de KMS de un almacén de claves externo.
19. Elija Siguiente.
20. En la sección This account (Esta cuenta), seleccione los usuarios y roles de IAM de esta Cuenta de AWS que pueden usar la clave KMS en operaciones criptográficas. Para obtener más información, consulte Permite a los usuarios de claves utilizar la clave de KMS.

    > **Note**
    >
    > Las políticas de IAM pueden otorgar permisos para usar la clave KMS a otros usuarios y roles de IAM.

21. (Opcional) Puede permitir que otras cuentas de Cuentas de AWS usen esta clave KMS en operaciones criptográficas. Para ello, en la parte inferior de la página de la sección Other Cuentas de AWS (Otra) elija Add another Cuenta de AWS (Agregar otra) e ingrese el ID de Cuenta de AWS de una cuenta externa. Para agregar varias cuentas externas, repita este paso.

> **Note**
>
> Los administradores de las otras cuentas de Cuentas de AWS también deben permitir el acceso a la clave KMS mediante la creación de políticas de IAM para sus usuarios. Para obtener más información, consulte Permitir a los usuarios de otras cuentas utilizar una clave KMS.

22. Seleccione Siguiente.
23. Revise los ajustes de clave que ha elegido. Aún puede volver atrás y cambiar todos los ajustes.
24. Cuando haya acabado, elija Finish (Finalizar) para crear la clave.

Si el procedimiento se realiza correctamente, la pantalla mostrará la nueva clave de KMS en el almacén de claves externo de su elección. Al elegir el nombre o alias de la nueva clave de KMS, la pantalla Cryptographic configuration (Configuración criptográfica) de su página de detalles mostrará el origen de la clave de KMS (External key store [Almacén de claves externo]), el nombre, el ID y el tipo del almacén de claves personalizados, y el ID, el uso de claves y el estado de la clave externa. Si el procedimiento falla, aparecerá un mensaje de error que describe el motivo del error. Para , consulte Solución de problemas de almacenes de claves externos.

> **Tip**
>
> Para facilitar la identificación de las claves de KMS en un almacén de claves personalizado, en la página Customer managed keys (Claves administradas por el cliente), agregue la columna Origin (Origen) y Custom key store ID (ID del almacén de claves personalizado). Para cambiar los campos de la tabla, seleccione el icono de engranaje en la esquina superior derecha de la página. Para obtener más detalles, consulte Personalización de las tablas clave KMS.

Crear una clave de KMS en un almacén de claves externo (API de AWS KMS)

Para crear una nueva clave KMS en un almacén de claves externo, utilice la CreateKeyoperación. Se requieren los siguientes parámetros:

- El valor `Origin` debe ser `EXTERNAL_KEY_STORE`.

- El parámetro `CustomKeyStoreId` identifica el almacén de claves externo. El `ConnectionState` del almacén de claves externo especificado debe ser `CONNECTED`. Para encontrar el `CustomKeyStoreId` y `ConnectionState`, utilice la operación `DescribeCustomKeyStores`.
- El parámetro `XksKeyId` identifica las claves externas. Esta clave externa debe cumplir con los requisitos para la asociación con una clave de KMS.

También puede utilizar cualquiera de los parámetros opcionales de la operación `CreateKey`, como los parámetros `Policy` o Tags (Etiquetas).

> **Note**
>
> No incluya información confidencial en los campos `Description` o `Tags`. Estos campos pueden aparecer en texto plano en CloudTrail los registros y otros resultados.

En los ejemplos de esta sección, se utiliza la AWS Command Line Interface (AWS CLI), pero puede usar cualquier lenguaje de programación admitido.

Este comando de ejemplo utiliza la CreateKeyoperación para crear una clave KMS en un almacén de claves externo. La respuesta incluye las propiedades de las claves de KMS, el ID del almacén de claves externo y el ID, el uso y el estado de la clave externa. Para obtener información específica acerca de estos campos, consulte Visualización de claves de KMS en un almacén de claves externo.

Antes de ejecutar este comando, reemplace el ID del almacén de claves personalizado de ejemplo por un ID válido.

```
$ aws kms create-key --origin EXTERNAL_KEY_STORE --custom-key-store-
id cks-1234567890abcdef0 --xks-key-id bb8562717f809024
{
  "KeyMetadata": {
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "CreationDate": "2022-12-02T07:48:55-07:00",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "CustomKeyStoreId": "cks-1234567890abcdef0",
    "Description": "",
    "Enabled": true,
    "EncryptionAlgorithms": [
```

```
      "SYMMETRIC_DEFAULT"
    ],
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeySpec": "SYMMETRIC_DEFAULT",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "MultiRegion": false,
    "Origin": "EXTERNAL_KEY_STORE",
    "XksKeyConfiguration": {
      "Id": "bb8562717f809024"
    }
  }
}
```

Visualización de claves de KMS en un almacén de claves externo

Para ver las claves de KMS en un almacén de claves externo, utilice la AWS KMS consola o la DescribeKeyoperación. Puede usar las mismas técnicas que usaría para ver cualquier clave de AWS KMS administrada por el cliente. Para conocer la información básica, consulte Consultar claves.

En la consola de AWS KMS, las claves de KMS en su almacén de claves externo se muestran en la página Customer managed keys (Claves administradas por el cliente), junto con todas las demás claves administradas por el cliente en su Cuenta de AWS y región. Para identificar las claves de KMS en un almacén de claves externo, filtre por el valor de origen distintivo, el almacén de claves externo y el ID del almacén de claves personalizado.

Para obtener más información, consulte Visualización de un almacén de claves externo, Monitoreo de un almacén de claves externo y Registrar llamadas a la AWS KMS API con AWS CloudTrail.

Temas

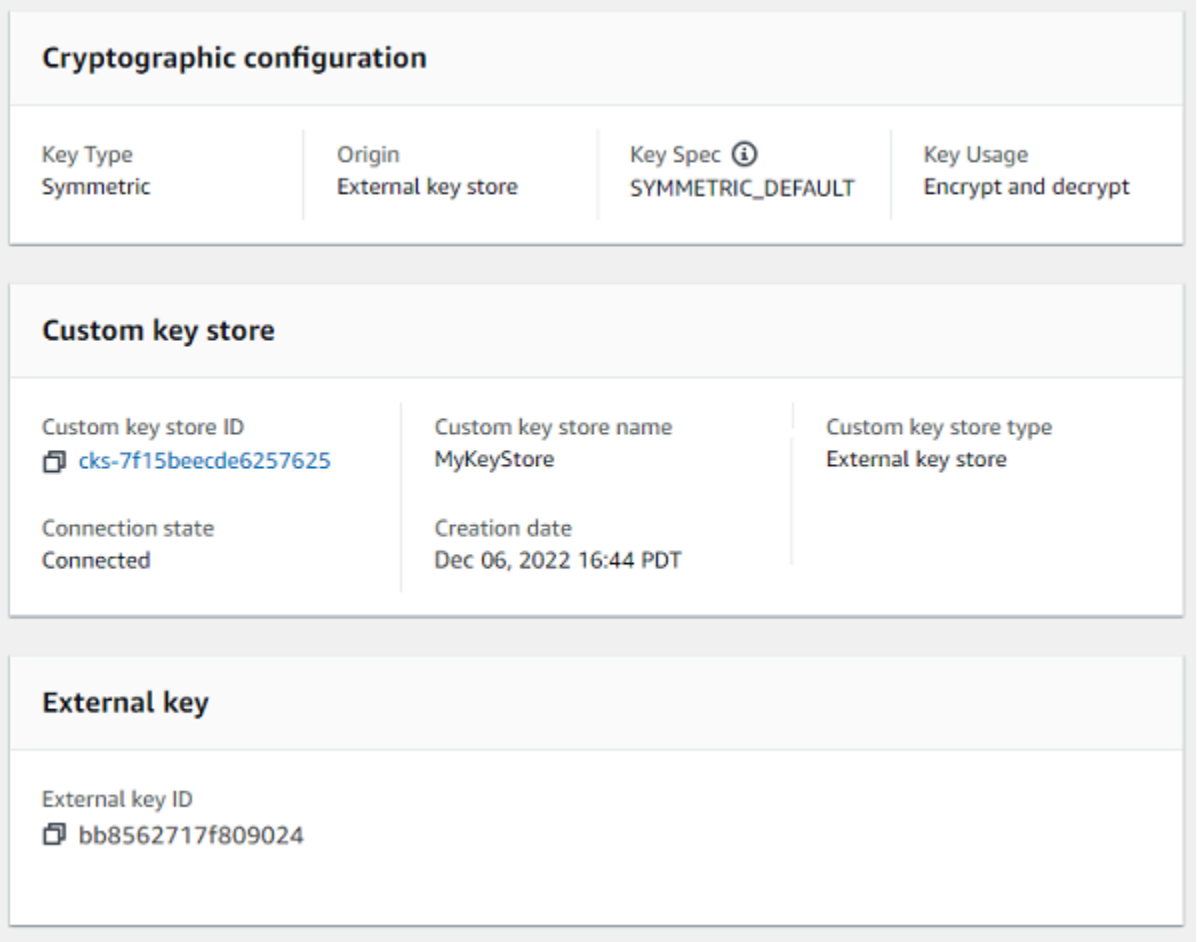
- Propiedades de las claves de KMS en un almacén de claves externo
- Visualización de claves de KMS en un almacén de claves externo (consola)
- Visualización de claves de KMS en un almacén de claves externo (API de AWS KMS)

Propiedades de las claves de KMS en un almacén de claves externo

Al igual que todas las claves de KMS, las claves de KMS en un almacén de claves externo tienen un ARN de clave, una especificación de clave y valores de uso de clave, pero también tienen

propiedades y valores de propiedad específicos para las claves de KMS en un almacén de claves externo. Por ejemplo, el valor de Origin (Origen) para todas las claves de KMS en almacenes de claves externos es External key store (Almacén de claves externas).

Para una clave de KMS en un almacén de claves externo, la pestaña Cryptographic configuration (Configuración criptográfica) en la consola de AWS KMS incluye dos secciones adicionales: Custom key store (Almacén de claves personalizado) y External key (Clave externa).



Propiedades del almacén de claves personalizado

Los siguientes valores aparecen en la sección Almacén de claves personalizado de la pestaña Configuración criptográfica y en la DescribeKeyrespuesta. Estas propiedades se aplican a todos los almacenes de claves personalizados, incluidos los almacenes de claves de AWS CloudHSM y los almacenes de claves externos.

ID del almacén de claves personalizadas

Un ID único que AWS KMS asigna al almacén de claves personalizado.

Nombre del almacén de claves personalizadas

Un nombre fácil de recordar que asigna al almacén de claves personalizado al crearlo. Puede cambiar este valor en cualquier momento.

Tipo de almacén de claves personalizado

El tipo de almacén de claves personalizado. Los valores válidos son AWS CloudHSM (`AWS_CLOUDHSM`) o Almacén de claves externo (`EXTERNAL_KEY_STORE`). No se puede cambiar el tipo después de crear el almacén de claves personalizado.

Fecha de creación

Fecha en la que se creó el almacén de claves personalizado. Este valor se muestra en la hora local de la Región de AWS.

Estado de la conexión

Indica si el almacén de claves personalizado está conectado a su almacén de claves de respaldo. El estado de conexión será `DISCONNECTED` solo si el almacén de claves personalizado nunca se ha conectado al almacén de claves de respaldo o se ha desconectado intencionadamente. Para obtener más detalles, consulte the section called “Estado de la conexión”.

Propiedades de claves externas

Las propiedades de la clave externa aparecen en la sección Clave externa de la pestaña Configuración criptográfica y en el `XksKeyConfiguration` elemento de la DescribeKeyrespuesta.

La sección External key (Clave externa) aparece en la consola de AWS KMS solo para las claves de KMS de los almacenes de claves externos. Proporciona información sobre la clave externa asociada a la clave de KMS. La clave externa es una clave criptográfica fuera de AWS que se usa como material de claves para la clave de KMS en el almacén de claves externo. Cuando cifra o descifra con la clave de KMS, la operación la realiza su administrador de claves externo utilizando la clave externa especificada.

Los siguientes valores aparecen en la sección External key (Clave externa).

ID de clave externa

El identificador de la clave externa en su administrador de claves externo. Este es el valor que utiliza el proxy del almacén de claves externo para identificar la clave externa. Usted especifica

el ID de la clave externa cuando crea la clave de KMS y no puede cambiarla. Si el valor del identificador de clave externa que utilizó para crear la clave de KMS cambia o deja de ser válida, debe programar la eliminación de la clave de KMS y crear una nueva clave de KMS con el valor de ID de clave externa correcto.

Visualización de claves de KMS en un almacén de claves externo (consola)

Para ver las claves de KMS en un almacén de claves externo (Consola)

1. Abra la consola de AWS KMS en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Para identificar las claves de KMS en su almacén de claves externo, agregue los campos de Origin (Origen) y de Custom key store ID (ID del almacén de claves personalizado) a su tabla de claves. Las claves de KMS de cualquier almacén de claves externo tienen un valor de Origin (Origen) de Custom key store ID (Almacén de claves externo).

   En la esquina superior derecha, elija el icono de engranaje, elija Origin (Origen) y Custom key store ID (ID de almacén de clave personalizado), luego elija Confirm (Confirmar).
5. Elija el alias o ID de clave de una clave de KMS en un almacén de claves externo.
6. Para ver las propiedades específicas de las claves de KMS en un almacén de claves externo, elija la pestaña Cryptographic configuration (Configuración criptográfica). Los valores especiales para las claves de KMS de un almacén de claves externo aparecen en las secciones Custom key store (Almacén de claves personalizado) y External key (Clave externa).

Visualización de claves de KMS en un almacén de claves externo (API de AWS KMS)

Para ver las claves de KMS en un almacén de claves externo (API)

Utiliza las mismas operaciones de AWS KMS API para ver las claves de KMS en un almacén de claves externo que usaría para cualquier clave de KMS, incluidas ListKeysDescribeKey, y GetKeyPolicy. Por ejemplo, la siguiente operación `describe-key` en la AWS CLI muestra los campos especiales para una clave de KMS en un almacén de claves externo. Antes de ejecutar un comando de este tipo, reemplace el ID de la clave KMS de ejemplo por un valor válido.

```
$ aws kms describe-key --key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

```
{
  "KeyMetadata": {
    "Arn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "AWSAccountId": "111122223333",
    "CreationDate": "2022-12-02T07:48:55-07:00",
    "CustomerMasterKeySpec": "SYMMETRIC_DEFAULT",
    "CustomKeyStoreId": "cks-1234567890abcdef0",
    "Description": "",
    "Enabled": true,
    "EncryptionAlgorithms": [
      "SYMMETRIC_DEFAULT"
    ],
    "KeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "KeyManager": "CUSTOMER",
    "KeySpec": "SYMMETRIC_DEFAULT",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT_DECRYPT",
    "MultiRegion": false,
    "Origin": "EXTERNAL_KEY_STORE",
    "XksKeyConfiguration": {
      "Id": "bb8562717f809024"
    }
  }
}
```


Utilizar claves de KMS en un almacén de claves externo

Después de crear una clave de KMS de cifrado simétrica en un almacén de claves externo, puede usarla para las siguientes operaciones criptográficas:

- Encrypt
- Decrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt

Las operaciones de cifrado simétrico que generan pares de claves de datos asimétricos no se admiten en los almacenes de claves personalizados. GenerateDataKeyPairGenerateDataKeyPairWithoutPlaintext

Se admite un contexto de cifrado para todas las operaciones criptográficas con claves de KMS en un almacén de claves externo. Como siempre, el uso de un contexto de cifrado es una de las mejores prácticas de seguridad que recomienda AWS KMS.

Cuando utilice su clave de KMS en una solicitud, identifique la clave de KMS por su ID de clave, ARN de clave, alias o ARN de alias. No tiene que especificar el almacén de claves externo. La respuesta incluye los mismos campos que se devuelven para cualquier clave KMS de cifrado simétrica. Sin embargo, cuando utiliza una clave de KMS en un almacén de claves externo, el administrador de claves externo realiza las operaciones de cifrado y descifrado mediante la clave externa especificada.

Para garantizar que el texto cifrado con una clave de KMS en un almacén de claves externo sea tan seguro como cualquier texto cifrado con una clave de KMS estándar, AWS KMS utiliza un cifrado doble. Los datos se cifran primero en AWS KMS mediante el uso de material de clave de AWS KMS. A continuación, su administrador de claves externo lo cifra utilizando la clave externa de la clave de KMS. Para descifrar el texto cifrado con doble cifrado, el administrador de claves externo descifra primero el texto cifrado mediante la clave externa de la clave de KMS. Luego se descifra en AWS KMS utilizando el material de clave de AWS KMS para la clave de KMS.

Para ello, se deben cumplir las siguientes condiciones.

- El estado de clave de la clave KMS debe ser `Enabled`. Para encontrar el estado de la clave, consulte el campo Estado de las claves administradas por el cliente, la AWS KMSconsola o el `KeyState` campo de la DescribeKeyrespuesta.
- El almacén de claves externo que aloja la clave de KMS debe estar conectado a su proxy del almacén de claves externo, es decir, el estado de conexión del almacén de claves externo debe ser `CONNECTED`.

  Puede ver el estado de la conexión en la página de almacenes de claves externos de la AWS KMS consola o en la DescribeCustomKeyStoresrespuesta. El estado de la conexión del almacén de claves externo también se muestra en la página de detalles de la clave de KMS en la consola de AWS KMS. En la página de detalles, elija la pestaña Cryptographic configuration (Configuración criptográfica) y consulte el campo Connection state (Estado de la conexión) en la sección Custom key store (Almacén de claves personalizado).

  Si el estado de la conexión es `DISCONNECTED`, primero debe conectarlo. Si el estado de la conexión es `FAILED`, debe resolver el problema, desconectar el almacén de claves externo y, a continuación, conectarlo. Para ver instrucciones, consulte Conectar y desconectar un almacén de claves externo.

- El proxy del almacén de claves externo debe poder encontrar la clave externa.
- La clave externa debe estar habilitada y debe realizar el cifrado y el descifrado.

  El estado de la clave externa es independiente y no se ve afectado por los cambios en el estado de la clave de KMS, incluida la habilitación y deshabilitación de la clave de KMS. Del mismo modo, deshabilitar o eliminar la clave externa no cambia el estado de la clave de KMS, pero las operaciones criptográficas que utilicen la clave de KMS asociada fallarán.

Si no se cumplen estas condiciones, la operación criptográfica dará error y AWS KMS devolverá una excepción `KMSInvalidStateException`. Puede que tenga que volver a conectar el almacén de claves externo o utilizar las herramientas del administrador de claves externo para reconfigurar o reparar la clave externa. Para obtener ayuda adicional, consulte the section called “Solución de problemas de almacenes de claves externos”.

Cuando utilice claves de KMS en un almacén de claves externo, tenga en cuenta que las claves de KMS de cada almacén de claves externo comparten una cuota de solicitudes del almacén de claves personalizado para operaciones criptográficas. Si supera la cuota, AWS KMS devuelve una `ThrottlingException`. Para obtener más información sobre la cuota de solicitudes del almacén de claves personalizado, consulte Cuotas de solicitudes del almacén de claves personalizado.

Programar la eliminación de claves de KMS de un almacén de claves externo

Si está seguro de que no necesitará una AWS KMS key para ninguna operación criptográfica, puede programar la eliminación de la clave KMS. Puede usar el mismo procedimiento que utilizaría para programar la eliminación de una clave KMS de AWS KMS. La eliminación de una clave de KMS de un almacén de claves externo no afecta a la clave externa que sirvió como material de claves.

Puede cancelar la eliminación programada de una clave de KMS durante su periodo de espera. Sin embargo, una clave de KMS eliminada no se puede recuperar. No puede volver a crear una clave de KMS de cifrado simétrico en un almacén de claves externo, incluso si usa la misma clave externa. Como cada clave de KMS simétrica de un almacén de claves externo tiene un material de claves de AWS KMS y metadatos únicos, solo la clave de AWS KMS que cifró un texto cifrado simétrico puede descifrarlo.

> **Warning**
>
> Eliminar una clave de KMS es una operación destructiva y potencialmente peligrosa que evita que recupere todo el cifrado de datos con la clave de KMS. Antes de programar la

eliminación de la clave de KMS, examine el uso anterior de la clave de KMS y cree una CloudWatch alarma de Amazon que le avise cuando alguien intente usar la clave de KMS mientras está pendiente de ser eliminada. Es preferible, siempre que sea posible, desactivar la clave KMS a eliminarla.

Cuando programa la eliminación de una clave de KMS de un almacén de claves externo, su estado de clave cambia a Pending deletion (Eliminación pendiente). La clave de KMS conservará el estado Pending deletion (Eliminación pendiente) durante todo el periodo de espera, incluso si la clave de KMS deja de estar disponible porque ha desconectado el almacén de claves externo. Esto permite cancelar la eliminación de la clave KMS en cualquier momento durante el período de espera. Cuando finaliza el periodo de espera, AWS KMS elimina la clave KMS de AWS KMS.

Al programar la eliminación de una clave de KMS de un almacén de claves externo, la clave de KMS queda inutilizable de inmediato (sujeto a la posible coherencia). Sin embargo, los recursos cifrados con claves de datos protegidas por la clave de KMS no se ven afectados hasta que se vuelva a utilizar la clave de KMS, por ejemplo, para descifrar la clave de datos. Este problema afecta a los Servicios de AWS, muchos de los cuales utilizan claves de datos para proteger sus recursos. Para obtener más detalles, consulte Cómo afectan las claves de KMS obsoletas a las claves de datos.

Puede monitorear la programación, la cancelación y la eliminación de la clave de KMS en sus registros de AWS CloudTrail.

Solución de problemas de almacenes de claves externos

La solución de la mayoría de los problemas con los almacenes de claves externos se indica mediante el mensaje de error que AWS KMS aparece con cada excepción o mediante el código de error de conexión que AWS KMS aparece cuando se produce un error al intentar conectar el almacén de claves externo a su proxy de almacén de claves externo. Sin embargo, algunos problemas son un poco más complejos.

Al diagnosticar un problema con un almacén de claves externo, localice primero la causa. Esto reducirá la gama de soluciones y hará que la solución de problemas sea más eficiente.

- AWS KMS — El problema puede estar dentro AWS KMS, por ejemplo, un valor incorrecto en la configuración del almacén de claves externo.
- Externo: el problema puede originarse fuera de AWS KMS, incluidos los problemas con la configuración o el funcionamiento del proxy del almacén de claves externo, el administrador de claves externo, las claves externas o el servicio de punto final de la VPC.

- Redes: puede tratarse de un problema de conectividad o de red, como un problema con el punto de conexión del proxy, el puerto o el dominio o nombre DNS privado.

> **Note**
>
> Cuando las operaciones de administración en almacenes de claves externos fallan, se generan varias excepciones diferentes. Sin embargo, las operaciones AWS KMS criptográficas se `KMSInvalidStateException` repiten cuando se producen errores relacionados con la configuración externa o el estado de conexión del almacén de claves externo. Para identificar el problema, utilice el texto del mensaje de error adjunto. La ConnectCustomKeyStoreoperación se realiza rápidamente antes de que se complete el proceso de conexión. Para determinar si el proceso de conexión se ha realizado correctamente, consulte el estado de conexión del almacén de claves externo. Si el proceso de conexión falla, AWS KMS devuelve un código de error de conexión que explica la causa y sugiere una solución.

Temas

Herramientas de solución de problemas para almacenes de claves externos

AWS KMS proporciona varias herramientas para ayudarle a identificar y resolver problemas con el almacén de claves externo y sus claves. Utilice estas herramientas junto con las herramientas proporcionadas con su proxy del almacén de claves externo y su administrador de claves externo.

> **Note**
>
> El proxy del almacén de claves externo y el administrador de claves externo pueden proporcionar métodos más sencillos para crear y mantener el almacén de claves externo y sus claves de KMS. Para obtener más detalles, consulte la documentación de sus herramientas externas.

AWS KMS excepciones y mensajes de error

AWS KMS proporciona un mensaje de error detallado sobre cualquier problema que encuentre. Puedes encontrar información adicional sobre AWS KMS las excepciones en la referencia de la AWS Key Management Service API y en AWS los SDK. Incluso si utilizas la AWS KMS consola, estas referencias pueden resultarte útiles. Por ejemplo, consulte la lista de errores de la operación `CreateCustomKeyStores`.

Si el problema surge en otro AWS servicio, por ejemplo, cuando utilizas una clave KMS en tu almacén de claves externo para proteger un recurso de otro AWS servicio, es posible que el AWS servicio proporcione información adicional para ayudarte a identificar el problema. Si el AWS servicio no proporciona el mensaje, puedes ver el mensaje de error en los CloudTrail registros que registran el uso de tu clave KMS.

CloudTrail registros

Todas las operaciones de la AWS KMS API, incluidas las acciones de la AWS KMS consola, se registran en AWS CloudTrail los registros. AWS KMS registra una entrada de registro para las operaciones correctas y fallidas. Para las operaciones fallidas, la entrada del registro incluye el nombre de la excepción de AWS KMS (`errorCode`) y el mensaje de error (`errorMessage`). Puede utilizar esta información como ayuda para identificar y resolver el error. Para ver un ejemplo, consulte Error de descifrado con una clave de KMS en un almacén de claves externo.

La entrada de registro también incluye el ID de la solicitud. Si la solicitud llegó a su proxy del almacén de claves externo, puede utilizar el ID de solicitud de la entrada de registro para buscar la solicitud correspondiente en sus registros de proxy, si su proxy los proporciona.

CloudWatch métricas

AWS KMS registra CloudWatch estadísticas detalladas de Amazon sobre el funcionamiento y el rendimiento de tu almacén de claves externo, como la latencia, la limitación, los errores de proxy, el estado del administrador de claves externo, el número de días que faltan para que caduque tu

certificado TLS y la antigüedad declarada de tus credenciales de autenticación de proxy. Puede utilizar estas métricas para desarrollar modelos de datos para el funcionamiento de su almacén de claves externo y CloudWatch alarmas que le avisen de problemas inminentes antes de que se produzcan.

> **Important**
>
> AWS KMS recomienda crear CloudWatch alarmas para supervisar las métricas del almacén de claves externo. Estas alarmas le avisarán de las señales tempranas de problemas antes de que se presenten.

Gráficos de monitorización

AWS KMS muestra gráficos de las CloudWatch métricas del almacén de claves externo en la página de detalles de cada almacén de claves externo de la AWS KMS consola. Puede utilizar los datos de los gráficos para localizar el origen de los errores, detectar problemas inminentes, establecer líneas de base y refinar los umbrales de alarma. CloudWatch Para obtener más detalles sobre la interpretación de los gráficos de monitoreo y el uso de sus datos, consulte Monitoreo de un almacén de claves externo.

Visualización de almacenes de claves externos y claves de KMS

AWS KMS muestra información detallada sobre los almacenes de claves externos y las claves de KMS del almacén de claves externo de la AWS KMS consola y sobre la respuesta a las operaciones y. DescribeCustomKeyStoresDescribeKey Estas pantallas incluyen campos especiales para almacenes de claves externos y claves de KMS con información que puede utilizar para solucionar problemas, como el estado de conexión del almacén de claves externo y el ID de clave externa asociada a la clave de KMS. Para más detalles, consulte Visualización de un almacén de claves externo y Visualización de claves de KMS en un almacén de claves externo.

XKS Proxy Test Client

AWS KMS proporciona un cliente de prueba de código abierto que verifica que el proxy del almacén de claves externo cumpla con la especificación de la API de proxy del almacén de claves AWS KMS externo. Puede utilizar este cliente de prueba para identificar y resolver problemas con su proxy del almacén de claves externo.

Errores de configuración

Al crear un almacén de claves externo, especifica los valores de propiedades que comprenden la configuración del almacén de claves externo, como la credencial de autenticación del proxy, el punto de conexión URI del proxy, la ruta URI del proxy y el nombre del servicio de punto de conexión de VPC. Cuando AWS KMS detecta un error en el valor de una propiedad, la operación falla y devuelve un error que indica el valor defectuoso.

Muchos problemas de configuración se pueden resolver al corregir el valor incorrecto. Puede corregir una ruta URI del proxy o una credencial de autenticación del proxy no válidas sin desconectar el almacén de claves externo. Para obtener las definiciones de estos valores, incluidos los requisitos de exclusividad, consulte Cumplir los requisitos previos. Para obtener instrucciones sobre cómo actualizar estos valores, consulte Edición de propiedades del almacén de claves externo.

Para evitar errores con la ruta URI del proxy y los valores de la credencial de autenticación del proxy, al crear o actualizar el almacén de claves externo, cargue un archivo de configuración del proxy en la consola de AWS KMS . Se trata de un archivo basado en JSON con la ruta URI del proxy y los valores de la credencial de autenticación del proxy que proporciona el proxy del almacén de claves externo o el administrador de claves externo. No puedes usar un archivo de configuración de proxy con las operaciones de la AWS KMS API, pero puedes usar los valores del archivo para ayudarte a proporcionar valores de parámetros para tus solicitudes de API que coincidan con los valores de tu proxy.

Errores de configuración general

Excepciones: `CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operaciones criptográficas), `XksProxyInvalidConfigurationException` (operaciones de administración, excepto `CreateKey`)

Códigos de error de conexión: `XKS_PROXY_INVALID_CONFIGURATION`, `XKS_PROXY_INVALID_TLS_CONFIGURATION`

En el caso de los almacenes de claves externos con conectividad de punto final público, AWS KMS comprueba los valores de las propiedades al crear y actualizar el almacén de claves externo. En el caso de los almacenes de claves externos con conectividad al servicio de punto de conexión de VPC, AWS KMS prueba los valores de propiedades al conectar y actualizar el almacén de claves externo.

> **Note**
>
> La operación `ConnectCustomKeyStore`, que es asincrónica, puede realizarse correctamente aunque falle el intento de conectar el almacén de claves externo a su proxy del almacén de claves externo. En ese caso, no hay ninguna excepción, pero el estado de conexión del almacén de claves externo es Failed (Error) y aparece un código de error de conexión que explica el mensaje de error. Para obtener más información, consulte Errores de conexión del almacén de claves externo.

Si AWS KMS detecta un error en el valor de una propiedad, se produce un error en la operación y se devuelve `XksProxyInvalidConfigurationException` con uno de los siguientes mensajes de error.

El proxy del almacén de claves externo rechazó la solicitud porque la ruta URI no era válida. Verifique la ruta URI del almacén de claves externo y actualícela si es necesario.

- La ruta URI del proxy es la ruta base para AWS KMS las solicitudes a las API del proxy. Si esta ruta es incorrecta, fallarán todas las solicitudes al proxy. Para ver la ruta URI del proxy actual del almacén de claves externo, utilice la consola de AWS KMS o la operación `DescribeCustomKeyStores`. Para encontrar la ruta URI del proxy correcta, consulte la documentación del proxy del almacén de claves externo. Para obtener ayuda para corregir el valor de la ruta URI del proxy, consulte Edición de propiedades del almacén de claves externo.
- La ruta URI del proxy del almacén de claves externo puede cambiar con las actualizaciones del proxy del almacén de claves externo o del administrador de claves externo. Para obtener información sobre estos cambios, consulte la documentación del proxy del almacén de claves externo o administrador de claves externo.

`XKS_PROXY_INVALID_TLS_CONFIGURATION`
AWS KMS no puede establecer una conexión TLS con el proxy del almacén de claves externo. Verifique la configuración de TLS, incluido su certificado.

- Todos los proxy del almacén de claves externo requieren un certificado TLS. El certificado TLS debe ser emitido por una autoridad de certificación (CA) pública que sea compatible con

almacenes de claves externos. Para obtener una lista de las CA compatibles, consulte Autoridades de certificación de confianza en la Especificación de la API de proxy del almacén de claves externo de AWS KMS .

- Para la conectividad a puntos de conexión públicos, el nombre común (CN) del asunto del certificado TLS debe coincidir con el nombre de dominio del punto de conexión URI del proxy del proxy del almacén de claves externo. Por ejemplo, si el punto de conexión público es https://myproxy.xks.example.com, el TLS, el CN del certificado TLS debe ser `myproxy.xks.example.com` o `*.xks.example.com`.
- Para la conectividad al servicio de punto de conexión de VPC, el nombre común (CN) del asunto del certificado TLS debe coincidir con el nombre DNS privado del servicio de punto de conexión de VPC. Por ejemplo, si el nombre DNS privado es myproxy-private.xks.example.com, el CN del certificado TLS debe ser `myproxy-private.xks.example.com` o `*.xks.example.com`.
- El certificado TLS no puede estar caducado. Para obtener la fecha de caducidad de un certificado TLS, utilice herramientas SSL, como OpenSSL. Para supervisar la fecha de caducidad de un certificado TLS asociado a un almacén de claves externo, usa la XksProxyCertificateDaysToExpire CloudWatch métrica. El número de días que faltan para la fecha de caducidad de la certificación TLS también aparece en la sección Supervisión de la AWS KMS consola.
- Si utiliza una conectividad a puntos de conexión públicos, utilice las herramientas de prueba de SSL para probar la configuración de SSL. Los errores de conexión TLS pueden deberse a un encadenamiento incorrecto de certificados.

Errores de configuración de conectividad al servicio de punto de conexión de VPC

Excepciones: `XksProxyVpcEndpointServiceNotFoundException`, `XksProxyVpcEndpointServiceInvalidConfigurationException`

Además de los problemas de conectividad generales, es posible que se produzcan los siguientes problemas al crear, conectar o actualizar un almacén de claves externo con la conectividad del servicio de punto final de VPC. AWS KMS prueba los valores de las propiedades de un almacén de claves externo con la conectividad del servicio de punto final de VPC al crear, conectar y actualizar el almacén de claves externo. Cuando las operaciones de administración fallan debido a errores de configuración, generan las siguientes excepciones:

```
XksProxyVpcEndpointServiceNotFoundException
```

Esto podría deberse a una de las siguientes causas:

- Un nombre del servicio de punto de conexión de VPC incorrecto. Compruebe que el nombre del servicio de punto de conexión de VPC del almacén de claves externo sea correcto y que coincida con el valor del punto de conexión URI del proxy del almacén de claves externo. Para encontrar el nombre del servicio de punto final de la VPC, utilice la consola de Amazon VPC o la operación. DescribeVpcEndpointServices Para encontrar el nombre del servicio de punto final de la VPC y el extremo URI del proxy de un almacén de claves externo existente, utilice la AWS KMS consola o la DescribeCustomKeyStoresoperación. Para obtener más detalles, consulte Visualización de un almacén de claves externo.
- El servicio de punto final de la VPC puede estar en un almacén de claves Región de AWS diferente al externo. Verifique que el servicio de punto de conexión de VPC y el almacén de claves externo estén en la misma región. (El nombre externo del nombre de la región, por ejemplo, forma parte del nombre del servicio de punto final de la VPC`us-east-1`, como com.amazonaws.vpce.us-east-1. vpce-svc-example.) Para obtener una lista de los requisitos del servicio de punto de conexión de VPC para un almacén de claves externo, consulte Servicio de punto de conexión de VPC. No puede mover un servicio de punto de conexión de VPC ni un almacén de claves externo a otra región. Sin embargo, puede crear un nuevo almacén de claves externo en la misma región que el servicio de punto de conexión de VPC. Para más detalles, consulte Configurar la conectividad del servicio de punto de conexión de VPC y Creación de un almacén de claves externo.
- AWS KMS no es un principal permitido para el servicio de punto final de la VPC. La lista de Entidades principales permitidas para el servicio de punto de conexión de VPC debe incluir el valor `cks.kms.<region>.amazonaws.com`, por ejemplo `cks.kms.eu-west-3.amazonaws.com`. Para obtener instrucciones sobre cómo agregar este valor, consulte Administrar permisos en la Guía de AWS PrivateLink .

XksProxyVpcEndpointServiceInvalidConfigurationException

Este error se produce cuando el servicio de punto de conexión de VPC no cumple uno de los siguientes requisitos:

- La VPC requiere al menos dos subredes privadas, cada una en una zona de disponibilidad diferente. Para agregar una subred a la VPC, consulte Crear una subred en la VPC en la Guía del usuario de Amazon VPC.

- El tipo de servicio de punto de conexión de VPC debe usar un equilibrador de carga de red, no un equilibrador de carga de puerta de enlace.
- No debe exigirse la aceptación del servicio de punto de conexión de VPC (la aceptación obligatoria debe ser falsa). Si se requiere la aceptación manual de cada solicitud de conexión, AWS KMS no podrá utilizar el servicio de punto final de la VPC para conectarse al proxy del almacén de claves externo. Para obtener más información, consulte Aceptar o rechazar solicitudes de conexión en la Guía de AWS PrivateLink .
- El servicio de punto de conexión de VPC debe tener un nombre DNS privado que sea un subdominio de un dominio público. Por ejemplo, si el nombre DNS privado es `https://myproxy-private.xks.example.com`, los dominios `xks.example.com` o `example.com` deben tener un servidor de DNS público. Para ver o cambiar el nombre DNS privado del servicio de punto de conexión de VPC, consulte Administrar nombres DNS de los servicios de punto de conexión de VPC en la Guía de AWS PrivateLink .
- El estado de verificación de dominio del dominio de su nombre DNS privado debe ser `verified`. Para ver y actualizar el estado de verificación del dominio de nombre DNS privado, consulte Verificación del dominio de su nombre DNS privado. Es posible que el estado de verificación actualizado tarde unos minutos en aparecer después de agregar el registro de texto requerido.

  > **Note**
  >
  > Un dominio DNS privado solo se puede verificar si es el subdominio de un dominio público. De lo contrario, el estado de verificación del dominio de DNS privado no cambiará, incluso después de agregar el registro TXT requerido.

- El nombre DNS privado del servicio de punto de conexión de VPC debe coincidir con el valor del punto de conexión URI del proxy para el almacén de claves externo. Para un almacén de claves externo con conectividad al servicio de punto de conexión de VPC, el punto de conexión URI del proxy debe ser `https://` seguido del nombre DNS privado del servicio de punto de conexión de VPC. Para ver el valor del punto de conexión URI del proxy, consulte Visualización de un almacén de claves externo. Para cambiar el valor del punto de conexión URI del proxy, consulte Edición de propiedades del almacén de claves externo.

Errores de conexión del almacén de claves externo

El proceso de conexión de un almacén de claves externo a su proxy de almacén de claves externo tarda unos cinco minutos en completarse. A menos que el error sea rápido, la operación

`ConnectCustomKeyStore` devuelve una respuesta HTTP 200 y un objeto JSON sin propiedades. Sin embargo, esta respuesta inicial no indica que la conexión se haya realizado correctamente. Para determinar si el almacén de claves externo está conectado, consulte su estado de conexión. Si la conexión falla, el estado de conexión del almacén de claves externo cambia `FAILED` y AWS KMS devuelve un código de error de conexión que explica la causa del error.

> **Note**
>
> Si el estado de conexión de un almacén de claves personalizado es `FAILED`, deberá desconectar el almacén de claves personalizado antes de conectarlo de nuevo. No puede conectar un almacén de claves personalizado que tenga el estado de conexión `FAILED`.

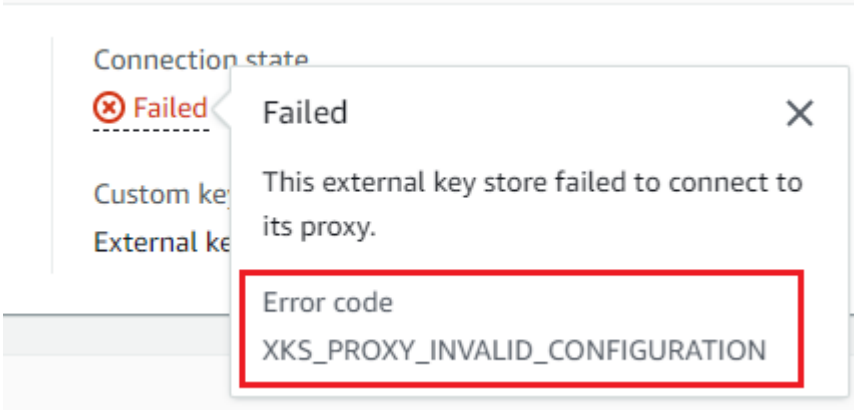
Para ver el estado de conexión de un almacén de claves externo:

- En la DescribeCustomKeyStoresrespuesta, vea el valor del `ConnectionState` elemento.
- En la AWS KMS consola, el estado de la conexión aparece en la tabla del almacén de claves externo. Además, en la página de detalles de cada almacén de claves externo, aparece el estado de conexión en la sección Configuración general.

Cuando el estado de la conexión es `FAILED`, el código de error de conexión ayuda a explicar el error.

Para ver el código de error de conexión:

- En la DescribeCustomKeyStoresrespuesta, vea el valor del `ConnectionErrorCode` elemento. Este elemento aparece en la respuesta `DescribeCustomKeyStores` solo cuando el `ConnectionState` es `FAILED`.
- Para ver el código de error de conexión en la AWS KMS consola, vaya a la página de detalles del almacén de claves externo y coloque el cursor sobre el valor de error.



Códigos de error de conexión para almacenes de claves externos

Los siguientes códigos de error de conexión aplican a los almacenes de claves externos

`INTERNAL_ERROR`

AWS KMS no se pudo completar la solicitud debido a un error interno. Intente realizar de nuevo la solicitud . Para las solicitudes`ConnectCustomKeyStore`, desconecte el almacén de claves personalizado antes de intentar conectarse de nuevo.

`INVALID_CREDENTIALS`

Uno o ambos valores de `XksProxyAuthenticationCredential` no son válidos en el proxy del almacén de claves externo especificado.

`NETWORK_ERRORS`

Los errores de red AWS KMS impiden conectar el almacén de claves personalizado al almacén de claves secundario.

`XKS_PROXY_ACCESS_DENIED`

AWS KMS a las solicitudes se les deniega el acceso al proxy del almacén de claves externo. Si el proxy del almacén de claves externo tiene reglas de autorización, compruebe que permitan a AWS KMS comunicarse con el proxy en su nombre.

`XKS_PROXY_INVALID_CONFIGURATION`

Un error de configuración impide que el almacén de claves externo se conecte a su proxy. Compruebe el valor de `XksProxyUriPath`.

`XKS_PROXY_INVALID_RESPONSE`

AWS KMS no puede interpretar la respuesta del proxy del almacén de claves externo. Si ve este código de error de conexión varias veces, comuníqueselo al proveedor del proxy del almacén de claves externo.

`XKS_PROXY_INVALID_TLS_CONFIGURATION`

AWS KMS no puede conectarse al proxy del almacén de claves externo porque la configuración de TLS no es válida. Compruebe que el proxy del almacén de claves externo sea compatible con TLS 1.2 o 1.3. Además, compruebe que el certificado TLS no esté caducado, que coincida con el nombre de host en el valor `XksProxyUriEndpoint` y que esté firmado por una autoridad de certificación de confianza incluida en la lista de Autoridades de certificación de confianza.

`XKS_PROXY_NOT_REACHABLE`

AWS KMS no puede comunicarse con el proxy del almacén de claves externo. Compruebe que `XksProxyUriEndpoint` y `XksProxyUriPath` sean correctos. Utilice las herramientas de su proxy del almacén de claves externo para comprobar que el proxy esté activo y disponible en su red. Además, compruebe que las instancias del administrador de claves externo funcionen correctamente. Los intentos de conexión fallan con este código de error de conexión si el proxy informa que todas las instancias del administrador de claves externo no están disponibles.

`XKS_PROXY_TIMED_OUT`

AWS KMS puede conectarse al proxy del almacén de claves externo, pero el proxy no responde AWS KMS en el tiempo asignado. Si ve este código de error de conexión varias veces, comuníqueselo al proveedor del proxy del almacén de claves externo.

`XKS_VPC_ENDPOINT_SERVICE_INVALID_CONFIGURATION`

La configuración del servicio de puntos finales de Amazon VPC no cumple con los requisitos de un almacén de claves AWS KMS externo.

- El servicio de punto de conexión de VPC debe ser un servicio de punto de conexión para los puntos de conexión de la interfaz de la Cuenta de AWS de la persona que llama.
- Debe tener un equilibrador de carga de red (NLB) conectado a al menos dos subredes, cada una en una zona de disponibilidad diferente.
- La `Allow principals` lista debe incluir el principal AWS KMS de servicio de la regiónc`ks.kms.<region>.amazonaws.com`, por ejemplo`cks.kms.us-east-1.amazonaws.com`.

- No debe requerir la aceptación de las solicitudes de conexión.
- Debe tener un nombre DNS privado. El nombre DNS privado de un almacén de claves externo con conectividad `VPC_ENDPOINT_SERVICE` debe ser único en su Región de AWS.
- El dominio del nombre DNS privado debe tener un estado de verificación `verified`.
- El certificado TLS especifica el nombre de host DNS privado en el que se puede acceder al punto de conexión.

`XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND`

AWS KMS no encuentra el servicio de punto final de la VPC que utiliza para comunicarse con el proxy del almacén de claves externo. Compruebe que `XksProxyVpcEndpointServiceName` es correcto y que la entidad principal del servicio de AWS KMS tiene permisos de consumidor del servicio en el servicio de punto de conexión de VPC de Amazon.

Errores de latencia y tiempo de espera

Excepciones: `CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operaciones criptográficas), `XksProxyUriUnreachableException` (operaciones de administración)

Códigos de error de conexión: `XKS_PROXY_NOT_REACHABLE`, `XKS_PROXY_TIMED_OUT`

Si no AWS KMS puede contactar con el proxy dentro del intervalo de tiempo de espera de 250 milisegundos, devuelve una excepción. `CreateCustomKeyStorey` `UpdateCustomKeyStore` volver. `XksProxyUriUnreachableException` Las operaciones criptográficas generan la `KMSInvalidStateException` estándar con un mensaje de error que describe el problema. Si `ConnectCustomKeyStore` falla, AWS KMS devuelve un código de error de conexión que describe el problema.

Los errores de tiempo de espera pueden ser problemas transitorios que se pueden resolver volviendo a intentar la solicitud. Si el problema persiste, compruebe que el proxy del almacén de claves externo esté activo y conectado a la red. Además, compruebe que el punto de conexión URI del proxy, la ruta URI del proxy y el nombre del servicio de punto de conexión de VPC (si lo hubiera) sean correctos en el almacén de claves externo. Compruebe también que el administrador de claves externo esté cerca del almacén Región de AWS de claves externo. Si necesita actualizar alguno de estos valores, consulte Edición de propiedades del almacén de claves externo.

Para realizar un seguimiento de los patrones de latencia, utiliza la `XksProxyLatency` CloudWatch métrica y el gráfico de latencia media (basado en esa métrica) de la sección Supervisión de la AWS

KMS consola. El proxy de su almacén de claves externo también puede generar registros y métricas que rastreen la latencia y los tiempos de espera.

`XksProxyUriUnreachableException`
AWS KMS no puede comunicarse con el proxy del almacén de claves externo. Esto puede ser un problema de red transitorio. Si aparece este error varias veces, compruebe que el proxy del almacén de claves externo esté activo y conectado a la red, y que el URI del punto de conexión sea correcto en el almacén de claves externo.

- El proxy del almacén de claves externo no respondió a una solicitud de API de AWS KMS proxy dentro del intervalo de espera de 250 milisegundos. Esto puede indicar un problema de red transitorio o un problema operativo o de rendimiento con el proxy. Si volver a intentarlo no resuelve el problema, notifíquelo al administrador de proxy del almacén de claves externo.

Los errores de latencia y tiempo de espera suelen manifestarse como errores de conexión. Cuando se produce un error en la ConnectCustomKeyStoreoperación, el estado de conexión del almacén de claves externo cambia `FAILED` y AWS KMS devuelve un código de error de conexión que explica el error. Para obtener una lista de los códigos de error de conexión y sugerencias para resolverlos, consulte Códigos de error de conexión para almacenes de claves externos. Las listas de códigos de conexión de Todos los almacenes de claves personalizados y Almacenes de claves externos aplican a los almacenes de claves externos. Los siguientes errores de conexión están relacionados con la latencia y los tiempos de espera.

`XKS_PROXY_NOT_REACHABLE`

-o bien-

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` , `XksProxyUriUnreachableException`
AWS KMS no puede comunicarse con el proxy del almacén de claves externo. Compruebe que el proxy del almacén de claves externo esté activo y conectado a la red y que su ruta URI y su nombre del servicio de VPC o URI de punto de conexión sean correctos en su almacén de claves externo.

Este error puede producirse por las siguientes razones:

- El proxy del almacén de claves externo no está activo o no está conectado a la red.
- Hay un error en los valores del punto de conexión URI del proxy, la ruta URI del proxy o el nombre del servicio de punto de conexión de VPC (si corresponde) en la configuración del almacén de claves externo. Para ver la configuración del almacén de claves externo, utilice la DescribeCustomKeyStoresoperación o consulte la página de detalles del almacén de claves externo en la AWS KMS consola.
- Es posible que haya un error de configuración de red, como un error de puerto, en la ruta de red entre AWS KMS y el proxy del almacén de claves externo. AWS KMS se comunica con el proxy del almacén de claves externo en el puerto 443. Este valor no se puede configurar.
- Cuando el proxy del almacén de claves externo informa (en una GetHealthStatusrespuesta) de que todas las instancias del administrador de claves externo `UNAVAILABLE` lo están, la ConnectCustomKeyStoreoperación falla con un `ConnectionErrorCode` de`XKS_PROXY_NOT_REACHABLE`. Para obtener ayuda, consulte la documentación del administrador de claves externo.
- Este error puede deberse a una gran distancia física entre el administrador de claves externo y el Región de AWS almacén de claves externo. La latencia del ping (tiempo de ida y vuelta de la red (RTT)) entre el administrador de claves externo Región de AWS y el administrador de claves externo no debe ser superior a 35 milisegundos. Puede que tenga que crear un almacén de claves externo en uno Región de AWS que esté más cerca del administrador de claves externo o mover el administrador de claves externo a un centro de datos que esté más cerca del Región de AWS.

`XKS_PROXY_TIMED_OUT`

-o bien-

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` , `XksProxyUriUnreachableException`
AWS KMS rechazó la solicitud porque el proxy del almacén de claves externo no respondió a tiempo. Intente realizar de nuevo la solicitud . Si ve este error varias veces, infórmelo al administr ador de proxy del almacén de claves externo.

Este error puede producirse por las siguientes razones:

- Este error puede deberse a una gran distancia física entre el administrador de claves externo y el proxy del almacén de claves externo. Si es posible, acerque el proxy del almacén de claves externo al administrador de claves externo.
- Los errores de tiempo de espera pueden producirse cuando el proxy no está diseñado para gestionar el volumen y la frecuencia de las solicitudes procedentes AWS KMS de él. Si tus CloudWatch métricas indican un problema persistente, notifícalo al administrador del proxy externo del almacén de claves.
- Se pueden producir errores de tiempo de espera cuando la conexión entre el administrador de claves externo y Amazon VPC para el almacén de claves externo no funciona correctamente. Si lo está utilizando AWS Direct Connect, compruebe que la VPC y el administrador de claves externo se puedan comunicar de forma eficaz. Para obtener ayuda para resolver cualquier problema, consulte Solución de problemas AWS Direct Connect en la Guía del AWS Direct Connect usuario.

`XKS_PROXY_TIMED_OUT`

-o bien-

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` , `XksProxyUriUnreachableException`
El proxy del almacén de claves externo no respondió a la solicitud en el tiempo establecido. Intente realizar de nuevo la solicitud . Si ve este error varias veces, infórmelo al administrador de proxy del almacén de claves externo.

- Este error puede deberse a una gran distancia física entre el administrador de claves externo y el proxy del almacén de claves externo. Si es posible, acerque el proxy del almacén de claves externo al administrador de claves externo.

Errores en las credenciales de autenticación

Excepciones: `CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operaciones criptográficas), `XksProxyIncorrectAuthenticationCredentialException` (operaciones de administración distintas de `CreateKey`)

Debe establecer y mantener una credencial de autenticación para su proxy AWS KMS de almacén de claves externo. A continuación, indica AWS KMS los valores de las credenciales al crear un

almacén de claves externo. Para cambiar la credencial de autenticación, realice el cambio en el proxy del almacén de claves externo. A continuación, actualice la credencial del almacén de claves externo. Si su proxy rota la credencial, debe actualizar la credencial del almacén de claves externo.

Si el proxy del almacén de claves externo no autentica una solicitud firmada con la credencial de autenticación de proxy del almacén de claves externo, el efecto depende de la solicitud:

- `CreateCustomKeyStore` y `UpdateCustomKeyStore` fallan con una `XksProxyIncorrectAuthenticationCredentialException`.
- `ConnectCustomKeyStore` se realiza correctamente, pero se produce un error en la conexión. El estado de la conexión es `FAILED` y el código de error de conexión es `INVALID_CREDENTIALS`. Para obtener más detalles, consulte Errores de conexión del almacén de claves externo.
- Las operaciones criptográficas devuelven `KMSInvalidStateException` para todos los errores de configuración y estado de conexión externos de un almacén de claves externo. El mensaje de error adjunto describe el problema.

> El proxy del almacén de claves externo rechazó la solicitud porque no pudo autenticar AWS KMS. Compruebe las credenciales del almacén de claves externo y actualícelas si es necesario.

Este error puede producirse por las siguientes razones:

- El ID de clave de acceso o la clave de acceso secreta del almacén de claves externo no coincide con los valores establecidos en el proxy del almacén de claves externo.

  Para corregir este error, actualice la credencial de autenticación de proxy del almacén de claves externo. Puede realizar este cambio sin desconectar el almacén de claves externo.
- Un proxy inverso entre AWS KMS y el proxy del almacén de claves externo podría manipular los encabezados HTTP de forma que se invalidaran las firmas de SiGv4. Para corregir este error, notifique al administrador de proxy.

Errores de estados de las claves

Excepciones: `KMSInvalidStateException`

`KMSInvalidStateException` se utiliza para dos propósitos distintos para las claves de KMS en almacenes de claves personalizados.

- Cuando una operación de administración, como `CancelKeyDeletion`, falla y devuelve esta excepción, indica que el estado de la clave de la clave de KMS no es compatible con la operación.
- Cuando se produce un error con `KMSInvalidStateException` en una operación criptográfica en una clave de KMS de un almacén de claves personalizado, puede indicar un problema con el estado de la clave de KMS. Sin embargo, la operación AWS KMS criptográfica se devuelve `KMSInvalidStateException` para todos los errores de configuración externa y de estado de conexión en un almacén de claves externo. Para identificar el problema, utilice el mensaje de error que acompaña a la excepción.

Para encontrar el estado clave necesario para las operaciones de una AWS KMS API, consulteEstados clave de AWS KMS las claves. Para buscar el estado de clave de una clave KMS en la página Customer managed keys (Claves administradas por el cliente) consulte el campo Status (Estado) de la clave KMS. O bien, utilice la DescribeKeyoperación y visualice el `KeyState` elemento en la respuesta. Para obtener más detalles, consulte Consultar claves.

> **Note**
>
> El estado de clave de una clave de KMS en un almacén de claves externo no indica nada sobre el estado de la clave externa asociada. Para obtener información sobre el estado de la clave externa, utilice el administrador de claves externo y las herramientas de proxy del almacén de claves externo.
> `CustomKeyStoreInvalidStateException` se refiere al estado de conexión del almacén de claves externo, no al estado de clave de una clave de KMS.

Una operación criptográfica en una clave KMS de un almacén de claves personalizado puede producir un error porque el estado de la clave KMS es `Unavailable` o `PendingDeletion`. (Las teclas deshabilitadas devuelven `DisabledException`).

- Una clave de KMS tiene un estado de `Disabled` clave solo cuando se deshabilita intencionadamente la clave de KMS en la AWS KMS consola o mediante esta DisableKeyoperación. Mientras una clave de KMS esté deshabilitada, puede consultarla y administrarla, pero no puede usarla en operaciones criptográficas. Para solucionar este problema, habilite la clave. Para obtener más detalles, consulte Habilitación y deshabilitación de claves.
- Una clave de KMS tiene un estado de clave `Unavailable` cuando el almacén de claves externo se desconecta de su proxy del almacén de claves externo. Para arreglar una clave de KMS no disponible, vuelva a conectar el almacén de claves externo. Después de volver a conectar el

almacén de claves externo, el estado de clave de las claves de KMS en el almacén de claves externo se restaura automáticamente al estado anterior, como `Enabled` o `Disabled`.

Una clave de KMS tiene un estado de clave `PendingDeletion` cuando se ha programado su eliminación y se encuentra en su periodo de espera. Un error de estado de clave en una clave de KMS que está pendiente de eliminación indica que la clave no se debe eliminar, ya sea porque se utiliza para el cifrado o porque es necesaria para el descifrado. Para volver a habilitar la clave de KMS, cancele la eliminación programada y, a continuación, habilite la clave. Para obtener más detalles, consulte Programación y cancelación de la eliminación de claves.

Errores de descifrado

Excepciones: `KMSInvalidStateException`

Cuando se produce un error en una operación de descifrado con una clave KMS de un almacén de claves externo, AWS KMS devuelve el estándar `KMSInvalidStateException` que utilizan las operaciones criptográficas para todos los errores de configuración externa y de estado de conexión en un almacén de claves externo. El mensaje de error indica el problema.

Para descifrar un texto cifrado que fue cifrado mediante doble cifrado, el administrador de claves externo utiliza primero la clave externa para descifrar la capa exterior del texto cifrado. A continuación, AWS KMS utiliza el material AWS KMS clave de la clave KMS para descifrar la capa interna del texto cifrado. AWS KMS o un administrador de claves externo puede rechazar un texto cifrado no válido o dañado.

Cuando se produce un error en el descifrado, aparecen los siguientes mensajes de error junto a `KMSInvalidStateException`. Indica un problema con el texto cifrado o el contexto de cifrado opcional de la solicitud.

El proxy del almacén de claves externo rechazó la solicitud porque el texto cifrado especificado o los datos autenticados adicionales están dañados, faltan o no son válidos por algún motivo.

- Cuando el proxy del almacén de claves externo o el administrador de claves externo informan que un texto cifrado o su contexto de cifrado no son válidos, normalmente indica que hay un problema con el texto cifrado o el contexto de cifrado de la solicitud enviada a. `Decrypt` AWS KMS Para `Decrypt` las operaciones, AWS KMS envía al proxy el mismo texto cifrado y el mismo contexto de cifrado que recibe en la solicitud. `Decrypt`

Este error puede deberse a un problema de red durante el transporte, como un bit invertido. Intente realizar de nuevo la solicitud `Decrypt`. Si el problema persiste, compruebe que el texto cifrado no esté alterado ni dañado. Además, compruebe que el contexto de cifrado de la `Decrypt` solicitud AWS KMS coincide con el contexto de cifrado de la solicitud que cifró los datos.

El texto cifrado que el proxy del almacén de claves externo envió para su descifrado, o el contexto de cifrado, está dañado, falta o no es válido por algún motivo.

- Cuando AWS KMS rechaza el texto cifrado que recibió del proxy, indica que el administrador de claves externo o el proxy devolvieron un texto cifrado no válido o dañado. AWS KMS

  Este error puede deberse a un problema de red durante el transporte, como un bit invertido. Intente realizar de nuevo la solicitud `Decrypt`. Si el problema persiste, compruebe que el administrador de claves externo funciona correctamente y que el proxy del almacén de claves externo no altera el texto cifrado que recibe del administrador de claves externo antes de devolverlo a. AWS KMS

Errores de clave externa

Una clave externa es una clave criptográfica del administrador de claves externo que sirve como material de clave externa para una clave de KMS. AWS KMS no puede acceder directamente a la clave externa. Debe solicitar al administrador de claves externo (a través del proxy del almacén de claves externo) que utilice la clave externa para cifrar datos o descifrar un texto cifrado.

Especifica el ID de clave externa en su administrador de claves externo cuando crea una clave de KMS en su almacén de claves externo. No se puede cambiar el ID de clave externa después de crear la clave de KMS. Para evitar problemas con la clave de KMS, la operación `CreateKey` solicita al proxy del almacén de claves externo que verifique el ID y la configuración de la clave externa. Si la clave externa no cumple los requisitos para su uso con una clave de KMS, se produce un error en la operación `CreateKey` y aparece un mensaje de excepción y error que identifica el problema.

Sin embargo, pueden producirse problemas después de que se crea la clave de KMS. Si una operación criptográfica falla debido a un problema con la clave externa, se produce un error y se genera una `KMSInvalidStateException` con un mensaje de error que indica el problema.

CreateKey errores en la clave externa

Excepciones: `XksKeyAlreadyInUseException`, `XksKeyNotFoundException`, `XksKeyInvalidConfigurationException`

La CreateKeyoperación intenta comprobar el identificador y las propiedades de la clave externa que se proporciona en el parámetro ID de clave externa (consola) o `XksKeyId` (API). Esta práctica está diseñada para detectar errores de forma temprana antes de intentar utilizar la clave externa con la clave de KMS.

Clave externa en uso

Cada clave de KMS de un almacén de claves externo debe usar una clave externa diferente. Cuando `CreateKey` reconoce que el identificador de clave externa (XksKeyId) de una clave de KMS no es único en el almacén de claves externo, se produce un error con un`XksKeyAlreadyInUseException`.

Si utiliza varios ID para la misma clave externa, `CreateKey` no reconocerá el duplicado. Sin embargo, las claves de KMS con la misma clave externa no son interoperables porque tienen diferentes metadatos y materiales de AWS KMS claves.

No se encontró la clave externa

Cuando el proxy del almacén de claves externo informa que no puede encontrar la clave externa utilizando el identificador de clave externa (XksKeyId) de la clave KMS, la `CreateKey` operación falla y vuelve `XksKeyNotFoundException` con el siguiente mensaje de error.

> El proxy del almacén de claves externo rechazó la solicitud porque no pudo encontrar la clave externa.

Este error puede producirse por las siguientes razones:

- Es posible que el ID de la clave externa (`XksKeyId`) de la clave de KMS no sea válido. Para encontrar el ID que su proxy de clave externa utiliza para identificar la clave externa, consulte la documentación sobre el proxy del almacén de claves externo o el administrador de claves externo.
- Puede que se haya eliminado la clave externa de su administrador de claves externo. Para investigar, utilice sus herramientas de administrador de claves externo. Si la clave externa se elimina permanentemente, utilice una clave externa diferente con la clave de KMS. Para obtener

una lista de los requisitos de la clave externa, consulte Requisitos para una clave de KMS en un almacén de claves externo.

No se cumplen los requisitos de clave externa

Cuando el proxy del almacén de claves externo informa que la clave externa no cumple con los requisitos para su uso con una clave KMS, la operación `CreateKey` falla y genera una `XksKeyInvalidConfigurationException` con uno de los siguientes mensajes de error.

La especificación de clave de la clave externa debe ser AES_256. La especificación de clave de la clave externa especificada es *<key-spec>* .

- La clave externa debe ser una clave de cifrado simétrica de 256 bits con una especificación de clave de AES_256. Si la clave externa especificada es de otro tipo, especifique el ID de una clave externa que cumpla este requisito.

El estado de la clave externa debe ser ENABLED (HABILITADA). El estado de la clave externa especificada es *<status>*.

- La clave externa debe estar habilitada en el administrador de claves externo. Si la clave externa especificada no está habilitada, utilice las herramientas del administrador de claves externo para habilitarla o especifique una clave externa habilitada.

El uso de clave de la clave externa debe incluir ENCRYPT (CIFRAR) y DECRYPT (DESCIFRAR). El uso de clave de la clave externa especificada es <*key-usage* >.

- La clave externa debe configurarse para el cifrado y el descifrado en el administrador de claves externo. Si la clave externa especificada no incluye estas operaciones, utilice las herramientas del administrador de claves externo para cambiar las operaciones o especifique una clave externa diferente.

Errores de operación criptográfica para la clave externa

Excepciones: `KMSInvalidStateException`

Cuando el proxy del almacén de claves externo no puede encontrar la clave externa asociada a la clave de KMS o la clave externa no cumple los requisitos para su uso con una clave de KMS, se produce un error en la operación criptográfica.

Los problemas de clave externa que se detectan durante una operación criptográfica son más difíciles de resolver que los problemas de clave externa detectados antes de crear la clave de KMS. No se puede cambiar el ID de clave externa después de crear la clave de KMS. Si la clave de KMS aún no ha cifrado ningún dato, puede eliminarla y crear una nueva con un ID de clave externa diferente. Sin embargo, el texto cifrado generado con la clave KMS no se puede descifrar con ninguna otra clave KMS, ni siquiera con la misma clave externa, ya que las claves tendrán metadatos y materiales clave diferentes AWS KMS . En su lugar, en la medida de lo posible, utilice las herramientas de administración de claves externas para resolver el problema con la clave externa.

Cuando el proxy del almacén de claves externo informa un problema con la clave externa, las operaciones criptográficas devuelven una `KMSInvalidStateException` con un mensaje de error que identifica el problema.

No se encontró la clave externa

Cuando el proxy del almacén de claves externo informa que no puede encontrar la clave externa utilizando el identificador de clave externa (XksKeyId) de la clave KMS, las operaciones criptográficas devuelven un mensaje de error `KMSInvalidStateException` con el siguiente mensaje de error.

> El proxy del almacén de claves externo rechazó la solicitud porque no pudo encontrar la clave externa.

Este error puede producirse por las siguientes razones:

- El ID de la clave externa (`XksKeyId`) de la clave de KMS ya no es válido.

  Para encontrar el ID de clave externa asociado a su clave de KMS, consulte los detalles de la clave de KMS. Para encontrar el ID que su proxy de clave externa utiliza para identificar la clave externa, consulte la documentación sobre el proxy del almacén de claves externo o el administrador de claves externo.

AWS KMS verifica el ID de clave externa cuando crea una clave KMS en un almacén de claves externo. Sin embargo, el ID puede dejar de ser válido, especialmente si el valor del ID de clave externa es un alias o un nombre mutable. No puede cambiar el ID de clave externa asociado a una clave de KMS existente. Para descifrar cualquier texto cifrado con la clave de KMS, debe volver a asociar la clave externa con el ID de clave externa existente.

Si aún no ha utilizado la clave de KMS para cifrar datos, puede crear una nueva clave de KMS con un ID de clave externa válido. Sin embargo, si ha generado texto cifrado con la clave de KMS, no puede usar ninguna otra clave de KMS para descifrar el texto cifrado, incluso si usa la misma clave externa.

- Puede que se haya eliminado la clave externa de su administrador de claves externo. Para investigar, utilice sus herramientas de administrador de claves externo. Si es posible, intente recuperar el material de clave de una copia o respaldo de su administrador de claves externo. Si la clave externa se elimina de forma permanente, cualquier texto cifrado con la clave de KMS asociada será irrecuperable.

Errores de configuración de claves externas

Cuando el proxy del almacén de claves externo informa que la clave externa no cumple con los requisitos para su uso con una clave KMS, la operación criptográfica genera una `KMSInvalidStateException` con uno de los siguientes mensajes de error.

El proxy del almacén de claves externo rechazó la solicitud porque la clave externa no admite la operación solicitada.

- La clave externa debe admitir tanto el cifrado como el descifrado. Si el uso de la clave no incluye el cifrado y el descifrado, utilice las herramientas de administración de claves externas para cambiar el uso de la clave.

El proxy del almacén de claves externo rechazó la solicitud porque la clave externa no está habilitada en el administrador de claves externo.

- La clave externa debe estar habilitada y disponible para su uso en el administrador de claves externo. Si el estado de la clave externa no es `Enabled`, utilice las herramientas del administrador de claves externo para habilitarla.

Problemas con el proxy

Excepciones:

`CustomKeyStoreInvalidStateException` (`CreateKey`), `KMSInvalidStateException` (operaciones criptográficas), `UnsupportedOperationException`, `XksProxyUriUnreachableException`, `XksProxyInvalidResponseException` (operaciones de administración distintas de `CreateKey`)

El proxy del almacén de claves externo interviene en todas las comunicaciones entre AWS KMS y el administrador de claves externo. Traduce AWS KMS las solicitudes genéricas a un formato que su administrador de claves externo pueda entender. Si el proxy del almacén de claves externo no cumple con la especificación de la API de proxy del almacén de claves AWS KMS externo, o si no funciona correctamente o no se puede comunicar con él AWS KMS, no podrá crear ni usar claves de KMS en su almacén de claves externo.

Si bien muchos errores mencionan el proxy del almacén de claves externo debido a su papel fundamental en la arquitectura del almacén de claves externo, esos problemas pueden originarse en el administrador de claves externo o en la clave externa.

Los problemas de esta sección se refieren a problemas con el diseño o el funcionamiento del proxy del almacén de claves externo. La resolución de estos problemas puede requerir un cambio en el software de proxy. Consulte a su administrador de proxy. Para ayudar a diagnosticar problemas con el proxy, AWS KMS proporciona XKS Proxy Text Client, un cliente de prueba de código abierto que comprueba que el proxy del almacén de claves externo cumple con la Especificación de la API de proxy del almacén de claves externo de AWS KMS.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` o `XksProxyUriUnreachableException`
El proxy del almacén de claves externo se encuentra en mal estado. Si ve este mensaje varias veces, notifíquelo al administrador de proxy del almacén de claves externo.

- Este error puede indicar un problema operativo o un error de software en el proxy del almacén de claves externo. Puedes encontrar las entradas de CloudTrail registro de la operación de AWS

KMS API que generó cada error. Este error puede resolverse si vuelve a intentar la operación. Sin embargo, si persiste, notifíquelo al administrador de proxy del almacén de claves externo.

- Cuando el proxy del almacén de claves externo informa (en una GetHealthStatusrespuesta) de que todas las instancias del administrador de claves externo lo estánUNAVAILABLE, los intentos de crear o actualizar un almacén de claves externo fallan, con esta excepción. Si el error persiste, consulte la documentación del administrador de claves externo.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` o `XksProxyInvalidResponseException`

AWS KMS no puede interpretar la respuesta del proxy del almacén de claves externo. Si ve este error varias veces, consulte con el administrador de proxy del almacén de claves externo.

- AWS KMS las operaciones generan esta excepción cuando el proxy devuelve una respuesta indefinida que AWS KMS no se puede analizar ni interpretar. Este error puede producirse ocasionalmente debido a problemas externos temporales o a errores de red esporádicos. Sin embargo, si persiste, podría indicar que el proxy del almacén de claves externo no cumple con la Especificación de la API de proxy del almacén de claves externo de AWS KMS. Notifique a su proveedor o administrador del almacén de claves externo.

`CustomKeyStoreInvalidStateException` , `KMSInvalidStateException` o `UnsupportedOperationException`

El proxy del almacén de claves externo rechazó la solicitud porque no admite la operación criptográfica solicitada.

- El proxy del almacén de claves externo debe admitir todas las API de proxy definidas en la Especificación de la API de proxy del almacén de claves externo de AWS KMS. Este error indica que el proxy no admite la operación relacionada con la solicitud. Notifique a su proveedor o administrador del almacén de claves externo.

Problemas de autorización de proxy

Excepciones: `CustomKeyStoreInvalidStateException`, `KMSInvalidStateException`

Algunos proxy del almacén de claves externo implementan requisitos de autorización para el uso de sus claves externas. Se permite, pero no es obligatorio, utilizar un proxy de almacén de claves externo para diseñar e implementar un esquema de autorización que permita a determinados usuarios solicitar ciertas operaciones en determinadas condiciones. Por ejemplo, un proxy puede permitir al usuario cifrar con una clave externa determinada, pero no descifrar con ella. Para obtener más información, consulte Autorización del proxy del almacén de claves externo (opcional).

La autorización del proxy se basa en los metadatos que AWS KMS incluye en sus solicitudes al proxy. Los campos `awsSourceVpc` y `awsSourceVpce` se incluyen en los metadatos solo cuando la solicitud proviene de un punto de conexión de VPC y solo cuando la persona que llama está en la misma cuenta que la clave de KMS.

```
"requestMetadata": {
    "awsPrincipalArn": string,
    "awsSourceVpc": string, // optional
    "awsSourceVpce": string, // optional
    "kmsKeyArn": string,
    "kmsOperation": string,
    "kmsRequestId": string,
    "kmsViaService": string // optional
}
```

Cuando el proxy rechaza una solicitud debido a una falla de autorización, se produce un error en la operación de AWS KMS relacionada. `CreateKey` genera un `CustomKeyStoreInvalidStateException`. Las operaciones criptográficas de AWS KMS generan una `KMSInvalidStateException`. Ambos utilizan el siguiente mensaje de error:

> El proxy del almacén de claves externo denegó el acceso a la operación. Compruebe que el usuario y la clave externa estén autorizados para esta operación e intente realizar la solicitud de nuevo.

- Para resolver el error, utilice el administrador de claves externo o las herramientas de proxy del almacén de claves externo para determinar por qué falló la autorización. A continuación, actualice el procedimiento que provocó la solicitud no autorizada o utilice las herramientas de proxy del almacén de claves externo para actualizar la política de autorización. No puede resolver este error en AWS KMS.

Referencia de tipos de claves

AWS KMS admite diferentes funciones para claves KMS de diferentes tipos. Por ejemplo, solo puede utilizar las claves KMS de cifrado simétricas para generar claves de datos simétricas y pares de claves de datos asimétricas. Además, la importación del material de claves y la rotación automática de claves son compatibles únicamente con las claves KMS de cifrado simétricas. Asimismo, solo puede crear claves KMS de cifrado simétricas en un almacén de claves personalizadas.

Esta referencia incluye dos tablas.

- La Tabla de tipos de claves muestra las operaciones de AWS KMS que son válidas para las claves de KMS de cifrado simétricas, las claves de KMS asimétricas y las claves de KMS HMAC.
- La tabla de características especiales muestra las operaciones de AWS KMS que son válidas para las claves de KMS para varias regiones, las claves de KMS con material de claves importado y las claves de KMS de almacenes de claves personalizados.

Tabla de tipos de claves

Es posible que tenga que desplazarse horizontal o verticalmente para ver todos los datos de esta tabla.

AWS KMS Operación de la API	Claves KMS de cifrado simétricas	Claves KMS HMAC	Claves de KMS asimétricas (ENCRYPT_DECRYPT)	Claves de KMS asimétricas (SIGN_VERIFY)
CancelKeyDeletion	✓	✓	✓	✓
CreateAlias	✓	✓	✓	✓
CreateGrant	✓	✓	✓	✓
CreateKey	✓	✓	✓	✓

AWS KMS Operación de la API	Claves KMS de cifrado simétricas	Claves KMS HMAC	Claves de KMS asimétricas (ENCRYPT_DECRYPT)	Claves de KMS asimétricas (SIGN_VERIFY)
Decrypt	✓	⊗	✓	⊗
DeleteAlias	✓	✓	✓	✓
DeleteImportedKeyMaterial Válido solo en las claves de KMS con material de claves importado (`Origin` es `EXTERNAL`).	✓	✓	✓	✓
DescribeKey	✓	✓	✓	✓
DisableKey	✓	✓	✓	✓
DisableKeyRotation	✓ Válido solo en claves de KMS con material de claves de AWS KMS (`Origin` es `AWS_KMS`).	⊗	⊗	⊗

AWS KMS Operación de la API	Claves KMS de cifrado simétricas	Claves KMS HMAC	Claves de KMS asimétricas (ENCRYPT_DECRYPT)	Claves de KMS asimétricas (SIGN_VERIFY)
EnableKey	✓	✓	✓	✓
EnableKeyRotation	✓ Válido solo en claves de KMS con material de claves de AWS KMS (`Origin` es `AWS_KMS`).	⊗	⊗	⊗
Encrypt	✓	⊗	✓	⊗
GenerateDataKey	✓	⊗	⊗	⊗
GenerateDataKeyPair Genera un par de claves de datos asimétricos protegido por una clave de KMS de cifrado simétrica.	✓ No es válido en claves de KMS en almacenes de claves personalizados.	⊗	⊗	⊗

AWS KMS Operación de la API	Claves KMS de cifrado simétricas	Claves KMS HMAC	Claves de KMS asimétricas (ENCRYPT_DECRYPT)	Claves de KMS asimétricas (SIGN_VERIFY)
GenerateDataKeyPairWithoutPlaintext Genera un par de claves de datos asimétricos protegido por una clave de KMS de cifrado simétrica.	✓ No es válido en claves de KMS en almacenes de claves personalizados.	⊗	⊗	⊗
GenerateDataKeyWithoutPlaintext	✓	⊗	⊗	⊗
GenerateMac	⊗	✓	⊗	⊗
GetKeyPolicy	✓	✓	✓	✓
GetKeyRotationStatus	✓	✓ (`KeyRotationEnabled` siempre será `false`.)	✓ (`KeyRotationEnabled` siempre será `false`.)	✓ (`KeyRotationEnabled` siempre será `false`.)

AWS KMS Operación de la API	Claves KMS de cifrado simétricas	Claves KMS HMAC	Claves de KMS asimétricas (ENCRYPT_DECRYPT)	Claves de KMS asimétricas (SIGN_VERIFY)
GetParametersForImport Válido solo en las claves de KMS con material de claves importado (`Origin` es `EXTERNAL`).	✓	✓	✓	✓
GetPublicKey	⊗	⊗	✓	✓
ImportKeyMaterial Válido solo en las claves de KMS con material de claves importado (`Origin` es `EXTERNAL`).	✓	✓	✓	✓
ListAliases	✓	✓	✓	✓
ListGrants	✓	✓	✓	✓
ListKeyPolicies	✓	✓	✓	✓
ListResourceTags	✓	✓	✓	✓
ListRetirableGrants	✓	✓	✓	✓
PutKeyPolicy	✓	✓	✓	✓
ReEncrypt	✓	⊗	✓	⊗

AWS KMS Operación de la API	Claves KMS de cifrado simétricas	Claves KMS HMAC	Claves de KMS asimétricas (ENCRYPT_DECRYPT)	Claves de KMS asimétricas (SIGN_VERIFY)
ReplicateKey - Válido solo en claves de varias regiones	✓	✓	✓	✓
RetireGrant	✓	✓	✓	✓
RevokeGrant	✓	✓	✓	✓
ScheduleKeyDeletion	✓	✓	✓	✓
Sign	⊗	⊗	⊗	✓
TagResource	✓	✓	✓	✓
UntagResource	✓	✓	✓	✓
UpdateAlias La clave de KMS actual y la nueva clave de KMS deben ser del mismo tipo (ambas simétricas o ambas asimétricas o ambas HMAC) y deben tener el mismo uso de clave.	✓	✓	✓	✓
UpdateKeyDescription	✓	✓	✓	✓

AWS KMS Operación de la API	Claves KMS de cifrado simétricas	Claves KMS HMAC	Claves de KMS asimétricas (ENCRYPT_DECRYPT)	Claves de KMS asimétricas (SIGN_VERIFY)
UpdateReplicaRegion - Válido solo en claves de varias regiones	✓	✓	✓	✓
Verificar	⊗	⊗	⊗	✓
VerifyMac	⊗	✓	⊗	⊗

Tabla de características especiales

En esta tabla, se muestran las operaciones de la API de AWS KMS que se admiten en cada tipo de clave de uso especial.

Al leer esta tabla, debe tener en cuenta las siguientes interacciones:

- Claves de varias regiones:
  - Las claves de varias regiones pueden ser claves de KMS de cifrado simétrico, claves de KMS asimétricas, claves de KMS HMAC y claves de KMS con material de claves importado.
  - No puede crear claves de varias regiones en un almacén de claves personalizado.
- Material de claves importado
  - Puede importar material de claves de KMS de cifrado simétrico, claves de KMS asimétricas y claves HMAC de KMS.
  - Puede crear claves de varias regiones con material de claves importado.
  - No puede crear claves con material de claves importado en un almacén de claves personalizado.
  - La rotación automática de claves `EnableKeyRotation`, `DisableKeyRotation`) no es compatible con las claves KMS con el material de claves importado.
- Almacenes de claves personalizados

- Los almacenes de claves personalizados solo admiten claves KMS de cifrado simétricas.
- Las operaciones simétricas en pares de claves asimétricas (`GenerateDataKeyPair`, `GenerateDataKeyPairWithoutPlaintext`) no se admiten en las claves de KMS de los almacenes de claves personalizados.
- Las claves KMS de almacenes de claves personalizados no admiten la rotación automática de claves (`EnableKeyRotation`, `DisableKeyRotation`).
- No puede crear claves de varias regiones en almacenes de claves personalizados.

Es posible que tenga que desplazarse horizontal o verticalmente para ver todos los datos de esta tabla.

AWS KMS Operación de la API	Claves de varias regiones	Material de claves importado	Las claves KMS en un almacén de claves personalizado
CancelKeyDeletion	✓	✓	✓
CreateAlias	✓	✓	✓
CreateGrant	✓	✓	✓
CreateKey Puede utilizar `CreateKey` para crear una clave principal de varias regiones, una clave de KMS con material de claves importado o una clave de KMS en un almacén de claves personalizado. Para crear una clave de réplica de varias regiones, utilice `ReplicateKey` .	✓	✓	✓
Decrypt	✓	✓	✓

AWS KMS Operación de la API	Claves de varias regiones	Material de claves importado	Las claves KMS en un almacén de claves personalizado
	Válido solo cuando `KeyUsage` es `ENCRYPT_DECRYPT`		
DeleteAlias	✓	✓	✓
DeleteImportedKeyMaterial	✓ Válido solo para claves con material de claves importado (`Origin` es `EXTERNAL`)	✓	⊗
DescribeKey	✓	✓	✓
DisableKey	✓	✓	✓
DisableKeyRotation	✓ Válido solo en claves de cifrado simétricas con material de claves de AWS KMS (`Origin` es `AWS_KMS`).	⊗	⊗

AWS KMS Operación de la API	Claves de varias regiones	Material de claves importado	Las claves KMS en un almacén de claves personalizado
EnableKey	✓ Válido solo con claves de cifrado de KMS simétricas	✓	✓
EnableKeyRotation	✓ Válido solo en claves de cifrado simétricas con material de claves de AWS KMS (`Origin` es `AWS_KMS`).	⊗	⊗
Encrypt	✓ Válido solo cuando `KeyUsage` es `ENCRYPT_DECRYPT`	✓	✓

AWS KMS Operación de la API	Claves de varias regiones	Material de claves importado	Las claves KMS en un almacén de claves personalizado
GenerateDataKey	✓ Válido solo con claves de cifrado de KMS simétricas	✓	✓
GenerateDataKeyPair	✓ Válido solo con claves de cifrado de KMS simétricas	✓	⊗
GenerateDataKeyPairWithoutPlaintext	✓ Válido solo con claves de cifrado de KMS simétricas	✓	⊗
GenerateDataKeyWithoutPlaintext	✓ Válido solo con claves de cifrado de KMS simétricas	✓	✓
GenerateMac Válido solo en claves HMAC de KMS	✓	✓	⊗

AWS KMS Operación de la API	Claves de varias regiones	Material de claves importado	Las claves KMS en un almacén de claves personalizado
GetKeyPolicy	✓	✓	✓
GetKeyRotationStatus	✓	✓ (`KeyRotationEnabled` siempre será `false`.)	⊗
GetParametersForImport	✓ Válido solo para claves con material de claves importado (`Origin` es `EXTERNAL`).	✓	⊗
GetPublicKey Válido solo para claves de KMS asimétricas.	✓	✓	⊗

AWS KMS Operación de la API	Claves de varias regiones	Material de claves importado	Las claves KMS en un almacén de claves personalizado
ImportKeyMaterial	✓ Válido solo para claves con material de claves importado (`Origin` es `EXTERNAL`).	✓	⊗
ListAliases	✓	✓	✓
ListGrants	✓	✓	✓
ListKeyPolicies	✓	✓	✓
ListResourceTags	✓	✓	✓
ListRetirableGrants	✓	✓	✓
PutKeyPolicy	✓	✓	✓
ReEncrypt	✓ Válido solo cuando `KeyUsage` es `ENCRYPT_DECRYPT`	✓	✓

AWS KMS Operación de la API	Claves de varias regiones	Material de claves importado	Las claves KMS en un almacén de claves personalizado
ReplicateKey	✓ Válido solo en claves principales de varias regiones.	✓ Válido solo en claves principales de varias regiones.	⊗
RetireGrant	✓	✓	✓
RevokeGrant	✓	✓	✓
ScheduleKeyDeletion	✓	✓	✓
Sign Válido solo cuando `KeyUsage` es `SIGN_VERIFY` .	✓	✓	⊗
TagResource	✓	✓	✓
UntagResource	✓	✓	✓
UpdateAlias La clave de KMS actual y la nueva clave de KMS deben ser del mismo tipo (ambas simétricas o ambas asimétricas o ambas HMAC) y deben tener el mismo uso de clave.	✓	✓	✓

AWS KMS Operación de la API	Claves de varias regiones	Material de claves importado	Las claves KMS en un almacén de claves personalizado
UpdateKeyDescription	✓	✓	✓
UpdateReplicaRegion	✓	✓ Válido solo en claves de varias regiones.	⊗
Verificar Solo es válido cuando `KeyUsage` es `SIGN_VERIFY` .	✓	✓	⊗
VerifyMac Válido solo en claves HMAC de KMS	✓	✓	⊗

Seguridad de AWS Key Management Service

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos que están diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS . Para obtener información acerca de los programas de conformidad que se aplican a AWS Key Management Service (AWS KMS), consulte los Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. En AWS KMS, además de la configuración y el uso de AWS KMS keys, usted es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación lo ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Key Management Service. Le mostrará cómo configurar AWS KMS para satisfacer sus objetivos de seguridad y conformidad.

Temas

Protección de los datos en AWS Key Management Service

AWS Key Management Service almacena y protege sus claves de cifrado para que estén altamente disponibles al mismo tiempo que le proporciona un control de acceso sólido y flexible.

Temas

Rotación del material de claves

De forma predeterminada, AWS KMS genera y protege el material de claves criptográficas para las claves de KMS. Además, AWS KMS ofrece opciones para el material de claves que se crea y protege fuera de AWS KMS. Para obtener más detalles sobre las claves de KMS y el material de claves, consulte AWS Key Management Service Cryptographic Details.

Protección del material de claves generado en AWS KMS

Al crear una clave de KMS, AWS KMS genera y protege de forma predeterminada el material criptográfico de la clave de KMS.

Para proteger el material de claves de las claves de KMS, AWS KMS confía en una flota distribuida de módulos de seguridad de hardware (HSM) validados por FIPS 140-2 Nivel 3. Cada HSM de AWS KMS es un dispositivo de hardware independiente especialmente diseñado para proporcionar funciones criptográficas dedicadas a fin de cumplir con los requisitos de seguridad y escalabilidad de AWS KMS. (Los HSM que AWS KMS utiliza en las regiones de China cuentan con la certificación de OSCCA y cumplen con todas las normas chinas pertinentes, pero no están validados de acuerdo con el Programa de validación de módulos criptográficos de FIPS 140-2).

El material de claves de una clave de KMS se cifra de forma predeterminada cuando se genera en el HSM. El material de claves se descifra solo en la memoria volátil del HSM y solo durante los pocos milisegundos que se necesitan para usarlo en una operación criptográfica. Siempre que el material de claves no esté en uso activo, se cifra dentro del HSM y se transfiere a un almacenamiento persistente de alta durabilidad (99,999999999 %) y baja latencia, donde permanece separado y aislado de los HSM. El material de claves de texto sin formato nunca sale de los límites de seguridad del HSM; nunca se escribe en un disco ni permanece en ningún medio de almacenamiento. (La única excepción es la clave pública de un par de claves asimétricas, que no es secreta).

AWS afirma como un principio de seguridad fundamental que no hay interacción humana con el material criptográfico de claves de texto sin formato de ningún tipo en ningún Servicio de AWS. No existe ningún mecanismo que permita a nadie, incluidos los operadores del Servicio de AWS, ver, acceder o exportar el material de claves en texto sin formato. Este principio se aplica incluso durante fallos catastróficos y eventos de recuperación de desastres. El material de claves de cliente en texto sin formato en AWS KMS se utiliza para operaciones criptográficas en los HSM validados por FIPS de AWS KMS únicamente en respuesta a las solicitudes autorizadas que el cliente o su delegado hagan al servicio.

En el caso de las claves administradas por el cliente, la Cuenta de AWS que crea la clave es la propietaria única e intransferible de la clave. La cuenta propietaria tiene el control total y exclusivo sobre las políticas de autorización que controlan el acceso a la clave. En el caso de las Claves administradas por AWS, Cuenta de AWS tiene el control total sobre las políticas de IAM que autorizan las solicitudes al Servicio de AWS.

Protección del material de claves generado fuera de AWS KMS

AWS KMS proporciona alternativas al material de claves generado en AWS KMS.

Almacenes de claves personalizados, una característica de AWS KMS opcional, le permite crear claves de KMS respaldadas por el material de claves generado y utilizado fuera de AWS KMS. Las claves de KMS de los almacenes de claves de AWS CloudHSM están respaldadas por las claves de los módulos de seguridad de hardware (AWS CloudHSM) que controla. Estos HSM están certificados por FIPS 140-2 Nivel 3. Las claves de KMS de los almacenes de claves externos están respaldadas por claves de un administrador de claves externo que el usuario controla y administra desde fuera de AWS, como un HSM físico en su centro de datos privado.

Otra característica opcional le permite importar el material de claves para obtener una clave KMS Para proteger el material de claves importado mientras está en tránsito en AWS KMS, tiene que cifrar el material de claves con una clave pública de un par de claves RSA generado en un HSM de AWS KMS. El material de claves importado se descifra en un HSM de AWS KMS y se vuelve a cifrar en una clave simétrica en el HSM. Como todo material de claves de AWS KMS, el material de claves importado de texto sin formato nunca sale de los HSM sin cifrar. Sin embargo, el cliente que proporcionó el material de claves es responsable del uso seguro, la durabilidad y el mantenimiento del material de claves fuera de AWS KMS.

Cifrado de datos

Los datos en AWS KMS constan de AWS KMS keys y el material de claves de cifrado que representan. Este material de claves solo existe en texto sin formato dentro de los módulos de seguridad de hardware (HSM) de AWS KMS y solo cuando estén en uso. De lo contrario, el material de la clave se cifra y se almacena en almacenamiento persistente duradero.

El material de claves que AWS KMS genera para claves KMS nunca sale del límite de los HSM de AWS KMS sin cifrar. No se exporta ni transmite en ninguna operación de la API de AWS KMS. La excepción es para Claves multirregión, donde AWS KMS utiliza un mecanismo de replicación entre regiones para copiar el material de clave de una clave multirregión desde un HSM en una Región de AWS a un HSM en una Región de AWS diferente. Para obtener más información, consulte Proceso de replicación de claves multirregión en Detalles criptográficos de AWS Key Management Service.

Temas

Cifrado en reposo

AWS KMS genera material de claves para AWS KMS keys en los módulos de seguridad de hardware (HSM) que cumplen con FIPS 140-2 Nivel 3. La única excepción son las regiones de China, donde los HSM que AWS KMS utiliza para generar las claves KMS cumplen con todas las normas chinas pertinentes, pero no están validados de acuerdo con el Programa de validación de módulos criptográficos de FIPS 140-2. Cuando no se utiliza, el material de claves se cifra mediante una clave de HSM y se escribe en un almacenamiento duradero y persistente. El material de las claves KMS y las claves de cifrado que protegen el material de claves nunca dejan los HSM en forma de texto sin formato.

El cifrado y la administración del material de claves para las claves KMS está completamente a cargo de AWS KMS.

Para obtener más información, consulte Uso de AWS KMS keys en Detalles criptográficos AWS Key Management Service

Cifrado en tránsito

El material de claves que AWS KMS genera para claves KMS nunca se exporta ni transmite en operaciones de la API de AWS KMS. AWS KMS utiliza identificadores clave para representar las

claves KMS en las operaciones de API. Del mismo modo, el material de las claves KMS en los almacenes de claves personalizados de AWS KMS no es exportable y nunca se transmite en operaciones de la API AWS KMS o AWS CloudHSM.

Sin embargo, algunas operaciones de la API de AWS KMS devuelven claves de datos. Además, los clientes pueden usar las operaciones de la API para importar material de claves para las claves KMS seleccionadas.

Todas las llamadas a la API de AWS KMS deben firmarse y transmitirse mediante el protocolo de seguridad de la capa de transporte (TLS). AWS KMS requiere TLS 1.2 y recomienda TLS 1.3 en todas las regiones. AWS KMS también es compatible con la TLS poscuántica híbrida para los puntos de conexión del servicio AWS KMS en todas las regiones, excepto en las regiones de China. AWS KMS no admite la TLS poscuántica híbrida para los puntos de conexión FIPS en AWS GovCloud (US). Las llamadas a AWS KMS también requieren un paquete de cifrado moderno que admita secreto perfecto en el futuro, lo que significa que el compromiso de cualquier secreto, como una clave privada, no comprometa también la clave de sesión.

Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utilice un punto de conexión de FIPS. Para utilizar los puntos de conexión estándar de AWS KMS o los puntos de conexión FIPS de AWS KMS, los clientes deben admitir TLS 1.2 o una versión posterior. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2. Para obtener una lista de los puntos de conexión FIPS de AWS KMS, consulte AWS Key Management Service endpoints and quotas en la Referencia general de AWS.

Las comunicaciones entre anfitriones de servicios de AWS KMS y los HSM están protegidos mediante la criptografía de curva elíptica (ECC) y el estándar de cifrado avanzado (AES) en un esquema de cifrado autenticado. Para obtener más detalles, consulte Seguridad de la comunicación interna en Detalles criptográficos de AWS Key Management Service

Privacidad del tráfico entre redes

AWS KMS admite una AWS Management Console y un conjunto de operaciones de API que le permiten crear y administrar AWS KMS keys y usarlos en operaciones criptográficas.

AWS KMS admite dos opciones de conectividad de red desde su red privada a AWS.

- Una conexión de una conexión de VPN IPSec a través de Internet
- AWS Direct Connect vincula su red interna con una ubicación de AWS Direct Connect a través de cable estándar Ethernet de fibra óptica.

Todas las llamadas de la API de AWS KMS deben firmarse y transmitirse mediante seguridad de la capa de transporte (TLS). Las llamadas también requieren un paquete de cifrado moderno que admita el secreto perfecto en el futuro. El tráfico a los módulos de seguridad de hardware (HSM) que almacenan material de claves para las claves KMS solo se permite desde anfitriones de la API de AWS KMS a través de la red interna de AWS

Para conectarse directamente a AWS KMS desde su nube virtual privada (VPC) sin enviar tráfico a través del Internet público, use puntos de enlace de la VPC, con AWS PrivateLink. Para obtener más información, consulte Conectar con AWS KMS a través de un punto de conexión de VPC.

AWS KMS admite también una opción de intercambio híbrido postcuántico de claves para el protocolo de cifrado de red Transport Layer Security (TLS). Puede utilizar esta opción de TLS cuando se conecte a los puntos de enlace de la API de AWS KMS.

Administración de identidades y accesos en AWS Key Management Service

AWS Identity and Access Management (IAM) ayuda a controlar de forma segura el acceso a los recursos de AWS. Los administradores de controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de AWS KMS. Para obtener más información, consulte Uso de políticas de IAM con AWS KMS.

Políticas de claves son el mecanismo principal para controlar el acceso a las claves KMS en AWS KMS. Cada clave KMS debe tener una política de claves. También puede utilizar políticas de IAM y concesiones, junto con las políticas de claves para controlar el acceso a sus claves KMS. Para obtener más información, consulte Autenticación y control de acceso de AWS KMS.

Si utiliza Amazon Virtual Private Cloud (Amazon VPC), puede crear un punto de conexión de VPC de interfaz para AWS KMS basado en AWS PrivateLink. También puede usar políticas de punto de enlace de la VPC para determinar qué entidades principales pueden acceder a su punto de enlace AWS KMS, qué llamadas API pueden realizar y a qué clave KMS pueden acceder. Para obtener más información, consulte Control del acceso a un punto de conexión de VPC.

Registro y monitorización en AWS Key Management Service

La monitorización es una parte importante de la comprensión de la disponibilidad, el estado y el uso de su AWS KMS keys en AWS KMS. La monitorización ayuda a mantener la seguridad, la fiabilidad,

la disponibilidad y el rendimiento de sus soluciones de AWS. AWS proporciona varias herramientas para monitorear las claves KMS.

Registros de AWS CloudTrail

Cada llamada a una operación de la API de AWS KMS se captura como un evento en un registro de AWS CloudTrail. Estos registros registran todas las llamadas a las API realizadas desde la consola AWS KMS, y las llamadas realizadas por AWS KMS y otros servicios de AWS. Las llamadas a la API entre cuentas, como las llamadas para usar una clave de KMS en otraCuenta de AWS, se registran en los CloudTrail registros de ambas cuentas.

Al solucionar problemas o auditar, puede utilizar el registro para reconstruir el ciclo de vida de una clave KMS. También puede ver su administración y uso de la clave KMS en operaciones criptográficas. Para obtener más información, consulte the section called “Iniciar sesión con AWS CloudTrail”.

Amazon CloudWatch Logs

Monitoree, almacene y tenga acceso a los archivos de registro de AWS CloudTrail u otras fuentes. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

PuesAWS KMS, CloudWatch almacena información útil que le ayuda a evitar problemas con sus claves de KMS y los recursos que protegen. Para obtener más información, consulte the section called “Monitorización con CloudWatch”.

Amazon EventBridge

AWS KMSgenera EventBridge eventos cuando se rota o se elimina su clave de KMS o cuando caduca el material de clave importado de su clave de KMS. Busque eventos de AWS KMS (operaciones de API) y diríjalos a una o más secuencias o funciones de destino para capturar información de estado. Para obtener más información, consulta the section called “Monitorización con Amazon EventBridge” la Guía del EventBridge usuario de Amazon.

Estadísticas de CloudWatch Amazon

Puede supervisar sus claves de KMS mediante CloudWatch métricas, que recopilan y procesan datos sin procesar para AWS KMS convertirlos en métricas de rendimiento. Los datos se registran en intervalos de dos semanas para que pueda ver las tendencias de la información actual e histórica. Esto le ayuda a comprender cómo se utilizan sus claves KMS y cómo su uso cambia con el tiempo. Para obtener información sobre el uso de CloudWatch métricas para supervisar las claves de KMS, consulteAWS KMS métricas y dimensiones.

CloudWatch Alarmas Amazon

Vea solo un cambio de alarma durante el periodo especificado. Luego, realice una o varias acciones según el valor de la métrica con respecto a un umbral durante varios períodos. Por ejemplo, puede crear una CloudWatch alarma que se active cuando alguien intente usar una clave de KMS que está programada para eliminarse en una operación criptográfica. Esto indica que la clave KMS todavía se está utilizando y probablemente no debería eliminarse. Para obtener más información, consulte the section called “Creación de una alarma”.

AWS Security Hub

Puede supervisar el uso que hace de AWS KMS para comprobar si cumple con los estándares y las prácticas recomendadas del sector en materia de seguridad usando AWS Security Hub. Security Hub utiliza controles de seguridad para evaluar las configuraciones de los recursos y los estándares de seguridad para ayudarle a cumplir varios marcos de conformidad. Para obtener más información, consulte AWS Key Management Service controls en la Guía del usuario de AWS Security Hub.

Validación de conformidad en AWS Key Management Service

Auditores externos evalúan la seguridad y la conformidad de AWS Key Management Service como parte de varios programas de conformidad de AWS. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Temas

Documentos de conformidad y seguridad

En los siguientes documentos de conformidad y seguridad se incluye AWS KMS. Para verlos, utilice AWS Artifact.

- Catálogo de controles de conformidad de informática en la nube (C5)
- Declaración de aplicabilidad (SoA) de ISO 27001:2013
- Certificación ISO 27001:2013
- Declaración de aplicabilidad (SoA) de ISO 27017:2015

- Certificación ISO 27017:2015
- Declaración de aplicabilidad (SoA) de ISO 27018:2015
- Certificación ISO 27018:2014
- Certificación ISO 9001:2015
- Declaración de conformidad (AOC) PCI DSS y resumen de responsabilidad
- Informe de controles de organizaciones de servicios (SOC) 1
- Informe de controles de organizaciones de servicios (SOC) 2
- Informe de controles de organizaciones de servicios (SOC) 2 para la confidencialidad
- FedRAMP-High

Para obtener ayuda con AWS Artifact, consulte Descarga de informes en AWS Artifact.

Más información

Su responsabilidad de conformidad al utilizar AWS KMS se determina en función de la confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables. Si su uso de AWS KMS está sujeto a la conformidad con un estándar publicado, AWS proporciona recursos para ayudarle:

- Servicios de AWS en el ámbito del programa del conformidad: esta página enumera los servicios de AWS que pertenecen al ámbito de programas de conformidad específicos. Para obtener información general, consulte Programas de conformidad de AWS.
- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- AWS Config: este servicio de AWS evalúa en qué medida las configuraciones de los recursos cumplen las prácticas internas, las directrices del sector y la normativa.
- AWS Security Hub: este producto de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su conformidad con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.

Resiliencia en AWS Key Management Service

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Además de la infraestructura global de AWS, AWS KMS ofrece varias características que le ayudan con sus necesidades de resiliencia y copia de seguridad de los datos. Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global de AWS.

Aislamiento regional

AWS Key Management Service (AWS KMS) es un servicio regional autosuficiente que está disponible en todas las Regiones de AWS. El diseño aislado regionalmente de AWS KMS garantiza que un problema de disponibilidad en una Región de AWS no puede afectar la operación de AWS KMS en cualquier otra región. AWS KMS está diseñado para garantizar un tiempo de inactividad planificado nulo, con todas las actualizaciones de software y las operaciones de escalado realizadas sin problemas e imperceptiblemente.

El Acuerdo de nivel de servicio (SLA) de AWS KMS incluye un compromiso de servicio del 99,999 % para todas las API de KMS. Para cumplir este compromiso, AWS KMS garantiza que todos los datos y la información de autorización necesarios para ejecutar una solicitud de la API estén disponibles en todos los hosts regionales que reciben la solicitud.

La infraestructura de AWS KMS se replica en al menos tres zonas de disponibilidad (AZ) en cada región. Para garantizar que los errores de varios hosts no afecten al rendimiento de AWS KMS, AWS KMS está diseñado para atender el tráfico de clientes de cualquiera de las zonas de disponibilidad de una región.

Los cambios realizados en las propiedades o permisos de una clave de KMS se replican en todos los hosts de la región para garantizar que cualquier host de la región pueda procesar de manera correcta la solicitud posterior. Solicitudes de operaciones criptográficas mediante el uso de la clave de KMS se reenvían a una flota de módulos de seguridad de hardware (HSM) de AWS KMS, cualquiera de los cuales puede realizar la operación con la clave de KMS.

Diseño de varios inquilinos

El diseño de varios inquilinos de AWS KMS permite cumplir el SLA de disponibilidad del 99,999 % y mantener altas tasas de solicitudes, al tiempo que protege la confidencialidad de las claves y los datos.

Se implementan varios mecanismos de cumplimiento de la integridad para garantizar que la clave de KMS especificada para la operación criptográfica sea siempre la que se utiliza.

El material de clave de texto sin formato para las claves de KMS está ampliamente protegido. El material de clave se cifra en el HSM tan pronto como se crea y el material de clave cifrado se mueve de inmediato al almacenamiento seguro y de baja latencia. La clave cifrada se recupera y se descifra dentro del HSM justo a tiempo para su uso. La clave de texto sin formato permanece en la memoria HSM solo durante el tiempo necesario para completar la operación criptográfica. Luego se vuelve a cifrar en el HSM y la clave cifrada se devuelve al almacenamiento. El material de claves de texto sin formato nunca sale de los HSM; nunca se escribe en un almacenamiento persistente.

Para obtener más información acerca de los mecanismos que AWS KMS utiliza para proteger sus claves, consulte Detalles criptográficos de AWS Key Management Service.

Prácticas recomendadas de resiliencia en AWS KMS

Para optimizar la resiliencia de los recursos de AWS KMS, tenga en cuenta las siguientes estrategias.

- Para respaldar la estrategia de copia de seguridad y recuperación de desastres, considere las claves de varias regiones, que son claves de KMS creadas en una Región de AWS y se replican solo en las regiones que especifique. Con claves de varias regiones, puede mover los recursos cifrados entre Regiones de AWS (dentro de la misma partición) sin exponer nunca el texto sin formato y descifrar el recurso, cuando sea necesario, en cualquiera de las regiones de destino. Las claves de varias regiones relacionadas son interoperables porque comparten el mismo material de clave y el mismo ID de clave, pero tienen políticas de clave independientes para el control de acceso de alta resolución. Para obtener más información, consulte Claves de varias regiones en AWS KMS.
- Para proteger las claves en un servicio de varios inquilinos, como AWS KMS, asegúrese de utilizar los controles de acceso, incluidos políticas de claves y las políticas de IAM. Además, puede enviar las solicitudes a AWS KMS mediante un punto de conexión de interfaz de VPC basado en AWS PrivateLink. Cuando lo hace, toda la comunicación entre la VPC de Amazon y AWS KMS se lleva a cabo completamente dentro de la red de AWS mediante un punto de conexión de AWS KMS

dedicado y restringido a la VPC. Puede proteger aún más estas solicitudes al crear una capa de autorización adicional mediante políticas de punto de conexión de VPC. Para obtener más información, consulte Conexión a AWS KMS mediante un punto de conexión de VPC.

Seguridad de la infraestructura en AWS Key Management Service

Al tratarse de un servicio administrado, AWS Key Management Service (AWS KMS) está protegido por los procedimientos de seguridad de red globales de AWS que se describen en Amazon Web Services: Información general sobre los procesos de seguridad.

Para obtener acceso a AWS KMS a través de la red, puede llamar a las operaciones de la API de AWS KMS que se describen en la Referencia de la API de AWS Key Management Service. AWS KMS requiere TLS 1.2 y recomienda TLS 1.3 en todas las regiones. AWS KMS también es compatible con la TLS poscuántica híbrida para los puntos de conexión del servicio AWS KMS en todas las regiones, excepto en las regiones de China. AWS KMS no admite la TLS poscuántica híbrido para los puntos de conexión FIPS en AWS GovCloud (US). Para utilizar los puntos de conexión estándar de AWS KMS o los puntos de conexión FIPS de AWS KMS, los clientes deben admitir TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos, como Java 7 y posteriores, son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede llamar a estas operaciones de la API desde cualquier ubicación de red, pero AWS KMS admite condiciones de políticas globales que le permiten controlar el acceso a una clave KMS en función de la dirección IP de origen, la VPC y el punto de enlace de VPC. Puede utilizar estas claves de condición en políticas de claves y en políticas de IAM. Sin embargo, estas condiciones pueden impedir que AWS utilice la clave KMS en su nombre. Para obtener más detalles, consulte AWS claves de condición globales.

Por ejemplo, la siguiente declaración de política de claves permite a los usuarios que pueden asumir la función `KMSTestRole` utilizar este AWS KMS key para las operaciones criptográficas especificadas, a menos que la dirección IP de origen sea una de las direcciones IP especificadas en la política.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"AWS":
    "arn:aws:iam::111122223333:role/KMSTestRole"},
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "NotIpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24",
          "203.0.113.0/24"
        ]
      }
    }
  }
}
```

Aislamiento de Hosts físicos

La seguridad de la infraestructura física que AWS KMS utiliza está sujeto a los controles que se describen en la sección Seguridad Física y Ambiental de la Amazon Web Services: Información general de los procesos de seguridad. Puede encontrar más detalles en los informes de conformidad y los resultados de auditoría de terceros enumerados en la sección anterior.

AWS KMS es compatible con módulos de seguridad de hardware reforzados dedicados (HSM) diseñados con controles específicos para resistir ataques físicos. Los HSM son dispositivos físicos que no tienen una capa de virtualización, como un hipervisor, que comparte el dispositivo físico entre varios inquilinos lógicos. El material de claves para AWS KMS keys se almacena solo en memoria volátil en los HSM, y solo mientras la clave KMS está en uso. Esta memoria se borra cuando el HSM sale del estado operativo, incluidos los cierres y reinicios previstos e imprevistos. Para obtener información detallada acerca de la operación de los HSM de AWS KMS, consulte Detalles criptográficosAWS Key Management Service.

Prácticas recomendadas de seguridad para AWS Key Management Service

AWS Key Management Service (AWS KMS) es compatible con muchas características de seguridad que puede implementar para mejorar la protección de las claves de cifrado, incluidas las políticas de claves y las políticas de IAM, una opción de contexto de cifrado para las operaciones criptográficas en claves de cifrado simétricas, un amplio conjunto de claves de condición para mejorar las políticas de claves, las políticas de IAM y las restricciones de concesión para limitar las concesiones.

Estas características de seguridad se describen en detalle en las AWS Key Management Service Prácticas recomendadas (PDF). Las directrices generales de este documento técnico no representan una solución de seguridad completa. Dado que no todas las mejores prácticas son adecuadas para todas las situaciones, no se pretende que sean prescriptivas.

Véase también

- Prácticas recomendadas para las políticas de IAM
- Prácticas recomendadas para concesiones de AWS KMS
- Consulte Prácticas recomendadas en IAM en la Guía del usuario de IAM.

Cuotas

Para que todos los usuarios puedan AWS KMS responder y ofrecer un rendimiento óptimo, AWS KMS aplica dos tipos de cuotas: las cuotas de recursos y las cuotas de solicitud. Cada cuota se calcula de forma independiente para cada región de cada Cuenta de AWS.

Todas AWS KMS las cuotas son ajustables, excepto la cuota de recursos del tamaño del documento de política clave, la cuota de recursos de rotación bajo demanda y la cuota de solicitud del almacén de AWS CloudHSM claves. Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas. Para solicitar una reducción de cuota, cambiar una cuota que no aparece en Service Quotas o cambiar una cuota en una en la Región de AWS que Service Quotas for no AWS KMS esté disponible, visite AWS Support Center y cree un caso.

Temas

Cuotas de recursos

AWS KMS establece cuotas de recursos para garantizar que pueda brindar un servicio rápido y resiliente a todos nuestros clientes. Algunas cuotas de recursos se aplican solo a los recursos que usted crea, pero no a los recursos que AWS los servicios crean para usted. Los recursos que usa pero que no están en la cuenta de Cuenta de AWS, como las Claves propiedad de AWS, no se contabilizan en estas cuotas.

Si ha superado un límite de recursos, las solicitudes para crear un recurso adicional de dicho tipo generan un mensaje de error `LimitExceededException`.

Todas las cuotas de AWS KMS recursos son ajustables, excepto la cuota de tamaño de los documentos de política clave y la cuota de recursos de rotación bajo demanda. Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas. Para solicitar una reducción de cuota, cambiar una cuota que no aparece en Service Quotas o cambiar una cuota en una en la Región de AWS que Service Quotas for no AWS KMS esté disponible, visite AWS Support Center y cree un caso.

En la siguiente tabla se enumeran y describen las cuotas de AWS KMS recursos de cada Cuenta de AWS región.

Nombre de la cuota	Valor predeterminado	Aplica a	Ajustable
AWS KMS keys	100 000	Claves administradas por el cliente	Sí
Alias por clave KMS	50	Alias creados por el cliente	Sí
Concesiones por clave KMS	50 000	Claves administradas por el cliente	Sí
Tamaño del documento de política de claves	32 KB (32 768 bytes)	Claves administradas por el cliente Claves administradas por AWS	No
Cuota de recursos de almacenes de claves personalizados	10	Cuenta de AWS y región	Sí

Además de las cuotas de recursos, AWS KMS utiliza las cuotas de solicitud para garantizar la capacidad de respuesta del servicio. Para obtener más detalles, consulte the section called “Cuotas de solicitudes”.

AWS KMS keys: 100 000

Puede tener hasta 100 000 claves administradas por el cliente en cada región de su Cuenta de AWS. Esta cuota se aplica a todas las claves administradas por el cliente en todas las Regiones de AWS , independientemente de su especificación o de su estado de clave. Cada clave de KMS se considera un recurso. Las Claves administradas por AWS y Claves propiedad de AWS no se contabilizan para esta cuota.

Alias por clave KMS: 50

Puede asociar hasta 50 alias con cada clave administrada por el cliente. Los alias a los que se AWS asocian Claves administradas por AWSno se tienen en cuenta para esta cuota. Es posible que encuentre esta cuota cuando cree o actualice un alias.

> **Note**
>
> La ResourceAliases condición kms: solo entra en vigor cuando la clave KMS cumple con esta cuota. Si una clave KMS supera esta cuota, las entidades principales que están autorizadas a usar la clave KMS mediante la condición `kms:ResourceAliases` se deniega el acceso a la clave KMS. Para obtener más detalles, consulte Acceso denegado debido a la cuota de alias.

La cuota de alias por clave de KMS reemplaza a la cuota de alias por región que limitaba el número total de alias en cada región de una. Cuenta de AWS AWS KMS ha eliminado la cuota de alias por región.

Concesiones por clave KMS: 50 000

Cada clave administrada por el cliente puede tener hasta 50 000 concesiones, incluidas las concesiones creadas por los servicios de AWS que están integrados con AWS KMS. Esta cuota no se aplica a Claves administradas por AWS o Claves propiedad de AWS.

Un efecto de esta cuota es que no puede realizar más de 50 000 operaciones con concesiones autorizadas que utilicen la misma clave KMS al mismo tiempo. Después de alcanzar la cuota, puede crear nuevas concesiones para la clave KMS solo cuando se retire o se revoque una concesión activa.

Por ejemplo, cuando adjunta un volumen de Amazon Elastic Block Store (Amazon EBS) a una instancia de Amazon Elastic Compute Cloud (Amazon EC2), el volumen se descifra para que pueda leerlo. Para obtener permiso para descifrar los datos, Amazon EBS crea una concesión para cada volumen. Por lo tanto, si todos los volúmenes de Amazon EBS utilizan la misma clave KMS, no puede adjuntar más de 50 000 volúmenes a la vez.

Tamaño del documento de política de claves; 32 KB

La longitud máxima de cada documento de política de claves es de 32 KB (32 768 bytes). Si utiliza un documento de política mayor para crear o actualizar la política de claves para una clave KMS, se producirá un error en la operación.

Esta cuota no es ajustable. No puede aumentarlo mediante Service Quotas ni creando un caso en AWS Support. Si su política de clave se está acercando al límite, considere la posibilidad de utilizar concesiones en lugar de declaraciones de política. Las concesiones son especialmente adecuadas para permisos temporales o muy específicos.

Se utiliza un documento de política clave cada vez que se crea o cambia una política clave mediante la vista predeterminada o la vista de política de la AWS Management Console operación o de la PutKeyPolicyoperación. Esta cuota se aplica al documento de política de claves, aunque utilice la vista predeterminada en la consola de AWS KMS , donde no se editan directamente las instrucciones JSON.

Cuota de recursos de almacenes de claves personalizados: 10

Puede crear hasta 10 almacenes de claves personalizados en cada Cuenta de AWS región. Si intenta crear más, la CreateCustomKeyStoreoperación fallará.

Esta cuota se aplica al número total de almacenes de claves personalizados en cada cuenta y región. Esto incluye todos los almacenes de claves de AWS CloudHSM y los almacenes de claves externos, independientemente del estado de su conexión.

Rotación bajo demanda: 10

Puede realizar la rotación de claves bajo demanda un máximo de 10 veces por clave KMS. Si intenta realizar más rotaciones bajo demanda, se produce un error en la RotateKeyOnDemandoperación.

Esta cuota no se puede ajustar. No puede aumentarlo mediante Service Quotas ni creando un caso en AWS Support. Para evitar alcanzar la cuota de rotación bajo demanda, te recomendamos utilizar la rotación automática de claves siempre que sea posible.

Cuotas de solicitudes

AWS KMS establece cuotas para el número de operaciones de API solicitadas por segundo. Las cuotas de solicitud varían según el funcionamiento de la API Región de AWS, la API y otros factores,

como el tipo de clave de KMS. Cuando superas una cuota de solicitud de API AWS KMS , limita la solicitud.

Todas las cuotas de AWS KMS solicitudes son ajustables, excepto la cuota de solicitud del almacén de AWS CloudHSM claves. Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas. Para solicitar una reducción de cuota, cambiar una cuota que no aparece en Service Quotas o cambiar una cuota en una en la Región de AWS que Service Quotas for no AWS KMS esté disponible, visite AWS Support Center y cree un caso.

Si supera la cuota solicitada para la GenerateDataKeyoperación, considere la posibilidad de utilizar la función de almacenamiento en caché de claves de datos del AWS Encryption SDK. La reutilización de las claves de datos podría reducir la frecuencia de sus solicitudes también. AWS KMS

Además de solicitar cuotas, AWS KMS utiliza cuotas de recursos para garantizar la capacidad de todos los usuarios. Para obtener más detalles, consulte Cuotas de recursos.

Para ver las tendencias de las tarifas de solicitudes, utilice la Consola Service Quotas. También puedes crear una CloudWatch alarma de Amazon que te avise cuando tu porcentaje de solicitudes alcance un porcentaje determinado del valor de la cuota. Para obtener más información, consulta Gestiona tus tasas de solicitudes de AWS KMS API mediante Service Quotas y Amazon CloudWatch en el blog AWS de seguridad.

Temas

- Solicita cuotas para cada operación AWS KMS de la API
- Aplicar cuotas de solicitudes
- Cuotas compartidas para operaciones criptográficas
- Solicitudes de la API realizadas en su nombre
- Solicitudes entre cuentas
- Cuotas de solicitudes del almacén de claves personalizado

Solicita cuotas para cada operación AWS KMS de la API

En esta tabla se muestra el código de cuota de Service Quotas y el valor predeterminado de cada cuota de AWS KMS solicitud. Todas las cuotas de AWS KMS solicitud son ajustables, excepto la cuota de solicitud del almacén de AWS CloudHSM claves.

> **Note**
>
> Es posible que tenga que desplazarse horizontal o verticalmente para ver todos los datos de esta tabla.

Nombre de la cuota	Límite predeterminado (solicitudes por segundo)

`Cryptographic operations (symmetric) request rate`
 	
Válido para:
 	
• `Decrypt`
• `Encrypt`
• `GenerateDataKey`
• `GenerateDataKeyWithoutPlaintext`
• `GenerateMac`
• `GenerateRandom`
• `ReEncrypt`
• `VerifyMac`
	Estas cuotas compartidas varían en función del Región de AWS tipo de clave KMS utilizada en la solicitud. Cada cuota se calcula por separado.
	
	• 5500 (compartidas)
	• 10 000 (compartidas) en las siguientes regiones:
	  • EE. UU. Este (Ohio), us-east-2
	  • Asia Pacífico (Singapur), ap-southeast-1
	  • Asia Pacífico (Sídney), ap-southeast-2
	  • Asia Pacífico (Tokio), ap-northeast-1
	  • Europa (Fráncfort), eu-central-1
	  • Europa (Londres), eu-west-2
	• 50 000 (compartidas) en las siguientes Regiones:
	  • EE.UU. Este (Norte de Virginia) (us-east-1)
	  • EE.UU. Oeste (Oregón) (us-west-2)
	  • Europa (Irlanda), eu-west-1

`Cryptographic operations (RSA) request rate` Válido para: • `Decrypt`	500 (compartidas) para claves KMS de RSA

Nombre de la cuota	Límite predeterminado (solicitudes por segundo)
• `Encrypt` • `ReEncrypt` • `Sign` • `Verify`	
`Cryptographic operations (ECC and SM2) request rate` Válido para: • `Decrypt`—solo se admite para claves KMS SM2 (solo para regiones de China) • `Encrypt`—solo compatible con claves KMS SM2 (solo para regiones de China) • `ReEncrypt` —solo compatible con claves KMS SM2 (solo para regiones de China) • `Sign` • `Verify`	300 (compartidas) para claves KMS de curva elíptica (ECC) y SM2 (solo para regiones de China)
`Custom key store request quotas` Válido para: • `Decrypt` • `Encrypt` • `GenerateDataKey` • `GenerateDataKeyWithoutPlaintext` • `GenerateRandom` • `ReEncrypt`	Las cuotas de solicitudes del almacén de claves personalizado se calculan por separado para cada almacén de claves personalizado. • 1800 (compartidas) por cada almacén de claves AWS CloudHSM • 1800 (compartidas) para cada almacén de claves externo.
`CancelKeyDeletion request rate`	5

Nombre de la cuota	Límite predeterminado (solicitudes por segundo)
ConnectCustomKeyStore request rate	5
CreateAlias request rate	5
CreateCustomKeyStore request rate	5
CreateGrant request rate	50
CreateKey request rate	5
DeleteAlias request rate	15
DeleteCustomKeyStore request rate	5
DeleteImportedKeyMaterial request rate	5
DescribeCustomKeyStores request rate	5
DescribeKey request rate	2000
DisableKey request rate	5
DisableKeyRotation request rate	5
DisconnectCustomKeyStore request rate	5
EnableKey request rate	5
EnableKeyRotation request rate	15

Nombre de la cuota	Límite predeterminado (solicitudes por segundo)
`GenerateDataKeyPair (ECC_NIST_P256) request rate` Válido para: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100
`GenerateDataKeyPair (ECC_NIST_P384) request rate` Válido para: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100
`GenerateDataKeyPair (ECC_NIST_P521) request rate` Válido para: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100
`GenerateDataKeyPair (ECC_SECG_P256K1) request rate` Válido para: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	100

Nombre de la cuota	Límite predeterminado (solicitudes por segundo)
`GenerateDataKeyPair (RSA_2048) request rate` Válido para: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	1
`GenerateDataKeyPair (RSA_3072) request rate` Válido para: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	0,5 (1 en cada intervalo de 2 segundos)
`GenerateDataKeyPair (RSA_4096) request rate` Válido para: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	0,1 (1 en cada intervalo de 10 segundos)
`GenerateDataKeyPair (SM2 – China Regions only) request rate` Válido para: • `GenerateDataKeyPair` • `GenerateDataKeyPairWithoutPlaintext`	25

Nombre de la cuota	Límite predeterminado (solicitudes por segundo)
`GetKeyPolicy request rate`	1 000
`GetKeyRotationStatus request rate`	1 000
`GetParametersForImport request rate`	0,25 (1 en cada intervalo de 4 segundos)
`GetPublicKey request rate`	2000
`ImportKeyMaterial request rate`	5
`ListAliases request rate`	500
`ListGrants request rate`	100
`ListKeyPolicies request rate`	100
`ListKeys request rate`	500
`ListKeyRotations request rate`	100
`ListResourceTags request rate`	2000
`ListRetirableGrants request rate`	100
`PutKeyPolicy request rate`	15
`ReplicateKey request rate` Una operación `ReplicateKey` cuenta como una solicitud `ReplicateKey` en la Región de la clave principal y dos solicitudes `CreateKey` en la Región de la réplica. Solo una de las solicitudes `CreateKey` es una ejecución en seco para detectar posibles problemas antes de crear la clave.	5
`RetireGrant request rate`	30

Nombre de la cuota	Límite predeterminado (solicitudes por segundo)
`RevokeGrant request rate`	30
`RotateKeyOnDemand request rate`	5
`ScheduleKeyDeletion request rate`	15
`TagResource request rate`	10
`UntagResource request rate`	5
`UpdateAlias request rate`	5
`UpdateCustomKeyStore request rate`	5
`UpdateKeyDescription request rate`	5
`UpdatePrimaryRegion request rate` Un operación `UpdatePrimaryRegion` cuenta como dos solicitudes `UpdatePrimaryRegion` ; una solicitud en cada una de las dos Regiones afectadas.	5

Aplicar cuotas de solicitudes

Al revisar las cuotas de solicitudes, tenga en cuenta la siguiente información.

- Las cuotas de solicitudes se aplican a claves administradas por el cliente y Claves administradas por AWS. El uso de Claves propiedad de AWSno tiene en cuenta las cuotas solicitadas para usted Cuenta de AWS, incluso cuando se utilizan para proteger los recursos de su cuenta.
- Las cuotas de solicitud se aplican a las solicitudes enviadas a puntos de conexión FIPS y puntos de conexión no FIPS. Para obtener una lista de los puntos finales del AWS KMS servicio, consulte los AWS Key Management Service puntos finales y las cuotas en. Referencia general de AWS

- La limitación controlada se basa en todas las solicitudes de las claves KMS de todos los tipos de la Región. Este total incluye las solicitudes de todos los directores del Cuenta de AWS, incluidas las solicitudes de AWS servicios en su nombre.
- Cada cuota de solicitud se calcula de forma independiente. Por ejemplo, las solicitudes de la CreateKeyoperación no afectan a la cuota de solicitudes de la CreateAliasoperación. Si las solicitudes `CreateAlias` se limitan de forma controlada, las solicitudes `CreateKey` aún pueden completarse correctamente.
- Aunque las operaciones criptográficas comparten una cuota, la cuota compartida se calcula de manera independiente de las cuotas para otras operaciones. Por ejemplo, las llamadas a las operaciones de cifrado y descifrado comparten una cuota de solicitudes, pero esa cuota es independiente de la cuota de las operaciones de administración, por ejemplo. EnableKey Por ejemplo, en la Región Europa (Londres), puede realizar 10 000 operaciones criptográficas en claves KMS simétricas más 5 operaciones `EnableKey` por segundo sin que se limiten de forma controlada.

Cuotas compartidas para operaciones criptográficas

AWS KMS las operaciones criptográficas comparten cuotas de solicitud. Puede solicitar cualquier combinación de las operaciones criptográficas admitidas por la clave KMS, solo para que el número total de operaciones criptográficas no supere la cuota de solicitud para ese tipo de clave KMS. Las excepciones son GenerateDataKeyPairy GenerateDataKeyPairWithoutPlaintext, que comparten una cuota independiente.

Las cuotas para distintos tipos de claves KMS se calculan de forma independiente. Cada cuota se aplica a todas las solicitudes de estas operaciones en la región Cuenta de AWS y con el tipo de clave indicado en cada intervalo de un segundo.

- La tasa de solicitudes de operaciones criptográficas (simétricas) es la cuota de solicitudes compartidas para operaciones criptográficas que utilizan claves KMS simétricas en una cuenta y región. Esta cuota se aplica a las operaciones criptográficas con claves de cifrado simétricas y claves HMAC, que también son simétricas.

  Por ejemplo, es posible que esté utilizando claves KMS simétricas Región de AWS con una cuota compartida de 10 000 solicitudes por segundo. Cuando realizas 7 000 GenerateDataKeysolicitudes por segundo y 2 000 solicitudes de descifrado por segundo, AWS KMS no se limitan tus solicitudes. Sin embargo, cuando realice 9500 solicitudes `GenerateDataKey` y 1000 solicitudes

Encrypt por segundo, AWS KMS limita de forma controlada las solicitudes porque superan la cuota compartida.

Las operaciones criptográficas en las claves KMS de cifrado simétrico de un almacén de claves personalizado cuentan tanto para la tasa de solicitudes de operaciones criptográficas (simétricas) de la cuenta como para la cuota de solicitudes del almacén de claves personalizado para el almacén de claves personalizado.

- La tasa de solicitudes de operaciones criptográficas (RSA) es la cuota de solicitudes compartidas para operaciones criptográficas que utilizan claves KMS asimétricas RSA.

  Por ejemplo, con una cuota de solicitudes de 500 operaciones por segundo, puede realizar 200 solicitudes de Cifrado y 100 solicitudes de Descifrado con claves KMS RSA que pueden cifrar y descifrar, además de 50 solicitudes de Firma y 150 solicitudes de Verificación con claves KMS RSA que pueden firmar y verificar.

- La tasa de solicitudes de operaciones criptográficas (ECC) es la cuota de solicitudes compartidas para operaciones criptográficas que utilizan claves KMS asimétricas de curva elíptica (ECC).

  Por ejemplo, con una cuota de solicitudes de 300 operaciones por segundo, puede realizar 100 solicitudes de Firma y 200 solicitudes de Verificación con claves KMS RSA que pueden firmar y verificar.

- La tasa de solicitudes de operaciones criptográficas (SM - solo en las regiones de China) es la cuota de solicitudes compartidas para operaciones criptográficas que utilizan claves KMS asimétricas SM.

  Por ejemplo, con una cuota de solicitudes de 300 operaciones por segundo, puede realizar 100 solicitudes de Cifrado y 100 solicitudes de Descifrado con claves KMS SM2 que pueden cifrar y descifrar, además de 50 solicitudes de Firma y 50 solicitudes de Verificación con claves KMS SM2 que pueden firmar y verificar.

- La cuota de solicitud de almacén de claves personalizadas es la cuota de solicitud compartida para operaciones criptográficas en claves KMS en un almacén de claves personalizado. Esta cuota se calcula por separado para cada almacén de claves personalizado.

  Las operaciones criptográficas en las claves KMS de cifrado simétrico de un almacén de claves personalizado cuentan tanto para la tasa de solicitudes de operaciones criptográficas (simétricas) de la cuenta como para la cuota de solicitudes del almacén de claves personalizado para el almacén de claves personalizado.

Las cuotas para distintos tipos de clave también se calculan de forma independiente. Por ejemplo, en la Región Asia Pacífico (Singapur), si utiliza claves KMS simétricas y asimétricas, puede realizar hasta 10 000 llamadas por segundo con claves KMS simétricas (incluidas claves HMAC) más un máximo de 500 llamadas adicionales por segundo con claves KMS asimétricas RSA, más un máximo de 300 solicitudes adicionales por segundo con claves KMS basadas en ECC.

Solicitudes de la API realizadas en su nombre

Puedes realizar solicitudes a la API directamente o mediante un AWS servicio integrado que realice las solicitudes a la API AWS KMS en tu nombre. La cuota se aplica a ambos tipos de solicitudes.

Por ejemplo, puede almacenar datos en Amazon S3 utilizando el cifrado del servidor con una clave KMS (SSE-KMS). Cada vez que carga o descarga un objeto de S3 cifrado con SSE-KMS, Amazon S3 realiza una solicitud `GenerateDataKey` (para cargas) o `Decrypt` (para descargas) AWS KMS en su nombre. Estas solicitudes se tienen en cuenta para su cuota, por lo AWS KMS que limita las solicitudes si supera un total combinado de 5 500 (o 10 000 o 50 000, según el volumen Región de AWS) de cargas o descargas por segundo de objetos de S3 cifrados con SSE-KMS.

Solicitudes entre cuentas

Cuando una de las aplicaciones de una aplicación Cuenta de AWS utiliza una clave de KMS propiedad de otra cuenta, se denomina solicitud multicuenta. En el caso de las solicitudes entre cuentas, AWS KMS limita de forma controlada la cuenta que realiza las solicitudes, no la cuenta que posee la clave KMS. Por ejemplo, si una aplicación de una cuenta A utiliza una clave KMS de la cuenta B, el uso de la clave KMS se aplica solo a las cuotas de la cuenta A.

Cuotas de solicitudes del almacén de claves personalizado

AWS KMS mantiene las cuotas de solicitud para las operaciones criptográficas en las claves de KMS en un almacén de claves personalizado. Esta solicitud de cuotas se calcula por separado para cada almacén de claves personalizado.

Cuota de solicitudes del almacén de claves personalizado	Valor predeterminado (solicitudes por segundo) para cada almacén de claves personalizado	Ajustable
AWS CloudHSM cuota de solicitud del almacén de claves	1800	No
Cuota de solicitudes del almacén de claves externo	1800	Sí

> **Note**
>
> AWS KMS las cuotas de solicitud de almacén de claves personalizadas no aparecen en la consola de Service Quotas. No puede ver ni administrar esta cuotas mediante las operaciones de la API de Service Quotas. Para solicitar un cambio en su cuota de solicitudes del almacén de claves externo, visite el Centro de AWS Support y cree un caso.
> Si el AWS CloudHSM clúster asociado a un almacén de AWS CloudHSM claves procesa numerosos comandos, incluidos aquellos que no están relacionados con el almacén de claves personalizado, es posible que obtengas un AWS KMS `ThrottlingException` lower-than-expected ritmo. Si esto ocurre, reduce la tasa de solicitudes a AWS KMS, reduce la carga no relacionada o usa un AWS CloudHSM clúster dedicado para tu almacén de AWS CloudHSM claves.
> AWS KMS informa de la limitación de las solicitudes de almacenes de claves externos en la `ExternalKeyStoreThrottle` CloudWatch métrica. Puede usar esta métrica para ver los patrones de limitación, crear alarmas y ajustar su cuota de solicitudes del almacén de claves externo.

Una solicitud de una operación criptográfica en una clave KMS en un almacén de claves personalizado cuenta para dos cuotas:

- Cuota de tasas de solicitud de operaciones criptográficas (simétricas) (por cuenta)

  Las solicitudes de operaciones criptográficas en las claves KMS de un almacén de claves personalizado se cuentan para la cuota `Cryptographic operations (symmetric)`

`request rate` para cada Cuenta de AWS y región. Por ejemplo, en Este de EE. UU. (norte de Virginia) (us-east-1), cada Cuenta de AWS puede tener hasta 50 000 solicitudes por segundo en claves KMS de cifrado simétrico, incluidas las solicitudes que usan una clave KMS en un almacén de claves personalizado.

- Cuota de solicitudes de almacén de claves personalizado (por almacén de claves personalizado)

  Las solicitudes de operaciones criptográficas en claves KMS en un almacén de claves personalizado también cuentan para un `Custom key store request quota` de 1800 operaciones por segundo. Estas cuotas se calculan por separado para cada almacén de claves personalizado. Pueden incluir solicitudes de varios usuarios Cuentas de AWS que utilizan claves de KMS en el almacén de claves personalizado.

Por ejemplo, si solicita una operación Encrypt en una clave KMS dentro de un almacén de claves personalizado (de cualquier tipo) en la región Este de EE. UU. (norte de Virginia) (us-east-1), cuenta para la cuota a nivel de cuenta `Cryptographic operations (symmetric) request rate` (50 000 solicitudes por segundo) para su cuenta y región, y para una `Custom key store request quota` (1800 solicitudes por segundo) para su almacén de claves personalizado. Sin embargo, una solicitud de una operación de administración PutKeyPolicy, como una clave KMS de un almacén de claves personalizado, solo se aplica a su cuota a nivel de cuenta (15 solicitudes por segundo).

Limitar las solicitudes AWS KMS

Para garantizar que AWS KMS puede proporcionar respuestas rápidas y confiables a las solicitudes de API de todos los clientes, limita las solicitudes de API que superan ciertos límites.

La limitación se produce cuando se AWS KMS rechaza una solicitud que, de otro modo, podría ser válida y se produce un `ThrottlingException` error como el siguiente.

```
You have exceeded the rate at which you may call KMS. Reduce the frequency of your
 calls.
(Service: AWSKMS; Status Code: 400; Error Code: ThrottlingException; Request ID: <ID>
```

AWS KMS limita las solicitudes que cumplen las siguientes condiciones.

- La tasa de solicitudes por segundo supera la cuota de AWS KMS solicitudes de una cuenta y una región.

Por ejemplo, si los usuarios de tu cuenta envían 1000 `DescribeKey` solicitudes en un segundo, limita AWS KMS todas las `DescribeKey` solicitudes subsiguientes en ese segundo.

Para responder a la limitación controlada, utilice una estrategia de interrupción y reintento. Esta estrategia se implementa automáticamente para los errores de HTTP 400 en algunos AWS SDK.

- Una velocidad alta o sostenida de solicitudes para cambiar el estado de la misma clave KMS. Esta condición se conoce a menudo como una “tecla de acceso rápido”.

  Por ejemplo, si una aplicación de tu cuenta envía una oleada persistente de `DisableKey` solicitudes de la misma clave de KMS `EnableKey` y las solicita, limita las AWS KMS solicitudes. Esta limitación se produce incluso si las solicitudes no superan el límite de solicitudes de las operaciones request-per-second y. `EnableKey` `DisableKey`

  Para responder a la limitación controlada, ajuste la lógica de la aplicación para que solo realice solicitudes requeridas o consolide las solicitudes de varias funciones.

- Es posible que las solicitudes de operaciones con las claves de KMS de un AWS CloudHSM almacén de claves se limiten a un lower-than-expected ritmo similar al que el AWS CloudHSM clúster asociado al almacén de AWS CloudHSM claves procesa numerosos comandos, incluidos aquellos que no están relacionados con el almacén de claves. AWS CloudHSM

  (ya AWS KMS no limita las solicitudes de operaciones con las claves de KMS de un AWS CloudHSM almacén de claves cuando no hay sesiones de PKCS #11 disponibles para el clúster. AWS CloudHSM En su lugar, lanza un `KMSInternalException` y recomienda que vuelvas a intentar la solicitud.)

Para ver las tendencias de las tarifas de solicitudes, utilice la Consola Service Quotas. También puedes crear una CloudWatch alarma de Amazon que te avise cuando tu porcentaje de solicitudes alcance un porcentaje determinado del valor de la cuota. Para obtener más información, consulta Gestiona tus tasas de solicitudes de AWS KMS API mediante Service Quotas y Amazon CloudWatch en el blog AWS de seguridad.

Todas AWS KMS las cuotas son ajustables, excepto la cuota de recursos del tamaño de los documentos de política clave, la cuota de recursos de rotación bajo demanda y la cuota de solicitudes del almacén de AWS CloudHSM claves. Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas. Para solicitar una reducción de cuota, cambiar una cuota que no aparece en Service Quotas o cambiar una cuota en

una en la Región de AWS que Service Quotas for no AWS KMS esté disponible, visite AWS Support Center y cree un caso.

> **Note**
>
> AWS KMS las cuotas de solicitud de almacén de claves personalizadas no aparecen en la consola de Service Quotas. No puede ver ni administrar esta cuotas mediante las operaciones de la API de Service Quotas. Para solicitar un cambio en su cuota de solicitudes del almacén de claves externo, visite el Centro de AWS Support y cree un caso.

Cómo los servicios de AWS usan AWS KMS

Muchos servicios de AWS utilizan AWS KMS para admitir el cifrado de los datos. Cuando un servicio de AWS se integra con AWS KMS, puede utilizar lasAWS KMS keys en su cuenta para proteger los datos que el servicio recibe, almacena o administra automáticamente. Para ver la lista completa de los servicios de AWS que están integrados con AWS KMS, consulte Integración con los servicios de AWS.

En los siguientes temas se explica en detalle cómo determinados servicios usan AWS KMS, incluidas las claves KMS que admiten, cómo administran las claves de datos, los permisos que necesitan y cómo realizar el seguimiento del uso que hace cada servicio de las claves KMS de su cuenta.

> **Important**
>
> Los servicios de AWS que se integran con AWS KMS utilizan solo claves KMS de cifrado simétricas para cifrar sus datos. Estos servicios no admiten cifrado con claves de KMS asimétricas. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Temas

- Cómo WorkMail usa Amazon AWS KMS
- Cómo WorkSpaces usa AWS KMS

Cómo AWS CloudTrail usa AWS KMS

Puede utilizar AWS CloudTrail para registrar las llamadas a la API de AWS y otra actividad de su Cuenta de AWS y para guardar la información registrada en los archivos de registro en un bucket de Amazon Simple Storage Service (Amazon S3) de su elección. De forma predeterminada, los archivos de registro que se CloudTrail colocan en su bucket de S3 se cifran mediante el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3). Pero, en su lugar, puede elegir utilizar el cifrado del lado del servidor una clave KMS (SSE-KMS). Para obtener información sobre cómo cifrar sus archivos de registro, consulte CloudTrail Cifrar archivos de registro con (AWS KMSSSE-KMS) en la Guía del CloudTrail usuario. AWS KMS keys AWS CloudTrail

> **Important**
>
> AWS CloudTrail y Amazon S3 solo admite CMK AWS KMS keys simétricas. No puede usar una clave KMS asimétrica para cifrar sus registros. CloudTrail Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

No paga ningún cargo por el uso de claves cuando CloudTrail lee o escribe archivos de registro cifrados con una clave SSE-KMS. Sin embargo, paga un cargo por el uso de la clave cuando accede a los archivos de CloudTrail registro cifrados con una clave SSE-KMS. Para obtener más información acerca de los precios de AWS KMS, consulte Precios de AWS Key Management Service. Para obtener información sobre CloudTrail los precios, consulte los AWS CloudTrailprecios y la administración de los costos en la Guía del AWS CloudTrailusuario.

Temas

- Conocer cuándo se usa su clave KMS

Conocer cuándo se usa su clave KMS

El cifrado de archivos de CloudTrail registro AWS KMS se basa en la función de Amazon S3 denominada cifrado del lado del servidor con un AWS KMS key (SSE-KMS). Para obtener más

información sobre SSE-KMS, consulte ¿Cómo Amazon Simple Storage Service (Amazon S3) utiliza AWS KMS? en esta guía o Proteger los datos utilizando cifrado del lado del servidor con claves KMS (SSE-KMS) en la Guía del desarrollador de Amazon Simple Storage Service.

Cuando configura AWS CloudTrail el SSE-KMS para cifrar sus archivos de registro y Amazon CloudTrail S3 lo usa AWS KMS keys cuando realiza determinadas acciones con esos servicios. En las secciones siguientes se explica cuándo y cómo dichos servicios pueden utilizar su clave KMS y se proporciona información adicional que puede utilizar para validar esta explicación.

Acciones que provocan CloudTrail que Amazon S3 utilice su clave de KMS

- Se configura CloudTrail para cifrar los archivos de registro con su AWS KMS key
- CloudTrail coloca un archivo de registro en su bucket de S3
- Obtenga un archivo de registro cifrado del bucket de S3

Se configura CloudTrail para cifrar los archivos de registro con su AWS KMS key

Al actualizar la CloudTrail configuración para usar la clave de KMS, CloudTrail envía una `GenerateDataKey`solicitud AWS KMS para comprobar que la clave de KMS existe y que CloudTrail tiene permiso para utilizarla con fines de cifrado. CloudTrail no utiliza la clave de datos resultante.

La solicitud `GenerateDataKey` incluye la siguiente información para el contexto de cifrado:

- El nombre del recurso de Amazon (ARN) de la ruta CloudTrail
- El ARN del depósito S3 y la ruta donde se entregan los archivos de CloudTrail registro

La `GenerateDataKey` solicitud da como resultado una entrada en CloudTrail los registros similar a la del siguiente ejemplo. Cuando veas una entrada de registro como esta, podrás determinar que CloudTrail (1) ha llamado a la `GenerateDataKey` operación AWS KMS (2) (3) para una ruta (4) específica. AWS KMScreó la clave de datos con una clave KMS específica (5).

> **Note**
>
> Es posible que tenga que desplazarse a la parte derecha para ver algunas de las llamadas en la siguiente entrada de registro de ejemplo.


```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::086441151436:user/
AWSCloudTrail",1
    "accountId": "086441151436",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "AWSCloudTrail",
    "sessionContext": {"attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2015-11-11T21:15:33Z"
    }},
    "invokedBy": "internal.amazonaws.com"
  },
  "eventTime": "2015-11-11T21:15:33Z",
  "eventSource":
 "kms.amazonaws.com",2
  "eventName":
 "GenerateDataKey",3
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
  "requestParameters": {
    "keyId": "arn:aws:kms:us-west-2:111122223333:alias/ExampleAliasForCloudTrailKMS
 key",
    "encryptionContext": {
      "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-west-2:111122223333:trail/
Default",4
      "aws:s3:arn": "arn:aws:s3:::example-bucket-for-CT-logs/AWSLogs/111122223333/"
    },
    "keySpec": "AES_256"
  },
  "responseElements": null,
```

```
  "requestID": "581f1f11-88b9-11e5-9c9c-595a1fb59ac0",
  "eventID": "3cdb2457-c035-4890-93b6-181832b9e766",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",(5)
    "accountId": "111122223333"
  }],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333"
}
```

CloudTrail coloca un archivo de registro en su bucket de S3

Cada vez que CloudTrail coloca un archivo de registro en su bucket de S3, Amazon S3 envía una `GenerateDataKey`solicitud AWS KMS en su nombre CloudTrail. En respuesta a esta solicitud, AWS KMS genera una clave de datos única y, a continuación, envía a Amazon S3 dos copias de la clave de datos, una en texto no cifrado y otra cifrada con la clave KMS especificada. Amazon S3 utiliza la clave de datos de texto sin formato para cifrar el archivo de CloudTrail registro y, a continuación, elimina la clave de datos de texto sin formato de la memoria tan pronto como sea posible tras su uso. Amazon S3 almacena la clave de datos cifrados como metadatos con el archivo de CloudTrail registro cifrado.

La solicitud `GenerateDataKey` incluye la siguiente información para el contexto de cifrado:

- El nombre del recurso de Amazon (ARN) de la ruta CloudTrail
- El ARN del objeto S3 (el archivo de CloudTrail registro)

Cada `GenerateDataKey` solicitud da como resultado una entrada en CloudTrail los registros similar a la del siguiente ejemplo. Cuando veas una entrada de registro como esta, podrás determinar que CloudTrail (1) ha llamado a la `GenerateDataKey` operación AWS KMS (2) (3) para una ruta (4) específica para proteger un archivo de registro específico

(5).
AWS KMScreó la clave de datos con la clave KMS especificada
(6),
que se muestra dos veces en la misma entrada de registro.

> **Note**
>
> Es posible que tenga que desplazarse a la parte derecha para ver algunas de las llamadas en la siguiente entrada de registro de ejemplo.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:i-34755b85",
    "arn": "arn:aws:sts::086441151436:assumed-role/AWSCloudTrail/
i-34755b85",1
    "accountId": "086441151436",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2015-11-11T20:45:25Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::086441151436:role/AWSCloudTrail",
        "accountId": "086441151436",
        "userName": "AWSCloudTrail"
      }
    },
    "invokedBy": "internal.amazonaws.com"
  },
  "eventTime": "2015-11-11T21:15:58Z",
  "eventSource":
 "kms.amazonaws.com",2
  "eventName":
 "GenerateDataKey",3
```

```
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {
      "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-west-2:111122223333:trail/
Default",4
      "aws:s3:arn": "arn:aws:s3:::example-bucket-for-CT-logs/
AWSLogs/111122223333/CloudTrail/us-west-2/2015/11/11/111122223333_CloudTrail_us-
west-2_20151111T2115Z_7JREEBimdK8d2nC9.json.gz"5
    },
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",6
    "keySpec": "AES_256"
  },
  "responseElements": null,
  "requestID": "66f3f74a-88b9-11e5-b7fb-63d925c72ffe",
  "eventID": "7738554f-92ab-4e27-83e3-03354b1aa898",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",6
    "accountId": "111122223333"
  }],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333"
}
```

Obtenga un archivo de registro cifrado del bucket de S3

Cada vez que obtiene un archivo de CloudTrail registro cifrado de su bucket de S3, Amazon S3 envía una `Decrypt`solicitud AWS KMS en su nombre para descifrar la clave de datos cifrados del archivo de registro. Como respuesta a esta solicitud, AWS KMS utiliza su clave KMS para descifrar la clave de datos y, a continuación, envía la clave de datos en texto no cifrado a Amazon S3. Amazon S3 utiliza la clave de datos de texto sin formato para descifrar el archivo de CloudTrail registro y, a continuación, elimina la clave de datos de texto sin formato de la memoria tan pronto como sea posible tras su uso.

La solicitud `Decrypt` incluye la siguiente información para el contexto de cifrado:

- El nombre del recurso de Amazon (ARN) de la ruta CloudTrail

- El ARN del objeto S3 (el archivo de CloudTrail registro)

Cada `Decrypt` solicitud da como resultado una entrada en CloudTrail los registros similar a la del siguiente ejemplo. Cuando aparece una entrada de registro como esta, se puede determinar que un usuario en su cuenta de Cuenta de AWS (1) ha llamado a la operación de AWS KMS (2) `Decrypt` (3) para un registro de seguimiento específico (4) y un archivo de registro específico (5). AWS KMS ha descifrado la clave de datos con una clave KMS específica (6).

> **Note**
>
> Es posible que tenga que desplazarse a la parte derecha para ver algunas de las llamadas en la siguiente entrada de registro de ejemplo.

```
{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::111122223333:role/cloudtrail-
admin",(1)
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "cloudtrail-admin",
    "sessionContext": {"attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2015-11-11T20:48:04Z"
    }},
```

```
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2015-11-11T21:20:52Z",
  "eventSource":
 "kms.amazonaws.com",(2)
  "eventName":
 "Decrypt",(3)
  "awsRegion": "us-west-2",
  "sourceIPAddress": "internal.amazonaws.com",
  "userAgent": "internal.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {
      "aws:cloudtrail:arn": "arn:aws:cloudtrail:us-west-2:111122223333:trail/
Default",(4)
      "aws:s3:arn": "arn:aws:s3:::example-bucket-for-CT-logs/
AWSLogs/111122223333/CloudTrail/us-west-2/2015/11/11/111122223333_CloudTrail_us-
west-2_20151111T2115Z_7JREEBimdK8d2nC9.json.gz"(5)
    }
  },
  "responseElements": null,
  "requestID": "16a0590a-88ba-11e5-b406-436f15c3ac01",
  "eventID": "9525bee7-5145-42b0-bed5-ab7196a16daa",
  "readOnly": true,
  "resources": [{
    "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",(6)
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

¿Cómo Amazon DynamoDB utiliza AWS KMS?

Amazon DynamoDB es un servicio de base de datos completamente administrado NoSQL escalable. DynamoDB se integra con AWS Key Management Service (AWS KMS) para admitir una característica de cifrado del lado del servidor de cifrado en reposo.

Con el cifrado en reposo, DynamoDB cifra de forma transparente todos los datos de los clientes en una tabla de DynamoDB, incluida su clave principal y los índices secundarios locales y globales, siempre que la tabla se almacene en el disco. (Si la tabla tiene una clave de ordenación, algunas de

las claves de ordenación que marcan los límites del intervalo se almacenan en texto no cifrado en los metadatos de la tabla). Cuando obtiene acceso a la tabla, DynamoDB descifra los datos de la tabla de forma transparente. No es necesario que cambie sus aplicaciones para utilizar o administrar tablas cifradas.

El cifrado en reposo protege también las secuencias de DynamoDB, las tablas globales y las copias de seguridad siempre que estos objetos se guardan en un soporte duradero. Las instrucciones acerca de las tablas de este tema se aplican también a estos objetos.

Todas las tablas de DynamoDB están cifradas. No existe la opción de habilitar o deshabilitar el cifrado para tablas nuevas o existentes. De forma predeterminada, todas las tablas están cifradas en una Clave propiedad de AWS en la cuenta de servicio de DynamoDB. Sin embargo, puede seleccionar una opción para cifrar algunas o todas las tablas con una clave administrada por el cliente o la Clave administrada de AWS para DynamoDB en su cuenta.

Para obtener más información sobre la compatibilidad de Amazon DynamoDB con las claves de KMS, consulte Cifrado en reposo de DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

¿Cómo Amazon Elastic Block Store (Amazon EBS) utiliza AWS KMS?

En este tema se habla en detalle de cómo Amazon Elastic Block Store (Amazon EBS) utiliza AWS KMS para cifrar volúmenes e instantáneas. Para obtener instrucciones básicas sobre el cifrado de volúmenes de Amazon EBS, consulte Cifrado de Amazon EBS.

Temas

- Cifrado de Amazon EBS
- Uso de claves KMS y claves de datos
- Contexto de cifrado de Amazon EBS
- Detección de errores de Amazon EBS
- Uso de AWS CloudFormation para crear volúmenes de Amazon EBS cifrados

Cifrado de Amazon EBS

Cuando se asocia un volumen de Amazon EBS cifrado a un tipo de instancia Amazon Elastic Compute Cloud (Amazon EC2 compatible, se cifran los datos almacenados que están en reposo en

el volumen, la E/S de disco y las instantáneas creadas a partir del volumen. El cifrado se produce en los servidores que alojan instancias de Amazon EC2.

Esta característica es compatible con todos los tipos de volúmenes de Amazon EBS. A los volúmenes cifrados se obtiene acceso del mismo modo que a otros volúmenes; el cifrado y el descifrado se gestionan de forma transparente y no requieren ninguna acción de su parte, la instancia EC2 o su aplicación. Las instantáneas de los volúmenes cifrados se cifran automáticamente y los volúmenes que se crean a partir de las instantáneas cifradas también se cifran de forma automática.

El estado de cifrado de un volumen de EBS se determina al crear el volumen. No puede cambiar el estado de cifrado de un volumen existente. Sin embargo, puede migrar datos entre volúmenes cifrados y no cifrados, y aplicar un nuevo estado de cifrado al copiar una instantánea.

Amazon EBS admite el cifrado opcional de forma predeterminada. Puede habilitar el cifrado automáticamente en todos los nuevos volúmenes de EBS y copias de instantáneas en su Cuenta de AWSy Región. Este ajuste de configuración no afecta a los volúmenes o instantáneas existentes. Para obtener más información, consulte Cifrado de forma predeterminada en la Guía del usuario de Amazon EC2 para instancias de Linux o en la Guía del usuario de Amazon EC2 para instancias de Windows.

Uso de claves KMS y claves de datos

Cuando crea un volumen Amazon EBS cifrado, se especifica un AWS KMS key. De manera predeterminada, Amazon EBS utiliza la Clave administrada de AWSpara Amazon EBS en su cuenta (`aws/ebs`). Sin embargo, puede especificar una clave administrada por el cliente que puede crear y administrar.

Para utilizar una clave administrada por el cliente, debe dar permiso a Amazon EBS para usar la clave KMS en su nombre. Para obtener una lista de los permisos necesarios, consulte Permisos para los usuarios de IAM en la Guía del usuario de Amazon EC2 para instancias de Linux o Guía del usuario de Amazon EC2 para instancias de Windows.

> **Important**
>
> Amazon EBS solo admite claves KMS simétricas. No se puede utilizar una clave KMS asimétrica para cifrar un volumen de Amazon EBS. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Para cada volumen, Amazon EBS pide AWS KMS para generar una clave de datos única cifrada bajo la clave KMS que especifique. Amazon EBS almacena la clave de datos cifrada con el volumen. A continuación, al adjuntar el volumen a una instancia de Amazon EC2, Amazon EBS llama a AWS KMS para descifrar la clave de datos. Amazon EBS utiliza la clave de datos de texto no cifrado en la memoria del hipervisor para cifrar las operaciones de E/S de disco en el volumen. Para obtener más información, consulte Cómo funciona el cifrado de EBS en la Guía del usuario de Amazon EC2 para instancias de Linux o en la Guía del usuario de Amazon EC2 para instancias de Windows.

Contexto de cifrado de Amazon EBS

En sus solicitudes GenerateDataKeyWithoutPlaintexty en las de DecryptAWS KMS, Amazon EBS utiliza un contexto de cifrado con un par nombre-valor que identifica el volumen o la instantánea de la solicitud. El nombre en el contexto de cifrado no varía.

Un contexto de cifrado es un conjunto de pares de clave-valor que contienen datos no secretos arbitrarios. Cuando se incluye un contexto de cifrado en una solicitud para cifrar datos, AWS KMS vincula criptográficamente el contexto de cifrado a los datos cifrados. Para descifrar los datos, es necesario pasar el mismo contexto de cifrado.

Para todos los volúmenes y para las instantáneas cifradas creadas con la CreateSnapshotoperación Amazon EBS, Amazon EBS utiliza el ID del volumen como valor de contexto de cifrado. En el campo `requestParameters` de una entrada de registro de CloudTrail, el contexto de cifrado es similar al siguiente:

```
"encryptionContext": {
  "aws:ebs:id": "vol-0cfb133e847d28be9"
}
```

Para las instantáneas cifradas creadas con la operación Amazon CopySnapshotEC2, Amazon EBS utiliza el ID de la instantánea como valor de contexto de cifrado. En el campo `requestParameters` de una entrada de registro de CloudTrail, el contexto de cifrado es similar al siguiente:

```
"encryptionContext": {
  "aws:ebs:id": "snap-069a655b568de654f"
}
```

Detección de errores de Amazon EBS

Para crear un volumen de EBS cifrado o adjuntar el volumen a una instancia EC2, Amazon EBS y la infraestructura de Amazon EC2 deben poder usar la clave KMS especificada para el cifrado del volumen de EBS. Cuando la clave KMS no es utilizable, por ejemplo, cuando su estado clave no es `Enabled`: la creación del volumen o el adjunto al volumen fallan.

En este caso, Amazon EBS envía un evento a Amazon EventBridge (anteriormente CloudWatch Events) para notificarle el error. En EventBridge, puede establecer reglas que activen acciones automáticas en respuesta a estos eventos. Para obtener más información, consulte Amazon CloudWatch Events para Amazon EBS en la Guía del usuario de Amazon EC2 para instancias de Linux, especialmente en las siguientes secciones:

- Clave de cifrado no válida al asociar o volver a asociar un volumen
- Clave de cifrado no válida al crear el volumen

Para solucionar estos errores, compruebe que esté habilitada la clave KMS que ha especificado para el cifrado del volumen de EBS. Para ello, primero consulte la clave KMS para determinar su estado de clave actual (la columna Status (Estado) de la AWS Management Console). A continuación, consulte la información de uno estos enlaces:

- Si el estado de clave de la clave KMS está deshabilitado, habilítelo.
- Si el estado de clave de la clave KMS está pendiente de importación, importe el material de claves.
- Si el estado de clave de la clave KMS es pendiente de eliminación, cancele la eliminación de la clave.

Uso de AWS CloudFormation para crear volúmenes de Amazon EBS cifrados

Puede usar AWS CloudFormation para crear volúmenes de Amazon EBS cifrados. Para obtener más información, consulte AWS::EC2::Volume en la Guía del usuario de AWS CloudFormation.

Cómo Amazon Elastic Transcoder utiliza AWS KMS

Puede utilizar Amazon Elastic Transcoder para convertir archivos multimedia almacenados en un bucket de Amazon S3 en formatos que necesiten los reproductores de los consumidores. Los

archivos tanto de entrada como de salida pueden cifrarse y descifrarse. En las secciones siguientes se explica cómo se usa AWS KMS tanto ambos procesos.

Temas

Cifrado del archivo de entrada

Para poder usar Elastic Transcoder, debe crear un bucket de Amazon S3 y cargar un archivo multimedia en él. Puede cifrar el archivo antes de cargarlo mediante el cifrado del lado del cliente AES o después de cargarlo mediante el cifrado del lado del servidor de Amazon S3.

Si elige el cifrado del lado del cliente mediante AES, es responsable de cifrar el archivo antes de cargarlo en Amazon S3, y debe proporcionar acceso a Elastic Transcoder a la clave de cifrado. Para ello, use AWS KMS key AWS KMS simétrica para proteger la clave de cifrado AES que ha usado para cifrar el archivo multimedia.

Si se decide por el cifrado del lado del servidor, permite a Amazon S3 que realice las tareas de cifrado y descifrado de todos los archivos en su nombre. Puede configurar Amazon S3 para que use una de los tres tipos diferentes de claves de cifrado para proteger la clave de datos única empleada para cifrar su archivo:

- Una clave de Amazon S3, una clave de cifrado que Amazon S3 posee y administra. No es parte de su Cuenta de AWS.
- La Clave administrada de AWS para Amazon S3, una clave KMS que forma parte de su cuenta, pero que es creada y administrada por AWS
- Cualquier clave administrada por el cliente simétrica que cree mediante AWS KMS

> **Important**
>
> Para el cifrado del lado del cliente y del lado del servidor, Elastic Transcoder solo admite claves KMS simétricas. No puede usar una clave KMS asimétrica para cifrar los archivos de

Elastic Transcoder. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Puede habilitar el cifrado y especificar una clave mediante la consola de Amazon S3 o las API de Amazon S3 adecuadas. Para obtener más información sobre cómo Amazon S3 realiza cifrado, consulte Protección de datos mediante el cifrado del lado del servidor con las claves KMS (SSE-KMS) en la Guía del usuario de Amazon Simple Storage Service.

Cuando protege su archivo de entrada utilizando Clave administrada de AWS para Amazon S3 en su cuenta o una clave administrada por el cliente, Amazon S3 y AWS KMS interactúan de la siguiente manera:

1. Amazon S3 solicita una clave de datos en texto no cifrado y una copia de la clave de datos cifrada con la clave KMS especificada.
2. AWS KMS crea una clave de datos, la cifra con la clave KMS especificada y, a continuación, envía la clave de datos en texto no cifrado y la clave de datos cifrada a Amazon S3.
3. almacén usa la clave de datos en texto no cifrado para cifrar el archivo multimedia y, a continuación, almacena el archivo en el bucket de Amazon S3 especificado.
4. Amazon S3 almacena la clave de datos cifrada junto con el archivo multimedia cifrado.

Descifrado del archivo de entrada

Si elige el cifrado del lado del servidor de Amazon S3 para cifrar el archivo de entrada, Elastic Transcoder no descifra el archivo. En su lugar, Elastic Transcoder se basa en Amazon S3 para realizar el descifrado en función de la configuración que especifique al crear un trabajo y una canalización.

Está disponible la siguiente combinación de configuraciones.

Modo de cifrado	Clave de AWS KMS	Significado
S3	Predeterminado	Amazon S3 crea y administra las claves usadas para cifrar y descifrar el archivo multimedia. El proceso es opaco para el usuario.

Modo de cifrado	Clave de AWS KMS	Significado
`S3-AWS-KMS`	Predeterminado	Amazon S3 utiliza una clave de datos cifrada por la Clave administrada de AWS predeterminada para Amazon S3 en su cuenta para cifrar el archivo multimedia.
`S3-AWS-KMS`	Personalizado (con ARN)	Amazon S3 utiliza una clave de datos cifrada por la clave administrada por el cliente especificada para cifrar el archivo multimedia.

Cuando se especifica `S3-AWS-KMS`, Amazon S3 y AWS KMS colaboran de la siguiente manera para realizar el descifrado.

1. Amazon S3 envía la clave de datos cifrada a AWS KMS.
2. AWS KMS descifra la clave de datos mediante la clave KMS apropiada y, a continuación, envía la clave de datos en texto no cifrado a Amazon S3.
3. Amazon S3 descifrar usa la clave de datos en texto no cifrado para descifrar el texto cifrado.

Si elige el cifrado del lado del cliente utilizando una clave AES, Elastic Transcoder recupera el archivo codificado del bucket de Amazon S3 y lo descifra. Elastic Transcoder utiliza la clave KMS que haya especificado al crear la canalización para descifrar la clave AES y, a continuación, usa la clave AES para descifrar el archivo multimedia.

Cifrado del archivo de salida

Elastic Transcoder cifra el archivo de salida en función de cómo se especifique la configuración de cifrado al crear un trabajo y una canalización. Están disponibles las siguientes opciones.

Modo de cifrado	Clave de AWS KMS	Significado
S3	Predeterminado	Amazon S3 crea y administra las claves usadas para cifrar el archivo de salida.
S3-AWS-KMS	Predeterminado	Amazon S3 utiliza una clave de datos creada por AWS KMS y cifrada por Clave administrada de AWS para Amazon S3 en su cuenta.
S3-AWS-KMS	Personalizado (con ARN)	Amazon S3 utiliza una clave de datos cifrada mediante la clave administrada por el cliente y especificada por el ARN para cifrar el archivo multimedia.
AES-	Predeterminado	Elastic Transcoder usa la Clave administrada de AWS para Amazon S3 en su cuenta para descifrar la clave AES especificada que ha proporcionado y usa dicha clave para cifrar el archivo de salida.
AES-	Personalizado (con ARN)	Elastic Transcoder usa la clave administrada por el cliente y especificada por el ARN para descifrar la clave AES especificada que ha proporcionado y usa dicha clave para cifrar el archivo de salida.

Al especificar que se utilice la Clave administrada de AWS para Amazon S3 en su cuenta o una clave administrada por el cliente para cifrar el archivo de salida, Amazon S3 y AWS KMS interactúan de la siguiente manera:

1. Amazon S3 solicita una clave de datos en texto no cifrado y una copia de la clave de datos cifrada con la clave KMS especificada.
2. AWS KMS crea una clave de datos, la cifra con la clave KMS y envía la clave de datos en texto no cifrado y la clave de datos cifrada a Amazon S3.
3. Amazon S3 cifra el archivo multimedia con la clave de datos y lo almacena en el bucket de Amazon S3 especificado.
4. Amazon S3 almacena la clave de datos cifrada junto con el archivo multimedia cifrado.

Al especificar que la clave AES proporcionada se usará para cifrar el archivo de salida, la clave AES se debe cifrar utilizando una clave KMS en AWS KMS. Elastic Transcoder, AWS KMS y el usuario interactúan de la siguiente forma:

1. El usuario cifra la clave AES llamando a la operación Encrypt (Cifrado) en la API de AWS KMS. AWS KMS cifra la clave mediante la clave KMS especificada. Puede especificar qué clave KMS se usará cuando se cree la canalización.
2. El usuario especifica el archivo que contiene la clave AES cifrada al crear el trabajo de Elastic Transcoder.
3. Elastic Transcoder descifra la clave llamando a la operación Decrypt (Cifrado) de la API de AWS KMS, pasando la clave cifrada como texto cifrado.
4. Elastic Transcoder usa la clave AES descifrada para cifrar el archivo multimedia de salida y, a continuación, elimina la clave AES descifrada de la memoria. Solo la copia cifrada originalmente definida en el trabajo se guarda en el disco.
5. Puede descargar el archivo de salida cifrado y descifrarlo localmente mediante la clave AES original que ha definido.

> **Important**
>
> AWS nunca almacena las claves de cifrado privadas. Por lo tanto, es importante que administre sus claves de forma segura. Si las pierde, no podrá descifrar los datos.

Protección de contenido HLS

HTTP Live Streaming (HLS) es un protocolo de transmisión flexible. Elastic Transcoder admite HLS mediante la división del archivo de entrada en archivos individuales más pequeños denominados segmentos multimedia. Un conjunto de los correspondientes segmentos multimedia individuales contiene el mismo material codificado a distintas velocidades de bits, lo que permite que el reproductor seleccione el flujo que mejor se adapte al ancho de banda disponible. Elastic Transcoder también crea listas de reproducción que contienen los metadatos de los distintos segmentos que están disponibles para transmitir.

Al habilitar la protección de contenido HLS, cada segmento multimedia se cifra con una clave de cifrado AES-128. Cuando se visualiza el contenido, el reproductor descarga la clave y descifra los segmentos multimedia durante el proceso de reproducción.

Se usan dos tipos de claves: una clave KMS y una clave de datos. Debe crear una clave KMS para usarla en el cifrado y descifrado de la clave de datos. Elastic Transcoder utiliza la clave de datos para cifrar y descifrar los segmentos multimedia. La clave de datos debe ser AES-128. Todas las variaciones y segmentos del mismo contenido se cifran con la misma clave de datos. Puede proporcionar una clave de datos o dejar que Elastic Transcoder la cree automáticamente.

La clave KMS se puede utilizar para cifrar la clave de datos en los puntos siguientes:

- Si proporciona su propia clave de datos, deberá cifrarla antes de pasarla a Elastic Transcoder.
- Si solicita que Elastic Transcoder genere la clave de datos, Elastic Transcoder cifrará la clave de datos automáticamente.

La clave KMS se puede utilizar para descifrar la clave de datos en los puntos siguientes:

- Elastic Transcoder descifra la clave de datos proporcionada cuando necesita usarla para cifrar el archivo de salida o para descifrar el archivo de entrada.
- Descifra una clave de datos generada por Elastic Transcoder y la usa para descifrar los archivos de salida.

Para obtener más información, consulte Protección de contenido HLS en la Guía del desarrollador de Amazon Elastic Transcoder.

Contexto de cifrado de Elastic Transcoder

Un contexto de cifrado es un conjunto de pares de clave-valor que contienen datos no secretos arbitrarios. Cuando se incluye un contexto de cifrado en una solicitud para cifrar datos, AWS KMS vincula criptográficamente el contexto de cifrado a los datos cifrados. Para descifrar los datos, es necesario pasar el mismo contexto de cifrado.

Elastic Transcoder utiliza el mismo contexto de cifrado en todas las solicitudes a la API de AWS KMS para la generación de claves de datos, el cifrado y el descifrado.

```
"service" : "elastictranscoder.amazonaws.com"
```

El contexto de cifrado se escribe en CloudTrail los registros para ayudarle a entender cómo se utilizó una clave AWS KMS KMS determinada. En el `requestParameters` campo de un archivo de CloudTrail registro, el contexto de cifrado es similar al siguiente:

```
"encryptionContext": {
  "service" : "elastictranscoder.amazonaws.com"
}
```

Para obtener más información sobre cómo configurar los trabajos de Elastic Transcoder para usar una de las opciones de cifrado admitidas, consulte Opciones de cifrado de datos en la Guía para desarrolladores de Amazon Elastic Transcoder.

Cómo Amazon EMR utiliza AWS KMS

Cuando utilice un clúster de Amazon EMR, puede configurarlo para cifrar los datos en reposo antes de guardarlos en una ubicación de almacenamiento persistente. Puede cifrar los datos en reposo en el sistema de archivos EMR (EMRFS), en los volúmenes de almacenamiento de nodos del clúster o en ambos. Para cifrar los datos en reposo, puede utilizar una AWS KMS key. En los siguientes temas se explica cómo un clúster Amazon EMR utiliza una clave KMS para cifrar los datos en reposo.

> **Important**
>
> Amazon EMR solo admite claves KMS simétricas. No se puede utilizar una clave KMS asimétrica para cifrar datos en reposo en un clúster de Amazon EMR. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Los clústeres de Amazon EMR también cifran los datos en tránsito, lo que significa que el clúster cifra los datos antes de enviarlos a través de la red. No puede utilizar una clave KMS para cifrar los datos en tránsito. Para obtener más información, consulte Cifrado de datos en tránsito en la Guía de administración de Amazon EMR.

Para obtener más información sobre todas las opciones de cifrado disponibles en Amazon EMR, consulte Opciones de cifrado en la Guía de administración de Amazon EMR.

Temas

- Cifrar datos en el sistema de archivos EMR (EMRFS)
- Cifrar datos en los volúmenes de almacenamiento de los nodos de clúster
- Contexto de cifrado

Cifrar datos en el sistema de archivos EMR (EMRFS)

Los clústeres de Amazon EMR usan dos sistemas de archivos distribuidos:

- Hadoop Distributed File System (HDFS). El cifrado HDFS no utiliza una clave KMS en AWS KMS.
- Sistema de archivos EMR (EMRFS). EMRFS es una implementación de HDFS que permite a los clústeres de Amazon EMR almacenar datos en Amazon Simple Storage Service (Amazon S3). EMRFS admite cuatro opciones de cifrado, dos de las cuales utilizan una clave KMS en AWS KMS. Para obtener más información acerca de las cuatro opciones de cifrado de EMRFS, consulte Opciones de cifrado en la Guía de administración de Amazon EMR.

Las dos opciones de cifrado de EMRFS que utilizan una clave KMS usan las siguientes características de cifrado que ofrece Amazon S3:

- Protección de los datos mediante el cifrado del lado del servidor con AWS Key Management Service (SSE-KMS). El clúster de Amazon EMR envía datos a Amazon S3. Amazon S3 utiliza una clave KMS para cifrar los datos antes de guardarlos en un bucket de S3. Para obtener más información sobre cómo funciona, consulte Proceso de cifrar datos en EMRFS con SSE-KMS.
- Protección de datos mediante el cifrado del lado del cliente (CSE-KMS). Los datos de Amazon EMR de Amazon se cifran bajo un AWS KMS key antes de su envío a Amazon S3 para el almacenamiento. Para obtener más información sobre cómo funciona, consulte Proceso de cifrar datos en EMRFS con CSE-KMS.

Al configurar un clúster de Amazon EMR para cifrar datos en EMRFS con una clave KMS, hay que elegir la clave KMS que se desea que utilice Amazon S3 o el clúster de Amazon EMR. Con SSE-KMS, puede elegir la Clave administrada de AWS para Amazon S3 con el alias aws/s3, o una clave simétrica administrada por el cliente que haya creado. Con el cifrado del lado del cliente, debe elegir una clave simétrica administrada por el cliente que cree. Si elige una clave administrada por el cliente, debe asegurarse de que el clúster de Amazon EMR tiene permiso para utilizar la clave KMS. Para obtener más información, consulte Uso de AWS KMS keys para el cifrado en la Guía de administración de Amazon EMR.

Tanto para el cifrado del lado del servidor como del lado del cliente, la clave KMS que elija es la clave raíz en un flujo de trabajo de cifrado de sobre. Los datos se encriptan con una clave de datos única que se cifra bajo la clave KMS en AWS KMS. Los datos cifrados y una copia cifrada de su clave de datos se almacenan juntos como un solo objeto cifrado en un bucket de S3. Para obtener más información sobre cómo funciona, consulte los siguientes temas.

Temas

- Proceso de cifrar datos en EMRFS con SSE-KMS
- Proceso de cifrar datos en EMRFS con CSE-KMS

Proceso de cifrar datos en EMRFS con SSE-KMS

Al configurar un clúster de Amazon EMR para usar SSE-KMS, el proceso de cifrado funciona del siguiente modo:

1. El clúster envía datos a Amazon S3 para almacenarlos en un bucket de S3.
2. Amazon S3 envía una GenerateDataKeysolicitud aAWS KMS, especificando el ID de clave de KMS que eligió al configurar el clúster para usar SSE-KMS. La solicitud incluye el contexto de cifrado; para obtener más información, consulte Contexto de cifrado.
3. AWS KMS genera una clave de cifrado de datos (clave de datos) única y, a continuación, envía dos copias de esta clave de datos a Amazon S3. Una copia está sin cifrar (texto no cifrado) y la otra se cifra con la clave KMS.
4. Amazon S3 utiliza la clave de datos de texto no cifrado para cifrar los datos que ha recibido en el paso 1 y, a continuación, elimina la clave de datos de texto no cifrado de la memoria tan pronto como sea posible después de utilizarla.
5. Amazon S3 almacena los datos cifrados y la copia cifrada de la clave de datos como un solo objeto cifrado en un bucket de S3.

El proceso de descifrado funciona de la siguiente manera:

1. El clúster solicita un objeto de datos cifrado de un bucket de S3.
2. Amazon S3 extrae la clave de datos cifrada del objeto de S3 y, a continuación, se la envía a AWS KMS con una solicitud Decrypt (Descifrado). La solicitud incluye un contexto de cifrado.
3. AWS KMS descifra la clave de datos cifrada con la misma clave KMS que se utilizó para cifrarla y, a continuación, envía la clave de datos descifrada (texto no cifrado) a Amazon S3.
4. Amazon S3 utiliza la clave de datos de texto no cifrado para descifrar los datos cifrados y, a continuación, elimina la clave de datos de texto no cifrado de la memoria tan pronto como sea posible después de utilizarla.
5. Amazon S3 envía los datos descifrados al clúster.

Proceso de cifrar datos en EMRFS con CSE-KMS

Al configurar un clúster de Amazon EMR para usar CSE-KMS, el proceso de cifrado funciona del siguiente modo:

1. Cuando esté listo para almacenar datos en Amazon S3, el clúster envía una GenerateDataKeysolicitud a AWS KMS la que especifica el ID de clave de la clave de KMS que eligió al configurar el clúster para usar CSE-KMS. La solicitud incluye el contexto de cifrado; para obtener más información, consulte Contexto de cifrado.
2. AWS KMS genera una clave de cifrado de datos (clave de datos) única y, a continuación, envía dos copias de esta clave de datos al clúster. Una copia está sin cifrar (texto no cifrado) y la otra copia se cifra con la clave KMS.
3. El clúster utiliza la clave de datos de texto no cifrado para cifrar los datos y, a continuación, elimina la clave de datos de texto no cifrado de la memoria tan pronto como sea posible después de utilizarla.
4. El clúster combina los datos cifrados y la copia cifrada de la clave de datos en un solo objeto cifrado.
5. El clúster envía el objeto cifrado a Amazon S3 para almacenarlo.

El proceso de descifrado funciona de la siguiente manera:

1. El clúster solicita el objeto de datos cifrado de un bucket de S3.
2. Amazon S3 envía el objeto cifrado al clúster.

3. El clúster extrae la clave de datos cifrada del objeto cifrado y, a continuación, se la envía a AWS KMS con una solicitud Decrypt. La solicitud incluye el contexto de cifrado.
4. AWS KMS descifra la clave de datos cifrada con la misma clave KMS que se utilizó para cifrarla y, a continuación, envía la clave de datos descifrada (texto no cifrado) al clúster.
5. El clúster utiliza la clave de datos de texto no cifrado para descifrar los datos cifrados y, a continuación, elimina la clave de datos de texto no cifrado de la memoria tan pronto como sea posible después de utilizarla.

Cifrar datos en los volúmenes de almacenamiento de los nodos de clúster

Un clúster de Amazon EMR es una colección de instancias de Amazon Elastic Compute Cloud (Amazon EC2). Cada instancia del clúster se denomina un nodo de clúster o nodo. Cada nodo puede tener dos tipos de volúmenes de almacenamiento: volúmenes de almacén de instancias y volúmenes de Amazon Elastic Block Store (Amazon EBS). Puede configurar el clúster para utilizar la Configuración de clave unificada de Linux (LUKS) para cifrar ambos tipos de volúmenes de almacenamiento en los nodos (pero no el volumen de arranque de cada nodo). Se denomina cifrado de disco local.

Al habilitar el cifrado de disco local para un clúster, puede cifrar la clave LUKS con una clave KMS en AWS KMS. Debe elegir una clave administrada por el cliente que cree; no puede utilizar una Clave administrada de AWS. Si elige una clave administrada por el cliente, debe asegurarse de que el clúster de Amazon EMR tiene permiso para utilizar la clave KMS. Para obtener más información, consulte Uso de AWS KMS keys para el cifrado en la Guía de administración de Amazon EMR.

Si habilita el cifrado del disco local mediante una clave KMS, el proceso de cifrado funciona del siguiente modo:

1. Cuando se lanza cada nodo del clúster, envía una GenerateDataKeysolicitud a AWS KMS la que especifica el ID de clave de la clave de KMS que eligió al habilitar el cifrado de disco local para el clúster.
2. AWS KMS genera una clave de cifrado de datos (clave de datos) única y, a continuación, envía dos copias de esta clave de datos al nodo. Una copia está sin cifrar (texto no cifrado) y la otra copia se cifra con la clave KMS.
3. El nodo utiliza una versión de la codificación de base64 de la clave de datos de texto no cifrado como la contraseña que protege la clave LUKS. El nodo guarda la copia cifrada de la clave de datos en su volumen de arranque.

4. Si el nodo se reinicia, el nodo reiniciado envía la clave de datos cifrada a AWS KMS con una solicitud Decrypt.
5. AWS KMS descifra la clave de datos cifrada con la misma clave KMS que se utilizó para cifrarla y, a continuación, envía la clave de datos descifrada (texto no cifrado) al nodo.
6. El nodo utiliza la versión de la codificación de base64 de la clave de datos de texto no cifrado como la contraseña para desbloquear la clave LUKS.

Contexto de cifrado

Cada servicio de AWS que está integrado con AWS KMS puede especificar el contexto de cifrado cuando el servicio utiliza AWS KMS para generar claves de datos o para cifrar o descifrar datos. El contexto de cifrado consta de información autenticada adicional que usa AWS KMS para comprobar la integridad de los datos. Cuando un servicio especifica el contexto de cifrado para una operación de cifrado, debe especificar el mismo contexto de cifrado para la operación de descifrado correspondiente; de lo contrario, el descifrado no se realizará correctamente. El contexto de cifrado también se escribe en los archivos de registro de AWS CloudTrail, lo que puede ayudarle a entender por qué se ha usado una determinada clave KMS.

En la siguiente sección se explica el contexto de cifrado que se utiliza en cada situación de cifrado de Amazon EMR que utiliza una clave KMS.

Contexto de cifrado para el cifrado de EMRFS con SSE-KMS

Con SSE-KMS, el clúster de Amazon EMR envía datos a Amazon S3 y, a continuación, Amazon S3 utiliza una clave KMS para cifrar los datos antes de guardarlos en un bucket de S3. En este caso, Amazon S3 utiliza el nombre de recurso de Amazon (ARN) del objeto S3 como contexto de cifrado para cada GenerateDataKeysolicitud de Decrypt a la que envía. AWS KMS El siguiente ejemplo muestra una representación JSON del contexto de cifrado que usa Amazon S3.

```
{ "aws:s3:arn" : "arn:aws:s3:::S3_bucket_name/S3_object_key" }
```

Contexto de cifrado para el cifrado de EMRFS con CSE-KMS

Con CSE-KMS, el clúster de Amazon EMR utiliza una clave KMS para cifrar los datos antes de enviarlos a Amazon S3 para almacenarlos. En este caso, el clúster utiliza el nombre de recurso de Amazon (ARN) de la clave de KMS como contexto de cifrado con cada GenerateDataKeysolicitud de Decrypt a la que envía. AWS KMS El siguiente ejemplo muestra una representación JSON del contexto de cifrado que usa el clúster.

```
{ "kms_cmk_id" : "arn:aws:kms:us-
east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef" }
```

Contexto de cifrado para el cifrado de disco local con LUKS

Cuando un clúster de Amazon EMR utiliza el cifrado de disco local con LUKS, los nodos del clúster no especifican el contexto de cifrado con las solicitudes GenerateDataKeyy Decrypt a las que envían. AWS KMS

¿Cómo AWS Nitro Enclaves utiliza AWS KMS?

AWS KMS admite la certificación criptográfica para AWS Nitro Enclaves. Las aplicaciones compatibles con AWS Nitro Enclaves hacen una llamada a las siguientes operaciones criptográficas de AWS KMS con un documento de certificación firmado para el enclave. Estas API de AWS KMS verifican que el documento de certificación proviene de un enclave de Nitro. A continuación, en lugar de devolver datos de texto sin formato en la respuesta, estas API cifran el texto sin formato con la clave pública del documento de certificación y devuelven texto cifrado solo con la clave privada correspondiente en el enclave.

- Decrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateRandom

En la siguiente tabla, se muestra en qué se diferencia la respuesta a las solicitudes a los enclaves de Nitro de la respuesta estándar para cada operación de API.

Operación de AWS KMS	Respuesta estándar	Respuesta para AWS Nitro Enclaves
`Decrypt`	Devuelve datos de texto sin formato	Devuelve los datos de texto sin formato cifrados por la clave pública del documento de certificación

Operación de AWS KMS	Respuesta estándar	Respuesta para AWS Nitro Enclaves
`GenerateDataKey`	Devuelve una copia en texto sin formato de la clave de datos (También devuelve una copia de la clave de datos cifrada por una clave de KMS)	Devuelve una copia de la clave de datos cifrada por la clave pública del documento de certificación (También devuelve una copia de la clave de datos cifrada por una clave de KMS)
`GenerateDataKeyPair`	Devuelve una copia de texto sin formato de la clave privada (También devuelve la clave pública y una copia de la clave privada cifrada por una clave de KMS)	Devuelve una copia de la clave privada cifrada por la clave pública del documento de certificación (También devuelve la clave pública y una copia de la clave privada cifrada por una clave de KMS)
`GenerateRandom`	Devuelve una cadena de bytes aleatoria	Devuelve la cadena de bytes aleatoria cifrada por la clave pública del documento de certificación

AWS KMS también admite claves de condición de política que puede utilizar para permitir operaciones de enclave en una clave de AWS KMS sólo cuando el documento de certificación tiene el contenido especificado. También puede supervisar las solicitudes a AWS KMS de su enclave de Nitro en sus registros de AWS CloudTrail.

Temas

- Cómo llamar a las API de AWS KMS para un enclave de Nitro
- Claves de condición de AWS KMS para Nitro Enclaves de AWS
- Supervisión de las solicitudes para enclaves de Nitro

Cómo llamar a las API de AWS KMS para un enclave de Nitro

Para llamar a las API de AWS KMS para un enclave de Nitro, use el parámetro `Recipient` de la solicitud para proporcionar el documento de certificación firmado del enclave y el algoritmo de cifrado que se utilizará con la clave pública del enclave. Cuando una solicitud incluye el parámetro `Recipient` con un documento de certificación firmado, la respuesta incluye un campo `CiphertextForRecipient` con el texto cifrado mediante la clave pública. El campo de texto sin formato es nulo o está vacío.

El parámetro `Recipient` debe especificar un documento de certificación firmado de un enclave de AWS Nitro. AWS KMS se basa en la firma digital del documento de certificación del enclave para demostrar que la clave pública en la solicitud procede de un enclave válido. No puede proporcionar su propio certificado para firmar digitalmente el documento de certificación.

Para especificar el parámetro `Recipient`, utilice el SDK de AWS Nitro Enclaves o cualquier otro SDK de AWS. El SDK de AWS Nitro Enclaves, que solo es compatible con un enclave de Nitro, agrega automáticamente el parámetro `Recipient` y sus valores a cada solicitud de AWS KMS. Si quiere realizar solicitudes para enclaves de Nitro en los SDK de AWS, debe especificar el parámetro `Recipient` y sus valores. La compatibilidad con la certificación criptográfica del enclave de Nitro en los SDK de AWS se introdujo en marzo de 2023.

AWS KMS también admite claves de condición de política que puede utilizar para permitir operaciones de enclave en una clave de AWS KMS sólo cuando el documento de certificación tiene el contenido especificado. También puede supervisar las solicitudes a AWS KMS de su enclave de Nitro en sus registros de AWS CloudTrail.

Para obtener información detallada sobre el `Recipient` parámetro y el campo de `CiphertextForRecipient` respuesta de AWS, consulte Decrypt, GenerateDataKeyGenerateDataKeyPair, y GenerateRandomlos temas de la AWS Key Management ServiceAPI Reference, el SDK de AWSNitro Enclaves o cualquier SDK. AWS Para obtener información sobre cómo configurar los datos y las claves de datos para el cifrado, consulte Usar la certificación criptográfica con AWS KMS.

Claves de condición de AWS KMS para Nitro Enclaves de AWS

Puede especificar claves de condición en las políticas de claves y políticas de IAM que controlan el acceso a los recursos de AWS KMS. Las instrucciones de política que incluyen una clave de condición solo entran en vigor cuando se cumplen sus condiciones.

AWS KMSproporciona claves de condición que limitan los permisos para las GenerateRandomoperaciones de Decrypt GenerateDataKey, GenerateDataKeyPair, y en función del contenido del documento de certificación firmado en la solicitud. Estas claves de condición solo funcionan cuando la solicitud de una operación de AWS KMS incluye el parámetro `Recipient` junto con un documento de certificación válido de un enclave de AWS Nitro. Para especificar el parámetro `Recipient`, utilice el SDK de AWS Nitro Enclaves o cualquier otro SDK de AWS.

Estas claves de condición de AWS KMS específicas del enclave son válidas en las declaraciones de políticas de claves y en las declaraciones de políticas de IAM aunque no aparezcan en la consola de IAM ni en la Referencia de autorizaciones de servicio de IAM.

km: 384 RecipientAttestation ImageSha

Claves de condición de AWS KMS	Tipo de condición	Tipo de valor	Operaciones de API	Tipo de política

`kms:RecipientAttestation:ImageSha384`	Cadena	Valor único	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Políticas de claves y políticas de IAM

La clave de condición `kms:RecipientAttestation:ImageSha384` controla el acceso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` y `GenerateRandom` con una clave de KMS cuando el resumen de la imagen del documento de certificación firmado de la solicitud coincide con el valor de la clave de condición. El valor `ImageSha384` corresponde a PCR0 en el documento de certificación. Esta clave de condición solo entra en vigor cuando el parámetro `Recipient` de la solicitud especifica un documento de certificación firmado para un enclave de AWS Nitro.

Este valor también se incluye en CloudTraillos eventos relacionados con las solicitudes de AWS KMS enclaves de Nitro.

> **Note**
>
> Esta clave de condición es válida en las declaraciones de política de claves y en las declaraciones de política de IAM aunque no aparezca en la consola de IAM ni en la Referencia de autorizaciones de servicio de IAM.

Por ejemplo, la siguiente declaración de política clave permite al `data-processing` rol usar la clave KMS para las operaciones de descifrado GenerateDataKeyGenerateDataKeyPair, y. GenerateRandom La clave de condición `kms:RecipientAttestation:ImageSha384` permite las operaciones solo cuando el valor de resumen de imagen (PCR0) del documento de certificación en la solicitud coincida con el valor de resumen de imagen de la condición. Esta clave de condición solo entra en vigor cuando el parámetro `Recipient` de la solicitud especifica un documento de certificación firmado para un enclave de AWS Nitro.

Si la solicitud no incluye un documento de certificación válido de un enclave de AWS Nitro, se deniega el permiso porque esta condición no se cumple.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": [
    "kms:Decrypt",
    "kms:GenerateDataKey",
    "kms:GenerateDataKeyPair",
    "kms:GenerateRandom"
  ],
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:ImageSha384":
 "9fedcba8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdef2abcdef3a
    }
  }
}
```

kms ::PCR RecipientAttestation <PCR_ID>

Claves de condición de AWS KMS	Tipo de condición	Tipo de valor	Operaciones de API	Tipo de política

`kms:RecipientAttestation:PCR<PCR_ID>`	Cadena	Valor único	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				Políticas de claves y políticas de IAM

La clave de condición `kms:RecipientAttestation:PCR<PCR_ID>` controla el acceso a `Decrypt`, `GenerateDataKey`, `GenerateDataKeyPair` y `GenerateRandom` con una clave de KMS solo cuando los registros de configuración de la plataforma (PCR) del documento de certificación firmado en la solicitud coincidan con el valor de la clave de condición. Esta clave de condición solo entra en vigor cuando el parámetro `Recipient` de la solicitud especifica un documento de certificación firmado de un enclave de AWS Nitro.

Este valor también se incluye en CloudTraillos eventos que representan solicitudes de enclaves AWS KMS de Nitro.

> **Note**
>
> Esta clave de condición es válida en las declaraciones de política de claves y en las declaraciones de política de IAM aunque no aparezca en la consola de IAM ni en la Referencia de autorizaciones de servicio de IAM.

Para especificar un valor de PCR, utilice el siguiente formato. Concatene el ID de PCR con el nombre de la clave de condición. El valor de PCR debe ser una cadena hexadecimal en minúsculas de hasta 96 bytes.

```
"kms:RecipientAttestation:PCRPCR_ID": "PCR_value"
```

Por ejemplo, la siguiente clave de condición especifica un valor particular para PCR1, que corresponde al hash del kernel utilizado para el enclave y el proceso de arranque.

```
kms:RecipientAttestation:PCR1:
 "0x1abcdef2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef
```

Por ejemplo, la siguiente declaración de política de claves permite al rol `data-processing` utilizar la clave de KMS para la operación Decrypt.

La clave de condición `kms:RecipientAttestation:PCR` en esta declaración permite la operación solo cuando el valor PCR1 del documento de conformidad firmado en la solicitud coincide con el valor `kms:RecipientAttestation:PCR1` de la condición. Use el operador de política `StringEqualsIgnoreCase` para requerir una comparación entre mayúsculas y minúsculas de los valores de PCR.

Si la solicitud no incluye un documento de certificación, se deniega el permiso porque esta condición no se cumple.

```
{
  "Sid" : "Enable enclave data processing",
  "Effect" : "Allow",
  "Principal" : {
    "AWS" : "arn:aws:iam::111122223333:role/data-processing"
  },
  "Action": "kms:Decrypt",
  "Resource" : "*",
  "Condition": {
    "StringEqualsIgnoreCase": {
      "kms:RecipientAttestation:PCR1":
 "0x1de4f2dcf774f6e3b679f62e5f120065b2e408dcea327bd1c9dddaea6664e7af79355814748447674530 82c6f15
    }
  }
}
```

Supervisión de las solicitudes para enclaves de Nitro

Puedes usar tus AWS CloudTrail registros para monitorear Decrypt, GenerateDataKeyGenerateDataKeyPair, y GenerateRandomlas operaciones de un AWS enclave

de Nitro. En estas entradas de registro, el campo `additionalEventData` tiene un campo `recipient` con el ID del módulo (`attestationDocumentModuleId`), el resumen de imagen (`attestationDocumentEnclaveImageDigest`) y los registros de configuración de la plataforma (PCR) del documento de certificación de la solicitud. Estos campos se incluyen solo cuando el parámetro `Recipient` de la solicitud especifica un documento de certificación firmado desde un enclave de AWS Nitro.

El ID del módulo es el ID del enclave de Nitro. El resumen de la imagen es el hash SHA384 de la imagen del enclave. Puede utilizar el resumen de la imagen y los valores de PCR en condiciones para las políticas de claves y las políticas de IAM. Para obtener información sobre las PCR, consulte Where to get an enclave's measurements en la Guía del usuario de AWS Nitro Enclaves.

En esta sección se muestra un ejemplo de entrada de CloudTrail registro para cada una de las solicitudes de enclave de Nitro admitidas. AWS KMS

Decrypt (para un enclave)

En el ejemplo siguiente, se muestra una entrada de registro de AWS CloudTrail de una operación Decrypt para un enclave de AWS Nitro.


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2020-07-27T22:58:24Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
```

```
    "additionalEventData": {
        "recipient": {
            "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
            "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
            "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
            "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
            "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
            "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
            "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
        }
    },
    "requestID": "b4a65126-30d5-4b28-98b9-9153da559963",
    "eventID": "e5a2f202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKey (para un enclave)

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro de una GenerateDataKeyoperación para un enclave de AWS Nitro.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:40Z",
    "eventSource": "kms.amazonaws.com",
```

```
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
        "numberOfBytes": 32
    },
    "responseElements": null,
    "additionalEventData": {
        "recipient": {
            "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
            "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
            "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
            "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
            "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
            "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
            "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
        }
    },
    "requestID": "e0eb83e3-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "a9dea4f9-8395-46c0-942c-f509c02c2b71",
    "readOnly": true,
    "resources": [{
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
        "accountId": "111122223333"
    }],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateDataKeyPair (para un enclave)

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro de una GenerateDataKeyPairoperación para un enclave de AWS Nitro.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::111122223333:user/Alice",
```

```
            "accountId": "111122223333",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice"
    },
    "eventTime": "2020-07-27T18:57:57Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyPair",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": {
        "keyPairSpec": "RSA_3072",
        "encryptionContext": {
            "Project": "Alpha"
        },
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "responseElements": null,
    "additionalEventData": {
        "recipient": {
            "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
            "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
            "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
            "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
            "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
            "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
            "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
        }
    },
    "requestID": "52fb127b-0fe5-42bb-8e5e-f560febde6b0",
    "eventID": "9b6bd6d2-529d-4890-a949-593b13800ad7",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

GenerateRandom (para un enclave)

El siguiente ejemplo muestra una entrada de AWS CloudTrail registro de una GenerateRandomoperación para un enclave de AWS Nitro.

```
{
    "eventVersion": "1.02",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-11-04T00:52:37Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateRandom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "recipient": {
            "attestationDocumentModuleId": "i-123456789abcde123-enc123456789abcde12",
            "attestationDocumentEnclaveImageDigest": "<AttestationDocument.PCR0>",
            "attestationDocumentEnclavePCR1": "<AttestationDocument.PCR1>",
            "attestationDocumentEnclavePCR2": "<AttestationDocument.PCR2>",
            "attestationDocumentEnclavePCR3": "<AttestationDocument.PCR3>",
            "attestationDocumentEnclavePCR4": "<AttestationDocument.PCR4>",
            "attestationDocumentEnclavePCR8": "<AttestationDocument.PCR8>"
        }
    },
    "requestID": "df1e3de6-63bc-11e4-bc2b-4198b6150d5c",
    "eventID": "239cb9f7-ae05-4c94-9221-6ea30eef0442",
    "readOnly": true,
    "resources": [],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

¿Cómo Amazon Redshift utiliza AWS KMS?

En este tema se explica cómo Amazon Redshift utiliza AWS KMS para cifrar los datos.

Temas

- Cifrado de Amazon Redshift
- Contexto de cifrado

Cifrado de Amazon Redshift

Un almacén de datos de Amazon Redshift es una colección de recursos de computación denominados nodos que están organizados en un grupo llamado clúster. Cada clúster ejecuta un motor Amazon Redshift y contiene una o más bases de datos.

Amazon Redshift usa una arquitectura de cuatro niveles basada en claves para el cifrado. La arquitectura consta de claves de cifrado de datos, una clave de base de datos, una clave de clúster y una clave maestra. Puede utilizar una AWS KMS key como clave raíz.

Las claves de cifrado de datos cifran los bloques de datos del clúster. A cada bloque de datos se le asigna una clave AES-256 generada aleatoriamente. Estas claves se cifran mediante la clave de base de datos del clúster.

La clave de base de datos cifra las claves de cifrado de datos del clúster. La clave de base de datos es una clave AES-256 generada aleatoriamente. Se almacena en disco en una red diferente del clúster de Amazon Redshift y se pasa al clúster a través de un canal seguro.

La clave del clúster cifra la clave de base de datos del clúster de Amazon Redshift. Puede usar AWS KMS, AWS CloudHSM o un módulo de seguridad por hardware (HSM) externo para administrar la clave del clúster. Consulte la documentación sobre cifrado de base de datos de Amazon Redshift para obtener más información.

Puede solicitar el cifrado marcando la casilla correspondiente en la consola de Amazon Redshift. Puede especificar una clave administrada por el cliente para usarla seleccionando una en la lista que aparece debajo del cuadro de cifrado. Si no especifica una clave administrada por el cliente, Amazon Redshift utiliza el Clave administrada de AWS para Amazon Redshift en tu cuenta.

> **Important**
>
> Amazon Redshift solo admite claves KMS de cifrado simétricas. No se puede utilizar una clave KMS asimétrica en un flujo de trabajo de Amazon Redshift cifrado. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Contexto de cifrado

Cada servicio que está integrado con AWS KMS especifica un contexto de cifrado cuando se solicitan claves de datos, cifrado y descifrado. El contexto de cifrado es información autenticada adicional (AAD) que usa AWS KMS para comprobar la integridad de los datos. Es decir, cuando se especifica un contexto de cifrado para una operación de cifrado, el servicio también lo especifica en la operación de descifrado; de lo contrario, el descifrado no se realizará correctamente. Amazon Redshift utiliza el ID de clúster y la hora de creación para el contexto de cifrado. En el `requestParameters` campo de un archivo de CloudTrail registro, el contexto de cifrado tendrá un aspecto similar al siguiente.

```
"encryptionContext": {
    "aws:redshift:arn": "arn:aws:redshift:region:account_ID:cluster:cluster_name",
    "aws:redshift:createtime": "20150206T1832Z"
},
```

Puede buscar el nombre del clúster en sus CloudTrail registros para saber qué operaciones se realizaron mediante una AWS KMS key (clave KMS). Las operaciones incluyen el cifrado del clúster, el descifrado del clúster y la generación de claves de datos.

¿Cómo Amazon Relational Database Service (Amazon RDS) utiliza AWS KMS?

Puede utilizar el Amazon Relational Database Service (Amazon RDS) para configurar, utilizar y escalar una base de datos relacional en la nube. Puede cifrar sus recursos de Amazon RDS con una clave Clave administrada de AWS o con una clave gestionada por el cliente. 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.

Para obtener información detallada sobre cómo Amazon RDS usa las claves de KMS para proteger sus recursos, consulte Cifrar los recursos de Amazon RDS y la administración de claves AWS KMS en la Guía del usuario de Amazon RDS.

Cómo AWS Secrets Manager usa AWS KMS

AWS Secrets Manager es un servicio de AWS que cifra y almacena secretos, los descifra de manera transparente y los devuelve en texto sin cifrar. Se ha diseñado especialmente para almacenar secretos de aplicación, como, por ejemplo, credenciales de inicio de sesión, que cambian periódicamente y no deben codificarse de forma rígida o almacenarse en texto sin formato en la aplicación. En lugar de credenciales de codificación rígida o búsquedas de tabla, la aplicación llama a Secrets Manager.

Secrets Manager también admite características que rotan periódicamente los secretos asociados con bases de datos de uso común. Siempre cifra secretos recién rotados antes de que se almacenen.

Secrets Manager se integra con AWS Key Management Service (AWS KMS) para cifrar todas las versiones de cada valor secreto con una clave de datos única que esté protegida por una AWS KMS key. Esta integración protege sus secretos bajo claves de cifrado que nunca dejan AWS KMS sin cifrar. También permite establecer permisos personalizados en la clave KMS y auditar las operaciones que generan, cifran y descifran las claves de datos que protegen sus secretos.

Para obtener información acerca de cómo Secrets Manager utiliza las claves KMS para proteger sus secretos, consulteCifrar y descifrar secretos en laAWS Secrets ManagerGuía del usuario.

Cómo Amazon Simple Email Service (Amazon SES) utiliza AWS KMS

Puede utilizar Amazon Simple Email Service (Amazon SES) para recibir el correo electrónico y, si lo desea, para cifrar los mensajes de correo electrónico recibidos antes de almacenarlos en un bucket de Amazon Simple Storage Service (Amazon S3) que haya elegido. Al configurar Amazon SES para cifrar los mensajes de correo electrónico, debe elegir la AWS KMS AWS KMS key con la que Amazon SES cifra los mensajes. Puede elegir la Clave administrada de AWS para Amazon SES (su alias es `aws/ses`) o puede elegir una clave administrada por el cliente simétrica que haya creado en AWS KMS.

> **Important**
>
> Amazon SES sólo admite claves simétricas de KMS. No puede utilizar una clave asimétrica de KMS para cifrar sus mensajes de correo electrónico de Amazon SES. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Para obtener más información sobre la recepción de correo electrónico con Amazon SES, vaya a Recepción de correo electrónico con Amazon SES en la Guía Amazon Simple Email Service para desarrolladores.

Temas

- Información general del cifrado de Amazon SES utilizando AWS KMS
- Contexto de cifrado de Amazon SES
- Dar permiso a Amazon SES para utilizar su AWS KMS key
- Obtener y descifrar mensajes de correo electrónico

Información general del cifrado de Amazon SES utilizando AWS KMS

Al configurar Amazon SES para recibir correo electrónico y cifrar los mensajes de correo electrónico antes de guardarlos en su bucket de S3, el proceso funciona del siguiente modo:

1. Se crea una regla de recepción para Amazon SES, especificando la acción de S3, un bucket de S3 para el almacenamiento y una AWS KMS key para el cifrado.
2. Amazon SES recibe un mensaje de correo electrónico que coincide con la regla de recepción.
3. Amazon SES solicita una clave de datos única cifrada con la clave KMS que ha especificado en la regla de recepción aplicable.
4. AWS KMS crea una clave de datos nueva, la cifra con la clave KMS especificada y, a continuación, envía copias cifradas y de texto no cifrado de la clave de datos a Amazon SES.
5. Amazon SES utiliza la clave de datos de texto no cifrado para cifrar el mensaje de correo electrónico y, a continuación, elimina la clave de datos de texto no cifrado de la memoria tan pronto como sea posible después de utilizarla.

6. Amazon SES coloca el mensaje de correo electrónico cifrado y la clave de datos cifrada en el bucket de S3 especificado. La clave de datos cifrada se almacena como metadatos con el mensaje de correo electrónico cifrado.

Para lograr Step 3 a través deStep 6, Amazon SES utiliza elAWS, suministrados por el cliente de cifrado de Amazon S3. Utilice el mismo cliente para recuperar los mensajes de correo electrónico cifrados de Amazon S3 y descifrarlos. Para obtener más información, consulte Obtener y descifrar mensajes de correo electrónico.

Contexto de cifrado de Amazon SES

Cuando Amazon SES solicita un clave de datos para cifrar los mensajes de correo electrónico recibidos (Step 3 en Información general del cifrado de Amazon SES utilizando AWS KMS), incluye un contexto de cifrado en la solicitud. El contexto de cifrado proporciona la información autenticada adicional (AAD) que AWS KMS usa para garantizar la integridad de los datos. El contexto de cifrado también se escribe en los archivos de registro de AWS CloudTrail, lo que puede ayudarle a entender por qué se ha usado una AWS KMS key determinada. Amazon SES usa lo siguiente para el contexto de cifrado:

- El ID de Cuenta de AWS en la que ha configurado Amazon SES para recibir mensajes de correo electrónico
- El nombre de la regla de recepción de Amazon SES que ha invocado la acción de S3 en el mensaje de correo electrónico
- El ID de mensaje de Amazon SES para el mensaje de correo electrónico

El siguiente ejemplo muestra una representación JSON del contexto de cifrado que usa Amazon SES:

```
{
  "aws:ses:source-account": "111122223333",
  "aws:ses:rule-name": "example-receipt-rule-name",
  "aws:ses:message-id": "d6iitobk75ur44p8kdnnp7g2n800"
}
```

Dar permiso a Amazon SES para utilizar su AWS KMS key

Para cifrar sus mensajes de correo electrónico, puede usar la Clave administrada de AWS en su cuenta de Amazon SES (`aws/ses`), o puede usar una clave administrada por el cliente que cree. Amazon SES ya tiene permiso para utilizar el Clave administrada de AWS en su nombre. Sin embargo, si especifica una clave administrada por el cliente al agregar la acción de S3 a la regla de recepción de Amazon SES, debe conceder permiso a Amazon SES para usar la clave KMS para cifrar los mensajes de correo electrónico.

Para conceder permiso a Amazon SES para usar la clave administrada por el cliente, agregue la siguiente declaración a la política de claves de dicha clave:

```
{
  "Sid": "Allow SES to encrypt messages using this KMS key",
  "Effect": "Allow",
  "Principal": {"Service": "ses.amazonaws.com"},
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContext:aws:ses:rule-name": false,
      "kms:EncryptionContext:aws:ses:message-id": false
    },
    "StringEquals": {"kms:EncryptionContext:aws:ses:source-account": "ACCOUNT-ID-
WITHOUT-HYPHENS"}
  }
}
```

Sustituya *ACCOUNT-ID-WITHOUT-HYPHENS* por el ID de 12 dígitos de la Cuenta de AWS en la que ha configurado Amazon SES para recibir mensajes de correo electrónico. Esta declaración de política permite a Amazon SES cifrar los datos con esta clave KMS solo en estas condiciones:

- Amazon SES debe especificar `aws:ses:rule-name` y `aws:ses:message-id` en el `EncryptionContext` de sus solicitudes de la API de AWS KMS.
- Amazon SES debe especificar `aws:ses:source-account` en el `EncryptionContext` de sus solicitudes de la API de AWS KMS y el valor de `aws:ses:source-account` debe coincidir con el ID de Cuenta de AWS especificado en la política de claves.

Para obtener más información sobre el contexto de cifrado que usa Amazon SES al cifrar sus mensajes de correo electrónico, consulte Contexto de cifrado de Amazon SES. Para obtener información general acerca de cómo AWS KMS utiliza el contexto de cifrado, consulte contexto de cifrado.

Obtener y descifrar mensajes de correo electrónico

Amazon SES no tiene permiso para descifrar los mensajes de correo electrónico cifrados y no puede descifrarlos automáticamente. Debe escribir código para obtener los mensajes de correo electrónico de Amazon S3 y descifrarlos. Para facilitar la operación, use el cliente de cifrado de Amazon S3. Los siguientes SDK de AWS incluyen el cliente de cifrado de Amazon S3:

- AWS SDK for Java: Consulte AmazonS3EncryptionClient y AmazonS3EncryptionClientV2 en la AWS SDK for JavaReferencia de la API.
- AWS SDK for Ruby: Consulte Aws::S3::Encryption::Client en la AWS SDK for RubyReferencia de la API.
- AWS SDK for .NET: Consulte AmazonS3EncryptionClient en la AWS SDK for .NETReferencia de la API.
- AWS SDK for Go: Consulte s3crypto en la AWS SDK for GoReferencia de la API.

El cliente de cifrado de Amazon S3 simplifica la creación de las solicitudes necesarias de Amazon S3 para recuperar el mensaje de correo electrónico cifrado y de AWS KMS para descifrar la clave de datos cifrada del mensaje y el descifrado del mensaje de correo electrónico. Por ejemplo, para descifrar correctamente la clave de datos cifrada debe pasar el mismo contexto de cifrado que ha pasado Amazon SES al solicitar la clave de datos desde AWS KMS (Step 3 en el Información general del cifrado de Amazon SES utilizando AWS KMS). El cliente de cifrado de Amazon S3 gestiona automáticamente este trabajo y gran parte de otras tareas.

Para ver el código de muestra que utiliza el cliente de cifrado de Amazon S3 en AWS SDK for Java para realizar el cifrado en el cliente, consulte lo siguiente:

- Uso de una clave KMS almacenada en AWS KMS en la Guía del usuario de Amazon Simple Storage Service.
- Amazon S3 Encryption con AWS Key Management Service en el Blog para desarrolladores de AWS.

¿Cómo Amazon Simple Storage Service (Amazon S3) utiliza AWS KMS?

Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que almacena datos como objetos dentro de buckets. Los buckets y los objetos que contienen son privados y solo se puede acceder a ellos si concede explícitamente permisos de acceso.

Amazon S3 se integra con AWS Key Management Service (AWS KMS) para proporcionar cifrado del lado del servidor de los objetos de Amazon S3. Simple Storage Service (Amazon S3) utiliza claves de AWS KMS para cifrar sus objetos de Amazon S3. Las claves de cifrado que protegen sus objetos nunca salen de AWS KMS sin cifrar. Esta integración también permite establecer permisos en la clave AWS KMS y auditar las operaciones que generan, cifran y descifran las claves de datos que protegen sus secretos.

Para reducir el volumen de llamadas a Amazon S3AWS KMS, utilice las claves de bucket de Amazon S3, que están protegidas por claves de KMS y key-encryption-keys que se reutilizan durante un tiempo limitado en Amazon S3. Las claves de bucket pueden reducir los costos de las solicitudes de AWS KMS hasta en un 99 por ciento. Puede configurar una clave de bucket para todos los objetos en un bucket de Amazon S3, o para un determinado objeto en un bucket de Amazon S3.

Para obtener más información sobre cómo Simple Storage Service (Amazon S3) utiliza AWS KMS, consulte Protección de datos mediante el cifrado del lado del servidor con las claves KMS (SSE-KMS) en la Guía del usuario de Amazon S3.

¿Cómo AWS Systems Manager Parameter Store utiliza AWS KMS?

Con AWS Systems Manager Parameter Store, puede crear parámetros de cadena segura, que son parámetros que tienen un nombre de parámetro en texto no cifrado y un valor de parámetro cifrado. Parameter Store utiliza AWS KMS para cifrar y descifrar los valores de los parámetros de parámetros de cadena segura.

Con Parameter Store, puede crear, almacenar y administrar datos como parámetros con valores. Puede crear un parámetro en Parameter Store y utilizarlo en varias aplicaciones y servicios de acuerdo con las políticas y los permisos que diseñe. Cuando necesite cambiar el valor de un parámetro, cambiará una instancia, y no tendrá que administrar una modificación propensa a errores

en varios orígenes. Parameter Store admite una estructura jerárquica para los nombres de los parámetros, por lo que puede asignar un parámetro para usos específicos.

Para administrar información confidencial, puede crear parámetros de cadena segura. Parameter Store utiliza AWS KMS keys para cifrar los valores de los parámetros de parámetros de cadena segura cuando estos se crean o se modifican. También utiliza claves KMS para descifrar los valores de los parámetros cuando se obtiene acceso a ellos. Puede utilizar la Clave administrada de AWS que Parameter Store crea para su cuenta o especificar su propia clave administrada por el cliente.

> **Important**
>
> Parameter Store solo admiteclaves KMS simétricas. No se puede utilizar una clave KMS asimétrica para cifrar los parámetros. Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Parameter Store admite dos niveles de parámetros de cadena segura: estándar y avanzado. Los parámetros estándar, que no pueden superar los 4096 bytes, se cifran y descifran directamente con la clave KMS que especifique. Para cifrar y descifrar parámetros de cadena segura avanzados, Parameter Store utiliza el cifrado de sobre con el AWS Encryption SDK. Puede convertir un parámetro de cadena segura estándar en un parámetro avanzado, pero no puede convertir un parámetro avanzado en uno estándar. Para obtener más información acerca de la diferencia entre los parámetros de cadena segura estándar y avanzados, consulte acerca de los parámetros avanzados de Systems Manager en la Guía del usuario de AWS Systems Manager.

Temas

- Proteger los parámetros de cadena segura estándar
- Proteger los parámetros de cadena segura avanzada
- Configurar permisos para cifrar y descifrar valores de parámetros
- Contexto de cifrado de Parameter Store
- Solución de problemas de claves KMS en Parameter Store

Proteger los parámetros de cadena segura estándar

rendimiento no realiza ninguna operación criptográfica. En lugar de ello, utiliza AWS KMS para cifrar y descifrar los valores de los parámetros de cadena segura. Cuando se crea o cambia el valor de un parámetro de cadena segura estándar, Parameter Store llama a la operación de Encrypt (cifrado)

de AWS KMS. Esta operación utiliza directamente una clave KMS de cifrado simétrica para cifrar el valor del parámetro en lugar de utilizar la clave KMS para generar una clave de datos.

Puede seleccionar la clave KMS que utiliza Parameter Store para cifrar el valor del parámetro. Si no especifica una clave KMS, Parameter Store utiliza la Clave administrada de AWS que Systems Manager crea automáticamente en su cuenta. Esta clave KMS tiene el alias `aws/ssm`.

Para ver la clave `aws/ssm` KMS predeterminada de su cuenta, utilice la DescribeKeyoperación en la AWS KMS API. El siguiente ejemplo utiliza el comando `describe-key` de la AWS Command Line Interface (AWS CLI) con el nombre de alias `aws/ssm`.

```
aws kms describe-key --key-id alias/aws/ssm
```

Para crear un parámetro de cadena segura estándar, utilice la PutParameteroperación en la API de Systems Manager. Omita el parámetro `Tier` o especifique un valor de `Standard`, que es el valor predeterminado. Incluya un parámetro `Type` con el valor `SecureString`. Para especificar una clave KMS, utilice el parámetro `KeyId`. El valor predeterminado es la Clave administrada de AWS de su cuenta, `aws/ssm`.

A continuación, Parameter Store llama a la operación `Encrypt` de AWS KMS con la clave KMS y el valor del parámetro en texto no cifrado. AWS KMS devuelve el valor del parámetro cifrado y Parameter Store lo almacena junto con el nombre del parámetro.

El siguiente ejemplo utiliza el comando put-parameter de Systems Manager y su parámetro `--type` en la AWS CLI para crear un parámetro de cadena segura. Como el comando omite los parámetros opcionales `--tier` y `--key-id`, Parameter Store crea un parámetro de cadena segura estándar y lo cifra bajo la Clave administrada de AWS.

```
aws ssm put-parameter --name MyParameter --value "secret_value" --type SecureString
```

El siguiente ejemplo similar utiliza el parámetro `--key-id` para especificar una clave KMS administrada por el cliente. En el ejemplo se utiliza un ID de clave KMS para identificar la clave KMS, pero se puede utilizar cualquier identificador de clave KMS válido. Como el comando omite el parámetro `Tier` (`--tier`), Parameter Store crea un parámetro de cadena segura estándar, no uno avanzado.

```
aws ssm put-parameter --name param1 --value "secret" --type SecureString --key-id
 1234abcd-12ab-34cd-56ef-1234567890ab
```

Cuando se obtiene un parámetro de cadena segura de Parameter Store, su valor está cifrado. Para obtener un parámetro, utilice la GetParameter operación de la API de Systems Manager.

El siguiente ejemplo utiliza el comando get-parameter de Systems Manager en la AWS CLI para obtener el parámetro `MyParameter` de Parameter Store sin descifrar su valor.

```
$  aws ssm get-parameter --name MyParameter

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value":
 "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg/9E464VRo68cvwAAAG8wbQYJKoZIhvcNAQcGoGAwXgIBADBZBgkqhkiG9
    }
}
```

Para descifrar el valor del parámetro antes de devolverlo, establezca el parámetro `WithDecryption` de `GetParameter` en `true`. Al utilizar `WithDecryption`, Parameter Store llama a la operación Decrypt (descifrado) de AWS KMS en su nombre para descifrar el valor del parámetro. En consecuencia, la solicitud `GetParameter` devuelve el parámetro con un valor en texto no cifrado, tal y como se muestra en el siguiente ejemplo.

```
$  aws ssm get-parameter --name MyParameter --with-decryption

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

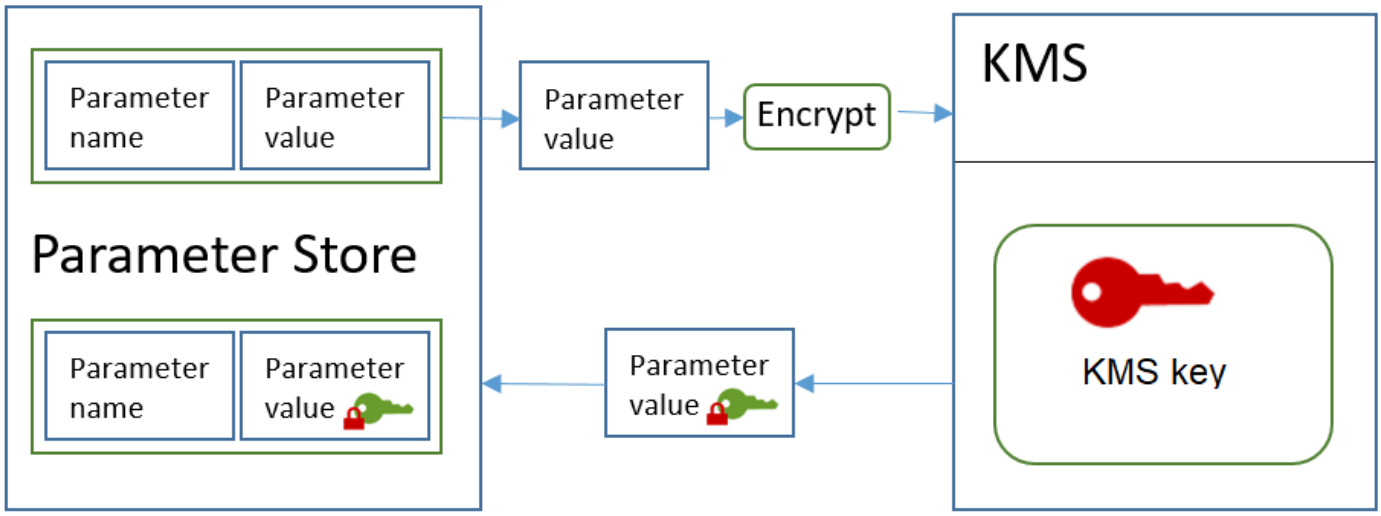
El siguiente flujo de trabajo muestra cómo Parameter Store utiliza una clave KMS para cifrar y descifrar un parámetro de cadena segura estándar.

Cifrar un parámetro estándar

1. Cuando utiliza `PutParameter` para crear un parámetro de cadena segura, Parameter Store envía una solicitud `Encrypt` a AWS KMS. Dicha solicitud incluye el valor del parámetro en texto no cifrado, la clave KMS que ha elegido y el contexto de cifrado de Parameter Store. Durante

la transmisión a AWS KMS, el valor en texto no cifrado del parámetro de cadena segura está protegido por seguridad de la capa de transporte (TLS).

2. AWS KMS cifra el valor del parámetro con la clave KMS y el contexto de cifrado especificados. Devuelve el texto cifrado a Parameter Store, que almacena el nombre del parámetro y su valor cifrado.



Descifrar un parámetro estándar

1. Cuando se incluye el parámetro `WithDecryption` en una solicitud `GetParameter`, Parameter Store envía una solicitud `Decrypt` a AWS KMS con el valor del parámetro de cadena segura cifrado y el contexto de cifrado de Parameter Store.
2. AWS KMS utiliza la misma clave KMS y el contexto de cifrado proporcionado para descifrar el valor cifrado. Devuelve el valor del parámetro en texto no cifrado (descifrado) a Parameter Store. Durante la transmisión, los datos en texto no cifrado están protegidos por TLS.
3. Parameter Store devuelve el valor del parámetro en texto no cifrado en la respuesta de `GetParameter`.

Proteger los parámetros de cadena segura avanzada

Cuando se utiliza `PutParameter` para crear un parámetro de cadena segura avanzado, Parameter Store usa el cifrado de sobre con el AWS Encryption SDK y una AWS KMS key de cifrado simétrica para proteger el valor del parámetro. Cada valor del parámetro avanzado se cifra con una clave de datos única y la clave de datos se cifra con una clave KMS. Puede usar la Clave administrada de AWS de la cuenta (`aws/ssm`) o cualquier clave administrada por el cliente.

El AWS Encryption SDK es una biblioteca cliente de código abierto que le ayuda a cifrar y descifrar datos mediante estándares y prácticas recomendadas del sector. Es compatible con varias plataformas y varios lenguajes de programación, incluida una interfaz de línea de comandos. Puede ver el código fuente y contribuir a su desarrollo en GitHub.

Para cada valor de parámetro de cadena segura, Parameter Store llama AWS Encryption SDK al para cifrar el valor del parámetro mediante una clave de datos única que AWS KMS genera (GenerateDataKey). El AWS Encryption SDK devuelve a Parameter Store un mensaje cifrado que incluye el valor del parámetro cifrado y una copia cifrada de la clave de datos única. Parameter Store almacena todo el mensaje cifrado en el valor del parámetro de cadena segura. A continuación, cuando se obtiene el valor de un parámetro de cadena segura avanzado, Parameter Store utiliza el AWS Encryption SDK para descifrar el valor del parámetro. Esto requiere una llamada a AWS KMS para descifrar la clave de datos cifrada.

Para crear un parámetro de cadena segura avanzado, utilice la PutParameteroperación en la API de Systems Manager. Establezca el valor del parámetro `Tier` en `Advanced`. Incluya un parámetro `Type` con el valor `SecureString`. Para especificar una clave KMS, utilice el parámetro `KeyId`. El valor predeterminado es la Clave administrada de AWS de su cuenta, `aws/ssm`.

```
aws ssm put-parameter --name MyParameter --value "secret_value" --type SecureString --
tier Advanced
```

El siguiente ejemplo similar utiliza el parámetro `--key-id` para especificar una clave administrada por el cliente. El ejemplo utiliza el Nombre de recurso de Amazon (ARN) de la clave KMS, pero puede utilizar cualquier identificador de clave KMS válido.

```
aws ssm put-parameter --name MyParameter --value "secret_value"
 --type SecureString --tier Advanced --key-id arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Cuando se obtiene un parámetro de cadena segura de Parameter Store, su valor es el mensaje cifrado que devuelve el AWS Encryption SDK. Para obtener un parámetro, utilice la GetParameter operación de la API de Systems Manager.

En el siguiente ejemplo se utiliza la operación `GetParameter` de Systems Manager para obtener el parámetro `MyParameter` de Parameter Store sin descifrar su valor.

```
$  aws ssm get-parameter --name MyParameter
```

```
{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value":
 "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg/9E464VRo68cvwAAAG8wbQYJKoZIhvcNAQcGoGAwXgIBADBZBgkqhkiG9
    }
}
```

Para descifrar el valor del parámetro antes de devolverlo, establezca el parámetro `WithDecryption` de `GetParameter` en `true`. Al utilizar `WithDecryption`, Parameter Store llama a la operación Decrypt (descifrado) de AWS KMS en su nombre para descifrar el valor del parámetro. En consecuencia, la solicitud `GetParameter` devuelve el parámetro con un valor en texto no cifrado, tal y como se muestra en el siguiente ejemplo.

```
$  aws ssm get-parameter --name MyParameter --with-decryption

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

No se puede convertir un parámetro de cadena segura avanzado en uno estándar, pero puede convertir una cadena segura estándar en una avanzada. Para convertir un parámetro de cadena segura estándar en una cadena segura avanzada, utilice la operación `PutParameter` con el parámetro `Overwrite`. El valor de `Type` debe ser `SecureString` y el valor de `Tier` debe ser `Advanced`. El parámetro `KeyId`, que identifica una clave administrada por el cliente, es opcional. Si lo omite, el Parameter Store utiliza el Clave administrada de AWS para la cuenta. Puede especificar cualquier clave KMS para la que la entidad principal tenga permiso, aunque utilice una clave KMS diferente para cifrar el parámetro estándar.

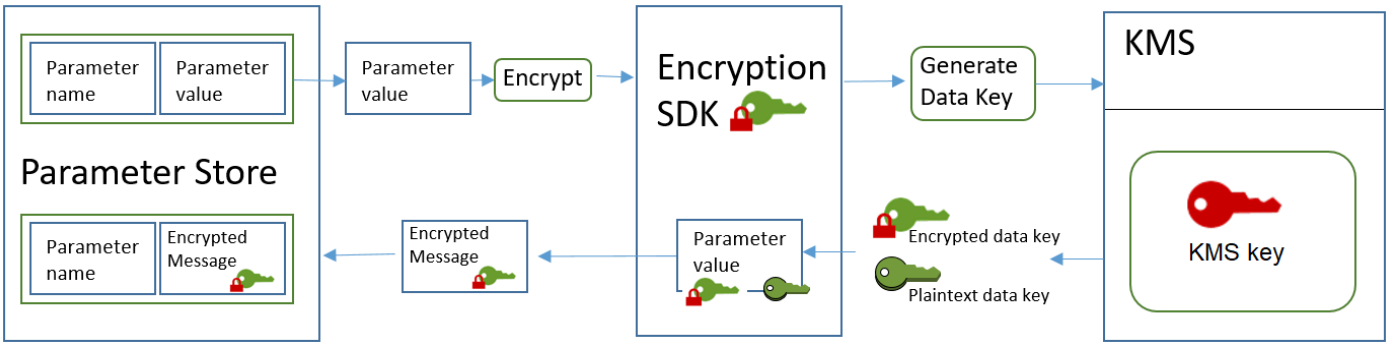
Cuando utiliza el parámetro `Overwrite`, el Parameter Store utiliza el AWS Encryption SDK para cifrar el valor del parámetro. A continuación, almacena el nuevo mensaje cifrado en Parameter Store.

```
$ aws ssm put-parameter --name myStdParameter --value "secret_value"  --type
 SecureString --tier Advanced --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --overwrite
```

El siguiente flujo de trabajo muestra cómo Parameter Store utiliza una clave KMS para cifrar y descifrar un parámetro de cadena segura avanzado.

Cifrar un parámetro avanzado

1. Cuando utiliza `PutParameter` para crear un parámetro de cadena segura avanzado, Parameter Store utiliza el AWS Encryption SDK y AWS KMS para cifrar el valor del parámetro. Parameter Store llama a AWS Encryption SDK con el valor del parámetro, la clave KMS que especificó y el contexto de cifrado de Parameter Store.
2. AWS Encryption SDKEnvía una GenerateDataKeysolicitud a AWS KMS con el identificador de la clave KMS que especificó y el contexto de cifrado del almacén de parámetros. AWS KMSdevuelve dos copias de la clave de datos única: una en texto sin formato y otra cifrada con la clave KMS. (El contexto de cifrado se utiliza al cifrar la clave de datos).
3. El AWS Encryption SDK usa la clave de datos en texto no cifrado para cifrar el valor del parámetro. Devuelve un mensaje cifrado que incluye el valor del parámetro cifrado, la clave de datos cifrada y otros datos, incluido el contexto de cifrado de Parameter Store.
4. Parameter Store almacena el mensaje cifrado como el valor del parámetro.



Descifrar un parámetro avanzado

1. Puede incluir el parámetro `WithDecryption` en una solicitud `GetParameter` para obtener un parámetro de cadena segura avanzado. Cuando lo haga, Parameter Store pasará el mensaje cifrado del valor del parámetro a un método de descifrado del AWS Encryption SDK.
2. El AWS Encryption SDK llama a la operación Decrypt (descifrado) de AWS KMS. Pasa la clave de datos cifrada y el contexto de cifrado de Parameter Store del mensaje cifrado.
3. AWS KMS utiliza la clave KMS y el contexto de cifrado de Parameter Store para descifrar la clave de datos cifrada. A continuación, devuelve la clave de datos en texto no cifrado (descifrada) al AWS Encryption SDK.

4. El AWS Encryption SDK utiliza la clave de datos en texto no cifrado para descifrar el valor del parámetro. Devuelve el valor del parámetro en texto no cifrado a Parameter Store.
5. Parameter Store verifica el contexto de cifrado y devuelve el valor del parámetro en texto no cifrado en la respuesta `GetParameter`.

Configurar permisos para cifrar y descifrar valores de parámetros

Para cifrar el valor de un parámetro de cadena segura estándar, el usuario necesita el permiso `kms:Encrypt`. Para cifrar el valor de un parámetro de cadena segura avanzado, el usuario necesita el permiso `kms:GenerateDataKey`. Para descifrar cualquier tipo de valor de un parámetro de cadena segura, el usuario necesita el permiso `kms:Decrypt`.

Puede utilizar las políticas de IAM; para conceder o denegar permisos a un usuario para llamar a las operaciones `PutParameter` y `GetParameter` de Systems Manager.

Además, si utiliza claves administradas por el cliente para cifrar valores de parámetros de cadena segura, puede utilizar políticas de IAM y de claves para administrar los permisos de cifrado y descifrado. Sin embargo, no puede establecer políticas de control de acceso para la clave KMS `aws/ssm` predeterminada. Para obtener información detallada sobre cómo controlar el acceso a las claves administradas por el cliente, consulte Autenticación y control de acceso de AWS KMS.

El siguiente ejemplo muestra una política de IAM diseñada para parámetros de cadena segura estándar. Permite que el usuario llame a la operación `PutParameter` de Systems Manager en todos los parámetros de la ruta `FinancialParameters`. La política también permite al usuario llamar a la operación `Encrypt` de AWS KMS en una clave administrada por el cliente de ejemplo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/
FinancialParameters/*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "kms:Encrypt"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

El siguiente ejemplo muestra una política de IAM diseñada para parámetros de cadena segura avanzados. Permite que el usuario llame a la operación `PutParameter` de Systems Manager en todos los parámetros de la ruta `ReservedParameters`. La política también permite al usuario llamar a la operación `GenerateDataKey` de AWS KMS en una clave administrada por el cliente de ejemplo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/
ReservedParameters/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

El último ejemplo también muestra una política de IAM que se puede utilizar para parámetros de cadena segura estándar o avanzados. Permite al usuario llamar a las operaciones `GetParameter` de Systems Manager (y a las operaciones relacionadas) en todos los parámetros de la ruta `ITParameters`. La política también permite al usuario llamar a la operación `Decrypt` de AWS KMS en una clave administrada por el cliente de ejemplo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter*"
            ],
            "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/ITParameters/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Contexto de cifrado de Parameter Store

Un contexto de cifrado es un conjunto de pares de clave-valor que contienen datos no secretos arbitrarios. Cuando se incluye un contexto de cifrado en una solicitud para cifrar datos, AWS KMS vincula criptográficamente el contexto de cifrado a los datos cifrados. Para descifrar los datos, es necesario pasar el mismo contexto de cifrado.

También se puede utilizar el contexto de cifrado para identificar una operación criptográfica en los registros y los registros de auditoría. El contexto de cifrado aparece en texto no cifrado en los registros, como los registros de AWS CloudTrail.

AWS Encryption SDK también tiene un contexto de cifrado, aunque se administra de forma distinta. Parameter Store proporciona el contexto de cifrado al método de cifrado. El AWS Encryption SDK vincula criptográficamente el contexto de cifrado a los datos cifrados. También incluye el contexto de cifrado en texto no cifrado en el encabezado del mensaje cifrado que devuelve. Sin embargo, a diferencia de AWS KMS, los métodos de descifrado de AWS Encryption SDK no toman un contexto de cifrado como entrada. En su lugar, cuando descifra datos, el AWS Encryption SDK obtiene el contexto de cifrado del mensaje cifrado. Parameter Store verifica que el contexto de cifrado incluye el valor que espera antes de devolverle el valor del parámetro en texto no cifrado.

Parameter Store utiliza el siguiente contexto de cifrado en sus operaciones criptográficas:

- Clave: `PARAMETER_ARN`
- Valor: el nombre de recurso de Amazon (ARN) del parámetro que se va a cifrar.

El formato del contexto de cifrado es el siguiente:

```
"PARAMETER_ARN":"arn:aws:ssm:<REGION_NAME>:<ACCOUNT_ID>:parameter/<parameter-name>"
```

Por ejemplo, Parameter Store incluye este contexto de cifrado en las llamadas para cifrar y descifrar el parámetro `MyParameter` en una Cuenta de AWS y región de ejemplo.

```
"PARAMETER_ARN":"arn:aws:ssm:us-west-2:111122223333:parameter/MyParameter"
```

Si el parámetro está en una ruta jerárquica de Parameter Store, la ruta y el nombre se incluyen en el contexto de cifrado. Por ejemplo, este contexto de cifrado se utiliza al cifrar y descifrar el parámetro `MyParameter` en la ruta `/ReadableParameters` en una Cuenta de AWS y región de ejemplo.

```
"PARAMETER_ARN":"arn:aws:ssm:us-west-2:111122223333:parameter/ReadableParameters/
MyParameter"
```

Puede descifrar el valor de un parámetro de cadena segura cifrado llamando a la operación `Decrypt` de AWS KMS con el contexto de cifrado correcto y el valor del parámetro cifrado devuelto por la operación `GetParameter` de Systems Manager. No obstante, le animamos a que descifre los valores de parámetros de Parameter Store mediante la operación `GetParameter` con el parámetro `WithDecryption`.

También puede incluir el contexto de cifrado en una política de IAM. Por ejemplo, puede permitir a un usuario que descifre únicamente el valor de un parámetro o un conjunto de valores de parámetros determinados.

La siguiente declaración de política de IAM de ejemplo permite al usuario obtener el valor del parámetro `MyParameter` y descifrar su valor mediante la clave KMS especificada. Sin embargo, los permisos solo se aplican cuando el contexto de cifrado coincide con la cadena especificada. Estos permisos no se aplican a ningún otro parámetro ni clave KMS, y la llamada a `GetParameter` da un error si el contexto de cifrado no coincide con la cadena.

Antes de utilizar una declaración de política como esta, sustituya los ARN de ejemplo por valores válidos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter*"
            ],
            "Resource": "arn:aws:ssm:us-west-2:111122223333:parameter/MyParameter"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Condition": {
                "StringEquals": {
                    "kms:EncryptionContext:PARAMETER_ARN":"arn:aws:ssm:us-
west-2:111122223333:parameter/MyParameter"
                }
            }
        }
    ]
}
```

Solución de problemas de claves KMS en Parameter Store

Para realizar operaciones en un parámetro de cadena segura, Parameter Store debe poder utilizar la clave KMS de AWS KMS especificada para la operación que se pretende realizar. La mayoría de los errores de Parameter Store relacionados con las claves KMS los provocan los siguientes problemas:

- Las credenciales que utiliza una aplicación no tienen permisos para realizar la acción especificada en la clave de KMs.

  Para solucionar este error, ejecute la aplicación con otras credenciales o revise la IAM o la política de claves que impide realizar la operación. Para obtener ayuda con la IAM de AWS KMS y las políticas de claves, consulte Autenticación y control de acceso de AWS KMS.

- No se encuentra la clave KMS.

Normalmente, esto ocurre cuando se utiliza un identificador incorrecto para la clave KMS. Localice los identificadores correctos para la clave KMS e intente ejecutar de nuevo el comando.

- La clave KMS no está habilitada. Cuando esto ocurre, Parameter Store devuelve una InvalidKeyIdexcepción con un mensaje de error detallado procedente deAWS KMS. Si el estado de la clave KMS es `Disabled`, habilítela. Si está `Pending Import`, complete el procedimiento de importación. Si el estado de la clave es `Pending Deletion`, cancele la eliminación de la clave o use una clave KMS distinta.

  Para buscar el key state (estado de la clave) de una clave KMS en la consola AWS KMS, en las claves administradas por el cliente o en la página Claves administradas por AWS, consulte la Status column (columna de estado). Para utilizar la AWS KMS API para buscar el estado de una clave de KMS, utilice la DescribeKeyoperación.

Cómo WorkMail usa Amazon AWS KMS

En este tema se explica cómo WorkMail utiliza Amazon AWS KMS para cifrar los mensajes de correo electrónico.

Temas

- WorkMail Descripción general de Amazon
- WorkMail Cifrado de Amazon
- Autorizar el uso de la clave KMS
- Contexto WorkMail de cifrado de Amazon
- Supervisión de la WorkMail interacción de Amazon con AWS KMS

WorkMail Descripción general de Amazon

Amazon WorkMail es un servicio de correo electrónico y calendario empresarial seguro y gestionado que admite los clientes de correo electrónico móviles y de escritorio existentes. Puedes crear una WorkMail organización de Amazon y asignarle uno o más dominios de correo electrónico de tu propiedad. A continuación, puede crear buzones de correo para los usuarios de correo electrónico y grupos de distribución de la organización.

Amazon cifra de WorkMail forma transparente todos los mensajes de los buzones de todas WorkMail las organizaciones de Amazon antes de que los mensajes se escriban en el disco y los descifra de

forma transparente cuando los usuarios acceden a ellos. No existe la opción de desactivar el cifrado. Para proteger las claves de cifrado que protegen los mensajes, Amazon WorkMail está integrado con AWS Key Management Service (AWS KMS).

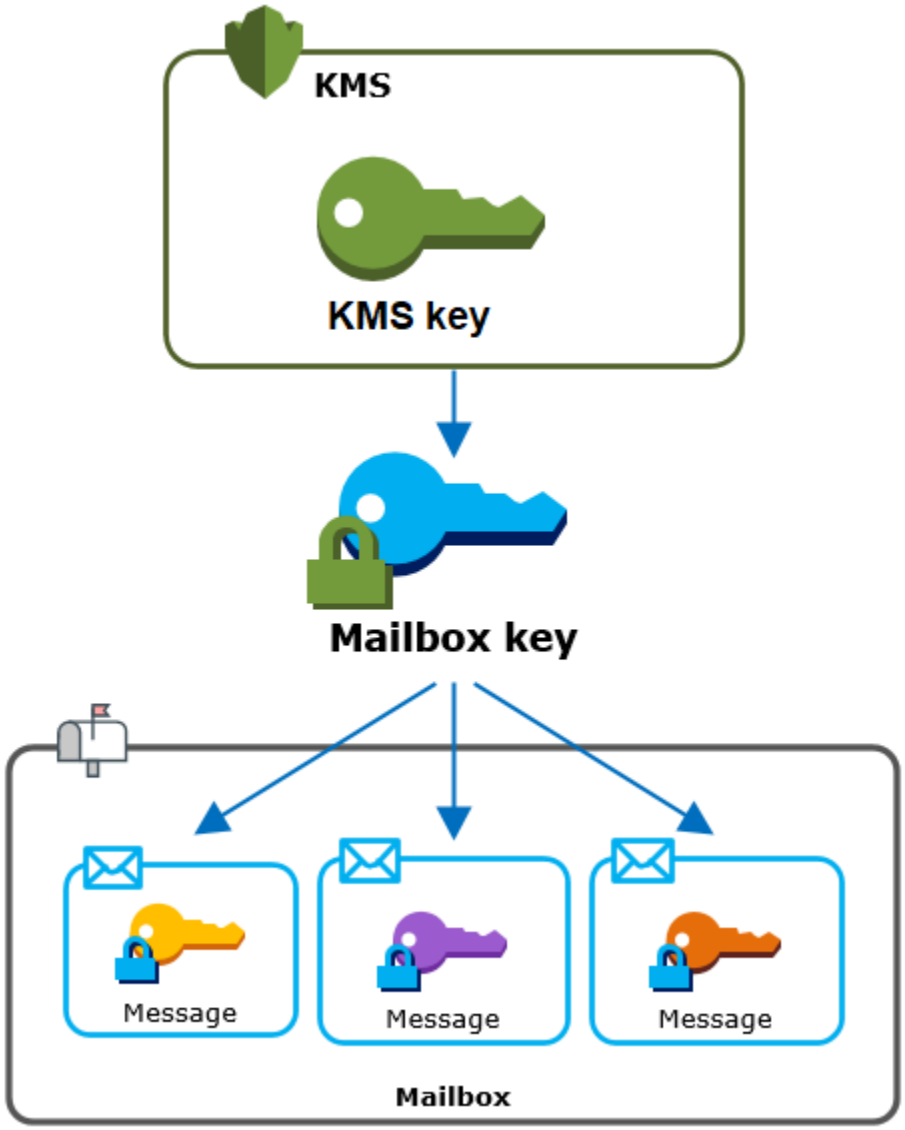
Amazon WorkMail también ofrece una opción para permitir a los usuarios enviar correos electrónicos firmados o cifrados. Esta característica de cifrado no utiliza AWS KMS.

WorkMail Cifrado de Amazon

En Amazon WorkMail, cada organización puede contener varios buzones, uno para cada usuario de la organización. Todos los mensajes, incluido los elementos de correo electrónico y de calendario, se almacenan en el buzón de correo del usuario.

Para proteger el contenido de los buzones de sus WorkMail organizaciones de Amazon, Amazon WorkMail cifra todos los mensajes de los buzones antes de escribirlos en el disco. Ninguno de los datos proporcionados por el cliente se almacena en texto no cifrado.

Cada mensaje se cifra con una clave de cifrado de datos única. La clave del mensaje se protege con una clave del buzón de correo, que es una clave de cifrado única que se utiliza únicamente para ese buzón de correo. La clave del buzón de correo se cifra con una AWS KMS key de la organización que nunca deja AWS KMS sin cifrar. En el siguiente diagrama se muestra la relación de los mensajes cifrados, claves de mensaje cifradas, clave de buzón de correo cifrada y la clave KMS de la organización en AWS KMS.



Una clave KMS para la organización

Al crear una WorkMail organización de Amazon, puedes seleccionar una AWS KMS key para la organización. Esta clave KMS protege todas las claves de buzón de correo de esa organización.

Si utilizas el procedimiento de configuración rápida para crear tu organización, Amazon WorkMail utilizará Clave administrada de AWSfor Amazon WorkMail (`aws/workmail`) en tuCuenta de AWS. Si utilizas la configuración estándar, puedes seleccionar la clave de Amazon WorkMail o una clave gestionada Clave administrada de AWS por el cliente que te pertenezca y gestione. Puede seleccionar la misma clave KMS o una clave KMS distinta para cada una de sus organizaciones, pero no puede cambiar la clave KMS una vez que la haya seleccionado.

> **Important**
>
> Amazon solo WorkMail admite claves KMS de cifrado simétrico. No puedes usar una clave KMS asimétrica para cifrar datos en Amazon. WorkMail Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Para buscar la clave KMS de su organización, utilice la entrada de AWS CloudTrail que registra las llamadas a AWS KMS.

Clave de cifrado única para cada buzón de correo

Al crear un buzón nuevo, Amazon WorkMail genera una clave de cifrado simétrica AES (Advanced Encryption Standard) exclusiva de 256 bits para el buzón, conocida como clave de buzón, fuera de. AWS KMS Amazon WorkMail usa la clave del buzón para proteger las claves de cifrado de cada mensaje del buzón.

Para proteger la clave del buzón, Amazon WorkMail pide AWS KMS que se cifre la clave del buzón bajo la clave KMS de la organización. A continuación, almacena la clave del buzón de correo cifrada en los metadatos del buzón.

> **Note**
>
> Amazon WorkMail utiliza una clave de cifrado de buzones simétrica para proteger las claves de los mensajes. Anteriormente, Amazon WorkMail protegía cada buzón con un key pair asimétrico. Utilizaba la clave pública para cifrar cada clave del mensaje y la clave privada para descifrarla. La clave privada del buzón de correo se protegía con la clave KMS de la organización. Los buzones de correo existentes pueden seguir utilizando un par de claves de buzón de correo asimétricas. Este cambio no afecta a la seguridad de la bandeja de entrada ni de sus mensajes.

Clave de cifrado única para cada mensaje

Cuando se añade un mensaje al buzón, Amazon WorkMail genera una clave de cifrado simétrica AES de 256 bits única para el mensaje externo a. AWS KMS Utiliza esta clave de mensaje para cifrar el mensaje. Amazon WorkMail cifra la clave del mensaje debajo de la clave del buzón y guarda la

clave del mensaje cifrado junto con el mensaje. A continuación, cifra la clave de buzón de correo con la clave KMS de la organización.

Creación de un nuevo buzón de correo

Cuando Amazon WorkMail crea un buzón nuevo, utiliza el siguiente proceso para prepararlo para que contenga los mensajes cifrados.

- Amazon WorkMail genera una clave de cifrado simétrica AES única de 256 bits para el buzón de correo externo a. AWS KMS
- Amazon WorkMail llama a la operación AWS KMS Encrypt. Pasa la clave del buzón de correo y el identificador de AWS KMS key de la organización. AWS KMS devuelve un texto cifrado de la clave del buzón de correo cifrada con la clave KMS.
- Amazon WorkMail almacena la clave del buzón cifrada con los metadatos del buzón.

Cifrar un mensaje del buzón de correo

Para cifrar un mensaje, Amazon WorkMail utiliza el siguiente proceso.

1. Amazon WorkMail genera una clave simétrica AES única de 256 bits para el mensaje. Utiliza la clave del mensaje en texto no cifrado y el algoritmo Advanced Encryption Standard (AES) para cifrar el mensaje fuera de AWS KMS.
2. Para proteger la clave del mensaje que se encuentra debajo de la clave del buzón, Amazon WorkMail necesita descifrar la clave del buzón, que siempre se almacena cifrada.

   Amazon WorkMail llama a la operación de AWS KMS descifrado y pasa la clave del buzón cifrada. AWS KMSusa la clave KMS de la organización para descifrar la clave del buzón y devuelve la clave de buzón de texto sin formato a Amazon. WorkMail
3. Amazon WorkMail utiliza la clave de buzón de texto sin formato y el algoritmo del Estándar de cifrado avanzado (AES) para cifrar la clave del mensaje fuera de. AWS KMS
4. Amazon WorkMail almacena la clave del mensaje cifrado en los metadatos del mensaje cifrado para que esté disponible para descifrarlo.

Descifrar un mensaje del buzón de correo

Para descifrar un mensaje, Amazon WorkMail utiliza el siguiente proceso.

1. Amazon WorkMail llama a la operación de AWS KMS descifrado y pasa la clave del buzón cifrada. AWS KMSusa la clave KMS de la organización para descifrar la clave del buzón y devuelve la clave de buzón de texto sin formato a Amazon. WorkMail
2. Amazon WorkMail utiliza la clave de buzón de texto sin formato y el algoritmo del Estándar de cifrado avanzado (AES) para descifrar la clave del mensaje cifrado fuera de. AWS KMS
3. Amazon WorkMail utiliza la clave del mensaje de texto sin formato para descifrar el mensaje cifrado.

Almacenamiento en caché de las claves del buzón de correo

Para mejorar el rendimiento y minimizar las llamadas aAWS KMS, Amazon almacena en WorkMail caché cada clave de buzón de texto simple de cada cliente de forma local durante un máximo de un minuto. Al final del período de almacenamiento en caché, la clave del buzón de correo se elimina. Si se requiere la clave del buzón de ese cliente durante el período de almacenamiento en caché, Amazon WorkMail puede obtenerla de la memoria caché en lugar de llamarAWS KMS. La clave del buzón de correo está protegida en la memoria caché y nunca se escribe en disco en texto sin formato.

Autorizar el uso de la clave KMS

Cuando Amazon WorkMail utiliza un AWS KMS key en las operaciones criptográficas, actúa en nombre del administrador del buzón.

Para utilizar la AWS KMS key para un secreto en su nombre, el administrador debe tener los siguientes permisos. Puede especificar estos permisos necesarios en una política de IAM o política de claves.

- `kms:Encrypt`
- `kms:Decrypt`
- `kms:CreateGrant`

Para permitir que la clave KMS se use solo para las solicitudes que se originan en Amazon WorkMail, puedes usar la clave de ViaService condición kms: con el `workmail.<region>.amazonaws.com` valor.

También puede utilizar las claves o los valores en el contexto de cifrado como condición para utilizar la clave KMS para operaciones criptográficas. Por ejemplo, puede utilizar un operador de condición

de cadena en un IAM o en un documento de política de claves, o bien utilizar una restricción de concesión en una concesión.

Política de claves para la Clave administrada de AWS

La política clave de Amazon WorkMail otorga a los usuarios permiso para usar la clave KMS para operaciones específicas solo cuando Amazon WorkMail realiza la solicitud en nombre del usuario. Clave administrada de AWS La política de claves no permite a ningún usuario utilizar la clave KMS directamente.

Esta política de claves, como las políticas de todas las Claves administradas por AWS, la establece el servicio. No puede cambiar la política de claves, pero puede verla en cualquier momento. Para obtener más detalles, consulte Consultar una política de claves.

Las declaraciones de política de la política de claves tienen el siguiente efecto:

- Permita que los usuarios de la cuenta y la región utilicen la clave KMS para operaciones criptográficas y para crear subvenciones, pero solo cuando la solicitud provenga de Amazon WorkMail en su nombre. La clave de condición `kms:ViaService` aplica esta restricción.
- Permite a la cuenta de Cuenta de AWS crear políticas de IAM que permiten a los usuarios ver propiedades de la clave KMS y revocar concesiones.

La siguiente es una política clave, a modo de ejemplo, Clave administrada de AWS para Amazon WorkMail.

```
{
  "Version" : "2012-10-17",
  "Id" : "auto-workmail-1",
  "Statement" : [ {
    "Sid" : "Allow access through WorkMail for all principals in the account that are
 authorized to use WorkMail",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "*"
    },
    "Action" : [ "kms:Decrypt", "kms:CreateGrant", "kms:ReEncrypt*", "kms:DescribeKey",
 "kms:Encrypt" ],
    "Resource" : "*",
    "Condition" : {
      "StringEquals" : {
```

```
        "kms:ViaService" : "workmail.us-east-1.amazonaws.com",
        "kms:CallerAccount" : "111122223333"
      }
    }
  }, {
    "Sid" : "Allow direct access to key metadata to the account",
    "Effect" : "Allow",
    "Principal" : {
      "AWS" : "arn:aws:iam::111122223333:root"
    },
    "Action" : [ "kms:Describe*", "kms:List*", "kms:Get*", "kms:RevokeGrant" ],
    "Resource" : "*"
  } ]
}
```

Uso de subvenciones para autorizar a Amazon WorkMail

Además de las políticas clave, Amazon WorkMail utiliza las concesiones para añadir permisos a la clave de KMS de cada organización. Para ver las concesiones de la clave KMS de su cuenta, utilice la ListGrantsoperación.

Amazon WorkMail utiliza las concesiones para añadir los siguientes permisos a la clave de KMS de la organización.

- Añade el `kms:Encrypt` permiso para permitir que Amazon WorkMail cifre la clave del buzón.
- Añada el `kms:Decrypt` permiso para permitir que Amazon WorkMail utilice la clave KMS para descifrar la clave del buzón. Amazon WorkMail requiere este permiso en una concesión porque la solicitud de lectura de los mensajes del buzón utiliza el contexto de seguridad del usuario que lee el mensaje. La solicitud no utiliza las credenciales de la Cuenta de AWS. Amazon WorkMail crea esta concesión cuando seleccionas una clave de KMS para la organización.

Para crear las subvenciones, Amazon WorkMail llama CreateGranten nombre del usuario que creó la organización. El permiso para crear la concesión proviene de la política de claves. Esta política permite a los usuarios de `CreateGrant` la cuenta solicitar la clave KMS de la organización cuando Amazon WorkMail realiza la solicitud en nombre de un usuario autorizado.

La política de claves también permite a la raíz de la cuenta revocar la concesión para la Clave administrada de AWS. Sin embargo, si revoca la concesión, Amazon WorkMail no podrá descifrar los datos cifrados de sus buzones.

Contexto WorkMail de cifrado de Amazon

Un contexto de cifrado es un conjunto de pares de clave-valor que contienen datos no secretos arbitrarios. Cuando se incluye un contexto de cifrado en una solicitud para cifrar datos, AWS KMS vincula criptográficamente el contexto de cifrado a los datos cifrados. Para descifrar los datos, es necesario pasar el mismo contexto de cifrado.

Amazon WorkMail utiliza el mismo formato de contexto de cifrado en todas las operaciones AWS KMS criptográficas. Puede utilizar el contexto de cifrado para identificar una operación criptográfica en los registros y registros de auditoría, como AWS CloudTrail y como una condición para la autorización en las políticas y concesiones.

En sus solicitudes de cifrado y descifrado, AWS KMS Amazon WorkMail utiliza un contexto de cifrado en el que la clave está `aws:workmail:arn` y el valor es el nombre de recurso de Amazon (ARN) de la organización.

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization ID"
```

Por ejemplo, el siguiente contexto de cifrado incluye un ARN de organización de ejemplo en la Región EE. UU. Este (Ohio) (`us-east-2`).

```
"aws:workmail:arn":"arn:aws:workmail:us-east-2:111122223333:organization/
m-68755160c4cb4e29a2b2f8fb58f359d7"
```

Supervisión de la WorkMail interacción de Amazon con AWS KMS

Puedes usar AWS CloudTrail Amazon CloudWatch Logs para realizar un seguimiento de las solicitudes que Amazon WorkMail envía AWS KMS en tu nombre.

Encrypt

Al crear un buzón nuevo, Amazon WorkMail genera una clave de buzón y llama AWS KMS para cifrarla. Amazon WorkMail envía una solicitud de cifrado a AWS KMS con la clave de buzón de correo de texto sin formato y un identificador para la clave de KMS de la organización de Amazon WorkMail .

El evento que registra la operación `Encrypt` es similar al siguiente evento de ejemplo. El usuario es el WorkMail servicio de Amazon. Los parámetros incluyen el ID de clave de KMS (`keyId`) y el contexto de cifrado de la WorkMail organización de Amazon. Amazon WorkMail también pasa la clave del buzón, pero no queda registrada en el CloudTrail registro.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-19T10:01:09Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-c6981ff7642446fa8772ba99c690e455"
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d"
    },
    "responseElements": null,
    "requestID": "76e96b96-7e24-4faf-a2d6-08ded2eaf63c",
    "eventID": "d5a59c18-128a-4082-aa5b-729f7734626a",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "d08e60f1-097e-4a00-b7e9-10bc3872d50c"
}
```


Decrypt

Cuando añades, ves o eliminas un mensaje del buzón, Amazon WorkMail te pide AWS KMS que descifre la clave del buzón. Amazon WorkMail envía una solicitud de descifrado a AWS KMS con

la clave del buzón cifrada y un identificador para la clave de KMS de la WorkMail organización de Amazon.

El evento que registra la operación `Decrypt` es similar al siguiente evento de ejemplo. El usuario es el WorkMail servicio de Amazon. Los parámetros incluyen la clave del buzón de correo cifrada (como un blob de texto cifrado), que no se registra en el registro, y el contexto de cifrado de la organización de Amazon. WorkMail AWS KMSobtiene el ID de la clave KMS a partir del texto cifrado.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "workmail.eu-west-1.amazonaws.com"
    },
    "eventTime": "2019-02-20T11:51:10Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "workmail.eu-west-1.amazonaws.com",
    "userAgent": "workmail.eu-west-1.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:workmail:arn": "arn:aws:workmail:eu-west-1:111122223333:organization/
m-c6981ff7642446fa8772ba99c690e455"
        }
    },
    "responseElements": null,
    "requestID": "4a32dda1-34d9-4100-9718-674b8e0782c9",
    "eventID": "ea9fd966-98e9-4b7b-b377-6e5a397a71de",
    "readOnly": true,
    "resources": [
        {
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d",
            "accountId": "111122223333",
            "type": "AWS::KMS::Key"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "sharedEventID": "241e1e5b-ff64-427a-a5b3-7949164d0214"
}
```

Cómo WorkSpaces usa AWS KMS

Puede utilizarlo WorkSpacespara aprovisionar un escritorio basado en la nube para cada uno de sus usuarios finales. WorkSpace Al lanzar una nueva WorkSpace, puede optar por cifrar sus volúmenes y decidir cuál usar AWS KMS keypara el cifrado. Puede elegir la clave Clave administrada de AWSpara WorkSpaces (aws/workspaces) o una clave simétrica gestionada por el cliente.

> **Important**
>
> WorkSpaces solo admite claves KMS de cifrado simétrico. No puede utilizar una clave KMS asimétrica para cifrar los volúmenes de un. WorkSpaces Para obtener ayuda para determinar si una clave KMS es simétrica o asimétrica, consulte Identificación de claves KMS asimétricas.

Para obtener más información sobre la creación WorkSpaces con volúmenes cifrados, consulta Encrypt a WorkSpace en la Guía de WorkSpaces administración de Amazon.

Temas

- Descripción general del WorkSpaces cifrado mediante AWS KMS
- WorkSpaces contexto de cifrado
- WorkSpaces Otorgar permiso para usar una clave KMS en su nombre

Descripción general del WorkSpaces cifrado mediante AWS KMS

Cuando crea WorkSpaces con volúmenes cifrados, WorkSpaces utiliza Amazon Elastic Block Store (Amazon EBS) para crear y gestionar esos volúmenes. Ambos servicios utilizan su AWS KMS key para trabajar con los volúmenes cifrados. Para obtener más información sobre el cifrado de volúmenes de EBS, consulte la siguiente documentación:

- ¿Cómo Amazon Elastic Block Store (Amazon EBS) utiliza AWS KMS? en esta guía
- Cifrado de Amazon EBS en la Guía del usuario de Amazon EC2 para instancias de Windows

Cuando se lanza WorkSpaces con volúmenes cifrados, el end-to-end proceso funciona de la siguiente manera:

1. Debe especificar la clave KMS que se utilizará para el cifrado, así como el WorkSpace usuario y el directorio correspondientes. Esta acción crea una concesión que permite WorkSpaces usar la clave KMS solo para este fin, es WorkSpace decir, solo para la WorkSpace asociada al usuario y al directorio especificados.
2. WorkSpaces crea un volumen de EBS cifrado para el volumen WorkSpace y especifica la clave de KMS que se va a utilizar, así como el usuario y el directorio del volumen (la misma información que especificó enStep 1). Esta acción crea una concesión que permite a Amazon EBS usar su clave de KMS solo para este WorkSpace volumen, es decir, solo para los WorkSpace asociados al usuario y directorio especificados y solo para el volumen especificado.
3. Amazon EBS solicita una clave de datos de volumen cifrada con su clave de KMS y especifica el ID del WorkSpace usuario `Sid` y del directorio, así como el ID del volumen, como contexto de cifrado.
4. AWS KMS crea una clave de datos, la cifra con su clave KMS y, a continuación, envía la clave de datos cifrada a Amazon EBS.
5. WorkSpaces utiliza Amazon EBS para adjuntar el volumen cifrado a su WorkSpace. Amazon EBS envía la clave de datos cifrados a AWS KMS con una `Decrypt`solicitud y especifica el WorkSpace nombre del usuario`Sid`, su ID de directorio y el ID de volumen, que se utiliza como contexto de cifrado.
6. AWS KMS utiliza su clave KMS para descifrar la clave de datos y, a continuación, envía la clave de datos en texto no cifrado a Amazon EBS.
7. Amazon EBS utiliza la clave de datos en texto no cifrado para cifrar todos los datos que se envían a los volúmenes cifrados y se reciben de ellos. Amazon EBS mantiene la clave de datos de texto sin formato en la memoria mientras el volumen esté conectado al. WorkSpace
8. Amazon EBS almacena la clave de datos cifrada (recibida enStep 4) junto con los metadatos del volumen para utilizarla en el futuro en caso de que reinicie o reconstruya el WorkSpace.
9. Cuando utilizas la AWS Management Console para eliminar una WorkSpace (o utilizas la `TerminateWorkspaces`acción de la WorkSpaces API) WorkSpaces y Amazon EBS retira las concesiones que le permitían usar tu clave de KMS para ello WorkSpace.

WorkSpaces contexto de cifrado

WorkSpaces no lo usa AWS KMS key directamente para operaciones criptográficas (como `Encrypt`,, `Decrypt`, etc.) `GenerateDataKey`, lo que significa que WorkSpaces no envía solicitudes AWS KMS que incluyan un contexto de cifrado. Sin embargo, cuando Amazon EBS

solicita una clave de datos cifrada para los volúmenes cifrados de su WorkSpaces (Step 3en elDescripción general del WorkSpaces cifrado mediante AWS KMS) y cuando solicita una copia en texto sin formato de esa clave de datos (Step 5), incluye el contexto de cifrado en la solicitud. El contexto de cifrado proporciona la información autenticada adicional (AAD) que AWS KMS usa para garantizar la integridad de los datos. El contexto de cifrado también se escribe en los archivos de registro de AWS CloudTrail, lo que puede ayudarle a entender por qué se ha usado una determinada AWS KMS key. Amazon EBS usa lo siguiente para el contexto de cifrado:

- El `sid` del AWS Directory Service usuario que está asociado al WorkSpace
- El ID de AWS Directory Service directorio del directorio que está asociado a WorkSpace
- El ID del volumen cifrado

El siguiente ejemplo muestra una representación JSON del contexto de cifrado que usa Amazon EBS:

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

WorkSpaces Otorgar permiso para usar una clave KMS en su nombre

Puede proteger los datos de su espacio de trabajo con la clave Clave administrada de AWS for WorkSpaces (aws/workspaces) o con una clave administrada por el cliente. Si utiliza una clave administrada por el cliente, debe dar WorkSpaces permiso para usar la clave KMS en nombre de los WorkSpaces administradores de su cuenta. El Clave administrada de AWS for WorkSpaces tiene los permisos necesarios de forma predeterminada.

Para preparar la clave gestionada por el cliente para utilizarla con WorkSpaces ella, utilice el siguiente procedimiento.

1. Agregue a los WorkSpaces administradores a la lista de usuarios clave de la política clave de la clave KMS
2. Otorgue a los WorkSpaces administradores permisos adicionales con una política de IAM

WorkSpaces los administradores también necesitan permiso para WorkSpaces utilizarla. Para obtener más información sobre estos permisos, consulte Control del acceso a WorkSpaces los recursos en la Guía de WorkSpaces administración de Amazon.

Parte 1: Añadir WorkSpaces administradores a los usuarios clave de una clave KMS

Para conceder a WorkSpaces los administradores los permisos que necesitan, puede utilizar la API AWS Management Console o la AWS KMS API.

Para añadir WorkSpaces administradores como usuarios clave de una clave de KMS (consola)

1. Inicie sesión en la AWS Management Console y abra la consola de AWS Key Management Service (AWS KMS) en https://console.aws.amazon.com/kms.
2. Para cambiar la Región de AWS, utilice el Selector de regiones ubicado en la esquina superior derecha de la página.
3. En el panel de navegación, elija Claves administradas por el cliente.
4. Elija el alias o el ID de clave de la clave administrada por el cliente que prefiera.
5. Seleccione la pestaña Key policy (Política de claves). En Key Users (Usuarios de claves), elija Add (Agregar).
6. En la lista de usuarios y roles de IAM, seleccione los usuarios y roles que corresponden a sus WorkSpaces administradores y, a continuación, elija Adjuntar.

Para añadir WorkSpaces administradores como usuarios clave de una clave de KMS (AWS KMSAPI)

1. Utilice la GetKeyPolicyoperación para obtener la política de claves existente y, a continuación, guarde el documento de política en un archivo.
2. Abra el documento de políticas en el editor de textos que prefiera. Agregue los usuarios y funciones de IAM que correspondan a sus WorkSpaces administradores a las declaraciones de política que otorgan permisos a los usuarios clave. A continuación, guarde el archivo.
3. Utilice la PutKeyPolicyoperación para aplicar la política clave a la clave de KMS.

Parte 2: Otorgar permisos adicionales a los WorkSpaces administradores

Si utiliza una clave administrada por el cliente para proteger sus WorkSpaces datos, además de los permisos de la sección de usuarios clave de la política de claves predeterminada, WorkSpaces los administradores necesitan permiso para crear concesiones en la clave de KMS. Además, si la

utilizan AWS Management Consolepara crear WorkSpaces con volúmenes cifrados, WorkSpaces los administradores necesitan permiso para enumerar los alias y las claves. Para obtener más información sobre la creación y edición de políticas de usuario de IAM, consulte Políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Para conceder estos permisos a sus WorkSpaces administradores, utilice una política de IAM. Añada una declaración de política similar a la del siguiente ejemplo a la política de IAM de cada WorkSpaces administrador. Reemplace el ARN de la clave KMS de ejemplo (*arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab*) por uno válido. Si sus WorkSpaces administradores utilizan únicamente la WorkSpaces API (no la consola), puede omitir la segunda declaración de política con los permisos `"kms:ListAliases"` y`"kms:ListKeys"`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Programación de la API de AWS KMS

Puede utilizar la API de AWS KMS para crear y administrar claves de KMS y funciones especiales, como almacenes de claves personalizadas y utilizar claves KMS en operaciones criptográficas. Para obtener más detalles, consulte la Referencia de API de la AWS Key Management Service.

El código de muestra de los siguientes temas muestra cómo utilizar los SDK de AWS para llamar a la API de AWS KMS.

Para obtener información sobre el uso de la consola de AWS KMS para realizar algunas de estas tareas, consulte Administración de claves.

Temas

Crear un cliente

Para usar el AWS SDK for Java, el AWS SDK for .NET, el AWS SDK for Python (Boto3)AWS SDK for RubyAWS SDK for PHP, el o el AWSSDK de Node.js para JavaScript escribir código que use la API AWS Key Management Service (AWS KMS), comience por crear un AWS KMS cliente.

El objeto de cliente que crea se utiliza en el código de ejemplo de los temas que aparecen a continuación.

Java

Para crear un cliente de AWS KMS en Java, utilice el compilador del cliente.

```
AWSKMS kmsClient = AWSKMSClientBuilder.standard().build();
```

Para obtener más información sobre el uso del compilador de clientes Java, consulte los siguientes recursos.

- Fluent Client Builders en el Blog para desarrolladores de AWS
- Creación de clientes de servicio en la Guía para desarrolladores de AWS SDK for Java
- AWSKMSClientBuilder en la Referencia de la API de AWS SDK for Java

C#

```
AmazonKeyManagementServiceClient kmsClient = new AmazonKeyManagementServiceClient();
```

Python

```
kms_client = boto3.client('kms')
```

Ruby

```
require 'aws-sdk-kms'  # in v2: require 'aws-sdk'

kmsClient = Aws::KMS::Client.new
```

PHP

Para crear un cliente de AWS KMS en PHP, utilice un objeto de cliente de AWS KMS y especifique la versión `2014-11-01`. Para obtener más información acerca de la clase KMSClient en la Referencia de la API o la AWS SDK for PHP.

```
// Create a KMSClient
$KmsClient = new Aws\Kms\KmsClient([
    'profile' => 'default',
    'version' => '2014-11-01',
    'region'  => 'us-east-1'
]);
```

Node.js

```
const kmsClient = new AWS.KMS();
```

Trabajo con claves

Los ejemplos de este tema utilizan la API de AWS KMS para crear, ver, habilitar y desactivar AWS KMS AWS KMS keys, y para generar claves de datos.

Temas

- Crear una clave KMS
- Generar una clave de datos
- Ver un AWS KMS key
- Obtener ID de clave y ARN clave de claves KMS
- Habilitación de AWS KMS keys
- Deshabilitación de AWS KMS key

Crear una clave KMS

Para crear una AWS KMS key(clave KMS), utilice la CreateKeyoperación. Los ejemplos de esta sección crean una clave KMS de cifrado simétrica. El parámetro `Description` utilizado en estos ejemplos es opcional.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Para obtener ayuda con la creación de claves KMS en la consola de AWS KMS, consulte Crear claves.

Java

Para obtener más detalles, consulte el método createKey en la Referencia de la API de AWS SDK for Java.

```
// Create a KMS key
//
String desc = "Key for protecting critical data";

CreateKeyRequest req = new CreateKeyRequest().withDescription(desc);
CreateKeyResult result = kmsClient.createKey(req);
```

C#

Para obtener más información, consulte el método CreateKey en AWS SDK for .NET.

```
// Create a KMS key
//
String desc = "Key for protecting critical data";

CreateKeyRequest req = new CreateKeyRequest()
{
    Description = desc
};
CreateKeyResponse response = kmsClient.CreateKey(req);
```

Python

Para obtener más información, consulte el método `create_key` en AWS SDK for Python (Boto3).

```
# Create a KMS key

desc = 'Key for protecting critical data'

response = kms_client.create_key(
    Description=desc
)
```

Ruby

Para obtener más información, consulte el método de instancia `create_key` en AWS SDK for Ruby.

```
# Create a KMS key

desc = 'Key for protecting critical data'

response = kmsClient.create_key({
  description: desc
})
```

PHP

Para obtener más información, consulte el método CreateKey en AWS SDK for PHP.

```
// Create a KMS key
//
$desc = "Key for protecting critical data";

$result = $KmsClient->createKey([
    'Description' => $desc
]);
```

Node.js

Para obtener más información, consulta la propiedad CreateKey en AWSel SDK JavaScript o en Node.js.

```
// Create a KMS key
//
const Description = 'Key for protecting critical data';

kmsClient.createKey({ Description }, (err, data) => {
  ...
});
```

PowerShell

Para crear una clave de KMS PowerShell, utilice el cmdlet New-. KmsKey

```
# Create a KMS key

$desc = 'Key for protecting critical data'
New-KmsKey -Description $desc
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Generar una clave de datos

Para generar una clave de datos simétrica, utilice la GenerateDataKeyoperación. Esta operación devuelve una clave de datos de texto sin formato y una copia de esa clave de datos cifrada bajo la clave KMS de cifrado simétrica especificada. Debe especificar `KeySpec` o `NumberOfBytes` (pero no ambos) en cada comando.

Para obtener ayuda sobre cómo utilizar la clave de datos para cifrar los datos, consulte AWS Encryption SDK. También puede usar la clave de datos en operaciones de HMAC.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más información, consulta el generateDataKey método en la referencia de la AWS SDK for Java API.

```
// Generate a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

GenerateDataKeyRequest dataKeyRequest = new GenerateDataKeyRequest();
dataKeyRequest.setKeyId(keyId);
dataKeyRequest.setKeySpec("AES_256");

GenerateDataKeyResult dataKeyResult = kmsClient.generateDataKey(dataKeyRequest);

ByteBuffer plaintextKey = dataKeyResult.getPlaintext();

ByteBuffer encryptedKey = dataKeyResult.getCiphertextBlob();
```

C#

Para obtener más información, consulte el método GenerateDataKey en AWS SDK for .NET.

```
// Generate a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
GenerateDataKeyRequest dataKeyRequest = new GenerateDataKeyRequest()
{
    KeyId = keyId,
    KeySpec = DataKeySpec.AES_256
};
```

```
GenerateDataKeyResponse dataKeyResponse = kmsClient.GenerateDataKey(dataKeyRequest);

MemoryStream plaintextKey = dataKeyResponse.Plaintext;

MemoryStream encryptedKey = dataKeyResponse.CiphertextBlob;
```

Python

Para obtener más información, consulte el método `generate_data_key` en AWS SDK for Python (Boto3).

```
# Generate a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.generate_data_key(
    KeyId=key_id,
    KeySpec='AES_256'
)

plaintext_key = response['Plaintext']

encrypted_key = response['CiphertextBlob']
```

Ruby

Para obtener más información, consulte el método de instancia `generate_data_key` en AWS SDK for Ruby.

```
# Generate a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.generate_data_key({
  key_id: key_id,
  key_spec: 'AES_256'
})
```

```
plaintext_key = response.plaintext

encrypted_key = response.ciphertext_blob
```

PHP

Para obtener más información, consulte el método GenerateDataKey en AWS SDK for PHP.

```
// Generate a data key
//
// Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$keySpec = 'AES_256';

$result = $KmsClient->generateDataKey([
    'KeyId' => $keyId,
    'KeySpec' => $keySpec,
]);

$plaintextKey = $result['Plaintext'];

$encryptedKey = $result['CiphertextBlob'];
```

Node.js

Para obtener más información, consulta la generateDataKey propiedad en el AWSSDK de JavaScript Node.js.

```
// Generate a data key
//
// Replace the following example key ARN with any valid key identfier
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const KeySpec = 'AES_256';
kmsClient.generateDataKey({ KeyId, KeySpec }, (err, data) => {
  if (err) console.log(err, err.stack);
  else {
    const { CiphertextBlob, Plaintext } = data;
      ...
  }
});
```

PowerShell

Para generar una clave de datos simétrica, utilice el cmdlet New-KMS DataKey.

En el resultado, la clave de texto sin formato (en la `Plaintext` propiedad) y la clave cifrada (en la propiedad) son objetos. `CiphertextBlob` MemoryStream Para convertirlos en cadenas, utilice los métodos de la `MemoryStream` clase o un cmdlet o una función que convierta `MemoryStream` los objetos en cadenas, como las funciones ConvertFrom- MemoryStream y ConvertFrom-Base64 del módulo Convert.

```
# Generate a data key

# Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$keySpec = 'AES_256'

$response = New-KmsDataKey -KeyId $keyId -KeySpec $keySpec
$plaintextKey = $response.Plaintext
$encryptedKey = $response.CiphertextBlob
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Ver un AWS KMS key

Para obtener información detallada sobre anAWS KMS key, incluidos el ARN y el estado de la clave de KMS, utilice la DescribeKeyoperación.

`DescribeKey` no obtiene alias. Para obtener los alias, utilice la ListAliasesoperación. Para ver ejemplos, consulte Trabajar con alias.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Para obtener ayuda con las claves KMS en la consola de AWS KMS, consulte Consultar claves.

Java

Para obtener más detalles, consulte el método describeKey en la Referencia de la API de AWS SDK for Java.

```
// Describe a KMS key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

DescribeKeyRequest req = new DescribeKeyRequest().withKeyId(keyId);
DescribeKeyResult result = kmsClient.describeKey(req);
```

C#

Para obtener más información, consulte el método DescribeKey en AWS SDK for .NET.

```
// Describe a KMS key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

DescribeKeyRequest describeKeyRequest = new DescribeKeyRequest()
{
    KeyId = keyId
};

DescribeKeyResponse describeKeyResponse = kmsClient.DescribeKey(describeKeyRequest);
```

Python

Para obtener más información, consulte el método `describe_key` en AWS SDK for Python (Boto3).

```
# Describe a KMS key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.describe_key(
```

```
    KeyId=key_id
)
```

Ruby

Para obtener más información, consulte el método de instancia `describe_key` en AWS SDK for Ruby.

```
# Describe a KMS key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.describe_key({
  key_id: key_id
})
```

PHP

Para obtener más información, consulte el método DescribeKey en AWS SDK for PHP.

```
// Describe a KMS key
//
// Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->describeKey([
    'KeyId' => $keyId,
]);
```

Node.js

Para obtener más información, consulte la propiedad DescribeKey en AWSel SDK JavaScript o en Node.js.

```
// Describe a KMS key
//
// Replace the following example key ARN with any valid key identfier
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.describeKey({ KeyId }, (err, data) => {
```

```
  ...
});
```

PowerShell

Para obtener información detallada sobre una clave de KMS, utilice el cmdlet Get-. KmsKey

```
# Describe a KMS key

# Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
Get-KmsKey -KeyId $keyId
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Obtener ID de clave y ARN clave de claves KMS

Para obtener los ID y los ARN clave delAWS KMS keys, utilice la ListKeysoperación. Estos ejemplos utilizan el parámetro opcional `Limit`, que establece el número máximo de claves KMS devueltas en cada llamada. Para obtener ayuda para identificar una clave KMS en una operación de AWS KMS, consulte Identificadores clave () KeyId.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Para obtener ayuda con la búsqueda de identificadores de clave y ARN de clave en la consola de AWS KMS, consulte Búsqueda del ID y el ARN de la clave.

Java

Para obtener más detalles, consulte el método listKeys en la Referencia de la API de AWS SDK for Java.

```
// List KMS keys in this account
//
Integer limit = 10;

ListKeysRequest req = new ListKeysRequest().withLimit(limit);
```

```
ListKeysResult result = kmsClient.listKeys(req);
```

C#

Para obtener más información, consulte el método ListKeys en AWS SDK for .NET.

```
// List KMS keys in this account
//
int limit = 10;

ListKeysRequest listKeysRequest = new ListKeysRequest()
{
    Limit = limit
};
ListKeysResponse listKeysResponse = kmsClient.ListKeys(listKeysRequest);
```

Python

Para obtener más información, consulte el método `list_keys` en AWS SDK for Python (Boto3).

```
# List KMS keys in this account

response = kms_client.list_keys(
    Limit=10
)
```

Ruby

Para obtener más información, consulte el método de instancia `list_keys` en AWS SDK for Ruby.

```
# List KMS keys in this account

response = kmsClient.list_keys({
  limit: 10
})
```

PHP

Para obtener más información, consulte el método ListKeys en AWS SDK for PHP.

```
// List KMS keys in this account
```

```
//
$limit = 10;

$result = $KmsClient->listKeys([
    'Limit' => $limit,
]);
```

Node.js

Para obtener más información, consulta la propiedad ListKeys en el AWSSDK o JavaScript en Node.js.

```
// List KMS keys in this account
//
const Limit = 10;
kmsClient.listKeys({ Limit }, (err, data) => {
  ...
});
```

PowerShell

Para obtener el identificador de clave y el ARN de clave de todas las claves de KMS de la cuenta y la región, utilice el cmdlet Get- KmsKeyList.

Para limitar el número de objetos de salida, este ejemplo usa el cmdlet Select-Object en lugar del parámetro `Limit`, que está quedando obsoleto en los cmdlet de la lista. Para obtener asistencia con la paginación de salida en AWS Tools for PowerShell, vea Paginación de salida con AWS Tools for PowerShell.

```
# List KMS keys in this account

$limit = 10
Get-KmsKeyList | Select-Object -First $limit
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Habilitación de AWS KMS keys

Para habilitar un deshabilitadoAWS KMS key, use la EnableKeyoperación.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Para obtener ayuda con la habilitación y deshabilitación de claves KMS en la consola de AWS KMS, consulte Habilitación y deshabilitación de claves.

Java

Para obtener más detalles sobre la implementación de Java, consulte el método enableKey en la Referencia de la API de AWS SDK for Java.

```
// Enable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

EnableKeyRequest req = new EnableKeyRequest().withKeyId(keyId);
kmsClient.enableKey(req);
```

C#

Para obtener más información, consulte el método EnableKey en AWS SDK for .NET.

```
// Enable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

EnableKeyRequest enableKeyRequest = new EnableKeyRequest()
{
    KeyId = keyId
};
kmsClient.EnableKey(enableKeyRequest);
```

Python

Para obtener más información, consulte el método `enable_key` en AWS SDK for Python (Boto3).

```
# Enable a KMS key
```

```
# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.enable_key(
    KeyId=key_id
)
```

Ruby

Para obtener más información, consulte el método de instancia `enable_key` en AWS SDK for Ruby.

```
# Enable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.enable_key({
  key_id: key_id
})
```

PHP

Para obtener más información, consulte el método EnableKey en AWS SDK for PHP.

```
// Enable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->enableKey([
    'KeyId' => $keyId,
]);
```

Node.js

Para obtener más información, consulte la propiedad EnableKey en AWSel SDK JavaScript de Node.js.

```
// Enable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.enableKey({ KeyId }, (err, data) => {
  ...
});
```

PowerShell

Para habilitar una clave KMS, utilice el cmdlet Enable-. KmsKey

```
# Enable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
Enable-KmsKey -KeyId $keyId
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Deshabilitación de AWS KMS key

Para deshabilitar una clave KMS, utilice la DisableKeyoperación. Desactivar una clave KMS impide que se utilice en operaciones criptográficas.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Para obtener ayuda con la habilitación y deshabilitación de claves KMS en la consola de AWS KMS, consulte Habilitación y deshabilitación de claves.

Java

Para obtener más detalles, consulte el método disableKey en la Referencia de la API de AWS SDK for Java.

```
// Disable a KMS key
```

```
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

DisableKeyRequest req = new DisableKeyRequest().withKeyId(keyId);
kmsClient.disableKey(req);
```

C#

Para obtener más información, consulte el método DisableKey en AWS SDK for .NET.

```
// Disable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

DisableKeyRequest disableKeyRequest = new DisableKeyRequest()
{
    KeyId = keyId
};
kmsClient.DisableKey(disableKeyRequest);
```

Python

Para obtener más información, consulte el método `disable_key` en AWS SDK for Python (Boto3).

```
# Disable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.disable_key(
    KeyId=key_id
)
```

Ruby

Para obtener más información, consulte el método de instancia `disable_key` en AWS SDK for Ruby.

```
# Disable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.disable_key({
  key_id: key_id
})
```

PHP

Para obtener más información, consulte el método DisableKey en AWS SDK for PHP.

```
// Disable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->disableKey([
    'KeyId' => $keyId,
]);
```

Node.js

Para obtener más información, consulta la propiedad DisableKey en AWSel SDK JavaScript o en Node.js.

```
// Disable a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.disableKey({ KeyId }, (err, data) => {
  ...
});
```

PowerShell

Para deshabilitar una clave KMS, utilice el cmdlet Disable-. KmsKey

```
# Disable a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
Disable-KmsKey -KeyId $keyId
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la Guía del usuario de AWS Tools for Windows PowerShell.

Trabajar con alias

Los ejemplos de este tema utilizan la API de AWS KMS para crear, ver, actualizar y eliminar alias. Para obtener información acerca de los alias, consulte the section called “Uso de alias”.

Temas

- Crear un alias
- Mostrar alias
- Actualizar un alias
- Eliminar un alias

Crear un alias

Al crear un AWS KMS key en la AWS Management Console, debe crear un alias para ello. Sin embargo, la CreateKeyoperación que crea una clave KMS no crea un alias.

Para crear un alias, utilice la CreateAliasoperación. El alias debe ser único en la cuenta y en la región de . No puede crear un alias que comience por `aws/`. El prefijo `aws/` está reservado por Amazon Web Services para Claves administradas por AWS.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para conocer detalles, consulte el método createAlias en la Referencia de la API de AWS SDK for Java.

```
// Create an alias for a KMS key
//
String aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
String targetKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

CreateAliasRequest req = new
 CreateAliasRequest().withAliasName(aliasName).withTargetKeyId(targetKeyId);
kmsClient.createAlias(req);
```

C#

Para obtener más información, consulte el método CreateAlias en AWS SDK for .NET.

```
// Create an alias for a KMS key
//
String aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
String targetKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

CreateAliasRequest createAliasRequest = new CreateAliasRequest()
{
    AliasName = aliasName,
    TargetKeyId = targetKeyId
};
kmsClient.CreateAlias(createAliasRequest);
```

Python

Para obtener más información, consulte el método `create_alias` en AWS SDK for Python (Boto3).

```
# Create an alias for a KMS key

alias_name = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
target_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.create_alias(
    AliasName=alias_name,
```

```
    TargetKeyId=key_id
)
```

Ruby

Para obtener más información, consulte el método de instancia `create_alias` en AWS SDK for Ruby.

```
# Create an alias for a KMS key

alias_name = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
target_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.create_alias({
  alias_name: alias_name,
  target_key_id: target_key_id
})
```

PHP

Para obtener más información, consulte el método CreateAlias en AWS SDK for PHP.

```
// Create an alias for a KMS key
//
$aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';


$result = $KmsClient->createAlias([
    'AliasName' => $aliasName,
    'TargetKeyId' =>  $keyId,
]);
```

Node.js

Para obtener más información, consulta la propiedad CreateAlias en AWSel SDK JavaScript o en Node.js.

```
// Create an alias for a KMS key
```

```
//
const AliasName = 'alias/projectKey1';

// Replace the following example key ARN with a valid key ID or key ARN
const TargetKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.createAlias({ AliasName, TargetKeyId }, (err, data) => {
  ...
});
```

PowerShell

Para crear un alias, utilice el cmdlet New-KMSalias. El nombre del alias distingue entre mayúsculas y minúsculas.

```
# Create an alias for a KMS key

$aliasName = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
$targetKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

New-KMSAlias -TargetKeyId $targetKeyId -AliasName $aliasName
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Mostrar alias

Para enumerar los alias de la cuenta y la región, utilice la ListAliasesoperación.

De forma predeterminada, el comando ListAliases devuelve todos los alias de la cuenta y la región. Esto incluye los alias que ha creado y asociado a las claves administradas por el cliente y los alias que AWS creó y asoció con su Claves administradas por AWS. La respuesta también podría incluir los alias que no tienen el campo `TargetKeyId`. Estos son los alias predefinidos que AWS ha creado, pero aún no se han asociado con una clave KMS.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más detalles sobre la implementación de Java, consulte el método listAliases en la Referencia de la API de AWS SDK for Java.

```
// List the aliases in this Cuenta de AWS
//
Integer limit = 10;

ListAliasesRequest req = new ListAliasesRequest().withLimit(limit);
ListAliasesResult result = kmsClient.listAliases(req);
```

C#

Para obtener más información, consulte el método ListAliases en AWS SDK for .NET.

```
// List the aliases in this Cuenta de AWS
//
int limit = 10;

ListAliasesRequest listAliasesRequest = new ListAliasesRequest()
{
    Limit = limit
};
ListAliasesResponse listAliasesResponse = kmsClient.ListAliases(listAliasesRequest);
```

Python

Para obtener más información, consulte el método `list_aliases` en AWS SDK for Python (Boto3).

```
# List the aliases in this Cuenta de AWS

response = kms_client.list_aliases(
    Limit=10
)
```

Ruby

Para obtener más información, consulte el método de instancia `list_aliases` en AWS SDK for Ruby.

```
# List the aliases in this Cuenta de AWS

response = kmsClient.list_aliases({
  limit: 10
})
```

PHP

Para obtener más información, consulte el método List Aliases en el AWS SDK for PHP.

```
// List the aliases in this Cuenta de AWS
//
$limit = 10;

$result = $KmsClient->listAliases([
    'Limit' => $limit,
]);
```

Node.js

Para obtener más información, consulta la propiedad ListAliases en AWSel SDK JavaScript o en Node.js.

```
// List the aliases in this Cuenta de AWS
//
const Limit = 10;
kmsClient.listAliases({ Limit }, (err, data) => {
  ...
});
```

PowerShell

Para ver una lista de los alias de la cuenta y la región, usa el cmdlet Get-KMS. AliasList

Para limitar el número de objetos de salida, este ejemplo usa el cmdlet Select-Object en lugar del parámetro `Limit`, que está quedando obsoleto en los cmdlet de la lista. Para obtener asistencia con la paginación de salida en AWS Tools for PowerShell, vea Paginación de salida con AWS Tools for PowerShell.

```
# List the aliases in this Cuenta de AWS
$limit = 10
```

```
$result = Get-KMSAliasList | Select-Object -First $limit
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Para mostrar solo los alias que están asociados con una determinada clave KMS en particular, utilice el parámetro `KeyId`. Su valor puede ser el ID de la clave o el ARN de la clave de cualquier clave KMS en la región. No puede especificar un nombre de alias o ARN de alias.

Java

Para obtener más detalles sobre la implementación de Java, consulte el método listAliases en la Referencia de la API de AWS SDK for Java.

```
// List the aliases for one KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

ListAliasesRequest req = new ListAliasesRequest().withKeyId(keyId);
ListAliasesResult result = kmsClient.listAliases(req);
```

C#

Para obtener más información, consulte el método ListAliases en AWS SDK for .NET.

```
// List the aliases for one KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

ListAliasesRequest listAliasesRequest = new ListAliasesRequest()
{
    KeyId = keyId
};
ListAliasesResponse listAliasesResponse = kmsClient.ListAliases(listAliasesRequest);
```

Python

Para obtener más información, consulte el método `list_aliases` en AWS SDK for Python (Boto3).

```
# List the aliases for one KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.list_aliases(
    KeyId=key_id
)
```

Ruby

Para obtener más información, consulte el método de instancia `list_aliases` en AWS SDK for Ruby.

```
# List the aliases for one KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.list_aliases({
  key_id: key_id
})
```

PHP

Para obtener más información, consulte el método List Aliases en el AWS SDK for PHP.

```
// List the aliases for one KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->listAliases([
    'KeyId' => $keyId,
```

```
]);
```

Node.js

Para obtener más información, consulta la propiedad ListAliases en AWSel SDK JavaScript o en Node.js.

```
// List the aliases for one KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
kmsClient.listAliases({ KeyId }, (err, data) => {
  ...
});
```

PowerShell

Para enumerar los alias de una clave KMS, utilice el `KeyId` parámetro del cmdlet Get-KMS. AliasList

```
# List the aliases for one KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

$response = Get-KmsAliasList -KeyId $keyId
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Actualizar un alias

Para asociar un alias existente a una clave de KMS diferente, utilice la UpdateAliasoperación.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más detalles sobre la implementación de Java, consulte el método updateAlias en la Referencia de la API de AWS SDK for Java.

```
// Updating an alias
//
String aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
String targetKeyId = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

UpdateAliasRequest req = new UpdateAliasRequest()
     .withAliasName(aliasName)
     .withTargetKeyId(targetKeyId);

kmsClient.updateAlias(req);
```

C#

Para obtener más información, consulte el método UpdateAlias en AWS SDK for .NET.

```
// Updating an alias
//
String aliasName = "alias/projectKey1";
// Replace the following example key ARN with a valid key ID or key ARN
String targetKeyId = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

UpdateAliasRequest updateAliasRequest = new UpdateAliasRequest()
{
    AliasName = aliasName,
    TargetKeyId = targetKeyId
};

kmsClient.UpdateAlias(updateAliasRequest);
```

Python

Para obtener más información, consulte el método `update_alias` en AWS SDK for Python (Boto3).

```
# Updating an alias
```

```
alias_name = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321'

response = kms_client.update_alias(
    AliasName=alias_name,
    TargetKeyID=key_id
)
```

Ruby

Para obtener más información, consulte el método de instancia `update_alias` en AWS SDK for Ruby.

```
# Updating an alias

alias_name = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321'

response = kmsClient.update_alias({
  alias_name: alias_name,
  target_key_id: key_id
})
```

PHP

Para obtener más información, consulte el método UpdateAlias en AWS SDK for PHP.

```
// Updating an alias
//
$aliasName = "alias/projectKey1";

// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321';

$result = $KmsClient->updateAlias([
    'AliasName' => $aliasName,
    'TargetKeyId' =>  $keyId,
```

```
]);
```

Node.js

Para obtener más información, consulta la propiedad UpdateAlias en AWSel SDK JavaScript o en Node.js.

```
// Updating an alias
//
const AliasName = 'alias/projectKey1';

// Replace the following example key ARN with a valid key ID or key ARN
const TargetKeyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321';
kmsClient.updateAlias({ AliasName, TargetKeyId }, (err, data) => {
  ...
});
```

PowerShell

Para cambiar la clave KMS que está asociada a un alias, use el cmdlet Update-KMSAlias. El nombre del alias distingue entre mayúsculas y minúsculas.

El cmdlet `Update-KMSAlias` no devuelve ningún resultado. Para comprobar que el comando ha funcionado, utilice el cmdlet AliasListGet-KMS.

```
# Updating an alias

$aliasName = 'alias/projectKey1'
# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321'

Update-KMSAlias -AliasName $aliasName -TargetKeyID $keyId
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Eliminar un alias

Para eliminar un alias, utilice la DeleteAliasoperación. La eliminación de un alias no afecta a la clave KMS asociada.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más detalles, consulte el método deleteAlias en la Referencia de la API de AWS SDK for Java.

```
// Delete an alias for a KMS key
//
String aliasName = "alias/projectKey1";

DeleteAliasRequest req  = new DeleteAliasRequest().withAliasName(aliasName);
kmsClient.deleteAlias(req);
```

C#

Para obtener más información, consulte el método DeleteAlias en AWS SDK for .NET.

```
// Delete an alias for a KMS key
//
String aliasName = "alias/projectKey1";

DeleteAliasRequest deleteAliasRequest = new DeleteAliasRequest()
{
    AliasName = aliasName
};
kmsClient.DeleteAlias(deleteAliasRequest);
```

Python

Para obtener más información, consulte el método `delete_alias` en AWS SDK for Python (Boto3).

```
# Delete an alias for a KMS key
```

```
alias_name = 'alias/projectKey1'

response = kms_client.delete_alias(
    AliasName=alias_name
)
```

Ruby

Para obtener más información, consulte el método de instancia `delete_alias` en AWS SDK for Ruby.

```
# Delete an alias for a KMS key

alias_name = 'alias/projectKey1'

response = kmsClient.delete_alias({
  alias_name: alias_name
})
```

PHP

Para obtener más información, consulte el método DeleteAlias en AWS SDK for PHP.

```
// Delete an alias for a KMS key
//
$aliasName = "alias/projectKey1";

$result = $KmsClient->deleteAlias([
    'AliasName' => $aliasName,
]);
```

Node.js

Para obtener más información, consulta la propiedad (deleteAlias) en AWSel SDK JavaScript o en Node.js.

```
// Delete an alias for a KMS key
//
const AliasName = 'alias/projectKey1';
kmsClient.deleteAlias({ AliasName }, (err, data) => {
  ...
```

```
});
```

PowerShell

Para eliminar un alias, utilice el cmdlet Remove-KMSalias. El nombre del alias distingue entre mayúsculas y minúsculas.

Como este cmdlet elimina el alias de forma permanente, PowerShell le pide que confirme el comando. El valor de `ConfirmImpact` es `High`, por lo que no se puede utilizar `ConfirmPreference` para suprimir esta solicitud. Si debe suprimir la solicitud de confirmación, agregue el parámetro común `Confirm` con el valor `$false`; por ejemplo: `-Confirm:$false`.

El cmdlet `Remove-KMSAlias` no devuelve ningún resultado. Para comprobar la eficacia del comando, utilice el cmdlet Get-KMS. AliasList

```
# Delete an alias for a KMS key

$aliasName = 'alias/projectKey1'
Remove-KMSAlias -AliasName $aliasName
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la Guía del usuario de AWS Tools for Windows PowerShell.

Cifrar y descifrar claves de datos

Los ejemplos de este tema utilizan las ReEncryptoperaciones Cifrar, Descifrar y de la AWS KMS API.

Estas operaciones están diseñadas para cifrar y descifrar claves de datos. Utilizan una AWS KMS keys en las operaciones de cifrado y no pueden aceptar más de 4 KB (4 096 bytes) de datos. Aunque es posible utilizarlas para cifrar pequeñas cantidades de datos como, por ejemplo, una contraseña o una clave RSA, no se han diseñado para cifrar los datos de las aplicaciones.

Para cifrar los datos de las aplicaciones, utilice las características de cifrado del lado del servidor de un servicio de AWS o una biblioteca de cifrado del lado del cliente, como el AWS Encryption SDK o el cliente de cifrado de Amazon S3.

Temas

- Cifrar una clave de datos

- Descifrando una clave de datos
- Volver a cifrar una clave de datos con otra AWS KMS key

Cifrar una clave de datos

La operación Encrypt se ha diseñado para cifrar claves de datos, pero no se utiliza con frecuencia. Las GenerateDataKeyWithoutPlaintextoperaciones GenerateDataKeyy devuelven claves de datos cifradas. Puede utilizar este método cuando mueva datos cifrados a una región diferente y desee cifrar su clave de datos con una clave KMS en la nueva región.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más detalles, consulte el método de cifrado en la Referencia de la API de AWS SDK for Java.

```
// Encrypt a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
ByteBuffer plaintext = ByteBuffer.wrap(new byte[]{1,2,3,4,5,6,7,8,9,0});

EncryptRequest req = new EncryptRequest().withKeyId(keyId).withPlaintext(plaintext);
ByteBuffer ciphertext = kmsClient.encrypt(req).getCiphertextBlob();
```

C#

Para obtener más información, consulte el método Encrypt en el AWS SDK for .NET.

```
// Encrypt a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
MemoryStream plaintext = new MemoryStream();
plaintext.Write(new byte[] { 1, 2, 3, 4, 5, 6, 7, 8, 9, 0 }, 0, 10);
```

```
EncryptRequest encryptRequest = new EncryptRequest()
{
    KeyId = keyId,
    Plaintext = plaintext
};
MemoryStream ciphertext = kmsClient.Encrypt(encryptRequest).CiphertextBlob;
```

Python

Para obtener más información, consulte el método encrypt en la AWS SDK for Python (Boto3).

```
# Encrypt a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
plaintext = b'\x01\x02\x03\x04\x05\x06\x07\x08\x09\x00'

response = kms_client.encrypt(
    KeyId=key_id,
    Plaintext=plaintext
)

ciphertext = response['CiphertextBlob']
```

Ruby

Para obtener más información, consulte el método de instancia encrypt en el AWS SDK for Ruby.

```
# Encrypt a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
plaintext = "\x01\x02\x03\x04\x05\x06\x07\x08\x09\x00"

response = kmsClient.encrypt({
  key_id: key_id,
  plaintext: plaintext
})

ciphertext = response.ciphertext_blob
```

PHP

Para obtener más información, consulte el método Encrypt en el AWS SDK for PHP.

```
// Encrypt a data key
//
// Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$message = pack('c*',1,2,3,4,5,6,7,8,9,0);

$result = $KmsClient->encrypt([
    'KeyId' => $keyId,
    'Plaintext' => $message,
]);

$ciphertext = $result['CiphertextBlob'];
```

Node.js

Para obtener más información, consulta la propiedad encrypt en el AWS SDK de JavaScript Node.js.

```
// Encrypt a data key
//
// Replace the following example key ARN with any valid key identfier
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const Plaintext = Buffer.from([1, 2, 3, 4, 5, 6, 7, 8, 9, 0]);
kmsClient.encrypt({ KeyId, Plaintext }, (err, data) => {
  if (err) console.log(err, err.stack); // an error occurred
  else {
    const { CiphertextBlob } = data;
      ...
  }
});
```

PowerShell

Para cifrar una clave de datos en una clave KMS, utilice el cmdlet Invoke-KMSEncrypt. Devuelve el texto cifrado como un `MemoryStream` (System.IO). MemoryStream) objeto. Puede utilizar el objeto `MemoryStream` como entrada para el cmdlet Invoke-KMSDecrypt.

AWS KMS también devuelve claves de datos como objetos `MemoryStream`. En este ejemplo, para simular una clave de datos de texto sin formato, creamos una matriz de bytes y la escribimos en un objeto `MemoryStream`.

Tenga en cuenta que el parámetro `Plaintext` de `Invoke-KMSEncrypt` toma una matriz de bytes (`byte[]`); no requiere un objeto `MemoryStream`. A partir de la AWSPowerShell versión 4.0, los parámetros de todos los AWSPowerShell módulos que utilizan matrices de bytes y `MemoryStream` objetos aceptan matrices de bytes, `MemoryStream` objetos, cadenas, matrices de cadenas y `FileInfo` (System.IO). FileInfo) objetos. Puede pasar cualquiera de estos tipos a `Invoke-KMSEncrypt`.

```
# Encrypt a data key

# Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

# Simulate a data key
 # Create a byte array
[byte[]] $bytes = 1, 2, 3, 4, 5, 6, 7, 8, 9, 0

 # Create a MemoryStream
$plaintext = [System.IO.MemoryStream]::new()

 # Add the byte array to the MemoryStream
$plaintext.Write($bytes, 0, $bytes.length)

# Encrypt the simulated data key
$response = Invoke-KMSEncrypt -KeyId $keyId -Plaintext $plaintext

# Get the ciphertext from the response
$ciphertext = $response.CiphertextBlob
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Descifrando una clave de datos

Para descifrar una clave de datos, use la operación Decrypt.

El `ciphertextBlob` que especifique debe ser el valor del `CiphertextBlob` campo de una respuesta GenerateDataKeyGenerateDataKeyWithoutPlaintext, o Cifrar, o el `PrivateKeyCiphertextBlob` campo de una GenerateDataKeyPairWithoutPlaintextrespuesta GenerateDataKeyPairo. También puede utilizar la operación `Decrypt` para descifrar los datos cifrados fuera de AWS KMS por la clave pública en una clave KMS asimétrica.

El parámetro `KeyId` no es necesario al descifrar con claves de cifrado KMS simétricas. AWS KMS puede obtener la clave KMS que se usó para cifrar los datos de los metadatos en el blob de texto cifrado. Pero siempre es una práctica recomendada especificar la clave KMS que está utilizando. Esta práctica garantiza que utilice la clave KMS deseada y le impide descifrar inadvertidamente un texto cifrado utilizando una clave KMS en la que no confía.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más detalles, consulte el método de descifrado en la Referencia de la API de AWS SDK for Java.

```
// Decrypt a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

ByteBuffer ciphertextBlob = Place your ciphertext here;

DecryptRequest req = new
 DecryptRequest().withCiphertextBlob(ciphertextBlob).withKeyId(keyId);
ByteBuffer plainText = kmsClient.decrypt(req).getPlaintext();
```

C#

Para obtener más información, consulte el método Decrypt en el AWS SDK for .NET.

```
// Decrypt a data key
//
// Replace the following example key ARN with any valid key identfier
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
```

```
MemoryStream ciphertextBlob = new MemoryStream();
// Write ciphertext to memory stream

DecryptRequest decryptRequest = new DecryptRequest()
{
    CiphertextBlob = ciphertextBlob,
    KeyId = keyId
};
MemoryStream plainText = kmsClient.Decrypt(decryptRequest).Plaintext;
```

Python

Para obtener más información, consulte el método decrypt en la AWS SDK for Python (Boto3).

```
# Decrypt a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
ciphertext = 'Place your ciphertext here'

response = kms_client.decrypt(
    CiphertextBlob=ciphertext,
    KeyId=key_id
)

plaintext = response['Plaintext']
```

Ruby

Para obtener más información, consulte el método de instancia decrypt en el AWS SDK for Ruby.

```
# Decrypt a data key

# Replace the following example key ARN with any valid key identfier
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

ciphertext = 'Place your ciphertext here'
ciphertext_packed = [ciphertext].pack("H*")

response = kmsClient.decrypt({
```

```
  ciphertext_blob: ciphertext_packed,
  key_id: key_id
})

plaintext = response.plaintext
```

PHP

Para obtener más información, consulte el método Decrypt en el AWS SDK for PHP.

```
// Decrypt a data key
//
// Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$ciphertext = 'Place your cipher text blob here';

$result = $KmsClient->decrypt([
     'CiphertextBlob' => $ciphertext,
     'KeyId' => $keyId,
]);

$plaintext = $result['Plaintext'];
```

Node.js

Para obtener más información, consulta la propiedad decrypt en el AWSSDK de Node.js JavaScript .

```
// Decrypt a data key
//
// Replace the following example key ARN with any valid key identfier
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const CiphertextBlob = 'Place your cipher text blob here';
kmsClient.decrypt({ CiphertextBlob, KeyId }, (err, data) => {
  if (err) console.log(err, err.stack); // an error occurred
  else {
    const { Plaintext } = data;
    ...
  }
});
```

PowerShell

Para descifrar una clave de datos, utilice el cmdlet Invoke-KMSEncrypt.

Este cmdlet devuelve el texto sin formato en forma de (System.IO). MemoryStream MemoryStream) objeto. Para convertirlo en una matriz de bytes, utilice cmdlets o funciones que conviertan objetos `MemoryStream` en matrices de bytes, como las funciones del módulo Convert.

Dado que este ejemplo utiliza el texto cifrado devuelto por un cmdlet de cifrado de AWS KMS, utiliza un objeto `MemoryStream` para el valor del parámetro `CiphertextBlob`. Sin embargo, el parámetro `CiphertextBlob` de `Invoke-KMSDecrypt` toma una matriz de bytes (`byte[]`); no requiere un objeto `MemoryStream`. A partir de la AWSPowerShell versión 4.0, los parámetros de todos los AWSPowerShell módulos que utilizan matrices de bytes y `MemoryStream` objetos aceptan matrices de bytes, `MemoryStream` objetos, cadenas, matrices de cadenas y `FileInfo` (System.IO). FileInfo) objetos. Puede pasar cualquiera de estos tipos a `Invoke-KMSDecrypt`.

```
# Decrypt a data key
# Replace the following example key ARN with any valid key identfier
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

[System.IO.MemoryStream]$ciphertext = Read-Host 'Place your cipher text blob here'

$response = Invoke-KMSDecrypt -CiphertextBlob $ciphertext -KeyId $keyId
$plaintext = $response.Plaintext
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools. KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Volver a cifrar una clave de datos con otra AWS KMS key

Para descifrar una clave de datos cifrada y volver a cifrarla inmediatamente con una clave diferenteAWS KMS key, utilice la operación. ReEncrypt Las operaciones se realizan en su totalidad en el servidor en AWS KMS, por lo que su texto no cifrado nunca se expondrá fuera de AWS KMS.

El `ciphertextBlob` que especifique debe ser el valor del `CiphertextBlob` campo de una respuesta GenerateDataKey, o Cifrar GenerateDataKeyWithoutPlaintext, o el `PrivateKeyCiphertextBlob` campo de una respuesta o.

GenerateDataKeyPairGenerateDataKeyPairWithoutPlaintext También puede utilizar la operación `ReEncrypt` para volver a cifrar los datos cifrados fuera de AWS KMS por la clave pública en una clave KMS asimétrica.

El parámetro `SourceKeyId` no es necesario al volver a cifrar con claves simétricas KMS de codificación. AWS KMS puede obtener la clave KMS que se usó para cifrar los datos de los metadatos en el blob de texto cifrado. Pero siempre es una práctica recomendada especificar la clave KMS que está utilizando. Esta práctica garantiza que utilice la clave KMS deseada y le impide descifrar inadvertidamente un texto cifrado utilizando una clave KMS en la que no confía.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más detalles, consulte el método reEncrypt en la Referencia de la API de la AWS SDK for Java.

```
// Re-encrypt a data key

ByteBuffer sourceCiphertextBlob = Place your ciphertext here;

// Replace the following example key ARNs with valid key identfiers
String sourceKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String destinationKeyId = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

ReEncryptRequest req = new ReEncryptRequest();
req.setCiphertextBlob(sourceCiphertextBlob);
req.setSourceKeyId(sourceKeyId);
req.setDestinationKeyId(destinationKeyId);
ByteBuffer destinationCipherTextBlob = kmsClient.reEncrypt(req).getCiphertextBlob();
```

C#

Para obtener más información, consulte el método ReEncrypt en AWS SDK for .NET.

```
// Re-encrypt a data key

MemoryStream sourceCiphertextBlob = new MemoryStream();
// Write ciphertext to memory stream
```

```
// Replace the following example key ARNs with valid key identfiers
String sourceKeyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String destinationKeyId = "arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321";

ReEncryptRequest reEncryptRequest = new ReEncryptRequest()
{
    CiphertextBlob = sourceCiphertextBlob,
    SourceKeyId = sourceKeyId,
    DestinationKeyId = destinationKeyId
};
MemoryStream destinationCipherTextBlob =
 kmsClient.ReEncrypt(reEncryptRequest).CiphertextBlob;
```

Python

Para obtener más información, consulte el método `re_encrypt` en AWS SDK for Python (Boto3).

```
# Re-encrypt a data key
ciphertext = 'Place your ciphertext here'

# Replace the following example key ARNs with valid key identfiers
source_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
destination_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321'

response = kms_client.re_encrypt(
    CiphertextBlob=ciphertext,
    SourceKeyId=source_key_id,
    DestinationKeyId=destination_key_id
)

destination_ciphertext_blob = response['CiphertextBlob']
```

Ruby

Para obtener más información, consulte el método de instancia `re_encrypt` en AWS SDK for Ruby.

```
# Re-encrypt a data key

ciphertext = 'Place your ciphertext here'
ciphertext_packed = [ciphertext].pack("H*")

# Replace the following example key ARNs with valid key identfiers
source_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
destination_key_id = 'arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321'

response = kmsClient.re_encrypt({
  ciphertext_blob: ciphertext_packed,
  source_key_id: source_key_id,
  destination_key_id: destination_key_id
})

destination_ciphertext_blob = response.ciphertext_blob.unpack('H*')
```

PHP

Para obtener más información, consulte el método ReEncrypt en AWS SDK for PHP.

```
// Re-encrypt a data key

$ciphertextBlob = 'Place your ciphertext here';

// Replace the following example key ARNs with valid key identfiers
$sourceKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$destinationKeyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321';

$result = $KmsClient->reEncrypt([
    'CiphertextBlob' => $ciphertextBlob,
    'SourceKeyId' => $sourceKeyId,
    'DestinationKeyId' => $destinationKeyId,
]);
```

Node.js

Para obtener más información, consulta la propiedad ReEncrypt en AWSel SDK JavaScript de Node.js.

```
// Re-encrypt a data key
const CiphertextBlob = 'Place your cipher text blob here';
// Replace the following example key ARNs with valid key identfiers
const SourceKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const DestinationKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321';

kmsClient.reEncrypt({ CiphertextBlob, SourceKeyId, DestinationKeyId }, (err, data)
 => {
  ...
});
```

PowerShell

Para volver a cifrar un texto cifrado con la misma clave de KMS o con una diferente, utilice el cmdlet Invoke-KMS. ReEncrypt

Dado que este ejemplo utiliza el texto cifrado devuelto por un cmdlet de cifrado de AWS KMS, utiliza un objeto `MemoryStream` para el valor del parámetro `CiphertextBlob`. Sin embargo, el parámetro `CiphertextBlob` de `Invoke-KMSReEncrypt` toma una matriz de bytes (`byte[]`); no requiere un objeto `MemoryStream`. A partir de la AWSPowerShell versión 4.0, los parámetros de todos los AWSPowerShell módulos que utilizan matrices de bytes y `MemoryStream` objetos aceptan matrices de bytes, objetos, cadenas, `MemoryStream` matrices de cadenas y (System.IO). `FileInfo` FileInfo) objetos. Puede pasar cualquiera de estos tipos a `Invoke-KMSReEncrypt`.

```
# Re-encrypt a data key

[System.IO.MemoryStream]$ciphertextBlob = Read-Host 'Place your cipher text blob
 here'

# Replace the following example key ARNs with valid key identfiers
$sourceKeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$destinationKeyId = 'arn:aws:kms:us-west-2:111122223333:key/0987dcba-09fe-87dc-65ba-
ab0987654321'

$response = Invoke-KMSReEncrypt -Ciphertext $ciphertextBlob -SourceKeyId
 $sourceKeyId -DestinationKeyId $destinationKeyId
$reEncryptedCiphertext = $response.CiphertextBlob
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la Guía del usuario de AWS Tools for Windows PowerShell.

Trabajar con las políticas de claves

Los ejemplos de este tema utilizan la API de AWS KMS para ver y cambiar las políticas de claves de AWS KMS keys.

Para obtener más detalles acerca de cómo utilizar las políticas de claves y las políticas de IAM para administrar el acceso a sus claves KMS, consulte Autenticación y control de acceso de AWS KMS. Para obtener ayuda sobre cómo escribir y dar formato a un documento de política JSON, consulte la Referencia de políticas JSON de IAM en la Guía de usuario de IAM.

Temas

- Mostrar los nombres de las políticas de claves
- Obtener una política de claves
- Configurar una política de claves

Mostrar los nombres de las políticas de claves

Para obtener los nombres de las políticas clave de unAWS KMS key, utilice la ListKeyPoliciesoperación. El único nombre de política de claves que se devuelve es default.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más información sobre la implementación de Java, consulta el listKeyPolicies método en la referencia de la AWS SDK for Java API.

```
// List key policies
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
```

```
ListKeyPoliciesRequest req = new ListKeyPoliciesRequest().withKeyId(keyId);
ListKeyPoliciesResult result = kmsClient.listKeyPolicies(req);
```

C#

Para obtener más información, consulte el método ListKeyPolicies en AWS SDK for .NET.

```
// List key policies
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

ListKeyPoliciesRequest listKeyPoliciesRequest = new ListKeyPoliciesRequest()
{
    KeyId = keyId
};
ListKeyPoliciesResponse listKeyPoliciesResponse =
 kmsClient.ListKeyPolicies(listKeyPoliciesRequest);
```

Python

Para obtener más información, consulte el método `list_key_policies` en AWS SDK for Python (Boto3).

```
# List key policies

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.list_key_policies(
    KeyId=key_id
)
```

Ruby

Para obtener más información, consulte el método de instancia `list_key_policies` en AWS SDK for Ruby.

```
# List key policies
```

```
# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.list_key_policies({
  key_id: key_id
})
```

PHP

Para obtener más información, consulte el método ListKeyPolicies en AWS SDK for PHP.

```
// List key policies
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

$result = $KmsClient->listKeyPolicies([
    'KeyId' => $keyId
]);
```

Node.js

Para obtener más información, consulta la listKeyPolicies propiedad en el AWSSDK correspondiente JavaScript a Node.js.

```
// List key policies
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

kmsClient.listKeyPolicies({ KeyId }, (err, data) => {
  ...
});
```

PowerShell

Para mostrar el nombre de la política de claves predeterminada, utilice el cmdlet Get-KMS KeyPolicyList.

```
# List key policies
```

```
# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$response = Get-KMSKeyPolicyList -KeyId $keyId
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Obtener una política de claves

Para obtener la política clave de unAWS KMS key, utilice la GetKeyPolicyoperación.

GetKeyPolicy requiere un nombre de política. El único nombre de política válido es default.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más información, consulta el getKeyPolicy método en la referencia AWS SDK for Java de la API.

```
// Get the policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String policyName = "default";

GetKeyPolicyRequest req = new
 GetKeyPolicyRequest().withKeyId(keyId).withPolicyName(policyName);
GetKeyPolicyResult result = kmsClient.getKeyPolicy(req);
```

C#

Para obtener más información, consulte el método GetKeyPolicy en AWS SDK for .NET.

```
// Get the policy for a KMS key
```

```
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String policyName = "default";

GetKeyPolicyRequest getKeyPolicyRequest = new GetKeyPolicyRequest()
{
    KeyId = keyId,
    PolicyName = policyName
};
GetKeyPolicyResponse getKeyPolicyResponse =
 kmsClient.GetKeyPolicy(getKeyPolicyRequest);
```

Python

Para obtener más información, consulte el método `get_key_policy` en AWS SDK for Python (Boto3).

```
# Get the policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
policy_name = 'default'

response = kms_client.get_key_policy(
    KeyId=key_id,
    PolicyName=policy_name
)
```

Ruby

Para obtener más información, consulte el método de instancia `get_key_policy` en AWS SDK for Ruby.

```
# Get the policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
policy_name = 'default'
```

```
response = kmsClient.get_key_policy({
  key_id: key_id,
  policy_name: policy_name
})
```

PHP

Para obtener más información, consulte el método GetKeyPolicy en AWS SDK for PHP.

```
// Get the policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$policyName = "default";

$result = $KmsClient->getKeyPolicy([
    'KeyId' => $keyId,
    'PolicyName' => $policyName
]);
```

Node.js

Para obtener más información, consulta la getKeyPolicy propiedad en el AWSSDK de JavaScript Node.js.

```
// Get the policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const PolicyName = 'default';
kmsClient.getKeyPolicy({ KeyId, PolicyName }, (err, data) => {
  ...
});
```

PowerShell

Para obtener la política de claves de una clave de KMS, utilice el cmdlet Get-KMS KeyPolicy. Este cmdlet devuelve la política de claves en forma de cadena (System.String) que se puede usar en un comando Write-KMS (). KeyPolicy `PutKeyPolicy` Para convertir las políticas de la cadena JSON en `PSCustomObject` objetos, usa el cmdlet -JSON. ConvertFrom

```
# Get the policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$policyName = 'default'

$response = Get-KMSKeyPolicy -KeyId $keyId -PolicyName $policyName
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Configurar una política de claves

Para crear o reemplazar la política de claves por una clave de KMS, utilice la PutKeyPolicyoperación.

`PutKeyPolicy` requiere un nombre de política. El único nombre de política válido es default.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más información, consulte el putKeyPolicy método en la referencia AWS SDK for Java de la API.

```
// Set a key policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String policyName = "default";
String policy = "{" +
                "  \"Version\": \"2012-10-17\"," +
                "  \"Statement\": [{" +
                "    \"Sid\": \"Allow access for ExampleRole\"," +
                "    \"Effect\": \"Allow\"," +
                // Replace the following example user ARN with a valid one
                "    \"Principal\": {\"AWS\": \"arn:aws:iam::111122223333:role/
ExampleKeyUserRole\"}," +
```

```
                "    \"Action\": [" +
                "      \"kms:Encrypt\"," +
                "      \"kms:GenerateDataKey*\"," +
                "      \"kms:Decrypt\"," +
                "      \"kms:DescribeKey\"," +
                "      \"kms:ReEncrypt*\"" +
                "    ]," +
                "    \"Resource\": \"*\"" +
                "  }]" +
                "}";

PutKeyPolicyRequest req = new
 PutKeyPolicyRequest().withKeyId(keyId).withPolicy(policy).withPolicyName(policyName);
kmsClient.putKeyPolicy(req);
```

C#

Para obtener más información, consulte el método PutKeyPolicy en AWS SDK for .NET.

```
// Set a key policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String policyName = "default";
String policy = "{" +
                "  \"Version\": \"2012-10-17\"," +
                "  \"Statement\": [{" +
                "    \"Sid\": \"Allow access for ExampleUser\"," +
                "    \"Effect\": \"Allow\"," +
                // Replace the following example user ARN with a valid one
                "    \"Principal\": {\"AWS\": \"arn:aws:iam::111122223333:role/
ExampleKeyUserRole\"}," +
                "    \"Action\": [" +
                "      \"kms:Encrypt\"," +
                "      \"kms:GenerateDataKey*\"," +
                "      \"kms:Decrypt\"," +
                "      \"kms:DescribeKey\"," +
                "      \"kms:ReEncrypt*\"" +
                "    ]," +
                "    \"Resource\": \"*\"" +
                "  }]" +
                "}";
```

```
PutKeyPolicyRequest putKeyPolicyRequest = new PutKeyPolicyRequest()
{
    KeyId = keyId,
    Policy = policy,
    PolicyName = policyName
};
kmsClient.PutKeyPolicy(putKeyPolicyRequest);
```

Python

Para obtener más información, consulte el método `put_key_policy` en AWS SDK for Python (Boto3).

```
# Set a key policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
policy_name = 'default'
policy = """
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "Allow access for ExampleUser",
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
        "Action": [
            "kms:Encrypt",
            "kms:GenerateDataKey*",
            "kms:Decrypt",
            "kms:DescribeKey",
            "kms:ReEncrypt*"
        ],
        "Resource": "*"
    }]
}"""

response = kms_client.put_key_policy(
    KeyId=key_id,
    Policy=policy,
    PolicyName=policy_name
)
```

Ruby

Para obtener más información, consulte el método de instancia put_key_policy en AWS SDK for Ruby.

```
# Set a key policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
policy_name = 'default'
policy = "{" +
  "  \"Version\": \"2012-10-17\"," +
  "  \"Statement\": [{" +
  "    \"Sid\": \"Allow access for ExampleUser\"," +
  "    \"Effect\": \"Allow\"," +
  # Replace the following example user ARN with a valid one
  "    \"Principal\": {\"AWS\": \"arn:aws:iam::111122223333:role/ExampleKeyUserRole
\"}," +
  "    \"Action\": [" +
  "      \"kms:Encrypt\"," +
  "      \"kms:GenerateDataKey*\"," +
  "      \"kms:Decrypt\"," +
  "      \"kms:DescribeKey\"," +
  "      \"kms:ReEncrypt*\"" +
  "    ]," +
  "    \"Resource\": \"*\"" +
  "  }]" +
  "}"

response = kmsClient.put_key_policy({
  key_id: key_id,
  policy: policy,
  policy_name: policy_name
})
```

PHP

Para obtener más información, consulte el método PutKeyPolicy en AWS SDK for PHP.

```
// Set a key policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
```

```
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$policyName = "default";

$result = $KmsClient->putKeyPolicy([
    'KeyId' => $keyId,
    'PolicyName' => $policyName,
    'Policy' => '{
        "Version": "2012-10-17",
        "Id": "custom-policy-2016-12-07",
        "Statement": [
            { "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal":
               { "AWS": "arn:aws:iam::111122223333:user/root" },
            "Action": [ "kms:*" ],
            "Resource": "*" },
            { "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal":
               { "AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole" },
            "Action": [
                "kms:Encrypt*",
                "kms:GenerateDataKey*",
                "kms:Decrypt*",
                "kms:DescribeKey*",
                "kms:ReEncrypt*"
            ],
            "Resource": "*" }
        ]
    } '
]);
```

Node.js

Para obtener más información, consulta la putKeyPolicy propiedad en el AWSSDK de JavaScript Node.js.

```
// Set a key policy for a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
```

```
const PolicyName = 'default';
const Policy = `{
    "Version": "2012-10-17",
    "Id": "custom-policy-2016-12-07",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:GenerateDataKey*",
                "kms:Decrypt*",
                "kms:DescribeKey*",
                "kms:ReEncrypt*"
            ],
            "Resource": "*"
        }
    ]
}`; // The key policy document

kmsClient.putKeyPolicy({ KeyId, Policy, PolicyName }, (err, data) => {
  ...
});
```

PowerShell

Para establecer una política de claves para una clave de KMS, utilice el cmdlet Write-KMS KeyPolicy. Este cmdlet no devuelve ningún resultado. Para comprobar la eficacia del comando, utilice el cmdlet Get-KMS. KeyPolicy

El parámetro `Policy` toma una cadena. Incluya la cadena entre comillas simples para convertirla en una cadena literal. No es necesario utilizar caracteres de continuación o caracteres de escape en la cadena literal.

```
# Set a key policy for a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$policyName = 'default'
$policy = '{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"
            },
            "Action": [
                "kms:Encrypt*",
                "kms:GenerateDataKey*",
                "kms:Decrypt*",
                "kms:DescribeKey*",
                "kms:ReEncrypt*"
            ],
            "Resource": "*"
        }]
    }'

Write-KMSKeyPolicy -KeyId $keyId -PolicyName $policyName -Policy $policy
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la Guía del usuario de AWS Tools for Windows PowerShell.

Trabajar con concesiones

Los ejemplos de este tema utilizan la API de AWS KMS para crear, ver, retirar y revocar concesiones en AWS KMS keys. Para obtener más información sobre el uso de concesiones en AWS KMS, consulte Concesiones en AWS KMS.

Temas

- Crear una concesión
- Consultar una concesión
- Retirar una concesión
- Revocar una concesión

Crear una concesión

Para crear una concesión para unAWS KMS key, utilice la CreateGrantoperación. La respuesta incluye solo el ID de concesión y el token de concesión. Para obtener información detallada sobre la subvención, utilice la ListGrantsoperación, tal y como se muestra enConsultar una concesión.

Estos ejemplos crean una concesión que permite a los usuarios que pueden asumir el `ExampleKeyUser` rol llamar a la GenerateDataKeyoperación con la clave KMS identificada por el `KeyId` parámetro.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para conocer detalles, consulte el método createGrant en la Referencia de la API de AWS SDK for Java.

```
// Create a grant
//
// Replace the following example key ARN with a valid key ID or key ARN
```

```
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String granteePrincipal = "arn:aws:iam::111122223333:role/ExampleKeyUser";
String operation = GrantOperation.GenerateDataKey.toString();

CreateGrantRequest request = new CreateGrantRequest()
    .withKeyId(keyId)
    .withGranteePrincipal(granteePrincipal)
    .withOperations(operation);

CreateGrantResult result = kmsClient.createGrant(request);
```

C#

Para obtener más información, consulte el método CreateGrant en AWS SDK for .NET.

```
// Create a grant
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String granteePrincipal = "arn:aws:iam::111122223333:role/ExampleKeyUser";
String operation = GrantOperation.GenerateDataKey;

CreateGrantRequest createGrantRequest = new CreateGrantRequest()
{
    KeyId = keyId,
    GranteePrincipal = granteePrincipal,
    Operations = new List<string>() { operation }
};

CreateGrantResponse createGrantResult = kmsClient.CreateGrant(createGrantRequest);
```

Python

Para obtener más información, consulte el método `create_grant` en AWS SDK for Python (Boto3).

```
# Create a grant

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
```

```
grantee_principal = 'arn:aws:iam::111122223333:role/ExampleKeyUser'
operation = ['GenerateDataKey']

response = kms_client.create_grant(
    KeyId=key_id,
    GranteePrincipal=grantee_principal,
    Operations=operation
)
```

Ruby

Para obtener más información, consulte el método de instancia `create_grant` en AWS SDK for Ruby.

```
# Create a grant

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
grantee_principal = 'arn:aws:iam::111122223333:role/ExampleKeyUser'
operation = ['GenerateDataKey']

response = kmsClient.create_grant({
  key_id: key_id,
  grantee_principal: grantee_principal,
  operations: operation
})
```

PHP

Para obtener más información, consulte el método CreateGrant en AWS SDK for PHP.

```
// Create a grant
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$granteePrincipal = "arn:aws:iam::111122223333:role/ExampleKeyUser";
$operation = ['GenerateDataKey']

$result = $KmsClient->createGrant([
    'GranteePrincipal' => $granteePrincipal,
    'KeyId' => $keyId,
```

```
    'Operations' => $operation
]);
```

Node.js

Para obtener más información, consulta la propiedad CreateGrant en AWSel SDK JavaScript de Node.js.

```
// Create a grant
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const GranteePrincipal = 'arn:aws:iam::111122223333:role/ExampleKeyUser';
const Operations: ["GenerateDataKey"];
kmsClient.createGrant({ KeyId, GranteePrincipal, Operations }, (err, data) => {
  ...
});
```

PowerShell

Para crear una concesión, utilice el cmdlet New-KMSGrant.

```
# Create a grant

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$granteePrincipal = 'arn:aws:iam::111122223333:role/ExampleKeyUser'
$operation = 'GenerateDataKey'

$response = New-KMSGrant -GranteePrincipal $granteePrincipal -KeyId $keyId -
Operation $operation
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Consultar una concesión

Para obtener información detallada sobre las concesiones de una clave KMS, utilice la ListGrantsoperación.

> **Note**
>
> El campo `GranteePrincipal` de la respuesta `ListGrants` generalmente contiene el principal beneficiario de la concesión. Sin embargo, cuando el principal beneficiario de la concesión es un servicio de AWS, el campo `GranteePrincipal` contiene la entidad principal de servicio, que puede representar varios beneficiarios principales distintos.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Estos ejemplos utilizan el parámetro opcional `Limits`, que determina cuántas concesiones devuelve la operación.

Java

Para obtener más detalles sobre la implementación de Java, consulte el método listGrants en la Referencia de la API de AWS SDK for Java.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
Integer limit = 10;

ListGrantsRequest req = new ListGrantsRequest().withKeyId(keyId).withLimit(limit);
ListGrantsResult result = kmsClient.listGrants(req);
```

C#

Para obtener más información, consulte el método ListGrants en AWS SDK for .NET.

```
// Listing grants on a KMS key
//
```

```
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
int limit = 10;

ListGrantsRequest listGrantsRequest = new ListGrantsRequest()
{
    KeyId = keyId,
    Limit = limit
};
ListGrantsResponse listGrantsResponse = kmsClient.ListGrants(listGrantsRequest);
```

Python

Para obtener más información, consulte el método `list_grants` en AWS SDK for Python (Boto3).

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kms_client.list_grants(
    KeyId=key_id,
    Limit=10
)
```

Ruby

Para obtener más información, consulte el método de instancia `list_grants` en AWS SDK for Ruby.

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

response = kmsClient.list_grants({
  key_id: key_id,
  limit: 10
```

```
})
```

PHP

Para obtener más información, consulte el método ListGrants en AWS SDK for PHP.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$limit = 10;

$result = $KmsClient->listGrants([
    'KeyId' => $keyId,
    'Limit' => $limit,
]);
```

Node.js

Para obtener más información, consulta la propiedad ListGrants en el AWSSDK o JavaScript en Node.js.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const Limit = 10;
kmsClient.listGrants({ KeyId, Limit }, (err, data) => {
  ...
});
```

PowerShell

Para ver los detalles de todas las AWS KMS concesiones de una clave KMS, usa el cmdlet GrantListGet-KMS.

Para limitar el número de objetos de salida, este ejemplo usa el cmdlet Select-Object en lugar del parámetro `Limit`, que está quedando obsoleto en los cmdlet de la lista. Para obtener asistencia con la paginación de salida en AWS Tools for PowerShell, vea Paginación de salida con AWS Tools for PowerShell.

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$limit = 10

$response = Get-KMSGrantList -KeyId $keyId | Select-Object -First $limit
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Debe especificar la clave KMS en cada operación `ListGrants`. Sin embargo, puede filtrar más la lista de concesiones especificando el ID de concesión o un principal beneficiario. Los siguientes ejemplos solo obtienen las concesiones para una clave KMS donde el rol de `test-engineer` es el principal beneficiario.

Java

Para obtener más detalles sobre la implementación de Java, consulte el método listGrants en la Referencia de la API de AWS SDK for Java.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String grantee = "arn:aws:iam::111122223333:role/test-engineer";

ListGrantsRequest req = new
 ListGrantsRequest().withKeyId(keyId).withGranteePrincipal(grantee);
ListGrantsResult result = kmsClient.listGrants(req);
```

C#

Para obtener más información, consulte el método ListGrants en AWS SDK for .NET.

```
// Listing grants on a KMS key
//
```

```
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";
String grantee = "arn:aws:iam::111122223333:role/test-engineer";

ListGrantsRequest listGrantsRequest = new ListGrantsRequest()
{
    KeyId = keyId,
    GranteePrincipal = grantee
};
ListGrantsResponse listGrantsResponse = kmsClient.ListGrants(listGrantsRequest);
```

Python

Para obtener más información, consulte el método `list_grants` en AWS SDK for Python (Boto3).

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
grantee = 'arn:aws:iam::111122223333:role/test-engineer'

response = kms_client.list_grants(
    KeyId=key_id,
    GranteePrincipal=grantee
)
```

Ruby

Para obtener más información, consulte el método de instancia `list_grants` en AWS SDK for Ruby.

```
# Listing grants on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
grantee = 'arn:aws:iam::111122223333:role/test-engineer'

response = kmsClient.list_grants({
  key_id: keyId,
```

```
  grantee_principal: grantee
})
```

PHP

Para obtener más información, consulte el método ListGrants en AWS SDK for PHP.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
$grantee = 'arn:aws:iam::111122223333:role/test-engineer';

$result = $KmsClient->listGrants([
    'KeyId' => $keyId,
    'GranteePrincipal' => $grantee,
]);
```

Node.js

Para obtener más información, consulta la propiedad ListGrants en el AWSSDK o JavaScript en Node.js.

```
// Listing grants on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';
const Grantee = 'arn:aws:iam::111122223333:role/test-engineer';

kmsClient.listGrants({ KeyId, Grantee }, (err, data) => {
  ...
});
```

PowerShell

Para ver los detalles de todas las AWS KMS concesiones de una clave KMS, usa el cmdlet GrantListGet-KMS.

```
# Listing grants on a KMS key
```

```
# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'
$grantee = 'arn:aws:iam::111122223333:role/test-engineer'
$response = Get-KMSGrantList -KeyId $keyId -GranteePrincipal $grantee
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Retirar una concesión

Para retirar la concesión de una clave KMS, utilice la RetireGrantoperación. Debe retirar una concesión para efectuar limpieza después de utilizarla.

Para retirar una concesión, proporcione el token de la concesión o ambos, el ID de la concesión y el ID de la clave KMS. Para esta operación, el ID de clave KMS debe ser Nombre de recurso de Amazon (ARN) de la clave KMS. La CreateGrantoperación devuelve el token de concesión. Las ListGrantsoperaciones CreateGrant y devuelven el ID de concesión.

RetireGrant no devuelve una respuesta. Para comprobar que fue eficaz, utilice la ListGrantsoperación.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más detalles, consulte el método retireGrant en la Referencia de la API de AWS SDK for Java.

```
// Retire a grant
//
String grantToken = Place your grant token here;

RetireGrantRequest req = new RetireGrantRequest().withGrantToken(grantToken);
kmsClient.retireGrant(req);
```

C#

Para obtener más información, consulte el método RetireGrant en AWS SDK for .NET.

```
// Retire a grant
//
String grantToken = "Place your grant token here";

RetireGrantRequest retireGrantRequest = new RetireGrantRequest()
{
    GrantToken = grantToken
};
kmsClient.RetireGrant(retireGrantRequest);
```

Python

Para obtener más información, consulte el método `retire_grant` en AWS SDK for Python (Boto3).

```
# Retire a grant

grant_token = Place your grant token here

response = kms_client.retire_grant(
    GrantToken=grant_token
)
```

Ruby

Para obtener más información, consulte el método de instancia `retire_grant` en AWS SDK for Ruby.

```
# Retire a grant

grant_token = Place your grant token here

response = kmsClient.retire_grant({
  grant_token: grant_token
})
```

PHP

Para obtener más información, consulte el método RetireGrant en AWS SDK for PHP.

```
// Retire a grant
//
```

```
$grantToken = 'Place your grant token here';

$result = $KmsClient->retireGrant([
    'GrantToken' => $grantToken,
]);
```

Node.js

Para obtener más información, consulte la propiedad RetireGrant en AWSel SDK JavaScript de Node.js.

```
// Retire a grant
//
const GrantToken = 'Place your grant token here';
kmsClient.retireGrant({ GrantToken }, (err, data) => {
  ...
});
```

PowerShell

Para retirar una concesión, utilice el cmdlet Disable-KMSGrant. Para obtener el token de concesión, utilice el cmdlet New-KMSGrant. El parámetro `GrantToken` toma una cadena, por lo que no es necesario convertir la salida que devuelve el cmdlet Read-Host.

```
# Retire a grant

$grantToken = Read-Host -Message Place your grant token here
Disable-KMSGrant -GrantToken $grantToken
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Revocar una concesión

Para revocar una concesión a una clave KMS, utilice la RevokeGrantoperación. Puede revocar una concesión para denegar explícitamente las operaciones que dependen de ella.

En los idiomas que requieren un objeto cliente, estos ejemplos usan el objeto cliente de AWS KMS que ha creado en Crear un cliente.

Java

Para obtener más detalles, consulte el método revokeGrant en la Referencia de la API de AWS SDK for Java.

```
// Revoke a grant on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

// Replace the following example grant ID with a valid one
String grantId = "grant1";

RevokeGrantRequest req = new
 RevokeGrantRequest().withKeyId(keyId).withGrantId(grantId);
kmsClient.revokeGrant(req);
```

C#

Para obtener más información, consulte el método RevokeGrant en AWS SDK for .NET.

```
// Revoke a grant on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
String keyId = "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab";

// Replace the following example grant ID with a valid one
String grantId = "grant1";

RevokeGrantRequest revokeGrantRequest = new RevokeGrantRequest()
{
    KeyId = keyId,
    GrantId = grantId
};
kmsClient.RevokeGrant(revokeGrantRequest);
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la AWS Tools for Windows PowerShellGuía del usuario de .

Python

Para obtener más información, consulte el método `revoke_grant` en AWS SDK for Python (Boto3).

```
# Revoke a grant on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

# Replace the following example grant ID with a valid one
grant_id = 'grant1'

response = kms_client.revoke_grant(
    KeyId=key_id,
    GrantId=grant_id
)
```

Ruby

Para obtener más información, consulte el método de instancia `revoke_grant` en AWS SDK for Ruby.

```
# Revoke a grant on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
key_id = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

# Replace the following example grant ID with a valid one
grant_id = 'grant1'

response = kmsClient.revoke_grant({
  key_id: key_id,
  grant_id: grant_id
})
```

PHP

Para obtener más información, consulte el método RevokeGrant en AWS SDK for PHP.

```
// Revoke a grant on a KMS key
```

```
//
// Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

// Replace the following example grant ID with a valid one
$grantId = "grant1";

$result = $KmsClient->revokeGrant([
    'KeyId' => $keyId,
    'GrantId' => $grantId,
]);
```

Node.js

Para obtener más información, consulta la propiedad RevokeGrant en AWSel SDK JavaScript o en Node.js.

```
// Revoke a grant on a KMS key
//
// Replace the following example key ARN with a valid key ID or key ARN
const KeyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab';

// Replace the following example grant ID with a valid one
const GrantId = 'grant1';
kmsClient.revokeGrant({ GrantId, KeyId }, (err, data) => {
  ...
});
```

PowerShell

Para revocar una concesión, utilice el cmdlet Revoke-KMSGrant.

```
# Revoke a grant on a KMS key

# Replace the following example key ARN with a valid key ID or key ARN
$keyId = 'arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab'

# Replace the following example grant ID with a valid one
$grantId = 'grant1'
```

```
Revoke-KMSGrant -KeyId $keyId -GrantId $grantId
```

Para usar los AWS KMS PowerShell cmdlets, instale AWS.Tools.KeyManagementServicemódulo. Para obtener más información, consulte la Guía del usuario de AWS Tools for Windows PowerShell.

Pruebas de llamadas a la API de AWS KMS

Para utilizar AWS KMS, debe tener credenciales que AWS pueda utilizar para autenticar las solicitudes a la API. Las credenciales deben incluir permisos para obtener acceso a las claves de KMS y alias. Los permisos vienen determinados por las políticas de claves, las políticas de IAM, las concesiones y los controles de acceso entre cuentas. Además de controlar el acceso a las claves de KMS, puede controlar el acceso a su CloudHSM y a los almacenes de claves personalizados.

Puede especificar el parámetro `DryRun` de la API para comprobar que dispone de los permisos necesarios para utilizar las claves de AWS KMS. También puede utilizar `DryRun` para comprobar que los parámetros de solicitud de una llamada a la API de AWS KMS estén especificados correctamente.

Temas

- ¿Cuál es el DryRun parámetro?
- Especificar DryRun con la API

¿Cuál es el DryRun parámetro?

`DryRun` es un parámetro de API opcional que se especifica para comprobar que las llamadas a la API de AWS KMS se realizan correctamente. Use `DryRun` para probar la llamada a la API antes de hacer una llamada a AWS KMS. Puede comprobar lo siguiente:

- Que cuenta con los permisos necesarios para utilizar las claves de AWS KMS.
- Que ha especificado correctamente los parámetros de la llamada.

AWS KMS admite el uso del parámetro `DryRun` en determinadas acciones de la API:

- CreateGrant
- Decrypt

- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- ReEncrypt
- RetireGrant
- RevokeGrant
- Sign
- Verificar
- VerifyMac

El uso del parámetro `DryRun` generará cargos y se facturará como una solicitud a la API estándar. Para obtener más información sobre los precios de AWS KMS, consulte Precios de AWS Key Management Service.

Todas las solicitudes a la API que utilizan el parámetro `DryRun` se aplican a la cuota de solicitudes a la API y pueden dar lugar a una excepción de limitación si se supera una cuota de solicitudes a la API. Por ejemplo, llamar a Decrypt con `DryRun` o sin `DryRun` cuenta para la misma cuota de operaciones criptográficas. Consulte Limitar las solicitudes AWS KMS para obtener más información.

Cada llamada a una operación de la API de AWS KMS se captura como un evento y se incluye en un registro de AWS CloudTrail. El resultado de cualquier operación que especifique el `DryRun` parámetro aparece en el CloudTrail registro. Para obtener más información, consulte Registrar llamadas a la AWS KMS API con AWS CloudTrail.

Especificar DryRun con la API

Para usar `DryRun`, especifique el parámetro `–dry-run` en los comandos de la AWS CLI y las llamadas a la API de AWS KMS que admiten el parámetro. Cuando lo haga, AWS KMS comprobará si la llamada se ha realizado correctamente. Las llamadas a AWS KMS que utilicen `DryRun` siempre fallarán y devolverán un mensaje con información sobre el motivo por el que se produjo el error en la llamada. El mensaje puede incluir las siguientes excepciones:

- `DryRunOperationException`: la solicitud se realizaría correctamente si `DryRun` no se especificara.
- `ValidationException`: se produjo un error en la solicitud al especificar un parámetro de API incorrecto.
- `AccessDeniedException`: no tiene permisos para realizar la acción de API especificada en el recurso de KMS.

Por ejemplo, el siguiente comando usa la CreateGrantoperación y crea una concesión que permite a los usuarios autorizados a asumir la `keyUserRole` función llamar a la operación de descifrado en una clave KMS simétrica específica. Se especifica el parámetro `DryRun`.

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --dry-run
```

Coherencia final de AWS KMS

La API de AWS KMS sigue un modelo de coherencia final debido a la naturaleza distribuida del sistema. Como resultado, es posible que los cambios en los recursos de AWS KMS no estén inmediatamente visibles para los comandos posteriores que ejecute.

Al realizar llamadas a la API de AWS KMS, es posible que se produzca una breve demora antes de que el cambio esté disponible en AWS KMS. Por lo general, el cambio tarda menos de unos segundos en propagarse por todo el sistema, pero en algunos casos puede tardar varios minutos. Es posible que se produzcan errores inesperados, como un error `NotFoundException` o `InvalidStateException`, en este periodo de tiempo. Por ejemplo, AWS KMS puede devolver un `NotFoundException` si llama a `GetParametersForImport` inmediatamente después de llamar a `CreateKey`.

Le recomendamos que configure una estrategia de reintentos en sus clientes de AWS KMS para reintentar automáticamente las operaciones tras un breve periodo de espera. Para obtener más información, consulte Retry behavior en la Guía de referencia de herramientas y SDK de AWS.

En el caso de las llamadas a la API relacionadas con las concesiones, puede utilizar un token de concesión para evitar posibles demoras y utilizar los permisos de una concesión de forma inmediata. Para obtener más información, consulte Eventual consistency (for grants).

Referencias

Las siguientes referencias proporcionan información útil sobre el uso y la administración de claves KMS.

- Referencia de tipos de clave. Muestra el tipo de clave KMS que admite cada operación de la API de AWS KMS.

  Para buscar: ¿Puedo habilitar y desactivar una clave KMS de firma RSA?
- Tabla estado de claves. Muestra cómo afecta el estado de la clave de una clave KMS a su uso en operaciones de la API de AWS KMS.

  Para buscar: ¿Puedo cambiar el alias de una clave KMS que está pendiente de eliminación?
- Referencia de permisos de la API de AWS KMS Proporciona información sobre los permisos necesarios para cada operación de la API de AWS KMS.

  Para buscar: ¿Puedo ejecutar GetKeyPolicyuna clave de otra AWS cuenta? ¿Puedo conceder el permiso `kms:Decrypt` en una política de IAM?
  - ViaService referencia. Enumera los servicios de AWS que admiten la clave de condición `kms:ViaService`.

    Para buscar: ¿Puedo usar la clave de `kms:ViaService` condición para permitir un permiso solo cuando proviene de Amazon ElastiCache? ¿Qué ocurre con Amazon Neptune?
- AWS KMS pricing. Enumera y explica el precio de las claves KMS.

  Para buscar: ¿Cuánto cuesta el uso de mis claves asimétricas?
- Cuotas de solicitudes de AWS KMS Enumera las cuotas por segundo para solicitudes de la API de AWS KMS en cada cuenta y región.

  Para buscar: ¿Cuántas solicitudes Decrypt puedo ejecutar en cada segundo? ¿Cuántas solicitudes Decrypt puedo ejecutar en claves KMS en mi almacén de claves personalizado?
- Cuotas de recursos de AWS KMS Enumera las cuotas de recursos de AWS KMS.

  Para encontrar: ¿Cuántas claves KMS puedo tener en cada región de mi cuenta? ¿Cuántos alias puedo tener en cada clave KMS?
- Servicios de AWS integrados con AWS KMS Enumera los servicios de AWS que utilizan claves KMS para proteger los recursos que crean, almacenan y administran.

Para buscar: ¿Amazon Connect utiliza claves KMS para proteger mis recursos de Connect?

Historial de documentos

En este tema se describen actualizaciones importantes en la Guía para desarrolladores de AWS Key Management Service .

Temas

Actualizaciones recientes

En la siguiente tabla se describen cambios importantes en esta documentación desde enero de 2018. Además de los cambios importantes que se indican a continuación, también actualizamos la documentación con frecuencia para mejorar las descripciones y los ejemplos y para dar cuenta de los comentarios que nos envía. Si desea recibir notificaciones sobre cambios importante, suscríbase a la fuente RSS.

Es posible que tenga que desplazarse horizontal o verticalmente para ver todos los datos de esta tabla.

Cambio	Descripción	Fecha
Actualizaciones de la rotación de claves	Se ha añadido la compatibilidad con periodos de rotación personalizados para realizar rotaciones clave automáticas, rotaciones clave bajo demanda y visibilidad de las rotaciones de materiales clave.	12 de abril de 2024
Actualizaciones a políticas administradas	Se agregaron nuevos permisos `AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy` que permiten	10 de noviembre de 2023

	AWS KMS monitorear los cambios en la VPC que contiene su AWS CloudHSM clúster, de modo que AWS KMS pueden proporcionar mensajes de error claros en caso de fallas.	
Actualización de funciones	Se ha agregado compatibilidad con el parámetro de API `DryRun`.	5 de julio de 2023
Actualización de funciones	Se agregó soporte para importar material clave para todos los tipos de AWS KMS claves, excepto para los almacenes de claves personalizados.	5 de junio de 2023
Actualización de funciones	Actualizaciones de las AWS KMS API para Nitro Enclaves	10 de marzo de 2023
Actualización de funciones	El algoritmo de `RSAES_PKCS1_V1_5` empaquetado está obsoleto. AWS KMS pondrá fin a todo el soporte a más `RSAES_PKCS1_V1_5` tardar el 1 de octubre de 2023, de conformidad con las directrices sobre la gestión de claves criptográficas del Instituto Nacional de Estándares y Tecnología (NIST). Le recomendamos que comience a utilizar un algoritmo de encapsulamiento diferente de inmediato.	28 de febrero de 2023

Actualización de funciones	Se ha añadido soporte para almacenes de claves externos, una función que te permite proteger tus AWS recursos mediante claves criptográficas externas. AWS	29 de noviembre de 2022
Cambio de cuota	Se aumentó la cuota AWS KMS keys de recursos a 100 000 claves de KMS en cada cuenta y región.	8 de julio de 2022
Actualización de funciones	Se agregó soporte para claves HMAC KMS en más Regiones de AWS	8 de julio de 2022
Nuevo tema	Se agregó el AWS Key Management Service tema Resiliencia al capítulo de seguridad de la Guía para AWS KMS desarrolladores.	14 de junio de 2022
Nueva característica	Se agregó soporte para AWS KMS claves y operaciones de API que generan y verifican códigos HMAC.	19 de abril de 2022
Cambio de documentación	Sustituir el término clave maestra del cliente (CMK) por AWS KMS key y clave KMS.	30 de agosto de 2021

Nueva característica	Se ha agregado compatibilidad para claves de varias regiones, un conjunto de claves KMS interoperables en diferentes regiones que tienen el mismo ID de clave y el mismo material de claves. Puede utilizar claves de varias regiones para cifrar datos en una región y descifrar datos en una región diferente.	8 de junio de 2021
Nueva característica	Se ha agregado compatibilidad con control de acceso basado en el atributo (ABAC). Puede usar etiquetas y alias para controlar el acceso a su. AWS KMS keys	17 de diciembre de 2020
Nueva característica	Se agregó compatibildidad para las políticas de punto de conexión de VPC.	9 de julio de 2020
Nuevo contenido	Explica las propiedades de seguridad de. AWS KMS	18 de junio de 2020
Nueva característica	Se agregó compatibilidad con claves de datos asimétricas AWS KMS keys y asimétricas.	25 de noviembre de 2019
Función actualizada	Puede ver la política clave de Claves administradas por AWS en la AWS KMS consola. Anteriormente, este rol se limitaba a las claves administradas por el cliente.	15 de noviembre de 2019

Nueva característica	Explica cómo utilizar algoritmos de intercambio híbrido postcuántico de claves en TLS para sus llamadas a AWS KMS.	4 de noviembre de 2019
Cambio de cuota	Se han aumentado las cuotas de recursos para algunas API que administran las claves KMS.	18 de septiembre de 2019
Cambio de cuota	Se han cambiado las cuotas de recursos en las claves KMS, los alias y las concesiones de cada clave KMS.	27 de marzo de 2019
Cambio de cuota	Se ha cambiado la cuota de solicitud por segundo para operaciones criptográficas que utilizan AWS KMS keys en un almacén de claves personalizadas.	7 de marzo de 2019
Nueva característica	Explica cómo crear y administrar almacenes de claves AWS KMS personalizados. Cada almacén de claves está respaldado por un AWS CloudHSM clúster que usted posee y controla.	26 de noviembre de 2018

Nueva consola	Explica cómo utilizar la nueva AWS KMS consola, que es independiente de la consola de IAM. La consola original y las instrucciones de uso estarán disponibles durante un breve periodo de tiempo para darle tiempo para familiari zarse con la nueva consola.	7 de noviembre de 2018
Cambio de cuota	Se modificó la cuota de solicitudes compartidas para su uso de AWS KMS keys.	21 de agosto de 2018
Nuevo contenido	Explica cómo se AWS Secrets Manager utilizan AWS KMS las claves para cifrar el valor secreto de un secreto.	13 de julio de 2018
Nuevo contenido	Explica cómo DynamoDB utiliza AWS KMS AWS KMS keys para prestar soporte a su opción de cifrado del servidor.	23 de mayo de 2018
Nueva característica	Explica cómo usar un punto de conexión privado en tu VPC para conectarte directame nte AWS KMS, en lugar de hacerlo a través de Internet.	22 de enero de 2018

Actualizaciones anteriores

En la siguiente tabla se describen los cambios importantes introducidos en la Guía para AWS Key Management Service desarrolladores antes de 2018.

Es posible que tenga que desplazarse horizontal o verticalmente para ver todos los datos de esta tabla.

Cambio	Descripción	Fecha
Nuevo contenido	Se ha agregado documentación sobre Etiquetado de claves.	15 de febrero de 2017
Nuevo contenido	Se ha agregado documentación sobre Supervisión de AWS KMS keys y Monitorización con Amazon CloudWatch.	31 de agosto de 2016
Nuevo contenido	Se ha agregado documentación sobre Material de claves importado.	11 de agosto de 2016
Nuevo contenido	Se ha agregado la siguiente documentación: Políticas de IAM, Referencia de permisos, y Claves de condición.	5 de julio de 2016
Actualización	Se han actualizado partes de la documentación en el capítulo Autenticación y control de acceso.	5 de julio de 2016
Actualización	Se ha actualizado la página Cuotas para reflejar las nuevas cuotas predeterminadas.	31 de mayo de 2016
Actualización	Se ha actualizado la página Cuotas para reflejar las nuevas cuotas predeterminadas y se ha actualizado la documentación de token de concesión para mejorar la claridad y la precisión.	11 de abril de 2016

Cambio	Descripción	Fecha
Nuevo contenido	Se ha agregado documentación sobre Conceder permiso a varias entidades principales de IAM para acceder a una clave KMS y Usar la condición de dirección IP.	17 de febrero de 2016
Actualización	Se han actualizado las páginas Políticas clave en AWS KMS y Cambiar una política de claves para mejorar la claridad y la precisión.	17 de febrero de 2016
Actualización	Se han actualizado las páginas de temas Administración de claves para mejorar la claridad.	5 de enero de 2016
Nuevo contenido	Se ha agregado documentación sobre Cómo AWS CloudTrail usa AWS KMS.	18 de noviembre de 2015
Nuevo contenido	Se han agregado instrucciones para Cambiar una política de claves.	18 de noviembre de 2015
Actualización	Se ha actualizado la documentación sobre ¿Cómo Amazon Relational Database Service (Amazon RDS) utiliza AWS KMS?.	18 de noviembre de 2015
Nuevo contenido	Se ha agregado documentación sobre Cómo WorkSpaces usa AWS KMS.	6 de noviembre de 2015

Cambio	Descripción	Fecha
Actualización	Se ha actualizado la página Políticas clave en AWS KMS para mejorar la claridad.	22 de octubre de 2015
Nuevo contenido	Se ha agregado documentación sobre Eliminación de AWS KMS keys, incluida la documentación complementaria sobre Creación de una alarma y Determinar el uso anterior de una clave KMS.	15 de octubre de 2015
Nuevo contenido	Se ha agregado documentación sobre Determinar el acceso a AWS KMS keys.	15 de octubre de 2015
Nuevo contenido	Se ha agregado documentación sobre Estados clave de AWS KMS las claves.	15 de octubre de 2015
Nuevo contenido	Se ha agregado documentación sobre Cómo Amazon Simple Email Service (Amazon SES) utiliza AWS KMS.	1 de octubre de 2015
Actualización	Se ha actualizado la página Cuotas para explicar las nuevas cuotas de solicitud.	31 de agosto de 2015
Nuevo contenido	Se agregó información sobre los cargos de uso AWS KMS. Consulte Precios de AWS KMS.	14 de agosto de 2015

Cambio	Descripción	Fecha
Nuevo contenido	Se agregaron cuotas de solicitudes a AWS KMS Cuotas.	11 de junio de 2015
Nuevo contenido	Se ha agregado un nuevo ejemplo de código de Java que demuestra el uso de la operación `UpdateAlias` . Consulte Actualizar un alias.	1 de junio de 2015
Actualización	Se ha movido la tabla de regiones de AWS Key Management Service a la Referencia general de AWS.	29 de mayo de 2015
Nuevo contenido	Se ha agregado documentación sobre Cómo Amazon EMR utiliza AWS KMS.	28 de enero de 2015
Nuevo contenido	Se ha agregado documentación sobre Cómo WorkMail usa Amazon AWS KMS.	28 de enero de 2015
Nuevo contenido	Se ha agregado documentación sobre ¿Cómo Amazon Relational Database Service (Amazon RDS) utiliza AWS KMS?.	6 de enero de 2015
Nuevo contenido	Se ha agregado documentación sobre Cómo Amazon Elastic Transcoder utiliza AWS KMS.	24 de noviembre de 2014

Cambio	Descripción	Fecha
Nueva guía	Se ha presentado la Guía para desarrolladores de AWS Key Management Service .	12 de noviembre de 2014

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.