aws

开发人员指南

AWS Key Management Service

AWS Key Management Service: 开发人员指南

Table of Contents

AWS Key Management Service

AWS Key Management Service（AWS KMS）是一项托管式服务，可让您轻松创建和控制用于保护您的数据的加密密钥。AWS KMS 使用硬件安全模块（HSM）根据 FIPS 140-2 加密模块验证计划保护和验证您的 AWS KMS keys。中国（北京）和中国（宁夏）区域不支持 FIPS 140-2 加密模块验证计划。AWS KMS 使用获得 OSCCA 认证的 HSM 来保护中国区域的 KMS 密钥。

AWS KMS 与大多数用于加密数据的其他 AWS 服务集成。AWS KMS 还与 AWS CloudTrail 集成以记录使用 KMS 密钥满足审计、法规和合规性需求的情况。

您可以使用 AWS KMS API 来创建和管理 KMS 密钥和特殊功能，如自定义密钥存储，并在加密操作中使用 KMS 密钥。有关详细信息，请参阅 AWS Key Management Service API 引用。

您可以创建和管理您的 AWS KMS keys：

- 创建、编辑和查看对称和非对称 KMS 密钥，包括 HMAC 密钥。
- 使用密钥策略、IAM policy 和授权控制对您的 KMS 密钥的访问。AWS KMS 支持基于属性的访问权限控制（ABAC）。您还可以通过使用条件键来优化策略。
- 创建、删除、列出和更新别名，即您的 KMS 密钥的友好名称。您还可以使用别名来控制对您的 KMS 密钥的访问。
- 标记您的 KMS 密钥以进行识别、自动化和成本跟踪。您还可以使用标签来控制对您的 KMS 密钥的访问。
- 启用和禁用 KMS 密钥。
- 启用和禁用 KMS 密钥中加密材料的自动轮换。
- 删除 KMS 密钥来完成密钥生命周期。

可以在加密操作中使用您的 KMS 密钥。有关示例，请参阅使用 AWS KMS API 进行编程。

- 使用对称或非对称 KMS 密钥对数据进行加密、解密和重新加密。
- 使用非对称 KMS 密钥对消息进行签名和验证。
- 生成可导出的对称数据密钥和非对称数据密钥对。
- 生成并验证 HMAC 代码。
- 生成适用于加密应用程序的随机数。

您还可以使用 AWS KMS 的高级功能

- 创建多区域密钥，它们就像是不同 AWS 区域 中的相同 KMS 密钥副本。
- 将加密材料导入 KMS 密钥。
- 在您的 AWS CloudHSM 集群支持的 AWS CloudHSM 密钥存储中创建 KMS 密钥。
- 在您的 AWS 之外的加密密钥支持的外部密钥存储中创建 KMS 密钥。
- 通过 VPC 中的私有端点直接连接到 AWS KMS。
- 使用混合后量子 TLS 可对发送到 AWS KMS 的数据进行前瞻性的传输中加密。

通过使用 AWS KMS，您能够更好地控制对加密数据的访问权限。您可以直接在应用程序中或通过与 AWS KMS 集成的 AWS 服务使用密钥管理和加密功能。无论您是在为 AWS 编写应用程序，还是在使用 AWS 服务，您都可以借助 AWS KMS 控制哪些人可以使用 AWS KMS keys 钥并访问您的加密数据。

AWS KMS 已与 AWS CloudTrail 集成，后者是一项将日志文件传输到您指定的 Amazon S3 存储桶的服务。通过使用， CloudTrail 您可以监控和调查您的 KMS 密钥是如何使用的、何时使用的，以及谁使用了这些密钥。

AWS 区域 中的 AWS KMS

支持 AWS KMS 的 AWS 区域 中列出了 AWS Key Management Service 终端节点和配额。如果 AWS KMS 支持的 AWS 区域 中不支持某项 AWS KMS 功能，则在有关该功能的主题中描述区域差异。

AWS KMS 定价

与其他 AWS 产品一样的是，使用 AWS KMS 不需要合同或最低购买。有关 AWS KMS 定价的更多信息，请参阅 AWS Key Management Service 定价。

服务水平协议

AWS Key Management Service 由定义服务可用性策略的服务等级协议提供支持。

了解更多

- 要了解 AWS KMS 中使用的术语和概念，请参阅 AWS KMS 概念。
- 有关 AWS KMS API 的更多信息，请参阅 AWS Key Management Service API 参考。有关使用不同的编程语言的示例，请参阅使用 AWS KMS API 进行编程。
- 要了解如何使用 AWS CloudFormation 模板来创建和管理密钥和别名，请参阅 AWS CloudFormation 用户指南中的 使用创建 AWS KMS 资源 AWS CloudFormation 和AWS Key Management Service资源类型参考。

- 有关 AWS KMS 如何使用密码术并保护 KMS 密钥的详细技术信息，请参阅 AWS Key Management Service 加密详细信息。加密详细信息文档没有描述 AWS KMS 如何在中国（北京）和中国（宁夏）区域工作。
- 如需每个 AWS 区域 中的 AWS KMS 端点的列表，包括 FIPS 端点，请参阅《AWS 一般参考》的 AWS Key Management Service 主题中的 Service endpoints。
- 有关 AWS KMS 相关问题的帮助，请参阅 AWS Key Management Service 论坛。

AWS 开发工具包中的 AWS KMS

- 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

AWS KMS 概念

了解 AWS Key Management Service (AWS KMS) 中使用的基本术语和概念，以及它们如何协同工作以帮助保护您的数据。

主题

- AWS KMS keys
- 客户密钥和 AWS 密钥
- 对称加密 KMS 密钥
- 非对称 KMS 密钥
- HMAC KMS 密钥
- 数据密钥
- 数据密钥对

- 别名
- 自定义密钥存储
- 加密操作
- 密钥标识符 (KeyId)
- 密钥材料
- 密钥材料源
- 密钥规范
- 密钥用法
- 信封加密
- 加密上下文
- 密钥策略
- 授权
- 审核 KMS 密钥用法
- 密钥管理基础设施

AWS KMS keys

AWS KMS keys（KMS 密钥）是 AWS KMS 中的主要资源。您可以使用 KMS 密钥加密、解密和重新加密数据。它还可以生成数据密钥，您可以在 AWS KMS 之外使用这些密钥。通常，您将使用对称加密 KMS 密钥，但也可以创建和使用非对称 KMS 密钥来进行加密或签名，并创建和使用 HMAC KMS 密钥来生成和验证 HMAC 标签。

> **Note**
>
> AWS KMS 正将术语客户托管密钥 (CMK) 替换为 AWS KMS key 和 KMS 密钥。这一概念并未改变。为防止破坏性更改，AWS KMS 保留了此术语的一些变体。

AWS KMS key 是加密密钥的逻辑表示形式。KMS 密钥包含密钥 ID、密钥规范、密钥用法、创建日期、描述和密钥状态等元数据。最重要的是，其中包含对您使用 KMS 密钥运行加密操作时所用的密钥材料的引用。

您可以使用在经 AWS KMS FIPS 验证的硬件安全模块中生成的加密密钥材料创建 KMS 密钥。对称 KMS 密钥的密钥材料和非对称 KMS 密钥的私有密钥永远不会让 AWS KMS 处于未加密状态。要使用

或管理 KMS 密钥，您必须使用 AWS KMS。有关创建和管理 KMS 密钥的信息，请参阅 管理 密钥。有关使用 KMS 密钥的信息，请参阅 AWS Key Management Service API 参考。

默认情况下，AWS KMS 为 KMS 密钥创建密钥材料。您无法提取、导出、查看或管理此密钥材料。唯一的例外是非对称密钥对的公有密钥，您可以将其导出以供 AWS 外部使用。此外，您无法删除此密钥材料；您必须删除 KMS 密钥。但是，您可以将自己的密钥材料导入 KMS 密钥，也可以使用自定义密钥存储来创建 KMS 密钥，这些密钥使用您的 AWS CloudHSM 集群中的密钥材料，或者您在 AWS 外部拥有和管理的外部密钥管理器中的密钥材料。

AWS KMS 也支持多区域密钥，它允许您加密一个 AWS 区域 中的数据，并在另一个 AWS 区域 中解密该数据。

有关创建和管理 KMS 密钥的信息，请参阅 管理 密钥。有关使用 KMS 密钥的信息，请参阅 AWS Key Management Service API 参考。

客户密钥和 AWS 密钥

您创建的 KMS 密钥是客户托管式密钥。使用 KMS 密钥加密服务资源的 AWS 服务 通常会为您创建密钥。AWS 服务 在您的 AWS 账户中创建的 KMS 密钥是 AWS 托管式密钥。AWS 服务 在服务账户中创建的 KMS 密钥是 AWS 拥有的密钥。

KMS 密钥的类型	可以查看 KMS 密钥元数据	可以管理 KMS 密钥	仅适用于我的 AWS 账户	自动轮换	定价
客户托管的密钥	是	是	支持	可选。每年（大约 365 天）	月度费用（按小时计费） 每次使用费用
AWS 托管式密钥	有	否	有	必需。每年（大约 365 天）	没有月度费用 每次使用费用（一些 AWS 服务 会为您支付这笔费用）
AWS 拥有的密钥	否	否	否	变化	无费用

与 AWS KMS 集成的 AWS 服务在其对 KMS 密钥的支持方面有所不同。默认情况下，一些 AWS 服务使用 AWS 拥有的密钥 或 AWS 托管式密钥 来加密您的数据。一些 AWS 服务支持客户托管式密钥。还有一些其他 AWS 服务支持所有类型的 KMS 密钥，从而使您能够轻松使用 AWS 拥有的密钥、实现 AWS 托管式密钥 的可见性或控制客户托管式密钥。有关 AWS 服务提供的加密选项的详细信息，请参阅服务的用户指南或开发人员指南中的静态加密 主题。

客户托管密钥

您创建的 KMS 密钥是客户托管式密钥。客户托管密钥是在您的 AWS 账户 中创建、拥有和管理的 KMS 密钥。您可以完全控制这些 KMS 密钥，包括建立和维护其密钥策略、IAM policy 和授权、启用和禁用它们、轮换其加密材料、添加标签、创建别名（引用了 KMS 密钥）以及计划删除 KMS 密钥。

客户托管密钥显示在 AWS KMS 的 AWS Management Console 的 Customer managed keys（客户托管密钥）页面上。要明确地标识客户托管密钥，请使用 DescribeKey 操作。对于客户托管密钥，`DescribeKey` 响应的 `KeyManager` 字段的值为 `CUSTOMER`。

您可以在加密操作中使用客户托管密钥并在 AWS CloudTrail 日志中审核其使用情况。此外，许多与 AWS KMS 集成的 AWS 服务使您能够指定客户托管密钥以保护为您存储和管理的数据。

客户托管密钥会产生月费以及超过免费套餐使用量的费用。这些费用将计入您的账户的 AWS KMS 配额。有关详细信息，请参阅 AWS Key Management Service 定价和配额。

AWS 托管式密钥

AWS 托管式密钥 是由与 AWS KMS 集成的 AWS 服务代表您在账户中创建、管理和使用的 KMS 密钥。

某些 AWS 服务可让您选择 AWS 托管式密钥或客户托管的密钥，从而保护您在该服务中的资源。通常，除非您需要控制保护资源的加密密钥，否则 AWS 托管式密钥是不错的选择。您不必创建或维护密钥或密钥策略，并且永远不会产生 AWS 托管式密钥月度费用。

您有权查看账户中的 AWS 托管式密钥、查看其密钥策略以及在 AWS CloudTrail 日志中审核其使用情况。但是，您无法更改 AWS 托管式密钥的任何属性、对它们进行轮换、更改其密钥策略或安排删除它们。此外，您无法在加密操作中直接使用 AWS 托管式密钥；创建它们的服务将代表您使用它们。

AWS 托管式密钥显示在 AWS KMS 的 AWS Management Console 的 AWS 托管式密钥 页面上。您也可以按别名标识大多数 AWS 托管式密钥，别名的格式为 `aws/`*`service-name`*，如 `aws/redshift`。要明确识别AWS 托管式密钥，请使用DescribeKey操作。对于 AWS 托管式密钥，`DescribeKey` 响应的 `KeyManager` 字段的值为 `AWS`。

所有的 AWS 托管式密钥 均每年自动轮换一次。您不能更改此轮换计划。

> **Note**
>
> 2022 年 5 月，AWS KMS 将 AWS 托管式密钥 的轮换时间表从每三年（约 1095 天）更改为每年（约 365 天）。
> 新的 AWS 托管式密钥 在创建一年后自动轮换，此后大约每年轮换一次。
> 现有的 AWS 托管式密钥 在他们最近一次轮换一年后自动轮换，此后每年轮换一次。

AWS 托管式密钥没有月度费用。您需为超出免费套餐的使用量付费，但某些 AWS 服务涵盖了这些费用。有关详细信息，请参阅服务的用户指南或开发人员指南中的静态加密主题。有关详细信息，请参阅 AWS Key Management Service 定价。

AWS 托管式密钥 不会计入您的账户各个区域中 KMS 密钥数量的资源配额。但是，当代表您账户中的委托人使用这些 KMS 密钥时，它们将计入请求配额。有关更多信息，请参阅 配额。

AWS 拥有的密钥

AWS 拥有的密钥 是 AWS 服务拥有并管理以用于多个 AWS 账户 中的 KMS 密钥的集合。虽然 AWS 拥有的密钥 不在您的 AWS 账户 中，但 AWS 服务可以使用 AWS 拥有的密钥 来保护您账户中的资源。

某些 AWS 服务可让您选择 AWS 拥有的密钥或客户托管的密钥。通常，除非您需要审核或控制保护资源的加密密钥，否则 AWS 拥有的密钥是不错的选择。AWS 拥有的密钥完全免费（没有月度费用或使用费用），它们不计入您账户的 AWS KMS 配额，而且简单易用。您不必创建或维护该密钥或其密钥策略。

AWS 拥有的密钥 的轮换因服务而异。有关特定 AWS 拥有的密钥 转换的信息，请参阅服务的用户指南或开发人员指南中的静态加密主题。

对称加密 KMS 密钥

创建 AWS KMS key后，默认情况下您将获得对称加密的 KMS 密钥。这是基本和最常用的 KMS 密钥类型。

在 AWS KMS 中，对称加密 KMS 密钥表示 256 位 AES-GCM 加密密钥，但在中国区域，它表示 128 位 SM4 加密密钥。对称密钥材料绝不会让 AWS KMS 处于未加密状态。要使用对称加密 KMS 密钥，您必须调用 AWS KMS。对称加密密钥用在对称加密中，加密和解密采用的是相同的密钥。除非任务明

确要求使用非对称加密，否则对称加密 KMS 密钥（永远不会让 AWS KMS 处于未加密状态）是个不错的选择。

与 AWS KMS 集成的 AWS 服务仅使用对称加密 KMS 密钥加密您的数据。这些服务不支持使用非对称 KMS 密钥进行加密。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

从技术上讲，对称密钥的密钥规范是 SYMMETRIC_DEFAULT，密钥用法是 ENCRYT_DECHLOT，加密算法是 SYMMETRIC_DEFAULT。有关更多信息，请参阅 SYMMETRIC_DEFAULT 密钥规范。

在 AWS KMS 中，可以使用对称加密 KMS 密钥加密、解密和重新加密数据，生成数据密钥和数据密钥对。您可以创建多区域对称加密 KMS 密钥，将自己的密钥材料导入对称加密 KMS 密钥中，并在自定义密钥存储中创建对称加密 KMS 密钥。有关您可以对不同类型 KMS 密钥执行的操作进行比较的表格，请参阅 密钥类型引用。

非对称 KMS 密钥

您可以在 AWS KMS 中创建非对称 KMS 密钥。非对称 KMS 密钥表示数学上相关的公有密钥和私有密钥对。私有密钥永远不会让 AWS KMS 处于未加密状态。要使用私有密钥，必须调用 AWS KMS。您可以通过调用 AWS KMS API 操作在 AWS KMS 内使用公有密钥，也可以下载公有密钥并在 AWS KMS 外部使用该密钥。您也可以创建多区域非对称 KMS 密钥。

您可以创建非对称 KMS 密钥，表示用于公有密钥加密或签名和验证的 RSA 密钥对或 SM2 密钥对（仅适用于中国区域），或表示用于签名和验证的椭圆曲线密钥对。

有关创建和使用非对称 KMS 密钥的更多信息，请参阅 AWS KMS 中的非对称密钥。

HMAC KMS 密钥

HMAC KMS 密钥表示长度不同的对称密钥，用于生成和验证 HMAC 散列消息认证码。HMAC 密钥的密钥材料绝不会让 AWS KMS 处于未加密状态。要使用 HMAC 密钥，请调用 `GenerateMac` 或 `VerifyMac` API 操作。

您也可以创建多区域 HMAC KMS 密钥。

有关创建和使用 HMAC KMS 密钥的更多信息，请参阅 AWS KMS 中的 HMAC 密钥。

数据密钥

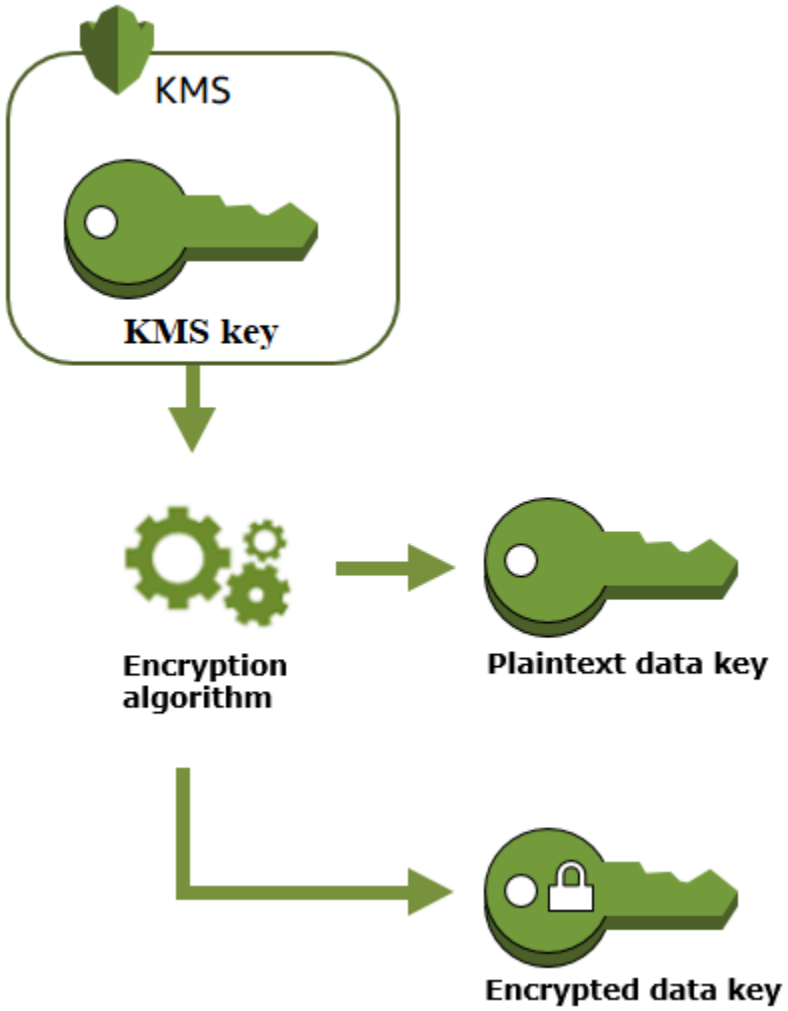
数据密钥是可用于加密数据的对称密钥，包括大量数据和其他数据加密密钥。与无法下载的对称 KMS 密钥不同的是，数据密钥可以返回给您在 AWS KMS 外部使用。

当 AWS KMS 生成数据密钥时，它会返回供立即使用的明文数据密钥（可选）和可以随数据安全存储的数据密钥的加密副本。准备好解密数据时，首先要求 AWS KMS 解密已加密的数据密钥。

AWS KMS 会生成、加密和解密数据密钥。但是，AWS KMS 不会存储、管理或跟踪您的数据密钥，也不会使用数据密钥执行加密操作。您必须在 AWS KMS 之外使用和管理数据密钥。有关安全使用数据密钥的帮助，请参阅 AWS Encryption SDK。

创建数据密钥

要创建数据密钥，请调用该GenerateDataKey操作。 AWS KMS生成数据密钥。然后，它会在您指定的对称加密 KMS 密钥下加密数据密钥的副本。此操作会返回数据密钥的明文副本以及由 KMS 密钥加密的数据密钥的副本。下图展示了此操作。

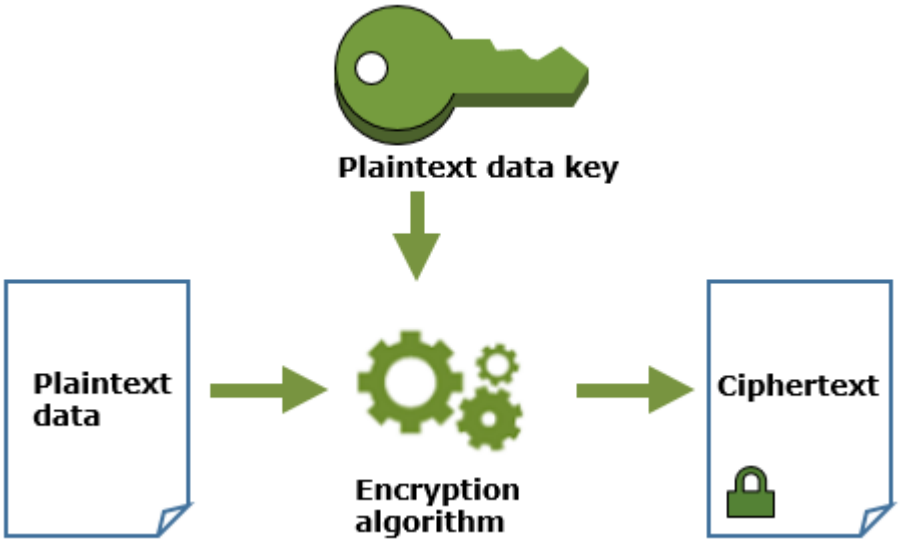


AWS KMS还支持该GenerateDataKeyWithoutPlaintext操作，该操作仅返回加密的数据密钥。当您需要使用数据密钥时，请要求 AWS KMS 解密它。

使用数据密钥加密数据

AWS KMS 无法使用数据密钥来加密数据。但您可以在 AWS KMS 之外使用数据密钥，例如使用 OpenSSL 或 AWS Encryption SDK 等加密库。

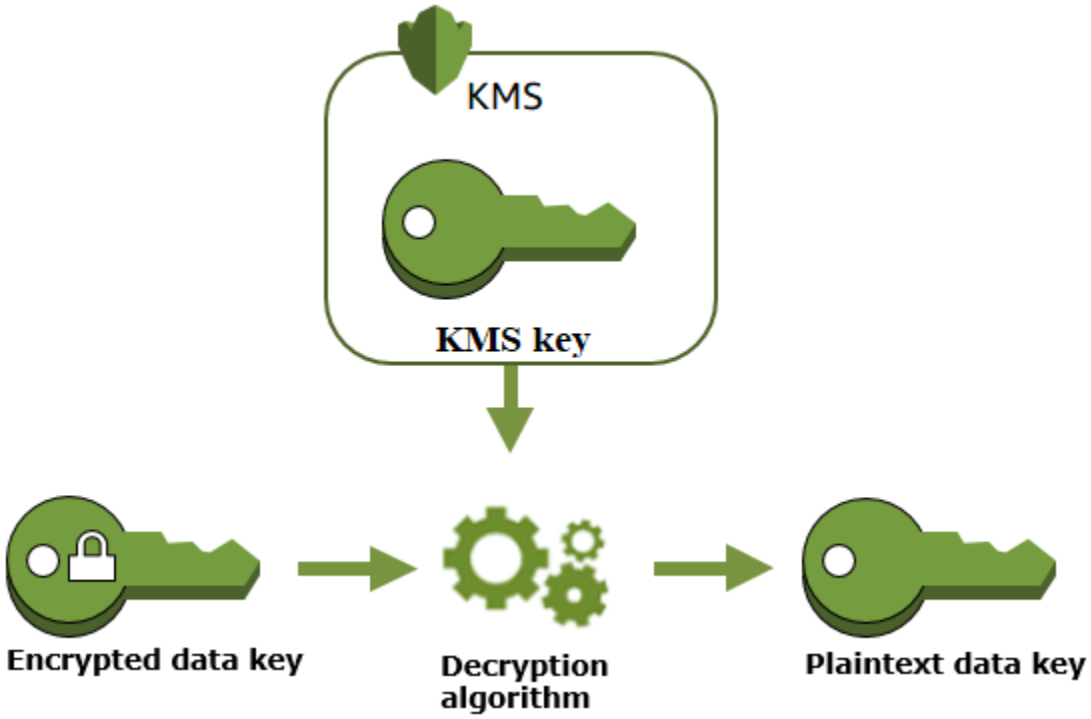
在使用明文数据密钥加密数据后，请尽快从内存中将其删除。您可以安全地存储加密数据密钥及加密数据，以便其可根据需要用于解密数据。



使用数据密钥解密数据

要解密数据，请将加密数据密钥传递至 Decrypt 操作。AWS KMS 使用您的 KMS 密钥解密数据密钥，然后再返回明文数据密钥。使用明文数据密钥解密数据，并尽快从内存中删除该明文数据密钥。

下图显示了如何使用 Decrypt 操作解密加密的数据密钥。



不可用的 KMS 密钥如何影响数据密钥

当 KMS 密钥不可用时，您可以立即发现（取决于最终一致性）。KMS 密钥的密钥状态会出现变更，以反映其新情况，并且加密操作中使用 KMS 密钥的所有请求都将失败。

但是，对由 KMS 密钥加密的数据密钥，以及由数据密钥加密的数据的影响会延迟，直至再次使用 KMS 密钥（例如用于解密数据密钥）。

KMS 密钥状态变为不可用的原因有许多，包括您可能执行的以下操作。

- 禁用 KMS 密钥
- 安排删除 KMS 密钥
- 从具有已导入密钥材料的 KMS 密钥中删除密钥材料，或允许导入的密钥材料过期。
- 断开托管 KMS 密钥的 AWS CloudHSM 密钥存储的连接，或从用作 KMS 密钥的密钥材料的 AWS CloudHSM 集群中删除密钥。
- 断开托管 KMS 密钥的外部密钥存储的连接，或干扰对外部密钥存储代理的加密和解密请求的任何其他操作，包括从其外部密钥管理器中删除外部密钥。

对于许多使用数据密钥来保护服务所管理的资源的 AWS 服务 来说，这种效果尤其重要。以下几个示例使用 Amazon Elastic Block Store（Amazon EBS）和 Amazon Elastic Compute Cloud（Amazon

EC2）。不同的 AWS 服务 以不同方式使用数据密钥。有关详细信息，请参阅 AWS 服务 的“安全性”一章的“数据保护”部分。

例如，考虑以下情景：

1. 您创建加密 EBS 卷并指定 KMS 密钥来保护该卷。Amazon EBS 要求 AWS KMS 使用您的 KMS 密钥来为该卷生成加密数据密钥。Amazon EBS 使用该卷的元数据存储加密数据密钥。
2. 当您将 EBS 卷附加到 EC2 实例时，Amazon EC2 使用您的 KMS 密钥来解密 EBS 卷的加密数据密钥。Amazon EC2 使用 Nitro 硬件中的数据密钥，该硬件负责对 EBS 卷的所有磁盘 I/O 进行加密。EBS 卷附加到 EC2 实例时，数据密钥会保留在 Nitro 硬件中。
3. 您执行的操作会使 KMS 密钥不可用。这不会立即影响 EC2 实例或 EBS 卷。卷附加到实例时，Amazon EC2 使用数据密钥（而不是 KMS 密钥），来对所有磁盘输入/输出进行加密。
4. 但是，当加密的 EBS 卷从 EC2 实例分离时，Amazon EBS 将从 Nitro 硬件中删除该数据密钥。下次将加密的 EBS 卷附加到 EC2 实例时，附加会失败，因为 Amazon EBS 无法使用 KMS 密钥来解密卷的加密数据密钥。要再次使用 EBS 卷，您必须使该 KMS 密钥可重新使用。

数据密钥对

数据密钥对是由数学上相关的公有密钥和私有密钥组成的非对称数据密钥。它们设计用于 AWS KMS 外部的客户端加密和解密或签名和验证。

与 OpenSSL 等工具生成的数据密钥对不同，AWS KMS 会将每个数据密钥对中的私有密钥置于您指定的 AWS KMS 中的对称加密 KMS 密钥的保护之下。但是，AWS KMS 不会存储、管理或跟踪数据密钥对，也不会使用数据密钥对执行加密操作。您必须在 AWS KMS 之外使用和管理数据密钥对。

AWS KMS 支持以下类型的数据密钥对：

- RSA 密钥对：RSA_2048、RSA_3072 和 RSA_4096
- 椭圆曲线密钥对：ECC_NIST_P256、ECC_NIST_P384、ECC_NIST_P521 和 ECC_SECG_P256K1
- SM 密钥对（仅限中国区域）：SM2

选择何种数据密钥对通常取决于使用案例或法规要求。大多数证书需要 RSA 密钥。椭圆曲线密钥通常用于数字签名。ECC_SECG_P256K1 密钥通常用于加密数字货币。AWS KMS 建议您使用 ECC 密钥对进行签名，并将 RSA 密钥对用于加密或签名，但不能同时使用两者。然而，AWS KMS 无法对 AWS KMS 以外的数据密钥对使用强制实施任何限制。

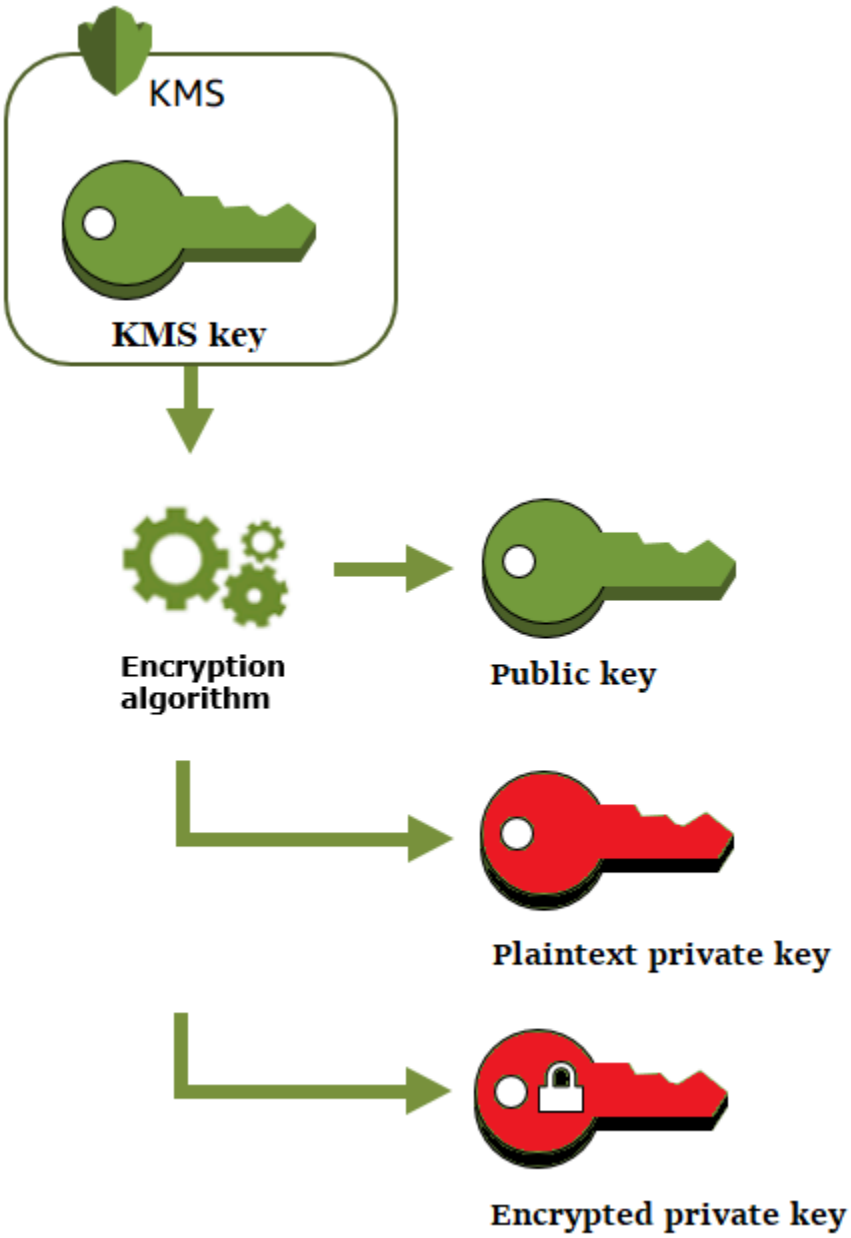
创建数据密钥对

要创建数据 key pair，请调用GenerateDataKeyPair或GenerateDataKeyPairWithoutPlaintext操作。指定要用于加密私有密钥的对称加密 KMS 密钥。

GenerateDataKeyPair 返回一个明文公有密钥、一个明文私有密钥和一个加密的私有密钥。如果您即刻需要明文私有密钥，例如生成数字签名，则可使用此操作。

GenerateDataKeyPairWithoutPlaintext 返回一个明文公有密钥和一个加密的私有密钥，但不返回明文私有密钥。如果您并非即刻需要明文私有密钥，例如使用公有密钥进行加密，则可使用此操作。稍后，如果您需要明文私有密钥来解密数据，则可调用 Decrypt 操作。

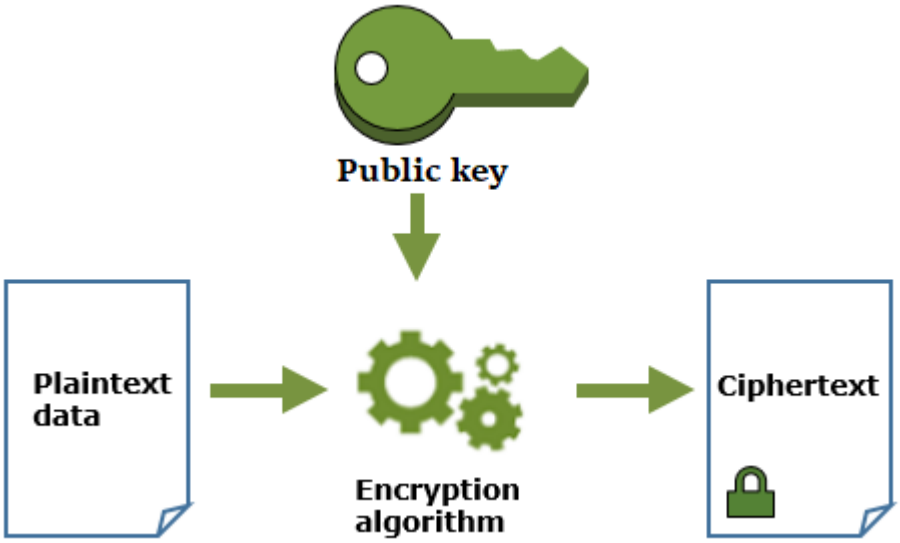
下图显示了 GenerateDataKeyPair 操作。GenerateDataKeyPairWithoutPlaintext 操作省略了明文私有密钥。



使用数据密钥对加密数据

使用数据密钥对加密时，用该密钥对的公有密钥加密数据，然后用同一密钥对的私有密钥解密数据。通常，当多方需要加密数据，而只有持有私有密钥的一方才能解密该数据时，您可以使用数据密钥对。

持有公有密钥的多方使用该密钥加密数据，如下图所示。

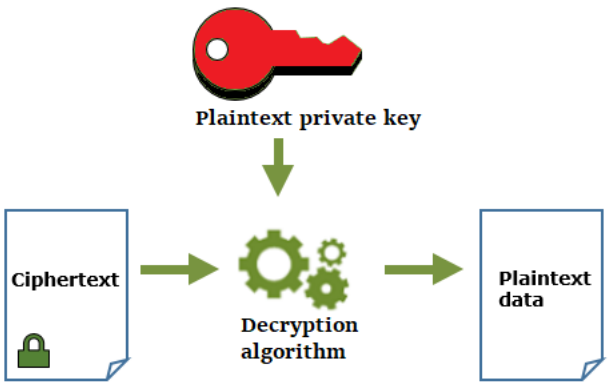


使用数据密钥对解密数据

要解密数据，请使用数据密钥对中的私有密钥。为使操作成功，公有密钥和私有密钥必须来自同一数据密钥对，并且必须使用相同的加密算法。

要对加密的私有密钥进行解密，请将其传递给 Decrypt 操作。使用明文私有密钥解密数据。然后尽快从内存中删除明文私有密钥。

下图显示了如何使用数据密钥对中的私有密钥解密密文。



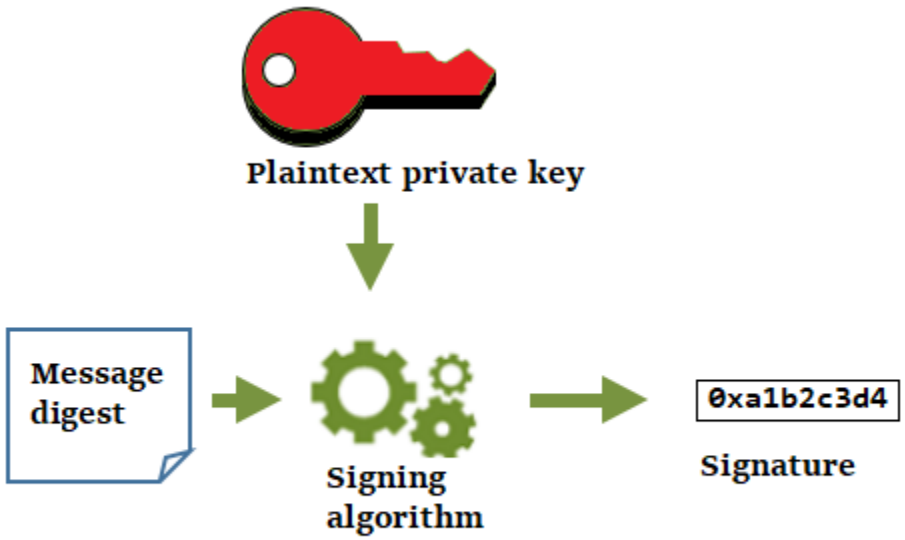
使用数据密钥对签署消息

要为消息生成加密签名，请使用数据密钥对中的私有密钥。持有公有密钥的任何人都可以使用该密钥来验证消息已使用私有密钥签名，并且自签名以后未曾更改。

如果加密私有密钥，请将加密的私有密钥传递给 Decrypt 操作。AWS KMS 使用 KMS 密钥对数据密钥进行解密，然后返回明文私有密钥。使用明文私有密钥生成签名。然后尽快从内存中删除明文私有密钥。

要签署消息，请使用加密哈希函数（如 OpenSSL 中的 `dgst` 命令）创建消息摘要。然后，将明文私有密钥传递给签名算法。结果是一个表示消息内容的签名。（您可能无需先创建摘要即可签署较短的消息。最大消息大小因您使用的签名工具而异。）

下图显示了如何使用数据密钥对中的私有密钥签署消息。

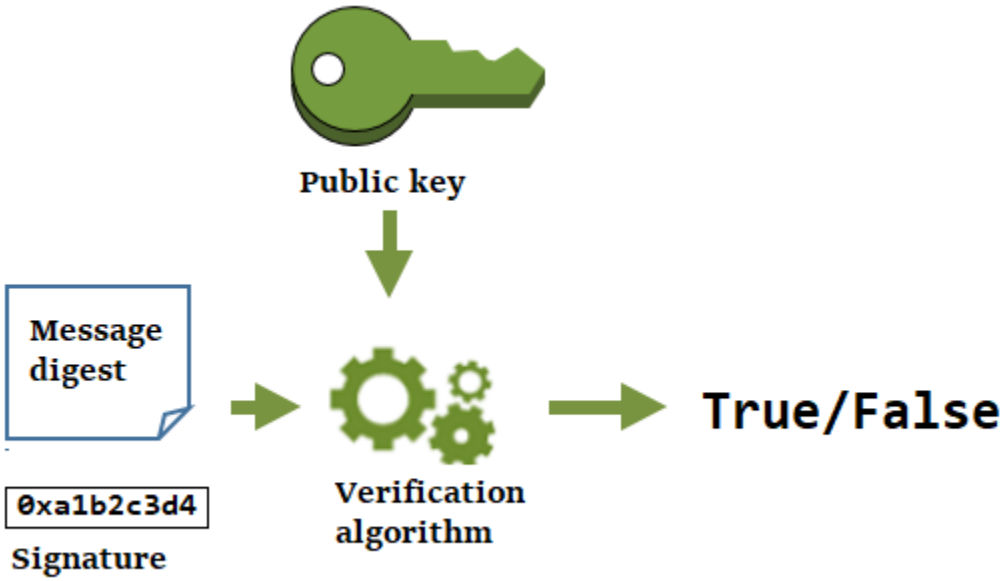


使用数据密钥对验证签名

持有数据密钥对中公有密钥的任何人，都可以使用该密钥来验证使用私有密钥生成的签名。验证确认已授权用户使用指定的私有密钥和签名算法签署了消息，并且消息自签名以后未曾更改。

要使验证成功，验证签名的一方必须生成相同类型的摘要，使用相同的算法，并使用与用于签署消息的私有密钥相对应的公有密钥。

下图显示了如何使用数据密钥对中的公有密钥验证消息签名。



别名

使用别名作为 KMS 密钥的友好名称。例如，您可以将 KMS 密钥引用为 test-key，而不是 1234abcd-12ab-34cd-56ef-1234567890ab。

别名可以更轻松地识别 AWS Management Console 中的 KMS 密钥。您可以使用别名在某些 AWS KMS 操作中识别 KMS 密钥，包括加密操作。在应用程序中，您可以使用单个别名引用每个 AWS 区域中的不同 KMS 密钥。

您还可以根据 KMS 密钥的别名允许和拒绝访问 KMS 密钥，而无需编辑策略或管理授权。此功能是 AWS KMS 对基于属性的访问控制 (ABAC) 的支持的一部分。有关更多信息，请参阅 AWS KMS 中的 ABAC。

在 AWS KMS 中，别名是独立的资源，而不是 KMS 密钥的属性。因此，您可以添加、更改和删除别名，而不会影响关联的 KMS 密钥。

> **Important**
>
> 不要在别名名称中包含机密或敏感信息。别名可能会以纯文本形式出现在 CloudTrail 日志和其他输出中。

了解更多：

- 有关别名的详细信息，请参阅 使用别名。
- 有关密钥标识符（包括别名）格式的信息，请参阅 密钥标识符 (KeyId)。
- 要获得查找与 KMS 密钥关联的别名的帮助，请参阅 查找别名和别名 ARN
- 有关使用多种编程语言创建和管理别名的示例，请参阅 使用别名。

自定义密钥存储

自定义密钥存储是由您拥有和管理的 AWS KMS 之外的密钥管理器支持的 AWS KMS 资源。在自定义密钥存储中使用 KMS 密钥进行加密操作时，加密操作实际上是在您的密钥管理器中使用加密密钥来执行。

AWS KMS 支持由 AWS CloudHSM 集群支持的 AWS CloudHSM 密钥存储以及由 AWS 之外的密钥管理器支持的外部密钥存储。

有关更多信息，请参阅 自定义密钥存储。

加密操作

在 AWS KMS 中，加密操作 是使用 KMS 密钥保护数据的 API 操作。由于 KMS 密钥保留在 AWS KMS 中，因此，您必须调用 AWS KMS 才能在加密操作中使用 KMS 密钥。

要使用 KMS 密钥执行加密操作，请使用 AWS 开发工具包、AWS Command Line Interface (AWS CLI) 或 AWS Tools for PowerShell。无法在 AWS KMS 控制台中执行加密操作。有关使用多种编程语言调用加密操作的示例，请参阅使用 AWS KMS API 进行编程。

下表列出了 AWS KMS 加密操作。它还显示操作中使用的 KMS 密钥的密钥类型和密钥使用要求。

操作	密钥类型	密钥用法
Decrypt	对称或非对称	ENCRYPT_DECRYPT
Encrypt	对称或非对称	ENCRYPT_DECRYPT
GenerateDataKey	对称	ENCRYPT_DECRYPT
GenerateDataKeyPair	对称 [1]	ENCRYPT_DECRYPT

操作	密钥类型	密钥用法
	在自定义密钥存储中的 KMS 密钥中不受支持。	
GenerateDataKeyPairWithoutPlaintext	对称 [1] 在自定义密钥存储中的 KMS 密钥中不受支持。	ENCRYPT_DECRYPT
GenerateDataKeyWithoutPlaintext	对称	ENCRYPT_DECRYPT
GenerateMac	HMAC	GENERATE_VERIFY_MAC
GenerateRandom	不适用。此操作不使用 KMS 密钥。	不适用
ReEncrypt	对称或非对称	ENCRYPT_DECRYPT
Sign	非对称	SIGN_VERIFY
验证	非对称	SIGN_VERIFY
VerifyMac	HMAC	GENERATE_VERIFY_MAC

[1] 生成受对称加密 KMS 密钥保护的非对称数据密钥对。

有关加密操作的权限的信息，请参阅 the section called “权限参考”。

为了使 AWS KMS 对所有用户具有响应性和较强的功能，AWS KMS 为每秒可以调用的加密操作数设置了配额。有关更多信息，请参阅 the section called “加密操作的共享配额”。

密钥标识符 (KeyId)

密钥标识符用作 KMS 密钥的名称。它们可帮助您在控制台中识别 KMS 密钥。您可以使用它们来指示要在 AWS KMS API 操作、密钥策略、IAM policy 和授权中使用的 KMS 密钥。密钥标识符值跟与 KMS 密钥关联的密钥材料完全无关。

AWS KMS 定义了多个密钥标识符。创建 KMS 密钥时，AWS KMS 生成密钥 ARN 和密钥 ID，这些是 KMS 密钥的属性。创建别名时，AWS KMS 会根据您定义的别名生成别名 ARN。您可以在 AWS Management Console 和 AWS KMS API 中查看密钥及别名标识符。

在 AWS KMS 控制台中，您可以按密钥 ARN、密钥 ID 或别名名称查看和筛选 KMS 密钥，并可按密钥 ID 和别名排序。有关在控制台中查找密钥标识符的帮助，请参阅the section called “查找密钥 ID 和密钥 ARN”。

在 AWS KMS API 中，用于标识 KMS 密钥的参数名为 `KeyId` 或其变体（例如 `TargetKeyId` 或 `DestinationKeyId`）。但是，这些参数的值不限于密钥 ID。一些参数可以使用任意有效的密钥标识符。有关每个参数值的信息，请参阅 AWS Key Management Service API 参考中的参数描述。

> **Note**
>
> 使用 AWS KMS API 时，请谨慎使用密钥标识符。不同的 API 需要不同的密钥标识符。通常，请在您的任务中使用最完整实用的密钥标识符。

AWS KMS 支持以下密钥标识符。

密钥 ARN

密钥 ARN 是 KMS 密钥的 Amazon Resource Name (ARN)。它是 KMS 密钥唯一的完全限定标识符。密钥 ARN 包括 AWS 账户、区域和密钥 ID。有关查找 KMS 密钥的密钥 ARN 的帮助，请参阅the section called “查找密钥 ID 和密钥 ARN”。

密钥 ARN 的格式如下：

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

以下是单区域 KMS 密钥的示例密钥 ARN。

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

多区域密钥的密钥 ARN 的 *key-id* 元素以 mrk- 前缀开头。以下是多区域密钥的示例密钥 ARN。

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

密钥 ID

密钥 ID 唯一地标识账户和区域中的 KMS 密钥。有关查找 KMS 密钥的密钥 ID 的帮助，请参阅 the section called “查找密钥 ID 和密钥 ARN”。

以下是单区域 KMS 密钥的示例密钥 ID。

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

多区域密钥的密钥 ID 以 mrk- 前缀开头。以下是多区域密钥的示例密钥 ID。

```
mrk-1234abcd12ab34cd56ef1234567890ab
```

别名 ARN

别名 ARN 是 AWS KMS 别名的 Amazon Resource Name (ARN)。它是别名及所表示 KMS 密钥的唯一的完全限定标识符。别名 ARN 包括 AWS 账户、区域和别名。

在任何给定时间，一个别名 ARN 标识一个特定的 KMS 密钥。但是，由于您可以更改与别名关联的 KMS 密钥，别名 ARN 在不同时间可以标识不同的 KMS 密钥。有关查找 KMS 密钥的别名 ARN 的帮助，请参阅 查找别名和别名 ARN。

别名 ARN 的格式如下：

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

以下是虚构的 ExampleAlias 的别名 ARN。

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

别名

别名是最多 256 个字符的字符串。它唯一地标识某个账户和区域内关联的一个 KMS 密钥。在 AWS KMS API 中，别名始终以 alias/ 开头。有关查找 KMS 密钥的别名的帮助，请参阅 查找别名和别名 ARN。

别名的格式如下：

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

例如：

```
alias/ExampleAlias
```

别名的 aws/ 前缀保留用于 AWS 托管式密钥。您无法使用此前缀创建别名。例如，Amazon Simple Storage Service (Amazon S3) 的 AWS 托管式密钥 的别名如下。

```
alias/aws/s3
```

密钥材料

密钥材料是加密算法中使用的位串。秘密密钥材料必须保密，以保护使用它的加密操作。公有密钥材料旨在用于共享。

每个 KMS 密钥的元数据中都包含对其密钥材料的引用。对称加密 KMS 密钥的密钥材料源可能会有所不同。您可以使用 AWS KMS 生成的密钥材料、在自定义密钥存储的 AWS CloudHSM 集群中生成的密钥材料，或者导入自己的密钥材料。如果您将 AWS KMS 密钥材料用于对称加密 KMS 密钥，您可以启用您的密钥材料自动轮换。

默认情况下，每个 KMS 密钥都具有唯一的密钥材料。但是，您可以使用相同的密钥材料创建一组多区域密钥。

密钥材料源

密钥材料源是标识 KMS 密钥中密钥材料的来源的 KMS 密钥属性。您在创建 KMS 密钥时选择密钥材料源，并且无法更改。密钥材料的来源会影响 KMS 密钥的安全性、耐久性、可用性、延迟和吞吐量特性。

要查找 KMS 密钥的密钥材料来源，请使用DescribeKey操作，或者在AWS KMS控制台中查看 KMS 密钥详情页面的 “加密配置” 选项卡上的 O rigin 值。有关帮助信息，请参阅查看密钥。

KMS 密钥可以具有以下密钥材料源值之一。

AWS_KMS

AWS KMS 在其自己的密钥存储中创建和管理 KMS 密钥的密钥材料。这是大多数 KMS 密钥的默认值和推荐值。

有关使用来自 AWS KMS 的密钥材料创建密钥的帮助，请参阅创建密钥。

EXTERNAL (Import key material)

KMS 密钥具有已导入的密钥材料。当您使用 External 密钥材料源创建 KMS 密钥时，KMS 密钥没有密钥材料。稍后，您可以将密钥材料导入 KMS 密钥。使用导入的密钥材料时，您需要保护和管理 AWS KMS 外部的密钥材料，包括在密钥材料过期时进行替换。有关更多信息，请参阅 关于导入的密钥材料。

有关为导入的密钥材料创建 KMS 密钥的帮助，请参阅 步骤 1：创建不带密钥材料的 KMS 密钥。

AWS_CLOUDHSM

AWS KMS 在 AWS CloudHSM 集群中为您的 AWS CloudHSM 密钥存储创建密钥材料。

有关在 AWS CloudHSM 密钥存储中创建 KMS 密钥的帮助，请参阅 在 AWS CloudHSM 密钥存储中创建 KMS 密钥。

EXTERNAL_KEY_STORE

密钥材料是 AWS 之外的密钥管理器中的加密密钥。仅针对外部密钥存储中的 KMS 密钥支持此来源。

有关在外部密钥存储中创建 KMS 密钥的帮助，请参阅 在外部密钥存储中创建 KMS 密钥。

密钥规范

密钥规范 是一种属性，用于表示密钥的加密配置。密钥规范的含义因密钥类型而异。

- AWS KMS 密钥 — 密钥规范将确定 KMS 密钥是对称密钥还是非对称密钥。它还可确定其密钥材料类型，及其支持的算法。密钥规范在创建 KMS 密钥时选择，并且无法更改。默认密钥规范 SYMMETRIC_DEFAULT 表示一组 256 位的对称加密密钥。

> **Note**
>
> KMS 密钥的 KeySpec 被称为 CustomerMasterKeySpec。该CreateKey操作的CustomerMasterKeySpec参数已被弃用。请改用 KeySpec 参数，它的工作方式相同。

为了防止发生重大更改，CreateKey和DescribeKey操作的响应现在包括两者KeySpec以及具有相同值CustomerMasterKeySpec的成员。

有关密钥规范的列表以及选择密钥规范的帮助信息，请参阅选择密钥规范。要查找 KMS 密钥的密钥规范，请使用DescribeKey操作，或者在AWS KMS控制台中查看 KMS 密钥详情页面上的加密配置选项卡。有关帮助信息，请参阅查看密钥。

要限制委托人在创建 KMS 密钥时可以使用的密钥规范，请使用 k ms: KeySpec 条件密钥。您还可以使用 kms:KeySpec 条件键，以允许主体根据特定密钥规范仅对 KMS 密钥调用 AWS KMS 操作。例如，您可以拒绝删除具有 RSA_4096 密钥规范的 KMS 密钥的计划权限。

- 数据密钥 (GenerateDataKey)-密钥规范确定 AES 数据密钥的长度。
- 数据密钥对 (GenerateDataKeyPair)-密钥对规范确定数据密钥对中密钥材料的类型。

密钥用法

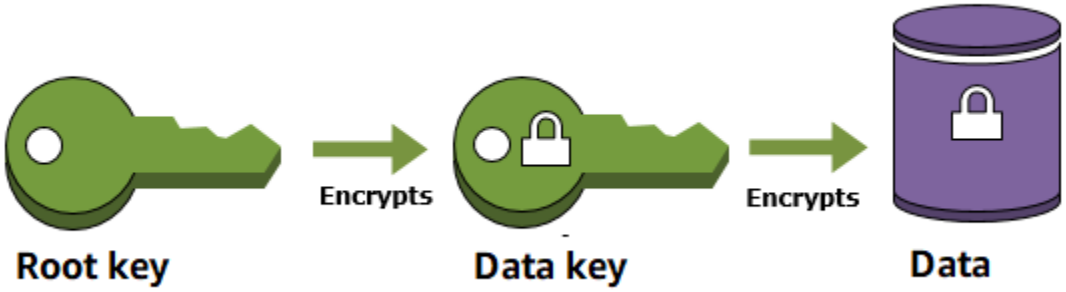
密钥用法属性决定密钥支持的加密操作。KMS 密钥的密钥用法可以是 ENCRYPT_DECRYPT、SIGN_VERIFY 或 GENERATE_VERIFY_MAC。每个 KMS 密钥都只能有一个密钥用法。将 KMS 密钥用于多种操作类型，会使两种操作的产物更容易受到攻击。

有关选择 KMS 密钥的密钥用法的帮助，请参阅 选择密钥用法。要查找 KMS 密钥的密钥使用情况，请使用DescribeKey操作，或者在AWS KMS控制台中选择 KMS 密钥详情页面上的加密配置选项卡。有关帮助信息，请参阅查看密钥。

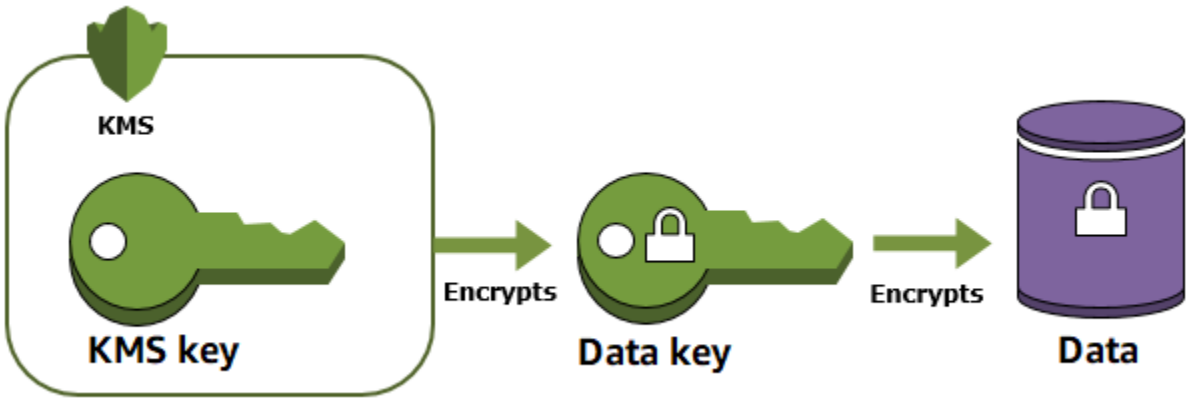
信封加密

在您加密数据后，数据将受到保护，但您必须保护加密密钥。一种策略是对其进行加密。信封加密 是一种加密方法，它使用数据密钥对明文数据进行加密，然后使用其他密钥对数据密钥进行加密。

您甚至可以使用其他加密密钥对数据加密密钥进行加密，并且在另一个加密密钥下加密该加密密钥。但是，最后，一个密钥必须以明文形式保留，以便您可以解密密钥和数据。此顶级明文密钥加密密钥称为根密钥。



AWS KMS 可通过安全地存储和管理加密密钥来帮助您保护它们。存储在 AWS KMS 中的根密钥（称为 AWS KMS keys）绝不会让 AWS KMS 经 FIPS 验证的硬件安全模块处于不加密状态。要使用 KMS 密钥，您必须调用 AWS KMS。



信封加密可提供以下多种优势：

- 保护数据密钥

  加密数据密钥时，您无需担心存储加密数据密钥，因为数据密钥本身就受到加密的保护。您可以安全地将加密数据与加密数据密钥一起存储。

- 使用多个密钥加密相同的数据

  加密操作可能非常耗时，特别是要加密的数据是大型对象时。您可以只重新加密保护原始数据的数据密钥，而无需使用不同的密钥多次重新加密原始数据。

- 结合多种算法的优势

  通常，与公有密钥算法相比，对称密钥算法速度更快，生成的密文更小。但公有密钥算法可提供固有的角色分离和更轻松的密钥管理。信封加密让您可以每种策略的优势结合起来。

加密上下文

所有使用对称加密 KMS 密钥的 AWS KMS 加密操作都接受“加密上下文”，它是一组包含有关数据的额外上下文信息的非机密可选键/值对。AWS KMS 将加密上下文用作额外验证数据（AAD）以支持身份验证加密。

在加密请求中包含加密上下文时，它以加密方式绑定到密文，这样就需要相同的加密上下文来解密（或解密并重新加密）数据。如果解密请求中提供的加密上下文不是区分大小写的完全匹配，解密请求将失败。只有加密上下文中键/值对的顺序可以改变。

> **Note**
>
> 您不能在使用非对称 KMS 密钥或 HMAC KMS 密钥的加密操作中指定加密上下文。非对称算法和 MAC 算法不支持加密上下文。

加密上下文不是密钥，且没有加密。它以明文显示在 AWS CloudTrail 日志中，以便您可以使用它来标识和分类加密操作。您的加密上下文不应包含敏感信息。我们建议您的加密上下文描述正在加密或解密的数据。例如，在加密文件时，您可以将文件路径的一部分用作加密上下文。

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

例如，在加密使用亚马逊弹性块存储 (Amazon EBS) CreateSnapshot操作创建的卷和快照时，Amazon EBS 使用卷 ID 作为加密上下文值。

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

您还可以使用加密上下文来细化或限制对您账户中 AWS KMS keys 的访问。您可以使用加密上下文作为授权中的约束，以及作为策略语句中的条件。

要了解如何使用加密上下文来保护加密数据的完整性，请参阅AWS安全博客 EncryptionContext上的“如何通过使用AWS Key Management Service来保护加密数据的完整性”一文。

有关加密上下文的更多信息。

加密上下文规则

AWS KMS 对加密上下文密钥和值强制执行以下规则。

- 加密上下文对中的键和值必须是简单的文本字符串。如果您使用其他类型（例如整数或浮点），则 AWS KMS 会将它解释为字符串。
- 加密上下文中的密钥和值可以包括 Unicode 字符。如果加密上下文包含密钥策略或 IAM policy 中不允许的字符，则您将无法在策略条件密钥中指定加密上下文，例如 kms:EncryptionContext:*context-key* 和 kms:EncryptionContextKeys。有关密钥策略文档规则的详细信息，请参阅 密钥策略格式。有关 IAM policy 档规则的详细信息，请参阅《IAM 用户指南》中的 IAM 名称要求。

策略中的加密上下文

加密上下文主要用于验证完整性和真实性。但是，您也可以使用加密上下文来控制对密钥策略和 IAM policy 中对称加密 AWS KMS keys 的访问。

仅当请求包含特定的加密上下文密钥或密钥值对时，k ms:: 和 kms: EncryptionContextKeys 条件密钥才允许（或拒绝）权限。EncryptionContext

例如，以下密钥策略语句允许 RoleForExampleApp 角色在 Decrypt 操作中使用 KMS 密钥。它使用 kms:EncryptionContext:*context-key* 条件键以仅在请求中的加密上下文包含 AppName:ExampleApp 加密上下文对时允许此权限。

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

有关这些加密上下文条件键的更多信息，请参阅 的条件密钥 AWS KMS。

授权中的加密上下文

当您创建授权时，您可以包含授权约束，为授予权限建立条件。AWS KMS 支持两个授权约束 `EncryptionContextEquals` 和 `EncryptionContextSubset`，这两个约束都涉及加密操作的请求中的加密上下文。在使用这些授权约束时，授权中的权限仅在加密操作请求中的加密上下文满足授权约束的要求时有效。

例如，您可以向`EncryptionContextEquals`授权添加允许该`GenerateDataKey`操作的授予约束。使用此约束时，授权仅在请求中的加密上下文与授权约束中的加密上下文大小写完全匹配时，允许操作。

```
$ 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}
```

来自被授予者委托人的以下请求将满足 `EncryptionContextEquals` 约束。

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

有关授权约束的详细信息，请参阅 使用授权约束。有关授权的详细信息，请参阅 the section called “授权”。

记录加密上下文

AWS KMS 使用 AWS CloudTrail 记录加密上下文，以便您可以确定访问了哪些 KMS 密钥和数据。日志条目会准确显示哪些 KMS 密钥被用来加密或解密了由日志条目中的加密上下文引用的特定数据。

> **Important**
>
> 由于加密上下文会被记录，它不得包含敏感信息。

存储加密上下文

为了简化在调用 Decrypt 或 ReEncrypt 操作时任何加密上下文的使用，可以将加密上下文与加密数据存储在一起。我们建议您仅存储足够的加密上下文，以帮助您在需要用于加密或解密时创建完整的加密上下文。

例如，如果加密上下文是文件的完全限定路径，仅将该路径部分与加密文件内容存储在一起。然后，当您需要完整的加密上下文时，可以从存储的片段重建它。如果有人擅自改动文件，例如重命名或将其移动到其他位置，加密上下文值更改，解密请求将失败。

密钥策略

在创建 KMS 密钥时，您可以确定可以使用和管理该 KMS 密钥的人员。这些权限包含在名为密钥策略的文档中。您可以使用密钥策略随时为客户托管密钥添加、删除或更改权限。但是，您无法编辑 AWS 托管式密钥 的密钥策略。有关更多信息，请参阅 中的关键政策 AWS KMS。

授权

授权是一种策略分析工具，允许 AWS 委托人将 AWS KMS keys 用于加密操作中。它还可以让他们查看 KMS 密钥 (DescribeKey) 以及创建和管理授权。在授权访问 KMS 密钥时，将考虑授权与密钥策略和 IAM policy。授权通常用于临时权限，因为您可以在不更改密钥策略或 IAM policy 的情况下创建授权、使用其权限并将其删除。由于授权可能非常具体，并且易于创建和撤销，因此它们通常用于提供临时权限或更精细的权限。

有关授权（包括授权术语）的详细信息，请参阅 AWS KMS 中的授权。

审核 KMS 密钥用法

您可以使用AWS CloudTrail来审核密钥使用情况。 CloudTrail 创建包含您账户的 AWS API 调用和相关事件历史记录的日志文件。这些日志文件包含通过 AWS 管理控制台、AWS 软件开发工具包和命令行工具发出的所有 AWS KMS API 请求。日志文件还包含 AWS 服务代表您向 AWS KMS 发出的请求。您可以使用这些日志文件来查找重要信息，包括使用 KMS 密钥的时间、所请求的操作、请求者的身份以及源 IP 地址。有关更多信息，请参阅 使用登录 AWS CloudTrail 和 AWS CloudTrail 用户指南。

密钥管理基础设施

加密术的常见做法是使用公开可用且经过同行评审的算法进行加密和解密，例如使用 AES (高级加密标准) 和私有密钥。加密术的主要问题之一是很难保持密钥的私密性。这通常是密钥管理基础设施 (KMI) 的工作。AWS KMS 可为您操作密钥基础设施。AWS KMS 会创建并安全地存储称为 AWS KMS keys

的根密钥。有关 AWS KMS 如何操作的更多信息，请参阅 AWS Key Management Service 加密详细信息。

管理 密钥

要开始使用 AWS KMS，请创建一个 AWS KMS key。

此部分中的主题介绍了如何管理基本 KMS 密钥、对称加密 KMS 密钥从创建到删除的整个过程。它包括以下主题：编辑和查看密钥、标记密钥、启用和禁用密钥、轮换密钥材质，以及使用 AWS 工具和服务来监控 KMS 密钥的使用情况。它还包括如下消息：使用 AWS CloudFormation 创建和管理 KMS 密钥，以及显示每个 AWS KMS 操作所需密钥状态的密钥状态引用。

有关创建、使用和管理其他类型的 KMS 密钥的信息，请参阅 特殊用途密钥。

主题

创建密钥

可以在AWS KMS keys中创建AWS Management Console，也可以使用CreateKey操作或AWS CloudFormation模板进行创建。在此过程中，您可以选择 KMS 密钥的类型、其区域性（单区域或多区域）以及密钥材料的来源（默认由 AWS KMS 为您创建密钥材料）。创建 KMS 密钥后，这些属性无法更改。您还可以设置 KMS 密钥的密钥策略，可以随时更改该策略。

本主题介绍如何创建基本 KMS 密钥、对称加密 KMS 密钥用于具有来自 AWS KMS 的密钥材料的单区域。您可以在 AWS 服务 中使用此 KMS 密钥保护您的资源。有关对称加密 KMS 密钥的详细信息，请参阅 SYMMETRIC_DEFAULT 密钥规范。有关创建其他类型密钥的帮助，请参阅 特殊用途密钥。

如果您要创建 KMS 密钥来加密在 AWS 服务中存储或管理的数据，请创建对称加密 KMS 密钥。与 AWS KMS 集成的 AWS 服务仅使用对称加密 KMS 密钥来加密您的数据。这些服务不支持使用非对称 KMS 密钥进行加密。有关如何确定要创建的 KMS 密钥类型的帮助信息，请参阅 选择一种 KMS 密钥类型。

> **Note**
>
> 对称 KMS 密钥现在称为对称加密 KMS 密钥。AWS KMS 支持两种对称 KMS 密钥、对称加密 KMS 密钥（默认类型）和 HMAC KMS 密钥，它们也是对称密钥。

当您在 AWS KMS 控制台中创建 KMS 密钥时，需要为其指定一个别名（友好名称）。`CreateKey` 操作不会为新 KMS 密钥创建别名。要为新的或现有的 KMS 密钥创建别名，请使用CreateAlias操作。有关在 AWS KMS 中的别名的详细信息，请参阅 使用别名。

本主题介绍如何创建对称加密 KMS 密钥。使用下表查找创建不同类型 KMS 密钥的说明。

创建 KMS 密钥的说明

KMS 密钥类型	说明
对称加密密钥（SYMMETRIC_DEFAULT）	the section called “创建对称加密 KMS 密钥”
非对称密钥	the section called “创建非对称 KMS 密钥”
HMAC 密钥	the section called “创建 HMAC 密钥”
多区域密钥（任何类型）	the section called “创建带导入的密钥材料的主密钥” the section called “创建带导入的密钥材料的副本密钥”
导入的密钥材料（“自带钥匙 – BYOK”）	the section called “步骤 1：创建不带密钥材料的 KMS 密钥”
AWS CloudHSM 密钥存储	the section called “在 AWS CloudHSM 密钥存储中创建 KMS 密钥”
外部密钥存储（“保管自己的钥匙 – HYOK”）	the section called “在外部密钥存储中创建 KMS 密钥”

了解更多：

- 要创建用于客户端加密的数据密钥，请使用GenerateDataKey操作。
- 要创建用于加密或签名的非对称 KMS 密钥，请参阅 创建非对称 KMS 密钥。
- 要创建 HMAC KMS 密钥，请参阅 创建 HMAC KMS 密钥。
- 要使用导入的密钥材料（“自备密钥”）创建 KMS 密钥，请参阅 导入密钥材料步骤 1：创建不带密钥材料的 AWS KMS key。
- 要创建多区域主密钥或副本密钥，请参阅 创建多区域密钥。
- 要在自定义密钥存储中创建 KMS 密钥（密钥材料源是自定义密钥存储（CloudHSM）），请参阅 在 AWS CloudHSM 密钥存储中创建 KMS 密钥。
- 要使用AWS CloudFormation模板创建 KMS 密钥，请参阅AWS CloudFormation用户指南AWS::KMS::Key中的。
- 要确定现有 KMS 密钥是对称还是非对称密钥，请参阅 识别非对称 KMS 密钥。
- 要以编程和命令行接口操作方式使用 KMS 密钥，您需要密钥 ID 或密钥 ARN。有关详细说明，请参阅 查找密钥 ID 和密钥 ARN。
- 有关应用于 KMS 密钥的配额的信息，请参阅 配额。

主题

创建 KMS 密钥的权限

要在控制台中或使用 API 创建 KMS 密钥，您必须在 IAM policy 中具有以下权限。在可能的情况下，使用条件键来限制权限。例如，您可以在 IAM 策略中使用 kms: KeySpec 条件密钥来允许委托人仅创建对称加密密钥。

有关创建密钥的委托人的 IAM policy 的示例，请参阅 允许用户创建 KMS 密钥。

> **Note**
>
> 请谨慎授予委托人管理标签和别名的权限。更改标签或别名可以允许或拒绝对客户托管密钥的权限。有关更多信息，请参阅 AWS KMS 中的 ABAC。

- km CreateKey s: 为必填项。
- km CreateAlias s: 需要在控制台中创建 KMS 密钥，其中每个新的 KMS 密钥都需要一个别名。
- km TagResource s: 需要在创建 KMS 密钥时添加标签。
- CreateServiceLinkedRolei@@ am: 是创建多区域主密钥所必需的。有关更多信息，请参阅 控制对多区域密钥的访问。

创建 KMS 密钥不需要 kms: PutKeyPolicy 权限。`kms:CreateKey` 权限包括设置初始密钥策略的权限。但是，您必须在创建 KMS 密钥时将此权限添加到密钥策略中，以确保您可以控制对 KMS 密钥的访问。另一种方法是使用BypassLockoutSafetyCheck参数，但不建议这样做。

KMS 密钥属于创建它们的 AWS 账户。创建 KMS 密钥的 IAM 用户不会被视为密钥的拥有者，且他们不会自动获得使用或管理自己所创建 KMS 密钥的权限。与任何其他主体一样，密钥创建者需要通过密钥策略、IAM policy 或授权获得权限。但是，拥有 `kms:CreateKey` 权限的主体可以设置初始密钥策略，并授予自己使用或管理密钥的权限。

创建对称加密 KMS 密钥

您可以在 AWS Management Console 中或使用 AWS KMS API 创建 KMS 密钥。

本主题介绍如何创建基本 KMS 密钥、对称加密 KMS 密钥用于具有来自 AWS KMS 的密钥材料的单区域。您可以在 AWS 服务 中使用此 KMS 密钥保护您的资源。有关创建其他类型密钥的帮助，请参阅特殊用途密钥。

创建对称加密 KMS 密钥（控制台）

您可以使用 AWS Management Console 创建 AWS KMS keys（KMS 密钥）。

> **Important**
>
> 不要在别名、描述或标签中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择 Create key。

5. 要创建对称加密 KMS 密钥，请为 Key type（密钥类型）选择 Symmetric（对称）。

   有关如何在 AWS KMS 控制台中创建非对称 KMS 密钥的信息，请参阅 创建非对称 KMS 密钥（控制台）。

6. 在 Key usage（密钥用法）中，已为您选择了 Encrypt and decrypt（加密和解密）选项。

   有关如何创建生成和验证 MAC 代码的 KMS 密钥的信息，请参阅 创建 HMAC KMS 密钥。

7. 请选择 Next（下一步）。

   有关Advanced options（高级选项）的更多信息，请参阅 特殊用途密钥。

8. 为 KMS 密钥键入别名。别名名称不能以 **aws/** 开头。**aws/** 前缀由 Amazon Web Services 预留，用于在您的账户中表示 AWS 托管式密钥。

   > **Note**
   >
   > 添加、删除或更新别名可以允许或拒绝对 KMS 密钥的权限。有关详细信息，请参阅 AWS KMS 中的 ABAC 和 使用别名控制对 KMS 密钥的访问。

   别名是一个显示名称，您可以使用它来标识 KMS 密钥。我们建议您选择一个别名，用来指示您计划保护的数据类型或计划与 KMS 密钥搭配使用的应用程序。

   在 AWS Management Console 中创建 KMS 密钥时需要别名。当您使用CreateKey操作时，它们是可选的。

9. （可选）为 KMS 密钥键入描述。

   现在，除非密钥状态为 `Pending Deletion` 或 `Pending Replica Deletion`，否则您可以随时添加描述或更新描述。要添加、更改或删除现有客户托管密钥的描述，请在中编辑描述AWS Management Console或使用UpdateKeyDescription操作。

10. (可选) 键入标签键和一个可选标签值。要向 KMS 密钥添加多个标签，请选择 Add tag（添加标签）。

    > **Note**
    >
    > 标记或取消标记 KMS 密钥可以允许或拒绝对 KMS 密钥的权限。有关详细信息，请参阅 AWS KMS 中的 ABAC 和 使用标签控制对 KMS 密钥的访问。

在将标签添加到 AWS 资源时，AWS 可生成成本分配报告，其中按标签汇总了使用情况和成本。标签还可以用来控制对 KMS 密钥的访问。有关轮换 KMS 密钥的信息，请参阅 标记密钥 和 AWS KMS 中的 ABAC。

11. 请选择 Next（下一步）。
12. 选择可管理 KMS 密钥的 IAM 用户和角色。

> **Note**
>
> 此密钥策略将授予 AWS 账户 对此 KMS 密钥的完全控制权。此控制权允许账户管理员使用 IAM policy 授予其他主体管理 KMS 密钥的权限。有关更多信息，请参阅 the section called “默认密钥策略”。
>
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

13. （可选）要阻止选定 IAM 用户和角色删除此 KMS 密钥，请在页面底部的 Key deletion（密钥删除）部分中，清除 Allow key administrators to delete this key（允许密钥管理员删除此密钥）复选框。
14. 请选择 Next（下一步）。
15. 选择可在加密操作中使用密钥的 IAM 用户和角色

> **Note**
>
> 此密钥策略将授予 AWS 账户 对此 KMS 密钥的完全控制权。此控制权允许账户管理员使用 IAM policy 授予其他主体在加密操作中使用 KMS 密钥的权限。有关更多信息，请参阅 the section called “默认密钥策略”。
>
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

16. （可选）您可以允许其他 AWS 账户 将此 KMS 密钥用于加密操作。为此，请在页面底部的 Other AWS 账户（其他 Amazon Web Services 账户）部分中，选择 Add another AWS 账户（添加另一个 Amazon Web Services 账户）并输入外部账户的 AWS 账户 账户标识号。要添加多个外部账户，请重复此步骤。

> **Note**
>
> 要允许外部账户中的委托人使用 KMS 密钥，外部账户的管理员必须创建提供这些权限的 IAM policy。有关更多信息，请参阅 允许其他账户中的用户使用 KMS 密钥。

17. 选择 下一步。
18. 检视您选择的密钥设置。您仍然可以返回并更改所有设置。
19. 选择 Finish（完成）以创建 KMS 密钥。

创建对称加密 KMS 密钥（AWS KMS API）

您可以使用该CreateKey操作来创建AWS KMS keys所有类型。这些示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

> **Important**
>
> 不要在 `Description` 或 `Tags` 字段中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

以下操作会创建最常用的 KMS 密钥，这是由 AWS KMS 生成的密钥材料提供支持的、单个区域中的对称加密密钥。该操作没有必需参数。不过，您可能还希望使用 `Policy` 参数指定密钥策略。您可以随时更改密钥策略 (PutKeyPolicy) 并添加可选元素，例如描述和标签。您还可以创建非对称密钥、多区域密钥、具有导入密钥材料的密钥以及自定义密钥存储中的密钥。

该`CreateKey`操作不允许您指定别名，但您可以使用该CreateAlias操作为新 KMS 密钥创建别名。

以下示例显示的是在没有任何参数的情况下调用 `CreateKey` 操作。此命令使用所有默认值。它将创建一个具有 AWS KMS 生成的密钥材料的对称加密 KMS 密钥。

```
$ 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"
        ],
    }
}
```

如果您不为新 KMS 密钥指定密钥策略，则 CreateKey 应用的默认密钥策略会不同于在您使用控制台创建新 KMS 密钥时控制台应用的默认密钥策略。

例如，此GetKeyPolicy操作调用将返回CreateKey适用的密钥策略。它授予了对 KMS 密钥的 AWS 账户 访问权限，并允许它为 KMS 密钥创建 AWS Identity and Access Management (IAM) 策略。有关 KMS 密钥的 IAM policy 和密钥策略的详细信息，请参阅 AWS KMS 的身份验证和访问控制

```
$ 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" : "*"
  } ]
}
```

使用别名

别名是 AWS KMS key 的友好名称。例如，别名允许您将 KMS 密钥引用为 test-key，而不是 1234abcd-12ab-34cd-56ef-1234567890ab。

您可以使用别名在AWS KMS控制台、操作和加密DescribeKey操作（例如 E n crypt 和）中标识 KMS 密钥。GenerateDataKey别名还使您能够轻松识别 AWS 托管式密钥。这些 KMS 密钥的别名始终具有 aws/*<service-name>* 形式。例如，适用于 Amazon DynamoDB 的 AWS 托管式密钥 的别名为 aws/dynamodb。您可以为项目建立类似的别名标准，例如在别名前加上项目或类别的名称。

您还可以根据 KMS 密钥的别名允许和拒绝访问 KMS 密钥，而无需编辑策略或管理授权。此功能是 AWS KMS 对基于属性的访问控制 (ABAC) 的一部分。有关更多信息，请参阅 使用别名控制对 KMS 密钥的访问。

别名的大部分功能来自于您随时更改与别名关联的 KMS 密钥的能力。别名可以使您的代码更易于编写和维护。例如，假设您使用别名来引用特定 KMS 密钥，并且您想要更改 KMS 密钥。在这种情况下，只需将别名与其他 KMS 密钥关联即可。您不需要更改您的代码。

别名还您更容易在不同 AWS 区域 中重用相同代码。在多个区域中创建具有相同名称的别名，并将每个别名与其区域中的 KMS 密钥关联。当代码在每个区域中运行时，别名将引用该区域中关联的 KMS 密钥。有关示例，请参阅在应用程序中使用别名。

您可以使用 CreateAliasAPI 或使用AWS CloudFormation模板在AWS KMS控制台中为 KMS 密钥创建别名。

AWS KMS API 提供对每个账户和区域中的别名的完全控制。API 包括创建别名 (CreateAlias)、查看别名和别名 ARN (ListAliases)、更改与别名关联的 KMS 密钥 (UpdateAlias) 以及删除别名 (DeleteAlias) 的操作。有关使用多种编程语言管理别名的示例，请参阅 the section called “使用别名”。

以下资源可帮助您了解更多信息：

- 有关 KMS 密钥标识符（包括别名）的信息，请参阅 密钥标识符 (KeyId)。
- 有关使用AWS CloudFormation模板为 KMS 密钥创建别名的帮助，请参阅AWS CloudFormation用户指南AWS::KMS::Alias中的。
- 要获得查找与 KMS 密钥关联的别名的帮助，请参阅 查找别名和别名 ARN
- 有关别名的资源配额和与别名相关的 API 操作的费率配额的信息，请参阅 配额。
- 有关使用多种编程语言创建和管理别名的示例，请参阅 使用别名。

主题

- 关于别名
- 管理别名
- 在应用程序中使用别名

- 控制对别名的访问
- 使用别名控制对 KMS 密钥的访问
- 查找 AWS CloudTrail 日志中的别名

关于别名

了解别名在 AWS KMS 中的作用方式。

别名是独立的 AWS 资源

别名不是 KMS 密钥的属性。您对别名执行的操作不会影响其关联的 KMS 密钥。您可以为 KMS 密钥创建别名，然后更新别名，使其与其他 KMS 密钥相关联。您甚至可以删除别名，而不会对关联的 KMS 密钥产生任何影响。但是，如果您删除 KMS 密钥，则会删除与该 KMS 密钥关联的所有别名。

如果您在 IAM policy 中指定别名作为资源，则该策略将引用别名，而不是关联的 KMS 密钥。

每个别名都有两种格式

在创建别名时，请指定别名。AWS KMS 会为您创建别名 ARN。

- 别名 ARN 是唯一标识别名的 Amazon Resource Name (ARN)。

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

- 别名名称在账户和所在区域中是唯一的。在 AWS KMS API 中，别名名称始终以 `alias/` 为前缀。此前缀在 AWS KMS 控制台中将省略。

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

别名不是密钥

别名可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。不要在别名名称中包含机密或敏感信息。

每个别名一次与一个 KMS 密钥关联

别名及其 KMS 密钥必须位于同一账户和区域中。

您可以将别名与相同 AWS 账户 和区域中的任何客户托管密钥关联。但是，您无权将别名与 AWS 托管式密钥 关联。

例如，此ListAliases输出显示test-key别名恰好与一个目标 KMS 密钥相关联，该密钥由TargetKeyId属性表示。

```
{
     "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
}
```

多个别名可以与同一 KMS 密钥关联

例如，您可以将 test-key 和 project-key 别名与同一个 KMS 密钥关联。

```
{
     "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
}
```

别名在账户和区域中必须是唯一的

例如，您在每个账户和区域中只能有一个 test-key 别名。别名区分大小写，但仅在大小写上不同的别名很容易出错。您不能更改别名名称。但是，您可以删除别名并使用所需名称创建新别名。

您可以在不同的区域中创建具有相同名称的别名。

例如，您可以在美国东部（弗吉尼亚北部）拥有 finance-key 别名，在欧洲（法兰克福）拥有 finance-key 别名。每个别名都将与其区域中的 KMS 密钥相关联。如果您的代码引用 alias/finance-key 之类的别名名称，您可以在多个区域中运行它。在每个区域中，它使用不同的 KMS 密钥。有关更多信息，请参阅 在应用程序中使用别名。

您可以更改与别名关联的 KMS 密钥

您可以使用该UpdateAlias操作将别名与其他 KMS 密钥相关联。例如，如果 `finance-key` 别名与 `1234abcd-12ab-34cd-56ef-1234567890ab` KMS 密钥关联，您可以对其进行更新，使其与 `0987dcba-09fe-87dc-65ba-ab0987654321` KMS 密钥关联。

但是，当前 KMS 密钥和新的 KMS 密钥必须是相同的类型（要么都是对称的，要么都是非对称的，要么都是 HMAC），并且它们必须具有相同的密钥用途（ENCRYPT_DECRYPT、SIGN_VERIFY 或 GENERATE_VERIFY_MAC）。此限制可防止使用别名的代码中出现错误。如果您必须将别名与其他类型的密钥关联，并且您已降低风险，则可以删除并重新创建别名。

有些 KMS 密钥没有别名

当您在 AWS KMS 控制台中创建 KMS 密钥时，您必须为其指定新别名。但是，使用该CreateKey操作创建 KMS 密钥时，不需要别名。此外，您还可以使用UpdateAlias操作来更改与别名关联的 KMS 密钥，使用该DeleteAlias操作来删除别名。因此，有些 KMS 密钥可能有多个别名，有些可能没有别名。

AWS 在您的账户中创建别名

AWS 在您的账户中为 AWS 托管式密钥 创建别名。这些别名具有 `alias/aws/<service-name>` 形式的名称，例如 `alias/aws/s3`。

有些 AWS 别名没有 KMS 密钥。这些预定义别名通常在您开始使用服务时就与 AWS 托管式密钥关联。

使用别名标识 KMS 密钥

在加密操作中，您可以使用别名或别名 ARN 来标识 KMS 密钥、DescribeKey和。GetPublicKey（如果 KMS 密钥位于不同的 AWS 账户 中，您必须使用其密钥 ARN 或别名 ARN。）别名不是 KMS 密钥在其他 AWS KMS 操作中的有效标识符。有关每个 AWS KMS API 操作的有效密钥标识符的信息，请参阅 AWS Key Management Service API 参考中的 `KeyId` 参数的描述。

您不能使用别名名称或别名 ARN 来标识 IAM policy 中的 KMS 密钥。要根据别名控制对 KMS 密钥的访问权限，请使用 k ms: RequestAlias 或 k ms: ResourceAliases 条件密钥。有关更多信息，请参阅 AWS KMS 中的 ABAC。

管理别名

授权用户可以创建、查看和删除别名。您也可以更新别名，也就说，将现有别名与其他 KMS 密钥相关联。

主题

创建别名

您可以在 AWS KMS 控制台中或使用 AWS KMS API 操作来创建别名。

别名必须为 1-256 个字符的字符串。它只能包含字母数字字符、正斜杠 (/)、下划线 (_) 和连字符 (-)。客户托管密钥的别名名称不能以开头 `alias/aws/` 开头。`alias/aws/` 前缀专门预留供 AWS 托管式密钥 使用。

您可以为新的 KMS 密钥或现有的 KMS 密钥创建别名。您可以添加别名，以便在项目或应用程序中使用特定 KMS 密钥。

创建别名（控制台）

当您在 AWS KMS 控制台中创建 KMS 密钥时，您必须为新的 KMS 密钥创建别名。要为现有 KMS 密钥创建别名，请使用 KMS 密钥详细信息页面上的 Aliases（别名）选项卡。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。您无法管理 AWS 托管式密钥 或 AWS 拥有的密钥 的别名。
4. 在表中，选择 KMS 密钥的密钥 ID 和别名。然后，在 KMS 密钥详细信息页面上，选择 Aliases（别名）选项卡。

   如果 KMS 密钥具有多个别名，则表中的 Aliases（别名）列会显示一个别名和一个别名摘要，例如（再加 n 个）。选择别名摘要将直接进入 KMS 密钥详细信息页面上的 Aliases（别名）选项卡中。
5. 在 Aliases（别名）选项卡上，选择 Create alias（创建别名）。输入别名名称，然后选择 Create alias（创建别名）。

> **Important**
>
> 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。

> **Note**
>
> 不要添加 `alias/` 前缀。控制台会为您自动添加。如果您输入 `alias/ExampleAlias`，实际的别名名称将是 `alias/alias/ExampleAlias`。

创建别名 (AWS KMS API)

要创建别名，请使用CreateAlias操作。与在控制台中创建 KMS 密钥的过程不同，该CreateKey操作不会为新的 KMS 密钥创建别名。

> **Important**
>
> 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。

您可以使用 `CreateAlias` 操作为没有别名的新 KMS 密钥创建别名。您也可以使用 `CreateAlias` 操作将别名添加到任何现有 KMS 密钥中或重新创建意外删除的别名。

在 AWS KMS API 操作中，别名名称必须以 `alias/` 开头，后跟一个名称（例如 `alias/ExampleAlias`）。别名在账户和 区域中必须是唯一的。要查找已在使用的别名，请使用ListAliases操作。别名名称区分大小写。

`TargetKeyId`可以是相同 AWS 区域 中的任何客户托管密钥。要标识 KMS 密钥，请使用其密钥 ID 或密钥 ARN。您不能使用另一个别名。

以下示例将创建 `example-key` 别名，并将其与指定的 KMS 密钥相关联。这些示例使用 AWS Command Line Interface (AWS CLI)。有关使用多种编程语言的示例，请参阅使用别名。

```
$ aws kms create-alias \
    --alias-name alias/example-key \
```

```
    --target-key-id 1234abcd-12ab-34cd-56ef-1234567890ab
```

CreateAlias 不返回任何输出。要查看新别名，请使用 ListAliases 操作。有关更多信息，请参阅 查看别名 (AWS KMS API)。

查看别名

别名使您能够轻松识别 AWS KMS 控制台中的 KMS 密钥。您可以在AWS KMS控制台中或使用ListAliases操作查看 KMS 密钥的别名。该DescribeKey操作返回 KMS 密钥的属性，但不包括别名。

查看别名（控制台）

AWS KMS 控制台中的客户托管密钥和 AWS 托管式密钥 页面显示与每个 KMS 密钥关联的别名。您还可以基于 KMS 密钥的别名搜索、排序和筛选 KMS 密钥。

下面的 AWS KMS 控制台图像显示示例账户的客户托管密钥页面上的别名。如图所示，有些 KMS 密钥没有别名。

如果 KMS 密钥具有多个别名，则 Aliases（别名）列会显示一个别名和一个别名摘要（再加 n 个）。别名摘要显示与 KMS 密钥相关联的其他别名数量，以及指向 Aliases（别名）选项卡上的 KMS 密钥的所有别名显示的链接。

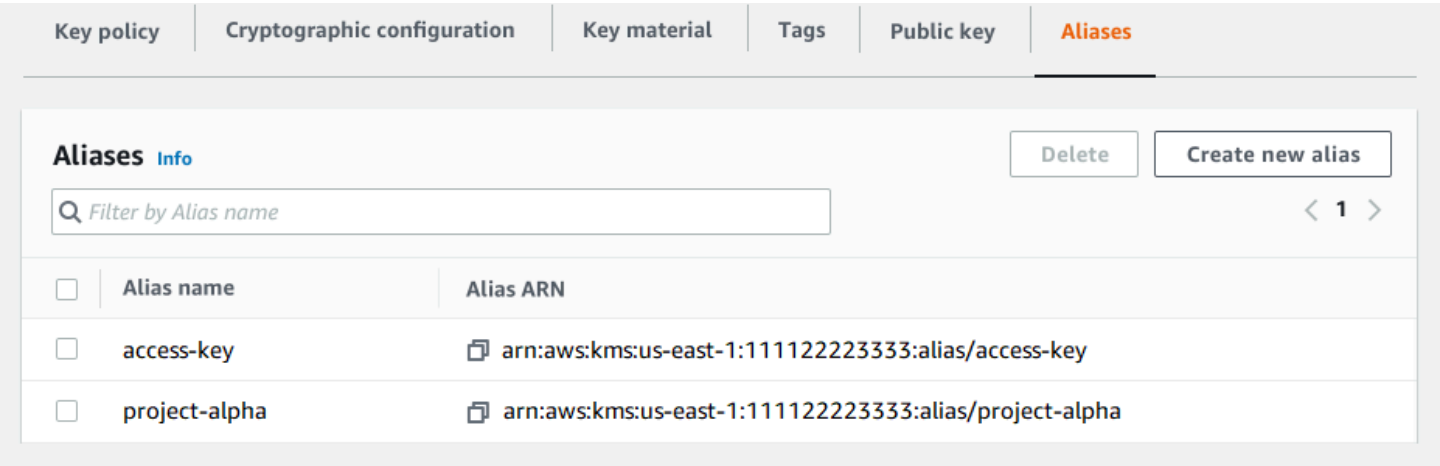
Aliases	Key ID	Status
-	1234abcd-12ab-34cd-56ef-1234567890ab	Enabled
access-key (+1 more)	0987dcba-09fe-87dc-65ba-ab0987654321	Enabled
finance	1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d	Enabled
RSA-4096-Encrypt	1234abcd-09fe-87dc-65ba-5e6f1a2b3c4d	Enabled
RSA-4096-Sign	0987dcba-09fe-34cd-56ef-1234567890ab	Enabled
project-key	1a2b3c4d-5e6f-87dc-65ba-ab0987654321	Enabled

每个 KMS 密钥的详细信息页面上的 Aliases（别名）选项卡显示 AWS 账户 和区域中的 KMS 密钥的所有别名的别名名称和别名 ARN。您也可以使用 Aliases（别名）选项卡创建别名和删除别名。

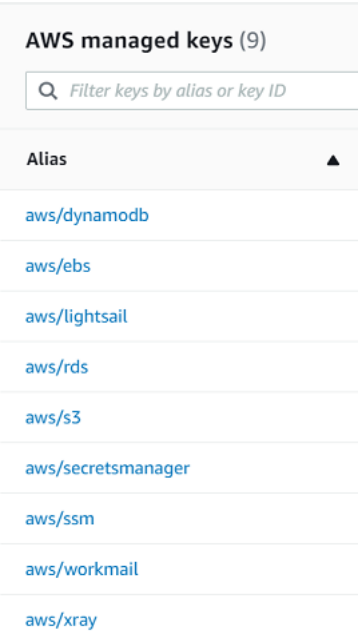
要查找 KMS 密钥的所有别名的名称和别名 ARN，请使用 Aliases（别名）选项卡。

- 要直接转到 Aliases（别名）选项卡上的 Aliases（别名）列中，选择别名摘要（再加 n 个）。仅当 KMS 密钥具有多个别名时，才会显示别名摘要。
- 或者，选择 KMS 密钥的别名或密钥 ID（这将打开 KMS 密钥的详细信息页面），然后选择 Aliases（别名）选项卡。这些选项卡在 General configuration（常规配置）部分下。

下图显示了示例 KMS 密钥的 Aliases（别名）选项卡。



您可以使用别名识别 AWS 托管式密钥，如此示例 AWS 托管式密钥 页面中所示。AWS 托管式密钥 的别名始终具有以下格式：aws/*<service-name>*。例如，适用于 Amazon DynamoDB 的 AWS 托管式密钥 的别名为 aws/dynamodb。



查看别名 (AWS KMS API)

该ListAliases操作返回账户和区域中别名的别名和别名 ARN。输出包括 AWS 托管式密钥 和客户托管密钥的别名。AWS 托管式密钥 的别名始终具有格式 aws/*<service-name>* ，如 aws/dynamodb。

该响应可能还包括没有 TargetKeyId 字段的别名。这些是 AWS 已创建但尚未与 KMS 密钥关联的预定义别名。

```
$ 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
        }
    ]
}
```

要获取与特定 KMS 密钥关联的所有别名，请使用 `ListAliases` 操作的可选 `KeyId` 参数。`KeyId` 参数采用 KMS 密钥的密钥 ID 或者密钥 ARN。

此示例获取与 `0987dcba-09fe-87dc-65ba-ab0987654321` KMS 密钥关联的所有别名。

```
$ 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
        }
    ]
}
```

`KeyId` 参数不采用通配符，但您可以使用编程语言的功能筛选响应。

例如，以下 AWS CLI 命令仅获取 AWS 托管式密钥 的别名。

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

例如，以下命令仅获取 access-key 别名。别名名称区分大小写。

```
$ 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"
    }
]
```

更新别名

由于别名是独立的资源，因此您可以更改与别名关联的 KMS 密钥。例如，如果test-key别名与一个 KMS 密钥关联，则可以使用该UpdateAlias操作将其与其他 KMS 密钥关联。这是手动轮换 KMS 密钥而不更改其密钥材料的几种方法之一。您还可以更新 KMS 密钥，以使将一个 KMS 密钥用于新资源的应用程序现在使用不同的 KMS 密钥。

您无法在 AWS KMS 控制台中更新别名。另外，您不能使用 UpdateAlias（或任何其他操作）更改别名名称。要更改别名名称，请删除当前别名，然后为 KMS 密钥创建新的别名。

更新别名时，当前 KMS 密钥和新 KMS 密钥必须为相同类型（均为对称、非对称或 HMAC）。它们还必须拥有相同的密钥用法（ENCRYPT_DECRYPT、SIGN_VERIFY 或 GENERATE_VERIFY_MAC）。此限制可防止使用别名的代码中出现加密错误。

以下示例首先使用ListAliases操作来显示test-key别名当前与 KMS 密钥相关联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
```

```
        }
    ]
}
```

接下来，它使用 UpdateAlias 操作将与 test-key 别名关联的 KMS 密钥更改为 KMS 密钥 0987dcba-09fe-87dc-65ba-ab0987654321。您不需要指定当前关联的 KMS 密钥，只需指定新的（“目标”）KMS 密钥。别名名称区分大小写。

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

要验证别名现在是否已与目标 KMS 密钥关联，请再次使用 ListAliases 操作。该 AWS CLI 命令使用 --query 参数来仅获取 test-key 别名。TargetKeyId 和 LastUpdatedDate 字段将更新。

```
$ 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
    }
]
```

删除别名

您可以在AWS KMS控制台中删除别名，也可以使用DeleteAlias操作来删除别名。删除别名之前，请确保别名未使用。虽然删除别名不会影响关联的 KMS 密钥，但它可能会为使用别名的任何应用程序造成问题。如果错误地删除了别名，您可以创建具有相同名称的新别名，并将其与相同或不同的 KMS 密钥关联。

如果您删除 KMS 密钥，则会删除与该 KMS 密钥关联的所有别名。

删除别名（控制台）

要在 AWS KMS 控制台中删除别名，请使用 KMS 密钥的详细信息页面上的 Aliases（别名）选项卡。您可以一次删除一个 KMS 密钥的多个别名。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。

2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。您无法管理 AWS 托管式密钥 或 AWS 拥有的密钥 的别名。
4. 在表中，选择 KMS 密钥的密钥 ID 和别名。然后，在 KMS 密钥详细信息页面上，选择 Aliases（别名）选项卡。

   如果 KMS 密钥具有多个别名，则表中的 Aliases（别名）列会显示一个别名和一个别名摘要，例如（再加 n 个）。选择别名摘要将直接进入 KMS 密钥详细信息页面上的 Aliases（别名）选项卡中。
5. 在 Aliases（别名）选项卡上，选中要删除的别名旁边的复选框。然后选择删除。

删除别名 (AWS KMS API)

要删除别名，请使用DeleteAlias操作。此操作一次删除一个别名。别名名称区分大小写，且前面必须带有 `alias/` 前缀。

例如，以下命令删除 `test-key` 别名。此命令不返回任何输出。

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

要验证别名是否已删除，请使用ListAliases操作。以下命令使用 AWS CLI 中的 `--query` 参数来仅获取 `test-key` 别名。响应中的空括号表示 `ListAliases` 响应不包含 `test-key` 别名。要消除括号，请使用 `--output text` 参数和值。

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

在应用程序中使用别名

您可以使用别名在应用程序代码中表示 KMS 密钥。AWS KMS加密运算中的`KeyId`参数DescribeKey、和GetPublicKey接受别名或别名 ARN。

例如，以下 `GenerateDataKey` 命令使用别名名称 (`alias/finance`) 来标识 KMS 密钥。别名名称是 `KeyId` 参数的值。

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

如果 KMS 密钥位于不同的 AWS 账户 中，您必须在这些操作中使用密钥 ARN 或别名 ARN。使用别名 ARN 时，请记住 KMS 密钥的别名是在拥有 KMS 密钥的账户中定义的，并且在每个区域中可能会有所不同。有关查找别名 ARN 的帮助，请参阅 查找别名和别名 ARN。

例如，以下 GenerateDataKey 命令使用不在调用者账户中的 KMS 密钥。ExampleAlias 别名与指定账户和区域中的 KMS 密钥相关联。

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

别名的最强大用途之一是在多个 AWS 区域 中运行的应用程序中。例如，您可能有一个使用 RSA 非对称 KMS 密钥进行签名和验证的全局应用程序。

- 在美国西部（俄勒冈）(us-west-2) 区域中，您需要使用 arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab。
- 在欧洲（法兰克福）(eu-central-1) 区域中，您需要使用 arn:aws:kms:eu-central-1:111122223333:key/0987dcba-09fe-87dc-65ba-ab0987654321
- 在亚太地区（新加坡）(ap-southeast-1) 区域中，您需要使用 arn:aws:kms:ap-southeast-1:111122223333:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d。

您可以在每个区域中创建不同版本的应用程序，也可以使用字典或 switch 语句为每个区域选择正确的 KMS 密钥。但在每个区域中创建具有相同别名名称的别名要容易得多。请记住，别名名称区分大小写。

```
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
```

然后，在代码中使用别名。当代码在每个区域中运行时，别名将引用该区域中关联的 KMS 密钥。例如，此代码将使用别名名称调用 Sign 操作。

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

但是，别名可能有被删除或更新为与其他 KMS 密钥关联的风险。在这种情况下，应用程序尝试使用别名名称验证签名将失败，您可能需要重新创建或更新别名。

要降低此风险，请谨慎授予委托人管理您在应用程序中使用的别名的权限。有关更多信息，请参阅 控制对别名的访问。

对于在多个 AWS 区域 中加密数据的应用程序，还有几个其他解决方案，包括 AWS Encryption SDK。

控制对别名的访问

创建或更改别名时，会影响别名及其关联的 KMS 密钥。因此，管理别名的委托人必须具有对别名和所有受影响的 KMS 密钥调用别名操作的权限。您可以通过使用密钥策略、IAM policy 和授权来提供这些权限。

> **Note**
>
> 请谨慎授予委托人管理标签和别名的权限。更改标签或别名可以允许或拒绝对客户托管密钥的权限。有关详细信息，请参阅 AWS KMS 中的 ABAC 和 使用别名控制对 KMS 密钥的访问。

有关控制对所有 AWS KMS 操作的访问的信息，请参阅 权限参考。

创建和管理别名的权限如下所示。

kms: CreateAlias

要创建别名，委托人需要别名和相关 KMS 密钥的以下权限。

- 别名的 `kms:CreateAlias`。在附加到允许创建别名的委托人的 IAM policy 中提供此权限。

  以下示例策略语句在 `Resource` 元素中指定特定别名。但是，您可以列出多个别名 ARN 或指定别名模式，例如“test*”。您还可以指定 `"*"` 的 `Resource` 值以允许委托人在账户和区域中创建任何别名。创建别名的权限也可以包含在对账户和区域中的所有资源的 `kms:Create*` 权限中。

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

- KMS 密钥的 `kms:CreateAlias`。此权限必须在密钥策略或者从密钥策略委派的 IAM policy 中提供。

```
{
  "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": "*"
}
```

您可以使用条件键限制可以与别名关联的 KMS 密钥。例如，您可以使用 k ms: KeySpec 条件密钥来允许委托人仅在非对称 KMS 密钥上创建别名。有关您可以用于限制对 KMS 密钥资源的 `kms:CreateAlias` 权限的条件键完整列表，请参阅 AWS KMS 权限。

kms: ListAliases

要列出账户和区域中的别名，委托人必须在 IAM policy 中具有 `kms:ListAliases` 权限。由于此策略与任何特定 KMS 密钥或别名资源无关，因此策略中资源元素的值必须为 `"*"`。

例如，以下 IAM policy 语句授予委托人列出账户和区域中所有 KMS 密钥和别名的权限。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
```

```
    "Action": [
      "kms:ListKeys",
      "kms:ListAliases"
    ],
    "Resource": "*"
  }
}
```

kms: UpdateAlias

要更改与别名关联的 KMS 密钥，委托人需要三个权限元素：一个用于别名，一个用于当前 KMS 密钥，另一个用于新的 KMS 密钥。

例如，假设您想要将 `test-key` 别名从具有密钥 ID 1234abcd-12ab-34cd-56ef-1234567890ab 的 KMS 密钥更改为具有密钥 ID 0987dcba-09fe-87dc-65ba-ab0987654321 的 KMS 密钥。在这种情况下，请包括类似于本部分中的示例的策略语句。

- 别名的 `kms:UpdateAlias`。您可以在附加到委托人的 IAM policy 中提供此权限。以下 IAM policy 指定了一个特定的别名。但是，您可以列出多个别名 ARN 或指定别名模式，例如 `"test*"`。您还可以指定 `"*"` 的 `Resource` 值以允许委托人在账户和区域中更新任何别名。

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

- 当前与别名关联的 KMS 密钥的 `kms:UpdateAlias`。此权限必须在密钥策略或者从密钥策略委派的 IAM policy 中提供。

```
{
  "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": "*"
}
```

- 操作将其与别名关联的 KMS 密钥的 `kms:UpdateAlias`。此权限必须在密钥策略或者从密钥策略委派的 IAM policy 中提供。

```
{
  "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": "*"
}
```

您可以使用条件键在 `UpdateAlias` 操作中限制其中一个或两个 KMS 密钥。例如，您可以使用 k ms: ResourceAliases 条件密钥来允许委托人仅在目标 KMS 密钥已具有特定别名时才更新别名。有关您可以用于限制对 KMS 密钥资源的 `kms:UpdateAlias` 权限的条件键完整列表，请参阅 AWS KMS 权限。

kms: DeleteAlias

要删除别名，委托人需要别名和相关 KMS 密钥的权限。

与往常一样，在授予委托人删除资源的权限时，您应该谨慎操作。但是，删除别名不会影响关联的 KMS 密钥。虽然这可能会导致依赖别名的应用程序出现故障，但如果错误地删除了别名，您可以重新创建别名。

- 别名的 `kms:DeleteAlias`。在附加到允许删除别名的委托人的 IAM policy 中提供此权限。

  以下示例策略语句在 `Resource` 元素中指定别名。但是，您可以列出多个别名 ARN 或指定别名模式，如 `"test*"`，您还可以指定 `"*"` 的 `Resource` 值，以允许委托人删除账户和区域中的任何别名。

```
{
  "Sid": "IAMPolicyForAnAlias",
  "Effect": "Allow",
  "Action": [
```

```
    "kms:CreateAlias",
    "kms:UpdateAlias",
    "kms:DeleteAlias"
  ],
  "Resource": "arn:aws:kms:us-west-2:111122223333:alias/test-key"
}
```

- 关联的 KMS 密钥的 `kms:DeleteAlias`。此权限必须在密钥策略或者从密钥策略委派的 IAM policy 中提供。

```
{
  "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": "*"
}
```

限制别名权限

当资源为 KMS 密钥时，您可以使用条件键限制别名权限。例如，以下 IAM policy 允许对特定账户和区域中的 KMS 密钥执行别名操作。但是，它使用 k ms: KeyOrigin 条件密钥进一步限制对密钥材料的 KMS 密钥的权限AWS KMS。

有关您可以用于限制对 KMS 密钥资源的别名权限的条件键完整列表，请参阅 AWS KMS 权限。

```
{
  "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"
    }
  }
}
```

您不能在资源为别名的策略语句中使用条件键。若要限制委托人可以管理的别名，请使用控制对别名访问的 IAM policy 语句的 Resource 元素的值。例如，以下策略语句允许委托人创建、更新或删除 AWS 账户 和区域中的任何别名，除非别名以 Restricted 开头。

```
{
  "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*"
}
```

使用别名控制对 KMS 密钥的访问

您可以根据与 KMS 密钥关联的别名来控制对 KMS 密钥的访问。为此，请使用 kms: RequestAlias 和 kms: ResourceAliases 条件密钥。此功能是 AWS KMS 对基于属性的访问控制 (ABAC) 的一部分。

kms:RequestAlias 条件键基于请求中的别名允许或拒绝对 KMS 密钥的访问。kms:ResourceAliases 条件键基于与 KMS 密钥关联的别名允许或拒绝对 KMS 密钥的访问。

这些功能不允许您通过使用策略语句的 resource 元素中的别名来标识 KMS 密钥。当别名是 resource 元素的值时，策略将应用于别名资源，而不是可能与其关联的任何 KMS 密钥。

> **Note**
>
> 标签和别名的更改最多可能需要 5 分钟的时间才能影响 KMS 密钥授权。最近的更改可能会在 API 操作中显示，然后才会影响授权。

使用别名控制对 KMS 密钥的访问权限时，请考虑以下事项：

- 使用别名来强化最低权限访问的最佳实践。仅为 IAM 委托人授予他们对必须使用或管理的 KMS 密钥的所需权限。例如，使用别名标识用于项目的 KMS 密钥。然后授予项目团队仅使用带有项目别名的 KMS 密钥的权限。
- 谨慎为委托人提供 `kms:CreateAlias`、`kms:UpdateAlias` 或 `kms:DeleteAlias` 权限，以允许他们添加、编辑和删除标签。当您使用别名控制对 KMS 密钥的访问时，更改别名可以授予委托人使用他们没有权限使用的 KMS 密钥的权限。它还可以拒绝对其他委托人执行其工作所需的 KMS 密钥的访问。
- 查看您的 AWS 账户 中当前有权管理别名和调整权限（如有必要）的委托人。不具有更改密钥策略或创建授权权限的密钥管理员可以控制对 KMS 密钥的访问，前提是他们有权管理别名。

  例如，控制台密钥管理员的默认密钥策略包括对 `kms:CreateAlias`、`kms:DeleteAlias` 和 `kms:UpdateAlias` 权限。IAM policy 可能会授予对您的 AWS 账户 中所有 KMS 密钥的别名权限。例如，AWSKeyManagementServicePowerUser托管策略允许委托人创建、删除和列出所有 KMS 密钥的别名，但不允许对其进行更新。
- 在设置依赖于别名的策略之前，请查看您的 AWS 账户 中的 KMS 密钥上的别名。请确保您的策略仅适用于您要包含的别名。使用CloudTrail 日志和CloudWatch 警报提醒您注意可能影响您的 KMS 密钥访问权限的别名更改。此外，ListAliases响应还包括每个别名的创建日期和上次更新日期。
- 别名策略条件使用模式匹配；它们不绑定到别名的特定实例。使用基于别名的条件键的策略会影响与模式匹配的所有新别名和现有别名。如果删除并重新创建与策略条件匹配的别名，则该条件将应用于新别名，就像对旧别名一样。

`kms:RequestAlias` 条件键依赖于操作请求中明确指定的别名。`kms:ResourceAliases` 条件键取决于与 KMS 密钥关联的别名，即使它们未出现在请求中。

kms: RequestAlias

基于标识请求中的 KMS 密钥的别名，允许或拒绝对 KMS 密钥的访问。您可以在密钥策略或 IAM 策略中使用 kms: RequestAlias 条件密钥。它适用于在请求中使用别名标识 KMS 密钥的操作，即加密操作DescribeKey、和GetPublicKey。它对别名操作无效，例如CreateAlias或DeleteAlias。

在条件键中，指定别名名称或别名名称模式。您不能指定别名 ARN。

例如，以下密钥策略语句允许委托人在 KMS 密钥上使用指定的操作。权限仅在请求使用包含可标识 KMS 密钥的 alpha 别名时有效。

```
{
  "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*"
    }
  }
}
```

以下来自授权委托人的示例请求将满足条件。但是，使用密钥 ID、密钥 ARN 或者其他别名的请求将无法满足条件，即使这些值标识了相同的 KMS 密钥。

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

kms: ResourceAliases

基于与 KMS 密钥关联的别名允许或拒绝访问 KMS 密钥，即使请求中未使用别名也是如此。k ms: ResourceAliases 条件密钥允许您指定别名或别名模式，例如alias/test*，这样您就可以在 IAM 策略中使用它来控制对同一区域中多个 KMS 密钥的访问权限。它对于使用 KMS 密钥的任何 AWS KMS 操作有效。

例如，以下 IAM policy 允许委托人在两个 AWS 账户 中的 KMS 密钥上管理自动密钥轮换。但是，该权限仅适用于与开头为 restricted 的别名相关联的 KMS 密钥。

```
{
```

```
  "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*"
        }
      }
    }
  ]
}
```

kms:ResourceAliases 条件是资源的条件，而不是请求的。因此，未指定别名的请求仍然可以满足条件。

以下示例请求（指定匹配别名）满足条件。

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

但是，下面的示例请求也满足条件，前提是指定的 KMS 密钥具有以 restricted 开头的别名，即使该别名未在请求中使用。

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

查找 AWS CloudTrail 日志中的别名

您可以使用别名表示 AWS KMS API 操作中的 AWS KMS key。当您执行此操作时，KMS 密钥的别名和密钥 ARN 将记录在事件的 AWS CloudTrail 日志条目中。别名显示在 requestParameters 字段中。密钥 ARN 显示在 resources 字段中。即使 AWS 服务使用您账户中的 AWS 托管式密钥 也是如此。

例如，以下GenerateDataKey请求使用project-key别名表示 KMS 密钥。

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

当此请求记录在 CloudTrail 日志中时，日志条目包括所使用的实际 KMS 密钥的别名和密钥 ARN。

```
{
    "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"
}
```

有关在 CloudTrail 日志中记录AWS KMS操作的详细信息，请参阅使用记录 AWS KMS API 调用 AWS CloudTrail。

查看密钥

您可以使用 AWS Management Console或 AWS Key Management Service（AWS KMS）API 来查看每个账户和区域中的 AWS KMS keys，包括您自行管理的 KMS 密钥以及由 AWS 托管的 KMS 密钥。

主题

- 在控制台中查看 KMS 密钥
- 使用 API 查看 KMS 密钥
- 查看 KMS 密钥的加密配置
- 查找密钥 ID 和密钥 ARN
- 查找别名和别名 ARN

在控制台中查看 KMS 密钥

在 AWS Management Console中，可以查看该账户和区域中的 KMS 密钥列表以及每个 KMS 密钥的详细信息。

> **Note**
>
> AWS KMS 控制台会显示您在自己的账户和区域中拥有查看权限的 KMS 密钥。其他 AWS 账户中的 KMS 密钥不会在控制台中显示，即使您拥有查看、管理和使用权限。要查看其他账户中的 KMS 密钥，请使用DescribeKey操作。

主题

- 导航到密钥表
- 导航到密钥详细信息
- 对您的 KMS 密钥进行排序和筛选
- 显示 KMS 密钥详细信息
- 自定义您的 KMS 密钥表

导航到密钥表

表中显示了每个账户和区域中的 AWS KMS keys。您创建的 KMS 密钥和 AWS 服务为您创建的 KMS 密钥，分别列在不同表中。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。要查看您账户中 AWS 为您所创建和管理的密钥，请在导航窗格中选择 AWS managed keys（Amazon 托管式密钥）。有关不同类型的 KMS 密钥的信息，请参阅 AWS KMS keys。

> **Tip**
>
> 要查看缺少别名的 AWS 托管式密钥，请使用 Customer managed keys（客户托管密钥）页面。
>
> AWS KMS 控制台还显示了帐户和区域中的自定义密钥存储。您在自定义密钥存储中创建的 KMS 密钥显示在 Customer managed keys（客户托管密钥）页面上。有关自定义密钥存储的信息，请参阅自定义密钥存储。

导航到密钥详细信息

账户和区域中的每个 AWS KMS key 都有一个详细信息页面。详细信息页面显示 KMS 密钥的常规配置部分，并包含允许授权用户查看和管理密钥的加密配置和密钥策略的选项卡。根据密钥类型，详细信息页面还可能包括 Aliases（别名）、Key material（密钥材料）、Key rotation（密钥轮换）、Public key（公有密钥）、Regionality（区域性）和 Tags（标签）选项卡。

要导航至 KMS 密钥的密钥详细信息页。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。要查看您账户中 AWS 为您所创建和管理的密钥，请在导航窗格中选择 AWS managed keys（Amazon 托管式密钥）。有关不同类型的 KMS 密钥的信息，请参阅 AWS KMS key。
4. 要打开密钥详细信息页面，请在密钥表中，选择 KMS 密钥的密钥 ID 或别名。

如果 KMS 密钥有多个别名，别名摘要（再加 n 个）将在其中一个别名的旁边显示。选择别名摘要将直接进入密钥详细信息页面上的 Aliases（别名）选项卡中。

对您的 KMS 密钥进行排序和筛选

为了更轻松地在控制台中查找 KMS 密钥，可以对密钥表进行排序和筛选。

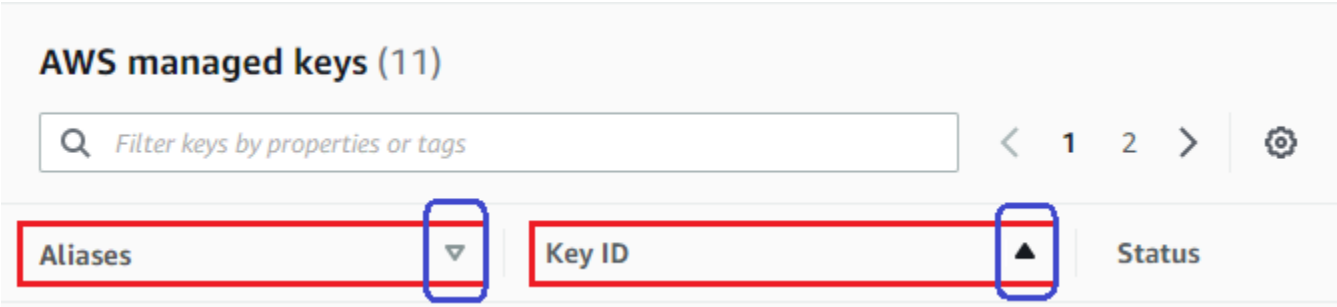
排序

您可以按照升序或降序，对 KMS 密钥的列值进行排序。此功能会对表中的所有 KMS 密钥进行排序，即使 KMS 密钥未显示在当前表页上。

可排序的列由列名称旁边的箭头指示。在 AWS 托管式密钥 页面上，您可以按 Aliases（别名）或 Key ID（密钥 ID）排序。在 Customer managed keys（客户托管密钥）页面上，可以按 Aliases（别名）、Key ID（密钥 ID）或 Key type（密钥类型）进行排序。

要按升序排列，请选择列标题，直至箭头向上。要按降序排列，请选择列标题，直至箭头向下。一次只能按一列排序。

例如，可以按照密钥 ID 的升序对 KMS 密钥进行排序（而不是默认设置的别名）。



当您在 Customer managed keys（客户托管密钥）页面上按 Key type（密钥类型）以升序对 KMS 密钥进行排序时，所有非对称密钥都显示在所有对称密钥之前。

筛选条件

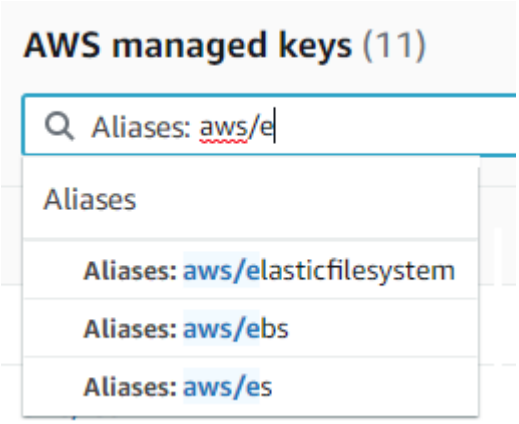
您可以按照 KMS 密钥的属性值或标签筛选 KMS 密钥。筛选条件将应用于表中的所有的 KMS 密钥，即使 KMS 密钥未显示在当前表页上。筛选不区分大小写。

筛选框中列出了可筛选的属性。在 AWS 托管式密钥 页面上，可以按别名和密钥 ID 进行筛选。在 Customer managed keys（客户托管密钥）页面上，可以按别名、密钥 ID、密钥类型属性和标签进行筛选。

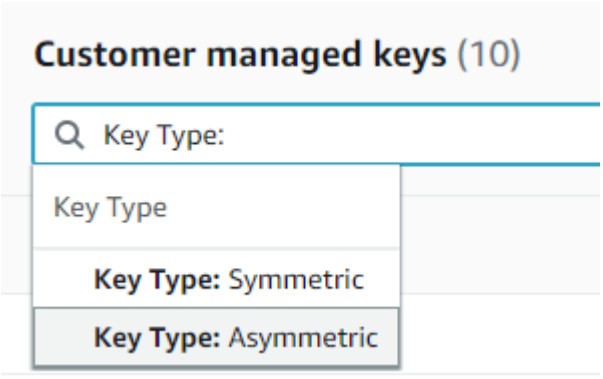
- 在 AWS 托管式密钥 页面上，可以按别名和密钥 ID 进行筛选。
- 在 Customer managed keys（客户托管密钥）页面上，可以按标签、别名、密钥 ID、密钥类型和区域性属性进行筛选。

要按属性值进行筛选，请选择筛选条件、属性名称，然后从实际属性值的列表中进行选择。要按标签进行筛选，请选择标签键，然后从实际标签值列表中进行选择。选择属性或标签键后，还可以键入全部或部分属性值或标签值。在做出选择之前，将看到结果的预览。

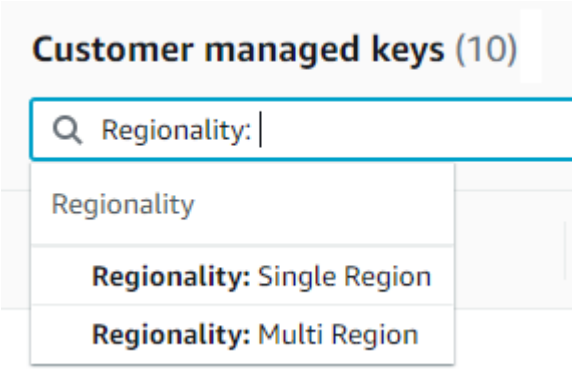
例如，要显示别名名称中包含 `aws/e` 的 KMS 密钥，请选择筛选框，选择 Alias（别名），键入 `aws/e`，然后按 `Enter` 或 `Return` 添加筛选条件。



要在 Customer managed keys（客户托管密钥）页面上仅显示非对称 KMS 密钥，请单击筛选条件框，选择 Key type（密钥类型），然后选择 Key type: Asymmetric（密钥类型：非对称）。仅当您在表中具有非对称 KMS 密钥时，才会显示 Asymmetric（非对称）选项。有关识别非对称 KMS 密钥的更多信息，请参阅 识别非对称 KMS 密钥。



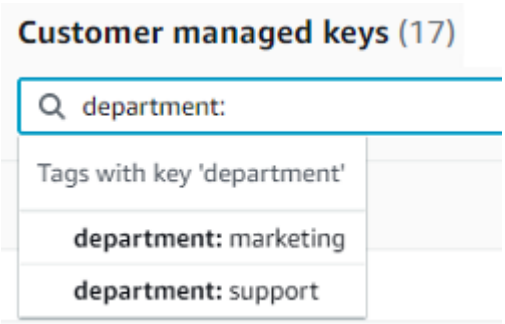
要仅显示多区域密钥，请在 Customer managed keys（客户托管密钥）页面上，选择筛选框，选择 Regionality（区域性），然后选择 Regionality: Multi-Region（区域性：多区域）。Multi-Region（多区域）选项仅当您在表中具有多区域密钥时才会显示。有关识别多区域密钥的更多信息，请参阅 查看多区域密钥。



标签筛选有点不同。要仅显示具有特定标签的 KMS 密钥，请选择筛选框，选择标签键，然后从实际标签值中进行选择。还可以键入全部或部分标签值。

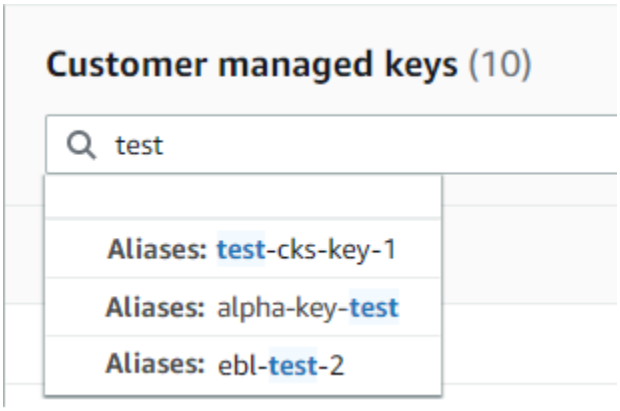
生成的表格将显示带有所选标签的所有 KMS 密钥。但是，它不显示标签。要查看标签，请选择 KMS 密钥的密钥 ID 或别名，然后在其详细信息页面上选择 Tags（标签）选项卡。别名显示在 General configuration（常规配置）部分下。

此筛选条件同时需要标签键和标签值。它不会通过仅键入标签键或仅键入标签值来找到 KMS 密钥。要按全部或部分标签键或值筛选标签，请使用ListResourceTags操作获取带标签的 KMS 密钥，然后使用您的编程语言的筛选功能。有关示例，请参阅ListResourceTags: 获取 KMS 密钥上的标签。

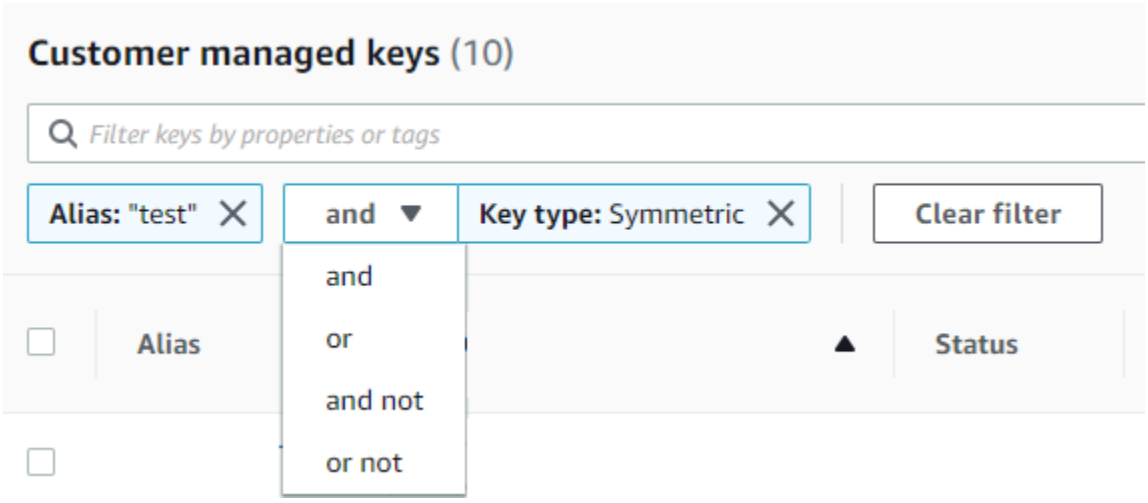


要搜索文本，请在筛选框中键入全部或部分别名、密钥 ID、密钥类型或标签键。（选择标签键后，您可以搜索标签值）。在做出选择之前，将看到结果的预览。

例如，要显示其标签键或可筛选属性中有 `test` 的 KMS 密钥，请在筛选框中键入 `test`。预览会显示筛选条件将选择的 KMS 密钥。在这种情况下，`test` 仅显示在别名属性中。



您可以同时使用多个筛选条件。添加其他筛选条件时，还可以选择逻辑运算符。

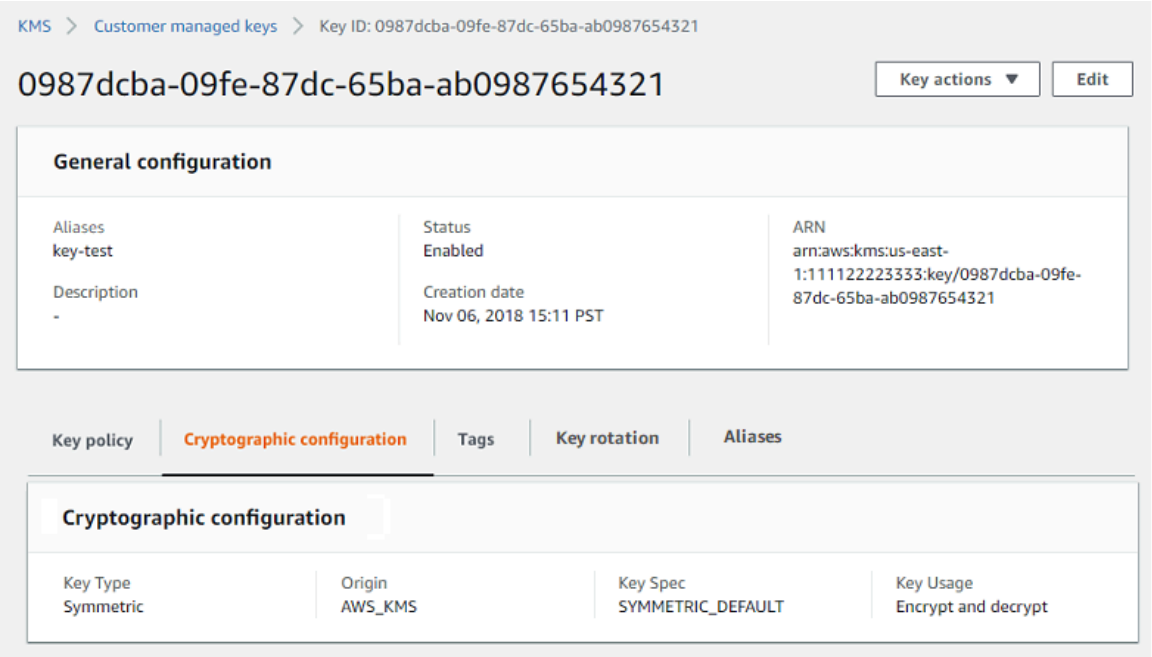


显示 KMS 密钥详细信息

每个 KMS 密钥的详细信息页面均显示 KMS 密钥的属性。该页面会因 KMS 密钥类型而略有不同。

要显示有关 KMS 密钥的详细信息，请在 AWS 托管式密钥 或 Customer managed keys（客户托管密钥）页面上，选择 KMS 密钥的别名或密钥 ID。

KMS 密钥的详细信息页面中包括 General Configuration（常规配置）部分，其中显示 KMS 密钥的基本属性。它还包括可以查看和编辑 KMS 密钥属性的选项卡，例如密钥策略、加密配置、标签、密钥材料（对于带有导入密钥材料的 KMS 密钥）、密钥轮换（对于对称加密 KMS 密钥）、区域性（对于多区域密钥）及公有密钥（对于非对称 KMS 密钥）。



以下列表描述了详细显示部分中的字段，包括选项卡中的字段。其中某些字段也在表格显示部分中以列的形式出现。

别名

位置：Aliases（别名）选项卡

KMS 密钥的友好名称。您可以使用别名标识控制台和一些 AWS KMS API 中的 KMS 密钥。有关更多信息，请参阅 使用别名。

Aliases（别名）选项卡显示与 AWS 账户 和区域中的 KMS 密钥关联的所有别名。

ARN

位置：General configuration（常规配置）部分

KMS 密钥的 Amazon Resource Name (ARN)。此值唯一标识 KMS 密钥。您可以使用此值识别 AWS KMS API 操作中的 KMS 密钥。

连接状态

表示自定义密钥存储是否已连接到其备用密钥存储。仅当在自定义密钥存储中创建 KMS 密钥时，此字段才会显示。

有关此字段值的信息，请参阅 AWS KMSAPI 参考ConnectionState中的。

创建日期

位置：General configuration（常规配置）部分

KMS 密钥的创建日期和时间。此值显示为设备的本地时间。时区不依赖于区域。

与 Expiration（到期）不同，创建仅指的是 KMS 密钥，而非其密钥材料。

CloudHSM 集群 ID

位置：Cryptographic configuration（加密配置）选项卡

包含 KMS 密钥的密钥材料的 AWS CloudHSM 集群的集群 ID。仅当在自定义密钥存储中创建 KMS 密钥时，此字段才会显示。

如果选择 CloudHSM 群集 ID，它会打开 AWS CloudHSM 控制台中的 Clusters（集群）页面。

自定义密钥存储 ID

位置：Cryptographic configuration（加密配置）选项卡

包含 KMS 密钥的自定义密钥存储的 ID。仅当在自定义密钥存储中创建 KMS 密钥时，此字段才会显示。

如果选择自定义密钥存储 ID，则会在 AWS KMS 控制台中打开 Custom key stores（自定义密钥存储）页面。

自定义密钥存储名称

位置：Cryptographic configuration（加密配置）选项卡

包含 KMS 密钥的自定义密钥存储的名称。仅当在自定义密钥存储中创建 KMS 密钥时，此字段才会显示。

自定义密钥存储类型

位置：Cryptographic configuration（加密配置）选项卡

指示自定义密钥存储是 AWS CloudHSM 密钥存储，还是外部密钥存储。仅当在自定义密钥存储中创建 KMS 密钥时，此字段才会显示。

描述

位置：General configuration（常规配置）部分

您可以编写和编辑的 KMS 密钥的简要、可选描述。要添加或更新客户托管密钥的描述，请选择 General Configuration（常规配置）上方的 Edit（编辑）。

加密算法

位置：Cryptographic configuration（加密配置）选项卡

列出可在 AWS KMS 中与 KMS 密钥一起使用的加密算法。仅当 Key type (密钥类型) 为 Asymmetric (对称) 且 Key usage (密钥用法) 为 Encrypt and decrypt (加密和解密) 时，此字段才会显示。有关 AWS KMS 支持的加密算法的信息，请参阅 SYMMETRIC_DEFAULT 密钥规范和 用于加密和解密的 RSA 密钥规范。

到期日期

位置：Key material（密钥材料）选项卡

KMS 密钥的密钥材料到期的日期和时间。此字段仅针对具有导入的密钥材料的 KMS 密钥显示，也就是说，仅当 Origin（源）为 External（外部）且 KMS 密钥的密钥材料已到期时，此字段才会显示。

外部密钥 ID

位置：Cryptographic configuration（加密配置）选项卡

与外部密钥存储中的 KMS 密钥关联的外部密钥的 ID。此字段仅适用于外部密钥存储中的 KMS 密钥。

外部密钥状态

位置：Cryptographic configuration（加密配置）选项卡

外部密钥存储代理报告的与 KMS 密钥关联的外部密钥的最新状态。此字段仅适用于外部密钥存储中的 KMS 密钥。

外部密钥用途

位置：Cryptographic configuration（加密配置）选项卡

在与 KMS 密钥关联的外部密钥上启用的加密操作。此字段仅适用于外部密钥存储中的 KMS 密钥。

密钥策略

位置：Key policy（密钥策略）选项卡

控制对 KMS 密钥以及 IAM policy 和授权的访问。每个 KMS 密钥都有一个密钥策略。它是唯一的强制性授权元素。要更改客户托管密钥的密钥策略，请在 Key policy（密钥策略）选项卡上选择 Edit（编辑）。有关更多信息，请参阅 the section called “密钥政策”。

密钥轮换

位置：Key rotation（密钥轮换）选项卡

启用和禁用客户托管 KMS 密钥中的密钥材料自动轮换。要更改客户托管式密钥的密钥轮换状态，请使用 Key rotation（密钥轮换）选项卡上的复选框。

您无法启用或禁用 AWS 托管式密钥 中的密钥材料轮换。AWS 托管式密钥 每年自动轮换一次。

密钥规范

位置：Cryptographic configuration（加密配置）选项卡

KMS 密钥中密钥材料的类型。AWS KMS 支持对称加密 KMS 密钥（SYMMETRIC_DEFAULT）、不同长度的 HMAC KMS 密钥以及具有不同长度 RSA 密钥的 KMS 密钥和具有不同曲线的椭圆曲线密钥。有关更多信息，请参阅 密钥规范。

密钥类型

位置：Cryptographic configuration（加密配置）选项卡

指示 KMS 密钥是 Symmetric（对称）还是 Asymmetric（非对称）的。

密钥用法

位置：Cryptographic configuration（加密配置）选项卡

指示 KMS 密钥可用于Encrypt and decrypt（加密和解密）、Sign and verify（签名和验证）或Generate and verify MAC（生成并验证 MAC）。有关更多信息，请参阅 密钥用法。

Origin

位置：Cryptographic configuration（加密配置）选项卡

KMS 密钥的密钥材料的来源。有效值为：

- AWS KMS，针对 AWS KMS 生成的密钥材料
- AWS CloudHSM，针对 AWS CloudHSM 密钥存储中的 KMS 密钥
- External（外部），针对导入的密钥材料（BYOK）
- External key store（外部密钥存储），针对外部密钥存储中的 KMS 密钥

MAC 算法

位置：Cryptographic configuration（加密配置）选项卡

列出可在 AWS KMS 中与 HMAC KMS 密钥一起使用的 MAC 算法。仅当密钥规范是 HMAC 密钥规范（HMAC_*）时，此字段才会显示。有关 AWS KMS 支持的 MAC 算法的信息，请参阅 HMAC KMS 密钥的密钥规范。

主键

位置：Regionality（区域性）选项卡

表示此 KMS 密钥是多区域主键。授权用户可以使用此部分将主键更改为另一个相关的多区域密钥。仅当 KMS 密钥是多区域主键时，此字段才会显示。

公有密钥

位置：Public key（公有密钥）选项卡

显示非对称 KMS 密钥的公有密钥。经授权的用户可以使用此选项卡复制和下载公有密钥。

区域性

位置：General configuration（常规配置）部分和 Regionality（区域性）选项卡

指示 KMS 密钥是单区域密钥、多区域主键，还是多区域副本密钥。仅当 KMS 密钥是多区域密钥时，此字段才会显示。

相关的多区域密钥

位置：Regionality（区域性）选项卡

显示所有相关多区域主键和副本键，但当前 KMS 密钥除外。仅当 KMS 密钥是多区域密钥时，此字段才会显示。

在主键的相关的多区域密钥部分，授权用户可以创建新的副本密钥。

副本密钥

位置：Regionality（区域性）选项卡

表示此 KMS 密钥是多区域副本密钥。仅当 KMS 密钥是多区域副本密钥时，此字段才会显示。

签名算法

位置：Cryptographic configuration（加密配置）选项卡

列出可在 AWS KMS 中与 KMS 密钥一起使用的签名算法。仅当 Key type (密钥类型) 为 Asymmetric (对称) 且 Key usage (密钥用法) 为 Sign and verify (签名和验证) 时，此字段才会显示。有关 AWS KMS 支持的签名算法的信息，请参阅用于签名和验证的 RSA 密钥规范和椭圆曲线密钥规范。

Status

位置：General configuration（常规配置）部分

KMS 密钥的密钥状态。您可以在加密操作中使用 KMS 密钥，前提是仅当状态为 Enabled（已启用）时。有关每个 KMS 密钥状态的详细说明及其对可以在 KMS 密钥上运行的操作的影响，请参阅密 AWS KMS 钥的关键状态。

标签

位置：Tags（标签）选项卡

描述 KMS 密钥的可选键值对。要添加或更改 KMS 密钥的标签，请在 Tags（标签）选项卡上选择 Edit（编辑）。

在将标签添加到 AWS 资源时，AWS 可生成成本分配报告，其中按标签汇总了使用情况和成本。标签还可以用来控制对 KMS 密钥的访问。有关轮换 KMS 密钥的信息，请参阅 标记密钥 和 AWS KMS 中的 ABAC。

自定义您的 KMS 密钥表

您可以自定义在 AWS Management Console 中显示在 AWS 托管式密钥 和 Customer managed keys（客户托管密钥）页面中的表来满足您的需求。您可以在每个页面上选择表列、AWS KMS keys 的数量（Page size（页面大小））以及文本换行。所选择的配置将在确认后保存，并在打开页面时重新应用。

要自定义您的 KMS 密钥表

1. 在 AWS 托管式密钥 或 Customer managed keys（客户托管密钥）页面上，选择页面右上角的设置图标

   （  ）。
2. 在 Preferences (首选项) 页面上，选择您的首选设置，然后选择 Confirm (确认)。

请考虑使用 Page size（页面大小）设置来增加每个页面上显示的 KMS 密钥数量，尤其当您通常使用易于滚动的设备时。

显示的数据列可能因表、作业角色以及账户和区域中的 KMS 密钥类型而异。下表提供了一些建议的配置。有关列的描述，请参阅显示 KMS 密钥详细信息。

建议的 KMS 密钥表配置

您可以自定义 KMS 密钥表中显示的列，以便显示所需的 KMS 密钥相关信息。

AWS 托管式密钥

默认情况下，AWS 托管式密钥 表显示 Aliases（别名）、Key ID（密钥 ID）和 Status（状态）列。这些列适合于大多数使用案例。

对称加密 KMS 密钥

如果只使用具有 AWS KMS 生成的密钥材料的对称加密 KMS 密钥，那么 Aliases（别名）、Key ID（密钥 ID）、Status（状态）和 Creation date（创建日期）列可能是最有用的。

非对称 KMS 密钥

如果使用非对称 KMS 密钥，那么除 Aliases（别名）、Key ID（密钥 ID）和 Status（状态）列之外，可考虑添加 Key type（密钥类型）、Key spec（密钥规范）和 Key usage（密钥用法）列。这些列将显示 KMS 密钥是对称还是非对称的、密钥材料的类型，以及 KMS 密钥是用于加密还是签名。

HMAC KMS 密钥

如果使用 HMAC KMS 密钥，那么除 Aliases（别名）、Key ID（密钥 ID）和 Status（状态）列之外，可考虑添加 Key spec（密钥规范）和 Key usage（密钥用法）列。这些列将显示 KMS 密钥是否是 HMAC 密钥。由于无法按密钥规范或密钥用法对 KMS 密钥进行排序，请使用别名和标签来识别 HMAC 密钥，然后使用 AWS KMS 控制台的筛选条件功能按别名或标签进行筛选。

导入的密钥材料

如果您的 KMS 密钥具有导入的密钥材料，请考虑添加 Origin（来源）和 Expiration date（到期日期）列。这些列将显示 KMS 密钥中的密钥材料是导入的还是 AWS KMS 生成的，以及密钥材料何时到期（如果有）。Creation date（创建日期）字段显示了 KMS 密钥的创建日期（不包含密钥材料）。该字段不体现密钥材料的任何特征。

自定义密钥存储中的密钥

如果您拥有自定义密钥存储中的 KMS 密钥，请考虑添加 Origin（来源）和 Custom key store ID（自定义密钥存储 ID）列。这些列表明 KMS 密钥位于自定义密钥存储中，显示自定义密钥存储类型，并标识自定义密钥存储。

多区域密钥

如果您有多区域密钥，请考虑添加 Regionality（区域性）列。这显示 KMS 密钥是单区域密钥、多区域主键，还是多区域副本密钥。

使用 API 查看 KMS 密钥

您可以使用 AWS Key Management Service (AWS KMS) API 查看 KMS 密钥。本部分演示几种返回现有 KMS 密钥详细信息的操作。此示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

主题

ListKeys: 获取所有 KMS 密钥的 ID 和 ARN

该ListKeys操作会返回账户和区域中所有 KMS 密钥的 ID 和 Amazon 资源名称 (ARN)。

例如，这个对 `ListKeys` 操作的调用会返回该虚构账户中每个 KMS 密钥的 ID 和 ARN。有关使用多种编程语言的示例，请参阅获取 KMS 密钥的密钥 ID 和密钥 ARN。

```
$ 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: 获取有关 KMS 密钥的详细信息

该DescribeKey操作返回有关指定 KMS 密钥的详细信息。要标识 KMS 密钥，请使用密钥 ID、密钥 ARN、别名名称或别名 ARN。

与仅显示调用者账户和区域中的 KMS 密钥的ListKeys操作不同，授权用户可以使用该DescribeKey操作来获取有关其他账户中 KMS 密钥的详细信息。

> **Note**
>
> DescribeKey 响应包括具有相同值的两个 KeySpec 和 CustomerMasterKeySpec 成员。CustomerMasterKeySpec 成员已弃用。

例如，这个对 DescribeKey 的调用会返回有关对称加密 KMS 密钥的信息。响应中的字段因 AWS KMS key 规范、密钥状态和密钥材料来源而异。有关使用多种编程语言的示例，请参阅查看 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"
        ]
```

```
    }
}
```

此示例对用于签名和验证的非对称 KMS 密钥调用 DescribeKey 操作。响应包括 AWS KMS 支持用于此 KMS 密钥的签名算法。

```
$ 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: 获取附加到 KMS 密钥的密钥策略

该GetKeyPolicy操作将获取附加到 KMS 密钥的密钥策略。要标识 KMS 密钥，请使用其密钥 ID 或密钥 ARN。您还必须指定策略名称，而策略名称始终是 default。（如果您的输出难以阅读，可在命令中添加 --output text 选项。）GetKeyPolicy 仅适用于调用方账户和区域中的 KMS 密钥。

有关使用多种编程语言的示例，请参阅获取密钥策略。

```
$ 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: 获取 KMS 密钥的别名和 ARN

该ListAliases操作返回账户和区域中的别名。响应中的 TargetKeyId 会显示别名所引用的 KMS 密钥的密钥 ID（如果有）。

默认情况下，ListAliases 命令会返回账户和区域中的所有别名。这包括您创建的别名（此别名与您的客户托管式密钥关联），以及 AWS 创建并与您账户中的 AWS 托管式密钥 关联的别名。您可以识别 AWS 别名，因为其名称的格式为 aws/*<service-name>*（例如 aws/dynamodb）。

响应可能还包含没有 TargetKeyId 字段的别名，如本示例中的 aws/redshift 别名。这些是 AWS 已创建但尚未与 KMS 密钥关联的预定义别名。

有关使用多种编程语言的示例，请参阅列出别名。

```
$ 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"
        },
    ]
}
```


要获取引用特定 KMS 密钥的别名，请使用 `KeyId` 参数。参数值可以是密钥 ID 或密钥 ARN。您不能指定别名名称或别名 ARN。

以下示例中的命令可获取引用客户托管密钥的别名。但也可以使用类似命令来查找引用 AWS 托管式密钥 的别名。

```
$ 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
        },
    ]
}
```

要仅获取 AWS 托管式密钥 的别名，请使用编程语言的功能筛选响应。

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

ListResourceTags: 获取 KMS 密钥上的标签

该ListResourceTags操作返回指定 KMS 密钥上的标签。API 返回一个 KMS 密钥的标签，但您可以循环运行命令，以获取账户和区域中所有 KMS 密钥的标签，或者获取您选择的一组 KMS 密钥的标签。此 API 一次返回一个页面，因此如果您在很多 KMS 密钥上有很多标签，则可能需要使用编程语言中的分页器来获取所需的所有标签。

`ListResourceTags` 操作会返回所有 KMS 密钥的标签，但 AWS 托管式密钥无标签。它仅适用于调用方账户和区域中的 KMS 密钥。

要查找 KMS 密钥的标签，请使用 `ListResourceTags` 操作。`KeyId` 参数是必需的。它接受密钥 ID 或者密钥 ARN。在运行此示例之前，请将示例密钥 ARN 替换为有效的 ARN。

```
$  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
}
```

您可能想要使用 ListResourceTags 操作来获取具有特定标签、标签键或标签值的账户和区域中的所有 KMS 密钥。要做到这一点，请使用您的编程语言的筛选功能。

例如，以下 Bash 脚本使用ListKeys和ListResourceTags操作使用Project标签密钥获取账户和区域中的所有 KMS 密钥。这两个操作都只获取结果的第一页。如果您有很多 KMS 密钥或很多标签，请使用语言的分页功能来获取每个操作的完整结果。在运行此示例之前，请将示例密钥 ID 替换为有效的 ID。

```
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
```

输出的格式如下面的示例输出所示。

```
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"
    }
]
```

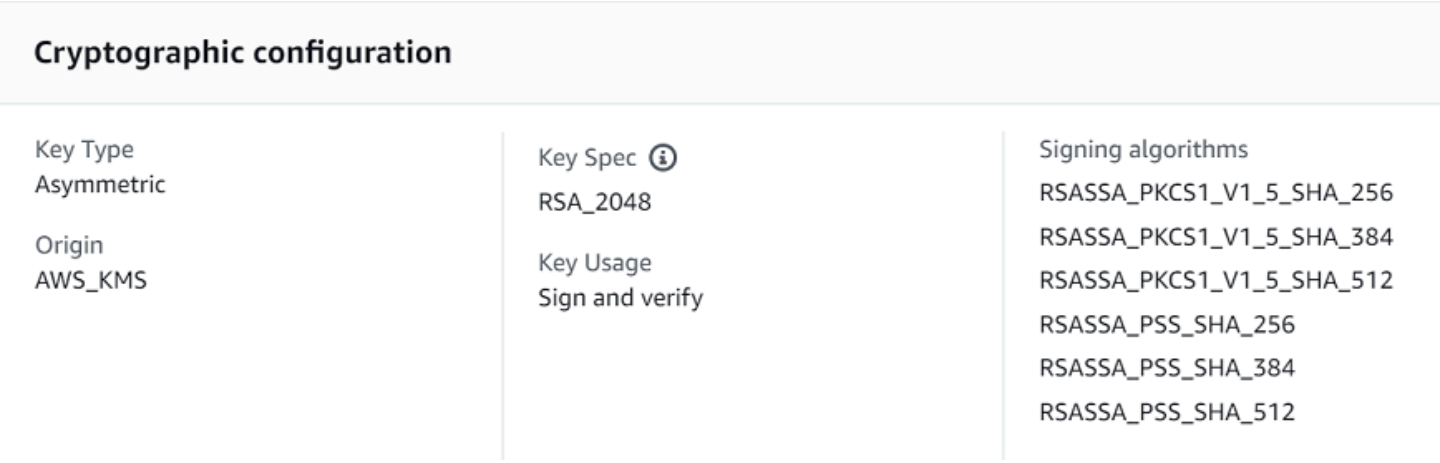
查看 KMS 密钥的加密配置

创建 KMS 密钥后，可以查看其加密配置。KMS 密钥配置在创建后无法更改。如果想采用不同配置，可删除 KMS 密钥并重新创建。

您可以在 AWS KMS 控制台中或通过使用 AWS KMS API，查找 KMS 密钥的加密配置，包括密钥规范、密钥用法以及支持的加密算法或签名算法。有关更多信息，请参阅 识别非对称 KMS 密钥。

在 AWS KMS 控制台中，每个 KMS 密钥的详细信息页面都包括 Cryptographic configuration（加密配置）选项卡，其中显示了有关 KMS 密钥的详细加密信息。例如，下图显示了用于签名和验证的 RSA KMS 密钥的 Cryptographic configuration（加密配置）选项卡。

某些特殊用途 KMS 密钥的 Cryptographic configuration（加密配置）选项卡还有其他专用部分。例如，自定义密钥存储中的 KMS 密钥的 Cryptographic configuration（加密配置）选项卡具有 Custom key stores（自定义密钥存储）部分。外部密钥存储中的 KMS 密钥的 Cryptographic configuration（加密配置）选项卡具有 External key（外部密钥）部分。



在 AWS KMS API 中，使用DescribeKey操作。响应中的 KeyMetadata 结构包括 KMS 密钥的加密配置。例如，对于用于签名和验证的 RSA KMS 密钥，DescribeKey 返回以下响应。

```
{
  "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"
    ]
  }
}
```

查找密钥 ID 和密钥 ARN

要识别 AWS KMS key，您可以使用密钥 ID 或 Amazon Resource Name（密钥 ARN）。在加密操作中，您也可以使用别名名称或别名 ARN。

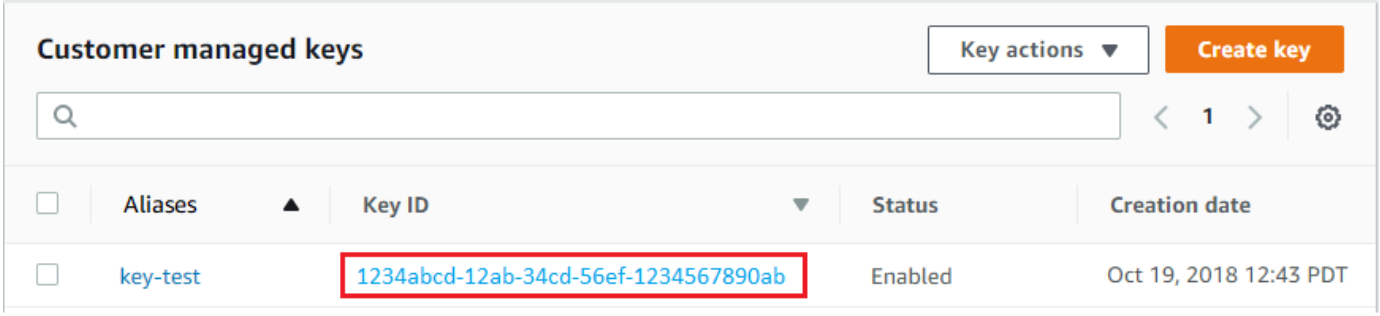
有关 AWS KMS 支持的 KMS 密钥标识符的详细信息，请参阅 密钥标识符 (KeyId)。要获取查找别名和别名 ARN 的帮助，请参阅 查找别名和别名 ARN。

要查找密钥 ID 和 ARN（控制台）

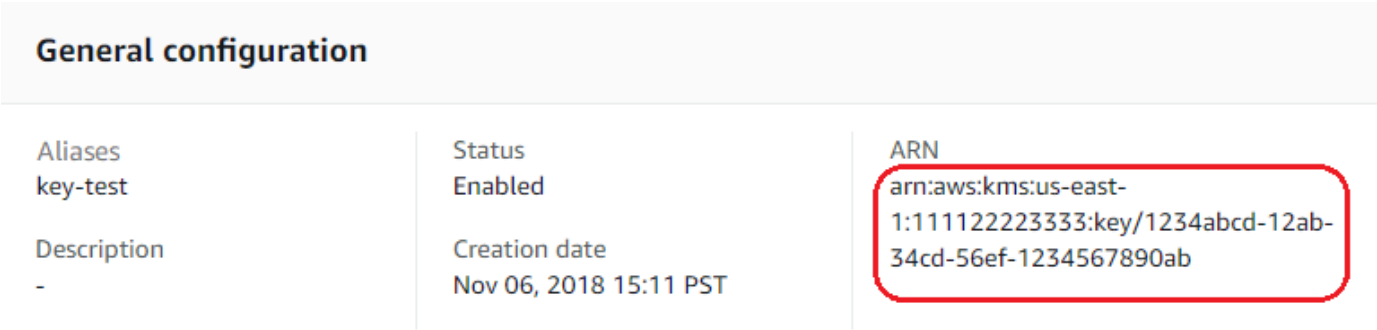
1. 从 https://console.aws.amazon.com/kms 打开 AWS KMS 控制台。

2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。要查看您账户中 AWS 为您所创建和管理的密钥，请在导航窗格中选择 AWS managed keys（Amazon 托管式密钥）。
4. 要查找 KMS 密钥的密钥 ID，请查看以 KMS 密钥别名开头的行。

   默认情况下，Key ID (密钥 ID) 列显示在表中。如果表中未显示“Key ID (密钥 ID)”列，可使用the section called “自定义您的 KMS 密钥表”中介绍的过程恢复该列。您还可以在 KMS 密钥的详细信息页面上查看其密钥 ID。



5. 要查找 KMS 密钥的 Amazon Resource Name (ARN)，请选择密钥 ID 或别名。密钥 ARN 显示在 General Configuration (常规配置) 部分中。



查找密钥 ID 和密钥 ARN (AWS KMS API)

要查找的密钥 ID 和密钥 ARNAWS KMS key，请使用操作。ListKeys有关使用多种编程语言的示例，请参阅获取密钥 ID 和 ARN和获取密钥 ID 和 ARN。

`ListKeys` 响应包括账户和区域中每个 KMS 密钥的密钥 ID 和密钥 ARN。

```
$ 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"
        }
    ]
}
```

查找别名和别名 ARN

别名是 AWS KMS AWS KMS keys（KMS 密钥）的友好名称。您可以在 AWS KMS 控制台或 AWS KMS API 中查找别名和别名 ARN。

有关 AWS KMS 支持的 KMS 密钥标识符的详细信息，请参阅 密钥标识符 (KeyId)。要获取查找密钥 ID 和密钥 ARN 的帮助，请参阅 查找密钥 ID 和密钥 ARN。

主题

- 要查找别名和别名 ARN（控制台）
- 要查找别名和别名 ARN (AWS KMS API)

要查找别名和别名 ARN（控制台）

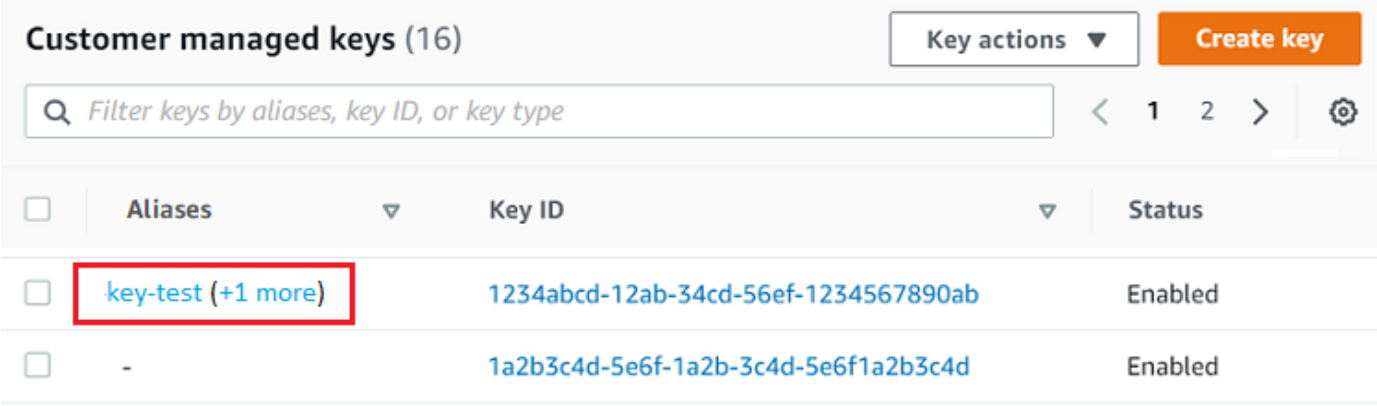
AWS KMS 控制台显示与 KMS 密钥关联的别名。

1. 从 https://console.aws.amazon.com/kms 打开 AWS KMS 控制台。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。要查看您账户中 AWS 为您所创建和管理的密钥，请在导航窗格中选择 AWS managed keys（Amazon 托管式密钥）。
4. Aliases（别名）列显示每个 KMS 密钥的别名。如果 KMS 密钥没有别名，则 Aliases（别名）列中会显示短划线 (-)。

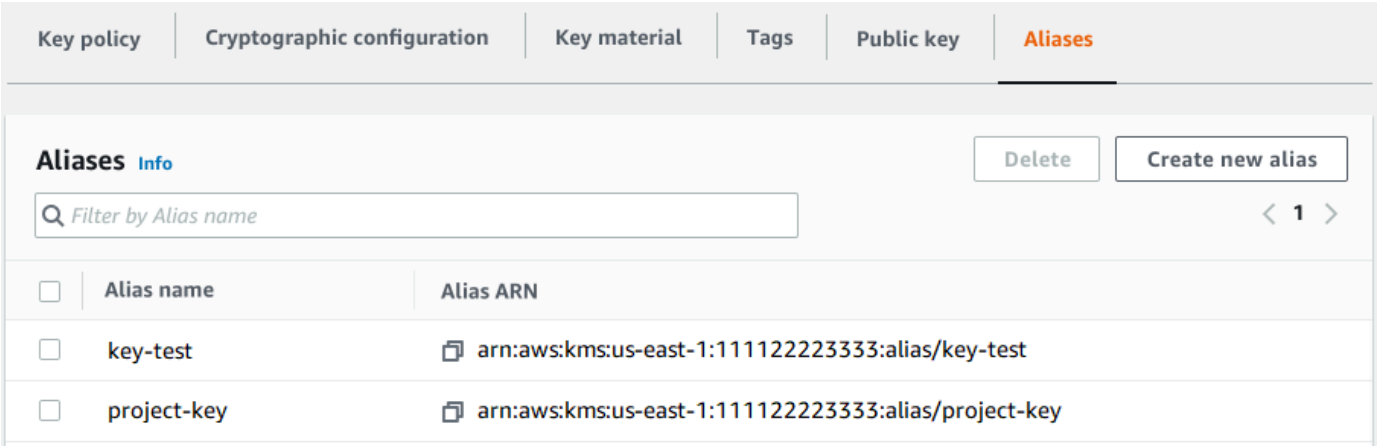
   如果 KMS 密钥具有多个别名，则 Aliases（别名）列还会包含别名摘要，例如（再加 n 个）。例如，以下 KMS 密钥有两个别名，其中一个是 `key-test`。

要查找 KMS 密钥的所有别名的名称和别名 ARN，请使用 Aliases（别名）选项卡。

- 要直接转到 Aliases（别名）选项卡上的 Aliases（别名）列中，选择别名摘要（再加 n 个）。仅当 KMS 密钥具有多个别名时，才会显示别名摘要。
- 或者，选择 KMS 密钥的别名或密钥 ID（这将打开 KMS 密钥的详细信息页面），然后选择 Aliases（别名）选项卡。这些选项卡在 General configuration（常规配置）部分下。



5. Aliases（别名）选项卡显示 KMS 密钥的所有别名的名称和别名 ARN。您还可以在此选项卡上创建和删除 KMS 密钥的别名。



要查找别名和别名 ARN (AWS KMS API)

要查找的别名和别名 ARNAWS KMS key，请使用操作。ListAliases有关使用多种编程语言的示例，请参阅列出别名和获取别名和 ARN。

默认情况下，响应包括账户和区域中每个别名的别名和别名 ARN。要仅获取特定 KMS 密钥的别名，请使用 `KeyId` 参数。

例如，以下命令仅获取带有密钥 ID 1234abcd-12ab-34cd-56ef-1234567890ab 的示例 KMS 密钥的别名。

```
$ 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
        }
    ]
}
```

编辑密钥

您可以在 AWS KMS 控制台中更改客户托管的密钥的以下属性，也可使用 AWS KMS API 进行更改。

您无法编辑 AWS 托管式密钥或 AWS 拥有的密钥的任何属性。这些密钥由创建它们的 AWS 服务管理。

描述

您可以在 KMS 密钥的详细信息页面上或使用UpdateKeyDescription操作来更改客户托管密钥的描述。

要编辑控制台中的密钥描述，请在 KMS 密钥详细信息页面的右上角选择 Edit（编辑）。

密钥策略

您可以在客户托管密钥的详细信息页面的密钥策略选项卡上或使用PutKeyPolicy操作来更改密钥策略。

有关更多信息，请参阅 更改密钥策略。

标签

您可以在 AWS KMS 控制台的在客户托管密钥页面或在客户托管密钥详细信息页面的 Tags（标签）选项卡上创建和删除标签。或者你可以使用TagResource和UntagResource操作。

有关更多信息，请参阅 标记密钥。

启用和禁用

您可以在 AWS KMS 控制台的客户托管密钥页面或在客户托管密钥详细信息页面上启用和禁用 KMS 密钥。或者你可以使用EnableKey和DisableKey操作。

有关更多信息，请参阅 启用和禁用密钥。

自动密钥轮换

您可以在客户托管密钥的详细信息页面的密钥轮换选项卡上启用和禁用自动密钥轮换，也可以使用EnableKeyRotation和DisableKeyRotation操作来启用和禁用自动密钥轮换。

有关更多信息，请参阅 旋转 AWS KMS keys。

另请参阅

更新别名

标记密钥

在 AWS KMS 中，您可以在创建 KMS 密钥和标记或取消标记现有 KMS 密钥时将标签添加到客户托管密钥，除非他们待删除。但不能在其他 AWS 账户 中标记别名、自定义密钥存储、AWS 托管式密钥、AWS 拥有的密钥 或 KMS 密钥。标签是可选的，但它们可能非常有用。

有关更多信息，请参阅 创建密钥 和 编辑密钥。有关标签的一般信息，包括最佳实践、标记策略以及标签的格式和语法，请参阅《Amazon Web Services 一般参考》中的 Tagging AWS resources。

主题

- 关于 AWS KMS 中的标签
- 在控制台中管理 KMS 密钥标签
- 使用 API 操作管理 KMS 密钥标签
- 控制对标签的访问

- 使用标签控制对 KMS 密钥的访问

关于 AWS KMS 中的标签

标签是您可以为 AWS 资源分配（或 AWS 可以分配）的可选元数据标记。每个标签都包含一个标签键和一个标签值，它们都是区分大小写的字符串。标签值可为空 (null) 字符串。资源上的每个标签必须具有不同的标签键，但您可以将相同的标签添加到多个 AWS 资源。每个资源最多可以有 50 个用户创建的标签。

不要在标签键或标签值中包含机密或敏感信息。标签可供许多 AWS 服务 访问，包括计费。

在 AWS KMS 中，您可以在创建 KMS 密钥和标记或取消标记现有 KMS 密钥时将标签添加到客户托管密钥，除非他们待删除。但不能在其他 AWS 账户 中标记别名、自定义密钥存储、AWS 托管式密钥、AWS 拥有的密钥 或 KMS 密钥。标签是可选的，但它们可能非常有用。

例如，您可以添加一个 `"Project"="Alpha"` 标签添加到您用于 Alpha 项目的所有 KMS 密钥和 Amazon S3 存储桶。

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

有关标签的一般信息，包括格式和语法，请参阅《Amazon Web Services 一般参考》中的 Tagging AWS resources。

标签可帮助您：

- 标识和整理您的 AWS 资源。许多 AWS 服务支持标记，因此，您可以将同一标签分配给来不同服务的资源，以指示这些资源是相关的。例如，您可以将相同的标签分配给 KMS 密钥和 Amazon Elastic Block Store (Amazon EBS) 卷或 AWS Secrets Manager 密钥。您还可以使用标签来标识 KMS 密钥以实现自动化。
- 跟踪您的 AWS 成本。在将标签添加到 AWS 资源时，AWS 可生成成本分配报告，其中按标签汇总了使用情况和成本。您可以使用此功能来跟踪项目、应用程序或成本中心的 AWS KMS 成本。

  有关对成本分配使用标签的更多信息，请参阅 AWS Billing 用户指南中的使用成本分配标签。有关适用于标签键和标签值的规则的信息，请参阅 AWS Billing 用户指南中的用户定义的标签限制。
- 控制对 AWS 资源的访问。基于 KMS 密钥的标签允许和拒绝对该密钥的访问是 AWS KMS 对基于属性的访问控制 (ABAC) 的支持的一部分。有关基于 AWS KMS keys 的标签控制对其访问的更多信息，请参阅 使用标签控制对 KMS 密钥的访问。有关使用标签控制对 AWS 资源的访问的更多一般信息，请参阅 IAM 用户指南中的使用资源标签控制对 AWS 资源的访问。

AWS KMS当您使用、或ListResourceTags操作时 TagResource，UntagResource会在AWS CloudTrail日志中写入一个条目。

在控制台中管理 KMS 密钥标签

在 AWS KMS 控制台中创建 KMS 密钥时，您可以将标签添加到 KMS 密钥。您也可以在控制台中使用 Tags（标签）选项卡添加、编辑和删除客户托管密钥上的标签。要添加、编辑、查看和删除 KMS 密钥的标签，您必须具有所需的权限。有关更多信息，请参阅 控制对标签的访问。

创建 KMS 密钥时添加标签

要在控制台中创建 KMS 密钥时添加标签，除了在控制台中创建 KMS 密钥和查看 KMS 密钥所需的权限之外，您还必须具有 IAM policy 中的 `kms:TagResource` 权限。权限至少必须涵盖账户和区域中的所有 KMS 密钥。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。（您无法管理 AWS 托管式密钥 的标签）
4. 选择密钥类型，然后选择 Next（下一步）。
5. 输入别名和可选的描述。
6. 输入一个标签键和可选的标签值。要添加其他标签，请选择 Add tag（添加标签）。要删除标签，请选择 Remove（删除）。完成新 KMS 密钥的标记后，选择 Next（下一步）。
7. 完成 KMS 密钥的创建。

查看和管理现有 KMS 密钥上的标签

要在控制台中添加、查看、编辑和删除标签，您需要具有对 KMS 密钥进行标记的权限。您可以从 KMS 密钥的密钥策略中获取此权限，或者如果密钥策略允许，还可以从包含 KMS 密钥的 IAM policy 获取此权限。除了在控制台中查看 KMS 密钥的权限之外，您还需要这些权限。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。（您无法管理 AWS 托管式密钥 的标签）
4. 您可以使用表筛选条件仅显示带有特定标签的 KMS 密钥。有关更多信息，请参阅 对您的 KMS 密钥进行排序和筛选。

5. 选中 KMS 密钥的别名旁的复选框。
6. 选择 Key actions、Add or edit tags。
7. 在 KMS 密钥的详细信息页面上，选择 Tags（标签）选项卡。

   - 要创建您的第一个标签，请选择 Create tag（创建标签），键入标签键（必需）和标签值（可选），然后选择 Save（保存）。

     如果将标签值留空，则实际标签值为 null 或空字符串。
   - 要添加标签，请选择 Edi（编辑），选择 Add tag（添加标签），键入标签键和标签值，然后选择 Save（保存）。
   - 要更改标签的名称或值，请选择 Edit (编辑)，进行更改，然后选择 Save (保存)。
   - 要删除标签，请选择 Edit (编辑)。在标签行上，选择 Remove (删除)，然后选择 Save (保存)。
8. 要保存您的更改，请选择保存更改。

使用 API 操作管理 KMS 密钥标签

您可以使用 AWS Key Management Service (AWS KMS) API 为您管理的 KMS 密钥添加、删除和列出标签。这些示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。您无法标记 AWS 托管式密钥。

要添加、编辑、查看和删除 KMS 密钥的标签，您必须具有所需的权限。有关更多信息，请参阅 控制对标签的访问。

主题

- CreateKey: 为新的 KMS 密钥添加标签
- TagResource: 为 KMS 密钥添加或更改标签
- ListResourceTags: 获取 KMS 密钥的标签
- UntagResource: 从 KMS 密钥中删除标签

CreateKey: 为新的 KMS 密钥添加标签

您可以在创建客户托管密钥时添加标签。要指定标签，请使用CreateKey操作的Tags参数。

要在创建 KMS 密钥时添加标签，调用方必须具有 IAM policy 中的 `kms:TagResource` 权限。权限至少必须涵盖账户和区域中的所有 KMS 密钥。有关更多信息，请参阅 控制对标签的访问。

CreateKey 的 Tags 参数的值是区分大小写的标签键和标签值对的集合。KMS 密钥上的每个标签都必须具有不同的标签名称。标签值可为 null 或空字符串。

例如，以下 AWS CLI 命令创建带有 Project:Alpha 标签的对称加密 KMS 密钥。指定多个键值对时，请使用空格分隔每个对。

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

当此命令成功时，它会返回一个 KeyMetadata 对象以及有关新 KMS 密钥的信息。但是，KeyMetadata 不包括标签。要获取标签，请使用ListResourceTags操作。

TagResource: 为 KMS 密钥添加或更改标签

该TagResource操作将向 KMS 密钥添加一个或多个标签。此操作不能用于添加或编辑不同 AWS 账户中的标签。

要添加标签，请指定新标签键和标签值。要编辑标签，请指定现有标签键和新标签值。KMS 密钥上的每个标签都必须具有不同的标签键。标签值可为 null 或空字符串。

例如，以下命令将 **Purpose** 和 **Department** 标签添加到示例 KMS 密钥中。

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

此命令成功执行后，不会返回任何输出。要查看 KMS 密钥上的标签，请使用ListResourceTags操作。

您也可以使用 TagResource 来更改现有标签的标签值。要替换标签值，请指定具有不同值的相同标签键。

例如，此命令会将 Purpose 标签的值从 Pretest 更改为 Test。

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

ListResourceTags: 获取 KMS 密钥的标签

该ListResourceTags操作获取 KMS 密钥的标签。KeyId 参数是必需的。此操作不能用于查看其他 AWS 账户 中的 KMS 密钥上的标签。

例如，以下命令获取示例 KMS 密钥的标签。

```
$ 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: 从 KMS 密钥中删除标签

该UntagResource操作会从 KMS 密钥中删除标签。要标识要删除的标签，请指定标签键。此操作不能用于从其他 AWS 账户 中的 KMS 密钥中删除标签。

当它成功时，UntagResource 操作不返回任何输出。此外，如果在 KMS 密钥上未找到指定的标签键，则不会抛出异常或返回响应。要确认操作是否奏效，请使用该ListResourceTags操作。

例如，此命令将从指定的 KMS 密钥中删除 **Purpose** 标签及其值。

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

控制对标签的访问

要在 AWS KMS 控制台中或通过使用 API 来添加、查看和删除标签，委托人需要标记权限。您可以在密钥策略中提供这些权限。您还可以在 IAM policy（包括 VPC 端点策略）中提供这些权限，但仅当密钥策略允许时。AWSKeyManagementServicePowerUser托管策略允许委托人对账户可以访问的所有 KMS 密钥进行标记、取消标记和列出标签。

您还可以通过将 AWS 全局条件键用于标签来限制这些权限。在中AWS KMS，这些条件可以控制对标记操作（例如TagResource和 UntagResource）的访问权限。

> **Note**
>
> 请谨慎授予委托人管理标签和别名的权限。更改标签或别名可以允许或拒绝对客户托管密钥的权限。有关详细信息，请参阅 AWS KMS 中的 ABAC 和 使用标签控制对 KMS 密钥的访问。

有关示例策略和更多信息，请参阅 IAM 用户指南中的根据标签键控制访问。

用于创建和管理标签的权限如下所示。

kms: TagResource

允许委托人添加或编辑标签。要在创建 KMS 密钥时添加标签，委托人必须在 IAM policy 中具有不限于特定 KMS 密钥的权限。

kms: ListResourceTags

允许委托人查看 KMS 密钥上的标签。

kms: UntagResource

允许委托人从 KMS 密钥中删除标签。

标记策略中的权限

您可以在密钥策略或 IAM policy 中提供权限标记。例如，以下示例密钥策略向选定用户授予标记 KMS 密钥的权限。它为所有可以担任示例管理员或开发人员角色的用户授予查看标签的权限。

```
{
  "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": "*"
    }
  ]
}
```

要授予委托人对多个 KMS 密钥的标记权限，您可以使用 IAM policy。为使此策略生效，每个 KMS 密钥的密钥策略都必须允许账户使用 IAM policy 来控制对 KMS 密钥的访问。

例如，以下 IAM policy 允许委托人创建 KMS 密钥。它还允许他们在指定账户中的所有 KMS 密钥上创建和管理标签。[这种组合允许委托人在创建 KMS 密钥时使用CreateKey操作的 Tags 参数向 KMS 密钥添加标签。]

```
{
  "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/*"
    }
  ]
}
```

限制标签权限

您可以通过使用策略条件限制标记权限。以下策略条件可应用于 kms:TagResource 和 kms:UntagResource 权限。例如，您可以使用 aws:RequestTag/*tag-key* 条件来允许委托人仅添加特定标签，或阻止委托人添加具有特定标签键的标签。或者，您可以使用 kms:KeyOrigin 条件来防止委托人标记或取消标记具有导入密钥材料的 KMS 密钥。

- aws：RequestTag
- a@@ ws:ResourceTag/tag-key（仅限 IAM 策略）
- aws：TagKeys
- kms: CallerAccount
- kms: KeySpec
- kms: KeyUsage
- kms: KeyOrigin
- kms: ViaService

作为使用标签控制对 KMS 密钥的访问的最佳实践，请使用 aws:RequestTag/*tag-key* 或 aws:TagKeys 条件键来确定允许哪些标签（或标签键）。

例如，以下 IAM policy 与上一个类似。但是，此策略允许委托人为具有 Project 标签键的标签创建标签 (TagResource) 并删除标签 UntagResource。

由于TagResource和UntagResource请求可以包含多个标签，因此您必须使用 aws: TagKeys 条件指定ForAllValues或ForAnyValue设置运算符。ForAnyValue 运算符要求请求中至少有一个标签键与策略中的其中一个标签键匹配。ForAllValues 运算符要求请求中所有的标签键与策略中的其中

一个标签键匹配。`true`如果请求中没有标签，则`ForAllValues`运算符也会返回，但 TagResource 如果未指定标签，则会 UntagResource失败。有关集合运算符的详细信息，请参阅 IAM 用户指南中的使用多个键和值。

```
{
  "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"}
      }
    }
  ]
}
```

使用标签控制对 KMS 密钥的访问

您可以基于 KMS 密钥上的标签控制对 AWS KMS keys 的访问权限。例如，您可以编写 IAM policy，以允许委托人仅启用和禁用具有特定标签的 KMS 密钥。或者，您可以使用 IAM policy 防止委托人在加密操作中使用 KMS 密钥，除非 KMS 密钥具有特定标签。

此功能是 AWS KMS 对基于属性的访问控制 (ABAC) 的一部分。有关使用标签控制对 AWS 资源的访问的信息，请参阅 IAM 用户指南中的什么是适用于 AWS 的 ABAC？以及使用资源标签控制对 AWS 资

源的访问。要获取有关解决与 ABAC 相关的访问问题的帮助，请参阅 适用于 AWS KMS 的 ABAC 的故障排除。

> **Note**
>
> 标签和别名的更改最多可能需要 5 分钟的时间才能影响 KMS 密钥授权。最近的更改可能会在 API 操作中显示，然后才会影响授权。

AWS KMS支持 aws:ResourceTag/tag-key 全局条件上下文密钥，它允许您根据 KMS 密钥上的标签控制对 KMS 密钥的访问。由于多个 KMS 密钥可以具有相同的标签，此功能可使您将权限应用于一组选定的 KMS 密钥。您还可以通过更改 KMS 密钥的标签轻松更改集合中的 KMS 密钥。

在 AWS KMS 中，`aws:ResourceTag/`*`tag-key`* 条件键仅在 IAM policy 中受支持。密钥策略（仅适用于一个 KMS 密钥）或不使用特定 KMS 密钥的操作（例如ListKeys或ListAliases操作）不支持它。

使用标签控制访问提供了一种简单、可扩展且灵活的方式来管理权限。但是，如果设计和管理不当，它可能会无意中允许或拒绝对您的 KMS 密钥的访问。如果您使用标签来控制访问，请考虑以下做法。

- 使用标签来强化最低权限访问的最佳实践。仅为 IAM 委托人授予他们对必须使用或管理的 KMS 密钥的所需权限。例如，使用标签来标记用于项目的 KMS 密钥。然后授予项目团队仅使用带有项目标签的 KMS 密钥的权限。
- 谨慎为委托人提供 `kms:TagResource` 和 `kms:UntagResource` 权限，以允许他们添加、编辑和删除标签。当您使用标签控制对 KMS 密钥的访问时，更改标签可以授予委托人使用他们没有权限使用的 KMS 密钥的权限。它还可以拒绝对其他委托人执行其工作所需的 KMS 密钥的访问。不具有更改密钥策略或创建授权权限的密钥管理员可以控制对 KMS 密钥的访问，前提是他们有权管理标签。

  如有可能，请使用策略条件，例如 `aws:RequestTag/`*`tag-key`* 或 `aws:TagKeys`，以将委托人的标记权限限制为特定 KMS 密钥上的特定标签或标签模式。
- 查看您的 AWS 账户 中当前具有标记和取消标记权限的委托人，并根据需要对其进行调整。例如，控制台密钥管理员的默认密钥策略包括对该 KMS 密钥的 `kms:TagResource` 和 `kms:UntagResource` 权限。IAM policy 可能允许对所有 KMS 密钥的标记和取消标记权限。例如，AWSKeyManagementServicePowerUser托管策略允许委托人标记、取消标记和列出所有 KMS 密钥上的标签。
- 在设置依赖于标签的策略之前，请查看您的 AWS 账户 中的 KMS 密钥上的标签。请确保您的策略仅适用于您要包含的标签。使用CloudTrail 日志和CloudWatch 警报提醒您注意可能影响您的 KMS 密钥访问权限的标签更改。

- 基于标签的策略条件使用模式匹配；它们不绑定到标签的特定实例。使用基于标签的条件键的策略会影响与模式匹配的所有新标签和现有标签。如果删除并重新创建与策略条件匹配的标签，则该条件将应用于新标签，就像对旧标签一样。

例如，请考虑以下 IAM policy。它允许委托人仅对您账户中位于亚太地区（新加坡）地区GenerateDataKeyWithoutPlaintext且有标签的 KMS 密钥调用和解密操作。`"Project"="Alpha"`您可以将此策略附加到示例 Alpha 项目中的角色。

```
{
  "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"
        }
      }
    }
  ]
}
```

以下示例 IAM policy 允许委托人使用账户中的 KMS 密钥执行特定加密操作。但它禁止主体对具有 `"Type"="Reserved"` 标签或不包含 `"Type"` 标签的 KMS 密钥使用这些加密操作。

```
{
  "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"
        }
      }
    }
  ]
}
```

启用和禁用密钥

您可以禁用和重新启用客户托管密钥。KMS 密钥在创建完成后默认处于启用状态。如果禁用 KMS 密钥，则在您重新启用它之前，它不能用于任何加密操作。

因为它是临时的且容易撤消，因此，禁用 KMS 密钥是删除 KMS 密钥的安全替代方法，此操作具有破坏性且不可撤销。如果您正在考虑删除 KMS 密钥，请先将其禁用，然后设置CloudWatch 警报或类似机制，确保您永远不需要使用该密钥来解密加密数据。

当您禁用 KMS 密钥时，它会立即变为不可用（视最终一致性而定）。不过，在再次使用 KMS 密钥（例如解密数据密钥）之前，使用受 KMS 密钥保护的数据密钥加密的资源不会受到影响。此问题会影响 AWS 服务，因为许多服务使用数据密钥来保护您的资源。有关更多信息，请参阅 不可用的 KMS 密钥如何影响数据密钥。

您无法启用或禁用 AWS 托管式密钥 或 AWS 拥有的密钥。AWS 托管式密钥 处于永久启动状态，以供使用 AWS KMS 的服务使用。AWS 拥有的密钥 仅由拥有它们的服务管理。

> **Note**
>
> AWS KMS 不会轮换已禁用的客户托管密钥的密钥材料。有关更多信息，请参阅 密钥轮换的工作原理。

主题

- 启用和禁用 KMS 密钥（控制台）
- 启用和禁用 KMS 密钥 (AWS KMS API)

启用和禁用 KMS 密钥（控制台）

您可以使用 AWS KMS 控制台以启用和禁用客户托管密钥。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选中要启用或禁用的 KMS 密钥对应的复选框。
5. 要启用 KMS 密钥，请依次选择 Key actions（密钥操作）、 Enable（启用）。要禁用 KMS 密钥，请依次选择 Key actions（密钥操作）、Disable（禁用）。

启用和禁用 KMS 密钥 (AWS KMS API)

该EnableKey操作启用了已禁用AWS KMS key的。这些示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。key-id 参数是必需的。

该操作不返回任何输出。要查看密钥状态，请使用DescribeKey操作。

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

该DisableKey操作会禁用已启用的 KMS 密钥。key-id 参数是必需的。

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

该操作不返回任何输出。要查看密钥状态，请使用DescribeKey操作并查看字Enabled段。

```
$ 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"
        ]
    }
}
```

旋转 AWS KMS keys

要为客户托管的密钥创建新的加密材料，您可以创建新的 KMS 密钥，然后更改您的应用程序或别名来使用新的 KMS 密钥。或者，您可以通过启用自动密钥轮换或按需轮换来轮换与现有 KMS 密钥关联的密钥材料。

默认情况下，当您为 KMS 密钥启用自动密钥轮换时，每年会为 KMS 密钥 AWS KMS 生成新的加密材料。您还可以指定自定义，rotation-period以定义启用自动密钥轮换以轮换密钥材料后的天数，以及此后每次自动轮换之间的天数。 AWS KMS 如果您需要立即启动密钥材料轮换，则无论是否启用了自动密钥轮换，都可以按需轮换。按需轮换不会更改现有的自动轮换计划。

AWS KMS 永久保存所有先前版本的加密材料，因此您可以解密使用该 KMS 密钥加密的任何数据。AWS KMS 在您删除 KMS 密钥之前，不会删除任何轮换的密钥材料。您可以在 Amazon CloudWatch 和 AWS Key Management Service 控制台中跟踪 KMS 密钥的密钥材料的轮换情况。 AWS CloudTrail 您还可以使用GetKeyRotationStatus操作来验证 KMS 密钥是否启用了自动轮换，并识别任何正在进行的按需轮换。您可以使用ListKeyRotations操作来查看已完成旋转的详细信息。

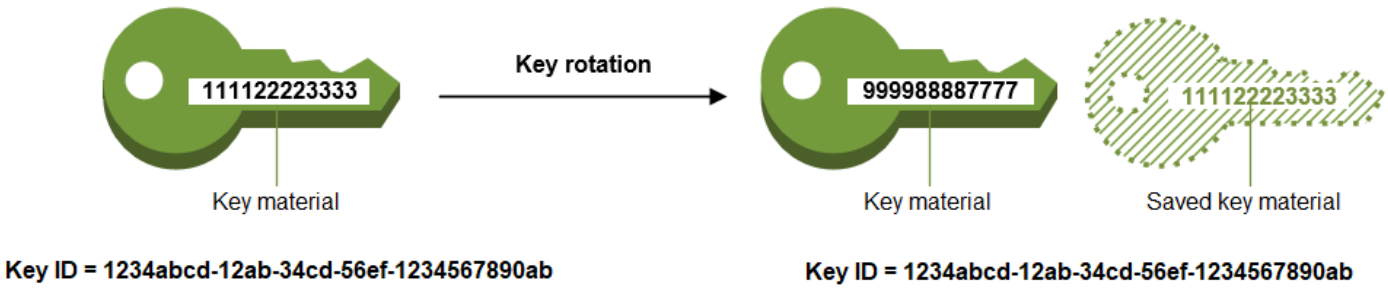
当您使用轮换的 KMS 密钥加密数据时， AWS KMS 使用当前的密钥材料。当您使用轮换的 KMS 密钥解密密文时，将 AWS KMS 使用用于加密密文的密钥材料的版本。您无法为解密操作选择特定版本的密钥材料，而是 AWS KMS 会自动选择正确的版本。由于使用适当的密钥材料进行 AWS KMS 透明解密，因此您可以安全地在应用程序中使用轮换的 KMS 密钥，而 AWS 服务 无需更改代码。

然而，自动密钥轮换对 KMS 密钥所保护的数据无效。它不会轮换 KMS 密钥生成的数据密钥，也不会对任何受 KMS 密钥保护的数据重新加密，并且它无法减轻数据密钥泄露的影响。

AWS KMS 仅支持对称加密 KMS 密钥使用 AWS KMS 创建的密钥材料进行自动和按需密钥轮换。对于客户托管式 KMS 密钥，自动轮换是可选项。 AWS KMS 始终坚持每年轮换一次 AWS 托管式 KMS 密钥的密钥材料。所AWS 拥有的 KMS 密钥的轮换由拥有该密钥的 AWS 服务管理。

> **Note**
>
> 的轮换期限在2022年5月 AWS 托管式密钥 发生了变化。有关更多信息，请参阅 AWS 托管式密钥。

密钥轮换只会更改密钥材料，即加密操作中所使用的加密密钥。不管密钥材料有没有变更或变更了多少次，该 KMS 密钥仍是相同的逻辑资源。KMS 密钥的属性不会发生变化，如下图所示。



您可能决定创建新的 KMS 密钥来替代原有的 KMS 密钥。这跟轮换现有 KMS 密钥的密钥材料具有相同效果，因此这通常被视为手动轮换密钥。如果您想要轮换不符合自动密钥轮换条件的 KMS 密钥，包括非对称 KMS 密钥、HMAC KMS 密钥、自定义密钥存储中的 KMS 密钥以及带有导入密钥材料的 KMS 密钥，则手动轮换是一个不错的选择。

密钥轮换和定价

AWS KMS 对为您的 KMS 密钥维护的密钥材料的第一次和第二次轮换收取月费。此次涨价以第二次轮换为上限，后续的任何轮换均不计费。有关详细信息，请参阅 AWS Key Management Service 定价。

> **Note**
>
> 您可以使用《AWS Cost Explorer Service》https://docs.aws.amazon.com/cost-management/latest/userguide/ce-what-is.html来查看您的密钥存储费用明细。例如，您可以通过将使用类型指定为 `$REGION-KMS-Keys` 并按 API 操作对数据进行分组来筛选视图，以查看按当前和轮换 KMS 密钥计费的密钥的总费用。
> 您可能仍会看到历史日期的旧 `Unknown` API 操作的实例。

密钥轮换和配额

在计算密钥资源配额时，无论轮换密钥材料版本的数量如何，每个 KMS 密钥均算作一个密钥。

有关密钥材料和轮换的详细信息，请参阅《AWS Key Management Service 加密详细信息》。

主题

- 为什么要轮换 KMS 密钥？
- 密钥轮换的工作原理
- 如何启用和禁用自动密钥轮换
- 如何执行按需密钥轮换

- 手动轮换密钥

为什么要轮换 KMS 密钥？

加密最佳实践不鼓励大量重复使用直接加密数据的密钥，例如生成的数据密钥。 AWS KMS 当 256 位数据密钥加密数百万条消息时，它们可能会耗尽并开始生成带有细微模式的加密文字，聪明的操作者可以利用这些密文来发现密钥中的位。为避免密钥耗尽，数据密钥最好仅使用一次或几次，这样可以有效地轮换密钥材料。

但是，KMS 密钥最常用作“包装密钥”，也称为“密钥加密密钥”。包装密钥不是加密数据，而是对加密数据的数据密钥进行加密。因此，其使用频率远低于数据密钥，并且几乎从未被重复使用到足以出现密钥耗尽的风险。

尽管耗尽风险非常低，但由于业务或合同规则或政府法规，您可能需要轮换 KMS 密钥。当您被迫轮换 KMS 密钥时，我们建议您在支持自动密钥轮换的情况下使用自动密钥轮换，在不支持自动密钥轮换时使用手动密钥轮换。

您可以考虑按需轮换，以演示关键材料轮换功能或验证自动化脚本。我们建议对计划外轮换使用按需轮换，并尽可能使用带有自定义轮换周期的自动密钥轮换。

密钥轮换的工作原理

密钥轮换设计 AWS KMS 为透明且易于使用。 AWS KMS 仅支持客户托管密钥的可选自动和按需密钥轮换。

自动轮换密钥

AWS KMS 在轮换周期定义的下一个轮换日期自动轮换 KMS 密钥。您无需记住或计划更新。

按需轮换

无论是否启用了自动密钥轮换，都要立即开始轮换与 KMS 密钥关联的密钥材料。

管理密钥材料

AWS KMS 即使禁用了密钥轮换，也会保留 KMS 密钥的所有密钥材料。 AWS KMS 只有在删除 KMS 密钥时才会删除密钥材料。

使用密钥材料

当您使用轮换的 KMS 密钥加密数据时， AWS KMS 使用当前的密钥材料。当您使用轮换 KMS 密钥解密密文时， AWS KMS 会使用与加密时所用密钥材料相同的版本。您无法为解密操作选择特定版本的密钥材料，而是 AWS KMS 会自动选择正确的版本。

轮换周期

轮换期限定义了在您启用自动密钥轮换后， AWS KMS 将轮换密钥材料的天数，以及此后每次自动密钥轮换之间的天数。如果您没有为启用自动密钥轮换`RotationPeriodInDays`时指定值，则默认值为 365 天。

您可以使用 k ms: RotationPeriodInDays 条件键进一步限制委托人可以在参数中`RotationPeriodInDays`指定的值。

轮换日期

AWS KMS 在轮换周期定义的轮换日期自动轮换 KMS 密钥。默认轮换周期为 365 天。

客户管理密钥

由于客户托管密钥的自动密钥轮换是可选的，并且可以随时启用和禁用，因此轮换日期取决于最近启用轮换的日期。如果您修改先前启用了自动密钥轮换功能的密钥的轮换周期，则日期可能会更改。在密钥的使用寿命内，轮换日期可能会发生多次变化。

例如，如果您在 2022 年 1 月 1 日创建客户托管密钥，并在 2022 年 3 月 15 日启用自动密钥轮换，默认轮换周期为 365 天，则会在 2023 年 3 月 15 日、2024 年 3 月 15 日以及之后每 365 天轮换密钥材料。 AWS KMS

以下示例假设启用了自动密钥轮换，默认轮换周期为 365 天。这些示例演示了可能影响密钥轮换周期的特殊情况。

- 禁用密钥轮换 - 如果您在任何时候禁用自动密钥轮换，KMS 密钥将继续使用禁用轮换时使用的密钥材料版本。如果您再次启用自动密钥轮换，则 AWS KMS 会根据新的启用轮换的日期轮换密钥材料。
- 已禁用 KMS 密钥-当 KMS 密钥处于禁用状态时， AWS KMS 不会对其进行轮换。但是，密钥轮换状态不会发生改变，并且在 KMS 密钥处于禁用状态时不能对其进行更改。重新启用 KMS 密钥后，如果密钥材料已超过其上次计划轮换日期，则 AWS KMS 会立即轮换。如果密钥材料没有错过上次预定的轮换日期，则 AWS KMS 恢复原来的密钥轮换计划。
- 待删除的 KMS 密钥-当 KMS 密钥处于待删除状态时， AWS KMS 不会对其进行轮换。密钥轮换状态设为 `false`，处于待删除状态时不能更改。如果删除被取消，将恢复之前的密钥轮换状态。如果密钥材料已超过其上次预定的轮换日期，则立即将其 AWS KMS 轮换。如果密钥材料没有错过上次预定的轮换日期，则 AWS KMS 恢复原来的密钥轮换计划。

AWS 托管式密钥

AWS KMS AWS 托管式密钥 每年自动轮换（大约 365 天）。您无法启用或禁用 AWS 托管式密钥 的密钥轮换。

的密钥材料在创建日期一年后首次轮换，此后每年（自上次轮换后大约 365 天）进行轮换。

AWS 托管式密钥

> **Note**
>
> 2022年5月，将轮换时间表 AWS 托管式密钥 从每三年（约1,095天） AWS KMS 改为每年（约365天）。
> 新 AWS 托管式密钥 版本在创建一年后自动轮换，此后大约每年轮换一次。
> 现有 AWS 托管式密钥 人员在最近一次轮换一年后自动轮换，此后每年轮换。

AWS 拥有的密钥

您无法启用或禁用 AWS 拥有的密钥的密钥轮换。的密钥轮换策略 AWS 拥有的密钥 由创建和管理密钥的 AWS 服务决定。有关详细信息，请参阅服务的用户指南或开发人员指南中的静态加密主题。

支持的 KMS 密钥类型

只有具有由 AWS KMS 生成（Origin = AWS_KMS）的密钥材料的对称加密 KMS 密钥支持自动密钥轮换。

以下类型的 KMS 密钥不支持自动密钥轮换，但您可以手动轮换这些 KMS 密钥。

- 非对称 KMS 密钥
- HMAC KMS 密钥
- 自定义密钥存储中的 KMS 密钥
- 具有导入密钥材料的 KMS 密钥

多区域密钥

您可以启用和禁用多区域密钥的自动密钥轮换。您只能对主密钥设置属性。 AWS KMS 同步密钥时，它会将属性设置从主键复制到其副本密钥。轮换主键的密钥材料时， AWS KMS 会自动将该密钥材料复制到其所有副本密钥中。有关更多信息，请参阅 轮换多区域密钥。

AWS 服务

您可以在用于 AWS 服务中的服务器端加密的客户托管密钥上启用自动密钥轮换。年度轮换是透明的，并与 AWS 服务兼容。

监控密钥轮换

AWS KMS 轮换AWS 托管式密钥或客户托管密钥的密钥材料时，它会向 Amazon EventBridge 写一个KMS CMK Rotation事件，将一个RotateKey 事件写入您的 AWS CloudTrail 日志。您可以使用这些记录验证 KMS 密钥是否已轮换。

您可以使用 AWS Key Management Service 控制台查看 KMS 密钥的剩余按需轮换次数以及 KMS 密钥所有已完成的密钥材料轮换的列表。

您可以使用ListKeyRotations操作来查看已完成旋转的详细信息。

最终一致性

密钥轮换受到与其他 AWS KMS 管理操作相同的最终一致性影响。新的密钥材料在整个 AWS KMS 中可用之前可能会有一些延迟。但是，轮换密钥材料不会导致加密操作中断或延迟。当前的密钥材料用于加密操作，直到新的密钥材料在整个 AWS KMS中可用为止。当自动轮换多区域密钥的密钥材料时，将 AWS KMS 使用当前密钥材料，直到新的密钥材料在所有带有相关多区域密钥的区域中都可用。

如何启用和禁用自动密钥轮换

默认情况下，当您为 KMS 密钥启用自动密钥轮换时，每年会为 KMS 密钥 AWS KMS 生成新的加密材料。您还可以指定自定义，rotation-period以定义启用自动密钥轮换以轮换密钥材料后的天数，以及此后每次自动轮换之间的天数。 AWS KMS

自动密钥轮换具有以下优点：

- KMS 密钥的属性，包括其密钥 ID、密钥 ARN、区域、策略和权限，在密钥轮换时不会发生改变。
- 您无需更改引用该 KMS 密钥的密钥 ID 或密钥 ARN 的应用程序或别名。
- 轮换密钥材料不会影响 AWS 服务中任何 KMS 密钥的使用。
- 启用密钥轮换后，将在 AWS KMS 轮换周期定义的下一个轮换日期自动轮换 KMS 密钥。您无需记住或计划更新。

授权用户可以使用 AWS KMS 控制台和 AWS KMS API 来启用和禁用自动密钥轮换，并查看密钥轮换状态。

主题

- 启用和禁用自动密钥轮换（控制台）
- 启用和禁用自动密钥轮换 (AWS KMS API)

启用和禁用自动密钥轮换（控制台）

1. 登录 AWS Management Console 并打开 AWS Key Management Service (AWS KMS) 控制台，网址为 https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。（您无法启用或禁用 AWS 托管式密钥的轮换。它们每年自动轮换一次。）
4. 选择 KMS 密钥的别名和密钥 ID。
5. 选择 Key rotation (密钥轮换) 选项卡。

   密钥轮换选项卡仅出现在对称加密 KMS 密钥的详细信息页面上，其中包含 AWS KMS 生成的密钥材料（来源为 AWS_KMS），包括多区域对称加密 KMS 密钥。

   您不能自动轮换非对称 KMS 密钥、HMAC KMS 密钥、具有导入的密钥材料的 KMS 密钥或自定义密钥存储中的 KMS 密钥。但是，您可以手动轮换它们。
6. 在“自动密钥轮换”部分，选择“编辑”。
7. 对于“密钥轮换”，选择“启用”。

   > **Note**
   >
   > 如果 KMS 密钥已禁用或待删除，则 AWS KMS 不会轮换密钥材料，也无法更新自动密钥轮换状态或轮换周期。启用 KMS 密钥或取消删除以更新自动密钥轮换配置。有关详细信息，请参阅 密钥轮换的工作原理 和 密 AWS KMS 钥的关键状态。
8. （可选）键入介于 90 到 2560 天之间的轮换周期。默认值为 365 天。如果您未指定自定义轮换周期，则 AWS KMS 将每年轮换密钥材料。

   您可以使用 k ms: RotationPeriodInDays 条件键来限制委托人可以为轮换周期指定的值。
9. 选择保存。

启用和禁用自动密钥轮换 (AWS KMS API)

您可以使用 AWS Key Management Service (AWS KMS) API 启用和禁用自动密钥轮换，并查看任何客户托管密钥的当前轮换状态。这些示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

该EnableKeyRotation操作可为指定的 KMS 密钥启用自动密钥轮换。该DisableKeyRotation操作将其禁用。要在这些操作中标识 KMS 密钥，请使用其密钥 ID 或密钥 ARN。在默认情况下，客户托管密钥的密钥轮换处于禁用状态。

您可以使用 k ms: RotationPeriodInDays 条件键来限制委托人可以为`EnableKeyRotation`请求的`RotationPeriodInDays`参数指定的值。

以下示例在指定的对称加密 KMS 密钥上启用密钥轮换，轮换周期为 180 天，并使用该GetKeyRotationStatus操作来查看结果。然后，它禁用了密钥轮换，并使用 GetKeyRotationStatus 查看更改。

```
$ 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
}
```

如何执行按需密钥轮换

无论是否启用了自动密钥轮换，您都可以按需轮换客户托管的 KMS 密钥中的密钥材料。禁用自动轮换 (DisableKeyRotation) 不会影响您执行按需轮换的能力，也不会取消任何正在进行的按需轮换。按需轮换不会更改现有的自动轮换计划。例如，假设一个启用了自动密钥轮换、轮换周期为 730 天的 KMS 密钥。如果密钥计划在 2024 年 4 月 14 日自动轮换，而您在 2024 年 4 月 10 日按需轮换，则密钥将按计划在 2024 年 4 月 14 日自动轮换，此后每 730 天自动轮换一次。

每个 KMS 密钥最多可以按需轮换 10 次。您可以使用 AWS KMS 控制台查看 KMS 密钥的剩余按需轮换次数。

仅对称加密 KMS 密钥支持按需密钥轮换。您无法按需轮换非对称 KMS 密钥、HMAC KMS 密钥、带有导入密钥材料的 KMS 密钥或自定义密钥存储中的 KMS 密钥。要按需轮换一组相关的多区域密钥，请调用主密钥的按需轮换。

授权用户可以使用 AWS KMS 控制台和 AWS KMS API 启动按需密钥轮换并查看密钥轮换状态。

主题

- 启动按需密钥轮换（控制台）
- 启动按需密钥轮换 (AWS KMS API)

启动按需密钥轮换（控制台）

1. 登录 AWS Management Console 并打开 AWS Key Management Service (AWS KMS) 控制台，网址为 https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。（您不能按需轮换 AWS 托管式密钥。 它们每年自动轮换。）
4. 选择 KMS 密钥的别名和密钥 ID。
5. 选择 Key rotation (密钥轮换) 选项卡。

   密钥轮换选项卡仅出现在对称加密 KMS 密钥的详细信息页面上，其中包含 AWS KMS 生成的密钥材料（来源为 AWS_KMS），包括多区域对称加密 KMS 密钥。

   您无法按需轮换非对称 KMS 密钥、HMAC KMS 密钥、带有导入密钥材料的 KMS 密钥或自定义密钥存储库中的 KMS 密钥。但是，您可以手动轮换它们。
6. 在按需密钥轮换部分中，选择轮换密钥。
7. 阅读并考虑警告以及有关密钥剩余按需轮换次数的信息。如果您决定不想继续按需轮换，请选择“取消”。
8. 选择旋转密钥以确认按需轮换。

> **Note**
>
> 按需轮换会受到与其他 AWS KMS 管理操作相同的最终一致性影响。新的密钥材料在整个 AWS KMS中可用之前可能会有一些延迟。当按需轮换完成时，控制台顶部的横幅会通知您。

启动按需密钥轮换 (AWS KMS API)

您可以使用 AWS Key Management Service (AWS KMS) API 启动按需密钥轮换，并查看任何客户托管密钥的当前轮换状态。这些示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

该RotateKeyOnDemand操作会立即启动指定的 KMS 密钥的按需密钥轮换。要在这些操作中标识 KMS 密钥，请使用其密钥 ID 或密钥 ARN。

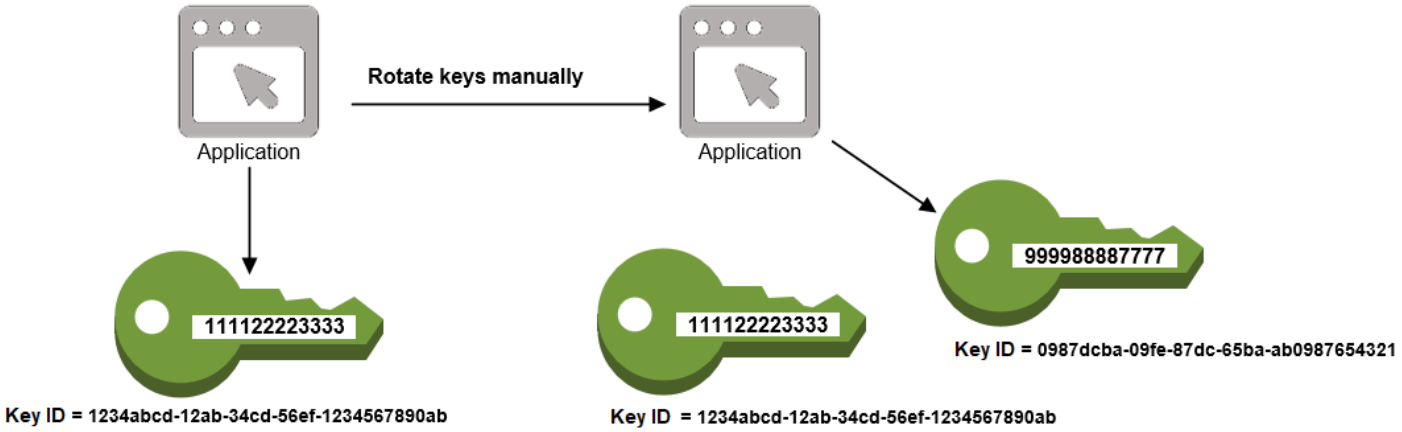
以下示例在指定的对称加密 KMS 密钥上启动按需密钥轮换，并使用该GetKeyRotationStatus操作验证按需轮换是否正在进行中。`kms:GetKeyRotationStatus`响应`OnDemandRotationStartDate`中的标识了启动正在进行的按需轮换的日期和时间。

```
$ 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
}
```

手动轮换密钥

您可能希望创建一个新的 KMS 密钥，并使用它替代当前的 KMS 密钥，而不启用自动密钥轮换。当新的 KMS 密钥使用的加密材料与当前 KMS 密钥使用的加密材料不相同时，使用新的 KMS 密钥与更

改现有 KMS 密钥的密钥材料具有相同的效果。使用一个 KMS 密钥替换另一个 KMS 密钥的过程被称为手动密钥轮换。



如果您想要轮换不符合自动密钥轮换条件的 KMS 密钥，例如非对称 KMS 密钥、HMAC KMS 密钥、自定义密钥存储中的 KMS 密钥以及带有导入密钥材料的 KMS 密钥，则手动轮换是一个不错的选择。

> **Note**
>
> 开始使用新的 KMS 密钥时，请务必启用原始 KMS 密钥，以便 AWS KMS 可以解密原始 KMS 密钥加密的数据。

当您手动轮换 KMS 密钥时，您还需要更新应用程序中对 KMS 密钥 ID 或密钥 ARN 的引用。将友好名称与 KMS 密钥关联的别名，可以使得这个过程变得更容易。使用别名来引用应用程序中的 KMS 密钥。之后，当您想更改应用程序所使用的 KMS 密钥（而不是编辑应用程序代码）时，更改别名的目标 KMS 密钥即可。有关更多信息，请参阅 在应用程序中使用别名。

> **Note**
>
> 指向手动轮换 KMS 密钥的最新版本的别名是、E ncrypt DescribeKey、、GenerateDataKeyGenerateDataKeyPairGenerateMac、和 S ign 操作的好解决方案。管理 KMS 密钥的操作中不允许使用别名，例如DisableKey或ScheduleKeyDeletion。对手动轮换的对称加密 KMS 密钥调用 Decrypt 操作时，请省略命令中的`KeyId`参数。 AWS KMS 自动使用加密密文的 KMS 密钥。
>
> 使用非对称 KMS 密钥调用`Decrypt`或验证，或使用 HMAC KMS 密钥VerifyMac进行调用时，必须使用该`KeyId`参数。当 `KeyId` 参数的值是不再指向执行加密操作的 KMS 密钥的别名时，

例如当手动轮换密钥时，这些请求将失败。为避免此错误，必须跟踪并为每个操作指定正确的 KMS 密钥。

要更改别名的目标 KMS 密钥，请使用 AWS KMS API 中的UpdateAlias操作。例如，此命令会更新 alias/TestKey 别名以指向新 KMS 密钥。由于该操作不返回任何输出，因此该示例使用该ListAliases操作来显示别名现在已与其他 KMS 密钥相关联，并且该LastUpdatedDate字段已更新。这些 ListAliases 命令使用中的query参数仅 AWS CLI 获取alias/TestKey别名。

```
$ 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
        },
    ]
}
```

监控 AWS KMS keys

对于了解 AWS KMS 中 AWS KMS keys 的可用性、状态和使用情况，以及维护 AWS 解决方案的可靠性、可用性和性能，监控是一个重要部分。从 AWS 解决方案的各个部分收集监控数据将有助于调试出现的多点故障。不过，在开始监控 KMS 密钥之前，应制定一个监控计划并在计划中回答下列问题：

- 监控目的是什么？
- 您将监控哪些资源？
- 监控这些资源的频率如何？
- 您将使用哪些监控工具？
- 谁负责执行监控任务？
- 出现情况时应通知谁？

下一步是监控 KMS 密钥在一段时间内的情况，以便为环境中正常的 AWS KMS 使用情况和预期建立基准。监控 KMS 密钥时，存储历史监控数据，以便将此数据与当前数据进行比较，从而确定正常模式和异常情况，并找出解决问题的方法。

例如，您可以监控影响 KMS 密钥的 AWS KMS API 活动和事件。当数据高于或低于既定标准时，您可能需要进行调查或采取纠正措施。

要建立正常模式的基准，应监控以下各项：

- AWS KMS数据层面操作的 API 活动。这些是使用 KMS 密钥的加密操作，例如解密、ReEncrypt加密和。GenerateDataKey
- 对您而言至关重要的AWS KMS控制层面操作的 API 活动。这些操作管理 KMS 密钥，您可能需要监控那些更改 KMS 密钥可用性的操作（例如ScheduleKeyDeletion、、CancelKeyDeletion、DisableKey、EnableKeyImportKeyMaterial、和DeleteImportedKeyMaterial）或更改 KMS 密钥的访问控制（例如PutKeyPolicy和 RevokeGrant）。
- 其他 AWS KMS 指标（如导入的密钥资料过期之前的剩余时间量）和事件（如导入的密钥资料到期，KMS 密钥的删除或密钥轮换）。

监控工具

AWS 为您提供了可用来监控 KMS 密钥的各种工具。您可以配置其中的一些工具来为您执行监控任务，但有些工具需要手动干预。建议您尽可能实现监控任务自动化。

自动监控工具

您可以使用以下自动化监控工具来监控 KMS 密钥并在发生更改时进行报告。

- AWS CloudTrail日志监控-在账户之间共享日志文件，通过将 CloudTrail 日志文件发送到 “CloudWatch 日志” 来实时监控日志文件，使用处理库编写日志CloudTrail 处理应用程序，并验证您的日志文件在传送后是否未更改 CloudTrail。有关更多信息，请参阅AWS CloudTrail用户指南中的使用 CloudTrail 日志文件。
- A CloudWatch mazon Alarms — 在您指定的时间段内观察单个指标，并根据该指标在多个时间段内相对于给定阈值的值执行一项或多项操作。该操作是发送到亚马逊简单通知服务 (Amazon SNS) Simple Notification Scaling 主题或亚马逊 EC2 Auto Scaling 策略的通知。 CloudWatch 警报不会仅仅因为它们处于特定状态就调用操作；该状态必须已更改并保持了指定的时间段。有关更多信息，请参阅 使用 Amazon 进行监控 CloudWatch。
- Amazon EventBridge — 匹配事件并将其路由到一个或多个目标函数或流，以捕获状态信息，并在必要时进行更改或采取纠正措施。有关更多信息，请参阅使用 Amazon 进行监控 EventBridge和 Amazon EventBridge 用户指南。
- Amazon CloudWatch Logs — 监控、存储和访问来自AWS CloudTrail或其他来源的日志文件。有关更多信息，请参阅 Amazon CloudWatch 日志用户指南。

手动监控工具

监控 KMS 密钥的另一个重要部分是手动监控 CloudWatch 警报和事件未涵盖的项目。AWS KMS、CloudWatchAWS Trusted Advisor、和其他AWS仪表板提供了AWS环境状态的 at-a-glance 视图。

您可以自定义 AWS KMS 控制台的 AWS 托管式密钥 和客户托管式密钥页面，显示有关每个 KMS 密钥的以下信息：

- 密钥 ID
- Status
- 创建日期
- 到期日期（对于具有导入密钥材料的 KMS 密钥）
- Origin
- 自定义密钥存储 ID（对于自定义密钥存储中的 KMS 密钥）

CloudWatch 控制台控制面板显示以下信息：

- 当前告警和状态
- 告警和资源图表
- 服务运行状况

此外，您还可以使用 CloudWatch 执行以下操作：

- 创建自定义控制面板以监控您关心的服务
- 绘制指标数据图，以排除问题并弄清楚趋势
- 搜索并浏览您所有的 AWS 资源指标
- 创建和编辑警报以接收有关问题的通知

AWS Trusted Advisor 可以帮助您监控 AWS 资源以提高性能、可靠性、安全性和成本效益。四个 Trusted Advisor 检查可供所有用户使用；超过 50 个检查可供具有“商业”或“企业”支持计划的用户使用。有关更多信息，请参阅 AWS Trusted Advisor。

使用记录 AWS KMS API 调用 AWS CloudTrail

AWS KMS 与记录用户AWS CloudTrail、角色和其他服务的所有呼叫 AWS KMS 的 AWS 服务集成。CloudTrail 将对的所有 API 调用捕获 AWS KMS 为事件，包括来自 AWS KMS 控制台、 AWS KMS API、 AWS CloudFormation 模板、 AWS Command Line Interface (AWS CLI) 和的调用 AWS Tools for PowerShell。

CloudTrail 记录所有 AWS KMS 操作，包括只读操作（例如ListAliases和）GetKeyRotationStatus、管理 KMS 密钥的操作（例如CreateKey和 PutKeyPolicy）以及加密操作（例如GenerateDataKey和解密）。它还会记录 AWS KMS 需要您的内部操作，例如DeleteExpiredKeyMaterial、DeleteKeySynchronizeMultiRegionKey、和RotateKey。

CloudTrail 记录成功的操作和失败的尝试调用，例如当呼叫者被拒绝访问资源时。在 KMS 密钥上的跨账户操作将记录在调用方的账户和 KMS 密钥所有者账户中。但是，因访问被拒绝而被拒绝的跨账户 AWS KMS 请求仅记录在来电者的账户中。

出于安全考虑， AWS KMS 日志条目中省略了某些字段，例如 E n crypt 请求的`Plaintext`参数以及对GetKeyPolicy任何加密操作的响应。为了便于搜索特定 KMS 密钥的 CloudTrail 日志条目，即使 API 操作未返回密钥 ARN，也要将受影响的 KMS 密钥的 AWS KMS 密钥 ARN AWS KMS 添加到某些密钥管理操作的日志条目的`responseElements`字段中。

尽管默认情况下，所有 AWS KMS 操作都记录为 CloudTrail 事件，但您可以从 CloudTrail 跟踪中排除 AWS KMS 操作。有关更多信息，请参阅 从跟踪中排除 AWS KMS 事件。

了解更多：

- 有关 AWS Nitro 飞地 AWS KMS 操作的 CloudTrail 日志示例，请参阅。监控 Nitro Enclave 的请求

主题

- 在中记录事件 CloudTrail
- 在中搜索事件 CloudTrail
- 从跟踪中排除 AWS KMS 事件
- AWS KMS 日志条目示例

在中记录事件 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当活动发生在中时 AWS KMS，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户事件（包括的事件） AWS KMS，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务 ，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail日志文件

要了解更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。要了解监控 KMS 密钥使用情况的其他方式，请参阅 监控 AWS KMS keys。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 如果请求是使用根凭证或 IAM 用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 如果请求是由其他人提出的 AWS 服务。

有关更多信息，请参阅CloudTrail 用户身份元素。

在中搜索事件 CloudTrail

要搜索 CloudTrail 日志条目，请使用CloudTrail 控制台或CloudTrail LookupEvents操作。 CloudTrail 支持用于筛选搜索的多种属性值，包括事件名称、用户名和事件源。

为了帮助您在中搜索 AWS KMS 日志条目 CloudTrail，请 AWS KMS 填充以下 CloudTrail 日志条目字段。

> **Note**
>
> 从 2022 年 12 月开始，在更改特定 KMS 密钥的所有管理操作中 AWS KMS 填充资源类型和资源名称属性。在以下操作的旧 CloudTrail 条目中，这些属性值可能为空：CreateAliasCreateGrant、DeleteAlias、DeleteImportedKeyMaterial、ImportKeyMaterial、Replicat和UpdatePrimaryRegion。

属性	值	日志条目
事件源（`EventSource`）	`kms.amazonaws.com`	全部操作。
资源类型（`ResourceType`）	`AWS::KMS::Key`	更改特定 KMS 密钥的管理操作，例如 `CreateKey` 和 `EnableKey`，而非 `ListKeys`。
资源名称（`ResourceName`）	密钥 ARN（或密钥 ID 和密钥 ARN）	更改特定 KMS 密钥的管理操作，例如 `CreateKey` 和 `EnableKey`，而非 `ListKeys`。

为了帮助您查找针对特定 KMS 密钥进行管理操作的日志条目，即使 AWS KMS 该 API 操作未返回密钥 ARN，也会在日志条目的`responseElements.keyId`元素中 AWS KMS 记录受影响 KMS 密钥的密钥 ARN。

例如，成功调用该DisableKey操作不会在响应中返回任何值，但DisableKey 日志条目中的值不是空值，而是包含已禁用的 KMS 密钥的密钥 ARN。`responseElements.keyId`

此功能于 2022 年 12 月添加，会影响以下 CloudTrail 日志条目：CreateAlias、CreateGrant、、DeleteAlias、DeleteKey、DisableKey、EnableKey、、EnableKeyRotatio和UpdatePrimaryRegion。

从跟踪中排除 AWS KMS 事件

为了记录其 AWS KMS 资源的使用和管理情况，大多数 AWS KMS 用户都依赖 CloudTrail 跟踪中的事件。该跟踪可以成为审核关键事件的重要数据来源，例如创建、禁用和删除 AWS KMS keys、更改密钥策略以及 AWS 服务代表您使用您的 KMS 密钥。在某些情况下， CloudTrail 日志条目中的元数据（例如加密操作中的加密上下文）可以帮助您避免或解决错误。

但是，由于 AWS KMS 可以生成大量事件，因此 AWS CloudTrail 允许您从跟踪中排除 AWS KMS 事件。此按跟踪设置排除所有 AWS KMS 事件；您不能排除特定 AWS KMS 事件。

> **Warning**
>
> 从 CloudTrail 日志中排除 AWS KMS 事件可能会掩盖使用您的 KMS 密钥的操作。请谨慎赋予委托人执行此操作所需的 `cloudtrail:PutEventSelectors` 权限。

要从跟踪中排除 AWS KMS 事件，请执行以下操作：

- 在 CloudTrail 控制台中，创建跟踪或更新跟踪时，请使用日志密钥管理服务事件设置。有关说明，请参阅《 AWS CloudTrail 用户指南》AWS Management Console中的 “使用记录管理事件”。
- 在 CloudTrail API 中，使用PutEventSelectors操作。将 `ExcludeManagementEventSources` 属性添加到值为 `kms.amazonaws.com` 的事件选择器中。有关示例，请参阅《 AWS CloudTrail 用户指南》中的示例：不记录 AWS Key Management Service 事件的跟踪。

您可以随时更改控制台设置或跟踪的事件选择器，以禁用此排除。然后，跟踪将开始记录 AWS KMS 事件。但是，它无法恢复排除生效期间发生 AWS KMS 的事件。

当您使用控制台或 API 排除 AWS KMS 事件时，生成的 CloudTrail `PutEventSelectors` API 操作也会记录在您的 CloudTrail 日志中。如果 AWS KMS 事件未出现在您的 CloudTrail 日志中，请查找`ExcludeManagementEventSources`属性设置为`PutEventSelectors`的事件`kms.amazonaws.com`。

AWS KMS 日志条目示例

AWS KMS 当您调用 AWS KMS 操作和 AWS 服务代表您调用操作时，会将条目写入您的日 CloudTrail 志。 AWS KMS 当它为您调用操作时，还会写入一个条目。例如，它会在删除您计划删除的 KMS 密钥时写入条目。

以下主题显示了 AWS KMS 操作 CloudTrail 日志条目的示例。

有关来 AWS KMS 自 AWS Nitro Enclaves 的请求的 CloudTrail 日志条目示例，请参阅。监控 Nitro Enclave 的请求

主题

- 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
- 验证
- Amazon EC2 示例一
- Amazon EC2 示例二

CancelKeyDeletion

以下示例显示了通过调用 CancelKeyDeletion 操作生成的 AWS CloudTrail 日志条目。关于删除 AWS KMS keys 的信息，请查阅 删除 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

以下示例显示了通过调用 ConnectCustomKeyStore 操作生成的 AWS CloudTrail 日志条目。有关连接自定义密钥存储的信息，请参阅 连接和断开 AWS CloudHSM 密钥存储。

```
{
    "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

以下示例显示了该CreateAlias操作的AWS CloudTrail日志条目。resources 元素包含别名和 KMS 密钥资源的字段。有关在 AWS KMS 中创建别名的信息，请参阅 创建别名。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在responseElements.keyId值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 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

以下示例显示了通过调用 AWS CloudHSM 密钥存储上的 `CreateCustomKeyStore` 操作生成的 AWS CloudTrail 日志条目。有关创建自定义密钥存储的信息，请参阅 创建 AWS CloudHSM 密钥存储。

```
{
    "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

以下示例显示了该CreateGrant操作的AWS CloudTrail日志条目。有关在 AWS KMS 中创建授权的信息，请参阅 AWS KMS 中的授权。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在`responseElements.keyId`值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 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

这些示例显示了CreateKey操作的AWS CloudTrail日志条目。

CreateKey日志条目可能源于CreateKey请求或对ReplicateKey请求的CreateKey操作。

以下示例显示了创建对称加密 KMS 密钥的CreateKey操作的 CloudTrail 日志条目。有关创建 KMS 密钥的信息，请参阅 创建密钥。

```
{
    "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"
}
```

以下示例显示了在密钥存储中创建对称加密 KMS 密钥的CreateKey操作的 CloudTrail AWS CloudHSM日志。


```
{
    "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"
}
```

以下示例显示了在外部密钥存储中创建对称加密 KMS 密钥的CreateKey操作的 CloudTrail 日志。

```
{
    "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

这些示例显示用于 Decrypt 操作的 AWS CloudTrail 日志条目。

requestParameters即使请求encryptionAlgorithm中未指定加密算法，Decrypt操作的 CloudTrail 日志条目也始终包含在中。省略了请求中的密文和响应中的明文。

主题

- 使用标准对称加密密钥解密
- 使用标准对称加密密钥解密失败
- 使用 AWS CloudHSM 密钥存储中的 KMS 密钥解密
- 使用外部密钥存储中的 KMS 密钥解密
- 使用外部密钥存储中的 KMS 密钥解密失败

使用标准对称加密密钥解密

以下是使用标准对称加密密钥的Decrypt操作的 CloudTrail 日志条目示例。

```
{
    "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"
}
```

使用标准对称加密密钥解密失败

以下示例 CloudTrail 日志条目记录了使用标准对称加密 KMS 密钥的失败Decrypt操作。包含异常（errorCode）和错误消息（errorMessage），可帮助您解决错误。

在这种情况下，Decrypt 请求中指定的对称加密 KMS 密钥不是用于加密数据的对称加密 KMS 密钥。

```
{
    "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"
}
```

使用 AWS CloudHSM 密钥存储中的 KMS 密钥解密

以下示例 CloudTrail 日志条目记录了在密钥库中使用 KMS AWS CloudHSM密钥进行的Decrypt操作。使用自定义密钥存储中的 KMS 密钥进行加密操作的所有日志条目都包含带有 customKeyStoreId 的 additionalEventData 字段。请求中未指定 additionalEventData。


```
{
    "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"
}
```

使用外部密钥存储中的 KMS 密钥解密

以下示例 CloudTrail 日志条目记录了在外部密钥存储中使用 KMS 密钥进行的Decrypt操作。除了customKeyStoreId，additionalEventData 字段包括外部密钥 ID（XksKeyId）。请求中未指定 additionalEventData。

```
{
    "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"
}
```

使用外部密钥存储中的 KMS 密钥解密失败

以下示例 CloudTrail 日志条目记录了使用外部密钥存储库中的 KMS 密钥Decrypt执行操作的失败请求。 CloudWatch 除了成功的请求外，还会记录失败的请求。记录失败时， CloudTrail 日志条目包括异常（ErrorCode）和随附的错误消息（ErrorMessage）。

如果失败的请求到达了您的外部密钥存储代理（如本示例所示），则您可以使用 requestId 值将失败的请求与您的外部密钥存储代理日志的相应请求关联起来（如果您的代理提供了这些请求）。

如需帮助解决外部密钥存储中的 Decrypt 请求，请参阅 解密错误。

```
{
    "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

以下示例显示了该DeleteAlias操作的AWS CloudTrail日志条目。有关删除别名的信息，请参阅 删除别名。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在`responseElements.keyId`值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 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

以下示例显示了通过调用 DeleteCustomKeyStore 操作生成的 AWS CloudTrail 日志条目。有关创建自定义密钥存储的信息，请参阅 删除 AWS CloudHSM 密钥存储。

```
{
    "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

将密钥材料导入AWS KMS key（KMS 密钥）时，可以为该密钥材料设置到期日期和时间。 AWS KMS 当您导入密钥材料（使用过期设置）和AWS KMS删除过期的密钥材料时，会在 CloudTrail 日志中记

录一个条目。有关创建带已导入密钥材料的 KMS 密钥的信息，请参阅 导入密钥的 AWS KMS 密钥材料。

以下示例显示了在 AWS KMS 删除过期的密钥材料时生成的 AWS CloudTrail 日志条目。

```
{
    "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

如果您将密钥材料导入 KMS 密钥，则可以使用DeleteImportedKeyMaterial操作随时删除导入的密钥材料。当您从 KMS 密钥中删除导入的密钥材料时，KMS 密钥的密钥状态会更改为 `PendingImport`，在任何加密操作中都无法使用 KMS 密钥。有关更多信息，请参阅 删除导入的密钥材料。

以下示例显示了为 `DeleteImportedKeyMaterial` 操作生成的 AWS CloudTrail 日志条目。

```
{
    "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

这些示例显示了在删除 KMS 密钥时生成的 AWS CloudTrail 日志条目。要删除 KMS 密钥，请使用ScheduleKeyDeletion操作。在指定的等待期到期后，AWS KMS删除 KMS 密钥并在 CloudTrail 日志中记录类似以下内容的条目以记录该事件。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在`responseElements.keyId`值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 ARN。

有关`ScheduleKeyDeletion`操作 CloudTrail 日志条目的示例，请参见ScheduleKeyDeletion。有关删除 KMS 密钥的信息，请参阅 删除 AWS KMS keys。

以下示例 CloudTrail 日志条目记录了包含密钥材料的 KMS 密钥的`DeleteKey`操作AWS 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"
}
```

以下 CloudTrail 日志条目记录了AWS CloudHSM自定义密钥存储库中 KMS 密钥的DeleteKey操作。


```
{
    "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

以下示例显示了通过调用 DescribeCustomKeyStores 操作生成的 AWS CloudTrail 日志条目。有关查看自定义密钥存储的信息，请参阅 查看 AWS CloudHSM 密钥存储。


```
{
    "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

以下示例显示了该DescribeKey操作的AWS CloudTrail日志条目。 AWS KMS当您调用DescribeKey操作或在AWS KMS控制台中查看 KMS 密钥时，会记录如下所示的条目。此调用是在 AWS KMS 管理控制台中查看密钥的结果。


```
{
    "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

以下示例显示了该DisableKey操作的AWS CloudTrail日志条目。有关在 AWS KMS 中启用和禁用的信息 AWS KMS keys 的信息，请参阅 启用和禁用密钥。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在`responseElements.keyId`值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 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

以下示例显示了通过调用 DisableKeyRotation 操作生成的 AWS CloudTrail 日志条目。有关启用自动轮换的信息，请参阅 旋转 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

以下示例显示了通过调用 DisconnectCustomKeyStore 操作生成的 AWS CloudTrail 日志条目。有关断开自定义密钥存储的信息，请参阅 连接和断开 AWS CloudHSM 密钥存储。

```
{
    "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

以下示例显示了该EnableKey操作的AWS CloudTrail日志条目。有关在 AWS KMS 中启用和禁用的信息 AWS KMS keys 的信息，请参阅 启用和禁用密钥。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在`responseElements.keyId`值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 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

以下示例显示了调用EnableKeyRotation操作的 AWS CloudTrail 日志条目。有关轮换密钥时写入的 CloudTrail 日志条目的示例，请参见RotateKey。有关轮换 AWS KMS keys的更多信息，请参阅 旋转 AWS KMS keys。

> **Note**
>
> rotation-period是一个可选的请求参数。如果您在启用自动密钥轮换时未指定轮换周期，则默认值为 365 天。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在`responseElements.keyId`值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 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

以下示例显示了 Encrypt 操作的一个 AWS CloudTrail 日志条目。


```
{
    "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

以下示例显示了该GenerateDataKey操作的AWS CloudTrail日志条目。

```
{
    "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

以下示例显示了该GenerateDataKeyPair操作的AWS CloudTrail日志条目。此示例记录了一个操作，该操作生成一个使用对称加密 AWS KMS key 加密的 RSA 密钥对。

```
{
    "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

以下示例显示了该GenerateDataKeyPairWithoutPlaintext操作的AWS CloudTrail日志条目。此示例记录了一个操作，该操作生成一个使用对称加密 AWS KMS key 加密的 RSA 密钥对。

```
{
    "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

以下示例显示了该GenerateDataKeyWithoutPlaintext操作的AWS CloudTrail日志条目。

```
{
    "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

以下示例显示了该GenerateMac操作的AWS CloudTrail日志条目。

```
{
    "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

以下示例显示了该GenerateRandom操作的AWS CloudTrail日志条目。因为此操作不使用 AWS KMS key，`resources` 字段为空。

```
{
    "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

以下示例显示了该GetKeyPolicy操作的AWS CloudTrail日志条目。有关查看 KMS 密钥的密钥策略的信息，请参阅 查看密钥策略。

```
{
    "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

以下示例显示了该GetKeyRotationStatus操作的 AWS CloudTrail 日志条目。有关自动和按需轮换 KMS 密钥材料的信息，请参阅旋转 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

以下示例显示了使用该GetParametersForImport操作时生成的AWS CloudTrail日志条目。此操作返回您在将密钥材料导入 KMS 密钥时使用的公有密钥和导入令牌。当您使用`GetParametersForImport`操作或使用AWS KMS控制台下载公钥和导入令牌时，会记录相同的 CloudTrail 条目。

```
{
    "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

以下示例显示了使用该ImportKeyMaterial操作时生成的AWS CloudTrail日志条目。当您使用ImportKeyMaterial操作或使用AWS KMS控制台将密钥材料导入到中时，也会记录相同的CloudTrail 条目AWS KMS key。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在responseElements.keyId值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 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

以下示例显示了该ListAliases操作的AWS CloudTrail日志条目。因为此操作不使用任何特定别名或 AWS KMS key，`resources` 字段为空。有关在 AWS KMS 中查看别名的信息，请参阅 查看别名。

```
{
    "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

以下示例显示了该ListGrant操作的AWS CloudTrail日志条目。有关 AWS KMS 的授权的信息，请参阅AWS KMS 中的授权。

```
{
    "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

以下示例显示了该ListKeyRotations操作的 AWS CloudTrail 日志条目。有关自动和按需轮换 KMS 密钥材料的信息，请参阅旋转 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

以下示例显示了通过调用 PutKeyPolicy 操作生成的 AWS CloudTrail 日志条目。有关更新密钥策略的信息，请参阅 更改密钥策略。

```
{
    "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

以下示例显示了该ReEncrypt操作的AWS CloudTrail日志条目。此日志条目中的 `resources` 字段按此顺序指定两个 AWS KMS keys，源 KMS 密钥和目标 KMS 密钥。

```
{
    "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

以下示例显示了通过调用 ReplicateKey 操作生成的 AWS CloudTrail 日志条目。一个ReplicateKey请求会产生一个ReplicateKey操作和一个CreateKey操作。

有关删除多区域密钥的信息，请参阅 创建多区域副本密钥。


```
{
    "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

以下示例显示了通过调用 RetireGrant 操作生成的 AWS CloudTrail 日志条目。有关停用授权的信息，请参阅 停用和撤销授权。


```
{
    "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

以下示例显示了通过调用 RevokeGrant 操作生成的 AWS CloudTrail 日志条目。有关撤销授权的信息，请参阅 停用和撤销授权。

```
{
    "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

这些示例显示了轮换操作的 AWS CloudTrail 日志条目 AWS KMS keys。有关轮换 KMS 密钥的信息，请参阅 旋转 AWS KMS keys。

以下示例显示了轮换启用了自动密钥轮换的对称加密 KMS 密钥的操作的 CloudTrail 日志条目。有关启用自动旋转的信息，请参阅如何启用和禁用自动密钥轮换。

有关记录该`EnableKeyRotation`操作的 CloudTrail 日志条目的示例，请参见EnableKeyRotation。

```
{
    "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"
}
```


以下示例显示了RotateKeyOnDemand操作的 CloudTrail 日志条目。有关按需轮换对称加密 KMS 密钥的信息，请参阅如何执行按需密钥轮换。

有关记录该RotateKeyOnDemand操作的 CloudTrail 日志条目的示例，请参见RotateKeyOnDemand。


```
{
    "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

以下示例显示了该RotateKeyOnDemand操作的 AWS CloudTrail 日志条目。有关轮换密钥时写入的 CloudTrail 日志条目的示例，请参见RotateKey。有关按需轮换 KMS 密钥的密钥材料的更多信息，请参阅如何执行按需密钥轮换。

```
{
    "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

这些示例显示了ScheduleKeyDeletion操作的AWS CloudTrail日志条目。

有关删除密钥时写入的 CloudTrail 日志条目的示例，请参见DeleteKey。关于删除 AWS KMS keys 的信息，请查阅 删除 AWS KMS keys。

以下示例记录对单区域 KMS 密钥的 `ScheduleKeyDeletion` 请求。

```
{
    "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"
}
```


以下示例记录对拥有副本密钥的多区域 KMS 密钥的 ScheduleKeyDeletion 请求。

由于 AWS KMS 在删除所有副本密钥之前不会删除多区域密钥，在 responseElements 字段中，keyState 是 PendingReplicaDeletion，deletionDate 字段会被省略。


```
{
    "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"
}
```

以下示例在 AWS CloudHSM 自定义密钥存储中记录对 KMS 密钥的 ScheduleKeyDeletion 请求。

```
{
    "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

这些示例显示用于 Sign 操作的 AWS CloudTrail 日志条目。

以下示例显示了使用非对称 RSA KMS 密钥为文件生成数字签名的签名操作的 CloudTrail 日志条目。

```
{
    "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

以下示例显示了 AWS KMS 同步多区域密钥时生成的一个 AWS CloudTrail 日志条目。同步涉及将多区域主键的共享属性复制到其副本密钥的跨区域调用。AWS KMS 会定期同步多区域密钥，以确保所有相关的多区域密钥具有相同的密钥材料。

CloudTrail 日志条目的`resources`元素包括多区域主键的密钥 ARN，包括其。AWS 区域此日志条目中未列出相关的多区域副本密钥及其区域。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在`responseElements.keyId`值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 ARN。

```
{
    "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

以下示例显示了调用TagResource操作以添加标签键为、标签值为的标签Department的AWS CloudTrail日志条目IT。

有关轮换密钥时写入的UntagResource CloudTrail 日志条目的示例，请参见UntagResource。有关标记 AWS KMS keys 的更多信息，请参阅 标记密钥。

```
{
    "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

以下示例显示了调用UntagResource操作以删除标签键为的标签的AWS CloudTrail日志条目Dept。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在responseElements.keyId值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 ARN。

有关TagResource CloudTrail 日志条目的示例，请参见TagResource。有关标记 AWS KMS keys 的更多信息，请参阅 标记密钥。

```
{
    "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

以下示例显示了该UpdateAlias操作的AWS CloudTrail日志条目。`resources` 元素包含别名和 KMS 密钥资源的字段。有关在 AWS KMS 中创建别名的信息，请参阅 创建别名。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在`responseElements.keyId`值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 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

以下示例显示了通过调用 UpdateCustomKeyStore 操作来更新自定义密钥存储的集群 ID 而生成的 AWS CloudTrail 日志条目。有关编辑自定义密钥存储的信息，请参阅 编辑 AWS CloudHSM 密钥存储设置。


```
{
    "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

以下示例显示了通过调用 UpdateKeyDescription 操作生成的 AWS CloudTrail 日志条目。

```
{
    "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

以下示例显示了通过对多区域密钥调用UpdatePrimaryRegion操作生成的AWS CloudTrail日志条目。

该UpdatePrimaryRegion操作写入两个 CloudTrail 日志条目：一个在区域中，多区域主键已转换为副本密钥，另一个在区域中，多区域副本密钥已转换为主键。

CloudTrail 2022 年 12 月或之后记录的此操作的日志条目在responseElements.keyId值中包含受影响 KMS 密钥的密钥 ARN，即使此操作不返回密钥 ARN。

以下示例显示了多区域密钥从主键更改为副本密钥 (us-west-2) 的区域UpdatePrimaryRegion中的 CloudTrail 日志条目。primaryRegion 字段显示了现在托管主键的区域 (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"
}
```

以下示例表示该区域的 CloudTrail 日志条目，其中多区域密钥从副本密钥更改为UpdatePrimaryRegion主键 (ap-northeast-1)。此日志条目没有标识以前的主要区域。

```
{
    "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

以下示例显示了该VerifyMac操作的AWS CloudTrail日志条目。

```
{
    "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"
}
```

验证

这些示例显示用于 Verify 操作的 AWS CloudTrail 日志条目。

以下示例显示了使用非对称 RSA KMS 密钥验证数字签名的验证操作的 CloudTrail 日志条目。


```
{
    "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"
```

```
}
```

Amazon EC2 示例一

以下示例记录了 IAM 主体如何在 Amazon EC2 管理控制台中使用默认卷密钥创建加密卷。

以下示例显示了一个 CloudTrail 日志条目，在该日志条目中，用户 Alice 在 Amazon EC2 管理控制台中使用默认卷密钥创建了一个加密卷。该 EC2 日志文件记录包含一个 `volumeId` 字段，其值为 `"vol-13439757"`。AWS KMS 记录包含一个 `encryptionContext` 字段，其值为 `"aws:ebs:id": "vol-13439757"`。同样，这两个记录的 `principalId` 和 `accountId` 都相互匹配。这些记录反映了一个事实，即创建加密卷生成的数据密钥被用于加密卷内容。

```
{
  "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"
```

```
    }
  ]
}
```

Amazon EC2 示例二

在以下示例中，运行 Amazon EC2 实例的 IAM 主体会创建并挂载一个使用 KMS 密钥加密的数据卷。此操作会生成多条 CloudTrail 日志记录。

创建卷时，Amazon EC2 将代表客户从 AWS KMS (`GenerateDataKeyWithoutPlaintext`) 获取加密的数据密钥。然后会创建一个授权 (`CreateGrant`)，从而允许它解密数据密钥。装载卷时，Amazon EC2 会调用 AWS KMS 来解密数据密钥 (`Decrypt`)。

Amazon EC2 实例的 `instanceId`、`"i-81e2f56c"` 将出现在 `RunInstances` 事件中。使用相同的实例 ID 来限定所创建授权的 `granteePrincipal` (`"111122223333:aws:ec2-infrastructure:i-81e2f56c"`) 以及 `Decrypt` 调用中的委托人的代入角色 (`"arn:aws:sts::111122223333:assumed-role/aws:ec2-infrastructure/i-81e2f56c"`)。

保护数据卷的 KMS 密钥的密钥 ARN、`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` 将出现在全部三个 AWS KMS 调用（`CreateGrant`、`GenerateDataKeyWithoutPlaintext` 和 `Decrypt`）中。

```
{
  "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"
    }
  ]
}
```


使用 Amazon 进行监控 CloudWatch

您可以 AWS KMS keys 使用 Amazon 进行监控 CloudWatch，该 AWS 服务可收集原始数据并将其处理 AWS KMS 为可读的、近乎实时的指标。这些数据会保存两周，从而使您能够访问历史信息，并更好地了解您 KMS 密钥的使用情况及其随时间推移而发生的变化。

您可以使用 Amazon CloudWatch 提醒您注意重要事件，例如以下事件。

- KMS 密钥中导入的密钥材料临近到期日期。
- 仍在使用待删除的 KMS 密钥。
- KMS 密钥中的密钥材料已自动轮换。
- KMS 密钥已删除。

您还可以创建一个 Amazon CloudWatch 警报，当您的请求率达到配额值的特定百分比时，提醒您。有关详情，请参阅AWS 安全博客 CloudWatch中的使用 Service Quotas 和 Amazon 管理您的 AWS KMS API 请求速率。

主题

- AWS KMS 指标和维度
- 查看 AWS KMS 指标
- 创建 CloudWatch 警报以监控 KMS 密钥

AWS KMS 指标和维度

AWS KMS 预定义了 Amazon CloudWatch 指标，使您可以更轻松地监控关键数据和创建警报。您可以使用 AWS Management Console 和 Amazon CloudWatch API 查看 AWS KMS 指标。

本部分列出了每个 AWS KMS 指标和每个指标的维度，并提供了一些基于这些指标和维度创建 CloudWatch 警报的基本指导。

> **Note**
>
> 维度组名称：
> 要在 Amazon CloudWatch 控制台中查看指标，请在 “指标” 部分，选择维度组名称。然后，您可以按 Metric name（指标名称）进行筛选。本主题包括各个 AWS KMS 指标的指标名称和维度组名称。

主题

- SecondsUntilKeyMaterialExpiration
- ExternalKeyStoreThrottle
- XksProxyCertificateDaysToExpire
- XksProxyCredentialAge
- XksProxyErrors
- XksExternalKeyManagerStates
- XksProxyLatency

SecondsUntilKeyMaterialExpiration

此指标跟踪 KMS 密钥中导入的密钥材料过期之前剩余的秒数。此指标仅对具有导入的密钥材料（密钥材料来源为 EXTERNAL）以及到期日期的 KMS 密钥有效。

使用此指标可以跟踪所导入密钥材料的到期之前剩余时间量。当该时间低于您定义的阈值时，您可能需要重新导入密钥材料并设置新的到期日期。SecondsUntilKeyMaterialExpiration 指标特定于

单个 KMS 密钥。您不能使用此指标来监控多个 KMS 密钥或将来可能创建的多个 KMS 密钥。有关创建 CloudWatch 警报以监控此指标的帮助，请参阅为导入的密钥材料过期创建 CloudWatch 警报。

该指标最有用的统计数据是 `Minimum`，它会告诉您指定统计周期内所有数据点的最小剩余时间。此指标的唯一有效单位是 `Seconds`。

维度组名称：Per-Key Metrics（各密钥指标）

`SecondsUntilKeyMaterialExpiration` 的维度

维度	描述；相关于 AWS
KeyId	每个 KMS 密钥的值。

ExternalKeyStoreThrottle

每个 AWS KMS 限制的外部密钥存储区中对 KMS 密钥进行加密操作的请求数（以 a 响应）。`ThrottlingException`此指标仅适用于外部密钥存储。

该`ExternalKeyStoreThrottle`指标仅适用于外部密钥存储中的 KMS 密钥，并且仅适用于加密操作和DescribeKey操作的请求。 AWS KMS 当请求速率超过外部密钥存储的自定义密钥库请求配额时，会限制这些请求。此指标不包括外部密钥存储代理或外部密钥管理器的节流。

使用此指标来查看和调整您的自定义密钥存储请求限额的值。如果此指标表明经常限制您对 AWS KMS 这些 KMS 密钥的请求，则可以考虑请求增加自定义密钥存储请求配额值。如需帮助，请参阅《服务限额用户指南》中的 申请上调限额。

如果您经常收到 `KMSInvalidStateException` 错误，其中包含一条说明请求“due to a very high request rate（由于请求率很高）”而被拒绝的消息，或者请求“because the external key store proxy did not respond in time（由于外部密钥存储代理未及时响应）”而被拒绝，则可能表明您的外部密钥管理器或外部密钥存储代理无法跟上当前的请求速率。如可能，请降低您的请求速率。您也可以考虑请求降低自定义密钥存储请求限额值。减少此配额值可能会增加限制（和`ExternalKeyStoreThrottle`指标值），但这表明 AWS KMS 在将多余的请求发送到您的外部密钥存储代理或外部密钥管理器之前，会迅速将其拒绝。要申请下调限额，请访问 AWS Support 中心 并创建工单。

维度组名称：Keystore Throttle Metrics（密钥存储限制指标）

维度	描述
CustomKeyStoreId	每个外部密钥存储的值。
KmsOperation	每个 AWS KMS API 操作的值。此指标仅适用于加密操作和对外部密钥存储中的 KMS 密钥的 `DescribeKey` 操作。
KeySpec	每个 KMS 密钥类型的值。对于外部密钥存储中 KMS 密钥的唯一支持的密钥规范是 SYMMETRIC_DEFAULT。

XksProxyCertificateDaysToExpire

距离您的外部密钥存储代理端点（`XksProxyUriEndpoint`）的 TLS 证书过期的天数。此指标仅适用于外部密钥存储。

使用此指标创建 CloudWatch 警报，告知您的 TLS 证书即将到期。证书过期后， AWS KMS 无法与外部密钥存储代理通信。在您续订证书之前，外部密钥存储中所有受 KMS 密钥保护的数据都将不可访问。

证书警报可防止证书过期，证书过期可能会影响您访问加密资源。设置警报，让您的组织有时间在证书过期之前续订证书。

维度组名称：XKS Proxy Certificate Metrics（XKS 代理证书指标）

维度	描述
CustomKeyStoreId	每个外部密钥存储的值。
CertificateName	TLS 证书中的主题名称（CN）。

XksProxyCredentialAge

自当前外部密钥存储代理身份验证凭证（`XksProxyAuthenticationCredential`）与外部密钥存储关联以来的天数。此计数从您在创建或更新外部密钥存储的过程中输入身份验证凭证时开始计算。此指标仅适用于外部密钥存储。

此值旨在提醒您身份验证凭证的使用时间。但是，由于我们从您将凭证与外部密钥存储关联时开始计算，而不是从您在外部密钥存储代理上创建身份验证凭证时开始计算，这可能无法准确地表明代理中的凭证使用时间。

使用此指标创建 CloudWatch 警报，提醒您轮换外部密钥存储代理身份验证凭据。

维度组名称：Per-Keystore Metrics（各密钥存储指标）

维度	描述
CustomKeyStoreId	每个外部密钥存储的值。

XksProxyErrors

与您的外部密钥存储代理 AWS KMS请求相关的异常数量。此计数包括外部密钥存储代理返回的异常 AWS KMS 以及外部密钥存储代理在 250 毫秒超时间隔 AWS KMS 内未响应时发生的超时错误。此指标仅适用于外部密钥存储。

使用此指标跟踪外部密钥存储中 KMS 密钥的错误率。这可显示最常见的错误，因此您可以确定工程工作的优先顺序。例如，产生较高不可重试错误率的 KMS 密钥，可能表明您的外部密钥存储配置存在问题。若要查看您的外部密钥存储配置，请参阅 查看外部密钥存储。若要编辑您的外部密钥存储设置，请参阅 编辑外部密钥存储属性。

维度组名称：XKS Proxy Error Metrics（XKS 代理错误指标）

维度	描述
CustomKeyStoreId	每个外部密钥存储的值。
KmsOperation	生成对 XKS 代理的请求的每个 AWS KMS API 操作的值。
XksOperation	每个外部密钥存储代理 API 操作的值。
KeySpec	每个 KMS 密钥类型的值。对于外部密钥存储中 KMS 密钥的唯一支持的密钥规范是 SYMMETRIC_DEFAULT。

维度	描述
ErrorType	值： • 可重试错误：可能是暂时性错误，例如网络错误。 • 不可重试错误：可能表示自定义密钥存储配置或外部组件存在问题。 • 不适用：请求成功；没有错误
Exception Name	值： • 异常名称 • 无：请求成功；没有错误

XksExternalKeyManagerStates

处于以下各个运行状况状态的外部密钥管理器实例的数量：`Active`、`Degraded` 和 `Unavailable`。此指标的信息来自与每个外部密钥存储关联的外部密钥存储代理。此指标仅适用于外部密钥存储。

以下是与外部密钥存储相关联的外部密钥管理器实例的运行状况。每个外部密钥存储代理都可能会使用不同的指标来衡量外部密钥管理器的运行状况。有关详细信息，请参阅外部密钥存储代理的相关文档。

- `Active`：外部密钥管理器运行正常。
- `Degraded`：外部密钥管理器运行状况不佳，但仍可以传输流量
- `Unavailable`：外部密钥管理器无法传输流量。

使用此指标创建 CloudWatch 警报，提醒您注意外部密钥管理器实例已降级和不可用。要确定哪些外部密钥管理器实例处于各个状态，请查阅您的外部密钥存储代理日志。

维度组名称：XKS External Key Manager Metrics（XKS 外部密钥管理器指标）

维度	描述
CustomKeyStoreId	每个外部密钥存储的值。

维度	描述
XksExternalKeyManagerState	每个运行状态的值。

XksProxyLatency

外部密钥存储代理响应 AWS KMS 请求所用的毫秒数。如果请求超时，则记录的值为 250 毫秒的超时限制。此指标仅适用于外部密钥存储。

使用此指标来评估您的外部密钥存储代理和外部密钥管理器的性能。例如，如果代理在加密和解密操作时经常超时，请咨询您的外部代理管理员。

响应缓慢还可能表示您的外部密钥管理器无法处理当前的请求流量。 AWS KMS 建议您的外部密钥管理器每秒能够处理多达 1800 个加密操作请求。如果您的外部密钥管理器无法处理每秒 1800 个请求的速率，请考虑请求降低自定义密钥存储中 KMS 密钥的请求限额。使用外部密钥存储中的 KMS 密钥进行加密操作的请求将采用快速失效机制，并出现节流异常，而不是由外部密钥存储代理或外部密钥管理器处理后拒绝。

维度组名称：XKS Proxy Latency Metrics（XKS 代理延迟指标）

维度	描述
CustomKeyStoreId	每个外部密钥存储的值。
KmsOperation	生成对 XKS 代理的请求的每个 AWS KMS API 操作的值。
XksOperation	每个外部密钥存储代理 API 操作的值。
KeySpec	每个 KMS 密钥类型的值。对于外部密钥存储中 KMS 密钥的唯一支持的密钥规范是 SYMMETRIC_DEFAULT。

查看 AWS KMS 指标

您可以使用 AWS Management Console 和 Amazon CloudWatch API 查看 AWS KMS 指标。

使用 CloudWatch 控制台查看指标

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 如果需要，可以更改区域。从导航栏中，选择 AWS 资源所在的区域。
3. 在导航窗格中，依次选择指标、所有指标。
4. 在 Browse（浏览）选项卡上，搜索 KMS，然后选择 KMS。
5. 选择要查看的指标维度组名称。

   例如，对于 SecondsUntilKeyMaterialExpiration 指标，请选择 Per-Key Metrics（各密钥指标）。
6. 要获取指标值的图表，请选择指标名称，然后选择 Add to graph。要将折线图转换为值，请选择 Line（折线），然后选择 Number（数字）。

使用亚马逊 CloudWatch API 查看指标

要使用 CloudWatch API 查看 AWS KMS 指标，请发送Namespace设置为的ListMetrics请求AWS/KMS。以下示例说明如何使用 AWS Command Line Interface (AWS CLI) 执行该操作。

```
$  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"
                }
            ]
        }
    ]
}
```

创建 CloudWatch 警报以监控 KMS 密钥

您可以根据 AWS KMS 指标创建 Amazon CloudWatch 警报。当指标值超过警报配置中指定的阈值时，警报会发送一封电子邮件。警报可以将电子邮件消息发送到 Amazon Simple Notification Service (Amazon SNS) 主题或 Amazon EC2 Auto Scaling 策略。有关 CloudWatch 警报的详细信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch 警报

针对到期的导入密钥材料创建警报

您可以使用该SecondsUntilKeyMaterialExpiration指标创建 CloudWatch 警报，在 KMS 密钥中导入的密钥材料即将过期时通知您。

当您将密钥材料导入 KMS 密钥中时，可以选择性地指定密钥材料的到期时间。当密钥材料过期时，AWS KMS 会删除密钥材料，KMS 密钥将无法使用。要再次使用该 KMS 密钥，您必须重新导入密钥材料。

有关说明，请参阅为导入的密钥材料过期创建 CloudWatch 警报。

创建待删除 KMS 密钥的使用情况的警报

当您为 KMS 密钥计划删除时， AWS KMS 会强制执行一段等待期，然后再删除 KMS 密钥。您可以利用这段等待期来确保现在或将来都不需要 KMS 密钥。您还可以配置 CloudWatch警报，以便在等待期

间有人或应用程序尝试在加密操作中使用 KMS 密钥时向您发出警报。如果您收到来自此类告警的通知，您可能需要取消删除 KMS 密钥。

有关说明，请参阅创建检测待删除 KMS 密钥的使用的警报。

创建警报以监控外部密钥存储

您可以根据外部密钥存储和外部密钥存储中的 KMS 密钥的指标创建 CloudWatch 警报。

例如，我们建议您设置 CloudWatch 警报，在外部密钥存储的 TLS 证书即将过期（XksProxyCertificateDaysToExpire）、您的外部密钥存储代理报告您的外部密钥管理器实例处于降级或不可用状态时（XksProxyHsmStates）通知您。

有关说明，请参阅 监控外部密钥存储。

使用 Amazon 进行监控 EventBridge

您可以使用亚马逊 EventBridge （前身为 Amazon CloudWatch Events）提醒您注意您的 KMS 密钥生命周期中的以下重要事件。

- KMS 密钥中的密钥材料已自动轮换。
- KMS 密钥中已导入的密钥材料到期。
- 计划删除的 KMS 密钥已被删除。

AWS KMS与 Amazon 集成 EventBridge ，可在影响您的 KMS 密钥的重要事件时通知您。每个事件都以 JSON（JavaScript对象表示法）表示，包括事件名称、事件发生的日期和时间以及受影响的事件。您可以收集这些事件，并设立将事件路由到一个或多个目标（如 AWS Lambda 函数、Amazon SNS 主题、Amazon SQS 队列、Amazon Kinesis Data Streams 中的流或内置目标）的规则。

有关 EventBridge 与其他类型的事件（包括记录读/写 API 请求AWS CloudTrail时发出的事件）一起使用的更多信息，请参阅 A ma EventBridge zon 用户指南。

以下主题描述了AWS KMS生成 EventBridge 的事件。

KMS CMK 轮换

AWS KMS 支持自动轮换对称加密 KMS 密钥中的密钥材料。每年进行密钥材料轮换对于客户托管密钥是可选项。AWS 托管式密钥 的密钥材料每年自动轮换一次。

每当AWS KMS轮换密钥材料时，它都会向发送一个KMS CMK Rotation事件。 EventBridge AWS KMS尽力生成此事件。

以下是该事件的示例。

```
{
  "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"
  }
}
```

KMS 导入的密钥材料过期

当您将密钥材料导入 KMS 密钥中时，您可以选择性地指定密钥材料的过期时间。当密钥材料过期时，AWS KMS会删除密钥材料并将相应KMS Imported Key Material Expiration的事件发送到 EventBridge。 AWS KMS尽力生成此事件。

以下是该事件的示例。

```
{
  "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"
  }
```

```
}
```

KMS CMK 删除

当您为 KMS 密钥计划删除时，AWS KMS 会强制执行一段等待期，然后再删除 KMS 密钥。等待期结束后，AWS KMS删除 KMS 密钥并向发送KMS CMK Deletion事件 EventBridge。 AWS KMS保证此 EventBridge 事件。由于重试，它可能会在几秒钟内生成多个删除同一 KMS 密钥的事件。

以下是该事件的示例。

```
{
  "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"
  }
}
```

使用创建 AWS KMS 资源 AWS CloudFormation

AWS Key Management Service 与一项服务集成 AWS CloudFormation，该服务可帮助您对 AWS 资源进行建模和设置，从而减少创建和管理资源和基础架构所花费的时间。您可以创建描述 KMS 密钥和别名的模板， AWS CloudFormation 将为您预置和配置这些资源。有关 AWS KMS 支持的信息 CloudFormation，请参阅《AWS CloudFormation 用户指南》中的 KMS 资源类型参考。

使用时 AWS CloudFormation，您可以重复使用模板来一致且重复地设置 AWS KMS 资源。只需描述一次您的资源，然后在多个 AWS 账户 区域中一遍又一遍地配置相同的资源。

要为和其他 AWS 服务配置 AWS KMS 和配置资源，必须了解AWS CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述了您要在 AWS CloudFormation 堆栈中配置的资源。如果你不熟悉 JSON 或 YAML，可以使用 D AWS CloudFormation esigner 来帮助你开始使用 AWS CloudFormation 模板。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的什么是 AWS CloudFormation Designer？。

区域

AWS KMS CloudFormation 所有支持的区域 AWS CloudFormation 都支持资源。

AWS KMSAWS CloudFormation 模板中的资源

AWS KMS 支持以下 AWS CloudFormation 资源。

- 该AWS::KMS::Key资源在中指定了 KMS 密钥 AWS Key Management Service。您可以使用此资源创建对称加密 KMS 密钥、用于加密或签名的非对称 KMS 密钥以及对称 HMAC KMS 密钥。您可以使用AWS::KMS::Key创建所有支持类型的多区域主密钥。要复制多区域密钥，请使用 AWS::KMS::ReplicaKey 资源。
- AWS::KMS::Alias 创建一个别名并将其与 KMS 密钥关联。KMS 密钥可以在模板中定义，也可以由其他机制创建。
- AWS::KMS::ReplicaKey 创建一个多区域副本密钥。要创建多区域主密钥，请使用 AWS::KMS::Key 资源。您不能使用此资源复制具有导入密钥材料的多区域密钥。有关多区域密钥的详细信息，请参阅 中的多区域密钥 AWS KMS。

> **Important**
>
> 如果您更改现有 KMS 密钥的 KeyUsage、KeySpec 或 MultiRegion 属性的值，则会安排删除现有 KMS 密钥，并使用指定值创建新的 KMS 密钥。
> 安排删除后，现有 KMS 密钥将无法使用。如果您不取消计划删除之外的现有 KMS 密钥，则删除 KMS 密钥后 AWS CloudFormation，在现有 KMS 密钥下加密的所有数据都将无法恢复。

模板创建的 KMS 密钥是您的实际资源 AWS 账户。授权委托人可以使用模板、 AWS KMS 控制台或 AWS KMS API 使用和管理模板创建的 KMS 密钥。当您从模板中删除 KMS 密钥时，系统将使用您提前指定的等待时间来计划删除 KMS 密钥。

例如，您可以使用 AWS CloudFormation 模板创建包含密钥策略、密钥规范、密钥用法、别名和您喜欢的标签的测试 KMS 密钥。您可以通过测试套件运行它，查看结果，然后使用模板计划删除测试密钥。稍后，您可以再次运行模板以创建具有相同属性的测试密钥。

或者，您可以使用 AWS CloudFormation 模板来定义满足您的业务规则和安全标准的特定 KMS 密钥配置。然后，您可以在需要创建 KMS 密钥的任何时候使用该模板。对于密钥配置错误，您无需担心。如果您的首选配置发生了更改，您可以使用模板更新 KMS 密钥。例如，您可以使用模板轻松地以编程方式对模板定义的所有 KMS 密钥启用自动密钥轮替。

有关 AWS KMS 资源的更多信息（包括示例），请参阅《AWS CloudFormation 用户指南》中的 KMS 资源类型参考。

了解更多关于 AWS CloudFormation

要了解更多信息 AWS CloudFormation，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation API 引用
- AWS CloudFormation 命令行界面用户指南

删除 AWS KMS keys

删除 AWS KMS key具有破坏性和潜在危险性。这将删除密钥材料以及与 KMS 密钥关联的所有元数据，并且不可撤销。删除 KMS 密钥后，您不能再解密用该密钥加密的数据，这意味着该数据将无法恢复。（唯一的例外是多区域副本密钥以及带有导入密钥材料的非对称密钥和 HMAC KMS 密钥。）对于用于加密的非对称 KMS 密钥来说，这种风险非常大，在这种情况下，用户可以在没有警告或错误的情况下继续生成带有公钥的加密文字，而这些加密文字在从 AWS KMS 中删除私钥后无法解密。

只有当您确定不再需要使用 KMS 密钥时，才能将其删除。如果您不确定，请考虑禁用 KMS 密钥，而不是将其删除。您可以重新启用被禁用的 KMS 密钥，取消 KMS 密钥的计划删除，但无法恢复已删除的 KMS。

您只能安排删除客户托管的密钥。您无法删除 AWS 托管式密钥或 AWS 拥有的密钥。

在删除 KMS 密钥之前，您可能想要了解使用该 KMS 密钥加密了多少密文。AWS KMS 不会存储此信息，也不会存储任何密文。要获取此信息，您必须确定 KMS 密钥的过去使用情况。如需帮助，请转到确定 KMS 密钥的过去使用情况。

AWS KMS 从不会删除您的 KMS 密钥，除非您明确安排删除它们并且强制的等待期到期。

但是，您可能会出于以下一个或多个原因而选择删除 KMS 密钥：

- 完成不再需要的 KMS 密钥的密钥生命周期
- 避免因维护不用的 KMS 密钥而产生的管理开销和成本
- 减少计入您的 KMS 密钥资源配额的 KMS 密钥数量

> **Note**
>
> 如果关闭您的 AWS 账户，您的 KMS 密钥将变得无法访问，您也不必再为它们付费。

在您计划删除 KMS 密钥且 KMS 密钥被实际删除时，AWS KMS 会将一个条目记录在 AWS CloudTrail 日志中。

有关删除多区域主密钥和副本密钥的信息，请参阅 删除多区域密钥。

主题

关于等待期限

因为删除 KMS 密钥具有破坏性且存在潜在危险，所以 AWS KMS 要求您将等待期限设置为 7-30 天。默认的等待期限为 30 天。

但是，实际等待期限可能最多比您计划的时间长 24 小时。要获取删除 KMS 密钥的实际日期和时间，请使用DescribeKey操作。或者在 AWS KMS 控制台中的 KMS 密钥详细信息页面的 General configuration（常规配置）部分中，参阅计划删除日期。请务必记下时区。

在等待期限内，KMS 密钥状态和密钥状态为 Pending deletion（等待删除）。

- 待删除的 KMS 密钥不能用于任何加密操作。
- AWS KMS 不会为待删除的 KMS 密钥轮换备用密钥。

等待期结束后，AWS KMS 会删除 KMS 密钥、其别名以及所有相关的 AWS KMS 元数据。

计划删除 KMS 密钥可能不会立即影响由 KMS 密钥加密的数据密钥。有关更多信息，请参阅 不可用的 KMS 密钥如何影响数据密钥。

请利用这段等待期来确保现在或将来都不需要 KMS 密钥。您可以配置 Amazon CloudWatch 警报，以便在等待期间有人或应用程序尝试使用 KMS 密钥时向您发出警告。要恢复 KMS 密钥，您可以在等待期限结束前取消密钥删除。等待期限结束后，将无法取消密钥删除，AWS KMS 将删除 KMS 密钥。

删除非对称 KMS 密钥

获得授权的用户可以删除对称 KMS 密钥或非对称 KMS 密钥。对于两种密钥类型，计划删除 KMS 密钥的过程是相同的。但是，由于非对称 KMS 密钥的公有密钥可以下载并在 AWS KMS 外部使用，因此操作会带来重大的额外风险，尤其是对于用于加密的非对称 KMS 密钥（密钥用法为 ENCRYPT_DECRYPT）。

- 您在计划删除 KMS 密钥时，KMS 密钥的密钥状态将更改为 Pending deletion（等待删除），并且 KMS 密钥将无法用在加密操作中。但是，计划删除对 AWS KMS 外部的公有密钥没有影响。持有公有密钥的用户可以继续使用该密钥加密消息。他们不会收到密钥状态已更改的任何通知。除非删除取消，否则使用公有密钥创建的密文将无法解密。
- 告警、日志以及其他检测试图使用等待删除的 KMS 密钥的策略，无法检测到 AWS KMS 外部公有密钥的使用。
- KMS 密钥删除后，涉及该 KMS 密钥的所有 AWS KMS 操作都将失败。但是，持有公有密钥的用户可以继续使用该密钥加密消息。这些密文将无法解密。

如果您必须删除密钥用法为的非对称 KMS 密钥ENCRYPT_DECRYPT，请使用您的 CloudTrail 日志条目来确定公有密钥是否已下载和共享。如果有，请验证该公有密钥是否在 AWS KMS 外部使用。然后，考虑禁用 KMS 密钥而不是将其删除。

对于具有导入密钥材料的非对称 KMS 密钥，可缓解删除非对称 KMS 密钥所带来的风险。有关更多信息，请参阅 删除具有导入密钥材料的 KMS 密钥。

删除多区域密钥

获得授权的用户可以计划删除多区域主密钥和副本密钥。然而，AWS KMS 将不会删除具有副本密钥的多区域主键。此外，只要主键存在，您就可以重新创建已删除的多区域副本密钥。有关更多信息，请参阅 删除多区域密钥。

删除具有导入密钥材料的 KMS 密钥

授权用户可以计划删除具有导入密钥材料的 KMS 密钥。此操作会永久删除 KMS 密钥及其密钥材料以及与 KMS 密钥关联的所有元数据。

即使您有密钥材料的副本，您也无法创建新的对称加密 KMS 密钥来解密具有导入密钥材料的已删除对称加密密钥的加密文字。但是，如果您拥有密钥材料，则可以有效地重新创建具有导入密钥材料的非对称 KMS 密钥或 HMAC KMS 密钥。有关更多信息，请参阅 删除具有导入密钥材料的 KMS 密钥。

控制密钥删除所需的权限

如果您使用 IAM policy 允许 AWS KMS 权限，则具有 AWS 管理员访问权限（`"Action": "*"`）或 AWS KMS 完全访问权限（`"Action": "kms:*"`）的 IAM 身份，都已被允许计划和取消 KMS 密钥的密钥删除。要允许密钥管理员安排和取消密钥策略中的密钥删除，请使用 AWS KMS 控制台或 AWS KMS API。

通常，只有密钥管理员才有权安排或取消密钥删除。但是，您可以通过向密钥策略或 IAM policy 添加 `kms:ScheduleKeyDeletion` 和 `kms:CancelKeyDeletion` 权限，将这些权限授予其他 IAM 身份。您还可以使用`kms:ScheduleKeyDeletionPendingWindowInDays`条件键进一步限制委托人可以在请求`PendingWindowInDays`参数中指定的值。ScheduleKeyDeletion

允许密钥管理员安排和取消密钥删除（控制台）。

授予密钥管理员计划和取消密钥删除的权限。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择要更改其权限的 KMS 密钥的别名或密钥 ID。
5. 选择 key policy（密钥策略）选项卡。
6. 下一步操作具体取决于密钥策略的默认视图和策略视图。只有在使用默认控制台密钥策略时，默认视图才可用。否则，仅策略视图可用。

   当默认视图可用时，Key policy（密钥策略）选项卡上会出现 Switch to policy view（切换到策略视图）或 Switch to default view（切换到默认视图）按钮。

   - 在默认视图中：

- 在 Key deletion（密钥删除）下，选择 Allow key administrators to delete this key（允许密钥管理员删除此密钥）。

- 在策略视图中：

  a. 选择编辑。

  b. 在密钥管理员的策略语句中，向 `Action` 元素添加 `kms:ScheduleKeyDeletion` 和 `kms:CancelKeyDeletion` 权限。

```
{
  "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. 选择保存更改。

允许密钥管理员计划和取消密钥删除的权限（AWS CLI）。

您可以使用 AWS Command Line Interface来添加计划和取消密钥删除所需的权限。

添加计划和取消密钥删除所需的权限

1. 使用 `aws kms get-key-policy` 命令检索现有的密钥策略，然后将策略文档保存到文件中。

2. 在您的首选文本编辑器中打开策略文档。在密钥管理员的策略语句中，添加 `kms:ScheduleKeyDeletion` 和 `kms:CancelKeyDeletion` 权限。以下示例显示了一个具有这两项权限的策略语句：

```
{
  "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. 使用 `aws kms put-key-policy` 命令将密钥策略应用于 KMS 密钥。

计划和取消密钥删除

以下过程介绍如何通过 AWS Management Console、AWS CLI 和 AWS SDK for Java 在 AWS KMS 中计划密钥删除和取消单区域 AWS KMS keys（KMS 密钥）的密钥删除。

有关计划删除多区域密钥的信息，请参阅 删除多区域密钥。

> **Warning**
>
> 删除 KMS 密钥具有破坏性和潜在危险性。只有当您确定不再需要使用 KMS 密钥并且将来也不再需要了，才能继续删除操作。如果您不确定，则应禁用 KMS 密钥，而不是将其删除。

在删除 KMS 密钥之前，您必须具有执行这一操作的权限。有关向密钥管理员授予这些权限的信息，请参阅 控制密钥删除所需的权限。您也可以使用 kms:ScheduleKeyDeletionPendingWindowInDays 条件键进一步限制等待时间，例如强制规定最短等待时间。

在您计划删除 KMS 密钥且 KMS 密钥被实际删除时，AWS KMS 会将一个条目记录在 AWS CloudTrail 日志中。

计划和取消密钥删除（控制台）

在 AWS Management Console 中，您可以一次安排和取消删除多个 KMS 密钥。

计划密钥删除

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。

   您无法安排删除 AWS 托管式密钥或 AWS 拥有的密钥。
4. 选中想要删除的 KMS 密钥旁边的复选框。
5. 依次选择 Key actions (密钥操作)、Schedule key deletion (计划密钥删除)。
6. 阅读并考虑警告，以及有关在等待期限内取消删除的信息。如果决定取消删除，请在页面底部选择 Cancel（取消）。
7. 对于 Waiting period (in days) (等待期限(天))，键入一个介于 7 和 30 之间的天数。
8. 查看正在删除的 KMS 密钥。
9. 选中 Confirm you want to schedule this key for deletion in ***<number of days>*** days（确认您要计划在 n 天后删除此密钥）旁的复选框。
10. 选择计划删除。

KMS 密钥状态将更改为等待删除。

取消密钥删除

1. 从 https://console.aws.amazon.com/kms 打开 AWS KMS 控制台。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。

4. 选中想要恢复的 KMS 密钥旁边的复选框。
5. 依次选择 Key actions (密钥操作)、Cancel key deletion (取消密钥删除)。

KMS 密钥状态将从待删除更改为已禁用。要使用 KMS 密钥，您必须将其启用。

计划和取消密钥删除（AWS CLI）

使用 `aws kms schedule-key-deletion` 命令安排删除客户托管的密钥，如以下示例所示。

您无法计划删除 AWS 托管式密钥或 AWS 拥有的密钥。

```
$ aws kms schedule-key-deletion --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --
pending-window-in-days 10
```

使用成功后，AWS CLI 将返回与以下示例中显示的输出类似的输出：

```
{
    "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "DeletionDate": 1598304792.0,
    "KeyState": "PendingDeletion",
    "PendingWindowInDays": 10
}
```

从 使用 `aws kms cancel-key-deletion`AWS CLI 命令取消密钥删除，如以下示例所示。

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

使用成功后，AWS CLI 将返回与以下示例中显示的输出类似的输出：

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

KMS 密钥的状态将从待删除更改为已禁用。要使用 KMS 密钥，您必须将其启用。

计划和取消密钥删除（AWS SDK for Java）

以下示例演示了如何使用 AWS SDK for Java 安排删除客户托管的密钥。此示例要求您在此之前将 `AWSKMSClient` 实例化为 `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);
```

以下示例演示如何使用AWS SDK for Java取消密钥删除。此示例要求您在此之前将 `AWSKMSClient` 实例化为 `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);
```

KMS 密钥的状态将从待删除更改为已禁用。要使用 KMS 密钥，您必须将其启用。

创建检测待删除 KMS 密钥的使用的警报

您可以结合亚马逊 CloudWatch 日志和亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 的功能来创建 CloudWatch 亚马逊警报，当您的账户中有人尝试使用待删除的 KMS 密钥时，该警报会通知您。AWS CloudTrail如果您收到此通知，则可能要取消删除该 KMS 密钥并重新考虑删除它的决定。

以下过程将创建一个警报，每当向 CloudTrail 日志文件写入 “*Key ARN* `is pending deletion`” 错误消息时，该警报就会通知您。此错误消息指示有人或应用程序尝试在加密操作中使用该 KMS 密钥。由于通知链接至错误消息，因此，当您使用待删除的 KMS 密钥中允许的 API 操作时（例如 `ListKeys`、`CancelKeyDeletion` 和 `PutKeyPolicy`），不会触发该通知。要查看返回此错误消息的 AWS KMS API 操作的列表，请参阅密 AWS KMS 钥的关键状态。

您收到的通知电子邮件不会列出 KMS 密钥或加密操作。可在 CloudTrail 日志中找到此信息。电子邮件会报告警报状态已从 OK (正常) 变为 Alarm (警报)。有关 CloudWatch警报和状态变化的更多信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch警报。

> **Warning**
>
> 此 Amazon CloudWatch 警报无法检测到在之外使用非对称 KMS 密钥的AWS KMS公钥。有关删除用于公有密钥加密的非对称 KMS 密钥的特殊风险的详细信息，包括创建无法解密的密文，请参阅 删除非对称 KMS 密钥。

主题

CloudWatch 警报要求

在创建 CloudWatch 警报之前，您必须创建AWS CloudTrail跟踪并配置为将 CloudTrail 日志文件传输 CloudTrail 到 Amazon Lo CloudWatch gs。您还需要针对警报通知使用 Amazon SNS 主题。

- 创建 CloudTrail 跟踪。

  CloudTrail 在您创建账户AWS 账户时会自动在您的账户上启用。但是，要持续记录账户中的事件（包括 AWS KMS 的事件），请创建跟踪。

- 配置 CloudTrail 以传送您的日志文件 CloudWatch 日志。

  配置将 CloudTrail 日志文件传送到 CloudWatch 日志。这样， CloudWatch 日志就可以监控尝试使用待删除的 KMS 密钥的 AWS KMS API 请求的日志。

- 创建 Amazon SNS 主题。

  当您的警报触发时，它会通过向 Amazon Simple Notification Service (Amazon SNS) 主题中的电子邮件地址发送电子邮件来通知您。

创建 CloudWatch 警报

在此过程中，您将创建一个 CloudWatch 日志组指标筛选器，用于查找待删除异常的实例。然后，根据日志组指标创建 CloudWatch 警报。有关日志组指标筛选条件的信息，请参阅 Amazon Logs 用户指南中的使用筛选条件从 CloudWatch 日志事件创建指标。

1. 创建用于解析 CloudTrail 日志的 CloudWatch 指标筛选器。

使用以下必填值，按照为日志组创建指标筛选条件中的说明进行操作。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
筛选条件模式	`{ $.eventSource = kms* && $.errorMessage = "* is pending deletion."}`
指标值	1

2. 根据您在步骤 1 中创建的指标筛选器创建 CloudWatch 警报。

   使用以下必填值按照基于日志组指标筛选器创建 CloudWatch 警报中的说明进行操作。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
指标筛选条件	您在步骤 1 中创建的指标筛选条件名称。
阈值类型	静态
Conditions	当 *metric-name* 大于 1 时
待报警的数据点	1 / 1
缺失数据处理	将缺失的数据作为好处理 (未超出阈值)

完成此过程后，每当您的新 CloudWatch警报进入ALARM状态时，您都会收到一条通知。如果您收到此警报的通知，可能意味着仍然需要计划删除的 KMS 密钥来加密或解密数据。在这种情况下，请取消删除 KMS 密钥并重新考虑删除它的决定。

确定 KMS 密钥的过去使用情况

在删除 KMS 密钥之前，您可能想要了解使用该 KMS 密钥加密了多少密文。AWS KMS 不会存储此信息，也不会存储任何密文。了解 KMS 密钥的过去使用情况可帮助您决定将来是否需要此 KMS 密钥。本主题建议多种有助于您确定 KMS 密钥的过去使用情况的策略。

> **Warning**
>
> 这些用于确定过去使用情况和实际使用情况的策略仅对 AWS 用户和 AWS KMS 操作有效。它们无法检测到 AWS KMS 外部非对称 KMS 密钥的公有密钥的使用情况。有关删除用于公有密钥加密的非对称 KMS 密钥的特殊风险的详细信息，包括创建无法解密的密文，请参阅 删除非对称 KMS 密钥。

主题

检查 KMS 密钥权限以确定潜在使用范围

通过确定当前有权访问 KMS 密钥的对象，可帮助您确定 KMS 密钥的广泛使用程度以及是否仍然需要此 KMS 密钥。要了解如何确定当前有权访问 KMS 密钥的对象，请转到 确定对 AWS KMS keys 的访问权限。

检查 AWS CloudTrail 日志以确定实际使用情况

您或许能够使用 KMS 密钥使用情况历史记录来帮助确定是否使用特定 KMS 密钥加密了密文。

所有 AWS KMS API 活动都记录在 AWS CloudTrail 日志文件中。如果您在 KMS 密钥所在的区域创建了 CloudTrail 跟踪，则可以检查 CloudTrail 日志文件以查看特定 KMS 密钥的所有 AWS KMS API 活动的历史记录。如果您没有跟踪，您仍然可以在活动历史记录中查看最近的事件。CloudTrail 有关如何AWS KMS使用的详细信息 CloudTrail，请参阅使用记录 AWS KMS API 调用 AWS CloudTrail。

以下示例显示了使用 KMS 密钥保护存储在亚马逊简单存储服务 (Amazon S3) Service 中的对象时生成的 CloudTrail 日志条目。在本示例中，对象通过使用 KMS 密钥 (SSE-KMS) 的服务器端加密保护数据上传到 Amazon S3 中。当您使用 SSE-KMS 将对象上传到 Amazon S3 时，需指定用于保护对象的 KMS 密钥。Amazon S3 使用该AWS KMSGenerateDataKey操作请求对象的唯一数据密钥，此请求事件 CloudTrail 使用类似于以下内容的条目登录：

```
{
  "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"
}
```

当您之后从 Amazon S3 下载此对象时，Amazon S3 会向 AWS KMS 发送 `Decrypt` 请求，以使用指定的 KMS 密钥解密对象的数据密钥。执行此操作时，您的 CloudTrail 日志文件将包含类似于以下内容的条目：

```
{
  "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 将记录所有 AWS KMS API 活动。通过评估这些日志条目，您可以确定特定 KMS 密钥的过去使用情况，这将有助于您确定是否需要将其删除。

要查看 AWS KMS API 活动如何在 CloudTrail 日志文件中显示的更多示例，请访问使用记录 AWS KMS API 调用 AWS CloudTrail。有关更多信息， CloudTrail 请访问AWS CloudTrail用户指南。

密 AWS KMS 钥的关键状态

AWS KMS key 始终有一个关键状态。KMS 密钥及其环境上的操作可以瞬时改变该密钥状态，或者直到其他操作更改其密钥状态为止。

本节中的表格显示了密钥状态如何影响 AWS KMS API 操作的调用。由于其密钥状态，对 KMS 密钥执行的操作预计会成功 (#)，失败 (X) ，或者仅在某些条件下成功 (?)。对于已导入密钥材料的 KMS 密钥，结果通常不同。

此表仅包括使用现有 KMS 密钥的 API 操作。省略了其他操作 ListKeys，例如CreateKey和。

主题

- 密钥状态和 KMS 密钥类型
- 密钥状态表

密钥状态和 KMS 密钥类型

KMS 密钥的类型决定了它可以具有的密钥状态。

- 所有 KMS 密钥都可以处于 `Enabled`、`Disabled` 和 `PendingDeletion` 状态。
- 大多数 KMS 密钥都在 `Enabled` 状态下创建。带导入的密钥材料的密钥在 `PendingImport` 状态下创建。
- `PendingImport` 状态仅适用于具有导入的密钥材料的 KMS 密钥。
- `Unavailable` 状态仅适用于自定义密钥存储中的 KMS 密钥。密钥库中的 KMS AWS CloudHSM 密钥是指`Unavailable`故意断开自定义密钥存储与其 AWS CloudHSM 集群的连接。当自定义密钥存储有意与其外部密钥存储代理断开连接时，外部密钥存储中的 KMS 密钥为 `Unavailable`。您可查看和管理不可用的 KMS 密钥，但无法在加密操作中使用它们。

自定义密钥中的 KMS 密钥的密钥状态不受其备用密钥的更改的影响。密钥存储中的 KMS AWS CloudHSM 密钥不受 AWS CloudHSM 集群中关联密钥材料更改的影响。外部密钥存储中的 KMS 密钥不受外部密钥管理器中其外部密钥的更改的影响。如果禁用或删除备用密钥，KMS 密钥状态不会改变，但使用 KMS 密钥的加密操作会失败。

- `Creating`、`Updating` 和 `PendingReplicaDeletion` 密钥状态仅适用于多区域密钥。
  - 多区域副本密钥在创建时处于临时 `Creating` 密钥状态。ReplicateKey操作完成后，此过程可能仍在进行中。复制过程完成后，副本密钥处于 `Enabled` 或 `PendingImport` 状态。
  - 多区域密钥在主区域正在更新时处于临时的 `Updating` 密钥状态。UpdatePrimaryRegion操作完成后，此过程可能仍在进行中。更新过程完成后，主密钥和副本密钥将恢复 `Enabled` 密钥状态。
  - 当您计划删除具有副本密钥的多区域主键时，主键处于 `PendingReplicaDeletion` 状态，直到其所有的副本密钥都被删除。然后，它的密钥状态更改为 `PendingDeletion`。有关更多信息，请参阅 删除多区域密钥。

密钥状态表

下表显示 KMS 密钥的密钥状态如何影响 AWS KMS 操作。

编号脚注的说明 ([n]) 处于本主题的末尾。

> **Note**
>
> 您可能需要水平或垂直滚动才能查看此表中的所有数据。

API	已启用	已禁用	待删除 待删除副本	待导入	不可用	Creating	Updating
CancelKeyDeletion	✗ [4]	✗ [4]	✓	✗ [4]	✗ [4]、[13]	✗ [4]	✗ [4]
CreateAlias	✓	✓	✗	✓	✓	✓	✓

API	已启用	已禁用	待删除 待删除副本	待导入	不可用	Creating	Updating
			[3]				
CreateGrant	✓	⊗ [1]	⊗ [2] 或 [3]	⊗ [5]	✓	⊗ [14]	✓
Decrypt	✓	⊗ [1]	⊗ [2] 或 [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
DeleteAlias	✓	✓	✓	✓	✓	✓	✓
DeleteImportedKeyMaterial	✓ [9]	✓ [9]	✓ [9]	✓ (无影响)	不适用	⊗ [14]	⊗ [15]
DescribeKey	✓	✓	✓	✓	✓	✓	✓
DisableKey	✓	✓	⊗ [3]	⊗ [5]	✓ [12]	⊗ [14]	⊗ [15]
DisableKeyRotation	? [7]	⊗ [1] 或 [7]	⊗ [3] 或 [7]	⊗ [6]	⊗ [7]	⊗ [14]	? [7]
EnableKey	✓	✓	⊗ [3]	⊗ [5]	✓ [12]	⊗ [14]	⊗ [15]

API	已启用	已禁用	待删除 待删除副本	待导入	不可用	Creating	Updating
EnableKeyRotation	[7]	[1] 或 [7]	[3] 或 [7]	[6]	[7]	[14]	[7]
Encrypt	✓	[1]	[2] 或 [3]	[5]	[11]	[14]	✓
GenerateDataKey	✓	[1]	[2] 或 [3]	[5]	[11]	[14]	✓
GenerateDataKeyPair	✓	[1]	[2] 或 [3]	[5]	[11]	[14]	✓
GenerateDataKeyPairWithoutPlaintext	✓	[1]	[2] 或 [3]	[5]	[11]	[14]	✓
GenerateDataKeyWithoutPlaintext	✓	[1]	[2] 或 [3]	[5]	[11]	[14]	✓
GenerateMac	✓	[1]	[2] 或 [3]	不适用	不适用	[14]	✓

API	已启用	已禁用	待删除 待删除副本	待导入	不可用	Creating	Updating
GetKeyPolicy							
GetKeyRotationStatus	 [7]	 [7]	 [7]	 [6]	 [7]	 [7]	 [7]
GetParametersForImport	 [9]	 [9]	 [8] 或 [9]		 [9]	 [14]	 [15]
GetPublicKey		 [1]	 [2] 或 [3]	不适用	不适用	 [14]	
ImportKeyMaterial	 [9]	 [9]	 [8] 或 [9]		 [9]	 [14]	
ListAliases							
ListGrants							
ListKeyPolicies							
ListKeyRotations	 [7]	 [7]	 [7]	 [6]	 [7]	 [7]	 [7]

API	已启用	已禁用	待删除 待删除副本	待导入	不可用	Creating	Updating
ListResourceTags	✓	✓	✓	✓	✓	✓	✓
PutKeyPolicy	✓	✓	✓	✓	✓	✓	✓
ReEncrypt	✓	⊗ [1]	⊗ [2] 或 [3]	⊗ [5]	⊗ [11]	⊗ [14]	✓
ReplicateKey	✓	⊗ [1]	⊗ [2] 或 [3]	⊗ [5]	不适用	⊗ [14]	⊗ [15]
RetireGrant	✓	✓	✓	✓	✓	✓	✓
RevokeGrant	✓	✓	✓	✓	✓	✓	✓
RotateKeyOnDemand	? [7]	⊗ [1] 或 [7]	⊗ [3] 或 [7]	⊗ [6]	⊗ [7]	⊗ [14]	? [7]
ScheduleKeyDeletion	✓	✓	⊗ [3]	✓	✓	✓	⊗ [15]
Sign	✓	⊗ [1]	⊗ [2] 或 [3]	不适用	不适用	⊗ [14]	✓

API	已启用	已禁用	待删除 待删除副本	待导入	不可用	Creating	Updating
TagResource	✓	✓	⊗ [3]	✓	✓	✓	✓
UntagResource	✓	✓	⊗ [3]	✓	✓	✓	✓
UpdateAlias	✓	✓	? [10]	✓	✓	✓	✓
UpdateKeyDescription	✓	✓	⊗ [3]	✓	✓	✓	✓
UpdatePrimaryRegion	✓	⊗ [1]	⊗ [2] 或 [3]	⊗ [5]	不适用	⊗ [14]	✓
验证	✓	⊗ [1]	⊗ [2] 或 [3]	不适用	不适用	⊗ [14]	✓
VerifyMac	✓	⊗ [1]	⊗ [2] 或 [3]	不适用	不适用	⊗ [14]	✓

表详细信息

- [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] 如果 KMS 密钥已导入密钥材料或位于自定义密钥存储中：UnsupportedOperationException。
- [8] 如果 KMS 密钥已导入密钥材料：KMSInvalidStateException
- [9] 如果 KMS 密钥无法导入或未导入密钥材料：UnsupportedOperationException。
- [10] 如果源 KMS 密钥正等待删除，则该命令将成功。如果目标 KMS 密钥正等待删除，则该命令将失败，并显示以下错误消息：KMSInvalidStateException : *<key ARN>* is pending deletion.
- [11] KMSInvalidStateException: *<key ARN>* is unavailable. 您无法在不可用的 KMS 密钥上执行此操作。
- [12] 操作成功，但 KMS 密钥的密钥状态未更改，直到它变得可用。
- [13] 虽然自定义密钥存储中的 KMS 密钥处于等待删除状态，但其密钥状态保持 PendingDeletion 不变，即使 KMS 密钥变得不可用也是如此。这允许您在等待期内随时取消删除 KMS 密钥。
- [14] 在复制多区域密钥 () 时会KMSInvalidStateException: *<key ARN>* is creating. AWS KMS 引发此异常。ReplicateKey
- [15] 在更新多区域密钥 () UpdatePrimaryRegion 的主区域时KMSInvalidStateException: *<key ARN>* is updating. AWS KMS 抛出此异常。

AWS KMS 的身份验证和访问控制

要使用 AWS KMS，您必须拥有 AWS 可以用来验证您的请求的凭证。此凭证必须包括 AWS 资源、AWS KMS keys和别名的访问权限。任何 AWS 主体都没有 KMS 密钥的权限，除非明确提供该权限且从未被拒绝。不存在使用或管理 KMS 密钥的隐式权限或自动权限。

管理对 AWS KMS 资源的访问权限的主要方式是使用策略。策略是用于描述哪些委托人可以访问什么资源的文档。附加到 IAM 身份的策略称作基于身份的策略（或 IAM policy），附加到其他类型资源的策略称作资源策略。KMS 密钥的 AWS KMS 资源策略称作密钥策略。所有 KMS 密钥都具有密钥策略。

若要控制对 AWS KMS 别名的访问，请使用 IAM policy。若要允许主体创建别名，您必须在 IAM policy 中提供别名权限，并在密钥策略中提供密钥权限。有关更多信息，请参阅 控制对别名的访问。

要控制对 KMS 密钥的访问，您可以使用下列策略机制。

- 密钥策略：每个 KMS 密钥都有密钥策略。密钥策略也是控制访问 KMS 密钥的主要机制。您只能使用密钥策略来控制访问，这意味着对 KMS 密钥的所有访问均在单个文档（密钥策略）中进行定义。有关使用密钥策略的更多信息，请参阅密钥政策。
- IAM policy ：您可以将 IAM policy 与密钥策略和授权结合使用，以控制对 KMS 密钥的访问。通过用这种方式控制访问，您可以管理 IAM 中各 IAM 身份的所有权限。若要使用 IAM policy 允许访问 KMS 密钥，密钥策略必须明确允许此访问。有关使用 IAM; 策略的更多信息，请参阅 IAM 策略。
- 授权：您可以将密钥策略与 IAM policy 结合使用，以允许对 KMS 密钥的访问。通过用这种方式控制访问权限，您可以在密钥策略中允许访问 KMS 密钥，并允许有关身份将其访问权限委托给其他身份。有关使用授权的更多信息，请参阅AWS KMS 中的授权。

KMS 密钥属于创建它们的 AWS 账户。但是，身份或主体（包括 AWS 账户根用户）没有使用或管理 KMS 密钥的权限，除非该权限在密钥策略、IAM policy 或授权中明确提供。创建 KMS 密钥的 IAM 身份不会被视为密钥所有者，且他们不会自动获得使用或管理自己所创建 KMS 密钥的权限。与任何其他身份一样，密钥创建者需要通过密钥策略、IAM policy 或授权获得权限。当然，拥有 `kms:CreateKey` 权限的身份可以设置初始密钥策略，并授予自己使用或管理密钥的权限。

下面各主题提供有关可如何使用 AWS Identity and Access Management (IAM) 的详细信息，以及通过控制可以访问资源的对象来保护资源的 AWS KMS 权限。

主题

- AWS KMS 访问控制中的概念

- 中的关键政策 AWS KMS
- 将 IAM 策略与配合使用 AWS KMS
- AWS KMS 中的授权
- 通过 VPC 终端节点连接到 AWS KMS
- 的条件密钥 AWS KMS
- AWS KMS 中的 ABAC
- 允许其他账户中的用户使用 KMS 密钥
- 将服务相关角色用于 AWS KMS
- 将混合后量子 TLS 与 AWS KMS 结合使用
- 确定对 AWS KMS keys 的访问权限
- AWS KMS 权限
- 测试您的权限

AWS KMS 访问控制中的概念

了解 AWS KMS 中讨论访问控制所用的概念。

主题

- 身份验证
- 授权
- 使用身份进行身份验证
- 使用策略管理访问
- AWS KMS 资源

身份验证

身份验证是验证您的身份的过程。要向 AWS KMS 发送请求，您必须使用您的 AWS 凭证登录 AWS。

授权

授权将提供发送创建、管理或使用 AWS KMS 资源的请求的权限。例如，您必须获得授权才能在加密操作中使用 KMS 密钥。

要控制对您的 AWS KMS 资源的访问，您可以使用 密钥策略、IAM policy 和 授权。每个 KMS 密钥都必须有一个密钥政策。如果密钥策略允许，您还可以使用 IAM policy 和授权来允许相关主体访问 KMS 密钥。要优化授权，您可以使用 条件键，以仅在请求或资源满足您指定的条件时才允许或拒绝访问。您还可以向您信任的 其他 AWS 账户 中的主体授予访问权限。

使用身份进行身份验证

身份验证是使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过分派 IAM 角色进行身份验证（登录到 AWS）。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWS IAM Identity Center（IAM Identity Center）用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接分派角色。

根据用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录到 AWS 的更多信息，请参阅《AWS 登录 用户指南》中的如何登录到您的 AWS 账户。

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包（SDK）和命令行界面（CLI），以便使用您的凭证以加密方式签署您的请求。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

无论使用何种身份验证方法，您都可能需要提供其它安全信息。例如，AWS 建议您使用多重身份验证（MFA）来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的在 AWS 中使用多重身份验证（MFA）。

AWS 账户 根用户

创建 AWS 账户 时，最初使用的是一个对账户中所有 AWS 服务 和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实操，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 AWS 服务。

联合身份是来自企业用户目录、Web 身份提供程序、AWS Directory Service、Identity Center 目录的用户，或任何使用通过身份来源提供的凭证来访问 AWS 服务的用户。当联合身份访问 AWS 账户时，他们担任角色，而角色提供临时凭证。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和组，也可以连接并同步到您自己的身份来源中的一组用户和组以跨所有 AWS 账户和应用程序使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？

IAM 用户和组

IAM 用户 是 AWS 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组 是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人分派。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

IAM 角色是 AWS 账户 中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 AWS Management Console 中暂时分派 IAM 角色。您可以调用 AWS CLI 或 AWS API 操作或使用自定义 URL 以代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户或角色可分派 IAM 角色，以暂时获得针对特定任务的不同权限。

- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户存取权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为座席）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 – 某些 AWS 服务使用其它 AWS 服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话：当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中启动另一个操作。FAS 使用主体调用 AWS 服务 的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务 委派权限的角色。
  - 服务相关角色 - 服务相关角色是与 AWS 服务关联的一种服务角色。服务可以代入角色来代表您执行操作。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 - 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅《IAM 用户指南》中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您将创建策略并将其附加到 AWS 身份或资源，以控制 AWS 中的访问。策略是 AWS 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，AWS 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。然后，管理员可以向角色添加 IAM 策略，并且用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 AWS Management Console、AWS CLI 或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的 创建 IAM 策略。

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是可以附加到AWS 账户中的多个用户、组和角色的独立策略。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅 IAM 用户指南 中的在托管策略与内联策略之间进行选择。

基于资源的策略

AWS KMS 密钥策略 是一种基于资源的策略，用于控制对 KMS 密钥的访问。每个 KMS 密钥都必须有一个密钥政策。您可以使用其他授权机制来允许对 KMS 密钥的访问，但仅在密钥策略允许时才可以这样操作。（您可以使用 IAM policy 拒绝对 KMS 密钥的访问，即使密钥策略未显式允许。）

基于资源的策略是附加到资源（如 KMS 密钥）的 JSON 策略文档，用于控制对该特定资源的访问。基于资源的策略定义了指定的主体可以对该资源执行的操作以及执行操作的条件。您无需在基于资源的策略中指定资源，但必须指定主体，例如账户、用户、角色、联合用户或 AWS 服务。基于资源的策略是位于管理该资源的服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 AWS 托管式策略，例如 `AWSKeyManagementServicePowerUser` 托管式策略。

访问控制列表（ACL）

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3、AWS WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》 中的访问控制列表（ACL）概览。

AWS KMS 不支持 ACL。

其他策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可以为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 字段中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略（SCP）– SCP 是 JSON 策略，指定了组织或组织单位（OU）在 AWS Organizations 中的最大权限。AWS Organizations 服务可以分组和集中管理您的企业拥有的多个 AWS 账户 账户。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略（SCP）。SCP 限制成员账户中实体（包括每个 AWS 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 AWS 如何确定在涉及多种策略类型时是否允许请求，请参阅《IAM 用户指南》中的策略评估逻辑。

AWS KMS 资源

在 AWS KMS 中，主要资源为 AWS KMS key。AWS KMS 也支持别名，别名是为 KMS 密钥提供友好名称的独立资源。一些 AWS KMS 操作允许您使用别名来标识 KMS 密钥。

KMS 密钥或别名的每个实例均具有标准格式的唯一 Amazon Resource Name (ARN)。在 AWS KMS 资源中，AWS 服务名称为 `kms`。

- AWS KMS key

  ARN 格式：

  `arn:`*`AWS partition name`*`:`*`AWS service name`*`:`*`AWS ##`*`:`*`AWS ## ID`*`:key/`*`key ID`*

  示例 ARN:

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

- 别名

  ARN 格式：

  ```
  arn:AWS partition name:AWS service name:AWS ##:AWS ## ID:alias/alias name
  ```

  示例 ARN:

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

AWS KMS 提供一组 API 操作，用以处理您的 AWS KMS 资源。有关在 AWS Management Console 和 AWS KMS API 操作中标识 KMS 密钥的更多信息，请参阅 密钥标识符 (KeyId)。有关 AWS KMS 操作的列表，请参阅 AWS Key Management Service API 参考。

中的关键政策 AWS KMS

密钥策略是的资源策略 AWS KMS key。密钥政策是控制对 KMS 密钥访问的主要方法。每个 KMS 密钥必须只有一个密钥策略。密钥策略中的语句确定谁有权限使用 KMS 密钥以及如何使用 KMS 密钥。您还可使用 IAM policy 和授权来控制对 KMS 密钥的访问，但每个 KMS 密钥必须有一个密钥策略。

任何 AWS 委托人（包括账户根用户或密钥创建者）都无权访问 KMS 密钥，除非在密钥策略、IAM 策略或授权中明确允许且从不被拒绝。

除非密钥策略明确允许，否则您不能使用 IAM policy 允许访问 KMS 密钥。未经密钥策略许可，允许权限的 IAM policy 无效。（您可以使用 IAM policy 来拒绝在未经密钥策略许可的情况下对 KMS 密钥的访问权限。）默认密钥策略启用 IAM policy。若要在密钥策略中启用 IAM policy，请添加 允许访问 AWS 账户 并启用 IAM policy 中所述的策略语句。

与全局性的 IAM policy 不同，密钥策略是区域性策略。密钥策略仅控制对同一区域中 KMS 密钥的访问。该策略对其他地区的 KMS 密钥无效。

主题

- 创建密钥策略
- 默认密钥策略
- 查看密钥策略

- 更改密钥策略
- 关键策略中的 AWS 服务权限

创建密钥策略

您可以在 AWS KMS 控制台中使用 AWS KMS API 操作（例如CreateKeyReplicateKeyPutKeyPolicy、和）或使用AWS CloudFormation 模板来创建和管理密钥策略。

在 AWS KMS 控制台中创建 KMS 密钥时，控制台将引导您完成基于控制台默认密钥策略创建密钥策略的步骤。使用 CreateKey 或 ReplicateKey API 时，如果您没有指定密钥策略，这些 API 将应用以编程方式创建密钥的默认密钥策略。使用 PutKeyPolicy API 时，需要指定密钥政策。

每个策略文档都可以有一个或多个策略语句。以下示例显示了具有一个策略语句的有效密钥策略文档。

```
{
  "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"
        }
      }
    }
  ]
}
```

主题

- 密钥策略格式
- 密钥策略中的元素
- 示例密钥策略

密钥策略格式

密钥策略文档必须符合以下规则：

- 最多 32KB（32768 字节）
- 密钥策略语句中的 Sid 元素可以包含空格。（IAM policy 文档的 Sid 元素中禁止使用空格。）

关键策略文档只能包含以下字符：

- 可打印的 ASCII 字符
- Basic Latin 和 Latin-1 Supplement 字符集中的可打印字符
- 制表符（\u0009）、换行符（\u000A）和回车（\u000D）特殊字符

密钥策略中的元素

密钥策略文档必须有以下元素：

版本

指定密钥策略文档版本。将版本设置为 2012-10-17（最新版本）。

语句

随附策略语句。密钥策略文档必须至少包含一个语句。

每个密钥策略语句最多包含六个元素。Effect、Principal、Action 和 Resource 是必需元素。

Sid

（可选）语句标识符（Sid），是可用于描述语句的任意字符串。密钥策略中的 Sid 可以包含空格。（您不能在 IAM policy Sid 元素中包含空格。）

效果

（必需）确定是允许还是拒绝该策略语句中的权限。有效值为 Allow 或 Deny。如果您没有显式允许对 KMS 密钥的访问，则隐式拒绝访问。您也可显式拒绝对 KMS 密钥的访问。您可以通过这种方式确保用户无法访问 CMK，即使其他策略允许访问也是如此。

主体

（必需）主题是获取策略语句中指定的权限的身份。您可以在密钥策略中将 IAM 用户、IAM 角色和某些 AWS 服务指定 AWS 账户为委托人。IAM 用户组 在任何策略类型中都不是有效主体。

星号值，例如，"AWS": "*" 表示所有账户中的所有 AWS 身份。

> **Important**
>
> 除非您使用条件限制密钥政策，否则不要在允许权限的任何密钥政策语句将主体设置为星号（*）。星号赋予每个身份使用 KMS 密钥的 AWS 账户 权限，除非其他策略声明明确拒绝。其他用户只要在自己的账户中拥有相应权限，就 AWS 账户 可以使用您的 KMS 密钥。

> **Note**
>
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

当密钥策略语句中的主体是表示为 arn:aws:iam::*111122223333*:root" 的 AWS 账户 主体时，该策略语句不授予任何 IAM 主体权限。相反，它 AWS 账户 允许使用 IAM 策略委派密钥策略中指定的权限。[尽管在账户标识符中使用了“root”，但是格式为 arn:aws:iam::*111122223333*:root" 的主体并不代表 AWS 账户根用户。但是，账户主体代表账户及其管理员（包括账户根用户）。]

当委托人是另一个 AWS 账户 或其委托人时，只有在使用 KMS 密钥和密钥策略的区域中启用该账户时，权限才会生效。有关默认情况下未启用的区域（“选择加入区域”）的信息，请参阅《AWS 一般参考》 中的 Managing AWS 区域。

要允许其他用户 AWS 账户 或其委托人使用 KMS 密钥，您必须在密钥策略和另一个账户的 IAM 策略中提供权限。有关更多信息，请参阅 允许其他账户中的用户使用 KMS 密钥。

操作

（必需）指定要允许或拒绝的 API 操作。例如，该kms:Encrypt操作对应于 “ AWS KMS 加密” 操作。您可以在策略语句中列出多个 Action。有关更多信息，请参阅 权限参考。

资源

（必需）在密钥策略中，资源元素的值为 "*"，这意味着“本 KMS 密钥”。星号 ("*") 标识密钥策略附加到的 KMS 密钥。

> **Note**
>
> 如果密钥策略语句中缺少必要的 `Resource` 元素，则策略语句将无效。没有 `Resource` 元素的密钥策略语句不适用于任何 KMS 密钥。
> 当关键策略语句缺少其`Resource`元素时， AWS KMS 控制台会正确报告错误，但CreateKey和 PutKeyPolicyAPI 会成功，即使策略声明无效。

状况

（可选）条件指定要使密钥策略生效而必须满足的要求。使用条件， AWS 可以评估 API 请求的上下文以确定政策声明是否适用。

要指定条件，您可以使用预定义的条件键。 AWS KMS 支持AWS 全局条件键和AWS KMS 条件键。为了支持基于属性的访问控制 (ABAC)， AWS KMS 提供了基于标签和别名控制对 KMS 密钥的访问的条件密钥。有关更多信息，请参阅 AWS KMS 中的 ABAC。

条件的格式为：

```
"Condition": {"condition operator": {"condition key": "condition value"}}
```

例如：

```
"Condition": {"StringEquals": {"kms:CallerAccount": "111122223333"}}
```

有关 AWS 策略语法的更多信息，请参阅 AWS IAM 用户指南中的 IAM 策略参考。

示例密钥策略

以下示例显示了对称加密 KMS 密钥的完整密钥策略。在阅读本章中的密钥策略概念时，您可以将它作为参考。此密钥策略将之前默认密钥策略部分的示例策略语句合并为一个密钥策略，该密钥策略可完成以下操作：

- 允许示例 AWS 账户 111122223333 对 KMS 密钥的完全访问权限。它其允许账户及其管理员（包括账户根用户在紧急情况下）在该账户中使用 IAM policy 来允许访问 KMS 密钥。
- 允许 `ExampleAdminRole` IAM 角色管理 KMS 密钥。
- 允许 `ExampleUserRole` IAM 角色使用 KMS 密钥。

```
{
    "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"
                }
            }
        }
    ]
}
```

默认密钥策略

创建 KMS 密钥时，您可以为新的 KMS 密钥指定密钥策略。如果您不提供一个，请为您 AWS KMS 创建一个。 AWS KMS 使用的默认密钥策略会有所不同，具体取决于您是在 AWS KMS 控制台中创建密钥还是使用 AWS KMS API。

以编程方式创建 KMS 密钥时采用的默认密钥策略

当您使用 AWS KMS API 以编程方式创建 KMS 密钥（包括使用AWS 软件开发工具包AWS Command Line Interface或 AWS Tools for PowerShell），并且未指定密钥策略时，会 AWS KMS 应用非常简单的默认密钥策略。此默认密钥策略有一个策略声明，该声明向拥有 KMS 密钥的用户授予使用 IAM 策

略的权限，以允许对 KMS 密钥进行所有 AWS KMS 操作。 AWS 账户 有关此策略语句的更多信息，请参阅允许访问 AWS 账户 并启用 IAM policy。

使用创建 KMS 密钥时的默认密钥策略 AWS Management Console

使用创建 KMS 密钥时 AWS Management Console，密钥策略以允许访问 AWS 账户 并启用 IAM 策略的策略声明开头。然后，控制台会添加密钥管理员声明、密钥用户声明以及（对于大多数密钥类型）一条允许委托人将 KMS 密钥用于其他 AWS 服务的声明。您可以使用 AWS KMS 控制台的功能来指定 IAM 用户、IAMRoles、 AWS 账户 谁是密钥管理员以及谁是关键用户（或两者兼而有之）。

权限

- 允许访问 AWS 账户 并启用 IAM policy
- 允许密钥管理员管理 KMS 密钥
- 允许密钥用户使用 KMS 密钥
  - 允许密钥用户使用 KMS 密钥进行加密操作
  - 允许密钥用户将 KMS 密钥与 AWS 服务一起使用

允许访问 AWS 账户 并启用 IAM policy

以下默认密钥策略语句至关重要。

- 它为拥有 KMS 密钥的人提供对 KMS 密钥的完全访问权限。 AWS 账户

  与其他 AWS 资源策略不同， AWS KMS 密钥策略不会自动向账户或其任何身份授予权限。若要授予账户管理员权限，密钥策略必须包含提供此权限的显式语句，如下所示。
- 除密钥策略外，还允许账户使用 IAM policy 允许对 KMS 密钥进行访问。

  如果没有此权限，尽管拒绝访问密钥的 IAM policy 仍然有效，但是允许访问密钥的 IAM policy 将无效。
- 此权限通过向账户管理员（包括账户根用户）授予无法删除的访问控制权限，来降低密钥变得无法管理的风险。

以下密钥策略语句是以编程方式创建的 KMS 密钥的完整默认密钥策略。这是 AWS KMS 控制台中创建的 KMS 密钥的默认密钥策略中的第一条策略声明。

```
{
```

```
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:root"
   },
  "Action": "kms:*",
  "Resource": "*"
}
```

允许 IAM policy 允许对 KMS 密钥的访问。

上面显示的密钥策略声明向拥有密钥的用户授予使用 IAM 策略和密钥策略的权限，以允许对 KMS 密钥执行所有操作 (kms:*)。 AWS 账户

本密钥策略声明中的主体是账户主体，其由此格式 (arn:aws:iam::*account-id*:root) 的 ARN 进行表示。账户委托人代表 AWS 账户及其管理员。

当密钥策略语句中的主体是账户主体时，该策略语句不会向任何 IAM 主体授予使用 KMS 密钥的权限。相反，其授予账户使用 IAM policy 委托密钥语句中指定的权限。此默认密钥策略语句允许账户使用 IAM policy 委托 KMS 密钥上所有操作 (kms:*) 的权限。

可以降低 KMS 密钥变得不可管理的风险。

与其他 AWS 资源策略不同， AWS KMS 密钥策略不会自动向账户或其任何委托人授予权限。若要授予任何主体（包括账户主体）权限，您必须使用明确提供权限的密钥策略语句。您无需授予账户主体或任何主体访问 KMS 密钥的权限。但是，授予账户主体访问权限有助于防止无法管理密钥。

例如，假设您创建的密钥策略仅授予一个用户访问 KMS 密钥的权限。如果删除该用户，则密钥将变得无法管理，您必须联系 AWS Support 才能重新获得 KMS 密钥的访问权限。

上面显示的密钥策略声明向账户委托人授予控制密钥的权限，账户委托人代表 AWS 账户 及其管理员，包括账户根用户。除非您删除 AWS 账户，否则账户根用户是唯一无法删除的主体。IAM 最佳实践不鼓励代表账户根用户采取操作，但紧急情况除外。但是，如果删除所有其他具有 KMS 密钥访问权限的用户和角色，则您可能需要充当账户根用户。

允许密钥管理员管理 KMS 密钥

控制台创建的默认密钥策略允许您选择账户中的 IAM 用户和角色，并使其成为密钥管理员。此语句称为密钥管理员语句。密钥管理员有权管理 KMS 密钥，但无权在加密操作中使用 KMS 密钥。在原定设置视图或策略视图中创建 KMS 密钥时，您可以将 IAM 用户和角色添加到密钥管理员列表。

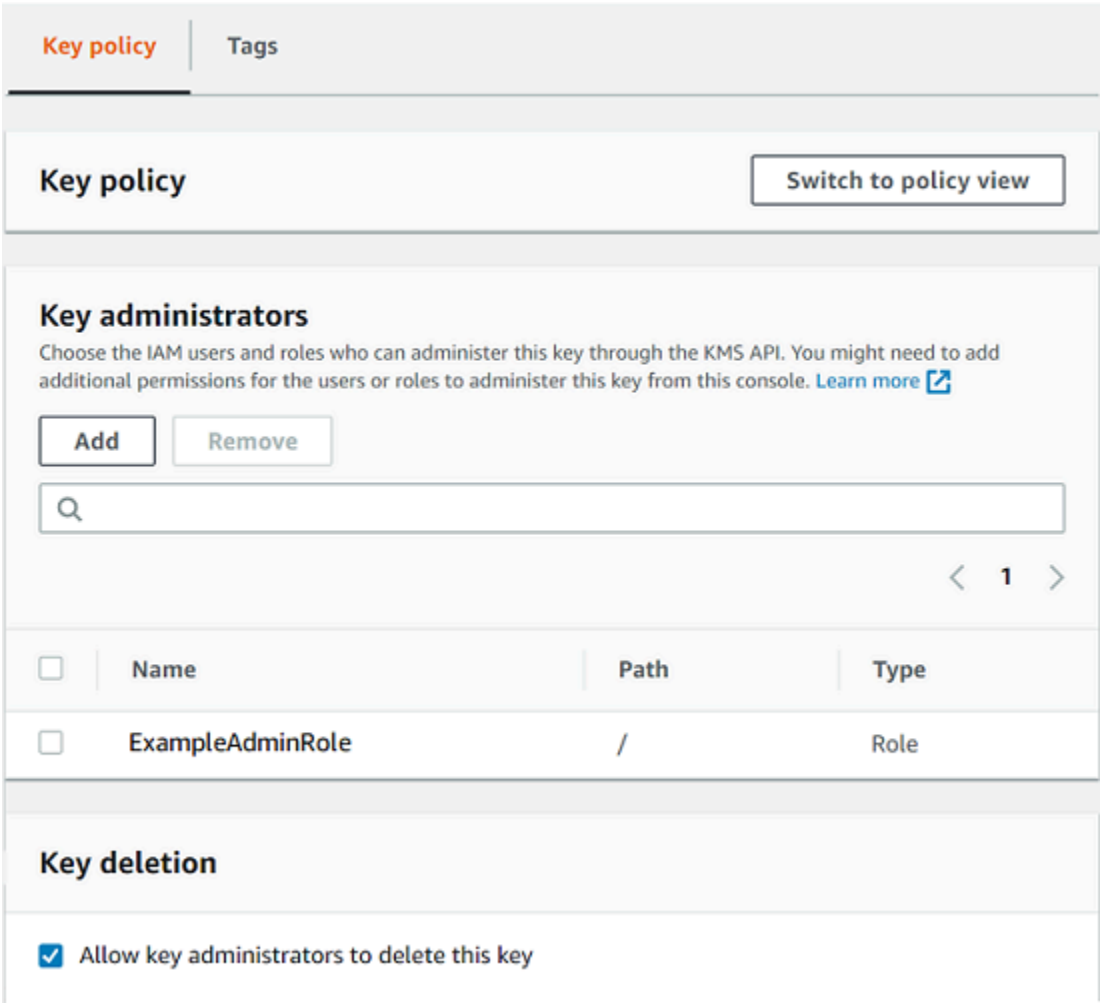
Warning

由于密钥管理员有权更改密钥策略和创建授权，因此他们可以向自己和其他人 AWS KMS 授予此策略中未指定的权限。
有权管理标签和别名的委托人也可以控制对 KMS 密钥的访问。有关更多信息，请参阅 AWS KMS 中的 ABAC。

Note

IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

以下示例在 AWS KMS 控制台的原定设置视图中显示了密钥管理员语句。



以下示例是 AWS KMS 控制台的策略视图中的密钥管理员语句。此密钥管理员语句适用于单区域对称加密 KMS 密钥。

```
{
  "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": "*"
}
```

最常见 KMS 密钥、单区域对称加密 KMS 密钥的原定设置密钥管理员语句允许以下权限。有关每个权限的详细信息，请参阅 AWS KMS 权限。

当您使用 AWS KMS 控制台创建 KMS 密钥时，控制台会将您指定的用户和角色添加到密钥管理员语句中的`Principal`元素中。

这些权限中有很多都包含通配符 (*)，使用它可以允许以指定动词开头的所有权限。因此，在 AWS KMS 添加新的 API 操作时，自动允许密钥管理员使用它们。您不必更新密钥策略即可包含新操作。如果您希望将密钥管理员限制在一组固定的 API 操作中，则可以更改密钥策略。

`kms:Create*`

允许 `kms:CreateAlias` 和 `kms:CreateGrant`。（`kms:CreateKey` 权限仅在 IAM policy 中有效。）

kms:Describe*

允许 kms:DescribeKey。需要 kms:DescribeKey 权限才能查看 AWS Management Console中 KMS 密钥的密钥详细信息页面。

kms:Enable*

允许 kms:EnableKey。对于对称加密 KMS 密钥，它还允许 kms:EnableKeyRotation。

kms:List*

允许 kms:ListGrants、kms:ListKeyPolicies 和 kms:ListResourceTags。（查看 AWS Management Console中的 KMS 密钥所需的 kms:ListAliases 和 kms:ListKeys 权限仅在 IAM policy 中有效。）

kms:Put*

允许 kms:PutKeyPolicy。此权限允许密钥管理员更改此 KMS 密钥的密钥策略。

kms:Update*

允许 kms:UpdateAlias 和 kms:UpdateKeyDescription。对于多区域密钥，它允许此 KMS 密钥上的 kms:UpdatePrimaryRegion。

kms:Revoke*

允许 kms:RevokeGrant，其允许密钥管理员删除授权，即使管理员不是授权中的停用主体。

kms:Disable*

允许 kms:DisableKey。对于对称加密 KMS 密钥，它还允许 kms:DisableKeyRotation。

kms:Get*

允许 kms:GetKeyPolicy 和 kms:GetKeyRotationStatus。对于具有导入密钥材料的 KMS 密钥，它允许 kms:GetParametersForImport。对于非对称 KMS 密钥，它允许 kms:GetPublicKey。需要 kms:GetKeyPolicy 权限才能查看 AWS Management Console中 KMS 密钥的密钥策略。

kms:Delete*

允许 kms:DeleteAlias。对于具有导入密钥材料的密钥，它允许 kms:DeleteImportedKeyMaterial。kms:Delete* 权限不允许密钥管理员删除 KMS 密钥 (ScheduleKeyDeletion)。

kms:TagResource

允许 kms:TagResource，以此允许密钥管理员向 KMS 密钥添加标签。由于标签也可用于控制对 KMS 密钥的访问，因此管理员通过此权限可允许或拒绝对 KMS 密钥的访问。有关更多信息，请参阅 AWS KMS 中的 ABAC。

kms:UntagResource

允许 kms:UntagResource，以此允许密钥管理员从 KMS 密钥删除标签。由于标签可用于控制对密钥的访问，因此管理员通过此权限可允许或拒绝对 KMS 密钥的访问。有关更多信息，请参阅 AWS KMS 中的 ABAC。

kms:ScheduleKeyDeletion

允许 kms:ScheduleKeyDeletion，以此允许密钥管理员删除此 KMS 密钥。要删除此权限，请清除 Allow key administrators to delete this key（允许密钥管理员删除此密钥）选项。

kms:CancelKeyDeletion

允许 kms:CancelKeyDeletion，以此允许密钥管理员取消此 KMS 密钥的删除。要删除此权限，请清除 Allow key administrators to delete this key（允许密钥管理员删除此密钥）选项。

AWS KMS 在创建特殊用途密钥时，将以下权限添加到默认密钥管理员语句中。

kms:ImportKeyMaterial

kms:ImportKeyMaterial 权限允许密钥管理员将密钥材料导入 KMS 密钥。仅当创建不含密钥材料的 KMS 密钥时，此权限才包含在密钥策略中。

kms:ReplicateKey

该kms:ReplicateKey权限允许密钥管理员在不同 AWS 区域创建多区域主密钥的副本。仅当您创建多区域主键或副本键时，此权限才会包含在密钥策略中。

kms:UpdatePrimaryRegion

kms:UpdatePrimaryRegion 权限允许密钥管理员将多区域副本密钥更改为多区域主键。仅当您创建多区域主键或副本键时，此权限才会包含在密钥策略中。

允许密钥用户使用 KMS 密钥

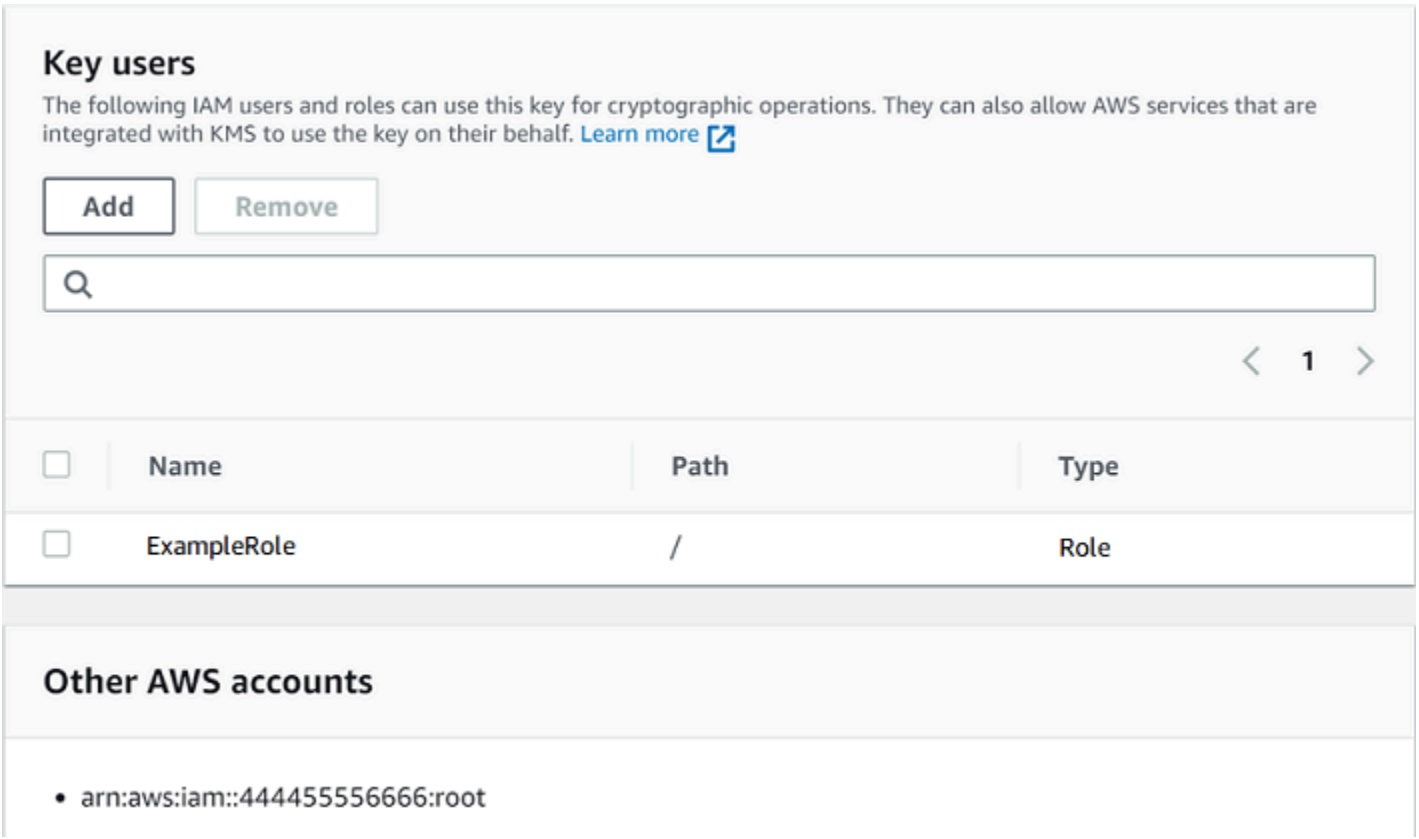
控制台为 KMS 密钥创建的默认密钥策略允许您在账户中选择 IAM 用户和 IAM 角色以及外部角色 AWS 账户，并使其成为密钥用户。

控制台将两个策略语句添加到密钥用户的密钥策略中。

- 直接使用 KMS 密钥 — 第一个密钥策略语句授予密钥用户将 KMS 密钥直接用于该类型 KMS 密钥支持的所有加密操作的权限。
- 将 KMS 密钥用于 AWS 服务 — 第二项策略声明允许密钥用户允许与其集成的 AWS 服务代表他们使用 KMS 密钥 AWS KMS 来保护资源，例如 Amazon S3 存储桶和 Amazon DynamoD B 表。

创建 KMS 密钥时，您可以将 IAM 用户、IAM 角色和其他 AWS 账户 角色添加到密钥用户列表中。您也可以使用控制台的默认密钥策略视图来编辑该列表，如下图所示。默认密钥策略视图可从密钥详细信息页面获取。有关允许其他 AWS 账户 用户使用 KMS 密钥的更多信息，请参阅允许其他账户中的用户使用 KMS 密钥。

> **Note**
>
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。



单区域对称的原定设置密钥用户语句允许以下权限。有关每个权限的详细信息，请参阅 AWS KMS 权限。

当您使用 AWS KMS 控制台创建 KMS 密钥时，控制台会将您指定的用户和角色添加到每个密钥用户语句中的`Principal`元素中。

```
{
  "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}}
}
```

允许密钥用户使用 KMS 密钥进行加密操作

密钥用户有权在 KMS 密钥支持的所有加密操作中直接使用 KMS 密钥。他们还可以使用该DescribeKey操作在 AWS KMS 控制台或使用 AWS KMS API 操作来获取有关 KMS 密钥的详细信息。

默认情况下，AWS KMS 控制台会将密钥用户语句添加到默认密钥策略中，如下例所示。由于支持的 API 操作不同，策略语句中针对对称加密 KMS 密钥、HMAC KMS 密钥、用于公有密钥加密的非对称 KMS 密钥以及用于签名和验证的非对称 KMS 密钥的操作略有不同。

对称加密 KMS 密钥

控制台将以下语句添加到对称加密 KMS 密钥的密钥策略中。

```
{
  "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": "*"
```

```
}
```

HMAC KMS 密钥

控制台将以下语句添加到 HMAC KMS 密钥的密钥策略中。

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleKeyUserRole"},
  "Action": [
    "kms:DescribeKey",
    "kms:GenerateMac",
    "kms:VerifyMac"
  ],
  "Resource": "*"
}
```

用于公有密钥加密的非对称 KMS 密钥

对于密钥用法为 Encrypt and decrypt（加密和解密）的非对称 KMS 密钥，控制台将以下语句添加到其密钥策略中。

```
{
  "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": "*"
}
```

用于签名和验证的非对称 KMS 密钥

对于密钥用法为 Sign and verify（签名和验证）的非对称 KMS 密钥，控制台将以下语句添加到其密钥策略中。

```
{
  "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": "*"
}
```

这些语句中的操作赋予密钥用户以下权限。

kms:Encrypt

允许密钥用户使用此 KMS 密钥加密数据。

kms:Decrypt

允许密钥用户使用此 KMS 密钥解密数据。

kms:DescribeKey

允许密钥用户获取有关此 KMS 密钥的详细信息，包括其标识符、创建日期和密钥状态。它还允许密钥用户在 AWS KMS 控制台中显示有关 KMS 密钥的详细信息。

kms:GenerateDataKey*

允许密钥用户请求对称数据密钥或非对称数据密钥对，以执行客户端加密操作。控制台使用* 通配符表示对以下 API 操作的权限：GenerateDataKey、GenerateDataKeyWithoutPlaintextGenerateDataKeyPair、和GenerateDataKeyPairWithoutPlaintext。这些权限仅对加密数据密钥的对称 KMS 密钥有效。

kms: GenerateMac

允许密钥用户使用 HMAC KMS 密钥生成 HMAC 标签。

kms: GetPublicKey

允许密钥用户下载非对称 KMS 密钥的公有密钥。与您共享此公钥的各方可以对外部的数据进行加密 AWS KMS。但是，这些密文只能通过调用 AWS KMS中的 Decrypt 操作进行解密。

kms: ReEncrypt *

允许密钥用户重新加密最初使用此 KMS 密钥加密的数据，或使用此 KMS 密钥重新加密之前已加密的数据。该ReEncrypt操作需要同时访问源 KMS 密钥和目标 KMS 密钥。为此，可以允许对源 KMS 密钥具备 `kms:ReEncryptFrom` 权限，对目标 KMS 密钥具备 `kms:ReEncryptTo` 权限。但是，为简单起见，控制台允许对两个 KMS 密钥具备 `kms:ReEncrypt*` 权限（采用 * 通配符）。

kms:Sign

允许密钥用户使用此 KMS 密钥签署消息。

kms:Verify

允许密钥用户使用此 KMS 密钥验证签名。

kms: VerifyMac

允许密钥用户使用 HMAC KMS 密钥验证 HMAC 标签。

允许密钥用户将 KMS 密钥与 AWS 服务一起使用

控制台中的默认密钥策略还为密钥用户提供了在使用授权的 AWS 服务中保护其数据所需的授予权限。AWS 服务通常使用授权来获得使用 KMS 密钥的特定和有限权限。

此密钥策略声明允许密钥用户创建、查看和撤消对 KMS 密钥的授权，但前提是授权操作请求来自与 AWS KMS集成的AWS 服务。kms: GrantIsFor AWSResource 策略条件不允许用户直接调用这些授权操作。当密钥用户允许时，AWS 服务可以代表用户创建授权，允许该服务使用 KMS 密钥来保护用户的数据。

密钥用户必须具备这些授权权限，才能一起使用 KMS 密钥和集成服务，但仅有这些权限还不够。密钥用户还必须具备使用集成服务的权限。有关向用户提供与集成的 AWS 服务的访问权限的详细信息 AWS KMS，请参阅集成服务的文档。

```
{
  "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}}
}
```

例如，密钥用户可以通过以下方式对 KMS 密钥使用这些权限。

- 将此 KMS 密钥与 Amazon Elastic Block Store (Amazon EBS) 和 Amazon Elastic Compute Cloud (Amazon EC2) 结合使用，将加密的 EBS 卷附加到 EC2 实例。密钥用户向 Amazon EC2 隐式授予使用 KMS 密钥将加密卷挂载到实例的权限。有关更多信息，请参阅 Amazon Elastic Block Store (Amazon EBS) 如何使用 AWS KMS。
- 将此 KMS 密钥用于 Amazon Redshift 以启动加密集群。密钥用户向 Amazon Redshift 隐式授予使用 KMS 密钥启动加密集群并创建加密快照的权限。有关更多信息，请参阅 Amazon Redshift 如何使用 AWS KMS。
- 将此 KMS 密钥与其他与 AWS KMS集成的AWS 服务一起使用，这些服务使用授权服务创建、管理或使用这些服务加密的资源。

默认密钥策略允许密钥用户向所有使用授权的集成服务委托授权权限。但是，您可以创建自定义密钥策略，将权限限制为指定 AWS 服务。有关更多信息，请参阅 kms: ViaService 条件键。

查看密钥策略

您可以在 AWS KMS API 中使用或GetKeyPolicy操作查看AWS KMS客户托管密钥AWS Management Console或账户AWS 托管式密钥中的密钥政策。但这些技术不能用于查看其他 AWS 账户 中的 KMS 密钥的密钥策略。

要了解有关 AWS KMS 密钥策略的更多信息，请参阅中的关键政策 AWS KMS。要了解如何确定哪些用户和角色有权访问 KMS 密钥，请参阅 the section called “确定访问权限”。

主题

- 查看密钥策略（控制台）
- 查看密钥策略 (AWS KMS API)

查看密钥策略（控制台）

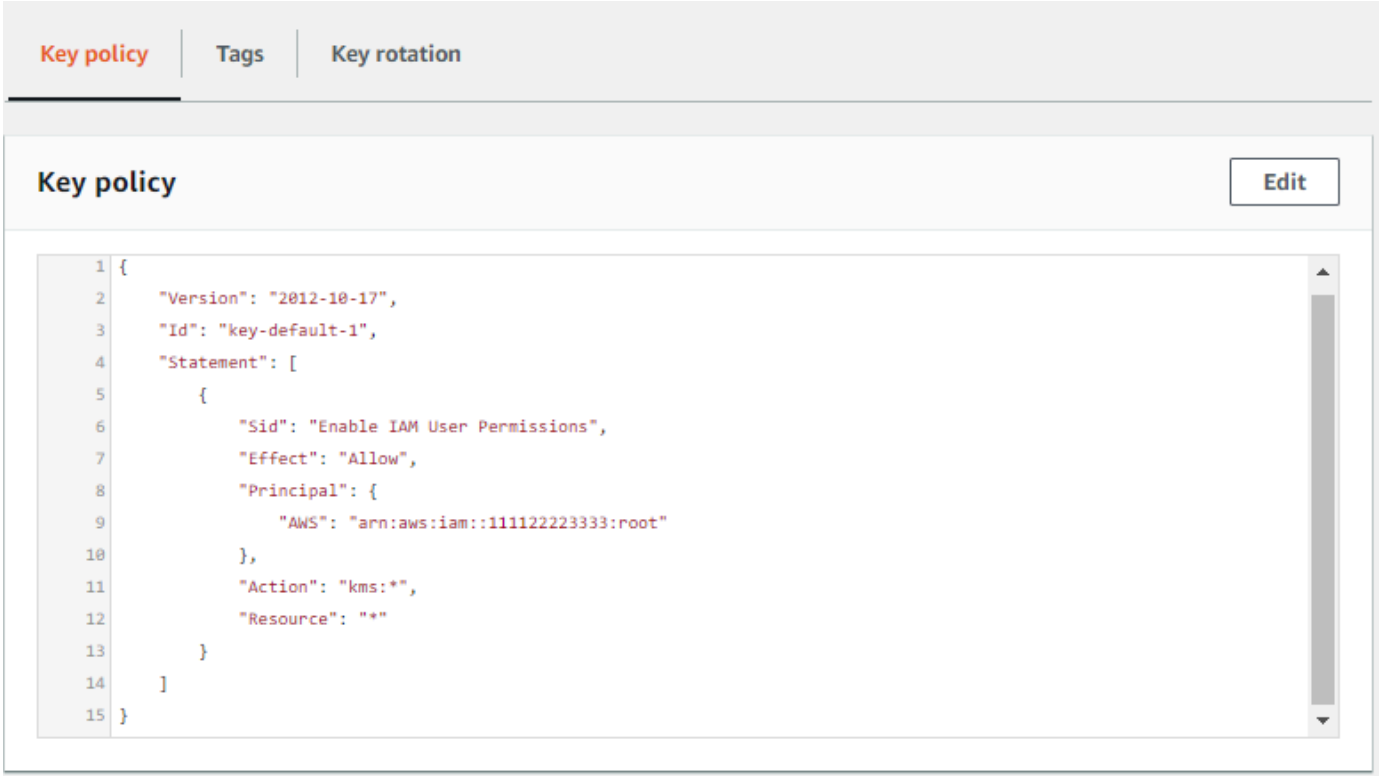
授权用户可以在 AWS Management Console 的 Key policy（密钥策略）选项卡上查看 AWS 托管式密钥 或客户托管密钥的密钥策略。

要在中查看 KMS 密钥的密钥策略AWS Management Console，您必须拥有 k ms: ListAliases、kms: DescribeKey 和 kms: GetKeyPolicy 权限。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 要查看您账户中 AWS 为您所创建和管理的密钥，请在导航窗格中选择 AWS managed keys（Amazon 托管式密钥）。要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。
4. 在 KMS 密钥列表中，选择要检查的 KMS 密钥的别名或密钥 ID。
5. 选择 Key policy (密钥策略) 选项卡。

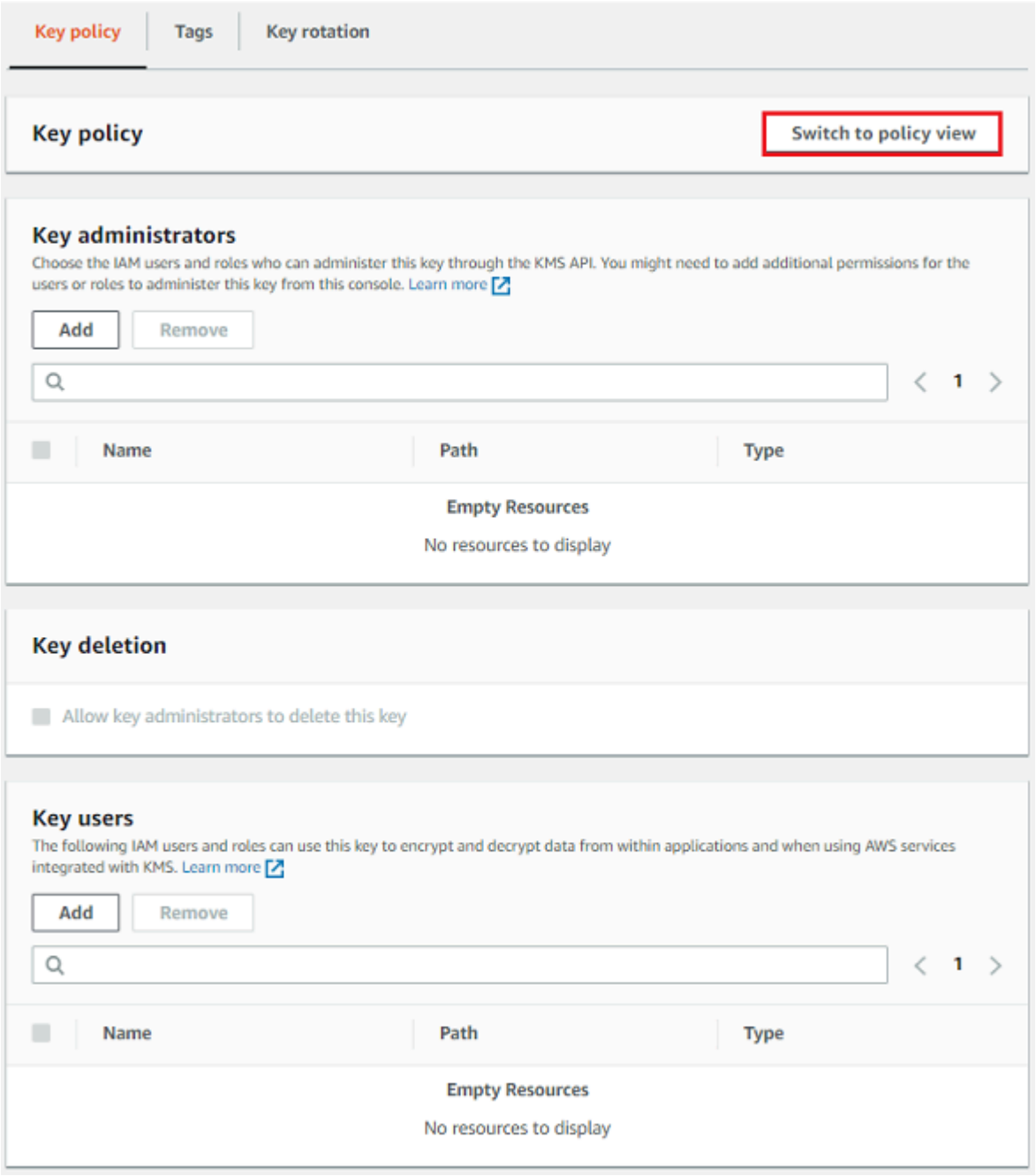
   在 Key policy（密钥策略）选项卡中，您可能会看到密钥策略文档。这是策略视图。在密钥策略语句中，可以看到由密钥策略授予 KMS 密钥访问权限的委托人，还可以看到他们能执行的操作。

   以下示例显示了默认密钥策略的策略视图。



   或者，如果 KMS 密钥是在 AWS Management Console 中创建的，那么您将看到默认视图，其中包含 Key administrators（密钥管理员）、Key deletion（密钥删除）和 Key Users（密钥用户）几个部分。要查看密钥策略文档，请选择 Switch to policy view (切换到策略视图)。

   以下示例显示了默认密钥策略的默认视图。



查看密钥策略 (AWS KMS API)

要在中获取 KMS 密钥的密钥策略AWS 账户，请使用 AWS KMS API 中的GetKeyPolicy操作。此操作不能用于查看其他帐户中的密钥策略。

以下示例使用 AWS Command Line Interface (AWS CLI) 中的get-key-policy命令，但您可以使用任何 AWS SDK 来发出此请求。

请注意，PolicyName 参数是必需的，即使其唯一的有效值为 default。此外，此命令请求以文本而不是 JSON 形式输出，以便更易于查看。

在运行此命令之前，请将示例密钥 ID 替换为您账户中的有效密钥 ID。

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

响应应类似于下图，返回默认密钥策略。

```
{
  "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" : "*"
  } ]
}
```

更改密钥策略

您可以使用AWS Management Console或PutKeyPolicy操作更改中某个 KMS 密钥的密钥策略。AWS 账户但这些技术不能用于更改其他 AWS 账户 中的 KMS 密钥的密钥策略。

当更改密钥策略时，请注意以下规则：

- 您可以查看 AWS 托管式密钥 或客户托管密钥的密钥策略，但只能更改客户托管密钥的密钥策略 AWS 托管式密钥 的策略由在账户中创建 KMS 密钥的 AWS 服务创建和管理。您无法查看或更改 AWS 拥有的密钥 的密钥策略。
- 您可以在密钥策略中添加或删除 IAM 用户、IAM 角色和 AWS 账户，并更改允许或拒绝这些主体执行的操作。有关在密钥策略中指定委托人和权限的方法的更多信息，请参阅密钥政策。
- 您无法向密钥策略添加 IAM 组，但可以添加多个 IAM 用户和 IAM 角色。有关更多信息，请参阅 允许多个 IAM 主体访问 KMS 密钥。
- 如果向密钥政策添加外部 AWS 账户，您还必须使用外部账户中的 IAM policy 向这些账户中的 IAM 用户、组或角色授予权限。有关更多信息，请参阅 允许其他账户中的用户使用 KMS 密钥。

- 所生成的密钥策略文档不能超过 32 KB（32,768 字节）。

主题

如何更改密钥策略

您可以通过三种不同的方式更改密钥策略，如以下各部分所述。

主题

使用 AWS Management Console默认视图

您可以使用控制台中名为默认视图的图形界面来更改密钥策略。

如果以下步骤与您在此控制台中看到的内容不一致，可能意味着，此密钥策略不是由此控制台创建的。也可能意味着，修改此密钥策略的方式不受控制台的默认视图的支持。在这种情况下，请按照使用 AWS Management Console策略视图或使用 AWS KMS API中的步骤操作。

1. 查看客户托管密钥的密钥策略，如 查看密钥策略（控制台） 中所述。（您无法更改 AWS 托管式密钥 的密钥策略。）
2. 确定要更改的内容。

   - 要添加或删除密钥管理员以及允许或阻止密钥管理员删除 KMS 密钥，请使用此页面的 Key administrators（密钥管理员）部分中的控件。密钥管理员管理 KMS 密钥，包括启用和禁用它、设置密钥策略以及启用密钥轮换。
   - 要添加或删除密钥用户以及允许或禁止外部 AWS 账户 使用 KMS 密钥，请使用此页面的 Key users（密钥用户）部分中的控件。密钥用户可以在加密操作（如加密、解密、重新加密和生成数据密钥）中使用 KMS 密钥。

使用 AWS Management Console策略视图

您可以使用控制台的策略视图更改密钥策略文档。

1. 查看客户托管密钥的密钥策略，如 查看密钥策略（控制台） 中所述。（您无法更改 AWS 托管式密钥 的密钥策略。）
2. 在密钥策略部分中，选择切换到策略视图。
3. 编辑密钥策略文档，然后选择 Save changes (保存更改)。

使用 AWS KMS API

您可以使用该PutKeyPolicy操作来更改您的 KMS 密钥的密钥策略AWS 账户。但不能对其他 AWS 账户中的 KMS 密钥使用此 API。

1. 使用GetKeyPolicy操作获取现有的密钥策略文档，然后将密钥策略文档保存到文件中。有关多种编程语言中的示例代码，请参阅 获取密钥策略。
2. 在您的首选文本编辑器中打开该密钥策略文档，编辑该密钥策略文档，然后保存文件。
3. 使用PutKeyPolicy操作将更新的密钥策略文档应用于 KMS 密钥。有关多种编程语言中的示例代码，请参阅 设置密钥策略。

有关将密钥策略从一个 KMS 密钥复制到另一个 KMS 密钥的GetKeyPolicy 示例，请参阅《AWS CLI命令参考》中的示例。

允许多个 IAM 主体访问 KMS 密钥

IAM 组不是密钥策略中的有效委托人。要允许多个 IAM 用户和角色访问 KMS 密钥，请执行下列操作中的一种：

- 将 IAM 角色作为密钥策略中的主体。多个授权用户可以根据需要代入该角色。有关详细信息，请参阅《IAM 用户指南》中的 IAM 角色。

  虽然您可以在密钥策略中列出多个 IAM 用户，但不建议采用这种做法，因为这将要求您在每次授权用户列表发生变化时更新密钥策略。此外，IAM 最佳实践也不鼓励使用具有长期凭证的 IAM 用户。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。
- 使用 IAM policy 向 IAM 组授予权限。要执行此操作，请确保密钥策略包含一个 启用 IAM policy 以允许访问 KMS 密钥 的语句，创建一个 IAM policy 以允许访问该 KMS 密钥，然后 将该策略附加到 IAM 组（其中包含授权 IAM 用户）。使用此方式，您不需要在授权用户列表发生更改时更改任何

策略。相反，您只需在相应的 IAM 组中添加或删除这些用户。有关详细信息，请参阅《IAM 用户指南》中的 IAM 用户组。

有关 AWS KMS 密钥政策和 IAM policy 如何协同工作的更多信息，请参阅 密钥访问故障排除。

关键策略中的 AWS 服务权限

许多 AWS 服务 AWS KMS keys 用来保护其管理的资源。在服务使用 AWS 拥有的密钥 或 AWS 托管式密钥 时，该服务会为这些 KMS 密钥建立和维护密钥策略。

但是，当您通过 AWS 服务使用客户托管式密钥时，您可以设置并维护密钥策略。该密钥策略必须允许服务具有代表您保护资源所需的最低权限。建议您遵循最低权限原则：仅授予服务所需的权限。您可以通过了解服务需要哪些权限，并使用 AWS 全局条件键和 AWS KMS 条件键来优化权限，以有效做到这一点。

要查找服务在客户托管式密钥上需要的权限，请参阅该服务的加密文档。例如，对于 Amazon Elastic Block Store (Amazon EBS) 所需的权限，请参阅适用于 Linux 实例的 Amazon EC2 用户指南或适用于 Windows 实例的 Amazon EC2 用户指南中的 IAM 用户的权限。有关 Secrets Manager 所需的权限，请参阅 AWS Secrets Manager 用户指南中的授权使用 KMS 密钥。

实施最低权限

当您向 AWS 服务授予使用 KMS 密钥的权限时，请确保该权限仅对服务必须代表您访问的资源有效。这种最低权限策略有助于防止在 AWS 服务之间传递请求时未经授权使用 KMS 密钥。

要实施最低权限策略，我们建议使用 AWS KMS 加密上下文条件密钥和全局来源 ARN 或源账户条件密钥。

使用加密上下文条件键

在使用 AWS KMS 资源时，实现最低特权权限的最有效方法是在允许委托人调用 AWS KMS 加密操作的策略中包含kms:EncryptionContext:context-key或kms:EncryptionContextKeys条件密钥。这些条件键特别有效，因为它们将权限与在加密资源时绑定到密文的加密上下文相关联。

仅当策略语句中的操作为或采用EncryptionContext参数的 AWS KMS 对称加密操作（例如CreateGrant或 Decrypt 之类GenerateDataKey的操作）时，才使用加密上下文条件密钥。（有关支持的操作列表，请参阅 kms:EncryptionContext:context-key 或 kms:EncryptionContextKeys）。如果您使用这些条件键来允许其他操作（例如）DescribeKey，则权限将被拒绝。

将值设置为服务在加密资源时使用的加密上下文。此信息通常可在服务文档的“安全性”章节中找到。例如，AWS Proton 的加密上下文标识 P AWS roton 资源及其关联的模板。AWS Secrets Manager 加密上下文标识密钥及其版本。Amazon Location 的加密上下文标识跟踪器或集合。

以下示例是密钥策略语句允许 Amazon Location Service 代表授权用户创建授权。本政策声明通过使用 k ms: ViaService、kms: 和kms:EncryptionContext:*context-key*条件密钥将权限绑定到特定的跟踪器资源来限制权限。CallerAccount

```
{
  "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"
    }
  }
}
```

使用 **aws:SourceArn** 或 **aws:SourceAccount** 条件键

密钥策略语句中的主体是 AWS 服务主体时，除了 kms:EncryptionContext:*context-key* 条件键外，我们强烈建议您使用 aws:SourceArn 或 aws:SourceAccount 全局条件键。只有当请求 AWS KMS 来自其他 AWS 服务时，ARN 和账户值才会包含在授权上下文中。这种条件的组合实施最低权限，避免了潜在的混淆代理情况。在密钥策略中，服务委托人通常不用作委托人，但某些 AWS 服务（例如）需要 AWS CloudTrail它。

要使用 aws:SourceArn 或 aws:SourceAccount 全局条件键，将值设置为正在加密的资源的 Amazon Resource Name (ARN) 或账户。例如，在提供 AWS CloudTrail 权限加密跟踪记录的密钥策略语句中，将 aws:SourceArn 的值设置为跟踪记录的 ARN。请尽可能使用更具体的 aws:SourceArn。将值设置为 ARN 或带通配符的 ARN 模式。如果您不知道资源的 ARN，请改用 aws:SourceAccount。

> **Note**
>
> 如果资源 ARN 包含 AWS KMS 密钥策略中不允许的字符，则不能在条件密钥的值中使用该资源 ARN。aws:SourceArn改为使用 aws:SourceAccount 条件键。有关密钥策略文档规则的详细信息，请参阅 密钥策略格式。

在以下示例密钥策略中，获得权限的主体是 AWS CloudTrail 服务主体 cloudtrail.amazonaws.com。为实施最低权限，本策略使用 aws:SourceArn 和 kms:EncryptionContext:*context-key* 条件键。该策略声明 CloudTrail 允许使用 KMS 密钥生成用于加密跟踪的数据密钥。aws:SourceArn 和 kms:EncryptionContext:*context-key* 条件会得到独立评估。使用 KMS 密钥进行指定操作的任何请求都必须满足这两个条件。

为了限制服务对示例账户 (111122223333) 和 us-west-2 区域中 finance 跟踪记录的权限，此策略语句将 aws:SourceArn 条件键设置为特定跟踪记录的 ARN。条件语句使用ArnEquals运算符来确保在匹配时独立评估 ARN 中的每个元素。此示例还使用 kms:EncryptionContext:*context-key* 条件键来限制对特定账户和区域中跟踪记录的权限。

在使用此密钥策略之前，请将示例账户 ID、区域和跟踪记录名称替换为您账户中的有效值。

```
{
  "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/*"
          ]
```

```
        }
      }
    }
  ]
}
```

将 IAM 策略与配合使用 AWS KMS

您可以使用 IAM 策略以及密钥策略、授权和 VPC 终端节点策略来控制对您 AWS KMS keys 的 in 的访问权限 AWS KMS。

> **Note**
>
> 要使用 IAM policy 控制对 KMS 密钥的访问，KMS 密钥的密钥政策必须授予账户使用 IAM policy 的权限。具体而言，密钥策略必须包含启用 IAM policy 的策略语句。
> 本节介绍如何使用 IAM 策略来控制对 AWS KMS 操作的访问权限。有关 IAM 的更多一般信息，请参阅 IAM 用户指南。

所有 KMS 密钥都必须具有密钥策略。IAM policy 是可选的。要使用 IAM policy 控制对 KMS 密钥的访问，KMS 密钥的密钥政策必须授予账户使用 IAM policy 的权限。具体而言，密钥策略必须包含启用 IAM policy 的策略语句。

IAM 策略可以控制对任何 AWS KMS 操作的访问权限。与密钥策略不同，IAM 策略可以控制对多个 KMS 密钥的访问权限，并为多个相关 AWS 服务的操作提供权限。但是，IAM 策略对于控制对操作的访问特别有用 CreateKey，例如无法由密钥策略控制的操作，因为它们不涉及任何特定的 KMS 密钥。

如果您 AWS KMS 通过亚马逊虚拟私有云 (Amazon VPC) 终端节点进行访问，则还可以在使用终端节点时使用 VPC 终端节点策略来限制对 AWS KMS 资源的访问。例如，在使用 VPC 终端节点时，您可能只允许您的委托人 AWS 账户 访问您的客户托管密钥。有关更多信息，请参阅 控制对 VPC 终端节点的访问。

有关编写和格式化 JSON 策略文档的帮助，请参阅 IAM 用户指南中的 IAM JSON 策略参考。

主题

- IAM policy 概述
- IAM policy 的最佳实践
- 在 IAM policy 语句中指定 KMS 密钥

- 使用 AWS KMS 控制台所需的权限
- AWS 高级用户的托管策略
- IAM 策略示例

IAM policy 概述

您可以通过以下方式使用 IAM policy：

- 将权限策略附加到角色以启用联合身份验证或跨账户权限 – 您可以将 IAM policy 附加到 IAM 角色以启用联合身份验证，允许跨账户权限，或者向运行在 EC2 实例上的应用程序授予权限。有关 IAM 角色各种使用场景的更多信息，请参阅 IAM 用户指南中的 IAM 角色。
- 将权限策略附加到用户或组 – 您可以附加允许某个用户或用户组调用 AWS KMS 操作的策略。但是，IAM 最佳实践建议您尽可能使用具有临时凭证的身份，例如 IAM 角色。

以下示例显示了具有 AWS KMS 权限的 IAM 策略。此策略允许附加到其上的 IAM 身份获取列出所有 KMS 密钥和别名。

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

与所有 IAM policy 一样，此策略没有 `Principal` 元素。将 IAM policy 附加到 IAM 身份时，该身份将获取策略中指定的权限。

有关显示所有 AWS KMS API 操作及其适用的资源的表格，请参阅权限参考。

IAM policy 的最佳实践

确保访问 AWS KMS keys 权限对您的所有 AWS 资源的安全至关重要。KMS 密钥用于保护您的许多最敏感的资源 AWS 账户。花点时间设计控制对 KMS 密钥的访问权限的密钥策略、IAM policy、授权和 VPC 端点策略。

在控制对 KMS 密钥的访问的 IAM policy 语句中，使用最低权限原则。仅为 IAM 委托人授予他们对必须使用或管理的 KMS 密钥的所需权限。

以下最佳实践适用于控制 AWS KMS 密钥和别名访问权限的 IAM 策略。有关一般性的 IAM policy 最佳实践，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

使用密钥策略

尽可能在影响一个 KMS 密钥的密钥策略中提供权限，而不是在可应用于许多 KMS 密钥的 IAM policy 中提供权限，包括其他 AWS 账户中的权限。这对于诸如 kms: PutKeyPolicy 和 kms: 之类的敏感权限尤其重要，对于决定如何保护数据的加密操作ScheduleKeyDeletion也是如此。

限制 CreateKey 权限

仅向需要密钥 (kms:CreateKey) 的委托人授予创建密钥 (kms:) 的权限。创建 KMS 密钥的委托人还会设置其密钥策略，以便他们可以授予自己和其他人使用和管理他们创建的 KMS 密钥的权限。允许此权限时，请考虑通过使用策略条件限制它。例如，您可以使用 kms: KeySpec 条件来限制对称加密 KMS 密钥的权限。

在 IAM policy 中指定 KMS 密钥

最佳实践是在策略语句的 Resource 元素中指定权限所应用到的每个 KMS 密钥的密钥 ARN。此实践限制委托人需要的 KMS 密钥的权限。例如，此 Resource 元素仅列出主体需要使用的 KMS 密钥。

```
"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"
]
```

当指定 KMS 密钥不切实际时，请使用一个限制访问可信 AWS 账户 和区域（例如）中的 KMS 密钥的Resourcearn:aws:kms:*region*:*account*:key/*值。或者限制对受信任方所有区域 (*) 的 KMS 密钥的访问权限 AWS 账户，例如arn:aws:kms:*:*account*:key/*。

您无法使用密钥 ID、别名名称或者别名 ARN 表示 IAM policy 的 Resource 字段中的 KMS 密钥。如果您指定别名 ARN，则策略将应用于别名，而不是 KMS 密钥。有关别名的 IAM policy 的信息，请参阅。控制对别名的访问

在 IAM policy 中避免使用 "Resource": "*"

谨慎地使用通配符 (*)。在密钥策略中，Resource 元素中的通配符表示密钥策略附加到的 KMS 密钥。但是在 IAM 策略中，仅在Resource元素 ("Resource": "*") 中使用通配符即可将权限应用

于委托人账户有权 AWS 账户 使用的所有 KMS 密钥。这可能包括其他密钥中的 KMS 密钥 AWS 账户，以及委托人账户中的 KMS 密钥。

例如，要在另一个账户中使用 KMS 密钥 AWS 账户，委托人需要获得外部账户中 KMS 密钥的密钥策略以及自己账户中的 IAM 策略的许可。假设一个任意账户授予了您对其 KMS 密钥的 AWS 账户 kms:Decrypt 权限。若如此，您账户中授予角色对所有 KMS 密钥 (`"Resource": "*"`) 的 `kms:Decrypt` 权限的 IAM policy 将满足要求的 IAM 部分。因此，可以担任该角色的委托人现在可以使用不可信账户中的 KMS 密钥解密密文。他们的操作条目会出现在两个账户的 CloudTrail 日志中。

特别是，避免在允许以下 API 操作的策略语句中使用 `"Resource": "*"`。可以在其他的 KMS 密钥上调用这些操作 AWS 账户。

- DescribeKey
- GetKeyRotationStatus
- 加密操作（加密、解密、、、、、GenerateDataKey、GenerateDataKeyPair、、GenerateDataKeyWithoutPlaintextGenerat名GetPublicKeyReEncrypt、验证）
- CreateGrant, ListGrants, ListRetirableGrants, RetireGrant, RevokeGrant

何时使用 "Resource": "*"

在 IAM policy 中，仅将 `Resource` 元素中的通配符用于需要它的权限。只有以下权限才需要 `"Resource": "*"` 元素。

- kms: CreateKey
- kms: GenerateRandom
- kms: ListAliases
- kms: ListKeys
- 自定义密钥存储库的权限，例如 k ms: CreateCustomKeyStore 和 kms: ConnectCustomKeyStore。

> **Note**
>
> 别名操作（kms:、kms: CreateAlias 、k ms: UpdateAlias、kms: DeleteAlias）的权限必须附加到别名和 KMS 密钥。您可以使用 IAM policy 中的 `"Resource": "*"` 来表示别名和 KMS 密钥，或者在 `Resource` 元素中指定别名和 KMS 密钥。有关示例，请参阅控制对别名的访问。

本主题中的示例提供了有关设计 KMS 密钥的 IAM policy 的详细信息和指导。有关一般 AWS KMS 最佳实践指南，请参阅AWS Key Management Service 最佳实践 (PDF)。有关所有 AWS 资源的 IAM 最佳实践，请参阅 IAM 用户指南中的 IAM 安全最佳实践。

在 IAM policy 语句中指定 KMS 密钥

您可以使用 IAM policy 来允许委托人使用或管理 KMS 密钥。KMS 密钥在策略语句的 `Resource` 元素中指定。

- 要在 IAM policy 语句中指定 KMS 密钥，必须使用其密钥 ARN。您不能使用密钥 ID、别名名称或别名 ARN 来标识 IAM policy 语句中的 KMS 密钥。

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

  要根据别名控制对 KMS 密钥的访问权限，请使用 k ms: RequestAlias 或 k ms: ResourceAliases 条件密钥。有关更多信息，请参阅 AWS KMS 中的 ABAC。

  仅在控制别名操作（例如、或）访问权限的策略声明中使用别名 ARN 作为CreateAlias资源。UpdateAliasDeleteAlias有关更多信息，请参阅 控制对别名的访问。
- 要在账户和区域中指定多个 KMS 密钥，请在密钥 ARN 的区域或资源 ID 位置中使用通配符 (*)。

  例如，要指定账户的美国西部（俄勒冈）区域中的所有 KMS 密钥，请使用“`Resource": "arn:aws:kms:us-west-2:111122223333:key/*`”。要指定账户的所有区域中的所有 KMS 密钥，请使用“`Resource": "arn:aws:kms:*:111122223333:key/*`”。
- 要表示所有 KMS 密钥，请单独使用通配符 ("*")。对于不使用任何特定 KMS 密钥（即、和）的操作 CreateKeyGenerateRandomListAliases，请使用此格式ListKeys。

在编写策略语句时，最佳实践是只指定委托人需要使用的 KMS 密钥，而不是授予他们对所有 KMS 密钥的访问权限。

例如，以下 IAM 策略声明仅允许委托人对策略声明`Resource`元素中列出的 KMS 密钥调用DescribeKeyGenerateDataKey、、Decrypt 操作。通过密钥 ARN 指定 KMS 密钥是一种最佳实践，可确保权限仅限于指定的 KMS 密钥。

```
{
  "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"
    ]
  }
}
```

要将权限应用于特定可信对象中的所有 KMS 密钥 AWS 账户，可以在区域和密钥 ID 位置中使用通配符 (*)。例如，以下策略语句允许委托人对两个可信示例账户的中的 KMS 密钥调用指定操作。

```
{
  "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/*"
    ]
  }
}
```

您还可以单独在 `Resource` 元素中使用通配符 ("*")。由于它允许访问帐户有权使用的所有 KMS 密钥，因此建议主要用于没有特定 KMS 密钥的操作和 `Deny` 语句。您还可以在仅允许不太敏感的只读操作的策略语句中使用它。要确定某项 AWS KMS 操作是否涉及特定的 KMS 密钥，请在中表的 “资源” 列中查找 KMS 密钥值the section called “权限参考”。

例如，以下策略语句使用 `Deny` 效果来禁止委托人对任何 KMS 密钥使用指定的操作。它在 `Resource` 元素中使用通配符来表示所有 KMS 密钥。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [
      "kms:CreateKey",
      "kms:PutKeyPolicy",
      "kms:CreateGrant",
      "kms:ScheduleKeyDeletion"
    ],
    "Resource": "*"
  }
}
```

以下策略语句单独使用通配符来表示所有 KMS 密钥。但它只允许不太敏感的只读操作和不适用于任何特定 KMS 密钥的操作。

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

使用 AWS KMS 控制台所需的权限

要使用 AWS KMS 控制台，用户必须拥有一组允许他们使用控制台中的 AWS KMS 资源的最低权限 AWS 账户。除这些 AWS KMS 权限以外，用户还必须拥有列出 IAM 用户和 IAM 角色的权限。如果您创建的 IAM 策略比所需的最低权限更严格，则 AWS KMS 控制台将无法按预期运行，供使用该 IAM 策略的用户使用。

有关允许用户对 AWS KMS 控制台进行只读访问所需的最低权限，请参阅允许用户在 AWS KMS 控制台中查看 KMS 密钥。

要允许用户使用 AWS KMS 控制台创建和管理 KMS 密钥，请将AWSKeyManagementServicePowerUser托管策略附加到用户，如下一节所述。

对于通过 AWS 开发工具包、AWS Command Line Interface 或 AWS Tools for PowerShell 使用 AWS KMS API 的用户，您不需要允许最低的控制台权限。但是，您的确需要授予以下用户使用 API 的权限。有关更多信息，请参阅 权限参考。

AWS 高级用户的托管策略

您可以使用 AWSKeyManagementServicePowerUser 托管式策略为您账户中的 IAM 主体授予高级用户的权限。高级用户可以创建 KMS 密钥、使用和管理他们创建的 KMS 密钥，以及查看所有 KMS 密钥和 IAM 身份。具有 AWSKeyManagementServicePowerUser 托管式策略的主体还可以从其他来源获取权限，包括密钥策略、其他 IAM policy 和授权。

AWSKeyManagementServicePowerUser是一项 AWS 托管 IAM 策略。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

> **Note**
>
> 此策略中特定于 KMS 密钥的权限（例如kms:TagResource和kms:GetKeyRotationStatus）仅在该 KMS 密钥的密钥策略明确允许使用 IAM 策略 AWS 账户 来控制对密钥的访问时才有效。要确认权限是否特定于 KMS 密钥，请参阅 AWS KMS 权限 并在 Resources（资源）列中查找 KMS 密钥的值。
>
> 此策略授予高级用户对任何 KMS 密钥执行操作的权限，以及允许该操作的密钥策略。对于跨账户权限（例如 kms:DescribeKey 和 kms:ListGrants），这可能包括不可信 AWS 账户中的 KMS 密钥。有关详细信息，请参阅 IAM policy 的最佳实践 和 允许其他账户中的用户使用 KMS 密钥。要确认权限是否对其他账户中的 KMS 密钥有效，请参阅 AWS KMS 权限 并查找 Cross-account use（跨账户使用）列中 Yes（是）的值。
>
> 为了让委托人能够毫无错误地查看 AWS KMS 控制台，委托人需要标记：permis GetResources sion，该标签未包含在AWSKeyManagementServicePowerUser策略中。您可以在单独的 IAM policy 中允许此权限。

AWSKeyManagementServicePowerUser托管 IAM 策略包括以下权限。

- 允许主体创建 KMS 密钥。由于此过程包括设置密钥策略，因此高级用户可以授予自己和其他人使用和管理他们创建的 KMS 密钥的权限。
- 允许主体创建和删除所有 KMS 密钥上的别名和标签。更改标签或别名可以允许或拒绝使用和管理 KMS 密钥的权限。有关更多信息，请参阅 AWS KMS 中的 ABAC。
- 允许主体获取有关所有 KMS 密钥的详细信息，包括其密钥 ARN、加密配置、密钥策略、别名、标签和轮换状态。

- 允许主体列出 IAM 用户、组和角色。
- 此策略不允许主体使用或管理他们未创建的 KMS 密钥。但他们可以更改所有 KMS 密钥上的别名和标签，这可能会允许或拒绝其使用或管理 KMS 密钥的权限。

```
{
    "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": "*"
        }
    ]
}
```

IAM 策略示例

在此部分中，可以找到允许执行各种 AWS KMS 操作的权限的示例 IAM policy。

> **Important**
>
> 仅当 KMS 密钥的密钥策略也允许时，才允许提供以下策略中的某些权限。有关更多信息，请参阅 权限参考。

有关编写和格式化 JSON 策略文档的帮助，请参阅 IAM 用户指南中的 IAM JSON 策略参考。

示例

- 允许用户在 AWS KMS 控制台中查看 KMS 密钥
- 允许用户创建 KMS 密钥
- 允许用户使用特定 KMS 密钥进行加密和解密 AWS 账户
- 允许用户使用特定 AWS 账户 和区域中的任何 KMS 密钥进行加密和解密
- 允许用户使用特定 KMS 密钥进行加密和解密
- 阻止用户禁用或删除任何 KMS 密钥

允许用户在 AWS KMS 控制台中查看 KMS 密钥

以下 IAM 策略允许用户以只读方式访问 AWS KMS 控制台。拥有这些权限的用户可以查看其中的所有 KMS 密钥 AWS 账户，但他们无法创建或更改任何 KMS 密钥。

要在AWS 托管式密钥和客户托管密钥页面上查看 K MS 密钥，即使密钥没有标签或别名ListAliases，委托人也需要 k m s:、kms: 和 tag: GetResources 权限。ListKeys在 KMS 密钥详细信息页面上查看可选的 KMS 密钥表列和数据需要其余权限，尤其是 kms: DescribeKey。需要 ia m: ListUsers 和 ia ListRoles m: 权限才能在默认视图中毫无错误地显示密钥策略。要查看自定义密钥存储库页面上的数据以及自定义密钥存储库中 KMS 密钥的详细信息，委托人还需要 k ms: DescribeCustomKeyStores 权限。

如果您限制用户的控制台对特定 KMS 密钥的访问，控制台将显示不可见的每个 KMS 密钥的错误。

此策略包含两个策略语句。第一个策略语句中的 `Resource` 元素允许对示例 AWS 账户的所有区域中的所有 KMS 密钥的指定权限。控制台查看器不需要额外的访问权限，因为 AWS KMS 控制台仅显示委托人账户中的 KMS 密钥。即使他们有权在其他版本中查看 KMS 密钥，也是如此 AWS 账户。其余 AWS KMS 和 IAM 权限需要一个`"Resource": "*"`元素，因为它们不适用于任何特定的 KMS 密钥。

```
{
  "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": "*"
    }
  ]
}
```

允许用户创建 KMS 密钥

以下 IAM policy 允许用户创建所有类型的 KMS 密钥。该`Resource`元素的值`*`是因为该`CreateKey`操作不使用任何特定的 AWS KMS 资源（KMS 密钥或别名）。

要限制用户使用特定类型的 KMS 密钥，请使用 k ms: KeySpec、kms: KeyUsage 和 k ms: KeyOrigin 条件密钥。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "kms:CreateKey",
    "Resource": "*"
  }
}
```

创建密钥的委托人可能需要一些相关权限。

- kms: PutKeyPolicy — 拥有`kms:CreateKey`权限的委托人可以为 KMS 密钥设置初始密钥策略。但是，`CreateKey`调用者必须拥有 k ms: PutKeyPolicy 权限，允许他们更改 KMS 密钥策略，或者必

须指定BypassPolicyLockoutSafetyCheck参数CreateKey，但不建议这样做。CreateKey 调用方可以从 IAM policy 中获得对 KMS 密钥的 kms:PutKeyPolicy 权限，也可以将此权限包含在他们正在创建的 KMS 密钥的密钥策略中。

- kms: TagResource — 要在CreateKey操作期间向 KMS 密钥添加标签，CreateKey调用者必须在 IAM 策略中TagResource拥有 kms: 权限。将此权限包含在新 KMS 密钥的密钥策略中是不够的。但是，如果 CreateKey 调用方在初始密钥策略中包括 kms:TagResource，他们可以在创建 KMS 密钥后在单独调用中添加标签。
- kms: CreateAlias — 在 AWS KMS 控制台中创建 KMS 密钥的委托人必须对 KMS 密钥和别名拥有 kms: CreateAlias 权限。（控制台进行两次调用；一次对 CreateKey，一次对 CreateAlias）。您必须在 IAM policy 中提供别名权限。您可以在密钥策略或 IAM policy 中提供 KMS 密钥权限。有关更多信息，请参阅 控制对别名的访问。

此外kms:CreateKey，以下 IAM 策略提供kms:TagResource对中所有 KMS 密钥的kms:CreateAlias权限 AWS 账户 以及对账户所有别名的权限。它还包括一些只能在 IAM policy 中提供的有用的只读权限。

此 IAM policy 不包含 kms:PutKeyPolicy 权限或可以在密钥策略中设置的任何其他权限。它是在密钥策略中设置这些权限的最佳实践，在该密钥策略中，这些权限专门应用于一个 KMS 密钥。

```
{
  "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": "*"
    }
  ]
}
```

允许用户使用特定 KMS 密钥进行加密和解密 AWS 账户

以下 IAM 策略允许用户使用 111122223333 中的 AWS 账户 任何 KMS 密钥加密和解密数据。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": "arn:aws:kms:*:111122223333:key/*"
  }
}
```

允许用户使用特定 AWS 账户 和区域中的任何 KMS 密钥进行加密和解密

以下 IAM 策略允许用户使用美国西部（俄勒冈）地区的任何 KMS 密钥加密和解密数据。 AWS 账户 111122223333

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt"
    ],
    "Resource": [
      "arn:aws:kms:us-west-2:111122223333:key/*"
    ]
  }
}
```

允许用户使用特定 KMS 密钥进行加密和解密

以下 IAM policy 允许用户使用 Resource 元素中指定的两个 KMS 密钥来加密和解密数据。在 IAM policy 语句中指定 KMS 密钥时，必须使用 KMS 密钥的密钥 ARN。

```
{
  "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"
    ]
  }
}
```

阻止用户禁用或删除任何 KMS 密钥

以下 IAM policy 阻止用户禁用或删除任何 KMS 密钥，即使其他 IAM policy 或密钥策略允许这些权限时也是如此。以显式方式拒绝权限的策略将覆盖所有其他策略，甚至包括那些以显式方式允许相同权限的策略。有关更多信息，请参阅 密钥访问故障排除。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": [
      "kms:DisableKey",
      "kms:ScheduleKeyDeletion"
    ],
    "Resource": "*"
  }
}
```

AWS KMS 中的授权

授权是一种策略分析工具，允许 AWS 主体将 KMS 密钥用于加密操作中。它还可以让他们查看 KMS 密钥 (DescribeKey) 以及创建和管理授权。在授权访问 KMS 密钥时，将考虑授权与密钥策略和 IAM policy。授权通常用于临时权限，因为您可以在不更改密钥策略或 IAM policy 的情况下创建授权、使用其权限并将其删除。

授权通常被与 AWS KMS 集成的 AWS 服务用来加密静态数据。该服务代表账户中的用户创建授权，使用其权限，并在其任务完成后立即停用授权。有关 AWS 服务如何使用授权的详细信息，请参阅服务的用户指南或开发人员指南中的 AWS 服务如何使用 AWS KMS 或静态加密主题。

有关演示如何通过多种编程语言使用授权的代码示例，请参阅 处理授权。

主题

关于授权

授权是一种非常灵活且有用的访问控制机制。当您为 KMS 密钥创建授权时，授权允许被授权主体对 KMS 密钥调用指定授权操作，前提是该授权中指定的所有条件都得到满足。

- 每个授权只允许访问一个 KMS 密钥。您可以在不同的 AWS 账户 中为 KMS 密钥创建授权。
- 授权可以允许访问 KMS 密钥，但不能拒绝访问。
- 每个授权都有一名被授权主体。被授权主体可以在 KMS 密钥的同一个 AWS 账户 中或在不同的账户中代表一个或多个身份。
- 授权只能允许授权操作。授权操作必须由授权中的 KMS 密钥支持。如果您指定了不支持的操作，则CreateGrant请求会失败并出现ValidationError异常。
- 被授权主体可以使用授权给予他们的权限，而无需指定授权，就像权限来自密钥策略或 IAM policy 一样。但是，由于 AWS KMS API 采用最终一致性模型，当您创建、停用或撤销授权时，可能会出现短暂的延迟，才能使更改在整个 AWS KMS 中可用。要立即使用授权中的权限，请使用授权令牌。

- 授权委托人可以删除授权（停用或者撤销它）。删除授权会清除授权允许的所有权限。您不必确定要添加或删除哪些策略来撤销授权。
- AWS KMS 限制每个 KMS 密钥上的授权数量。有关更多信息，请参阅 每个 KMS 密钥的授权数：50000。

在创建授权和给予其他人创建授权的权限时务必谨慎。创建授权的权限会带来安全影响，就像允许 kms: PutKeyPolicy 权限设置策略一样。

- 有权为 KMS 密钥 (`kms:CreateGrant`) 创建授权的用户可以使用授权来允许用户和角色（包括 AWS 服务）使用 KMS 密钥。委托人可以是您自己的 AWS 账户 中的身份或其他账户或组织中的身份。
- 授权只能允许 AWS KMS 运算符子集。您可以使用授权允许委托人查看 KMS 密钥，在加密操作中使用它，以及创建和停用授权。有关详细信息，请参阅授权操作。您还可以使用授权约束来限制对称加密密钥授权中的权限。
- 委托人可以获得从密钥策略或 IAM policy 创建授权的权限。通过策略获得的 `kms:CreateGrant` 权限的主体可以为基于 KMS 密钥的任何授权操作创建授权。这些主体无需拥有他们对密钥的授权权限。当您在策略中允许 `kms:CreateGrant` 权限时，您可以使用策略条件来限制此权限。
- 委托人还可以获得从授权创建授权的权限。这些委托人只能委派他们被授予的权限，即使他们具有来自策略的其他权限也是如此。有关更多信息，请参阅 授予 CreateGrant 权限。

有关与授权相关的概念的帮助，请参阅授权术语。

授权概念

为了有效地使用授权，您需要了解 AWS KMS 使用的术语和概念。

授权约束

限制授权中的权限的条件。目前，AWS KMS 基于请求中的加密上下文支持将授权约束用于加密操作。有关更多信息，请参阅 使用授权约束。

授权 ID

KMS 密钥的授权的唯一标识符。您可以使用授权 ID 和密钥标识符来标识RetireGrant或RevokeGrant请求中的授权。

授权操作

您可以在授权中允许的 AWS KMS 操作。如果您指定其他操作，则CreateGrant请求会失败，但会出现ValidationError异常。这些也是接受授权令牌的操作。有关这些权限的详细信息，请参阅AWS KMS 权限。

这些授权操作实际上代表使用操作的权限。因此，对于 ReEncrypt 操作，您可以指定 ReEncryptFrom、ReEncryptTo 或此两者 ReEncrypt*。

授权操作包括：

- 加密操作
  - Decrypt
  - Encrypt
  - GenerateDataKey
  - GenerateDataKeyPair
  - GenerateDataKeyPairWithoutPlaintext
  - GenerateDataKeyWithoutPlaintext
  - GenerateMac
  - ReEncryptFrom
  - ReEncryptTo
  - Sign
  - 验证
  - VerifyMac
- 其他操作
  - CreateGrant
  - DescribeKey
  - GetPublicKey
  - RetireGrant

您允许的授权操作必须由授权中的 KMS 密钥支持。如果您指定了不支持的操作，则CreateGrant请求会失败并出现ValidationError异常。例如，对称加密 KMS 密钥的授权不能允许 Sign、Verify、GenerateMac 或 VerifyMac 操作。非对称 KMS 密钥的授权不能允许生成数据密钥或数据密钥对的操作。

授权令牌

AWS KMS API 采用最终一致性模型。当您创建授权时，可能会出现短暂的延迟，才能使更改在整个 AWS KMS 中可用。更改通常需要不到几秒钟的时间即可在整个系统中传播，但在某些情况下，可能需要几分钟。如果您尝试在系统中完全传播之前使用授权，您可能会收到访问被拒绝的错误。授权令牌允许您引用授权并立即使用授权权限。

授权令牌是代表授权的唯一、非秘密、长度可变的 base64 编码字符串。您可以使用授权令牌来标识任何授权操作中的授权。但是，由于令牌值是哈希摘要，它不会显示有关授权的任何详细信息。

授权令牌设计为仅在授权传播到整个 AWS KMS 中时使用。之后，被授权者委托人可以在不提供授权令牌或授权的任何其他证据的情况下使用授权中的权限。您可以随时使用授权令牌，但是一旦授权达到最终一致性，AWS KMS 就会使用授权来确定权限，而不是授权令牌。

例如，以下命令调用该GenerateDataKey操作。它使用授权令牌来表示给予调用者（被授权者委托人）对指定的 KMS 密钥调用 `GenerateDataKey` 的权限的授权。

```
$ aws kms generate-data-key \
        --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
        --key-spec AES_256 \
        --grant-token $token
```

您还可以使用授权令牌来标识管理授权的操作中的授权。例如，即将退休的委托人可以在调用RetireGrant操作时使用授权令牌。

```
$ aws kms retire-grant \
        --grant-token $token
```

`CreateGrant` 是返回授权令牌的唯一操作。您无法从任何其他AWS KMS操作或该操作的CloudTrail 日志事件中获取授权令牌。 CreateGrant ListGrants和ListRetirableGrants操作返回授权 ID，但不返回授权令牌。

有关更多信息，请参阅 使用授权令牌。

被授权者委托人

获取授权中指定的权限的身份。每个授权都有一个被授权主体，但被授权主体可以代表多个身份。

被授权者主体可以是任何 AWS 主体，包括 AWS 账户（根）、IAM 用户、IAM 角色、联合角色或用户或代入的角色用户。被授权者委托人可以与 KMS 密钥位于同一账户中，也可以位于不同的账户中。但是，被授权者委托人不能是服务委托人、IAM 组，或 AWS组织。

> **Note**
>
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

停用（授权）

终止授权。当您使用完权限时，将停用授权。

撤销和停用授权都会删除授权。但是，停用由授权中指定的委托人完成。撤消通常由密钥管理员执行。有关更多信息，请参阅 停用和撤销授权。

停用委托人

可以停用授权的委托人。您可以在授权中指定停用委托人，但这不是必需的。停用委托人可以是任何 AWS 委托人，包括 AWS 账户、IAM 用户、IAM 角色、联合身份用户以及代入的角色用户。停用委托人可以与 KMS 密钥位于同一账户中，也可以位于不同的账户中。

> **Note**
>
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

除了授权中指定的停用委托人外，还可通过在其中创建授权的 AWS 账户 停用授权。如果授权允许 `RetireGrant` 操作，被授权者委托人可以停用授权。另外，AWS 账户 或 停用委托人的 AWS 账户 可以委派权限以停用相同 AWS 账户 中的 IAM 委托人的授权。有关更多信息，请参阅 停用和撤销授权。

撤销（授予）

终止授权。您将撤销积极拒绝授权允许的权限的授权。

撤销和停用授权都会删除授权。但是，停用由授权中指定的委托人完成。撤消通常由密钥管理员执行。有关更多信息，请参阅 停用和撤销授权。

最终一致性（用于授权）

AWS KMS API 采用最终一致性模型。当您创建、停用或撤销授权时，可能会出现短暂的延迟，才能使更改在整个 AWS KMS 中可用。更改通常需要不到几秒钟的时间即可在整个系统中传播，但在某些情况下，可能需要几分钟。

如果您遇到意外错误，您可能会注意到这个短暂的延迟。例如，如果您尝试在整个 AWS KMS 知晓授权前管理一个新的授权或使用新授权中的权限，您可能会收到访问被拒绝错误。如果您停用或撤销授权，则被授权者委托人可能仍然能够在短时间内使用其权限，直到完全删除该授权为止。典型的策略是重试请求，且一些 AWS 开发工具包包括自动退避和重试逻辑。

AWS KMS 具有缓解这一短暂延迟的功能。

- 要立即使用新授权中的权限，请使用授权令牌。您可以使用授权令牌来引用任何授权操作中的授权。有关说明，请参阅使用授权令牌。
- 该CreateGrant操作具有一个Name参数，可防止重试操作创建重复的授权。

> **Note**
>
> 授权令牌将取代授权的有效性，直到服务中的所有终端节点都使用新的授权状态更新为止。在大多数情况下，最终一致性将在五分钟内实现。

有关更多信息，请参阅AWS KMS 最终一致性。

AWS KMS 授权的最佳实践

AWS KMS 建议在创建、使用和管理授权时使用以下最佳实践。

- 将授权中的权限限制为被授权者委托人所需的权限。使用最小特权访问权限的原则。
- 使用特定的被授权者委托人（如 IAM 角色），并授予被授权委托人仅使用他们所需的 API 操作的权限。
- 使用加密上下文授权约束以确保调用方正在将 KMS 密钥用于预期目的。有关如何在请求中使用加密上下文来保护数据的详细信息，请参阅AWS安全博客 EncryptionContext中的如何使用AWS Key Management Service和保护加密数据的完整性。

> **Tip**
>
> 尽可能使用EncryptionContextEqual授权约束。EncryptionContextSubset授权约束更难正确使用。如果您需要使用它，请仔细阅读文档并测试授权约束以确保它按预期工作。

- 删除重复的授权。重复授权具有相同的密钥 ARN、API 操作、被授权者委托人、加密上下文和名称。如果您停用或撤销原始授予，但保留重复项授权，则剩余的重复授权将构成意外的权限提升。

为了在重试 CreateGrant 请求时避免重复授权，请使用 Name 参数。要检测重复的授权，请使用ListGrants操作。如果您意外创建了重复授权，请尽快停用或撤销该授权。

> **Note**
>
> AWS 托管密钥的授权可能看起来像重复授权，但具有不同的被授权者委托人。ListGrants 响应中的 GranteePrincipal 字段通常包含授权的被授权者委托人。但是，当授权中的被授权者委托人是 AWS 服务时，GranteePrincipal 字段包含服务委托人，该委托人可能表示多个不同的被授权者委托人。

- 请记住，授权不会自动过期。当权限不再需要时，立即停用或撤销授权。未删除的授权可能会对加密资源造成安全风险。

创建授权

在创建授权之前，请了解用于自定义授权的选项。您可以使用授权约束来限制授权中的权限。此外，了解授予 CreateGrant 权限的相关信息。获得从授权创建授权的权限的委托人在其可以创建的授权中受到限制。

主题

- 创建授予
- 使用授权约束
- 授予 CreateGrant 权限

创建授予

要创建授权，请调用该CreateGrant操作。指定 KMS 密钥，被授权者委托人，以及允许的授权操作的列表。您还可以指定一个可选的停用委托人。要自定义授权，请使用可选 Constraints 参数来定义授予约束。

当您创建、停用或撤销授权时，可能会出现短暂的延迟（通常不到五分钟），才能使更改在整个 AWS KMS 中可用。有关更多信息，请参阅最终一致性（用于授权）。

例如，以下 CreateGrant 命令会创建一个授权，以允许被授权代入 keyUserRole 角色的用户对指定的 对称 KMS 密钥 调用 解密 操作。授权使用 RetiringPrincipal 参数，指定可以停用授权的委托人。其中还包含一个授权约束，仅当请求中的加密上下文包含 "Department": "IT" 时才允许该权限。

```
$  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}
```

如果您的代码重试 CreateGrant 操作，或者使用自动重试请求的 AWS SDK，请使用可选的 Name 参数来防止创建重复授权。如果 AWS KMS 针对与现有授权具有相同属性（包括名称）的授权获取一个 CreateGrant 请求，它会将该请求识别为重试，并且不创建新授权。您无法使用 Name 值来标识任何 AWS KMS 操作中的授权。

> **Important**
>
> 不要在授权名称中包含机密或敏感信息。它可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

```
$ 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}
```

有关演示如何通过多种编程语言使用授权的代码示例，请参阅 处理授权。

使用授权约束

授权约束设置授权给予被授权者委托人的权限的条件。授权约束取代密钥策略或 IAM policy 中的条件键。每个授权约束值最多可以包含 8 个加密上下文对。每个授权约束中的加密上下文值不能超过 384 个字符。

> **Important**
>
> 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。

AWS KMS 支持两个授权约束 EncryptionContextEquals 和 EncryptionContextSubset，两者都在加密操作的请求中建立了对加密上下文的要求。

加密上下文授权约束旨在与具有加密上下文参数的授权操作结合使用。

- 加密上下文约束仅在对称加密 KMS 密钥的授权中有效。使用其他 KMS 密钥的加密操作不支持加密上下文。
- 对于 DescribeKey 和 RetireGrant 操作，加密上下文约束将被忽略。DescribeKey 和 RetireGrant 不包括加密上下文参数，但您可以将这些操作包含在具有加密上下文约束的授权中。
- 您可以将授权中的加密上下文约束用于 CreateGrant 操作。加密上下文约束要求使用 CreateGrant 权限创建的任何授权具有同样严格或更严格的加密上下文约束。

AWS KMS 支持以下加密上下文授权约束。

EncryptionContextEquals

使用 EncryptionContextEquals 为允许的请求指定精确的加密上下文。

EncryptionContextEquals 要求请求中的加密上下文对与授权约束中加密上下文对区分大小写的完全匹配。上下文对可以按任意顺序显示，不过每一对中的键和值不能有改变。

例如，如果 EncryptionContextEquals 授权约束需要 "Department": "IT" 加密上下文对，则授权仅在请求中的加密上下文完全是 "Department": "IT" 时，允许指定类型的请求。

EncryptionContextSubset

使用 EncryptionContextSubset 来要求请求包含特定的加密上下文对。

EncryptionContextSubset 要求请求中包含授权约束中的所有加密上下文对（区分大小写的完全匹配），但请求也可以包含其他的加密上下文对。上下文对可以按任意顺序显示，不过每一对中的键和值不能有改变。

例如，如果 EncryptionContextSubset 授权约束需要 Department=IT 加密上下文对，则授权在请求中的加密上下文为 "Department": "IT" 或者包含 "Department": "IT" 以及其他加密上下文对（例如 "Department": "IT","Purpose": "Test"）时，允许指定类型的请求。

要在对称加密 KMS 密钥的授权中指定加密上下文约束，请在CreateGrant操作中使用Constraints参数。此命令创建的授权将向被授权代入 keyUserRole 角色的用户调用 解密 操作的权限。不过，该权限仅在 Decrypt 请求中的加密上下文是 "Department": "IT" 加密上下文对时有效。

```
$ 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}
```

生成的授权与以下项目类似。请注意，向 keyUserRole 角色授予的权限仅在 Decrypt 请求使用授权约束中指定的相同加密上下文对时有效。要查找 KMS 密钥的授权，请使用ListGrants操作。

```
$ 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"
        }
    ]
}
```

为了满足 EncryptionContextEquals 授权约束，Decrypt 操作的请求中的加密上下文必须是 "Department": "IT" 对。来自被授予者委托人的以下请求将满足 EncryptionContextEquals 授权约束。

```
$ 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
```

当授权约束为 EncryptionContextSubset 时，请求中的加密上下文对必须在授权约束中包含加密上下文对，不过请求也可以包括其他加密上下文对。以下授权约束要求请求中的一个加密上下文对是 "Deparment": "IT"。

```
"Constraints": {
   "EncryptionContextSubset": {
       "Department": "IT"
   }
}
```

来自被授权者委托人的以下请求将满足本示例中 EncryptionContextEqual 和 EncryptionContextSubset 授权约束的要求。

```
$ 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
```

但是，来自被授权者委托人的以下请求将满足 EncryptionContextSubset 授权约束，但不满足 EncryptionContextEquals 授权约束。

```
$ 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
```

AWS 服务通常会在向其授予使用 AWS 账户 中的 KMS 密钥的权限的授权中使用加密上下文约束。例如，Amazon DynamoDB 使用类似下面的授权来获得为账户中的 DynamoDB 使用 AWS 托管式密钥 的权限。此授权中的 EncryptionContextSubset 授权约束使授权中的权限仅在请求中的加密上下文包含 "subscriberID": "111122223333" 和 "tableName": "Services" 对时有效。此授权约束意味着，授权仅允许 DynamoDB 将指定的 KMS 密钥用于 AWS 账户 中的特定表。

要获得此输出，请在您的账户中ListGrants对 Dynam AWS 托管式密钥 oDB 运行该操作。

```
$ 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"
        }
    ]
}
```

授予 CreateGrant 权限

授权可以包括调用 CreateGrant 操作的权限。但是，当被授权者委托人获取从授权中，而不是从策略中调用 CreateGrant 的权限时，该权限将收到限制。

- 被授权者委托人只能创建允许父授权中部分或全部操作的授权。
- 他们创建的授权中的授权约束必须至少与父授权中的约束一样严格。

这些限制不适用于从策略中获取 CreateGrant 权限的委托人，尽管它们的权限可以由策略条件限制。

例如，考虑一个授权，该授权允许被授权委托人调用 GenerateDataKey、Decrypt 和 CreateGrant 操作。我们将允许 CreateGrant 权限的授权称为父授权。

```
# 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"
                }
            },
        }
    ]
}
```

被授权者委托人 exampleUser 可以使用此权限创建授权，其中包括在原始授权中指定的操作的任意子集，例如 CreateGrant 和 Decrypt。子级授权不能包含其他操作，如 ScheduleKeyDeletion 或者 ReEncrypt。

此外，子授权中的授权约束必须与父授权具有相同的限制或更严格的限制。例如，子授权可以添加对到父授权中的 EncryptionContextSubset 约束，但不能从中删除对。子授权可以将 EncryptionContextSubset 约束更改为 EncryptionContextEquals 约束，但不能反之。

例如，被授权者委托人可以使用从父级授权那里获得的 CreateGrant 权限以创建以下子级授权。子级授权中的操作是父级授权中操作的子集，并且授权约束更严格。

```
# 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"
                }
            },
        }
    ]
}
```

子级授权中的被授权者委托人 anotherUser 可以使用它们的 CreateGrant 权限来创建授权。然而，anotherUser 创建的授权必须将操作包含在其父授权或子集中，并且授权约束必须相同或更严格。

管理授权

具有所需权限的委托人可以查看、使用和删除（停用或撤销）授权。要优化创建和管理授权的权限，AWS KMS 支持多个策略条件，您可在密钥策略和 IAM policy 中使用它们。

主题

- 控制对授权的访问
- 查看授权

- 使用授权令牌
- 停用和撤销授权

控制对授权的访问

您可以控制对在密钥策略、IAM policy 和授权中创建和管理授权的操作的访问权限。从授权中获得 `CreateGrant` 权限的委托人具有更有限的授权权限。

API 操作	密钥策略或 IAM policy	授权
CreateGrant	✓	✓
ListGrants	✓	-
ListRetirableGrants	✓	-
停用授权	（有限。请参阅 停用和撤销授权）	✓
RevokeGrant	✓	-

您在使用密钥策略或 IAM policy 以控制对创建和管理授权的操作的访问时，可以使用一个或多个以下策略条件来限制权限。AWS KMS 支持以下所有与授权相关的条件键。有关详细信息和示例，请参阅 AWS KMS 条件键。

kms: GrantConstraintType

允许委托人仅在授权包含指定的授权约束时创建授权。

kms: GrantIsFor AWSResource

允许仅在AWS 服务与 AWS KMS 集成时调用 `CreateGrant`、`ListGrants` 或 `RevokeGrant` 的主体代表主体发送请求。

kms: GrantOperations

允许委托人创建授权，但将授权限制为指定操作。

kms: GranteePrincipal

允许委托人仅为指定的被授权者委托人创建授权。

kms: RetiringPrincipal

允许委托人仅在授权指定特定的停用委托人时创建授权。

查看授权

要查看授权，请使用ListGrants操作。您必须指定授权所适用的 KMS 密钥。您还可以按授权 ID 或被授权者委托人筛选授权列表。有关更多示例，请参阅查看授予。

要查看AWS 账户和地区中具有特定退休本金的所有补助金，请使用ListRetirableGrants。响应包括每项授权的详细信息。

> **Note**
>
> `ListGrants` 响应中的 `GranteePrincipal` 字段通常包含授权的被授权者委托人。但是，当授权中的被授权者委托人是 AWS 服务时，`GranteePrincipal` 字段包含服务委托人，该委托人可能表示多个不同的被授权者委托人。

例如，以下命令列出 KMS 密钥的所有授权。

```
$  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"
            ]
```

```
        }
    ]
}
```

使用授权令牌

AWS KMS API 采用最终一致性模型。创建授权时，授权可能不会立即生效。可能会出现短暂的延迟，才能使更改在整个 AWS KMS 中可用。更改通常需要不到几秒钟的时间即可在整个系统中传播，但在某些情况下，可能需要几分钟。更改完全传播到整个系统后，被授权者主体可以使用授权中的权限，而无需指定授权令牌或授权的任何证据。然而，如果授权太新，尚未被所有 AWS KMS 知晓，则请求可能会失败，并显示 AccessDeniedException 错误。

要立即使用新授权中的权限，请使用该授权的授权令牌。保存CreateGrant操作返回的授权令牌。然后为 AWS KMS 操作提交请求中的授权令牌。您可以将授权令牌提交给任何 AWS KMS 授权操作，且您可以在同一请求中提交多个授权令牌。

以下示例使用该CreateGrant操作创建允许GenerateDataKey和解密操作的授权。它将保存 CreateGrant 在 token 变量中返回的授权令牌。然后，在调用 GenerateDataKey 操作时，它使用 token 变量中的授权令牌。

```
# 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
```

具有权限的主体也可以使用授权令牌来停用新授权，即使授权在整个 AWS KMS 中可用之前。（ RevokeGrant 操作不接受授权令牌。 ）有关更多信息，请参阅 停用和撤销授权。

```
# Retire the grant
$ aws kms retire-grant --grant-token $token
```

停用和撤销授权

要删除某个授权，请停用或撤销该授权。

RetireGrant和RevokeGrant操作彼此非常相似。这两个操作都会删除授权，从而消除授权允许的权限。这些操作之间的主要区别在于它们是如何获得授权的。

RevokeGrant

与大多数 AWS KMS 操作一样，对 RevokeGrant 操作的访问通过密钥策略和 IAM policy 控制。任何kms:RevokeGrant获得许可的委托人都可以调用RevokeGrant该 API。该权限包含在授予给密钥管理员的标准权限中。通常，管理员会撤销授权以拒绝授权允许的权限。

RetireGrant

授权决定谁可以停用它。此设计使您能够控制授权的生命周期，而无需更改密钥策略或 IAM policy。通常，当您使用授权的权限时，将停用授权。

授权可以通过授权中指定的可选停用委托人停用。被授权者委托人还可以停用授权，但只有当他们也是停用委托人或者授权包括 RetireGrant 操作时。作为备份，在其中创建授权的 AWS 账户 可以停用授权。

有一个可用于 IAM policy 的 kms:RetireGrant 权限，但它具有有限的实用工具。授权中指定的委托人无需 kms:RetireGrant 权限即可停用授权。单独的 kms:RetireGrant 权限不允许委托人停用授权。kms:RetireGrant 权限在密钥策略中无效。

- 若要拒绝停用授权的权限，您可以使用具有 kms:RetireGrant 权限的 Deny 操作。
- 拥有 KMS 密钥的 AWS 账户可以将 kms:RetireGrant 权限委托给账户中的 IAM 主体。
- 如果停用主体是其他 AWS 账户，则该其他账户中的管理员可以使用 kms:RetireGrant 将停用授权的权限委托给该账户中的 IAM 主体。

AWS KMS API 采用最终一致性模型。当您创建、停用或撤销授权时，可能会出现短暂的延迟，才能使更改在整个 AWS KMS 中可用。更改通常需要不到几秒钟的时间即可在整个系统中传播，但在某些情况下，可能需要几分钟。如果您需要在某个新授权可在整个 AWS KMS 中使用前立即删除它，请使用授予令牌停用该授权。您不能使用授权令牌撤销授权。

通过 VPC 终端节点连接到 AWS KMS

您可以通过 Virtual Private Cloud（VPC）中的一个私有接口终端节点直接连接到 AWS KMS。当您使用接口 VPC 端点时，您的 VPC 与 AWS KMS 之间的通信完全在 AWS 网络内进行。

AWS KMS 支持由 AWS PrivateLink 提供支持的 Amazon Virtual Private Cloud（Amazon VPC）端点。每个 VPC 终端节点都由您的 VPC 子网中一个或多个使用私有 IP 地址的弹性网络接口 (ENI) 代表。

接口 VPC 终端节点将您的 VPC 直接连接到 AWS KMS，而无需 Internet 网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。VPC 中的实例不需要公有 IP 地址便可与 AWS KMS 进行通信。

区域

AWS KMS 支持所有支持 AWS KMS 的 AWS 区域 中的 VPC 端点和 VPC 端点策略。

主题

AWS KMS VPC 端点注意事项

请先查看 AWS PrivateLink 指南中的接口终端节点属性和限制主题，然后再为 AWS KMS 设置接口 VPC 终端节点。

AWS KMS 对 VPC 终端节点的支持包括以下内容。

- 您可以使用 VPC 端点从 VPC 调用所有 AWS KMS API 操作。
- 您可以创建连接到 AWS KMS 区域端点或 AWS KMS FIPS 端点的接口 VPC 端点。
- 您可以使用 AWS CloudTrail 日志来审核您通过 VPC 终端节点使用 KMS 密钥的情况。有关更多信息，请参阅 记录您的 VPC 终端节点。

为 AWS KMS 创建 VPC 终端节点

您可以使用 Amazon VPC 控制台或 Amazon VPC API 为 AWS KMS 创建 VPC 终端节点。有关更多信息，请参阅 AWS PrivateLink 指南中的创建接口端点。

- 要为 AWS KMS 创建 VPC 终端节点，请使用以下服务名称：

```
com.amazonaws.region.kms
```

例如，在美国西部（俄勒冈）区域 (us-west-2)，服务名称为：

```
com.amazonaws.us-west-2.kms
```

- 要创建连接到 AWS KMS FIPS 端点的 VPC 端点，请使用以下服务名称：

```
com.amazonaws.region.kms-fips
```

例如，在美国西部（俄勒冈）区域 (us-west-2)，服务名称为：

```
com.amazonaws.us-west-2.kms-fips
```

为了更轻松地使用 VPC 终端节点，您可以为 VPC 终端节点启用私有 DNS 名称。如果选择 Enable DNS Name（启用 DNS 名称）选项，标准 AWS KMS DNS 主机名将解析为您的 VPC 端点。例如，`https://kms.us-west-2.amazonaws.com` 将解析为连接到服务名称 `com.amazonaws.us-west-2.kms` 的 VPC 端点。

此选项可让您更轻松地使用 VPC 终端节点。默认情况下，AWS 开发工具包和 AWS CLI 使用标准 AWS KMS DNS 主机名，因此您不需要在应用程序和命令中指定 VPC 终端节点 URL。

有关更多信息，请参阅 AWS PrivateLink 指南中的通过接口终端节点访问服务。

连接到 AWS KMS VPC 终端节点

您可以使用 AWS 开发工具包、AWS CLI 或 AWS Tools for PowerShell 通过 VPC 终端节点连接到 AWS KMS。要指定 VPC 终端节点，请使用其 DNS 名称。

例如，此 list-keys 命令使用 `endpoint-url` 参数指定 VPC 终端节点。要使用类似命令，请将示例中的 VPC 终端节点 ID 替换为您账户中的 ID。

```
$ aws kms list-keys --endpoint-url https://vpce-1234abcdf5678c90a-09p7654s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com
```

如果在创建 VPC 终端节点时启用了私有主机名，则无需在 CLI 命令或应用程序配置中指定 VPC 终端节点 URL。标准 AWS KMS DNS 主机名将解析为您的 VPC 端点。默认情况下，AWS CLI 和开发工具

包使用此主机名，因此您可以立即开始使用 VPC 端点连接到 AWS KMS 区域端点，而无需在您的脚本和应用程序中更改任何内容。

要使用私有主机名，您的 VPC 的 `enableDnsHostnames` 和 `enableDnsSupport` 属性必须设置为 `true`。要设置这些属性，请使用ModifyVpcAttribute操作。有关详细信息，请参阅《Amazon VPC 用户指南》中的查看和更新 VPC 的 DNS 属性。

控制对 VPC 终端节点的访问

要控制对 AWS KMS 的 VPC 终端节点的访问，请附加 VPC 终端节点策略到您的 VPC 终端节点中。终端节点策略确定委托人是否可以使用 VPC 终端节点调用对 AWS KMS 资源的 AWS KMS 操作。

您可以在创建终端节点时创建 VPC 终端节点策略，并且可以随时更改 VPC 终端节点策略。使用 VPC 管理控制台或CreateVpcEndpoint或ModifyVpcEndpoint操作。您还可以通过使用 AWS CloudFormation 模板创建和更改 VPC 终端节点策略。有关使用 VPC 管理控制台的帮助，请参阅 AWS PrivateLink 指南中的创建接口终端节点和修改接口终端节点。

> **Note**
>
> AWS KMS 支持从 2020 年 7 月开始的 VPC 终端节点策略。在该日期之前创建的 AWS KMS 的 VPC 终端节点具有默认的 VPC 终端节点策略，但您可以随时更改它。

有关编写和格式化 JSON 策略文档的帮助，请参阅 IAM 用户指南中的 IAM JSON 策略参考。

主题

- 关于 VPC 终端节点策略
- 默认的 VPC 终端节点策略
- 创建 VPC 端点策略
- 查看 VPC 终端节点策略

关于 VPC 终端节点策略

对于使用 VPC 终端节点才能成功的 AWS KMS 请求，委托人需要来自以下两个来源的权限：

- 密钥策略、IAM policy 或者授权必须授予委托人对资源（KMS 密钥或别名）调用操作的权限。
- VPC 终端节点策略必须授予委托人使用终端节点发出请求的权限。

例如，密钥策略可能授予委托人对特定 KMS 密钥调用 Decrypt 的权限。但是，VPC 终端节点策略可能不允许该委托人通过使用终端节点对该 KMS 密钥调用 Decrypt。

或者，VPC 终端节点策略可能允许委托人使用终端节点调DisableKey用某些 KMS 密钥。但是，如果委托人没有来自密钥策略、IAM policy 或授权的权限，请求将失败。

默认的 VPC 终端节点策略

每个 VPC 终端节点都有 VPC 终端节点策略，但您无需指定策略。如果未指定策略，则默认的终端节点策略允许所有委托人对终端节点上的所有资源执行所有操作。

然而，对于 AWS KMS 资源，委托人还必须有权从密钥策略、IAM policy 或者授权中调用操作。因此，在实践中，默认策略表示，如果委托人有权对资源调用操作，他们也可以通过使用终端节点调用该操作。

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Principal": "*",
      "Resource": "*"
    }
  ]
}
```

要允许主体仅将 VPC 终端节点用于其允许操作的子集，请创建或更新改 VPC 终端节点策略。

创建 VPC 端点策略

VPC 终端节点策略确定委托人是否有权使用 VPC 终端节点对资源执行操作。对于 AWS KMS 资源，委托人还必须有权从密钥策略、IAM policy 或者授权中执行操作。

每个 VPC 终端节点策略语句都需要以下元素：

- 可执行操作的委托人
- 可执行的操作
- 可对其执行操作的资源

策略语句不指定 VPC 终端节点。它适用于策略所附加到的任何 VPC 终端节点。有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问权限。

下面是用于 AWS KMS 的 VPC 终端节点策略的示例。当连接到 VPC 终端节点时，此策略允许 ExampleUser 使用 VPC 终端节点对指定 KMS 密钥调用指定的操作。使用类似于此策略的策略之前，请将示例委托人和密钥 ARN 替换为您账户中的有效值。

```
{
   "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 记录使用 VPC 终端节点的所有操作。但是，您的 CloudTrail 日志不包括其他账户中的委托人请求的操作或其他账户中的 KMS 密钥的操作。

因此，您可能需要创建 VPC 终端节点策略，以防止外部账户中的委托人使用 VPC 终端节点对本地账户中的任何密钥的调用任何 AWS KMS 操作。

以下示例使用 aws: PrincipalAccount 全局条件密钥拒绝所有委托人访问所有 KMS 密钥的所有操作，除非委托人位于本地账户中。使用类似于此策略的策略之前，请使用有效值替换示例账户 ID。

```
{
  "Statement": [
    {
      "Sid": "AccessForASpecificAccount",
      "Principal": {"AWS": "*"},
      "Action": "kms:*",
      "Effect": "Deny",
      "Resource": "arn:aws:kms:*:111122223333:key/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "111122223333"
```

```
        }
      }
    }
  ]
}
```

查看 VPC 终端节点策略

要查看终端节点的 VPC 终端节点策略，请使用 VPC 管理控制台或DescribeVpcEndpoints操作。

以下 AWS CLI 命令获取具有指定 VPC 终端节点 ID 的终端节点的策略。

在使用此命令之前，请将示例终端节点 ID 替换为您账户中的有效终端节点 ID。

```
$ aws ec2 describe-vpc-endpoints \
--query 'VpcEndpoints[?VpcEndpointId==`vpce-1234abcdf5678c90a`].[PolicyDocument]'
--output text
```

在策略语句中使用 VPC 终端节点

您可以在请求来自于 VPC 或使用 VPC 终端节点时控制对 AWS KMS 资源和操作的访问。为此，请在密钥策略或 IAM policy 中使用以下全局条件键之一。

- 使用 `aws:sourceVpce` 条件键基于 VPC 终端节点授予或限制访问。
- 使用 `aws:sourceVpc` 条件键基于托管私有终端节点的 VPC 授予或限制访问。

> **Note**
>
> 根据您的 VPC 终端节点创建密钥策略和 IAM policy 时要小心。如果策略语句要求请求来自特定的 VPC 或 VPC 终端节点，则来自代表您使用 AWS KMS 资源的集成 AWS 服务的请求可能会失败。有关帮助信息，请参阅 在具有 AWS KMS 权限的策略中使用 VPC 终端节点条件。此外，当请求来自 Amazon VPC 终端节点时，`aws:sourceIP` 条件键也不起作用。要限制对 VPC 终端节点的请求，请使用 `aws:sourceVpce` 或 `aws:sourceVpc` 条件键。有关更多信息，请参阅《AWS PrivateLink 指南》中的 VPC 终端节点和 VPC 终端节点服务的身份和访问管理。

您可以使用这些全局条件密钥来控制对AWS KMS keys（KMS 密钥）、别名的访问权限，以及对此类操作的访问权限 CreateKey，这些操作不依赖于任何特定资源。

例如，以下示例密钥策略允许用户仅在请求使用指定的 VPC 终端节点时，才使用 KMS 密钥执行某些加密操作。当用户向 AWS KMS 发出请求时，系统会将请求中的 VPC 终端节点 ID 与策略中的 `aws:sourceVpce` 条件键值进行比较。如果它们不匹配，则请求会被拒绝。

要使用类似这样的策略，请将占位符 AWS 账户 ID 和 VPC 终端节点 ID 替换为您账户中的有效值。

```
{
    "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"
                }
            }
        }

    ]
}
```

您还可以使用 `aws:sourceVpc` 条件键基于 VPC 终端节点所在的 VPC 限制对您的 KMS 密钥的访问。

以下示例密钥策略仅允许来自 vpc-12345678 的命令管理 KMS 密钥。另外，它只允许来自 vpc-2b2b2b2b 的命令使用 KMS 密钥执行加密操作。如果应用程序在一个 VPC 中运行，但您使用第二个隔离的 VPC 执行管理功能，则可以使用这样的策略。

要使用类似这样的策略，请将占位符 AWS 账户 ID 和 VPC 终端节点 ID 替换为您账户中的有效值。

```
{
    "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": "*",
        }
    ]
}
```

记录您的 VPC 终端节点

AWS CloudTrail 记录使用 VPC 终端节点的所有操作。当对 AWS KMS 的请求使用 VPC 终端节点时，VPC 终端节点 ID 出现在记录该请求的 AWS CloudTrail 日志条目中。您可以使用终端节点 ID 来审核您的 AWS KMS VPC 终端节点的使用情况。

但是，您的 CloudTrail 日志不包括其他账户中的委托人请求的操作或其他账户中对 KMS 密钥和别名的 AWS KMS操作请求。此外，为了保护您的 VPC，被 VPC 终端节点策略拒绝但却以其他方式允许的请求不记录在 AWS CloudTrail 中。

例如，此示例日志条目记录了使用 VPC 终端节点的 GenerateDataKey 请求。vpcEndpointId 字段出现在日志条目的末尾。

```
{
  "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"
}
```

的条件密钥 AWS KMS

您可以在密钥策略和 IAM 策略中指定控制 AWS KMS 资源访问的条件。仅当条件为 True 时，策略语句才有效。例如，您可能希望策略语句仅在特定日期后生效。或者，您可能希望策略语句根据 API 请求中是否存在特定值来控制访问。

要指定条件，请结合使用策略语句的 Condition 元素中的条件键与 IAM 条件运算符。有些条件键通常适用于 AWS；另一些则特定于 AWS KMS。

条件密钥值必须遵守密 AWS KMS 钥策略和 IAM 策略的字符和编码规则。有关密钥策略文档规则的详细信息，请参阅 密钥策略格式。有关 IAM policy 文档规则的详细信息，请参阅《IAM 用户指南》中的 IAM 名称要求。

主题

- AWS 全局条件键
- AWS KMS 条件键
- AWS KMSAWS Nitro Enclaves 的条件密钥

AWS 全局条件键

AWS 定义全局条件密钥，这是一组策略条件密钥，适用于使用 IAM 进行访问控制的所有 AWS 服务。AWS KMS 支持所有全局条件键。您可以在 AWS KMS 密钥策略和 IAM 策略中使用它们。

例如，只有当请求中的委托人由条件键值中的 Amazon 资源名称 AWS KMS key (ARN) 表示时，您才可以使用 aws: PrincipalArn 全局条件密钥允许访问 (KMS 密钥)。要在中支持基于属性的访问控制 (ABAC) AWS KMS，您可以在 IAM 策略中使用 aws:ResourceTag/tag-key 全局条件密钥来允许访问带有特定标签的 KMS 密钥。

在委托人为 AWS 服务主体的策略中，为了防止AWS 服务被用作混淆的副手，您可以使用aws:SourceArn或aws:SourceAccount全局条件键。有关更多信息，请参阅 使用 aws:SourceArn 或 aws:SourceAccount 条件键。

有关 AWS 全局条件密钥的信息，包括可用的请求类型，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。有关在 IAM policy 中使用全局条件键的示例，请参阅 IAM 用户指南中的控制对请求的访问和控制标签密钥。

以下主题提供有关使用基于 IP 地址和 VPC 终端节点的条件键的特殊指导。

主题

- 在具有 AWS KMS 权限的策略中使用 IP 地址条件
- 在具有 AWS KMS 权限的策略中使用 VPC 终端节点条件

在具有 AWS KMS 权限的策略中使用 IP 地址条件

您可以使用 AWS KMS 在集成 AWS 服务中保护您的数据。但是，在允许或拒绝访问的同一策略声明中指定 IP 地址aws:SourceIp条件运算符或条件密钥时，请谨慎行事 AWS KMS。例如，“AWS 基于源 IP 拒绝访问” 中的AWS策略将 AWS 操作限制为来自指定 IP 范围的请求。

请考虑以下情况：

1. 您向 IAM 身份附加了如下所示的策略AWS： AWS 基于源 IP 拒绝访问。您将aws:SourceIp 条件键的值设置为该用户公司的 IP 地址范围。此 IAM 身份还附加了允许其使用 Amazon EBS、Amazon EC2 和 AWS KMS的其他策略。
2. 该身份试图将一个加密的 EBS 卷挂载到 EC2 实例。即使用户有权使用所有相关服务，此操作也会失败并显示授权错误。

第 2 步失败，因为解密卷加密数据密钥的请求来自与 Amazon EC2 基础设施关联的 IP 地址。 AWS KMS 要想成功，请求必须来自始发用户的 IP 地址。由于步骤 1 中的策略明确拒绝除来自指定 IP 地址以外的所有请求，因此将不允许 Amazon EC2 对 EBS 卷的加密数据密钥进行解密。

此外，当请求来自 Amazon VPC 终端节点时，aws:sourceIP 条件键也不起作用。要限制对 VPC 终端节点（包括 AWS KMS VPC 终端节点）的请求，请使用 aws:sourceVpce 或 aws:sourceVpc 条件键。有关更多信息，请参阅 Amazon VPC 用户指南 中的 VPC 终端节点 - 控制终端节点的使用。

在具有 AWS KMS 权限的策略中使用 VPC 终端节点条件

AWS KMS 支持由提供支持的亚马逊虚拟私有云（亚马逊 VPC）终端节点AWS PrivateLink。当请求来自 VPC 或使用 VPC 终端节点时，您可以在密钥策略和 IAM 策略中使用以下全局条件密钥来控制对 AWS KMS 资源的访问。有关更多信息，请参阅 在策略语句中使用 VPC 终端节点。

- aws:SourceVpc 将访问限制为来自指定 VPC 的请求。
- aws:SourceVpce 将访问限制为来自指定 VPC 终端节点的请求。

如果您使用这些条件密钥来控制对 KMS 密钥的访问，则可能会无意中拒绝访问代表您使用的 AWS AWS KMS 服务。

请注意避免出现类似 IP 地址条件键示例的情况。如果您将对 KMS 密钥的请求限制在 VPC 或 VPC 终端节点上，则 AWS KMS 从 Amazon S3 或 Amazon EBS 等集成服务对的调用可能会失败。即使源请求最终来源于 VPC 或 VPC 终端节点，也会发生这种情况。

AWS KMS 条件键

AWS KMS 提供了一组可在密钥策略和 IAM 策略中使用的条件密钥。这些条件键特定于 AWS KMS。例如，在控制对对称加密 KMS 密钥的访问时，您可以使用 kms:EncryptionContext:*context-key* 条件键以请求特定的加密上下文。

API 操作请求的条件

许多 AWS KMS 条件密钥根据 AWS KMS 操作请求中参数的值来控制对 KMS 密钥的访问。例如，您可以在 IAM 策略中使用 k ms: KeySpec 条件密钥，仅当CreateKey请求中的KeySpec参数值为时才允许使用该CreateKey操作RSA_4096。

即使该参数未出现在请求中（例如当使用参数的默认值时），此类条件也会起作用。例如，您可以使用 k ms: KeySpec 条件密钥允许用户仅在KeySpec参数值为（默认值）时才使用该CreateKey操作。SYMMETRIC_DEFAULT此条件允许 KeySpec 参数值为 SYMMETRIC_DEFAULT 的请求，以及无 KeySpec 参数的请求。

API 操作中使用的 KMS 密钥的条件

某些 AWS KMS 条件密钥可以根据操作中使用的 KMS 密钥的属性来控制对操作的访问。例如，您可以使用 kms: KeyOrigin 条件允许委托人仅GenerateDataKey在 KMS 密钥的密钥为时调用 KMS 密钥。`Origin AWS_KMS`要了解某个条件键能否以这种方式使用，请参阅条件键的说明。

该操作必须是 KMS 密钥资源操作，即为特定 KMS 密钥授权的操作。若要标识 KMS 密钥资源操作，请在操作和资源表中，在操作的 `Resources` 列中查找的 `KMS key` 的值。如果您将这种类型的条件密钥用于未经特定 KMS 密钥资源授权的操作（例如）ListKeys，则该权限将无效，因为条件永远无法满足。授权 `ListKeys` 操作时未涉及 KMS 密钥资源，也无 `KeySpec` 属性。

以下主题描述了每个 AWS KMS 条件键，并包括演示策略语法的示例策略语句。

使用带有条件键的集合运算符

当策略条件比较两组值（例如请求中的标签集和策略中的标签集）时，您需要告诉 AWS 如何比较这两组值。为此，IAM 定义了两个集合运算符 `ForAnyValue` 和 `ForAllValues`。仅将集合运算符用于需要它们的多值条件键。不要将集合运算符用于单值条件键。像往常一样，在生产环境中使用策略语句之前，始终全面测试这些策略语句。

条件键是单值或多值。要确定 AWS KMS 条件键是单值还是多值，请参阅条件键描述中的值类型列。

- 单值条件键在授权上下文（请求或资源）中最多具有一个值。例如，由于每个 API 调用只能来自一个 AWS 账户，因此 k m CallerAccount s: 是单值条件密钥。不要将集合运算符用于单值条件键。
- 多值条件键在授权上下文（请求或资源）中具有多个值。例如，由于每个 KMS 密钥可以有多个别名，因此 k ms: ResourceAliases 可以有多个值。多值条件键需要一个集合运算符。

请注意，单值条件键和多值条件键之间的差异取决于授权上下文中的值数量；而不是策略条件中的值数量。

> **Warning**
>
> 将集合运算符用于单值条件键可能会创建过于宽容（或过于限制）的策略语句。仅将集合运算符用于多值条件键。
>
> 如果您创建或更新包含带有 kms:EncryptionContext: 上下文密钥或`aws:RequestTag/`*`tag-key`*条件密钥的`ForAllValues`集合运算符的策略， AWS KMS 则会返回以下错误消息：
>
> ```
> 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.
> ```

有关 ForAnyValue 和 ForAllValues 集合运算符的详细信息，请参阅 IAM 用户指南中的使用多个键和值。有关在单值条件下使用ForAllValues集合运算符的风险的信息，请参阅 IAM 用户指南中的安全警告- ForAllValues 使用单值密钥。

主题

- kms: BypassPolicyLockoutSafetyCheck
- kms: CallerAccount
- kms:CustomerMasterKeySpec（已弃用）
- kms:CustomerMasterKeyUsage（已弃用）
- kms: DataKeyPairSpec
- kms: EncryptionAlgorithm
- kms:EncryptionContext: 上下文密钥
- kms: EncryptionContextKeys
- kms: ExpirationModel
- kms: GrantConstraintType
- kms: GrantIsFor AWSResource
- kms: GrantOperations
- kms: GranteePrincipal
- kms: KeyOrigin
- kms: KeySpec
- kms: KeyUsage
- kms: MacAlgorithm
- kms: MessageType
- kms: MultiRegion
- kms: MultiRegionKeyType
- kms: PrimaryRegion
- kms: ReEncryptOnSameKey
- kms: RequestAlias
- kms: ResourceAliases
- kms: ReplicaRegion
- kms: RetiringPrincipal

- kms: RotationPeriodInDays
- kms: ScheduleKeyDeletionPendingWindowInDays
- kms: SigningAlgorithm
- kms: ValidTo
- kms: ViaService
- kms: WrappingAlgorithm
- kms: WrappingKeySpec

kms: BypassPolicyLockoutSafetyCheck

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:BypassPolicyLockoutSafetyCheck	布尔值	单值	CreateKey PutKeyPolicy	仅限 IAM policy 密钥策略和 IAM policy

kms:BypassPolicyLockoutSafetyCheck条件键根据请求中BypassPolicyLockoutSafetyCheck参数的值控制对CreateKey和PutKeyPolicy操作的访问权限。

以下示例 IAM policy 语句阻止用户绕过策略锁定安全检查，方式为当 CreateKey 请求中 BypassPolicyLockoutSafetyCheck 参数的值为 true. 时，拒绝用户创建 KMS 密钥的权限

```
{
  "Effect": "Deny",
  "Action": [
    "kms:CreateKey",
    "kms:PutKeyPolicy"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
```

```
  }
}
```

您还可以在 IAM policy 或密钥策略中使用 kms:BypassPolicyLockoutSafetyCheck 条件键控制对 PutKeyPolicy 操作的访问权限。密钥策略中的以下示例策略语句阻止用户在更改 KMS 密钥的策略时绕过策略锁定安全检查。

此策略语句不是使用显式 Deny，而是结合使用 Allow 和 Null 条件运算符，以仅当请求不含 BypassPolicyLockoutSafetyCheck 参数时，允许访问。如果未使用此参数，则默认值为 false。此较弱的策略语句在少数有必要绕过的情况下可覆盖。

```
{
  "Effect": "Allow",
  "Action": "kms:PutKeyPolicy",
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:BypassPolicyLockoutSafetyCheck": true
    }
  }
}
```

另请参阅

- kms: KeySpec
- kms: KeyOrigin
- kms: KeyUsage

kms: CallerAccount

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:CallerAccount	String	单值	KMS 密钥资源操作 自定义密钥存储操作	密钥策略和 IAM 策略

您可以使用此条件键允许或拒绝对 AWS 账户中所有身份（用户和角色）的访问。在密钥策略中，您可以使用 Principal 元素来指定策略语句所适用的身份。Principal 元素的语法未提供指定 AWS 账户账户中的所有身份的方式。但是你可以通过将此条件键与指定所有 AWS 身份的Principal元素结合起来来实现这种效果。

您可以使用它来控制对任何 KMS 密钥资源操作（即使用特定 KMS 密钥的任何 AWS KMS 操作）的访问权限。若要标识 KMS 密钥资源操作，请在操作和资源表中，在操作的 Resources 列中查找的 KMS key 的值。它也适用于管理自定义密钥存储的操作。

例如，以下密钥策略语句演示了如何使用 kms:CallerAccount 条件键。本政策声明包含在 Amazon EBS AWS 托管式密钥 的关键政策中。它将指定所有 AWS 身份的Principal元素与kms:CallerAccount条件键相结合，以有效地允许访问 AWS 账户 111122223333 中的所有身份。它包含一个额外的 AWS KMS 条件密钥 (kms:ViaService)，通过仅允许通过 Amazon EBS 发出的请求来进一步限制权限。有关更多信息，请参阅 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（已弃用）

kms:CustomerMasterKeySpec 条件键已弃用。请改用 kms: KeySpec 条件密钥。

kms:CustomerMasterKeySpec 和 kms:KeySpec 条件键的运行方式相同。只有名称不同。建议使用 kms:KeySpec。但是，为了避免破坏性更改， AWS KMS 支持这两个条件键。

kms:CustomerMasterKeyUsage（已弃用）

kms:CustomerMasterKeyUsage 条件键已弃用。请改用 kms: KeyUsage 条件密钥。

kms:CustomerMasterKeyUsage 和 kms:KeyUsage 条件键的运行方式相同。只有名称不同。建议使用 kms:KeyUsage。但是，为了避免破坏性更改， AWS KMS 支持这两个条件键。

kms: DataKeyPairSpec

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:DataKeyPairSpec	String	单值	GenerateDataKeyPair GenerateDataKeyPairWithoutPlaintext	密钥策略和 IAM policy

您可以使用此条件键根据请求中KeyPairSpec参数的值来控制对GenerateDataKeyPair和GenerateDataKeyPairWithoutPlaintext操作的访问权限。例如，您可以仅允许用户生成特定类型的数据密钥对。

以下示例密钥策略语句使用 kms:DataKeyPairSpec 条件键，以仅允许用户使用 KMS 密钥生成 RSA 数据密钥对。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": [
    "kms:GenerateDataKeyPair",
    "kms:GenerateDataKeyPairWithoutPlaintext"
  ],
```

```
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:DataKeyPairSpec": "RSA*"
    }
  }
}
```

另请参阅

- kms: KeySpec
- the section called “kms: EncryptionAlgorithm”
- the section called “kms:EncryptionContext: 上下文密钥”
- the section called “kms: EncryptionContextKeys”

kms: EncryptionAlgorithm

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:EncryptionAlgorithm	String	单值	Decrypt Encrypt GenerateDataKey GenerateDataKeyPair GenerateDataKeyPairWithoutPlaintext GenerateDataKeyWithoutPlaintext	密钥策略和 IAM 策略

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
			ReEncrypt	

您可以使用 kms:EncryptionAlgorithm 条件键，根据操作中使用的加密算法，控制对加密操作的访问。对于 “加密”、“解密” 和 “ReEncrypt操作”，它根据请求中EncryptionAlgorithm参数的值来控制访问权限。对于生成数据密钥和数据密钥对的操作，则根据用于加密数据密钥的加密算法控制访问。

此条件密钥对以外执行的操作没有影响 AWS KMS，例如使用外部非对称 KMS 密钥对中的公钥进行加密。 AWS KMS

EncryptionAlgorithm 请求中的参数

要允许用户仅将特定加密算法用于 KMS 密钥，请使用包含 Deny 效果和 StringNotEquals 条件运算符的策略语句。例如，以下示例密钥策略语句禁止可担任 ExampleRole 角色的主体，在指定的加密操作中使用此对称 KMS 密钥，除非请求中的加密算法为 RSAES_OAEP_SHA_256，与 RSA KMS 密钥结合使用的非对称加密算法。

与允许用户使用特定加密算法的策略语句不同，具有双重否定的策略语句（如上例），会阻止此 KMS 密钥的其他策略和授权允许此角色使用其他加密算法。此密钥策略语句中的 Deny 优先于任何包含 Allow 效果的密钥策略或 IAM policy，并且优先于此 KMS 密钥及其委托人的所有授权。

```
{
  "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"
    }
  }
}
```

用于操作的加密算法

您也可以使用 kms:EncryptionAlgorithm 条件键基于操作中使用的加密算法控制对操作的访问权限，即使在请求中未指定算法时也是如此。这使您能够要求或禁止 SYMMETRIC_DEFAULT 算法，它可能不会在请求中指定，因为它是默认值。

通过此功能，您还可以使用 kms:EncryptionAlgorithm 条件键，控制对生成数据密钥和数据密钥对的操作的访问。这些操作仅使用对称加密 KMS 密钥和 SYMMETRIC_DEFAULT 算法。

例如，此 IAM policy 限制其委托人只能使用对称加密。除非请求中指定的或操作中使用的加密算法为 SYMMETRIC_DEFAULT，否则策略将拒绝对示例帐户中的任何 KMS 密钥进行加密操作的访问。包括对权限的GenerateDataKey*添加GenerateDataKeyGenerateDataKeyWithoutPlaintextGenerateDataKeyPair、、和GenerateDataKeyPairWithoutPlaintext。条件对这些操作没有影响，因为它们始终使用对称加密算法。

```
{
  "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"
    }
  }
}
```

另请参阅

- the section called “kms: MacAlgorithm”
- kms: SigningAlgorithm

kms:EncryptionContext: 上下文密钥

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型

`kms:EncryptionContext: context-key`	String	单值	`CreateGrant`
			`Encrypt`
			`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateDataKeyPairWithoutPlaintext`
			`GenerateDataKeyWithoutPlaintext`
			`ReEncrypt`
				密钥策略和 IAM policy

您可以使用 `kms:EncryptionContext:context-key` 条件键，根据加密操作请求中的加密上下文，控制对对称加密 KMS 密钥的访问。使用此条件键可评估加密上下文对中的键和值。要仅评估加密上下文密钥或无论密钥或值如何，都需要加密上下文，请使用 kms: EncryptionContextKeys 条件密钥。

> **Note**
>
> 条件键值必须遵守密钥策略和 IAM policy 的字符规则。在加密上下文中有效的某些字符在策略中无效。您可能无法使用此条件键来表示全部有效的加密上下文值。有关密钥策略文档规则的

详细信息，请参阅 密钥策略格式。有关 IAM policy 文档规则的详细信息，请参阅《IAM 用户指南》中的 IAM 名称要求。

您不能在使用非对称 KMS 密钥或 HMAC KMS 密钥的加密操作中指定加密上下文。非对称算法和 MAC 算法不支持加密上下文。

要使用 km s:EncryptionContext: 上下文密钥条件密钥，请将上下文密钥占位符替换为加密*#####*。使用加密上下文值替换 *context-value* 占位符。

```
"kms:EncryptionContext:context-key": "context-value"
```

例如，下面的条件键指定一个加密上下文，其键为 AppName，值为 ExampleApp (AppName = ExampleApp)。

```
"kms:EncryptionContext:AppName": "ExampleApp"
```

这是一个单值条件键。条件键中的密钥指定特定的加密上下文键 (context-key)。尽管您可以在每个 API 请求中包含多个加密上下文对，但具有指定 context-key 的加密上下文对只能有一个值。例如，kms:EncryptionContext:Department 条件键仅适用于具有 Department 密钥的加密上下文对，任何具有 Department 密钥的给定加密上下文对都只能有一个值。

不要将集合运算符用于 kms:EncryptionContext:*context-key* 条件键。如果您创建一个具有 Allow 操作，kms:EncryptionContext:*context-key* 条件键和 ForAllValues 集合运算符的策略语句，则条件允许没有加密上下文的请求以及带有未在策略条件中指定的加密上下文对的请求。

Warning

请勿将 ForAnyValue 或 ForAllValues 集合运算符用于此单值条件键。这些集合运算符可以创建一个策略条件，该条件不需要您计划要求的值，并允许您计划禁止的值。
如果您创建或更新包含带有 kms:: conte xt-key 的ForAllValues集合运算符的策略， AWS KMS 则会返回以下错误消息EncryptionContext：
`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.`

若要要求特定的加密上下文对，请结合使用 kms:EncryptionContext:*context-key* 条件键与 StringEquals 运算符。

以下示例密钥策略语句允许可以担任角色的委托人仅在请求中的加密上下文包括 AppName:ExampleApp 对时使用 GenerateDataKey 请求中的 KMS 密钥。允许使用其他加密上下文对。

密钥名称区分大小写。值是否区分大小写由条件运算符确定，例如 StringEquals。有关更多信息，请参阅 加密上下文条件区分大小写。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:AppName": "ExampleApp"
    }
  }
}
```

要要求加密上下文对并禁止所有其他加密上下文对，请在策略声明kms:EncryptionContextKeys中同时使用 kms:EncryptionContext: conte xt-key。以下密钥策略语句使用 kms:EncryptionContext:AppName 条件要求请求中的 AppName=ExampleApp 加密上下文对。它还结合使用 kms:EncryptionContextKeys 条件键与 ForAllValues 集合运算符以仅允许 AppName 加密上下文键。

ForAllValues 集合运算符将请求中的加密上下文键限制为 AppName。如果 kms:EncryptionContextKeys 条件与 ForAllValues 集合运算符在策略语句中单独使用，则此集合运算符将允许没有加密上下文的请求。但是，如果请求没有加密上下文，则 kms:EncryptionContext:AppName 条件将失败。有关 ForAllValues 集合运算符的详细信息，请参阅 IAM 用户指南中的使用多个键和值。

```
{
  "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"
      ]
    }
  }
}
```

您还可以使用此条件键拒绝对特定操作的 KMS 密钥的访问。如果请求中的加密上下文包含 `Stage=Restricted` 加密上下文对，以下示例密钥策略语句使用 `Deny` 效果，以禁止委托人使用 KMS 密钥。此条件允许使用其他加密上下文对进行请求，包括具有 `Stage` 键和其他值的加密上下文对，例如 `Stage=Test`。

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": "Restricted"
    }
  }
}
```

使用多个加密上下文对

您可以要求或禁止多个加密上下文对。您还可以要求几个加密上下文对之一。有关用于解释这些条件的逻辑的详细信息，请参阅 IAM 用户指南中的创建具有多个键或值的条件。

> **Note**
>
> 本主题的早期版本显示了使用和 se ForAllValues t 运算符ForAnyValue和 kms:EncryptionContext: conte xt-key 条件密钥的策略声明。将集合运算符与单值条件键结合使用可能会导致允许没有加密上下文和未指定加密上下文对的请求的策略。
> 例如，具有 Allow 效果、ForAllValues 集合运算符和 "kms:EncryptionContext:Department": "IT" 条件键的策略条件不会将加密上下文限制为“Department=IT”对。它允许没有加密上下文的请求和具有未指定加密上下文对的请求，例如 Stage=Restricted。
> 请查看您的政策，并使用 kms:EncryptionContext: conte xt- key 将集合运算符从任何条件中删除。尝试使用此格式创建或更新策略失败，并显示 OverlyPermissiveCondition 异常。要纠正此错误，请删除集合运算符。

若需要多个加密上下文对，请列出相同条件下的对。以下示例密钥策略语句需要两个加密上下文对 Department=IT 和 Project=Alpha。由于条件具有不同的键（kms:EncryptionContext:Department 和 kms:EncryptionContext:Project）它们由 AND 运算符隐式连接。允许其他加密上下文对，但它们不是必需的。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:Decrypt",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Department": "IT",
      "kms:EncryptionContext:Project": "Alpha"
    }
  }
}
```

若需要一个加密上下文对或另一个加密上下文对，请将每个条件键放在单独的策略语句中。以下示例密钥策略需要 Department=IT 或 Project=Alpha 对，或此两者。允许其他加密上下文对，但它们不是必需的。

```
{
```

```
 "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"
  }
 }
}
```

要要求特定的加密对并排除所有其他加密上下文对，请在策略声明kms:EncryptionContextKeys中同时使用 kms:EncryptionContext: conte xt-key。以下密钥策略声明使用 kms:EncryptionContext: 上下文密钥条件来要求同时包含Department=IT和Project=Alpha对的加密上下文。它结合使用 kms:EncryptionContextKeys 条件键与 ForAllValues 集合运算符以仅允许 Department 和 Project 加密上下文键。

ForAllValues 集合运算符将请求中的加密上下文键限制为 Department 和 Project。如果在条件中单独使用它，则此集合运算符将允许没有加密上下文的请求，但是在此配置中，此条件下的 kms:EncryptionContext: conte xt-key 将失败。

```
{
  "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"
      ]
    }
  }
}
```

您还可以禁止多个加密上下文对。如果请求中的加密上下文包含 Stage=Restricted 或 Stage=Production 对，以下示例密钥策略语句使用 Deny 效果，以禁止委托人使用 KMS 密钥。

相同键 (kms:EncryptionContext:Stage) 的多个值（Restricted 和 Production）用 OR 隐式连接。有关详细信息，请参阅 IAM 用户指南中的具有多个键或值的条件的评估逻辑。

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:Stage": [
         "Restricted",
         "Production"
      ]
    }
  }
}
```

加密上下文条件区分大小写

在解密操作中指定的加密上下文，与加密操作中指定的加密上下文必须是区分大小写的精确匹配。只有当加密上下文中有多个上下文对时，上下文对的顺序可以改变。

但是，在策略条件中，条件键不区分大小写。条件值是否区分大小写由您使用的策略条件运算符确定，例如 StringEquals 或 StringEqualsIgnoreCase。

因此，由 kms:EncryptionContext: 前缀和 *context-key* 替换组成的条件键不区分大小写。使用此条件的策略不检查条件键任何元素的大小写。条件值（即 *context-value* 替换）是否区分大小写由策略条件运算符确定。

例如，以下策略语句在加密上下文包含 Appname 键时允许操作，不论其大小写如何。StringEquals 条件要求 ExampleApp 按照其指定的大小写。

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

要要求使用区分大小写的加密上下文密钥，请使用 k ms: EncryptionContextKeys 策略条件和区分大小写的条件运算符，例如。StringEquals在此策略条件中，由于加密上下文键是此策略条件中的值，它是否区分大小写由条件运算符确定。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": "kms:GenerateDataKey",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
  }
}
```

要要求对加密上下文密钥和值进行区分大小写的评估，请在同一个策略声明中同时使用kms:EncryptionContextKeys和 kmsEncryptionContext:: 上下文密钥策略条件。区分大小写的条件运算符（例如 StringEquals）始终适用于条件的值。加密上下文键（例如 AppName）是 kms:EncryptionContextKeys 条件的值。加密上下文值（例如ExampleApp）是 kms:EncryptionContext: 上下文密钥条件的值。

例如，在以下示例密钥策略语句中，由于 StringEquals 运算符区分大小写，加密上下文键和加密上下文值均区分大小写。

```
{
  "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"
    }
  }
}
```

在加密上下文条件中使用变量

加密上下文对中的键和值必须是简单的文本字符串。它们不能是整数或对象，也不能是任何未完全解析的类型。如果您使用其他类型，例如整数或浮点数，则将其 AWS KMS 解释为文字字符串。

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

不过，kms:EncryptionContext:*context-key* 条件键的值可以是 IAM policy 变量。在运行时根据请求中的值解析这些策略变量。例如，aws:CurrentTime 解析为请求的时间，aws:username 解析为调用方的友好名称。

您可以使用这些策略变量来创建一个策略语句，该语句包含的条件需要加密上下文中非常具体的信息，例如调用方的用户名。由于它包含一个变量，因此，您可以对所有能够代入该角色的用户使用相同的策略语句。您无需为每个用户编写单独的策略语句。

请考虑这样一种情况：您希望所有能够代入角色的用户都使用同一 KMS 密钥来加密和解密其数据。但是，您希望仅允许这些用户解密其加密的数据。首先，要求每个请求都 AWS KMS 包含一个加密上下文，其中密钥是`user`，值是调用者的 AWS 用户名，例如以下内容。

```
"encryptionContext": {
    "user": "bob"
}
```

然后，要强制执行此要求，您可以使用与以下示例中的策略语句类似的策略语句。此策略语句向 `TestTeam` 角色授予使用 KMS 密钥加密和解密数据的权限。不过，此权限仅在请求中的加密上下文包含 `"user": "`*`<username>`*`"` 对时有效。为了表示用户名，条件使用 `aws:username` 策略变量。

在评估请求时，调用方的用户名将替换条件中的变量。同样地，条件要求 `"user": "bob"`（对于“bob”）和 `"user": "alice"`（对于“alice”）的加密上下文。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/TestTeam"
  },
  "Action": [
    "kms:Decrypt",
    "kms:Encrypt"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:EncryptionContext:user": "${aws:username}"
    }
  }
}
```

您只能在 `kms:EncryptionContext:`*`context-key`* 条件键的值中使用 IAM policy 变量。不能在键中使用变量。

也可以在变量中使用提供程序特定的上下文键。这些上下文密钥唯一标识使用 Web 联合身份验证登录 AWS 的用户。

与所有变量一样，这些变量只能用于 kms:EncryptionContext:*context-key* 策略条件，而不能用于实际加密上下文。此外，它们只能用于条件的值，而不能用于条件的键。

例如，以下键策略语句与上一个类似。不过，条件需要加密上下文，其中键为 sub，并且值唯一标识已登录 Amazon Cognito 用户池的用户。有关识别 Amazon Cognito 中的用户和角色的详细信息，请参阅 Amazon Cognito 开发人员指南中的 IAM 角色。

```
{
  "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}"
    }
  }
}
```

另请参阅

- the section called “kms: EncryptionContextKeys”
- the section called “kms: GrantConstraintType”

kms: EncryptionContextKeys

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:EncryptionContextKeys	字符串（列表）	多值	CreateGrant Decrypt Encrypt	密钥策略和 IAM policy

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
			GenerateDataKey GenerateDataKeyPair GenerateDataKeyPairWithoutPlaintext GenerateDataKeyWithoutPlaintext ReEncrypt	

您可以使用 kms:EncryptionContextKeys 条件键，根据加密操作请求中的加密上下文，控制对对称加密 KMS 密钥的访问。使用此条件键仅评估各个加密上下文对中的键。要同时评估加密上下文中的键和值，请使用 kms:EncryptionContext:*context-key* 条件键。

您不能在使用非对称 KMS 密钥或 HMAC KMS 密钥的加密操作中指定加密上下文。非对称算法和 MAC 算法不支持加密上下文。

> **Note**
>
> 条件密钥值（包括加密上下文密钥）必须符合密 AWS KMS 钥策略的字符和编码规则。您可能无法使用此条件键来表示所有有效的加密上下文键。有关密钥策略文档规则的详细信息，请参阅 密钥策略格式。有关 IAM policy 文档规则的详细信息，请参阅《IAM 用户指南》中的 IAM 名称要求。

这是一个多值条件键。您可以在每个 API 请求中指定多个加密上下文对。kms:EncryptionContextKeys 会将请求中的加密上下文键与策略中的加密上下文键集进行比

较。要确定如何比较这些集，您必须在策略条件中提供 ForAnyValue 或 ForAllValues 集合运算符。有关集合运算符的详细信息，请参阅 IAM 用户指南中的使用多个键和值。

- ForAnyValue：请求中的至少一个加密上下文键必须匹配策略条件中的加密上下文键。允许其他加密上下文键。如果请求中没有加密上下文，则不满足此条件。
- ForAllValues：请求中的每个加密上下文键必须匹配策略条件中的加密上下文键。此集合运算符将加密上下文键限制为策略条件中的键。它不需要任何加密上下文键，但禁止未指定的加密上下文键。

以下示例密钥策略语句结合使用 kms:EncryptionContextKeys 条件键与 ForAnyValue 集合运算符。此策略语句允许对指定运算使用 KMS 密钥，但仅当请求中至少有一个加密上下文对包括 AppName 键（忽视其值）时，才允许为指定运算使用 KMS 密钥。

例如，此密钥策略语句允许包含两个加密上下文对 AppName=Helper 和 Project=Alpha 的 GenerateDataKey 请求，因为第一个加密上下文对满足此条件。只有 Project=Alpha 或没有加密上下文的请求都会失败。

由于StringEquals条件操作区分大小写，因此此策略声明要求加密上下文密钥的拼写和大小写。不过您可以使用忽略键大小写的条件运算符，例如 StringEqualsIgnoreCase。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "kms:EncryptionContextKeys": "AppName"
    }
  }
}
```

您也可以使用 kms:EncryptionContextKeys 条件键在使用 KMS 密钥的加密操作中要求加密上下文（任何加密上下文）。

以下示例密钥策略语句结合使用 kms:EncryptionContextKeys 条件键和 Null 条件运算符，仅允许在 API 请求中的加密上下文不为 null 时允许访问 KMS 密钥。此条件不检查加密上下文的键或值。它只验证加密上下文是否存在。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
  "Action": [
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "Null": {
      "kms:EncryptionContextKeys": false
    }
  }
}
```

另请参阅

- kms:EncryptionContext: 上下文密钥
- kms: GrantConstraintType

kms: ExpirationModel

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:ExpirationModel	String	单值	ImportKeyMaterial	密钥策略和 IAM policy

kms:ExpirationModel条件键根据请求中ExpirationModel参数的值控制对ImportKeyMaterial操作的访问权限。

ExpirationModel 是可选参数，用于确定导入的密钥材料是否过期。有效值为 KEY_MATERIAL_EXPIRES 和 KEY_MATERIAL_DOES_NOT_EXPIRE。默认值为 KEY_MATERIAL_EXPIRES。

到期日期和时间由ValidTo参数的值决定。除非 ExpirationModel 参数的值为 KEY_MATERIAL_DOES_NOT_EXPIRE，否则 ValidTo 参数是必需的。您也可以使用 k ms: ValidTo 条件密钥要求特定的到期日期作为访问条件。

以下示例策略语句使用 kms:ExpirationModel 条件键，以仅允许用户在请求包含 ExpirationModel 参数且其值为 KEY_MATERIAL_DOES_NOT_EXPIRE 时将密钥材料导入 KMS 密钥。

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

您也可以使用 kms:ExpirationModel 条件键，以仅允许用户在密钥材料过期时导入密钥材料。以下示例密钥策略语句结合使用 kms:ExpirationModel 条件键和 空值条件运算符，以仅允许用户在请求没有 ExpirationModel 参数时导入密钥材料。的默认值 ExpirationModel 为KEY_MATERIAL_EXPIRES。

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

```
  }
}
```

另请参阅

- kms: ValidTo
- kms: WrappingAlgorithm
- kms: WrappingKeySpec

kms: GrantConstraintType

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:GrantConstraintType	String	单值	CreateGrant	密钥策略和 IAM policy

您可以使用此条件键根据请求中的授权约束类型来控制对CreateGrant操作的访问权限。

创建授权时，您可以选择性地指定授权约束，以仅在存在特定加密上下文时允许授予操作权限。授权约束可以是以下两种类型之一：EncryptionContextEquals 或 EncryptionContextSubset。您可以使用此条件键来检查请求中包含哪种类型。

> **Important**
>
> 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。

以下示例密钥策略语句使用 kms:GrantConstraintType 条件键，以仅允许用户在请求中包含 EncryptionContextEquals 授权约束时创建授权。以下示例显示了密钥策略中的策略语句。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/RoleForExampleApp"
  },
```

```
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GrantConstraintType": "EncryptionContextEquals"
    }
  }
}
```

另请参阅

- kms:EncryptionContext: 上下文密钥
- kms: EncryptionContextKeys
- kms: GrantIsFor AWSResource
- kms: GrantOperations
- kms: GranteePrincipal
- kms: RetiringPrincipal

kms: GrantIsFor AWSResource

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型

`kms:GrantIsForAWSResource`	布尔值	单值	`CreateGrant`
			`ListGrants`
			`RevokeGrant`
				密钥策略和 IAM policy

仅当与之集成的AWS 服务代表用户 AWS KMS调用RevokeGrant操作时 CreateGrant，才允许或拒绝对ListGrants、或操作的权限。此策略条件不允许用户直接调用这些授权操作。

以下示例密钥策略语句使用 `kms:GrantIsForAWSResource` 条件键。它允许与 AWS KMS之集成的 AWS 服务（例如 Amazon EBS）代表指定的委托人针对此 KMS 密钥创建授权。

```
{
  "Effect": "Allow",
  "Principal": {
```

```
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:GrantIsForAWSResource": true
    }
  }
}
```

另请参阅

- kms: GrantConstraintType
- kms: GrantOperations
- kms: GranteePrincipal
- kms: RetiringPrincipal

kms: GrantOperations

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:GrantOperations	String	多值	CreateGrant	密钥策略和 IAM policy

您可以使用此条件密钥根据请求中的授权CreateGrant操作来控制对操作的访问权限。例如，您可以允许用户创建委托加密权限（但不委托解密权限）的授权。有关授权的更多信息，请参阅使用授权。

这是一个多值条件键。kms:GrantOperations 将比较 CreateGrant 请求中的授权操作集合与策略中的授权操作集合。要确定如何比较这些集，您必须在策略条件中提供 ForAnyValue 或 ForAllValues 集合运算符。有关集合运算符的详细信息，请参阅 IAM 用户指南中的使用多个键和值。

- ForAnyValue：请求中的至少一个授权操作必须匹配策略条件中的授权操作之一。允许其他授权操作。

- ForAllValues：请求中的每个授予操作都必须与策略条件中的授权操作相匹配。此集合运算符将授权操作限制为策略条件中指定的操作。它不需要任何授权操作，但它禁止未指定的授权操作。

  ForAllValues 当请求中没有授予操作但CreateGrant不允许时，也会返回 true。如果 Operations 参数缺失或具有 null 值，则 CreateGrant 请求失败。

以下示例密钥策略语句使用 kms:GrantOperations 条件键，以仅允许在授权操作为 Encrypt、ReEncryptTo 或此两者时创建授权。如果授权包括任何其他操作，则 CreateGrant 请求失败。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "ForAllValues:StringEquals": {
      "kms:GrantOperations": [
        "Encrypt",
        "ReEncryptTo"
      ]
    }
  }
}
```

如果将策略条件中的集合运算符更改为 ForAnyValue，则策略语句将要求授权中至少有一个授权操作是 Encrypt 或 ReEncryptTo，但它允许其他授权操作，例如 Decrypt 或 ReEncryptFrom。

另请参阅

- kms: GrantConstraintType
- kms: GrantIsFor AWSResource
- kms: GranteePrincipal
- kms: RetiringPrincipal

kms: GranteePrincipal

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:GranteePrincipal	String	单值	CreateGrant	IAM 和密钥策略

您可以使用此条件键根据请求中GranteePrincipal参数的值来控制对CreateGrant操作的访问权限。例如，您可以仅允许在 CreateGrant 请求中的被授权主体与条件语句中指定的主体匹配时创建使用 KMS 密钥的授权。

要指定被授权人委托人，请使用委托人的亚马逊资源名称 (ARN)。 AWS 有效的委托人包括 AWS 账户 IAM 用户、IAM 角色、联合用户和代入角色用户。有关委托人的 ARN 语法的帮助，请参阅 IAM 用户指南中的 IA M ARN。

以下示例密钥策略语句使用 kms:GranteePrincipal 条件键，以仅允许在授权中的被授权主体为 LimitedAdminRole 时创建 KMS 密钥授权。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:CreateGrant",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:GranteePrincipal": "arn:aws:iam::111122223333:role/LimitedAdminRole"
    }
  }
}
```

另请参阅

- kms: GrantConstraintType
- kms: GrantIsFor AWSResource
- kms: GrantOperations

- kms: RetiringPrincipal

kms: KeyOrigin

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:KeyOrigin	String	单值	CreateKey KMS 密钥资源操作	IAM 策略 密钥策略和 IAM 策略

kms:KeyOrigin 条件键根据操作创建的或操作中使用的 KMS 密钥的 Origin 属性值，控制对操作的访问。它作为资源条件或请求条件工作。

您可以使用此条件键根据请求中 O rigin 参数的值来控制对CreateKey操作的访问权限。Origin 的有效值为 AWS_KMS、AWS_CLOUDHSM 和 EXTERNAL。

例如，只有在 () 中生成密钥材料、仅当密钥材料是在与自定义密钥存储库关联的 AWS CloudHSM 集群 AWS KMS (AWS_KMS) 中生成密钥材料时，或者仅当密钥材料是从外部来源 (AWS_CLOUDHSMEXTERNAL) 导入时，才能创建 KMS 密钥。

以下示例密钥策略声明仅在创建密钥材料时才使用kms:KeyOrigin条件密钥创 AWS KMS 建 KMS 密钥。

```
{
  "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"
        }
      }
    }
  ]
}
```

还可以使用 kms:KeyOrigin 条件键，根据用于操作的 KMS 密钥的 Origin 属性，控制对使用或管理 KMS 密钥的操作的访问。该操作必须是 KMS 密钥资源操作，即为特定 KMS 密钥授权的操作。若要标识 KMS 密钥资源操作，请在操作和资源表中，在操作的 Resources 列中查找的 KMS key 的值。

例如，以下 IAM policy 允许委托人执行指定的 KMS 密钥资源操作，但只能使用账户中在自定义密钥存储中创建的 KMS 密钥。

```
{
  "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"
    }
  }
}
```

另请参阅

- kms: BypassPolicyLockoutSafetyCheck
- kms: KeySpec
- kms: KeyUsage

kms: KeySpec

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:KeySpec	String	单值	CreateKey KMS 密钥资源操作	IAM 策略 密钥策略和 IAM 策略

kms:KeySpec 条件键根据操作创建的或操作中使用的 KMS 密钥的 KeySpec 属性值，控制对操作的访问。

您可以在 IAM 策略中使用此条件密钥，根据CreateKey请求中KeySpec参数的值来控制对CreateKey操作的访问权限。例如，您可以使用此条件允许用户仅创建对称加密 KMS 密钥或仅创建 HMAC KMS 密钥。

以下示例 IAM policy 语句使用 kms:KeySpec 条件键，允许主体仅创建 RSA 非对称 KMS 密钥。权限仅在请求中的 KeySpec 以 RSA_ 开头时有效。

```
{
  "Effect": "Allow",
```

```
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:KeySpec": "RSA_*"
    }
  }
}
```

还可以使用 kms:KeySpec 条件键，根据用于操作的 KMS 密钥的 KeySpec 属性，控制对使用或管理 KMS 密钥的操作的访问。该操作必须是 KMS 密钥资源操作，即为特定 KMS 密钥授权的操作。若要标识 KMS 密钥资源操作，请在操作和资源表中，在操作的 Resources 列中查找的 KMS key 的值。

例如，以下 IAM policy 允许主体执行指定的 KMS 密钥资源操作，但只能使用账户中的对称加密 KMS 密钥。

```
{
  "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"
    }
  }
}
```

另请参阅

- kms: BypassPolicyLockoutSafetyCheck
- kms:CustomerMasterKeySpec（已弃用）
- kms: DataKeyPairSpec
- kms: KeyOrigin
- kms: KeyUsage

kms: KeyUsage

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:KeyUsage	String	单值	CreateKey KMS 密钥资源操作	IAM 策略 密钥策略和 IAM 策略

kms:KeyUsage 条件键根据操作创建的或操作中使用的 KMS 密钥的 KeyUsage 属性值，控制对操作的访问。

您可以使用此条件键根据请求中KeyUsage参数的值来控制对CreateKey操作的访问权限。KeyUsage 的有效值为 ENCRYPT_DECRYPT、SIGN_VERIFY 和 GENERATE_VERIFY_MAC。

例如，您可以仅在 KeyUsage 为 ENCRYPT_DECRYPT 时允许创建 KMS 密钥，或者在 KeyUsage 为 SIGN_VERIFY 时拒绝用户权限。

以下示例 IAM policy 语句使用 kms:KeyUsage 条件键，以仅允许在 KeyUsage 为 ENCRYPT_DECRYPT 时创建 KMS 密钥。

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:KeyUsage": "ENCRYPT_DECRYPT"
    }
  }
}
```

还可以使用 kms:KeyUsage 条件键，根据操作中的 KMS 密钥的 KeyUsage 属性，控制对使用或管理 KMS 密钥的操作的访问。该操作必须是 KMS 密钥资源操作，即为特定 KMS 密钥授权的操作。若要标识 KMS 密钥资源操作，请在操作和资源表中，在操作的 Resources 列中查找的 KMS key 的值。

例如，以下 IAM policy 允许委托人执行指定的 KMS 密钥资源操作，但只能使用账户中用于签名和验证的 KMS 密钥。

```
{
  "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"
    }
  }
}
```

另请参阅

- kms: BypassPolicyLockoutSafetyCheck
- kms:CustomerMasterKeyUsage（已弃用）
- kms: KeyOrigin
- kms: KeySpec

kms: MacAlgorithm

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:MacAlgorithm	String	单值	GenerateMac VerifyMac	密钥策略和 IAM policy

您可以使用kms:MacAlgorithm条件键根据请求中MacAlgorithm参数的值来控制对GenerateMac和VerifyMac操作的访问权限。

以下示例密钥策略允许可以代入 testers 角色的用户仅在请求中的 MAC 算法为 HMAC_SHA_384 或 HMAC_SHA_512 时使用 HMAC KMS 密钥生成和验证 HMAC 标签。此策略使用两个独立的策略语句，

每个语句都有自己的条件。如果在单个条件语句中指定多个 MAC 算法，则该条件需要两种算法，而不是其中一种算法。

```
{
  "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"
        }
      }
    }
  ]
}
```

另请参阅

- the section called “kms: EncryptionAlgorithm”
- kms: SigningAlgorithm

kms: MessageType

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:MessageType	String	单值	Sign Verify	密钥策略和 IAM 策略

kms:MessageType 条件键基于请求中 MessageType 参数的值控制对 Sign 和 Verify 操作的访问权限。MessageType 的有效值为 RAW 和 DIGEST。

例如，以下密钥策略语句使用 kms:MessageType 条件键，以允许使用非对称 KMS 密钥签署消息，而不是消息摘要。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:Sign",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:MessageType": "RAW"
    }
  }
}
```

另请参阅

- the section called “kms: SigningAlgorithm”

kms: MultiRegion

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:MultiRegion	布尔值	单值	CreateKey KMS 密钥资源操作	密钥策略和 IAM 策略

您可以使用此条件键以允许仅对单区域密钥或仅对多区域密钥进行操作。kms:MultiRegion条件密钥根据 KMS 密钥的MultiRegion属性值控制对 KMS 密钥的CreateKey操作和操作的访问权限。 AWS KMS 有效值为 true（多区域）或 false（单区域）。所有 KMS 密钥都具有 MultiRegion 属性。

例如，以下 IAM policy 语句使用 kms:MultiRegion 条件键，允许委托人仅创建单区域密钥。

```
{
  "Effect": "Allow",
  "Action": "kms:CreateKey",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:MultiRegion": false
    }
  }
}
```

kms: MultiRegionKeyType

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:MultiRegionKeyType	String	单值	CreateKey KMS 密钥资源操作	密钥策略和 IAM 策略

您可以使用此条件键以允许仅对多区域主键或仅对多区域副本密钥执行操作。kms:MultiRegionKeyType条件密钥根据 KMS 密钥的MultiRegionKeyType属性控制对 KMS 密钥的CreateKey操作和操作的访问权限。 AWS KMS 有效值为 PRIMARY 和 REPLICA。只有多区域密钥具有 MultiRegionKeyType 属性。

通常情况下，您可以使用 IAM policy 中的 kms:MultiRegionKeyType 条件键以控制对多个 KMS 密钥的访问。但是，由于给定的多区域密钥可以更改为主密钥或副本密钥，因此您可能希望在密钥策略中使用此条件，以便仅当特定的多区域密钥为主密钥或副本密钥时才允许操作。

IAM policy 语句使用 kms:MultiRegionKeyType 条件键，以允许委托人仅对 AWS 账户中指定的多区域副本密钥计划和取消删除密钥。

```
{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "arn:aws:kms:*:111122223333:key/*",
  "Condition": {
    "StringEquals": {
      "kms:MultiRegionKeyType": "REPLICA"
    }
  }
}
```

要允许或拒绝访问所有多区域密钥，您可以将这两个值或 null 值用于 kms:MultiRegionKeyType。但是，为此，建议使用 k ms: MultiRegion 条件密钥。

kms: PrimaryRegion

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:PrimaryRegion	字符串（列表）	单值	UpdatePrimaryRegion	密钥策略和 IAM policy

您可以使用此条件键来限制UpdatePrimaryRegion操作中的目标区域。它们 AWS 区域 可以托管您的多区域主密钥。

kms:PrimaryRegion条件键根据PrimaryRegion参数的值控制对UpdatePrimaryRegion操作的访问权限。该PrimaryRegion参数指定要提升 AWS 区域 为主密钥的多区域副本密钥。条件的值是一个或多个 AWS 区域 名称，例如us-east-1或ap-southeast-2，或者区域名称模式，例如 eu-*

例如，以下密钥策略语句使用 kms:PrimaryRegion 条件键，以允许委托人将多区域密钥的主区域更新为四个指定的区域之一。

```
{
  "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"
      ]
    }
  }
}
```

kms: ReEncryptOnSameKey

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:ReEncryptOnSameKey	布尔值	单值	ReEncrypt	密钥策略和 IAM policy

您可以使用此条件密钥来控制对ReEncrypt操作的访问权限，具体取决于请求指定的目标 KMS 密钥是否与用于原始加密的目标密钥相同。

例如，以下密钥策略语句使用 kms:ReEncryptOnSameKey 条件键，以仅允许在目标 KMS 密钥与用于原始加密的 KMS 密钥相同时进行重新加密。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:ReEncrypt*",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:ReEncryptOnSameKey": true
    }
  }
}
```

kms: RequestAlias

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:RequestAlias	字符串（列表）	单值	加密操作 DescribeKey GetPublicKey	密钥策略和 IAM policy

您可以使用此条件键，仅在请求使用特定别名来标识 KMS 密钥时允许操作。kms:RequestAlias 条件键基于标识请求中的 KMS 密钥的别名控制对加密操作中使用的 KMS 密钥 GetPublicKey 或 DescribeKey 的访问。（此策略条件对GenerateRandom操作没有影响，因为该操作不使用 KMS 密钥或别名。）

此条件支持中的基于属性的访问控制 (ABAC) AWS KMS，允许您根据 KMS 密钥的标签和别名控制对 KMS 密钥的访问。您可以使用标签和别名，在不更改策略或授权的情况下，允许或拒绝对 KMS 密钥的访问权限。有关更多信息，请参阅 AWS KMS 中的 ABAC。

要在此策略条件下指定别名，请使用别名名称，例如 alias/project-alpha，或别名名称模式，例如 alias/*test*。您无法在此条件键的值中指定别名 ARN。

为了满足此条件，请求中的 KeyId 参数的值必须是匹配的别名名称或别名 ARN。如果请求使用不同的密钥标识符，即使标识相同的 KMS 密钥，它也不能满足条件。

例如，以下密钥策略声明允许委托人对 KMS 密钥调用GenerateDataKey操作。但是，仅当请求中的 KeyId 参数的值为 alias/finance-key 或具有该别名名称（例如 arn:aws:kms:us-west-2:111122223333:alias/finance-key）的别名 ARN 时才允许此操作。

```
{
  "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"
    }
  }
}
```

您不能使用此条件键来控制对别名操作（例如CreateAlias或）的访问权限DeleteAlias。有关控制对别名操作的访问的信息，请参阅 控制对别名的访问。

kms: ResourceAliases

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:ResourceAliases	字符串（列表）	多值	KMS 密钥资源操作	仅限 IAM policy

使用此条件键可根据与 KMS 密钥关联的别名来控制对 KMS 密钥的访问。该操作必须是 KMS 密钥资源操作，即为特定 KMS 密钥授权的操作。若要标识 KMS 密钥资源操作，请在操作和资源表中，在操作的 Resources 列中查找的 KMS key 的值。

此条件在 AWS KMS中支持基于属性的访问控制 (ABAC)。使用 ABAC，您可以根据分配给 KMS 密钥的标签以及与 KMS 密钥关联的别名来控制对 KMS 密钥的访问。您可以使用标签和别名，在不更改策略或授权的情况下，允许或拒绝对 KMS 密钥的访问权限。有关更多信息，请参阅 AWS KMS 中的 ABAC。

别名在 AWS 账户 和区域中必须是唯一的，但此条件允许您控制对同一区域中的多个 KMS 密钥（使用StringLike比较运算符）或每个账户中不同的 KMS 密钥 AWS 区域 的访问权限。

> **Note**
>
> 仅当 KMS 密钥符合每个 KMS 密钥配额的别名时，km s: ResourceAliases 条件才有效。如果 KMS 密钥超出此配额，则由 kms:ResourceAliases 条件授权使用 KMS 密钥的委托人将被拒绝访问 KMS 密钥。

要在此策略条件下指定别名，请使用别名名称，例如 alias/project-alpha，或别名名称模式，例如 alias/*test*。您无法在此条件键的值中指定别名 ARN。要满足条件，操作中使用的 KMS 密钥必须具有指定的别名。是否或者如何在操作请求中标识 KMS 密钥并不重要。

这是一个多值条件键，用于将与 KMS 密钥关联的别名集与策略中的别名集进行比较。要确定如何比较这些集，您必须在策略条件中提供 ForAnyValue 或 ForAllValues 集合运算符。有关集合运算符的详细信息，请参阅 IAM 用户指南中的使用多个键和值。

- ForAnyValue：至少有一个与 KMS 密钥关联的别名必须与策略条件中的别名匹配。允许使用其他别名。如果 KMS 密钥没有别名，则不满足条件。
- ForAllValues：与 KMS 密钥关联的每个别名都必须与策略中的别名相匹配。此集合运算符将与 KMS 密钥关联的别名限制为策略条件中的别名。它不需要任何别名，但它会禁止未指定的别名。

例如，以下 IAM 策略声明允许委托人对指定 AWS 账户 的 KMS 密钥中与finance-key别名关联的任何 KMS 密钥调用该GenerateDataKey操作。（受影响的 KMS 密钥的密钥策略还必须允许委托人的账户将它们用于此操作。）为了指示条件在可能与 KMS 密钥关联的很多别名中的一个为 alias/finance-key 时得到满足，条件使用 ForAnyValue 集合运算符。

由于 kms:ResourceAliases 条件基于资源，而不是请求，对于与 finance-key 别名关联的任何 KMS 密钥，对 GenerateDataKey 的调用成功，即使请求使用密钥 ID 或密钥 ARN 来标识 KMS 密钥。

```
{
  "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"
    }
  }
}
```

以下示例 IAM policy 语句允许委托人启用和禁用 KMS 密钥，但仅当 KMS 密钥的所有别名都包含“Test”时。此策略语句使用两个条件。带有 ForAllValues 集合运算符的条件要求与 KMS 密钥关联的所有别名都包括“Test”。带有 ForAnyValue 集合运算符的条件要求 KMS 密钥至少具有一个带有“Test”的别名。如果不使用 ForAnyValue 条件，此策略语句将允许委托人使用没有别名的 KMS 密钥。

```
{
  "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 条件键	条件类型	值类型	API 操作	策略类型
kms:ReplicaRegion	字符串（列表）	单值	ReplicateKey	密钥策略和 IAM policy

您可以使用此条件密钥来限制委托人 AWS 区域 可以复制多区域密钥的范围。kms:ReplicaRegion条件键根据请求中ReplicaRegion参数的值控制对ReplicateKey操作的访问权限。此参数为新的副本密钥指定 AWS 区域 。

条件的值是一个或多个 AWS 区域 名称，例如us-east-1或ap-southeast-2，或者名称模式，例如eu-*。有关 AWS KMS 支持的名称列表 AWS 区域 ，请参阅中的AWS Key Management Service 终端节点和配额 AWS 一般参考。

例如，以下密钥策略声明使用kms:ReplicaRegion条件密钥，仅当ReplicaRegion参数的值为指定区域之一时，委托人才能调用该ReplicateKey操作。

```
{
  "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"
      ]
    }
  }
}
```

此条件键仅控制对ReplicateKey操作的访问权限。要控制对UpdatePrimaryRegion操作的访问权限，请使用 k ms: PrimaryRegion 条件密钥。

kms: RetiringPrincipal

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:RetiringPrincipal	字符串（列表）	单值	CreateGrant	密钥策略和 IAM policy

您可以使用此条件键根据请求中RetiringPrincipal参数的值来控制对CreateGrant操作的访问权限。例如，您可以仅在 CreateGrant 请求中的 RetiringPrincipal 与条件语句中的 RetiringPrincipal 匹配时，允许创建使用 KMS 密钥的授权。

要指定即将退出的委托人，请使用委托人的 Amazon 资源名称 (ARN)。 AWS 有效的委托人包括 AWS 账户 IAM 用户、IAM 角色、联合用户和代入角色用户。有关委托人的 ARN 语法的帮助，请参阅 IAM 用户指南中的 IA M ARN。

以下示例密钥策略声明允许用户为 KMS 密钥创建授权。kms:RetiringPrincipal条件键将权限限制为授予中即将退休的委托人为的CreateGrant请求。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"
    }
  }
}
```

另请参阅

- kms: GrantConstraintType
- kms: GrantIsFor AWSResource
- kms: GrantOperations

- kms: GranteePrincipal

kms: RotationPeriodInDays

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:RotationPeriodInDays	数值	单值	EnableKeyRotation	密钥策略和 IAM policy

您可以使用此条件键来限制委托人可以在EnableKeyRotation请求RotationPeriodInDays参数中指定的值。

RotationPeriodInDays指定每个自动密钥轮换日期之间的天数。 AWS KMS 允许您指定介于 90 到 2560 天之间的轮换周期，但您可以使用kms:RotationPeriodInDays条件键进一步限制轮换周期，例如在有效范围内强制规定最短轮换周期。

例如，以下密钥策略声明使用kms:RotationPeriodInDays条件密钥来防止在轮换周期小于或等于 180 天时委托人启用密钥轮换。

```
{
  "Effect": "Deny",
  "Action": "kms:EnableKeyRotation",
  "Principal": "*",
  "Resource": "*",
  "Condition" : {
      "NumericLessThanEquals" : {
        "kms:RotationPeriodInDays" : "180"
      }
  }
}
```

kms: ScheduleKeyDeletionPendingWindowInDays

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:ScheduleKeyDeletionPendingWindowInDays	数值	单值	ScheduleKeyDeletion	密钥策略和 IAM policy

您可以使用此条件键来限制委托人可以在ScheduleKeyDeletion请求PendingWindowInDays参数中指定的值。

PendingWindowInDays指定删除密钥之前 AWS KMS 要等待的天数。 AWS KMS 允许您指定 7 到 30 天之间的等待期，但您可以使用kms:ScheduleKeyDeletionPendingWindowInDays条件键进一步限制等待时间，例如在有效范围内强制规定最短等待时间。

例如，以下密钥政策语句使用 kms:ScheduleKeyDeletionPendingWindowInDays 条件键，以防止主体安排在等待时间小于或等于 21 天时删除密钥。

```
{
  "Effect": "Deny",
  "Action": "kms:ScheduleKeyDeletion",
  "Principal": "*",
  "Resource": "*",
  "Condition" : {
      "NumericLessThanEquals" : {
        "kms:ScheduleKeyDeletionPendingWindowInDays" : "21"
      }
  }
}
```

kms: SigningAlgorithm

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:SigningAlgorithm	String	单值	Sign Verify	密钥策略和 IAM policy

您可以使用kms:SigningAlgorithm条件键根据请求中SigningAlgorithm参数的值来控制对 “签名” 和 “验证” 操作的访问权限。此条件密钥对以外执行的操作没有影响 AWS KMS，例如使用外部非对称 KMS 密钥对中的公钥验证签名。 AWS KMS

以下示例密钥策略允许可担任 testers 角色的用户，仅当用于请求的签名算法为 RSASSA_PSS 算法（如 RSASSA_PSS_SHA512）时，才能使用 KMS 密钥签署消息。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/testers"
  },
  "Action": "kms:Sign",
  "Resource": "*",
  "Condition": {
    "StringLike": {
      "kms:SigningAlgorithm": "RSASSA_PSS*"
    }
  }
}
```

另请参阅

- kms: EncryptionAlgorithm
- the section called “kms: MacAlgorithm”
- the section called “kms: MessageType”

kms: ValidTo

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:ValidTo	Timestamp	单值	ImportKeyMaterial	密钥策略和 IAM policy

kms:ValidTo条件密钥根据请求中ValidTo参数的值控制对ImportKeyMaterial操作的访问权限，该值决定了导入的密钥材料何时过期。此值用 Unix 时间表示。

默认情况下，ImportKeyMaterial 请求中需要 ValidTo 参数。但是，如果ExpirationModel参数的值为KEY_MATERIAL_DOES_NOT_EXPIRE，则该ValidTo参数无效。您也可以使用 kms: ExpirationModel 条件键来要求ExpirationModel参数或特定的参数值。

以下示例策略语句允许用户在 KMS 密钥中导入密钥材料。kms:ValidTo 条件键将权限限制为 ImportKeyMaterial 请求，其中 ValidTo 值小于或等于 1546257599.0（2018 年 12 月 31 日晚上 11:59:59）。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:ImportKeyMaterial",
  "Resource": "*",
  "Condition": {
    "NumericLessThanEquals": {
      "kms:ValidTo": "1546257599.0"
    }
  }
}
```

另请参阅

- kms: ExpirationModel
- kms: WrappingAlgorithm
- kms: WrappingKeySpec

kms: ViaService

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:ViaService	String	单值	KMS 密钥资源操作	密钥策略和 IAM policy

kms:ViaService条件密钥将 KMS 密钥的使用限制为来自指定 AWS 服务的请求。您可以在每个 kms:ViaService 条件键中指定一个或多个服务。该操作必须是 KMS 密钥资源操作，即为特定 KMS 密钥授权的操作。若要标识 KMS 密钥资源操作，请在操作和资源表中，在操作的 Resources 列中查找的 KMS key 的值。

例如，以下密钥策略语句使用 kms:ViaService 条件键以允许仅在请求来自于美国西部（俄勒冈）区域的 Amazon EC2 或 Amazon RDS 时代表 ExampleRole 将客户托管密钥用于指定操作。

```
{
  "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"
      ]
    }
  }
}
```

您也可以使用 kms:ViaService 条件键以在请求来自特定服务时拒绝使用 KMS 密钥的权限。例如，密钥策略中的以下策略语句使用 kms:ViaService 条件键以防止在代表 ExampleRole 发出来自 AWS Lambda 的请求时将客户托管密钥用于 Encrypt 操作。

```
{
  "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

在使用 kms:ViaService 条件键时，服务代表 AWS 账户中的委托人发出请求。这些委托人必须具有以下权限：

- 使用 KMS 密钥的权限。委托人需要向集成服务授予这些权限，这样此服务才能代表委托人使用客户托管的密钥。有关更多信息，请参阅 AWS 服务如何使用 AWS KMS。
- 使用集成服务的权限。有关向用户提供与集成的 AWS 服务的访问权限的详细信息 AWS KMS，请参阅集成服务的文档。

所有 AWS 托管式密钥 都使用其密钥策略文档中的 kms:ViaService 条件键。此条件允许 KMS 密钥仅用于来自创建 KMS 密钥的服务的请求。要查看的密钥策略 AWS 托管式密钥，请使用GetKeyPolicy操作。

kms:ViaService 条件键在 IAM 和密钥策略语句中有效。您指定的服务必须与 AWS KMS集成并支持 kms:ViaService 条件键。

支持 **kms:ViaService** 条件键的服务

下表列出了 AWS 与客户托管密钥集成 AWS KMS 并支持在客户托管密钥中使用kms:ViaService条件密钥的服务。此表中的服务可能并非在所有地区都可用。在所有 AWS 分区中使用 AWS KMS ViaService 名称的.amazonaws.com后缀。

> **Note**
>
> 您可能需要水平或垂直滚动才能查看此表中的所有数据。

服务名称	AWS KMS ViaService 名字
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 网关	backup-gateway. *AWS_region* .amazonaws.com
Amazon Chime SDK	chimevoiceconnector. *AWS_region* .amazonaws.com
AWS CodeArtifact	codeartifact. *AWS_region* .amazonaws.com

服务名称	AWS KMS ViaService 名字
Amazon CodeGuru Reviewer	codeguru-reviewer. *AWS_region* .amazonaws.com
Amazon Comprehend	comprehend. *AWS_region* .amazonaws.com
Amazon Connect	connect.*AWS_region* .amazonaws.com
Amazon Connect Customer Profiles	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 （仅限 EBS）
Amazon Elastic Container Registry (Amazon ECR)	ecr.*AWS_region* .amazonaws.com
Amazon Elastic File System (Amazon EFS)	elasticfilesystem. *AWS_region* .amazonaws.com

服务名称	AWS KMS ViaService 名字
Amazon ElastiCache	在条件键值中包含两个 ViaService 名称： • elasticache. *AWS_region* .amazonaws.com • dax.*AWS_region* .amazonaws.com
AWS Elemental MediaTailor	mediatailor. *AWS_region* .amazonaws.com
AWS 实体分辨率	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 (for Apache Cassandra)	cassandra. *AWS_region* .amazonaws.com

服务名称	AWS KMS ViaService 名字
Amazon Kinesis	kinesis.*AWS_region* .amazonaws.com
Amazon Data Firehose	firehose. *AWS_region* .amazonaws.com
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
Amazon Managed Workflows for Apache Airflow (MWAA)	airflow.*AWS_region* .amazonaws.com

服务名称	AWS KMS ViaService 名字
适用于 Redis 的 Amazon MemoryDB	memorydb. *AWS_region* .amazonaws.com
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
亚马逊 OpenSearch 服务	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 性能详情	rds.*AWS_region* .amazonaws.com
Amazon Redshift	redshift. *AWS_region* .amazonaws.com
Amazon Redshift 查询编辑器 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

服务名称	AWS KMS ViaService 名字
Amazon 复制的数据存储	ards.*AWS_region* .amazonaws.com
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 联系人	ssm-contacts. *AWS_region* .amazonaws.com
Amazon Timestream	timestream. *AWS_region* .amazonaws.com
Amazon Translate	translate. *AWS_region* .amazonaws.com

服务名称	AWS KMS ViaService 名字
AWS Verified Access	verified-access. *AWS_region* .amazonaws.com
Amazon WorkMail	workmail. *AWS_region* .amazonaws.com
Amazon WorkSpaces	workspaces. *AWS_region* .amazonaws.com
Amazon WorkSpaces 瘦客户机	thinclient. *AWS_region* .amazonaws.com
Amazon WorkSpaces Web	workspaces-web. *AWS_region* .amazonaws.com
AWS X-Ray	xray.*AWS_region* .amazonaws.com

kms: WrappingAlgorithm

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:WrappingAlgorithm	String	单值	GetParametersForImport	密钥策略和 IAM policy

此条件键根据请求中WrappingAlgorithm参数的值控制对GetParametersForImport操作的访问权限。您可以使用此条件要求委托人在导入过程中使用特定算法来加密密钥材料。当对所需公有密钥和导入令牌的请求指定不同的包装算法时，它们会失败。

以下示例密钥策略语句使用 kms:WrappingAlgorithm 条件键为示例用户提供调用 GetParametersForImport 操作的权限，但阻止他们使用 RSAES_OAEP_SHA_1 包装算法。当 GetParametersForImport 请求中的 WrappingAlgorithm 是 RSAES_OAEP_SHA_1 时，操作会失败。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:GetParametersForImport",
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "kms:WrappingAlgorithm": "RSAES_OAEP_SHA_1"
    }
  }
}
```

另请参阅

- kms: ExpirationModel
- kms: ValidTo
- kms: WrappingKeySpec

kms: WrappingKeySpec

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型
kms:WrappingKeySpec	String	单值	GetParametersForImport	密钥策略和 IAM policy

此条件键根据请求中WrappingKeySpec参数的值控制对GetParametersForImport操作的访问权限。您可以使用此条件，要求委托人在导入过程中使用特定的公有密钥类型。如果请求指定了不同密钥类型，它会失败。

由于 WrappingKeySpec 参数值的唯一有效值为 RSA_2048，阻止用户使用此值将有效阻止它们使用 GetParametersForImport 操作。

以下示例策略语句使用 kms:WrappingAlgorithm 条件键要求请求中的 WrappingKeySpec 为 RSA_4096。

```
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::111122223333:role/ExampleRole"
  },
  "Action": "kms:GetParametersForImport",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:WrappingKeySpec": "RSA_4096"
    }
  }
}
```

另请参阅

- kms: ExpirationModel
- kms: ValidTo
- kms: WrappingAlgorithm

AWS KMSAWS Nitro Enclaves 的条件密钥

AWS Nitro Enclaves 是 Amazon EC2 的一项功能，它允许您创建称为飞地的隔离计算环境，以保护和处理高度敏感的数据。 AWS KMS 提供条件键来支持 AWS Nitro Enclaves。这些条件密钥仅对请求获得 Nitro Enclave 有效。 AWS KMS

当您使用来自安全区的签名认证文档调用 Decrypt GenerateDataKeyGenerateDataKeyPair、、或 GenerateRandomAPI 操作时，这些 API 会使用认证文档中的公钥对响应中的明文进行加密，并返回密文而不是纯文本。此加密文字只能使用 Enclave 中的私有密钥进行解密。有关更多信息，请参阅 AWS Nitro Enclaves 如何使用 AWS KMS。

通过以下条件键，您可以根据签名证明文档的内容限制这些操作的权限。在允许操作之前，请将安全区中的证明文档与这些条件键中的值进行 AWS KMS 比较。 AWS KMS

kms:RecipientAttestation: ImageSha 384

AWS KMS 条件密钥	条件类型	值类型	API 操作	策略类型

`kms:RecipientAttestation:ImageSha384`	String	单值	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				密钥策略和 IAM policy

当请求中的已签名证明文档中的映像摘要与条件键中的值相匹配时，`kms:RecipientAttestation:ImageSha384` 条件键使用 KMS 密钥控制对 `Decrypt`、`GenerateDataKey`、`GenerateDataKeyPair` 和 `GenerateRandom` 的访问。`ImageSha384` 值对应于证明文档中的 PCR0。仅当请求中的`Recipient`参数为 AWS Nitro 飞地指定了已签名的认证文档时，此条件密钥才有效。

此值也包含在请求获得 Nitro 飞地CloudTrail AWS KMS 的事件中。

> **Note**
>
> 此条件键在密钥策略语句和 IAM policy 语句中有效，即使没有出现在 IAM 控制台或 IAM 服务授权引用中。

例如，以下密钥策略声明允许该`data-processing`角色使用 KMS 密钥进行解密、GenerateDataKeyGenerateDataKeyPair、和GenerateRandom操作。`kms:RecipientAttestation:ImageSha384` 条件键仅允许在请求中的证明文档的映像摘要值（PCR0）与条件中的映像摘要值匹配时执行操作。仅当请求中的`Recipient`参数为 AWS Nitro 飞地指定了已签名的认证文档时，此条件密钥才有效。

如果请求中不包括来自 AWS Nitro 飞地的有效证明文件，则会因为不满足此条件而拒绝许可。

```
{
  "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 条件密钥	条件类型	值类型	API 操作	策略类型
kms:RecipientAttestation:PCR<PCR_ID>	String	单值	Decrypt GenerateDataKey GenerateDataKeyPair GenerateRandom	密钥策略和 IAM policy

kms:RecipientAttestation:PCR<PCR_ID> 条件键仅在请求中的已签名证明文档的平台配置注册（PCR）与条件键中的 PCR 匹配时，通过 KMS 密钥控制对

Decrypt、GenerateDataKey、GenerateDataKeyPair 和 GenerateRandom 的访问。仅当请求中的Recipient参数指定来自 AWS Nitro 飞地的已签名认证文档时，此条件密钥才有效。

此值也包含在代表对 Nitro 飞地 AWS KMS 的请求CloudTrail的事件中。

> **Note**
>
> 此条件键在密钥策略语句和 IAM policy 语句中有效，即使没有出现在 IAM 控制台或 IAM 服务授权引用中。

要指定 PCR 值，请使用以下格式。将 PCR ID 连接到条件键名称。PCR 值必须是最多 96 个字节的小写十六进制字符串。

```
"kms:RecipientAttestation:PCRPCR_ID": "PCR_value"
```

例如，以下条件键指定 PCR1 的特定值，该值对应于用于 Enclave 和引导启动过程的内核的哈希值。

```
kms:RecipientAttestation:PCR1:
 "0x1abcdef2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef
```

以下示例密钥政策语句允许 data-processing 角色将 KMS 密钥用于 Decrypt 操作。

此语句中的 kms:RecipientAttestation:PCR 条件键仅在请求中的签名证明文档的 PCR1 值与条件中的 kms:RecipientAttestation:PCR1 值匹配时允许执行操作。使用 StringEqualsIgnoreCase 策略运算符来要求对 PCR 值进行不区分大小写的比较。

如果请求不包含证明文档，则权限将被拒绝，因为不满足此条件。

```
{
  "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
```

```
    }
  }
}
```

AWS KMS 中的 ABAC

基于属性的访问控制 (ABAC) 是一种授权策略，它基于属性来定义权限。AWS KMS 通过允许您根据与 KMS 密钥关联的标签和别名控制对客户托管密钥的访问来支持 ABAC。在 AWS KMS 中启用 ABAC 的标签和别名条件键提供了一种功能强大且灵活的方式来授权委托人使用 KMS 密钥，而无需编辑策略或管理授权。但是，您应该小心使用这些功能，以免委托人无意中允许或拒绝访问。

如果您使用 ABAC，请注意管理标签和别名的权限现在是访问控制权限。在部署依赖于标签或别名的策略之前，请确保您知道所有 KMS 密钥上的现有标签和别名。添加、删除和更新别名，以及标记和取消标记密钥时，采取合理的预防措施。仅授予需要管理标签和别名权限的委托人该权限，并限制他们可以管理的标签和别名。

> **注意事项**
>
> 将 ABAC 用于 AWS KMS 时，请谨慎授予委托人管理标签和别名的权限。更改标签或别名可以允许或拒绝对 KMS 密钥的权限。不具有更改密钥策略或创建授权权限的密钥管理员可以控制对 KMS 密钥的访问，前提是他们有权管理标签或别名。
>
> 标签和别名的更改最多可能需要 5 分钟的时间才能影响 KMS 密钥授权。最近的更改可能会在 API 操作中显示，然后才会影响授权。
>
> 要根据 KMS 密钥别名控制对它的访问权限，必须使用条件键。您不能使用别名来表示策略语句的 `Resource` 元素中的 KMS 密钥元素。当别名出现在 `Resource` 元素时，策略语句将应用于别名，而不是关联的 KMS 密钥。

了解更多

- 有关 AWS KMS 对 ABAC 支持的详细信息，包括示例，请参阅 使用别名控制对 KMS 密钥的访问 和 使用标签控制对 KMS 密钥的访问。
- 有关使用标签控制对 AWS 资源的访问的更多一般信息，请参阅 IAM 用户指南中的什么是适用于 AWS 的 ABAC？以及使用资源标签控制对 AWS 资源的访问。

AWS KMS 的 ABAC 条件键

要根据 KMS 密钥的标签和别名授权访问 KMS 密钥，请在密钥政策或 IAM policy 中使用以下条件键。

ABAC 条件键	描述	策略类型	AWS KMS 操作
aws：ResourceTag	KMS 密钥上的标签（键和值）与策略中的标签（键和值）或标签模式匹配	仅限 IAM policy	KMS 密钥资源操作 [2]
aws:RequestTag/tag-key	请求中的标签（键和值）与策略中的标签（键和值）或标签模式匹配	密钥政策和 IAM policy [1]	TagResource, UntagResource
aws：TagKeys	请求中的标签键与策略中的标签键匹配	密钥政策和 IAM policy [1]	TagResource, UntagResource
kms: ResourceAliases	与 KMS 密钥关联的别名与策略中的别名或别名模式匹配	仅限 IAM policy	KMS 密钥资源操作 [2]
kms: RequestAlias	表示请求中的 KMS 密钥的别名与策略中的别名或别名模式匹配。	密钥政策和 IAM policy [1]	加密操作，，DescribeKeyGetPublicKey

[1] 任何可在密钥政策中使用的条件键也可以在 IAM policy 中使用，但只有在密钥政策允许它时。

[2] KMS 密钥资源操作是特定 KMS 密钥授权的操作。若要标识 KMS 密钥资源操作，请在 AWS KMS 权限表中，在操作的 `Resources` 列中查找的 KMS 密钥的值。

例如，您可以使用这些条件键创建以下策略。

- 具有 `kms:ResourceAliases` 的 IAM policy，可授予将 KMS 密钥与特定别名或别名模式结合使用的权限。这与依赖于标签的策略略有不同：尽管您可以在策略中使用别名模式，但每个别名在 AWS 账户 和区域中必须是唯一的。这使您能够将策略应用于选定的 KMS 密钥集，而无需在策略语句中列出 KMS 密钥的密钥 ARN。要从集中添加或删除 KMS 密钥，请更改 KMS 密钥的别名。
- 带有 `kms:RequestAlias` 的密钥策略，可允许委托人在 `Encrypt` 操作中使用 KMS 密钥，但前提是仅当 `Encrypt` 请求使用该别名标识 KMS 密钥时。

- 带有 aws:ResourceTag/*tag-key* 的 IAM policy，可拒绝将 KMS 密钥与特定标签键和标签值结合使用的权限。这让您能够将策略应用于选定的 KMS 密钥集，而无需在策略语句中列出 KMS 密钥的密钥 ARN。要在集中添加或删除 KMS 密钥，请标记或取消标记 KMS 密钥。
- 带有 aws:RequestTag/*tag-key* 的 IAM policy，可允许委托人仅删除 "Purpose"="Test" KMS 密钥标签。
- 带有 aws:TagKeys 的 IAM policy，可拒绝使用 Restricted 标签键标记或取消标记 KMS 密钥的权限。

ABAC 使访问管理具有灵活性和可扩展性。例如，您可以使用 aws:ResourceTag/*tag-key* 条件键创建 IAM policy，该策略允许委托人仅在 KMS 密钥具有 Purpose=Test 标签时将 KMS 密钥用于特定操作。该策略适用于 AWS 账户 的所有区域中的所有 KMS 密钥。

当附加到用户或角色时，以下 IAM policy 允许委托人将带有 Purpose=Test 标签的所有现有 KMS 密钥用于指定操作。要提供对新的或现有 KMS 密钥的访问权限，您不需要更改策略。只需将 Purpose=Test 标签附加到 KMS 密钥。同样，要从具有 Purpose=Test 标签的 KMS 密钥中删除此访问权限，请编辑或删除标签。

```
{
  "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"
        }
      }
    }
  ]
}
```

但是，如果您使用此功能，在管理标记和别名时要加小心。添加、更改或删除标签或别名可能会无意中允许或拒绝对 KMS 密钥的访问。不具有更改密钥策略或创建授权权限的密钥管理员可以控制对 KMS 密钥的访问，前提是他们有权管理标签和别名。为了减轻这种风险，请考虑限制管理标签的权限和别名。例如，您可能想要仅允许特色级委托人管理 `Purpose=Test` 标签。有关详细信息，请参阅 使用别名控制对 KMS 密钥的访问 和 使用标签控制对 KMS 密钥的访问。

标签还是别名？

AWS KMS 支持带有标签和别名的 ABAC。这两种选项都提供了灵活、可扩展的访问控制策略，但它们彼此略有不同。

您可能会根据您的特定 AWS 使用模式决定是使用标签还是使用别名。例如，如果您已经向大多数管理员授予了标记权限，则基于别名控制授权策略可能会更容易。或者，如果您接近每个 KMS 密钥的别名数量配额，您可能更喜欢基于标签的授权策略。

以下益处是大家都感兴趣的。

基于标签的访问控制的益处

- 不同类型的 AWS 资源的授权机制相同。

  您可以使用相同的标签或标签键来控制对多种资源类型的访问，例如 Amazon Relational Database Service（Amazon RDS）集群、Amazon Elastic Block Store（Amazon EBS）卷和 KMS 密钥。此功能支持多种不同的授权模型，这些模型比传统的基于角色的访问控制更加灵活。
- 授权访问一组 KMS 密钥。

  您可以使用标签来管理对同一 AWS 账户 和区域中的一组 KMS 密钥的访问权限。将相同的标签或标签键分配给您选择的 KMS 密钥。然后创建一个基于标签或标签密钥的简单 easy-to-maintain 策略声明。要在授权组中添加或删除 KMS 密钥，请添加或删除标签；您无需编辑策略。

基于别名的访问控制的益处

- 根据别名授权对加密操作的访问。

  大多数基于请求的属性策略条件，包括 a ws:RequestTag/tag-key，仅影响添加、编辑或删除属性的操作。但是 k ms: RequestAlias 条件密钥根据用于在请求中识别 KMS 密钥的别名来控制对加密操作的访问。例如，您可以授予委托人在 `Encrypt` 操作中使用 KMS 密钥的权限，但只有当 `KeyId` 参数的值为 `alias/restricted-key-1` 时。要满足此条件，需要以下所有条件：
  - KMS 密钥必须与该别名相关联。

- 请求必须使用别名来标识 KMS 密钥。
- 委托人必须拥有使用受 `kms:RequestAlias` 条件约束的 KMS 密钥的权限。

如果您的应用程序通常使用别名名称或别名 ARN 来引用 KMS 密钥，这将特别有用。

- 提供非常有限的权限。

别名在 AWS 账户 和区域中必须是唯一的。因此，基于别名授予委托人访问 KMS 密钥的权限可能比基于标签授予他们访问权限更严格。与别名不同，标签可分配给同一账户和区域中的多个 KMS 密钥。如果选择，则可以使用别名模式（例如 `alias/test*`）为委托人授予对同一账户和区域中一组 KMS 密钥的访问权限。但是，允许或拒绝访问特定别名允许对 KMS 密钥进行非常严格的控制。

适用于 AWS KMS 的 ABAC 的故障排除

基于 KMS 密钥的标签和别名控制对 KMS 密钥的访问非常方便，且功能强大。但是，它容易出现一些您希望防止的可预测错误。

由于标签更改而更改访问权限

如果某个标签被删除或其值被更改，则仅能基于该标签访问 KMS 密钥的委托人将被拒绝访问 KMS 密钥。当拒绝策略语句中包含的标签添加到 KMS 密钥时，也会发生这种情况。向 KMS 密钥添加与策略相关的标签可以允许访问应被拒绝访问 KMS 密钥的委托人。

例如，假设委托人可以基于 `Project=Alpha` 标签访问 KMS 密钥，例如以下示例 IAM policy 语句提供的权限。

```
{
  "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"
        }
```

```
      }
    }
  ]
}
```

如果该标签已从该 KMS 密钥中删除或标签值发生更改，则委托人不再具有将 KMS 密钥用于指定操作的权限。当委托人尝试在使用客户托管密钥的AWS服务中读取或写入数据时，这一点可能会变得显而易见。要跟踪标签的更改，请查看您的 CloudTrail日志TagResource或UntagResource 条目。

要在不更新策略的情况下恢复访问，请更改 KMS 密钥上的标签。这一措施除了短时间在整个 AWS KMS 中生效之后，产生的影响极小。为了防止这样的错误，请仅向需要它的委托人授予标记和取消标记权限，并将其标记权限限制到他们需要管理的标签。更改标签之前，请搜索策略以检测依赖于标签的访问权限，并在具有该标签的所有区域中获取 KMS 密钥。您可以考虑在更改特定标签时创建 Amazon CloudWatch 警报。

由于别名更改而导致的访问权限更改

如果别名被删除或与其他 KMS 密钥关联，则仅能基于该别名访问 KMS 密钥的委托人将被拒绝访问 KMS 密钥。当拒绝策略语句中包含与 KMS 密钥关联的别名时，也会发生这种情况。向 KMS 密钥添加与策略相关的别名也可以允许访问应被拒绝访问 KMS 密钥的委托人。

例如，以下 IAM 策略声明使用 k ms: ResourceAliases 条件密钥允许使用任意指定别名访问账户中不同区域的 KMS 密钥。

```
{
  "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"
```

```
            ]
          }
        }
      }
    ]
}
```

要跟踪别名更改，请查看 CloudTrail 日志中是否有CreateAliasUpdateAlias、和DeleteAlias条目。

要在不更新策略的情况下恢复访问，请更改与 KMS 密钥关联的别名。由于每个别名只能与账户和区域中的一个 KMS 密钥相关联，因此管理别名比管理标签要困难一些。恢复一些委托人对一个 KMS 密钥的访问权限可能会拒绝相同或其他委托人对其他 KMS 密钥的访问。

为了防止出现此错误，请仅向需要它的委托人授予别名管理权限，并将其别名管理权限限制到他们需要管理的别名。在更新或删除别名之前，请搜索策略以检测依赖于别名的访问权限，并在与别名关联的所有区域中查找 KMS 密钥。

由于别名配额而拒绝访问

如果 KMS 密钥超过该账户和地区每个 KMS 密钥配额的默认别名，则获得 kms: ResourceAliases 条件授权使用 KMS 密钥的用户将获得AccessDenied例外。

要恢复访问，请删除与 KMS 密钥关联的别名，使其符合配额。或者使用备用机制授予用户访问 KMS 密钥的权限。

延迟的授权更改

您对标签和别名的更改最多可能需要 5 分钟的时间才能影响 KMS 密钥授权。因此，标签或别名更改可能会在 API 操作影响授权之前反映在响应中。此延迟可能会比影响大多数 AWS KMS 操作的短暂最终一致性延迟长。

例如，您可能拥有一个 IAM policy，允许某些委托人使用带有 "Purpose"="Test" 标签的任何 KMS 密钥。然后，您将 "Purpose"="Test" 标签添加到 KMS 密钥。尽管TagResource操作已完成且ListResourceTags响应确认标签已分配给 KMS 密钥，但委托人可能在长达五分钟内无法访问 KMS 密钥。

为了防止出现错误，请将此预期延迟构建到您的代码中。

由于别名更新而失败的请求

当您更新别名时，您将现有别名与另一个 KMS 密钥关联。

解密和指定别名或别名 ARN 的ReEncrypt请求可能会失败，因为该别名现在与未加密密文的 KMS 密钥相关联。这种情况通常会返回 IncorrectKeyException 或者 NotFoundException。或者如果请求中没有 KeyId 或 DestinationKeyId 参数，则操作可能会失败，并出现 AccessDenied 异常，因为调用方不再具有对加密密文的 KMS 密钥的访问权限。

您可以通过查看CreateAliasUpdateAlias、和 CloudTrail 日志条目的DeleteAlias日志来跟踪更改。您还可以在ListAliases响应中使用该LastUpdatedDate字段的值来检测更改。

例如，以下ListAliases示例响应显示kms:ResourceAliases条件中的ProjectAlpha_Test别名已更新。因此，基于别名具有访问权限的委托人将失去对先前关联的 KMS 密钥的访问权限。相反，他们可以访问新关联的 KMS 密钥。

```
$ 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
        }
    ]
}
```

这种变化的补救办法并不简单。您可以再次更新别名以将其与原始 KMS 密钥关联。但是，在执行操作之前，您需要考虑该更改对当前关联的 KMS 密钥的影响。如果委托人在加密操作中使用后一个 KMS 密钥，他们可能需要继续访问该密钥。在这种情况下，您可能需要更新策略以确保委托人有权使用这两个 KMS 密钥。

您可以防止出现这样的错误：在更新别名之前，搜索策略以检测依赖于别名的访问。然后，在与别名关联的所有区域中获取 KMS 密钥。请仅向需要它的委托人授予别名管理权限，并将其别名管理权限限制到他们需要管理的别名。

允许其他账户中的用户使用 KMS 密钥

您可以允许其他 AWS 账户中的用户或角色使用您账户中的 KMS 密钥。跨账户访问需要在 KMS 密钥的密钥策略和外部用户账户的 IAM policy 中拥有权限。

跨账户权限仅对以下操作有效：

- 加密操作
- CreateGrant
- DescribeKey
- GetKeyRotationStatus
- GetPublicKey
- ListGrants
- RetireGrant
- RevokeGrant

如果您向另一个账户中的用户授予对其他操作的权限，则这些权限将不起作用。例如，如果您向其他账户中的委托人授予 IAM 策略中的 k ms: ListKeys 权限，或者在密钥策略中ScheduleKeyDeletion授予 KMS: 密钥权限，则该用户尝试对您的资源调用这些操作仍会失败。

有关在不同账户中使用 KMS 密钥进行 AWS KMS 操作的详细信息，请参阅 AWS KMS 权限 和 在其他账户中使用 KMS 密钥 中的跨账户使用列。AWS Key Management Service API 参考中每个 API 描述中还有一个跨账户使用部分。

> **Warning**
>
> 请谨慎授予委托人使用 KMS 密钥的权限。只要有可能，请按照最小特权原则。仅针对用户所需的操作为他们授予对所需的 KMS 密钥的访问权。
> 此外，请谨慎使用任何不熟悉的 KMS 密钥，尤其是其他账户中的 KMS 密钥。恶意用户可能会授予您使用其 KMS 密钥获取有关您或您账户的信息的权限。
> 有关使用策略保护您账户中的资源的更多信息，请参阅 IAM policy 的最佳实践。

要将使用 KMS 密钥的权限授予其他账户中的用户和角色，您必须使用两种不同类型的策略：

- KMS 密钥的密钥策略必须向外部账户（或外部账户中的用户和角色）授予使用 KMS 密钥的权限。密钥策略在拥有 KMS 密钥的账户中。
- 外部账户中的 IAM policy 必须将密钥策略权限委托给其用户和角色。这些策略在外部账户中设置，并向该账户中的用户和角色授予权限。

密钥策略决定谁可以访问 KMS 密钥。IAM policy 决定谁确实能够访问 KMS 密钥。单独的密钥策略和 IAM policy 都不足够，您必须更改此两者。

要编辑密钥策略，您可以使用中的策略视图AWS Management Console或使用CreateKey或PutKeyPolicy操作。有关在创建 KMS 密钥时设置密钥策略的帮助信息，请参阅 创建其他账户可以使用的 KMS 密钥。

有关编辑 IAM policy 时的帮助信息，请参阅。将 IAM 策略与配合使用 AWS KMS

有关说明密钥策略和 IAM policy 如何协同工作以允许在其他账户中使用 KMS 密钥的示例，请参阅。示例 2：用户代入的角色具有使用不同 AWS 账户 中的 KMS 密钥的权限

您可以在您的 AWS CloudTrail 日志中查看对 KMS 密钥产生的跨账户 AWS KMS 操作。在其他账户中使用 KMS 密钥的操作将记录在调用方的账户和 KMS 密钥所有者账户中。

主题

> **Note**
>
> 本主题中的示例展示了如何结合使用密钥策略和 IAM policy 来提供和限制对 KMS 密钥的访问。这些通用示例不是为了表示任何特定的 AWS 服务 对于 KMS 密钥需要的权限。有关 AWS 服务 需要的权限的信息，请参阅服务文档中的加密主题。

步骤 1：在本地账户中添加密钥策略语句

KMS 密钥的密钥策略是谁可以访问 KMS 密钥以及他们可以执行哪些操作的主要决定因素。密钥策略始终在拥有 KMS 密钥的账户中。与 IAM policy 不同，密钥策略不指定资源。资源是指与密钥策略关联的 KMS 密钥。在提供跨账户权限时，KMS 密钥的密钥策略必须向外部账户（或外部账户中的用户和角色）授予使用 KMS 密钥的权限。

要向外部账户授予使用 KMS 密钥的权限，请向密钥策略添加一条语句用于指定此外部账户。在密钥策略的 `Principal` 元素中，输入外部账户的 Amazon Resource Name (ARN)。

当您在密钥策略中指定外部账户时，外部账户中的 IAM 管理员可以使用 IAM policy 来将这些权限委派给外部账户中的任何用户和角色。他们还可以决定用户和角色可以执行在密钥策略中指定的哪些操作。

只有在托管 KMS 密钥及其密钥策略的区域中启用了外部账户时，授予给外部账户及其委托人的权限才有效。有关默认情况下未启用的区域（“选择加入区域”）的信息，请参阅《AWS 一般参考》 中的 Managing AWS 区域。

例如，假定您希望允许账户 444455556666 使用账户 111122223333 中的对称加密 KMS 密钥。为此，请将与以下示例中的策略语句类似的策略语句添加到账户 111122223333 中 KMS 密钥的密钥策略。此策略语句授权外部账户 444455556666 在加密操作中使用对称加密 KMS 密钥的 KMS 密钥。

> **Note**
>
> 以下示例演示了与其他账户共享 KMS 密钥的示例密钥策略。请将示例 `Sid`、`Principal` 和 `Action` 的值替换为 KMS 密钥预期用途的有效值。

```
{
    "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": "*"
}
```

您可以在密钥策略中指定特定的外部用户和角色，而不是向外部账户授予权限。但是，这些用户和角色无法使用该 KMS 密钥，直到外部账户中的 IAM 管理员将适当的 IAM policy 附加到其身份。IAM policy 可以向在密钥策略中指定的所有或部分外部用户和角色授予权限。并且，它们可以允许执行在密钥策略中指定的所有或部分操作。

在密钥策略中指定身份会限制外部账户中的 IAM 管理员可以提供的权限。但是，它使两个账户的策略管理变得更加复杂。例如，假定您需要添加用户或角色。您必须将该身份添加到拥有 KMS 密钥的账户中的密钥策略，并在此身份的账户中创建 IAM policy。

要在密钥策略中指定特定外部用户或角色，请在 `Principal` 元素中输入外部账户中的用户或角色的 Amazon Resource Name (ARN)。

例如，以下示例密钥策略语句允许账户 `444455556666` 中的 `ExampleRole` 使用账户 `111122223333` 中的 KMS 密钥。此密钥策略语句授权外部账户 `444455556666` 在加密操作中使用对称加密 KMS 密钥的 KMS 密钥。

> **Note**
>
> 以下示例演示了与其他账户共享 KMS 密钥的示例密钥策略。请将示例 `Sid`、`Principal` 和 `Action` 的值替换为 KMS 密钥预期用途的有效值。

```
{
    "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**
>
> 除非您使用条件限制密钥政策，否则不要在允许权限的任何密钥政策语句将主体设置为星号（*）。星号表示允许每个 AWS 账户 权限中的每个身份使用 KMS 密钥，除非另一个策略语句明确拒绝它。其他 AWS 账户 中的用户只要在自己的账户中拥有相应的权限，就可以使用您的 KMS 密钥。

您还需要确定您想要向外部账户授予哪些权限。有关针对 KMS 密钥的权限的列表，请参阅 AWS KMS 权限。

您可以向外部账户授予权限以便在加密操作中使用 KMS 密钥，并将 KMS 密钥和与 AWS KMS 集成的 AWS 服务一起使用。为此，请使用 AWS Management Console 的密钥用户部分。有关更多信息，请参阅 创建其他账户可以使用的 KMS 密钥。

要在密钥策略中指定其他权限，请编辑密钥策略文档。例如，您可能希望授予用户解密但不加密的权限，或者查看 KMS 密钥但不使用 KMS 密钥的权限。要编辑密钥策略文档，您可以使用AWS Management Console或CreateKey或PutKeyPolicy操作中的策略视图。

步骤 2：在外部账户中添加 IAM policy

拥有 KMS 密钥的账户中的密钥策略设置权限的有效范围。但是，在附加委派这些权限的 IAM policy 或使用授权来管理对 KMS 密钥的访问之前，外部账户中的用户和角色无法使用此 KMS 密钥。IAM policy 在外部账户中设置。

如果密钥策略向外部账户授予权限，则可以将 IAM policy 附加到账户中的任何用户或角色。但是，如果密钥策略向指定的用户或角色授予权限，则 IAM policy 只能将这些权限授予全部或部分指定用户和角色。如果 IAM policy 向其他外部用户或角色授予使用 KMS 密钥的权限，则它不起作用。

密钥策略还限制 IAM policy 中的操作。IAM policy 可以委派在密钥策略中指定的所有或部分操作。如果 IAM policy 列出未在密钥策略中指定的操作，则这些权限无效。

以下示例 IAM policy 允许委托人使用账户 111122223333 中的 KMS 密钥执行加密操作。要向账户 444455556666 中的用户和角色授予此权限，请将策略附加到账户 444455556666 中的用户或角色。

> **Note**
>
> 以下示例演示了与其他账户共享 KMS 密钥的示例 IAM policy。请将示例 `Sid`、`Resource` 和 `Action` 的值替换为 KMS 密钥预期用途的有效值。

```
{
    "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"
}
```

请注意有关该策略的以下详细信息：

- 与密钥策略不同，IAM policy 语句不包含 `Principal` 元素。在 IAM policy 中，委托人是附加了策略的身份。
- IAM policy 中的 `Resource` 元素标识委托人可以使用的 KMS 密钥。要指定 KMS 密钥，请将其密钥 ARN 添加到 `Resource` 元素中。
- 您可以在 `Resource` 元素中指定多个 KMS 密钥。但是，如果您没有在 `Resource` 元素中指定特定的 KMS 密钥，您可能会无意中比预期授予针对更多 KMS 密钥的权限。
- 要允许外部用户将 KMS 密钥和与 AWS KMS 集成的 AWS 服务一起使用，您可能需要向密钥策略或 IAM policy 添加权限。有关更多信息，请参阅 允许将外部 KMS 密钥与 AWS 服务结合使用。

有关使用 IAM policy 的更多信息，请参阅 IAM 策略。

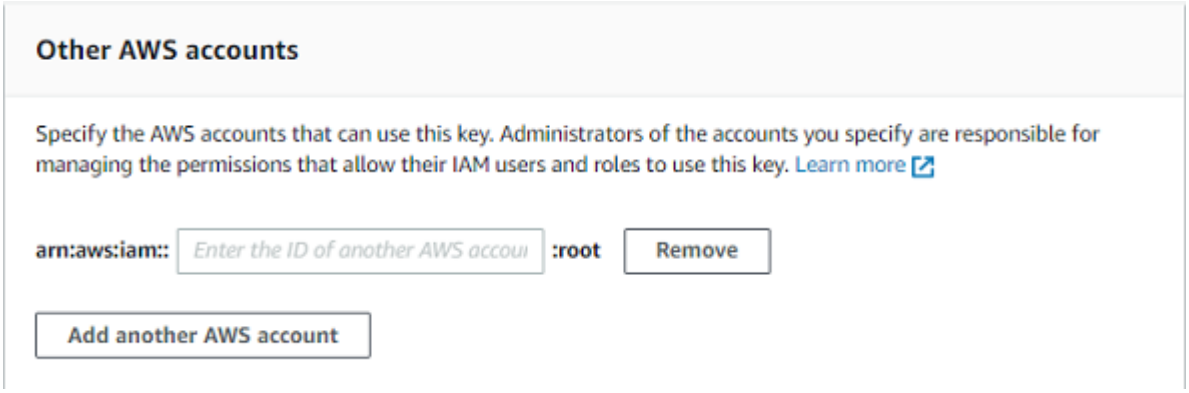
创建其他账户可以使用的 KMS 密钥

使用该CreateKey操作创建 KMS 密钥时，您可以使用其`Policy`参数来指定密钥策略，该策略向外部账户或外部用户和角色授予使用 KMS 密钥的权限。您还必须在外部账户中添加 IAM policy，以

将这些权限委派给此账户的用户和角色，即使在密钥策略中指定了用户和角色也是如此。您可以使用PutKeyPolicy操作随时更改密钥策略。

当您在 AWS Management Console 中创建 KMS 密钥时，还会创建其密钥策略。当您在密钥管理员和密钥用户部分中选择身份时，AWS KMS 会将这些身份的策略语句添加到 KMS 密钥的密钥策略中。

密钥用户部分还允许您将外部账户添加为密钥用户。



当您输入外部账户的账户 ID 时，AWS KMS 向密钥策略添加两个语句。此操作仅影响密钥策略。外部账户中的用户和角色无法使用该 KMS 密钥，直到您附加 IAM policy 以向他们授予部分或所有这些权限。

第一个密钥策略语句向外部账户授予在加密操作中使用 KMS 密钥的权限。

> **Note**
>
> 以下示例演示了与其他账户共享 KMS 密钥的示例密钥策略。请将示例 `Sid`、`Principal` 和 `Action` 的值替换为 KMS 密钥预期用途的有效值。

```
{
    "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": "*"
    }
```

第二个密钥策略语句允许外部账户在 KMS 上创建、查看和撤消授权，但仅限请求来自与 AWS KMS 集成的 AWS 服务的情况。这些权限允许加密用户数据的其他 AWS 服务使用 KMS 密钥。

这些权限专为加密AWS服务（例如 Amazon）中的用户数据的 KMS 密钥而设计 WorkMail。这些服务通常使用授权来获取以用户名义使用 KMS 密钥所需的权限。有关更多信息，请参阅 允许将外部 KMS 密钥与 AWS 服务结合使用。

```
{
    "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"
        }
    }
}
```

如果这些权限不能满足您的需求，则可以在控制台策略视图中或使用PutKeyPolicy操作对其进行编辑。您可以指定特定的外部用户和角色，而不是向外部账户授予权限。您可以更改策略指定的操作。您可以使用全局和 AWS KMS 策略条件来细化权限。

允许将外部 KMS 密钥与 AWS 服务结合使用

您可以向不同账户中的用户授予将您的 KMS 密钥和与 AWS KMS 集成的服务一起使用的权限。例如，外部账户中的用户可以使用您的 KMS 密钥加密 Amazon S3 存储桶中的对象或加密存储在 AWS Secrets Manager 中的密钥。

密钥策略必须向外部用户或外部用户的账户授予使用 KMS 密钥的权限。此外，您需要将 IAM policy 附加到某个身份，以向用户授予使用 AWS 服务的权限。该服务还可能要求用户在密钥策略或 IAM policy 中具有其他权限。有关 AWS 服务需要对客户管理型密钥拥有的权限列表，请参阅相关服务的用户指南或开发人员指南中“安全”章节的“数据保护”主题。

在其他账户中使用 KMS 密钥

如果您有权在另一个 AWS 账户 中使用 KMS 密钥，您可以在 AWS Management Console、AWS 开发工具包、AWS CLI 和 AWS Tools for PowerShell 中使用 KMS 密钥。

要在 shell 命令或 API 请求中标识其他账户中的 KMS 密钥，请使用以下密钥标识符。

- 对于加密操作DescribeKeyGetPublicKey、和，请使用 KMS 密钥的密钥 ARN 或别名 ARN。
- 对于CreateGrant、GetKeyRotationStatusListGrants、和 RevokeGrant，请使用 KMS 密钥的密钥 ARN。

如果您只输入密钥 ID 或别名名称，AWS 会假定 KMS 密钥位于您的账户中。

AWS KMS 控制台不会在其他账户中显示 KMS 密钥，即使您有权使用它们。此外，在其他 AWS 服务的控制台中显示的 KMS 密钥的列表不包括其他账户中的 KMS 密钥。

要在 AWS 服务的控制台中指定不同账户中的 KMS 密钥，您必须输入 KMS 密钥的密钥 ARN。所需的密钥标识符因服务而异，并且在服务控制台及其 API 操作之间可能会有所不同。有关详细信息，请参阅服务文档。

将服务相关角色用于 AWS KMS

AWS Key Management Service 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特类型的 IAM 角色，它与 AWS KMS 直接相关。服务相关角色由 AWS KMS 定义，并包含该服务代表您调用其他 AWS 服务所需的全部权限。

服务相关角色使 AWS KMS 的设置更轻松，因为您不必手动添加必要的权限。AWS KMS 定义其服务相关角色的权限，除非另行定义，否则仅 AWS KMS 可以担任其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

只有在先删除相关资源后，才能删除服务相关角色。这将保护您的 AWS KMS 资源，因为您不会无意中删除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅使用 IAM 的 AWS 服务并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

AWS KMS 自定义密钥存储的服务相关角色权限

AWS KMS使用名为的服务相关角色AWSServiceRoleForKeyManagementServiceCustomKeyStores来支持自定义密钥存储。此服务相关角色授予 AWS KMS 权限以查看您的 AWS CloudHSM 集群并创建网络基础设施，以支持自定义密钥存储与其 AWS CloudHSM 集群之间的连接。AWS KMS 将在您创建自定义密钥存储时创建此角色。您无法直接创建此服务相关角色。

AWSServiceRoleForKeyManagementServiceCustomKeyStores 服务相关角色信任 `cks.kms.amazonaws.com` 来代入该角色。因此，只有 AWS KMS 才能代入此服务相关角色。

此角色中的权限限制为 AWS KMS 为了将自定义密钥存储连接到 AWS CloudHSM 集群而执行的操作。它不会向 AWS KMS 提供任何额外权限。例如，AWS KMS 无权创建、管理或删除您的 AWS CloudHSM 集群、HSM 或备份。

有关 AWSServiceRoleForKeyManagementServiceCustomKeyStores 角色的更多信息，包括权限列表以及有关如何查看角色、编辑角色描述、删除角色和让 AWS KMS 为您重新创建角色的说明，请参阅授权 AWS KMS 管理 AWS CloudHSM 和 Amazon EC2 资源。

AWS KMS 多区域密钥的服务相关角色权限

AWS KMS使用名为的服务相关角色AWSServiceRoleForKeyManagementServiceMultiRegionKeys来支持多区域密钥。此服务相关角色授予 AWS KMS 权限以将多区域主密钥的密钥材料的任何更改同步到其副本密钥。AWS KMS 将仅在您创建多区域主密钥时创建此角色。您无法直接创建此服务相关角色。

AWSServiceRoleForKeyManagementServiceMultiRegionKeys 服务相关角色信任 `mrk.kms.amazonaws.com` 来代入该角色。因此，只有 AWS KMS 才能代入此服务相关角色。此角色的权限限制为 AWS KMS 为了保持相关多区域密钥中的密钥材料同步而执行的操作。它不会向 AWS KMS 提供任何额外权限。

有关 AWSServiceRoleForKeyManagementServiceMultiRegionKeys 角色的更多信息，包括权限列表以及有关如何查看角色、编辑角色描述、删除角色和让 AWS KMS 为您重新创建角色的说明，请参阅授权 AWS KMS 同步多区域密钥。

AWS KMS 更新了 AWS 托管式策略

查看有关 AWS KMS 的 AWS 托管策略更新的详细信息（从该服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅 AWS KMS 文档历史记录 页面上的 RSS 源。

更改	描述	日期
AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy – 对现有策略的更新	AWS KMS添加了`ec2:DescribeVpcs` `ec2:DescribeNetworkAcls` 、和`ec2:DescribeNetworkInterfaces` 权限以监控包含您的AWS CloudHSM集群的 VPC 中的变化，以便在出现故障时AWS KMS可以提供清晰的错误消息。	2023 年 11 月 10 日
AWS KMS 开启了跟踪更改	AWS KMS 为其 AWS 托管式策略开启了跟踪更改。	2023 年 11 月 10 日

将混合后量子 TLS 与 AWS KMS 结合使用

AWS Key Management Service (AWS KMS) 支持对传输层安全 (TLS) 网络加密协议使用混合后量子密钥交换选项。当您连接到 AWS KMS API 终端节点时，可以使用此 TLS 选项。我们在标准化后量子算法之前提供了此功能，因此您可以开始测试这些密钥交换协议对 AWS KMS 调用产生的影响。这些混合后量子密钥交换功能是可选的，至少与我们目前使用的 TLS 加密一样安全，并且有可能会提供额外的长期安全优势。不过，与目前使用的传统密钥交换协议相比，它们会影响延迟和吞吐量性能。

您发送到 AWS Key Management Service (AWS KMS) 的数据，在传输过程中由传输层安全 (TLS) 连接提供的加密机制进行保护。借助 AWS KMS 支持对 TLS 会话使用的传统密码套件，使得对密钥交换机制进行的暴力攻击在现有技术下是不可行的。不过，如果大规模量子计算在未来得到广泛应用，那么 TLS 密钥交换机制中使用的传统密码套件将会容易受到这些攻击。如果您正在开发的应用程序依赖于通过 TLS 连接传输的数据的长期保密性，则应考虑在大规模量子计算机投入使用之前，采用迁移到后量子密码加密技术的计划。AWS 正在努力针对这个远景做好准备，我们希望您也能做好充分的准备。

为了保护今天加密的数据，让这些数据在未来免受可能的攻击，AWS 正在积极参与密码社区，一起开发抗量子密码算法或后量子算法。我们在 AWS KMS 中实施了混合后量子密钥交换密码套件，通过将传统加密算法与后量子算法相结合，可确保 TLS 连接至少与传统密码套件一样强大。

这些混合密码套件可以在大多数 AWS 区域 中用于您的生产工作负载。不过，由于混合密码套件的性能特征及带宽要求与传统密钥交换机制的性能特征及带宽要求有所不同，我们建议您在不同条件下针对 AWS KMS API 调用开展测试。

反馈

与以前一样，我们希望您能够提供反馈并参与我们的开源存储库。我们尤其希望了解您的基础设施如何与新形式的 TLS 流量进行交互。

- 要提供有关本主题的反馈，请使用此页面右上角的反馈链接。
- 我们正在的s2n-tls存储库中以开源方式开发这些混合密码套件。 GitHub要提供有关密码套件可用性方面的反馈，或者共享全新的测试条件或结果，请在 s2n-tls 存储库中创建问题。
- 我们正在编写代码示例，用于在aws-kms-pq-tls-example GitHub存储库AWS KMS中使用混合后量子 TLS。要提出问题或分享有关配置 HTTP 客户端或 AWS KMS 客户端以使用混合密码套件的想法，请在 aws-kms-pq-tls-example 存储库中创建问题。

支持 AWS 区域

AWS KMS 的后量子 TLS 在所有 AWS KMS 支持的 AWS 区域 均可用，但中国（北京）和中国（宁夏）除外。

> **Note**
>
> AWS KMS 在 AWS GovCloud (US) 中不支持 FIPS 端点的混合后量子 TLS。

有关每个 AWS 区域 中 AWS KMS 端点的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Key Management Service endpoints and quotas。有关 FIPS 端点的信息，请参阅《Amazon Web Services 一般参考》中的 FIPS endpoints。

关于 TLS 中的混合后量子密钥交换

AWS KMS 支持混合后量子密钥交换密码套件。您可以在 Linux 系统上使用 AWS SDK for Java 2.x 和 AWS 公共运行时，以配置使用这些密码套件的 HTTP 客户端。然后，无论您何时使用 HTTP 客户端连接到 AWS KMS 端点，都会使用混合密码套件。

此 HTTP 客户端使用 s2n-tls，后者是 TLS 协议的开源实现。s2n-tls 使用的混合密码套件只能用于密钥交换，而不能用于直接数据加密。在密钥交换过程中，客户端和服务器会计算将用于加密和解密传输中的数据的密钥。

s2n-tls 使用的算法是混合算法，它结合了椭圆曲线 Diffie-Hellman (ECDH)（目前 TLS 中使用的传统密钥交换算法）与 Kyber（公有密钥加密和密钥生成算法，美国国家标准和技术研究院（NIST）已指定此算法为第一个标准后量子密钥协商算法）。此混合算法单独使用每个算法来生成密钥。然后，以加密

方式结合使用这两个密钥。使用 s2n-tls 时，您可以 配置 HTTP 客户端 来优先使用后量子 TLS，后者会将 ECDH 与 Kyber 放在优先列表的首位。传统密钥交换算法包含在优先列表中以确保兼容性，但它们的优先顺序较低。

尽管正在进行的研究表明 Kyber 算法缺乏预期的后量子密码强度，但混合密钥至少与目前使用的单个 ECDH 密钥一样强大。在关于后量子算法的研究完成之前，我们建议使用混合算法，而不是单独使用后量子算法。

将混合后量子 TLS 与 AWS KMS 结合使用

您可以对 AWS KMS 调用使用混合后量子 TLS。在设置 HTTP 客户端测试环境时，请注意以下信息：

传输中加密

s2n-tls 中的混合密码套件仅用于传输中加密。它们在数据从客户端传输到 AWS KMS 终端节点的过程中保护您的数据。AWS KMS 不会使用这些密码套件来加密使用 AWS KMS keys 保护的数据。

相反，AWS KMS 在使用 KMS 密钥加密您的数据时，它使用 256 位密钥的对称加密技术和 Galoas 计数器模式中的高级加密标准 (AES-GCM) 算法，该算法已具备抗量子性。理论上，在未来针对使用 256 位 AES-GCM 密钥创建的密文的大规模量子计算攻击中，密钥的有效安全性将会降至 128 位。此安全级别足以对抗对 AWS KMS 密文进行的暴力破解攻击。

支持的系统

目前，仅在 Linux 系统上支持使用 s2n-tls 中的混合密码套件。此外，这些密码套件仅在支持 AWS 公共运行时的开发工具包中受支持，例如 AWS SDK for Java 2.x。有关示例，请参阅如何配置混合后量子 TLS。

AWS KMS 终端节点

在使用混合密码套件时，请使用标准 AWS KMS 终端节点。s2n-tls 中的混合密码套件与适用于 AWS KMS 的通过 FIPS 140-2 验证的端点不兼容。

在使用 s2n-tls 配置 HTTP 客户端以优先使用后量子 TLS 连接时，后量子密码将位于密码优先列表的首位。但是，在优先列表中，传统非混合密码处于较低的优先顺序，以便实现兼容性。使用 AWS KMS 通过 FIPS 140-2 验证的端点配置 HTTP 客户端，以优先使用后量子 TLS 连接时，s2n-tls 将协商使用传统的非混合密钥交换密码。

有关每个 AWS 区域 中 AWS KMS 端点的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Key Management Service endpoints and quotas。有关 FIPS 端点的信息，请参阅《Amazon Web Services 一般参考》中的 FIPS endpoints。

预期性能

我们在早期开展的基准测试表明，s2n-tls 中的混合密码套件比传统 TLS 密码套件的速度更慢。根据网络配置文件、CPU 速度、内核数量和调度速率的不同，效果也不尽相同。有关性能测试的结果，请参阅如何使用 Kyber 调整 TLS 以实现混合后量子加密。

如何配置混合后量子 TLS

在此过程中，为 AWS 公共运行时 HTTP 客户端添加一个 Maven 依赖项。然后配置一个优先使用后量子 TLS 的 HTTP 客户端。然后，创建使用 HTTP 客户端的 AWS KMS 客户端。

要查看演示混合后量子 TLS 与 AWS KMS 结合使用的配置过程以及具体使用方法的完整工作示例，请参阅 aws-kms-pq-tls-example 存储库。

> **Note**
>
> AWS 公共运行时 HTTP 客户端现已开放预览版，并于 2023 年 2 月全面开放。在正式发行版中，`tlsCipherPreference` 类和 `tlsCipherPreference()` 方法参数已替换为 `postQuantumTlsEnabled()` 方法参数替。如果您在预览期间使用此示例，则需要更新您的代码。

1. 将 AWS 公共运行时客户端添加到您的 Maven 依赖项中。我们建议您使用最新可用版本。

   例如，以下语句将 AWS 公共运行时客户端的版本 `2.20.0` 添加到您的 Maven 依赖项中。

   ```
   <dependency>
       <groupId>software.amazon.awssdk</groupId>
       <artifactId>aws-crt-client</artifactId>
       <version>2.20.0</version>
   </dependency>
   ```

2. 要启用混合后量子密码套件，请将 AWS SDK for Java 2.x 添加到您的项目中并进行初始化。然后按照以下示例所示，在您的 HTTP 客户端上启用混合后量子密码套件。

   此代码使用 `postQuantumTlsEnabled()` 方法参数配置 AWS 公告运行时 HTTP 客户端，以优先使用推荐的混合后量子密码套件（即 ECDH 与 Kyber）。然后使用配置的 HTTP 客户端来构建一个 AWS KMS 异步客户端实例（即 `KmsAsyncClient`）。此代码完成后，`KmsAsyncClient` 实例上的所有 AWS KMS API 请求都将使用混合后量子 TLS。

   ```
   // Configure HTTP client
   ```

```
SdkAsyncHttpClient awsCrtHttpClient = AwsCrtAsyncHttpClient.builder()
          .postQuantumTlsEnabled(true)
          .build();

// Create the AWS KMS async client
KmsAsyncClient kmsAsync = KmsAsyncClient.builder()
         .httpClient(awsCrtHttpClient)
         .build();
```

3. 使用后量子 TLS 测试您的 AWS KMS 调用。

   在配置的 AWS KMS 客户端上调用 AWS KMS API 操作时，会使用混合后量子 TLS 将您的调用传输到 AWS KMS 终端节点。要测试您的配置，您需要调用一个 AWS KMS API，例如 `ListKeys`。

   ```
   ListKeysReponse keys = kmsAsync.listKeys().get();
   ```

针对 AWS KMS 测试混合后量子 TLS

请考虑在调用 AWS KMS 的应用程序上，使用混合密码套件运行下面的测试。

- 运行负载测试和基准测试。混合密码套件的执行方式与传统密钥交换算法有所不同。您可能需要调整连接超时，以便增加握手时间。如果您在 AWS Lambda 函数内部运行，请增大执行超时设置。
- 请尝试从不同位置进行连接。根据您的请求采用的网络路径，您可能会发现中间主机、代理或带有深度数据包检查 (DPI) 功能的防火墙阻止了请求。这可能是由于在 TLS 握手ClientHello部分使用了新的密码套件，或者是较大的密钥交换消息所致。如果您在解决这些问题时遇到麻烦，请与安全团队或 IT 管理员一起，更新相关配置并取消阻止新的 TLS 密码套件。

了解有关 AWS KMS 中的后量子 TLS 的更多信息

有关在 AWS KMS 中使用混合后量子 TLS 的更多信息，请参阅以下资源。

- 要了解 AWS 的后量子密码学，包括博客文章和研究论文的链接，请参阅 后量子密码学。
- 有关 s2n-tls 的信息，请参阅推出新的开源 TLS 实施 s2n-tls 和使用 s2n-tls。
- 有关 AWS 公共运行时 HTTP 客户端的信息，请参阅《AWS SDK for Java 2.x 开发者指南》中的 配置基于 AWS CRT 的 HTTP 客户端。
- 有关美国国家标准和技术研究所 (NIST) 开展的后量子密码加密技术项目的信息，请参阅后量子密码加密技术。

- 有关 NIST 后量子密码标准化的信息，请参阅 后量子密码标准化。

确定对 AWS KMS keys 的访问权限

要确定当前有权访问 AWS KMS key 的所有对象，您必须检查 KMS 密钥的密钥策略、应用于 KMS 密钥的所有授权，以及所有潜在 AWS Identity and Access Management (IAM) 策略。您可以执行该操作来确定 KMS 密钥的潜在使用范围或帮助您满足合规性或审计要求。以下主题有助于您生成当前有权访问 KMS 密钥的 AWS 委托人（身份）的完整列表。

主题

检查密钥策略

密钥策略是控制对 KMS 密钥访问的主要方法。每个 KMS 密钥都有且只有一个密钥策略。

如果密钥策略由默认密钥策略组成或包含默认密钥策略，则密钥策略允许账户中的 IAM 管理员使用 IAM policy 控制对 KMS 密钥的访问。此外，如果密钥策略赋予其他 AWS 账户 使用 KMS 密钥的权限，则外部账户中的 IAM 管理员可以使用 IAM policy 委派这些权限。要确定可访问 KMS 密钥的委托人的完整列表，请检查 IAM policy。

要查看AWS KMS客户托管密钥或您账户AWS 托管式密钥中的密钥政策，请在 AWS KMS API 中使用AWS Management Console或GetKeyPolicy操作。要查看密钥策略，必须对 KMS 密钥具备 `kms:GetKeyPolicy` 权限。有关查看 KMS 密钥的密钥策略的说明，请参阅 the section called “查看密钥策略”。

检查密钥策略文档，并记下每个策略语句的 `Principal` 元素中指定的所有委托人。在具有 `Allow` 后果的策略语句中，`Principal` 元素中的 IAM 用户、IAM 角色 和 AWS 账户将拥有对此 KMS 密钥的访问权限。

> **Note**
>
> 除非您使用条件限制密钥政策，否则不要在允许权限的任何密钥政策语句将主体设置为星号（*）。星号表示允许每个 AWS 账户 权限中的每个身份使用 KMS 密钥，除非另一个策略语句

明确拒绝它。其他 AWS 账户 中的用户只要在自己的账户中拥有相应的权限，就可以使用您的 KMS 密钥。

以下示例使用默认密钥策略中的策略语句来演示如何执行该操作。

Example 策略语句 1

```
{
  "Sid": "Enable IAM User Permissions",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
  "Action": "kms:*",
  "Resource": "*"
}
```

在策略语句 1 中，arn:aws:iam::111122223333:root 是指向 AWS 账户 111122223333 的 AWS 账户主体。（这不是账户的根用户。）默认情况下，当您使用 AWS Management Console创建新的 KMS 密钥，或以编程方式创建新的 KMS 密钥但未提供密钥策略时，密钥策略文档中将包含与此类似的策略语句。

如果密钥策略文档中具有允许访问 AWS 账户的语句，则将使该账户中的 IAM policy 允许访问 KMS 密钥。这意味着，即使账户中的用户和角色未在密钥策略文档中显式列为主体，也可以访问 KMS 密钥。请务必检查所有列为委托人的 AWS 账户 中的所有 IAM policy，以确定它们是否允许访问此 KMS 密钥。

Example 策略语句 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": "*"
}
```

在政策声明 2 中，arn:aws:iam::111122223333:role/KMSKeyAdmins提及 AWS 账户 111122223333 KeyAdmins 中名为 KMS 的 IAM 角色。被授权代入该角色的用户被允许执行策略语句中列出的操作，即用于管理 KMS 密钥的管理操作。

Example 策略语句 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": "*"
}
```

在政策声明 3 中，arn:aws:iam::111122223333:role/EncryptionApp指的是在 AWS 账户 111122223333 EncryptionApp 中命名的 IAM 角色。被授权代入此角色的主体被允许执行策略语句中列出的操作，这包括对称加密 KMS 密钥的 加密操作。

Example 策略语句 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}}
}
```

在政策声明 4 中，`arn:aws:iam::111122223333:role/EncryptionApp`指的是在 AWS 账户 111122223333 EncryptionApp 中命名的 IAM 角色。被授权代入此角色的主体被允许执行策略语句中列出的操作。向大多数与 AWS KMS 集成的 AWS 服务（特别是使用授权的服务）委托 KMS 密钥使用权限时，都将需要将这些操作以及示例策略语句 3 中允许的操作结合使用。`Condition`元素中的 kms:GrantIsFor AWSResource 值可确保只有当委托是与授权集成AWS KMS并使用授权进行授权的AWS服务时，才允许委托。

要了解可以在密钥策略文档中指定委托人的所有不同方法，请参阅 IAM 用户指南中的指定委托人。

要了解有关 AWS KMS 密钥策略的更多信息，请参阅中的关键政策 AWS KMS。

检查 IAM policy

除密钥策略和授权外，您还可以使用 IAM policy 来允许对 KMS 密钥的访问。有关 IAM policy 和密钥策略如何协同工作的更多信息，请参阅 密钥访问故障排除。

要确定当前可通过 IAM policy 访问 KMS 密钥的委托人，可以使用基于浏览器的 IAM policy simulator 工具，也可以向 IAM API 发出请求。

检查 IAM policy 的方法

- 使用 IAM policy simulator 检查 IAM policy
- 使用 IAM API 检查 IAM policy

使用 IAM policy simulator 检查 IAM policy

IAM policy simulator 有助于您了解哪些委托人可以通过 IAM policy 访问 KMS 密钥。

使用 IAM policy simulator 确定对 KMS 密钥的访问权限

1. 登录 AWS Management Console，然后打开位于 https://policysim.aws.amazon.com/ 的 IAM policy simulator。
2. 在用户、组和角色窗格中，选择您要模拟其策略的用户、组或角色。
3. (可选) 清除您要从模拟中忽略的任何策略旁边的复选框。要模拟所有策略，则将所有策略保持选中状态。

4. 在策略模拟器窗格中，执行以下操作：

   a. 对于选择服务，请选择 Key Management Service。

   b. 要模拟特定 AWS KMS 操作，请针对选择操作选择要模拟的操作。要模拟所有 AWS KMS 操作，请选择全选。

5. （可选）默认情况下，策略模拟器会模拟对所有 KMS 密钥的访问。要模拟对特定 KMS 密钥的访问，请选择 Simulation Settings（模拟设置），然后键入要模拟的 KMS 密钥的 Amazon Resource Name (ARN)。

6. 选择 Run Simulation (运行模拟)。

您可以在结果部分查看模拟的结果。对 AWS 账户 中的每个用户、组和角色重复第 2 至 6 步。

使用 IAM API 检查 IAM policy

您可以使用 IAM API 以编程方式检查 IAM policy。以下步骤提供了如何执行该操作的一般概述：

1. 对于密钥策略中AWS 账户列为委托人的每个用户（即按以下格式指定的每个AWS账户委托人：`"Principal": {"AWS": "arn:aws:iam::111122223333:root"}`），使用 IAM API 中的ListUsers和ListRoles操作获取账户中的所有用户和角色。
2. 对于列表中的每个用户和角色，使用 IAM API 中的SimulatePrincipalPolicy操作，传入以下参数：
   - 对于 `PolicySourceArn`，指定列表中用户或角色的 Amazon Resource Name (ARN)。您只能为每个 `SimulatePrincipalPolicy` 请求指定一个 `PolicySourceArn`，因此必须多次调用此操作，针对列表中的每个用户和角色分别调用一次。
   - 对于 `ActionNames` 列表，指定要模拟的每个 AWS KMS API 操作。要模拟所有 AWS KMS API 操作，请使用 `kms:*`。要测试单独的 AWS KMS API 操作，请在每个 API 操作之前添加“`kms:`”，例如“`kms:ListKeys`”。有关 AWS KMS API 操作的完整列表，请参阅《AWS Key Management Service API 参考》中的 操作。
   - （可选）要确定用户或角色是否有权访问特定的 KMS 密钥，请使用 `ResourceArns` 参数指定 KMS 密钥的 Amazon 资源名称（ARN）列表。要确定用户或角色是否有权访问任何 KMS 密钥，请忽略 `ResourceArns` 参数。

IAM 通过以下评估决策来响应每个 `SimulatePrincipalPolicy` 请求：`allowed`、`explicitDeny` 或 `implicitDeny`。对于每个包含评估决策 `allowed` 的响应，其中包含允许的特定 AWS KMS API 操作的名称。它还包括评估中使用的 KMS 密钥的 ARN（如果有）。

检查授予

授权是一种高级机制，用于指定您或与 AWS KMS 集成的 AWS 服务可用于指定使用 KMS 密钥的方式和时间的权限。授权将附加到 KMS 密钥，每个授权都包含一位委托人，此委托人可获得使用 KMS 密钥和所允许的操作列表的权限。授权是密钥策略的替代方案，对特定的使用案例很有用。有关更多信息，请参阅 AWS KMS 中的授权。

要获取 KMS 密钥的授权列表，请使用AWS KMSListGrants操作。您可以检查 KMS 密钥的授权来确定当前有权通过这些授权使用 KMS 密钥的对象。例如，下面是某个授权的 JSON 表示形式，此授权使用中的 list-grantsAWS CLI 命令获取。

```
{"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"}}
}]}
```

要了解有权使用 KMS 密钥的对象，可查找 "GranteePrincipal" 元素。在上述示例中，被授权委托人是与 EC2 实例 i-5d476fab 关联的假设用户角色。EC2 基础设施使用此角色将加密的 EBS 卷 vol-5cccfb4e 附加到此实例。在此情况下，EC2 基础设施角色有权使用 KMS 密钥，因为您之前创建了受此 KMS 密钥保护的加密的 EBS 卷。之后，您将此卷附加到了 EC2 实例。

下面是 JSON 表示形式的另一个授权示例，此授权使用 中的 list-grantsAWS CLI 命令获取。在以下示例中，被授权者委托人是另一个 AWS 账户。

```
{"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",
```

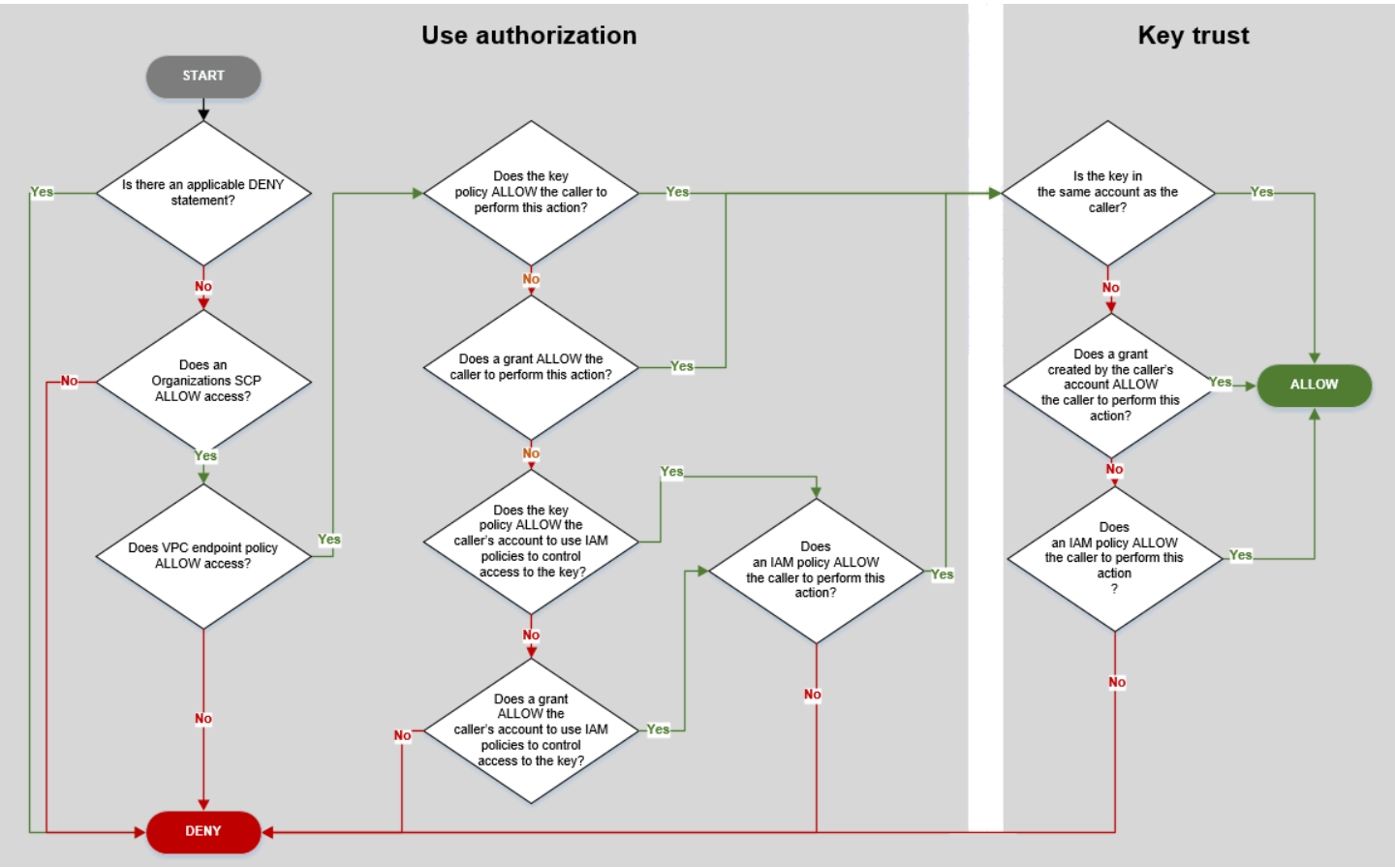
```
  "CreationDate": 1.444151269E9
}]}
```

密钥访问故障排除

在授予对 KMS 密钥的访问权限时，AWS KMS 将评估以下内容：

- 附加到 KMS 密钥的密钥策略。密钥策略始终在拥有 KMS 密钥的 AWS 账户 和区域中定义。
- 附加到发出请求的用户或角色的所有 IAM policy。管理委托人对 KMS 密钥的使用的 IAM policy 始终在委托人的 AWS 账户 中定义。
- 应用于 KMS 密钥的所有授权。
- 可能应用于请求以使用 KMS 密钥的其他类型的策略，例如 AWS Organizations 服务控制策略和 VPC 终端节点策略。这些策略是可选的，并且在默认情况下允许执行所有操作，但您可以使用它们限制授予委托人的权限。

AWS KMS 同时评估这些策略机制，以确定是允许还是拒绝对 KMS 密钥的访问。为执行此操作，AWS KMS 使用与以下流程图中所示流程相似的流程。以下流程图提供策略评估流程的可视化表示。



此流程图分为两个部分。这两个部分按顺序显示，但通常会同时对它们进行评估。

- 使用授权根据其密钥政策、IAM policy、授权和其他适用的策略来确定是否允许您使用 KMS 密钥。
- 密钥信任确定您是否应信任允许您使用的 KMS 密钥。一般而言，您信任 AWS 账户 中的资源。但是，如果您的账户中的授权或 IAM policy 允许您使用 KMS 密钥，您也可以自信地使用不同 AWS 账户 中的 KMS 密钥。

您可以使用此流程图了解为什么允许或拒绝向发起人授予使用 KMS 密钥的权限。您还可以使用它评估您的策略和授权。例如，此流程图显示某个调用方可能被显式 DENY 语句拒绝访问，或者由于在密钥政策、IAM policy 或授权中没有显式 ALLOW 语句而被拒绝访问。

流程图可以解释一些常见的许可方案。

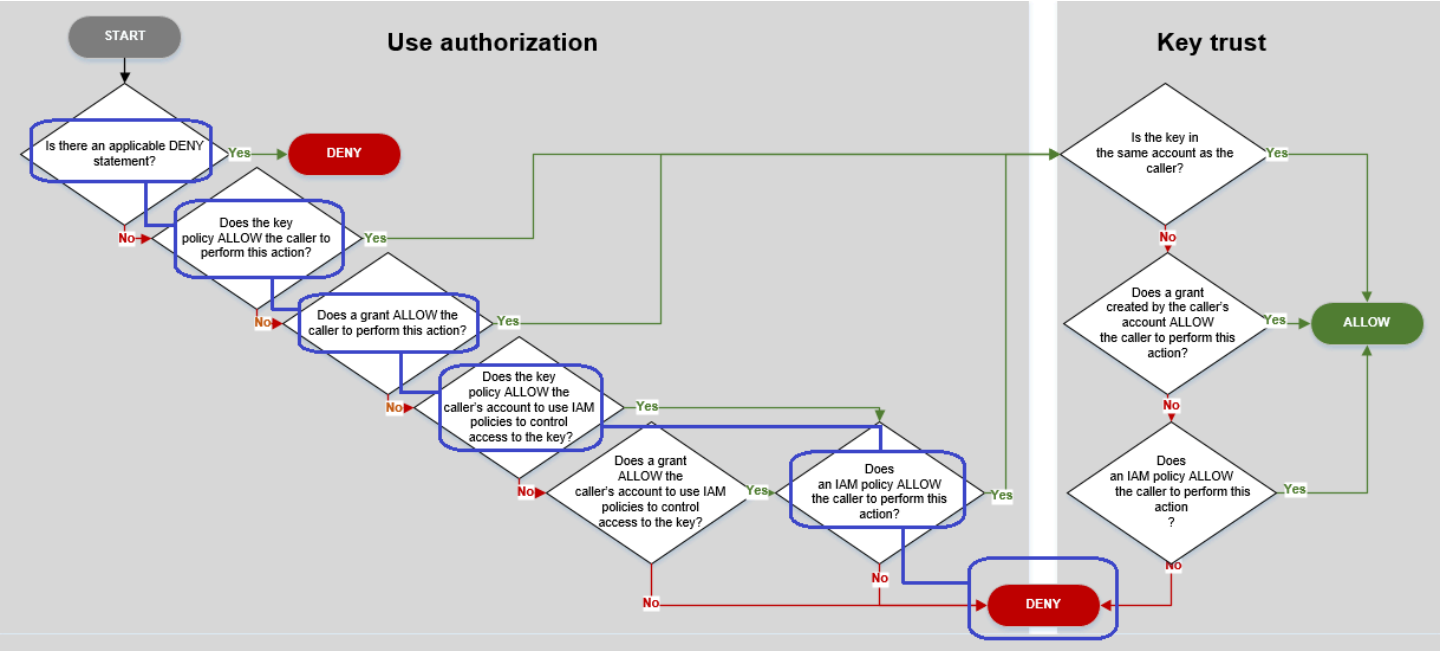
权限示例

- 示例 1：用户被拒绝访问其 AWS 账户 中的 KMS 密钥
- 示例 2：用户代入的角色具有使用不同 AWS 账户 中的 KMS 密钥的权限

示例 1：用户被拒绝访问其 AWS 账户 中的 KMS 密钥

Alice 是 111122223333 AWS 账户 中的 IAM 用户。她被拒绝访问同一 AWS 账户 中的 KMS 密钥。为什么 Alice 无法使用 KMS 密钥？

在这种情况下，Alice 被拒绝访问该 KMS 密钥，因为没有密钥政策、IAM policy 或为她授予所需权限的授权。KMS 密钥的密钥政策允许 AWS 账户 使用 IAM policy 控制对 KMS 密钥的访问，但任何 IAM policy 均未向 Alice 授予使用 KMS 密钥的权限。



考虑用于此示例的相关策略。

- Alice 想要使用的 KMS 密钥具有默认密钥策略。此政策允许拥有 KMS 密钥的 AWS 账户 使用 IAM policy 控制对 KMS 密钥的访问。此密钥政策满足流程图中的密钥政策是否允许调用方账户使用 IAM policy 来控制对密钥的访问？条件。

```
{
  "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" : "*"
  } ]
}
```

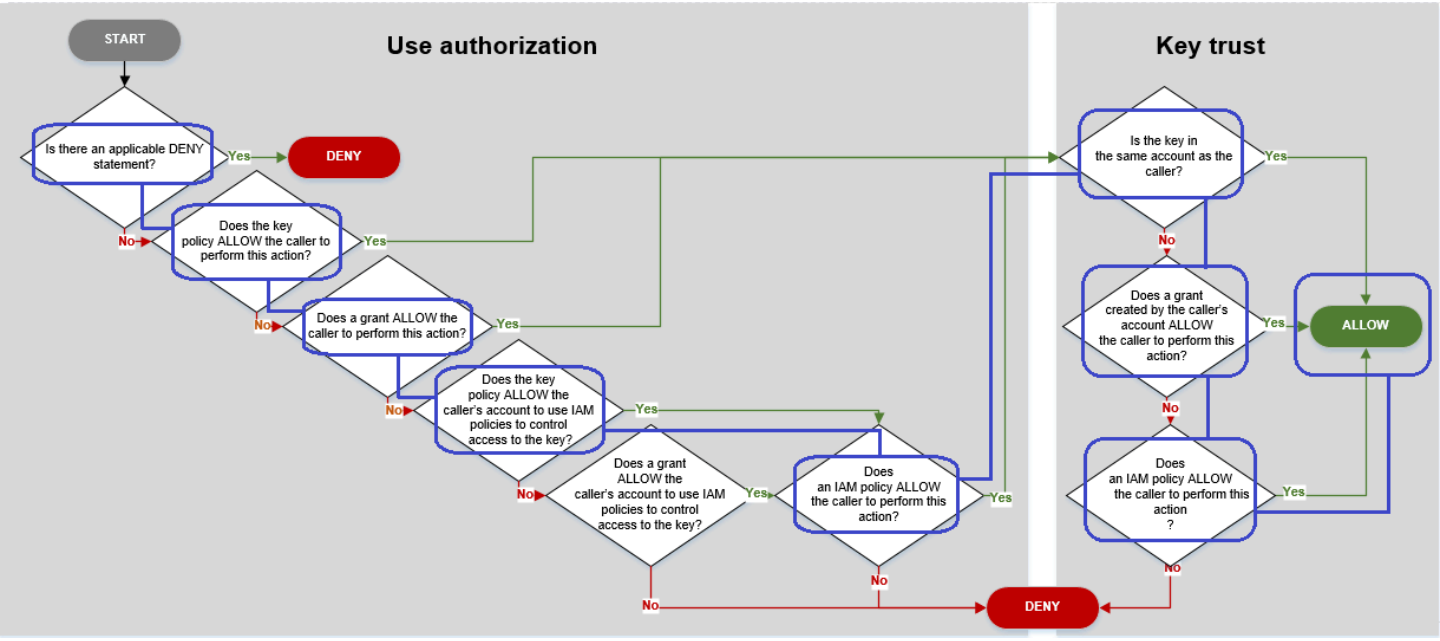
- 但是，没有任何密钥政策、IAM policy 或授权向 Alice 授予 KMS 密钥使用权限。因此，Alice 被拒绝使用 KMS 密钥的权限。

示例 2：用户代入的角色具有使用不同 AWS 账户 中的 KMS 密钥的权限

Bob 是账户 1 (111122223333) 中的一个用户。他可以在加密操作中使用账户 2 (444455556666) 中的 KMS 密钥。如何才能实现？

> **Tip**
>
> 在评估跨账户权限时，请记住，密钥策略在 KMS 密钥的账户中指定。IAM policy 在调用方账户中指定，即使调用方使用的是不同的账户。有关提供对 KMS 密钥的跨账户访问的详细信息，请参阅 允许其他账户中的用户使用 KMS 密钥。

- 账户 2 中 KMS 密钥的密钥政策允许账户 2 使用 IAM policy 来控制对 KMS 密钥的访问。
- 账户 2 中 KMS 密钥的密钥策略允许账户 1 在加密操作中使用 KMS 密钥。但是，账户 1 必须使用 IAM policy 授予其委托人对 KMS 密钥的访问权限。
- 账户 1 中的 IAM policy 允许 `Engineering` 角色将账户 2 中的 KMS 密钥用于加密操作。
- Bob 是账户 1 中的用户，有权限代入 `Engineering` 角色。
- Bob 可以信任此 KMS 密钥，因为即使它不在他的账户中，他账户中的一个 IAM policy 也会向他授予使用此 KMS 密钥的显式权限。



考虑一下 Bob（账户 1 中的用户）使用账户 2 中 KMS 密钥的策略。

- KMS 密钥的密钥政策允许账户 2（444455556666，拥有 KMS 密钥的账户）使用 IAM policy 来控制对 KMS 密钥的访问。此密钥策略还允许账户 1 (111122223333) 在加密操作中使用 KMS 密钥（在策略语句的 `Action` 元素中指定）。但是，账户 1 中的任何人都无法使用账户 2 中的 KMS 密钥，直到账户 1 定义授权委托人访问 KMS 密钥的 IAM policy。

  在流程图中，账户 2 中的此密钥政策满足密钥政策是否允许调用方账户使用 IAM policy 来控制对密钥的访问？条件。

```
{
    "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": "*"
        }
    ]
}
```

- 调用方的 AWS 账户（账户 1，111122223333）中的 IAM policy 委托人授予使用账户 2 (444455556666) 中的 KMS 密钥执行加密操作的权限。Action 元素向该委托人委派的权限与账户 2 中的密钥策略向账户 1 授予的权限相同。要将这些权限授予账户 1 中的 Engineering 角色，将此内联策略嵌入到 Engineering 角色中。

  仅当账户 2 中的 KMS 密钥的密钥政策向账户 1 授予使用此 KMS 密钥的权限时，类似于此策略的跨账户 IAM policy 才有效。此外，账户 1 只能向其委托人授予执行此密钥策略已授予该账户的操作的权限。

  在流程图中，这满足 IAM policy 是否允许调用方执行此操作？条件。

```
{
    "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"
            ]
        }
    ]
}
```

- 最后一个必需元素是账户 1 中 Engineering 角色的定义。此角色中的 AssumeRolePolicyDocument 允许 Bob 代入 Engineering 角色。

```
{
    "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 权限

此表旨在帮助您了解 AWS KMS 权限，以便您可以控制对 AWS KMS 资源的访问权限。表格下方会显示列标题的定义。

您还可以在服务授权参考 AWS Key Management Service主题的操作、资源和条件键中了解 AWS KMS 权限。但是，该主题并未列出可用于优化每个权限的所有条件键。

> **Note**
>
> 您可能需要水平或垂直滚动才能查看表中的所有数据。

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
CancelKeyDeletion kms:CancelKeyDeletion	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
				kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService
ConnectCustomKeyStore kms:ConnectCustomKeyStore	IAM policy	否	*	kms: CallerAccount

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
CreateAlias kms:CreateAlias 要使用此操作，调用方需要对以下两个资源具有 kms:CreateAlias 权限： • 别名（在 IAM policy 中） • KMS 密钥（在密钥策略中） 有关更多信息，请参阅 控制对别名的访问。	IAM policy（适用于别名） 密钥策略（适用于 KMS 密钥）	否	别名 KMS 密钥	无（控制对别名的访问时） KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService
CreateCustomKeyStore kms:CreateCustomKeyStore	IAM policy	否	*	kms: CallerAccount

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
CreateGrant kms:CreateGrant	密钥策略	是	KMS 密钥	加密上下文条件： kms:EncryptionContext:上下文密钥 kms: EncryptionContextKeys 授予条件： kms: GrantConstraintType kms: GranteePrincipal kms: GrantIsForAWSResource kms: GrantOperations kms: RetiringPrincipal KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
				a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService
CreateKey kms:CreateKey	IAM policy	否	*	kms: BypassPolicyLockoutSafetyCheck kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ViaService a@@ ws:RequestTag/tag-key（AWS 全局条件密钥） a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） a@@ ws:TagKeys（AWS 全局条件密钥）

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
Decrypt kms:Decrypt	密钥策略	是	KMS 密钥	加密操作的条件 kms: EncryptionAlgorithm kms: RequestAlias 加密上下文条件： kms:EncryptionContext: 上下文密钥 kms: EncryptionContextKeys KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
DeleteAlias kms:DeleteAlias	IAM policy（适用于别名）	否	别名	无（控制对别名的访问时）
要使用此操作，调用方需要对以下两个资源具有 kms:DeleteAlias 权限： • 别名（在 IAM policy 中） • KMS 密钥（在密钥策略中） 有关更多信息，请参阅 控制对别名的访问。	密钥策略（适用于 KMS 密钥）	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService
DeleteCustomKeyStore kms:DeleteCustomKeyStore	IAM policy	否	*	kms: CallerAccount

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
DeleteImportedKeyMaterial kms:DeleteImportedKeyMaterial	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService
DescribeCustomKeyStores kms:DescribeCustomKeyStores	IAM policy	否	*	kms: CallerAccount

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
DescribeKey kms:DescribeKey	密钥策略	是	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 其他条件： kms: RequestAlias

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
DisableKey kms:DisableKey	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
DisableKeyRotation kms:DisableKeyRotation	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService
DisconnectCustomKeyStore kms:DisconnectCustomKeyStore	IAM policy	否	*	kms: CallerAccount

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
EnableKey kms:EnableKey	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
EnableKeyRotation kms:EnableKeyRotation	密钥策略	否	KMS 密钥（仅限对称）	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 自动密钥轮换条件： kms: RotationPeriodInDays

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
Encrypt kms:Encrypt	密钥策略	是	KMS 密钥	加密操作的条件 kms: EncryptionAlgorithm kms: RequestAlias 加密上下文条件： kms:EncryptionContext: 上下文密钥 kms: EncryptionContextKeys KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
GenerateDataKey kms:GenerateDataKey	密钥策略	是	KMS 密钥（仅限对称）	加密操作的条件 kms: EncryptionAlgorithm kms: RequestAlias 加密上下文条件： kms:EncryptionContext: 上下文密钥 kms: EncryptionContextKeys KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
GenerateDataKeyPair kms:GenerateDataKeyPair	密钥策略	是	KMS 密钥（仅限对称） 生成受对称加密 KMS 密钥保护的非对称数据密钥对。	数据密钥对的条件： kms: DataKeyPairSpec 加密操作的条件 kms: EncryptionAlgorithm kms: RequestAlias 加密上下文条件： kms:EncryptionContext: 上下文密钥 kms: EncryptionContextKeys KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥）

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
				kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
GenerateDataKeyPairWithoutPlaintext kms:GenerateDataKeyPairWithoutPlaintext	密钥策略	是	KMS 密钥（仅限对称） 生成受对称加密 KMS 密钥保护的非对称数据密钥对。	数据密钥对的条件： kms: DataKeyPairSpec 加密操作的条件 kms: EncryptionAlgorithm kms: RequestAlias 加密上下文条件： kms:EncryptionContext: 上下文密钥 kms: EncryptionContextKeys KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥）

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
				kms: ViaService
GenerateDataKeyWithoutPlaintext kms:GenerateDataKeyWithoutPlaintext	密钥策略	是	KMS 密钥（仅限对称）	加密操作的条件 kms: EncryptionAlgorithm kms: RequestAlias 加密上下文条件： kms:EncryptionContext:上下文密钥 kms: EncryptionContextKeys KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
GenerateMac kms:GenerateMac	密钥策略	是	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 加密操作的条件： kms: MacAlgorithm kms: RequestAlias
GenerateRandom kms:GenerateRandom	IAM policy	不适用	*	无

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
GetKeyPolicy kms:GetKeyPolicy	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
GetKeyRotationStatus kms:GetKeyRotationStatus	密钥策略	是	KMS 密钥（仅限对称）	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
GetParametersForImport kms:GetParametersForImport	密钥策略	否	KMS 密钥	kms: WrappingAlgorithm kms: WrappingKeySpec KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
GetPublicKey kms:GetPublicKey	密钥策略	是	KMS 密钥（仅限非对称）	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 其他条件： kms: RequestAlias

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
ImportKeyMaterial kms:ImportKeyMaterial	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 其他条件： kms: ExpirationModel kms: ValidTo
ListAliases kms:ListAliases	IAM policy	否	*	无

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
ListGrants kms:ListGrants	密钥策略	是	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 其他条件： kms: GrantIsForAWSResource

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
ListKeyPolicies kms:ListKeyPolicies	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
ListKeyRotations kms:ListKeyRotations	密钥策略	否	KMS 密钥（仅限对称）	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService
ListKeys kms:ListKeys	IAM policy	否	*	无

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
ListResourceTags kms:ListResourceTags	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService
ListRetirableGrants kms:ListRetirableGrants	IAM policy	指定的委托人必须位于本地账户中，但操作将返回所有账户中的授权。	*	无

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
PutKeyPolicy kms:PutKeyPolicy	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 其他条件： kms: BypassPolicyLockoutSafetyCheck

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
ReEncrypt kms:ReEncryptFrom kms:ReEncryptTo 要使用此操作，调用方需要对以下两个 KMS 密钥具有权限： • KMS 密钥上的 kms:ReEncryptFrom ，用于解密 • KMS 密钥上的 kms:ReEncryptTo ，用于加密	密钥策略	是	KMS 密钥	加密操作的条件 kms: EncryptionAlgorithm kms: RequestAlias 加密上下文条件： kms:EncryptionContext: 上下文密钥 kms: EncryptionContextKeys KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 其他条件：

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
				kms: ReEncryptOnSameKey
ReplicateKey kms:ReplicateKey 要使用此操作，调用方需要具有以下权限： • 多区域主键上的 kms:ReplicateKey • 副本区域中的 IAM policy 中的 kms:CreateKey	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 其他条件： kms: ReplicaRegion

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
RetireGrant kms:RetireGrant 撤销授予的权限主要由授予决定。单独的策略无法允许访问此操作。有关更多信息，请参阅 停用和撤销授权。	IAM policy （此权限在密钥策略中无效。）	是	KMS 密钥	kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥）
RevokeGrant kms:RevokeGrant	密钥策略	是	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 其他条件： kms: GrantIsForAWSResource

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
RotateKeyOnDemand kms:RotateKeyOnDemand	密钥策略	否	KMS 密钥（仅限对称）	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
ScheduleKeyDeletion kms:ScheduleKeyDeletion	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
Sign kms:Sign	密钥策略	是	KMS 密钥（仅限非对称）	签名和验证条件： kms: MessageType kms: RequestAlias kms: SigningAlgorithm KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
TagResource kms:TagResource	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 标记条件： a@@ ws:RequestTag/tag-key（AWS 全局条件密钥） a@@ ws:TagKeys（AWS 全局条件密钥）

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
UntagResource kms:UntagResource	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 标记条件： a@@ ws:RequestTag/tag-key（AWS 全局条件密钥） a@@ ws:TagKeys（AWS 全局条件密钥）

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
UpdateAlias kms:UpdateAlias	IAM policy（适用于别名）	否	别名	无（控制对别名的访问时）
要使用此操作，调用方需要对以下三个资源具有 kms:UpdateAlias 权限： • 别名 • 当前关联的 KMS 密钥 • 新关联的 KMS 密钥 有关更多信息，请参阅 控制对别名的访问。	密钥策略（适用于 KMS 密钥）	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService
UpdateCustomKeyStore kms:UpdateCustomKeyStore	IAM policy	否	*	kms: CallerAccount

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
UpdateKeyDescription kms:UpdateKeyDescription	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
UpdatePrimaryRegion kms:UpdatePrimaryRegion 要使用此操作，调用方需要对将成为副本密钥的多区域主键和将成为主键的多区域副本密钥同时具有 kms:UpdatePrimaryRegion 权限。	密钥策略	否	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 其他条件 kms: PrimaryRegion

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
验证 kms:Verify	密钥策略	是	KMS 密钥（仅限非对称）	签名和验证条件： kms: MessageType kms: RequestAlias kms: SigningAlgorithm KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService

操作和权限	策略类型	跨账户使用	资源（适用于 IAM policy）	AWS KMS 条件键
VerifyMac kms:VerifyMac	密钥策略	是	KMS 密钥	KMS 密钥操作的条件： kms: CallerAccount kms: KeySpec kms: KeyUsage kms: KeyOrigin kms: MultiRegion kms: MultiRegionKeyType kms: ResourceAliases a@@ ws:ResourceTag/tag-key（AWS 全局条件密钥） kms: ViaService 加密操作的条件： kms: MacAlgorithm kms: RequestAlias

列描述

此表中的各列提供以下信息：

- 操作和权限列出了每个 AWS KMS API 操作以及允许该操作的权限。您可以在策略语句的 Action 元素中指定操作。
- 策略类型指示权限是否可在密钥策略或 IAM policy 中使用。

密钥策略意味着您可以在密钥策略中指定权限。当密钥政策包含启用 IAM policy 的策略语句时，您可以在 IAM policy 中指定权限。

IAM policy 意味着您只能在 IAM policy 中指定权限。

- 跨账户使用显示了授权用户可以对其他 AWS 账户中的资源执行的操作。

  值 Yes（是）表示委托人可以对其他 AWS 账户中的资源执行操作。

  值 No（否）表示委托人只能对其自己的 AWS 账户中的资源执行操作。

  如果您为不同账户中的委托人授予一个不能在跨账户资源上使用的权限，则该权限将无效。例如，如果您向其他账户中的委托人授予对您账户中 K MS 密钥的TagResource权限，则他们尝试在您的账户中标记 KMS 密钥将失败。

- 资源列出了权限适用的 AWS KMS 资源。 AWS KMS 支持两种资源类型：KMS 密钥和别名。在密钥策略中，`Resource` 元素的值始终为 `*`，这表示密钥策略附加到的 KMS 密钥。

  使用以下值表示 IAM 策略中的 AWS KMS 资源。

  KMS 密钥

  当资源是 KMS 密钥时，请使用其密钥 ARN。有关帮助信息，请参阅 the section called “查找密钥 ID 和密钥 ARN”。

  `arn:`*`AWS_partition_name`*`:kms:`*`AWS_Region`*`:`*`AWS_account_ID`*`:key/`*`key_ID`*

  例如：

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

  别名

  当资源是别名时，请使用其别名 ARN。有关帮助信息，请参阅 the section called “查找别名和别名 ARN”。

  `arn:`*`AWS_partition_name`*`:kms:`*`AWS_region`*`:`*`AWS_account_ID`*`:alias/`*`alias_name`*

  例如：

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

***（星号）**

当权限不适用于特定资源（KMS 密钥或别名）时，请使用星号 (*)。

在 IAM AWS KMS 权限策略中，`Resource`元素中的星号表示所有 AWS KMS 资源（KMS 密钥和别名）。当 AWS KMS 权限不适用于任何特定的 KMS 密钥或别名时，您也可以在`Resource`元素中使用星号。例如，当允许或拒绝 `kms:CreateKey` 或 `kms:ListKeys` 权限时，您可以将 `Resource` 元素设置为 `*`，也可以设置为账户特定的变体，例如 `arn:`*`AWS_partition_name`*`:kms:`*`AWS_region`*`:`*`AWS_account_ID`*`:*`。

- AWS KMS 条件键列出了可用于控制对操作的访问的 AWS KMS 条件键。您可以在策略的 `Condition` 元素中指定条件。有关更多信息，请参阅 AWS KMS 条件键。此列还包括所有服务都支持但并非所有 AWS 服务都支持的AWSAWS KMS全局条件键。

测试您的权限

要使用 AWS KMS，您必须拥有 AWS 可以用来验证您的 API 请求的凭证。此凭证必须包括访问 KMS 密钥和别名的权限。权限由密钥政策、IAM policy、授权和跨账户存取控制决定。除了控制对 KMS 密钥的访问外，您还可以控制对 CloudHSM 和自定义密钥存储的访问权限。

您可以指定 `DryRun` API 参数来确认您具有使用 AWS KMS 密钥的所需权限。您还可以使用 `DryRun` 来验证 AWS KMS API 调用中的请求参数指定是否正确。

主题

- DryRun 参数是什么？
- 使用 API DryRun 进行指定

DryRun 参数是什么？

`DryRun` 是一个可选的 API 参数，您可以指定该参数来验证 AWS KMS API 调用是否成功。在实际调用 AWS KMS 之前，请使用 `DryRun` 测试您的 API 调用。您可以验证如下内容。

- 您具有使用 AWS KMS 密钥的所需权限。
- 您已正确指定调用中的参数。

AWS KMS 支持在某些 API 操作中使用 `DryRun` 参数：

- CreateGrant

- Decrypt
- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac
- ReEncrypt
- RetireGrant
- RevokeGrant
- Sign
- 验证
- VerifyMac

使用 DryRun 参数将产生费用，并将按标准 API 请求计费。有关 AWS KMS 定价的更多信息，请参阅 AWS Key Management Service 定价。

使用 DryRun 参数的所有 API 请求都适用于 API 的请求限额，如果您超过 API 请求限额，则可能会导致节流异常。例如，无论使用 DryRun 还是不使用 DryRun 调用 Decrypt，都将计入相同的加密操作限额。请参阅限制请求 AWS KMS，了解更多信息。

对 AWS KMS API 操作的每次调用都被捕获为事件并记录在 AWS CloudTrail 日志中。任何指定DryRun参数的操作的输出都会出现在您的 CloudTrail 日志中。有关更多信息，请参阅 使用记录 AWS KMS API 调用 AWS CloudTrail。

使用 API DryRun 进行指定

要使用 DryRun，请在支持该参数的 AWS CLI 命令和 AWS KMS API 调用中指定 –dry-run 参数。当您这样做时，AWS KMS 将验证您的调用是否会成功。使用 DryRun 的 AWS KMS 调用将始终失败并返回一条消息，其中包含有关调用失败原因的信息。消息可能包括以下例外情况：

- DryRunOperationException - 如果 DryRun 未指定，则请求会成功。
- ValidationException - 请求因指定错误的 API 参数而失败。
- AccessDeniedException - 您无权在 KMS 资源上执行指定的 API 操作。

例如，以下命令使用该CreateGrant操作并创建授权，允许有权担任该keyUserRole角色的用户对指定的对称 KMS 密钥调用 Decry pt 操作。DryRun 参数已指定。

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --dry-run
```

特殊用途密钥

AWS Key Management Service (AWS KMS) 支持不同用途的多种不同类型密钥。

创建 AWS KMS key时，默认情况下您将获得对称加密 KMS 密钥。在 AWS KMS 中，对称加密 KMS 密钥表示用来加密和解密的 256 位 AES-GCM 密钥，但在中国区域，它表示使用 SM4 加密的 128 位对称密钥。对称密钥材料绝不会让 AWS KMS 处于未加密状态。除非任务明确要求使用非对称加密或 HMAC 密钥，否则对称加密 KMS 密钥（永远不会让 AWS KMS 处于未加密状态）是个不错的选择。此外，与 AWS KMS 集成的 AWS 服务仅使用对称加密 KMS 密钥加密您的数据。这些服务不支持使用非对称 KMS 密钥进行加密。

在 AWS KMS 中，可以使用对称加密 KMS 密钥加密、解密和重新加密数据，生成数据密钥和数据密钥对，并生成随机字节字符串。您可以将自己的密钥材料导入对称加密 KMS 密钥中，并在自定义密钥存储中创建对称加密 KMS 密钥。有关可以对对称 KMS 密钥和非对称 KMS 密钥执行的操作的比较表格，请参阅 密钥类型引用。

AWS KMS 也支持以下特殊用途的 KMS 密钥类型：

- 用于公有密钥加密的非对称 RSA 密钥
- 用于签名和验证的非对称 RSA 和 ECC 密钥
- 非对称 SM2 密钥（仅限中国区域）用于公有密钥加密或签名和验证
- 用于生成和验证散列消息认证码的 HMAC 密钥
- 多区域密钥（对称和非对称）的工作方式与不同 AWS 区域 中相同密钥的副本一样
- 具有您所提供导入密钥材料的密钥
- 由 AWS CloudHSM 集群或 AWS 外部的外部密钥管理器支持的自定义密钥存储中的密钥。

选择一种 KMS 密钥类型

AWS KMS 支持多种类型的 KMS 密钥：对称加密密钥、对称 HMAC 密钥、非对称加密密钥和非对称签名密钥。

KMS 密钥不同，因为它们包含不同的加密密钥材料。

- 对称加密 KMS 密钥：表示单个 256 位 AES-GCM 加密密钥，但在中国区域，它表示 128 位 SM4 加密密钥。对称密钥材料绝不会让 AWS KMS 处于未加密状态。要使用对称加密 KMS 密钥，必须调用 AWS KMS。

对称加密密钥是默认的 KMS 密钥，是大多数用途的理想选择。如果您需要 KMS 密钥来保护 AWS 服务 中的数据，除非指示您使用其他类型的密钥，否则请使用对称加密密钥。

- 非对称 KMS 密钥：表示为数学上相关的公有密钥和私有密钥对，可用于加密和解密或签名和验证，但不能同时用于二者。私有密钥永远不会让 AWS KMS 处于未加密状态。您可以通过调用 AWS KMS API 操作在 AWS KMS 内使用公有密钥，或下载公有密钥并在 AWS KMS 外部使用该密钥。
- HMAC KMS 密钥（对称）：表示长度不同的对称密钥，用于生成和验证散列消息认证码。HMAC KMS 密钥中的密钥材料绝不会让 AWS KMS 处于未加密状态。要使用 HMAC KMS 密钥，您必须调用 AWS KMS。

创建的 KMS 密钥类型在很大程度上取决于计划使用 KMS 密钥的方式，以及安全要求和授权要求。创建 KMS 密钥时，请记住，KMS 密钥的加密配置（包括其密钥规范和密钥用法）是在创建 KMS 密钥时建立的，无法更改。

请根据使用案例，遵照以下指南确定所需的 KMS 密钥类型。

加密和解密数据

对于需要加密和解密数据的大多数使用案例，使用对称 KMS 密钥。AWS KMS 使用的对称加密算法快速、高效，并可确保数据的机密性和真实性。它支持具有附加身份验证数据 (AAD) 的身份验证加密，这些数据定义为加密上下文。此 KMS 密钥类型要求加密数据的发送人和接收人都具备有效的 AWS 凭证才能调用 AWS KMS。

如果使用案例需要无法调用 AWS KMS 的用户在 AWS 外部进行加密，那么非对称 KMS 密钥是个不错的选择。您可以分发非对称 KMS 密钥的公有密钥，以允许这些用户对数据进行加密。需要解密该数据的应用程序，可以在 AWS KMS 内部使用非对称 KMS 密钥的私有密钥。

签署消息并验证签名

要签署消息并验证签名，必须使用非对称 KMS 密钥。您可以将 KMS 密钥与表示 RSA 密钥对、椭圆曲线（ECC）密钥对或 SM2 密钥对的密钥规范一起使用（仅限中国区域）。选择哪种密钥规范由想要使用的签名算法决定。推荐使用 ECC 密钥对支持的 ECDSA 签名算法，而不是 RSA 签名算法。不过，您可能需要使用特定的密钥规范和签名算法来支持在 AWS 之外验证签名的用户。

执行公有密钥加密

要执行公有密钥加密，必须将非对称 KMS 密钥与 RSA 密钥规范或 SM2 密钥规范一起使用（仅限中国区域）。要使用 KMS 密钥对的公有密钥为 AWS KMS 中的数据进行加密，请使用 Encrypt 操作。还可以下载公有密钥，并与需要在 AWS KMS 外部加密数据的各方共享。

下载非对称 KMS 密钥的公有密钥后，可以在 AWS KMS 外部使用该密钥。但它不再受 AWS KMS 中保护 KMS 密钥的安全控制的约束。例如，不能使用 AWS KMS 密钥策略或授权来控制公有密钥的使用。也不能使用 AWS KMS 支持的加密算法来控制密钥是否仅用于加密和解密。有关更多详细信息，请参阅下载公有密钥的特殊注意事项。

要对在 AWS KMS 外部采用公有密钥加密的数据进行解密，请调用 Decrypt 操作。如果使用 `SIGN_VERIFY` 的密钥用法通过 KMS 密钥中的公有密钥对数据进行加密，则 `Decrypt` 操作会失败。如果数据采用 AWS KMS 不支持用于选定密钥规范对密钥的算法进行加密，则此操作也将失败。有关密钥规范和支持算法的更多信息，请参阅非对称密钥规范。

为避免上述错误，在 AWS KMS 外部使用公有密钥的任何人都必须存储密钥配置。AWS KMS控制台和GetPublicKey响应提供了共享公钥时必须包含的信息。

生成并验证 HMAC 代码

要生成和验证散列消息认证码，请使用 HMAC 密钥。当您在 AWS KMS 中创建 HMAC 密钥时、AWS KMS 创建和保护您的密钥材料，并确保您对密钥使用正确的 MAC 算法。HMAC 代码也可以用作伪随机数，在某些情况下用于对称签名和令牌化。

HMAC KMS 密钥是对称密钥。在 AWS KMS 控制台中创建 HMAC KMS 密钥时，选择 `Symmetric` 密钥类型。

与 AWS 服务结合使用

要创建一个 KMS 密钥，以便用于集成到 AWS KMS 的 AWS 服务，请参阅该服务的文档。加密数据的 AWS 服务需要对称加密 KMS 密钥。

除上述注意事项外，KMS 密钥加密操作的密钥规范不同，其价格和请求限额也不同。有关 AWS KMS 定价的信息，请参阅 AWS Key Management Service 定价。有关请求配额的信息，请参阅 请求配额。

选择密钥用法

KMS 密钥的密钥用法 决定了 KMS 密钥是用于加密和解密、签名和验证签名，还是生成和验证 HMAC 标签。每个 KMS 密钥只有一个密钥用法。将 KMS 密钥用于多种操作类型，会使所有操作的产物更容易受到攻击。

如下表所示，对称加密 KMS 密钥只能用于加密和解密。HMAC KMS 密钥只能用于生成和验证 HMAC 代码。椭圆曲线 (ECC) KMS 密钥只能用于签名和验证。您需要仅为 RSA KMS 密钥作出密钥用法决策。

KMS 密钥类型的有效密钥用法

KMS 密钥类型	加密和解密 ENCRYPT_DECRYPT	签名和验证 SIGN_VERIFY	生成并验证 MAC GENERATE_VERIFY_MAC
对称加密 KMS 密钥	✓	⊗	⊗
HMAC KMS 密钥（对称）	⊗	⊗	✓
具有 RSA 密钥对的非对称 KMS 密钥	✓	✓	⊗
具有 ECC 密钥对的非对称 KMS 密钥	⊗	✓	⊗
具有 SM2 密钥对的非对称 KMS 密钥（仅限中国区域）	✓	✓	⊗

在 AWS KMS 控制台中，首先选择密钥类型（对称或非对称），然后选择密钥用法。您选择的密钥类型决定了将会显示哪些密钥用法选项。您选择的密钥用法决定了将会显示哪些密钥规范（如果）。

要在 AWS KMS 控制台中选择密钥用法，请执行以下操作：

- 对于对称加密 KMS 密钥（默认值），选择 Encrypt and decrypt（加密和解密）。
- 对于 HMAC KMS 密钥，请选择 Generate and verify MAC（生成并验证 MAC）。
- 对于具有椭圆曲线（ECC）密钥材料的非对称 KMS 密钥，选择 Sign and verify（签名和验证）。
- 对于具有 RSA 密钥材料的非对称 KMS 密钥，选择 Encrypt and decrypt（加密和解密）或 Sign and verify（签名和验证）。
- 对于具有 SM2 密钥材料的非对称 KMS 密钥，选择 Encrypt and decrypt（加密和解密）或 Sign and verify（签名和验证）。SM2 密钥规范仅限中国区域使用。

要允许委托人仅针对特定的密钥使用创建 KMS 密钥，请使用 k ms: KeyUsage 条件密钥。还可以使用 kms:KeyUsage 条件键，允许委托人根据 KMS 密钥的密钥用法对其调用 API 操作。例如，可以允许仅当 KMS 密钥的密钥用法为 SIGN_VERIFY 时禁用 KMS 密钥的权限。

选择密钥规范

创建非对称 KMS 密钥或 HMAC KMS 密钥时，可以选择其密钥规范。密钥规范是每个 AWS KMS key 的属性，表示 KMS 密钥的加密配置。密钥规范在创建 KMS 密钥时选择，并且无法更改。如果选择了错误的密钥规范，可删除 KMS 密钥，然后创建一个新的密钥规范。

> **Note**
>
> KMS 密钥的密钥规范被称为“客户主密钥规范”。该CreateKey操作的CustomerMasterKeySpec参数已被弃用。请改用 KeySpec 参数。CreateKey和DescribeKey操作的响应包括具有相同值的KeySpec和CustomerMasterKeySpec成员。

密钥规范决定了 KMS 密钥是对称还是非对称、KMS 密钥中的密钥材料类型，以及 AWS KMS 支持用于 KMS 密钥的加密算法、签名算法或消息认证码（MAC）算法。选择哪个密钥规范通常取决于使用案例和法规要求。但是，KMS 密钥加密操作的密钥规范不同，其价格和限额也不同。有关定价的详细信息，请参阅 AWS Key Management Service 定价。有关请求配额的信息，请参阅 请求配额。

要确定允许您账户中的委托人用于 KMS 密钥的密钥规范，请使用 k ms: KeySpec 条件密钥。

对于 KMS 密钥，AWS KMS 支持以下密钥规范：

对称加密密钥规范（默认值）

- SYMMETRIC_DEFAULT

HMAC 密钥规范

- HMAC_224
- HMAC_256
- HMAC_384
- HMAC_512

RSA 密钥规范（加密和解密或签名和验证）

- RSA_2048

- RSA_3072
- RSA_4096

椭圆曲线密钥规范

- 非对称 NIST 推荐的椭圆曲线密钥对（签名和验证）
  - ECC_NIST_P256 (secp256r1)
  - ECC_NIST_P384 (secp384r1)
  - ECC_NIST_P521 (secp521r1)
- 其他非对称椭圆曲线密钥对（签名和验证）
  - ECC_SECG_P256K1 (secp256k1)，常用于加密货币。

SM2 密钥规范（加密和解密或签名和验证）

- SM2（仅限中国区域）

AWS KMS 中的非对称密钥

AWS KMS 支持非对称 KMS 密钥，这些密钥代表与数学相关的 RSA、椭圆曲线（ECC）或 SM2（仅限中国区域）公有和私有密钥对。这些密钥对在通过 FIPS 140-2 加密模块验证计划认证的 AWS KMS 硬件安全模块中生成，中国（北京）和中国（宁夏）区域除外。私有密钥永远不会让 AWS KMS HSM 处于未加密状态。您可以下载公有密钥并在 AWS 外部分发和使用该密钥。您可以创建非对称 KMS 密钥进行加密和解密，或签名和验证，但不能同时用于二者。

您可以在 AWS 账户 中创建和管理非对称 KMS 密钥，包括设置用于控制密钥访问权限的密钥策略、IAM policy 和授权、启用和禁用 KMS 密钥、创建标签和别名，以及删除 KMS 密钥。您可以在 AWS CloudTrail 日志的 AWS 中审核使用或管理非对称 KMS 密钥的所有操作。

AWS KMS 还提供了非对称数据密钥对，这些密钥设计用于 AWS KMS 外部的客户端加密。非对称数据密钥对中的私有密钥由 AWS KMS 中的对称加密 KMS 密钥保护。

本主题将介绍非对称 KMS 密钥的工作原理、它们与其他 KMS 密钥之间的差异，以及如何确定需要采用哪种 KMS 密钥保护数据。还将介绍非对称数据密钥对的工作原理，以及如何在 AWS KMS 外部使用这些密钥。

区域

AWS KMS 支持的所有 AWS 区域 中都支持非对称 KMS 密钥和非对称数据密钥对。

了解更多

- 若要创建非对称 KMS 密钥，请参阅 创建非对称 KMS 密钥。若要创建对称加密 KMS 密钥，请参阅 创建密钥。
- 若要创建多区域非对称 KMS 密钥，请参阅 创建多区域密钥。
- 要了解 KMS 密钥是对称的还是非对称的，请参阅 识别非对称 KMS 密钥。
- 有关比较应用于每种 KMS 密钥类型的 AWS KMS API 操作的表格，请参阅 the section called “密钥类型引用”。
- 要控制对账户中的委托人可用于 KMS 密钥和数据密钥的密钥规范、密钥用法、加密算法和签名算法的访问权限，请参阅 the section called “AWS KMS 条件键”。
- 要了解适用于不同类型 KMS 密钥的请求配额，请参阅 the section called “请求配额”。
- 要了解如何使用非对称 KMS 密钥签署消息和验证签名，请参阅 AWS 安全博客中的采用 AWS KMS 的新的非对称密钥功能进行数字签名。

主题

非对称 KMS 密钥

您可以在 AWS KMS 中创建非对称 KMS 密钥。非对称 KMS 密钥表示数学上相关的公有密钥和私有密钥对。公有密钥可以交给任何人，即使他们不可靠，但私有密钥必须保密。

在非对称 KMS 密钥中，私有密钥是在 AWS KMS 中创建的，它永远不会让 AWS KMS 处于未加密状态。要使用私有密钥，必须调用 AWS KMS。您可以通过调用 AWS KMS API 操作在 AWS KMS 内使用公有密钥。或者，可以下载公有密钥并在 AWS KMS 外部使用该密钥。

如果使用案例需要无法调用 AWS KMS 的用户在 AWS 外部进行加密，那么非对称 KMS 密钥是个不错的选择。但是，如果您要创建 KMS 密钥来加密在 AWS 服务中存储或管理的数据，请使用对称加密 KMS 密钥。与 AWS KMS 集成的 AWS 服务仅使用对称加密 KMS 密钥来加密您的数据。这些服务不支持使用非对称 KMS 密钥进行加密。

AWS KMS 支持三种类型的非对称 KMS 密钥。

- RSA KMS 密钥：具有 RSA 密钥对的 KMS 密钥，用于加密和解密或签名和验证（但不能同时用于二者）。AWS KMS 支持多种密钥长度，以满足不同的安全要求。
- 椭圆曲线 (ECC) KMS 密钥：具有椭圆曲线密钥对的 KMS 密钥，用于签名和验证。AWS KMS 支持多种常用的曲线。
- SM2 KMS 密钥（仅限中国区域）：具有 SM2 密钥对的 KMS 密钥，用于加密和解密或签名和验证（但不能同时用于二者）。

有关选择非对称密钥配置的帮助，请参阅 选择一种 KMS 密钥类型。有关 AWS KMS 支持用于 RSA KMS 密钥的加密和签名算法的技术详细信息，请参阅 RSA 密钥规范。有关 AWS KMS 支持用于 ECC KMS 密钥的签名算法的技术详细信息，请参阅椭圆曲线密钥规范。有关 AWS KMS 支持用于 SM2 KMS 密钥的加密和签名算法的技术详细信息（仅限中国区域），请参阅 SM2 密钥规范。

有关可以对对称 KMS 密钥和非对称 KMS 密钥执行的操作的比较表格，请参阅比较对称 KMS 密钥与非对称 KMS 密钥。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

区域

AWS KMS 支持的所有 AWS 区域 中都支持非对称 KMS 密钥和非对称数据密钥对。

创建非对称 KMS 密钥

您可以在AWS KMS控制台、使用 CreateKeyAPI 或使用AWS CloudFormation模板创建非对称 KMS 密钥。非对称 KMS 密钥表示可用于加密或签名的公有密钥和私有密钥对。私有密钥保留在 AWS KMS 内。要下载公有密钥在 AWS KMS 外部使用，请参阅 下载公有密钥。

创建 KMS 密钥来加密在 AWS 服务中存储或管理的数据，请使用对称加密 KMS 密钥。与 AWS KMS 集成的 AWS 服务不支持非对称 KMS 密钥。有关如何确定是创建对称 KMS 密钥还是非对称 KMS 密钥的帮助信息，请参阅 选择一种 KMS 密钥类型。

有关创建 KMS 密钥所需权限的信息，请参阅 创建 KMS 密钥的权限。

主题

- 创建非对称 KMS 密钥（控制台）
- 创建非对称 KMS 密钥 (AWS KMS API)

创建非对称 KMS 密钥（控制台）

您可以使用 AWS Management Console 创建非对称 AWS KMS keys（KMS 密钥）。每个非对称 KMS 密钥表示一个公有密钥和私有密钥对。

> **Important**
>
> 不要在别名、描述或标签中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择 Create key。
5. 要创建非对称 KMS 密钥，请在 Key type（密钥类型）中选择 Asymmetric（非对称）。

   有关如何在 AWS KMS 控制台中创建对称加密 KMS 密钥的信息，请参阅 创建对称加密 KMS 密钥（控制台）。
6. 要创建用于公有密钥加密的非对称 KMS 密钥，请在 Key usage（密钥用法）中选择 Encrypt and decrypt（加密和解密）。或者，要创建用于签署消息和验证签名的非对称 KMS 密钥，请在 Key usage（密钥用法）中选择 Sign and verify（签名和验证）。

   有关选择密钥用法值的帮助信息，请参阅选择密钥用法。
7. 为非对称 KMS 密钥选择规范（密钥规范）。

   通常，选择哪个密钥规范取决于法规、安全或业务要求。也可能受需要加密或签名的消息大小的影响。一般来说，加密密钥越长，对暴力攻击的抵抗力越强。

   有关选择密钥规范的帮助信息，请参阅选择密钥规范。
8. 请选择 Next（下一步）。
9. 为 KMS 密钥键入别名。别名名称不能以 **aws/** 开头。**aws/** 前缀由 Amazon Web Services 预留，用于在您的账户中表示 AWS 托管式密钥。

   别名是您可以用于标识控制台和一些 AWS KMS API 中的 KMS 密钥的友好名称。我们建议您选择一个别名，用来指示您计划保护的数据类型或计划与 KMS 密钥搭配使用的应用程序。

   在 AWS Management Console 中创建 KMS 密钥时需要别名。使用CreateKey操作时无法指定别名，但可以使用控制台或CreateAlias操作为现有 KMS 密钥创建别名。有关更多信息，请参阅 使用别名。
10. （可选）为 KMS 密钥键入描述。

输入一个描述，用来说明您计划保护的数据类型或计划与 KMS 密钥配合使用的应用程序。

现在，除非密钥状态为 `Pending Deletion` 或 `Pending Replica Deletion`，否则您可以随时添加描述或更新描述。要添加、更改或删除现有客户托管密钥的描述，请在中编辑描述AWS Management Console或使用UpdateKeyDescription操作。

11. (可选) 键入标签键和一个可选标签值。要向 KMS 密钥添加多个标签，请选择 Add tag（添加标签）。

    在将标签添加到 AWS 资源时，AWS 可生成成本分配报告，其中按标签汇总了使用情况和成本。标签还可以用来控制对 KMS 密钥的访问。有关轮换 KMS 密钥的信息，请参阅 标记密钥 和 AWS KMS 中的 ABAC。

12. 请选择 Next（下一步）。

13. 选择可管理 KMS 密钥的 IAM 用户和角色。

    > **Note**
    >
    > 此密钥策略将授予 AWS 账户 对此 KMS 密钥的完全控制权。此控制权允许账户管理员使用 IAM policy 授予其他主体管理 KMS 密钥的权限。有关更多信息，请参阅 the section called “默认密钥策略”。
    > IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

14. （可选）要阻止选定 IAM 用户和角色删除此 KMS 密钥，请在页面底部的 Key deletion（密钥删除）部分中，清除 Allow key administrators to delete this key（允许密钥管理员删除此密钥）复选框。

15. 请选择 Next（下一步）。

16. 选择可将 KMS 密钥用于加密操作的 IAM 用户和角色。

    > **Note**
    >
    > 此密钥策略将授予 AWS 账户 对此 KMS 密钥的完全控制权。此控制权允许账户管理员使用 IAM policy 授予其他主体在加密操作中使用 KMS 密钥的权限。有关更多信息，请参阅 the section called “默认密钥策略”。
    > IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

17. （可选）您可以允许其他 AWS 账户 将此 KMS 密钥用于加密操作。为此，请在页面底部的 Other AWS 账户（其他 Amazon Web Services 账户）部分中，选择 Add another AWS 账户（添加另一个 Amazon Web Services 账户）并输入外部账户的 AWS 账户 账户标识号。要添加多个外部账户，请重复此步骤。

    > **Note**
    >
    > 若要允许外部账户中的主体使用 KMS 密钥，外部账户的管理员必须创建提供这些权限的 IAM policy。有关更多信息，请参阅 允许其他账户中的用户使用 KMS 密钥。

18. 选择 下一步。
19. 检视您选择的密钥设置。您仍然可以返回并更改所有设置。
20. 选择 Finish（完成）以创建 KMS 密钥。

创建非对称 KMS 密钥 (AWS KMS API)

您可以使用该CreateKey操作来创建非对称AWS KMS key的。这些示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

创建非对称 KMS 密钥时，必须指定 KeySpec 参数，该参数决定了所创建的密钥类型。此外，还必须指定 KeyUsage 值是 ENCRYPT_DECRYPT 还是 SIGN_VERIFY。创建 KMS 密钥后，这些属性无法更改。

该CreateKey操作不允许您指定别名，但您可以使用该CreateAlias操作为新 KMS 密钥创建别名。

> **Important**
>
> 不要在 Description 或 Tags 字段中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

以下示例使用 CreateKey 操作，创建一个 4096 位 RSA 密钥的非对称 KMS 密钥，用于公有密钥加密。

```
$ 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
    }
}
```

以下示例命令创建一个非对称 KMS 密钥，表示一对用于签名和验证的 ECDSA 密钥。不能创建用于加密和解密的椭圆曲线密钥对。

```
$ 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"
```

```
    }
}
```

下载公有密钥

您可以通过使用 AWS Management Console或 AWS KMS API，查看、复制和下载非对称 KMS 密钥对的公有密钥。您必须具备对非对称 KMS 密钥的 `kms:GetPublicKey` 权限。

每个非对称 KMS 密钥对均包含一个永远不会让 AWS KMS 处于未加密状态的私有密钥，和一个可以下载和共享的公有密钥。

可以共享公有密钥，让其他人在 AWS KMS 外部加密数据，但您只能用私有密钥解密数据。或者，允许其他人在 AWS KMS 外部验证您使用私有密钥生成的数字签名。

在 AWS KMS 内部使用非对称 KMS 密钥中的公有密钥时，您将从每个 AWS KMS 操作中包含的身份验证、授权和日志记录中获益。您还可以降低对无法解密的数据进行加密的风险。这些功能在 AWS KMS 外部无效。有关更多信息，请参阅 下载公有密钥的特殊注意事项。

> **Tip**
>
> 正在寻找数据密钥或 SSH 密钥？ 本主题介绍如何管理 AWS Key Management Service 中的非对称密钥，私有密钥在其中不可导出。有关私钥受对称加密 KMS 密钥保护的可导出数据密钥对，请参阅。GenerateDataKeyPair有关下载与 Amazon EC2 实例关联的公有密钥的帮助，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》和《适用于 Windows 实例的 Amazon EC2 用户指南》中的检索公有密钥。

主题

下载公有密钥的特殊注意事项

为保护 KMS 密钥，AWS KMS 提供了访问控制、身份验证加密和每个操作的详细日志。AWS KMS 还允许您暂时或永久地阻止使用 KMS 密钥。最后，AWS KMS 操作旨在最大限度降低对无法解密的数据进行加密的风险。在 AWS KMS 外部使用下载的公有密钥时，这些功能不可用。

授权

在 AWS KMS 内控制对 KMS 密钥访问的密钥政策和 IAM policy 对在 AWS 外部执行的操作没有影响。任何可获得公有密钥的用户都可以在 AWS KMS 外部使用该公有密钥，即使这些用户无权使用 KMS 密钥加密数据或验证签名。

密钥用法限制

密钥用法限制在 AWS KMS 之外是无效的。如果您使用 KeyUsage 为 SIGN_VERIFY 的 KMS 密钥调用 Encrypt 操作，则 AWS KMS 操作将失败。但是，如果您在 AWS KMS 外部使用 KeyUsage 为 SIGN_VERIFY 的 KMS 密钥的公有密钥加密数据，数据将无法解密。

算法限制

对 AWS KMS 支持的加密算法和签名算法的限制，在 AWS KMS 之外是无效的。如果在 AWS KMS 外部使用 KMS 密钥的公有密钥加密数据，并使用 AWS KMS 不支持的加密算法，则数据将无法解密。

禁用和删除 KMS 密钥

为阻止在 AWS KMS 内的加密操作中使用 KMS 密钥所能采取的措施，不会阻止任何人在 AWS KMS 外部使用公有密钥。例如，禁用 KMS 密钥、调度删除 KMS 密钥、删除 KMS 密钥或删除 KMS 密钥的密钥材料，对 AWS KMS 外部的公有密钥没有影响。如果删除非对称 KMS 密钥或者删除或丢失其密钥材料，那么在 AWS KMS 外部使用公有密钥加密的数据将无法恢复。

日志记录

记录每个 AWS KMS 操作（包括请求、响应、日期、时间和授权用户）的 AWS CloudTrail 日志，不会记录 AWS KMS 外部公有密钥的使用情况。

使用 SM2 密钥对进行离线验证（仅限中国区域）

要使用 SM2 公钥验证 AWS KMS 外部的签名，您必须指定区分 ID。默认情况下，AWS KMS 使用 1234567812345678 作为区分 ID。有关更多信息，请参阅使用 SM2 密钥对进行离线验证（仅限中国区域）。

下载公有密钥（控制台）

您可以使用 AWS Management Console 查看、复制和下载 AWS 账户 中的非对称 KMS 密钥的公有密钥。要在不同 AWS 账户 中下载非对称 KMS 密钥的公有密钥，请使用 AWS KMS API。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。

2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择非对称 KMS 密钥的别名或密钥 ID。
5. 选择 Cryptographic configuration（加密配置）选项卡。记录 Key spec（密钥规范）、Key usage（密钥用法）和 Encryption algorithms（密钥算法）或 Signing Algorithms（签名算法）字段的值。您需要使用这些值才能在 AWS KMS 外部使用公有密钥。在共享公有密钥时，请务必共享以上信息。
6. 选择 Public key (公有密钥) 选项卡。
7. 要将公有密钥复制到剪贴板，请选择 Copy (复制)。要将公有密钥下载到文件，请选择 Download (下载)。

下载公有密钥 (AWS KMS API)

该GetPublicKey操作返回非对称 KMS 密钥中的公钥。它还会返回在 AWS KMS 外部正确使用公有密钥所需的关键信息，包括密钥用法和加密算法。请务必保存这些值，并在共享公有密钥时共享它们。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

要指定 KMS 密钥，请使用其密钥 ID、密钥 ARN、别名名称或别名 ARN。使用别名时，应加上 alias/ 前缀。要指定不同 AWS 账户 中的 KMS 密钥，必须使用其密钥 ARN 或别名 ARN。

在运行此命令之前，请将示例别名替换为 KMS 密钥的有效标识符。要运行此命令，必须具备对 KMS 密钥的 `kms:GetPublicKey` 权限。

```
$ 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..."
}
```

识别非对称 KMS 密钥

要确定特定 KMS 密钥是非对称 KMS 密钥，请查找密钥类型或密钥规范。可以使用 AWS KMS 控制台或 AWS KMS API。

其中一些方法还将向您显示 KMS 密钥的加密配置的其他方面，包括密钥用法以及 KMS 密钥支持的加密或签名算法。您可以查看现有 KMS 密钥的加密配置，但无法更改该配置。

有关查看 KMS 密钥的一般信息，包括排序、筛选和选择在控制台中显示的列，请参阅 在控制台中查看 KMS 密钥。

主题

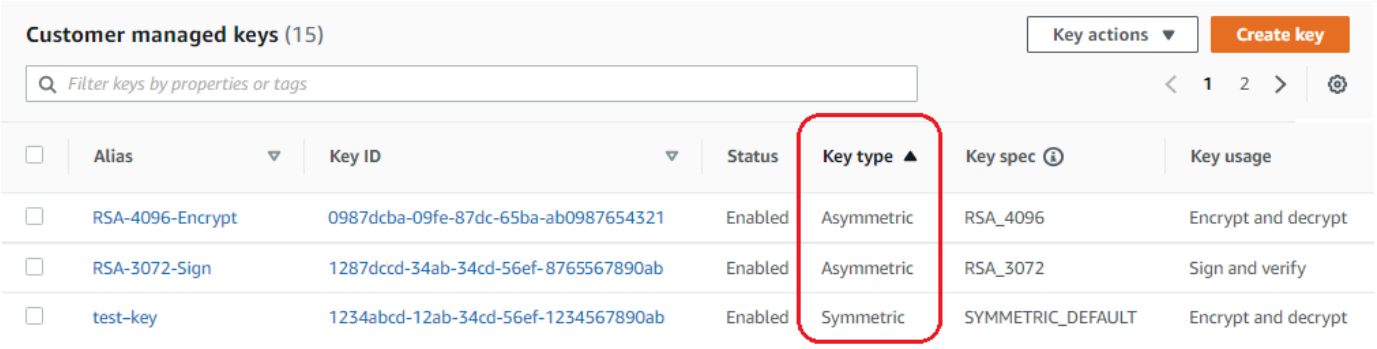
在 KMS 密钥表中查找密钥类型

在 AWS KMS 控制台中，Key type（密钥类型）列显示每个 KMS 密钥是对称还是非对称 KMS 密钥。您可以将 Key type（密钥类型）列添加到控制台中 Customer managed keys（客户托管式密钥）或 AWS 托管式密钥 页面上的 KMS 密钥表中。

要识别您的 KMS 密钥表中的对称和非对称 KMS 密钥，请使用以下过程。

1. 从 https://console.aws.amazon.com/kms 打开 AWS KMS 控制台。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。要查看您账户中 AWS 为您所创建和管理的密钥，请在导航窗格中选择 AWS managed keys（Amazon 托管式密钥）。
4. Key type（密钥类型）列显示每个 KMS 密钥是对称还是非对称 KMS 密钥。您还可以按 Key type（密钥类型）值进行排序和筛选。

   如果您的 KMS 密钥表中未显示 Key type（密钥类型）列，请选择页面右上角的齿轮图标，选择 Key type（密钥类型），然后选择 Confirm（确认）。您还可以添加 Key spec (密钥规范) 和 Key usage (密钥用途) 列。



在详细信息页面上查找密钥类型

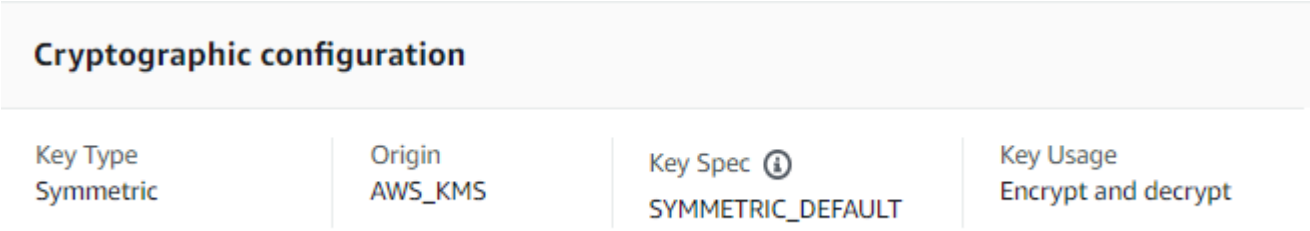
在 AWS KMS 控制台中，每个 KMS 密钥的详细信息页面都包含一个 Cryptographic Configuration（加密配置）选项卡，该选项卡显示密钥类型（对称或非对称）以及有关 KMS 密钥的其他加密详细信息。

要在 KMS 密钥的详细信息页面上识别对称和非对称 KMS 密钥，请使用以下过程。

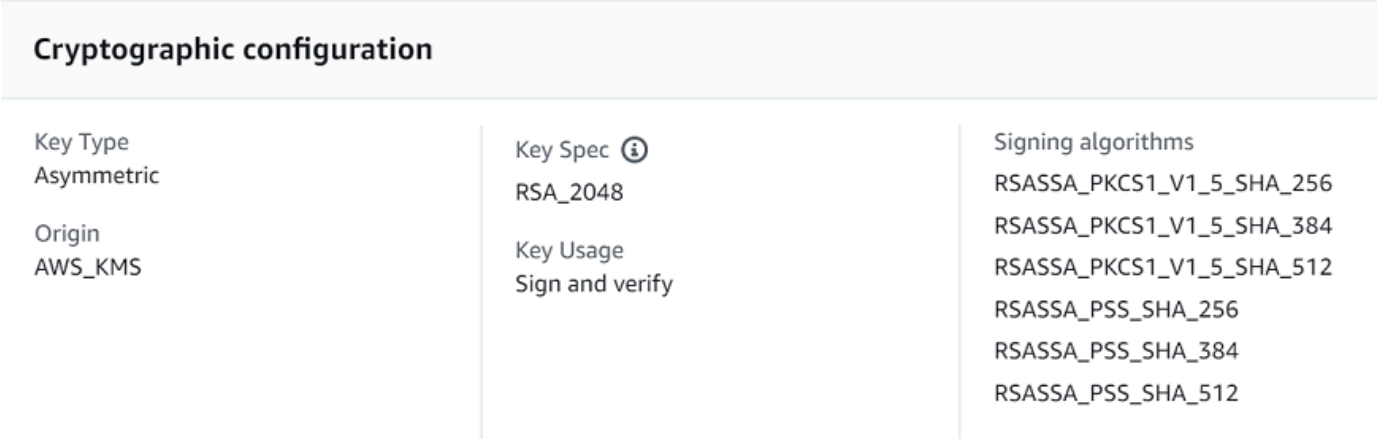
1. 从 https://console.aws.amazon.com/kms 打开 AWS KMS 控制台。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 要查看您账户中自己所创建和管理的密钥，请在导航窗格中选择 Customer managed keys (客户托管密钥)。要查看您账户中 AWS 为您所创建和管理的密钥，请在导航窗格中选择 AWS managed keys（Amazon 托管式密钥）。
4. 选择 KMS 密钥的别名和密钥 ID。
5. 选择 Cryptographic configuration（加密配置）选项卡。这些选项卡在 General configuration（常规配置）部分下。

   Cryptographic configuration（加密配置）选项卡显示 Key Type（密钥类型），用于指示密钥是对称还是非对称。其中还显示有关 KMS 密钥的其他详细信息，包括 Key Usage（密钥用法），密钥用法指明 KMS 密钥可用于加密和解密还是签名和验证。对于非对称 KMS 密钥，其中显示 KMS 密钥支持的加密算法或签名算法。

   例如，以下是对称加密 KMS 密钥的示例 Cryptographic configuration（加密配置）选项卡。



下面是一个用于签名和验证的非对称 RSA KMS 密钥的示例 Cryptographic configuration（加密配置）选项卡。



使用 AWS KMS API 查找密钥规范

要确定 KMS 密钥是对称的还是非对称的，请使用操作。DescribeKey响应中的 KeySpec 字段包含 KMS 密钥的密钥规范。对于对称加密 KMS 密钥，KeySpec 的值为 SYMMETRIC_DEFAULT。其他值都指明是非对称 KMS 密钥或 HMAC KMS 密钥。

> **Note**
>
> CustomerMasterKeySpec 成员已弃用。请改用KeySpec。为了防止破坏性的更改，DescribeKey 响应包括具有相同值的 KeySpec 和 CustomerMasterKeySpec 成员。

例如，对于对称加密 KMS 密钥，DescribeKey 返回以下响应。KeySpec 值为 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"
    ]
  }
}
```

用于签名和验证的非对称 RSA KMS 密钥的 DescribeKey 响应与此示例相似。KeySpec 值为 RSA_2048，KeyUsage 为 SIGN_VERIFY。SigningAlgorithms 元素列出 KMS 密钥的有效签名算法。

```
{
  "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"
    ]
  }
}
```

非对称密钥规范

以下主题提供了有关 AWS KMS 为非对称 KMS 密钥支持的密钥规范的技术信息。包括有关对称加密密钥的 SYMMETRIC_DEFAULT 密钥规范的信息以便进行比较。

主题

RSA 密钥规范

使用 RSA 密钥规范时，AWS KMS 会创建具有 RSA 密钥对的非对称 KMS 密钥。私有密钥永远不会让 AWS KMS 处于未加密状态。在 AWS KMS 内部可以使用公有密钥，或者下载公有密钥供 AWS KMS 外部使用。

> **Warning**
>
> 在 AWS KMS 外部加密数据时，请确保您可以解密密文。如果您使用已从 AWS KMS 删除的 KMS 密钥中的公有密钥、配置用于签名和验证的 KMS 密钥中的公有密钥或者使用 KMS 密钥不支持的加密算法，则数据将无法恢复。

在 AWS KMS 中，可以使用具有 RSA 密钥对的非对称 KMS 密钥进行加密和解密或签名和验证，但不能同时用于二者。此属性（称为 密钥用法）与密钥规范分开确定，但应该在选择密钥规范之前做出决定。

AWS KMS 支持以下 RSA 密钥规范，用于加密和解密或签名和验证：

- RSA_2048
- RSA_3072
- RSA_4096

RSA 密钥规范因 RSA 密钥长度（以位为单位）而异。选择哪个 RSA 密钥规范可能取决于安全标准或任务要求。一般来说，可使用对任务而言实用又实惠的最大密钥。KMS 密钥加密操作的 RSA 密钥规

范不同，其价格也不同。有关 AWS KMS 定价的信息，请参阅 AWS Key Management Service 定价。有关请求配额的信息，请参阅 请求配额。

用于加密和解密的 RSA 密钥规范

使用 RSA 非对称 KMS 密钥行加密和解密时，用公有密钥加密，然后用私有密钥解密。在 AWS KMS 中为 RSA KMS 密钥调用 `Encrypt` 操作时，AWS KMS 使用 RSA 密钥对中的公有密钥和您指定的加密算法来加密数据。要解密密文，请调用 `Decrypt` 操作并指定相同的 KMS 密钥和加密算法。AWS KMS 随后使用 RSA 密钥对中的私有密钥解密数据。

也可以下载公有密钥，并在 AWS KMS 外部使用该密钥加密数据。请确保使用 AWS KMS 支持用于 RSA KMS 密钥的加密算法。要解密密文，请采用相同的 KMS 密钥和加密算法调用 `Decrypt` 函数。

对于具有 RSA 密钥规范的 KMS 密钥，AWS KMS 支持两种加密算法。这些算法在 PKCS #1 2.2 版中定义，它们内部使用的哈希函数有所不同。在 AWS KMS 中，RSAES_OAEP 算法始终使用相同的哈希函数实现哈希目的和掩码生成函数 (MGF1)。调用 Encrypt 和 Decrypt 操作时，需要指定加密算法。您可以为每个请求选择不同的算法。

支持 RSA 密钥规范的加密算法

加密算法	算法描述
RSAES_OAEP_SHA_1	PKCS #1 2.2 版，7.1 节。具有 OAEP 填充且采用 SHA-1 实现哈希和 MGF1 掩码生成函数以及空标签的 RSA 加密。
RSAES_OAEP_SHA_256	PKCS #1，7.1 节。具有 OAEP 填充且采用 SHA-256 实现哈希和 MGF1 掩码生成函数以及空标签的 RSA 加密。

无法将 KMS 密钥配置为使用特定的加密算法。但是，您可以使用 kms: EncryptionAlgorithm 策略条件来指定允许委托人使用 KMS 密钥的加密算法。

要获取 KMS 密钥的加密算法，请在AWS KMS控制台中查看 KMS 密钥的加密配置或使用DescribeKey操作。 AWS KMS当您在AWS KMS控制台中或使用GetPublicKey操作下载公钥时，还会提供密钥规范和加密算法。

您可以根据可在每个请求中加密的明文数据的长度，选择 RSA 密钥规范。下表显示了在对 Encrypt 操作的单次调用中，可以加密的明文的最大长度（以字节为单位）。值因密钥规范和加密算法而异。为进行比较，使用对称加密 KMS 密钥一次最多可加密 4096 字节。

要计算这些算法的最大明文长度（以字节为单位），请使用以下公式：(*key_size_in_bits* / 8) - (2 * *hash_length_in_bits*/8) - 2。例如，对于具有 SHA-256 的 RSA_2048，最大明文长度为 (2048/8) - (2 * 256/8) -2 = 190 字节。

Encrypt 操作中的最大明文长度（以字节为单位）

	加密算法	
密钥规范	RSAES_OAEP_SHA_1	RSAES_OAEP_SHA_256
RSA_2048	214	190
RSA_3072	342	318
RSA_4096	470	446

用于签名和验证的 RSA 密钥规范

使用 RSA 非对称 KMS 密钥进行签名和验证时，用私有密钥为消息生成签名，然后用公有密钥验证签名。

在 AWS KMS 中为非对称 KMS 密钥调用 `Sign` 操作时，AWS KMS 使用 RSA 密钥对中的私有密钥、消息和您指定的签名算法来生成签名。要验证签名，请调用 Verify 操作。指定签名以及相同的 KMS 密钥、消息和签名算法。AWS KMS 随后使用 RSA 密钥对中的公有密钥验证签名。也可以下载公有密钥，并在 AWS KMS 外部使用该密钥验证签名。

对于具有 RSA 密钥规范的所有 KMS 密钥，AWS KMS 支持以下签名算法。在您调用 Sign 和 Verify 操作后，需要指定签名算法。您可以为每个请求选择不同的算法。使用 RSA 密钥对进行签名时，首选 RSASSA-PSS 算法。为了与现有应用程序兼容，我们包含了 RSASSA-PKCS1-v1_5 算法。

支持 RSA 密钥规范的签名算法

签名算法	算法描述
RSASSA_PSS_SHA_256	PKCS #1 2.2 版，8.1 节，具有 PSS 填充且采用 SHA-256 实现消息摘要和 MGF1 掩码生成函数以及 256 位盐的 RSA 签名

签名算法	算法描述
RSASSA_PSS_SHA_384	PKCS #1 2.2 版，8.1 节，具有 PSS 填充且采用 SHA-384 实现消息摘要和 MGF1 掩码生成函数以及 384 位盐的 RSA 签名
RSASSA_PSS_SHA_512	PKCS #1 2.2 版，8.1 节，具有 PSS 填充且采用 SHA-512 实现消息摘要和 MGF1 掩码生成函数以及 512 位盐的 RSA 签名
RSASSA_PKCS1_V1_5_SHA_256	PKCS #1 2.2 版，8.2 节，具有 PKCS #1v1.5 填充和 SHA-256 的 RSA 签名
RSASSA_PKCS1_V1_5_SHA_384	PKCS #1 2.2 版，8.2 节，具有 PKCS #1v1.5 填充和 SHA-384 的 RSA 签名
RSASSA_PKCS1_V1_5_SHA_512	PKCS #1 2.2 版，8.2 节，具有 PKCS #1v1.5 填充和 SHA-512 的 RSA 签名

无法将 KMS 密钥配置为使用特定的签名算法。但是，您可以使用 kms: SigningAlgorithm 策略条件来指定允许委托人使用 KMS 密钥的签名算法。

要获取 KMS 密钥的签名算法，请在AWS KMS控制台中或使用DescribeKey操作查看 KMS 密钥的加密配置。 AWS KMS当您在AWS KMS控制台中或使用GetPublicKey操作下载公钥时，还会提供密钥规范和签名算法。

椭圆曲线密钥规范

在使用椭圆曲线 (ECC) 密钥规范时，AWS KMS 会创建具有 ECC 密钥对的非对称 KMS 密钥用于签名和验证。生成签名的私有密钥永远不会让 AWS KMS 处于未加密状态。您可以在 AWS KMS 内部使用公有密钥验证签名，或者下载公有密钥供 AWS KMS 外部使用。

对于非对称 KMS 密钥，AWS KMS 支持以下 ECC 密钥规范。

- 非对称 NIST 推荐的椭圆曲线密钥对（签名和验证）
  - ECC_NIST_P256 (secp256r1)
  - ECC_NIST_P384 (secp384r1)
  - ECC_NIST_P521 (secp521r1)

- 其他非对称椭圆曲线密钥对（签名和验证）
  - ECC_SECG_P256K1 (secp256k1)，常用于加密货币。

选择哪个 ECC 密钥规范可能取决于安全标准或任务要求。一般来说，可使用对任务而言实用又实惠的点最多的曲线。

如果您正在创建非对称 KMS 密钥以用于加密货币，请使用 ECC_SEG_P256K1 密钥规范。此密钥规范也可以用于其他目的，但比特币和其他加密货币必须使用此密钥规范。

使用不同 ECC 密钥规范的 KMS 密钥定价不同，并受不同的请求配额限制。有关 AWS KMS 定价的信息，请参阅 AWS Key Management Service 定价。有关请求配额的信息，请参阅 请求配额。

下表显示了 AWS KMS 对于每个 ECC 密钥规范支持的签名算法。无法将 KMS 密钥配置为使用特定的签名算法。但是，您可以使用 kms: SigningAlgorithm 策略条件来指定允许委托人使用 KMS 密钥的签名算法。

支持 ECC 密钥规范的签名算法

密钥规范	签名算法	算法描述
ECC_NIST_P256	ECDSA_SHA_256	NIST FIPS 186-4，6.4 节，使用密钥指定的曲线并采用SHA-256 实现消息摘要的 ECDSA 签名。
ECC_NIST_P384	ECDSA_SHA_384	NIST FIPS 186-4，6.4 节，使用密钥指定的曲线并采用 SHA-384 实现消息摘要的 ECDSA 签名。
ECC_NIST_P521	ECDSA_SHA_512	NIST FIPS 186-4，6.4 节，使用密钥指定的曲线并采用 SHA-512 实现消息摘要的 ECDSA 签名。
ECC_SECG_P256K1	ECDSA_SHA_256	NIST FIPS 186-4，6.4 节，使用密钥指定的曲线并采用SHA-256 实现消息摘要的 ECDSA 签名。

SM2 密钥规范（仅限中国区域）

SM2 密钥规范是在 GM/T 系列规范中定义的椭圆曲线密钥规范，这一系列规范由中国国家商用密码管理办公室（OSCCA）发布。SM2 密钥规范仅限中国区域使用。使用 SM2 密钥规范时，AWS KMS 会创建具有 SM2 密钥对的非对称 KMS 密钥。您可以在 AWS KMS 内使用 SM2 密钥对，或者下载公有密钥以供在 AWS KMS 外部使用。

与 ECC 密钥规范不同，您可以使用 SM2 KMS 密钥进行签名和验证，或者加密和解密。在创建 KMS 密钥时，您必须指定密钥用途，并且密钥一经创建便无法更改。

AWS KMS 支持以下 SM2 加密算法和签名算法：

- SM2PKE 加密算法

  SM2PKE 是一种由 OSCCA 在 GM/T 0003.4-2012 中定义的基于椭圆曲线的加密算法。

- SM2DSA 签名算法

  SM2DSA 是一种由 OSCCA 在 GM/T 0003.2-2012 中定义的基于椭圆曲线的签名算法。SM2DSA 需要一个区分 ID，该 ID 使用 SM3 哈希算法进行哈希处理，然后会与您传递到 AWS KMS 的消息或消息摘要相结合。然后由 AWS KMS 对这个连接的值进行哈希处理和签名。

借助 SM2 进行离线操作（仅限中国区域）

您可以下载 SM2 密钥对的公有密钥以在离线操作中使用，即 AWS KMS 外部的操作。但是，离线使用 SM2 公有密钥时，您可能需要手动执行额外的转换和计算。SM2DSA 操作可能需要您提供区分 ID 或计算消息摘要。SM2PKE 加密操作可能需要您将原始加密文字输出转换为某种 AWS KMS 可以接受的格式。

为了帮助您使用这些操作，Java 的 `SM2OfflineOperationHelper` 类为您执行任务提供了方法。您可以将此帮助程序类用作其他加密提供程序的模型。

> **Important**
>
> `SM2OfflineOperationHelper` 参考代码旨在兼容 Bouncy Castle 版本 1.68。如需其他版本的帮助，请联系 bouncycastle.org。

使用 SM2 密钥对进行离线验证（仅限中国区域）

要使用 SM2 公有密钥验证 AWS KMS 外部的签名，您必须指定区分 ID。当您将原始消息 `MessageType:RAW` 传递到签名 API 时，AWS KMS 将使用 OSCCA 在 GM/T 0009-2012 中定义的默认区分 ID 1234567812345678。您不能在 AWS KMS 中指定自己的区分 ID。

但是，如果您在 AWS 外部生成消息摘要，可以指定自己的区分 ID，然后将消息摘要 `MessageType:DIGEST` 传递到 AWS KMS 以进行签名。要执行此操作，请更改 `SM2OfflineOperationHelper` 类中的 `DEFAULT_DISTINGUISHING_ID` 值。您指定的区分 ID 可以是长度不超过 8192 个字符的任何字符串。在 AWS KMS 为消息摘要签名后，您需要消息摘要或消息以及用于计算摘要的区分 ID 以进行离线验证。

`SM2OfflineOperationHelper` 类

在 AWS KMS 内，原始加密文字转换和 SM2DSA 消息摘要计算会自动进行。并非所有加密提供程序都按相同的方式实现 SM2。有些库（比如 OpenSSL 版本 1.1.1 和更高版本）会自动执行这些操作。AWS KMS 在使用 OpenSSL 版本 3.0 进行测试时确认了此行为。使用以下带有库的 `SM2OfflineOperationHelper` 类，比如 Bouncy Castle，这需要您手动执行这些转换和计算。

`SM2OfflineOperationHelper` 类为以下离线操作提供了方法：

- 消息摘要计算

  要离线生成可用于离线验证或传递到 AWS KMS 以进行签名的消息摘要，请使用 `calculateSM2Digest` 方法。`calculateSM2Digest` 方法通过 SM3 哈希算法生成消息摘要。GetPublicKeyAPI 会以二进制格式返回您的公钥。您必须将二进制密钥解析为 Jav PublicKey a。提供解析后的公有密钥与消息。该方法会自动将您的消息与默认的区分 ID 1234567812345678 相结合，但您可以通过更改 `DEFAULT_DISTINGUISHING_ID` 值来设置自己的区分 ID。

- 验证

  要离线验证签名，请使用 `offlineSM2DSAVerify` 方法。`offlineSM2DSAVerify` 方法会使用根据指定区分 ID 计算出的消息摘要和您提供的原始消息来验证数字签名。GetPublicKeyAPI 会以二进制格式返回您的公钥。您必须将二进制密钥解析为 Jav PublicKey a。向解析后的公有密钥提供原始消息和要验证的签名。有关更多详细信息，请参阅使用 SM2 密钥对进行离线验证。

- Encrypt

  要离线加密明文，请使用 `offlineSM2PKEEncrypt` 方法。此方法可确保加密文字采用某种 AWS KMS 可以解密的格式。`offlineSM2PKEEncrypt` 方法会对明文进行加密，然后将

SM2PKE 生成的原始加密文字转换为 ASN.1 格式。GetPublicKeyAPI 会以二进制格式返回您的公钥。您必须将二进制密钥解析为 Jav PublicKey a。为解析后的公有密钥提供您想要加密的明文。

如果您不确定是否需要进行转换，请使用以下 OpenSSL 操作来测试加密文字的格式。如果操作失败，则需要将加密文字转换为 ASN.1 格式。

```
openssl asn1parse -inform DER -in ciphertext.der
```

默认情况下，在为 SM2DSA 操作生成消息摘要时，SM2OfflineOperationHelper 类使用默认的区分 ID 1234567812345678。

```
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");
    }
}
```

SYMMETRIC_DEFAULT 密钥规范

默认密钥规范 SYMMETRIC_DEFAULT 是对称加密 KMS 密钥的密钥规范。当您在 AWS KMS 控制台中选择Symmetric（对称）密钥类型和Encrypt and decrypt（加密和解密）密钥用法时，它会选择 SYMMETRIC_DEFAULT 密钥规范。在CreateKey操作中，如果您未指定KeySpec值，则会选择SYMMETRIC_DEFAULT。如果您没有理由使用其他密钥规范，SymMETIC_DEFAULT 是个不错的选择。

SYMMETRIC_DEFAULT 目前代表 AES-256-GCM，这是一种基于伽罗瓦计数器模式 (GCM) 中的高级加密标准 (AES) 的对称算法，具有 256 位密钥，是用于安全加密的行业标准。此算法生成的密文支持附加身份验证数据 (AAD)，如加密上下文，且 GCM 对密文提供额外的完整性检查。有关技术详细信息，请参阅 AWS Key Management Service加密详细信息。

在 AES-256-GCM 下加密的数据现在和将来都受到保护。密码学家认为这种算法具备抗量子性。理论上，在未来针对使用 256 位 AES-GCM 密钥创建的密文的大规模量子计算攻击中，密钥的有效安全性将会降至 128 位。但是，此安全级别足以对抗对 AWS KMS 密文进行的暴力破解攻击。

唯一的例外是，在中国区域 SYMMETRIC_DEFAULT 表示使用 SM4 加密的 128 位对称密钥。您只能在中国区域内创建 128 位的 SM4 密钥。您无法在中国区域内创建 256 位的 AES-GCM KMS 密钥。

在 AWS KMS 中，可以使用对称加密 KMS 密钥加密、解密和重新加密数据，保护生成的数据密钥和数据密钥对。与 AWS KMS 集成的 AWS 服务使用对称加密 KMS 密钥来加密静态数据。您可以将自己的密钥材料导入对称加密 KMS 密钥中，并在自定义密钥存储中创建对称加密 KMS 密钥。有关可以对对

称 KMS 密钥和非对称 KMS 密钥执行的操作的比较表格，请参阅比较对称 KMS 密钥与非对称 KMS 密钥。

有关 AWS KMS 和对称加密密钥的技术详细信息，请参阅 AWS Key Management Service 加密详细信息。

AWS KMS 中的 HMAC 密钥

HMAC 散列消息认证码 KMS 密钥是用于生成和验证 AWS KMS 内的 HMAC 的对称密钥。与每个 HMAC KMS 密钥关联的唯一密钥材料提供了 HMAC 算法所需的秘密密钥。您可以将 HMAC KMS 密钥与 `GenerateMac` 和 `VerifyMac` 操作结合使用以验证 AWS KMS 中的数据的完整性和真实性。

HMAC 算法结合了加密哈希函数和共享密钥。他们获取消息和密钥，例如 HMAC KMS 密钥中的密钥材料，然后返回一个唯一的固定大小的代码或标签。即使是消息的一个字符发生了变化，或者密钥不完全相同，生成的标签也会完全不同。通过要求提供密钥，HMAC 还提供了真实性；如果没有密钥，就不可能生成相同的 HMAC 标签。HMAC 有时被称为对称签名，因为它们像数字签名一样工作，但使用单个密钥进行签名和验证。

AWS KMS 使用的 HMAC KMS 密钥和 HMAC 算法符合 RFC 2104 中定义的行业标准。该AWS KMSGenerateMac操作会生成标准的 HMAC 标签。这些密钥对在通过 FIPS 140-2 加密模块验证计划认证的 AWS KMS 硬件安全模块中生成（中国（北京）和中国（宁夏）区域除外）并且绝不会使 AWS KMS 处于未加密状态。要使用 HMAC KMS 密钥，您必须调用 AWS KMS。

您可使用 HMAC KMS 密钥确定消息的真实性，例如 JSON Web 令牌（JWT）、令牌化的信用卡信息或提交的密码。它们也可以用作安全的密钥派生函数（KDF），尤其是在需要确定性密钥的应用程序中。

HMAC KMS 密钥比应用软件的 HMAC 具有优势，因为密钥材料完全在 AWS KMS 内部生成和使用，受制于您对密钥设置的访问控制。

> **Tip**
>
> 最佳实践建议您限制包括 HMAC 在内的任何签名机制的有效时间。这阻止了行为者利用已签名信息反复地或是在消息被取代很久之后建立有效性的攻击。HMAC 标签不包含时间戳，但是您可以在令牌或消息中包含时间戳，以帮助您检测何时刷新 HMAC。

授权用户可以在 AWS 账户中创建、管理和使用 HMAC KMS 密钥。这包括启用和禁用密钥、设置和更改别名和标签，以及计划删除 HMAC KMS 密钥。您还可以使用密钥策略、IAM policy 和授权来控制对 HMAC KMS 密钥的访问。您可以在 AWS CloudTrail 日志的 AWS 中审核使用或管理 HMAC KMS 密

钥的所有操作。您可创建具有导入密钥材料的 HMAC KMS 密钥。您也可以在多个 AWS 区域 中创建行为与相同 HMAC KMS 密钥的副本类似的 HMAC 多区域 KMS 密钥。

HMAC KMS 密钥只支持 `GenerateMac` 和 `VerifyMac` 加密操作。您不能使用 HMAC KMS 密钥加密数据或签名消息，也不能在 HMAC 操作中使用任何其他类型的 KMS 密钥。当您使用 `GenerateMac` 操作时，您可提供最多为 4096 个字节的消息、HMAC KMS 密钥以及与 HMAC 密钥规范兼容的 MAC 算法，`GenerateMac` 将计算 HMAC 标签。要验证 HMAC 标签，您必须提供 HMAC 标签以及相同的消息、HMAC KMS 密钥和 `GenerateMac` 用于计算原始 HMAC 标签的 MAC 算法。`VerifyMac` 操作计算 HMAC 标签并验证它与提供的 HMAC 标签是否相同。如果输入和计算的 HMAC 标签不相同，则验证失败。

HMAC KMS 密钥不支持自动密钥轮换，并且您无法在自定义密钥存储中创建 HMAC KMS 密钥。

如果您创建 KMS 密钥以加密 AWS 服务中的数据，请使用对称加密密钥。您不能使用 HMAC KMS 密钥。

区域

AWS KMS 支持的所有 AWS 区域 均支持 HMAC KMS 密钥。

了解更多

- 有关选择 KMS 密钥类型的帮助，请参阅 选择一种 KMS 密钥类型。
- 有关比较每种 KMS 密钥类型支持的 AWS KMS API 操作的表格，请参阅 密钥类型引用。
- 有关创建多区域 HMAC KMS 密钥的信息，请参阅 中的多区域密钥 AWS KMS。
- 要检查 AWS KMS 控制台为 HMAC KMS 密钥设置的默认密钥策略的差异，请参阅 the section called “允许密钥用户将 KMS 密钥与 AWS 服务一起使用”。
- 有关 HMAC KMS 密钥定价的信息，请参阅 AWS Key Management Service 定价。
- 有关应用于 HMAC KMS 密钥的配额的信息，请参阅 资源配额 和 请求配额。
- 有关删除 HMAC KMS 密钥的信息，请参阅 删除 AWS KMS keys。
- 要了解如何使用 HMAC 创建 JSON Web 令牌，请参阅 AWS 安全博客中的如何在 AWS KMS 内保护 HMAC。
- 收听播客：在官方 AWS 播客上介绍 HMAC AWS Key Management Service。

主题

- HMAC KMS 密钥的密钥规范
- 创建 HMAC KMS 密钥

- 控制对 HMAC KMS 密钥的访问
- 查看 HMAC KMS 密钥

HMAC KMS 密钥的密钥规范

AWS KMS 支持不同长度的对称 HMAC 密钥。您选择的密钥规范可取决于安全、法规或业务要求。密钥的长度决定了GenerateMac和VerifyMac操作中使用的 MAC 算法。一般来说，较长的密钥更安全。使用适用于您的使用场景的最长密钥。

HMAC 密钥规范	MAC 算法
HMAC_224	HMAC_SHA_224
HMAC_256	HMAC_SHA_256
HMAC_384	HMAC_SHA_384
HMAC_512	HMAC_SHA_512

创建 HMAC KMS 密钥

您可以在 AWS KMS 控制台中、通过使用 CreateKey API 或通过使用 AWS CloudFormation 模板创建 HMAC KMS 密钥。

AWS KMS 为 HMAC KMS 密钥支持多个密钥规范。您选择的密钥规范可能取决于法规、安全或业务要求。一般来说，密钥越长，对暴力攻击的抵抗力越强。

> **Important**
>
> 不要在别名、描述或标签中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

如果创建 KMS 密钥来加密 AWS 服务中的数据，请使用对称加密 KMS 密钥。与 AWS KMS 集成的 AWS 服务不支持非对称 KMS 密钥或 HMAC KMS 没有。要获取有关创建对称加密 KMS 密钥的帮助，请参阅 创建密钥。

了解更多

- 要确定要创建哪种 KMS 密钥，请参阅 选择一种 KMS 密钥类型。
- 您可以使用本主题介绍的过程创建多区域主 HMAC KMS 密钥。要复制多区域 HMAC 密钥，请参阅 the section called “创建副本密钥”。
- 有关创建 KMS 密钥所需权限的信息，请参阅 创建 KMS 密钥的权限。
- 有关使用AWS CloudFormation模板创建 HMAC KMS 密钥的信息，请参阅AWS CloudFormation用户指南AWS::KMS::Key中的。

主题

创建 HMAC KMS 密钥（控制台）

您可以使用 AWS Management Console 创建 HMAC KMS 密钥。HMAC KMS 密钥是对称密钥，其密钥用法为Generate and verify MAC（生成并验证 MAC）。您也可以创建多区域 HMAC 密钥。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择 Create key。
5. 对于 Key type (密钥类型)，选择 Symmetric (对称)。

   HMAC KMS 密钥是对称密钥。您可以使用相同的密钥生成和验证 HMAC 标签。
6. 对于 Key usage（密钥用法），请选择 Generate and verify MAC（生成并验证 MAC）。

   生成并验证 MAC 是 HMAC KMS 密钥的唯一有效密钥用法。

   > **Note**
   >
   > Key usage（密钥用法）仅在所选区域支持 HMAC KMS 密钥时才会显示对称密钥。
7. 为 HMAC KMS 密钥选择规范（密钥规范）。

   您选择的密钥规范可取决于法规、安全或业务要求。一般来说，较长的密钥更安全。

8. 要创建多区域 主 HMAC 密钥，在 Advanced options（高级选项）下，选择 Multi-Region key（多区域密钥）。您为此 KMS 密钥定义的共享属性（例如密钥类型和密钥用法）将与其副本密钥共享。有关更多信息，请参阅 创建多区域密钥。

   您无法使用该过程创建副本密钥。要创建多区域副本 HMAC 密钥，请按照创建副本密钥的说明。

9. 请选择 Next（下一步）。

10. 为 KMS 密钥键入别名。别名名称不能以 **aws/** 开头。**aws/** 前缀由 Amazon Web Services 预留，用于在您的账户中表示 AWS 托管式密钥。

    我们建议您使用将 KMS 密钥标识为 HMAC 密钥的别名，例如 `HMAC/test-key`。这将便于您在 AWS KMS 控制台中识别 HMAC 密钥，您可以在其中按标签和别名对密钥进行排序，但不能按密钥规范或密钥用法进行排序和筛选。

    在 AWS Management Console 中创建 KMS 密钥时需要别名。使用CreateKey操作时无法指定别名，但可以使用控制台或CreateAlias操作为现有 KMS 密钥创建别名。有关更多信息，请参阅 使用别名。

11. （可选）为 KMS 密钥输入描述。

    输入一个描述，用来说明您计划保护的数据类型或计划与 KMS 密钥配合使用的应用程序。

    现在，除非密钥状态为 `Pending Deletion` 或 `Pending Replica Deletion`，否则您可以随时添加描述或更新描述。要添加、更改或删除现有客户托管密钥的描述，请在中编辑描述AWS Management Console或使用UpdateKeyDescription操作。

12. （可选）输入标签键和一个可选标签值。要向 KMS 密钥添加多个标签，请选择 Add tag（添加标签）。

    考虑添加将密钥识别为 HMAC 密钥的标签，例如 `Type=HMAC`。这将便于您在 AWS KMS 控制台中识别 HMAC 密钥，您可以在其中按标签和别名对密钥进行排序，但不能按密钥规范或密钥用法进行排序和筛选。

    在将标签添加到 AWS 资源时，AWS 可生成成本分配报告，其中按标签汇总了使用情况和成本。标签还可以用来控制对 KMS 密钥的访问。有关轮换 KMS 密钥的信息，请参阅 标记密钥 和 AWS KMS 中的 ABAC。

13. 请选择 Next（下一步）。

14. 选择可管理 KMS 密钥的 IAM 用户和角色。

> **Note**
>
> 此密钥策略将授予 AWS 账户 对此 KMS 密钥的完全控制权。此控制权允许账户管理员使用 IAM policy 授予其他主体管理 KMS 密钥的权限。有关更多信息，请参阅 the section called “默认密钥策略”。
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

15. （可选）要阻止选定 IAM 用户和角色删除此 KMS 密钥，请在页面底部的 Key deletion（密钥删除）部分中，清除 Allow key administrators to delete this key（允许密钥管理员删除此密钥）复选框。
16. 请选择 Next（下一步）。
17. 选择可将 KMS 密钥用于加密操作的 IAM 用户和角色。

> **Note**
>
> 此密钥策略将授予 AWS 账户 对此 KMS 密钥的完全控制权。此控制权允许账户管理员使用 IAM policy 授予其他主体在加密操作中使用 KMS 密钥的权限。有关更多信息，请参阅 the section called “默认密钥策略”。
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

18. （可选）您可以允许其他 AWS 账户 将此 KMS 密钥用于加密操作。为此，请在页面底部的 Other AWS 账户（其他 Amazon Web Services 账户）部分中，选择 Add another AWS 账户（添加另一个 Amazon Web Services 账户）并输入外部账户的 AWS 账户 账户标识号。要添加多个外部账户，请重复此步骤。

> **Note**
>
> 要允许外部账户中的委托人使用 KMS 密钥，外部账户的管理员必须创建提供这些权限的 IAM policy。有关更多信息，请参阅 允许其他账户中的用户使用 KMS 密钥。

19. 选择 下一步。
20. 检视您选择的密钥设置。您仍然可以返回并更改所有设置。
21. 选择 Finish（完成）以创建 HMAC KMS 密钥。

创建 HMAC KMS 密钥（AWS KMS API）

您可以使用该CreateKey操作创建 HMAC KMS 密钥。这些示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

创建 HMAC KMS 密钥时，必须指定 KeySpec 参数，该参数决定了 KMS 密钥的类型。另外，您必须指定 GENERATE_VERIFY_MAC 的 KeyUsage 值，尽管它是 HMAC 密钥的唯一有效密钥用法值。要创建多区域 HMAC KMS 密钥，添加值为 true 的 MultiRegion 参数。创建 KMS 密钥后，这些属性无法更改。

该CreateKey操作不允许您指定别名，但您可以使用该CreateAlias操作为新 KMS 密钥创建别名。我们建议您使用将 KMS 密钥标识为 HMAC 密钥的别名，例如 HMAC/test-key。这将便于您在 AWS KMS 控制台中识别 HMAC 密钥，您可以在其中按别名对密钥进行排序和筛选，但不能按密钥规范或密钥用法进行排序和筛选。

如果您尝试在不支持 HMAC 密钥的 AWS 区域 中创建 HMAC KMS 密钥，CreateKey 操作将返回 UnsupportedOperationException

以下示例使用 CreateKey 操作来创建 512 位的 HMAC KMS 密钥。

```
$ 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
    }
}
```

控制对 HMAC KMS 密钥的访问

要控制对 HMAC KMS 密钥的访问，您可以使用密钥策略，每个 KMS 密钥都需要此操作。您还可以使用 IAM policy 和授权。

AWS KMS 控制台中创建的 HMAC 密钥的原定设置密钥策略授予密钥用户调用 GenerateMac 和 VerifyMac 操作的权限。但是，它不包括设计将授权与 AWS 服务结合使用的密钥策略语句。如果您通过使用 CreateKey 操作创建 HMAC 密钥，您必须在密钥政策或 IAM policy 中指定这些权限。

您可以使用 AWS 全局条件键和 AWS KMS 条件键优化和限制对 HMAC 密钥的权限。例如，您可以使用 kms:ResourceAliases 条件键基于与 HMAC 密钥关联的别名控制对 AWS KMS 操作的访问。以下 AWS KMS 策略条件对于 HMAC 密钥的策略很有用。

- 使用 kms:MacAlgorithm 条件键，以限制主体在其调用 GenerateMac 和 VerifyMac 操作时请求的算法。例如，您可以允许主体调用 GenerateMac 操作，但仅限在请求中的 MAC 算法为 HMAC_SHA_384 时。
- 使用 kms:KeySpec 条件键，允许或阻止主体创建某些类型的 HMAC 密钥。例如，要允许委托人仅创建 HMAC 密钥，您可以允许该CreateKey操作，但使用kms:KeySpec条件仅允许具有HMAC_384密钥规范的密钥。

  您还可以使用 kms:KeySpec 条件键，根据密钥的密钥规范，控制对 KMS 密钥上的其他操作的访问。例如，您只能允许主体仅在具有 HMAC_256 密钥规范的 KMS 密钥上计划和取消密钥删除。
- 使用 kms:KeyUsage 条件键，允许或阻止主体创建任何 HMAC 密钥。例如，要允许委托人仅创建 HMAC 密钥，您可以允许该CreateKey操作，但使用kms:KeyUsage条件仅允许使用密钥的GENERATE_VERIFY_MAC密钥。

  您还可以使用 kms:KeyUsage 条件键，根据密钥的密钥用法，控制对 KMS 密钥上的其他操作的访问。例如，您可以仅允许主体在具有 GENERATE_VERIFY_MAC 密钥用法的 KMS 密钥上启用和禁用。

您也可以创建 GenerateMac 和 VerifyMac 操作的授权，它们为授权操作。对于 HMAC 密钥，不能在授权中使用加密上下文授权约束。HMAC 标签格式不支持加密上下文值。

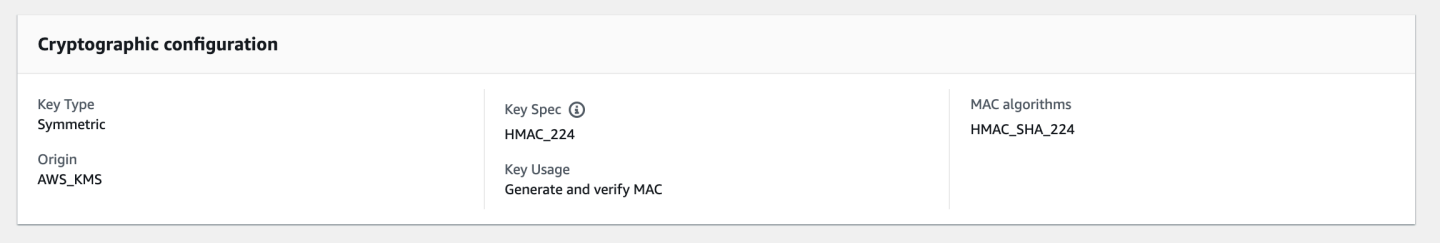
查看 HMAC KMS 密钥

您可以在 AWS KMS 控制台中或使用 DescribeKey API 查看 HMAC KMS 密钥。您可以在AWS CloudTrail日志和亚马逊 CloudWatch中监控 HMAC KMS 密钥的使用情况。有关查看 KMS 密钥的基本说明，请参阅 查看密钥。

您可以按以 HMAC 开头的密钥规范或其密钥用法（始终为Generate and verify MAC（GENERATE_VERIFY_MAC）生成和验证 MAC）区分 HMAC KMS 密钥与其他类型的 KMS 密钥。

HMAC KMS 密钥包含在 AWS KMS 控制台的 Customer managed keys（客户托管密钥）页面上的表中。但是，您无法按密钥规范或密钥用法对 KMS 密钥进行排序或筛选。为了更轻松地查找 HMAC 密钥，为其分配独特的别名或标签。然后，您可以按别名或标签进行排序或筛选。

在 HMAC KMS 密钥的 密钥详细信息页面中，您可以在 Cryptographic configuration（加密配置）选项卡上找到其配置详细信息。



中的多区域密钥 AWS KMS

AWS KMS 支持多区域密钥，这些密钥 AWS KMS keys 位于不同的 AWS 区域 位置，可以互换使用，就好像您在多个区域中使用相同的密钥一样。每组相关的多区域密钥都具有相同的密钥材料和密钥 ID，因此您可以将数据合二为一， AWS 区域 然后使用不同的密钥进行解密， AWS 区域 而无需重新加密或进行跨区域调用。 AWS KMS

与所有 KMS 密钥一样，多区域密钥永远不会处于 AWS KMS 未加密状态。您可以创建用于加密或签名的对称或非对称多区域密钥，创建用于生成和验证 HMAC 标签的 HMAC 多区域密钥，以及使用导入的密钥材料或生成的密钥材料创建多区域密钥。 AWS KMS 您必须独立管理每个多区域密钥，包括创建别名和标签、设置其密钥策略和授权以及有选择性地启用和禁用它们。您可以在可使用单区域密钥进行的所有加密操作中使用多区域密钥。

多区域密钥是一个灵活而强大的解决方案，适用于许多常见的数据安全场景。

灾难恢复

> 在备份和恢复架构中，即使发生中断，多区域密钥也允许您不间断地处理加密数据。 AWS 区域 备份区域中维护的数据可以在备份区域中解密，备份区域中新加密的数据可以在恢复该区域后在主区域中解密。

全球数据管理

在全球运营的企业需要将全球分布的数据一致地提供到各个 AWS 区域。您可以在数据所在的所有区域中创建多区域密钥，然后将密钥用作单区域密钥，而不会出现跨区域调用的延迟或在每个区域中使用不同密钥重新加密数据的成本。

分布式签名应用程序

需要跨区域签名功能的应用程序可以使用多区域非对称签名密钥以在不同的 AWS 区域一致、反复地生成同样的数字签名。

如果将证书链与单个全局信任存储 [对于单个根证书颁发机构（CA）] 及根 CA 签名的区域中间 CA 结合使用，则不需要多区域密钥。但是，如果您的系统不支持中间 CA（如应用程序签名），则可以使用多区域密钥来实现区域证书的一致性。

跨多个区域的双活应用程序

某些工作负载和应用程序可以跨越双活架构中的多个区域。对于这些应用程序，多区域密钥可以通过提供相同的密钥材料对可能跨区域边界移动的数据进行并发加密和解密操作来降低复杂性。

您可以将多区域密钥与客户端加密库结合使用，例如 AWS Encryption SDK、DynamoDB 加密客户端和 Amazon S3 客户端加密。有关在 Amazon DynamoDB 全局表和 DynamoDB 加密客户端中使用多区域密钥的示例，请参阅安全博客中的使用多区域密钥在客户端加密全球数据 AWS KMS。 AWS

AWS 与之集成的 AWS KMS用于静态加密或数字签名的服务目前将多区域密钥视为单区域密钥。他们可能会重新包装或重新加密在区域之间移动的数据。例如，甚至是在复制受多区域密钥保护的对象时，Amazon S3 跨区域复制也会在目标区域的 KMS 密钥下解密和重新加密数据。

多区域键不是全局键。创建一个多区域主键，然后将其复制到您在 AWS 分区中选择的区域。然后单独管理每个区域中的多区域键。 AWS 也 AWS KMS 不会自动代表您创建多区域密钥或将多区域密钥复制到任何区域。 AWS 托管式密钥，即 AWS 服务在您的账户中为您创建的 KMS 密钥，始终是单区域密钥。

您不能将现有的单区域密钥转换为多区域密钥。此设计可确保使用现有单区域密钥保护的所有数据都保持相同的数据驻留和数据主权属性。

对于大多数数据安全需求，区域资源的区域隔离和容错能力使标准的 AWS KMS 单区域密钥成为最合适的解决方案。但是，当您需要跨多个区域加密或对客户端应用程序中的数据进行签名时，多区域密钥可能是解决方案。

区域

除中国（北京）和中国（宁夏）外 AWS 区域 ，所有支持的地区都 AWS KMS 支持多区域密钥。

定价和配额

一组相关的多区域密钥中的每个密钥都被视为一个 KMS 密钥，用于定价和配额。AWS KMS 配额是针对账户的每个区域单独计算的。每个区域中的多区域密钥的使用和管理将计入该区域的配额。

支持的 KMS 密钥类型

您可以创建以下类型的多区域 KMS 密钥：

- 对称加密 KMS 密钥
- 非对称 KMS 密钥
- HMAC KMS 密钥
- 具有导入密钥材料的 KMS 密钥

您不能在自定义密钥存储中创建多区域密钥。

主题

- 控制对多区域密钥的访问
- 创建多区域密钥
- 查看多区域密钥
- 管理多区域密钥
- 将密钥材料导入到多区域密钥中
- 删除多区域密钥

多区域密钥的安全注意事项

仅在需要 AWS KMS 多区域密钥时才使用多区域密钥。多区域密钥为工作负载提供灵活且可扩展的解决方案，这些工作负载可在 AWS 区域 之间移动加密数据或需要跨区域访问。如果您必须跨区域共享、移动或备份受保护的数据，或者需要为在不同区域运行的应用程序创建相同的数字签名，请考虑使用多区域密钥。

但是，创建多区域密钥的过程会跨 AWS KMS内的 AWS 区域 边界移动您的密钥材料。由多区域密钥生成的密文可能会由多个地理位置的多个相关密钥进行解密。对于区域隔离的服务和资源也有很大的益

处。每个 AWS 区域 都是隔离的，独立于其他区域。区域提供容错能力、稳定性和弹性，还可以减少延迟。它们使您能够创建保持可用且不受其他区域中断影响的冗余资源。在中 AWS KMS，它们还确保每个密文只能用一个密钥解密。

多区域密钥还会引发新的安全注意事项：

- 使用多区域密钥，控制访问和强制执行数据安全策略变得更加复杂。您需要确保在多个隔离区域的密钥上对策略进行一致的审计。您需要使用策略来强制实施边界，而不是依赖单独的密钥。

  例如，您需要对数据设置策略条件，以防止一个区域的薪酬团队能够读取另一个区域的工资单数据。此外，您还必须使用访问控制来防止一个区域中的多区域密钥保护一个租户的数据，而另一个区域中的相关多区域密钥保护另一个租户的数据的情况。
- 跨区域审计密钥也更为复杂。使用多区域密钥，您需要检查和协调多个区域的审计活动，以便全面了解受保护数据的关键活动。
- 遵守数据驻留要求可能会变得更加复杂。使用隔离的区域，您可以确保数据驻留和数据主权合规性。给定区域中的 KMS 密钥只能解密该区域中的敏感数据。在一个区域中加密的数据可以保持完全保护，并且在任何其他区域都无法访问。

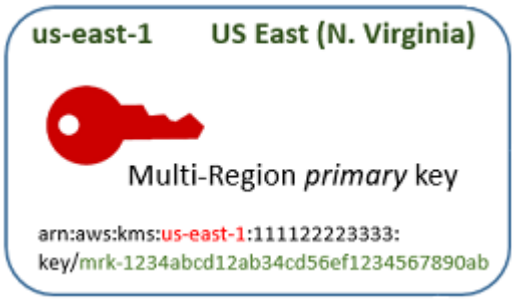
  要使用多区域密钥验证数据驻留和数据主权，您需要实施访问策略并跨多个区域编译 AWS CloudTrail 事件。

为了便于您管理多区域密钥的访问控制，复制多区域密钥 (k ms: ReplicateKey) 的权限与创建密钥的标准权限 (k ms: CreateKey) 是分开的。此外，还 AWS KMS 支持多区域密钥的多种政策条件`kms:MultiRegion`，包括允许或拒绝创建、使用或管理多区域密钥的权限`kms:ReplicaRegion`，以及限制可以将多区域密钥复制到的区域。有关更多信息，请参阅 控制对多区域密钥的访问。

多区域密钥的工作原理

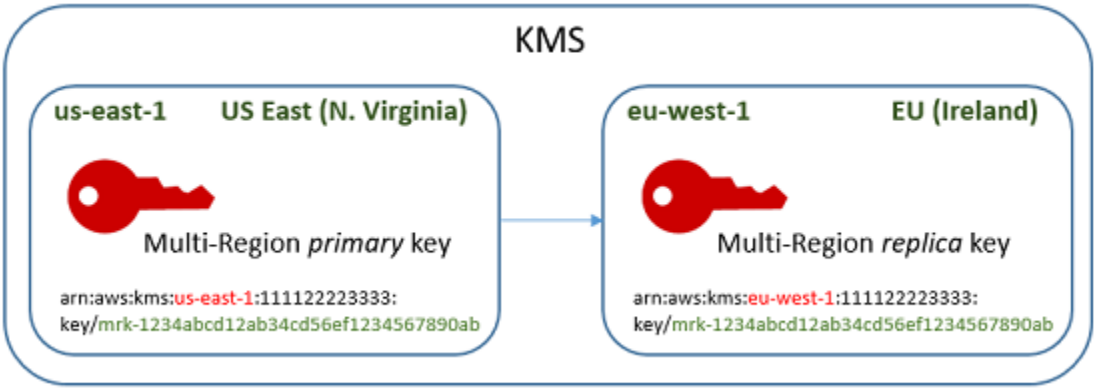
首先，您要在 AWS KMS 支持的（例如美国东部（弗吉尼亚北部）中创建 AWS 区域 对称或非对称的多区域主键。只有在创建密钥时，才能决定密钥是单区域还是多区域；以后不能更改此属性。与任何 KMS 密钥一样，您可以为多区域密钥设置密钥策略，并且可以创建授权，并添加别名和标签以进行分类和授权。（这些是独立属性，不与其他密钥共享或同步。）您可以在加密操作中使用多区域主键进行加密或签名。

您可以在 AWS KMS 控制台中创建多区域主密钥，也可以使用`MultiRegion`参数设置为的 CreateKeyAPI 来`true`创建多区域主密钥。请注意，多区域密钥具有一个以 `mrk-` 开头的独特密钥 ID。您可以使用 `mrk-` 前缀以编程方式识别 MRK。



如果您愿意，可以将多区域主键复制到同一AWS 分区 AWS 区域 中的一个或多个不同的分区，例如欧洲（爱尔兰）。完成后，在指定区域 AWS KMS 创建与主键相同的密钥 ID 和其他共享属性的副本密钥。然后，它将密钥材料安全地跨区域边界传输，并将其与目标区域中的新 KMS 密钥相关联，一切都在 AWS KMS中进行。结果会产生两个相关的多区域密钥（主键和副本密钥），它们可以互换使用。

您可以在 AWS KMS 控制台中或使用 ReplicateKeyAPI 创建多区域副本密钥。



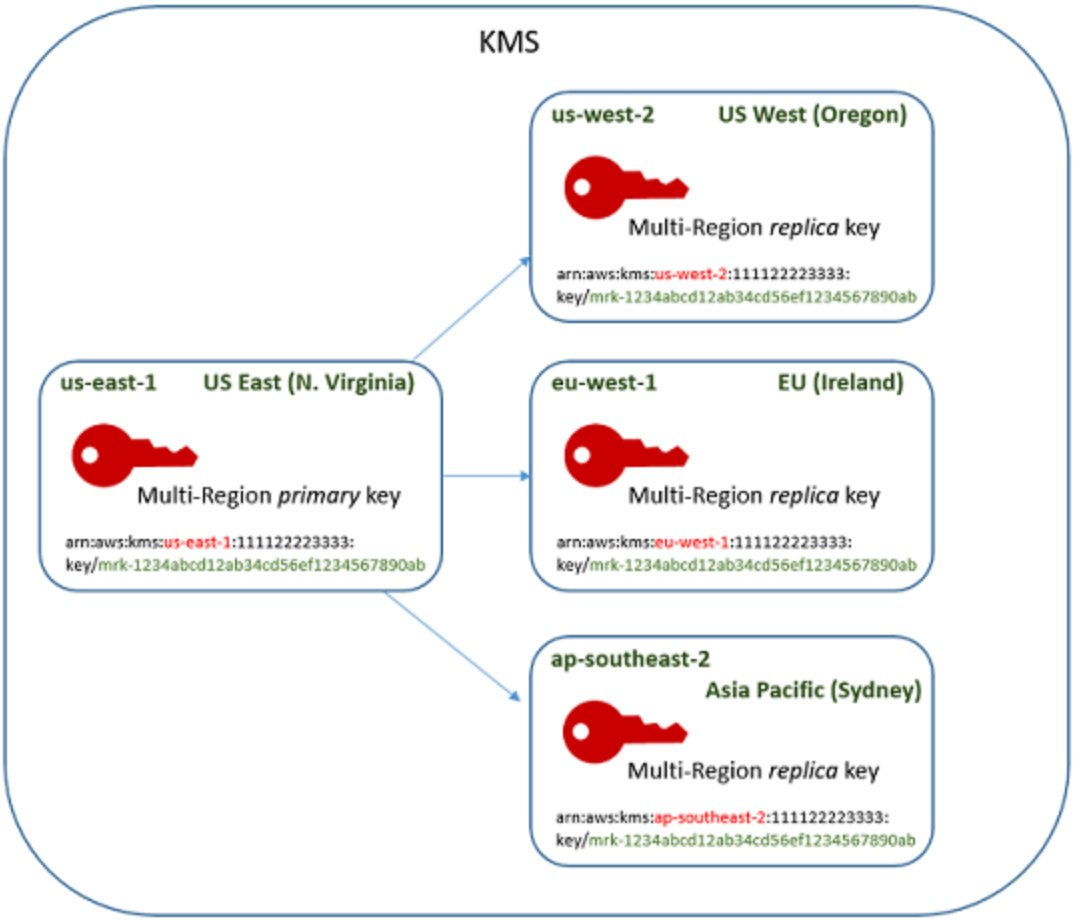
由此产生的多区域副本密钥是一个功能齐全的 KMS 密钥，具有与主键相同的共享属性。在所有其他方面，它是一个独立的 KMS 密钥，具有自己的说明、密钥策略、授权、别名和标签。启用或禁用多区域密钥对相关的多区域密钥没有影响。您可以在加密操作中独立使用主密钥和副本密钥，也可以协调它们的使用。例如，您可以使用美国东部（弗吉尼亚北部）区域的主键对数据进行加密，将数据移动到欧洲（爱尔兰）区域，然后使用副本密钥解密数据。

相关的多区域密钥具有相同的密钥 ID。它们的密钥 ARN（Amazon Resource Name）仅在 Region（区域）字段中有所不同。例如，多区域主键和副本密钥可能具有以下示例密钥 ARN。密钥 ID（密钥 ARN 中的最后一个元素）是相同的。两个密钥都具有多区域密钥的独特密钥 ID，该 ID 以 mrk- 开头。

```
Primary key: arn:aws:kms:us-
east-1:111122223333:key/mrk-1234abcd12ab34cd56ef12345678990ab
Replica key: arn:aws:kms:eu-
west-1:111122223333:key/mrk-1234abcd12ab34cd56ef12345678990ab
```

为了实现互操作性，需要具有相同的密钥 ID。加密时，将 KM AWS KMS S 密钥的密钥 ID 绑定到密文，因此只能使用该 KMS 密钥或具有相同密钥 ID 的 KMS 密钥来解密密文。此功能还使相关的多区域密钥易于识别，并且可以更轻松地互换使用它们。例如，在应用程序中使用它们时，您可以通过它们的共享密钥 ID 来引用相关的多区域密钥。然后，在必要时，指定区域或 ARN 以区分它们。

随着数据需求的变化，您可以将主键复制到同一分区 AWS 区域 中的其他分区，例如美国西部（俄勒冈）和亚太地区（悉尼）。结果会产生四个具有相同的密材料和密钥 ID 的相关多区域密钥，如下图所示。您可以独立管理密钥。您可以独立使用它们，也可以以协调的方式使用它们。例如，您可以在亚太地区（悉尼）区域使用副本密钥对数据进行加密，将数据移动到美国西部（俄勒冈）区域，然后在美国西部（俄勒冈）区域使用副本密钥对其进行解密。



多区域密钥的其他注意事项包括以下内容。

同步共享属性 -如果多区域密钥的共享属性发生变化，则 AWS KMS 会自动同步从主键到其所有副本密钥的更改。您不能请求或强制同步共享属性。 AWS KMS 为您检测并同步所有更改。但是，您可以使用 CloudTrail 日志中的SynchronizeMultiRegionKey事件来审核同步。

例如，如果您在对称的多区域主密钥上启用自动密钥轮换，则会将该设置 AWS KMS 复制到其所有副本密钥中。轮换密钥材料时，轮换将在所有相关的多区域密钥之间同步，因此它们继续具有相同的当前密钥材料，并可访问所有旧版本的密钥材料。如果创建新的副本密钥，则该密钥具有与所有相关多区域密钥相同的当前密钥材料，并可访问密钥材料的所有以前版本。有关更多信息，请参阅 轮换多区域密钥。

更改主键 — 每组多区域密钥必须只有一个主键。主键是唯一可以复制的密钥。它也是其副本密钥的共享属性的来源。但是，您可以将主键更改为副本密钥，并将其中一个副本密钥提升为主键。您可以执行此操作，以便从特定区域删除多区域主键，或将主键定位在离项目管理员更近的区域中。有关更多信息，请参阅 更新主区域。

删除多区域密钥-与所有 KMS 密钥一样，您必须计划删除多区域密钥，然后再 AWS KMS 将其删除。密钥处于待删除状态时，您无法在任何加密操作中使用它。但是，在删除多区域主键的所有副本密钥之前， AWS KMS 不会将其删除。有关更多信息，请参阅 删除多区域密钥。

概念

以下术语和概念用于多区域密钥。

多区域密钥

多区域密钥是不同 AWS 区域中具有相同的密钥 ID 和密钥材料（以及其他共享属性）的一组 KMS 密钥之一。每个多区域密钥都是一个功能齐全的 KMS 密钥，可以完全独立于其相关的多区域密钥使用。由于所有相关的多区域密钥都具有相同的密钥 ID 和密钥材料，因此它们具有互操作性，也就是说，任何密钥中的任何相关多区域密钥 AWS 区域 都可以解密由任何其他相关多区域密钥加密的密文。

您可以在创建 KMS 密钥时设置其多区域属性。您不能更改现有密钥的多区域属性。您不能将单区域密钥转换为多区域密钥，或将多区域密钥转换为单区域密钥。要将现有工作负载移动到多区域方案中，您必须重新加密数据或使用新的多区域密钥创建新的签名。

多区域密钥可以是对称的，也可以是非对称的，它可以使用 AWS KMS 密钥材料或导入的密钥材料。您不能在自定义密钥存储中创建多区域密钥。

在一组相关的多区域密钥中，任何时候都只有一个主键。您可以在其他 AWS 区域中创建该主键的副本密钥。您还可以更新主区域，从而将主键更改为副本密钥，并将指定的副本密钥更改为主键。但是，每个主键或副本密钥中只能保留一个主键或副本密钥 AWS 区域。所有区域都必须位于同一个 AWS 分区。

您可以在相同或不同的 AWS 区域中拥有多组相关多区域密钥。尽管相关的多区域密钥是可互操作的，但不相关的多区域密钥不可互操作。

主键

多区域主密钥是一个 KMS 密钥，可以复制到同一分区 AWS 区域 中的其他密钥。每组多区域密钥只有一个主键。

主键与副本密钥的区别在以下几方面：

- 只有主键可以复制。
- 主键是其副本密钥的共享属性的来源，包括密钥材料和密钥 ID。
- 您只能在主键上启用和禁用自动密钥轮换。
- 您可以随时计划删除主键。但是在删除主键的所有副本密钥之前， AWS KMS 不会删除该主键。

不过，主密钥和副本密钥在任何加密属性中都没有区别。您可以互换使用主键及其副本密钥。

您不需要复制主键。您可以像使用任何 KMS 密钥一样使用它，并在有用时复制它。但是，由于多区域密钥与单区域密钥具有不同的安全属性，因此我们建议您仅在计划复制多区域密钥时才创建多区域密钥。

副本密钥

多区域副本密钥是一个 KMS 密钥，它具有与其主键和相关副本密钥相同的密钥 ID 和密钥材料，但位于不同的 AWS 区域中。

副本密钥是功能齐全的 KMS 密钥，具有其自己的密钥策略、授权、别名、标签和其他属性。它不是主键或任何其他密钥的副本或指针。即使某个副本密钥的主键及所有相关的副本密钥都被禁用，您也可以使用该副本密钥。您还可以将副本密钥转换为主键，将主键转换为副本密钥。副本密钥被创建后，仅依赖于其主键进行密钥轮换和更新主区域。

主密钥和副本密钥在任何加密属性中都没有区别。您可以互换使用主键及其副本密钥。通过主密钥或副本密钥加密的数据可以通过相同的密钥或任何相关的主密钥或副本密钥进行解密。

复制

您可以将多区域主键复制到同一分区 AWS 区域 中的其他主键中。完成后，在指定区域 AWS KMS 创建多区域副本密钥，其密钥 ID 和其他共享属性与其主键相同。然后，它将密钥材料安全地跨区域边界传输，并将其与新的副本密钥相关联，一切都在 AWS KMS中进行。

共享属性

共享属性是与其副本密钥共享的多区域主键的属性。 AWS KMS 使用与主键相同的共享属性值创建副本密钥。然后，它会定期将主键的共享属性值与其副本密钥同步。您不能在副本密钥上设置这些属性。

以下是多区域密钥的共享属性。

- 密钥 ID — (密钥 ARN 的 Region 元素不同。)
- 密钥材料
- 密钥材料源
- 密钥规范和加密算法
- 密钥用法
- 自动密钥轮换 — 您只能在主键上启用和禁用自动密钥轮换。将使用共享密钥材料的所有版本创建新的副本密钥。有关更多信息，请参阅 轮换多区域密钥。
- 按需轮换-只能对主键执行按需轮换。将使用共享密钥材料的所有版本创建新的副本密钥。有关更多信息，请参阅 轮换多区域密钥。

您还可以将相关多区域密钥的主名称和副本名称视为共享属性。当您创建新的副本密钥或更新主密钥时，会将更改 AWS KMS 同步到所有相关的多区域密钥。完成这些更改后，所有相关的多区域密钥都会准确列出其主键和副本密钥。

多区域密钥的所有其他属性都是独立属性，包括说明、密钥策略、授权、启用和禁用的密钥状态、别名和标签。您可以在所有相关的多区域密钥上为这些属性设置相同的值，但如果更改独立属性的值，AWS KMS 不会同步它。

您可以跟踪多区域密钥的共享属性的同步情况。在您的 AWS CloudTrail 日志中，查找该SynchronizeMultiRegionKey事件。

控制对多区域密钥的访问

您可以在合规性、灾难恢复和备份场景中使用多区域密钥，这些场景在使用单区域密钥的情况下更为复杂。但是，由于多区域密钥的安全属性与单区域密钥的安全属性明显不同，我们建议在授权创建、管理和使用多区域密钥时务必谨慎。

> **Note**
>
> 在 `Resource` 字段中包通配符的现有 IAM policy 语句现在同时应用于单区域密钥和多区域密钥。要将其限制为单区域 KMS 密钥或多区域密钥，请使用 k ms: MultiRegion 条件密钥。

使用您的授权工具防止在单区域足够的任何情况下创建和使用多区域密钥。允许委托人仅将多区域密钥复制到需要它们的 AWS 区域。仅向需要多区域密钥的委托人授予多区域密钥权限，并且仅为需要它们的任务授予其权限。

您可以使用密钥政策、IAM policy 和授权来允许 IAM 委托人在您的 AWS 账户 中管理和使用多区域密钥。每个多区域密钥都是一个独立的资源，具有唯一的密钥 ARN 和密钥策略。您需要为每个密钥建立和维护密钥政策，并确保新的和现有的 IAM policy 实施您的授权策略。

主题

- 多区域密钥的授权基础知识
- 授权多区域密钥管理员和用户
- 授权 AWS KMS 同步多区域密钥

多区域密钥的授权基础知识

为多区域密钥设计密钥政策和 IAM policy 时，请考虑以下原则。

- 密钥策略 — 每个多区域密钥都是一个独立的 KMS 密钥资源，具有自己的密钥策略。您可以将相同或不同的密钥策略应用于相关多区域密钥集中的每个密钥。密钥策略不是多区域密钥的共享属性。AWS KMS 不会在相关的多区域密钥之间复制或同步密钥策略。

  当您在 AWS KMS 控制台中创建副本密钥时，为方便起见，控制台将显示主密钥的当前密钥策略。您可以使用此密钥策略、对其进行编辑或删除和替换。但是，即使您接受主密钥策略不变，AWS KMS 也不会同步策略。例如，如果您更改主密钥的密钥策略，则副本密钥的密钥策略将保持不变。
- 默认密钥策略-使用CreateKey和`ReplicateKey`操作创建多区域密钥时，除非您在请求中指定密钥策略，否则将应用默认密钥策略。这与应用于单区域密钥的默认密钥策略相同。
- IAM policy — 与所有 KMS 密钥一样，只要当密钥政策允许时，您才可以使用 IAM policy 来控制对多区域密钥的访问。IAM policy 在默认情况下适用于所有 AWS 区域。但是，您可以使用条件键（例如 a ws: RequestedRegion ）来限制对特定区域的权限。

要创建主密钥和副本密钥，委托人必须对应用于创建密钥的区域的 IAM policy 具有 `kms:CreateKey` 权限。

- 授权 — AWS KMS 授权是区域性的。每个授权都允许对一个 KMS 密钥的权限。您可以使用授权来允许对多区域主密钥或副本密钥的权限。但是，您不能使用单个授权来允许对多个 KMS 密钥的权限，即使它们是相关的多区域密钥。
- 密钥 ARN — 每个多区域密钥都有一个唯一的密钥 ARN。相关多区域密钥的密钥 ARN 具有相同的分区、账户和密钥 ID，但区域不同。

  要将 IAM policy 语句应用于特定的多区域密钥，请使用其密钥 ARN 或包含该区域的密钥 ARN 模式。要将 IAM policy 语句应用于所有相关多区域密钥，请在 ARN 的区域元素中使用通配符 (*)，如下例所示。

```
{
  "Effect": "Allow",
  "Action": [
    "kms:Describe*",
    "kms:List*"
  ],
  "Resource": {
      "arn:aws:kms:*::111122223333:key/mrk-1234abcd12ab34cd56ef1234567890ab"
  }
}
```

  要将策略声明应用于您的所有多区域密钥AWS 账户，您可以使用 k ms: MultiRegion 策略条件或包含独特`mrk-`前缀的密钥 ID 模式。

- 服务相关角色-创建多区域主键的委托人必须拥有 iam: 权限。CreateServiceLinkedRole

  为了同步相关多区域密钥的共享属性，AWS KMS 会代入 IAM 服务相关角色。在您创建多区域主密钥的任何时候，AWS KMS 都会在 AWS 账户 中创建服务相关角色。（如果角色存在，AWS KMS 将重新创建它，这没有任何有害影响。）该角色在所有区域中都有效。AWS KMS要允许创建（或重新创建）服务相关角色，创建多区域主键的委托人必须拥有 iam: 权限。CreateServiceLinkedRole

授权多区域密钥管理员和用户

创建和管理多区域密钥的委托人需要在主区域和副本区域中具有以下权限：

- `kms:CreateKey`

- kms:ReplicateKey
- kms:UpdatePrimaryRegion
- iam:CreateServiceLinkedRole

创建主密钥

要创建多区域主密钥，委托人需要在主密钥所在区域有效的 IAM 策略中的 kms: CreateKey 和 iam: CreateServiceLinkedRole 权限。具有这些权限的委托人可以创建单区域和多区域密钥，除非您限制其权限。

该iam:CreateServiceLinkedRole权限允许AWS KMS创建AWSServiceRoleForKeyManagementServiceMultiRegionKeys角色以同步相关多区域密钥的共享属性。

例如，此 IAM policy 允许委托人创建任何类型的 KMS 密钥。

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

要允许或拒绝创建多区域主密钥的权限，请使用 k ms: MultiRegion 条件密钥。有效值为 true（多区域密钥）或 false（单区域密钥）。例如，以下 IAM policy 语句使用 Deny 操作与 kms:MultiRegion 条件键来防止委托人创建多区域密钥。

```
{
  "Version": "2012-10-17",
  "Statement":{
      "Action":"kms:CreateKey",
      "Effect":"Deny",
      "Resource":"*",
      "Condition": {
          "Bool": "kms:MultiRegion": true
```

```
      }
  }
}
```

复制密钥

要创建多区域副本密钥，委托人需要以下权限：

- km ReplicateKey s：主密钥的密钥策略中的权限。
- kms：在副本密钥区域有效的 IAM 策略中的CreateKey权限。

允许这些权限时请谨慎。它们允许委托人创建 KMS 密钥和授权其使用的密钥策略。kms:ReplicateKey 权限还授权跨 AWS KMS 内的区域边界传输密钥材料。

要限制可以复制多区域密钥的范围，请使用 k ms: ReplicaRegion 条件密钥。AWS 区域它只限制 kms:ReplicateKey 权限。否则，会没有效果。例如，以下密钥策略允许委托人复制该主密钥，但仅限在指定区域中进行。

```
{
  "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"
      ]
    }
  }
}
```

更新主区域

授权的委托人可以将副本密钥转换为主密钥，从而将以前的主密钥更改为副本密钥。该操作称为更新主区域。要更新主区域，委托人需要两个区域的 kms: UpdatePrimaryRegion 权限。您可以在密钥政策或 IAM policy 中提供这些权限。

- 主密钥上的 kms:UpdatePrimaryRegion。此权限必须在主密钥区域中有效。
- 副本密钥上的 kms:UpdatePrimaryRegion。此权限必须在副本密钥区域中有效。

例如，以下密钥策略向可以担任管理员角色的用户授予更新 KMS 密钥的主区域的权限。此 KMS 密钥可以是此操作中的主密钥或副本密钥。

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

要限制AWS 区域可以托管主密钥的，请使用 k ms: PrimaryRegion 条件密钥。例如，以下 IAM policy 语句允许委托人在 AWS 账户 中更新多区域密钥的主区域，但仅当新的主区域是指定区域之一时才可以。

```
{
  "Effect": "Allow",
  "Action": "kms:UpdatePrimaryRegion",
  "Resource": {
      "arn:aws:kms:*:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": {
      "kms:PrimaryRegion": [
         "us-west-2",
         "sa-east-1",
         "ap-southeast-1"
      ]
    }
  }
}
```

使用和管理多区域密钥

默认情况下，有权在 AWS 账户 和区域中使用和管理 KMS 密钥的委托人也有权使用和管理多区域密钥。但是，您可以使用 k ms: MultiRegion 条件密钥来仅允许单区域密钥或仅允许多区域密钥。或者

使用 k ms: MultiRegionKeyType 条件密钥仅允许多区域主键或仅允许副本密钥。两个条件密钥都控制对CreateKey操作和使用现有 KMS 密钥的任何操作（例如 Enc rypt 或）的访问权限EnableKey。

以下示例 IAM policy 语句使用 kms:MultiRegion 条件键，以防委托人使用或管理任何多区域密钥。

```
{
  "Effect": "Deny",
  "Action": "kms:*",
  "Resource": "*",
  "Condition": {
    "Bool": "kms:MultiRegion": true
  }
}
```

此示例 IAM policy 语句使用 kms:MultiRegionKeyType 条件，以允许委托人计划和取消删除密钥，但仅限于多区域副本密钥。

```
{
  "Effect": "Allow",
  "Action": [
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": {
      "arn:aws:kms:us-west-2:111122223333:key/*"
  },
  "Condition": {
    "StringEquals": "kms:MultiRegionKeyType": "REPLICA"
  }
}
```

授权 AWS KMS 同步多区域密钥

为了支持多区域密钥、AWS KMS 使用 IAM 服务相关角色。这个角色为 AWS KMS 授予同步共享属性所需的权限。您可以在AWS CloudTrail日志中查看记录AWS KMS同步共享属性的SynchronizeMultiRegionKey CloudTrail 事件。

关于多区域密钥的服务相关角色

服务相关角色是一种 IAM 角色，该角色可向一个 AWS 服务提供代表您调用其他 AWS 服务的权限。该角色旨在使您能够更轻松地使用多项集成式 AWS 服务的功能，而无需创建和维护复杂的 IAM policy。

对于多区域密钥，使用策略AWS KMS创建AWSServiceRoleForKeyManagementServiceMultiRegionKeys服务相关角色。AWSKeyManagementServiceMultiRegionKeysServiceRolePolicy此策略将授予角色 `kms:SynchronizeMultiRegionKey` 权限，从而允许它同步多区域密钥的共享属性。

由于AWSServiceRoleForKeyManagementServiceMultiRegionKeys服务相关角色仅受信任`mrk.kms.amazonaws.com`，因此AWS KMS只能担任此服务相关角色。此角色仅限于 AWS KMS 同步多区域共享属性所需的操作。它不会向 AWS KMS 提供任何额外权限。例如，AWS KMS 无权创建、复制或删除任何 KMS 密钥。

有关 AWS 服务如何使用服务相关角色的更多信息，请参阅 IAM 用户指南中的使用服务相关角色。

创建服务相关角色

AWS KMS如果您创建多区域密钥AWS 账户时会自动在中创建AWSServiceRoleForKeyManagementServiceMultiRegionKeys服务相关角色（如果该角色尚不存在）。您无法直接创建或重新创建此服务相关角色。

编辑服务相关角色描述

您无法编辑AWSServiceRoleForKeyManagementServiceMultiRegionKeys服务相关角色中的角色名称或策略声明，但可以编辑角色描述。有关说明，请参阅 IAM 用户指南中的编辑服务相关角色。

删除服务相关角色

AWS KMS不会从您的中删除AWSServiceRoleForKeyManagementServiceMultiRegionKeys服务相关角色AWS 账户，也无法将其删除。但是，除非您的AWS 账户和区域中有多区域密钥，否则AWS KMS不会代入该AWSServiceRoleForKeyManagementServiceMultiRegionKeys角色或使用其任何权限。

创建多区域密钥

您可以在控制台中或使用 AWS KMS API 创建多区域密钥。

您在此过程中设置的多区域属性是不可改变的。您不能将单区域密钥转换为多区域密钥，或将多区域密钥转换为单区域密钥。

主题

- 创建多区域主密钥
- 创建多区域副本密钥

创建多区域主密钥

您可以在 AWS KMS 控制台中或使用 AWS KMS API 创建多区域主密钥。您可以在 AWS KMS 支持多区域密钥所在的任何 AWS 区域 中创建主密钥。

要创建多区域主密钥，委托人需要与创建任何 KMS 密钥相同的权限，包括 IAM 策略中的 kms: CreateKey 权限。委托人还需要 iam: CreateServiceLinkedRole 权限。您可以使用 kms: MultiRegionKeyType 条件密钥来允许或拒绝创建多区域主密钥的权限。

这些指令会创建一个具有 AWS KMS 生成的密钥材料的多区域主密钥。要创建带已导入密钥材料的多区域主密钥，请参阅 创建带导入的密钥材料的主密钥。

主题

创建多区域主密钥（控制台）

要在 AWS KMS 控制台中创建多区域主密钥，请使用用于创建任何 KMS 密钥的相同过程。您可以在高级选项中选择多区域密钥。有关完整说明，请参阅创建密钥。

> **Important**
>
> 不要在别名、描述或标签中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择 Create key。
5. 选择对称或非对称密钥类型。对称密钥为原定设置。

   您可以创建多区域对称密钥和非对称密钥，包括对称的多区域 HMAC KMS 密钥。
6. 选择您的密钥使用方法。Encrypt and decrypt（加密和解密）是原定设置。

有关帮助信息，请参阅 the section called “创建密钥”、the section called “创建非对称 KMS 密钥” 或 the section called “创建 HMAC 密钥”。

7. 展开 Advanced options (高级选项)。
8. 在密钥材料源下，要使 AWS KMS 生成主密钥和副本密钥将共享的密钥材料，请选择 KMS。如果您 将密钥材料导入 到主密钥和副本密钥中，请选择 External (Import key material) [外部（导入密钥材料）]。
9. 在多区域复制下，选择 Allow this key to be replicated into other Regions（允许将此密钥复制到其他区域中）。

   创建 KMS 密钥之后，您无法再更改此设置。
10. 为主密钥键入别名。

    别名不是多区域密钥的共享属性。您可以为多区域主密钥及其副本密钥指定相同的别名或不同的别名。AWS KMS 不同步多区域密钥的别名。

    > **Note**
    >
    > 添加、删除或更新别名可以允许或拒绝对 KMS 密钥的权限。有关详细信息，请参阅 AWS KMS 中的 ABAC 和 使用别名控制对 KMS 密钥的访问。

11. （可选）键入主密钥的描述。

    描述不是多区域密钥的共享属性。您可以为多区域主密钥及其副本密钥指定相同的描述或不同的描述。AWS KMS 不同步多区域密钥的密钥描述。
12. (可选) 键入标签键和一个可选标签值。要向主密钥分配多个标签，请选择 Add tag（添加标签）。

    标签不是多区域密钥的共享属性。您可以为多区域主密钥及其副本密钥指定相同的标签或不同的标签。AWS KMS 不同步多区域密钥的标签。您可以随时更改 KMS 密钥上的标签。

    > **Note**
    >
    > 标记或取消标记 KMS 密钥可以允许或拒绝对 KMS 密钥的权限。有关详细信息，请参阅 AWS KMS 中的 ABAC 和 使用标签控制对 KMS 密钥的访问。

13. 选择可管理主密钥的 IAM 用户和角色。

> **Note**
>
> IAM 策略可以向其他 IAM 用户和角色授予管理 KMS 密钥的权限。
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

此步骤将开始为主密钥创建密钥策略的过程。密钥策略不是多区域密钥的共享属性。您可以为多区域主密钥及其副本密钥指定相同的密钥策略或不同的密钥策略。AWS KMS 不同步多区域密钥的密钥策略。条件密钥值必须遵守密钥策略和 IAM policy 的字符和编码规则。

14. 完成创建密钥策略的步骤，包括选择密钥用户。审查密钥策略后，请选择 Finish（完成）以创建 KMS 密钥。

创建多区域主密钥 (AWS KMS API)

要创建多区域主键，请使用CreateKey操作。使用带 `True` 值的 `MultiRegion` 参数。

例如，以下命令在调用者的 AWS 区域 (us-east-1) 中创建多区域主密钥。它接受所有其他属性的默认值，包括密钥策略。多区域主密钥的默认值与所有其他 KMS 密钥的默认值相同，包括默认密钥策略。此过程将创建一个对称加密密钥，即默认 KMS 密钥。

响应包含 `MultiRegion` 元素和 `MultiRegionConfiguration` 元素，其中包含典型的子元素和不含副本密钥的多区域主密钥的值。多区域密钥的密钥 ID 总是以 `mrk-` 开头。

> **Important**
>
> 不要在 `Description` 或 `Tags` 字段中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

```
$ 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": [ ]
      }
    }
}
```

创建多区域副本密钥

您可以在AWS KMS控制台、使用ReplicateKey操作或使用AWS CloudFormation模板创建多区域副本密钥。您不能使用该CreateKey操作来创建副本密钥。

您可以使用这些步骤复制任何多区域主密钥，包括对称加密 KMS 密钥，非对称 KMS 密钥，或者 HMAC KMS 密钥。

此操作完成后，新的副本密钥具有暂时性的密钥状态 `Creating`。创建新副本密钥的过程完成几秒钟后，此密钥状态将变为`Enabled`（或 PendingImport）。当密钥状态为 `Creating` 时，您可以管理该密钥，但不能将其用于加密操作。如果您以编程方式创建和使用副本密钥，请在使用副本密钥之前重试`KMSInvalidStateException`或调DescribeKey用检查其`KeyState`值。

如果误删了副本密钥，您可以使用此过程来重新创建副本密钥。如果您在同一区域中复制相同的主密钥，则您创建的新副本密钥将具有与原始副本密钥相同的共享属性。

> **Important**
>
> 不要在别名、描述或标签中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

了解更多

- 要创建带已导入密钥材料的多区域副本密钥，请参阅 创建带导入的密钥材料的副本密钥。
- 要使用AWS CloudFormation模板创建副本密钥，请参阅AWS CloudFormation用户指南AWS::KMS::ReplicaKey中的。

主题

副本区域

您通常会基于您的业务模式和法规要求选择将多区域密钥复制到 AWS 区域 中。例如，您可以将密钥复制到保留资源的区域中。或者，为了符合灾难恢复要求，您可以将密钥复制到地理位置偏远的区域中。

以下是对副本区域的 AWS KMS 要求。如果您选择的区域不符合这些要求，则尝试复制密钥失败。

- 每个区域一个相关的多区域密钥 — 您不能在与主密钥相同的区域中创建副本密钥，也不能在与主密钥的另一个副本相同的区域中创建副本密钥。

  如果您尝试在已具有该主密钥副本的区域中复制主密钥，则尝试会失败。如果区域中的当前副本密钥处于 `PendingDeletion` 密钥状态，您可以取消副本密钥删除或者等待副本密钥被删除。
- 同一区域中的多个不相关的多区域密钥 — 您可以在同一个区域中拥有多个不相关的多区域密钥。例如，您可以在 `us-east-1` 区域中拥有两个多区域主密钥。每个主密钥在 `us-west-2` 区域中都可以有一个副本密钥。
- 同一分区中的区域 — 副本密钥区域必须位于与主密钥区域相同的 AWS 分区中。
- 必须启用区域 — 如果某个区域默认已禁用，则无法在该区域中创建任何资源，直到为您的 AWS 账户 启用该区域为止。

创建副本密钥（控制台）

在 AWS KMS 控制台中，您可以在同一操作中创建多区域主密钥的一个或多个副本。

此过程类似于在控制台中创建标准的单区域 KMS 密钥。但是，由于副本密钥基于主密钥，因此您不能为共享属性选择值，例如密钥规范（对称或非对称）、密钥用法或密钥来源。

您可以指定不共享的属性，包括别名、标签、描述和密钥策略。为方便起见，控制台会显示主密钥的当前属性值，但您可以更改它们。即使您保留主密钥值，AWS KMS 也不会保持这些值同步。

> **Important**
>
> 不要在别名、描述或标签中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择多区域主密钥的密钥 ID 或别名。此操作将打开 KMS 密钥的密钥详细信息页面。

   要识别多区域主密钥，请使用右上角的工具图标将 Regionality（区域性）列添加到表中。
5. 选择 Regionality（区域性）选项卡。
6. 在 Related multi-Region keys（相关的多区域密钥）部分中，选择 Create new replica keys（创建新的副本密钥）。

   Related multi-Region keys（相关的多区域密钥）部分显示主密钥及其副本密钥的区域。您可以使用此显示来帮助您为新副本密钥选择区域。
7. 选择一个或多个 AWS 区域。此过程将在您选择的每个区域中创建一个副本密钥。

   菜单仅包含与主密钥处于相同 AWS 分区中的区域。已具有相关多区域密钥的区域显示出来，但不可选。您可能没有权限将密钥复制到菜单上的所有区域。

   完成选择 Regions（区域）后，关闭菜单。将显示您选择的区域。要取消复制到某个区域，请选择 Region（区域）名称旁边的 X。
8. 为副本密钥键入别名。

控制台将显示主密钥的当前别名之一，但您可以对其进行更改。您可以为多区域主密钥及其副本密钥指定相同的别名或不同的别名。别名不是多区域密钥的共享属性。AWS KMS 不同步多区域密钥的别名。

添加、删除或更新别名可以允许或拒绝对 KMS 密钥的权限。有关详细信息，请参阅 AWS KMS 中的 ABAC 和 使用别名控制对 KMS 密钥的访问。

9. （可选）键入副本密钥的描述。

   控制台将显示主密钥的当前描述，但您可以对其进行更改。描述不是多区域密钥的共享属性。您可以为多区域主密钥及其副本密钥指定相同的描述或不同的描述。AWS KMS 不同步多区域密钥的密钥描述。

10. (可选) 键入标签键和一个可选标签值。要为副本密钥分配多个标签，请选择 Add tag（添加标签）。

    控制台将显示当前附加到主密钥的标签，但您可以更改它们。标签不是多区域密钥的共享属性。您可以为多区域主密钥及其副本密钥指定相同的标签或不同的标签。AWS KMS 不同步多区域密钥的标签。

    标记或取消标记 KMS 密钥可以允许或拒绝对 KMS 密钥的权限。有关详细信息，请参阅 AWS KMS 中的 ABAC 和 使用标签控制对 KMS 密钥的访问。

11. 选择可管理副本密钥的 IAM 用户和角色。

    > **Note**
    >
    > IAM policy 可以向其他 IAM 用户和角色授予管理副本密钥的权限。
    > IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

    此步骤将开始为副本密钥创建密钥策略的过程。控制台将显示主密钥的当前密钥策略，但您可以对其进行更改。密钥策略不是多区域密钥的共享属性。您可以为多区域主密钥及其副本提供相同的密钥策略或不同的密钥策略。AWS KMS 不同步密钥策略。您可以随时更改任何 KMS 密钥的密钥策略。

12. 完成创建密钥策略的步骤，包括选择密钥用户。审查密钥策略后，请选择 Finish（完成）以创建副本密钥。

创建副本密钥 (AWS KMS API)

要创建多区域副本密钥，请使用ReplicateKey操作。您不能使用该CreateKey操作来创建副本密钥。此操作一次创建一个副本密钥。您指定的区域必须符合副本密钥的区域要求。

当您使用 ReplicateKey 操作时，无需为多区域密钥的任何共享属性指定值。共享属性值从主密钥复制并保持同步。但是，您可以为未共享的属性指定值。否则，AWS KMS 将为 KMS 密钥应用标准默认值，而不是主密钥的值。

> **Note**
>
> 如果您还没有为 Description、KeyPolicy 或 Tags 参数指定值，AWS KMS 将创建带空字符串描述的副本密钥、默认的密钥政策，不带标签。
> 不要在 Description 或 Tags 字段中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

例如，以下命令在亚太地区（悉尼）区域 (ap-southeast-2) 中创建一个多区域副本密钥。此副本密钥基于美国东部（弗吉尼亚北部）区域 (us-east-1) 中的主密钥建模，它由 KeyId 参数的值进行标识。此示例接受所有其他属性的默认值，包括密钥策略。

响应描述了新的副本密钥。它包含共享属性的字段，例如 KeyId、KeySpec、KeyUsage 和密钥材料来源 (Origin)。它还包括独立于主密钥的属性，例如 Description、密钥策略 (ReplicaKeyPolicy) 和标签 (ReplicaTags)。

响应还包括主密钥的密钥 ARN 和区域及其所有副本密钥，包括刚刚在 ap-southeast-2 区域中创建的密钥。在此示例中，ReplicaKey 元素表明此主密钥已在欧洲（爱尔兰）区域 (eu-west-1) 复制。

```
$ 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": []
}
```


查看多区域密钥

您可以在 AWS KMS 控制台中和通过使用 AWS KMS API 操作来查看单区域和多区域密钥。

主题

- 在控制台中查看多区域区域

- 在 API 中查看多区域秘钥

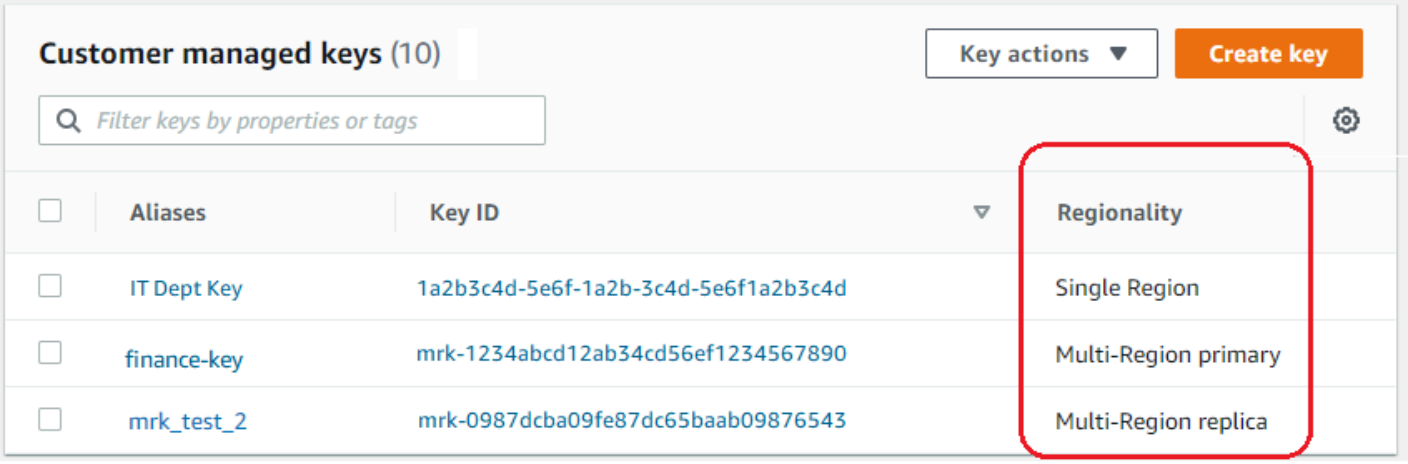
在控制台中查看多区域区域

在 AWS KMS 控制台中，您可以查看所选区域中的 KMS 密钥。但是，如果您有多区域密钥，则可以查看其在其他 AWS 区域 中的相关多区域密钥。

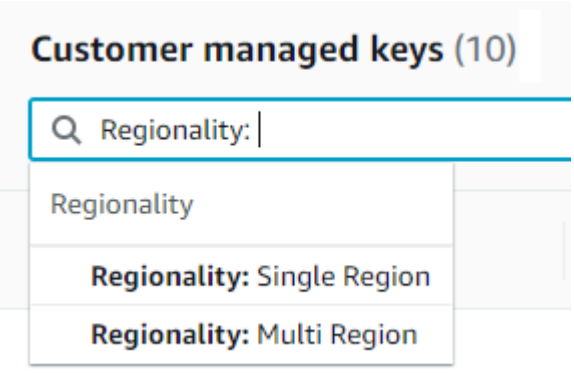
AWS KMS 控制台中的客户托管式密钥表仅显示所选区域中的 KMS 密钥。您可以查看所选区域中的多区域主密钥和副本密钥。要更改 AWS 区域，请使用页面右上角的区域选择器。

AWS 托管式密钥 表没有区域性功能，因为 AWS 托管式密钥 始终是单区域密钥。

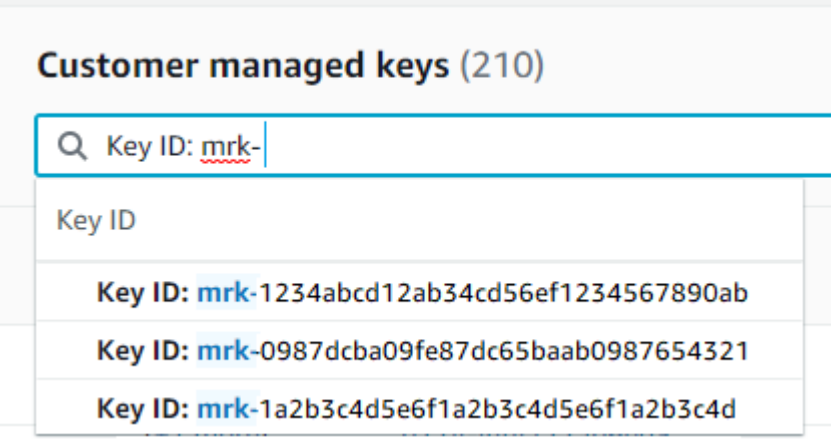
- 为了便于标识多区域密钥，请将 Regionality（区域性）列添加到您的密钥表中。有关帮助信息，请参阅 自定义您的 KMS 密钥表。



- 要在密钥表中仅显示单区域密钥或仅显示多区域密钥，请按每个密钥的 Regionality（区域性）属性筛选您的密钥。有关帮助信息，请参阅 对您的 KMS 密钥进行排序和筛选。



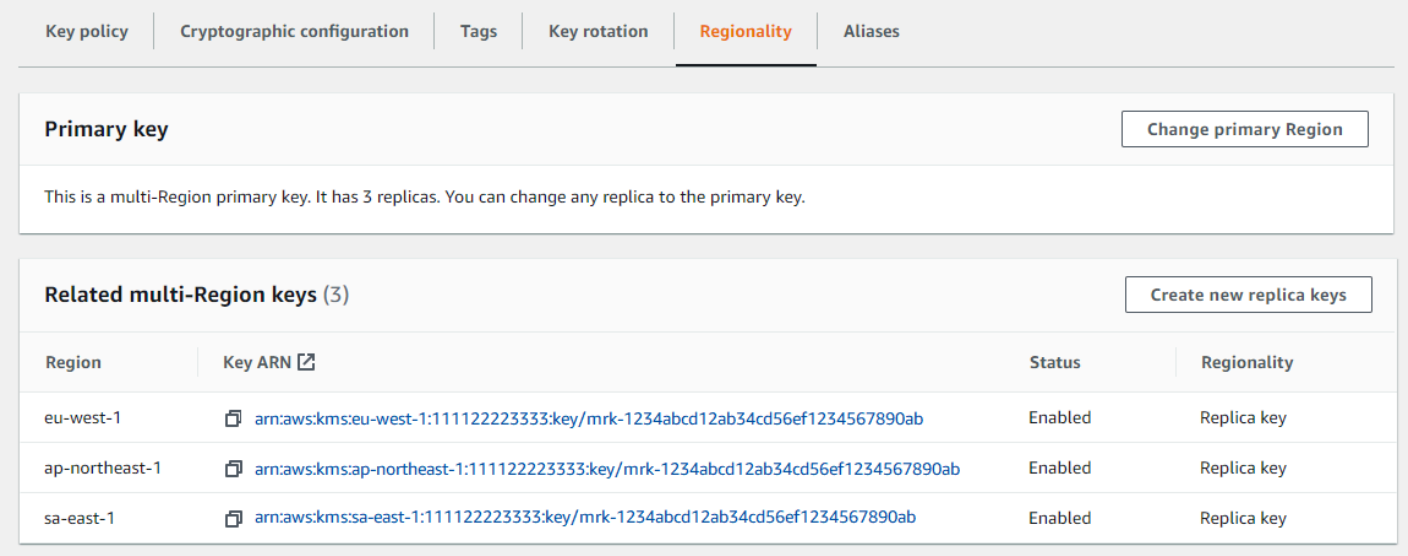
- 您还可以对您的客户托管密钥表进行排序，并筛选其中是否有独特的 mrk- 密钥 ID 前缀。



- 有关多区域主密钥或副本密钥的详细信息，请转至该密钥的详细信息页面，然后选择 Regionality（区域性）选项卡。

  主密钥的 Regionality（区域性）选项卡包括 Change primary Region（更改主区域）和 Create new replica keys（创建新的副本密钥）按钮。（副本密钥的 Regionality（区域性）选项卡没有任何按钮。）Related multi-Region keys（相关的多区域密钥）部分列出了与当前密钥相关的所有多区域密钥。如果当前密钥是副本密钥，则此列表将包括主密钥。

  如果您从相关的多区域密钥表中选择相关的多区域密钥，AWS KMS 控制台更改为所选密钥的区域，并打开密钥的详细信息页面。例如，如果您从下面的示例 Related multi-Region keys（相关多区域密钥）部分中选择 `sa-east-1` 区域中的副本密钥，AWS KMS 控制台将更改为 `sa-east-1` 区域，以显示该副本密钥的详细信息页面。您可以执行此操作来查看副本密钥的别名或密钥策略。要再次更改区域，请使用页面右上角的 Region selector（区域选择器）。



在 API 中查看多区域秘钥

要在 AWS KMS API 中查看多区域密钥，请使用DescribeKey操作。它将显示指定的密钥及其所有相关的多区域密钥。

与 AWS KMS 控制台相同的是，AWS KMS API 操作是区域性的。例如，当您调用ListKeys或ListAliases操作时，它们仅返回当前或指定区域中的资源。但是，当您对多区域密钥调用 DescribeKey 操作时，响应将包括其他 AWS 区域 中的所有相关多区域密钥。

例如，下面的 DescribeKey 请求将获取有关亚太区域（东京）(ap-northeast-1) 区域中示例多区域副本密钥的详细信息。

```
$ aws kms describe-key \
        --key-id arn:aws:kms:ap-northeast-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab \
        --region ap-northeast-1
```

响应中的大部分 KeyMetadata 描述了请求主题所在的的亚太地区（东京）区域中的副本密钥。但是，MultiRegionConfiguration 元素描述了美国西部（俄勒冈）(us-west-2) 区域中的主密钥及其在其他 AWS 区域 中的副本密钥，包括亚太地区（东京）区域中的副本。DescribeKey 会为所有相关的多区域密钥返回相同的 MultiRegionConfiguration 值。

```
{
    "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"
                }
            ]
        }
    }
}
```

管理多区域密钥

对于大多数操作，您需要以与使用和管理单区域密钥相同的方法管理多区域密钥。您可以启用和禁用密钥、设置和更新别名、密钥策略、授权和标签。但是，多区域密钥的管理在以下方面有所不同。

- 您可以更新主区域。这会将其中一个副本密钥更改为主密钥，将当前主密钥更改为副本密钥。
- 您仅在主密钥上管理自动密钥轮换。
- 您可以从任何相关的主密钥或副本密钥中获取非对称多区域密钥的公有密钥。

您在创建 KMS 密钥时设置的多区域属性为不可改变。您不能将单区域密钥转换为多区域密钥，或将多区域密钥转换为单区域密钥。

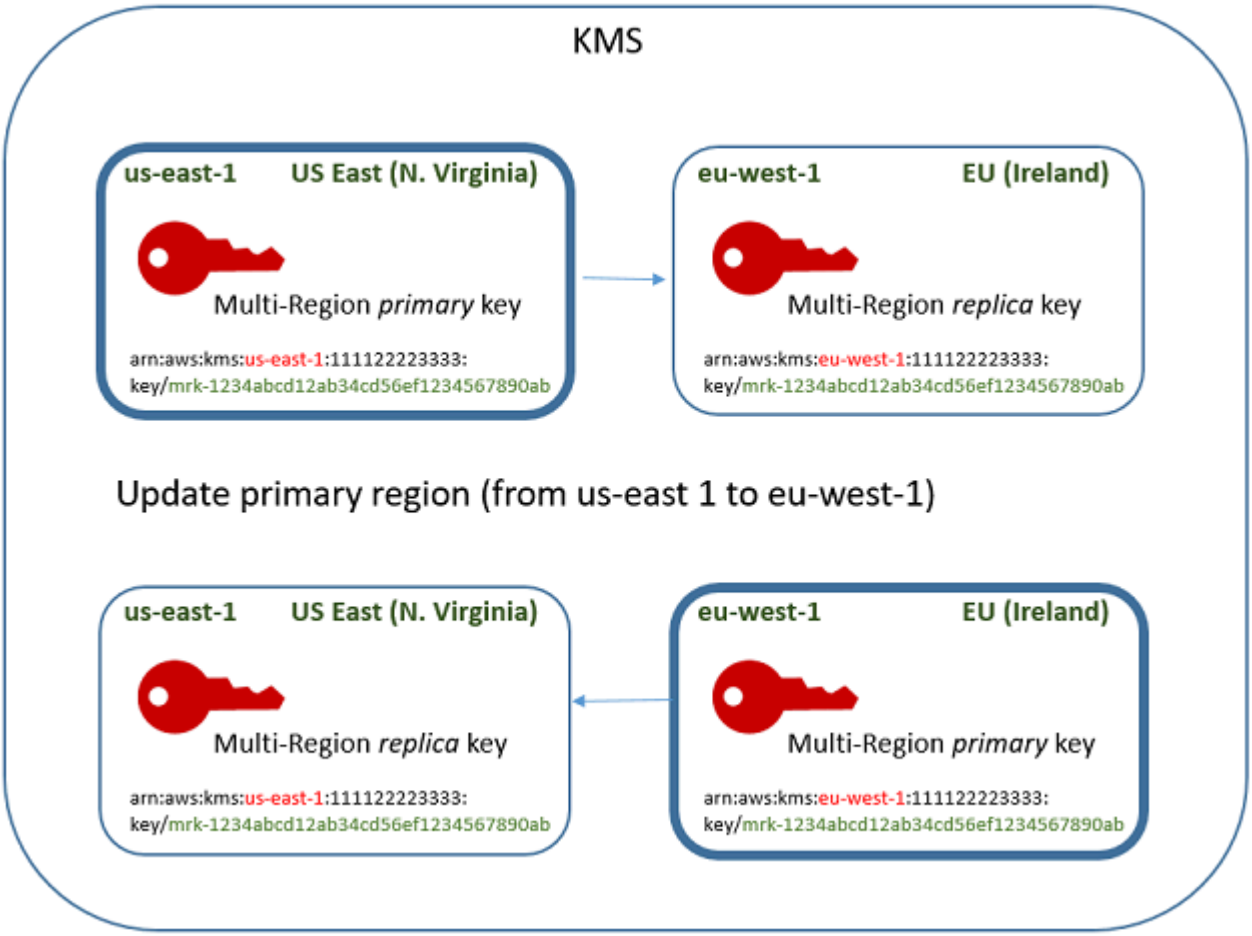
更新主区域

每组相关的多区域密钥都必须具有一个主密钥。但您可以更改主密钥。此操作称为更新主区域，会将当前主密钥转换为副本密钥，并将其中一个相关的副本密钥转换为主密钥。如果您需要在维护副本密钥的同时删除当前主密钥，或者在与密钥管理员相同的区域中查找主密钥，则可以执行此操作。

您可以选择任何相关的副本密钥作为新的主密钥。操作开始时，主密钥和副本密钥都必须处于 `Enabled` 密钥状态。

即使在此操作完成后，更新主区域的过程可能仍要进行几秒钟。在此期间，旧的主密钥和新的主密钥具有临时密钥状态 Updating（正在更新）。当密钥状态为 `Updating` 时，您可以在加密操作中使用密钥，但不能复制新的主密钥或执行某些管理操作，例如启用或禁用这些密钥。诸如之类的操作DescribeKey可能会将新旧主键同时显示为副本。当更新完成时，`Enabled` 密钥状态将恢复。

假设您在美国东部（弗吉尼亚北部）(us-east-1) 区域中有一个主密钥，在欧洲（爱尔兰）(eu-west-1) 区域有一个副本密钥。您可以使用更新功能将美国东部（弗吉尼亚北部）(us-east-1) 区域中的主密钥更改为副本密钥，并将欧洲（爱尔兰）(eu-west-1) 区域中的副本密钥更改为主密钥。



更新过程完成后，欧洲（爱尔兰）(eu-west-1) 区域中的多区域密钥为多区域主密钥，美国东部（弗吉尼亚北部）(us-east-1) 区域中的密钥是其副本密钥。如果存在其他相关的副本密钥，则它们将成为新主密钥的副本密钥。下次 AWS KMS 同步多区域密钥的共享属性时，它将从新的主键中获取共享属性并将其复制到其副本密钥，包括以前的主键。

更新操作不会影响任何多区域密钥的密钥 ARN。它也不会影响共享属性（如密钥材料）或独立属性（如密钥策略）。不过，您可能需要对新的主密钥的密钥策略进行更新。例如，您可能需要向新的主密钥添加 kms: ReplicateKey 权限以供受信任的委托人使用，然后将其从新的副本密钥中删除。

`Updating` 密钥状态

更新主区域的过程比影响大多数 AWS KMS 操作的短暂的最终一致性延迟要长一些。当 `UpdatePrimaryRegion` 操作返回或者您在控制台中完成了更新程序后，此过程仍然可能在进行中。诸如之类的操作DescribeKey可能会将新旧主键同时显示为副本，直到该过程完成。

在更新主区域的过程中，旧的主密钥和新的主密钥处于 `Updating` 密钥状态。更新过程成功完成后，两个密钥都返回到 `Enabled` 密钥状态。处于 `Updating` 状态时，某些管理操作（如启用和禁用密钥）将不可用。不过，您可以继续在加密操作中使用这两个密钥，而不会中断。有关 `Updating` 密钥状态的影响的信息，请参阅 密 AWS KMS 钥的关键状态。

更新主区域（控制台）

您可以在 AWS KMS 控制台中更新主键。从当前主密钥的密钥详细信息页面开始。

1. 登录 AWS Management Console 并打开 AWS Key Management Service (AWS KMS) 控制台，网址为 https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择多区域主密钥的密钥 ID 或别名。这将打开主密钥的密钥详细信息页面。

   要识别多区域主密钥，请使用右上角的工具图标将 Regionality（区域性）列添加到表中。
5. 选择 Regionality（区域性）选项卡。
6. 在 Primary key（主密钥）部分中，选择 Change primary Region（更改主区域）。
7. 选择新的主密钥的区域。您只能从菜单中选择一个区域。

   Change primary Regions（更改主区域）菜单仅包含具有相关多区域密钥的区域。您可能没有权限更新菜单上的所有区域中的主区域。
8. 选择 Change primary Region（更改主区域）。

更新主要区域 (AWS KMS API)

要更改一组相关的多区域密钥中的主键，请使用UpdatePrimaryRegion操作。

使用 KeyId 参数来标识当前主密钥。使用PrimaryRegion参数来指示新 AWS 区域 主键的。如果主密钥在新的主区域中还没有副本，则操作将失败。

以下示例将主密钥从 us-west-2 区域中的多区域密钥更改为其在 eu-west-1 区域中的副本密钥。KeyId 参数标识 us-west-2 区域中的当前主密钥。该PrimaryRegion参数指定 AWS 区域 了新主键的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
```

如果成功，此操作不会返回任何输出，只返回 HTTP 状态代码。要查看效果，请对其中一个多区域密钥调用DescribeKey操作。您可能需要等到密钥状态返回 Enabled。虽然密钥状态为 Updating（正在更新），但密钥的值可能仍处于变化中。

例如，以下 DescribeKey 调用将获取有关 eu-west-1 区域中多区域密钥的详细信息。输出显示，eu-west-1 区域中的多区域密钥现在为主密钥。us-west-2 区域中相关的多区域密钥（相同的密钥 ID）现在已成为副本密钥。

```
$ 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"
              }
           ]
        }
    }
}
```

轮换多区域密钥

您可以启用和禁用自动轮换，并按需轮换多区域密钥中的密钥材料。密钥轮换是多区域密钥的共享属性。

仅在主密钥上启用和禁用自动密钥轮换。您只能在主键上启动按需轮换。

- AWS KMS 同步多区域密钥时，它会将密钥轮换属性设置从主键复制到其所有相关的副本密钥。
- AWS KMS 轮换密钥材料时，它会为主键创建新的密钥材料，然后将新的密钥材料跨区域边界复制到所有相关的副本密钥中。密钥材料永远不会处于 AWS KMS 未加密状态。此步骤经过精心控制，以确保在加密操作中使用任何密钥之前密钥材料完全同步。
- AWS KMS 在主密钥及其每个副本密钥中都提供该密钥材料之前，不会使用新的密钥材料加密任何数据。
- 复制已轮换的主密钥时，新的副本密钥具有相关多区域密钥的当前密钥材料和所有先前版本的密钥材料。

此模式可确保相关的多区域密钥完全可互操作。任何多区域密钥都可以解密由相关多区域密钥加密的任何密文，即使密文在创建密钥之前已加密。

非对称 KMS 密钥或带有导入密钥材料的 KMS 密钥不支持自动密钥轮换。有关自动和按需密钥轮换的信息，请参阅旋转 AWS KMS keys。

下载公有密钥

创建多区域非对称 KMS 密钥时， AWS KMS 会为主密钥创建 RSA 或椭圆曲线 (ECC) 密钥对。然后，它会将该密钥对复制到主密钥的每个副本。因此，您可以从主密钥或其任何副本密钥下载公有密钥。您总是会获得相同的密钥材料。

有关在之外下载和使用公钥的信息 AWS KMS，请参阅下载公有密钥的特殊注意事项。有关说明，请参阅 下载公有密钥。

将密钥材料导入到多区域密钥中

您可以将自己的密钥材料导入到多区域 KMS 密钥中。您使用自己的密钥材料创建的多区域密钥是可互操作的。您可以对一个区域中的数据进行加密，并使用相关的多区域密钥在任何其他区域中解密该数据。

但是，您必须管理密钥材料。

- AWS KMS 不会将密钥材料从具有导入密钥材料的主密钥中复制或同步到其副本密钥。您必须将相同的密钥材料导入相关的主密钥和副本密钥中。
- 导入密钥材料时，您可以单独设置每个密钥的到期模型和到期日期。您可以为相关的多区域密钥配置相同或不同的过期模式和过期日期。如果密钥材料接近到期日期，您必须将密钥材料重新导入受影响的多区域密钥。

  相关多区域密钥的密钥状态是相互独立的。例如，如果主密钥中的密钥材料过期，则其副本密钥不受影响。

相同的副本密钥的区域要求适用于带导入的密钥材料的多区域密钥。如果您将相同的密钥材料导入到单区域密钥或不相关的多区域密钥中，则这些 KMS 密钥不可互操作。

您可创建具有导入对称、非对称或 HMAC 密钥材料的多区域密钥。AWS KMS 不支持在自定义密钥存储中导入的密钥材料。而且，您不能为具有导入密钥材料的 KMS 密钥启用自动密钥轮换。

除了具有多区域功能外，带有导入密钥材料的多区域密钥还与其他带有导入密钥材料的 KMS 密钥相同。有关创建和配置带有导入密钥材料的单区域密钥的详细信息，请参阅 关于导入的密钥材料。

主题

为什么不是所有带有导入密钥材料的 KMS 密钥都可互操作？

带有导入密钥材料的单区域 KMS 密钥不可互操作，即使它们具有相同的密钥材料也是如此。AWS KMS 使用 KMS 密钥加密数据时，它会以加密方式将某些密钥元数据绑定到密文。这样可以保护密文，以便只有加密数据的 KMS 密钥才能解密该数据。

多区域密钥设计为可互操作。除了具有相同的密钥材料外，它们还具有相同的密钥 ID 和其他元数据。因此，它们生成的密文可以通过任何相关的多区域密钥进行解密。因此，多区域密钥的信任属性与单区域密钥的信任属性不同。但对于某些客户来说，在多个区域中解密的好处超过了依赖单个 AWS 区域中的单个 KMS 密钥的密文的安全值。

创建带导入的密钥材料的主密钥

要创建带导入的密钥材料的主密钥，请先创建不带密钥材料的 KMS 密钥。创建不带密钥材料的主密钥时，必须指定反映计划导入的密钥材料类型的密钥规范。然后，将您的密钥材料导入到主密钥中。

创建不包含密钥材料的多区域主密钥的过程几乎与创建不包含密钥材料的单区域密钥的过程相同。唯一的区别是您指定密钥是多区域密钥。

使用导入的密钥材料创建多区域主密钥的权限与使用密钥材料创建多区域主密钥所需的权限相同，包括 IAM 策略中的 AWS KMS k ms: CreateKey 和 iam: CreateServiceLinkedRole 权限。您可以使用 kms: MultiRegionKeyType 和 k ms: KeyOrigin 条件密钥来允许或拒绝使用导入的密钥材料创建多区域主密钥的权限。

在 AWS KMS 控制台中使用导入的密钥材料创建主密钥时，请使用 Advanced options（高级选项）部分中的设置。创建 KMS 密钥后，这些属性无法更改。

- 将 Key material origin（密钥材料源）设置为 External (Import key material) [外部（导入密钥材料）]。
- 将 Multi-Region replication（多区域复制）设置为 Allow this key to be replicated into other Regions（允许此密钥复制到其他区域中）。

使用CreateKey操作创建包含导入密钥材料的主键时，请使用Origin和MultiRegion参数并指定KeySpec和KeyUsage。以下示例创建了一个可以导入 ECC_NIST_P384 密钥材料的 EXTERNAL KMS 密钥。

```
$ aws kms create-key --origin EXTERNAL --key-spec ECC_NIST_P384 --key-usage SIGN_VERIFY
 --multi-region
```

结果将生成一个不包含密钥材料且密钥状态为 PendingImport 的多区域主密钥。

要启用此 KMS 密钥，您必须下载公有密钥和导入令牌，使用公有密钥加密密钥材料，然后导入密钥材料。有关说明，请参阅导入密钥的 AWS KMS 密钥材料。

创建带导入的密钥材料的副本密钥

您可以在 AWS KMS 控制台中或使用 AWS KMS API 操作创建多区域副本密钥。要复制具有导入的密钥材料的多区域主密钥，请使用您用于创建具有 AWS KMS 密钥材料的副本密钥的相同程序。然而，结果是不同的。复制过程不会返回具有与主密钥相同的密钥材料的副本密钥，而是返回一个不包含密钥材料且密钥状态为 PendingImport 的副本密钥。要启用副本密钥，您必须将相同的密钥材料导入到您导入主密钥的副本密钥中。

虽然不复制密钥材料，但 AWS KMS 会创建具有相同密钥 ID、密钥规范、密钥用法和密钥材料源的副本密钥作为主密钥。它还可确保您导入到副本密钥中的密钥材料与导入到主密钥中的密钥材料相同。

要创建带导入的密钥材料的副本密钥：

1. 创建带已导入密钥材料的多区域主密钥。
2. 请执行以下操作之一。

   在 AWS KMS 控制台中，选择带已导入密钥材料的多区域主密钥。然后，在其 Regionality（区域性）选项卡上，选择 Create new replica keys（创建新副本密钥）。有关说明，请参阅创建副本密钥（控制台）。

   或者使用该ReplicateKey操作。对于 KeyId 参数，输入带导入的密钥材料的多区域主密钥的密钥 ID 或密钥 ARN。有关说明，请参阅创建副本密钥 (AWS KMS API)。
3. 对于每个新的副本密钥，请按照以下步骤下载公有密钥和导入令牌。使用公有密钥对主密钥的密钥材料进行加密，然后在副本密钥中导入主密钥的密钥材料。您的每个副本密钥都需要不同的公有密钥和导入令牌。

如果您尝试导入到副本密钥中的密钥材料与其主密钥不同，则操作将失败。AWS KMS 不需要协调过期模式和过期日期，但您可以为多区域密钥建立业务规则。有关说明，请参阅导入密钥的 AWS KMS 密钥材料。

复制带有导入密钥材料的密钥的权限

要创建带导入的密钥材料的副本密钥，您必须具有以下权限。

在主密钥区域中：

- kms：在主键ReplicateKey上（在主键的区域中）。将此权限包含在主密钥的密钥策略或 IAM policy 中。

在副本密钥区域中：

- kms：CreateKey在 IAM 策略中。
- kms: GetParametersForImport。您可以将此权限包含在副本密钥的密钥策略或 IAM policy 中。
- kms: ImportKeyMaterial。您可以将此权限包含在副本密钥的密钥策略或 IAM policy 中。
- 复制时必须TagResource使用 k@@ ms: 才能分配标签。将此权限包含在副本区域的 IAM policy 中。
- km CreateAlias s: 需要在AWS KMS控制台中复制密钥。有关详细信息，请参阅控制对别名的访问。

删除多区域密钥

当您不再使用多区域主密钥或副本密钥时，您可以计划删除该密钥。

尽管删除 KMS 密钥应始终谨慎操作，但删除多区域密钥的副本的风险较小，前提是主密钥仍然存在于 AWS KMS 中。如果从其区域中删除副本密钥，但发现在已删除密钥下加密的密文，则可以使用任何相关的多区域密钥解密该密文。您还可以通过将主密钥再次复制到副本密钥区域来重新创建副本密钥。

但是，删除主密钥及其所有副本密钥是一个非常危险的操作，相当于删除单区域密钥。

> **Warning**
>
> 删除 KMS 密钥具有破坏性和潜在危险性。只有当您确定不再需要使用 KMS 密钥并且将来也不再需要了，才能继续删除操作。如果您不确定，则应禁用 KMS 密钥，而不是将其删除。

要删除主密钥，必须先删除其所有的副本密钥。如果您必须从特定区域删除主密钥而不删除其副本密钥，请通过更新主区域将主密钥更改为副本密钥。

在安排删除任何 KMS 密钥之前，请查看删除 AWS KMS keys主题中的注意事项，以及说明如何确定 KMS 密钥的过去使用情况以及如何设置警 CloudWatch 报以提醒您在等待期间使用 KMS 密钥的主题。在删除非对称多区域密钥的主密钥之前，请查看删除非对称密钥主题。

主题

- 删除多区域密钥的权限
- 如何删除副本密钥
- 如何删除主密钥

删除多区域密钥的权限

要计划删除多区域密钥，您只需要以下权限。

- km ScheduleKeyDeletion s: — 安排删除多区域密钥并设置其等待期。

我们还强烈建议您拥有以下相关权限。

- km CancelKeyDeletion s: — 取消计划删除多区域密钥。
- k@@ m DescribeKey s: — 查看多区域密钥的密钥状态和相关的多区域密钥列表。
- km DisableKey s: — 让您可以选择禁用多区域密钥而不是将其删除。
- km EnableKey s: — 用于在取消删除多区域密钥后恢复其功能。

您还可以包括复制主密钥和更改主密钥的权限。

- kms: ReplicateKey
- kms: UpdateReplicaRegion

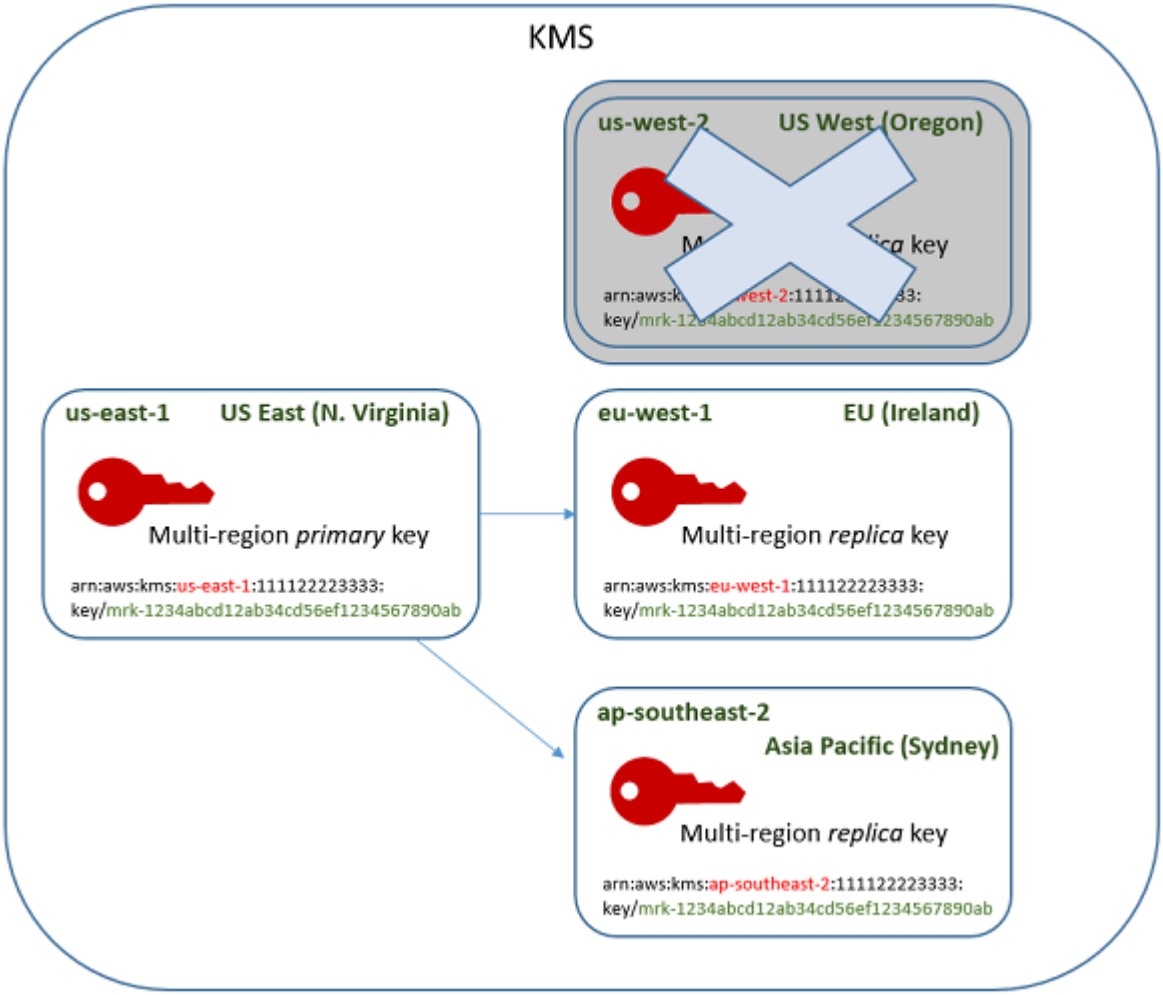
您可以将这些权限包含在 IAM policy 中，但最佳做法是将这些权限放在密钥政策中，在此策略中，这些权限仅应用于您需要管理的 KMS 密钥。

如何删除副本密钥

您可以使用 AWS KMS 控制台或 AWS KMS API 删除副本密钥。您可以随时删除副本密钥。它不依赖于任何其他 KMS 密钥的密钥状态。

如果您误删了副本密钥，可以通过在同一区域中复制相同主密钥，以此方式来重新创建副本密钥。您创建的新副本密钥具有与原始副本密钥相同的共享属性。

删除多区域副本密钥的过程与删除单区域密钥相同。



1. 计划删除副本密钥。选择 7-30 天的等待时间。默认的等待期限为 30 天。
2. 在等待期内，副本密钥的密钥状态更改为 `Pending deletion` (`PendingDeletion`)，并且您不能在加密操作中使用它。
3. 您可以在等待期内的任何时间点取消对副本密钥的计划删除。密钥状态更改为 `Disabled`，但您可以重新启用 KMS 密钥。
4. 等待期到期后，AWS KMS 将删除副本密钥。

您可以查看您的 AWS CloudTrail 日志中的操作的记录。AWS KMS 将记录计划删除 KMS 密钥的操作和删除 KMS 密钥的操作。

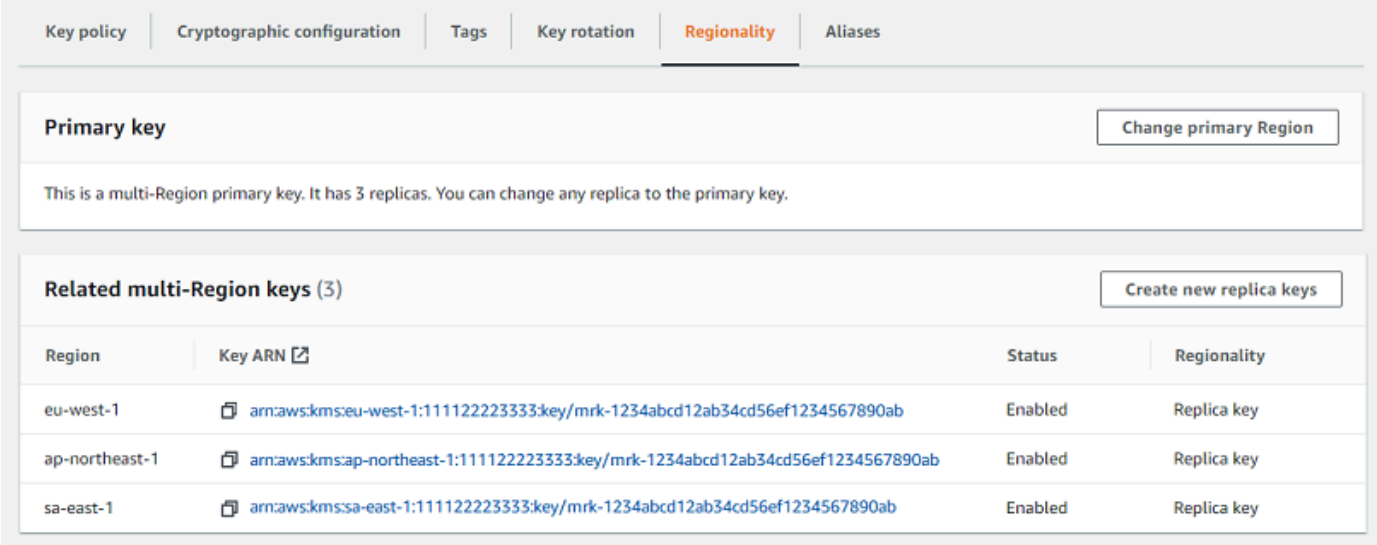
删除副本密钥（控制台）

要计划删除多区域副本密钥，请使用您用于计划删除单区域密钥的相同程序。

因为相关副本密钥位于不同 AWS 区域 中，您无法计划一次删除多个副本密钥。要删除所有相关的副本密钥，请使用类似于以下内容的模式。

计划删除所有相关副本密钥

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 在导航窗格中，选择客户托管密钥。
3. 使用页面右上角的 Region selector（区域选择器）选择多区域主密钥的区域。
4. 选择主密钥的别名和密钥 ID。
5. 选择 Regionality（区域性）选项卡。



6. 在 Related multi-Region keys（相关的多区域密钥）部分中，选择副本密钥的密钥 ARN。

   此操作将在新的浏览器选项卡中打开副本密钥的密钥详细信息页面。控制台设置为副本密钥区域。
7. 从 Key actions（密钥操作）菜单中，选择 Schedule key deletion（计划删除密钥）。

   此操作将启动计划删除密钥的过程。完成计划密钥删除过程。有关更多信息，请参阅 计划和取消密钥删除（控制台）。
8. 返回到显示主密钥的 Regionality（区域性）选项卡的浏览器选项卡。（您可能需要刷新此页面才能看到副本密钥的更新状态。）选择另一个副本密钥的密钥 ARN，然后重复计划删除副本密钥的过程。

删除副本密钥 (AWS KMS API)

要计划删除多区域副本密钥，请使用ScheduleKeyDeletion操作。要标识 KMS 密钥，请使用其密钥 ID 或密钥 ARN。使用多区域密钥时，您可以通过使用具有显式 Region（区域）值的密钥 ARN 减少错误的发生率。

例如，此命令将从 us-west-2（美国西部（俄勒冈））区域删除副本密钥。由于命令没有指定等待时间，因此等待时间设置为默认值 30 天。

```
$ aws kms schedule-key-deletion \
    --region us-west-2 \
    --key-id arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

如果命令成功，将返回密钥 ARN (KeyId)、等待时间 (PendingWindowInDays)、删除日期 (DeletionDate) 和当前密钥状态 (KeyState)（预计将为 PendingDeletion）。

删除多区域副本密钥时，请确保验证密钥 ARN 中的密钥 ID 和区域值是否与您期望的值相同。

```
{
    "KeyId": "arn:aws:kms:us-west-2:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "DeletionDate": 1599523200.0,
    "KeyState": "PendingDeletion",
    "PendingWindowInDays": 30
}
```

要以编程方式删除多区域主密钥的所有副本，请创建包含副本密钥的区域列表。然后，对于列表中的每个区域，调用 ScheduleKeyDeletion 操作，如上所示。

与永久删除的单区域密钥不同的是，您可以通过将主密钥复制到已删除副本密钥所在的区域来恢复副本密钥。

要检查副本密钥的状态并查看多区域密钥的主键和副本密钥，请使用DescribeKey操作。

如何删除主密钥

您可以随时计划删除多区域主密钥。然而，AWS KMS 将不会删除具有副本密钥的多区域主密钥，即使它们已计划删除。

要删除主密钥，您必须计划删除其所有副本密钥，然后等待副本密钥被删除。删除主密钥所需的等待时间从删除主密钥的最后一个副本密钥开始。如果您必须从特定区域删除主密钥而不删除其副本密钥，请通过更新主区域将主密钥更改为副本密钥。

如果主密钥不包含副本密钥，则该过程与删除副本密钥或者删除任何区域性 KMS 密钥相同。

如果某个主密钥已计划删除，则无法用它来执行加密操作，也无法复制它。但是，除非它们也被计划删除，否则其副本密钥不受影响。

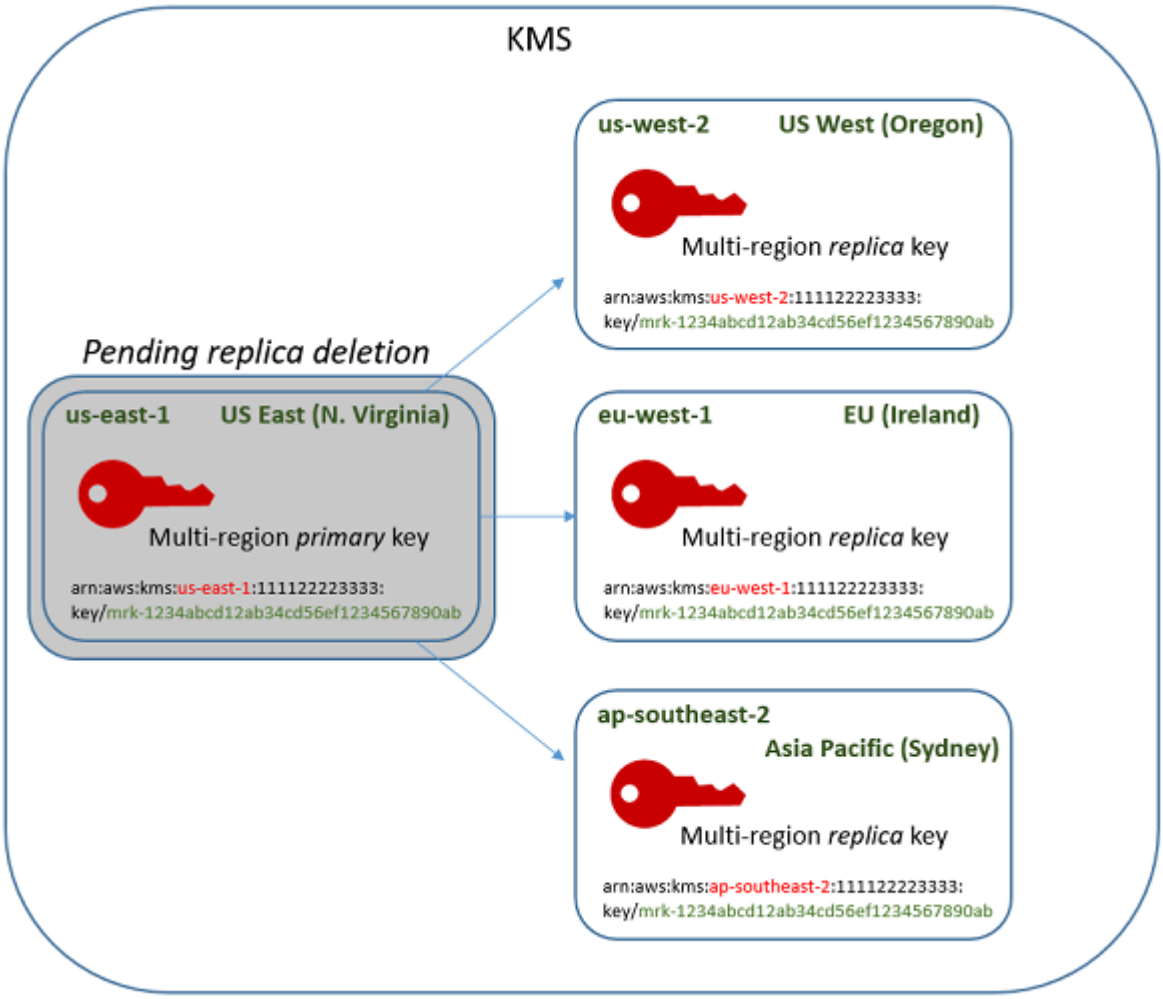
您可以使用 AWS KMS 控制台或 AWS KMS API 来计划删除主密钥和副本密钥。您可以在计划删除副本密钥之前、之后或同时计划删除主密钥。过程可能如下所示。

1. 计划删除主密钥。选择 7-30 天的等待时间。默认的等待期限为 30 天。但是，在删除所有副本密钥之前，主密钥的等待期不会开始。

   如果任何副本密钥仍然存在，主密钥的密钥状态更改为 `Pending replica deletion` (`PendingReplicaDeletion`)。否则，它将更改为 `Pending deletion` (`PendingDeletion`)。无论哪种情况，都不能在加密操作中使用主密钥，也无法复制它。

   计划删除主密钥不会影响副本密钥。它们的密钥状态仍为启用状态，您可以在加密操作中使用它们。如果未删除副本密钥，主密钥的 `Pending replica deletion` 状态可以无限期地持续存在。

```
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
```



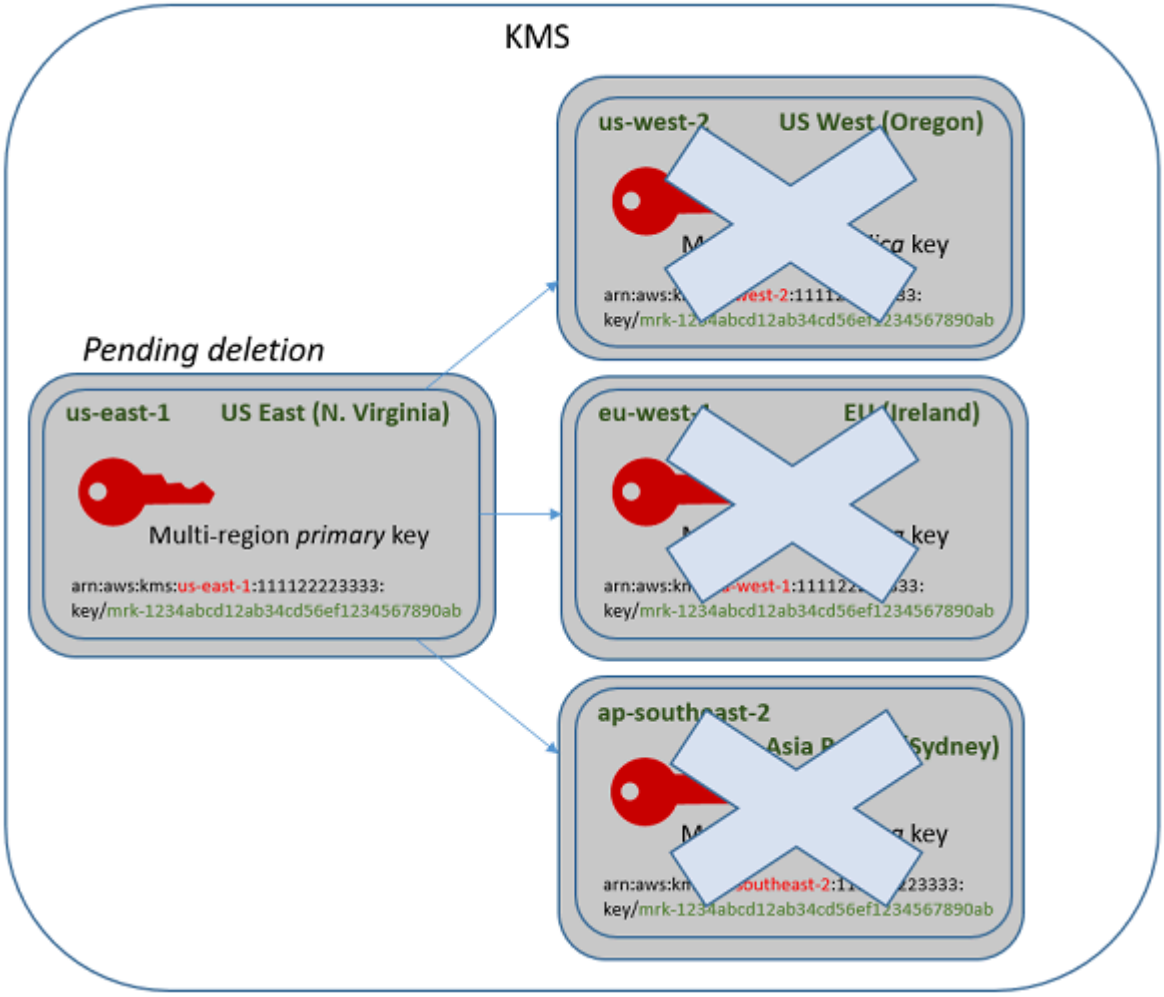
2. 计划删除每个副本密钥。选择 7-30 天的等待时间。默认的等待期限为 30 天。您可以同时删除多个副本密钥。他们的等待期同时运行。在等待期内，副本密钥的密钥状态更改为 Pending deletion (PendingDeletion)，并且您不能在加密操作中使用这些 KMS 密钥。

   例如，如果您有三个副本密钥，则可以同时计划删除所有三个副本密钥。他们可以具有相同或不同的等待时间。请注意，主密钥上的等待期尚未开始。它的密钥状态为 PendingReplicaDeletion，因为它具有现有的副本密钥。

```
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. 您可以取消对主密钥或任何副本密钥的计划删除，直到它被删除。密钥状态更改为 Disabled，但您可以重新启用 KMS 密钥。
4. 当最后一个副本密钥的等待时间到期时，AWS KMS 将删除最后一个副本密钥。主密钥的密钥状态从 Pending replica deletion (PendingReplicaDeletion) 更改为 Pending deletion (PendingDeletion)，主密钥的 7-30 天等待期开始。

```
KMS key:                    Key state:
Primary key (us-east-1)       Pending deletion (waiting period 30 days)
```



5. 等待期到期后，AWS KMS 将删除主密钥。

删除带有副本的主密钥的最短时间为 14 天。

如果计划删除主密钥和所有副本密钥的等待期为 7 天，则副本密钥将在 7 天后删除。主密钥在第 14 天被删除。

- 第 1 天：计划删除主密钥和副本密钥，最短等待时间为 7 天。副本密钥的 7 天删除等待期开始。主密钥的删除等待期尚未开始。
- 第 7 天：副本密钥的删除等待期结束。AWS KMS 删除所有副本密钥。删除最后一个副本密钥后，主密钥的 7 天删除等待期将开始。
- 第 14 天：主密钥的删除等待期结束。AWS KMS 删除主密钥。

您可以查看您的 AWS CloudTrail 日志中的操作的记录。AWS KMS 将记录计划删除每个 KMS 密钥的操作和删除 KMS 密钥的操作。

删除主密钥（控制台）

要删除多区域主密钥，请按以下步骤操作。

计划密钥删除

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选中想要删除的主密钥旁边的复选框。您还可以选择一个或多个 KMS 密钥，包括此主密钥的副本。
5. 依次选择 Key actions (密钥操作)、Schedule key deletion (计划密钥删除)。
6. 阅读并考虑警告，以及有关在等待期限内取消删除的信息。如果决定取消删除，请选择 Cancel (取消)。
7. 对于 Waiting period (in days) (等待期限(天))，键入一个介于 7 和 30 之间的天数。如果您选择了多个 KMS 密钥，则选择的等待时间将应用于所有选定的 KMS 密钥。副本密钥的等待期同时运行，但主密钥的等待时间不会开始，直到 AWS KMS 删除最后一个副本密钥。
8. 选中 Confirm that you want to delete this key in ***<number of days>*** days（确认您要在 n 天后删除此密钥）旁的复选框。
9. 选择计划删除。

要检查 KMS 密钥的删除状态，请在主密钥的 detail page（详细信息）页面上，参阅 General configuration（常规配置）部分。密钥状态将显示在 Status（状态）字段中。当主密钥的密钥状态更改为 `Pending deletion` 时，将显示计划删除日期。

您也可以在多区域密钥的详细信息页面的 Regionality（区域性）选项卡上检查密钥状态（状态）。有关更多信息，请参阅 查看多区域密钥。

删除主密钥 (AWS KMS API)

要删除多区域副本密钥，请使用ScheduleKeyDeletion操作。要标识 KMS 密钥，请使用其密钥 ID 或密钥 ARN。使用多区域密钥时，您可以通过使用具有显式 Region（区域）值的密钥 ARN 减少错误的发生率。

例如，此命令将从 us-east-1（美国东部（弗吉尼亚北部））区域删除主密钥。由于命令没有指定等待时间，因此等待时间设置为默认值 30 天。

```
$ aws kms schedule-key-deletion \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab
```

如果命令成功，则它会返回密钥 ARN、生成的密钥状态和等待期 (PendingWindowInDays)。

如果主密钥不包含副本密钥，则主密钥的密钥状态为 PendingDeletion，并且输出包括 DeletionDate 字段。如果仍有任何副本密钥，则主密钥的密钥状态为 PendingReplicaDeletion，且 DeletionDate 因为不确定而被省略。即使副本密钥也计划删除，您也可以取消计划的删除。

删除多区域主密钥时，请确保验证密钥 ARN 中的密钥 ID 和区域值是否与您期望的值相同。

```
{
    "KeyId": "arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab",
    "KeyState": "PendingReplicaDeletion",
    "PendingWindowInDays": 30
}
```

要检查您的 KMS 密钥的删除状态，请使用对主密钥或任何剩余副本密钥的DescribeKey操作。主密钥的等待周期时钟不会启动，直到删除最后一个副本并且密钥状态更改为 PendingDeletion。

要计算主密钥的预期删除日期，请循环遍历响应中的副本密钥 ARN，在每个密钥上运行 DescribeKey，获取最新的 DeletionDate 值，然后添加主密钥的 PendingDeletionWindowInDays 值。副本密钥的等待期同时运行。

在以下示例中，KMS 密钥是具有现有副本密钥的多区域主密钥。因为密钥状态为 PendingReplicaDeletion，响应包括等待时间 (PendingWindowInDays)，而不是 DeletionDate。主密钥的实际删除日期取决于删除副本密钥的时间。

```
$ 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
    }
}
```

删除所有副本后，DescribeKey 输出将显示密钥状态为 PendingDeletion 的其余主密钥。当密钥状态为 PendingDeletion 时，会显示 DeletionDate 字段，而不是 PendingWindowInDays 字段。

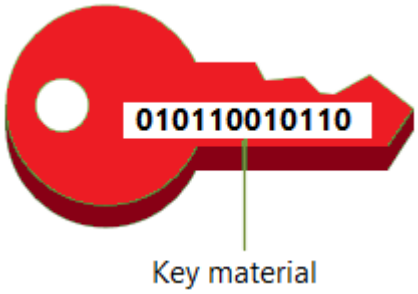
```
$ aws kms describe-key \
    --key-id arn:aws:kms:us-east-1:111122223333:key/
mrk-1234abcd12ab34cd56ef1234567890ab

{
    "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": []
        }
    }
}
```

导入密钥的 AWS KMS 密钥材料

您可以使用您提供的密钥材料创建 AWS KMS keys（KMS 密钥）。

KMS 密钥是加密密钥的逻辑表示形式。KMS 密钥的元数据包括数据加密和解密所用密钥材料的 ID。默认情况下，当您创建 KMS 密钥时， AWS KMS 会为该 KMS 密钥生成密钥材料。但是，您可以创建不带密钥材料的 KMS 密钥，然后将自己的密钥材料导入该 KMS 密钥中，这个功能通常被称为“自带密钥 (BYOK)”。



> **Note**
>
> AWS KMS 不支持解密外部的任何密文 AWS KMS，即使 AWS KMS 密文是在 KMS 密钥下使用导入的密钥材料加密的。 AWS KMS 不会发布此任务所需的密文格式，并且格式可能会更改，恕不另行通知。

除自定义密钥存储中的 KMS 密钥外，所有类型的 KMS 密钥都支持导入的密钥材料。

当您使用导入的密钥材料时，您仍需对密钥材料负责，同时 AWS KMS 允许使用密钥材料的副本。出于以下一个或多个原因，您可以选择执行该操作：

- 证明使用符合您要求的熵源生成了密钥材料。

- 将您自己的基础设施中的密钥材料与 AWS 服务一起使用，并用于管理 AWS KMS 其中的密钥材料的生命周期 AWS。
- 在中使用现有的、成熟的密钥 AWS KMS，例如用于代码签名、PKI 证书签名和证书固定的应用程序的密钥
- 为中的密钥材料设置过期时间 AWS 并手动将其删除，但也可以使其在将来再次可用。相比之下，计划密钥删除需要 7 到 30 天的等待期限，之后，您不能恢复已删除的 KMS 密钥。
- 拥有密钥材料的原始副本，并将其保存在外部，以便在密钥材料 AWS 的整个生命周期中提高耐用性和灾难恢复。
- 对于非对称密钥和 HMAC 密钥，导入会创建兼容且可互操作的密钥，这些密钥可在内部和外部运行。 AWS

您可以使用导入的密钥材料来审核和监控 KMS 密钥的使用和管理。 AWS KMS 在创建 KMS 密钥、下载封装公钥和导入令牌以及导入密钥材料时，会在 AWS CloudTrail 日志中记录事件。 AWS KMS 还会记录手动删除导入的密钥材料或 AWS KMS 删除过期的密钥材料时的事件。

有关使用导入密钥材料的 KMS 密钥与使用由生成的密钥材料的 KMS 密钥之间重要区别的信息 AWS KMS，请参阅关于导入的密钥材料。

支持的 KMS 密钥

AWS KMS 支持以下类型的 KMS 密钥的导入密钥材料。您无法将密钥材料导入自定义密钥存储中的 KMS 密钥。

- 对称加密 KMS 密钥
- 非对称 RSA KMS 密钥（用于加密或签名，但不能同时用于两者）
- 非对称椭圆曲线（ECC）KMS 密钥（仅限签名）
- 非对称 SM2 KMS 密钥-仅限中国区域（用于加密或签名，但不能同时用于两者）
- HMAC KMS 密钥
- 支持的所有类型的多区域密钥。

区域

所有支持的密钥材料均 AWS 区域 支持导入的密钥材料。 AWS KMS

在中国区域，对称加密 KMS 密钥的密钥材料要求与其他地区不同。有关更多信息，请参阅 导入密钥材料步骤 3：加密密钥材料。

主题

计划导入密钥材料

导入的密钥材料允许您在生成的加密密钥下保护您的 AWS 资源。您导入的密钥材料与特定的 KMS 密钥相关联。您可以将相同的密钥材料重新导入到同一 KMS 密钥中，但不能将不同的密钥材料导入 KMS 密钥，也无法将专为导入的密钥材料设计的 KMS 密钥转换为带有密钥材料的 KMS AWS KMS 密钥。

了解更多：

- the section called “选择包装公有密钥规范”
- the section called “选择包装算法”

主题

关于导入的密钥材料

在决定将密钥材料导入之前 AWS KMS，您应该了解导入的密钥材料的以下特征。

您可以生成密钥材料

> 您负责使用符合您的安全要求的随机源来生成密钥材料。

您可以删除密钥材料

您可以从 KMS 密钥中删除导入的密钥材料，以便立即使 KMS 密钥不可用。此外，当您将密钥材料导入 KMS 密钥中时，您可以确定密钥是否到期，并设置其到期时间。到期时间到来时， AWS KMS 删除密钥材料。如果没有密钥材料，则该 KMS 密钥无法用于任何加密操作。要还原密钥，必须将相同密钥材料重新导入到密钥中。

您无法更改密钥材料

当您将密钥材料导入 KMS 密钥中时，该 KMS 密钥将与该密钥材料永久关联。您可以重新导入相同的密钥材料，但不能将不同的密钥材料导入该 KMS 密钥。而且，您不能为具有导入密钥材料的 KMS 密钥启用自动密钥轮换。但是，您可以手动轮换带有导入密钥材料的 KMS 密钥。

您无法更改密钥材料源

专用于导入的密钥材料的 KMS 密钥拥有一个 EXTERNAL 的源值，该值无法更改。您不能将导入的密钥材料的 KMS 密钥转换为使用任何其他来源（包括）的密钥材料 AWS KMS。同样，您不能将包含密钥材料的 KMS AWS KMS 密钥转换为专为导入的密钥材料而设计的密钥。

您无法导出密钥材料

您无法导出您导入的任何密钥材料。 AWS KMS 无法以任何形式将导入的密钥材料退还给您。您必须在外部保存导入的密钥材料的副本 AWS，最好是在密钥管理器中，例如硬件安全模块 (HSM)，以便在删除密钥材料或密钥材料过期时可以重新导入。

您可创建具有导入密钥材料的多区域密钥

具有导入密钥材料的多区域具有包含导入密钥材料的 KMS 密钥的功能，并且可以在 AWS 区域之间进行互操作。要创建具有导入密钥材料的多区域密钥，您必须将相同的密钥材料导入 KMS 主密钥和每个副本密钥。有关更多信息，请参阅 将密钥材料导入到多区域密钥中。

非对称密钥和 HMAC 密钥具有可移植性和互操作性

您可以在外部使用非对称密钥材料和 HMAC 密钥材料，与具有相同导入密钥材料的 AWS AWS KMS 密钥进行互操作。

与 AWS KMS 对称密文不同，对称密文与算法中使用的 KMS 密钥密不可分，它 AWS KMS 使用标准 HMAC 和非对称格式进行加密、签名和 MAC 生成。因此，这些密钥是可移植的，并且支持传统的托管密钥方案。

当您的 KMS 密钥导入了密钥材料后，您可以使用外部导入的密钥材料 AWS 来执行以下操作。

- HMAC 密钥 – 您可以使用导入的密钥材料验证由 HMAC KMS 密钥生成的 HMAC 标签。您还可以将 HMAC KMS 密钥与导入的密钥材料一起使用，以验证由外部的密钥材料生成的 HMAC 标签。 AWS

- 非对称加密密钥 — 您可以使用外部的私有非对称加密密钥 AWS 来解密由 KMS 密钥和相应的公钥加密的密文。您还可以使用非对称 KMS 密钥来解密在外部生成的非对称密文。 AWS
- 非对称签名密钥 — 您可以使用带有导入密钥材料的非对称签名 KMS 密钥来验证由您的私有签名密钥在外部生成的数字签名。 AWS您还可以在外部使用非对称公有签名密钥 AWS 来验证非对称 KMS 密钥生成的签名。

如果您在相同的 AWS 区域中将相同的密钥材料导入不同的 KMS 密钥中，则这些密钥也是可以互操作的。要在不同版本中创建可互操作的 KMS 密钥 AWS 区域，请使用导入的密钥材料创建多区域密钥。

对称加密密钥不可移植或互操作

生 AWS KMS 成的对称密文不可移植或互操作。 AWS KMS 不会发布可移植性所需的对称密文格式，并且格式可能会更改，恕不另行通知。

- AWS KMS 即使您使用已导入的密钥材料，也无法解密您在外部加密的 AWS对称密文。
- AWS KMS 不支持解密外部的任何 AWS KMS 对称密文，即使密文是在 KMS 密钥下使用导入的密钥材料加密的。 AWS KMS
- 具有相同导入密钥材料的 KMS 密钥不可互操作。 AWS KMS 生成每个 KMS 密钥特有的密文的对称密文。此加密文字格式保证只有加密数据的 KMS 密钥才能解密数据。

此外，您不能使用任何 AWS 工具（例如AWS Encryption SDK或 Amazon S3 客户端加密）来解密对称密文 AWS KMS 。

因此，您不能使用带有导入密钥材料的密钥来支持密钥托管安排，在这种安排中，有权有条件访问密钥材料的授权第三方可以在外部解密某些密文。 AWS KMS要支持密钥托管，请使用 AWS Encryption SDK 来通过独立于 AWS KMS的密钥加密您的消息。

您需要对可用性和持久性负责

AWS KMS 旨在保持导入的密钥材料的高可用性。但是 AWS KMS 不能将进口密钥材料的耐久性保持在与 AWS KMS 生成的密钥材料相同的水平。有关更多信息，请参阅 保护导入的密钥材料。

保护导入的密钥材料

您导入的密钥材料在传输中和静态时都受到保护。在导入密钥材料之前，您需要使用在 FIPS 140-2 加密模块验证计划下验证的 AWS KMS 硬件安全模块 (HSM) 中生成的 RSA 密钥对的公钥来加密（或“包装”）密钥材料。您可以使用包装公有密钥直接加密密钥材料，也可以使用 AES 对称密钥加密密钥材料，然后使用 RSA 公有密钥加密 AES 对称密钥。

收到后，使用 HSM 中的相应私钥对 AWS KMS 密钥材料进行解密，然后使用仅存在于 AWS KMS HSM 易失性存储器中的 AES 对称密钥对其进行重新加密。您的密钥材料绝不会让 HSM 处于纯文本状态。它仅在使用时解密，并且仅在 HSM 中 AWS KMS 解密。

您的 KMS 密钥与导入的密钥材料的使用完全取决于您在 KMS 密钥上设置的访问控制策略。此外，您还可以使用别名和标签来识别和控制对 KMS 密钥的访问。您可以启用和禁用密钥，查看和编辑其属性，并使用类似于 AWS CloudTrail的服务对其进行监控。

但是，您将保留密钥材料的唯一故障保护副本。作为这种额外控制措施的回报，您应对进口密钥材料的耐用性和整体可用性负责。 AWS KMS 旨在保持导入的密钥材料的高可用性。但是 AWS KMS 不能将进口密钥材料的耐久性保持在与 AWS KMS 生成的密钥材料相同的水平。

在以下情况下，这种持久性的差异是有意义的：

- 当您为导入的密钥材料设置过期时间时，将在密钥材料到期后将其 AWS KMS 删除。 AWS KMS 不会删除 KMS 密钥或其元数据。您可以创建一个 Amazon CloudWatch 警报，在导入的密钥材料即将到期时通知您。

  您无法删除为 KMS 密钥 AWS KMS 生成的密钥材料，也不能将 AWS KMS 密钥材料设置为过期，但您可以轮换密钥材料。
- 手动删除导入的密钥材料时， AWS KMS 会删除密钥材料，但不会删除 KMS 密钥或其元数据。相比之下，计划密钥删除需要 7 到 30 天的等待期限，之后， AWS KMS 将永久删除密钥材料、其元数据及其密钥材料。
- 万一发生某些影响整个地区的故障 AWS KMS （例如完全断电）， AWS KMS 则无法自动恢复导入的密钥材料。但是， AWS KMS 可以恢复 KMS 密钥及其元数据。

您必须在您控制的系统之外保留一份导入 AWS 的密钥材料的副本。我们建议您将导入的密钥材料的可导出副本存储在密钥管理系统中，例如 HSM。如果您导入的密钥材料被删除或过期，则其关联的 KMS 密钥将无法使用，直到您重新导入相同的密钥材料。如果您导入的密钥材料永久丢失，则以 KMS 密钥加密的任何加密文字都将无法恢复。

导入密钥材料的权限

要使用导入的密钥材料创建和管理 KMS 密钥，用户需要在此过程中执行操作的权限。在您创建 KMS 密钥时，您可以在密钥策略中提供 `kms:GetParametersForImport`、`kms:ImportKeyMaterial` 和 `kms:DeleteImportedKeyMaterial` 权限。在 AWS KMS 控制台中，当您使用外部密钥材料来源创建密钥时，会自动为密钥管理员添加这些权限。

若要使用导入的密钥材料创建 KMS 密钥，委托人需要以下权限。

- kms: CreateKey（IAM 策略）
  - 要将此权限限制为使用已导入密钥材料的 KMS 密钥，请使用值为 kms: KeyOrigin 策略条件EXTERNAL。

```
{
  "Sid": "CreateKMSKeysWithoutKeyMaterial",
  "Effect": "Allow",
  "Resource": "*",
  "Action": "kms:CreateKey",
  "Condition": {
    "StringEquals": {
      "kms:KeyOrigin": "EXTERNAL"
    }
  }
}
```

- kms: GetParametersForImport（密钥策略或 IAM 策略）
  - 要将此权限限制为使用特定包装算法和封装密钥规范的请求，请使用 k ms: WrappingAlgorithm 和 k ms: WrappingKeySpec 策略条件。
- kms: ImportKeyMaterial（密钥策略或 IAM 策略）
  - 要允许或禁止过期的密钥材料并控制过期日期，请使用 kms: ExpirationModel 和 kms: ValidTo 策略条件。

要重新导入导入的密钥材料，委托人需要 k ms: GetParametersForImport 和 kms: ImportKeyMaterial 权限。

要删除导入的密钥材料，委托人需要 kms: DeleteImportedKeyMaterial 权限。

例如，要授予示例使用导入的密钥材料管理 KMS 密钥所有方面的 KMSAdminRole 权限，请在 KMS 密钥的密钥策略中加入如下所示的密钥策略声明。

```
{
  "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"
  ]
}
```

导入密钥材料的要求

您导入的密钥材料必须与相关 KMS 密钥的密钥规范兼容。对于非对称密钥对，仅导入密钥对的私钥。AWS KMS 从私钥派生公钥。

AWS KMS 支持使用导入的密钥材料的 KMS 密钥的以下密钥规范。

KMS 密钥的密钥类型	密钥材料要求
对称加密密钥 SYMMETRIC_DEFAULT	256 位（32 字节）的二进制数据 在中国区域，必须是 128 位（16 字节）的二进制数据。
HMAC 密钥 HMAC_224 HMAC_256 HMAC_384 HMAC_512	HMAC 密钥材料必须符合 RFC 2104。 密钥长度必须与密钥规范指定的长度相匹配。
RSA 非对称私有密钥 RSA_2048 RSA_3072 RSA_4096	您导入的 RSA 非对称私有密钥必须是符合 RFC 3447 的密钥对的一部分。 模数：2048 位、3072 位或 4096 位 素数数量：2（不支持多素数 RSA 密钥） 非对称密钥材料必须采用符合 RFC 5208 的公钥加密标准 (PKCS) #8 格式进行 BER 编码或 DER 编码。
椭圆曲线非对称私有密钥	您导入的 ECC 非对称私有密钥必须是符合 RFC 5915 的密钥对的一部分。

KMS 密钥的密钥类型	密钥材料要求
ECC_NIST_P256 (secp256r1) ECC_NIST_P384 (secp384r1) ECC_NIST_P521 (secp521r1) ECC_SECG_P256K1 (secp256k1)	曲线：NIST P-256、NIST P-384、NIST P-521 或 Secp256k1 参数：仅限命名曲线（拒绝带有显式参数的 ECC 密钥） 公共点坐标：可以是压缩坐标、未压缩坐标或投影坐标 非对称密钥材料必须采用符合 RFC 5208 的公钥加密标准 (PKCS) #8 格式进行 BER 编码或 DER 编码。
SM2 非对称私钥（仅限中国区域）	您导入的 SM2 非对称私钥必须是符合 GM/T 0003 的密钥对的一部分。 曲线：SM2 参数：仅限命名曲线（拒绝带有显式参数的 SM2 关键帧） 公共点坐标：可以是压缩坐标、未压缩坐标或投影坐标 非对称密钥材料必须采用符合 RFC 5208 的公钥加密标准 (PKCS) #8 格式进行 BER 编码或 DER 编码。

管理导入的密钥材料

这些主题说明了如何将密钥材料导入和重新导入 KMS 密钥，以及如何创建自动过期的导入密钥材料。

主题

- 导入密钥材料的概述
- 重新导入密钥材料
- 标识具有导入密钥材料的 KMS 密钥

- 为导入的密钥材料过期创建 CloudWatch 警报
- 删除导入的密钥材料
- 删除具有导入密钥材料的 KMS 密钥

导入密钥材料的概述

以下概述说明了如何将密钥材料导入 AWS KMS。如需了解该过程中每个步骤的更多详细信息，请参阅相应主题。

1. 创建不具有密钥材料的 KMS 密钥 - 源必须是 EXTERNAL。密钥来源为EXTERNAL表示密钥是为导入的密钥材料设计的，因此无法 AWS KMS 为 KMS 密钥生成密钥材料。在后面的步骤中，您会将自己的密钥材料导入此 KMS 密钥中。

   您导入的密钥材料必须与关联 AWS KMS 密钥的密钥规格兼容。有关兼容性的更多信息，请参阅 the section called “导入密钥材料的要求”。
2. 下载包装公有密钥和导入令牌 – 在完成步骤 1 后，请下载公有密钥和导入令牌。当您的密钥材料导入时，这些物品可以保护您的密钥材料 AWS KMS。

   在此步骤中，您将选择 RSA 包装密钥的类型（“密钥规范”）以及用于加密向 AWS KMS传输的传输中数据的包装算法。每次导入或重新导入相同的密钥材料时，您可以选择不同的包装密钥规范和包装密钥算法。
3. 加密密钥材料 – 使用在步骤 2 中下载的包装公有密钥加密您在自己的系统上创建的密钥材料。
4. 导入密钥材料 – 上传您在步骤 3 中创建的已加密的密钥材料以及您在步骤 2 中下载的导入令牌。

   在此阶段，您可以设置可选的过期时间。导入的密钥材料过期后，将其 AWS KMS 删除，KMS 密钥将无法使用。要继续使用该 KMS 密钥，您必须重新导入相同的密钥材料。

   导入操作成功完成后，KMS 密钥的密钥状态将从 `PendingImport` 变为 `Enabled`。现在，您可以在加密操作中使用 KMS 密钥。

AWS KMS 在创建 KMS 密钥、下载封装公钥和导入令牌以及导入密钥材料时，会在 AWS CloudTrail 日志中记录一个条目。 AWS KMS 还会在您删除导入的密钥材料或 AWS KMS 删除过期的密钥材料时记录一个条目。

重新导入密钥材料

如果您管理带有导入的密钥材料的 KMS 密钥，则可能需要重新导入密钥材料。您可以通过重新导入密钥材料替换过期或删除的密钥材料，或者更改密钥材料的到期模型或到期日期。

当您将密钥材料导入 KMS 密钥中时，该 KMS 密钥将与该密钥材料永久关联。您可以重新导入相同的密钥材料，但不能将不同的密钥材料导入该 KMS 密钥。您不能轮换密钥材料， AWS KMS 也无法为具有导入密钥材料的 KMS 密钥创建密钥材料。

您可以在可满足您的安全要求任何时间点重新导入密钥材料。您不必等到密钥材料达到或接近其过期时间。

要重新导入密钥材料，请使用您首次用来导入密钥材料的相同过程，但以下情况除外。

- 使用现有 KMS 密钥，而不是创建新的 KMS 密钥。您可以跳过导入过程的步骤 1。
- 重新导入密钥材料时，您可以更改到期模型和到期日期。

每次将密钥材料导入 KMS 密钥时，您需要为 KMS 密钥下载并使用新的包装密钥和导入令牌。包装过程不会影响密钥材料的内容，因此，您可以使用不同的包装公有密钥和不同的包装算法来导入相同的密钥材料。

标识具有导入密钥材料的 KMS 密钥

在创建不带密钥材料的 KMS 密钥时，KMS 密钥的 `Origin` 属性的值为 `EXTERNAL`，并且它不能更改。与密钥状态不同，`Origin` 值不依赖于是否存在密钥材料。

您可以使用 `EXTERNAL` 源值来标识专为导入的密钥材料而设计的 KMS 密钥。您可以在 AWS KMS 控制台中或使用DescribeKey操作来找到密钥来源。您还可以使用控制台或 API 查看密钥材料的属性，例如它是否以及何时过期。

要标识带导入的密钥材料的 KMS 密钥（控制台）

1. 打开 AWS KMS 控制台，网址为 https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 使用以下任一方法可查看 KMS 密钥的 `Origin` 属性。
   - 要向 KMS 密钥表添加 Origin（源）列，请在右上角选择 Settings（设置）图标。选择 Origin (源)，然后选择 Confirm (确认)。“源”列可让您轻松标识具有外部（导入密钥材料）源属性值的 KMS 密钥。
   - 要查找特定 KMS 密钥的 `Origin` 属性的值，请选择该 KMS 密钥的密钥 ID 或别名。然后，选择 Cryptographic configuration（加密配置）选项卡。这些选项卡在 General configuration（常规配置）部分下。
4. 要查看有关密钥材料的详细信息，请选择 Key material（密钥材料）选项卡。此选项卡仅显示在具有导入密钥材料的 KMS 密钥的详细信息页面上。

使用导入的密钥材料 (AWS KMS API) 识别 KMS 密钥

使用该DescribeKey操作。此响应包含 KMS 密钥的 `Origin` 属性、过期模型和过期日期，如以下示例所示。

```
$  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"
        ]
    }
}
```

为导入的密钥材料过期创建 CloudWatch 警报

您可以创建一个 CloudWatch 警报，在 KMS 密钥中导入的密钥材料即将过期时通知您。例如，警报可以在距离到期时间少于 30 天时通知您。

当您将密钥材料导入 KMS 密钥中时，可以选择性地指定密钥材料的到期时间。当密钥材料过期时，AWS KMS 会删除密钥材料，KMS 密钥将无法使用。要再次使用该 KMS 密钥，您必须重新导入密钥材料。但是，如果您在密钥材料到期之前将其重新导入，则可以避免中断使用该 KMS 密钥的进程。

此警报使用 AWS KMS 发布到的`SecondsUntilKeyMaterialExpires`指标，CloudWatch 用于导入的密钥材料已过期的 KMS 密钥。每个警报都使用此指标来监控特定 KMS 密钥的导入密钥材料。您

无法为所有具有到期密钥材料的 KMS 密钥创建单个警报，也无法为未来可能创建的 KMS 密钥创建警报。

要求

监控导入密钥材料过期的 CloudWatch 警报需要以下资源。

- 带有已到期导入密钥材料的 KMS 密钥。有关帮助信息，请参阅 标识具有导入密钥材料的 KMS 密钥。
- Amazon SNS 主题。有关详情，请参阅亚马逊 CloudWatch 用户指南中的创建 Ama zon SNS 主题。

创建警报

使用以下必填值按照基于静态阈值创建 CloudWatch 警报中的说明进行操作。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
选择指标	选择 KMS，然后选择每密钥指标。 选择带有 KMS 密钥和 `SecondsUntilKeyMaterialExpires` 指标的行。然后选择 Select metric（选择指标）。 指标列表仅显示导入密钥材料已到期的 KMS 密钥的 `SecondsUntilKeyMaterialExpires` 指标。如果您在账户和区域中没有带这些属性的 KMS 密钥，则此列表为空。
Statistic	最低
周期	1 minute
阈值类型	静态
当 ...	当 *`metric-name`* 大于 1 时

删除导入的密钥材料

您可以随时从 KMS 密钥中删除导入的密钥材料。此外，当导入的带有过期日期的密钥材料到期时，AWS KMS 会删除该密钥材料。在这两种情况下，密钥材料被删除时，KMS 密钥的密钥状态将更改为“待导入”，并且在您重新导入相同密钥材料之前，KMS 密钥不能用于任何加密操作。（您无法将任何其他密钥材料导入 KMS 密钥。）

除了禁用 KMS 密钥和撤回权限外，还可以将删除密钥材料用作一种策略，以快速但暂时地停止使用 KMS 密钥。相比之下，计划删除具有导入密钥材料的 KMS 密钥也会很快停止使用 KMS 密钥。但是，如果在等待期内未取消删除，则会永久删除 KMS 密钥、密钥材料和所有密钥元数据。有关更多信息，请参阅 the section called “删除具有导入密钥材料的 KMS 密钥”。

要删除密钥材料，您可以使用 AWS KMS 控制台或 DeleteImportedKeyMaterialAPI 操作。 AWS KMS 当您删除导入的密钥材料和AWS KMS 删除过期的密钥材料时，会在 AWS CloudTrail 日志中记录一个条目。

主题

- 删除密钥材料会如何影响 AWS 服务
- 删除密钥材料（控制台）
- 删除密钥材料 (AWS KMS API)

删除密钥材料会如何影响 AWS 服务

当您删除密钥材料时，没有密钥材料的 KMS 密钥会立即变为不可用（视最终一致性而定）。不过，在再次使用 KMS 密钥（例如解密数据密钥）之前，使用受 KMS 密钥保护的数据密钥加密的资源不会受到影响。此问题会影响 AWS 服务，其中许多使用数据密钥来保护您的资源。有关更多信息，请参阅不可用的 KMS 密钥如何影响数据密钥。

删除密钥材料（控制台）

您可以使用 AWS Management Console 来删除密钥材料。

1. 登录 AWS Management Console 并打开 AWS Key Management Service (AWS KMS) 控制台，网址为 https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 请执行以下操作之一：

- 选中带导入密钥材料的 KMS 密钥对应的复选框。依次选择 Key actions、Delete key material。
- 选择带导入密钥材料的 KMS 密钥的别名或密钥 ID。选择 Key material（密钥材料）选项卡，然后选择 Delete key material（删除密钥材料）。

5. 确认要删除该密钥材料，然后选择 Delete key material。KMS 密钥的状态（对应于其密钥状态）更改为 Pending import（等待导入）。

删除密钥材料 (AWS KMS API)

要使用 AWS KMS API 删除密钥材料，DeleteImportedKeyMaterial请发送请求。以下示例说明如何使用 AWS CLI 执行该操作。

将 *1234abcd-12ab-34cd-56ef-1234567890ab* 替换为您要删除其密钥材料的 KMS 密钥的密钥 ID。在该操作中，您可以使用 KMS 密钥的密钥 ID 或 ARN，但不能使用别名。

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

删除具有导入密钥材料的 KMS 密钥

删除具有导入密钥材料的 KMS 密钥的密钥材料是临时的，并且是可撤销的。要恢复密钥，请重新导入其密钥材料。

相反，删除 KMS 密钥操作是不可逆的。如果您计划删除密钥且所需的等待期已过期，则 AWS KMS 永久且不可逆转地删除 KMS 密钥、其密钥材料以及与 KMS 密钥关联的所有元数据。

但是，删除具有导入密钥材料的 KMS 密钥的风险和后果取决于 KMS 密钥的类型（“密钥规范”）。

- 对称加密密钥 - 如果删除对称加密 KMS 密钥，则所有由该密钥加密的其余加密文字都无法恢复。即使您拥有相同的密钥材料，也无法创建新的对称加密 KMS 密钥来解密已删除的对称加密 KMS 密钥的加密文字。每个 KMS 密钥独有的元数据以加密方式绑定到每个对称加密文字。此安全功能保证只有加密对称加密文字的 KMS 密钥才能解密该加密文字，但阻止您重新创建等效的 KMS 密钥。
- 非对称密钥和 HMAC 密钥 — 如果您拥有原始密钥材料，则可以创建与已删除的非对称密钥或 HMAC KMS 密钥具有相同加密属性的新 KMS 密钥。 AWS KMS 生成标准 RSA 密文和签名、ECC 签名和 HMAC 标记，其中不包含任何独特的安全功能。此外，您还可以在 AWS之外使用 HMAC 密钥或非对称密钥对的私有密钥。

  使用相同的非对称或 HMAC 密钥材料创建的新 KMS 密钥将具有不同的密钥标识符。您必须创建新的密钥政策，重新创建所有别名，并更新现有的 IAM policy 和授权，以引用新的密钥。

导入密钥材料步骤 1：创建不带密钥材料的 AWS KMS key

默认情况下，当您创建 KMS 密钥时，AWS KMS 会为您创建密钥材料。要改为导入自己的密钥材料，请先创建不带密钥材料的 KMS 密钥。然后导入密钥材料。要创建不带密钥材料的 KMS 密钥，请使用 AWS KMS控制台或CreateKey操作。

要创建不具有密钥材料的密钥，请指定 EXTERNAL 的源。KMS 密钥的源属性是不可变的。创建完成后，无法将专为导入密钥材料设计的 KMS 密钥转换为带有 AWS KMS 中的密钥材料或任何其他源的 KMS 密钥。

带 EXTERNAL 且无密钥材料的 KMS 密钥的密钥状态为 PendingImport。KMS 密钥可以无限保留在 PendingImport 状态。但是，您不能在加密操作中使用处于 PendingImport 状态的 KMS 密钥。导入密钥材料时，KMS 密钥的密钥状态会更改为 Enabled，您可以在加密操作中使用该密钥。

AWS KMS在创建 KMS 密钥、下载公钥和导入令牌以及导入密钥材料时，会在AWS CloudTrail日志中记录事件。 AWS KMS还会在您删除导入的密钥材料或AWS KMS删除过期的密钥材料时记录 CloudTrail 事件。

有关创建带有导入密钥材料的多区域密钥的信息，请参阅 将密钥材料导入到多区域密钥中。

主题

- 创建不带密钥材料的 KMS 密钥（控制台）
- 创建不带密钥材料的 KMS 密钥 (AWS KMS API)

创建不带密钥材料的 KMS 密钥（控制台）

您只需为导入的密钥材料创建一次 KMS 密钥。您可以根据需要多次将相同的密钥材料导入和重新导入到现有的 KMS 密钥中，但不能将不同的密钥材料导入一个 KMS 密钥。有关更多信息，请参阅 步骤 2：下载包装公有密钥和导入令牌。

要在您的 客户管理型密钥 表中查找带有导入的密钥材料的现有 KMS 密钥，请使用右上角的齿轮图标显示 KMS 密钥列表中的 Origin（源）列。导入的密钥的源值为外部（导入密钥材料）。

要使用导入的密钥材料创建 KMS 密钥，请首先按照基本说明创建首选密钥类型的 KMS 密钥，但以下情况除外。

选择密钥用法后，请执行以下操作：

1. 展开 Advanced options (高级选项)。

2. 对于 Key material origin（密钥材料源），请选择 External (Import key material) [外部（导入密钥材料）]。
3. 选择我了解使用导入密钥的安全性和持久性影响旁边的复选框，表示您了解使用导入密钥材料的影响。要了解这些含义，请参阅保护导入的密钥材料。
4. 返回基本说明。对于该类型的所有 KMS 密钥，基本过程的其余步骤都相同。

选择完成时，您创建了一个 KMS 密钥，该密钥没有密钥材料，状态（密钥状态）为待导入。

但是，控制台不会返回到客户托管密钥表，而是显示一个页面，您可以在其中下载导入密钥材料所需的公有密钥和导入令牌。现在，您可以立即继续下载步骤，也可以选择取消停止下载。您可以随时返回此下载步骤。

下一步: 步骤 2：下载包装公有密钥和导入令牌。

创建不带密钥材料的 KMS 密钥 (AWS KMS API)

要使用 AWS KMSAPI 创建不含密钥材料的对称加密 KMS 密钥，请发送`Origin`参数设置为`EXTERNAL`的CreateKey请求。以下示例说明如何使用 AWS Command Line Interface (AWS CLI) 执行该操作。

```
$ aws kms create-key --origin EXTERNAL
```

该命令成功执行后，您会看到类似以下内容的输出。AWS KMS 密钥的 `Origin` 为 `EXTERNAL`，且其 `KeyState` 为 `PendingImport`。

> **Tip**
>
> 如果命令不成功，则可能会看到 `KMSInvalidStateException` 或 `NotFoundException`。您可以重试请求。

```
{
    "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"
        ]
    }
}
```

从命令输出中复制 KeyId 值，以供后面的步骤使用，然后继续 步骤 2：下载包装公有密钥和导入令牌。

> **Note**
>
> 此命令创建对称加密 KMS 密钥，其 KeySpec 为 SYMMETRIC_DEFAULT，KeyUsage 为 ENCRYPT_DECRYPT。您可以使用可选参数 --key-spec 和 --key-usage 来创建非对称或 HMAC KMS 密钥。有关更多信息，请参阅 CreateKey 操作。

导入密钥材料步骤 2：下载包装公有密钥和导入令牌

创建不 AWS KMS key 带密钥材料的后，使用 AWS KMS 控制台或 GetParametersForImportAPI 下载包装公钥和该 KMS 密钥的导入令牌。包装公有密钥和导入令牌是一个不可分割的集合，必须一起使用。

您将使用包装公有密钥来加密您的密钥材料以供传输。在下载 RSA 封装密钥对之前，请选择 RSA 封装密钥对的长度（密钥规范），以及将用于加密导入的密钥材料以便在步骤 3 中传输的封装算法。AWS KMS 还支持 SM2 封装密钥规范（仅限中国区域）。

每个包装公有密钥和导入令牌集的有效期为 24 小时。如果您不在 24 小时的下载期限内使用它们导入密钥材料，则必须下载新的公有密钥和令牌集。您可以随时下载新的包装公有密钥和导入令牌集。这使您可以更改 RSA 包装密钥长度（“密钥规范”）或替换丢失的集。

您也可以下载包装公有密钥和导入令牌，以将相同的密钥材料重新导入 KMS 密钥中。您可以执行此操作来设置或更改密钥材料的过期时间，或者恢复过期或删除的密钥材料。每次将密钥材料导入时，都必须下载并重新加密密钥材料。 AWS KMS

包装公有密钥的使用

下载内容包括您独有的公钥 AWS 账户，也称为封装公钥。

在导入密钥材料之前，请使用公共封装密钥对密钥材料进行加密，然后将加密的密钥材料上传到 AWS KMS。 AWS KMS 收到您的加密密钥材料后，它会使用相应的私钥对密钥材料进行解密，然后在 AES 对称密钥下重新加密密钥材料，所有这些都在 AWS KMS 硬件安全模块 (HSM) 中完成。

使用导入令牌

下载包括一个带有元数据的导入令牌，以确保您的密钥材料导入正确。将加密的密钥材料上传到时 AWS KMS，必须上传在此步骤中下载的相同导入令牌。

选择包装公有密钥规范

为了在导入过程中保护您的密钥材料，您可以使用从中 AWS KMS下载的封装公钥和支持的封装算法对其进行加密。您在下载包装公有密钥和导入令牌之前选择密钥规范。所有封装密钥对都是在 AWS KMS 硬件安全模块 (HSM) 中生成的。私有密钥永远不会让 HSM 处于纯文本状态。

RSA 包装关键规格

包装公有密钥的密钥规范决定了 RSA 密钥对中密钥的长度，该密钥对在传输到 AWS KMS的过程中可以保护您的密钥材料。一般来说，我们建议使用实用的最长的包装公有密钥。我们提供多种包装公有密钥规范，以支持各种 HSM 和密钥管理器。

AWS KMS 支持以下用于导入所有类型密钥材料的 RSA 封装密钥的关键规范，除非另有说明。

- RSA_4096（首选）
- RSA_3072
- RSA_2048

> **Note**
>
> 不支持以下组合：ECC_NIST_P521 密钥材料、RSA_2048 公有包装密钥规范和 RSAES_OAEP_SHA_* 包装算法。
> 您不能使用 RSA_2048 公有包装密钥直接包装 ECC_NIST_P521 密钥材料。使用更大的包装密钥或 RSA_AES_KEY_WRAP_SHA_* 包装算法。

SM2 封装密钥规范（仅限中国地区）

AWS KMS 支持以下用于导入非对称密钥材料的 SM2 封装密钥的密钥规范。

- SM2

选择包装算法

要在导入过程中保护您的密钥材料，请使用下载的包装公有密钥和支持的包装算法为其加密。

AWS KMS 支持多种标准 RSA 封装算法和两步混合包装算法。通常，我们建议使用与您导入的密钥材料和包装密钥规范兼容的最安全的包装算法。通常，选择硬件安全模块 (HSM) 支持的算法或用于保护密钥材料的密钥管理系统。

下表显示了每种类型的密钥材料和 KMS 密钥支持的包装算法。算法是以首选项顺序列出的。

密钥材料	支持的包装算法和规范
对称加密密钥 256 位 AES 密钥 128 位 SM4 密钥（仅限中国区域）	包装算法： RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 已淘汰的包装算法： RSAES_PKCS1_V1 **Note** 截至 2023 年 10 月 10 日，AWS KMS 不支持 RSAES_PKCS1_V1_5 包装算法。 包装密钥规范： RSA_2048 RSA_3072 RSA_4096

密钥材料	支持的包装算法和规范
非对称 RSA 私有密钥	包装算法： RSA_AES_KEY_WRAP_SHA_256 RSA_AES_KEY_WRAP_SHA_1 SM2PKE（仅限中国区域） 包装密钥规范： RSA_2048 RSA_3072 RSA_4096 SM2（仅限中国区域）
非对称椭圆曲线（ECC）私有密钥 您不能使用 RSAES_OAEP_SHA_* 包装算法和 RSA_2048 包装密钥规范来包装 ECC_NIST_P521 密钥材料。	包装算法： RSA_AES_KEY_WRAP_SHA_256 RSA_AES_KEY_WRAP_SHA_1 RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 SM2PKE（仅限中国区域） 包装密钥规范： RSA_2048 RSA_3072 RSA_4096 SM2（仅限中国区域）

密钥材料	支持的包装算法和规范
非对称 SM2 私钥（仅限中国区域）	包装算法： RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 SM2PKE（仅限中国区域） 包装密钥规范： RSA_2048 RSA_3072 RSA_4096 SM2（仅限中国区域）
HMAC 密钥	包装算法： RSAES_OAEP_SHA_256 RSAES_OAEP_SHA_1 包装密钥规范： RSA_2048 RSA_3072 RSA_4096

> **Note**
>
> 中国区域不支持RSA_AES_KEY_WRAP_SHA_256和RSA_AES_KEY_WRAP_SHA_1包装算法。

- RSA_AES_KEY_WRAP_SHA_256 – 一种两步混合包装算法，该算法将加密密钥材料与您生成的 AES 对称密钥相结合，然后使用下载的 RSA 公有包装密钥和 RSAES_OAEP_SHA_256 包装算法对 AES 对称密钥进行加密。

封RSA_AES_KEY_WRAP_SHA_*装 RSA 私钥材料需要使用封装算法，但中国地区除外，您必须使用SM2PKE包装算法。

- RSA_AES_KEY_WRAP_SHA_1 – 一种两步混合包装算法，该算法将加密密钥材料与您生成的 AES 对称密钥相结合，然后使用下载的 RSA 包装公有密钥和 RSAES_OAEP_SHA_1 包装算法对 AES 对称密钥进行加密。

  封RSA_AES_KEY_WRAP_SHA_*装 RSA 私钥材料需要使用封装算法，但中国地区除外，您必须使用SM2PKE包装算法。
- RSAES_OAEP_SHA_256 – RSA 加密算法，使用最优非对称加密填充 (OAEP) 与 SHA-256 哈希函数。
- RSAES_OAEP_SHA_1 – RSA 加密算法，使用最优非对称加密填充 (OAEP) 与 SHA-1 哈希函数。
- RSAES_PKCS1_V1_5（已弃用；自 2023 年 10 月 10 日起，AWS KMS 不支持 RSAES_PKCS1_V1_5 包装算法）— 填充格式在 PKCS #1 版本 1.5 中定义的 RSA 加密算法。
- SM2PKE（仅限中国地区）— OSCCA 在 GM/T 0003.4-2012 中定义的基于椭圆曲线的加密算法。

主题

下载包装公有密钥和导入令牌（控制台）

您可以使用 AWS KMS 控制台下载封装公钥和导入令牌。

1. 如果您刚刚完成创建不带密钥材料的 KMS 密钥的步骤并且您位于 Download wrapping key and import token（下载包装密钥和导入令牌）页面上，请跳至 Step 9。
2. 登录 AWS Management Console 并打开 AWS Key Management Service (AWS KMS) 控制台，网址为 https://console.aws.amazon.com/kms。
3. 要更改 AWS 区域，请使用页面右上角的区域选择器。
4. 在导航窗格中，选择客户托管密钥。

> **Tip**
>
> 您只能将密钥材料导入源为外部（导入密钥材料）的 KMS 密钥中。这指示已创建不带密钥材料的 KMS 密钥。要向表中添加 Origin (源) 列，请在页面右上角，选择设置图标

()。
打开 Origin (源)，然后选择 Confirm (确认)。

5. 选择待导入的 KMS 密钥的别名或密钥 ID。
6. 选择 Cryptographic configuration（加密配置）选项卡并查看其值。这些选项卡在 General configuration（常规配置）部分下。

   您只能将密钥材料导入源为外部（导入密钥材料）的 KMS 密钥。有关创建带已导入密钥材料的 KMS 密钥的信息，请参阅 导入密钥的 AWS KMS 密钥材料。
7. 选择密钥材料选项卡，然后选择导入密钥材料。

   密钥材料选项卡仅针对源值为外部（导入密钥材料）的 KMS 密钥显示。
8. 对于选择包装密钥规范，选择您的 KMS 密钥的配置。创建此密钥后，您无法更改密钥规范。
9. 对于选择包装算法，请选择您将用于为密钥材料加密的选项。有关这些选项的详细信息，请参阅选择包装算法。
10. 选择下载包装公有密钥和导入令牌，然后保存文件。

    如果有 Next (下一步) 选项，而且要立即继续执行此过程，请选择 Next (下一步)。要稍后再继续，请选择 Cancel (取消)。
11. 解压缩 `.zip` 文件，即您在上一步 (`Import_Parameters_<key_id>_<timestamp>`) 中保存的文件。

    此文件夹包含以下文件：

    - 将公钥封装在名为的文件中`WrappingPublicKey.bin`。
    - 名为 `ImportToken.bin` 的文件中的导入令牌。
    - 名为 README.txt 的文本文件。此文件包含以下相关信息：包装公有密钥、用于为密钥材料加密的包装算法，以及包装公有密钥和导入令牌的过期日期和时间。
12. 要继续执行此过程，请参阅为您的密钥材料加密。

下载封装公钥和导入令牌 (AWS KMS API)

要下载公钥和导入令牌，请使用 GetParametersForImportAPI。指定将与导入的密钥材料关联的 KMS 密钥。此 KMS 密钥的 Origin 值必须为 `EXTERNAL`。

此示例指定了 RSA_AES_KEY_WRAP_SHA_256 包装算法、RSA_3072 包装公有密钥规范和示例密钥 ID。将这些示例值替换为有效的下载值。在该操作中，对于密钥 ID，您可以使用密钥 ID 或密钥 ARN，但不能使用别名名称或别名 ARN。

```
$ 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
```

该命令成功执行后，您会看到类似以下内容的输出：

```
{
    "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)"
}
```

为了准备下一步的数据，base64 会对公有密钥和导入令牌进行解码，并将解码后的值保存在文件中。

要对公有密钥进行 base64 解码并导入令牌：

1. 复制 base64 编码公有密钥 (由示例输出中*#### (base64 ##)* 表示)，将其粘贴到新文件中，然后保存文件。向文件提供一个描述性名称，例如 PublicKey.b64。
2. 使用 OpenSSL 对文件的内容进行 base64 解码，然后将解码后的数据保存到一个新文件中。以下示例会对您在上一步骤 (PublicKey.b64) 中保存的文件中的数据进行解码，并将输出保存到一个名为 WrappingPublicKey.bin 的新文件中。

   ```
   $ openssl enc -d -base64 -A -in PublicKey.b64 -out WrappingPublicKey.bin
   ```

3. 复制 base64 编码导入令牌 (由示例输出中*#### (base64 ##)*表示)，将其粘贴到新文件中，然后保存文件。为文件指定一个描述性名称，例如 importtoken.b64。
4. 使用 OpenSSL 对文件的内容进行 base64 解码，然后将解码后的数据保存到一个新文件中。以下示例会对您在上一步骤 (ImportToken.b64) 中保存的文件中的数据进行解码，并将输出保存到一个名为 ImportToken.bin 的新文件中。

   ```
   $ openssl enc -d -base64 -A -in importtoken.b64 -out ImportToken.bin
   ```

继续执行步骤 3：加密密钥材料。

导入密钥材料步骤 3：加密密钥材料

下载公有密钥和导入令牌后，使用您下载的公有密钥和指定的包装算法对密钥材料进行加密。如果您需要替换公有密钥或导入令牌，或者更改包装算法，则必须下载新的公有密钥和导入令牌。有关 AWS KMS 支持的公钥和封装算法的信息，请参阅选择包装公有密钥规范和选择包装算法。

密钥材料必须采用二进制格式。有关详细信息，请参阅导入密钥材料的要求。

> **Note**
>
> 对于非对称密钥对，仅加密和导入私钥。 AWS KMS 从私钥派生公钥。
> 不支持以下组合：ECC_NIST_P521 密钥材料、RSA_2048 公有包装密钥规范和 RSAES_OAEP_SHA_* 包装算法。
> 您不能使用 RSA_2048 公有包装密钥直接包装 ECC_NIST_P521 密钥材料。使用更大的包装密钥或 RSA_AES_KEY_WRAP_SHA_* 包装算法。
> 中国区域不支持 RSA_AES_KEY_WRAP_SHA_256 和 RSA_AES_KEY_WRAP_SHA_1 包装算法。

通常，您可以在将密钥材料从硬件安全模块 (HSM) 或密钥管理系统导出时对其进行加密。有关如何以二进制格式导出密钥材料的信息，请参阅有关 HSM 或密钥管理系统的文档。您还可以参阅以下部分，该部分使用 OpenSSL 提供了概念验证演示。

加密密钥材料时，请使用与您在下载公有密钥和导入令牌时指定的相同的包装算法。要查找您指定的包装算法，请查看关联GetParametersForImport请求的 CloudTrail 日志事件。

生成用于测试的密钥材料

以下 OpenSSL 命令生成每种支持类型的密钥材料以供测试。这些示例仅用于测试和 proof-of-concept 演示。对于生产系统，请使用更安全的方法来生成您的密钥材料，例如硬件安全模块或密钥管理系统。

要将非对称密钥对的私有密钥转换为 DER 编码格式，请将密钥材料生成命令传送到以下 `openssl pkcs8` 命令。`topk8` 参数指示 OpenSSL 将私有密钥作为输入并返回 PKCS#8 格式的密钥。（默认行为恰恰相反。）

```
openssl pkcs8 -topk8 -outform der -nocrypt
```

以下命令为每种支持的密钥类型生成测试密钥材料。

- 对称加密密钥（32 字节）

  此命令生成 256 位的对称密钥（32 字节的随机字符串）并将其保存在 PlaintextKeyMaterial.bin 文件中。您无需对这些密钥材料进行编码。

```
openssl rand -out PlaintextKeyMaterial.bin 32
```

  仅在中国区域，您必须生成 128 位的对称密钥（16 字节的随机字符串）。

```
openssl rand -out PlaintextKeyMaterial.bin 16
```

- HMAC 密钥

  此命令生成指定大小的随机字节字符串。您无需对这些密钥材料进行编码。

  您的 HMAC 密钥的长度必须与 KMS 密钥的密钥规范定义的长度相匹配。例如，如果 KMS 密钥为 HMAC_384，则必须导入 384 位（48 字节）的密钥。

```
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
```

- RSA 私有密钥

```
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
```

- ECC 私有密钥

```
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
```

- SM2 私钥（仅限中国区域）

```
openssl genpkey -algorithm ec -pkeyopt ec_paramgen_curve:sm2 | openssl pkcs8 -topk8 -
outform der -nocrypt > SM2_PrivateKey.der
```

使用 OpenSSL 加密密钥材料的示例

以下示例说明如何使用 OpenSSL 通过您下载的公有密钥对密钥材料进行加密。要使用 SM2 公钥加密密钥材料（仅限中国区域），请使用该SM2OfflineOperationHelper类。

> **Important**
>
> 这些示例仅为概念验证演示。对于生产系统，请使用更安全的方法 (如商业 HSM 或密钥管理系统) 来生成和存储您的密钥材料。
> 不支持以下组合：ECC_NIST_P521 密钥材料、RSA_2048 公有包装密钥规范和 RSAES_OAEP_SHA_* 包装算法。
> 您不能使用 RSA_2048 公有包装密钥直接包装 ECC_NIST_P521 密钥材料。使用更大的包装密钥或 RSA_AES_KEY_WRAP_SHA_* 包装算法。

RSAES_OAEP_SHA_1

AWS KMS 支持对称加密密钥 (SYMMETRIC_DEFAULT)、椭圆曲线 (ECC) 私钥、SM2 私钥和 HMAC 密钥的 RSAES_OAEP_SHA_1。

RSAES_OAEP_SHA_1 不支持 RSA 私有密钥。此外，您不能使用采用任何 RSAES_OAEP_SHA_* 包装算法的 RSA_2048 公有包装密钥来包装 ECC_NIST_P521（secp521r1）私有密钥。您必须使用更大的公有包装密钥或 RSA_AES_KEY_WRAP 包装算法。

以下示例使用您下载的公有密钥和 RSAES_OAEP_SHA_1 包装算法对密钥材料进行加密，并将其保存在 EncryptedKeyMaterial.bin 文件中。

在本示例中：

- *WrappingPublicKey.bin* 是包含下载的包装公有密钥的文件。
- *PlaintextKeyMaterial.bin* 是包含您正在加密的密钥材料的文件，例如 PlaintextKeyMaterial.bin、HMAC_384_PlaintextKey.bin 或 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 支持对称加密密钥 (SYMMETRIC_DEFAULT)、椭圆曲线 (ECC) 私钥、SM2 私钥和 HMAC 密钥的 RSAES_OAEP_SHA_256。

RSAES_OAEP_SHA_256 不支持 RSA 私有密钥。此外，您不能使用采用任何 RSAES_OAEP_SHA_* 包装算法的 RSA_2048 公有包装密钥来包装 ECC_NIST_P521（secp521r1）私有密钥。您必须使用更大的公有密钥或 RSA_AES_KEY_WRAP 包装算法。

以下示例使用您下载的公有密钥和 RSAES_OAEP_SHA_256 包装算法对密钥材料进行加密，并将其保存在 EncryptedKeyMaterial.bin 文件中。

在本示例中：

- *WrappingPublicKey.bin* 是包含已下载的公有包装密钥的文件。如果您是从控制台下载的公有密钥，则此文件的名称为 wrappingKey_*KMS key_key_ID_timestamp*（例如，wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909）。

- *PlaintextKeyMaterial.bin* 是包含您正在加密的密钥材料的文件，例如 PlaintextKeyMaterial.bin、HMAC_384_PlaintextKey.bin 或 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

RSA_AES_KEY_WRAP_SHA_1 包装算法涉及两个加密操作。

1. 使用您生成的 AES 对称密钥和 AES 对称加密算法对密钥材料进行加密。
2. 使用您下载的公有密钥和 RSAES_OAEP_SHA_1 包装算法加密您使用的 AES 对称密钥。

AWS KMS 支持 RSA_AES_KEY_WRAP_SHA_* 封装算法，适用于所有支持的导入密钥材料类型和所有支持的公钥规范。RSA_AES_KEY_WRAP_SHA_* 算法是唯一支持包装 RSA 密钥材料的包装算法。

RSA_AES_KEY_WRAP_SHA_1 包装算法需要 OpenSSL 版本 3.x 或更高版本。

1. 生成 256 位 AES 对称加密密钥

   此命令生成由 256 个随机位组成的 AES 对称加密密钥，并将其保存在 aes-key.bin 文件中

   ```
   # Generate a 32-byte AES symmetric encryption key
   $ openssl rand -out aes-key.bin 32
   ```

2. 使用 AES 对称加密密钥加密您的密钥材料

   此命令使用 AES 对称加密密钥对您的密钥材料进行加密，并将加密的密钥材料保存在 key-material-wrapped.bin 文件中。

在此示例命令中：

- *PlaintextKeyMaterial.bin* 是包含您要导入的密钥材料的文件，例如 PlaintextKeyMaterial.bin、HMAC_384_PlaintextKey.bin、RSA_3072_PrivateKey.
  或 ECC_NIST_P521_PrivateKey.der。
- *aes-key.bin* 是包含您在上一个命令中生成的 256 位 AES 对称加密密钥的文件。

```
# 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. 使用公有密钥加密您的 AES 对称加密密钥

此命令使用您下载的公有密钥和 RSAES_OAEP_SHA_1 包装算法对您的 AES 对称加密密钥进行加密，对其进行 DER 编码，然后将其保存在 aes-key-wrapped.bin 文件中。

在此示例命令中：

- *WrappingPublicKey.bin* 是包含已下载的公有包装密钥的文件。如果您是从控制台下载的公有密钥，则此文件的名称为 wrappingKey_*KMS key_key_ID_timestamp*（例如，wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909
- *aes-key.bin* 是包含您在本示例序列的第一个命令中生成的 256 位 AES 对称加密密钥的文件。

```
# 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. 生成要导入的文件

   将文件与加密的密钥材料连接起来，并将文件与加密的 AES 密钥连接起来。将它们保存在 EncryptedKeyMaterial.bin 文件中，也就是您要在 步骤 4：导入密钥材料 中导入的文件。

   在此示例命令中：

   - *key-material-wrapped.bin* 是包含您的已加密密钥材料的文件。
   - *aes-key-wrapped.bin* 是包含已加密 AES 加密密钥的文件。

```
# 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

RSA_AES_KEY_WRAP_SHA_256 包装算法涉及两个加密操作。

1. 使用您生成的 AES 对称密钥和 AES 对称加密算法对密钥材料进行加密。
2. 使用您下载的公有密钥和 RSAES_OAEP_SHA_256 包装算法加密您使用的 AES 对称密钥。

AWS KMS 支持 RSA_AES_KEY_WRAP_SHA_* 封装算法，适用于所有支持的导入密钥材料类型和所有支持的公钥规范。RSA_AES_KEY_WRAP_SHA_* 算法是唯一支持包装 RSA 密钥材料的包装算法。

RSA_AES_KEY_WRAP_SHA_256 包装算法需要 OpenSSL 版本 3.x 或更高版本。

1. 生成 256 位 AES 对称加密密钥

   此命令生成由 256 个随机位组成的 AES 对称加密密钥，并将其保存在 aes-key.bin 文件中

```
# Generate a 32-byte AES symmetric encryption key
$ openssl rand -out aes-key.bin 32
```

2. 使用 AES 对称加密密钥加密您的密钥材料

   此命令使用 AES 对称加密密钥对您的密钥材料进行加密，并将加密的密钥材料保存在 key-material-wrapped.bin 文件中。

在此示例命令中：

- *PlaintextKeyMaterial.bin* 是包含您要导入的密钥材料的文件，例如 PlaintextKeyMaterial.bin、HMAC_384_PlaintextKey.bin、RSA_3072_PrivateKey.
  或 ECC_NIST_P521_PrivateKey.der。
- *aes-key.bin* 是包含您在上一个命令中生成的 256 位 AES 对称加密密钥的文件。

```
# 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. 使用公有密钥加密您的 AES 对称加密密钥

此命令使用您下载的公有密钥和 RSAES_OAEP_SHA_256 包装算法对您的 AES 对称加密密钥进行加密，对其进行 DER 编码，然后将其保存在 aes-key-wrapped.bin 文件中。

在此示例命令中：

- *WrappingPublicKey.bin* 是包含已下载的公有包装密钥的文件。如果您是从控制台下载的公有密钥，则此文件的名称为 wrappingKey_*KMS key_key_ID_timestamp*（例如，wrappingKey_f44c4e20-f83c-48f4-adc6-a1ef38829760_0809092909
- *aes-key.bin* 是包含您在本示例序列的第一个命令中生成的 256 位 AES 对称加密密钥的文件。

```
# 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. 生成要导入的文件

   将文件与加密的密钥材料连接起来，并将文件与加密的 AES 密钥连接起来。将它们保存在 EncryptedKeyMaterial.bin 文件中，也就是您要在 步骤 4：导入密钥材料 中导入的文件。

   在此示例命令中：

   - *key-material-wrapped.bin* 是包含您的已加密密钥材料的文件。
   - *aes-key-wrapped.bin* 是包含已加密 AES 加密密钥的文件。

```
# Combine the encrypted AES key and encrypted key material in a file
$ cat aes-key-wrapped.bin key-material-wrapped.bin > EncryptedKeyMaterial.bin
```

继续执行步骤 4：导入密钥材料。

导入密钥材料步骤 4：导入密钥材料

在加密密钥材料之后，您可以导入密钥材料，以将其与 AWS KMS key 配合使用。要导入密钥材料，请上传在步骤 3：加密密钥材料中加密的密钥材料以及在步骤 2：下载包装公有密钥和导入令牌中下载的导入令牌。您必须将密钥材料导入您在下载公有密钥和导入令牌时指定的同一 KMS 密钥中。成功导入密钥材料时，KMS 密钥的密钥状态会更改为 Enabled，您可以在加密操作中使用 KMS 密钥。

当您导入密钥材料时，您可以为密钥材料设置可选的过期日期。当密钥材料过期后，AWS KMS 将删除密钥材料，并且 KMS 密钥将变为不可用。要在加密操作中使用该 KMS 密钥，您必须重新导入相同的密钥材料。导入密钥材料后，无法设置、更改或取消当前导入的到期日期。要更改这些值，您必须删除并重新导入相同的密钥材料。

要导入密钥材料，您可以使用AWS KMS控制台或 ImportKeyMaterialAPI。您也可以通过发出 HTTP 请求，或使用 AWS 开发工具包、AWS Command Line Interface 或 AWS Tools for PowerShell 直接使用 API。

导入密钥材料时，会在AWS CloudTrail日志中添加一个记录ImportKeyMaterial操作的ImportKeyMaterial条目。无论您使用AWS KMS控制台还是 AWS KMS API， CloudTrail 条目都是一样的。

设置过期时间（可选）

导入 KMS 密钥的密钥材料时，可以将密钥材料的可选过期日期和时间设置为自导入之日起 365 天中的任意一天。当导入的密钥材料过期后，AWS KMS 会将其删除。此操作会将 KMS 密钥的密钥状态更改为 `PendingImport`，这将阻止在任何加密操作中使用该密钥。要使用 KMS 密钥，您必须重新导入原始密钥材料的副本。

确保导入的密钥材料经常过期，可帮助您满足监管要求，但这样做会给在 KMS 密钥下加密的数据带来额外的风险。在您重新导入原始密钥材料的副本之前，包含过期密钥材料的 KMS 密钥不可用，并且在 KMS 密钥下加密的任何数据都不可访问。如果您出于任何原因未能重新导入密钥材料（例如，丢失原始密钥材料的副本），则 KMS 密钥将永久不可用，在 KMS 密钥下加密的数据将无法恢复。

为了降低这种风险，请确保导入的密钥材料副本可访问，并设计一个系统，以在密钥材料过期并中断您的 AWS 工作负载之前将其删除并重新导入。我们建议您针对导入的密钥材料的过期设置警报，这样您就有足够的时间在密钥材料过期之前重新导入密钥材料。您还可以使用 CloudTrail 日志来审核导入（和重新导入）密钥材料和删除导入的密钥材料的AWS KMS操作，以及删除过期密钥材料的操作。

您无法将不同的密钥材料导入 KMS 密钥，AWS KMS 也无法还原、恢复或重现已删除的密钥材料。您可以通过编程定期删除和重新导入已导入的密钥材料，而无需设置过期时间，但是保留原始密钥材料副本的要求相同。

在导入密钥材料时，确定导入的密钥材料是否以及何时过期。但是您可以开启和关闭过期时间，也可以通过删除和重新导入密钥材料来设置新的过期时间。使用`ExpirationModel`参数开启过期时间 (`KEY_MATERIAL_EXPIRES`) 和关闭 (`KEY_MATERIAL_DOES_NOT_EXPIRE`)，使用`ValidTo`参数设置到期时间。ImportKeyMaterial自导入数据起的最大天数为 365 天；没有最短天数，但必须是未来时间。

导入密钥材料（控制台）

您可以使用 AWS Management Console导入密钥材料。

1. 如果您在上传已包装的密钥材料页面上，请跳至 Step 8。
2. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
3. 要更改 AWS 区域，请使用页面右上角的区域选择器。
4. 在导航窗格中，选择客户托管密钥。
5. 选择已为其下载公有密钥和导入令牌的 KMS 密钥的密钥 ID 或别名。
6. 选择 Cryptographic configuration（加密配置）选项卡并查看其值。这些选项卡位于 General configuration（常规配置）部分下 KMS 密钥的详细信息页面上。

您只能将密钥材料导入源为外部（导入密钥材料）的 KMS 密钥。有关创建带已导入密钥材料的 KMS 密钥的信息，请参阅 导入密钥的 AWS KMS 密钥材料。

7. 选择密钥材料选项卡，然后选择导入密钥材料。密钥材料选项卡仅针对源值为外部（导入密钥材料）的 KMS 密钥显示。

   如果您下载了密钥材料、导入令牌并加密了密钥材料，请选择下一步。

8. 在加密的密钥材料和导入令牌部分，执行以下操作。

   a. 在包装的密钥材料下，选择选择文件。然后上传包含您的已包装（已加密）密钥材料的文件。

   b. 在导入令牌下，选择选择文件。上传包含您已下载的导入令牌的文件。

9. 在 Expiration option (过期选项) 部分中，确定密钥材料是否过期。要设置到期日期和时间，请选择 Key material expires (密钥材料过期)，并使用日历选择日期和时间。您可以指定的日期距当前日期和时间最多 365 天。

10. 选择 Upload key material (上传密钥材料)。

导入密钥材料 (AWS KMS API)

要导入密钥材料，请使用ImportKeyMaterial操作。以下示例使用 AWS CLI，但您可以使用受支持的任何编程语言。

要使用此示例，请执行以下操作：

1. 将 *1234abcd-12ab-34cd-56ef-1234567890ab* 替换为您在下载公有密钥和导入令牌时指定的 KMS 密钥的密钥 ID。要标识 KMS 密钥，请使用其密钥 ID 或密钥 ARN。该操作不能使用别名或别名 ARN。
2. 将 *EncryptedKeyMaterial.bin* 替换为包含加密的密钥材料的文件的名称。
3. 将 *ImportToken.bin* 替换为包含导入令牌的文件的名称。
4. 如果希望导入的密钥材料过期，请将 `expiration-model` 参数的值设置为其默认值 `KEY_MATERIAL_EXPIRES`，或省略 `expiration-model` 参数。然后，将 `valid-to` 参数的值替换为您希望密钥材料过期的日期和时间。日期和时间最长为请求时间起 365 天。

```
$ 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
```

如果不希望导入的密钥材料过期，请将 expiration-model 参数的值设置为 KEY_MATERIAL_DOES_NOT_EXPIRE，并从命令中省略 valid-to 参数。

```
$ 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**
>
> 如果命令不成功，则可能会看到 KMSInvalidStateException 或 NotFoundException。您可以重试请求。

自定义密钥存储

密钥存储 是用于存储加密密钥的安全位置。AWS KMS 中的默认密钥存储还支持生成和管理其存储的密钥的方法。默认情况下，您在 AWS KMS 中创建的 AWS KMS keys 在硬件安全模块（HSM）中生成并受其保护，这些模块是 FIPS 140-2 验证的加密模块。KMS 密钥的密钥材料绝不会让 HSM 处于未加密状态。

不过，如果您需要加强对 HSM 的控制，则可以创建自定义密钥存储。

自定义密钥存储是 AWS KMS 中的逻辑密钥存储，由您拥有和管理的 AWS KMS 之外的密钥管理器提供支持。自定义密钥存储将 AWS KMS 的方便、全面的密钥管理界面与拥有和控制密钥材料和加密操作的能力结合。在自定义密钥存储中使用 KMS 密钥时，加密操作实际上是通过您的密钥管理器使用您的加密密钥来执行。因此，您对加密密钥的可用性和持久性以及 HSM 的运行承担更多责任。

AWS KMS 支持两种类型的自定义密钥存储。

- AWS CloudHSM 密钥存储是由 AWS CloudHSM 集群支持的 AWS KMS 自定义密钥存储。当您在 AWS CloudHSM 密钥存储中创建 KMS 密钥时，AWS KMS 将在关联的 AWS CloudHSM 集群中生成 256 位、持久且不可导出的高级加密标准（AES）对称密钥。此密钥材料绝不会让您的 AWS CloudHSM 集群处于未加密状态。当在 AWS CloudHSM 密钥存储中使用 KMS 密钥时，集群中的 HSM 中会执行加密操作。AWS CloudHSM 集群由经 FIPS 140-2 3 级认证的的硬件安全模块（HSM）提供支持。

- 外部密钥存储是由您在 AWS 之外拥有和控制的外部密钥管理器所支持的 AWS KMS 自定义密钥存储。在使用外部密钥存储中的 KMS 密钥时，将使用加密密钥通过外部密钥管理器执行解密操作。外部密钥存储旨在支持来自不同供应商的各种外部密钥管理器。

  AWS KMS 绝不会直接查看、访问您的外部密钥管理器或与您的外部密钥管理器或加密密钥交互。在使用外部密钥存储中的 KMS 密钥加密或解密时，将使用外部密钥通过外部密钥管理器执行操作。您保留对加密密钥的完全控制权，包括无需与 AWS 交互即可拒绝或停止加密操作的能力。但是，由于距离和额外的处理，外部密钥存储中的 KMS 密钥的延迟性可能会较高、性能可能会较差，并且可能有与 AWS KMS 中的包含密钥材料的 KMS 密钥不同的可用性特征。有关与 AWS KMS 外部密钥存储功能兼容的密钥管理器的更多信息，请参阅《AWS Key Management Service 常见问题》中的哪些外部供应商支持 XKS 代理规范？。

这两种类型的自定义密钥存储与标准 AWS KMS 密钥存储不同，两种类型之间也有很大不同。他们的安全模型、责任范围、性能、价格和用例也大不相同。在选择自定义密钥存储之前，请阅读相关文档，确认额外的配置和维护责任是针对额外控制的明智的权衡之举。但是，如果您操作所依据的规则和条例要求直接控制密钥材料，那么自定义密钥存储可能是一个不错的选择。

不支持的功能

AWS KMS 在自定义密钥存储中不支持以下功能。

- 非对称 KMS 密钥
- 非对称数据密钥对
- HMAC KMS 密钥
- 具有导入密钥材料的 KMS 密钥
- 自动密钥轮换
- 多区域密钥

主题

- AWS CloudHSM 钥匙库
- 外部密钥存储

AWS CloudHSM 钥匙库

密 AWS CloudHSM 钥库是由集AWS CloudHSM 群支持的自定义密钥存储库。在自定义密钥存储AWS KMS key中创建时， AWS KMS 会在您拥有和管理的 AWS CloudHSM 集群中为 KMS 密钥生成和存

储不可提取的密钥材料。在自定义密钥存储中使用 KMS 密钥时，会在集群中的 HSM 中执行加密操作。此功能结合了的便利性和广泛集 AWS KMS 成，并增加了对 AWS CloudHSM 集群的控制 AWS 账户。

AWS KMS 为创建、使用和管理自定义密钥存储库提供全面的控制台和 API 支持。在自定义密钥存储中使用 KMS 密钥的方式，与使用任何 KMS 密钥相同。例如，您可以使用 KMS 密钥生成数据密钥和加密数据。您还可以将自定义密钥存储库中的 KMS 密钥与支持客户托管密钥的 AWS 服务一起使用。

我是否需要自定义密钥存储？

对于大多数用户来说，由 FIPS 140-2 验证的加密模块保护的默认 AWS KMS 密钥库可以满足他们的安全要求。无需添加额外的维护责任层或额外服务的依赖项。

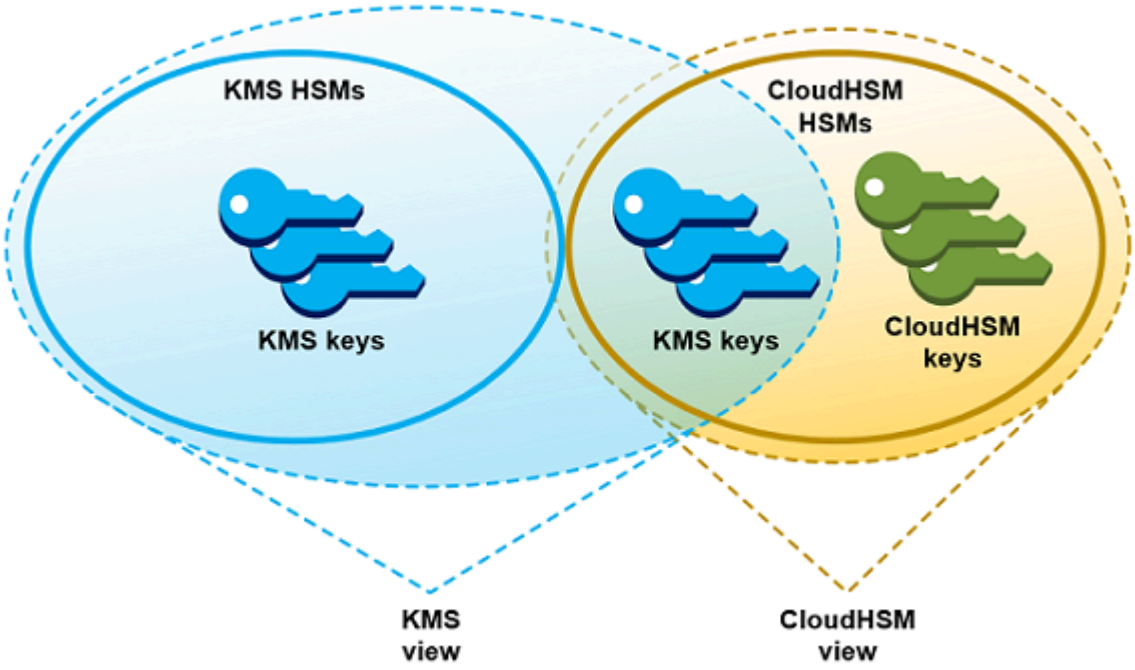
但是，如果您的组织具有以下任何要求，则可能要考虑创建自定义密钥存储：

- 在单租户 HSM 或您可以直接控制的 HSM 中，您有明确要求保护的密钥。
- 您需要能够立即从中移除密钥材料 AWS KMS。
- 您需要能够独立于 AWS KMS 或审核密钥的所有使用情况 AWS CloudTrail。

自定义密钥存储如何工作？

每个自定义密钥存储库都与您的集 AWS CloudHSM 群相关联 AWS 账户。当您将自定义密钥库连接到其集群时， AWS KMS 会创建支持该连接的网络基础架构。然后，它使用集群中专用加密用户的凭据登录到集群中的密钥 AWS CloudHSM 客户端。

您可以在中创建和管理您的自定义密钥存储， AWS KMS 并在中创建和管理您的 HSM 集群。 AWS CloudHSM在 AWS KMS 自定义密钥存储 AWS KMS keys 中创建时，可以在中查看和管理 KMS 密钥 AWS KMS。但是，您也可以在中查看和管理他们的密钥材料 AWS CloudHSM，就像在集群中查看和管理其他密钥一样。



您可以使用自定义密钥存储库 AWS KMS 中生成的密钥材料创建对称加密 KMS 密钥。然后，使用与在密钥库中用于密钥库中的 KMS 密钥相同的方法来查看和管理自定义密钥存储区中的 AWS KMS KMS 密钥。您可以使用 IAM 和密钥策略控制访问，创建标签和别名，启用和禁用 KMS 密钥，以及计划密钥删除。您可以使用 KMS 密钥进行加密操作，并将其与集成的 AWS 服务一起 AWS KMS使用。

此外，您可以完全控制 AWS CloudHSM 集群，包括创建和删除 HSM 以及管理备份。您可以使用 AWS CloudHSM 客户端和支持的软件库来查看、审计和管理 KMS 密钥的密钥材料。当自定义密钥存储断开连接时， AWS KMS 无法对其进行访问，用户也无法使用自定义密钥存储区中的 KMS 密钥进行加密操作。增加的控制层使自定义密钥存储成为需要它的组织的强大解决方案。

从何处开始？

要创建和管理 AWS CloudHSM 密钥库，您可以使用 AWS KMS 和的功能 AWS CloudHSM。

1. 从... 开始 AWS CloudHSM。创建活动 AWS CloudHSM 集群或选择现有集群。集群必须在不同的可用区中具有至少两个活动 HSM。然后，在该集群中为 AWS KMS创建一个专用加密用户 (CU) 账户。
2. 在中 AWS KMS，创建与所选 AWS CloudHSM 集群关联的自定义密钥库。 AWS KMS 提供了一个完整的管理界面，允许您创建、查看、编辑和删除自定义密钥库。

3. 准备好使用自定义密钥库时，请将其连接到其关联的 AWS CloudHSM 集群。 AWS KMS 创建支持连接所需的网络基础架构。之后，它将使用专用加密用户账户凭证登录集群，以便它可以在集群中生成和管理密钥材料。
4. 现在，您可以在自定义密钥存储中创建对称加密 KMS 密钥。在创建 KMS 密钥时指定自定义密钥存储。

如果您在任何时候遇到困难，都可以在对自定义密钥存储进行故障排除主题中查找帮助。如果您的问题未得到解答，请使用本指南的每页底部的反馈链接或在 AWS Key Management Service 开发论坛上发布问题。

配额

AWS KMS 允许每个 AWS 账户 和区域中最多有 10 个自定义密钥存储库，包括AWS CloudHSM 密钥存储库和外部密钥存储库，无论它们的连接状态如何。此外，在密钥存储中使用 KMS 密钥还有 AWS KMS 请求配额。 AWS CloudHSM

定价

有关 AWS KMS 自定义密钥存储库和客户托管密钥在自定义密钥存储库中的成本的信息，请参阅AWS Key Management Service 定价。有关 AWS CloudHSM 集群和 HSM 成本的信息，请参阅AWS CloudHSM 定价。

区域

AWS KMS 除了亚太地区（墨尔本）、中国（北京）、中国（宁夏）和欧洲（西班牙）之外，在所有支持 AWS 区域 的地方 AWS KMS 都支持 AWS CloudHSM 密钥存储。

不支持的功能

AWS KMS 不支持自定义密钥存储库中的以下功能。

- 非对称 KMS 密钥
- 非对称数据密钥对
- HMAC KMS 密钥
- 具有导入密钥材料的 KMS 密钥
- 自动密钥轮换
- 多区域密钥

主题

AWS CloudHSM 密钥存储概念

本主题介绍了 AWS CloudHSM 密钥存储中使用的一些概念。

AWS CloudHSM 密钥存储

AWS CloudHSM 密钥存储是与您拥有和管理的 AWS CloudHSM 集群的关联的自定义密钥存储。AWS CloudHSM 集群由经 FIPS 140-2 3 级认证的硬件安全模块（HSM）提供支持。

当您在 AWS CloudHSM 密钥存储中创建 KMS 密钥时，AWS KMS 将在关联的 AWS CloudHSM 集群中生成 256 位、持久且不可导出的高级加密标准（AES）对称密钥。此密钥材料绝不会让您的 HSM 处于未加密状态。在 AWS CloudHSM 密钥存储中使用 KMS 密钥时，会在集群中的 HSM 中执行加密操作。

AWS CloudHSM 密钥存储将 AWS KMS 的方便、全面的密钥管理界面与 AWS 账户 中的 AWS CloudHSM 集群提供的额外控制相结合。此集成功能可让您在 AWS KMS 中创建、管理和使用 KMS 密钥，同时保持对存储 KMS 密钥的密钥材料的 HSM 的完全控制，包括管理集群、HSM 和备份。您可以使用 AWS KMS 控制台和 API 来管理 AWS CloudHSM 密钥存储及其 KMS 密钥。您还可以使用 AWS CloudHSM 控制台、API、客户端软件和关联的软件库来管理关联的集群。

您可以查看和管理您的 AWS CloudHSM 密钥存储、编辑其属性，并将其与关联的 AWS CloudHSM 集群连接和断开连接。如果您需要删除 AWS CloudHSM 密钥存储，则必须先删除 AWS CloudHSM 密钥存储中的 KMS 密钥，方法为计划其删除并等到宽限期结束。删除 AWS CloudHSM 密钥存储会从 AWS KMS 中移除资源，但不会影响您的 AWS CloudHSM 集群。

AWS CloudHSM 集群

每个 AWS CloudHSM 密钥存储均与一个 AWS CloudHSM 集群关联。当您在 AWS CloudHSM 密钥存储中创建 AWS KMS key 时，AWS KMS 将在关联的集群中创建其密钥材料。当您在 AWS CloudHSM 密钥存储中使用 KMS 密钥时，将在关联的集群中执行加密操作。

每个 AWS CloudHSM 集群只能与一个 AWS CloudHSM 密钥存储关联。您选择的集群无法与另一个 AWS CloudHSM 密钥存储关联或无法和与其他 AWS CloudHSM 密钥存储关联的集群共享备份历

史记录。集群必须初始化且处于活动状态，并且必须与 AWS CloudHSM 密钥存储位于相同的 AWS 账户 和区域中。您可以创建新集群或使用现有集群。AWS KMS 不需要集群的专用权。要在 AWS CloudHSM 密钥存储中创建 KMS 密钥，其关联的集群必须包含至少两个活动 HSM。所有其他操作都只需要一个 HSM。

您在创建 AWS CloudHSM 密钥存储时指定 AWS CloudHSM 集群，并且无法更改它。但是，您可以替换与原始集群共享备份历史记录的任何集群。这样，您就可以删除该集群（如有必要），然后将它替换为从其备份之一创建的集群。您可以完全控制关联的 AWS CloudHSM 集群，从而能管理用户和密钥、创建和删除 HSM 以及使用和管理备份。

当您准备好使用 AWS CloudHSM 密钥存储时，您可以将其连接到关联的 AWS CloudHSM 集群。您可以随时连接和断开自定义密钥存储。连接自定义密钥存储后，您可以创建和使用其 KMS 密钥。断开密钥存储后，您可以查看和管理 AWS CloudHSM 密钥存储及其 KMS 密钥。但您无法创建新 KMS 密钥或在 AWS CloudHSM 密钥存储中使用 KMS 密钥以进行加密操作。

`kmsuser` 加密用户

为了代表您创建和管理关联的 AWS CloudHSM 集群中的密钥材料，AWS KMS 在名为 `kmsuser` 的集群中使用专用的 AWS CloudHSM 加密用户 (CU)。`kmsuser` CU 是一个标准 CU 账户，它将自动同步到集群中的所有 HSM 并保存在集群备份中。

在创建 AWS CloudHSM 密钥存储之前，您在 cloudhsm_mgmt_util 中使用 createUser 命令在您的 AWS CloudHSM 集群中创建 `kmsuser` CU 账户。然后，当您创建 AWS CloudHSM 密钥存储时，您向 AWS KMS 提供 `kmsuser` 账户密码。当您连接自定义密钥存储时，AWS KMS 将以 `kmsuser` CU 身份登录到集群并轮换其密码。AWS KMS 会在安全存储之前对您的 `kmsuser` 密码进行加密。轮换密码时，新密码也会以相同的方式加密和存储。

只要 AWS CloudHSM 密钥存储处于连接状态，AWS KMS 将保持以 `kmsuser` 身份登录。您不应将此 CU 账户用于其他目的。但是，您保留对 `kmsuser` CU 账户的最终控制权。您可以随时查找 `kmsuser` 拥有的密钥的密钥句柄。必要时，您可以断开自定义密钥存储，更改 `kmsuser` 密码，以 `kmsuser` 身份登录到集群并查看和管理 `kmsuser` 拥有的密钥。

有关创建 `kmsuser` CU 账户的说明，请参阅创建 `kmsuser` 加密用户。

在 AWS CloudHSM 密钥存储中的 KMS 密钥

您可以使用 AWS KMS 或 AWS KMS API 在 AWS CloudHSM 密钥存储中创建 AWS KMS keys。您将使用对任何 KMS 密钥使用的同一方法。唯一的区别在于您必须标识 AWS CloudHSM 密钥存储并指定密钥材料的源是 AWS CloudHSM 集群。

当您在 AWS CloudHSM 密钥存储中创建一个 KMS 密钥时，AWS KMS 将在 AWS KMS 中创建 KMS 密钥，并在其关联集群中生成 256 位、持久且不可导出的高级加密标准（AES）对称密钥材料。在加密操作中使用 AWS KMS 密钥时，该操作将在 AWS CloudHSM 集群中使用基于集群的 AES 密钥执行。尽管 AWS CloudHSM 支持不同类型的对称和非对称密钥，但 AWS CloudHSM 密钥存储仅支持 AES 对称加密密钥。

您可以在 AWS KMS 控制台中查看 AWS CloudHSM 密钥存储中的 KMS 密钥，并使用控制台选项显示自定义密钥存储 ID。您还可以使用该DescribeKey操作来查找AWS CloudHSM密钥库 ID 和AWS CloudHSM集群 ID。

AWS CloudHSM 密钥存储中的 KMS 密钥与 AWS KMS 中的任何 KMS 密钥的工作方式相同。授权用户需要相同的权限来使用和管理 KMS 密钥。您可使用相同的控制台过程和 API 操作来查看和管理 AWS CloudHSM 密钥存储中的 KMS 密钥。这包括启用和禁用 KMS 密钥、创建和使用标签和别名以及设置和更改 IAM 和密钥策略。您可以使用 AWS CloudHSM 密钥存储中的 KMS 密钥进行加密操作，并将它们与支持使用客户托管密钥的集成 AWS 服务结合使用。但是，您不能启用自动密钥轮换或者将密钥材料导入 AWS CloudHSM 密钥存储中的 KMS 密钥。

您还可以将相同的过程用于 AWS CloudHSM 密钥存储中的 KMS 密钥的计划删除。在等待期限结束后，AWS KMS 将从 KMS 中删除 KMS 密钥。然后，它将尽可能从关联的 AWS CloudHSM 集群中删除 KMS 密钥的密钥材料。但是，您可能需要从集群及其备份中手动删除孤立密钥材料。

控制对 AWS CloudHSM 密钥存储的访问

您可以使用 IAM policy 控制对 AWS CloudHSM 密钥存储和 AWS CloudHSM 集群的访问。您可以使用密钥策略、IAM policy 和授权来控制对 AWS CloudHSM 密钥存储中的 AWS KMS keys 的访问。我们建议您仅向用户、组和角色提供他们可能执行的任务所需的权限。

主题

- 向 AWS CloudHSM 密钥存储管理员和用户授权
- 授权 AWS KMS 管理 AWS CloudHSM 和 Amazon EC2 资源

向 AWS CloudHSM 密钥存储管理员和用户授权

在设计您的 AWS CloudHSM 密钥存储时，请确保使用和管理它的主体仅具有其所需的权限。以下列表描述了 AWS CloudHSM 密钥存储管理员和用户所需的最低权限。

- 创建和管理 AWS CloudHSM 密钥存储的主体需要以下权限才能使用 AWS CloudHSM 密钥存储 API 操作。

  - `cloudhsm:DescribeClusters`
  - `kms:CreateCustomKeyStore`
  - `kms:ConnectCustomKeyStore`
  - `kms:DeleteCustomKeyStore`
  - `kms:DescribeCustomKeyStores`
  - `kms:DisconnectCustomKeyStore`
  - `kms:UpdateCustomKeyStore`
  - `iam:CreateServiceLinkedRole`
- 创建和管理与您的 AWS CloudHSM 密钥存储关联的 AWS CloudHSM 集群的主体需要创建和初始化 AWS CloudHSM 集群的权限。这包括创建或使用 Amazonn 虚拟私有云（VPC）、创建子网和创建 Amazon EC2 实例所需的权限。他们可能还需要创建和删除 HSM 以及管理备份。有关所需权限的列表，请参阅《AWS CloudHSM User Guide》中的 Identity and access management for AWS CloudHSM。
- 在您的 AWS CloudHSM 密钥存储中创建和管理 AWS KMS keys 的主体需要具有与在 AWS KMS 中创建和管理任何 KMS 密钥的人员相同的权限。AWS CloudHSM 密钥存储中的 KMS 密钥的默认密钥策略与 AWS KMS 中的 KMS 密钥的默认密钥策略相同。基于属性的访问权限控制（ABAC）使用标签和别名来控制对 KMS 密钥的访问，对 AWS CloudHSM 密钥存储中的 KMS 密钥也有效。
- 使用 AWS CloudHSM 密钥存储中的 KMS 密钥进行加密操作的主体需要使用 KMS 密钥执行加密操作的权限，如 kms:Decrypt。您可以在密钥策略或 IAM policy 中提供这些权限。但是，他们无需任何额外权限即可在 AWS CloudHSM 密钥存储中使用 KMS 密钥。

授权 AWS KMS 管理 AWS CloudHSM 和 Amazon EC2 资源

为了支持您的 AWS CloudHSM 密钥存储，AWS KMS 需要获取有关您的 AWS CloudHSM 集群的信息的权限。它还需要创建将您的 AWS CloudHSM 密钥存储连接到其 AWS CloudHSM 集群的网络基础设施的权限。要获得这些权限，AWS KMS请在AWS 账户中创建AWSServiceRoleForKeyManagementServiceCustomKeyStores服务相关角色。创建 AWS CloudHSM 密钥存储的用户必须具有能让其创建服务相关角色的 `iam:CreateServiceLinkedRole` 权限。

主题

- 关于 AWS KMS 服务相关角色
- 创建服务相关角色
- 编辑服务相关角色描述

- 删除服务相关角色

关于 AWS KMS 服务相关角色

服务相关角色是一种 IAM 角色，该角色可向一个 AWS 服务提供代表您调用其他 AWS 服务的权限。该角色旨在使您能够更轻松地使用多项集成式 AWS 服务的功能，而无需创建和维护复杂的 IAM policy。有关更多信息，请参阅 将服务相关角色用于 AWS KMS。

对于AWS CloudHSM密钥存储，使用AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy策略AWS KMS创建AWSServiceRoleForKeyManagementServiceCustomKeyStores服务相关角色。此策略向该角色授予以下权限：

- cloudhsm: describe* — 检测连接到您的自定义密钥存储AWS CloudHSM库的集群中的更改。
- ec2: CreateSecurityGroup — 在连接AWS CloudHSM密钥存储库以创建安全组时使用，该组允许AWS CloudHSM集群AWS KMS之间的网络流量流动。
- ec2: AuthorizeSecurityGroupIngress — 当您连接AWS CloudHSM密钥存储以允许网络访问包含您的AWS CloudHSM集群的 VPC 时使用。AWS KMS
- ec2: CreateNetworkInterface — 在连接AWS CloudHSM密钥库以创建用于AWS CloudHSM集群AWS KMS之间通信的网络接口时使用。
- ec2: RevokeSecurityGroupEgress — 当您连接AWS CloudHSM密钥存储库以从AWS KMS创建的安全组中删除所有出站规则时使用。
- ec2: DeleteSecurityGroup — 用于断开AWS CloudHSM密钥存储的连接，以删除连接AWS CloudHSM密钥库时创建的安全组。
- ec2: DescribeSecurityGroups — 用于监控在包含您的AWS CloudHSM集群的 VPC 中AWS KMS创建的安全组中的更改，以便在出现故障时AWS KMS可以提供清晰的错误消息。
- ec2: DescribeVpcs — 用于监控包含您的AWS CloudHSM集群的 VPC 中的更改，AWS KMS以便在出现故障时提供清晰的错误消息。
- ec2: DescribeNetworkAcls — 用于监控包含您的AWS CloudHSM集群的 VPC 的网络 ACL 的变化，AWS KMS以便在出现故障时提供清晰的错误消息。
- ec2: DescribeNetworkInterfaces — 用于监控在包含您的AWS CloudHSM集群的 VPC 中AWS KMS创建的网络接口的变化，以便在出现故障时AWS KMS可以提供清晰的错误消息。

```
{
```

```
  "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": "*"
    }
  ]
}
```

由于AWSServiceRoleForKeyManagementServiceCustomKeyStores服务相关角色仅受信任`cks.kms.amazonaws.com`，因此AWS KMS只能担任此服务相关角色。该角色受限于 AWS KMS 查看您的 AWS CloudHSM 集群并将 AWS CloudHSM 密钥存储连接到其关联 AWS CloudHSM 集群所需的操作。它不会向 AWS KMS 提供任何额外权限。例如，AWS KMS 无权创建、管理或删除您的 AWS CloudHSM 集群、HSM 或备份。

区域

与AWS CloudHSM密钥库功能一样，该AWSServiceRoleForKeyManagementServiceCustomKeyStores角色在所有可用AWS 区域的地方AWS KMSAWS CloudHSM都受支持。有关每项服务支持的 AWS 区域 的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Key Management Service Endpoints and Quotas 和 AWS CloudHSM endpoints and quotas。

有关 AWS 服务如何使用服务相关角色的更多信息，请参阅《IAM 用户指南》中的使用服务相关角色。

创建服务相关角色

AWS KMS如果角色尚不存在，则在创建AWS CloudHSM密钥库AWS 账户时会在中自动创建AWSServiceRoleForKeyManagementServiceCustomKeyStores服务相关角色。您无法直接创建或重新创建此服务相关角色。

编辑服务相关角色描述

您无法在AWSServiceRoleForKeyManagementServiceCustomKeyStores 服务相关角色中编辑角色名称或策略语句，但可以编辑角色描述。有关说明，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除服务相关角色

AWS KMSAWS 账户即使您已经删除了所有AWS CloudHSM密钥库，也不会从中删除AWSServiceRoleForKeyManagementServiceCustomKeyStores服务相关角色。尽管目前没有删除AWSServiceRoleForKeyManagementServiceCustomKeyStores服务相关角色的程序，AWS KMS但除非您有有效的AWS CloudHSM密钥存储，否则不要代入该角色或使用其权限。

管理 CloudHSM 自定义密钥存储

通过使用 AWS Management Console和 AWS KMS API，您可以管理自定义密钥存储。例如，您可以查看自定义密钥存储、编辑其属性、从其关联的 AWS CloudHSM 集群连接和断开连接以及删除自定义密钥存储。

主题

- 创建 AWS CloudHSM 密钥存储
- 查看 AWS CloudHSM 密钥存储
- 编辑 AWS CloudHSM 密钥存储设置
- 连接和断开 AWS CloudHSM 密钥存储
- 删除 AWS CloudHSM 密钥存储

创建 AWS CloudHSM 密钥存储

您可以在账户中创建一个或多个 AWS CloudHSM 密钥存储。每个 AWS CloudHSM 密钥存储均与相同 AWS 账户 和区域中的一个 AWS CloudHSM 集群关联。在创建 AWS CloudHSM 密钥存储之前，您需要汇编先决条件。然后，在使用 AWS CloudHSM 密钥存储之前，您必须连接它和它的 AWS CloudHSM 集群。

> **Note**
>
> 如果您尝试创建一个属性值与断开连接的现有 AWS CloudHSM 密钥存储相同的 AWS CloudHSM 密钥存储，AWS KMS 不会创建新的 AWS CloudHSM 密钥存储，也不会引发异常或显示错误。相反，AWS KMS 将副本识别为重试的可能结果，并返回现有 AWS CloudHSM 密钥存储的 ID。

> **Tip**
>
> 您无需立即连接 AWS CloudHSM 密钥存储。您可以将它保持断开状态，直到您准备好使用它为止。但是，要验证它是否已正确配置，您可能需要连接它，查看其连接状态，然后断开它。

主题

汇编先决条件

每个 AWS CloudHSM 密钥存储均由一个 AWS CloudHSM 集群提供支持。要创建 AWS CloudHSM 密钥存储，您必须指定一个尚未与其他密钥存储关联的活动 AWS CloudHSM 集群。您还需要在集群的 HSM 中创建一个专用的加密用户 (CU)，AWS KMS 可使用该用户代表您创建和管理密钥。

在创建 AWS CloudHSM 密钥存储之前，请执行以下操作：

选择一个 AWS CloudHSM 集群

每个 AWS CloudHSM 密钥存储正好与一个 AWS CloudHSM 集群关联。在 AWS CloudHSM 密钥存储中创建 AWS KMS keys 时，AWS KMS 会在 AWS KMS 中创建 KMS 密钥元数据，例如 ID 和 Amazon 资源名称（ARN）。然后，它会在关联集群的 HSM 中创建密钥材料。您可以创建新的 AWS CloudHSM 集群或使用现有的集群。AWS KMS 不需要对集群的独占访问权限。

所选 AWS CloudHSM 集群将与 AWS CloudHSM 密钥存储永久关联。在创建 AWS CloudHSM 密钥存储后，您可以为关联集群更改集群 ID，但您指定的集群必须与原始集群共享备份历史记录。要使用不相关的集群，您需要创建新的 AWS CloudHSM 密钥存储。

您选择的 AWS CloudHSM 集群必须具有以下特征：

- 集群必须处于活动状态。

  您必须创建集群，将其初始化，安装适用于您的平台的 AWS CloudHSM 客户端软件，然后激活该集群。有关详细说明，请参阅《AWS CloudHSM User Guide》中的 Getting started with AWS CloudHSM。

- 集群必须与 AWS CloudHSM 密钥存储位于相同的账户和区域中。您无法将一个区域中的 AWS CloudHSM 密钥存储与另一个区域中的集群相关联。要在多个区域中创建密钥基础设施，必须在每个区域中创建 AWS CloudHSM 密钥存储和集群。
- 集群不能与同一账户和区域中的其他自定义密钥存储关联。此账户和区域中的每个 AWS CloudHSM 密钥存储都必须与不同的 AWS CloudHSM 集群关联。您无法指定已与自定义密钥存储关联的集群，也无法指定与关联集群共享备份历史记录的集群。共享备份历史记录的集群具有相同的集群证书。要查看集群的集群证书，请使用AWS CloudHSM控制台或DescribeClusters操作。

  如果您将 AWS CloudHSM 集群备份到不同的区域，则它将被视为一个不同的集群，并且您可以将备份关联到其区域中的自定义密钥存储。但是，两个自定义密钥存储中的 KMS 密钥不可互操作，即使它们具有相同的备用密钥。AWS KMS 会将元数据绑定到加密文字，以确保只能由加密所用 KMS 密钥进行解密。
- 必须在区域中的至少两个可用区中为集群配置私有子网。由于 AWS CloudHSM 并非在所有可用区中都受支持，因此，我们建议您在该区域的所有可用区中创建私有子网。您无法为现有集群重新配置子网，但可以从备份创建集群（在集群配置中具有不同的子网）。

  > **Important**
  >
  > 创建 AWS CloudHSM 密钥存储后，不要删除为其 AWS CloudHSM 集群配置的任何私有子网。如果 AWS KMS 未找到集群配置中的所有子网，则尝试连接到自定义密钥存储会失败，并显示 `SUBNET_NOT_FOUND` 连接错误状态。有关更多信息，请参阅 如何修复连接故障。
- 集群的安全组 (`cloudhsm-cluster-<cluster-id>-sg`) 必须包含允许端口 2223-2225 上的 TCP 流量的入站规则和出站规则。入站规则中的 Source (源) 和出站规则中的 Destination (目标) 必须匹配安全组 ID。在创建集群时，默认情况下会设置这些规则。请勿删除或更改它们。
- 集群必须在不同的可用区中包含至少两个活动 HSM。要验证 HSM 的数量，请使用AWS CloudHSM控制台或DescribeClusters操作。如有必要，您可以添加 HSM。

查找信任锚点证书

在创建自定义密钥存储时，您必须将 AWS CloudHSM 集群的信任锚点证书上传到 AWS KMS。AWS KMS 需要信任锚点证书才能将 AWS CloudHSM 密钥存储连接到 AWS CloudHSM 集群。

每个活动 AWS CloudHSM 集群均有一个信任锚点证书。在初始化集群时，您将生成此证书，将它保存在 `customerCA.crt` 文件中，并将它复制到已连接到集群的主机。

为 AWS KMS 创建 **kmsuser** 加密用户

为了管理您的 AWS CloudHSM 密钥存储，AWS KMS 会登录到选定集群中的 kmsuser 加密用户（CU）账户。在创建您的 AWS CloudHSM 密钥存储之前，您必须创建 kmsuser CU。然后，在创建 AWS CloudHSM 密钥存储时，您向 AWS KMS 提供 kmsuser 密码。在将 AWS CloudHSM 密钥存储连接到其关联的 AWS CloudHSM 集群时，AWS KMS 将以 kmsuser 身份登录并轮换 kmsuser 密码。

> **Important**
>
> 在创建 kmsuser CU 时，请勿指定 2FA 选项。如果这样做，AWS KMS 将无法登录，并且您的 AWS CloudHSM 密钥存储将无法连接到此 AWS CloudHSM 集群。一旦指定 2FA，便无法撤消它。相反，您必须删除 CU 并重新创建它。

要创建 kmsuser CU，请使用以下过程。

1. 按照《AWS CloudHSM User Guide》中的 Getting started with CloudHSM Management Utility (CMU)主题所述，启动 cloudhsm_mgmt_util。
2. 在 cloudhsm_mgmt_util 中使用 createUser 命令创建名为 kmsuser 的 CU。密码必须由 7 到 32 个字母数字字符组成。它区分大小写，并且不能包含任何特殊字符。

   例如，以下示例命令将创建密码为 kmsPswd 的 kmsuser CU。

   ```
   aws-cloudhsm> createUser CU kmsuser kmsPswd
   ```

创建 AWS CloudHSM 密钥存储（控制台）

在 AWS Management Console 中创建 AWS CloudHSM 密钥存储时，您可以添加并创建先决条件作为工作流的一部分。但是，如果您事先已汇编这些先决条件，则此过程会更快。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择自定义密钥存储、AWS CloudHSM 密钥存储。
4. 选择 “创建密钥库”。
5. 为自定义密钥存储输入友好名称。该名称在您账户的所有自定义密钥存储中必须具备唯一性。

> **Important**
>
> 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。

6. 为 AWS CloudHSM 密钥存储选择一个 AWS CloudHSM 集群。或者，要创建新的 AWS CloudHSM 集群，请选择 Create an AWS CloudHSM cluster（创建 Amazon CloudHSM 集群）链接。

   该菜单显示您账户和区域中尚未与 AWS CloudHSM 密钥存储关联的 AWS CloudHSM 集群。该集群必须满足要求（与关联自定义密钥存储相关）。

7. 选择 Choose file（选择文件），然后为选定的 AWS CloudHSM 集群上传信任锚点证书。这是您在初始化集群时创建的 `customerCA.crt` 文件。

8. 输入您在选定集群中创建的 `kmsuser` 加密用户 (CU) 的密码。

9. 选择创建。

当该过程成功时，新的 AWS CloudHSM 密钥存储将显示在账户和区域的 AWS CloudHSM 密钥存储列表中。如果该过程失败，则会显示一条错误消息，描述问题并提供有关如何解决该问题的帮助。如果您需要更多帮助，请参阅对自定义密钥存储进行故障排除。

如果您尝试创建一个属性值与断开连接的现有 AWS CloudHSM 密钥存储相同的 AWS CloudHSM 密钥存储，AWS KMS 不会创建新的 AWS CloudHSM 密钥存储，也不会引发异常或显示错误。相反，AWS KMS 将副本识别为重试的可能结果，并返回现有 AWS CloudHSM 密钥存储的 ID。

下一步：不会自动连接新的 AWS CloudHSM 密钥存储。您必须先连接自定义密钥存储与其关联的 AWS CloudHSM 集群，然后才能在 AWS CloudHSM 密钥存储中创建 AWS KMS keys。

创建 AWS CloudHSM 密钥存储区（API）

您可以使用该CreateCustomKeyStore操作来创建与账户和区域中的AWS CloudHSM集群关联的新AWS CloudHSM密钥存储。这些示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

`CreateCustomKeyStore` 操作需要以下参数值。

- CustomKeyStoreName — 自定义密钥库的友好名称，在账户中是唯一的。

> **Important**
>
> 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。

- CloudHsmClusterId — 满足AWS CloudHSM密钥存储要求的AWS CloudHSM集群的集群 ID。
- KeyStorePassword — 指定集群中 kmsuser CU 账户的密码。
- TrustAnchorCertificate — 您在初始化集群时创建的customerCA.crt文件的内容。

以下示例使用虚构的集群 ID。在运行命令之前，请将其替换为有效的集群 ID。

```
$ 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>
```

如果您使用的是 AWS CLI，则可指定信任锚点证书文件而不是其内容。在下面的示例中，customerCA.crt 文件位于根目录中。

```
$ 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
```

当此操作成功时，CreateCustomKeyStore 将返回自定义密钥存储 ID，如以下示例响应中所示。

```
{
    "CustomKeyStoreId": cks-1234567890abcdef0
}
```

如果操作失败，请更正异常指示的错误，然后重试。有关其他帮助，请参阅对自定义密钥存储进行故障排除。

如果您尝试创建一个属性值与断开连接的现有 AWS CloudHSM 密钥存储相同的 AWS CloudHSM 密钥存储，AWS KMS 不会创建新的 AWS CloudHSM 密钥存储，也不会引发异常或显示错误。相反，AWS KMS 将副本识别为重试的可能结果，并返回现有 AWS CloudHSM 密钥存储的 ID。

下一步：要使用 AWS CloudHSM 密钥存储，可将它连接到其 AWS CloudHSM 集群。

查看 AWS CloudHSM 密钥存储

您可以使用AWS KMS控制台或DescribeCustomKeyStores操作查看每个账户和区域中的AWS CloudHSM密钥存储区。

另请参阅：

- 查看外部密钥存储
- 在 AWS CloudHSM 密钥存储中查看 KMS 密钥
- 使用记录 AWS KMS API 调用 AWS CloudTrail

主题

- 查看 AWS CloudHSM 密钥存储（控制台）
- 查看 AWS CloudHSM 密钥存储（API）

查看 AWS CloudHSM 密钥存储（控制台）

在 AWS Management Console 中查看 AWS CloudHSM 密钥存储时，可查看以下内容：

- 自定义密钥存储名称和 ID
- 关联的 AWS CloudHSM 集群的 ID
- 集群中的 HSM 的数量
- 当前连接状态

连接状态 [Status（状态）] 值 Disconnected（已断开连接）表示自定义密钥存储是新的且从未连接过，或者已有意断开与其 AWS CloudHSM 集群的连接。但是，如果您尝试使用已连接的自定义密钥存储中的 KMS 密钥失败，则可能表示自定义密钥存储或其 AWS CloudHSM 集群存在问题。有关帮助信息，请参阅 如何修复失败的 KMS 密钥。

要查看给定账户和区域中的 AWS CloudHSM 密钥存储，请使用以下过程。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择自定义密钥存储、AWS CloudHSM 密钥存储。

要自定义显示，请单击显示在 Create key store (创建密钥存储) 按钮下方的齿轮图标。

查看 AWS CloudHSM 密钥存储（API）

要查看您的AWS CloudHSM密钥存储库，请使用DescribeCustomKeyStores操作。默认情况下，此操作将返回账户和区域中的所有自定义密钥存储。不过，您可以使用 CustomKeyStoreId 或 CustomKeyStoreName 参数（但不能同时使用两者）将输出限制到特定的自定义密钥存储。对于 AWS CloudHSM 密钥存储，输出内容包含自定义密钥存储 ID 和名称、自定义密钥存储类型、关联 AWS CloudHSM 集群的 ID 以及连接状态。如果连接状态指示错误，则输出还包含描述错误原因的错误代码。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

例如，以下命令返回账户和区域中的所有自定义密钥存储。您可以使用 Limit 和 Marker 参数来浏览输出中的自定义密钥存储。

```
$ aws kms describe-custom-key-stores
```

以下示例命令使用 CustomKeyStoreName 参数以仅获取具有 ExampleCloudHSMKeyStore 友好名称的自定义密钥存储。您可以在每个命令中使用 CustomKeyStoreName 或 CustomKeyStoreId 参数（但不能同时使用二者）。

以下示例输出表示已连接到其 AWS CloudHSM 集群的 AWS CloudHSM 密钥存储。

> **Note**
>
> 在 DescribeCustomKeyStores 响应中添加了 CustomKeyStoreType 字段，以区分 AWS CloudHSM 密钥存储和外部密钥存储。

```
$ 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>"
        }
    ]
}
```

ConnectionState 为 Disconnected 表示自定义密钥存储从未连接过，或者它已有意从其 AWS CloudHSM 集群断开连接。但是，如果尝试使用已连接的 AWS CloudHSM 密钥存储中的 KMS 密钥失败，则可能表示 AWS CloudHSM 密钥存储或其 AWS CloudHSM 集群存在问题。有关帮助信息，请参阅 如何修复失败的 KMS 密钥。

如果自定义密钥存储的 ConnectionState 为 FAILED，则 DescribeCustomKeyStores 响应包含一个说明错误原因的 ConnectionErrorCode 元素。

例如，在以下输出中，INVALID_CREDENTIALS 值指示自定义密钥存储连接因 kmsuser 密码无效而导致失败。有关此连接失败及其他连接错误失败的帮助，请参阅对自定义密钥存储进行故障排除。

```
$ 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>"
        }
    ]
}
```

编辑 AWS CloudHSM 密钥存储设置

您可以更改现有 AWS CloudHSM 密钥存储的设置。必须断开自定义密钥存储与其 AWS CloudHSM 集群的连接。

要编辑 AWS CloudHSM 密钥存储设置，请执行以下操作：

1. 断开自定义密钥存储与其 AWS CloudHSM 集群的连接。在自定义密钥存储断开连接时，您无法在自定义密钥存储中创建 AWS KMS keys（KMS 密钥），并且无法使用其包含的 KMS 密钥进行加密操作。

2. 编辑一个或多个 AWS CloudHSM 密钥存储设置。
3. 重新连接自定义密钥存储至其 AWS CloudHSM 集群。

您可以在自定义密钥存储中编辑以下设置：

自定义密钥存储的友好名称。

输入新的友好名称。新名称在您 AWS 账户 的所有自定义密钥存储中必须具备唯一性。

> **Important**
>
> 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。

关联的 AWS CloudHSM 集群的集群 ID。

编辑此值以使用相关 AWS CloudHSM 集群替换原始集群。如果自定义密钥存储的 AWS CloudHSM 集群损坏或被删除，则可使用此功能来修复自定义密钥存储。

指定一个 AWS CloudHSM 集群，该集群与原始集群共享备份历史记录并满足要求以与自定义密钥存储关联，包括不同可用区中的两个活动 HSM。共享备份历史记录的集群具有相同的集群证书。要查看集群的集群证书，请使用DescribeClusters操作。您无法使用编辑功能来将自定义密钥存储与不相关的 AWS CloudHSM 集群相关联。

`kmsuser` 加密用户 (CU) 的当前密码。

向 AWS KMS 告知 AWS CloudHSM 集群中 `kmsuser` CU 的当前密码。此操作不会更改 AWS CloudHSM 集群中 `kmsuser` CU 的密码。

如果更改 AWS CloudHSM 集群中 `kmsuser` CU 的密码，请使用此功能来向 AWS KMS 告知新的 `kmsuser` 密码。否则，AWS KMS 将无法登录集群并且所有将自定义密钥存储连接到集群的尝试都将失败。

主题

- 编辑 AWS CloudHSM 密钥存储（控制台）
- 编辑 AWS CloudHSM 密钥存储（API）

编辑 AWS CloudHSM 密钥存储（控制台）

在编辑 AWS CloudHSM 密钥存储时，您可以更改任何可配置的值。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择自定义密钥存储、AWS CloudHSM 密钥存储。
4. 选择要编辑的 AWS CloudHSM 密钥存储的行。

   如果 “连接状态” 列中的值不是 “已断开连接”，则必须先断开自定义密钥存储的连接，然后才能对其进行编辑。[从 Key store actions（密钥存储操作）菜单中选择 Disconnect（断开连接）。]

   当某个 AWS CloudHSM 密钥存储断开时，您可以管理 AWS CloudHSM 密钥存储及其 KMS 密钥，但无法在 AWS CloudHSM 密钥存储中创建或使用 KMS 密钥。
5. 从 Key store actions（密钥存储操作）菜单中选择 Edit（编辑）。
6. 执行以下一项或多项操作。
   - 为自定义密钥存储键入新的友好名称。
   - 键入相关 AWS CloudHSM 集群的集群 ID。
   - 键入关联的 AWS CloudHSM 集群中 `kmsuser` 加密用户的当前密码。
7. 选择保存。

   在此过程成功后，将显示一条消息，描述您编辑的设置。如果此过程失败，则会显示一条错误消息，描述问题并提供有关如何解决问题的帮助。如果您需要更多帮助，请参阅对自定义密钥存储进行故障排除。
8. 重新连接自定义密钥存储。

   要使用 AWS CloudHSM 密钥存储，您必须在编辑后重新连接它。您可以让 AWS CloudHSM 密钥存储保留断开状态。不过，在其断开连接后，您无法在 AWS CloudHSM 密钥存储中创建 KMS 密钥或在加密操作中使用 AWS CloudHSM 密钥存储中的 KMS 密钥。

编辑 AWS CloudHSM 密钥存储（API）

要更改AWS CloudHSM密钥库的属性，请使用UpdateCustomKeyStore操作。您可以在同一命令中更改自定义密钥存储的多个属性。如果此操作成功，则 AWS KMS 返回 HTTP 200 响应和无属性的 JSON 对象。要验证更改是否有效，请使用DescribeCustomKeyStores操作。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

首先使用DisconnectCustomKeyStore断开自定义密钥存储与其AWS CloudHSM集群的连接。将示例自定义密钥存储 ID cks-1234567890abcdef0 替换为实际 ID。

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

第一个示例用于UpdateCustomKeyStore将AWS CloudHSM密钥库的友好名称更改为DevelopmentKeys。该命令使用 CustomKeyStoreId 参数标识 AWS CloudHSM 密钥存储，使用 CustomKeyStoreName 指定自定义密钥存储的新名称。

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-custom-key-store-name DevelopmentKeys
```

以下示例将与 AWS CloudHSM 密钥存储关联的集群更改为同一集群的其他备份。该命令使用 CustomKeyStoreId 参数标识 AWS CloudHSM 密钥存储，使用 CloudHsmClusterId 参数指定新集群 ID。

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --cloud-hsm-cluster-id cluster-1a23b4cdefg
```

以下示例向 AWS KMS 告知当前 kmsuser 密码为 ExamplePassword。该命令使用 CustomKeyStoreId 参数标识 AWS CloudHSM 密钥存储，使用 KeyStorePassword 参数指定当前密码。

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --key-store-password ExamplePassword
```

最后一个命令将 AWS CloudHSM 密钥存储重新连接到 AWS CloudHSM 集群。您可以将自定义密钥存储保留断开状态，但必须先连接它，然后才能创建新的 KMS 密钥或使用现有 KMS 密钥来进行加密操作。将示例自定义密钥存储 ID 替换为实际 ID。

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

连接和断开 AWS CloudHSM 密钥存储

新的 AWS CloudHSM 密钥存储未连接。您需要先将 AWS KMS keys 连接到其关联的 AWS CloudHSM 集群，然后才能在 AWS CloudHSM 密钥存储中创建和使用这些密钥。您可以随时连接和断开 AWS CloudHSM 密钥存储，并查看其连接状态。

您无需连接 AWS CloudHSM 密钥存储。您可以将 AWS CloudHSM 密钥存储保持在无限期断开的状态并且仅在您需要使用它时进行连接。但是，您可能希望定期测试连接以验证设置是否正确以及自定义密钥存储是否可以连接。

> **Note**
>
> 仅当密钥存储从未连接或您显式断开密钥存储连接时，AWS CloudHSM 密钥存储才会具有 `DISCONNECTED` 状态。如果您的 AWS CloudHSM 密钥存储状态为 `CONNECTED`，但您在使用它时遇到问题，请确保其关联的 AWS CloudHSM 集群处于活动状态，并且包含至少一个活动 HSM。如需帮助解决连接失败问题，请参阅 the section called “对自定义密钥存储进行故障排除”。

主题

- 连接 AWS CloudHSM 密钥存储
- 断开 AWS CloudHSM 密钥存储的连接
- 连接 AWS CloudHSM 密钥存储（控制台）
- 连接自定义密钥存储 (API)
- 断开 AWS CloudHSM 密钥存储（控制台）
- 断开 AWS CloudHSM 密钥存储（API）

连接 AWS CloudHSM 密钥存储

当您连接 AWS CloudHSM 密钥存储时，AWS KMS 会查找关联的 AWS CloudHSM 集群，连接到该集群，并以 `kmsuser` 加密用户（CU）身份登录 AWS CloudHSM 客户端，然后轮换 `kmsuser` 密码。只要 AWS CloudHSM 密钥存储处于连接状态，AWS KMS 仍然保持登录到 AWS CloudHSM 客户端的状态。

为了建立连接，AWS KMS 在集群的 Virtual Private Cloud (VPC) 中创建一个名为 `kms-<custom key store ID>` 的安全组。该安全组具有一个允许来自集群安全组的入站流量的规则。AWS KMS 还会在集群的私有子网的每个可用区中创建一个弹性网络接口 (ENI)。AWS KMS 会将 ENI 添加

到 kms-*<cluster ID>* 安全组和集群的安全组。每个 ENI 的描述都是 KMS managed ENI for cluster *<cluster-ID>*。

连接过程可能需要较长时间才能完成；最多 20 分钟。

在连接 AWS CloudHSM 密钥存储之前，请验证它是否符合要求。

- 其关联的 AWS CloudHSM 集群必须至少包含一个活动 HSM。要查找集群中的 HSM 数量，请在 AWS CloudHSM控制台中查看集群或使用DescribeClusters操作。如有必要，您可以添加 HSM。
- 集群必须具有 kmsuser 加密用户（CU）账户，但当您连接 AWS CloudHSM 密钥存储时，该 CU 无法登录到集群。要获取有关注销的帮助，请参阅 如何注销并重新连接。
- AWS CloudHSM 密钥存储的连接状态不能是 DISCONNECTING 或 FAILED。要查看连接状态，请使用AWS KMS控制台或DescribeCustomKeyStores响应。如果连接状态为 FAILED，请断开自定义密钥存储，修复问题，然后连接它。

如需帮助解决连接失败问题，请参阅 如何修复连接故障。

连接 AWS CloudHSM 密钥存储后，您可以在其中创建 KMS 密钥，然后在加密操作中使用现有 KMS 密钥。

断开 AWS CloudHSM 密钥存储的连接

当您断开 AWS CloudHSM 密钥存储时，AWS KMS 将从 AWS CloudHSM 客户端注销，从关联的 AWS CloudHSM 集群断开，然后移除它创建用于支持连接的网络基础设施。

当某个 AWS CloudHSM 密钥存储断开时，您可以管理 AWS CloudHSM 密钥存储及其 KMS 密钥，但无法在 AWS CloudHSM 密钥存储中创建或使用 KMS 密钥。密钥存储的连接状态为 DISCONNECTED，自定义密钥存储中的 KMS 密钥的密钥状态为 Unavailable，除非它们是 PendingDeletion。您可以随时重新连接 AWS CloudHSM 密钥存储。

当您断开自定义密钥存储时，密钥存储中的 KMS 密钥立即变得不可用（视最终一致性而定）。不过，在再次使用 KMS 密钥（例如解密数据密钥）之前，使用受 KMS 密钥保护的数据密钥加密的资源不会受到影响。此问题会影响 AWS 服务，因为许多服务使用数据密钥来保护您的资源。有关更多信息，请参阅 不可用的 KMS 密钥如何影响数据密钥。

> **Note**
>
> 虽然自定义密钥存储已断开连接，但在自定义密钥存储中创建 KMS 密钥或在加密操作中使用现有 KMS 密钥的所有尝试都将失败。此操作可以阻止用户存储和访问敏感数据。

为了更好地估计断开自定义密钥存储的影响，请在自定义密钥存储中标识 KMS 密钥，并确定其过去的使用情况。

您可能出于以下原因断开 AWS CloudHSM 密钥存储：

- 轮换 **kmsuser** 密码。每当 AWS KMS 连接到 AWS CloudHSM 集群时，它就会更改 kmsuser 密码。要强制轮换密码，只需断开并重新连接。
- 审核 AWS CloudHSM 集群中的 KMS 密钥的密钥材料。当您断开自定义密钥存储时，AWS KMS 会退出 AWS CloudHSM 客户端中的 kmsuser 加密用户账户。这样，您便能以 kmsuser CU 身份登录到集群并审核和管理 KMS 密钥的密钥材料。
- 在 AWS CloudHSM 密钥存储中立即禁用所有 KMS 密钥。您可以使用AWS Management Console或DisableKey操作禁用和重新启用密AWS CloudHSM钥存储中的 KMS 密钥。这些操作会快速完成，但它们一次只针对一个 KMS 密钥。断开 AWS CloudHSM 密钥存储的连接会立即将 AWS CloudHSM 密钥中的所有 KMS 密钥的密钥状态更改为 Unavailable，这将阻止在任何加密操作中使用这些 KMS 密钥。
- 修复失败的连接尝试。如果连接 AWS CloudHSM 密钥存储的尝试失败（自定义密钥存储的连接状态为 FAILED），则必须在尝试再次连接 AWS CloudHSM 密钥存储之前将其断开。

连接 AWS CloudHSM 密钥存储（控制台）

要在 AWS Management Console 中连接 AWS CloudHSM 密钥存储，请首先从 Custom key stores（自定义密钥存储）页面中选择 AWS CloudHSM 密钥存储。连接过程可能最多需要 20 分钟才能完成。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择自定义密钥存储、AWS CloudHSM 密钥存储。
4. 选择要连接的 AWS CloudHSM 密钥存储的行。

   如果AWS CloudHSM密钥库的连接状态为“失败”，则必须在连接自定义密钥库之前断开其连接。
5. 从 Key store actions（密钥存储操作）菜单中选择 Connect（连接）。

AWS KMS 将开始连接自定义密钥存储的过程。它将查找关联的 AWS CloudHSM 集群，构建所需的网络基础设施，连接到网络基础设施，以 kmsuser CU 身份登录到 AWS CloudHSM 集群，然后轮换 kmsuser 密码。操作完成后，连接状态更改为“已连接”。

如果操作失败，则会出现一条描述失败原因的错误消息。在尝试再次连接之前，请查看 AWS CloudHSM 密钥存储的连接状态。如果失败，则必须先断开自定义密钥存储库的连接，然后再重新连接。如果您需要帮助，请参阅对自定义密钥存储进行故障排除。

下一步：the section called “在 AWS CloudHSM 密钥存储中创建 KMS 密钥”。

连接自定义密钥存储 (API)

要连接已断开连接的AWS CloudHSM密钥库，请使用ConnectCustomKeyStore操作。关联的 AWS CloudHSM 集群必须包含至少一个活动 HSM，且连接状态不能为 FAILED。

连接过程需要较长时间才能完成；最多 20 分钟。除非该过程迅速失败，否则 操作将返回 HTTP 200 响应和无属性的 JSON 对象。但是，此初始响应不指示连接是否成功。要确定自定义密钥库的连接状态，请参阅DescribeCustomKeyStores响应。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

要确定 AWS CloudHSM 密钥存储，请使用自定义密钥存储 ID。您可以在控制台的自定义密钥存储页面上找到 ID，也可以使用不带参数的DescribeCustomKeyStores操作来找到 ID。在运行此示例之前，请将示例 ID 替换为有效的 ID。

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

要验证AWS CloudHSM密钥库是否已连接，请使用DescribeCustomKeyStores操作。默认情况下，此操作将返回您的账户和区域中的所有自定义密钥存储。但您可以使用 CustomKeyStoreId 或 CustomKeyStoreName 参数（但不能同时使用两者）将响应限制到特定自定义密钥存储。ConnectionState 值 CONNECTED 表示自定义密钥存储已连接到其 AWS CloudHSM 集群。

> **Note**
>
> 在 DescribeCustomKeyStores 响应中添加了 CustomKeyStoreType 字段，以区分 AWS CloudHSM 密钥存储和外部密钥存储。

```
$ 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"
   ],
}
```

如果 ConnectionState 值为 FAILED，ConnectionErrorCode 元素将指示失败的原因。在此情况下，AWS KMS 在您的账户中找不到集群 ID 为 cluster-1a23b4cdefg 的 AWS CloudHSM 集群。如果您删除了该集群，则可以从原始集群的备份还原它，然后编辑自定义密钥存储的集群 ID。有关响应连接错误代码的帮助信息，请参阅 如何修复连接故障。

```
$ 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"
   ],
}
```

下一步：在 AWS CloudHSM 密钥存储中创建 KMS 密钥。

断开 AWS CloudHSM 密钥存储（控制台）

要在 AWS Management Console 中断开已连接的 AWS CloudHSM 密钥存储，请首先从 Custom Key Stores（自定义密钥存储）页面选择该 AWS CloudHSM 密钥存储。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择自定义密钥存储、AWS CloudHSM 密钥存储。
4. 选择要断开连接的外部密钥存储的行。
5. 从 Key store actions（密钥存储操作）菜单中选择 Disconnect（断开连接）。

操作完成后，连接状态将从 “断开连接” 更改为 “已断开连接”。如果操作失败，则会出现一条错误消息，描述问题并提供有关如何修复它的帮助。如果您需要更多帮助，请参阅对自定义密钥存储进行故障排除。

断开 AWS CloudHSM 密钥存储（API）

要断开连接的AWS CloudHSM密钥存储库，请使用DisconnectCustomKeyStore操作。如果此操作成功，则 AWS KMS 返回 HTTP 200 响应和无属性的 JSON 对象。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

本示例将断开 AWS CloudHSM 密钥存储。在运行此示例之前，请将示例 ID 替换为有效的 ID。

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

要验证AWS CloudHSM密钥存储是否已断开连接，请使用DescribeCustomKeyStores操作。默认情况下，此操作将返回您的账户和区域中的所有自定义密钥存储。但您可以使用 CustomKeyStoreId 和 CustomKeyStoreName 参数（但不能同时使用两者）将响应限制到特定自定义密钥存储。DISCONNECTED 的 ConnectionState 值表示 AWS CloudHSM 密钥存储示例未连接到其 AWS CloudHSM 集群。

```
$ 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>"
   ],
}
```

删除 AWS CloudHSM 密钥存储

当您删除 AWS CloudHSM 密钥存储时，AWS KMS 会从 KMS 中删除有关 AWS CloudHSM 密钥存储的所有元数据，包括有关其与 AWS CloudHSM 集群的关联的信息。此操作不会影响 AWS CloudHSM 集群、其 HSM 或其用户。您可以创建与同一 AWS CloudHSM 集群关联的新 AWS CloudHSM 密钥存储，但无法撤消删除操作。

您只能删除已与其 AWS CloudHSM 集群断开连接且不包含任何 AWS KMS keys 的 AWS CloudHSM 密钥存储。在删除自定义密钥存储之前，请执行以下操作。

- 验证您是否永远不需要将密钥存储中的任何 KMS 密钥用于任何加密操作。然后从密钥存储中执行所有 KMS 密钥的计划删除。有关在 AWS CloudHSM 密钥存储中查找 KMS 密钥的帮助信息，请参阅在 AWS CloudHSM 密钥存储中查找 KMS 密钥。
- 确认已删除所有 KMS 密钥。要在 AWS CloudHSM 密钥存储中查看 KMS 密钥，请参阅 在 AWS CloudHSM 密钥存储中查看 KMS 密钥。
- 从其 AWS CloudHSM 集群断开 AWS CloudHSM 密钥存储。

请考虑断开其与关联的 AWS CloudHSM 集群的连接，而不是删除 AWS CloudHSM 密钥存储。当某个 AWS CloudHSM 密钥存储断开连接时，您可以管理 AWS CloudHSM 密钥存储及其 AWS KMS keys。不过，您无法在 AWS CloudHSM 密钥存储中创建或使用 KMS 密钥。您可以随时重新连接 AWS CloudHSM 密钥存储。

主题

- 删除 AWS CloudHSM 密钥存储（控制台）
- 删除 AWS CloudHSM 密钥存储（API）

删除 AWS CloudHSM 密钥存储（控制台）

要在 AWS Management Console 中删除 AWS CloudHSM 密钥存储，请首先从 Custom key stores（自定义密钥存储）页面中选择 AWS CloudHSM 密钥存储。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择自定义密钥存储、AWS CloudHSM 密钥存储。
4. 找到表示要删除的 AWS CloudHSM 密钥存储的行。如果AWS CloudHSM密钥库的 “连接” 状态不是 “已断开连接”，则必须先断开AWS CloudHSM密钥库的连接，然后才能将其删除。
5. 从 Key store actions（密钥存储操作）菜单中选择 Delete（删除）。

在操作完成后，会显示一条成功消息，并且 AWS CloudHSM 密钥存储不再显示在密钥存储列表中。如果操作失败，则会显示一条错误消息，描述问题并提供有关如何解决该问题的帮助。如果您需要更多帮助，请参阅对自定义密钥存储进行故障排除。

删除 AWS CloudHSM 密钥存储（API）

要删除密AWS CloudHSM钥库，请使用DeleteCustomKeyStore操作。如果此操作成功，则 AWS KMS 返回 HTTP 200 响应和无属性的 JSON 对象。

要开始操作，请确认 AWS CloudHSM 密钥存储不包含任何 AWS KMS keys。您无法删除包含 KMS 密钥的自定义密钥存储。第一个示例命令使用ListKeys和在AWS CloudHSM密钥库AWS KMS keys中搜索 DescribeKey，示例 *cks-1234567890abc* def0 自定义密钥库 ID。在此情况下，该命令不会返回任何 KMS 密钥。如果是，请使用ScheduleKeyDeletion操作安排每个 KMS 密钥的删除。

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'
```

接下来，断开 AWS CloudHSM 密钥存储。此示例命令使用DisconnectCustomKeyStore操作断开AWS CloudHSM密钥库与其AWS CloudHSM集群的连接。在运行此命令之前，请将示例自定义密钥存储 ID 替换为有效 ID。

Bash

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Disconnect-KMSCustomKeyStore -CustomKeyStoreId cks-1234567890abcdef0
```

断开自定义密钥库的连接后，您可以使用DeleteCustomKeyStore操作将其删除。

Bash

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

PowerShell

```
PS C:\> Remove-KMSCustomKeyStore -CustomKeyStoreId cks-1234567890abcdef0
```

在 CloudHSM 密钥存储中管理 KMS 密钥

您可以在 AWS CloudHSM 密钥存储中创建、查看、管理、使用和计划删除 AWS KMS keys。您使用的过程与用于其他 KMS 密钥的过程非常相似。唯一的区别是您在创建 KMS 密钥时指定了 AWS CloudHSM 密钥存储。然后，AWS KMS 在与 AWS CloudHSM 密钥存储关联的 AWS CloudHSM 集群中为 KMS 密钥创建不可提取的密钥材料。在 AWS CloudHSM 密钥存储中使用 KMS 密钥时，会在集群中的 HSM 中执行加密操作。

支持的功能

除了此部分中讨论的过程之外，您还可以使用 AWS CloudHSM 密钥存储中的 KMS 密钥执行下列操作：

- 使用密钥策略、IAM policy 和授权来授予对 KMS 密钥的访问权限。
- 启用和禁用 KMS 密钥。
- 分配标签并创建别名，然后使用基于属性的访问权限控制（ABAC）授予对 KMS 密钥的访问权限。
- 使用 KMS 密钥进行加密操作，包括加密、解密、重新加密和生成数据密钥。
- 将 KMS 密钥和与 AWS KMS 集成的 AWS 服务结合使用并支持客户托管密钥。
- 在AWS CloudTrail日志和 Amazon CloudWatch 监控工具中跟踪您的 KMS 密钥的使用情况。

不支持的功能

- AWS CloudHSM 密钥存储仅支持对称加密 KMS 密钥。您无法在 AWS CloudHSM 密钥存储中创建 HMAC KMS 密钥、非对称 KMS 密钥或非对称数据密钥对。
- 您无法向 AWS CloudHSM 密钥存储中的 KMS 密钥导入密钥材料。AWS KMS 为 AWS CloudHSM 集群中的 KMS 密钥生成密钥材料。
- 您无法启用或禁用 AWS CloudHSM 密钥存储中 KMS 密钥的密钥材料的自动轮换。

主题

- 在 AWS CloudHSM 密钥存储中创建 KMS 密钥
- 在 AWS CloudHSM 密钥存储中查看 KMS 密钥

- 在 AWS CloudHSM 密钥存储中使用 KMS 密钥
- 查找 KMS 密钥和密钥材料
- 计划从 AWS CloudHSM 密钥存储删除 KMS 密钥

在 AWS CloudHSM 密钥存储中创建 KMS 密钥

在创建 AWS CloudHSM 密钥存储后，您可以在密钥存储中创建 AWS KMS keys。它们必须为具有 AWS KMS 生成的密钥材料的对称加密 KMS 密钥。您不能在自定义密钥存储中创建非对称 KMS 密钥、HMAC KMS 密钥或具有导入的密钥材料的 KMS 密钥。此外，您不能在自定义密钥存储中使用对称加密 KMS 密钥来生成非对称数据密钥对。

要在 AWS CloudHSM 密钥存储中创建 KMS 密钥，AWS CloudHSM 密钥存储必须连接到其关联的 AWS CloudHSM 集群，并且集群必须包含不同可用区中的至少两个活动 HSM。要查找 HSM 的连接状态和数量，请在 AWS Management Console 中查看 AWS CloudHSM 密钥存储页面。使用 API 操作时，使用DescribeCustomKeyStores操作验证AWS CloudHSM密钥库是否已连接。要验证集群中活动 HSM 的数量及其可用区，请使用AWS CloudHSMDescribeClusters操作。

在 AWS CloudHSM 密钥存储中创建 KMS 密钥时，AWS KMS 会在 AWS KMS 中创建 KMS 密钥。但是，它会在关联的 AWS CloudHSM 集群中为 KMS 密钥创建密钥材料。具体而言，AWS KMS 作为您创建的 `kmsuser` CU 登录到集群。然后，它在集群中创建持久的、不可提取的 256 位高级加密标准 (AES) 对称密钥。AWS KMS 将密钥标签属性的值（仅在集群中可见）设置为 KMS 密钥的 Amazon Resource Name (ARN)。

当命令成功时，新 KMS 密钥的密钥状态为 `Enabled`，其源为 `AWS_CLOUDHSM`。创建任何 KMS 密钥后便无法更改其源。当您在AWS KMS控制台的密AWS CloudHSM钥存储库中或使用DescribeKey操作查看 KMS 密钥时，可以看到典型的属性，例如其密钥 ID、密钥状态和创建日期。但是，您也可以查看自定义密钥存储 ID 和（可选）AWS CloudHSM 集群 ID。有关更多信息，请参阅 在 AWS CloudHSM 密钥存储中查看 KMS 密钥。

如果您在 AWS CloudHSM 密钥存储中创建 KMS 密钥的尝试失败，请查看错误消息以帮助您确定原因。该消息可能指明未连接 AWS CloudHSM 密钥存储（`CustomKeyStoreInvalidStateException`）或关联的 AWS CloudHSM 集群没有此操作（`CloudHsmClusterInvalidConfigurationException`）所需的两个活动 HSM。有关帮助信息，请参阅对自定义密钥存储进行故障排除。

有关在 AWS CloudHSM 密钥存储中创建 KMS 密钥的操作的 AWS CloudTrail 日志示例，请参阅 CreateKey。

主题

- 在 AWS CloudHSM 密钥存储中创建 KMS 密钥（控制台）
- 在 AWS CloudHSM 密钥存储中创建 KMS 密钥（API）

在 AWS CloudHSM 密钥存储中创建 KMS 密钥（控制台）

按照以下过程在 AWS CloudHSM 密钥存储中创建对称加密 KMS 密钥。

> **Note**
>
> 不要在别名、描述或标签中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择 Create key。
5. 选择 Symmetric (对称)。
6. 在 Key usage（密钥用法）中，已为您选择了 Encrypt and decrypt（加密和解密）选项。请勿对其进行更改。
7. 选择 Advanced options (高级选项)。
8. 对于密钥材料源，选择 AWS CloudHSM 密钥存储。

   您不能在 AWS CloudHSM 密钥存储中创建多区域密钥。
9. 请选择 Next（下一步）。
10. 为新 KMS 密钥选择 AWS CloudHSM 密钥存储。要创建新的 AWS CloudHSM 密钥存储，请选择 Create custom key store（创建自定义密钥存储）。

    您选择的AWS CloudHSM密钥库的状态必须为 “已连接”。其关联的 AWS CloudHSM 集群必须处于活动状态且在不同的可用区中包含至少两个活动 HSM。

    有关连接 AWS CloudHSM 密钥存储的帮助信息，请参阅 连接和断开 AWS CloudHSM 密钥存储。有关添加 HSM 的帮助，请参阅 AWS CloudHSM 用户指南中的添加 HSM。
11. 请选择 Next（下一步）。
12. 为 KMS 密钥键入别名和可选的描述。

13. （可选）。在 Add Tags（添加标签）页面上，添加标识或分类 KMS 密钥的标签。

    在将标签添加到 AWS 资源时，AWS 可生成成本分配报告，其中按标签汇总了使用情况和成本。标签还可以用来控制对 KMS 密钥的访问。有关轮换 KMS 密钥的信息，请参阅 标记密钥 和 AWS KMS 中的 ABAC。

14. 请选择 Next（下一步）。

15. 在 Key Administrators（密钥管理员）部分中，选择可管理 KMS 密钥的 IAM 用户和角色。有关更多信息，请参阅允许密钥管理员管理 KMS 密钥。

    > **Note**
    >
    > IAM 策略可以向其他 IAM 用户和角色授予使用 KMS 密钥的权限。
    > IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

16. （可选）要阻止这些密钥管理员删除此 KMS 密钥，请清除页面底部与 Allow key administrators to delete this key（允许密钥管理员删除此密钥）对应的框。

17. 请选择 Next（下一步）。

18. 在 This account（此账户）部分中，选择此 AWS 账户 中可以在加密操作中使用 KMS 密钥的 IAM 用户和角色。有关更多信息，请参阅允许密钥用户使用 KMS 密钥。

    > **Note**
    >
    > IAM policy 可以向其他 IAM 用户和角色授予使用 KMS 密钥的权限。
    > IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

19. （可选）您可以允许其他 AWS 账户 将此 KMS 密钥用于加密操作。为此，请在页面底部的 Other AWS 账户（其他 Amazon Web Services 账户）部分中，选择 Add another AWS 账户（添加另一个 Amazon Web Services 账户）并输入外部账户的 AWS 账户 ID。要添加多个外部账户，请重复此步骤。

    > **Note**
    >
    > 其他 AWS 账户 的管理员还必须为其用户创建 IAM policy，以允许访问此 KMS 密钥。有关更多信息，请参阅 允许其他账户中的用户使用 KMS 密钥。

20. 选择 下一步。
21. 检视您选择的密钥设置。您仍然可以返回并更改所有设置。
22. 完成后，选择 Finish（完成）以创建密钥。

该过程成功后，显示屏将在您选择的 AWS CloudHSM 密钥存储中显示新 KMS 密钥。当您选择新 KMS 密钥的名称或别名时，其详细信息页面上的 Cryptographic configuration（加密配置）选项卡会显示 KMS 密钥的源（AWS CloudHSM），自定义密钥存储的名称、ID 和类型，以及 AWS CloudHSM 集群的 ID。如果此过程失败，则会出现一条描述失败的错误消息。

> **Tip**
>
> 要更轻松地识别自定义密钥存储中的 KMS 密钥，请在 Customer managed keys（客户托管密钥）页面上，将 Custom key store ID（自定义密钥存储 ID）列添加到显示中。单击右上角的齿轮图标并选择 Custom key store ID (自定义密钥存储 ID)。有关更多信息，请参阅 自定义您的 KMS 密钥表。

在 AWS CloudHSM 密钥存储中创建 KMS 密钥（API）

要在密钥库中创建新的 AWS KMS key（KMS AWS CloudHSM 密钥），请使用CreateKey操作。使用 `CustomKeyStoreId` 参数识别自定义密钥存储并指定 `Origin` 值 `AWS_CLOUDHSM`。

您可能还需要使用 `Policy` 参数指定密钥策略。您可以随时更改密钥策略 (PutKeyPolicy) 并添加可选元素，例如描述和标签。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

以下示例首先调用该DescribeCustomKeyStores操作以验证AWS CloudHSM密钥库是否已连接到其关联的AWS CloudHSM集群。默认情况下，此操作将返回您的账户和区域中的所有自定义密钥存储。要仅描述特定的 AWS CloudHSM 密钥存储，请使用 `CustomKeyStoreId` 或 `CustomKeyStoreName` 参数（而不是同时使用两者）。

在运行此命令之前，请将示例自定义密钥存储 ID 替换为有效的 ID。

> **Note**
>
> 不要在 Description 或 Tags 字段中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

```
$ 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"
   ],
}
```

下一个示例命令使用该DescribeClusters操作来验证与 (cluster-1a23b4cdefgExampleKeyStore) 关联的AWS CloudHSM集群是否至少有两个活动的 HSM。如果集群的 HSM 少于两个，则 CreateKey 操作将失败。

```
$ 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"
        }
    ]
}
```

此示例命令使用CreateKey操作在密钥库中创建 KMS AWS CloudHSM 密钥。要在 AWS CloudHSM 密钥存储中创建 KMS 密钥，您必须提供 AWS CloudHSM 密钥存储的自定义密钥存储 ID，并指定 `Origin` 值为 `AWS_CLOUDHSM`。

该响应包含自定义密钥存储和 AWS CloudHSM 集群的 ID。

在运行此命令之前，请将示例自定义密钥存储 ID 替换为有效的 ID。

```
$ 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"
    ]
  }
}
```

在 AWS CloudHSM 密钥存储中查看 KMS 密钥

要在 AWS CloudHSM 密钥存储中查看 AWS KMS keys，请使用您要用于查看任何 AWS KMS 客户托管密钥的相同方法。要了解基本知识，请参阅查看密钥。要确定您的 AWS CloudHSM 集群中用作 KMS 密钥的密钥材料的密钥，请参阅 查找 KMS 密钥和密钥材料。要了解如何查看记录自定义密钥存储中所有 API 操作的 AWS CloudTrail 日志，请参阅 使用记录 AWS KMS API 调用 AWS CloudTrail。

在 AWS KMS 控制台中，“客户托管密钥”页面会显示自定义密钥存储中的 KMS 密钥以及您的 AWS 账户 和区域中的所有其他客户托管密钥。

但是，以下值特定于 AWS CloudHSM 密钥存储中的 KMS 密钥。

- 存储 KMS 密钥的 AWS CloudHSM 密钥存储的名称和 ID。
- 包含其密钥材料的关联 AWS CloudHSM 集群的集群 ID。
- AWS KMS 控制台中的 `AWS CloudHSM` 或 API 响应中的 `AWS_CLOUDHSM` 的 `Origin` 值。
- 密钥状态值可以是 `Unavailable`。有关解析状态的帮助，请参阅如何修复不可用的 KMS 密钥。

在 AWS CloudHSM 密钥存储中查看 KMS 密钥（控制台）

1. 从 https://console.aws.amazon.com/kms 打开 AWS KMS 控制台。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。

4. 在右上角，选择齿轮图标，选择 Custom key store ID (自定义密钥存储 ID) 和 Origin (源)，然后选择 Confirm (确认)。
5. 要确定任何 AWS CloudHSM 密钥存储中的 KMS 密钥，请查找 Origin（源）值为 AWS CloudHSM 的 KMS 密钥。要标识特定 AWS CloudHSM 密钥存储中的 KMS 密钥，请查看 Custom key store ID（自定义密钥存储 ID）列中的值。
6. 在 AWS CloudHSM 密钥存储中选择 KMS 密钥的别名或密钥 ID。

   此页面显示了有关 KMS 密钥的详细信息，包括其 Amazon Resource Name (ARN)、密钥策略和标签。
7. 选择 Cryptographic configuration（加密配置）选项卡。这些选项卡在 General configuration（常规配置）部分下。

   本部分中包含有关与 KMS 密钥关联的 AWS CloudHSM 密钥存储和 AWS CloudHSM 集群的信息。

在自定义密钥存储中查看 KMS 密钥（API）

您可以使用相同的 AWS KMS API 操作在密钥存储中查看用于任何 KMS 密AWS CloudHSM钥的 KMS 密钥 ListKeys，包括DescribeKey、和GetKeyPolicy。例如，AWS CLI 中的以下 `describe-key` 操作显示 AWS CloudHSM 密钥存储中 KMS 密钥的特殊字段。在运行与此类似的命令之前，请将示例 KMS 密钥 ID 替换为有效值。

```
$ 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"
    }
}
```

有关在 AWS CloudHSM 密钥存储中查找 KMS 密钥或标识 AWS CloudHSM 集群中用作 KMS 密钥的密钥材料的密钥，请参阅 查找 KMS 密钥和密钥材料。

在 AWS CloudHSM 密钥存储中使用 KMS 密钥

在 AWS CloudHSM 密钥存储中创建对称加密 KMS 密钥后，您可以将其用于以下加密操作：

- Encrypt
- Decrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt

自定义密钥存储库不支持生成非对称数据密钥对GenerateDataKeyPair和GenerateDataKeyPairWithoutPlaintext的操作。

当您在请求中使用 KMS 密钥时，按 KMS 密钥的 ID 或别名对其进行标识；您无需指定 AWS CloudHSM 密钥存储或 AWS CloudHSM 集群。响应包含为任何对称加密 KMS 密钥返回的相同字段。

但是，在 AWS CloudHSM 密钥存储中使用 KMS 密钥时，加密操作完全在与 AWS CloudHSM 密钥存储关联的 AWS CloudHSM 集群中执行。该操作使用集群中与您选择的 KMS 密钥关联的密钥材料。

要做到这一点，必须满足以下条件。

- KMS 密钥的密钥状态必须为 `Enabled`。要查找密钥状态，请使用AWS KMS控制台中的状态`KeyState`字段或DescribeKey响应中的字段。
- AWS CloudHSM 密钥存储必须连接到其 AWS CloudHSM 集群。它在AWS KMS控制台或DescribeCustomKeyStores响应`ConnectionState`中的状态必须为`CONNECTED`。
- 与自定义密钥存储关联的 AWS CloudHSM 集群必须包含至少一个活动 HSM。要查找集群中活动 HSM 的数量，请使用AWS KMS控制台、AWS CloudHSM控制台或DescribeClusters操作。

- AWS CloudHSM 集群必须包含 KMS 密钥的密钥材料。如果已从集群中删除密钥材料，或者已从未包含密钥材料的备份中创建 HSM，则加密操作将失败。

如果未满足这些条件，则加密操作失败，并且 AWS KMS 会返回 `KMSInvalidStateException` 异常。通常，您只需重新连接 AWS CloudHSM 密钥存储。有关其他帮助，请参阅如何修复失败的 KMS 密钥。

在 AWS CloudHSM 密钥存储中使用 KMS 密钥时，请注意每个 AWS CloudHSM 密钥存储中的 KMS 密钥针对加密操作共享自定义密钥存储请求限额。如果您超过该配额，则 AWS KMS 将返回 `ThrottlingException`。如果与 AWS CloudHSM 密钥存储关联的 AWS CloudHSM 集群正在处理大量命令（包括与 AWS CloudHSM 密钥存储不相关的命令），则您可能以较低速率获得 `ThrottlingException`。如果您收到任何请求的 `ThrottlingException`，请降低您的请求速率并重试这些命令。有关自定义密钥存储请求限额的详细信息，请参阅 自定义密钥存储请求限额。

查找 KMS 密钥和密钥材料

如果您管理 AWS CloudHSM 密钥存储，则可能需要在每个 AWS CloudHSM 密钥存储中标识 KMS 密钥。例如，您可能需要执行以下某些任务。

- 在 AWS CloudTrail 日志中跟踪 AWS CloudHSM 密钥存储中的 KMS 密钥。
- 预测断开 AWS CloudHSM 密钥存储对 KMS 密钥的影响。
- 在删除 AWS CloudHSM 密钥存储之前计划删除 KMS 密钥。

此外，您可能需要标识 AWS CloudHSM 集群中用作 KMS 密钥的密钥材料的密钥。尽管 AWS KMS 管理 KMS 密钥和密钥材料，但您仍可以控制并负责管理 AWS CloudHSM 集群、HSM 和备份以及 HSM 中的密钥。您可能需要标识密钥以便审核密钥材料，防止意外删除密钥材料或在删除 KMS 密钥后将密钥材料从 HSM 和集群备份中删除。

AWS CloudHSM 密钥存储中 KMS 密钥的所有密钥材料由 `kmsuser` 加密用户（CU）拥有。AWS KMS 将密钥标签属性（该属性仅在 AWS CloudHSM 中可查看）设置为 KMS 密钥的 Amazon 资源名称（ARN）。

要查找 KMS 密钥和密钥材料，请使用下列任一方法。

- 在 AWS CloudHSM 密钥存储中查找 KMS 密钥 – 如何在一个或所有 AWS CloudHSM 密钥存储中标识 KMS 密钥。
- 查找 AWS CloudHSM 密钥存储的所有密钥 – 如何在集群中查找用作 AWS CloudHSM 密钥存储中 KMS 密钥的密钥材料的所有密钥。

- 查找 KMS 密钥的 AWS CloudHSM 密钥 – 如何在集群中查找用作 AWS CloudHSM 密钥存储中特定 KMS 密钥的密钥材料的密钥。
- 查找 AWS CloudHSM 密钥的 KMS 密钥 — 如何在集群中查找特定密钥的 KMS 密钥。

在 AWS CloudHSM 密钥存储中查找 KMS 密钥

如果您管理 AWS CloudHSM 密钥存储，则可能需要在每个 AWS CloudHSM 密钥存储中标识 KMS 密钥。您可以使用此信息在 AWS CloudTrail 日志中跟踪 KMS 密钥操作，预测断开自定义密钥存储对 KMS 密钥的影响或在删除 AWS CloudHSM 密钥存储前计划删除 KMS 密钥。

在 AWS CloudHSM 密钥存储中查找 KMS 密钥（控制台）

要在特定的 AWS CloudHSM 密钥存储中查找 KMS 密钥，请在 Customer managed keys（客户托管密钥）页面上，查看 Custom Key Store Name（自定义密钥存储名称）或 Custom Key Store ID（自定义密钥存储 ID）字段中的值。要确定任何 AWS CloudHSM 密钥存储中的 KMS 密钥，请查找 Origin（源）值为 AWS CloudHSM 的 KMS 密钥。要向显示添加可选列，请选择页面右上角的齿轮图标。

在 AWS CloudHSM 密钥存储中查找 KMS 密钥（API）

要在密钥存储中查找 KMS 密AWS CloudHSM钥，请使用ListKeys和DescribeKey操作，然后按`CustomKeyStoreId`值筛选。在运行示例之前，请将虚构的自定义密钥存储 ID 值替换为有效值。

Bash

要在特定的 AWS CloudHSM 密钥存储中查找 KMS 密钥，请获取账户和区域中的所有 KMS 密钥。然后，按自定义密钥存储 ID 进行筛选。

```
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
```

要获取账户和区域中任何 AWS CloudHSM 密钥存储的 KMS 密钥，请搜索值为 `AWS_CloudHSM` 的 `CustomKeyStoreType`。

```
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

要在特定的AWS CloudHSM密钥存储中查找 KMS 密钥，请使用 Get KmsKeyList 和 Get-KmsKey cmdlet 获取账户和区域中的所有 KMS 密钥。然后，按自定义密钥存储 ID 进行筛选。

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreId -eq
 'cks-1234567890abcdef0'
```

要在账户和区域的任何密AWS CloudHSM钥存储中获取 KMS 密钥，请筛选 CustomKeyStoreType 值AWS_CLOUDHSM。

```
PS C:\> Get-KMSKeyList | Get-KMSKey | where CustomKeyStoreType -eq 'AWS_CLOUDHSM'
```

查找 AWS CloudHSM 密钥存储的所有密钥

您可以标识 AWS CloudHSM 集群中用作 AWS CloudHSM 密钥存储的密钥材料的密钥。为此，请使用 cloudhsm_mgmt_util 中的findAllKeys命令查找拥有或共享的所有密钥的密钥句柄。kmsuser除非您以 kmsuser 身份登录并在 AWS KMS 外部创建了密钥，否则 kmsuser 拥有的所有密钥都表示 KMS 密钥的密钥材料。

集群中的任何加密管理者都可以在不断开 AWS CloudHSM 密钥存储的情况下运行此命令。

1. 按照 Getting started with CloudHSM Management Utility (CMU) [CloudHSM 管理实用工具（CMU）入门] 主题所述的过程，启动 cloudhsm_mgmt_util。
2. 使用加密管理者 (CO) 账户登录 cloudhsm_mgmt_util。
3. 使用 listUsers 命令查找 kmsuser 加密用户的用户 ID。

   在此示例中，kmsuser 具有用户 ID 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. 使用findAllKeys命令查找kmsuser拥有或共享的所有密钥的按键手柄。将示例用户 ID（3）替换为集群中 kmsuser 的实际用户 ID。

   示例输出显示 kmsuser 在集群中的两个 HSM 上拥有密钥句柄为 8、9 和 262162 的密钥。

```
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)
```

查找 AWS CloudHSM 密钥的 KMS 密钥

如果您知道 kmsuser 在集群中拥有的密钥的密钥句柄，则可以使用密钥标签来标识 AWS CloudHSM 密钥存储中的关联 KMS 密钥。

当 AWS KMS 在 AWS CloudHSM 集群中为 KMS 密钥创建密钥材料时，它会在密钥标签中写入 KMS 密钥的 Amazon Resource Name (ARN)。除非您已更改标签值，否则可在 key_mgmt_util 或 cloudhsm_mgmt_util 中使用 getAttribute 命令将密钥与其 KMS 密钥关联。

要运行此过程，您需要临时断开 AWS CloudHSM 密钥存储，以便能以 kmsuser CU 身份登录。

> **Note**
>
> 虽然自定义密钥存储已断开连接，但在自定义密钥存储中创建 KMS 密钥或在加密操作中使用现有 KMS 密钥的所有尝试都将失败。此操作可以阻止用户存储和访问敏感数据。

1. 断开 AWS CloudHSM 密钥存储（如果尚未断开），然后以 kmsuser 身份登录 key_mgmt_util，如 如何断开和登录 中所述。

2. 使用 key_mgmt_util 或 cloudhsm_mgmt_util 中的 `getAttribute` 命令获取特定密钥句柄的标签属性（`OBJ_ATTR_LABEL`、属性 3）。

   例如，此命令使用 cloudhsm_mgmt_util 中的 `getAttribute` 来获取密钥句柄为 `262162` 的密钥的标签属性（属性 3）。输出显示密钥 `262162` 用作 ARN 为 `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` 的 KMS 密钥的密钥材料。在运行此命令之前，请将示例密钥句柄替换为有效句柄。

   对于密钥属性的列表，请使用 listAttributes 命令或查看 AWS CloudHSM 用户指南中的密钥属性参考。

   ```
   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. 注销 key_mgmt_util 或 cloudhsm_mgmt_util，并重新连接 AWS CloudHSM 密钥存储，如 如何注销并重新连接 中所述。

查找 KMS 密钥的 AWS CloudHSM 密钥

您可以在 AWS CloudHSM 密钥存储中使用 KMS 密钥的 KMS 密钥 ID 来标识 AWS CloudHSM 集群中用作其密钥材料的密钥。然后，您可以使用其密钥句柄在 AWS CloudHSM 客户端命令中标识密钥。

当 AWS KMS 在 AWS CloudHSM 集群中为 KMS 密钥创建密钥材料时，它会在密钥标签中写入 KMS 密钥的 Amazon Resource Name (ARN)。除非您已更改标签值，否则可在 key_mgmt_util 中使用 findKey 命令来获取 KMS 密钥的密钥材料的密钥句柄。要运行此过程，您需要临时断开 AWS CloudHSM 密钥存储，以便能以 `kmsuser` CU 身份登录。

> **Note**
>
> 虽然自定义密钥存储已断开连接，但在自定义密钥存储中创建 KMS 密钥或在加密操作中使用现有 KMS 密钥的所有尝试都将失败。此操作可以阻止用户存储和访问敏感数据。

1. 断开 AWS CloudHSM 密钥存储（如果尚未断开），然后以 `kmsuser` 身份登录 key_mgmt_util，如 如何断开和登录 中所述。

2. 在 key_mgmt_util 中使用 findKey 命令在 AWS CloudHSM 密钥存储中搜索其标签与 KMS 密钥的 ARN 匹配的密钥。将 -l（小写 L 表示“标签”）参数的值中的示例 KMS 密钥 ARN 替换为有效 KMS 密钥 ARN。

   例如，此命令查找其标签与示例 KMS 密钥 ARN `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` 匹配的密钥。示例输出显示密钥句柄为 262162 的密钥的标签中包含指定的 KMS 密钥 ARN。现在，您可以在其他 key_mgmt_util 命令中使用此密钥句柄。

```
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. 注销 key_mgmt_util 并重新连接自定义密钥存储，如如何注销并重新连接中所述。

计划从 AWS CloudHSM 密钥存储删除 KMS 密钥

如果您确定您不需要在任何加密操作中使用 AWS KMS key，您可以计划删除 KMS 密钥。同样使用用于计划从 AWS KMS 删除任何 KMS 密钥的过程。此外，让 AWS CloudHSM 密钥存储保持连接状态，以便 AWS KMS 可以在等待期到期后从关联的 AWS CloudHSM 集群中删除对应的密钥材料。

您可以在 AWS CloudTrail 日志中监控 KMS 密钥的计划、取消和删除。

> **Warning**
>
> 删除 KMS 密钥是一种具有破坏性且潜在危险的操作，可阻止您恢复使用 KMS 密钥加密的所有数据。在安排删除 KMS 密钥之前，请检查 KMS 密钥的过去使用情况，并创建一个 Amazon CloudWatch 警报，当有人试图使用 KMS 密钥等待删除时，该警报会提醒您。如有可能，禁用 KMS 密钥而不是将其删除。

如果您计划从 AWS CloudHSM 密钥存储中删除 KMS 密钥，其密钥状态将变为 Pending deletion（等待删除）。KMS 密钥将在整个等待期处于 Pending deletion（等待删除）状态，即使 KMS 密钥因您断开自定义密钥存储而不可用时都是如此。这允许您在等待期内随时取消删除 KMS 密钥。

等待期到期后，AWS KMS 将从 AWS KMS 删除 KMS 密钥。然后，AWS KMS 将尽可能从关联的 AWS CloudHSM 集群中删除密钥材料。如果 AWS KMS 无法删除密钥材料（如当密钥存储与 AWS KMS 断开连接时），您可能需要手动从集群中删除孤立密钥材料。

AWS KMS 不会从集群备份中删除密钥材料。即使您从 AWS KMS 删除 KMS 密钥并且从 AWS CloudHSM 集群删除其密钥材料，通过备份创建的集群也可能包含已删除的密钥材料。要永久删除密钥材料，请 KMS 密钥的查看创建日期。然后，删除所有集群备份（可能包含密钥材料）。

当您计划从 AWS CloudHSM 密钥存储中删除 KMS 密钥时，KMS 密钥将立即变得不可用（取决于最终一致性）。不过，在再次使用 KMS 密钥（例如解密数据密钥）之前，使用受 KMS 密钥保护的数据密钥加密的资源不会受到影响。此问题会影响 AWS 服务，因为许多服务使用数据密钥来保护您的资源。有关详细信息，请参阅不可用的 KMS 密钥如何影响数据密钥。

对自定义密钥存储进行故障排除

AWS CloudHSM 密钥存储被设计为可用且有弹性。不过，为了让 AWS CloudHSM 密钥存储正常运行，您必须修复存在的一些错误情况。

主题

- 如何修复不可用的 KMS 密钥
- 如何修复失败的 KMS 密钥
- 如何修复连接故障
- 如何响应加密操作失败
- 如何修复无效的 kmsuser 凭证
- 如何删除孤立密钥材料
- 如何恢复 KMS 密钥的已删除密钥材料
- 如何以 kmsuser 身份登录

如何修复不可用的 KMS 密钥

AWS CloudHSM 密钥存储中 AWS KMS keys 的密钥状态通常为 `Enabled`。与所有 KMS 密钥相似，当您禁用 AWS CloudHSM 密钥存储中的 KMS 密钥或者计划删除这些密钥时，密钥状态会发生变化。但是，与其他 KMS 密钥不同，自定义密钥存储中的 KMS 密钥还可具有密钥状态 `Unavailable`。

密钥状态 Unavailable 表示 KMS 密钥位于被故意断开连接的自定义密钥存储中，并且尝试重新连接该集群（如果有）失败。当某个 KMS 密钥不可用时，您可以查看和管理该 KMS 密钥，但不能将其用于加密操作。

要查找 KMS 密钥的密钥状态，请在 Customer managed keys（客户托管密钥）页面上，查看 KMS 密钥的 Status（状态）字段。或者，使用DescribeKey操作并查看响应中的KeyState元素。有关更多信息，请参阅 查看密钥。

已断开的自定义密钥存储中的 KMS 密钥的密钥状态将为 Unavailable 或 PendingDeletion。计划从自定义密钥存储中删除的 KMS 密钥的密钥状态为 Pending Deletion，即使自定义密钥存储已断开连接也是如此。这使您可以取消计划的密钥删除而无需重新连接自定义密钥存储。

要修复不可用的 KMS 密钥，请重新连接自定义密钥存储。重新连接自定义密钥存储后，自定义密钥存储中的 KMS 密钥的密钥状态将自动还原到之前的状态，例如 Enabled 或 Disabled。待删除的 KMS 密钥将保持 PendingDeletion 状态。但是，当问题仍然存在时，启用和禁用不可用的 KMS 密钥不会更改其密钥状态。仅当密钥变得可用时，启用或禁用操作才会生效。

如需帮助解决失败的连接，请参阅如何修复连接故障。

如何修复失败的 KMS 密钥

在 AWS CloudHSM 密钥存储中创建和使用 KMS 密钥的问题可能由 AWS CloudHSM 密钥存储、其关联的 AWS CloudHSM 集群、KMS 密钥或其密钥材料导致。

当某个 AWS CloudHSM 密钥存储与其 AWS CloudHSM 集群断开连接时，该自定义密钥存储中 KMS 密钥的密钥状态为 Unavailable。在断开的 AWS CloudHSM 密钥存储中创建 KMS 密钥的所有请求都将返回 CustomKeyStoreInvalidStateException 异常。所有加密、解密、重新加密或生成数据密钥的请求都将返回 KMSInvalidStateException 异常。要修复该问题，请重新连接 AWS CloudHSM 密钥存储。

但是，您使用 AWS CloudHSM 密钥存储 KMS 密钥进行加密操作的尝试可能会失败，即使其密钥状态为 Enabled 并且 AWS CloudHSM 密钥存储的连接状态为 Connected 也是如此。这可能由以下任一情况导致。

- KMS 密钥的密钥材料可能已从关联的 AWS CloudHSM 集群中删除。要进行调查，请查找 KMS 密钥的密钥材料的密钥句柄，并在必要时尝试恢复密钥材料。
- 所有 HSM 都已从与 AWS CloudHSM 密钥存储关联的 AWS CloudHSM 集群中删除。要在加密操作中使用 AWS CloudHSM 密钥存储中的某个 KMS 密钥，其 AWS CloudHSM 集群必须至少包含一个活动 HSM。要验证AWS CloudHSM集群中 HSM 的数量和状态，请使用AWS CloudHSM控制

台或DescribeClusters操作。要向集群添加 HSM，请使用AWS CloudHSM控制台或CreateHsm操作。

- 与 AWS CloudHSM 密钥存储关联的 AWS CloudHSM 集群已删除。要修复该问题，请从与原始集群相关的备份创建一个集群，例如原始集群的备份或用于创建原始集群的备份。然后，在自定义密钥存储设置中编辑集群 ID。有关说明，请参阅如何恢复 KMS 密钥的已删除密钥材料。
- 与自定义密钥存储关联的 AWS CloudHSM 集群没有任何可用的 PKCS #11 会话。这种情况通常发生在高突发流量期间，此时需要额外的会话来服务流量。要响应带有关 PKCS #11 会话的错误消息的 `KMSInternalException`，请退后并重试该请求。

如何修复连接故障

如果您尝试连接 AWS CloudHSM 密钥存储到其 AWS CloudHSM 集群，但操作失败，则 AWS CloudHSM 密钥存储的连接状态将更改为 `FAILED`。要查找AWS CloudHSM密钥库的连接状态，请使用AWS KMS控制台或DescribeCustomKeyStores操作。

另外，由于容易检测到集群配置错误，一些连接尝试会很快失败。在这种情况下，连接状态仍为 `DISCONNECTED`。这些失败将返回错误消息或例外来说明尝试失败的原因。查看例外描述和集群要求，纠正问题，更新 AWS CloudHSM 密钥存储（如有必要）并尝试重新连接。

当连接状态为时`FAILED`，运行DescribeCustomKeyStores操作并查看响应中的`ConnectionErrorCode`元素。

> **Note**
>
> 当 AWS CloudHSM 密钥存储的连接状态为 `FAILED` 时，您必须先断开 AWS CloudHSM 密钥存储，然后再尝试重新连接它。您无法连接具有 `FAILED` 连接状态的 AWS CloudHSM 密钥存储。

- `CLUSTER_NOT_FOUND` 表示 AWS KMS 找不到具有指定集群 ID 的 AWS CloudHSM 集群。这可能是因为向 API 操作提供了错误的集群 ID，或者集群被删除而不是被替换。要修复此错误，请验证集群 ID，例如使用AWS CloudHSM控制台或DescribeClusters操作。如果集群已被删除，请从源的最新备份创建一个集群。然后，断开 AWS CloudHSM 密钥存储，编辑 AWS CloudHSM 密钥存储集群 ID 设置，并重新连接 AWS CloudHSM 密钥存储到集群。
- `INSUFFICIENT_CLOUDHSM_HSMS` 表示关联的 AWS CloudHSM 集群不包含任何 HSM。要连接，集群必须至少具有一个 HSM。要查找集群中 HSM 的数量，请使用DescribeClusters操作。要解决此错误，请添加至少一个 HSM 到集群。如果您添加了多个 HSM，最好在不同的可用区中创建它们。

- INSUFFICIENT_FREE_ADDRESSES_IN_SUBNET 表明 AWS KMS 无法将 AWS CloudHSM 密钥存储连接至其 AWS CloudHSM 集群，因为至少有一个与集群关联的私有子网没有任何可用的 IP 地址。AWS CloudHSM 密钥存储连接需要在每个关联的私有子网中有一个空闲的 IP 地址，但最好有两个空闲的 IP 地址。

  您无法将 IP 地址（CIDR 块）添加到现有子网。如有可能，请移动或删除在子网中使用 IP 地址的其他资源，例如未使用的 EC2 实例或弹性网络接口。除此之外，您可以通过 AWS CloudHSM 集群的近期备份创建一个集群，集群中包含具有更多可用地址空间的新的或现有私有子网。然后，要将新集群与您的 AWS CloudHSM 密钥存储关联，请断开自定义密钥存储，将 AWS CloudHSM 密钥存储的集群 ID 更改为新集群的 ID，然后尝试再次连接。

  > **Tip**
  >
  > 要避免重置 kmsuser 密码，请使用 AWS CloudHSM 集群的最新备份。

- INTERNAL_ERROR 指示 AWS KMS 因内部错误而无法完成请求。重试 请求。对于 ConnectCustomKeyStore 请求，先断开 AWS CloudHSM 密钥存储，然后再尝试重新连接它。
- INVALID_CREDENTIALS 表示 AWS KMS 无法登录到关联的 AWS CloudHSM 集群，因为它没有正确的 kmsuser 账户密码。如需帮助解决此错误，请参阅如何修复无效的 kmsuser 凭证。
- NETWORK_ERRORS 通常表示暂时性网络问题。断开 AWS CloudHSM 密钥存储，等待几分钟，然后重试连接。
- SUBNET_NOT_FOUND 表示 AWS CloudHSM 集群配置中至少有一个子网已被删除。如果 AWS KMS 无法找到集群配置中的所有子网，则尝试将 AWS CloudHSM 密钥存储连接到 AWS CloudHSM 集群将失败。

  要修复此错误，请从同一 AWS CloudHSM 集群的最近备份创建集群。（此过程使用 VPC 和私有子网创建新的集群配置。）验证新集群是否满足自定义密钥存储的要求，并记下新集群 ID。然后，要将新集群与您的 AWS CloudHSM 密钥存储关联，请断开自定义密钥存储，将 AWS CloudHSM 密钥存储的集群 ID 更改为新集群的 ID，然后尝试再次连接。

  > **Tip**
  >
  > 要避免重置 kmsuser 密码，请使用 AWS CloudHSM 集群的最新备份。

- USER_LOCKED_OUT 表示 kmsuser 加密用户 (CU) 账户无法访问关联的 AWS CloudHSM 集群，因为失败的密码尝试过多。如需帮助解决此错误，请参阅如何修复无效的 kmsuser 凭证。

要修复此错误，请断开 AWS CloudHSM 密钥存储并使用 cloudhsm_mgmt_util 中的 changePswd 命令以更改 kmsuser 账户密码。然后，编辑自定义密钥存储的 kmsuser 密码设置并重试连接。如需帮助，请使用如何修复无效的 kmsuser 凭证主题中所述的过程。

- USER_LOGGED_IN 表示 kmsuser CU 帐户已登录到关联的 AWS CloudHSM 集群。这会阻止 AWS KMS 轮换 kmsuser 账户密码和登录到群集。要修复此错误，请从集群中注销 kmsuser CU。如果您更改了用于登录到集群的 kmsuser 密码，则还必须更新 AWS CloudHSM 密钥存储的密钥存储密码值。有关帮助信息，请参阅 如何注销并重新连接。
- USER_NOT_FOUND 表示 AWS KMS 无法在关联的 AWS CloudHSM 集群中找到 kmsuser CU 账户。要修复此错误，请在集群中创建 kmsuser CU 账户，然后更新 AWS CloudHSM 密钥存储的密钥存储密码值。有关帮助信息，请参阅 如何修复无效的 kmsuser 凭证。

如何响应加密操作失败

在自定义密钥存储中使用 KMS 密钥的加密操作可能会失败，并显示 KMSInvalidStateException。以下错误消息可能附带 KMSInvalidStateException。

KMS 无法与您的 CloudHSM 集群进行通信。这可能是暂时的网络问题。如果您反复看到此错误，请验证 AWS CloudHSM 集群 VPC 的网络 ACL 和安全组规则是否正确。

- 虽然它是 HTTPS 400 错误，但它可能是由于暂时的网络问题引起的。要进行响应，首先重试请求。但是，如果继续失败，请检查网络组件的配置。此错误很可能是由于网络组件（例如阻止传出流量的防火墙规则或 VPC 安全组规则）的错误配置引起的。

KMS 无法与您的 AWS CloudHSM 集群通信，因为 kmsuser 已被锁定。如果您反复看到此错误，请断开 AWS CloudHSM 密钥存储的连接并重置 kmsuser 账户的密码。更新自定义密钥存储的 kmsuser 密码，然后重试请求。

- 此错误消息表示 kmsuser 加密用户（CU）账户无法访问关联的 AWS CloudHSM 集群，因为失败的密码尝试过多。如需帮助解决此错误，请参阅如何断开和登录。

如何修复无效的 **kmsuser** 凭证

当您连接 AWS CloudHSM 密钥存储时，AWS KMS 会以 kmsuser 加密用户（CU）身份登录到关联的 AWS CloudHSM 集群。在 AWS CloudHSM 密钥存储断开之前，它将保持登录状态。DescribeCustomKeyStores 响应显示 ConnectionState 值 FAILED 以及 ConnectionErrorCode 值 INVALID_CREDENTIALS，如以下示例中所示。

如果您断开 AWS CloudHSM 密钥存储并更改 kmsuser 密码，AWS KMS 将无法使用 kmsuser CU 账户的凭证登录到 AWS CloudHSM 集群。因此，所有连接 AWS CloudHSM 密钥存储的尝试都将失败。DescribeCustomKeyStores 响应显示 ConnectionState 值 FAILED 以及 ConnectionErrorCode 值 INVALID_CREDENTIALS，如以下示例中所示。

```
$ 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"
   ],
}
```

此外，在使用不正确的密码登录到集群的尝试失败五次后，AWS CloudHSM 将锁定用户账户。要登录到集群，您必须更改账户密码。

如果 AWS KMS 在尝试以 kmsuser CU 身份登录到集群时获得锁定响应，连接 AWS CloudHSM 密钥存储的请求将失败。DescribeCustomKeyStores响应中包含ConnectionState的ConnectionErrorCode值为FAILED，值为USER_LOCKED_OUT，如以下示例所示。

```
$ 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"
   ],
}
```

要修复上述任一状况，请使用以下过程。

1. 断开 AWS CloudHSM 密钥存储。
2. 运行DescribeCustomKeyStores操作并查看响应中ConnectionErrorCode元素的值。
   - 如果 ConnectionErrorCode 值为 INVALID_CREDENTIALS，请确定 kmsuser 账户的当前密码。必要时，请使用 cloudhsm_mgmt_util 中的 changePswd 命令将密码设置为已知值。
   - 如果 ConnectionErrorCode 值是 USER_LOCKED_OUT，您必须使用 cloudhsm_mgmt_util 中的 changePswd 命令更改 kmsuser 密码。
3. 编辑 kmsuser 密码设置，使其与当前集群中的 kmsuser 密码匹配。此操作将告知 AWS KMS 要用来登录到集群的密码。它不会更改集群中的 kmsuser 密码。
4. 连接自定义密钥存储。

如何删除孤立密钥材料

在计划从 AWS CloudHSM 密钥存储中删除 KMS 密钥后，您可能需要从关联的 AWS CloudHSM 集群中手动删除对应的密钥材料。

当您在 AWS CloudHSM 密钥存储中创建 KMS 密钥时，AWS KMS 将在 AWS KMS 中创建 KMS 密钥元数据并在关联的 AWS CloudHSM 集群中生成密钥材料。当您计划在 AWS CloudHSM 密钥存储中删除 KMS 密钥时，在等待期过后，AWS KMS 将删除 KMS 密钥元数据。然后，AWS KMS 将尽可能从 AWS CloudHSM 集群中删除对应的密钥材料。如果 AWS KMS 无法访问集群（例如与 AWS CloudHSM 密钥存储断开连接或 kmsuser 密码更改），尝试可能会失败。AWS KMS 不会尝试从集群备份中删除密钥材料。

AWS KMS 会报告其尝试从 AWS CloudTrail 日志 DeleteKey 事件条目中的集群中删除密钥材料的结果。它会在 additionalEventData 元素的 backingKeysDeletionStatus 元素中显示，如以下示例条目所示。该条目还包含 KMS 密钥 ARN、AWS CloudHSM 集群 ID 和密钥材料的密钥句柄 (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"
}
```


要从关联的 AWS CloudHSM 集群中删除密钥材料，请使类似于下面的过程。本示例使用 AWS CLI 和 AWS CloudHSM 命令行工具，但您可以使用 AWS Management Console而不是 CLI。

1. 断开 AWS CloudHSM 密钥存储（如果尚未断开），然后登录到 key_mgmt_util，如 如何断开和登录 中所述。
2. 使用 key_mgmt_util 中的 deleteKey 命令从集群内的 HSM 中删除密钥。

   例如，以下命令从集群内的 HSM 中删除密钥 262162。密钥句柄列在 CloudTrail 日志条目中。

```
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. 注销 key_mgmt_util 并重新连接 AWS CloudHSM 密钥存储，如 如何注销并重新连接 中所述。

如何恢复 KMS 密钥的已删除密钥材料

如果删除了 AWS KMS key 的密钥材料，则 KMS 密钥不可用，并且在 KMS 密钥下加密的所有密文都无法解密。如果从关联的 AWS CloudHSM 集群中删除了 AWS CloudHSM 密钥存储中的 KMS 密钥的密钥材料，则会出现这种情况。但是，可以恢复该密钥材料。

当您在 AWS CloudHSM 密钥存储中创建 AWS KMS key（KMS 密钥）时，AWS KMS 将登录到关联的 AWS CloudHSM 集群并创建 KMS 密钥的密钥材料。它还会将密码更改为只有它知道的值，并且只要连接了 AWS CloudHSM 密钥存储，它就会保持登录状态。由于只有密钥所有者（即创建密钥的 CU）才能删除密钥，因此不太可能意外地从 HSM 中删除密钥。

但是，如果从集群内的 HSM 中删除 KMS 密钥的密钥材料，KMS 密钥的密钥状态最终将变为 UNAVAILABLE。如果您尝试使用 KMS 密钥进行加密操作，该操作将失败并出现 KMSInvalidStateException 异常。最重要的是，在 KMS 密钥下加密的任何数据都无法解密。

在某些情况下，您可以通过从包含密钥材料的备份创建集群来恢复已删除的密钥材料。仅当在密钥存在且未被删除的情况下创建了一个备份时，此策略才有效。

使用以下过程恢复密钥材料。

1. 查找包含密钥材料的集群备份。备份还必须包含支持集群及其加密数据所需的所有用户和密钥。

   使用DescribeBackups操作列出集群的备份。然后，使用备份时间戳帮助您选择一个备份。要将输出限制为与 AWS CloudHSM 密钥存储关联的集群，请使用 Filters 参数，如以下示例所示。

```
$ aws cloudhsmv2 describe-backups --filters clusterIds=<cluster ID>
{
    "Backups": [
        {
```

```
            "ClusterId": "cluster-1a23b4cdefg",
            "BackupId": "backup-9g87f6edcba",
            "CreateTimestamp": 1536667238.328,
            "BackupState": "READY"
        },
             ...
    ]
}
```

2. 从所选备份创建集群。验证备份是否包含已删除的密钥以及集群所需的其他用户和密钥。
3. 断开 AWS CloudHSM 密钥存储，以便您可以编辑其属性。
4. 编辑 AWS CloudHSM 密钥存储的集群 ID。输入您从备份创建的集群的集群 ID。由于该集群与原始集群共享备份历史记录，新集群 ID 应该是有效的。
5. 重新连接 AWS CloudHSM 密钥存储。

如何以 **kmsuser** 身份登录

为了创建和管理 AWS CloudHSM 密钥存储的 AWS CloudHSM 集群中的密钥材料，AWS KMS 将使用 kmsuser 加密用户（CU）账户。您在集群中创建 kmsuser CU 账户并在创建 AWS CloudHSM 密钥存储时将该账户的密码提供给 AWS KMS。

一般而言，AWS KMS 将管理 kmsuser 账户。但是，对于某些任务，您需要断开 AWS CloudHSM 密钥存储，以 kmsuser CU 身份登录到集群，并使用 cloudhsm_mgmt_util 和 key_mgmt_util 命令行工具。

> **Note**
>
> 虽然自定义密钥存储已断开连接，但在自定义密钥存储中创建 KMS 密钥或在加密操作中使用现有 KMS 密钥的所有尝试都将失败。此操作可以阻止用户存储和访问敏感数据。

本主题介绍了如何断开 AWS CloudHSM 密钥存储并以 kmsuser 身份登录、运行 AWS CloudHSM 命令行工具以及注销并重新连接 AWS CloudHSM 密钥存储。

主题

- 如何断开和登录
- 如何注销并重新连接

如何断开和登录

每当需要以 kmsuser CU 身份登录到关联的集群时，请使用以下过程。

1. 断开 AWS CloudHSM 密钥存储（如果尚未断开）。可以使用 AWS KMS 控制台或 AWS KMS API。

   当您的 AWS CloudHSM 密钥已连接时，您便已经以 kmsuser 身份登录 AWS KMS。这将防止您以 kmsuser 身份登录或更改 kmsuser 密码。

   例如，此命令用于断开示例密钥存储的连接。DisconnectCustomKeyStore将示例 AWS CloudHSM 密钥存储 ID 替换为有效的 ID。

   ```
   $ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
   ```

2. 启动 cloudhsm_mgmt_util。使用 AWS CloudHSM 用户指南的准备运行 cloudhsm_mgmt_util 部分中所述的程序。
3. 在 AWS CloudHSM 集群上以加密管理者 (CO) 身份登录到 cloudhsm_mgmt_util。

   例如，以下命令以名为 admin 的 CO 的身份进行登录。将示例 CO 用户名和密码替换为有效值。

   ```
   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. 使用 changePswd 命令将 kmsuser 账户的密码更改为您知道的值。（AWS KMS 将在您连接 AWS CloudHSM 密钥存储时轮换密码。）密码必须由 7 到 32 个字母数字字符组成。它区分大小写，并且不能包含任何特殊字符。

   例如，此命令会将 kmsuser 密码更改为 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. 使用您设置的密码以 kmsuser 身份登录到 key_mgmt_util 或 cloudhsm_mgmt_util。有关详细说明，请参阅 cloudhsm_mgmt_util 入门和 key_mgmt_util 入门。您使用的工具取决于任务。

   例如，以下命令将登录到 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
```

如何注销并重新连接

1. 执行任务，然后从命令行工具注销。如果您不注销，重新连接 AWS CloudHSM 密钥存储的尝试将失败。

```
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. 为自定义密钥存储编辑 kmsuser 密码设置。

   这将告知 AWS KMS 集群中的 kmsuser 的当前密码。如果忽略此步骤，AWS KMS 将无法以 kmsuser 身份登录到集群，并且重新连接自定义密钥存储的所有尝试都将失败。您可以使用AWS KMS控制台或UpdateCustomKeyStore操作的KeyStorePassword参数。

   例如，以下命令将告知 AWS KMS 当前密码为 tempPassword。将示例密码替换为实际密码。

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --
key-store-password tempPassword
```

3. 重新连接 AWS KMS 密钥存储至其 AWS CloudHSM 集群。将示例 AWS CloudHSM 密钥存储 ID 替换为有效的 ID。在连接过程中，AWS KMS 会将 kmsuser 密码更改为只有它知道的值。

ConnectCustomKeyStore操作很快就会恢复，但连接过程可能需要很长时间。初始响应不指示连接过程是否成功。

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

4. 使用该DescribeCustomKeyStores操作验证AWS CloudHSM密钥库是否已连接。将示例 AWS CloudHSM 密钥存储 ID 替换为有效的 ID。

   在本示例中，连接状态字段表明 AWS CloudHSM 密钥存储现已连接。

```
$ 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"
   ],
}
```

外部密钥存储

外部密钥存储允许您使用外部的加密密钥来保护您的 AWS 资源。 AWS此高级功能专为受监管的工作负载设计，这些工作负载必须使用存储在您控制的外部密钥管理系统中的加密密钥加以保护。外部密钥存储支持AWS 数字主权承诺，为您提供对数据的主权控制权 AWS，包括能够使用您拥有并在外部控制的密钥材料进行加密。 AWS

外部密钥存储库是由您拥有并在外部管理的外部密钥管理器支持的自定义密钥存储库 AWS。您的外部密钥管理器可以是实体或虚拟硬件安全模块（HSM），也可以是任何能够生成和使用加密密钥的基于硬件或软件的系统。在外部密钥存储中使用 KMS 密钥的加密和解密操作，由您的外部密钥管理器使用加密密钥材料执行，该功能称为持有自己的密钥（HYOK）。

AWS KMS 切勿直接与外部密钥管理器交互，也无法创建、查看、管理或删除您的密钥。相反，仅与您提供的外部密钥存储代理（XKS 代理）软件进行 AWS KMS 交互。您的外部密钥存储代理负责调解与您的外部密钥管理器 AWS KMS 之间的所有通信。它会将来自 AWS KMS 您的外部密钥管理器的所有请求传送回您的外部密钥管理器，并将来自外部密钥管理器的响应传回到。 AWS KMS外部密钥存储代

理还将来自 AWS KMS 的通用请求转换为外部密钥管理器可以理解的供应商特定格式，允许您将外部密钥存储与来自不同供应商的密钥管理器一起使用。

您可以在外部密钥存储中使用 KMS 密钥进行客户端加密，包括使用 AWS Encryption SDK。但是外部密钥存储是服务器端加密的重要资源，它允许您使用外部的加密密钥对 AWS 资源 AWS 服务 进行多重保护。 AWS AWS 服务 支持用于对称加密的客户托管密钥还支持外部密钥存储中的 KMS 密钥。有关服务支持的详细信息，请参阅 AWS 服务集成。

外部密钥存储允许您 AWS KMS 用于受监管的工作负载，在这些工作负载中，加密密钥必须在外部存储和使用 AWS。不过，这样的工作负载与标准责任共担模型相去甚远，会造成额外的运营负担。对大多数客户而言，可用性和延迟的更大风险将超过外部密钥存储的预期安全优势。

外部密钥存储允许您控制信任根密钥。在外部密钥存储中以 KMS 密钥加密的数据，只能使用您控制的外部密钥管理器进行解密。如果您暂时撤消对外部密钥管理器的访问权限，例如断开外部密钥存储库的连接或断开外部密钥管理器与外部密钥存储代理的连接，则在恢复加密密钥之前，将 AWS 失去对加密密钥的所有访问权限。在此期间，无法解密以 KMS 密钥加密的加密文字。如果您永久撤消对外部密钥管理器的访问权限，在外部密钥存储中以 KMS 密钥加密的所有加密文字都不可恢复。唯一的例外是那些会短暂缓存受您的 KMS 密钥保护的数据密钥的 AWS 服务。这些数据密钥将继续有效，直到您停用资源或缓存过期。有关更多信息，请参阅 不可用的 KMS 密钥如何影响数据密钥。

外部密钥存储可以解锁受监管工作负载的少数用例，在这些用例中，加密密钥必须完全由您控制且无法访问 AWS。不过，这是您运营基于云的基础设施方式的重大变化，也是责任共担模型的重大转变。对大多数工作负载而言，额外的运营负担以及可用性和性能的更大风险将超过外部密钥存储所带来的预期安全优势。

了解更多：

- AWS 新闻博客中的宣布推出 AWS KMS 外部密钥存储。

我需要外部密钥存储吗？

对于大多数用户而言，受 FIPS 140-2 Security Level 3 验证的硬件安全模块保护的默认 AWS KMS 密钥存储可以满足他们的安全、控制和监管要求。外部密钥存储用户会承担大量成本、维护和故障排除负担，以及与延迟、可用性和可靠性有关的风险。

在考虑外部密钥存储时，请花一些时间了解备选方案，包括由您拥有和管理的 AWS CloudHSM 集群支持的 AWS CloudHSM 密钥存储，以及在您自己的 HSM 中生成并可以按需从 KMS 密钥中删除的带

有导入密钥材料的 KMS 密钥。特别要注意的是，导入过期间隔非常短的密钥材料可以提供类似级别的控制，却不会带来性能或可用性风险。

如果您有以下要求，则外部密钥存储可能是适合您组织的解决方案：

- 您需要在本地密钥管理器中使用加密密钥，或者在您控制范围之外的密钥管理器中使用加密密钥。AWS
- 您必须证明，在云端之外，您加密密钥的保留完全由自己控制。
- 您必须使用具有独立授权的加密密钥进行加密和解密。
- 密钥材料必须受辅助、独立的审计路径的约束。

如果您选择外部密钥存储，请将其使用限制在需要使用 AWS之外的加密密钥进行保护的工作负载。

责任共担模式

标准 KMS 密钥使用在 AWS KMS 拥有和管理的 HSM 中生成和使用的密钥材料。您可以在 KMS 密钥上建立访问控制策略，并配置 AWS 服务 该策略使用 KMS 密钥来保护您的资源。 AWS KMS 负责您的 KMS 密钥中密钥材料的安全性、可用性、延迟和耐久性。

外部密钥存储中的 KMS 密钥依赖外部密钥管理器中的密钥材料和操作。因此，责任的天平朝着您的方向移动。您对外部密钥管理器中加密密钥的安全性、可靠性、耐用性和性能负责。 AWS KMS 负责迅速响应请求并与您的外部密钥存储代理进行通信，并负责维护我们的安全标准。为确保每个外部密钥存储的密文至少与标准密文一样强，请 AWS KMS 先使用您的 KMS AWS KMS 密钥特有的 AWS KMS 密钥材料对所有明文进行加密，然后将其发送给您的外部密钥管理器以使用您的外部密钥进行加密，这种过程称为双重加密。因此，无论是 AWS KMS 还是外部密钥材料的所有者，都无法单独解密双重加密的加密文字。

您要对以下事项负责：维护符合您监管和性能标准的外部密钥管理器，提供和维护符合 AWS KMS 外部密钥存储代理 API 规范的外部密钥存储代理，以及确保密钥材料的可用性和持久性。您还必须创建、配置和维护外部密钥存储。当出现由您维护的组件导致的错误时，您必须做好识别和解决错误的准备，以便 AWS 服务能够在不造成不当干扰的情况下访问您的资源。 AWS KMS 提供故障排除指导，帮助您确定问题的原因和最可能的解决方案。

查看 AWS KMS 记录外部密钥存储的 Amazon CloudWatch 指标和维度。 AWS KMS 强烈建议您创建 CloudWatch 警报来监控您的外部密钥存储，这样您就可以在性能和操作问题出现之前检测到这些问题的早期迹象。

发生了什么变化？

外部密钥存储仅支持对称加密 KMS 密钥。在内部 AWS KMS，您使用和管理外部密钥存储库中的 KMS 密钥的方式与管理其他客户托管密钥的方式大致相同，包括设置访问控制策略和监控密钥使用情况。您可以使用具有相同参数的相同 API 来请求使用了外部密钥存储中的 KMS 密钥的加密操作，该外部密钥存储可用于任何 KMS 密钥。定价也与标准 KMS 密钥相同。有关详细信息，请参阅 在外部密钥存储中管理 KMS 密钥、在外部密钥存储中使用 KMS 密钥 和 AWS Key Management Service 定价。

不过，使用外部密钥存储时，以下原则会发生变化：

- 您对密钥操作的可用性、持久性和延迟负责。
- 您对外部密钥管理器系统的开发、购买、运营和许可的所有费用负责。
- 您可以对来自 AWS KMS 外部密钥存储代理的所有请求实施独立授权。
- 您可以监控、审核和记录外部密钥存储代理的所有操作以及外部密钥管理器中与 AWS KMS 请求相关的所有操作。

从何处开始？

要创建和管理外部密钥存储，您需要选择外部密钥存储代理连接选项、汇编先决条件，然后创建和配置外部密钥存储。要开始使用，请参阅 规划外部密钥存储。

配额

AWS KMS 允许每个 AWS 账户 和区域中最多有 10 个自定义密钥存储库，包括AWS CloudHSM 密钥存储库和外部密钥存储库，无论其连接状态如何。此外，使用外部密钥存储中 KMS 密钥 存在 AWS KMS 请求限额。

如果您为外部密钥存储代理选择 VPC 代理连接，则所需组件（例如 VPC、子网和网络负载均衡器）也可能存在限额。有关这些限额的信息，请使用服务限额控制台。

区域

为了最大限度地减少网络延迟，请在离外部密钥管理器最近的 AWS 区域 中创建外部密钥存储组件。如果可行，请选择网络往返时间（RTT）不超过 35 毫秒的区域。

除中国（北京）和中国（宁夏）外， AWS KMS 所有支持外部密钥存储的 AWS 区域 地区均支持外部密钥存储。

不支持的功能

AWS KMS 不支持自定义密钥存储库中的以下功能。

- 非对称 KMS 密钥
- 非对称数据密钥对
- HMAC KMS 密钥
- 具有导入密钥材料的 KMS 密钥
- 自动密钥轮换
- 多区域密钥

主题

外部密钥存储概念

本主题介绍了外部密钥存储中用到的一些概念。

主题

- 双重加密

外部密钥存储

外部密钥存储库是由您拥有和管理的外部密钥管理器支持的 AWS KMS 自定义密钥存储库。 AWS 外部密钥存储中的每个 KMS 密钥都与您外部密钥管理器中的外部密钥相关联。在外部密钥存储中使用 KMS 密钥进行加密或解密时，该操作将在您的外部密钥管理器中使用您的外部密钥执行，这种安排称为持有自己的密钥（HYOK）。此功能专为需要在自己的外部密钥管理器中维护加密密钥的组织设计。

外部密钥存储可确保保护您的 AWS 资源的加密密钥和操作保留在您的外部密钥管理器中，由您控制。AWS KMS 向您的外部密钥管理器发送请求以加密和解密数据，但 AWS KMS 无法创建、删除或管理任何外部密钥。来自 AWS KMS 外部密钥管理器的所有请求均由您提供、拥有和管理的外部密钥存储代理软件组件进行中介。

AWS 支持 AWS KMS 客户托管密钥的服务可以使用外部密钥存储区中的 KMS 密钥来保护您的数据。因此，您的数据最终由使用您外部密钥管理器中的加密操作的密钥进行保护。

与标准 KMS 密钥相比，外部密钥存储中的 KMS 密钥具有根本上不同的信任模型、责任共担安排和性能预期。使用外部密钥存储时，您要对密钥材料和加密操作的安全性和完整性负责。外部密钥存储中 KMS 密钥的可用性和延迟情况，受硬件、软件、网络组件以及 AWS KMS 与外部密钥管理器之间的距离的影响。您还可能会为外部密钥管理器以及外部密钥管理器与之通信所需的网络和负载平衡基础设施支付额外费用 AWS KMS

您可以将外部密钥存储作为更广泛的数据保护策略的一部分加以使用。对于您保护的每项 AWS 资源，您可以决定哪些资源需要在外部密钥存储中使用 KMS 密钥，哪些可以由标准 KMS 密钥保护。这可以让您灵活地为特定的数据分类、应用程序或项目选择 KMS 密钥。

外部密钥管理器

外部密钥管理器是 AWS 之外的组件，可以生成 256 位 AES 对称密钥并执行对称加密和解密。外部密钥存储的外部密钥管理器，可以是实体硬件安全模块（HSM）、虚拟 HSM 或带/不带 HSM 组件的软件密钥管理器。它可以位于外部的任何地方 AWS，包括您的本地、本地或远程数据中心或任何云中。您的外部密钥存储可以由单个外部密钥管理器提供支持，也可以由共享加密密钥的多个相关密钥管理器实例（例如 HSM 集群）提供支持。外部密钥存储旨在支持来自不同供应商的各种外部管理器。有关外部密钥管理器要求的详细信息，请参阅 规划外部密钥存储。

外部密钥

外部密钥存储中的每个 KMS 密钥都与外部密钥管理器中的加密密钥（称为外部密钥）相关联。在使用外部密钥存储中的 KMS 密钥加密或解密时，将使用外部密钥在外部密钥管理器中执行加密操作。

> **Warning**
>
> 外部密钥对 KMS 密钥的操作至关重要。如果外部密钥丢失或遭删除，则以相关 KMS 密钥加密的加密文字将无法恢复。

使用外部密钥存储时，外部密钥必须是已启用且可以执行加密和解密的 256 位 AES 密钥。有关详细的外部密钥要求，请参阅 外部密钥存储中 KMS 密钥的要求。

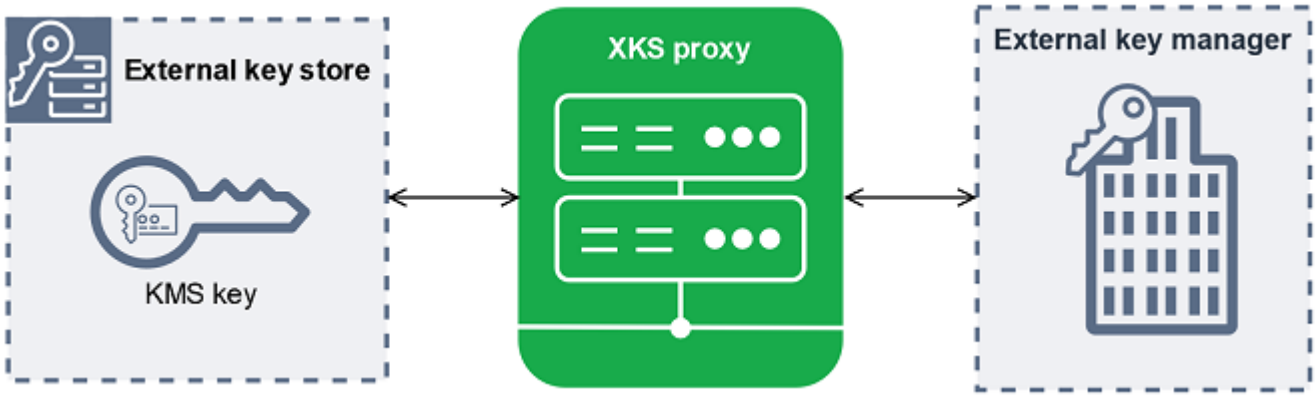
AWS KMS 无法创建、删除或管理任何外部密钥。您的加密密钥材料永远不会离开外部密钥管理器。在外部密钥存储中创建 KMS 密钥时，您需要提供外部密钥的 ID（`XksKeyId`）。您无法更改与 KMS 密钥关联的外部密钥 ID，即便外部密钥管理器可以轮换与外部密钥 ID 关联的密钥材料。

除了外部密钥，外部密钥存储中的 KMS 密钥还具有 AWS KMS 密钥材料。受 KMS 密钥保护的数据首先 AWS KMS 使用密 AWS KMS 钥材料进行加密，然后由您的外部密钥管理器使用您的外部密钥进行加密。这种双重加密过程可确保受您 KMS 密钥保护的加密文字始终至少与仅受 AWS KMS保护的加密文字一样强大。

许多加密密钥具有不同类型的标识符。在外部密钥存储中创建 KMS 密钥时，您要提供外部密钥存储代理用来引用外部密钥的外部密钥 ID。如果使用了错误的标识符，尝试在外部密钥存储中创建 KMS 密钥会失败。

外部密钥存储代理

外部密钥存储代理（“XKS 代理”）是客户拥有和客户管理的软件应用程序，用于调解与您的外部密钥管理器 AWS KMS 之间的所有通信。它还将通用 AWS KMS 请求转换为供应商特定的外部密钥管理器可以理解的格式。外部密钥存储需要外部密钥存储代理。每个外部密钥存储会关联一个外部密钥存储代理。



AWS KMS 无法创建、删除或管理任何外部密钥。您的加密密钥材料永远不会离开外部密钥管理器。AWS KMS 与您的外部密钥管理器之间的所有通信均由您的外部密钥存储代理进行中介。 AWS KMS 向外部密钥存储代理发送请求并接收来自外部密钥存储代理的响应。外部密钥存储代理负责将请求从您的外部密钥管理器传输 AWS KMS 到您的外部密钥管理器，并将来自外部密钥管理器的响应传回到 AWS KMS

您拥有并管理外部密钥存储的外部密钥存储代理，并负责其维护和操作。您可以根据开源外部密钥存储代理 API 规范开发外部密钥存储代理 API 规范，该规范 AWS KMS 发布或从供应商那里购买代理应用程序。您的外部密钥存储代理可能包含在您的外部密钥管理器中。为了支持代理开发， AWS KMS 还提供了外部密钥存储代理示例 (aws-kms-xks-proxy) 和测试客户端 (xks-kms-xksproxy-test-client)，用于验证您的外部密钥存储代理是否符合规范。

要进行身份验证 AWS KMS，代理使用服务器端 TLS 证书。要向您的代理进行身份验证， AWS KMS 请使用 Sigv4 代理身份验证凭据对外部密钥存储代理的所有请求进行签名。或者，您的代理可以启用双向 TLS (mTLS)，以进一步保证它只接受来自 AWS KMS的请求。

您的外部密钥存储代理必须支持 HTTP/1.1 或更高版本以及 TLS 1.2 或更高版本，并至少使用以下密码套件之一：

- TLS_AES_256_GCM_SHA384 (TLS 1.3)
- TLS_CHACHA20_POLY1305_SHA256 (TLS 1.3)

> **Note**
>
> AWS GovCloud (US) Region 不支持 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)

要在外部密钥存储中创建和使用 KMS 密钥，必须先将外部密钥存储连接到其外部密钥存储代理。您也可以根据需要断开外部密钥存储与其代理的连接。在这样做时，外部密钥存储中的所有 KMS 密钥都会变得不可用，也不能用于任何加密操作。

外部密钥存储代理连接

外部密钥存储代理连接（“XKS 代理连接”）描述了 AWS KMS 用于与外部密钥存储代理进行通信的方法。

您在创建外部密钥存储时指定代理连接选项，该选项将成为外部密钥存储的属性。您可以通过更新自定义密钥存储属性来更改代理连接选项，但必须确定外部密钥存储代理仍然可以访问相同的外部密钥。

AWS KMS 支持以下连接选项：

- 公共终端节点连接-通过 Internet 将外部密钥存储代理的请求 AWS KMS 发送到您控制的公共终端节点。此选项易于创建和维护，但可能无法满足每次安装的安全要求。
- VPC 终端节点服务连接 — AWS KMS 向您创建和维护的亚马逊虚拟私有云（亚马逊 VPC）终端节点服务发送请求。您可以在 Amazon VPC 内托管外部密钥存储代理，也可以将外部密钥存储代理托管在 Amazon VPC 之外 AWS 并仅用于通信。

有关外部密钥存储代理连接选项的详细信息，请参阅 选择代理连接选项。

外部密钥存储代理身份验证凭证

要向外部密钥存储代理进行身份验证， AWS KMS 请使用签名 V4 (Sigv4) 身份验证凭据对外部密钥存储代理的所有请求进行签名。您在代理上建立并维护身份验证凭据，然后在创建外部存储 AWS KMS 时提供此凭据。

> **Note**
>
> AWS KMS 用于签署 XKS 代理请求的 Sigv4 凭据与您的中的委托人关联的任何 Sigv4 凭据无关。 AWS Identity and Access Management AWS 账户不要将任何 IAM SigV4 凭证重复用于外部密钥存储代理。

每个代理身份验证凭证有两个部分。在创建外部密钥存储或更新外部密钥存储的身份验证凭证时，必须提供这两部分。

- 访问密钥 ID：标识秘密访问密钥。您能以明文形式提供此 ID。
- 秘密访问密钥：凭证的秘密部分。 AWS KMS 在存储凭据之前对凭据中的私有访问密钥进行加密。

您随时可以编辑凭证设置，例如输入了错误值时、在代理上更改凭证时或者代理轮换证书时。有关对外部密钥存储代理 AWS KMS 进行身份验证的技术细节，请参阅《 AWS KMS 外部密钥存储代理 API 规范》中的身份验证。

为了允许您在不中断外部密钥存储中使用 KMS 密钥的凭证的情况下轮换凭证，我们建议外部密钥存储代理至少支持两个有效的身份验证凭据。 AWS 服务 AWS KMS这样可以确保在您向 AWS KMS提供新凭证时，以前的凭证继续有效。

为了帮助您跟踪代理身份验证凭证的使用年限， AWS KMS 定义了 Amazon CloudWatch 指标。XksProxyCredentialAge您可以使用此指标创建 CloudWatch 警报，当您的凭证期限达到您设定的阈值时，该警报会通知您。

为了进一步确保您的外部密钥存储代理仅响应 AWS KMS，一些外部密钥代理支持相互传输层安全性协议（mTLS）。有关更多信息，请参阅 mTLS 身份验证（可选）。

代理 API

要支持 AWS KMS 外部密钥存储，外部密钥存储代理必须实现所需的代理 API，如AWS KMS 外部密钥存储代理 API 规范中所述。这些代理 API 请求是 AWS KMS 发送到代理的唯一请求。即便您从不直接发送这些请求，了解这些请求也可能有助于您修复外部密钥存储或其代理可能出现的任何问题。例如，在其外部密钥存储的 Amazon CloudWatch 指标中 AWS KMS 包含有关这些 API 调用的延迟和成功率的信息。有关更多信息，请参阅 监控外部密钥存储。

下表列出并描述了每个代理 API。它还包括触发对 AWS KMS 代理 API 的调用的 AWS KMS 操作以及与代理 API 相关的任何操作异常。

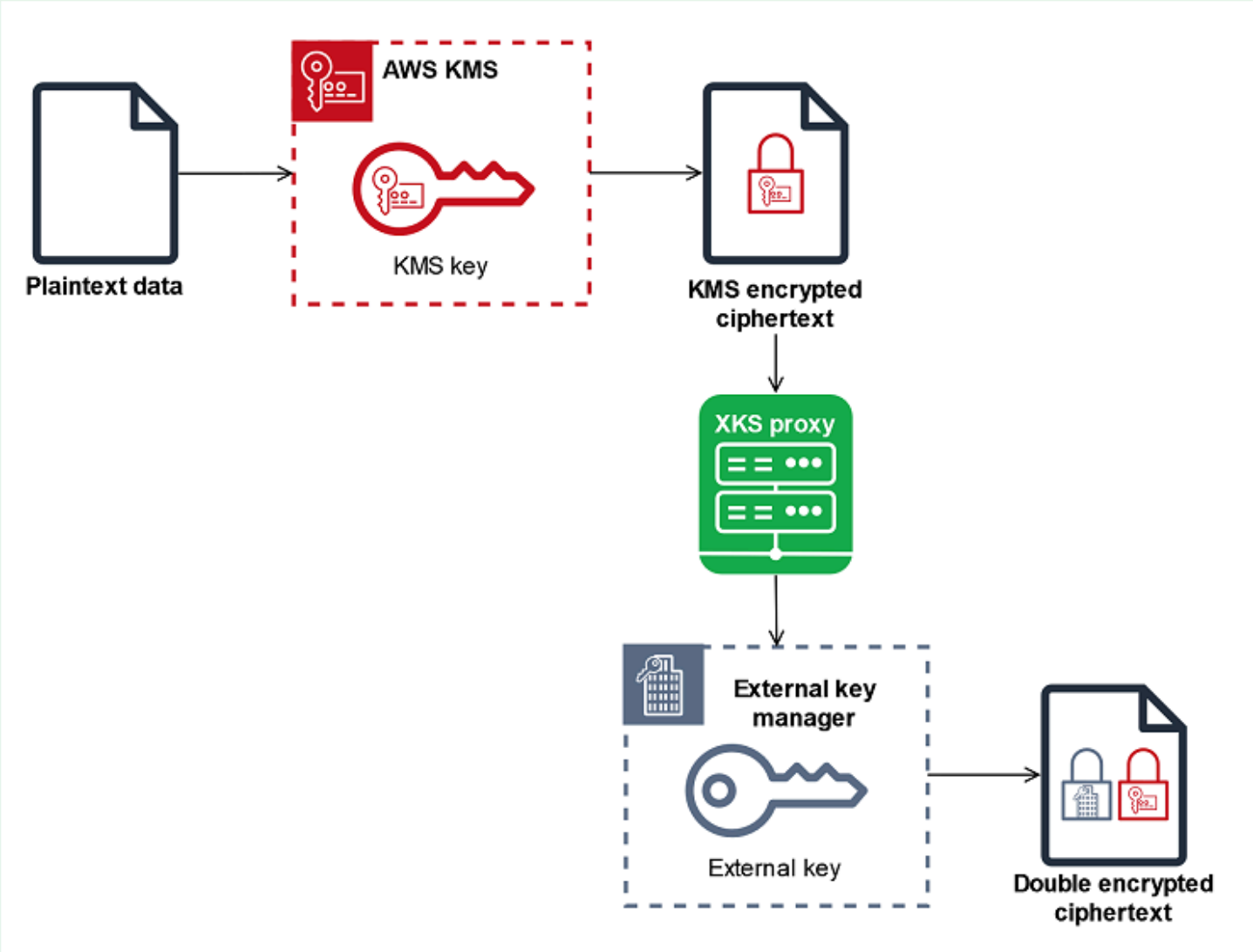
代理 API	描述	相关 AWS KMS 操作
Decrypt	AWS KMS 发送要解密的密文以及要使用的外部密钥的 ID。所需的加密算法为 AES_GCM。	解密，ReEncrypt
Encrypt	AWS KMS 发送要加密的数据以及要使用的外部密钥的 ID。所需的加密算法为 AES_GCM。	加密、GenerateDataKey、GenerateDataKeyWithoutPlaintext、ReEncrypt
GetHealthStatus	AWS KMS 请求有关代理和您的外部密钥管理器状态的信息。 每个外部密钥管理器的状态可以是以下状态之一。 • `Active`：正常，可以传输流量 • `Degraded`：不正常，但可以传输流量 • `Unavailable`：不正常，不可以传输流量	CreateCustomKeyStore（用于公共终端节点连接）、ConnectCustomKeyStore（用于 VPC 终端节点服务连接） 如果所有外部密钥管理器实例都处于 `Unavailable` 状态，则尝试创建或连接密钥存储将失败并显示 `XksProxyUriUnreachableException`。

代理 API	描述	相关 AWS KMS 操作
GetKeyMetadata	AWS KMS 请求有关与您的外部密钥存储库中的 KMS 密钥关联的外部密钥的信息。 响应内容包含密钥规范（AES_256）、密钥用法（[ENCRYPT, DECRYPT] ），以及外部密钥处于 ENABLED 还是 DISABLED 状态。	CreateKey 如果密钥规范不是 AES_256，或者密钥用法不是 [ENCRYPT, DECRYPT]，或者状态为 DISABLED，则 CreateKey 操作将失败并显示 XksKeyInvalidConfigurationException 。

双重加密

由外部密钥存储中的 KMS 密钥加密的数据经过两次加密。首先， AWS KMS 使用特定于 KMS AWS KMS 密钥的密钥材料对数据进行加密。然后，外部密钥管理器使用外部密钥加密经过 AWS KMS加密的加密文字。此过程称为双重加密。

双重加密可确保外部密钥存储中经 KMS 密钥加密的数据至少与经标准 KMS 密钥加密的加密文字一样强大。它还可以保护您从外部密钥存储代理传输 AWS KMS 的纯文本。您可以借助双重加密保留对加密文字的完全控制。如果您通过外部代理永久撤消 AWS 对外部密钥的访问权限， AWS 中剩余的任何加密文字都会受到有效的加密粉碎处理。



要启用双重加密，外部密钥存储中的每个 KMS 密钥都有两个加密备用密钥：

- KMS AWS KMS 密钥独有的密钥材料。此密钥材料是生成的，仅用于 AWS KMS FIPS 140-2 安全等级 3 认证的硬件安全模块 (HSM)。
- 外部密钥管理器中的外部密钥。

双重加密具有以下效果：

- AWS KMS 如果不通过外部密钥存储代理访问您的外部密钥，则无法解密外部密钥存储库中由 KMS 密钥加密的任何密文。
- 即使您有外部密钥材料，也无法解密外部密钥存储库中由 KMS 密钥加密的任何密文。 AWS

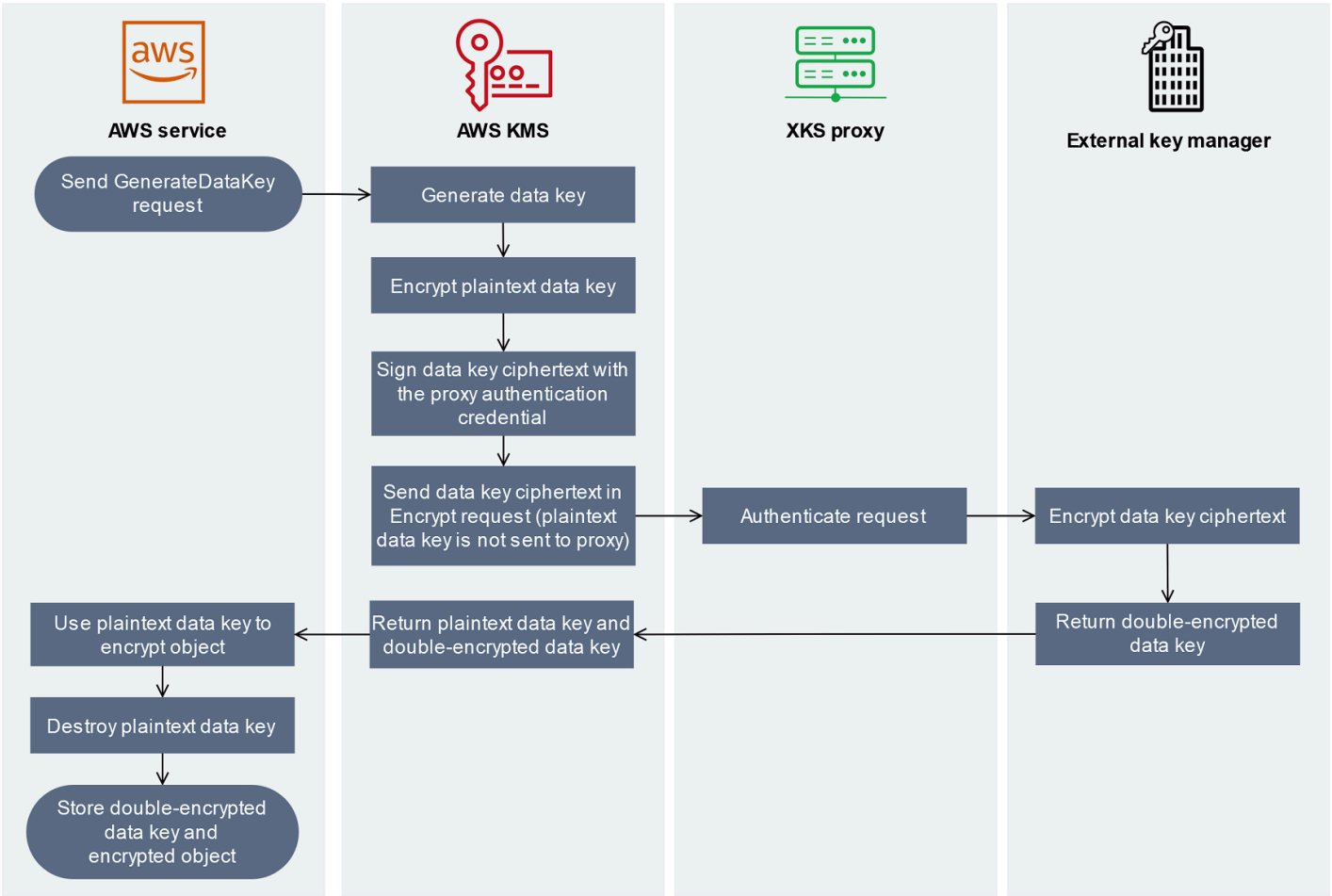
- 即使您拥有外部密钥材料，也无法重新创建已从外部密钥存储中删除的 KMS 密钥。每个 KMS 密钥都有包含在对称加密文字中的唯一元数据。新的 KMS 密钥将无法解密由原始密钥加密的加密文字，即使其使用相同的外部密钥材料也是如此。

有关实际应用中的双重加密示例，请参见 外部密钥存储的工作原理。

外部密钥存储的工作原理

您的外部密钥存储、外部密钥存储代理和外部密钥管理器会协同保护您的 AWS 资源。以下过程描述了典型 AWS 服务 的加密工作流程，即使用由 KMS 密钥保护的唯一数据密钥对每个对象进行加密。在本例中，您选择了外部密钥存储中的 KMS 密钥来保护对象。该示例说明了如何 AWS KMS 使用双重加密来保护传输中的数据密钥，并确保外部密钥存储库中的 KMS 密钥生成的密文始终至少与由标准对称 KMS 密钥加密并包含密钥材料的密文一样强大。 AWS KMS

与之集成的每个实际 AWS 服务 使用的加密方法各 AWS KMS 不相同。有关详细信息，请参阅 AWS 服务 文档“安全”章节中的“数据保护”主题。



1. 您向 AWS 服务 资源中添加了一个新对象。要加密对象，请 AWS KMS 使用外部密钥存储库中的 KMS 密钥 AWS 服务 向发送GenerateDataKey请求。
2. AWS KMS 生成 256 位对称数据密钥，并准备通过外部密钥存储代理将纯文本数据密钥的副本发送到外部密钥管理器。 AWS KMS 使用与外部密钥存储库中的 KMS 密钥关联的密钥材料对纯文本数据AWS KMS 密钥进行加密，从而开始双重加密过程。
3. AWS KMS 向与外部密钥存储关联的外部密钥存储代理发送加密请求。该请求包括要加密的数据密钥密文以及与 KMS 密钥关联的外部密钥的 ID。 AWS KMS 使用外部密钥存储代理的代理身份验证凭据对请求进行签名。

   数据密钥的明文副本不会发送到外部密钥存储代理。
4. 外部密钥存储代理对请求进行身份验证，然后将加密请求传递给您的外部密钥管理器。

   一些外部密钥存储代理还实现了可选的授权策略，该策略仅允许选定的主体在特定条件下执行操作。
5. 您的外部密钥管理器使用指定的外部密钥对数据密钥加密文字进行加密。外部密钥管理器将经过双重加密的数据密钥返回给外部密钥存储代理，后者再将其返回给 AWS KMS。
6. AWS KMS 将纯文本数据密钥和该数据密钥的双重加密副本返回到。 AWS 服务
7. AWS 服务 使用纯文本数据密钥对资源对象进行加密，销毁纯文本数据密钥，并将加密的数据密钥与加密对象一起存储。

   有些人 AWS 服务 可能会缓存纯文本数据密钥以用于多个对象，或者在使用资源时重复使用。有关更多信息，请参阅 不可用的 KMS 密钥如何影响数据密钥。

要解密加密对象， AWS 服务 必须在 Decrypt 请求 AWS KMS 中将加密的数据密钥发回给。要解密加密的数据密钥， AWS KMS 必须使用外部密钥的 ID 将加密的数据密钥发送回您的外部密钥存储代理服务器。如果对外部密钥存储代理的解密请求因任何原因失败，则 AWS KMS 无法解密加密的数据密钥， AWS 服务 也无法解密加密对象。

控制对外部密钥存储的访问

与标准 KMS 密钥一起使用的所有 AWS KMS 访问控制功能（密钥策略、IAM policy 和授权）的工作方式，与外部密钥存储中的 KMS 密钥的工作方式相同。您可以使用 IAM policy 来控制对创建和管理外部密钥存储的 API 操作的访问。您可以使用 IAM policy 和密钥策略来控制对外部密钥存储中 AWS KMS keys 的访问。您还可以使用 AWS 组织的服务控制策略和 VPC 端点策略来控制对外部密钥存储中 KMS 密钥的访问。

我们建议您仅向用户和角色提供他们可能执行的任务所需的权限。

主题

授权外部密钥存储管理器

创建和管理外部密钥存储的主体需要自定义密钥存储操作的权限。以下列表描述了外部密钥存储管理器所需的最低权限。由于自定义密钥存储不是 AWS 资源，因此您无法为其他 AWS 账户 中外部密钥存储的主体提供权限。

- `kms:CreateCustomKeyStore`
- `kms:DescribeCustomKeyStores`
- `kms:ConnectCustomKeyStore`
- `kms:DisconnectCustomKeyStore`
- `kms:UpdateCustomKeyStore`
- `kms:DeleteCustomKeyStore`

创建外部密钥存储的主体需要权限来创建和配置外部密钥存储组件。主体只能在自己的账户中创建外部密钥存储。要创建具有 VPC 端点服务连接的外部密钥存储，主体必须具有创建以下组件的权限：

- Amazon VPC
- 公有子网和私有子网
- 网络负载均衡器和目标组
- Amazon VPC 端点服务

有关详细信息，请参阅 Amazon VPC 的身份和访问管理、VPC 端点和 VPC 端点服务的身份和访问管理以及 Elastic Load Balancing API 权限。

授权外部密钥存储中 KMS 密钥的用户

在您外部密钥存储中创建和管理 AWS KMS keys 的主体需要具有与在 AWS KMS 中创建和管理任何 KMS 密钥的人员相同的权限。外部密钥存储中的 KMS 密钥的默认密钥策略与 AWS KMS 中 KMS 密

钥的默认密钥策略相同。基于属性的访问权限控制（ABAC）使用标签和别名来控制对 KMS 密钥的访问，对外部密钥存储中的 KMS 密钥也有效。

使用自定义密钥存储中的 KMS 密钥进行加密操作的委托人需要使用 KMS 密钥执行加密操作的权限，如 kms:Decrypt。您可以在 IAM 或密钥策略中提供这些权限。但是，他们无需任何额外权限即可在自定义密钥存储中使用 KMS 密钥。

要设置仅适用于外部密钥存储中 KMS 密钥的权限，请使用值为 EXTERNAL_KEY_STORE 的 kms:KeyOrigin 策略条件。您可以使用此条件来限制 kms: CreateKey 权限或任何特定于 KMS 密钥资源的权限。例如，以下 IAM policy 允许其所连接的身份对账户中的所有 KMS 密钥调用指定操作，只要这些 KMS 密钥位于外部密钥存储中。请注意，您可以限制对外部密钥存储中的 KMS 密钥和 AWS 账户 中的 KMS 密钥的权限，但不能限制到账户中任何特定的外部密钥存储。

```
{
  "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"
    }
  }
}
```

授权 AWS KMS 与外部密钥存储代理通信

AWS KMS 仅通过您提供的外部密钥存储代理与外部密钥管理器通信。AWS KMS 使用签名版本 4（SigV4）流程和您指定的外部密钥存储代理身份验证凭证对请求进行签名，从而对代理进行身份验证。如果您使用公有端点连接作为外部密钥存储代理，则 AWS KMS 不需要任何其他权限。

不过，如果使用的是 VPC 端点服务连接，您必须授予 AWS KMS 权限来创建到 Amazon VPC 端点服务的接口端点。无论外部密钥存储代理位于您的 VPC 中还是其他地方，都需要此权限，但使用 VPC 端点服务与 AWS KMS 通信不需要。

AWS KMS要允许创建接口终端节点，请使用 Amazon VPC 控制台或ModifyVpcEndpointServicePermissions操作。允许以下主体的权限：cks.kms.*<region>*.amazonaws.com。

例如，以下 AWS CLI 命令允许 AWS KMS 连接到美国西部（俄勒冈州）（us-west-2）区域中的指定 VPC 端点服务。在使用此命令之前，请将 Amazon VPC 服务 ID 和 AWS 区域 替换为配置的有效值。

```
modify-vpc-endpoint-service-permissions
--service-id vpce-svc-12abc34567def0987
--add-allowed-principals '["cks.kms.us-west-2.amazonaws.com"]'
```

要移除此权限，请使用 Amazon VPC 控制台或ModifyVpcEndpointServicePermissions带RemoveAllowedPrincipals参数的。

外部密钥存储代理授权（可选）

一些外部密钥存储代理针对其外部密钥的使用执行授权要求。允许但不要求使用外部密钥存储代理来设计和实现授权方案，该方案允许特定用户仅在特定条件下请求特定操作。例如，可以将代理配置为允许用户 A 使用特定的外部密钥进行加密，但不允许使用该外部密钥进行解密。

代理授权独立于 AWS KMS 对所有外部密钥存储代理要求的基于 SigV4 的代理身份验证。其还独立于授权访问影响外部密钥存储或其 KMS 密钥的操作的密钥策略、IAM policy 和授权。

要按外部密钥存储代理启用授权，AWS KMS 会在每个代理 API 请求中包含元数据，包括调用者、KMS 密钥、AWS KMS 操作和 AWS 服务（如果有）。外部密钥代理 API 版本 1（v1）的请求元数据如下所示。

```
"requestMetadata": {
    "awsPrincipalArn": string,
    "awsSourceVpc": string, // optional
    "awsSourceVpce": string, // optional
    "kmsKeyArn": string,
    "kmsOperation": string,
    "kmsRequestId": string,
    "kmsViaService": string // optional
}
```

例如，仅当请求由特定 AWS 服务（kmsViaService）代表主体发出时，您可以将代理配置为允许来自特定主体（awsPrincipalArn）的请求。

如果代理授权失败，相关 AWS KMS 操作也将失败，并显示一条解释错误的消息。有关详细信息，请参阅 代理授权问题。

mTLS 身份验证（可选）

要让外部密钥存储代理对来自 AWS KMS 的请求进行身份验证，AWS KMS 会使用外部密钥存储的签名版本 4（SigV4）代理身份验证凭证对所有发送到外部密钥存储代理的请求进行签名。

为了进一步确保您的外部密钥存储代理仅响应 AWS KMS 请求，一些外部密钥代理支持相互传输层安全性协议（mTLS），即交易双方使用证书相互进行身份验证。mTLS 在标准 TLS 提供的服务器端身份验证中添加了客户端身份验证（外部密钥存储代理服务器对 AWS KMS 客户端进行身份验证）。在极少数情况下，代理身份验证凭证会遭到泄露，mTLS 会阻止第三方成功向外部密钥存储代理发出 API 请求。

要实现 mTLS，请将您的外部密钥存储代理配置为仅接受具有以下属性的客户端 TLS 证书：

- TLS 证书上的主题通用名称必须是 `cks.kms.<Region>.amazonaws.com`，例如 `cks.kms.eu-west-3.amazonaws.com`。
- 证书必须链接到与 Amazon Trust Services 关联的证书颁发机构。

规划外部密钥存储

在创建外部密钥存储之前，选择连接选项以确定 AWS KMS 与外部密钥存储的通信方式。您选择的连接选项决定了规划过程的剩余步骤。

了解更多：

- 查看创建外部密钥存储的过程，包括汇编先决条件。这将帮助您确保在创建外部密钥存储时拥有所需的所有组件。
- 了解如何控制对外部密钥存储的访问，包括外部密钥存储管理员和用户所需的权限。
- 了解AWS KMS记录外部密钥存储的 Amazon CloudWatch 指标和维度。我们强烈建议您创建警报来监控外部密钥存储，以便您就可以检测出性能和操作问题的早期迹象。

选择代理连接选项

如果您要创建外部密钥存储，则需要确定 AWS KMS 与外部密钥存储代理的通信方式。此选择将决定您需要的组件以及组件的配置方式。AWS KMS 支持以下连接选项。选择能满足性能和安全目标的选项。

在开始之前，请确认您需要外部密钥存储。大多数客户可以使用由 AWS KMS 密钥材料支持的 KMS 密钥。

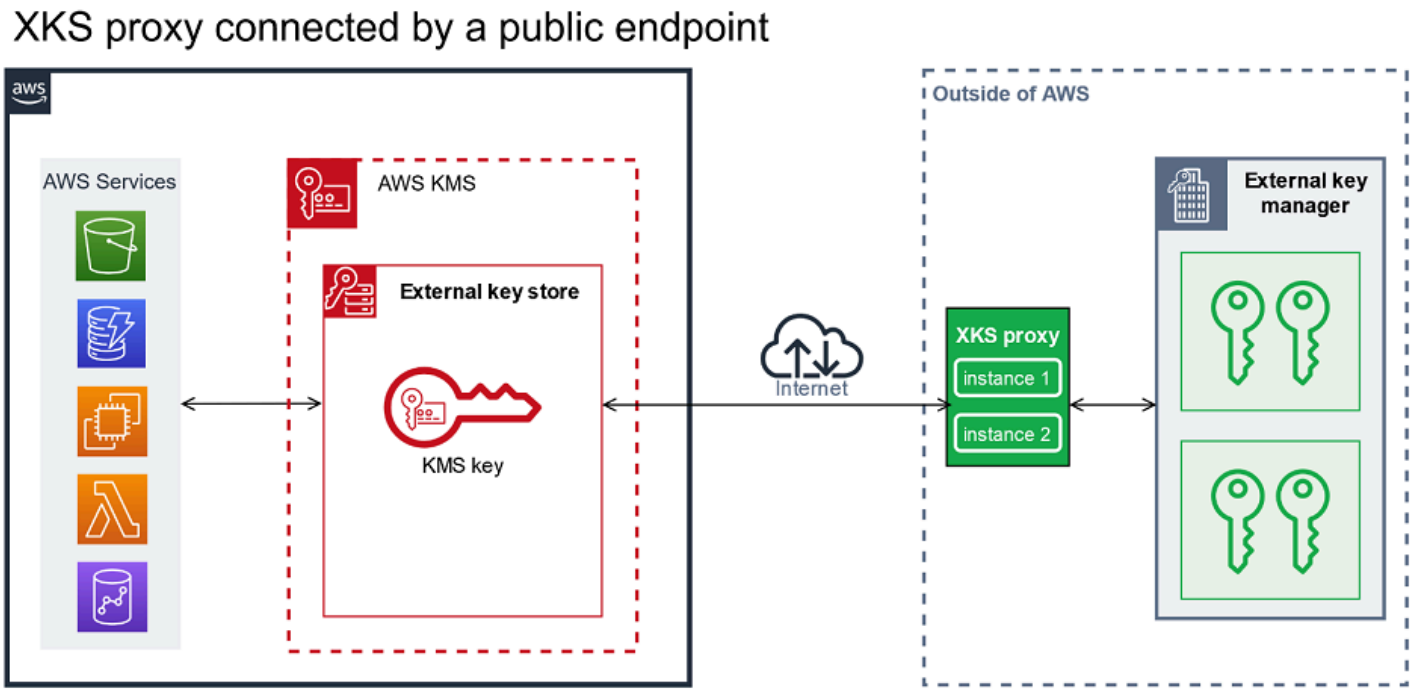
> **Note**
>
> 如果您的外部密钥存储代理构建到外部密钥管理器中，则您的连接可能是预先确定的。有关详细信息，请参阅外部密钥管理器或外部密钥存储代理的文档。

即使在正在运行的外部密钥存储上，您也可以更改外部密钥存储代理的连接选项。但是，必须仔细规划和执行该过程，以尽可能减少中断和避免错误，并确保继续访问加密数据的加密密钥。

公有端点连接

AWS KMS 使用公有端点通过 Internet 连接到外部密钥存储代理（XKS 代理）。

此连接选项更易于设置和维护，并且可以与某些密钥管理模型很好地匹配。但是，此选项可能无法满足某些组织的安全要求。



要求

如果您选择公有端点连接，则需要满足以下条件。

- 您的外部密钥存储代理必须可以在可公开路由的端点上访问。

- 您可以将同一个公有端点用于多个外部密钥存储，前提是这些外部密钥存储使用不同的代理 URI 路径值。
- 您不能在同一 AWS 区域 中将同一端点用于具有公有端点连接的外部密钥存储和任何具有 VPC 端点服务连接的外部密钥存储，即使密钥存储位于不同的 AWS 账户 中也是如此。
- 您必须获得由外部密钥存储支持的公有证书颁发机构颁发的 TLS 证书。有关列表，请参阅 Trusted Certificate Authorities（受信任的证书颁发机构）。

  TLS 证书上的主题公用名（CN）必须与外部密钥存储代理的代理 URI 端点中的域名相匹配。例如，如果公有端点是 `https://myproxy.xks.example.com`，即 TLS，则 TLS 证书上的 CN 必须为 `myproxy.xks.example.com` 或 `*.xks.example.com`。
- 确保 AWS KMS 与外部密钥存储代理之间的任何防火墙都允许流入和流出代理上的端口 443。AWS KMS 在端口 443 上通信。此值不可配置。

有关外部密钥存储的所有要求，请参阅 Assemble the prerequisites（汇编先决条件）。

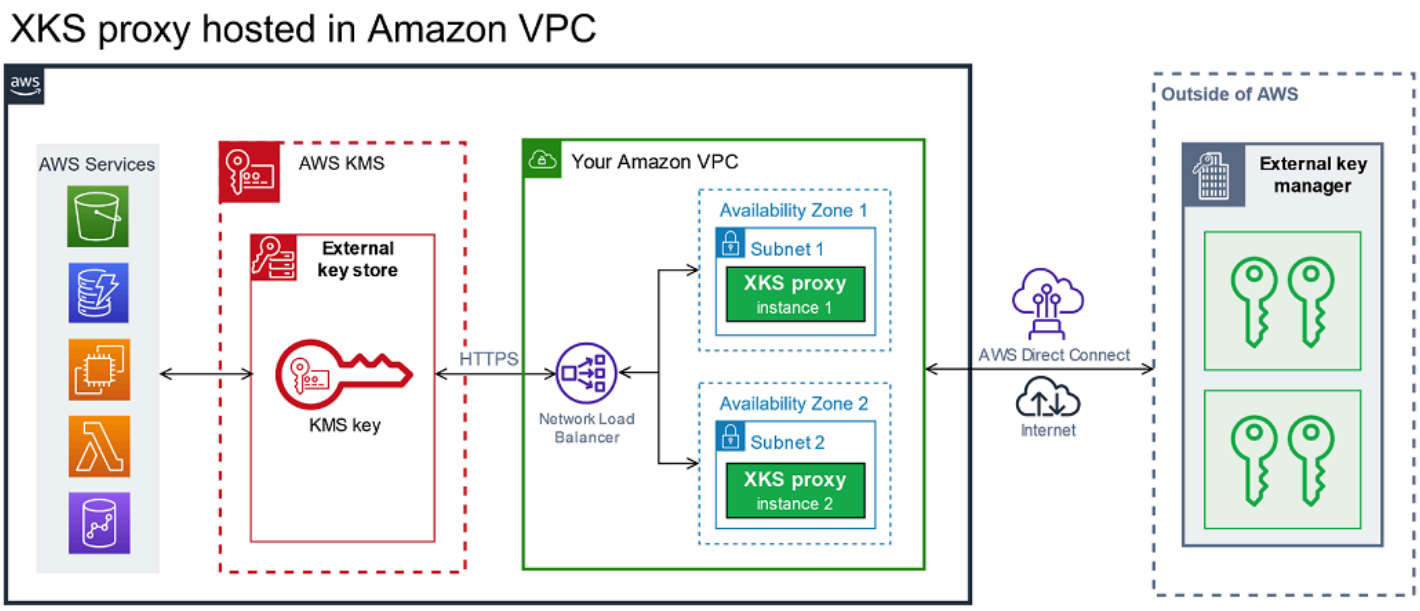
VPC 端点服务连接

AWS KMS 通过创建指向您创建和配置的 Amazon VPC 端点服务的接口端点，来连接到外部密钥存储代理（XKS 代理）。您负责创建 VPC 端点服务并将您的 VPC 连接到外部密钥管理器。

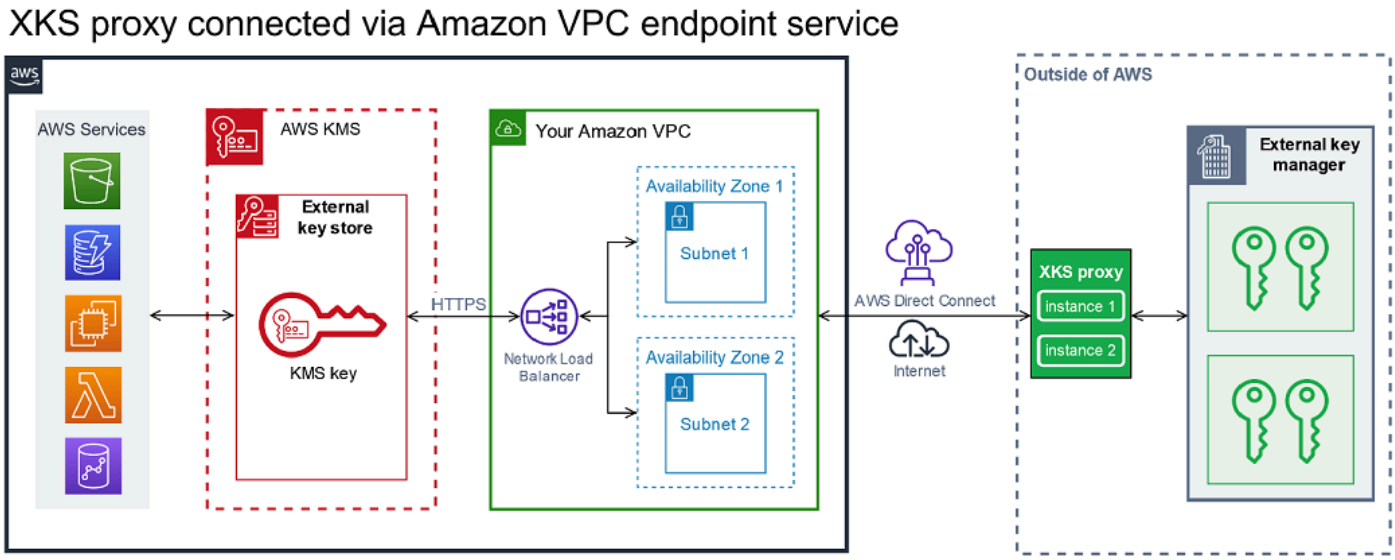
您的端点服务可以使用任何支持的网络到 Amazon VPC 选项进行通信，包括 AWS Direct Connect。

此连接选项的设置和维护更为复杂。但是此连接选项使用了 AWS PrivateLink，以便 AWS KMS 可以在不使用公有 Internet 的情况下私密地连接到 Amazon VPC 和外部密钥存储代理。

您可以在您的 Amazon VPC 中找到外部密钥存储代理。



或者，在 AWS 外部找到您的外部密钥存储代理，并仅将 Amazon VPC 端点服务用于与 AWS KMS 进行安全通信。



配置 VPC 端点服务连接

请遵循本节中提供的指导创建和配置使用 VPC 端点服务连接的外部密钥存储所需的 AWS 资源和相关组件。此连接选项列出的资源是对所有外部密钥存储所需资源的补充。创建和配置所需资源后，您可以创建外部密钥存储。

您可以在 Amazon VPC 中找到外部密钥存储代理，也可以在 AWS 外部找到代理，并使用 VPC 端点服务进行通信。

在开始之前，请确认您需要外部密钥存储。大多数客户可以使用由 AWS KMS 密钥材料支持的 KMS 密钥。

> **Note**
>
> VPC 端点服务连接所需的某些元素可能包含在您的外部密钥管理器中。此外，您的软件可能有其他配置要求。在创建和配置本节中的 AWS 资源之前，请参阅您的代理和密钥管理器文档。

主题

- VPC 端点服务连接的要求
- 创建 Amazon VPC 和子网
- 创建目标组
- 创建网络负载均衡器
- 创建 VPC 端点服务
- 验证私有 DNS 名称域
- 授权 AWS KMS 连接到 VPC 端点服务

VPC 端点服务连接的要求

如果您为外部密钥存储选择 VPC 端点服务连接，则需要以下资源。

为了最大限度地减少网络延迟，请在离外部密钥管理器最近的受支持的 AWS 区域 中创建 AWS 组件。如果可行，请选择网络往返时间（RTT）不超过 35 毫秒的区域。

- 连接到外部密钥管理器的 Amazon VPC。它必须在两个不同的可用区中至少拥有两个私有子网。

  您可以将现有 Amazon VPC 用于外部密钥存储，前提是此 VPC 符合与外部密钥存储一起使用的要求。多个外部密钥存储可以共享一个 Amazon VPC，但每个外部密钥存储必须有自己的 VPC 端点服务和私有 DNS 名称。
- 由 AWS PrivateLink 提供支持的 Amazon VPC 端点服务具有网络负载均衡器和目标组。

  端点服务不能要求接受。此外，您必须将 AWS KMS 添加为允许的主体。这允许 AWS KMS 创建接口端点，以便其可以与您的外部密钥存储代理进行通信。
- VPC 端点服务在其 AWS 区域 中的唯一私有 DNS 名称。

私有 DNS 名称必须是更高级别的公有域的子域。例如，如果私有 DNS 名称为 myproxy-private.xks.example.com，则其必须是公有域（例如 xks.example.com 或 example.com）的子域。

您必须针对私有 DNS 名称的 DNS 域验证所有权。

- 由受支持的公有证书颁发机构为您的外部密钥存储代理颁发的 TLS 证书。

  TLS 证书上的主题通用名称（CN）必须与私有 DNS 名称相匹配。例如，若私有 DNS 名称为 myproxy-private.xks.example.com，则 TLS 证书上的 CN 必须为 myproxy-private.xks.example.com 或 *.xks.example.com。

有关外部密钥存储的所有要求，请参阅 Assemble the prerequisites（汇编先决条件）。

创建 Amazon VPC 和子网

VPC 端点服务连接需要连接到外部密钥管理器的 Amazon VPC，该管理器至少拥有两个私有子网。您可以创建 Amazon VPC 或使用满足外部密钥存储要求的现有 Amazon VPC。有关创建新 VPC 的帮助，请参阅《Amazon Virtual Private Cloud 用户指南》中的创建 VPC。

Amazon VPC 的要求

若要使用 VPC 端点服务连接外部密钥存储，Amazon VPC 必须具有以下属性：

- 必须与您的外部密钥存储位于相同 AWS 账户 和受支持的区域中。
- 需要至少两个私有子网，每个子网均位于不同的可用区内。
- Amazon VPC 的私有 IP 地址范围不得与托管外部密钥管理器的数据中心的私有 IP 地址范围重叠。
- 所有组件都必须使用 IPv4。

您可以通过多种方式将 Amazon VPC 连接到外部密钥存储代理。选择能满足性能和安全需求的选项。有关列表，请参阅将 VPC 连接到其他网络和 Network-to-Amazon VPC connectivity options（网络到 Amazon VPC 连接选项）。有关详细信息，请参阅 AWS Direct Connect 和《AWS Site-to-Site VPN 用户指南》https://docs.aws.amazon.com/vpn/latest/s2svpn/。

为外部密钥存储创建 Amazon VPC

使用下面的说明为外部密钥存储创建 Amazon VPC。仅当您选择 VPC 端点服务连接选项时，才需要 Amazon VPC。您可以使用满足外部密钥存储要求的现有 Amazon VPC。

按照创建 VPC、子网和其他 VPC 资源主题中的说明使用以下必需值。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
IPv4 CIDR 块	输入 VPC 的 IP 地址。Amazon VPC 的私有 IP 地址范围不得与托管外部密钥管理器的数据中心的私有 IP 地址范围重叠。
可用区（AZ）的数量	2 或更多
公有子网的数量	不需要任何内容（0）
私有子网的数量	每个 AZ 一个
NAT 网关	不需要任何内容。
VPC 端点	不需要任何内容。
启用 DNS 主机名	有
启用 DNS 解析	有

请务必测试您的 VPC 通信。例如，如果您的外部密钥存储代理不在 Amazon VPC 中，请在 Amazon VPC 中创建 Amazon EC2 实例，验证 Amazon VPC 是否可以与外部密钥存储代理通信。

将 VPC 连接到外部密钥管理器

使用 Amazon VPC 支持的任何网络连接选项将 VPC 连接到托管外部密钥管理器的数据中心。确保 VPC（或外部密钥存储代理，如果在 VPC 中）中的 Amazon EC2 实例可以与数据中心和外部密钥管理器通信。

创建目标组

在创建所需的 VPC 端点服务之前，创建其必需的组件、网络负载均衡器（NLB）和目标组。网络负载均衡器（NLB）在多个运行状况良好的目标之间分配请求，其中任何一个目标都可以为请求提供服务。在此步骤中，您将为外部密钥存储代理创建至少具有两台主机的目标组，并将您的 IP 地址注册到目标组。

使用以下必填值，按照配置目标组主题中的说明使用以下必需值。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
Target type	IP 地址
协议	TCP
端口	443
IP 地址类型	IPv4
VPC	选择 VPC，您将在其中为外部密钥存储创建 VPC 端点服务。
运行状况检查协议和路径	运行状况检查协议和路径将与外部密钥存储代理配置不同。请参阅外部密钥管理器或外部密钥存储代理的文档。 若要为您的目标组配置运行状况检查，请参阅《网络负载均衡器的弹性负载均衡用户指南》中的目标组的运行状况检查。
网络	其他私有 IP 地址
IPv4 地址	外部密钥存储代理的私有地址
端口	443

创建网络负载均衡器

网络负载均衡器将网络流量（包括从 AWS KMS 到外部密钥存储代理的请求）分配到配置的目标。

按照配置负载均衡器和侦听器主题中的说明配置和添加侦听器，并使用以下必需值创建负载均衡器。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
Scheme	Internal
IP 地址类型	IPv4
网络映射	选择 VPC，您将在其中为外部密钥存储创建 VPC 端点服务。

Field	Value
Mapping	选择您为 VPC 子网配置的两个可用区（至少两个）。验证子网名称和私有 IP 地址。
协议	TCP
端口	443
默认操作：转发至	选择网络负载均衡器的目标组。

创建 VPC 端点服务

通常，您创建到服务的端点。但是，创建 VPC 端点服务时，您就是提供商，AWS KMS 会创建指向您服务的端点。对于外部密钥存储，使用您在上一个步骤中创建的网络负载均衡器创建 VPC 端点服务。该 VPC 端点服务必须与外部密钥存储位于相同的 AWS 账户 和受支持的区域中。

多个外部密钥存储可以共享一个 Amazon VPC，但每个外部密钥存储必须有自己的 VPC 端点服务和私有 DNS 名称。

按照创建端点服务主题中的说明创建具有以下必需值的 VPC 端点服务。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
负载均衡器类型	网络
可用的负载均衡器	选择您在之前的步骤中创建的网络负载均衡器。 如果新的负载均衡器未出现在列表中，请验证其状态是否为活动。负载均衡器状态可能需要几分钟才能从预置中变为活动。
需要接受	False。取消选中复选框。 不需要接受。未经手动接受，AWS KMS 无法连接到 VPC 端点服务。如果需要接受，则创建外部密钥存储的尝试会失败，并出现 `XksProxyInvalidConfigurationException` 异常。

Field	Value
启用私有 DNS 名称	将私有 DNS 名称与服务关联
私有 DNS 名称	输入在其 AWS 区域 中唯一的私有 DNS 名称。 私有 DNS 名称必须是更高级别的公有域的子域。例如，如果私有 DNS 名称为 myproxy-private.xks.example.com ，则其必须是公有域（例如 xks.example.com 或 example.com ）的子域。 此私有 DNS 名称必须与在外部密钥存储代理上配置的 TLS 证书中的主题公用名（CN）相匹配。例如，若私有 DNS 名称为 myproxy-private.xks.example.com ，则 TLS 证书上的 CN 必须为 myproxy-private.xks.example.com 或 *.xks.example.com 。 如果证书和私有 DNS 名称不匹配，则将外部密钥存储连接到其外部密钥存储代理的尝试会失败，连接错误代码为 XKS_PROXY_INVALID_TLS_CONFIGURATION 。有关更多信息，请参阅 常规配置错误。
支持的 IP 地址类型	IPv4

验证私有 DNS 名称域

创建 VPC 端点服务时，其域验证状态为 pendingVerification。使用 VPC 端点服务创建外部密钥存储之前，此状态必须为 verified。若要验证您是否拥有与私有 DNS 名称关联的域，您必须在公有 DNS 服务器中创建 TXT 记录。

例如，如果 VPC 端点服务的私有 DNS 名称为 myproxy-private.xks.example.com，则必须在公有域中创建 TXT 记录，例如 xks.example.com 或 example.com，以公有域为准。AWS PrivateLink 先在 xks.example.com 上查找 TXT 记录，然后再在 example.com 上查找。

> **Tip**
>
> 添加 TXT 记录后，Domain verification status（域验证状态）值可能需要几分钟才能从 pendingVerification 变为 verify。

首先，使用以下任一方法找到域的验证状态。有效值包括 `verified`、`pendingVerification` 和 `failed`。

- 在 Amazon VPC 控制台中，选择 Endpoint services（端点服务），然后选择您的端点服务。在详细信息窗格中，查看 Domain verification status（域验证状态）。
- 使用该DescribeVpcEndpointServiceConfigurations操作。`State` 值在 `ServiceConfigurations.PrivateDnsNameConfiguration.State` 字段中。

如果验证状态不是 `verified`，请按照 Domain ownership verification（域所有权验证）主题中的说明将 TXT 记录添加到域的 DNS 服务器并验证 TXT 记录是否已发布。然后再次检查您的验证状态。

您无需为私有 DNS 域名创建 A 记录。当 AWS KMS 创建指向 VPC 端点服务的接口端点时，AWS PrivateLink 会自动创建托管区，其中包含 AWS KMS VPC 中私有域名所需的 A 记录。对于具有 VPC 端点服务连接的外部密钥存储，将外部密钥存储连接到其外部密钥存储代理时，就会发生这种情况。

授权 AWS KMS 连接到 VPC 端点服务

您必须将 AWS KMS 添加到 VPC 端点服务的 Allow principals（允许主体）列表中。这允许 AWS KMS 创建指向 VPC 端点服务的接口端点。如果 AWS KMS 不是允许的主体，则创建外部密钥存储的尝试将失败，并出现 `XksProxyVpcEndpointServiceNotFoundException` 异常。

按照《AWS PrivateLink 指南》中管理权限主题中的说明进行操作。使用以下必需值。

Field	Value
ARN	`cks.kms.<region>.amazonaws.com` 例如，`cks.kms.us-east-1.amazonaws.com`

下一步：创建外部密钥存储

管理外部密钥存储

您可以使用 AWS KMS 控制台或 AWS KMS API 管理外部密钥存储。您可以创建外部密钥存储、查看和编辑其属性、监控其性能、将其与外部密钥存储代理连接和断开连接，以及删除外部密钥存储。

主题

- 创建外部密钥存储
- 编辑外部密钥存储属性

- 查看外部密钥存储
- 监控外部密钥存储
- 连接和断开外部密钥存储
- 删除外部密钥存储

创建外部密钥存储

您可以在每个 AWS 账户 和区域中创建一个或多个外部密钥存储。每个外部密钥存储都必须关联 AWS 之外的外部密钥管理器，以及用于调解 AWS KMS 与外部密钥管理器之间通信的外部密钥存储代理（XKS 代理）。有关更多信息，请参阅 规划外部密钥存储。在开始之前，请确认您需要外部密钥存储。大多数客户可以使用由 AWS KMS 密钥材料支持的 KMS 密钥。

> **Tip**
>
> 一些外部密钥管理器为创建外部密钥存储提供了更简单的方法。有关详细信息，请参阅外部密钥管理器的文档。

在创建外部密钥存储之前，您需要汇编先决条件。在创建过程中，您要指定外部密钥存储的属性。最重要的是，您要指明 AWS KMS 中的外部密钥存储是使用公有端点还是 VPC 端点服务来连接外部密钥存储代理。您还要指定连接详细信息，包括代理的 URI 端点，以及代理端点内的路径（AWS KMS 会在其中向代理发送 API 请求）。

- 如果您使用公有端点连接，请确保 AWS KMS 可以使用 HTTPS 连接通过互联网与代理通信。这包括在外部密钥存储代理上配置 TLS，并确保 AWS KMS 与代理之间的任何防火墙都允许流量在代理的端口 443 上流入和流出。在创建使用公有端点连接的外部密钥存储时，AWS KMS 通过向外部密钥存储代理发送状态请求来测试连接。此测试会验证端点是否可访问，以及外部密钥存储代理是否会接受使用外部密钥存储代理身份验证凭证签名的请求。如果此测试请求失败，则创建外部密钥存储的操作将失败。
- 如果使用 VPC 端点服务连接，请确保网络负载均衡器、私有 DNS 名称和 VPC 端点服务配置正确且可运行。如果外部密钥存储代理不在 VPC 中，则需要确保 VPC 端点服务可以与外部密钥存储代理通信。（在将外部密钥存储连接到外部密钥存储代理时，AWS KMS 会测试 VPC 端点服务连接。）

其他注意事项：

- AWS KMS记录 Amazon CloudWatch 指标和维度，尤其是外部密钥存储的指标和维度。基于其中一些指标的监控图表会显示在每个外部密钥存储的 AWS KMS 控制台中。我们强烈建议您使用这些指

标创建警报来监控外部密钥存储。这些警报会在发生性能和操作问题之前提醒您注意相关问题的早期迹象。有关说明，请参阅监控外部密钥存储。

- 外部密钥存储受资源限额的限制。在外部密钥存储中使用 KMS 密钥受请求限额的限制。在设计外部密钥存储实现之前，请查看这些限额。

> **Note**
>
> 检查您的配置中是否存在可能使其无法运行的循环依赖关系。
> 例如，如果您使用 AWS 资源创建外部密钥存储代理，请确保操作代理不需要通过该代理访问的外部密钥存储中有 KMS 密钥。

所有新的外部密钥存储都在断开连接的状态下创建。在外部密钥存储中创建 KMS 密钥之前，您必须将其连接到外部密钥存储代理。要更改外部密钥存储的属性，请编辑外部密钥存储设置。

主题

汇编先决条件

在创建外部密钥存储之前，您需要汇编所需的组件，包括用于支持外部密钥存储的外部密钥管理器，以及将 AWS KMS 请求转换为外部密钥管理器可理解格式的外部密钥存储代理。

所有外部密钥存储都需要以下组件。除了这些组件，您还需要提供组件来支持自己选择的外部密钥存储代理连接选项。

> **Tip**
>
> 您的外部密钥管理器可能包含其中一些组件，或者可以为您配置这些组件。有关详细信息，请参阅外部密钥管理器的文档。
> 如果您在 AWS KMS 控制台中创建外部密钥存储，则可以选择上传基于 JSON 的代理配置文件，该文件指定代理 URI 路径和代理身份验证凭证。一些外部密钥存储代理会为您生成此文件。有关详细信息，请参阅外部密钥存储代理或外部密钥管理器的文档。

外部密钥管理器

每个外部密钥存储都需要至少一个外部密钥管理器实例。这可以是实体或虚拟硬件安全模块（HSM），也可以是密钥管理软件。

您可以使用单个密钥管理器，但我们建议准备至少两个共享加密密钥的相关密钥管理器实例，以便实现冗余配置。外部密钥存储不需要独占使用外部密钥管理器。不过，外部密钥管理器必须有能力处理 AWS 服务以预期频率发来的加密和解密请求，这些服务使用外部密钥存储中的 KMS 密钥来保护您的资源。您的外部密钥管理器应配置为每秒最多处理 1800 个请求，并在 250 毫秒的超时限制内响应每个请求。我们建议您将外部密钥管理器放置在靠近 AWS 区域 的位置，让网络往返时间（RTT）不超过 35 毫秒。

如果外部密钥存储代理允许，则可以更改与外部密钥存储代理关联的外部密钥管理器，但新的外部密钥管理器必须是具有相同密钥材料的备份或快照。如果与 KMS 密钥关联的外部密钥无法再供外部密钥存储代理使用，AWS KMS 便无法解密使用 KMS 密钥加密的加密文字。

外部密钥存储代理必须可以访问外部密钥管理器。如果代理的GetHealthStatus响应报告所有外部密钥管理器实例都是`Unavailable`，则所有创建外部密钥存储的尝试都将失败，并显示为`XksProxyUriUnreachableException`。

外部密钥存储代理

您必须指定符合 AWS KMS 外部密钥存储代理 API 规范中设计要求的外部密钥存储代理（XKS 代理）。您可以开发或购买外部密钥存储代理，也可以使用外部密钥管理器提供或内置的外部密钥存储代理。AWS KMS 建议将外部密钥存储代理配置为每秒处理最多 1800 个请求，并在 250 毫秒的超时限制内响应每个请求。我们建议您将外部密钥管理器放置在靠近 AWS 区域 的位置，让网络往返时间（RTT）不超过 35 毫秒。

您可以将外部密钥存储代理用于多个外部密钥存储，但每个外部密钥存储必须在其请求的外部密钥存储代理中具有唯一的 URI 端点和路径。

如果您使用的是 VPC 端点服务连接，则可以在 Amazon VPC 中找到您的外部密钥存储代理，但这不是必需的。您可以将代理放置在 AWS 之外（例如您的私有数据中心内），并且只使用 VPC 端点服务与代理通信。

代理身份验证凭证

要创建外部密钥存储，必须指定外部密钥存储代理身份验证凭证（`XksProxyAuthenticationCredential`）。

您必须在外部密钥存储代理上为 AWS KMS 建立身份验证凭证（`XksProxyAuthenticationCredential`）。AWS KMS 使用签名版本 4（SigV4）流程和外部密钥存储代理身份验证凭证对代理的请求进行签名，从而对您的代理进行身份验证。您可以在创建外部密钥存储时指定身份验证凭证，并且可以随时对其进行更改。如果代理要轮换凭证，则务必更新外部密钥存储的凭证值。

代理身份验证凭证有两个部分。您必须为外部密钥存储提供这两部分。

- 访问密钥 ID：标识秘密访问密钥。您能以明文形式提供此 ID。
- 秘密访问密钥：凭证的秘密部分。AWS KMS 在存储凭证之前对凭证中的秘密访问密钥进行加密。

AWS KMS 用于对外部密钥存储代理的请求进行签名的 SigV4 凭证，与同 AWS 账户中 AWS Identity and Access Management 主体关联的任何 SigV4 凭证无关。不要将任何 IAM SigV4 凭证重复用于外部密钥存储代理。

代理连接

要创建外部密钥存储，您必须指定外部密钥存储代理连接选项（`XksProxyConnectivity`）。

AWS KMS 可以使用公有端点或 Amazon Virtual Private Cloud（Amazon VPC）端点服务，与您的外部密钥存储代理通信。公有端点虽然更易于配置和维护，但可能无法满足每次安装的安全要求。如果您选择 Amazon VPC 端点服务连接选项，则必须创建和维护所需的组件，包括在两个不同可用区内至少有两个子网的 Amazon VPC、具有网络负载均衡器和目标组的 VPC 端点服务，以及 VPC 端点服务的私有 DNS 名称。

您可以为外部密钥存储更改代理连接选项。不过，您必须确保外部密钥存储中与 KMS 密钥相关的密钥材料持续可用。否则，AWS KMS 无法解密使用这些 KMS 密钥加密的任何加密文字。

有关确定哪种代理连接选项最适合外部密钥存储的帮助信息，请参阅 选择代理连接选项。有关创建和配置 VPC 端点服务连接的帮助信息，请参阅 配置 VPC 端点服务连接。

代理 URI 端点

要创建外部密钥存储，您必须指定 AWS KMS 用于向外部密钥存储代理发送请求的端点（`XksProxyUriEndpoint`）。

协议必须是 HTTPS。AWS KMS 在端口 443 上通信。不要在代理 URI 端点值中指定端口。

- 公有端点连接 – 为外部密钥存储代理指定公开可用的端点。在创建外部密钥存储之前，此端点必须可供访问。

- VPC 端点服务连接 – 指定 `https://`，后接 VPC 端点服务的私有 DNS 名称。

在外部密钥存储代理上配置的 TLS 服务器证书必须与外部密钥存储代理 URI 端点中的域名相匹配，并且由支持外部密钥存储的证书颁发机构颁发。有关列表，请参阅 Trusted Certificate Authorities（受信任的证书颁发机构）。在颁发 TLS 证书之前，证书颁发机构会要求您提供域所有权证明。

TLS 证书上的主题通用名称（CN）必须与私有 DNS 名称相匹配。例如，若私有 DNS 名称为 `myproxy-private.xks.example.com`，则 TLS 证书上的 CN 必须为 `myproxy-private.xks.example.com` 或 `*.xks.example.com`。

您可以更改代理 URI 端点，但请确保外部密钥存储代理有权访问与外部密钥存储中的 KMS 密钥关联的密钥材料。否则，AWS KMS 无法解密使用这些 KMS 密钥加密的任何加密文字。

唯一性要求

- 合并的代理 URI 端点（`XksProxyUriEndpoint`）和代理 URI 路径（`XksProxyUriPath`）值在 AWS 账户 和区域中必须具备唯一性。
- 使用公有端点连接的外部密钥存储可以共享相同的代理 URI 端点，前提是这些外部密钥存储具有不同的代理 URI 路径值。
- 使用公有端点连接的外部密钥存储，不能采用与同一 AWS 区域 中具有 VPC 端点服务连接的任何外部密钥存储相同的代理 URI 端点值，即使密钥存储位于不同 AWS 账户 也是如此。
- 每个具有 VPC 端点连接的外部密钥存储都必须有自己的私有 DNS 名称。代理 URI 端点（私有 DNS 名称）在 AWS 账户 和区域中必须具备唯一性。

代理 URI 路径

要创建外部密钥存储，您必须在外部密钥存储代理中指定所需代理 API 的基本路径。该值必须以 / 开头且以 /kms/xks/v1 结尾，其中 `v1` 表示外部密钥存储代理的 AWS KMS API 版本。此路径可以在必要元素之间包含可选前缀，例如 `/example-prefix/kms/xks/v1`。要找到此值，请参阅外部密钥存储代理的文档。

AWS KMS 将代理请求发送到由代理 URI 端点和代理 URI 路径串联指定的地址。例如，若代理 URI 端点为 `https://myproxy.xks.example.com`，代理 URI 路径为 `/kms/xks/v1`，AWS KMS 会将其代理 API 请求发送到 `https://myproxy.xks.example.com/kms/xks/v1`。

您可以更改代理 URI 路径，但要确保外部密钥存储代理有权访问与外部密钥存储中的 KMS 密钥关联的密钥材料。否则，AWS KMS 无法解密使用这些 KMS 密钥加密的任何加密文字。

唯一性要求

- 合并的代理 URI 端点（`XksProxyUriEndpoint`）和代理 URI 路径（`XksProxyUriPath`）值在 AWS 账户 和区域中必须具备唯一性。

VPC 终端节点服务

指定用于与外部密钥存储代理通信的 Amazon VPC 端点服务的名称。只有使用 VPC 端点服务连接的外部密钥存储才需要此组件。有关为外部密钥存储设置和配置 VPC 端点服务的帮助信息，请参阅 配置 VPC 端点服务连接。

VPC 端点服务必须具有以下属性：

- 该 VPC 端点服务必须与外部密钥存储位于相同的 AWS 账户 和区域中。
- 其必须有至少连接到两个子网的网络负载均衡器（NLB），每个子网位于不同的可用区中。
- VPC 端点服务的允许主体列表必须包括区域 `cks.kms.<region>.amazonaws.com` 的 AWS KMS 服务主体，例如 `cks.kms.us-east-1.amazonaws.com`。
- 其不得要求接受连接请求。
- 其必须在更高级别的公有域内具有私有 DNS 名称。例如，在 `xks.example.com` 公有域中，私有 DNS 名称可能为 myproxy-private.xks.example.com。

  使用 VPC 端点服务连接的外部密钥存储的私有 DNS 名称，在其 AWS 区域 中必须具备唯一性。
- 私有 DNS 名称域的域验证状态必须为 `verified`。
- 在外部密钥存储代理上配置的 TLS 服务器证书，必须指定可访问端点的私有 DNS 主机名。

唯一性要求

- 具有 VPC 端点连接的外部密钥存储可以共享 Amazon VPC，但每个外部密钥存储必须有自己的 VPC 端点服务和私有 DNS 名称。

代理配置文件

代理配置文件是基于 JSON 的可选文件，其中包含外部密钥存储的代理 URI 路径和代理身份验证凭证属性的值。在 AWS KMS 控制台中创建或编辑外部密钥存储时，您可以上传代理配置文件来为外部密钥存储提供配置值。使用此文件可以避免键入和粘贴错误，并确保外部密钥存储中的值与外部密钥存储代理中的值相匹配。

代理配置文件由外部密钥存储代理生成。要了解外部密钥存储代理是否提供代理配置文件，请参阅您的外部密钥存储代理文档。

下面是具有虚拟值的格式正确的代理配置文件示例。

```
{
  "XksProxyUriPath": "/example-prefix/kms/xks/v1",
  "XksProxyAuthenticationCredential": {
    "AccessKeyId": "ABCDE12345670EXAMPLE",
    "RawSecretAccessKey": "0000EXAMPLEFA5FT0mCc3DrGUe2sti527BitkQ0Zr9MO9+vE="
  }
}
```

只有在 AWS KMS 控制台中创建或编辑外部密钥存储时，才能上传代理配置文件。您不能将其与CreateCustomKeyStore或UpdateCustomKeyStore操作一起使用，但可以使用代理配置文件中的值来确保参数值正确无误。

创建外部密钥存储（控制台）

在创建外部密钥存储之前，请查看 规划外部密钥存储，选择代理连接类型，并确保已创建和配置了所有必需的组件。如果需要查找任何所需值的帮助信息，请查阅外部密钥存储代理或密钥管理软件的文档。

> **Note**
>
> 在 AWS Management Console 中创建外部密钥存储时，您可以上传基于 JSON 的代理配置文件，其中包含代理 URI 路径和代理身份验证凭证的值。一些代理会为您生成此文件，但其并非必要项目。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Custom key stores（自定义密钥存储）、External key stores（外部密钥存储）。
4. 选择 Create external key store（创建外部密钥存储）。
5. 为外部密钥存储输入易记名称。该名称在您账户的所有外部密钥存储中必须具备唯一性。

> **Important**
>
> 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。

6. 选择代理连接类型。

   您的代理连接选择决定了外部密钥存储代理所需的组件。有关做出此选择的帮助信息，请参阅 选择代理连接选项。

7. 选择或输入此外部密钥存储的 VPC 端点服务的名称。此步骤仅在外部密钥存储代理连接类型为 VPC 端点服务时出现。

   VPC 端点服务及其 VPC 必须满足外部密钥存储的要求。有关更多信息，请参阅 the section called “汇编先决条件”。

8. 输入代理 URI 端点。协议必须是 HTTPS。AWS KMS 在端口 443 上通信。不要在代理 URI 端点值中指定端口。

   如果 AWS KMS 识别出您在上一步中指定的 VPC 端点服务，则会为您填写此字段。

   若使用公有端点连接，请输入公开可用的端点 URI。若使用 VPC 端点连接，输入 `https://`，后接 VPC 端点服务的私有 DNS 名称。

9. 要输入代理 URI 路径前缀和代理身份验证凭证的值，请上传代理配置文件或手动输入值。

   - 如果您有包含代理 URI 路径和代理身份验证凭证值的可选代理配置文件，请选择 Upload configuration file（上传配置文件）。然后按照步骤上传该文件。

     上传文件后，控制台会在可编辑字段中显示文件中的值。您可以立即更改值，也可以在创建外部密钥存储后编辑这些值。

     要显示秘密访问密钥的值，请选择 Show secret access key（显示私有访问密钥）。

   - 如果您没有代理配置文件，则可以手动输入代理 URI 路径和代理身份验证凭证值。

     a. 如果没有代理配置文件，您可以手动输入代理 URI。控制台提供所需的 /kms/xks/v1 值。

        如果代理 URI 路径包含可选前缀，例如 `/example-prefix/kms/xks/v1` 中的 `example-prefix`，请在 Proxy URI path prefix（代理 URI 路径前缀）字段中输入该前缀。如若没有，则将字段留空。

b. 如果没有代理配置文件，您可以手动输入代理身份验证凭证。访问密钥 ID 和秘密访问密钥均为必填项。

- 在 Proxy credential: Access key ID（代理凭证：访问密钥 ID）中，输入代理身份验证凭证的访问密钥 ID。访问密钥 ID 标识秘密访问密钥。
- 在 Proxy credential: Secret access key（代理凭证：秘密访问密钥）中，输入代理身份验证凭证的秘密访问密钥。

要显示秘密访问密钥的值，请选择 Show secret access key（显示私有访问密钥）。

此过程不会设置或更改您在外部密钥存储代理上建立的身份验证凭证。其只是将这些值关联到外部密钥存储。有关设置、更改和轮换代理身份验证凭证的信息，请参阅外部密钥存储代理或密钥管理软件的文档。

如果您的代理身份验证凭证发生变化，请编辑外部密钥存储的凭证设置。

10. 选择 Create external key store（创建外部密钥存储）。

当该过程成功时，新的外部密钥存储将显示在账户和区域的外部密钥存储列表中。如果该过程失败，则会显示一条错误消息，描述问题并提供有关如何解决该问题的帮助。如果您需要更多帮助，请参阅CreateKey 外部密钥错误。

下一步：不会自动连接新的外部密钥存储。在外部密钥存储中创建 AWS KMS keys 之前，您必须将外部密钥存储连接到其外部密钥存储代理。

创建外部密钥存储（API）

您可以使用该CreateCustomKeyStore操作来创建新的外部密钥存储库。如果需要查找所需参数值的帮助信息，请参阅外部密钥存储代理或密钥管理软件的文档。

> **Tip**
>
> 使用 `CreateCustomKeyStore` 操作时，您无法上传代理配置文件。不过，您可以使用代理配置文件中的值来确保参数值正确无误。

要创建外部密钥存储，`CreateCustomKeyStore` 操作需要以下参数值。

- `CustomKeyStoreName` - 外部密钥存储的易记名称，该名称在账户中具备唯一性。

> **Important**
>
> 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。

- `CustomKeyStoreType` – 指定 `EXTERNAL_KEY_STORE`。
- `XksProxyConnectivity` – 指定 `PUBLIC_ENDPOINT` 或 `VPC_ENDPOINT_SERVICE`。
- `XksProxyAuthenticationCredential` – 指定访问密钥 ID 和秘密访问密钥。
- `XksProxyUriEndpoint` – AWS KMS 用于与外部密钥存储代理通信的端点。
- `XksProxyUriPath` – 代理 API 在代理内的路径。
- `XksProxyVpcEndpointServiceName` – 仅当 `XksProxyConnectivity` 值为 `VPC_ENDPOINT_SERVICE` 时才需要。

> **Note**
>
> 如果您使用 AWS CLI 版本 1.0，请在指定具有 HTTP 或 HTTPS 值的参数（例如 `XksProxyUriEndpoint` 参数）之前运行以下命令。
>
> ```
> aws configure set cli_follow_urlparam false
> ```
>
> 否则，AWS CLI 版本 1.0 会将参数值替换为在该 URI 地址找到的内容，从而导致以下错误：
>
> ```
> Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve
> https:// : received non 200 status code of 404
> ```

以下示例使用虚拟值。在运行命令之前，将虚拟值替换为外部密钥存储的有效值。

创建使用公有端点连接的外部密钥存储。

```
$ 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>
```

创建使用 VPC 端点服务连接的外部密钥存储。

```
$ 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>
```

当此操作成功时，CreateCustomKeyStore 将返回自定义密钥存储 ID，如以下示例响应中所示。

```
{
    "CustomKeyStoreId": cks-1234567890abcdef0
}
```

如果操作失败，请更正异常指示的错误，然后重试。有关其他帮助，请参阅排查外部密钥存储的问题。

下一步：要使用外部密钥存储，请将其连接到外部密钥存储代理。

编辑外部密钥存储属性

您可以编辑现有外部密钥存储的选定属性。

在连接或断开外部密钥存储后，您可以编辑某些属性。若要编辑其他属性，则必须先断开外部密钥存储与其外部密钥存储代理的连接。外部密钥存储的连接状态必须为 DISCONNECTED。在外部密钥存储断开后，您可以管理密钥存储及其 KMS 密钥，但无法在外部密钥存储中创建或使用 KMS 密钥。要查找外部密钥存储库的连接状态，请使用DescribeCustomKeyStores操作或查看外部密钥存储详细信息页面上的 “常规配置” 部分。

在更新外部密钥存储库的属性之前，使用新值向外部密钥存储代理AWS KMS发送GetHealthStatus请求。如果请求成功，则表明您可以使用更新后的属性值连接到外部密钥存储代理并进行身份验证。如果请求失败，编辑操作也将失败，并且会显示标识错误的异常。

编辑操作完成后，外部密钥存储的更新属性值将显示在 AWS KMS 控制台和 DescribeCustomKeyStores 响应中。不过，要让更改完全生效，可能需要长达五分钟的时间。

如果您在 AWS KMS 控制台中编辑外部密钥存储，则可以选择上传基于 JSON 的代理配置文件，该文件指定代理 URI 路径和代理身份验证凭证。一些外部密钥存储代理会为您生成此文件。有关详细信息，请参阅外部密钥存储代理或外部密钥管理器的文档。

> **Warning**
>
> 更新后的属性值必须将您的外部密钥存储连接到与先前值相同的外部密钥管理器的代理，或者使用相同的加密密钥对外部密钥管理器进行备份或快照。如果外部密钥存储永久失去对与其 KMS 密钥关联的外部密钥的访问权限，则在这些外部密钥下加密的加密文字将无法恢复。特别要注意的是，更改外部密钥存储的代理连接可能会阻止 AWS KMS 访问外部密钥。

> **Tip**
>
> 一些外部密钥管理器为编辑外部密钥存储属性提供了更简单的方法。有关详细信息，请参阅外部密钥管理器的文档。

您可以更改外部密钥存储的以下属性。

可编辑的外部密钥存储属性	任何连接状态	需要断开连接状态
自定义密钥存储名称 自定义密钥存储必需的易记名称。 **Important** 不要在此字段中包含机密或敏感信息。此字段可能会以纯文本形式显示在 CloudTrail 日志和其他输出中。	✓	
代理身份验证凭证 () XksProxyAuthenticationCredential （即使只更改一个元素，您也必须同时指定访问密钥 ID 和秘密访问密钥。）	✓	

可编辑的外部密钥存储属性	任何连接状态	需要断开连接状态
代理 URI 路径 (XksProxyUriPath)	✓	
代理连接 (XksProxyConnectivity) （您还必须更新代理 URI 端点。如果要更改为 VPC 端点服务连接，则必须指定代理 VPC 端点服务名称。）		✓
代理 URI 端点 (XksProxyUriEndpoint) 如果更改代理端点 URI，您可能还需要更改关联的 TLS 证书。		✓
代理 VPC 终端节点服务名称 (XksProxyVpcEndpointServiceName) （此字段是 VPC 端点服务连接的必填字段）		✓

主题

- 编辑外部密钥存储器（控制台）
- 编辑外部密钥存储（API）

编辑外部密钥存储器（控制台）

编辑密钥存储时，您可以更改任何可编辑的值。某些更改要求将外部密钥存储与其外部密钥存储代理断开连接。

如果您正在编辑代理 URI 路径或代理身份验证凭证，则可以输入新值或上传包含新值的外部密钥存储代理配置文件。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Custom key stores（自定义密钥存储）、External key stores（外部密钥存储）。

4. 选择要编辑的外部密钥存储的行。
5. 如有必要，请断开外部密钥存储与其外部密钥存储代理的连接。从 Key store actions（密钥存储操作）菜单中选择 Disconnect（断开连接）。
6. 从 Key store actions（密钥存储操作）菜单中选择 Edit（编辑）。
7. 更改一个或多个可编辑的外部密钥存储属性。您还可以上传包含代理 URI 路径和代理身份验证凭证值的外部密钥存储代理配置文件。即使文件中指定的某些值没有更改，也可以使用代理配置文件。
8. 选择 Update external key store（更新外部密钥存储）。
9. 查看警告，如果您决定继续，请确认警告，然后选择 Update external key store（更新外部密钥存储）。

   在此过程成功后，将显示一条消息，描述您编辑的属性。如果此过程失败，则会显示一条错误消息，描述问题并提供有关如何解决问题的帮助。
10. 如有必要，重新连接外部密钥存储。从 Key store actions（密钥存储操作）菜单中选择 Connect（连接）。

    您可以让外部密钥存储保持断开状态。不过，在其断开连接后，您无法在外部密钥存储中创建 KMS 密钥或在加密操作中使用外部密钥存储中的 KMS 密钥。

编辑外部密钥存储（API）

要更改外部密钥存储库的属性，请使用UpdateCustomKeyStore操作。您可以在同一操作中更改外部密钥存储的多个属性。如果此操作成功，则 AWS KMS 返回 HTTP 200 响应和无属性的 JSON 对象。

使用 `CustomKeyStoreId` 参数标识外部密钥存储。使用其他参数更改属性。您不能在 `UpdateCustomKeyStore` 操作中使用代理配置文件。只有 AWS KMS 控制台支持代理配置文件。不过，您可以使用代理配置文件来帮助自己确定外部密钥存储代理的正确参数值。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

在开始之前，如有必要，请断开外部密钥存储与其外部密钥存储代理的连接。更新后，如有必要，您可以将外部密钥存储重新连接到其外部密钥存储代理。您可以让外部密钥存储保持断开状态，但之后必须先重新连接，才能在密钥存储中创建新的 KMS 密钥或在密钥存储中使用现有 KMS 密钥来进行加密操作。

> **Note**
>
> 如果您使用 AWS CLI 版本 1.0，请在指定具有 HTTP 或 HTTPS 值的参数（例如 XksProxyUriEndpoint 参数）之前运行以下命令。
>
> ```
> aws configure set cli_follow_urlparam false
> ```
>
> 否则，AWS CLI 版本 1.0 会将参数值替换为在该 URI 地址找到的内容，从而导致以下错误：
>
> ```
> Error parsing parameter '--xks-proxy-uri-endpoint': Unable to retrieve
> https:// : received non 200 status code of 404
> ```

更改外部密钥存储的名称

第一个示例使用UpdateCustomKeyStore操作将外部密钥存储库的友好名称更改为XksKeyStore。该命令使用 CustomKeyStoreId 参数标识自定义密钥存储，使用 CustomKeyStoreName 指定自定义密钥存储的新名称。将所有示例值替换为外部密钥存储的实际值。

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 --new-
custom-key-store-name XksKeyStore
```

更改代理身份验证凭证

以下示例更新了 AWS KMS 用于向外部密钥存储代理进行身份验证的代理身份验证凭证。如果凭证在代理上轮换，您可以使用这样的命令来更新凭证。

首先更新外部密钥存储代理上的凭证。然后使用此功能将更改报告给 AWS KMS。（您的代理将暂时支持旧凭证和新凭证，让您有时间在 AWS KMS 中更新凭证。）

您必须始终在凭证中同时指定访问密钥 ID 和秘密访问密钥，即使只更改了一个值也是如此。

前两个命令设置变量来保存凭证值。UpdateCustomKeyStore 操作使用 CustomKeyStoreId 参数来标识外部密钥存储。该操作使用 XksProxyAuthenticationCredential 参数及其 AccessKeyId 和 RawSecretAccessKey 字段来指定新凭证。将所有示例值替换为外部密钥存储的实际值。

```
$ 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
```

更改代理 URI 路径

以下示例更新了代理 URI 路径（XksProxyUriPath）。代理 URI 端点和代理 URI 路径的组合在 AWS 账户 和区域中必须具备唯一性。将所有示例值替换为外部密钥存储的实际值。

```
$ aws kms update-custom-key-store --custom-key-store-id cks-1234567890abcdef0 \
            --xks-proxy-uri-path /kms/xks/v1
```

更改 VPC 端点服务连接

以下示例使用UpdateCustomKeyStore操作将外部密钥存储代理连接类型更改为VPC_ENDPOINT_SERVICE。要进行此更改，您必须指定 VPC 端点服务连接所需的值，包括 VPC 端点服务名称（XksProxyVpcEndpointServiceName）和包含 VPC 端点服务的私有 DNS 名称的代理 URI 端点（XksProxyUriEndpoint）值。将所有示例值替换为外部密钥存储的实际值。

```
$ 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
```

更改为公有端点连接

以下示例将外部密钥存储代理连接类型更改为 PUBLIC_ENDPOINT。进行此更改时，必须更新代理 URI 端点（XksProxyUriEndpoint）值。将所有示例值替换为外部密钥存储的实际值。

> **Note**
>
> VPC 端点连接提供的安全性高于公有端点连接。在更改为公有端点连接之前，请考虑其他选项，包括在本地找到外部密钥存储代理以及仅使用 VPC 进行通信。

```
$ 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
```

查看外部密钥存储

您可以使用AWS KMS控制台或使用DescribeCustomKeyStores操作来查看每个账户和区域中的外部密钥存储库。

查看外部密钥存储时，可以看到以下内容：

- 有关密钥存储的基本信息，包括其易记名称、ID、密钥存储类型和创建日期。
- 外部密钥存储代理的配置信息，包括连接类型、代理 URI 端点和路径，以及当前代理身份验证凭证的访问密钥 ID。
- 如果外部密钥存储代理使用 VPC 端点服务连接，则控制台将显示 VPC 端点服务的名称。
- 当前连接状态。

> **Note**
>
> 如果连接状态值为 Disconnected（已断开连接），则表示外部密钥存储从未连接过，或者已有意与其外部密钥存储代理断开连接。但是，如果您尝试使用已连接的外部密钥存储中的 KMS 密钥时失败，则可能表示该外部密钥存储或其代理存在问题。有关帮助信息，请参阅外部密钥存储连接错误。

- 带有 Amazon CloudWatch 指标图表的 “监控” 部分，旨在帮助您检测和解决外部密钥存储的问题。有关解释图表、在规划和故障排除中使用图表以及根据图表中的指标创建 CloudWatch 警报的帮助，请参阅监控外部密钥存储。

另请参阅：

- 在外部密钥存储中查看 KMS 密钥
- 使用记录 AWS KMS API 调用 AWS CloudTrail

主题

- 外部密钥存储属性
- 查看外部密钥存储（控制台）
- 查看外部密钥存储（API）

外部密钥存储属性

外部密钥库的以下属性在AWS KMS控制台和DescribeCustomKeyStores响应中可见。

自定义密钥存储属性

以下值出现在每个自定义密钥存储的详细信息页面的 General configuration（常规配置）部分中。这些属性适用于所有自定义密钥存储，包括 AWS CloudHSM 密钥存储和外部密钥存储。

自定义密钥存储 ID

AWS KMS 分配给自定义密钥存储的唯一 ID。

自定义密钥存储名称

在创建自定义密钥存储时为其分配的易记名称。您可以随时更改此值。

自定义密钥存储类型

自定义密钥存储的类型。有效值为 AWS CloudHSM（AWS_CLOUDHSM）或外部密钥存储（EXTERNAL_KEY_STORE）。创建自定义密钥存储后无法更改其类型。

创建日期

创建自定义密钥存储的日期。此日期显示为 AWS 区域 的本地时间。

连接状态

表示自定义密钥存储已连接到其备用密钥存储。仅当自定义密钥存储从未连接到其备用密钥存储或故意断开连接时，连接状态才会为 DISCONNECTED。有关更多信息，请参阅 the section called “连接状态”。

外部密钥存储配置属性

以下值显示在每个外部密钥存储详细信息页面的外部密钥存储代理配置部分和DescribeCustomKeyStores响应XksProxyConfiguration元素中。有关每个字段的详细描述，包括唯一性要求，以及有关帮助确定每个字段的正确值的详细描述，请参阅 Creating an external key store（创建外部密钥存储）主题中的 the section called “汇编先决条件”。

代理连接

指示外部密钥存储是使用公有端点连接还是 VPC 端点服务连接。

代理 URI 端点

AWS KMS 用于连接到外部密钥存储代理的端点。

代理 URI 路径

来自代理 URI 端点的路径，AWS KMS 将其用于发送代理 API 请求。

代理凭证：访问密钥 ID

您在外部密钥存储代理上建立的代理身份验证凭证的一部分。访问密钥 ID 标识出凭证中的秘密访问密钥。

AWS KMS 使用 SigV4 签名流程和代理身份验证凭证来签署其对您外部密钥存储代理的请求。签名中的凭证允许外部密钥存储代理代表您对来自 AWS KMS 的请求进行身份验证。

VPC 端点服务名称

支持您的外部密钥存储的 Amazon VPC 端点服务的名称。此值仅在外部密钥存储使用 VPC 端点服务连接时显示。您可以在 VPC 中找到您的外部密钥存储代理，也可以使用 VPC 端点服务与您的外部密钥存储代理安全地进行通信。

查看外部密钥存储（控制台）

要查看给定账户和区域中的外部密钥存储，请按照以下流程操作。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Custom key stores（自定义密钥存储）、External key stores（外部密钥存储）。
4. 要查看有关外部密钥存储的详细信息，请选择密钥存储名称。

查看外部密钥存储（API）

要查看您的外部密钥存储库，请使用DescribeCustomKeyStores操作。默认情况下，此操作将返回账户和区域中的所有自定义密钥存储。不过，您可以使用 `CustomKeyStoreId` 或 `CustomKeyStoreName` 参数（但不能同时使用两者）将输出限制到特定的自定义密钥存储。

对于自定义密钥存储，输出包含自定义密钥存储 ID、名称和类型以及密钥存储的连接状态。如果连接状态为 `FAILED`，则输出还包含描述错误原因的 `ConnectionErrorCode`。有关解释外部密钥存储 `ConnectionErrorCode` 的帮助，请参阅 外部密钥存储的连接错误代码。

对于外部密钥存储，输出还包括 XksProxyConfiguration 元素。此元素包括连接类型、代理 URI 端点、代理 URI 路径和代理身份验证凭证的访问密钥 ID。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

例如，以下命令返回账户和区域中的所有自定义密钥存储。您可以使用 Limit 和 Marker 参数来浏览输出中的自定义密钥存储。

```
$ aws kms describe-custom-key-stores
```

以下示例命令使用 CustomKeyStoreName 参数以仅获取具有 ExampleXksPublic 易记名称的示例外部密钥存储。此示例密钥存储使用公有端点连接。该密钥存储连接到其外部密钥存储代理。

```
$ 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"
      }
    }
  ]
}
```

以下命令获取具有 VPC 端点服务连接的示例外部密钥存储。在此示例中，外部密钥存储连接到其外部密钥存储代理。

```
$ 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"
      }
    }
  ]
}
```

ConnectionState 为 Disconnected 则表示外部密钥存储从未连接过，或者已有意与其与外部密钥存储代理断开连接。但是，如果您尝试使用已连接的外部密钥存储中的 KMS 密钥时失败，则可能表示该外部密钥存储代理或其他外部组件存在问题。

如果外部密钥存储的 ConnectionState 为 FAILED，则 DescribeCustomKeyStores 响应包含说明错误原因的 ConnectionErrorCode 元素。

例如，在以下输出中，XKS_PROXY_TIMED_OUT 值表示 AWS KMS 可以连接到外部密钥存储代理，但由于外部密钥存储代理未在分配的时间内响应 AWS KMS，所以连接失败。如果您反复看到此连接错误代码，请通知您的外部密钥存储代理供应商。有关此连接失败及其他连接错误失败的帮助，请参阅排查外部密钥存储的问题。

```
$ 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"
      }
    }
  ]
}
```

监控外部密钥存储

AWS KMS收集与外部密钥存储库的每次交互的指标，并将其发布到您的 CloudWatch 账户中。这些指标用于在每个外部密钥存储的详细信息页面的监控部分生成图表。以下主题详细介绍了如何使用图表来识别和排查影响外部密钥存储的操作和配置问题。我们建议使用这些 CloudWatch 指标来设置警报，以便在外部密钥存储未按预期运行时通知您。有关更多信息，请参阅使用 Amazon 进行监控 CloudWatch。

主题

- 查看图表
- 解释图表
- 设置警报

查看图表

您可以在不同的详细程度下查看图表。默认情况下，每个图表使用三小时的时间范围和五分钟的汇总期。您可以在控制台中调整图表视图，但是当关闭外部密钥存储的详细信息页面或刷新浏览器时，您的更改将恢复为默认设置。有关亚马逊 CloudWatch 术语的帮助，请参阅亚马逊 CloudWatch 概念。

查看数据点详细信息

每个图表中的数据通过 AWS KMS 指标收集。若要查看有关特定数据点的更多信息，请将鼠标悬停在折线图上的数据点上方。这将显示一个弹出窗口，其中包含有关派生该图表的指标的更多信息。每个列表项都显示记录在该数据点的维度值。如果该数据点的维度值没有可用的指标数据，则弹出窗口将显示空值（–）。有些图表记录了单个数据点的多个维度和值。其他图表，例如可靠性图表，使用指标收集的数据来计算唯一值。每个列表项均与不同的折线图颜色关联。

修改时间范围

若要修改时间范围，请在监控部分的右上角选择一个预定义的时间范围。预定义的时间范围从 1 小时到 1 周（1 小时、3 小时、12 小时、1 天、3 天或者 1 周）。这将调整所有图表的时间范围。如果您想查看不同时间范围内的特定图表，或者想要设置自定义时间范围，请放大图表或在 Amazon CloudWatch 控制台中查看。

放大图表

您可以使用缩微贴图缩放功能来重点查看折线图和图表的堆叠部分，而无需在放大和缩小视图之间进行切换。例如，您可以使用缩微贴图缩放功能来重点查看折线图中的峰值，以便将该峰值与同一时间线的监控部分中的其他图表进行比较。

1. 选择并拖动要突出的图表区域，然后释放拖动对象。
2. 要重置缩放，选择 Reset zoom（重置缩放）图标，该图标看起来像放大镜里面包含减号 (-) 符号。

放大图表

若要放大图表，请选择单个图表右上角的菜单图标，然后选择 Enlarge（放大）。将鼠标悬停在图表上方时，也可以选择菜单图标旁边显示的放大图标。

放大图表可让您通过指定不同的时间段、自定义时间范围或刷新间隔来进一步修改图表的视图。关闭放大视图时，这些更改将恢复为默认设置。

修改时间段

1. 选择 Period options（时间段选项）菜单。默认情况下，此菜单显示的值为：5 minutes（5 分钟）。
2. 选择一个时间段，预定义的时间段从 1 秒到 30 天不等。

   例如，您可以选择一分钟视图，这在您排查问题时会非常有用。或者，选择不太详细的一小时视图。这在您查看更大的时间范围（例如 3 天）来了解一段时间内的趋势时会很有用。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的周期。

修改时间范围或时区

1. 选择一个预定义的时间范围，此范围的跨度从 1 小时到 1 周（1 小时、3 小时、12 小时、1 天、3 天或 1 周）。或者，您也可以选择 Custom（自定义）来设置自己的时间范围。
2. 选择 Custom（自定义）。

   a. 时间范围：选择方框左上角的 Absolute（绝对）选项卡。使用日历选取器或文本字段框指定时间范围。

   b. 时区：选择方框右上角的下拉菜单。您可以将时区更改为 UTC（协调世界时）或 Local time zone（本地时区）。
3. 在指定时间范围后，选择 Apply（应用）。

修改图表中数据的刷新频率

1. 选择右上角的 Refresh options（刷新选项）菜单。
2. 选择刷新间隔（关闭、10 秒、1 分钟、2 分钟、5 分钟或 15 分钟）。

在 Amazon CloudWatch 控制台中查看图表

监控部分中的图表来自AWS KMS发布到 Amazon 的预定义指标 CloudWatch。你可以在 CloudWatch 控制台中打开它们并将其保存到 CloudWatch 仪表板中。如果您有多个外部密钥存储库，则可以在中打开它们各自的图表 CloudWatch 并将其保存到单个仪表板中，以比较它们的运行状况和使用情况。

添加到 CloudWatch 控制面板

选择右上角的 “添加到控制面板”，将所有图表添加到 Amazon CloudWatch 控制面板。您可以选择现有的控制面板或创建一个新控制面板。有关使用此控制面板创建图表和警报的自定义视图的信息，请参阅《亚马逊 CloudWatch 用户指南》中的 “使用亚马逊 CloudWatch控制面板”。

在 CloudWatch 指标中查看

选择单个图表右上角的菜单图标，然后选择在指标中查看，即可在 Amazon CloudWatch 控制台中查看此图表。在 CloudWatch 控制台中，您可以将此单个图表添加到仪表板并修改时间范围、周期和刷新间隔。有关更多信息，请参阅《Amazon CloudWatch 用户指南》中的 “绘制指标”。

解释图表

AWS KMS 提供了多个图表来监控 AWS KMS 控制台中的外部密钥存储的运行状况。这些图表为自动配置，派生自 AWS KMS 指标。

图形数据作为您对外部密钥存储和外部密钥进行的调用的一部分收集。在您未进行任何调用的时间范围内，您可能会看到数据填充图表，此数据来自 AWS KMS 代表您进行的定期 `GetHealthStatus` 调用，以检查外部密钥存储代理和外部密钥管理器的状态。如果您的图表显示 No data available（无可用数据）消息，则表示在该时间范围内没有记录任何调用，或者您的外部密钥存储处于 `DISCONNECTED` 状态。您可以通过将视图调整到更大的时间范围来确定外部密钥存储断开连接的时间。

主题

- 请求总数
- 可靠性
- 延迟
- 前 5 个异常
- 证书过期天数

请求总数

在给定时间范围内收到的针对特定外部密钥存储的 AWS KMS 请求总数。使用此图表来确定您是否面临节流的风险。

AWS KMS 建议您的外部密钥管理器每秒能够处理多达 1800 个加密操作请求。如果您在五分钟内接通 540000 个电话，则有节流的风险。

您可以监控外部密钥存储中 AWS KMS 使用 ExternalKeyStoreThrottle 指标进行节流的 KMS 密钥的加密操作请求数量。

如果您经常收到 KMSInvalidStateException 错误，其中包含一条说明请求“due to a very high request rate”（由于请求率很高）而被拒绝的消息，则可能表明您的外部密钥管理器或外部密钥存储代理无法跟上当前的请求速率。如可能，请降低您的请求速率。您也可以考虑请求降低自定义密钥存储请求限额值。降低此限额值可能会增加节流的风险，但这表示多余的请求在发送到外部密钥存储代理或外部密钥管理器之前会很快被 AWS KMS 拒绝。要申请下调限额，请访问 AWS Support 中心 并创建工单。

总请求数图表派生自 XksProxyErrors 指标，该指标收集有关 AWS KMS 从外部密钥存储代理收到的成功和失败响应的数据。当您查看特定数据点时，弹出窗口会显示 CustomKeyStoreId 维度的值以及在该数据点记录的 AWS KMS 请求总数。CustomKeyStoreId 将始终相同。

可靠性

外部密钥存储代理返回的成功响应或不可重试错误的 AWS KMS 请求百分比。使用此图表评估外部密钥存储代理的运行状况。

当图表显示的值小于 100% 时，该值表示代理没有响应，或者响应了可重试错误。这可能表明网络存在问题、外部密钥存储代理或外部密钥管理器速度缓慢或实施错误。

如果请求包含错误的凭证，且代理响应了 AuthenticationFailedException，则该图仍将显示 100% 的可靠性，因为代理在外部密钥存储代理 API 请求中识别出了错误的值，因此预计会出现故障。如果可靠性图表的百分比为 100%，则您的外部密钥存储代理将按预期进行响应。如果图表显示的值小于 100%，则代理会响应可重试错误或超时。例如，如果代理由于请求速率过高而响应了 ThrottlingException，则图表将显示较低的可靠性百分比，因为代理无法识别请求中导致其失败的特定问题。这是因为可重试错误可能是临时性问题，可以通过重试请求解决。

以下错误响应将降低可靠性百分比。您可以使用 前 5 个异常 图表和 XksProxyErrors 指标进一步监控代理返回每个可重试错误的频率。

- InternalException

- DependencyTimeoutException
- ThrottlingException
- XksProxyUnreachableException

可靠性图表派生自 XksProxyErrors 指标，该指标收集有关 AWS KMS 从外部密钥存储代理收到的成功和失败响应的数据。只有当响应的 ErrorType 值为 Retryable 时，可靠性百分比才会降低。当您查看特定数据点时，弹出窗口会显示 CustomKeyStoreId 维度的值以及在该数据点记录的 AWS KMS 请求的可靠性百分比。CustomKeyStoreId 将始终相同。

我们建议使用该XksProxyErrors指标创建 CloudWatch 警报，通过在一分钟内记录超过五个可重试错误时提醒您潜在的网络问题。有关更多信息，请参阅 为可重试的错误创建 Amazon CloudWatch 警报。

延迟

外部密钥存储代理响应 AWS KMS 请求所用的毫秒数。使用此图表来评估您的外部密钥存储代理和外部密钥管理器的性能。

AWS KMS 希望外部密钥存储代理在 250 毫秒内响应每个请求。如果网络超时，AWS KMS 将重试一次请求。如果代理再次失败，则记录的延迟是两次请求尝试的合计超时限制，图表将显示大约 500 毫秒。在代理未在 250 毫秒超时限制内响应的所有其他情况下，记录的延迟为 250 毫秒。如果代理在加密和解密操作时经常超时，请咨询您的外部代理管理员。有关解决延迟问题的帮助，请参阅 延迟和超时错误。

响应缓慢还可能表明您的外部密钥管理器无法处理当前的请求流量。AWS KMS 建议您的外部密钥管理器每秒能够处理高达 1800 个加密操作请求。如果您的外部密钥管理器无法处理每秒 1800 个请求的速率，请考虑请求降低自定义密钥存储中 KMS 密钥的请求限额。使用外部密钥存储中的 KMS 密钥进行加密操作的请求将采用快速失效机制，并出现节流异常，而不是由外部密钥存储代理或外部密钥管理器处理后拒绝。

延迟图表派生自 XksProxyLatency 指标。当您查看特定数据点时，弹出窗口会显示相应的 KmsOperation 和 XksOperation 维度的值以及该数据点的操作记录的平均延迟。列表项按从最高延迟到最低延迟的顺序排列。

我们建议使用该XksProxyLatency指标创建 CloudWatch 警报，以便在延迟接近超时限制时通知您。有关更多信息，请参阅 为响应超时创建 Amazon CloudWatch 警报。

前 5 个异常

在给定时间范围内失败的加密和管理操作的前五个异常。使用此图表跟踪最常见的错误，因此您可以确定工程工作的优先顺序。

此计数包括 AWS KMS 从外部密钥存储代理收到的异常以及无法与外部密钥存储代理建立通信时 AWS KMS 在内部返回的 XksProxyUnreachableException。

可重试错误率高可能表示网络错误，而不可重试错误率高可能表示外部密钥存储的配置存在问题。例如，AuthenticationFailedExceptions 中的峰值表示 AWS KMS 中配置的身份验证凭证与外部密钥存储代理之间存在差异。若要查看您的外部密钥存储配置，请参阅 查看外部密钥存储。若要编辑您的外部密钥存储设置，请参阅 编辑外部密钥存储属性。

AWS KMS 从外部密钥库代理收到的异常与 AWS KMS 在操作失败时返回的异常不同。对于与外部密钥存储的外部配置或连接状态有关的所有操作失败，AWS KMS 加密操作都会返回 KMSInvalidStateException。若要确定问题，请使用随附的错误消息文本。

下表显示了可能出现在前 5 个异常图表中的异常以及 AWS KMS 向您返回的相应异常。

错误类型	图表中显示的异常	AWS KMS 向您返回的异常
不可重试	**AccessDeniedException** 有关问题排查帮助，请参阅代理授权问题。	**CustomKeyStoreInvalidStateException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。
不可重试	**AuthenticationFailedException** 有关问题排查帮助，请参阅身份验证凭证错误。	**XksProxyIncorrectAuthenticationCredentialException** 响应 CreateCustomKeyStore 和 UpdateCustomKeyStore 操作。 **CustomKeyStoreInvalidStateException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。
可重试	**DependencyTimeoutException**	**XksProxyUriUnreachableException** 响应

错误类型	图表中显示的异常	AWS KMS 向您返回的异常
	有关问题排查帮助，请参阅延迟和超时错误。	CreateCustomKeyStore 和 UpdateCustomKeyStore 操作。 **CustomKeyStoreInvalidStateException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。
可重试	**InternalException** 外部密钥库代理拒绝了该请求，因为该请求无法与外部密钥管理器通信。验证外部密钥存储代理配置是否正确以及外部密钥管理器是否可用。	**XksProxyInvalidResponseException** 响应 CreateCustomKeyStore 和 UpdateCustomKeyStore 操作。 **CustomKeyStoreInvalidStateException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。
不可重试	**InvalidCiphertextException** 有关问题排查帮助，请参阅解密错误。	**KMSInvalidStateException** 响应加密操作。
不可重试	**InvalidKeyUsageException** 有关问题排查帮助，请参阅外部密钥的加密操作错误。	**XksKeyInvalidConfigurationException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。

错误类型	图表中显示的异常	AWS KMS 向您返回的异常
不可重试	**InvalidStateException** 有关问题排查帮助，请参阅外部密钥的加密操作错误。	**XksKeyInvalidConfigurationException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。
不可重试	**InvalidUriPathException** 有关问题排查帮助，请参阅常规配置错误。	**XksProxyInvalidConfigurationException** 响应 CreateCustomKeyStore 和 UpdateCustomKeyStore 操作。 **CustomKeyStoreInvalidStateException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。
不可重试	**KeyNotFoundException** 有关问题排查帮助，请参阅外部密钥错误。	**XksKeyNotFoundException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。

错误类型	图表中显示的异常	AWS KMS 向您返回的异常
可重试	**ThrottlingException** 由于请求速率过高，外部密钥存储代理拒绝了该请求。使用外部密钥存储中的 KMS 密钥降低调用频率。	**XksProxyUriUnreachableException** 响应 CreateCustomKeyStore 和 UpdateCustomKeyStore 操作。 **CustomKeyStoreInvalidStateException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。
不可重试	**UnsupportedOperationException** 有关问题排查帮助，请参阅外部密钥的加密操作错误。	**XksKeyInvalidResponseException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。
不可重试	**ValidationException** 有关问题排查帮助，请参阅代理问题。	**XksProxyInvalidResponseException** 响应 CreateCustomKeyStore 和 UpdateCustomKeyStore 操作。 **CustomKeyStoreInvalidStateException** 响应 CreateKey 操作。 **KMSInvalidStateException** 响应加密操作。

错误类型	图表中显示的异常	AWS KMS 向您返回的异常
可重试	**XksProxyUnreachableException** 如果您反复看到此错误，请验证您的外部密钥存储代理是否处于活动状态并已连接到网络，以及其在外部密钥存储中的 URI 路径和端点 URI 或 VPC 服务名称是否正确。	**XksProxyUriUnreachableException** 响应 `CreateCustomKeyStore` 和 `UpdateCustomKeyStore` 操作。 **CustomKeyStoreInvalidStateException** 响应 `CreateKey` 操作。 **KMSInvalidStateException** 响应加密操作。

前 5 个异常图表派生自 XksProxyErrors 指标。当您查看特定数据点时，弹出窗口会显示 `ExceptionName` 维度的值以及在该数据点记录的异常的次数。五个列表项按最常见的异常到最少见的异常顺序排列。

我们建议使用该XksProxyErrors指标创建 CloudWatch 警报，通过在一分钟内记录超过五个不可重试的错误时提醒您潜在的配置问题。有关更多信息，请参阅 为不可重试的错误创建 Amazon CloudWatch 警报。

证书过期天数

距离您的外部密钥存储代理端点（`XksProxyUriEndpoint`）的 TLS 证书过期的天数。使用此图表监控即将过期的 TLS 证书。

证书过期后，AWS KMS 将无法与外部密钥存储代理通信。在您续订证书之前，外部密钥存储中所有受 KMS 密钥保护的数据都将不可访问。

距离证书过期的天数图表派生自 XksProxyCertificateDaysToExpire 指标。我们强烈建议您使用此指标来创建 CloudWatch 警报，通知您即将到期。证书过期可能会影响您访问加密资源。设置警报，让您的组织有时间在证书过期之前续订证书。有关更多信息，请参阅 为证书到期创建 Amazon CloudWatch 警报。

设置警报

监控部分中的图表概述了给定时间段内外部密钥存储和外部密钥存储中 KMS 密钥的运行状况。但是，您可以根据外部密钥存储指标创建 Amazon CloudWatch 警报，以便在指标值超过您指定的阈值时通

知您。警报可以将消息发送到 Amazon Simple Notification Service（Amazon SNS）主题或 Amazon EC2 Auto Scaling 策略。有关 CloudWatch 警报的详细信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch 警报。

在创建亚马逊 CloudWatch 警报之前，您需要一个亚马逊 SNS 主题。有关详情，请参阅亚马逊 CloudWatch 用户指南中的创建 Ama zon SNS 主题。

主题

- 为证书到期创建 Amazon CloudWatch 警报
- 为响应超时创建 Amazon CloudWatch 警报
- 为可重试的错误创建 Amazon CloudWatch 警报
- 为不可重试的错误创建 Amazon CloudWatch 警报

为证书到期创建 Amazon CloudWatch 警报

此警报使用AWS KMS发布到的XksProxyCertificateDaysToExpire指标 CloudWatch 来记录与您的外部密钥存储代理端点关联的 TLS 证书的预期到期时间。您无法为账户中的所有外部密钥存储创建单个警报，也无法为将来可能会创建的外部密钥存储创建警报。

我们建议将警报设置为在证书将要过期的前 10 天提醒您，但您应设置最适合您需求的阈值。

创建警报

使用以下必填值按照基于静态阈值创建 CloudWatch 警报中的说明进行操作。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
选择指标	选择 KMS，然后选择 XKS Proxy Certificate Metrics（XKS 代理证书指标）。 选中要监控的 `XksProxyCertificateName` 旁的复选框。 然后选择 Select metric（选择指标）。
Statistic	最低
周期	5 分钟
阈值类型	静态

Field	Value
当 ...	无论何时`Lower`都XksProxyCertificateDaysToExpire是`10`。

为响应超时创建 Amazon CloudWatch 警报

此警报使用AWS KMS发布 CloudWatch到的XksProxyLatency指标来记录外部密钥存储代理响应请求所花费的毫秒数。AWS KMS您无法为账户中的所有外部密钥存储创建单个警报，也无法为将来可能会创建的外部密钥存储创建警报。

AWS KMS 希望外部密钥存储代理在 250 毫秒内响应每个请求。我们建议设置警报，以在外部密钥存储代理响应时间超过 200 毫秒时提醒您，但您应该设置最适合您需求的阈值。

创建警报

使用以下必填值按照基于静态阈值创建 CloudWatch 警报中的说明进行操作。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
选择指标	选择 KMS，然后选择 XKS Proxy Latency Metrics（XKS 代理延迟指标）。 选中要监控的 `KmsOperation` 旁的复选框。 然后选择 Select metric（选择指标）。
Statistic	平均值
周期	5 分钟
阈值类型	静态
当 ...	无论何时`Greater`都XksProxyLatency是`200`。

为可重试的错误创建 Amazon CloudWatch 警报

此警报使用AWS KMS发布到的XksProxyErrors指标 CloudWatch 来记录与您的外部密钥存储代理AWS KMS请求相关的异常数量。您无法为账户中的所有外部密钥存储创建单个警报，也无法为将来可能会创建的外部密钥存储创建警报。

可重试错误会降低您的可靠性百分比，并可能表示网络错误。我们建议设置警报，以在一分钟内记录超过五个可重试错误时提醒您，但您应该设置最适合您需求的阈值。

使用以下必填值按照基于静态阈值创建 CloudWatch 警报中的说明进行操作。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
选择指标	选择 Query（查询）选项卡。 对于 Namespace（命名空间），选择 AWS/KMS。 对于 Metric name（指标名称），输入 SUM(XksProxyErrors) 。 对于 Filter by（筛选条件），输入 ErrorType = Retryable 。 选择运行。然后选择 Select metric（选择指标）。
标签	#####
周期	1 minute
阈值类型	静态
当 ...	每当 q1 Greater 5 时。

为不可重试的错误创建 Amazon CloudWatch 警报

此警报使用AWS KMS发布到的XksProxyErrors指标 CloudWatch 来记录与您的外部密钥存储代理AWS KMS请求相关的异常数量。您无法为账户中的所有外部密钥存储创建单个警报，也无法为将来可能会创建的外部密钥存储创建警报。

不可重试错误可能表示您的外部密钥存储的配置存在问题。我们建议设置警报，以在一分钟内记录超过五个不可重试错误时提醒您，但您应该设置最适合您需求的阈值。

使用以下必填值按照基于静态阈值创建 CloudWatch 警报中的说明进行操作。对于其他字段，请接受默认值并按要求提供名称。

Field	Value
选择指标	选择 Query（查询）选项卡。 对于 Namespace（命名空间），选择 AWS/KMS。 对于 Metric name（指标名称），输入 SUM(XksProxyErrors) 。 对于 Filter by（筛选条件），输入 ErrorType = Non-retryable 。 选择运行。然后选择 Select metric（选择指标）。
标签	######
周期	1 minute
阈值类型	静态
当 ...	每当 q1 Greater 5 时。

连接和断开外部密钥存储

新外部密钥存储未连接。要在外部密钥存储中创建和使用 AWS KMS keys，您需要将外部密钥存储连接到其外部密钥存储代理。您可以随时连接和断开外部密钥存储，并查看其连接状态。

在外部密钥存储断开后，AWS KMS 无法与外部密钥存储代理通信。因此，您可以查看和管理外部密钥存储及其现有 KMS 密钥。不过，您不能在外部密钥存储中创建 KMS 密钥，也不能在加密操作中使用其 KMS 密钥。您可能需要在某些时候断开外部密钥存储的连接，例如编辑外部密钥存储的属性时，但要进行相应计划。断开密钥存储的连接可能会中断使用其 KMS 密钥的 AWS 服务的运行。

您无需连接外部密钥存储。您可以将外部密钥存储保持在无限期断开的状态并且仅在您需要使用它时进行连接。但是，您可能希望定期测试连接以验证设置是否正确以及自定义密钥存储是否可以连接。

当您断开自定义密钥存储时，密钥存储中的 KMS 密钥立即变得不可用（视最终一致性而定）。不过，在再次使用 KMS 密钥（例如解密数据密钥）之前，使用受 KMS 密钥保护的数据密钥加密的资源不会受到影响。此问题会影响 AWS 服务，因为许多服务使用数据密钥来保护您的资源。有关更多信息，请参阅 不可用的 KMS 密钥如何影响数据密钥。

> **Note**
>
> 仅当密钥存储从未连接或您明确断开密钥存储连接时，外部密钥存储才会具有 DISCONNECTED 状态。CONNECTED 状态并不表示外部密钥存储或其支持组件正在高效运行。有关外部密钥存储组件性能的信息，请参阅每个外部密钥存储详细信息页面 Monitoring（监控）部分中的图表。有关更多信息，请参阅 监控外部密钥存储。
>
> 您的外部密钥管理器可能会提供其他方法来停止和重新启动 AWS KMS 外部密钥存储代理与外部密钥存储代理之间或外部密钥存储代理与外部密钥管理器之间的通信。有关详细信息，请参阅外部密钥管理器的文档。

主题

连接外部密钥存储

外部密钥存储连接到其外部密钥存储代理后，您可以在外部密钥存储中创建 KMS 密钥，然后在加密操作中使用现有 KMS 密钥。

将外部密钥存储连接到其外部密钥存储代理的过程因外部密钥存储的连接而异。

- 当您将外部密钥存储与公共端点连接连接时，AWS KMS会向外部密钥存储代理发送GetHealthStatus 请求以验证代理 URI 端点、代理 URI 路径和代理身份验证凭据。来自代理的成功响应可确认代理 URI 端点和代理 URI 路径准确且可访问，并且代理对使用外部密钥存储的代理身份验证凭证签名的请求进行了身份验证。
- 在使用 VPC 端点服务连接将外部密钥存储连接到其外部密钥存储代理时，AWS KMS 会执行以下操作：
  - 确认代理 URI 端点中指定的私有 DNS 名称的域名已通过验证。
  - 创建从 AWS KMS VPC 到您 VPC 端点服务的接口端点。

- 为代理 URI 端点中指定的私有 DNS 名称创建私有托管区
- 向外部密钥存储代理发送GetHealthStatus请求。来自代理的成功响应可确认代理 URI 端点和代理 URI 路径准确且可访问，并且代理对使用外部密钥存储的代理身份验证凭证签名的请求进行了身份验证。

连接操作即开始连接您的自定义密钥存储的过程，但是将外部密钥存储连接到其外部代理大约需要五分钟。连接操作的成功响应并不表示外部密钥存储已连接。要确认连接是否成功，请使用AWS KMS控制台或DescribeCustomKeyStores操作查看外部密钥存储库的连接状态。

当连接状态为 FAILED 时，连接错误代码会显示在 AWS KMS 控制台中并添加到 DescribeCustomKeyStore 响应中。有关解释连接错误代码的帮助信息，请参阅 外部密钥存储的连接错误代码。

断开外部密钥存储

从外部密钥存储代理断开具有 VPC 端点服务连接的外部密钥存储时，AWS KMS 会删除其与 VPC 端点服务的接口端点，并移除其为支持连接而创建的网络基础设施。具有公有端点连接的外部密钥存储不需要等效流程。此操作不会影响 VPC 端点服务或其支持的任何组件，也不会影响外部密钥存储代理或任何外部组件。

外部密钥存储断开连接后，AWS KMS 不会向外部密钥存储代理发送任何请求。外部密钥存储的连接状态为 DISCONNECTED。已断开连接的外部密钥存储中的 KMS 密钥处于 UNAVAILABLE 密钥状态（除非处于待删除状态），这表示此类密钥不能用于加密操作。不过，您仍然可以查看和管理外部密钥存储及其现有 KMS 密钥。

已断开连接状态被设计为临时且可逆的状态。您可以随时重新连接外部密钥存储。通常无需重新配置。不过，如果关联的外部密钥存储代理的任何属性在断开连接时发生了变化，例如轮换了代理身份验证凭证，则必须在重新连接之前编辑外部密钥存储设置。

> **Note**
>
> 虽然自定义密钥存储已断开连接，但在自定义密钥存储中创建 KMS 密钥或在加密操作中使用现有 KMS 密钥的所有尝试都将失败。此操作可以阻止用户存储和访问敏感数据。

为了更好地估计断开外部密钥存储的影响，请在外部密钥存储中标识 KMS 密钥，并确定其过去的使用情况。

您可能出于以下原因断开外部密钥存储：

- 编辑其属性。在外部密钥存储处于连接状态时，您可以编辑自定义密钥存储名称、代理 URI 路径和代理身份验证凭证。不过，要编辑代理连接类型、代理 URI 端点或 VPC 端点服务名称，您必须先断开外部密钥存储的连接。有关更多信息，请参阅 编辑外部密钥存储属性。
- 停止 AWS KMS 和外部密钥存储代理之间的所有通信。您还可以通过禁用端点或 VPC 端点服务来停止 AWS KMS 与代理之间的通信。此外，您的外部密钥存储代理或密钥管理软件可能会提供其他机制，防止 AWS KMS 与代理进行通信或防止代理访问外部密钥管理器。
- 禁用外部密钥存储中的所有 KMS 密钥。您可以使用AWS KMS控制台或DisableKey操作在外部密钥存储中禁用和重新启用 KMS 密钥。这些操作会快速完成（视最终一致性而定），但一次只针对一个 KMS 密钥。断开外部密钥存储会将外部密钥存储中所有 KMS 密钥的密钥状态更改为 `Unavailable`，这将阻止在任何加密操作中使用这些 KMS 密钥。
- 修复失败的连接尝试。如果连接外部密钥存储的尝试失败（自定义密钥存储的连接状态为 `FAILED`），则必须在尝试再次连接外部密钥存储之前将其断开。

连接状态

连接和断开会改变自定义密钥存储的连接状态。AWS CloudHSM 密钥存储和外部密钥存储的连接状态值相同。

要查看自定义密钥库的连接状态，请使用DescribeCustomKeyStores操作或AWS KMS控制台。连接状态显示在每个自定义密钥存储表中、每个自定义密钥存储详细信息页面的 General configuration（常规配置）部分中，以及自定义密钥存储中 KMS 密钥 Cryptographic configuration（加密配置）选项卡上。有关详细信息，请参阅 查看 AWS CloudHSM 密钥存储 和 查看外部密钥存储。

自定义密钥存储可能具有以下连接状态之一：

- `CONNECTED`：自定义密钥存储已连接到其备用密钥存储。您可以在自定义密钥存储中创建和使用 KMS 密钥。

  AWS CloudHSM 密钥存储的备用密钥存储是其关联的 AWS CloudHSM 集群。外部密钥存储的备用密钥存储是外部密钥存储代理及其支持的外部密钥管理器。

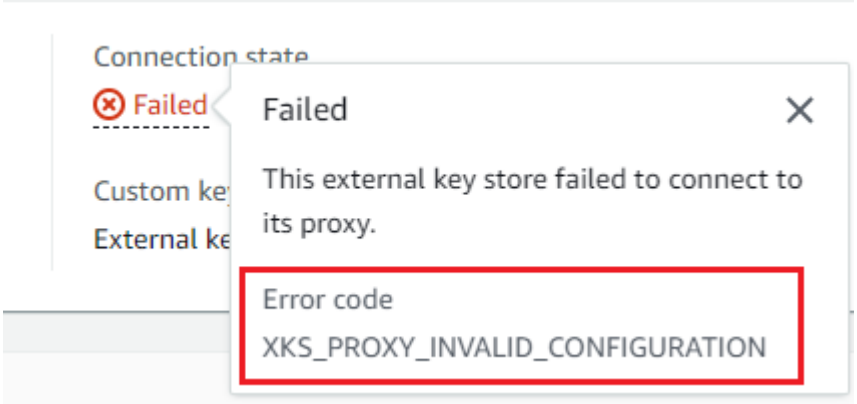
  CONNECTED（已连接）状态表示连接成功且自定义密钥存储未被故意断开。但该状态并不表示连接运行正常。有关与您的AWS CloudHSM密钥库关联的AWS CloudHSM集群状态的信息，请参阅AWS CloudHSM用户指南AWS CloudHSM中的获取 CloudWatch 指标。有关外部密钥存储的状态和操作的信息，请参阅每个外部密钥存储详细信息页面 Monitoring（监控）部分的图表。有关更多信息，请参阅 监控外部密钥存储。
- `CONNECTING`：连接自定义密钥存储的过程正在进行。这是一种暂时状态。

- DISCONNECTED：自定义密钥库从未与其后端连接过，或者使用AWS KMS控制台或DisconnectCustomKeyStore操作故意断开了连接。
- DISCONNECTING：断开自定义密钥存储的过程正在进行。这是一种暂时状态。
- FAILED：尝试连接自定义密钥存储失败。DescribeCustomKeyStores响应ConnectionErrorCode中的表示问题所在。

要连接自定义密钥存储，其连接状态必须为 DISCONNECTED。如果连接状态为 FAILED，则使用 ConnectionErrorCode 来识别和解决问题。接着断开自定义密钥存储，然后再尝试重新连接。如需帮助解决连接失败问题，请参阅 外部密钥存储连接错误。有关响应连接错误代码的帮助信息，请参阅外部密钥存储的连接错误代码。

要查看连接错误代码，请执行以下操作：

- 在DescribeCustomKeyStores响应中，查看ConnectionErrorCode元素的值。只有当 ConnectionState 为 FAILED 时，此元素才会出现在 DescribeCustomKeyStores 响应中。
- 要在 AWS KMS 控制台中查看连接错误代码，请将鼠标悬停在外部密钥存储详细信息页面的 Failed（失败）值上。



连接外部密钥存储（控制台）

您可以使用 AWS KMS 控制台将外部密钥存储连接到其外部密钥存储代理。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Custom key stores（自定义密钥存储）、External key stores（外部密钥存储）。

4. 选择要连接的外部密钥存储的行。

   如果外部密钥存储的连接状态为 FAILED（失败），则必须在连接之前断开外部密钥存储。

5. 从 Key store actions（密钥存储操作）菜单中选择 Connect（连接）。

该连接过程通常需要五分钟才能完成。操作完成后，连接状态更改为 CONNECTED（已连接）。

如果连接状态为 Failed（失败），请将鼠标悬停在连接状态上方以查看连接错误代码，从中了解错误的原因。有关响应连接错误代码的帮助信息，请参阅 外部密钥存储的连接错误代码。要连接处于 Failed（失败）连接状态的外部密钥存储，必须先断开自定义密钥存储。

连接外部密钥存储（API）

要连接已断开连接的外部密钥存储库，请使用ConnectCustomKeyStore操作。

在连接之前，外部密钥存储的连接状态必须为 DISCONNECTED。如果连接状态为 FAILED，请断开外部密钥存储，再进行连接。

该连接过程可能需要五分钟才能完成。除非该过程迅速失败，否则 ConnectCustomKeyStore 将返回 HTTP 200 响应和无属性的 JSON 对象。但是，此初始响应不指示连接是否成功。要确定外部密钥存储是否已连接，请查看DescribeCustomKeyStores响应中的连接状态。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

要确定外部密钥存储，请使用自定义密钥存储 ID。您可以在控制台的自定义密钥存储页面上或使用DescribeCustomKeyStores操作来找到 ID。在运行此示例之前，请将示例 ID 替换为有效的 ID。

```
$ aws kms connect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

ConnectCustomKeyStore 操作不会在响应中返回 ConnectionState。要验证外部密钥存储是否已连接，请使用DescribeCustomKeyStores操作。默认情况下，此操作将返回您的账户和区域中的所有自定义密钥存储。但您可以使用 CustomKeyStoreId 或 CustomKeyStoreName 参数（但不能同时使用两者）将响应限制到特定自定义密钥存储。ConnectionState 值为 CONNECTED 表示外部密钥存储已连接到其外部密钥存储代理。

```
$ 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"
      }
    }
  ]
}
```

如果 DescribeCustomKeyStores 响应中的 ConnectionState 值为 FAILED，则该 ConnectionErrorCode 元素指示失败的原因。

在以下示例中，ConnectionErrorCode 的 XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND 值表示 AWS KMS 找不到用于与外部密钥存储代理通信的 VPC 端点服务。验证 XksProxyVpcEndpointServiceName 是否正确无误，AWS KMS 服务主体是否是 Amazon VPC 端点服务允许的主体，以及 VPC 端点服务是否不要求接受连接请求。有关响应连接错误代码的帮助信息，请参阅 外部密钥存储的连接错误代码。

```
$ 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"
      }
```

```
    }
  ]
}
```

断开外部密钥存储（控制台）

您可以使用 AWS KMS 控制台将外部密钥存储连接到其外部密钥存储代理。完成此过程大约需要 5 分钟。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Custom key stores（自定义密钥存储）、External key stores（外部密钥存储）。
4. 选择要断开连接的外部密钥存储的行。
5. 从 Key store actions（密钥存储操作）菜单中选择 Disconnect（断开连接）。

当操作完成时，连接状态将从 DISCONNECTING 变为 DISCONNECTED。如果操作失败，则会出现一条错误消息，描述问题并提供有关如何修复它的帮助。如果您需要更多帮助，请参阅外部密钥存储连接错误。

断开外部密钥存储（API）

要断开连接的外部密钥存储库，请使用DisconnectCustomKeyStore操作。如果此操作成功，则 AWS KMS 返回 HTTP 200 响应和无属性的 JSON 对象。该过程可能需要五分钟才能完成。要查找外部密钥存储库的连接状态，请使用DescribeCustomKeyStores操作。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

此示例断开具有 VPC 端点服务连接的外部密钥存储。在运行此示例之前，请将示例自定义密钥存储 ID 替换为有效 ID。

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

要验证外部密钥存储是否已断开连接，请使用DescribeCustomKeyStores操作。默认情况下，此操作将返回您的账户和区域中的所有自定义密钥存储。但您可以使用 `CustomKeyStoreId` 和 `CustomKeyStoreName` 参数（但不能同时使用两者）将响应限制到特定自定义密钥存

储。DISCONNECTED 的 ConnectionState 值表示此示例外部密钥存储不再连接到其外部密钥存储代理。

```
$ 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"
      }
    }
  ]
}
```

删除外部密钥存储

删除外部密钥存储时，AWS KMS 会从 AWS KMS 中删除有关外部密钥存储的所有元数据，包括有关其外部密钥存储代理的信息。此操作不会影响外部密钥存储代理、外部密钥管理器、外部密钥或您为支持外部密钥存储而创建的任何 AWS 资源，例如 Amazon VPC 或 VPC 端点服务。

在删除外部密钥存储之前，必须从密钥存储中删除所有 KMS 密钥，并从其外部密钥存储代理断开密钥存储。否则，尝试删除密钥存储将失败。

删除外部密钥存储是不可逆的操作，但您可以创建新的外部密钥存储并将其与同一个外部密钥存储代理和外部密钥管理器相关联。不过，即使可以访问相同的外部密钥材料，您也无法在外部密钥存储中重新创建对称加密 KMS 密钥。AWS KMS 在每个 KMS 密钥独有的对称加密文字中包含元数据。此安全功能确保只有加密数据的 KMS 密钥才能解密数据。

与其删除外部密钥存储，不如考虑断开连接。在外部密钥存储断开连接后，您可以管理外部密钥存储及其 AWS KMS keys，但无法在外部密钥存储中创建或使用 KMS 密钥。您可以随时重新连接外部密钥存储并恢复使用其 KMS 密钥来加密和解密数据。我们不对已断开连接的外部密钥存储代理或其不可用的 KMS 密钥收取任何费用。

主题

删除外部密钥存储中（控制台）

您可以使用 AWS KMS 控制台删除外部密钥存储。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Custom key stores（自定义密钥存储）、External key stores（外部密钥存储）。
4. 找到表示要删除的外部密钥存储的行。如果外部密钥存储的 Connection state（连接状态）不是 DISCONNECTED（已断开连接），则必须断开外部密钥存储，然后才能将其删除。
5. 从 Key store actions（密钥存储操作）菜单中选择 Delete（删除）。

在操作完成后，会显示一条成功消息，并且外部密钥存储不再显示在密钥存储列表中。如果操作失败，则会显示一条错误消息，描述问题并提供有关如何解决该问题的帮助。如果您需要更多帮助，请参阅排查外部密钥存储的问题。

删除外部密钥存储中（API）

要删除外部密钥存储库，请使用DeleteCustomKeyStore操作。如果此操作成功，则 AWS KMS 返回 HTTP 200 响应和无属性的 JSON 对象。

首先，断开外部密钥存储的连接。在运行此命令之前，请将示例自定义密钥存储 ID 替换为有效 ID。

```
$ aws kms disconnect-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

断开外部密钥存储后，您可以使用该DeleteCustomKeyStore操作将其删除。

```
$ aws kms delete-custom-key-store --custom-key-store-id cks-1234567890abcdef0
```

要确认外部密钥存储已删除，请使用DescribeCustomKeyStores操作。

```
$ aws kms describe-custom-key-stores
```

```
{
    "CustomKeyStores": []
}
```

如果指定的自定义密钥存储名称或 ID 已不存在，AWS KMS 则会返回 `CustomKeyStoreNotFoundException` 异常。

```
$ aws kms describe-custom-key-stores --custom-key-store-id cks-1234567890abcdef0

An error occurred (CustomKeyStoreNotFoundException) when calling the
 DescribeCustomKeyStore operation:
```

在外部密钥存储中管理 KMS 密钥

若要在外部密钥存储中创建、查看、管理、使用和计划删除 KMS 密钥，您使用的过程与用于其他 KMS 密钥的过程非常相似。但是，在外部密钥存储中创建 KMS 密钥时，您需要指定外部密钥存储和外部密钥。在外部密钥存储中使用 KMS 密钥时，外部密钥管理器将使用指定的外部密钥执行加密和解密操作。

AWS KMS 无法在外部密钥管理器中创建、查看、更新或删除任何加密密钥。AWS KMS 绝不会直接访问您的外部密钥管理器或任何外部密钥。所有加密操作请求均由您的外部密钥存储代理调解。若要在外部密钥存储中使用 KMS 密钥，必须先将托管 KMS 密钥的外部密钥存储连接到其外部密钥存储代理。

支持的功能

除了此部分中讨论的过程之外，您还可以使用外部密钥存储中的 KMS 密钥执行下列操作：

- 使用密钥策略、IAM policy 和授权以控制对 KMS 密钥的访问。
- 启用和禁用 KMS 密钥。这些操作不会影响外部密钥管理器中的外部密钥。
- 分配标签并创建别名，然后使用基于属性的访问权限控制（ABAC）授予对 KMS 密钥的访问权限。
- 将 KMS 密钥和与 AWS KMS 集成的 AWS 服务 结合使用并支持客户托管密钥。

不支持的功能

- 外部密钥存储仅支持对称加密 KMS 密钥。您无法在外部密钥存储中创建 HMAC KMS 密钥或非对称 KMS 密钥。
- GenerateDataKeyPair外部GenerateDataKeyPairWithoutPlaintext密钥存储库中的 KMS 密钥不支持和。
- 您不能使用 AWS CloudFormation 模板创建外部密钥存储或在外部密钥存储中创建 KMS 密钥。

- 外部密钥存储不支持多区域密钥。
- 外部密钥存储不支持拥有导入密钥材料的 KMS 密钥。
- 外部密钥存储中的 KMS 密钥不支持自动密钥轮换。

主题

在外部密钥存储中创建 KMS 密钥

在创建并连接外部密钥存储后，您可以在密钥存储中创建 AWS KMS keys。它们必须是源值为外部密钥存储（EXTERNAL_KEY_STORE）的对称加密 KMS 密钥。您不能在自定义密钥存储中创建非对称 KMS 密钥、HMAC KMS 密钥或具有导入的密钥材料的 KMS 密钥。此外，您不能在自定义密钥存储中使用对称加密 KMS 密钥来生成非对称数据密钥对。

与标准 KMS 密钥相比，外部密钥存储中 KMS 密钥的延迟、耐久性和可用性可能较差，因为这些密钥依赖位于 AWS 外部的组件。在外部密钥存储中创建或使用 KMS 密钥之前，请验证您是否需要具有外部密钥存储属性的密钥。

> **Note**
>
> 一些外部密钥管理器为在外部密钥存储中创建 KMS 密钥提供了更简单的方法。有关详细信息，请参阅外部密钥管理器的文档。

若要在外部密钥存储中创建 KMS 密钥，请指定以下内容：

- 外部密钥存储的 ID。
- 外部密钥存储（EXTERNAL_KEY_STORE）的密钥材料源。
- 与外部密钥存储关联的外部密钥管理器中现有外部密钥的 ID。此外部密钥用作 KMS 密钥的密钥材料。创建 KMS 密钥后，您无法更改外部密钥 ID。

  AWS KMS 在请求加密和解密操作时为外部密钥存储代理提供外部密钥 ID。AWS KMS 无法直接访问您的外部密钥管理器或其任何加密密钥。

除了外部密钥，外部密钥存储中的 KMS 密钥还具有 AWS KMS 密钥材料。使用 KMS 密钥加密的所有数据首先使用密钥的 AWS KMS 密钥材料在 AWS KMS 中加密，再由您的外部密钥管理器使用外部密钥进行加密。这种双重加密过程可确保外部密钥存储中受 KMS 密钥保护的加密文字至少与仅受 AWS KMS 保护的加密文字一样强大。有关更多信息，请参阅 外部密钥存储的工作原理。

CreateKey 操作成功后，新 KMS 密钥的密钥状态为 Enabled。在外部密钥存储中查看 KMS 密钥时，您可以看到典型属性，例如其密钥 ID、密钥规格、密钥用法、密钥状态以及创建日期。但是您也可以看到外部密钥存储的 ID 和连接状态以及外部密钥的 ID。

如果您在外部密钥存储中创建 KMS 密钥的尝试失败，请查看错误消息以确定原因。错误消息可能表明外部密钥存储未连接（CustomKeyStoreInvalidStateException），您的外部密钥存储代理无法找到具有指定外部密钥 ID（XksKeyNotFoundException）的外部密钥，或者外部密钥已与同一外部密钥存储 XksKeyAlreadyInUseException 中的 KMS 密钥相关联。

.

有关在外部密钥存储中创建 KMS 密钥的操作的 AWS CloudTrail 日志示例，请参阅 CreateKey。

主题

- 外部密钥存储中 KMS 密钥的要求
- 在外部密钥存储中创建 KMS 密钥（控制台）
- 在外部密钥存储中创建 KMS 密钥（AWS KMS API）

外部密钥存储中 KMS 密钥的要求

若要在外部密钥存储中创建 KMS 密钥，外部密钥存储、KMS 密钥和用作 KMS 密钥外部加密密钥材料的外部密钥需要具有以下属性。

外部密钥存储要求

- 必须连接到其外部密钥存储代理。

  若要查看外部密钥存储的连接状态，请参阅 查看外部密钥存储。若要连接外部密钥存储，请参阅 连接和断开外部密钥存储。

KMS 密钥要求

创建 KMS 密钥后，您无法更改这些属性。

- 密钥规范：SYMMETRIC_DEFAULT
- 密钥用法：ENCRYPT_DECRYPT
- 密钥材料源：EXTERNAL_KEY_STORE
- 多区域：FALSE

外部密钥要求

- 256 位 AES 加密密钥（256 个随机位）。KeySpec 的外部密钥必须是 AES_256。
- 已启用并可供使用。Status 的外部密钥必须是 ENABLED。
- 已配置以进行密钥和解密。KeyUsage 的外部密钥必须包含 ENCRYPT 和 DECRYPT。
- 仅与此 KMS 密钥结合使用。外部密钥存储中的每个 KMS key 都必须与不同的外部密钥关联。

  AWS KMS 还建议将外部密钥专门用于外部密钥存储。此限制更易于识别和解决密钥问题。
- 可由外部密钥存储的外部密钥存储代理访问。

  如果外部密钥存储代理无法使用指定的外部密钥 ID 找到密钥，则 CreateKey 操作将失败。
- 可以处理您使用 AWS 服务 产生的预期流量。AWS KMS 建议准备好外部密钥以每秒处理多达 1800 个请求。

在外部密钥存储中创建 KMS 密钥（控制台）

有两种方法可以在外部密钥存储中创建 KMS 密钥。

- 方法 1（推荐）：选择外部密钥存储，然后在该外部密钥存储中创建 KMS 密钥。
- 方法 2：创建 KMS 密钥，然后指明该密钥在外部密钥存储中。

如果您使用方法 1，在创建密钥之前选择了外部密钥存储，AWS KMS 将为您选择所有必需的 KMS 密钥属性并填写外部密钥存储的 ID。此方法可让您避免在创建 KMS 密钥时可能犯的错误。

> **Note**
>
> 不要在别名、描述或标签中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

方法 1（推荐）：在外部密钥存储中开始

若要使用此方法，请选择您的外部密钥存储，然后创建 KMS 密钥。AWS KMS 控制台为您选择所有必需属性并填写外部密钥存储的 ID。此方法可让您避免在创建 KMS 密钥时可能犯的许多错误。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Custom key stores（自定义密钥存储）、External key stores（外部密钥存储）。
4. 选择外部密钥存储的名称。
5. 在右上角，选择 Create a KMS key in this key store（在此密钥存储中创建 KMS 密钥）。

   如果未连接外部密钥存储，系统将提示您将其连接。如果连接尝试失败，则需要解决问题并连接外部密钥存储，然后才能在其中创建新的 KMS 密钥。

   如果已连接外部密钥存储，您将被重定向到 Customer managed keys（客户托管密钥）页面以创建密钥。已为您选择了必需的 Key configuration（密钥配置）值。此外，外部密钥存储的自定义密钥存储 ID 已填写，但您可以对其进行更改。
6. 在外部密钥管理器中输入外部密钥的密钥 ID。此外部密钥必须满足与 KMS 密钥一起使用的要求。创建 KMS 密钥后，您无法更改此值。

   如果外部密钥有多个 ID，请输入外部密钥存储代理用于识别外部密钥的密钥 ID。
7. 请确认您打算在指定的外部密钥存储中创建 KMS 密钥。
8. 请选择 Next（下一步）。

   此过程的其余步骤与创建标准 KMS 密钥的步骤相同。
9. 为 KMS 密钥键入别名（必需）和描述（可选）。
10. （可选）。在 Add Tags（添加标签）页面上，添加标识或分类 KMS 密钥的标签。

    在将标签添加到 AWS 资源时，AWS 可生成成本分配报告，其中按标签汇总了使用情况和成本。标签还可以用来控制对 KMS 密钥的访问。有关轮换 KMS 密钥的信息，请参阅 标记密钥 和 AWS KMS 中的 ABAC。
11. 请选择 Next（下一步）。
12. 在 Key Administrators（密钥管理员）部分中，选择可管理 KMS 密钥的 IAM 用户和角色。有关更多信息，请参阅允许密钥管理员管理 KMS 密钥。

> **Note**
>
> IAM 策略可以向其他 IAM 用户和角色授予使用 KMS 密钥的权限。
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

13. （可选）要阻止这些密钥管理员删除此 KMS 密钥，请清除 Allow key administrators to delete this key（允许密钥管理员删除此密钥）复选框。

    删除 KMS 密钥是一种具有破坏性且不可撤销的操作，将导致加密文字不可恢复。即使您拥有外部密钥材料，也无法在外部密钥存储中重新创建对称 KMS 密钥。但是，删除 KMS 密钥会影响关联的外部密钥。有关从外部密钥存储中删除 KMS 密钥的信息，请参阅 计划从外部密钥存储删除 KMS 密钥。

14. 请选择 Next（下一步）。

15. 在 This account（此账户）部分中，选择此 AWS 账户 中可以在加密操作中使用 KMS 密钥的 IAM 用户和角色。有关更多信息，请参阅允许密钥用户使用 KMS 密钥。

> **Note**
>
> IAM policy 可以向其他 IAM 用户和角色授予使用 KMS 密钥的权限。
> IAM 最佳实践不鼓励使用具有长期凭证的 IAM 用户。而应尽可能使用提供临时凭证的 IAM 角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 安全最佳实践。

16. （可选）您可以允许其他 AWS 账户 将此 KMS 密钥用于加密操作。为此，请在页面底部的 Other AWS 账户（其他 Amazon Web Services 账户）部分中，选择 Add another AWS 账户（添加另一个 Amazon Web Services 账户）并输入外部账户的 AWS 账户 ID。要添加多个外部账户，请重复此步骤。

> **Note**
>
> 其他 AWS 账户 的管理员还必须为其用户创建 IAM policy，以允许访问此 KMS 密钥。有关更多信息，请参阅 允许其他账户中的用户使用 KMS 密钥。

17. 选择 下一步。

18. 检视您选择的密钥设置。您仍然可以返回并更改所有设置。

19. 完成后，选择 Finish（完成）以创建密钥。

方法 2：在客户托管密钥中开始

此过程与使用 AWS KMS 密钥材料创建对称加密密钥的过程相同。但是，在此过程中，您需要指定外部密钥存储的自定义密钥存储 ID 和外部密钥的密钥 ID。您还必须为外部密钥存储中的 KMS 密钥指定必需的属性值，例如密钥规格和密钥用法。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择 Create key。
5. 选择 Symmetric (对称)。
6. 在 Key usage（密钥用法）中，已为您选择了 Encrypt and decrypt（加密和解密）选项。请勿对其进行更改。
7. 选择 Advanced options (高级选项)。
8. 对于 Key material origin（密钥材料源），选择 External key store（外部密钥存储）。
9. 请确认您打算在指定的外部密钥存储中创建 KMS 密钥。
10. 请选择 Next（下一步）。
11. 请选择代表新 KMS 密钥外部密钥存储的行。

    您无法选择已断开连接的外部密钥存储。若要连接已断开连接的密钥存储，请选择密钥存储名称，然后从 Key store actions（密钥存储操作）中选择 Connect（连接）。有关更多信息，请参阅 连接外部密钥存储（控制台）。
12. 在外部密钥管理器中输入外部密钥的密钥 ID。此外部密钥必须满足与 KMS 密钥一起使用的要求。创建 KMS 密钥后，您无法更改此值。

    如果外部密钥有多个 ID，请输入外部密钥存储代理用于识别外部密钥的密钥 ID。
13. 请选择 Next（下一步）。

    此过程的其余步骤与创建标准 KMS 密钥的步骤相同。
14. 为 KMS 密钥键入别名和可选的描述。
15. （可选）。在 Add Tags（添加标签）页面上，添加标识或分类 KMS 密钥的标签。

    在将标签添加到 AWS 资源时，AWS 可生成成本分配报告，其中按标签汇总了使用情况和成本。标签还可以用来控制对 KMS 密钥的访问。有关轮换 KMS 密钥的信息，请参阅 标记密钥 和 AWS KMS 中的 ABAC。

16. 请选择 Next（下一步）。
17. 在 Key Administrators（密钥管理员）部分中，选择可管理 KMS 密钥的 IAM 用户和角色。有关更多信息，请参阅允许密钥管理员管理 KMS 密钥。

> **Note**
>
> IAM 策略可以向其他 IAM 用户和角色授予使用 KMS 密钥的权限。

18. （可选）要阻止这些密钥管理员删除此 KMS 密钥，请清除 Allow key administrators to delete this key（允许密钥管理员删除此密钥）复选框。

    删除 KMS 密钥是一种具有破坏性且不可撤销的操作，将导致加密文字不可恢复。即使您拥有外部密钥材料，也无法在外部密钥存储中重新创建对称 KMS 密钥。但是，删除 KMS 密钥会影响关联的外部密钥。有关从外部密钥存储中删除 KMS 密钥的信息，请参阅 计划从外部密钥存储删除 KMS 密钥。
19. 请选择 Next（下一步）。
20. 在 This account（此账户）部分中，选择此 AWS 账户 中可以在加密操作中使用 KMS 密钥的 IAM 用户和角色。有关更多信息，请参阅允许密钥用户使用 KMS 密钥。

> **Note**
>
> IAM policy 可以向其他 IAM 用户和角色授予使用 KMS 密钥的权限。

21. （可选）您可以允许其他 AWS 账户 将此 KMS 密钥用于加密操作。为此，请在页面底部的 Other AWS 账户（其他 Amazon Web Services 账户）部分中，选择 Add another AWS 账户（添加另一个 Amazon Web Services 账户）并输入外部账户的 AWS 账户 ID。要添加多个外部账户，请重复此步骤。

> **Note**
>
> 其他 AWS 账户 的管理员还必须为其用户创建 IAM policy，以允许访问此 KMS 密钥。有关更多信息，请参阅 允许其他账户中的用户使用 KMS 密钥。

22. 选择 下一步。
23. 检视您选择的密钥设置。您仍然可以返回并更改所有设置。
24. 完成后，选择 Finish（完成）以创建密钥。

该过程成功后，显示内容将在您选择的外部密钥存储中显示新 KMS 密钥。选择新 KMS 密钥的名称或别名时，其详细信息页面上的 Cryptographic configuration（加密配置）选项卡会显示 KMS 密钥的源 [External key store（外部密钥存储）]，自定义密钥存储的名称、ID 和类型，以及外部密钥的 ID、密钥用法和状态。如果此过程失败，则会出现一条描述失败的错误消息。对于 ，请参阅 排查外部密钥存储的问题。

> **Tip**
>
> 若要更轻松地识别自定义密钥存储中的 KMS 密钥，请在 Customer managed keys（客户托管密钥）页面上，将 Origin（源）和 Custom key store ID（自定义密钥存储 ID）列添加到显示中。若要更改表格字段，请选择页面右上角的齿轮图标。有关更多信息，请参阅 自定义您的 KMS 密钥表。

在外部密钥存储中创建 KMS 密钥（AWS KMS API）

要在外部密钥存储中创建新的 KMS 密钥，请使用CreateKey操作。以下参数为必需参数：

- `Origin` 值必须为 `EXTERNAL_KEY_STORE`。
- `CustomKeyStoreId` 参数标识您的外部密钥存储。指定外部密钥存储的 `ConnectionState` 必须是 `CONNECTED`。若要找到 `CustomKeyStoreId` 和 `ConnectionState`，请使用 `DescribeCustomKeyStores` 操作。
- `XksKeyId` 参数标识外部密钥。此外部密钥必须满足与 KMS 密钥关联的要求。

您也可以使用 `CreateKey` 操作的任何可选参数，例如使用 `Policy` 或 Tags（标签）参数。

> **Note**
>
> 不要在 `Description` 或 `Tags` 字段中包含机密或敏感信息。这些字段可能以纯文本形式出现在 CloudTrail 日志和其他输出中。

本部分中的示例使用 AWS Command Line Interface (AWS CLI)，但您可以使用任何受支持的编程语言。

此示例命令使用该CreateKey操作在外部密钥存储中创建 KMS 密钥。响应包括 KMS 密钥的属性、外部密钥存储的 ID 以及外部密钥的 ID、用法和状态。有关这些字段的详细信息，请参阅 在外部密钥存储中查看 KMS 密钥。

在运行此命令之前，请将示例自定义密钥存储 ID 替换为有效的 ID。

```
$ 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"
    }
  }
}
```

在外部密钥存储中查看 KMS 密钥

要查看外部密钥存储库中的 KMS 密钥，请使用AWS KMS控制台或DescribeKey操作。您可以使用用于查看任何 AWS KMS 客户托管密钥的相同方法。要了解基本知识，请参阅查看密钥。

在 AWS KMS 控制台中，Customer managed keys（客户托管密钥）页面会显示外部密钥存储中的 KMS 密钥以及 AWS 账户 和区域中的所有其他客户托管密钥。若要识别外部密钥存储中的 KMS 密钥，请按独特的源值、External key store（外部密钥存储）和自定义密钥存储 ID 进行筛选。

有关更多信息，请参阅 查看外部密钥存储、监控外部密钥存储 和 使用记录 AWS KMS API 调用 AWS CloudTrail。

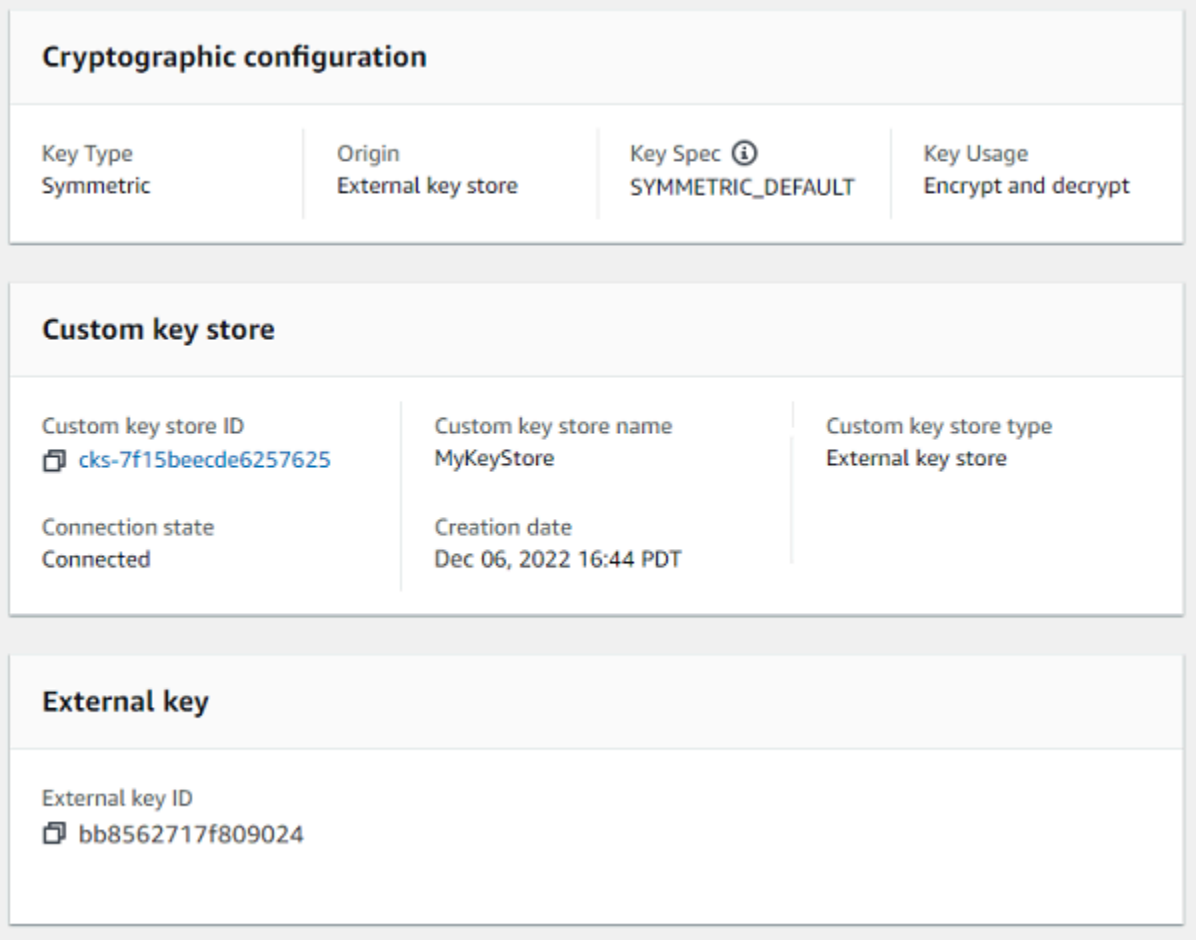
主题

- 外部密钥存储中的 KMS 密钥属性
- 在外部密钥存储中查看 KMS 密钥（控制台）
- 在外部密钥存储中查看 KMS 密钥（AWS KMS API）

外部密钥存储中的 KMS 密钥属性

与所有 KMS 密钥一样，外部密钥存储中的 KMS 密钥具有密钥 ARN、密钥规范和密钥用法值，但是这些密钥也具有特定于外部密钥存储中 KMS 密钥的属性和属性值。例如，外部密钥存储中所有 KMS 密钥的 Origin（源）值均为 External key store（外部密钥存储）。

对于外部密钥存储中的 KMS 密钥，AWS KMS 控制台中的 Cryptographic configuration（加密配置）选项卡包括另外两个部分：Custom key store（自定义密钥存储）和 External key（外部密钥）。



自定义密钥存储属性

以下值显示在 “加密配置” 选项卡的 “自定义密钥库” 部分和DescribeKey响应中。这些属性适用于所有自定义密钥存储，包括 AWS CloudHSM 密钥存储和外部密钥存储。

自定义密钥存储 ID

AWS KMS 分配给自定义密钥存储的唯一 ID。

自定义密钥存储名称

在创建自定义密钥存储时为其分配的易记名称。您可以随时更改此值。

自定义密钥存储类型

自定义密钥存储的类型。有效值为 AWS CloudHSM（`AWS_CLOUDHSM`）或外部密钥存储（`EXTERNAL_KEY_STORE`）。创建自定义密钥存储后无法更改其类型。

创建日期

创建自定义密钥存储的日期。此日期显示为 AWS 区域 的本地时间。

连接状态

表示自定义密钥存储已连接到其备用密钥存储。仅当自定义密钥存储从未连接到其备用密钥存储或故意断开连接时，连接状态才会为 `DISCONNECTED`。有关更多信息，请参阅 the section called “连接状态”。

外部密钥属性

外部密钥属性显示在加密配置选项卡的外部密钥部分和DescribeKey响应的`XksKeyConfiguration`元素中。

External key（外部密钥）部分出现在 AWS KMS 控制台中，仅适用于外部密钥存储中的 KMS 密钥。此部分提供有关与 KMS 密钥关联的外部密钥的信息。外部密钥是 AWS 外部的加密密钥，用作外部密钥存储中 KMS 密钥的密钥材料。使用 KMS 密钥加密或解密时，将由外部密钥管理器使用指定的外部密钥执行此操作。

以下值显示在 External key（外部密钥）部分中。

外部密钥 ID

外部密钥管理器中外部密钥的标识符。这是外部密钥存储代理用来识别外部密钥的值。外部密钥 ID 在您创建 KMS 密钥时指定，并且无法更改。如果您用于创建 KMS 密钥的外部密钥 ID 值更改或失效，则必须安排删除 KMS 密钥，并使用正确的外部密钥 ID 值创建新的 KMS 密钥。

在外部密钥存储中查看 KMS 密钥（控制台）

在外部密钥存储中查看 KMS 密钥（控制台）

1. 从 https://console.aws.amazon.com/kms 打开 AWS KMS 控制台。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 若要在外部密钥存储中识别 KMS 密钥，请将 Origin（源）和 Custom key store ID（自定义密钥存储 ID）字段添加到密钥表中。任何外部密钥存储中的 KMS 密钥均具有 External key store（外部密钥存储）的 Origin（源）值。

   在右上角，选择齿轮图标，选择 Origin（源）和 Custom key store ID（自定义密钥存储 ID），然后选择 Confirm（确认）。
5. 在外部密钥存储中选择 KMS 密钥的别名或密钥 ID。
6. 若要在外部密钥存储中查看特定于 KMS 密钥的属性，选择 Cryptographic configuration（加密配置）选项卡。外部密钥存储中 KMS 密钥的特殊值显示在 Custom key store（自定义密钥存储）和 External key（外部密钥）部分中。

在外部密钥存储中查看 KMS 密钥（AWS KMS API）

在外部密钥存储中查看 KMS 密钥（API）

您可以使用相同的 AWS KMS API 操作在外部密钥存储中查看用于任何 KMS 密钥（包括ListKeysDescribeKey、和）的 KMS 密钥GetKeyPolicy。例如，AWS CLI 中的以下 `describe-key` 操作显示外部密钥存储中 KMS 密钥的特殊字段。在运行与此类似的命令之前，请将示例 KMS 密钥 ID 替换为有效值。

```
$ 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"
    }
  }
}
```

在外部密钥存储中使用 KMS 密钥

在外部密钥存储中创建对称加密 KMS 密钥后，您可以将其用于以下加密操作：

- Encrypt
- Decrypt
- GenerateDataKey
- GenerateDataKeyWithoutPlaintext
- ReEncrypt

自定义密钥存储库不支持生成非对称数据密钥对GenerateDataKeyPair和GenerateDataKeyPairWithoutPlaintext的对称加密操作。

使用外部密钥存储中的 KMS 密钥的所有加密操作都支持加密上下文。与往常一样，AWS KMS 建议使用加密上下文，这是一种安全最佳实践。

在请求中使用 KMS 密钥时，请通过密钥 ID、密钥 ARN、别名或别名 ARN 识别 KMS 密钥。您无需指定外部密钥存储。响应包含为任何对称加密 KMS 密钥返回的相同字段。但是，在外部密钥存储中使用 KMS 密钥时，外部密钥管理器将使用与 KMS 密钥关联的外部密钥执行加密和解密操作。

为了确保外部密钥存储中经 KMS 密钥加密的加密文字至少与经标准 KMS 密钥加密的加密文字一样安全，AWS KMS 将使用双重加密。首先在 AWS KMS 中使用 AWS KMS 密钥材料对数据进行加密。然后，外部密钥管理器使用 KMS 密钥的外部密钥对其进行加密。若要解密双重加密的加密文字，首先由外部密钥管理器使用 KMS 密钥的外部密钥解密加密文字。然后在 AWS KMS 中使用 KMS 密钥的 AWS KMS 密钥材料进行解密。

要做到这一点，必须满足以下条件。

- KMS 密钥的密钥状态必须为 Enabled。要查找密钥状态，请参阅AWS KMS控制台上客户托管密钥的状态KeyState字段或DescribeKey响应中的字段。
- 托管 KMS 密钥的外部密钥存储必须连接到其外部密钥存储代理，也就是说，外部密钥存储的连接状态必须为 CONNECTED。

  您可以在AWS KMS控制台的外部密钥存储页面或DescribeCustomKeyStores响应中查看连接状态。外部密钥存储的连接状态也显示在 AWS KMS 控制台中 KMS 密钥的详细信息页面上。在详细信息页面上，选择 Cryptographic configuration（加密配置）选项卡，然后查看 Custom key store（自定义密钥存储）部分中的 Connection state（连接状态）字段。

  如果连接状态为 DISCONNECTED，则必须先将其连接。如果连接状态为 FAILED，则必须解决问题，断开外部密钥存储的连接，再将其连接。有关说明，请参阅 连接和断开外部密钥存储。
- 外部密钥存储代理必须能够找到外部密钥。
- 必须启用外部密钥并且必须执行加密和解密操作。

  外部密钥的状态独立于 KMS 密钥，并且不受 KMS 密钥的密钥状态变化影响，包括启用和禁用 KMS 密钥。同样，禁用或删除外部密钥不会更改 KMS 密钥的密钥状态，但使用关联的 KMS 密钥执行的加密操作将失败。

如果未满足这些条件，则加密操作失败，并且 AWS KMS 会返回 KMSInvalidStateException 异常。您可能需要重新连接外部密钥存储或使用外部密钥管理器工具来重新配置或修复外部密钥。有关其他帮助，请参阅the section called “排查外部密钥存储的问题”。

在外部密钥存储中使用 KMS 密钥时，请注意每个外部密钥存储中的 KMS 密钥针对加密操作共享自定义密钥存储请求限额。如果您超过该配额，则 AWS KMS 将返回 ThrottlingException。有关自定义密钥存储请求限额的详细信息，请参阅 自定义密钥存储请求限额。

计划从外部密钥存储删除 KMS 密钥

如果您确定您不需要在任何加密操作中使用 AWS KMS key，您可以计划删除 KMS 密钥。同样使用用于计划从 AWS KMS 删除任何 KMS 密钥的过程。从外部密钥存储中删除 KMS 密钥对作为其密钥材料的外部密钥没有影响。

您可以在强制等待期期间取消删除 KMS 密钥的计划。但是，删除的 KMS 密钥不可恢复。即使您拥有外部密钥，也无法在外部密钥存储中重新创建对称加密 KMS 密钥。由于外部密钥存储中的每个对称 KMS 密钥都有唯一的 AWS KMS 密钥材料和元数据，因此只有加密对称加密文字的 AWS KMS 密钥才能对其进行解密。

> **Warning**
>
> 删除 KMS 密钥是一种具有破坏性且潜在危险的操作，可阻止您恢复使用 KMS 密钥加密的所有数据。在安排删除 KMS 密钥之前，请检查 KMS 密钥的过去使用情况，并创建一个 Amazon CloudWatch 警报，当有人试图使用 KMS 密钥等待删除时，该警报会提醒您。如有可能，禁用 KMS 密钥而不是将其删除。

如果您计划从外部密钥存储中删除 KMS 密钥，其密钥状态将变为 Pending deletion（待删除）。KMS 密钥将在整个等待期处于 Pending deletion（待删除）状态，即使 KMS 密钥因您断开外部密钥存储而不可用时都是如此。这允许您在等待期内随时取消删除 KMS 密钥。等待期到期后，AWS KMS 将从 AWS KMS 删除 KMS 密钥。

当您计划从外部密钥存储中删除 KMS 密钥时，KMS 密钥将立即变得不可用（取决于最终一致性）。不过，在再次使用 KMS 密钥（例如解密数据密钥）之前，使用受 KMS 密钥保护的数据密钥加密的资源不会受到影响。此问题会影响 AWS 服务，因为许多服务使用数据密钥来保护您的资源。有关更多信息，请参阅 不可用的 KMS 密钥如何影响数据密钥。

您可以在 AWS CloudTrail 日志中监控 KMS 密钥的计划、取消和删除。

排查外部密钥存储的问题

大多数外部密钥存储问题的解决方法由每个异常时 AWS KMS 显示的错误消息或尝试将外部密钥存储库连接到其外部密钥存储代理失败时 AWS KMS 返回的连接错误代码来指示。但是，有些问题较为复杂。

在诊断外部密钥存储的问题时，首先需要找到原因。这将缩小补救措施的范围，提高故障排除的效率。

- AWS KMS — 问题可能出在内部 AWS KMS，例如外部密钥存储配置中的值不正确。
- 外部 — 问题可能源于外部 AWS KMS，包括外部密钥存储代理、外部密钥管理器、外部密钥或 VPC 端点服务的配置或操作问题。
- 网络 – 可能是连接或网络问题，例如您的代理端点、端口或私有 DNS 名称或域有问题。

> **Note**
>
> 当外部密钥存储的管理操作失败时，这些操作会生成几个不同的异常。但是，所有与外部密钥存储库的外部配置或连接状态相关的失败都会返回 AWS KMS `KMSInvalidStateException`加密操作。若要确定问题，请使用随附的错误消息文本。

在连接过程完成之前，ConnectCustomKeyStore操作很快就会成功。要确定连接过程是否成功，请查看外部密钥存储的连接状态。如果连接过程失败，则 AWS KMS 将返回连接错误代码，用于解释原因并提出补救措施建议。

主题

外部密钥存储故障排除工具

AWS KMS 提供了多种工具来帮助您识别和解决外部密钥存储库及其密钥的问题。请将这些工具与随外部密钥存储代理和外部密钥管理器提供的工具结合使用。

> **Note**
>
> 您的外部密钥存储代理和外部密钥管理器可能会提供更简单的方法来创建和维护外部密钥存储及其 KMS 密钥。有关详细信息，请参阅外部工具的相关文档。

AWS KMS 异常和错误消息

AWS KMS 提供了有关它遇到的任何问题的详细错误消息。您可以在 AWS Key Management Service API 参考和 AWS 软件开发工具包中找到有关 AWS KMS 异常的更多信息。即使你使用的是 AWS KMS 控制台，你也可能会发现这些参考资料很有帮助。例如，您可以参阅 `CreateCustomKeyStores` 操作的错误列表。

如果问题出现在其他 AWS 服务中，例如当您使用外部密钥存储中的 KMS 密钥来保护其他 AWS 服务中的资源时，该 AWS 服务可能会提供其他信息来帮助您识别问题。如果 AWS 服务未提供消息，则可以在记录您的 KMS 密钥使用情况的CloudTrail 日志中查看错误消息。

CloudTrail 日志

每 AWS KMS 个 API 操作，包括 AWS KMS 控制台中的操作，都记录在 AWS CloudTrail 日志中。AWS KMS 记录成功和失败操作的日志条目。对于失败的操作，日志条目包括 AWS KMS 异常名称（`errorCode`）和错误消息（`errorMessage`）。您可以使用此信息来确定和解决错误。有关示例，请参阅使用外部密钥存储中的 KMS 密钥解密失败。

日志条目还包括请求 ID。如果请求到达您的外部密钥存储代理，则您可以使用日志条目中的请求 ID，在代理日志中查找相应的请求（前提是您的代理提供日志）。

CloudWatch 指标

AWS KMS 记录有关您的外部密钥存储操作和性能的详细亚马逊 CloudWatch 指标，包括延迟、限制、代理错误、外部密钥管理器状态、距您的 TLS 证书到期的天数以及您的代理身份验证证书报告的使用期限。您可以使用这些指标为外部密钥存储的操作开发数据模型，并使用 CloudWatch 警报在即将发生的问题发生之前提醒您。

> **Important**
>
> AWS KMS 建议您创建 CloudWatch 警报以监控外部密钥存储指标。这些警报将在问题出现之前提醒您注意问题的早期迹象。

监控图表

AWS KMS 在 AWS KMS 控制台中每个外部密钥存储的详细信息页面上显示外部密钥存储 CloudWatch 指标的图表。您可以使用图表中的数据来帮助定位错误来源、检测即将发生的问题、建立基线和完善 CloudWatch 警报阈值。有关监控图标解释和使用其数据的详细信息，请参阅 监控外部密钥存储。

显示外部密钥存储和 KMS 密钥

AWS KMS 在 AWS KMS 控制台的外部密钥存储区以及对和DescribeKey操作的响应中显示有关您的外部密钥存储和 KMS 密钥的DescribeCustomKeyStores详细信息。这些显示信息包括外部密钥存储和 KMS 密钥的特殊字段，其中包含可用于故障排除的信息，例如外部密钥存储的连接状态和与 KMS 密钥关联的外部密钥的 ID。有关详细信息，请参阅 查看外部密钥存储 和 在外部密钥存储中查看 KMS 密钥。

XKS 代理测试客户端

AWS KMS 提供了一个开源测试客户端，用于验证您的外部密钥存储代理是否符合AWS KMS 外部密钥库代理 API 规范。您可以使用此测试客户端来确定和解决外部密钥存储代理的问题。

配置错误

创建外部密钥存储时，您需要指定构成外部密钥存储配置的属性值，例如代理身份验证凭证、代理 URI 端点、代理 URI 路径和 VPC 端点服务名称。当 AWS KMS 检测到属性值中有错误时，操作将失败并返回一个指示错误值的错误。

通过修复错误的值，可以解决许多配置问题。您可以修复无效的代理 URI 路径或代理身份验证凭证，而无需断开外部密钥存储的连接。有关这些值的定义，包括唯一性要求，请参阅 汇编先决条件。有关更新这些值的说明，请参阅 编辑外部密钥存储属性。

为避免代理 URI 路径和代理身份验证凭证值出错，在创建或更新外部密钥存储时，请将代理配置文件上传到 AWS KMS 控制台。这是一个基于 JSON 的文件，其中包含由外部密钥存储代理或外部密钥管理器提供的代理 URI 路径和代理身份验证凭证值。您不能在 AWS KMS API 操作中使用代理配置文件，但您可以使用该文件中的值来帮助您为 API 请求提供与代理中的值相匹配的参数值。

常规配置错误

异常：`CustomKeyStoreInvalidStateException`（`CreateKey`）、`KMSInvalidStateException`（加密操作）、`XksProxyInvalidConfigurationException`（管理操作，`CreateKey` 除外）

连接错误代码：`XKS_PROXY_INVALID_CONFIGURATION`、`XKS_PROXY_INVALID_TLS_CONFIGURATION`

对于具有公共端点连接的外部密钥存储，请在创建和更新外部密钥存储时 AWS KMS 测试属性值。对于使用 VPC 端点服务连接的外部密钥存储， AWS KMS 会在您连接和更新外部密钥存储时测试属性值。

> **Note**
>
> 即使尝试将外部密钥存储连接到其外部密钥存储代理失败，异步 `ConnectCustomKeyStore` 操作也可能会成功。在这种情况下，不会出现异常，但外部密钥存储的连接状态为“Failed（失败）”，并且连接错误代码将说明错误消息。有关更多信息，请参阅 外部密钥存储连接错误。

如果在属性值中 AWS KMS 检测到错误，则操作将失
败`XksProxyInvalidConfigurationException`并返回以下错误消息之一。

由于 URI 路径无效，外部密钥存储代理拒绝了该请求。请验证外部密钥存储的 URI 路径，并在必要时进行更新。

- 代理 URI 路径是向代理 API AWS KMS 发出请求的基本路径。如果此路径不正确，则对代理的所有请求都将失败。如需查看外部密钥存储的当前代理 URI 路径，请使用 AWS KMS 控制台或 `DescribeCustomKeyStores` 操作。如需查找正确的代理 URI 路径，请参阅您的外部密钥存储代理文档。有关更正代理 URI 路径值的帮助，请参阅 编辑外部密钥存储属性。
- 随着外部密钥存储代理或外部密钥管理器的更新，外部密钥存储代理的代理 URI 路径可能会发生变化。有关此类变化的详细信息，请参阅外部密钥存储代理或外部密钥管理器的文档。

`XKS_PROXY_INVALID_TLS_CONFIGURATION`
AWS KMS 无法与外部密钥存储代理建立 TLS 连接。请验证 TLS 配置，包括其证书。

- 所有外部密钥存储代理都需要 TLS 证书。TLS 证书必须由支持外部密钥存储的公有证书颁发机构（CA）颁发。有关受支持的 CA 列表，请参阅 AWS KMS 外部密钥存储代理 API 规范中的 Trusted Certificate Authorities（受信任的证书颁发机构）。
- 对于公有端点连接，TLS 证书上的主题公用名（CN）必须与外部密钥存储代理的代理 URI 端点中的域名相匹配。例如，如果公有端点是 https://myproxy.xks.example.com，即 TLS，则 TLS 证书上的 CN 必须为 `myproxy.xks.example.com` 或 `*.xks.example.com`。
- 对于 VPC 端点服务连接，TLS 证书上的主题公用名（CN）必须与您的 VPC 端点服务的私有 DNS 名称相匹配。例如，如果私有 DNS 名称是 myproxy-private.xks.example.com，则 TLS 证书上的 CN 必须为 `myproxy-private.xks.example.com` 或 `*.xks.example.com`。
- TLS 证书不得过期。要获取 TLS 证书的到期日期，请使用 SSL 工具，例如 OpenSSL。要监控与外部密钥存储库关联的 TLS 证书的到期日期，请使用该XksProxyCertificateDaysToExpire CloudWatch 指标。 AWS KMS 控制台的 “监控” 部分还会显示 TLS 认证到期日期的天数。
- 如果您使用公有端点连接，请使用 SSL 测试工具来测试您的 SSL 配置。TLS 连接错误可能是由不正确的证书链导致。

VPC 端点服务连接配置错误

异常：`XksProxyVpcEndpointServiceNotFoundException`、`XksProxyVpcEndpointServiceInvali`

除了一般的连接问题外，在创建、连接或更新具有 VPC 终端节点服务连接的外部密钥存储库时，您可能会遇到以下问题。 AWS KMS 在创建、连接和更新外部密钥存储库时，测试具有 VPC 终端节点服务连接的外部密钥存储的属性值。当管理操作由于配置错误而失败时，这些操作会生成以下异常：

XksProxyVpcEndpointServiceNotFoundException

原因可能是以下之一：

- VPC 端点服务名称不正确。请验证外部密钥存储的 VPC 端点服务名称是否正确，以及是否与外部密钥存储的代理 URI 端点值相匹配。要查找 VPC 终端节点服务名称，请使用 Amazon VPC 控制台或DescribeVpcEndpointServices操作。要查找现有外部密钥存储区的 VPC 终端节点服务名称和代理 URI 终端节点，请使用 AWS KMS 控制台或DescribeCustomKeyStores操作。有关更多信息，请参阅 查看外部密钥存储。
- VPC 终端节点服务可能位于与外部密钥存储区 AWS 区域 不同的位置。请验证 VPC 端点服务和外部密钥存储是否处于同一区域。（区域名称的外部名称，例如，是 VPC 终端节点服务名称的一部分`us-east-1`，例如 com.amazonaws.vpce.us-east-1。 vpce-svc-example。）有关对外部密钥存储的 VPC 端点服务的要求列表，请参阅 VPC 终端节点服务。您无法将 VPC 端点服务或外部密钥存储移至其他区域。但是，您可以在 VPC 端点服务所在的同一区域中创建新的外部密钥存储。有关详细信息，请参阅 配置 VPC 端点服务连接 和 创建外部密钥存储。
- AWS KMS 不是 VPC 终端节点服务的允许委托人。VPC 端点服务的 Allow principals（允许主体）列表必须包含 `cks.kms.<region>.amazonaws.com` 值，例如 `cks.kms.eu-west-3.amazonaws.com`。有关添加此值的说明，请参阅《AWS PrivateLink 指南》中的管理权限。

XksProxyVpcEndpointServiceInvalidConfigurationException

当 VPC 端点服务无法满足以下要求之一时，就会出现此错误：

- VPC 需要至少两个私有子网，每个子网均位于不同的可用区内。有关将子网添加到 VPC 中的帮助，请参阅《Amazon VPC 用户指南》中的在您的 VPC 中创建子网。

- 您的 VPC 端点服务类型必须使用网络负载均衡器，而不是网关负载均衡器。
- 不得要求 VPC 端点服务接受请求 [Acceptance required（需要接受）必须是“false”]。如果需要手动接受每个连接请求，则 AWS KMS 无法使用 VPC 终端节点服务连接到外部密钥存储代理。有关详细信息，请参阅《AWS PrivateLink 指南》中的接受或拒绝连接请求。
- VPC 端点服务必须具有私有 DNS 名称，该名称是公有域的子域。例如，如果私有 DNS 名称为 `https://myproxy-private.xks.example.com`，则 `xks.example.com` 或 `example.com` 域必须具有公有 DNS 服务器。要查看或更改 VPC 端点服务的私有 DNS 名称，请参阅《AWS PrivateLink 指南》中的管理 VPC 端点服务的 DNS 名称。
- 您的私有 DNS 名称域的 Domain verification status（域验证状态）必须为 `verified`。要查看和更新私有 DNS 名称域的验证状态，请参阅 验证私有 DNS 名称域。添加所需的文本记录后，可能需要几分钟才能显示更新的验证状态。

> **Note**
>
> 只有当私有 DNS 域是公有域的子域时，才能对其进行验证。否则，即使您添加了所需的 TXT 记录，私有 DNS 域的验证状态也不会更改。

- VPC 端点服务的私有 DNS 名称必须与外部密钥存储的代理 URI 端点值相匹配。对于使用 VPC 端点服务连接的外部密钥存储，代理 URI 端点必须是 `https://`，后跟 VPC 端点服务的私有 DNS 名称。要查看代理 URI 端点值，请参阅 查看外部密钥存储。要更改代理 URI 端点值，请参阅 编辑外部密钥存储属性。

外部密钥存储连接错误

将外部密钥存储连接到其外部密钥存储代理的过程大约需要五分钟才能完成。除非该过程迅速失败，否则 `ConnectCustomKeyStore` 操作将返回 HTTP 200 响应和无属性的 JSON 对象。但是，此初始响应不指示连接是否成功。要确定外部密钥存储是否已连接，请查看其连接状态。如果连接失败，则外部密钥存储库的连接状态将更改为`FAILED`并 AWS KMS 返回一个解释失败原因的连接错误代码。

> **Note**
>
> 当自定义密钥存储的连接状态为 `FAILED` 时，您必须先断开自定义密钥存储的连接，然后再尝试重新连接。您无法连接具有 `FAILED` 连接状态的自定义密钥存储。

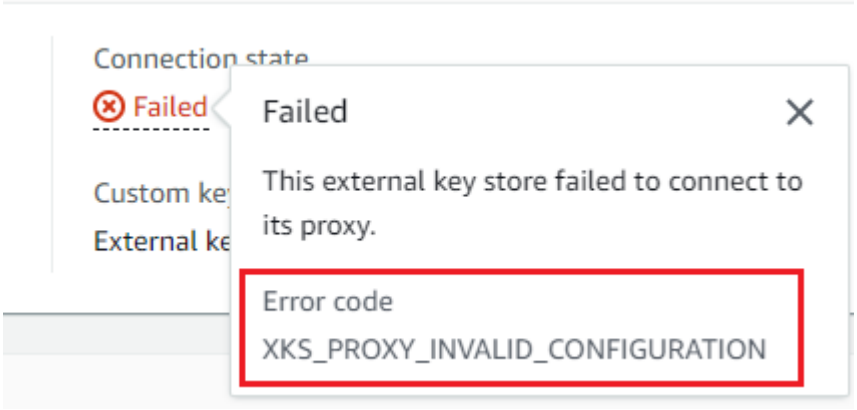
查看外部密钥存储的连接状态：

- 在DescribeCustomKeyStores响应中，查看ConnectionState元素的值。
- 在 AWS KMS 控制台中，连接状态显示在外部密钥存储表中。此外，每个外部密钥存储的详细信息页面上的 General configuration（常规配置）部分中也显示了 Connection state（连接状态）。

当连接状态为 FAILED 时，连接错误代码有助于解释错误。

要查看连接错误代码，请执行以下操作：

- 在DescribeCustomKeyStores响应中，查看ConnectionErrorCode元素的值。只有当 ConnectionState 为 FAILED 时，此元素才会出现在 DescribeCustomKeyStores 响应中。
- 要在 AWS KMS 控制台中查看连接错误代码，请在外部密钥存储的详细信息页面上将鼠标悬停在 Faile d 值上。



外部密钥存储的连接错误代码

以下连接错误代码适用于外部密钥存储

INTERNAL_ERROR

AWS KMS 由于内部错误，无法完成请求。重试 请求。对于 ConnectCustomKeyStore 请求，先断开自定义密钥存储，然后再尝试重新连接它。

INVALID_CREDENTIALS

其中一个或两个 XksProxyAuthenticationCredential 值在指定的外部密钥存储代理上无效。

NETWORK_ERRORS

网络错误使自定义密钥存储无法 AWS KMS 连接到其备用密钥库。

XKS_PROXY_ACCESS_DENIED

AWS KMS 请求被拒绝访问外部密钥库代理。如果外部密钥存储代理有授权规则，请验证这些规则是否允许 AWS KMS 代表您与代理进行通信。

XKS_PROXY_INVALID_CONFIGURATION

配置错误导致外部密钥存储无法连接到其代理。验证 XksProxyUriPath 的值。

XKS_PROXY_INVALID_RESPONSE

AWS KMS 无法解释来自外部密钥存储代理的响应。如果您反复看到此连接错误代码，请通知您的外部密钥存储代理供应商。

XKS_PROXY_INVALID_TLS_CONFIGURATION

AWS KMS 由于 TLS 配置无效，无法连接到外部密钥库代理。请验证外部密钥存储代理是否支持 TLS 1.2 或 1.3。此外，请验证 TLS 证书是否未过期，其是否与 XksProxyUriEndpoint 值中的主机名匹配，以及是否由受信任的证书颁发机构列表中包含的受信任的证书颁发机构签名。

XKS_PROXY_NOT_REACHABLE

AWS KMS 无法与您的外部密钥存储代理通信。请验证 XksProxyUriEndpoint 和 XksProxyUriPath 是否正确。使用外部密钥存储代理的工具来验证该代理是否处于活动状态并在其网络上可用。此外，请验证您的外部密钥管理器实例是否正常运行。如果代理报告所有外部密钥管理器实例都不可用，则连接尝试失败，并显示此连接错误代码。

XKS_PROXY_TIMED_OUT

AWS KMS 可以连接到外部密钥存储代理，但该代理 AWS KMS 在分配的时间内没有响应。如果您反复看到此连接错误代码，请通知您的外部密钥存储代理供应商。

XKS_VPC_ENDPOINT_SERVICE_INVALID_CONFIGURATION

Amazon VPC 终端节点服务配置不符合 AWS KMS 外部密钥存储的要求。

- VPC 端点服务必须是调用方 AWS 账户中的接口端点的端点服务。
- 其必须有至少连接到两个子网的网络负载均衡器（NLB），每个子网位于不同的可用区中。
- 该Allow principals列表必须包括该地区的 AWS KMS 服务主体cks.kms.<region>.amazonaws.com，例如cks.kms.us-east-1.amazonaws.com。
- 其不得要求接受连接请求。
- 其必须具有私有 DNS 名称。使用 VPC_ENDPOINT_SERVICE 连接的外部密钥存储的私有 DNS 名称在其 AWS 区域中必须是唯一的。
- 私有 DNS 名称域的验证状态必须为 verified。

- TLS 证书指定了端点可以访问的私有 DNS 主机名。

XKS_VPC_ENDPOINT_SERVICE_NOT_FOUND

AWS KMS 找不到用于与外部密钥存储代理通信的 VPC 终端节点服务。请验证 XksProxyVpcEndpointServiceName 是否正确，以及 AWS KMS 服务主体是否拥有 Amazon VPC 端点服务中的服务使用者权限。

延迟和超时错误

异常：CustomKeyStoreInvalidStateException（CreateKey）、KMSInvalidStateException（加密操作）、XksProxyUriUnreachableException（管理操作）

连接错误代码：XKS_PROXY_NOT_REACHABLE、XKS_PROXY_TIMED_OUT

当 AWS KMS 无法在 250 毫秒的超时间隔内联系代理时，它会返回异常。 CreateCustomKeyStore然后UpdateCustomKeyStore返回XksProxyUriUnreachableException。加密操作 会返回标准 KMSInvalidStateException，其中包含描述问题的错误消息。如果ConnectCustomKeyStore失败，则 AWS KMS 返回描述问题的连接错误代码。

超时错误可能是暂时性问题，可以通过重试请求来解决。如果问题仍然存在，请验证您的外部密钥存储代理是否处于活动状态并已连接到网络，以及其在外部密钥存储中的代理 URI 端点、代理 URI 路径和 VPC 端点服务名称（如果有）是否正确。此外，请验证您的外部密钥管理器是否接近外部密钥存储库。 AWS 区域 如果您需要更新其中任何值，请参阅 编辑外部密钥存储属性。

要跟踪延迟模式，请使用 AWS KMS 控制台监控部分中的指标和平均延迟图表（基于该指标）。XksProxyLatency CloudWatch 您的外部密钥存储代理可能还会生成跟踪延迟和超时的日志和指标。

XksProxyUriUnreachableException
AWS KMS 无法与外部密钥存储代理通信。这可能是暂时的网络问题。如果您反复看到此错误，请验证您的外部密钥存储代理是否处于活动状态并已连接到网络，以及其在外部密钥存储中的端点 URI 是否正确。

- 外部密钥存储代理未在 250 毫秒的超时间隔内响应 AWS KMS 代理 API 请求。这可能表示出现临时网络问题或代理存在操作或性能问题。如果重试不能解决该问题，请通知您的外部密钥存储代理管理员。

延迟和超时错误通常表现为连接失败。ConnectCustomKeyStore操作失败时，外部密钥存储库的连接状态将更改为FAILED并 AWS KMS 返回解释错误的连接错误代码。有关连接错误代码的列表和解决错误的建议，请参阅 外部密钥存储的连接错误代码。All custom key stores（所有自定义密钥存储）和 External key stores（外部密钥存储）的连接代码列表适用于外部密钥存储。以下连接错误与延迟和超时有关。

`XKS_PROXY_NOT_REACHABLE`

–或者–

`CustomKeyStoreInvalidStateException`，`KMSInvalidStateException`，`XksProxyUriUnreachableException`
AWS KMS 无法与外部密钥存储代理通信。请验证您的外部密钥存储代理是否处于活动状态并已连接到网络，以及其在外部密钥存储中的 URI 路径和端点 URI 或 VPC 服务名称是否正确。

出现此错误可能的原因如下：

- 外部密钥存储代理未处于活动状态或未连接到网络。
- 外部密钥存储配置中的代理 URI 端点、代理 URI 路径或 VPC 端点服务名称（如果适用）值有错误。要查看外部密钥存储配置，请使用DescribeCustomKeyStores操作或在 AWS KMS 控制台中查看外部密钥存储的详细信息页面。
- 与外部密钥存储代理之间的网络路径上可能存在网络配置错误 AWS KMS ，例如端口错误。 AWS KMS 通过端口 443 与外部密钥存储代理进行通信。此值不可配置。
- 当外部密钥存储代理报告（在GetHealthStatus响应中）所有外部密钥管理器实例均为时`UNAVAILABLE`，ConnectCustomKeyStore操作将失败，并显示为`ConnectionErrorCode``XKS_PROXY_NOT_REACHABLE`。有关帮助信息，请参阅外部密钥管理器的文档。
- 此错误可能是由于外部密钥管理器 AWS 区域 与外部密钥存储库之间的物理距离较远所致。 AWS 区域 和外部密钥管理器之间的 ping 延迟（网络往返时间 (RTT)）不得超过 35 毫秒。您可能需要在离外部密钥管理器更近的地方创建外部密钥存储库，或者将外部密钥管理器移到离外部密钥管理器更近的数据中心 AWS 区域。 AWS 区域

`XKS_PROXY_TIMED_OUT`

–或者–

`CustomKeyStoreInvalidStateException` ，`KMSInvalidStateException` ，`XksProxyUriUnreachableException`
AWS KMS 拒绝了该请求，因为外部密钥存储代理没有及时响应。重试 请求。如果您反复看到此错误，请将其报告给您的外部密钥存储代理管理员。

出现此错误可能的原因如下：

- 此错误可能是由外部密钥管理器与外部密钥存储代理之间的物理距离过远所致。如可行，请将外部密钥存储代理移到离外部密钥管理器更近的地方。
- 如果代理不是为处理来自的请求量和频率而设计的，则可能会发生超时错误 AWS KMS。如果您的 CloudWatch 指标显示问题持续存在，请通知您的外部密钥存储代理管理员。
- 当外部密钥管理器与外部密钥存储的 Amazon VPC 之间的连接无法正常运行时，可能会出现超时错误。如果您正在使用 AWS Direct Connect，请验证您的 VPC 和外部密钥管理器是否可以有效通信。要获得解决任何问题的帮助，请参阅 AWS Direct Connect 用户指南 AWS Direct Connect中的疑难解答。

`XKS_PROXY_TIMED_OUT`

–或者–

`CustomKeyStoreInvalidStateException` ，`KMSInvalidStateException` ，`XksProxyUriUnreachableException`
外部密钥存储代理未在分配的时间内响应请求。重试 请求。如果您反复看到此错误，请将其报告给您的外部密钥存储代理管理员。

- 此错误可能是由外部密钥管理器与外部密钥存储代理之间的物理距离过远所致。如可行，请将外部密钥存储代理移到离外部密钥管理器更近的地方。

身份验证凭证错误

异常：`CustomKeyStoreInvalidStateException`（`CreateKey`）、`KMSInvalidStateException`（加密操作）、`XksProxyIncorrectAuthenticationCredentialException`（管理操作，`CreateKey` 除外）

您在外部密钥存储代理 AWS KMS 上建立和维护的身份验证凭据。然后， AWS KMS 在创建外部密钥存储库时告诉凭据值。要更改身份验证凭证，请在外部密钥存储代理中进行更改。然后，针对外部密钥存储更新凭证。如果您的代理轮换凭证，则必须针对外部密钥存储更新凭证。

如果外部密钥存储代理无法针对您的外部密钥存储，对具有代理身份验证凭证签名的请求进行身份验证，则效果取决于请求：

- `CreateCustomKeyStore` 和 `UpdateCustomKeyStore` 失败，并显示 `XksProxyIncorrectAuthenticationCredentialException`。
- `ConnectCustomKeyStore` 成功，但连接失败。连接状态为 `FAILED`，连接错误代码为 `INVALID_CREDENTIALS`。有关更多信息，请参阅 外部密钥存储连接错误。
- 加密操作 将返回 `KMSInvalidStateException` 外部密钥存储中的所有外部配置错误和连接状态错误。随附的错误消息描述了问题。

外部密钥存储代理拒绝了该请求，因为其无法对 AWS KMS进行身份验证。请验证外部密钥存储的凭证，并在必要时进行更新。

出现此错误可能的原因如下：

- 外部密钥存储的访问密钥 ID 或秘密访问密钥与在外部密钥存储代理上建立的值不匹配。

  要修复此错误，请针对外部密钥存储更新代理身份验证凭证。无需断开外部密钥存储的连接即可进行此更改。
- AWS KMS 和外部密钥存储代理之间的反向代理可能正在操纵 HTTP 标头，从而使 SigV4 签名失效。要修复此错误，请通知您的代理管理员。

密钥状态错误

异常：`KMSInvalidStateException`

`KMSInvalidStateException` 对自定义密钥存储中的 KMS 密钥有两个不同的用途。

- 当管理操作（例如 `CancelKeyDeletion`）失败并返回此异常时，这表明 KMS 密钥的密钥状态与该操作不兼容。
- 当对自定义密钥存储中 KMS 密钥的加密操作失败，并显示 `KMSInvalidStateException` 时，这可能表明 KMS 密钥的密钥状态存在问题。但是， AWS KMS 加密操作会返

回KMSInvalidStateException外部密钥存储库中的所有外部配置错误和连接状态错误。要确定问题，请使用随异常显示的错误消息。

要查找 AWS KMS API 操作所需的密钥状态，请参阅密 AWS KMS 钥的关键状态。要查找 KMS 密钥的密钥状态，请在 Customer managed keys（客户托管密钥）页面上，查看 KMS 密钥的 Status（状态）字段。或者，使用DescribeKey操作并查看响应中的KeyState元素。有关更多信息，请参阅 查看密钥。

> **Note**
>
> 外部密钥存储中 KMS 密钥的密钥状态并不表明其关联的外部密钥的状态。有关外部密钥状态的信息，请使用外部密钥管理器和外部密钥存储代理工具。
>
> CustomKeyStoreInvalidStateException 指的是外部密钥存储的连接状态，而不是 KMS 密钥的密钥状态。

对自定义存储中 KMS 密钥的加密操作可能会失败，因为 KMS 密钥的密钥状态为 Unavailable 或 PendingDeletion。（禁用的密钥将返回 DisabledException。）

- 只有当您在 AWS KMS 控制台或使用DisableKey操作故意禁用 KMS 密钥时，KMS 密钥才会处于密钥状态。Disabled当某个 KMS 密钥已禁用时，您可以查看和管理该密钥，但不能在加密操作中使用该密钥。要修复此问题，请启用密钥。有关更多信息，请参阅 启用和禁用密钥。
- 当外部密钥存储与其外部密钥存储代理断开连接时，KMS 密钥会处于 Unavailable 密钥状态。要修复不可用的 KMS 密钥，请重新连接外部密钥存储。重新连接外部密钥存储后，外部密钥存储中的 KMS 密钥的密钥状态将自动还原到之前的状态，例如 Enabled 或 Disabled。

  在计划删除 KMS 密钥，或 KMS 密钥处于等待期时，其会处于 PendingDeletion 密钥状态。待删除的 KMS 密钥的密钥状态错误表明不应删除该密钥，因为其正在用于加密，或者其是解密所必需的密钥。要重新启用 KMS 密钥，请取消计划的删除，然后启用密钥。有关更多信息，请参阅 计划和取消密钥删除。

解密错误

异常：KMSInvalidStateException

当使用外部密钥存储库中的 KMS 密钥执行解密操作失败时，将 AWS KMS 返回加密操作用于处理外部密钥存储库上所有外部配置错误和连接状态错误的标准KMSInvalidStateException。此错误消息指示该问题。

要解密使用 双重加密 进行加密的加密文字，外部密钥管理器应首先使用外部密钥解密加密文字的外层。然后 AWS KMS 使用 KMS AWS KMS 密钥中的密钥材料来解密密文的内层。无效或损坏的加密文字可能会被外部密钥管理器或 AWS KMS拒绝。

解密失败时，会随 KMSInvalidStateException 出现以下错误消息。它表示请求中的加密文字或可选加密上下文存在问题。

外部密钥存储代理拒绝了该请求，因为指定的加密文字或其他经过身份验证的数据已损坏、丢失或无效。

- 当外部密钥存储代理或外部密钥管理器报告密文或其加密上下文无效时，通常表示发送到的请求中的密文或加密上下文存在问题。Decrypt AWS KMS对于Decrypt操作， AWS KMS 向代理发送它在请求中收到的相同密文和加密上下文。Decrypt

  此错误可能由传输过程中的网络问题引起，例如位反转。重试 Decrypt 请求。如果问题仍然存在，请验证加密文字是否未被更改或损坏。此外，请验证Decrypt请求中的加密上下文是否与加密数据的请求中的加密上下文 AWS KMS 相匹配。

外部密钥存储代理提交解密的加密文字或加密上下文已损坏、丢失或无效。

- AWS KMS 拒绝从代理收到的密文时，表示外部密钥管理器或代理向其返回了无效或损坏的密文。AWS KMS

  此错误可能由传输过程中的网络问题引起，例如位反转。重试 Decrypt 请求。如果问题仍然存在，请验证外部密钥管理器是否运行正常，并且外部密钥存储代理在返回外部密钥管理器之前不会更改从外部密钥管理器接收的密文。 AWS KMS

外部密钥错误

外部密钥是外部密钥管理器中的加密密钥，用作 KMS 密钥的外部密钥材料。 AWS KMS 无法直接访问外部密钥。其必须要求外部密钥管理器（通过外部密钥存储代理）使用外部密钥来加密数据或解密加密文字。

在外部密钥存储中创建 KMS 密钥时，您可以在其外部密钥管理器中指定外部密钥的 ID。创建 KMS 密钥后，您无法更改外部密钥 ID。为防止 KMS 密钥出现问题，CreateKey 操作会要求外部密钥存储代

理验证外部密钥的 ID 和配置。如果外部密钥不符合与 KMS 密钥一起使用的要求，则 CreateKey 操作将失败，并显示说明问题的异常和错误消息。

但是，在创建 KMS 密钥后，可能会出现问题。如果加密操作因外部密钥问题而失败，则此操作将会失败并返回 KMSInvalidStateException，以及一条包含说明问题的错误消息。

CreateKey 外部密钥错误

异常：XksKeyAlreadyInUseException、XksKeyNotFoundException、XksKeyInvalidConfigurati

该CreateKey操作尝试验证您在外部密钥 ID（控制台）或XksKeyId（API）参数中提供的外部密钥的 ID 和属性。这种做法是为了在您尝试结合使用 KMS 密钥和外部密钥之前及早发现错误。

正在使用外部密钥

外部密钥存储中的每个 KMS 密钥都必须使用不同的外部密钥。当CreateKey识别出 KMS 密钥的外部密钥 ID (XksKeyId) 在外部密钥存储中不是唯一的，则会失败，并显示为XksKeyAlreadyInUseException。

如果您为同一个外部密钥使用多个 ID，CreateKey 无法识别重复的密钥。但是，具有相同外部密钥的 KMS 密钥不可互操作，因为它们具有不同的 AWS KMS 密钥材料和元数据。

未找到外部密钥

当外部密钥存储代理报告无法使用 KMS 密钥的外部密钥 ID (XksKeyId) 找到外部密钥时，CreateKey操作将失败XksKeyNotFoundException并返回以下错误消息。

> 外部密钥存储代理拒绝了该请求，因为其无法找到外部密钥。

出现此错误可能的原因如下：

- KMS 密钥的外部密钥（XksKeyId）ID 可能无效。要查找外部密钥代理用于识别外部密钥的 ID，请参阅外部密钥存储代理或外部密钥管理器文档。
- 外部密钥可能已从您的外部密钥管理器中删除。要进行调查，请使用外部密钥管理器工具。如果外部密钥已永久删除，请将其他外部密钥与 KMS 密钥结合使用。有关外部密钥的列表或要求，请参阅 外部密钥存储中 KMS 密钥的要求。

未符合外部密钥要求

当外部密钥存储代理报告外部密钥不 符合要求，无法与 KMS 密钥一起使用时，CreateKey 操作将会失败并返回 XksKeyInvalidConfigurationException，以及如下错误消息中的一条。

外部密钥的密钥规格必须为 AES_256。指定的外部密钥的密钥规格为 *<key-spec>* 。

- 外部密钥必须是 256 位对称加密密钥，密钥规格为 AES_256。如果指定的外部密钥是不同的类型，请指定符合此要求的外部密钥的 ID。

外部密钥的状态必须为“ENABLED”（已启用）。指定外部密钥的状态为 *<status>*。

- 必须在外部密钥管理器中启用外部密钥。如果未启用指定的外部密钥，请使用外部密钥管理器工具将其启用，或指定已启用的外部密钥。

外部密钥的密钥用法必须包括“ENCRYPT”（加密）和“DECRYPT”（解密）。指定的外部密钥的密钥用法是 <*key-usage* >。

- 必须在外部密钥管理器中配置外部密钥以进行加密和解密。如果指定的外部密钥不包括这些操作，请使用外部密钥管理器工具更改操作，或指定其他外部密钥。

外部密钥的加密操作错误

异常：KMSInvalidStateException

当外部密钥存储代理找不到与 KMS 密钥关联的外部密钥，或者外部密钥不符合与 KMS 密钥一起使用的要求时，加密操作将失败。

在加密操作期间检测到的外部密钥问题比在创建 KMS 密钥之前检测到的外部密钥问题更难解决。创建 KMS 密钥后，您无法更改外部密钥 ID。如果 KMS 密钥尚未加密任何数据，则可以删除 KMS 密钥并使用其他外部密钥 ID 创建一个新密钥。但是，使用 KMS 密钥生成的密文无法被任何其他 KMS 密钥解密，即使是具有相同外部密钥的密钥也是如此，因为密钥将具有不同的密钥元数据和不同的密钥材料。AWS KMS 相反，应尽可能使用外部密钥管理器工具来解决外部密钥的问题。

当外部密钥存储代理报告外部密钥问题时，加密操作会返回 KMSInvalidStateException，以及一条说明该问题的错误消息题。

未找到外部密钥

当外部密钥存储代理报告无法使用 KMS 密钥的外部密钥 ID (XksKeyId) 找到外部密钥时，加密操作会返回`KMSInvalidStateException`带有以下错误消息的。

> 外部密钥存储代理拒绝了该请求，因为其无法找到外部密钥。

出现此错误可能的原因如下：

- KMS 密钥的外部密钥（`XksKeyId`）ID 不再有效。

  要查找与您的 KMS 密钥关联的外部密钥 ID，请查看 KMS 密钥的详细信息。要查找外部密钥代理用于识别外部密钥的 ID，请参阅外部密钥存储代理或外部密钥管理器文档。

  AWS KMS 在外部密钥存储中创建 KMS 密钥时会验证外部密钥 ID。但是，ID 可能会失效，尤其是在外部密钥 ID 值是别名或可变名称的情况下。您无法更改与现有 KMS 密钥关联的外部密钥 ID。要对通过 KMS 密钥加密的任何加密文字进行解密，必须将外部密钥与现有外部密钥 ID 重新关联。

  如果您尚未使用 KMS 密钥加密数据，则可以使用有效的外部密钥 ID 创建新的 KMS 密钥。但是，如果您已使用 KMS 密钥生成加密文字，则即使使用相同的外部密钥，也无法使用任何其他 KMS 密钥来对加密文字进行解密。
- 外部密钥可能已从您的外部密钥管理器中删除。要进行调查，请使用外部密钥管理器工具。如果可能，请尝试从外部密钥管理器的副本或备份中恢复密钥材料。如果外部密钥已永久删除，则以关联的 KMS 密钥加密的任何加密文字都将无法恢复。

外部密钥配置错误

当外部密钥存储代理报告外部密钥不 符合要求，不能与 KMS 密钥一起使用时，加密操作将返回`KMSInvalidStateException`，以及如下错误消息中的一条。

> 外部密钥存储代理拒绝了该请求，因为外部密钥不支持所请求的操作。

- 外部密钥必须同时支持加密和解密。如果密钥用法不包括加密和解密，请使用外部密钥管理器工具更改密钥用法。

外部密钥存储代理拒绝了该请求，因为该外部密钥未在外部密钥管理器中启用。

- 外部密钥必须在外部密钥管理器中启用并处于可用状态。如果外部密钥的状态不是 Enabled，请使用外部密钥管理器工具将其启用。

代理问题

例外：

CustomKeyStoreInvalidStateException（CreateKey）、KMSInvalidStateException（加密操
作）、UnsupportedOperationException、XksProxyUriUnreachableException、XksProxyInva
理操作，CreateKey 除外）

外部密钥存储代理调解 AWS KMS 和外部密钥管理器之间的所有通信。它将通用 AWS KMS 请求转换为您的外部密钥管理器可以理解的格式。如果外部密钥存储代理不符合AWS KMS 外部密钥存储代理 API 规范，或者运行不正常或无法与之通信 AWS KMS，则您将无法在外部密钥存储中创建或使用 KMS 密钥。

尽管许多错误都提到了外部密钥存储代理（因其在外部密钥存储架构中起着关键作用），但这些问题可能源于外部密钥管理器或外部密钥。

本节中的问题与外部密钥存储代理的设计或运行问题有关。要解决这些问题，可能需要更改代理软件。请咨询您的代理管理员。为帮助解决代理问题， AWS KMS 提供 XKS 代理测试客户端，这是一个开源测试客户端，可用于验证您的外部密钥存储代理是否符合 AWS KMS 外部密钥存储代理 API 规范。

CustomKeyStoreInvalidStateException 、KMSInvalidStateException 或 XksProxyUriUnreachableException
外部密钥存储代理运行状况不佳。如果您反复看到此消息，请通知您的外部密钥存储代理管理员。

- 此错误可能表示外部密钥存储代理存在运行问题或软件错误。您可以找到生成每个错误的 AWS KMS API 操作的 CloudTrail 日志条目。重试该操作可能会解决此错误。但是，如果问题仍然存在，请通知您的外部密钥存储代理管理员。
- 当外部密钥存储代理报告（在GetHealthStatus响应中）所有外部密钥管理器实例均为外部密钥管理器实例时UNAVAILABLE，尝试创建或更新外部密钥存储将失败，但会出现此异常。如果此错误仍然存在，请查阅您的外部密钥管理器文档。

`CustomKeyStoreInvalidStateException` 、`KMSInvalidStateException` 或 `XksProxyInvalidResponseException`
AWS KMS 无法解释来自外部密钥存储代理的响应。如果您反复看到此错误，请咨询您的外部密钥存储代理管理员。

- AWS KMS 当代理返回 AWS KMS 无法解析或解释的未定义响应时，操作会生成此异常。此错误可能由于暂时的外部问题或偶然的网络错误而偶尔发生。但是，如果此错误持续存在，则可能表明外部密钥存储代理不符合 AWS KMS 外部密钥存储代理 API 规范。通知您的外部密钥存储管理员或供应商。

`CustomKeyStoreInvalidStateException` 、`KMSInvalidStateException` 或 `UnsupportedOperationException`

外部密钥存储代理拒绝了该请求，因为其不支持所请求的加密操作。

- 外部密钥存储代理应支持 AWS KMS 外部密钥存储代理 API 规范中定义的所有代理 API。此错误表示代理不支持与请求相关的操作。通知您的外部密钥存储管理员或供应商。

代理授权问题

异常：`CustomKeyStoreInvalidStateException`、`KMSInvalidStateException`

一些外部密钥存储代理针对其外部密钥的使用执行授权要求。允许（但并非必需）外部密钥存储代理设计并实施授权方案，以允许特定用户在特定条件下请求特定操作。例如，代理可能允许用户使用特定的外部密钥进行加密，但不允许使用该外部密钥进行解密。有关更多信息，请参阅 外部密钥存储代理授权（可选）。

代理授权基于其对代理的请求中 AWS KMS 包含的元数据。仅当请求来自 VPC 端点且调用者与 KMS 密钥位于同一个账户时，`awsSourceVpc` 和 `awsSourceVpce` 字段才包含在元数据中。

```
"requestMetadata": {
    "awsPrincipalArn": string,
    "awsSourceVpc": string, // optional
    "awsSourceVpce": string, // optional
    "kmsKeyArn": string,
```

```
    "kmsOperation": string,
    "kmsRequestId": string,
    "kmsViaService": string // optional
}
```

当代理由于授权失败而拒绝请求时，相关的 AWS KMS 操作将会失败。CreateKey 会返回 CustomKeyStoreInvalidStateException。 AWS KMS 加密操作将返回 KMSInvalidStateException。两者都使用以下错误消息：

> 外部密钥存储代理拒绝对该操作的访问。请验证用户和外部密钥是否均已获得执行此操作的授权，然后重试请求。

- 要解决错误，请使用外部密钥管理器或外部密钥存储代理工具来确定授权失败的原因。然后，更新导致未经授权的请求的过程，或使用外部密钥存储代理工具更新授权策略。您无法在 AWS KMS中解决此错误。

密钥类型引用

不过，对于不同类型的 KMS 密钥，AWS KMS 支持不同功能。例如，只能使用对称加密 KMS 密钥生成对称数据密钥和非对称数据密钥对。此外，只有对称加密 KMS 密钥支持导入密钥材料和自动密钥轮换，并且在自定义密钥存储中只能创建对称加密 KMS 密钥。

此参考包括两个表。

- 密钥类型表列出了对对称加密 KMS 密钥、非对称 KMS 密钥，以及 HMAC KMS 密钥有效的 AWS KMS 操作。
- 特殊功能表列出了对多区域 KMS 密钥、包含导入的密钥材料的 KMS 密钥，以及自定义密钥存储中的 KMS 密钥有效的 AWS KMS 操作。

密钥类型表

您可能需要水平或垂直滚动才能查看此表中的所有数据。

AWS KMS API 操作	对称加密 KMS 密钥	HMAC KMS 密钥	非对称 KMS 密钥 (ENCRYPT_DECRYPT)	非对称 KMS 密钥 (SIGN_VERIFY)
CancelKeyDeletion	✓	✓	✓	✓
CreateAlias	✓	✓	✓	✓
CreateGrant	✓	✓	✓	✓
CreateKey	✓	✓	✓	✓
Decrypt	✓	⊗	✓	⊗
DeleteAlias	✓	✓	✓	✓
DeleteImportedKeyMaterial 仅在包含导入的密钥材料的 KMS 密钥上有效（`Origin` 为 `EXTERNAL`）。	✓	✓	✓	✓
DescribeKey	✓	✓	✓	✓
DisableKey	✓	✓	✓	✓
DisableKeyRotation	✓ 仅在包含 AWS KMS 密钥材料	⊗	⊗	⊗

AWS KMS API 操作	对称加密 KMS 密钥	HMAC KMS 密钥	非对称 KMS 密钥 (ENCRYPT_DECRYPT)	非对称 KMS 密钥 (SIGN_VERIFY)
	的 KMS 密钥上有效（Origin 为 AWS_KMS）。			
EnableKey	✓	✓	✓	✓
EnableKeyRotation	✓ 仅在包含 AWS KMS 密钥材料的 KMS 密钥上有效（Origin 为 AWS_KMS）。	⊗	⊗	⊗
Encrypt	✓	⊗	✓	⊗
GenerateDataKey	✓	⊗	⊗	⊗
GenerateDataKeyPair 生成受对称加密 KMS 密钥保护的非对称数据密钥对。	✓ 在自定义密钥存储中的 KMS 密钥上无效。	⊗	⊗	⊗

AWS KMS API 操作	对称加密 KMS 密钥	HMAC KMS 密钥	非对称 KMS 密钥 (ENCRYPT_DECRYPT)	非对称 KMS 密钥 (SIGN_VERIFY)
GenerateDataKeyPairWithoutPlaintext 生成受对称加密 KMS 密钥保护的非对称数据密钥对。	✓ 在自定义密钥存储中的 KMS 密钥上无效。	⊗	⊗	⊗
GenerateDataKeyWithoutPlaintext	✓	⊗	⊗	⊗
GenerateMac	⊗	✓	⊗	⊗
GetKeyPolicy	✓	✓	✓	✓
GetKeyRotationStatus	✓	✓ （KeyRotationEnabled 将始终为 false。）	✓ （KeyRotationEnabled 将始终为 false。）	✓ （KeyRotationEnabled 将始终为 false。）
GetParametersForImport 仅在包含导入的密钥材料的 KMS 密钥上有效（Origin 为 EXTERNAL）。	✓	✓	✓	✓
GetPublicKey	⊗	⊗	✓	✓

AWS KMS API 操作	对称加密 KMS 密钥	HMAC KMS 密钥	非对称 KMS 密钥 (ENCRYPT_DECRYPT)	非对称 KMS 密钥 (SIGN_VERIFY)
ImportKeyMaterial 仅在包含导入的密钥材料的 KMS 密钥上有效（`Origin` 为 `EXTERNAL`）。	✓	✓	✓	✓
ListAliases	✓	✓	✓	✓
ListGrants	✓	✓	✓	✓
ListKeyPolicies	✓	✓	✓	✓
ListResourceTags	✓	✓	✓	✓
ListRetirableGrants	✓	✓	✓	✓
PutKeyPolicy	✓	✓	✓	✓
ReEncrypt	✓	⊗	✓	⊗
ReplicateKey - 仅在多区域密钥上有效	✓	✓	✓	✓
RetireGrant	✓	✓	✓	✓
RevokeGrant	✓	✓	✓	✓

AWS KMS API 操作	对称加密 KMS 密钥	HMAC KMS 密钥	非对称 KMS 密钥 (ENCRYPT_DECRYPT)	非对称 KMS 密钥 (SIGN_VERIFY)
ScheduleKeyDeletion	✓	✓	✓	✓
Sign	⊗	⊗	⊗	✓
TagResource	✓	✓	✓	✓
UntagResource	✓	✓	✓	✓
UpdateAlias 当前 KMS 密钥和新的 KMS 密钥必须为相同类型（要么都是对称的，要么都是非对称的，要么都是 HMAC），并且它们必须用于相同的密钥用途。	✓	✓	✓	✓
UpdateKeyDescription	✓	✓	✓	✓
UpdateReplicaRegion - 仅在多区域密钥上有效	✓	✓	✓	✓
验证	⊗	⊗	⊗	✓
VerifyMac	⊗	✓	⊗	⊗

特殊功能表

此表显示了每种类型的特殊用途密钥上支持的 AWS KMS API 操作。

在阅读此表时，请注意以下交互：

- 多区域密钥：
  - 多区域密钥可以是对称加密 KMS 密钥、非对称 KMS 密钥、HMAC KMS 密钥，以及包含导入的密钥材料的 KMS 密钥。
  - 您不能在自定义密钥存储中创建多区域密钥。
- 导入的密钥材料
  - 您可以导入对称加密 KMS 密钥、非对称 KMS 密钥和 HMAC KMS 密钥的密钥材料。
  - 您可创建具有导入密钥材料的多区域密钥。
  - 您不能在自定义密钥存储中使用导入的密钥材料创建密钥。
  - 带有导入密钥材料的 KMS 密钥不支持自动密钥轮换 (`EnableKeyRotation`、`DisableKeyRotation`)。
- 自定义密钥存储
  - 自定义密钥存储仅支持对称加密 KMS 密钥。
  - 自定义密钥存储中的 KMS 密钥不支持对非对称密钥对（`GenerateDataKeyPair`、`GenerateDataKeyPairWithoutPlaintext`）进行对称操作。
  - 自定义密钥存储中的 KMS 密钥不支持自动密钥转换 (`EnableKeyRotation`、`DisableKeyRotation`)。
  - 您不能在自定义密钥存储中创建多区域密钥。

您可能需要水平或垂直滚动才能查看此表中的所有数据。

AWS KMS API 操作	多区域密钥	导入的密钥材料	自定义密钥存储中的 KMS 密钥
CancelKeyDeletion	✓	✓	✓
CreateAlias	✓	✓	✓
CreateGrant	✓	✓	✓
CreateKey	✓	✓	✓

AWS KMS API 操作	多区域密钥	导入的密钥材料	自定义密钥存储中的 KMS 密钥
您可以使用 CreateKey 创建多区域主键、包含导入的密钥材料的 KMS 密钥，或自定义密钥存储中的 KMS 密钥。若要创建多区域副本密钥，请使用 ReplicateKey 。			
Decrypt	✓ 仅当 KeyUsage 为 ENCRYPT_DECRYPT 时才有效	✓	✓
DeleteAlias	✓	✓	✓
DeleteImportedKeyMaterial	✓ 仅对包含导入的密钥材料的密钥有效（Origin 为 EXTERNAL ）	✓	⊗
DescribeKey	✓	✓	✓
DisableKey	✓	✓	✓
DisableKeyRotation	✓ 仅在包含 AWS KMS 密钥材料的对称加密密钥上有效（Origin 为 AWS_KMS ）。	⊗	⊗

AWS KMS API 操作	多区域密钥	导入的密钥材料	自定义密钥存储中的 KMS 密钥
EnableKey	✓ 仅在对称加密 KMS 密钥上有效	✓	✓
EnableKeyRotation	✓ 仅在包含 AWS KMS 密钥材料的对称加密密钥上有效（`Origin` 为 `AWS_KMS`）。	⊗	⊗
Encrypt	✓ 仅当 `KeyUsage` 为 `ENCRYPT_DECRYPT` 时才有效	✓	✓
GenerateDataKey	✓ 仅在对称加密 KMS 密钥上有效	✓	✓
GenerateDataKeyPair	✓ 仅在对称加密 KMS 密钥上有效	✓	⊗

AWS KMS API 操作	多区域密钥	导入的密钥材料	自定义密钥存储中的 KMS 密钥
GenerateDataKeyPairWithoutPlaintext	✓ 仅在对称加密 KMS 密钥上有效	✓	⊗
GenerateDataKeyWithoutPlaintext	✓ 仅在对称加密 KMS 密钥上有效	✓	✓
GenerateMac 仅在 HMAC KMS 密钥上有效	✓	✓	⊗
GetKeyPolicy	✓	✓	✓
GetKeyRotationStatus	✓	✓ （KeyRotationEnabled 将始终为 false。）	⊗
GetParametersForImport	✓ 仅对包含已导入的密钥材料的密钥有效（Origin 为 EXTERNAL）。	✓	⊗
GetPublicKey 仅对非对称 KMS 密钥有效。	✓	✓	⊗

AWS KMS API 操作	多区域密钥	导入的密钥材料	自定义密钥存储中的 KMS 密钥
ImportKeyMaterial	✓ 仅对包含已导入的密钥材料的密钥有效（Origin 为 EXTERNAL）。	✓	⊗
ListAliases	✓	✓	✓
ListGrants	✓	✓	✓
ListKeyPolicies	✓	✓	✓
ListResourceTags	✓	✓	✓
ListRetirableGrants	✓	✓	✓
PutKeyPolicy	✓	✓	✓
ReEncrypt	✓ 仅当 KeyUsage 为 ENCRYPT_DECRYPT 时才有效	✓	✓
ReplicateKey	✓ 仅在多区域主键上有效。	✓ 仅在多区域主键上有效。	⊗

AWS KMS API 操作	多区域密钥	导入的密钥材料	自定义密钥存储中的 KMS 密钥
RetireGrant	✓	✓	✓
RevokeGrant	✓	✓	✓
ScheduleKeyDeletion	✓	✓	✓
Sign 仅当 KeyUsage 为 SIGN_VERIFY 时才有效。	✓	✓	⊗
TagResource	✓	✓	✓
UntagResource	✓	✓	✓
UpdateAlias – 当前 KMS 密钥和新的 KMS 密钥必须为相同类型（要么都是对称的，要么都是非对称的，要么都是 HMAC），并且它们必须用于相同的密钥用途。	✓	✓	✓
UpdateKeyDescription	✓	✓	✓
UpdateReplicaRegion	✓	✓ 仅在多区域密钥上有效。	⊗

AWS KMS API 操作	多区域密钥	导入的密钥材料	自定义密钥存储中的 KMS 密钥
验证 仅当 KeyUsage 为 SIGN_VERIFY 时才有效。	✓	✓	⊗
VerifyMac 仅在 HMAC KMS 密钥上有效	✓	✓	⊗

AWS Key Management Service 的安全性

AWS 十分重视云安全性。作为 AWS 客户，您将从专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构中受益。

安全性是 AWS 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。第三方审核员定期测试和验证我们的安全性的有效性，作为 AWS 合规性计划的一部分。要了解适用于 AWS Key Management Service（AWS KMS）的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。在 AWS KMS 中，除了配置和使用 AWS KMS keys 之外，您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 AWS Key Management Service 时应用责任共担模型。它说明了如何配置 AWS KMS 以实现您的安全性和合规性目标。

主题

AWS Key Management Service 中的数据保护

AWS Key Management Service 存储和保护您的加密密钥，使其具有高度可用性，同时为您提供强大而灵活的访问控制。

主题

- 数据加密
- 互联网络流量隐私保护

保护密钥材料

默认情况下，AWS KMS 生成并保护 KMS 密钥的加密密钥材料。此外，AWS KMS 还为在 AWS KMS 外部创建和保护的密钥材料提供选项。有关 KMS 密钥和密钥材料的技术详细信息，请参阅 AWS Key Management Service 加密详细信息

保护 AWS KMS 中生成的密钥材料

默认情况下，当您创建 KMS 密钥时，AWS KMS 会为该 KMS 密钥生成并保护加密材料。

为了保护 KMS 密钥的密钥材料，AWS KMS 依靠经过 FIPS 140-2 安全级别 3 级验证的硬件安全模块（HSM）组成的分布式实例集。每个 AWS KMS HSM 都是专用、独立的硬件设备，旨在提供专用的加密功能，以满足 AWS KMS 的安全性和可扩展性要求。（在中国区域中，AWS KMS 使用的 HSM 已经过 OSCCA 认证并符合所有相关的中国法规，但未经过 FIPS 140-2 加密模块验证计划验证。）

在 HSM 中生成 KMS 密钥的密钥材料时，默认情况下会对其进行加密。密钥材料仅在 HSM 易失性存储器中解密，并且仅在加密操作中使用该密钥所需的几毫秒内解密。每当密钥材料未处于活跃使用状态时，都会在 HSM 中对其进行加密，然后传输到高度耐用（99.999999999%）、低延迟的永久存储中，在那里与 HSM 保持分离和隔离。明文密钥材料永远不会离开 HSM 安全边界；并且永远不会写入磁盘或持久性存放在任何存储介质中。（唯一的例外是非对称密钥对的公有密钥，此密钥对不是秘密的。）

AWS 断言，作为一项基本的安全原则，任何 AWS 服务 中任何类型的明文加密密钥材料都不存在人为交互。任何人（包括 AWS 服务 操作员）都无法查看、访问或导出明文密钥材料。即使在灾难性故障和灾难恢复事件中，该原则也适用。AWS KMS 中的明文客户密钥材料仅用于 AWS KMS 中经过 FIPS 验证的 HSM 的加密操作，以响应客户或其代表向服务提出的授权请求。

对于客户托管密钥，创建密钥的 AWS 账户 是密钥的唯一且不可转让的拥有者。拥有者账户对控制密钥访问权限的授权策略拥有完全和排他性的控制权。对于 AWS 托管式密钥，AWS 账户 可以完全控制授权向 AWS 服务 提出请求的 IAM policy。

保护 AWS KMS 外部生成的密钥材料

AWS KMS 提供 AWS KMS 中生成的密钥材料的替代方案。

自定义密钥存储是一项可选的 AWS KMS 功能，允许您创建由 AWS KMS 外部生成和使用的密钥材料提供支持的 KMS 密钥。AWS CloudHSM 密钥存储中的 KMS 密钥由您控制的 AWS CloudHSM 硬件

安全模块中的密钥提供支持。这些 HSM 已经过 FIPS 140-2 安全 3 级认证。外部密钥存储中的 KMS 密钥由您在 AWS 外部控制和管理的外部密钥管理器中的密钥支持，例如私有数据中心的物理 HSM。

另一个可选功能可使您为 KMS 密钥导入密钥材料。为了在导入的密钥材料传输到 AWS KMS 时对其进行保护，您可以使用 AWS KMS HSM 中生成的 RSA 密钥对中的公钥来加密密钥材料。导入的密钥材料在 AWS KMS HSM 中进行解密，并使用 HSM 中的对称密钥进行重新加密。与所有 AWS KMS 密钥材料一样，明文导入的密钥材料绝不会让 HSM 处于未加密状态。但是，提供密钥材料的客户负责密钥材料在 AWS KMS 之外的安全使用、持久性和维护。

数据加密

AWS KMS 中的数据包含 AWS KMS keys 以及它们所代表的加密密钥材料。此密钥材料仅在其使用时以明文形式存在于 AWS KMS 硬件安全模块 (HSM) 中。否则，密钥材料将被加密并存储在持久性存储中。

AWS KMS 生成为 KMS 密钥生成的密钥材料永远不会使 AWS KMS HSM 未加密。它不会在任何 AWS KMS API 操作中导出或传输。多区域密钥除外，此时 AWS KMS 会使用跨区域复制机制将多区域密钥的密钥材料从一个 AWS 区域 中的 HSM 复制到另一个 AWS 区域 中的 HSM。有关详细信息，请参阅 AWS Key Management Service 加密详细信息中的多区域密钥复制过程。

主题

- 静态加密
- 传输中加密

静态加密

AWS KMS 在兼容 FIPS 140-2 安全 3 级的硬件安全模块（HSM）中为 AWS KMS keys 生成密钥材料。唯一的例外是中国区域，在这些区域中，AWS KMS 用于生成 KMS 密钥的 HSM 符合所有相关的中国法规，但未经过 FIPS 140-2 加密模块验证计划验证。密钥材料未使用时，会利用 HSM 密钥进行加密，并写入耐久的持久性存储中。KMS 密钥的密钥材料和保护密钥材料的加密密钥永远不会以明文形式离开 HSM。

KMS 密钥的密钥材料的加密和管理完全由 AWS KMS 处理。

有关更多详细信息，请参阅 AWS Key Management Service 加密详细信息中的使用 AWS KMS keys。

传输中加密

AWS KMS 为 KMS 密钥生成的密钥材料永远不会在 AWS KMS API 操作中导出或传输。AWS KMS 使用密钥标识符来表示 API 操作中的 KMS 密钥。同样，AWS KMS 自定义密钥存储中 KMS 密钥的密钥材料不可导出，并且永远不会在 AWS KMS 或 AWS CloudHSM API 操作中传输。

然而，一些 AWS KMS API 操作会返回数据密钥。此外，客户可以使用 API 操作来为选定的 KMS 密钥导入密钥材料。

所有 AWS KMS API 调用必须使用传输层安全性协议（TLS）进行签名和传输。AWS KMS 需要 TLS 1.2，但建议所有区域使用 TLS 1.3。AWS KMS 还支持所有区域（中国区域除外）的 AWS KMS 服务端点的混合后量子 TLS。AWS KMS 不支持 AWS GovCloud (US) 中的 FIPS 端点的混合后量子 TLS。对 AWS KMS 的调用还需要一个现代化的密码套件，该套件支持完美向前保密，这意味着任何密钥（如私有密钥）的泄露都不会影响会话密钥。

如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。要使用标准 AWS KMS 端点或 AWS KMS FIPS 端点，客户端必须支持 TLS 1.2 或更高版本。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。有关 AWS KMS FIPS 端点的列表，请参阅 AWS 一般参考 中的 AWS Key Management Service 端点和限额。

AWS KMS 服务主机和 HSM 之间的通信在经过身份验证的加密方案中使用椭圆曲线加密 (ECC) 和高级加密标准 (AES) 进行保护。有关更多详细信息，请参阅 AWS Key Management Service 加密详细信息中的内部通信安全。

互联网络流量隐私保护

AWS KMS 支持 AWS Management Console 以及一组使您能够创建和管理 AWS KMS keys 并在加密操作中使用它们的 API 操作。

AWS KMS 支持两种网络连接选项，从您的私有网络到 AWS。

- Internet 上的 IPsec VPN 连接
- AWS Direct Connect，该服务通过标准的以太网光纤电缆将您的内部网络链接到 AWS Direct Connect 位置。

所有 AWS KMS API 调用必须使用传输层安全性 (TLS) 进行签名和传输。这些调用还需要一个现代化的密码套件，该套件支持完美向前保护。仅允许通过 AWS 内部网络从已知的 AWS KMS API 主机向存储 KMS 密钥的密钥材料的硬件安全模块 (HSM) 传输流量。

要在不通过公共 Internet 发送流量的情况从您的 Virtual Private Cloud (VPC) 直接连接到 AWS KMS，请使用 AWS PrivateLink 提供支持的 VPC 终端节点。有关更多信息，请参阅 通过 VPC 终端节点连接到 AWS KMS。

AWS KMS 还支持对传输层安全 (TLS) 网络加密协议使用混合后量子密钥交换选项。当您连接到 AWS KMS API 终端节点时，可以结合使用此选项与 TLS。

适用于 AWS Key Management Service 的身份和访问管理

AWS Identity and Access Management（IAM）可以帮助您安全地控制对 AWS 资源的访问。管理员控制谁可以通过身份验证（登录）并被授权（具有权限）来使用 AWS KMS 资源。有关更多信息，请参阅 将 IAM 策略与配合使用 AWS KMS。

密钥策略是控制对 AWS KMS 中的 KMS 密钥访问的主要机制。每个 KMS 密钥都必须有一个密钥策略。您可以使用 IAM policy 和授权以及密钥政策来控制对您的 KMS 密钥的访问。有关更多信息，请参阅 AWS KMS 的身份验证和访问控制。

如果使用的是 Amazon Virtual Private Cloud（Amazon VPC），则可以创建接口 VPC 终端节点到 AWS PrivateLink 支持的 AWS KMS。您还可以使用 VPC 终端节点策略来确定哪些委托人可以访问您的 AWS KMS 终端节点，他们可以进行哪些 API 调用，以及他们可以访问哪些 KMS 密钥。有关详细信息，请参阅控制对 VPC 终端节点的访问。

AWS Key Management Service 中的日志记录和监控

监控是了解 AWS KMS 中的 AWS KMS keys 的可用性、状态和使用情况的重要环节。监控有助于保持您的 AWS 解决方案的安全性、可靠性、可用性和性能。AWS 提供了多种用于监控 KMS 密钥的工具。

AWS CloudTrail 日志

对 AWS KMS API 操作的每次调用都被捕获为 AWS CloudTrail 日志中的事件。这些日志记录来自 AWS KMS 控制台的所有 API 调用，以及 AWS KMS 和其他 AWS 服务进行的调用。跨账户 API 调用（例如调用不同AWS 账户账户中的 KMS 密钥）会记录在两个账户的 CloudTrail 日志中。

在进行故障排除或审核时，您可以使用日志重新构建 KMS 密钥的生命周期。您还可以查看其在加密操作中对 KMS 密钥的管理和使用情况。有关更多信息，请参阅 the section called “使用登录 AWS CloudTrail”。

亚马逊 CloudWatch 日志

监控、存储和访问来自 AWS CloudTrail 或其他来源的日志文件。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

对于AWS KMS， CloudWatch 存储有用的信息，可帮助您防止 KMS 密钥及其保护的资源出现问题。有关更多信息，请参阅 the section called “使用监控 CloudWatch”。

亚马逊 EventBridge

AWS KMS当您的 KMS 密钥被轮换或删除，或者您的 KMS 密钥中导入的密钥材料过期时，会生成 EventBridge 事件。搜索 AWS KMS 事件（API 操作），并将这些事件路由到一个或多个目标函数或流中，以捕获状态信息。有关更多信息，请参阅the section called “使用 Amazon 进行监控 EventBridge”和 Amazon EventBridge 用户指南。

亚马逊 CloudWatch 指标

您可以使用指标监控您的 KMS 密钥，这些 CloudWatch 指标收集原始数据并将其处理AWS KMS为性能指标。数据以两周为间隔记录，因此您可以查看当前信息和历史信息的趋势。这有助于您了解 KMS 密钥的使用情况以及它们的使用情况随时间推移的变化。有关使用 CloudWatch 指标监控 KMS 密钥的信息，请参阅AWS KMS 指标和维度。

亚马逊 CloudWatch 警报

监控您指定的时间段内的某个指标的变化。然后在多个时间段内根据相对于给定阈值的指标值执行操作。例如，您可以创建一个 CloudWatch 警报，当有人尝试使用计划在加密操作中删除的 KMS 密钥时触发该警报。这表示 KMS 密钥仍在使用中，可能不应删除。有关更多信息，请参阅 the section called “创建警报”。

AWS Security Hub

您可以使用 AWS Security Hub 监控您的 AWS KMS 使用情况，确保安全行业标准和最佳实践合规性。Security Hub 使用安全控件来评估资源配置和安全标准，以帮助您遵守各种合规框架。有关更多信息，请参阅《AWS Security Hub User Guide》中的 AWS Key Management Service controls。

AWS Key Management Service 的合规性验证

作为多个 AWS Key Management Service 合规性计划的一部分，第三方审计员将评估 AWS 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

主题

合规性和安全性文档

以下合规性和安全性文档涵盖 AWS KMS。要查看它们，请使用 AWS Artifact。

- 云计算合规性控制目录 (C5)
- ISO 27001:2013 适用性声明 (SoA)
- ISO 27001:2013 认证
- ISO 27017:2015 适用性声明 (SoA)
- ISO 27017:2015 认证
- ISO 27018:2015 适用性声明 (SoA)
- ISO 27018:2014 认证
- ISO 9001:2015 认证
- PCI DSS 合规证明 (AOC) 和责任摘要
- 服务组织控制 (SOC) 1 报告
- 服务组织控制 (SOC) 2 报告
- 服务组织控制 (SOC) 2 保密性报告
- FedRAMP-高

有关使用 AWS Artifact 的帮助，请参阅在 AWS Artifact 中下载报告。

了解更多信息

您在使用 AWS KMS 时的合规性责任由您的数据的敏感性、您公司的合规性目标以及适用的法律法规决定。如果您对 AWS KMS 的使用需遵守发布的标准，AWS 将提供以下有用资源：

- 合规性计划范围内的 AWS 服务 – 此页面列出在特定合规性计划范围内的 AWS 服务。有关一般信息，请参阅 AWS合规性计划。
- 安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- AWS 合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS Config – 此 AWS 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。

- AWS Security Hub – 此 AWS 服务向您提供 AWS 中安全状态的全面视图。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实操。有关受支持服务及控制的列表，请参阅 Security Hub 控制参考。

AWS Key Management Service 中的故障恢复能力

AWS全球基础设施围绕AWS 区域和可用区构建。AWS 区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

除了 AWS 全球基础设施之外，AWS KMS 还提供了多种功能，以帮助支持您的数据弹性和备份需求。有关 AWS 区域和可用区的更多信息，请参阅 AWS 全球基础设施。

区域隔离

AWS Key Management Service（AWS KMS）是一种可自我维持的区域性服务，在所有 AWS 区域开放。AWS KMS 采用区域隔离设计，可确保任何一个 AWS 区域的可用性问题不会影响在任何其他区域的 AWS KMS 操作。AWS KMS 的设计目标是确保零计划停机时间，所有软件更新和扩缩操作都将在不知不觉中无缝执行。

AWS KMS 服务水平协议（SLA）为所有 KMS API 均提供 99.999% 的服务承诺。为履行这一承诺，AWS KMS 会确保执行 API 请求所需的所有数据和授权信息在接收该请求的所有区域主机上都可用。

AWS KMS 基础设施会在每个区域的至少三个可用区（AZ）中复制。为确保多个主机故障不会影响 AWS KMS 性能，AWS KMS 旨在服务于来自区域中任何 AZ 的客户流量。

您对 KMS 密钥属性或权限所做的更改将复制到该区域中的所有主机，以确保该区域中的任何主机都能正确处理后续请求。有关使用 KMS 密钥的加密操作请求将会转发给某个 AWS KMS 硬件安全模块（HSM）队列，其中任何一个模块都可以使用 KMS 密钥执行操作。

多租户设计

AWS KMS 的多租户设计使其能够达到 99.999% 的可用性 SLA，并保持较高的请求率，同时保护密钥和数据的保密性。

通过部署多个完整性控制执行机制，以确保实际用于执行加密操作的 KMS 密钥始终是您为该操作指定的密钥。

KMS 密钥的明文密钥材料受到全面保护。密钥材料在创建后将立即在 HSM 中加密，并且加密后的密钥材料会立即移动到安全、低延迟的存储中。加密后的密钥仅在使用时才在 HSM 中检索和解密。明文密钥仅在完成加密操作所需的时间内驻留在 HSM 内存中。然后会在 HSM 中重新加密，并将加密后的密钥退回存储。明文密钥材料永远不会离开 HSM；并且永远不会写入持久性存储。

要详细了解 AWS KMS 使用的密钥保护机制，请参阅 AWS Key Management Service 加密详细信息。

AWS KMS 中的弹性最佳实践

为了优化 AWS KMS 资源的弹性，请考虑以下策略。

- 要支持备份和灾难恢复策略，请考虑使用多区域密钥，这是指在一个 AWS 区域中创建并且仅复制到您指定区域的 KMS 密钥。借助多区域密钥，您可以在 AWS 区域之间（在同一个分区内）移动加密资源而永远不会暴露密钥明文，并且可根据需要在其中的任何一个任何目标区域解密该资源。相关的多区域密钥是可互操作的，因为它们共享相同的密钥材料和密钥 ID，但使用独立的密钥策略以实现高精度访问控制。有关详细信息，请参阅 AWS KMS 中的多区域密钥。
- 要保护 AWS KMS 等多租户服务中的密钥，请务必使用访问控制，包括密钥策略和 IAM policy。此外，您可以使用 AWS PrivateLink 支持的 VPC 接口端点将请求发送至 AWS KMS。执行此操作时，您的 Amazon VPC 和 AWS KMS 之间的所有通信将完全位于 AWS 网络内，使用您的 VPC 限定使用的专用 AWS KMS 端点进行。您可以使用 VPC 端点策略创建额外的授权层，从而进一步保护这些请求的安全。有关详细信息，请参阅通过 VPC 端点连接到 AWS KMS。

AWS Key Management Service 中的基础设施安全性

作为一项托管服务，AWS Key Management Service (AWS KMS) 由 Amazon Web Services：安全流程概述中所述的 AWS 全球网络安全程序提供保护。

要通过网络访问 AWS KMS，您可以调用《AWS Key Management Service API Reference》https://docs.aws.amazon.com/kms/latest/APIReference/中描述的 AWS KMS API 操作。AWS KMS 在所有区域使用 TLS 1.2，但建议使用 TLS 1.3。AWS KMS 还支持所有区域（中国区域除外）的 AWS KMS 服务端点的混合后量子 TLS。AWS KMS 不支持 AWS GovCloud (US) 中的 FIPS 端点的混合后量子 TLS。要使用标准 AWS KMS 端点或 AWS KMS FIPS 端点，客户端必须支持 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

您可以从任何网络位置调用这些 API 操作，但 AWS KMS 支持全局策略条件，该条件允许您根据源 IP 地址、VPC 和 VPC 终端节点控制对 KMS 密钥的访问。您可以在密钥策略和 IAM policy 中使用这些条件键。然而，这些条件可以防止 AWS 代表您使用 KMS 密钥。有关更多信息，请参阅 AWS 全局条件键。

例如，以下密钥策略语句允许代入 KMSTestRole 角色的用户将此 AWS KMS key 用于指定的加密操作，除非源 IP 地址是策略中指定的 IP 地址之一。

```
{
  "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"
        ]
      }
    }
  }
}
```

物理主机的隔离

AWS KMS 使用的物理基础设施的安全性受 Amazon Web Services：安全流程概述的物理和环境安全部分中所述的控制措施约束。您可以在上一节中列出的合规性报告和第三方审计结果中找到更多详细信息。

AWS KMS 由专用的硬化硬件安全模块 (HSM) 提供支持，该模块采用特定控件设计，可抵御物理攻击。HSM 是不具有虚拟化层（如虚拟机管理程序）的物理设备，可在多个逻辑租户之间共享物理设

备。AWS KMS keys 的密钥材料仅存储在 HSM 上的易失存储器中，并且仅在 KMS 密钥正在使用时才存储。当 HSM 退出操作状态（包括预期和意外关机和重置）时，此内存将被擦除。有关 AWS KMS HSM 的操作的详细信息，请参阅 AWS Key Management Service 加密详细信息。

AWS Key Management Service 的安全最佳实践

AWS Key Management Service (AWS KMS) 支持多项安全功能，您可以实施这些功能增强对加密密钥的保护，例如密钥政策和 IAM policy、在对称加密密钥上进行加密操作的加密上下文选项、大量用于优化密钥政策和 IAM policy的条件键以及限制授权的授权约束。

AWS Key Management Service 最佳实践 (PDF) 中详细介绍了这些安全功能。本技术论文中的一般准则并不代表完整的安全解决方案。由于并非所有最佳实践都适用于所有情况，因此这些做法并不是规范性的。

另请参阅

- IAM policy 的最佳实践
- AWS KMS 授权的最佳实践
- IAM 用户指南中的 IAM 安全最佳实践

配额

为了提高所有用户的 AWS KMS 响应能力和性能， AWS KMS 应用了两种类型的配额，即资源配额和请求配额。对于每个 AWS 账户的每个区域，每个配额均单独计算。

除密钥策略文档大小资源 AWS KMS 配额、按需轮换资源配额和密AWS CloudHSM 钥存储请求配额外，所有配额均可调整。要请求提高限额，请参阅《服务限额用户指南》中的请求提高限额。要申请减少配额、更改未在 Service Quotas 中列出的配额，或者在没有服务配额 AWS 区域 的情况下更改配额，请访问AWS Support 中心并创建案例。 AWS KMS

主题

- 资源配额
- 请求配额
- 限制请求 AWS KMS

资源配额

AWS KMS 建立资源配额，以确保它能够为我们的所有客户提供快速而有弹性的服务。某些资源配额仅适用于您创建的资源，而不适用于 AWS 服务为您创建的资源。如果您使用的资源不属于您的 AWS 账户，例如 AWS 拥有的密钥，那么这些资源不会计入相应配额。

如果已超出资源限制，那么创建该资源类型的其他请求会生成 `LimitExceededException` 错误消息。

除密钥策略文档大小配额和按需轮换资源配额外，所有 AWS KMS 资源配额均可调整。要请求提高限额，请参阅《服务限额用户指南》中的请求提高限额。要申请减少配额、更改未在 Service Quotas 中列出的配额，或者在没有服务配额 AWS 区域 的情况下更改配额，请访问AWS Support 中心并创建案例。 AWS KMS

下表列出并描述了每个 AWS 账户 区域的 AWS KMS 资源配额。

限额名称	默认值	适用于	可调整
AWS KMS keys	100000	客户管理密钥	是
每个 KMS 密钥的别名	50	客户创建的别名	是

限额名称	默认值	适用于	可调整
每个 KMS 密钥的授权数	50000	客户管理密钥	是
密钥策略文档大小	32 KB（32,768 字节）	客户管理密钥 AWS 托管式密钥	否
自定义密钥存储资源限额	10	AWS 账户 和区域	是

除资源配额外，还 AWS KMS 使用请求配额来确保服务的响应能力。有关更多信息，请参阅 the section called “请求配额”。

AWS KMS keys：100000

在您的 AWS 账户的每个区域中，您最多可以拥有 100000 个客户托管的密钥。此配额适用于所有 AWS 区域 中的所有客户托管的密钥，不考虑其密钥规范或密钥状态。每个 KMS 密钥都视为一个资源。AWS 托管式密钥 和 AWS 拥有的密钥 不计入此限额。

每个 KMS 密钥的别名数：50

您最多可以将 50 个别名与每个客户托管密钥关联。 AWS 关联的别名AWS 托管式密钥不计入此配额。您在创建或更新别名时可能会遇到此配额。

> **Note**
>
> 仅当 KMS 密钥符合此配额时，kms: ResourceAliases 条件才有效。如果 KMS 密钥超出此配额，则由 `kms:ResourceAliases` 条件授权使用 KMS 密钥的委托人将被拒绝访问 KMS 密钥。有关更多信息，请参阅 由于别名配额而拒绝访问。

每个 KMS 的别名密钥配额取代了限制每个区域中别名总数的每个区域的别名配额。 AWS 账户 AWS KMS 取消了每个区域的别名配额。

每个 KMS 密钥的授权数：50000

每个客户托管密钥最多可以拥有 50000 个授权数，其中包括与 AWS KMS集成的AWS 服务所创建的授权。此配额不适用于 AWS 托管式密钥 或 AWS 拥有的密钥。

此配额的作用之一是，您不能同时执行超过 50000 个使用相同 KMS 密钥的授权操作。在达到配额之后，您只能在停用或撤消了有效授权时才能在 KMS 密钥上创建新授权。

例如，当您将 Amazon Elastic Block Store (Amazon EBS) 卷附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例时，该卷将被解密，以便您能读取。为获得解密数据的权限，Amazon EBS 将为每个卷创建授权。因此，如果所有 Amazon EBS 卷都使用相同的 KMS 密钥，那么您一次附加的卷不能超过 50000 个。

密钥策略文档大小：32 KB

每个密钥策略文档的最大长度为 32 KB（32768 字节）。如果采用更大的策略文档来创建或更新 KMS 密钥的密钥策略，操作将失败。

此配额不可调整。您不能通过使用 Service Quotas 或在中创建案例来增加配额 AWS Support。如果您的密钥策略已接近限制，请考虑使用授权而不是策略语句。授权特别适合临时权限或非常特定的权限。

每当您使用或PutKeyPolicy操作中的默认视图或策略视图来创建或更改密钥策略时 AWS Management Console，都可以使用密钥策略文档。即使您使用 AWS KMS 控制台中的默认视图（您不能在其中直接编辑 JSON 语句），此配额也适用于您的密钥策略文档。

自定义密钥存储资源限额：10

您最多可以在每个 AWS 账户 地区创建 10 个自定义密钥存储库。如果您尝试创建更多内容，则CreateCustomKeyStore操作将失败。

此限额适用于每个账户和区域中的自定义密钥存储总数，包括所有 AWS CloudHSM 密钥存储和外部密钥存储，无论其连接状态如何。

按需轮换：10

每个 KMS 密钥最多可以按需轮换 10 次。如果您尝试执行更多按需轮换，则RotateKeyOnDemand操作将失败。

此限额不可调整。您不能通过使用 Service Quotas 或在中创建案例来增加配额 AWS Support。为防止达到按需轮换配额，我们建议尽可能使用自动密钥轮换。

请求配额

AWS KMS 为每秒钟内请求的 API 操作数量设定配额。请求配额因 API 操作 AWS 区域、和其他因素（例如 KMS 密钥类型）而异。当您超过 API 请求配额时， AWS KMS 会限制该请求。

除AWS CloudHSM 密钥库 AWS KMS 请求配额外，所有请求配额均可调整。要请求提高限额，请参阅《服务限额用户指南》中的请求提高限额。要申请减少配额、更改未在 Service Quotas 中列出的配额，或者在没有服务配额 AWS 区域 的情况下更改配额，请访问AWS Support 中心并创建案例。 AWS KMS

如果您超出了该GenerateDataKey操作的请求配额，请考虑使用的数据密钥缓存功能 AWS Encryption SDK。重复使用数据密钥可能会将您的请求频率降至 AWS KMS.

除了请求配额外，还 AWS KMS 使用资源配额来确保所有用户的容量。有关更多信息，请参阅 资源配额。

要查看请求速率的趋势，请使用 Service Quotas 控制台。您还可以创建一个 Amazon CloudWatch 警报，当您的请求率达到配额值的特定百分比时，提醒您。有关详情，请参阅AWS 安全博客 CloudWatch中的使用 Service Quotas 和 Amazon 管理您的 AWS KMS API 请求速率。

主题

每个 AWS KMS API 操作的请求配额

下表列出了 S ervice Quotas 配额代码和每个 AWS KMS 请求配额的默认值。除AWS CloudHSM 密钥库 AWS KMS 请求配额外，所有请求配额均可调整。

> **Note**
>
> 您可能需要水平或垂直滚动才能查看此表中的所有数据。

限额名称	默认值（每秒请求数）

Cryptographic operations (symmetric) request rate
 	
适用对象：
 	
• Decrypt
• Encrypt
• GenerateDataKey
• GenerateDataKeyWithoutPlaintext
• GenerateMac
• GenerateRandom
• ReEncrypt
• VerifyMac
	这些共享配额因请求中使用的 KMS 密钥 AWS 区域 和类型而异。每个配额都单独计算。
	
	• 5500（共享）
	• 在以下区域中为 10000（共享）：
	  • 美国东部（俄亥俄），us-east-2
	  • 亚太地区（新加坡），ap-southeast-1
	  • 亚太区域（悉尼），ap-southeast-2
	  • 亚太区域（东京），ap-northeast-1
	  • 欧洲（法兰克福），eu-central-1
	  • 欧洲（伦敦），eu-west-2
	• 在以下区域中为 50000（共享）：
	  • 美国东部（弗吉尼亚北部），us-east-1
	  • 美国西部（俄勒冈），us-west-2
	  • 欧洲（爱尔兰），eu-west-1

Cryptographic operations (RSA) request rate 适用对象： • Decrypt • Encrypt • ReEncrypt • Sign • Verify	500（共享），对于 RSA KMS 密钥
Cryptographic operations (ECC and SM2) request rate 适用对象：	椭圆曲线 (ECC) 和 SM2（仅限中国区域）KMS 密钥为 300（共享）

限额名称	默认值（每秒请求数）
• Decrypt—仅支持 SM2（仅限中国区域）KMS 密钥 • Encrypt—仅支持 SM2（仅限中国区域）KMS 密钥 • ReEncrypt —仅支持 SM2（仅限中国区域）KMS 密钥 • Sign • Verify	
Custom key store request quotas 适用对象： • Decrypt • Encrypt • GenerateDataKey • GenerateDataKeyWithoutPlaintext • GenerateRandom • ReEncrypt	自定义密钥存储限额 针对每个自定义密钥存储单独计算 • 每个 AWS CloudHSM 密钥库有 1,800 个（共享） • 每个外部密钥存储 1800 次（共享）
CancelKeyDeletion request rate	5
ConnectCustomKeyStore request rate	5
CreateAlias request rate	5
CreateCustomKeyStore request rate	5
CreateGrant request rate	50
CreateKey request rate	5
DeleteAlias request rate	15

限额名称	默认值（每秒请求数）
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
GenerateDataKeyPair (ECC_NIST_P256) request rate 适用对象： • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext	100
GenerateDataKeyPair (ECC_NIST_P384) request rate 适用对象： • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext	100

限额名称	默认值（每秒请求数）
GenerateDataKeyPair (ECC_NIST_P521) request rate 适用对象： • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext	100
GenerateDataKeyPair (ECC_SECG_P256K1) request rate 适用对象： • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext	100
GenerateDataKeyPair (RSA_2048) request rate 适用对象： • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext	1
GenerateDataKeyPair (RSA_3072) request rate 适用对象： • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext	0.5（每 2 秒间隔为 1）

限额名称	默认值（每秒请求数）
GenerateDataKeyPair (RSA_4096) request rate 适用对象： • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext	0.1（每 10 秒间隔为 1）
GenerateDataKeyPair (SM2 – China Regions only) request rate 适用对象： • GenerateDataKeyPair • GenerateDataKeyPairWithoutPlaintext	25
GetKeyPolicy request rate	1000
GetKeyRotationStatus request rate	1000
GetParametersForImport request rate	0.25（每 4 秒间隔为 1）
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

限额名称	默认值（每秒请求数）
ListResourceTags request rate	2000
ListRetirableGrants request rate	100
PutKeyPolicy request rate	15
ReplicateKey request rate ReplicateKey 操作在主键的区域中计为一个 ReplicateKey 请求，在副本密钥区域中计为两个 CreateKey 请求。其中一个 CreateKey 请求是在创建密钥之前检测潜在问题的排练。	5
RetireGrant request rate	30
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 UpdatePrimaryRegion 操作计数为两个 UpdatePrimaryRegion 请求；两个受影响区域中每个区域都有一个请求。	5

应用请求配额

审查请求配额时，请记住以下信息。

- 请求配额同时适用于客户托管密钥和 AWS 托管式密钥。的使用AWS 拥有的密钥不计入您的请求配额 AWS 账户，即使这些配额用于保护您账户中的资源也是如此。
- 请求配额适用于发送到 FIPS 终端节点和非 FIPS 终端节点的请求。有关 AWS KMS 服务终端节点的列表，请参阅中的AWS Key Management Service 终端节点和配额 AWS 一般参考。
- 限制基于对区域内所有类型 KMS 密钥的所有请求。此总数包括来自所有委托人的请求 AWS 账户，包括代表您的 AWS 服务部门提出的请求。
- 每个请求配额都是单独计算的。例如，对CreateKey操作的请求不会影响该CreateAlias操作的请求配额。如果 `CreateAlias` 请求受到限制，`CreateKey` 请求仍可成功完成。
- 虽然加密操作共享一个配额，但共享配额是独立于其他操作的配额计算的。例如，对 Encrypt 和 Decrypt 操作的调用共享请求配额，但该配额与管理操作的配额无关，例如。EnableKey例如，在欧洲（伦敦）区域，每秒可使用对称 KMS 密钥执行 10000 次加密操作，加上 5 次 `EnableKey` 操作，而不受限制。

加密操作的共享配额

AWS KMS 加密操作共享请求配额。您可以请求 KMS 密钥支持的加密操作的任意组合，只要加密操作的总数不超过该 KMS 密钥类型的请求配额。唯一的例外是GenerateDataKeyPair和 GenerateDataKeyPairWithoutPlaintext，它们共享单独的配额。

不同类型的 KMS 密钥的配额单独计算。每个配额适用于在每隔一秒钟的时间间隔内使用给定密钥类型在 AWS 账户 和区域中执行这些操作的所有请求。

- 加密操作（对称）请求速率是在账户和区域中使用对称 KMS 密钥进行加密操作的共享请求配额。此配额适用于使用对称加密密钥和 HMAC 密钥的加密操作，这些密钥也是对称的。

  例如，您可能在共享配额为每秒 10,000 个请求的 AWS 区域 中使用对称 KMS 密钥。当你每秒发出 7,000 个GenerateDataKey请求和每秒 2,000 个解密请求时， AWS KMS 不会限制你的请求。但是，如果您每秒发出 9500 个 `GenerateDataKey` 请求和 1000 个加密请求， AWS KMS 会限制您的请求，因为请求数量超出了共享配额。

  对 自定义密钥存储 中 对称加密 KMS 密钥 的加密操作将会计入账户的加密操作（对称）请求率 和自定义密钥存储的 自定义密钥存储请求限额。
- 加密操作 (RSA) 请求速率 是使用 RSA 非对称 KMS 密钥的加密操作的共享请求配额。

例如，如果请求配额为每秒 500 个操作，您可以使用可以加密和解密的 RSA KMS 密钥发出 200 个 Encrypt 请求和 100 个 Decrypt 请求；另外，通过可以签名和验证的 RSA KMS 密钥发出 50 个 Sign 请求和 150 个 Verify 请求。

- 加密操作 (ECC) 请求速率 是使用椭圆曲线 (ECC) 非对称 KMS 密钥的加密操作的共享请求配额。

  例如，如果请求配额为每秒 300 个操作，您可以使用可以签名和验证的 RSA KMS 密钥发出 100 个签名请求和 200 个验证请求。

- Cryptographic operations (SM — China Regions only) request rate（加密操作（SM – 仅限中国区域）请求速率）是使用 SM 非对称 KMS 密钥的加密操作的共享请求配额。

  例如，如果请求配额为每秒 300 次操作，您可以使用可以加密和解密的 SM2 KMS 密钥发出 100 个 Encrypt 请求和 100 个 Decrypt 请求；另外，通过可以签名和验证的 SM2 KMS 密钥发出 50 个 Sign 请求和 50 个 Verify 请求。

- 自定义密钥存储请求限额是对自定义密钥存储中 KMS 密钥进行加密操作的共享请求限额。此限制针对每个自定义密钥存储单独计算。

  对 自定义密钥存储 中 对称加密 KMS 密钥 的加密操作将会计入账户的加密操作（对称）请求率和自定义密钥存储的 自定义密钥存储请求限额。

不同密钥类型的配额也是单独计算的。例如，在亚太地区（新加坡）区域中，如果同时使用对称 KMS 密钥和非对称 KMS 密钥，则使用对称 KMS 密钥（包括 HMAC 密钥）每秒最多可发出 10000 次调用，另外加上使用 RSA 非对称 KMS 密钥每秒最多可发出 500 次调用，另外再加上使用基于 ECC 的 KMS 密钥每秒最多可发出 300 个请求。

代表您发出的 API 请求

您可以直接发出 API 请求，也可以使用代表您发出 API 请求 AWS KMS 的集成 AWS 服务。该配额对两种类型的请求都适用。

例如，您可以使用借助 KMS 密钥的服务器端加密 (SSE-KMS)，将数据存储在 Amazon S3 中。每次您上传或下载使用 SSE-KMS 加密的 S3 对象时，Amazon S3 都会代表您发出`GenerateDataKey`（用于上传）或`Decrypt`（用于下载）请求。 AWS KMS 这些请求计入您的配额，因此，如果您每秒上传或下载使用 SSE-KM AWS KMS S 加密的 S3 对象的总数超过 5,500 个（或 10,000 或 50,000 个，视您而定 AWS 区域），则会限制这些请求。

跨账户请求

当一个应用程序中的一个应用程序 AWS 账户 使用另一个账户拥有的 KMS 密钥时，它被称为跨账户请求。对于跨账户请求， AWS KMS 会限制发出请求的帐户，而不是拥有 KMS 密钥的账户。例如，如果账户 A 中的应用程序使用账户 B 中的 KMS 密钥，那么仅对该 KMS 密钥的使用应用账户 A 中的配额。

自定义密钥存储请求限额

AWS KMS 维护对自定义密钥存储库中的 KMS 密钥进行加密操作的请求配额。这些请求限额针对每个自定义密钥存储单独计算。

自定义密钥存储请求限额	每个自定义密钥存储的默认值（每秒请求数）	可调整
AWS CloudHSM 密钥库请求配额	1800	否
外部密钥存储 请求限额	1800	是

> **Note**
>
> AWS KMS 自定义密钥库请求配额不会显示在 Service Quotas 控制台中。您无法通过服务限额 API 操作查看或管理这些限额。要请求更改您的外部密钥存储请求限额，请访问 AWS Support 中心 并创建工单。
>
> 如果与 AWS CloudHSM 密钥库关联的 AWS CloudHSM 集群正在处理大量命令，包括那些与自定义密钥存储无关的命令，那么你可能会得到一个 AWS KMS `ThrottlingException`速 lower-than-expected 率。如果发生这种情况，请将请求速率降低到 AWS KMS，减少不相关的负载，或者为 AWS CloudHSM 密钥存储使用专用 AWS CloudHSM 集群。
>
> AWS KMS 报告指标中外部密钥存储请求的`ExternalKeyStoreThrottle` CloudWatch 限制。您可以使用此指标来查看节流模式、创建警报和调整外部密钥存储请求限额。

对自定义密钥存储中的 KMS 密钥进行 加密操作 的请求将计入这两个限额：

- 加密操作（对称）请求率限额（每账户）

对自定义密钥存储中 KMS 密钥进行加密操作的请求将计入每个 AWS 账户 和区域的 `Cryptographic operations (symmetric) request rate` 限额。例如，在美国东部（弗吉尼亚州北部）（us-east-1），每个 AWS 账户 每秒最多可以有 5 万个有关对称 KMS 密钥的请求，包括使用自定义密钥存储中 KMS 密钥的请求。

- 自定义密钥存储请求限额（每自定义密钥存储）

  对自定义密钥存储中 KMS 密钥进行加密操作的请求也将计入每秒 1800 次操作的 `Custom key store request quota`。这些限额针对每个自定义密钥存储单独计算。它们可能包括来自多个 AWS 账户 在自定义密钥存储中使用 KMS 密钥的请求。

例如，在美国东部（弗吉尼亚州北部）（us-east-1）区域对一个自定义密钥存储中 KMS 密钥的加密操作将计入该账户和区域的 `Cryptographic operations (symmetric) request rate` 账户级别限额（每秒 5 万个请求），以及其自定义密钥存储的 `Custom key store request quota`（每秒 1800 个请求）。但是，对自定义密钥存储库中的 KMS 密钥进行管理操作的请求仅适用于其账户级别配额（每秒 15 个请求）。PutKeyPolicy

限制请求 AWS KMS

为了确保 AWS KMS 能够对所有客户的 API 请求提供快速、可靠的响应，它会限制超出特定界限的 API 请求。

当 AWS KMS 拒绝原本可能有效的请求并返回类似以下`ThrottlingException`错误时，就会发生 @@ 限制。

```
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 限制对以下条件的请求。

- 每秒的请求速率超过了账户和区域的 AWS KMS 请求配额。

  例如，如果您账户中的用户在一秒钟内提交 1000 个`DescribeKey`请求，则会在该秒钟内 AWS KMS 限制所有后续`DescribeKey`请求。

  要对限制进行响应，请使用退避和重试策略。此策略是针对某些 AWS SDK 中的 HTTP 400 错误自动实现的。

- 用于更改同一 KMS 密钥状态的请求突发或持续高速率。这种情况通常称为“热键”。

  例如，如果您账户中的某个应用程序持续发送对相同 KMS 密钥的`EnableKey`和`DisableKey`请求，则会 AWS KMS 限制这些请求。即使请求未超过`EnableKey`和`DisableKey`操作的请求限制，request-per-second 也会发生这种限制。

  要响应限制，请调整您的应用程序逻辑，使其只发出必需的请求或合并多个函数的请求。

- 当与密AWS CloudHSM 钥存储库关联的 AWS CloudHSM 集群正在处理大量命令（包括与密钥存储无关的命令）时，对 AWS CloudHSM 密钥存储中 KMS 密 AWS CloudHSM 钥的操作请求可能会受到限制。 lower-than-expected

  （当AWS KMS 集群没有可用的 PKCS #11 会话时，不再限制对密钥库中 KMS 密钥的操作请求。AWS CloudHSM AWS CloudHSM 相反，它会抛出，`KMSInternalException`并建议您重试请求。）

要查看请求速率的趋势，请使用 Service Quotas 控制台。您还可以创建一个 Amazon CloudWatch 警报，当您的请求率达到配额值的特定百分比时，提醒您。有关详情，请参阅AWS 安全博客 CloudWatch中的使用 Service Quotas 和 Amazon 管理您的 AWS KMS API 请求速率。

除密钥策略文档大小资源 AWS KMS 配额、按需轮换资源配额和密AWS CloudHSM 钥存储请求配额外，所有配额均可调整。要请求提高限额，请参阅《服务限额用户指南》中的请求提高限额。要申请减少配额、更改未在 Service Quotas 中列出的配额，或者在没有服务配额 AWS 区域 的情况下更改配额，请访问AWS Support 中心并创建案例。 AWS KMS

> **Note**
>
> AWS KMS 自定义密钥库请求配额不会显示在 Service Quotas 控制台中。您无法通过服务限额 API 操作查看或管理这些限额。要请求更改您的外部密钥存储请求限额，请访问 AWS Support 中心 并创建工单。

AWS 服务如何使用 AWS KMS

许多 AWS 服务使用 AWS KMS 来对数据加密提供支持。如果某项 AWS 服务与 AWS KMS 相集成，您即可使用您账户中的 AWS KMS keys 保护该服务为您接收、存储或管理的数据。有关与 AWS KMS 集成的 AWS 服务的完整列表，请参阅 AWS 服务集成。

以下主题详细讨论了特定服务如何使用 AWS KMS（包括其支持的 KMS 密钥）、这些服务如何管理数据密钥、所需的权限、以及如何跟踪您账户中每项服务使用 KMS 密钥的情况。

> **Important**
>
> 与 AWS KMS 集成的 AWS 服务仅使用对称加密 KMS 密钥加密您的数据。这些服务不支持使用非对称 KMS 密钥进行加密。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

主题

AWS CloudTrail 如何使用 AWS KMS

您可以使用 AWS CloudTrail 来记录 AWS 账户 的 AWS API 调用和其他活动，以及将已记录的信息保存到您选择的 Amazon Simple Storage Service (Amazon S3) 存储桶中的日志文件。默认情况下， CloudTrail 放入 S3 存储桶的日志文件使用服务器端加密和 Amazon S3 托管加密密钥进行加密 (SSE-S3)。但是，您可以选择改为使用具有 KMS 密钥的服务器端加密 (SSE-KMS)。要了解如何使用加密 CloudTrail 日志文件AWS KMS，请参阅用户指南中的使用 AWS KMS keys(SSE-KMS) 加密 CloudTrail 日志文件。AWS CloudTrail

> **Important**
>
> AWS CloudTrail 和 Amazon S3 仅支持对称 AWS KMS keys。您不能使用非对称 KMS 密钥来加密您的 CloudTrail 日志。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

CloudTrail 读取或写入使用 SSE-KMS 密钥加密的日志文件时，您无需支付密钥使用费。但是，当您访问使用 SSE-KMS 密钥加密的 CloudTrail 日志文件时，您需要支付密钥使用费。有关 AWS KMS 定价的信息，请参阅 AWS Key Management Service 定价。有关 CloudTrail 定价的信息，请参阅《AWS CloudTrail用户指南》中的定AWS CloudTrail价和管理成本。

主题

- 了解何时使用您的 KMS 密钥

了解何时使用您的 KMS 密钥

使用基于 Amazon S3 的AWS KMS功能对 CloudTrail 日志文件进行加密，该功能称为服务器端加密 AWS KMS key (SSE-KMS)。要了解 SSE-KMS 的详情，请参阅本指南中的 Amazon Simple Storage Service (Amazon S3) 如何使用 AWS KMS，或 Amazon Simple Storage Service 用户指南中通过具有 KMS 密钥的服务器端加密 (SSE-KMS) 保护数据。

当您配置AWS CloudTrail为使用 SSE-KMS 加密日志文件时， CloudTrail Amazon S3 AWS KMS keys 会在您对这些服务执行某些操作时使用您的日志文件。以下部分说明了这些服务将何时以及如何使用您的 KMS 密钥，并提供了您可以用于验证此说明的其他信息。

导致 CloudTrail 和 Amazon S3 使用您的 KMS 密钥的操作

- 您配置 CloudTrail 为使用您的日志文件进行加密 AWS KMS key

- CloudTrail 将日志文件放入您的 S3 存储桶
- 从 S3 存储桶中获得加密的日志文件

您配置 CloudTrail 为使用您的日志文件进行加密 AWS KMS key

当您更新 CloudTrail配置以使用您的 KMS 密钥时， CloudTrail 会向发送GenerateDataKey请求，AWS KMS以验证 KMS 密钥是否存在以及是否 CloudTrail 有权使用它进行加密。 CloudTrail 不使用生成的数据密钥。

GenerateDataKey 请求包括加密上下文的以下信息：

- 跟踪的亚马逊资源名称 (ARN) CloudTrail
- S3 存储桶的 ARN 和 CloudTrail 日志文件的传送路径

该GenerateDataKey请求会在您的 CloudTrail 日志中生成一个类似于以下示例的条目。当你看到这样的日志条目时，你可以确定那个 CloudTrail (1) 为特定的跟踪 AWS KMS (2) 调用了 () GenerateDataKey 操作 (4))。3 AWS KMS在特定的 KMS 密钥下创建了数据密钥 (5))。

> **Note**
>
> 您可能需要滚动到右侧以查看以下示例日志条目中的某些标注。

```
{
  "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 将日志文件放入您的 S3 存储桶

每次 CloudTrail 将日志文件放入您的 S3 存储桶时，Amazon S3 都会代表向发送GenerateDataKey请求 CloudTrail。AWS KMS为了响应该请求，AWS KMS 会生成一个唯一的数据密钥，然后将该数据密钥的两个副本发送给 Amazon S3，一个为明文，另一个则使用指定的 KMS 密钥进行了加密。Amazon S3 使用纯文本数据密钥对 CloudTrail 日志文件进行加密，然后在使用后尽快从内存中删除纯文本数据密钥。Amazon S3 将加密的数据密钥作为元数据存储在加密的 CloudTrail 日志文件中。

GenerateDataKey 请求包括加密上下文的以下信息：

- 跟踪的亚马逊资源名称 (ARN) CloudTrail
- S3 对象（ CloudTrail 日志文件）的 ARN

每个GenerateDataKey请求都会在您的 CloudTrail 日志中生成一个条目，类似于以下示例。当你看到这样的日志条目时，你可以确定 CloudTrail (1) 为特定跟踪 AWS KMS (2) 调用了 (3) GenerateDataKey 操作 (4)，以保护特定的日志文件 (5)。AWS KMS在指定的 KMS 密钥 (6) 下创建了数据密钥，在同一个日志条目中显示了两次。

> **Note**
>
> 您可能需要滚动到右侧以查看以下示例日志条目中的某些标注。

```
{
  "eventVersion": "1.02",
  "userIdentity": {
```

```
    "type": "AssumedRole",
    "principalId": "AROACKCEVSQ6C2EXAMPLE:i-34755b85",
    "arn": "arn:aws:sts::086441151436:assumed-role/AWSCloudTrail/
i-34755b85",
    "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",
  "eventName":
 "GenerateDataKey",
  "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",
      "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"
    },
    "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "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",
    "accountId": "111122223333"
  }],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333"
}
```

从 S3 存储桶中获得加密的日志文件

每次您从 S3 存储桶获取加密的 CloudTrail 日志文件时，Amazon S3 都会代表您向发送解密该日志文件的加密数据密钥的Decrypt请求。AWS KMS为了响应该请求，AWS KMS 使用您的 KMS 密钥将数据密钥解密，然后将明文数据密钥发送到 Amazon S3。Amazon S3 使用纯文本数据密钥解密 CloudTrail 日志文件，然后在使用后尽快从内存中删除纯文本数据密钥。

Decrypt 请求包括加密上下文的以下信息：

- 跟踪的亚马逊资源名称 (ARN) CloudTrail
- S3 对象（ CloudTrail 日志文件）的 ARN

每个Decrypt请求都会在您的 CloudTrail 日志中生成一个条目，类似于以下示例。
当您看到与此类似的日志条目时，便可以确定您的 AWS 账户中的某个 IAM 用户
（ 1 ）
调用了特定跟踪
（ 2 ）
和特定日志文件
（ 3 ）
的 AWS
KMS（ 4
操作
（ 5 ）。
KMS 使用特定 KMS 密钥
（ 6 ）
解密了数据密钥。

> **Note**
>
> 您可能需要滚动到右侧以查看以下示例日志条目中的某些标注。

```
{
  "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",
    "accountId": "111122223333"
  }],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

Amazon DynamoDB 如何使用 AWS KMS

Amazon DynamoDB 是一种完全托管的 NoSQL 数据库服务。DynamoDB 与 AWS Key Management Service (AWS KMS) 集成以支持静态加密服务器端加密功能。

利用静态加密，DynamoDB 可以透明方式对 DynamoDB 表中的所有客户数据进行加密，包括其主键及本地和全局二级索引，只要该表已保存到磁盘。（如果表具有排序键，则标记范围边界的一些排序键将以明文形式存储在表元数据中。）当您访问表时，DynamoDB 会以透明方式解密表数据。您无需更改应用程序即可使用或管理加密表。

此外，在将 DynamoDB 流、全局表和备份保存到持久性媒体时，静态加密可以保护这些对象。有关本主题中表的语句也适用于这些对象。

将对所有 DynamoDB 表进行加密。没有为新表或现有表启用或禁用加密的选项。默认情况下，所有表都在 DynamoDB 服务账户中的 AWS 拥有的密钥 下加密。但是，您可以选择一个选项来为您账户中的 DynamoDB 在客户托管密钥或 AWS 托管式密钥 下对部分或全部表进行加密。

有关 Amazon DynamoDB 对 KMS 密钥的支持的详细信息，请参阅《Amazon DynamoDB 开发人员指南》中的静态 DynamoDB 加密。

Amazon Elastic Block Store (Amazon EBS) 如何使用 AWS KMS

本主题详细讨论了 Amazon Elastic Block Store (Amazon EBS) 如何使用 AWS KMS 来加密卷和快照。有关加密 Amazon EBS 卷的基本说明，请参阅 Amazon EBS 加密。

主题

- Amazon EBS 加密
- 使用 KMS 密钥和数据密钥
- Amazon EBS 加密上下文

- 检测 Amazon EBS 故障
- 使用 AWS CloudFormation 创建加密的 Amazon EBS 卷

Amazon EBS 加密

将加密的 Amazon EBS 卷附加到支持的 Amazon Elastic Compute Cloud (Amazon EC2)实例类型时，该卷上静态存储的数据、磁盘输入/输出以及从加密卷创建的快照都会被加密。加密在托管 Amazon EC2 实例的服务器上进行。

所有 Amazon EBS 卷类型都支持此功能。您可以通过与访问其他卷相同的方式来访问加密卷；加密和解密以透明方式处理，您的 EC2 实例或您的应用程序都无需执行其他任何操作。加密 卷的快照会自动加密，通过加密 快照创建的卷也会自动加密。

EBS 卷的加密状态在您创建该卷时就已经确定了。您不能更改现有卷的加密状态。但是，您可以在加密卷和未加密卷之间迁移数据，并在复制快照时应用新的加密状态。

默认情况下，Amazon EBS 支持可选加密。您可以自动启用对您的 AWS 账户 和区域中所有新 EBS 卷和快照副本的加密。此配置设置不会影响现有卷或快照。有关详细信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南或适用于 Windows 实例的 Amazon EC2 用户指南中的默认加密。

使用 KMS 密钥和数据密钥

当您创建一个加密的 Amazon EBS 卷时，您可以指定 AWS KMS key。默认情况下，Amazon EBS 将在您的账户 (aws/ebs) 中将 AWS 托管式密钥 Amazon EBS。不过，您可以指定自己创建和管理的客户托管的密钥。

要使用客户托管的密钥，您必须向 Amazon EBS 授予代表您使用 KMS 密钥的权限。有关所需权限的列表，请参阅适用于 Linux 实例的 Amazon EC2 用户指南或适用于 Windows 实例的 Amazon EC2 用户指南中的 IAM 用户的权限。

> **Important**
>
> Amazon EBS 仅支持对称 KMS 密钥。不能使用非对称 KMS 密钥来加密 Amazon EBS 卷。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

对于每个卷，Amazon EBS 要求 AWS KMS 生成一个使用您指定的 KMS 密钥进行加密的唯一数据密钥。Amazon EBS 使用该卷存储加密数据密钥。然后，当您将卷附加到 Amazon EC2 实例时，Amazon EBS 会调用 AWS KMS 来解密数据密钥。Amazon EBS 使用管理程序内存中的明文数据

密钥来加密卷的所有磁盘输入/输出。有关详细信息，请参阅适用于 Linux 实例的 Amazon EC2 用户指南或适用于 Windows 实例的 Amazon EC2 用户指南中的 EBS 加密工作原理。

Amazon EBS 加密上下文

在对的请求GenerateDataKeyWithoutPlaintext和解密请求中，AWS KMSAmazon EBS 使用带有名称/值对的加密上下文，用于标识请求中的卷或快照。加密上下文中的名称不会发生变化。

加密上下文 是一组包含任意非机密数据的键值对。在请求中包含加密上下文以加密数据时，AWS KMS 以加密方式将加密上下文绑定到加密的数据。要解密数据，您必须传入相同的加密上下文。

对于所有卷以及通过 Amazon EBS CreateSnapshot操作创建的加密快照，Amazon EBS 使用卷 ID 作为加密上下文值。在 CloudTrail 日志条目的 `requestParameters` 字段中，加密上下文类似于以下内容：

```
"encryptionContext": {
  "aws:ebs:id": "vol-0cfb133e847d28be9"
}
```

对于通过 Amazon EC2 CopySnapshot操作创建的加密快照，Amazon EBS 使用快照 ID 作为加密上下文值。在 CloudTrail 日志条目的 `requestParameters` 字段中，加密上下文类似于以下内容：

```
"encryptionContext": {
  "aws:ebs:id": "snap-069a655b568de654f"
}
```

检测 Amazon EBS 故障

要创建加密 EBS 卷或将卷附加到 EC2 实例，Amazon EBS 和 Amazon EC2 基础设施必须能够使用您为 EBS 卷加密指定的 KMS 密钥。当 KMS 密钥不可用时—例如，当其密钥状态处于 `Enabled` 时—卷创建或卷附加操作将失败。

在这种情况下，Amazon EBS 会向亚马逊发送一个事件 EventBridge（以前称为“ CloudWatch 事件”），以通知您有关失败的信息。在中 EventBridge，您可以建立触发自动操作以响应这些事件的规则。有关更多信息，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》中的 Amazon Ebs CloudWatch 活动，尤其是以下部分：

- 附加或重新附加卷时加密密钥无效
- 创建卷时加密密钥无效

要修复这些故障，请确保您为 EBS 卷加密指定的 KMS 密钥处于启用状态。为此，请先查看 KMS 密钥以确定其当前密钥状态（AWS Management Console 中的 Status（状态）列）。然后，请参阅以下任一链接中的信息：

- 如果 KMS 密钥的密钥状态为已禁用，则启用它。
- 如果 KMS 密钥的密钥状态为待导入，则导入密钥材料。
- 如果 KMS 密钥的密钥状态为待删除，则取消密钥删除。

使用 AWS CloudFormation 创建加密的 Amazon EBS 卷

您可以使用 AWS CloudFormation 创建加密的 Amazon EBS 卷。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的 AWS::EC2::Volume。

Amazon Elastic Transcoder 如何使用 AWS KMS

您可以使用 Amazon Elastic Transcoder 将存储在 Amazon S3 存储桶中的媒体文件转换为消费者播放设备所要求的格式。对于输入文件和输出文件，均可以进行加密和解密。以下各部分讨论如何使用 AWS KMS 执行这两个过程。

主题

- 为输入文件加密
- 将输入文件解密
- 为输出文件加密
- HLS 内容保护
- Elastic Transcoder 加密上下文

为输入文件加密

您必须先创建 Amazon S3 存储桶并将您的媒体文件上传到该存储桶中，然后才可以使用 Elastic Transcoder。您可以在上传前使用 AES 客户端加密为该文件加密，也可以在上传后使用 Amazon S3 服务器端加密为该文件加密。

如果您选择使用 AES 的客户端加密，则您需负责在将文件上传到 Amazon S3 之前为文件加密，并且您必须为 Elastic Transcoder 提供对加密密钥的访问权限。通过使用对称 AWS KMS AWS KMS key 保护您用于为媒体文件加密的 AES 加密密钥，即可实现此目的。

如果您选择服务器端加密，即表示您要允许 Amazon S3 代表您对所有文件进行加密和解密。您可以将 Amazon S3 配置为使用以下三种不同的加密密钥类型之一来保护用于为您的文件加密的唯一数据密钥：

- Amazon S3 密钥，Amazon S3 拥有和管理的加密密钥。它不属于您的 AWS 账户 的一部分。
- Amazon S3 的 AWS 托管式密钥，该 KMS 密钥属于您账户的一部分，但由 AWS 创建和管理
- 您使用 AWS KMS 创建的任何对称客户托管密钥

> **Important**
>
> 对于客户端和服务器端加密，Elastic Transcoder 只支持对称 KMS 密钥。不能使用非对称 KMS 密钥来加密您的 Elastic Transcoder 文件。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

您可以使用 Amazon S3 控制台或相应的 Amazon S3 API 启用加密并指定密钥。有关 Amazon S3 如何执行加密的更多信息，请参阅 Amazon Simple Storage Service 用户指南中的使用具有 KMS 密钥的服务器端加密 (SSE-KMS) 保护数据。

在使用账户中的 Amazon S3 的 AWS 托管式密钥 或客户托管密钥来保护输入文件时，Amazon S3 和 AWS KMS 将通过以下方式进行交互：

1. Amazon S3 请求明文数据密钥以及使用指定 KMS 密钥加密的数据密钥的副本。
2. AWS KMS 创建数据密钥，使用指定的 KMS 密钥为其进行加密，然后将明文数据密钥和加密的数据密钥发送到 Amazon S3。
3. Amazon S3 使用明文数据密钥为媒体文件加密，然后将该文件存储在指定的 Amazon S3 存储桶中。
4. Amazon S3 将加密的数据密钥与加密的媒体文件一起存储。

将输入文件解密

如果您选择使用 Amazon S3 服务器端加密来为输入文件加密，则 Elastic Transcoder 不会将该文件解密。相反，Elastic Transcoder 依赖于 Amazon S3 执行解密，具体取决于您创建任务和管道时指定的设置。

可用的设置组合如下：

加密模式	AWS KMS 密钥	含义
S3	默认	Amazon S3 创建并管理用于为媒体文件加密和解密的密钥。此过程对用户是不透明的。
S3-AWS-KMS	默认	Amazon S3 使用由您的账户中用于 Amazon S3 的默认 AWS 托管式密钥 加密的数据密钥来为媒体文件加密。
S3-AWS-KMS	自定义 (使用 ARN)	Amazon S3 使用由指定的客户托管密钥加密的数据密钥来为媒体文件加密。

如果已指定 S3-AWS-KMS，Amazon S3 和 AWS KMS 采用以下方式协同工作来执行解密。

1. Amazon S3 向 AWS KMS 发送加密的数据密钥。
2. AWS KMS 使用适当的 KMS 密钥为数据密钥解密，然后将明文数据密钥发送回到 Amazon S3。
3. Amazon S3 使用明文数据密钥将密文解密。

如果您选择采纳 AES 密钥的客户端加密，Elastic Transcoder 将从 Amazon S3 存储桶中检索加密的文件并将其解密。Elastic Transcoder 使用您创建管道时指定的 KMS 密钥将 AES 密钥解密，然后使用 AES 密钥将媒体文件解密。

为输出文件加密

Elastic Transcoder 根据您创建任务和管道时是如何指定加密设置的为输出文件加密。可用选项如下：

加密模式	AWS KMS 密钥	含义
S3	默认	Amazon S3 创建并管理用于为输出文件加密的密钥。
S3-AWS-KMS	默认	Amazon S3 使用 AWS KMS 创建并通过 AWS 托管式密钥

加密模式	AWS KMS 密钥	含义
		为您的账户中的 Amazon S3 加密的数据密钥。
S3-AWS-KMS	自定义 (使用 ARN)	Amazon S3 使用由 ARN 指定的客户托管密钥加密的数据密钥来为媒体文件加密。
AES-	默认	Elastic Transcoder 使用您的账户中用于 Amazon S3 的 AWS 托管式密钥 为您提供的指定 AES 密钥解密，并使用该密钥为输出文件加密。
AES-	自定义 (使用 ARN)	Elastic Transcoder 使用 ARN 指定的客户托管密钥为您提供的指定 AES 密钥解密，并使用该密钥为输出文件加密。

当您指定使用账户中 Amazon S3 的 AWS 托管式密钥 或客户托管密钥来加密输出文件时，Amazon S3 和 AWS KMS 将通过以下方式进行交互：

1. Amazon S3 请求明文数据密钥以及使用指定 KMS 密钥加密的数据密钥的副本。
2. AWS KMS 创建数据密钥，使用 KMS 密钥为其进行加密，然后将明文数据密钥和加密的数据密钥发送到 Amazon S3。
3. Amazon S3 使用该数据密钥为媒体文件加密，并将其存储在指定的 Amazon S3 存储桶中。
4. Amazon S3 将加密的数据密钥与加密的媒体文件一起存储。

当您指定使用您提供的 AES 密钥为输出文件解密时，必须使用 AWS KMS 中的 KMS 密钥为该 AES 密钥加密。Elastic Transcoder、AWS KMS 和您使用以下方式进行交互：

1. 您可以通过在 AWS KMS API 中调用 Encrypt 操作来加密 AES 密钥。AWS KMS 使用指定的 KMS 密钥为密钥加密。您在创建管道时指定要使用的 KMS 密钥。
2. 您在创建 Elastic Transcoder 作业时指定包含加密的 AES 密钥的文件。

3. Elastic Transcoder 通过在 AWS KMS API 中调用 Decrypt 操作来为密钥解密，将加密的密钥以密文形式传递。
4. Elastic Transcoder 使用解密的 AES 密钥来为输出媒体文件加密，然后从内存中删除已解密的 AES 密钥。仅将您最初在任务中定义的加密副本保存到磁盘。
5. 您可以下载加密的输出文件，并使用您定义的原始 AES 密钥在本地将其解密。

> **Important**
>
> AWS 不会存储您的私有加密密钥。因此，请务必妥善安全地管理您的密钥。如果您丢失了加密密钥，将无法解密数据。

HLS 内容保护

HTTP 实时流 (HLS) 是自适应流式处理协议。Elastic Transcoder 通过将您的输入文件拆分为更小的名为媒体区段的单个文件来支持 HLS。一组相应的单个媒体区段包含以不同比特率编码的相同材料，使玩家可以选择最适合可用带宽的流。Elastic Transcoder 还将创建播放列表，列表中包含可流式处理的各种区段的元数据。

当您启用 HLS 内容保护 时，将使用 128 位 AES 加密密钥为每个媒体区段加密。在查看内容时，玩家可在播放过程中下载密钥并为媒体区段解密。

使用两种类型的密钥：KMS 密钥和数据密钥。您必须创建 KMS 密钥以用于为数据密钥加密和解密。Elastic Transcoder 使用该数据密钥为媒体区段加密和解密。数据密钥必须为 AES-128。对于相同内容的所有变体和区段，使用相同数据密钥进行加密。您可以提供数据密钥，或者让 Elastic Transcoder 为您创建数据密钥。

在以下时间点，可以使用 KMS 密钥为数据密钥加密。

- 如果您提供自己的数据密钥，则必须在将其传递给 Elastic Transcoder 之前对其进行加密。
- 如果您请求 Elastic Transcoder 生成数据密钥，则 Elastic Transcoder 会为您将数据密钥加密。

在以下时间点，可以使用 KMS 密钥将数据密钥解密。

- Elastic Transcoder 在需要使用数据密钥为输出文件加密或为输入文件解密时将您提供的数据密钥解密。
- 您将解密由 Elastic Transcoder 生成的数据密钥，并使用它来将输出文件解密。

有关更多信息，请参阅 Amazon Elastic Transcoder 开发人员指南中的 HLS 内容保护。

Elastic Transcoder 加密上下文

加密上下文 是一组包含任意非机密数据的键值对。在请求中包含加密上下文以加密数据时，AWS KMS 以加密方式将加密上下文绑定到加密的数据。要解密数据，您必须传入相同的加密上下文。

Elastic Transcoder 在所有 AWS KMS API 请求中使用相同的加密上下文，以生成数据密钥、加密和解密。

```
"service" : "elastictranscoder.amazonaws.com"
```

加密上下文写入 CloudTrail 日志是为了帮助您了解给定的 AWS KMS KMS 密钥是如何使用的。在 CloudTrail 日志文件`requestParameters`字段中，加密上下文类似于以下内容：

```
"encryptionContext": {
  "service" : "elastictranscoder.amazonaws.com"
}
```

有关如何配置 Elastic Transcoder 作业以使用其中一个受支持的加密选项的更多信息，请参阅 Amazon Elastic Transcoder 开发人员指南中数据加密选项。

Amazon EMR 如何使用 AWS KMS

当您使用 Amazon EMR 集群时，您可以将集群配置为静态加密数据，然后将其保存到持久性存储位置。您可以在 EMR 文件系统 (EMRFS) 上、在群集节点的存储卷上，或同时在这两者上对静态数据进行加密。要加密静态数据，您可以使用 AWS KMS key。以下主题介绍 Amazon EMR 集群如何使用 KMS 密钥来加密静态数据。

> **Important**
>
> Amazon EMR 仅支持对称 KMS 密钥。不能使用非对称 KMS 密钥来加密 Amazon EMR 集群中的静态数据。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

Amazon EMR 集群也可以加密传输中的数据，这意味着集群会先加密数据，然后将其通过网络发送。您不能使用 KMS 密钥加密传输中的数据。有关更多信息，请参阅 Amazon EMR 管理指南中的传输中的数据加密。

有关 Amazon EMR 中所有可用加密选项的更多信息，请参阅 Amazon EMR 管理指南中的加密选项。

主题

在 EMR 文件系统 (EMRFS) 上加密数据

Amazon EMR 集群使用两个分布式文件系统：

- Hadoop Distributed File System（HDFS）。HDFS 加密不会使用 AWS KMS 中的 KMS 密钥。
- EMR 文件系统 (EMRFS)。EMRFS 是一种 HDFS 实施，使 Amazon EMR 集群能够在 Amazon Simple Storage Service (Amazon S3) 中存储数据。EMRFS 支持四种加密选项，其中两种会使用 AWS KMS 中的 KMS 密钥。有关全部四种 EMRFS 加密选项的更多信息，请参阅 Amazon EMR 管理指南中的加密选项。

使用 KMS 密钥的两个 EMRFS 加密选项使用 Amazon S3 提供的以下加密功能：

- 使用具有 AWS Key Management Service 的服务器端加密 (SSE-KMS) 保护数据。Amazon EMR 集群会将数据发送到 Amazon S3。Amazon S3 使用 KMS 密钥加密数据，然后将其保存到 S3 存储桶。有关其工作方式的更多信息，请参阅使用 SSE-KMS 在 EMRFS 上加密数据的过程。
- 使用客户端加密保护数据 (CSE-KMS)。Amazon EMR 中的数据通过 AWS KMS key 进行加密，然后发送到 Amazon S3 进行存储。有关其工作方式的更多信息，请参阅使用 CSE-KMS 在 EMRFS 上加密数据的过程。

当您将 Amazon EMR 集群配置为使用 KMS 密钥在 EMRFS 上加密数据时，请选择您希望 Amazon S3 或 Amazon EMR 集群使用的 KMS 密钥。借助 SSE-KMS，您可以为 Amazon S3 选择 AWS 托管式密钥（具有别名 aws/s3）或您创建的对称客户托管密钥。使用客户端加密时，必须选择您创建的对称客户托管式密钥。当您选择客户托管密钥时，您必须确保 Amazon EMR 集群有权使用该 KMS 密钥。有关更多信息，请参阅 Amazon EMR 管理指南中的将 AWS KMS keys 用于加密。

对于服务器端和客户端加密这两者而言，您选择的 KMS 密钥就是信封加密工作流程中的根密钥。数据使用唯一的数据密钥加密，该密钥通过 AWS KMS 中的 KMS 密钥进行加密。已加密的数据及其数据密钥的加密副本将作为单个加密对象共同存储在 S3 存储桶中。有关其工作方式的更多信息，请参阅以下主题。

主题

使用 SSE-KMS 在 EMRFS 上加密数据的过程

当您将 Amazon EMR 集群配置为使用 SSE-KMS 时，加密过程的工作方式如下所示：

1. 集群将数据发送到 Amazon S3，以存储在 S3 存储桶中。
2. Amazon S3 向发送GenerateDataKey请求AWS KMS，指定您在将集群配置为使用 SSE-KMS 时选择的 KMS 密钥的密钥 ID。该请求包含加密上下文；有关更多信息，请参阅加密上下文。
3. AWS KMS 生成一个唯一数据加密密钥（数据密钥），然后将此数据密钥的两个副本发送到 Amazon S3。一个副本未加密（明文），另一个副本使用 KMS 密钥加密。
4. Amazon S3 使用明文数据密钥加密它在步骤 1 中收到的数据，并在使用后尽快从内存中删除该明文数据密钥。
5. Amazon S3 将已加密的数据及数据密钥的加密副本作为单个加密对象共同存储在 S3 存储桶中。

解密过程的工作方式如下所示：

1. 群集从 S3 存储桶请求加密的数据对象。
2. Amazon S3 从 S3 对象提取加密的数据密钥，然后使用 Decrypt 请求将已加密的数据密钥发送给 AWS KMS。该请求包括一个加密上下文。
3. AWS KMS 借助加密数据密钥时使用的同一 KMS 密钥解密该加密数据密钥，然后将已解密的（明文）数据密钥发送到 Amazon S3。
4. Amazon S3 使用明文数据密钥解密已加密的数据，并在使用后尽快从内存中删除该明文数据密钥。
5. Amazon S3 将解密数据发送给集群。

使用 CSE-KMS 在 EMRFS 上加密数据的过程

当您将 Amazon EMR 集群配置为使用 CSE-KMS 时，加密过程的工作方式如下所示：

1. 当集群准备好在 Amazon S3 中存储数据时，它会向发送GenerateDataKey请求AWS KMS，指定您在将集群配置为使用 CSE-KMS 时选择的 KMS 密钥的密钥 ID。该请求包含加密上下文；有关更多信息，请参阅加密上下文。

2. AWS KMS 生成一个唯一数据加密密钥（数据密钥），然后将此数据密钥的两个副本发送到群集。一个副本未加密（明文），另一个副本使用 KMS 密钥加密。
3. 群集使用明文数据密钥加密数据，并在使用后尽快从内存中删除该明文数据密钥。
4. 群集将已加密的数据及数据密钥的加密副本组合为单个加密对象。
5. 集群将加密的对象发送给 Amazon S3 进行存储。

解密过程的工作方式如下所示：

1. 群集从 S3 存储桶请求加密的数据对象。
2. Amazon S3 将加密的对象发送给集群。
3. 群集从加密的对象提取加密的数据密钥，然后使用 AWS KMSDecrypt 请求将已加密的数据密钥发送给 。该请求包括加密上下文。
4. AWS KMS 借助加密数据密钥时使用的同一 KMS 密钥解密该加密数据密钥，然后将已解密的（明文）数据密钥发送到集群。
5. 群集使用明文数据密钥解密已加密的数据，并在使用后尽快从内存中删除该明文数据密钥。

在集群节点的存储卷上加密数据

Amazon EMR 集群是 Amazon Elastic Compute Cloud（Amazon EC2）实例的集合。群集中的每个实例称作群集节点或节点。每个节点都可以有两类存储卷：实例存储卷和 Amazon Elastic Block Store (Amazon EBS) 卷。您可以将群集配置为使用 Linux Unified Key Setup (LUKS) 来加密节点上的两类存储卷 (但不包括每个节点的启动卷)。这称为本地磁盘加密。

在为集群启用本地磁盘加密后，您可以选择使用 AWS KMS 中的 KMS 密钥加密 LUKS 密钥。您必须选择您创建的客户托管密钥；不能使用 AWS 托管式密钥。如果您选择客户托管密钥，您必须确保 Amazon EMR 集群有权使用该 KMS 密钥。有关更多信息，请参阅 Amazon EMR 管理指南中的将 AWS KMS keys 用于加密。

当您使用 KMS 密钥启用本地磁盘加密时，加密过程的工作方式如下所示：

1. 当每个群集节点启动时，它会向发送GenerateDataKey请求AWS KMS，指定您在为群集启用本地磁盘加密时选择的 KMS 密钥的密钥 ID。
2. AWS KMS 生成一个唯一数据加密密钥（数据密钥），然后将此数据密钥的两个副本发送到节点。一个副本未加密（明文），另一个副本使用 KMS 密钥加密。
3. 该节点将明文数据密钥的 base64 编码版本作为保护 LUKS 密钥的密码。节点会将加密的数据密钥副本保存在启动卷上。

4. 如果节点重启，重启节点会使用 AWS KMSDecrypt 请求将已加密的数据密钥发送到 。
5. AWS KMS 借助加密数据密钥时使用的同一 KMS 密钥解密该加密数据密钥，然后将已解密的（明文）数据密钥发送到节点。
6. 该节点将明文数据密钥的 base64 编码版本作为解锁 LUKS 密钥的密码。

加密上下文

与 AWS KMS 集成的每项 AWS 服务在使用 AWS KMS 生成数据密钥或者加密或解密数据时都可以指定加密上下文。加密上下文是 AWS KMS 检查数据完整性时使用的额外的身份验证信息。当服务为加密操作指定加密上下文时，它还必须为对应的解密操作指定同一加密上下文，否则解密会失败。加密上下文也将写入 AWS CloudTrail 日志文件中，这可以帮助您了解为什么要使用指定的 KMS 密钥。

以下部分介绍每个使用 KMS 密钥的 Amazon EMR 加密场景中使用的加密上下文。

使用 SSE-KMS 的 EMRFS 加密的加密上下文

借助 SSE-KMS，Amazon EMR 集群将数据发送到 Amazon S3，然后，Amazon S3 使用 KMS 密钥加密数据，然后将其存储到 S3 存储桶中。在本例中，Amazon S3 使用 S3 对象的亚马逊资源名称 (ARN) 作为其发送到的每个GenerateDataKey和解密请求的加密上下文。AWS KMS以下示例显示了 Amazon S3 使用的加密上下文的 JSON 表示形式。

```
{ "aws:s3:arn" : "arn:aws:s3:::S3_bucket_name/S3_object_key" }
```

使用 CSE-KMS 的 EMRFS 加密的加密上下文

借助 CSE-KMS，Amazon EMR 集群使用 KMS 密钥加密数据，然后将其发送到 Amazon S3 进行存储。在这种情况下，集群使用 KMS 密钥的 Amazon 资源名称 (ARN) 作为其发送到的每个密钥GenerateDataKey和解密请求的加密上下文。AWS KMS以下示例显示了群集使用的加密上下文的 JSON 表示形式。

```
{ "kms_cmk_id" : "arn:aws:kms:us-
east-2:111122223333:key/0987ab65-43cd-21ef-09ab-87654321cdef" }
```

使用 LUKS 的本地磁盘加密的加密上下文

当 Amazon EMR 集群使用 LUKS 的本地磁盘加密时，群集节点不会使用它们发送到的GenerateDataKey和解密请求来指定加密上下文。AWS KMS

AWS Nitro Enclaves 如何使用 AWS KMS

AWS KMS 支持 AWS Nitro Enclaves 的加密证明。支持 AWS Nitro Enclaves 的应用程序使用 Enclave 的已签名证明文档调用以下 AWS KMS 加密操作。这些 AWS KMS API 可验证证明文档是否来自 Nitro Enclave。然后，这些 API 不是在响应中返回明文数据，而是使用证明文档中的公有密钥对明文进行加密，并返回只能通过 Enclave 中相应的私有密钥解密的加密文字。

- Decrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateRandom

下表显示了对 Nitro Enclave 请求的响应与每个 API 操作的标准响应有何不同。

AWS KMS 操作	标准响应	对 AWS Nitro Enclaves 的响应
`Decrypt`	返回明文数据	返回证明文档中由公有密钥加密的明文数据
`GenerateDataKey`	返回数据密钥的明文副本 （还会返回由 KMS 密钥加密的数据密钥副本）	返回证明文档中由公有密钥加密的数据密钥副本 （还会返回由 KMS 密钥加密的数据密钥副本）
`GenerateDataKeyPair`	返回私有密钥的明文副本 （还会返回公有密钥和由 KMS 密钥加密的私有密钥副本）	返回证明文档中由公有密钥加密的私有密钥副本 （还会返回公有密钥和由 KMS 密钥加密的私有密钥副本）
`GenerateRandom`	返回一个随机字节字符串	返回证明文档中由公有密钥加密的随机字节字符串

AWS KMS 支持策略条件键，您可以使用这些键根据证明文件的内容允许或拒绝对 AWS KMS 密钥执行 Enclave 操作。您还可以在 AWS CloudTrail 日志中监控对 AWS KMS Nitro Enclave 的请求。

主题

如何为 Nitro Enclave 调用 AWS KMS API

要为 Nitro Enclave 调用 AWS KMS API，请使用请求中的 `Recipient` 参数为 Enclave 提供已签名的证明文档以及用于 Enclave 的公有密钥的加密算法。当请求中包含带有已签名证明文档的 `Recipient` 参数时，响应将包含一个具有由公有密钥加密的加密文字的 `CiphertextForRecipient` 字段。明文字段为空。

`Recipient` 参数必须指定来自 AWS Nitro Enclave 的已签名证明文档。AWS KMS 依赖于 Enclave 证明文档的数字签名来证明请求中的公有密钥来自于有效的 Enclave。您不能提供自己的证书来对证明文档进行数字签名。

要指定 `Recipient` 参数，请使用 AWS Nitro Enclaves 开发工具包 或任何 AWS 开发工具包。AWS Nitro Enclaves 开发工具包仅在 Nitro Enclave 内受支持，会自动将 `Recipient` 参数及其值添加到每个 AWS KMS 请求中。要在 AWS 开发工具包中请求 Nitro Enclave，必须指定 `Recipient` 参数及其值。AWS 开发工具包中对 Nitro Enclave 加密证明的支持于 2023 年 3 月推出。

AWS KMS 支持策略条件键，您可以使用这些键根据证明文件的内容允许或拒绝对 AWS KMS 密钥执行 Enclave 操作。您还可以在 AWS CloudTrail 日志中监控对 AWS KMS Nitro Enclave 的请求。

有关`Recipient`参数和 AWS `CiphertextForRecipient` 响应字段的详细信息，请参阅 AWS Key Management ServiceAPI 参考、AWSNitro Enclaves 软件开发工具包或任何软件开发工具包中的解密、、和GenerateRandom主题。GenerateDataKeyGenerateDataKeyPairAWS有关为加密设置数据和数据密钥的信息，请参阅将加密证明与 AWS KMS 结合使用。

AWS Nitro Enclaves 的 AWS KMS 条件键

您可以在控制 AWS KMS 资源访问的密钥政策和 IAM policy 中指定条件键。包含条件键的策略声明只有在满足条件时才有效。

AWS KMS提供了条件密钥，这些条件密钥根据请求中已签名的证明文档的内容限制解密GenerateDataKeyGenerateDataKeyPair、、和GenerateRandom操作的权限。这些条件键仅在 AWS KMS 操作请求中包含带有来自 AWS Nitro Enclave 的有效证明文档的 `Recipient` 参数时才起作用。要指定 `Recipient` 参数，请使用 AWS Nitro Enclaves 开发工具包 或任何 AWS 开发工具包。

特定于 Enclave 的 AWS KMS 条件键在密钥政策语句和 IAM policy 语句中有效，即使没有出现在 IAM 控制台或 IAM《服务授权参考》中。

kms:RecipientAttestation: ImageSha 384

AWS KMS 条件键	条件类型	值类型	API 操作	策略类型

`kms:RecipientAttestation:ImageSha384`	字符串	单值	`Decrypt`
			`GenerateDataKey`
			`GenerateDataKeyPair`
			`GenerateRandom`
				密钥策略和 IAM policy

当请求中的已签名证明文档中的映像摘要与条件键中的值相匹配时，`kms:RecipientAttestation:ImageSha384` 条件键使用 KMS 密钥控制对 `Decrypt`、`GenerateDataKey`、`GenerateDataKeyPair` 和 `GenerateRandom` 的访问。`ImageSha384` 值对应于证明文档中的 PCR0。仅当请求中的 `Recipient` 参数为 AWS Nitro Enclave 指定了已签名的证明文档时，此条件键才有效。

此值也包含在请求获得 Nitro 飞地CloudTrailAWS KMS的事件中。

> **Note**
>
> 此条件键在密钥策略语句和 IAM policy 语句中有效，即使没有出现在 IAM 控制台或 IAM 服务授权引用中。

例如，以下密钥策略声明允许该`data-processing`角色使用 KMS 密钥进行解密、GenerateDataKeyGenerateDataKeyPair、和GenerateRandom操作。`kms:RecipientAttestation:ImageSha384` 条件键仅允许在请求中的证明文档的映像摘要值（PCR0）与条件中的映像摘要值匹配时执行操作。仅当请求中的 `Recipient` 参数为 AWS Nitro Enclave 指定了已签名的证明文档时，此条件键才有效。

如果请求不包含来自 AWS Nitro Enclave 的有效证明文档，则权限将被拒绝，因为不满足此条件。

```
{
  "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 条件键	条件类型	值类型	API 操作	策略类型
kms:RecipientAttestation:PCR<PCR_ID>	字符串	单值	Decrypt GenerateDataKey GenerateDataKeyPair GenerateRandom	密钥策略和 IAM policy

`kms:RecipientAttestation:PCR<PCR_ID>` 条件键仅在请求中的已签名证明文档的平台配置注册（PCR）与条件键中的 PCR 匹配时，通过 KMS 密钥控制对 `Decrypt`、`GenerateDataKey`、`GenerateDataKeyPair` 和 `GenerateRandom` 的访问。仅当请求中的 `Recipient` 参数指定来自 AWS Nitro Enclave 的已签名证明文档时，该条件键才有效。

此值也包含在代表对 Nitro 飞地AWS KMS的请求CloudTrail的事件中。

> **Note**
>
> 此条件键在密钥策略语句和 IAM policy 语句中有效，即使没有出现在 IAM 控制台或 IAM 服务授权引用中。

要指定 PCR 值，请使用以下格式。将 PCR ID 连接到条件键名称。PCR 值必须是最多 96 个字节的小写十六进制字符串。

```
"kms:RecipientAttestation:PCRPCR_ID": "PCR_value"
```

例如，以下条件键指定 PCR1 的特定值，该值对应于用于 Enclave 和引导启动过程的内核的哈希值。

```
kms:RecipientAttestation:PCR1:
 "0x1abcdef2abcdef3abcdef4abcdef5abcdef6abcdef7abcdef8abcdef9abcdef8abcdef7abcdef6abcdef5abcdef
```

以下示例密钥政策语句允许 `data-processing` 角色将 KMS 密钥用于 Decrypt 操作。

此语句中的 `kms:RecipientAttestation:PCR` 条件键仅在请求中的签名证明文档的 PCR1 值与条件中的 `kms:RecipientAttestation:PCR1` 值匹配时允许执行操作。使用 `StringEqualsIgnoreCase` 策略运算符来要求对 PCR 值进行不区分大小写的比较。

如果请求不包含证明文档，则权限将被拒绝，因为不满足此条件。

```
{
  "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":
 "0x1de4f2dcf774f6e3b679f62e5f120065b2e408dcea327bd1c9dddaea6664e7af79355814748447674530082c6f15
    }
  }
}
```

监控 Nitro Enclave 的请求

您可以使用AWS CloudTrail日志来监控 AWS Nitro 飞地的解密GenerateDataKeyGenerateDataKeyPair、、和GenerateRandom操作。在这些日志条目中，additionalEventData 字段包含一个 recipient 字段，该字段包含来自请求中证明文档的模块 ID (attestationDocumentModuleId)、映像摘要 (attestationDocumentEnclaveImageDigest) 和平台配置寄存器（PCR）。仅当请求中的 Recipient 参数指定来自 AWS Nitro Enclave 的已签名证明文档时，才会包含这些字段。

模块 ID 是 Nitro Enclave 的 Enclave ID。映像摘要是 Enclave 映像的 SHA384 哈希值。您可以在密钥政策和 IAM policy 的条件中使用映像摘要和 PCR 值。有关 PCR 的信息，请参阅《AWS Nitro Enclave User Guide》中的 Where to get an enclave's measurements。

本节显示了每个受支持的 Nitro 安全区请求的 CloudTrail 日志条目示例。AWS KMS

解密（适用于 Enclave）

以下示例显示了 AWS Nitro enclave 的 Decrypt 操作的一个 AWS CloudTrail 日志条目。

```
{
    "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（用于飞地）

以下示例显示了 AWS Nitro 安全区GenerateDataKey操作的AWS CloudTrail日志条目。

```
{
    "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（用于飞地）

以下示例显示了 AWS Nitro 安全区GenerateDataKeyPair操作的AWS CloudTrail日志条目。

```
{
    "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（用于飞地）

以下示例显示了 AWS Nitro 安全区GenerateRandom操作的AWS CloudTrail日志条目。

```
{
    "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"
}
```

Amazon Redshift 如何使用 AWS KMS

本主题讨论 Amazon Redshift 如何使用 AWS KMS 加密数据。

主题

Amazon Redshift 加密

Amazon Redshift 数据仓库是一个由称作节点的各种计算资源构成的集合，这些节点已整理到名为集群的组中。每个集群运行一个 Amazon Redshift 引擎并包含一个或多个数据库。

Amazon Redshift 使用基于密钥的四层架构来进行加密。此架构包括数据加密密钥、数据库密钥、群集密钥和根密钥。您可以使用 AWS KMS key 作为根密钥。

数据加密密钥对群集中的数据块进行加密。每个数据块分配有一个随机生成的 AES-256 密钥。这些密钥使用群集的数据库密钥进行加密。

数据库密钥对群集中的数据加密密钥进行加密。数据库密钥是随机生成的 AES-256 密钥。它存储在独立于 Amazon Redshift 集群的网络中的磁盘上，并跨安全通道传递到集群中。

群集密钥对 Amazon Redshift 群集的数据库密钥进行加密。您可以使用 AWS KMS、AWS CloudHSM 或外部硬件安全模块 (HSM) 来管理群集密钥。有关更多详细信息，请参阅 Amazon Redshift 数据库加密文档。

您可以通过选中 Amazon Redshift 控制台中相应的框请求加密。您可以从加密框下方显示的列表中选择，指定一个客户托管密钥。如果您不指定客户托管的密钥，则 Amazon Redshift 将 AWS 托管式密钥用于您账户下的 Amazon Redshift。

> **Important**
>
> Amazon Redshift 仅支持对称加密 KMS 密钥。您不能在 Amazon Redshift 加密工作流中使用非对称 KMS 密钥。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

加密上下文

与 AWS KMS 集成的每项服务在请求数据密钥、加密和解密时会指定一个加密上下文。加密上下文是 AWS KMS 用于检查数据完整性而使用的额外的身份验证数据 (AAD)。也就是说，在为加密操作指定加密上下文时，该服务还要为解密操作指定同一加密上下文，否则解密会失败。Amazon Redshift 使用加密上下文的集群 ID 和创建时间。在 CloudTrail 日志文件`requestParameters`字段中，加密上下文将与之类似。

```
"encryptionContext": {
    "aws:redshift:arn": "arn:aws:redshift:region:account_ID:cluster:cluster_name",
    "aws:redshift:createtime": "20150206T1832Z"
},
```

您可以在 CloudTrail 日志中搜索集群名称，以了解使用AWS KMS key（KMS 密钥）执行了哪些操作。这些操作包括集群加密、集群解密以及生成数据密钥。

Amazon Relational Database Service (Amazon RDS) 如何使用 AWS KMS

您可以使用 Amazon Relational Database Service (Amazon RDS)在云中设置、操作和扩展关系数据库。您可以使用 AWS 托管式密钥 或客户管理型密钥加密您的 Amazon RDS 资源。Amazon RDS 在 Amazon Elastic Block Store (Amazon EBS) 加密上构建，可为数据库卷提供全磁盘加密。

有关 Amazon RDS 如何使用 KMS 密钥保护资源的详细信息，请参阅《Amazon RDS 用户指南》中的加密 Amazon RDS 资源 和 AWS KMS 密钥管理。

AWS Secrets Manager 如何使用 AWS KMS

AWS Secrets Manager 是一项 AWS 服务，可加密和存储您的密钥，以透明方式解密密钥并将明文密钥返回给您。它专门用于存储定期更改且不应硬编码或以明文形式存储在应用程序中的应用程序密钥，如登录凭证。作为对硬编码凭证或表查找的替代，您的应用程序调用了 Secrets Manager。

Secrets Manager 也支持定期轮换与常用数据库关联的密钥的功能。它总是先对新轮换的密钥加密，然后再进行存储。

Secrets Manager 集成到 AWS Key Management Service (AWS KMS)，用受 AWS KMS key 保护的唯一数据密钥对每个密钥值的每个版本进行加密。这种集成可根据从不会使 AWS KMS 处于未加密状

态的加密密钥来保护您的密钥。它还允许您设置对 KMS 密钥的自定义权限，并审核用于保护密钥的生成、加密和解密数据密钥的操作。

有关 Secrets Manager 如何使用 KMS 密钥来保护您的密钥的信息，请参阅 AWS Secrets Manager 用户指南中的加密和解密密钥。

Amazon Simple Email Service (Amazon SES) 如何使用 AWS KMS

您可以使用 Amazon Simple Email Service (Amazon SES) 接收电子邮件并（选择性地）加密收到的电子邮件，然后再将它们存储在您选择的 Amazon Simple Storage Service (Amazon S3) 存储桶中。如果您将 Amazon SES 配置为加密电子邮件，则必须选择 Amazon SES 加密邮件时要使用的 AWS KMS AWS KMS key。您可以为 Amazon SES（其别名为 `aws/ses`）选择 AWS 托管式密钥，也可以选择您在 AWS KMS 中创建的对称客户托管式密钥。

> **Important**
>
> Amazon SES 仅支持对称 KMS 密钥。不能使用非对称 KMS 密钥来加密 Amazon SES 电子邮件。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

有关如何使用 Amazon SES 接收电子邮件的更多信息，请转至 Amazon Simple Email Service 开发人员指南中的使用 Amazon SES 接收电子邮件。

主题

- 使用 AWS KMS 的 Amazon SES 加密概述
- Amazon SES 加密上下文
- 为 Amazon SES 提供使用您的 AWS KMS key 的权限
- 获取和解密电子邮件

使用 AWS KMS 的 Amazon SES 加密概述

当您将 Amazon SES 配置为接收电子邮件并加密电子邮件，然后将其保存到 S3 存储桶时，其过程将如下所述：

1. 您为 Amazon SES 创建一个接收规则，同时指定 S3 操作、用于存储的 S3 存储桶以及用于加密的 AWS KMS key。
2. Amazon SES 接收与您的接收规则匹配的电子邮件。

3. Amazon SES 请求已使用您在适用接收规则中指定的 KMS 密钥加密的唯一数据密钥。
4. AWS KMS 创建一个新的数据密钥，使用指定的 KMS 密钥对其进行加密，然后将已加密的数据密钥明文副本发送到 Amazon SES。
5. Amazon SES 使用明文数据密钥加密电子邮件，并在使用后尽快从内存中删除该明文数据密钥。
6. Amazon SES 将加密的电子邮件和加密的数据密钥放入指定的 S3 存储桶中。加密的数据密钥将存储为加密电子邮件的元数据。

为了通过 Step 6 完成 Step 3，Amazon SES 使用 AWS 提供的 Amazon S3 加密客户端。使用同一客户端从 Amazon S3 检索加密的电子邮件并对其进行解密。有关更多信息，请参阅 获取和解密电子邮件。

Amazon SES 加密上下文

当 Amazon SES 请求数据密钥来加密您收到的电子邮件时（使用 AWS KMS 的 Amazon SES 加密概述 中的 Step 3），它会在请求中包含加密上下文。加密上下文提供 AWS KMS 用于确保数据完整性而使用的额外的身份验证数据 (AAD)。加密上下文也将写入您的 AWS CloudTrail 日志文件，这有助于您了解为什么使用给定的 AWS KMS key（KMS 密钥）。Amazon SES 会使用以下加密上下文：

- 您已在其中将 Amazon SES 配置为接收电子邮件的 AWS 账户 的 ID
- 对电子邮件调用 S3 操作的 Amazon SES 接收规则的规则名称
- 电子邮件的 Amazon SES 邮件 ID

以下示例显示了 Amazon SES 使用的加密上下文的 JSON 表示形式：

```
{
  "aws:ses:source-account": "111122223333",
  "aws:ses:rule-name": "example-receipt-rule-name",
  "aws:ses:message-id": "d6iitobk75ur44p8kdnnp7g2n800"
}
```

为 Amazon SES 提供使用您的 AWS KMS key 的权限

要加密您的电子邮件，您可以将您账户中的 AWS 托管式密钥 用于 Amazon SES (aws/ses)，或者可以使用您创建的客户托管式密钥。Amazon SES 已有权代表您使用 AWS 托管式密钥。但是，如果您在添加 S3 操作到您的 Amazon SES 接收规则时指定客户托管密钥，您必须授予 Amazon SES 使用 KMS 密钥加密您的电子邮件的权限。

要为 Amazon SES 提供使用客户托管密钥的权限，请将以下语句添加到 KMS 密钥的密钥策略中：

```
{
  "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"}
  }
}
```

将 *ACCOUNT-ID-WITHOUT-HYPHENS* 替换为您已在其中将 Amazon SES 配置为接收电子邮件的 AWS 账户 的 12 位数 ID。此策略语句仅允许 Amazon SES 在以下条件下使用此 KMS 密钥加密数据：

- Amazon SES 必须在其 AWS KMS API 请求的 `EncryptionContext` 中指定 `aws:ses:rule-name` 和 `aws:ses:message-id`。
- Amazon SES 必须在其 AWS KMS API 请求的 `EncryptionContext` 中指定 `aws:ses:source-account`，并且 `aws:ses:source-account` 的值必须与密钥策略中指定的 AWS 账户 ID 匹配。

有关 Amazon SES 在加密电子邮件时使用的加密上下文的更多信息，请参阅 Amazon SES 加密上下文。有关 AWS KMS 如何使用加密上下文的一般信息，请参阅加密上下文。

获取和解密电子邮件

Amazon SES 无权解密您的加密电子邮件，也无法为您解密它们。您必须编写代码以从 Amazon S3 获取电子邮件并解密它们。为方便起见，请使用 Amazon S3 加密客户端。以下 AWS 开发工具包中包含 Amazon S3 加密客户端：

- AWS SDK for Java – 请参阅 AWS SDK for Java API 参考中的 AmazonS3EncryptionClient 和 AmazonS3EncryptionClientV2。

- AWS SDK for Ruby – 请参阅 AWS SDK for Ruby API 参考中的 Aws::S3::Encryption::Client。
- AWS SDK for .NET – 请参阅 AWS SDK for .NET API 参考中的 AmazonS3EncryptionClient。
- AWS SDK for Go – 请参阅 AWS SDK for Go API 参考中的 s3crypto。

Amazon S3 加密客户端可简化以下工作：构建 Amazon S3 的必要请求，以检索加密电子邮件；构建对 AWS KMS 的必要请求，以解密邮件的加密数据密钥；以及解密电子邮件。例如，要成功解密加密的数据密钥，您传递的加密上下文必须与 Amazon SES 在从 AWS KMS 请求数据密钥时传递的加密上下文相同（使用 AWS KMS 的 Amazon SES 加密概述 中的 Step 3）。Amazon S3 加密客户端可以为您处理这一情况及其他许多工作。

对于使用 AWS SDK for Java 中的 Amazon S3 加密客户端执行客户端解密的示例代码，请参阅以下内容：

- Amazon Simple Storage Service 用户指南中的使用存储在 AWS KMS 中的 KMS 密钥。
- AWS 开发人员博客上的使用 AWS Key Management Service 进行 Amazon S3 加密

Amazon Simple Storage Service (Amazon S3) 如何使用 AWS KMS

Amazon Simple Storage Service (Amazon S3) 是一种对象存储服务，可将数据以对象形式存储在存储桶中。存储桶及其中的对象是私有的，只有在您明确授予访问权限时才可以访问。

Amazon S3 与 AWS Key Management Service（AWS KMS）集成，可提供对 Amazon S3 对象的服务器端加密。Amazon S3 使用 AWS KMS 密钥对 Amazon S3 对象进行加密。这种加密密钥从不会使 AWS KMS 处于未加密状态，从而保护您的对象。这种集成还允许您对 AWS KMS 密钥设置权限，并审计生成、加密和解密用于保护您密钥的数据密钥的操作。

要减少对 Amazon S3 的调用量AWS KMS，请使用 Amazon S3 存储桶密钥，这些密钥受 KMS 密钥保护 key-encryption-keys ，可在有限的时间内在 Amazon S3 中重复使用。存储桶密钥可以将 AWS KMS 请求的成本降低高达 99%。您可以在 Amazon S3 存储桶中配置适用于所有对象的存储桶密钥，或在 Amazon S3 存储桶中配置适用于特定对象的存储桶密钥。

有关 Amazon S3 如何使用 AWS KMS 的更多信息，请参阅《Amazon S3 用户指南》中的使用具有 KMS 密钥的服务器端加密 (SSE-KMS) 保护数据。

AWS Systems Manager Parameter Store 如何使用 AWS KMS

通过使用 AWS Systems Manager Parameter Store，您可以创建安全字符串参数，这些参数具有明文参数名称和加密的参数值。Parameter Store 使用 AWS KMS 加密和解密安全字符串参数的参数值。

借助 Parameter Store，您可以将数据作为具有值的参数进行创建、存储和管理。您可以在 Parameter Store 中创建一个参数，然后在多个受您设计的策略和权限限制的应用程序和服务中使用该参数。在需要更改参数值时，您可以更改一个实例，而不是管理对众多源进行的更改，后者很容易出错。Parameter Store 支持参数名称采用分层结构，因此，您可以将某个参数限制为用于特定的用途。

要管理敏感数据，您可以创建安全字符串参数。在创建或更改安全字符串参数值时，Parameter Store 使用 AWS KMS keys 加密它们的参数值。在访问这些参数值时，它也使用 KMS 密钥解密这些值。您可以使用 Parameter Store 为您的账户创建的 AWS 托管式密钥，或者指定您自己的客户托管密钥。

> **Important**
>
> Parameter Store 仅支持对称 KMS 密钥。不能使用非对称 KMS 密钥来加密您的参数。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

Parameter Store 支持两个层级的安全字符串参数：标准和高级。不能超过 4096 字节的标准参数直接在指定的 KMS 密钥下进行加密和解密。为了加密和解密高级安全字符串参数，Parameter Store 将信封加密与 AWS Encryption SDK 结合使用。您可以将标准安全字符串参数转换为高级参数，但不能将高级参数转换为标准参数。有关标准和高级安全字符串参数之间的差别的更多信息，请参阅 AWS Systems Manager 用户指南中的关于 Systems Manager 高级参数。

主题

保护标准安全字符串参数

Parameter Store 不执行任何加密操作。相反，它依赖于 AWS KMS 加密和解密安全字符串参数值。在创建或更改标准参数值时，Parameter Store 会调用 AWS KMS Encrypt 操作。该操作直接使用对称加密 KMS 密钥加密参数值，而不是使用 KMS 密钥生成数据密钥。

您可以选择 Parameter Store 使用的 KMS 密钥加密参数值。如果未指定 KMS 密钥，Parameter Store 将使用 Systems Manager 在您的账户中自动创建的 AWS 托管式密钥。此 KMS 密钥具有 `aws/ssm` 别名。

要查看您账户的默认 aws/ssm KMS 密钥，请使用 AWS KMS API 中的DescribeKey操作。以下示例在别名为 describe-key 的 AWS Command Line Interface (AWS CLI) 中使用 aws/ssm 命令。

```
aws kms describe-key --key-id alias/aws/ssm
```

要创建标准的安全字符串参数，请使用 Systems Manager API 中的PutParameter操作。省略 Tier 参数或指定 Standard 的值（它是默认值）。请包含具有 SecureString 值的 Type 参数。要指定 KMS 密钥，请使用 KeyId 参数。默认值为您的账户的 AWS 托管式密钥，即 aws/ssm。

然后，Parameter Store 使用 KMS 密钥和明文参数值调用 AWS KMS Encrypt 操作。AWS KMS 返回加密的参数值， 将该值与参数名称一起存储。

以下示例在 AWS CLI 中使用 Systems Manager put-parameter 命令及其 --type 参数创建安全字符串参数。由于该命令省略了可选的 --tier 和 --key-id 参数，因此，Parameter Store 将创建标准安全字符串参数，并在 AWS 托管式密钥 下对其进行加密

```
aws ssm put-parameter --name MyParameter --value "secret_value" --type SecureString
```

以下类似的示例使用 --key-id 参数指定客户托管密钥。该示例使用 KMS 密钥 ID 标识 KMS 密钥，但您可以使用任何有效的 KMS 密钥标识符。由于该命令省略了 Tier 参数 (--tier)，因此，Parameter Store 将创建标准安全字符串参数而非高级参数。

```
aws ssm put-parameter --name param1 --value "secret" --type SecureString --key-id
 1234abcd-12ab-34cd-56ef-1234567890ab
```

从 Parameter Store 中获取安全字符串参数时，将对该参数值进行加密。要获取参数，请使用 Systems Manager API 中的GetParameter 操作。

以下示例在 AWS CLI 中使用 Systems Manager get-parameter 命令从 Parameter Store 中获取 MyParameter 参数，而不解密该参数值。

```
$  aws ssm get-parameter --name MyParameter

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value":
 "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg/9E464VRo68cvwAAAG8wbQYJKoZIhvcNAQcGoGAwXgIBADBZBgkqhkiG9
```

```
    }
}
```

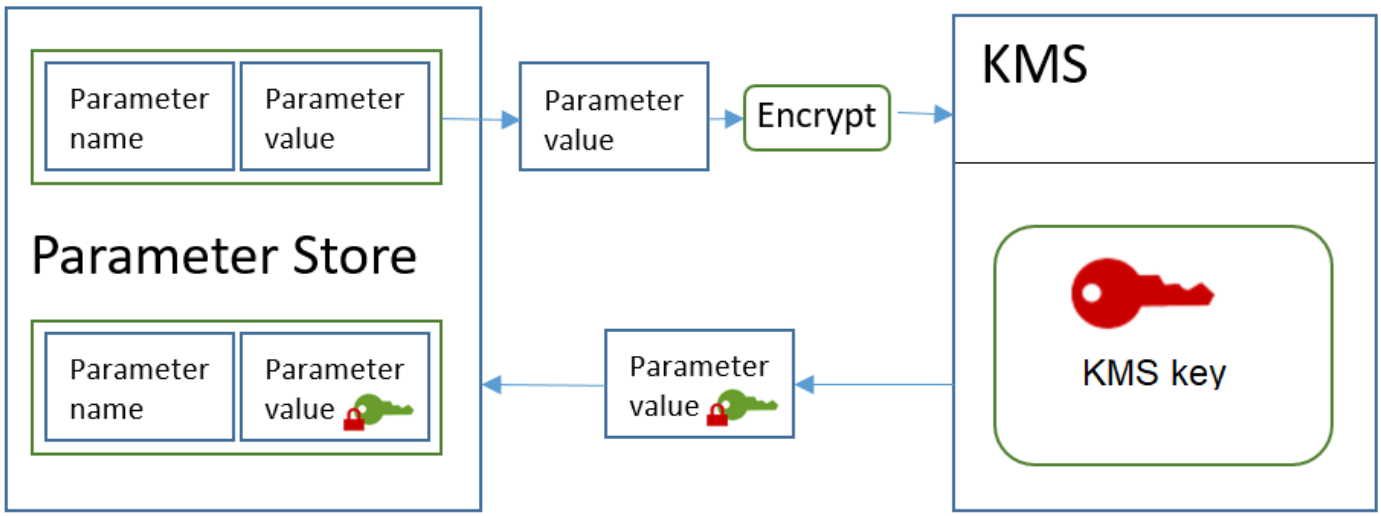
要在返回之前解密参数值，请将 `GetParameter` 的 `WithDecryption` 参数设置为 `true`。在使用 `WithDecryption` 时，Parameter Store 代表您调用 AWS KMS Decrypt 操作以解密该参数值。因此，`GetParameter` 请求返回参数以及明文参数值，如以下示例中所示。

```
$  aws ssm get-parameter --name MyParameter --with-decryption

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

以下工作流程演示 Parameter Store 如何使用 KMS 密钥加密和解密标准安全字符串参数。

加密标准参数

1. 当您使用 `PutParameter` 创建安全字符串参数时，Parameter Store 将发送 `Encrypt` 请求至 AWS KMS。该请求包含明文参数值、您选择的 KMS 密钥和 Parameter Store 加密上下文。在传输到 AWS KMS 期间，将通过传输层安全性 (TLS) 保护安全字符串参数中的明文值。
2. AWS KMS 使用指定的 KMS 密钥和加密上下文来加密参数值。它将密文返回到 Parameter Store，后者将存储参数名称及其加密值。



解密标准参数

1. 当您在 GetParameter 请求中包含 WithDecryption 参数时，Parameter Store 向 AWS KMS 发送包含加密的安全字符串参数值和 Parameter Store 加密上下文的 Decrypt 请求。
2. AWS KMS 使用相同的 KMS 密钥和提供的加密上下文来解密加密的值。它向 Parameter Store 返回明文（解密的）参数值。在传输期间，将通过 TLS 保护明文数据。
3. Parameter Store 在 GetParameter 响应中向您返回明文参数值。

保护高级安全字符串参数

在使用 PutParameter 创建高级安全字符串参数时，Parameter Store 使用信封加密与 AWS Encryption SDK 和对称加密 AWS KMS key 来保护参数值。每个高级参数值都使用唯一数据密钥加密，数据密钥使用 KMS 密钥加密。您可以将 AWS 托管式密钥 用于账户 (aws/ssm) 或任何客户托管密钥。

AWS Encryption SDK 是一个开源客户端库，可帮助您使用行业标准和最佳实践来加密和解密数据。它在多个平台上受支持并支持多种编程语言，包括命令行界面。您可以在中查看源代码并为其开发做出贡献 GitHub。

对于每个安全字符串参数值，Parameter Store 会调用，使用AWS KMS生成 (GenerateDataKey) 的唯一数据密钥对参数值进行加密。AWS Encryption SDKAWS Encryption SDK 向 Parameter Store 返回一条加密消息（其中包含加密参数值）和唯一数据密钥的加密副本。Parameter Store 将整个加密消息存储在安全字符串参数值中。之后，在您获取高级安全字符串参数值时，Parameter Store 使用 AWS Encryption SDK 解密参数值。这需要调用 AWS KMS 以解密加密的数据密钥。

要创建高级安全字符串参数，请使用 Systems Manager API 中的PutParameter操作。将 Tier 参数的值设置为 Advanced。请包含具有 SecureString 值的 Type 参数。要指定 KMS 密钥，请使用 KeyId 参数。默认值为您的账户的 AWS 托管式密钥，即 aws/ssm。

```
aws ssm put-parameter --name MyParameter --value "secret_value" --type SecureString --
tier Advanced
```

以下类似的示例使用 --key-id 参数指定客户托管密钥。此示例使用 KMS 密钥的 Amazon Resource Name (ARN)，但您可以使用任何有效的 KMS 密钥标识符。

```
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
```

在从 Parameter Store 获取安全字符串参数时，其值为 AWS Encryption SDK 所返回的加密消息。要获取参数，请使用 Systems Manager API 中的GetParameter 操作。

以下示例使用 Systems Manager `GetParameter` 操作从 Parameter Store 获取 `MyParameter` 参数，而不解密其值。

```
$  aws ssm get-parameter --name MyParameter

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value":
 "AQECAHgnOkMROh5LaLXkA4j0+vYi6tmM17Lg/9E464VRo68cvwAAAG8wbQYJKoZIhvcNAQcGoGAwXgIBADBZBgkqhkiG9
    }
}
```

要在返回之前解密参数值，请将 `GetParameter` 的 `WithDecryption` 参数设置为 `true`。在使用 `WithDecryption` 时，Parameter Store 代表您调用 AWS KMS Decrypt 操作以解密该参数值。因此，`GetParameter` 请求返回参数以及明文参数值，如以下示例中所示。

```
$  aws ssm get-parameter --name MyParameter --with-decryption

{
    "Parameter": {
        "Type": "SecureString",
        "Name": "MyParameter",
        "Value": "secret_value"
    }
}
```

您无法将高级安全字符串参数转换为标准参数，但可以将标准安全字符串参数转换为高级参数。要将标准安全字符串参数转换为高级安全字符串，请将 `PutParameter` 操作与 `Overwrite` 参数结合使用。`Type` 必须为 `SecureString`，并且 `Tier` 值必须为 `Advanced`。`KeyId` 参数（它标识客户托管密钥）是可选的。如果省略它，Parameter Store 将 AWS 托管式密钥 用于账户。您可以指定委托人有权使用的任何 KMS 密钥，即使您使用不同的 KMS 密钥来加密标准参数也是如此。

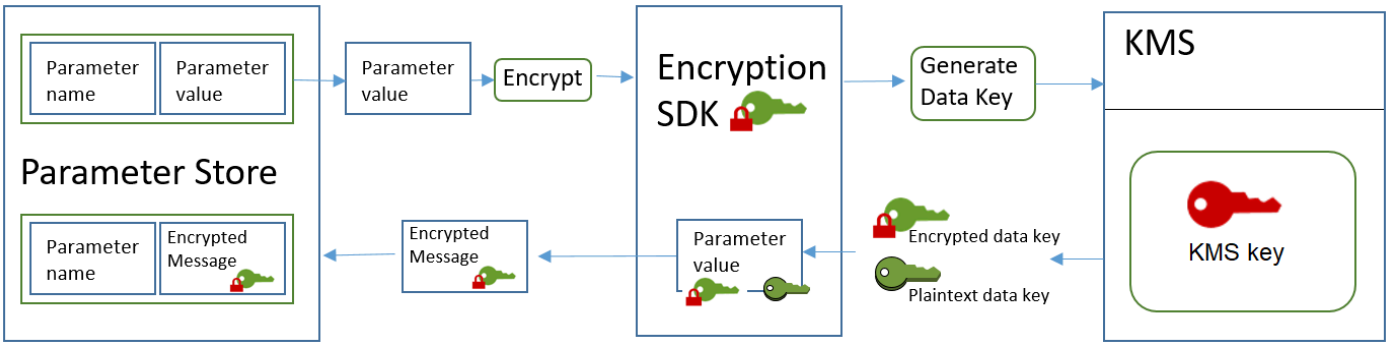
当您使用 `Overwrite` 参数时，Parameter Store 使用 AWS Encryption SDK 对参数值进行加密。然后，它会将新加密的消息存储在 Parameter Store 中。

```
$ aws ssm put-parameter --name myStdParameter --value "secret_value"  --type
 SecureString --tier Advanced --key-id 1234abcd-12ab-34cd-56ef-1234567890ab --overwrite
```

以下工作流程演示 Parameter Store 如何使用 KMS 密钥加密和解密高级安全字符串参数。

加密高级参数

1. 在使用 `PutParameter` 创建高级安全字符串参数时，Parameter Store 使用 AWS Encryption SDK 和 AWS KMS 加密参数值。Parameter Store 使用参数值、您指定的 KMS 密钥和 Parameter Store 加密上下文调用 AWS Encryption SDK。
2. AWS KMS使用您指定的 KMS 密钥的标识符和参数存储加密上下文向AWS Encryption SDK发送GenerateDataKey请求。 AWS KMS返回唯一数据密钥的两个副本：一个为纯文本，另一个使用 KMS 密钥加密。（加密数据密钥时将使用加密上下文。）
3. AWS Encryption SDK 使用明文数据密钥对参数值进行加密。它返回一条加密消息，其中包含加密的参数值、加密的数据密钥和其他数据（包括 Parameter Store 加密上下文）。
4. Parameter Store 将加密消息存储为参数值。



解密高级参数

1. 您可以将 `WithDecryption` 参数包含在 `GetParameter` 请求中以获取高级安全字符串参数。在执行此操作时，Parameter Store 将加密消息从参数值传递到 AWS Encryption SDK 的解密方法。
2. AWS Encryption SDK 调用 AWS KMS Decrypt 操作。它传入加密消息中的加密的数据密钥和 Parameter Store 加密上下文。
3. AWS KMS 使用 KMS 密钥和 Parameter Store 加密上下文解密加密的数据密钥。然后，它向 AWS Encryption SDK 返回明文（解密的）数据密钥 。
4. AWS Encryption SDK 使用明文数据密钥对参数值进行解密。它向 Parameter Store 返回明文参数值。
5. Parameter Store 验证您的加密上下文，并在 `GetParameter` 响应中向您返回明文参数值。

设置权限以加密和解密参数值

要加密标准安全字符串参数值，用户需要 kms:Encrypt 权限。要加密高级安全字符串参数值，用户需要 kms:GenerateDataKey 权限。要解密任一类型的安全字符串参数值，用户需要 kms:Decrypt 权限。

您可以使用 IAM policy 允许或拒绝用户调用 Systems Manager PutParameter 和 GetParameter 操作的权限。

如果您使用客户托管密钥加密安全字符串参数值，则可使用 IAM policy 和密钥策略来管理加密和解密权限。不过，您无法为默认的 aws/ssm KMS 密钥制定访问控制策略。有关控制对客户托管密钥的访问的详细信息，请参阅 AWS KMS 的身份验证和访问控制。

以下示例显示了一个用于标准安全字符串参数的 IAM policy。此策略允许用户对 FinancialParameters 路径中的所有参数调用 Systems Manager PutParameter 操作。此策略还允许用户对示例客户托管密钥调用 AWS KMS Encrypt 操作。

```
{
    "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"
        }
    ]
}
```

下一个示例显示用于高级安全字符串参数的 IAM policy。此策略允许用户对 ReservedParameters 路径中的所有参数调用 Systems Manager PutParameter 操作。此策略还允许用户对示例客户托管密钥调用 AWS KMS GenerateDataKey 操作。

```
{
    "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"
        }
    ]
}
```

最后一个示例还显示了一个 IAM policy，该策略可用于标准或高级安全字符串参数。此策略允许用户对 `ITParameters` 路径中的所有参数调用 Systems Manager `GetParameter` 操作（以及相关操作）。此策略还允许用户对示例客户托管密钥调用 AWS KMS `Decrypt` 操作。

```
{
    "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"
        }
    ]
}
```

Parameter Store 加密上下文

加密上下文 是一组包含任意非机密数据的键值对。在请求中包含加密上下文以加密数据时，AWS KMS 以加密方式将加密上下文绑定到加密的数据。要解密数据，您必须传入相同的加密上下文。

您还可以使用加密上下文在审核记录和日志中识别加密操作。加密上下文在日志中以明文形式显示，例如，AWS CloudTrail 日志。

AWS Encryption SDK 也接受加密上下文，尽管它以不同方式处理该上下文。Parameter Store 向加密方法提供加密上下文。AWS Encryption SDK 以加密方式将加密上下文绑定到加密数据。它还以明文形式将加密上下文包含在其返回的加密消息的标头中。但与 AWS KMS 不同，AWS Encryption SDK 解密方法不将加密上下文作为输入。相反，当它解密数据时，AWS Encryption SDK 会从加密的消息中获取加密上下文。Parameter Store 在向您返回明文参数值之前验证加密上下文中是否包含它所期望的值。

Parameter Store 在加密操作中使用以下加密上下文：

- 键：PARAMETER_ARN
- 值：要加密的参数的 Amazon Resource Name (ARN)。

加密上下文的格式如下所示：

```
"PARAMETER_ARN":"arn:aws:ssm:<REGION_NAME>:<ACCOUNT_ID>:parameter/<parameter-name>"
```

例如，Parameter Store 在调用中包含此加密上下文，以在示例 AWS 账户 和区域中加密和解密 MyParameter 参数。

```
"PARAMETER_ARN":"arn:aws:ssm:us-west-2:111122223333:parameter/MyParameter"
```

如果该参数位于 Parameter Store 分层路径中，则在加密上下文中包含路径和名称。例如，在示例 AWS 账户 和区域中加密和解密 /ReadableParameters 路径中的 MyParameter 参数时，将使用此加密上下文。

```
"PARAMETER_ARN":"arn:aws:ssm:us-west-2:111122223333:parameter/ReadableParameters/
MyParameter"
```

您可以使用正确的加密上下文和 Systems Manager `GetParameter` 操作返回的加密参数值调用 AWS KMS `Decrypt` 操作，以解密加密的安全字符串参数值。不过，我们建议您将 `GetParameter` 操作与 `WithDecryption` 参数一起使用以解密 Parameter Store 参数值。

您还可以在 IAM policy 中包含加密上下文。例如，您可以允许用户仅解密某个特定参数值或一组参数值。

以下示例 IAM policy 语句允许用户获取 `MyParameter` 参数值，以及使用指定的 KMS 密钥解密该参数值。不过，只有在加密上下文与指定的字符串匹配时，这些权限才适用。这些权限不适用于任何其他参数或 KMS 密钥；如果加密上下文与该字符串不匹配，对 `GetParameter` 的调用将失败。

使用类似于此策略语句的策略语句之前，请使用有效值替换示例 ARN。

```
{
    "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"
                }
            }
        }
    ]
}
```

对 Parameter Store 中的 KMS 密钥问题进行故障排除

要对安全字符串参数执行任何操作，Parameter Store 必须能够使用您为预期操作指定的 AWS KMS KMS 密钥。与 KMS 密钥相关的大多数 Parameter Store 故障都是由以下问题造成的：

- 应用程序使用的凭证无权对 KMS 密钥执行指定的操作。

  要修复该错误，请使用不同的凭证运行应用程序，或者修改妨碍执行该操作的 IAM 或密钥策略。有关 AWS KMS IAM 和密钥策略的帮助，请参阅AWS KMS 的身份验证和访问控制。

- 找不到 KMS 密钥。

  在 KMS 密钥使用不正确的标识符时，通常会发生这种情况。请查找 KMS 密钥的正确标识符，然后重试该命令。

- KMS 密钥未启用。发生这种情况时，Parameter Store 会返回一个InvalidKeyId异常，其中包含来自的详细错误消息AWS KMS。如果 KMS 密钥状态为 `Disabled`，请启用它。如果状态为 `Pending Import`，请完成导入过程。如果密钥状态为 `Pending Deletion`，请取消密钥删除或使用不同的 KMS 密钥。

  要在 AWS KMS 控制台中、Customer managed keys（客户托管密钥）或 AWS 托管式密钥 页面上查找 KMS 密钥的密钥状态，请参见 Status column（状态列）。要使用 AWS KMS API 查找 KMS 密钥的状态，请使用DescribeKey操作。

亚马逊如何 WorkMail 使用 AWS KMS

本主题讨论 Amazon AWS KMS 如何 WorkMail 使用加密电子邮件。

主题

- 亚马逊 WorkMail 概述
- 亚马逊 WorkMail 加密
- 授权使用 KMS 密钥
- Amazon WorkMail 加密环境
- 监控亚马逊与之的 WorkMail 互动 AWS KMS

亚马逊 WorkMail 概述

Amazon WorkMail 是一项安全、托管的企业电子邮件和日历服务，支持现有的桌面和移动电子邮件客户端。您可以创建一个 Amazon WorkMail 组织并为其分配一个或多个您拥有的电子邮件域。然后，您可以为组织中的电子邮件用户和通讯组创建邮箱。

在将邮件写入磁盘之前，Amazon 会 WorkMail 透明地加密所有 Amazon WorkMail 组织邮箱中的所有邮件，并在用户访问邮件时透明地解密这些邮件。没有用于禁用加密的选项。为了保护保护消息的加密密钥，Amazon 集成 WorkMail 了 AWS Key Management Service (AWS KMS)。

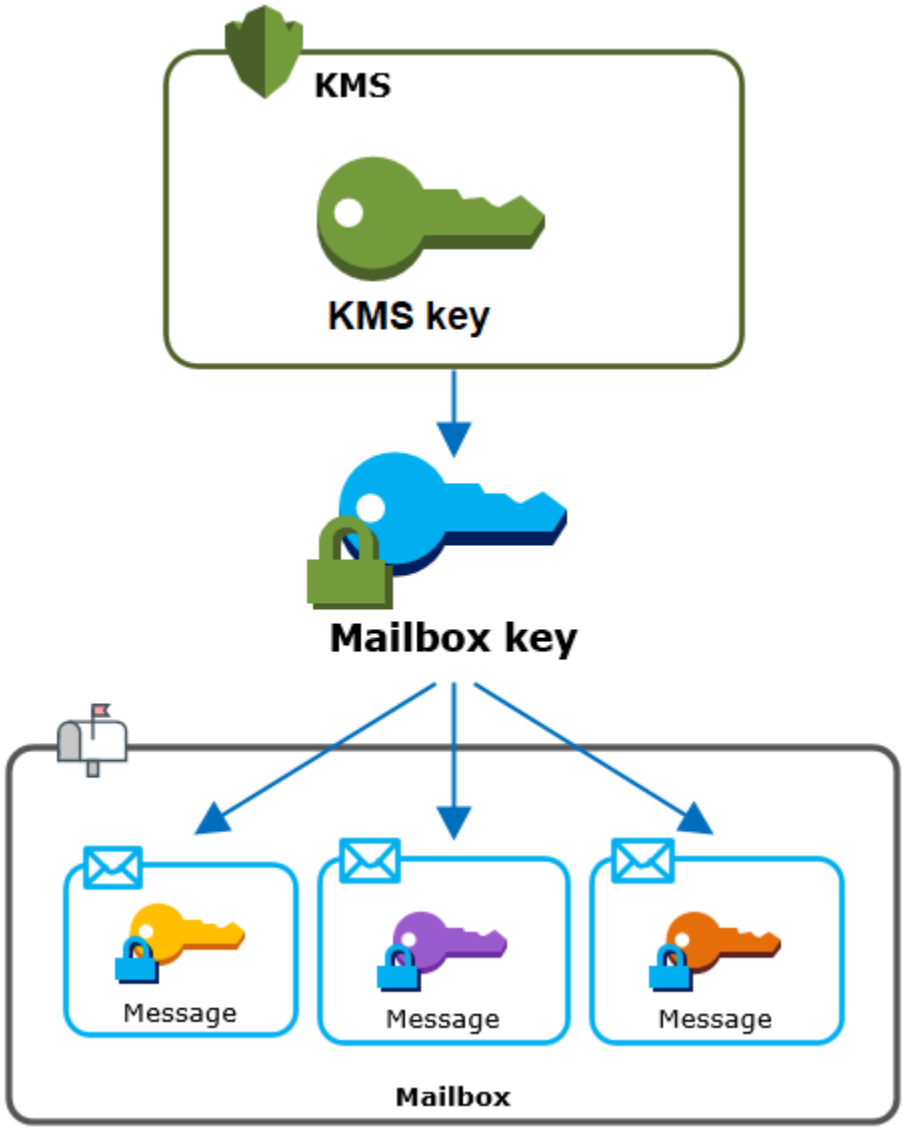
Amazon WorkMail 还提供了允许用户发送签名或加密电子邮件的选项。此加密功能不使用 AWS KMS。

亚马逊 WorkMail 加密

在 Amazon 中 WorkMail，每个组织可以包含多个邮箱，组织中的每个用户对应一个邮箱。所有消息（包括电子邮件和日历项）都存储在用户的邮箱中。

为了保护您的 Amazon WorkMail 组织中的邮箱内容，Amazon 会在所有邮箱邮件写入磁盘之前对其进行 WorkMail 加密。任何客户提供的信息均为明文形式存储。

每条消息都使用唯一的数据加密密钥进行加密。邮件密钥受邮箱密钥保护，邮箱密钥是仅用于该邮箱的唯一加密密钥。对于始终对 AWS KMS 加密的组织，使用 AWS KMS key 对邮箱密钥进行加密。下图显示了 AWS KMS 中加密消息、加密消息密钥、加密邮箱密钥和组织中 KMS 密钥之间的关系。



组织的 KMS 密钥

创建 Amazon WorkMail 组织时，您可以AWS KMS key为该组织选择一个。此 KMS 密钥保护该组织中的所有邮箱密钥。

如果您使用快速设置程序来创建您的组织，Amazon 将在您的中 WorkMail 使用 f AWS 托管式密钥or Amazon WorkMail (`aws/workmail`) AWS 账户。如果您使用标准设置，则可以选择AWS 托管式密钥适用于 Amazon 的密钥 WorkMail 或您拥有和管理的客户托管密钥。您可以为每个组织选择相同的 KMS 密钥或不同的 KMS 密钥，但在选择 KMS 密钥后，无法更改它。

> **Important**
>
> Amazon 仅 WorkMail 支持对称加密 KMS 密钥。您不能使用非对称 KMS 密钥对 Amazon WorkMail 中的数据进行加密。要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

要查找组织的 KMS 密钥，请使用记录对 AWS KMS 的调用的 AWS CloudTrail 日志条目。

每个邮箱的唯一加密密钥

当您创建新邮箱时，Amazon WorkMail 会为其外部的邮箱生成一个唯一的 256 位高级加密标准 (AES) 对称加密密钥，称为邮箱密钥。AWS KMSAmazon WorkMail 使用邮箱密钥来保护邮箱中每封邮件的加密密钥。

为了保护邮箱密钥，Amazon WorkMail 要求AWS KMS对组织的 KMS 密钥下的邮箱密钥进行加密。然后，它将加密的邮箱密钥存储在邮箱元数据中。

> **Note**
>
> Amazon WorkMail 使用对称邮箱加密密钥来保护消息密钥。以前，Amazon 使用非对称密钥对 WorkMail 保护每个邮箱。它使用公有密钥加密每个消息密钥，并使用私有密钥解密该密钥。私有邮箱密钥受组织的 KMS 密钥保护。现有邮箱可能仍使用非对称邮箱密钥对。此更改不会影响邮箱或其消息的安全。

每个消息的唯一加密密钥

将邮件添加到邮箱后，Amazon WorkMail 会为外部的邮件生成唯一的 256 位 AES 对称加密密钥。AWS KMS它使用这个消息密钥对消息进行加密。Amazon WorkMail 对邮箱密钥下的消息密钥进行加密，并将加密的消息密钥与邮件一起存储。然后，它使用组织的 KMS 密钥加密邮箱密钥。

创建新邮箱

Amazon WorkMail 创建新邮箱时，会使用以下过程来准备用于保存加密邮件的邮箱。

- Amazon 为外部的邮箱 WorkMail 生成唯一的 256 位 AES 对称加密密钥。AWS KMS
- 亚马逊 WorkMail 称之为 “AWS KMS加密” 操作。它为组织传入邮箱密钥和 AWS KMS key 的标识符。AWS KMS 返回使用 KMS 密钥加密的邮箱密钥的密文。

- Amazon 将加密的邮箱密钥与邮箱元数据一起 WorkMail 存储。

加密邮箱消息

要对消息进行加密，Amazon WorkMail 使用以下流程。

1. 亚马逊 WorkMail 为消息生成一个唯一的 256 位 AES 对称密钥。它使用明文消息密钥和高级加密标准 (AES) 算法在 AWS KMS 外加密消息。
2. 为了保护邮箱密钥下的消息密钥，Amazon WorkMail 需要解密邮箱密钥，该密钥始终以加密形式存储。

   Amazon WorkMail 调用 “AWS KMS解密” 操作并传入加密的邮箱密钥。 AWS KMS使用组织的 KMS 密钥解密邮箱密钥，然后将纯文本邮箱密钥返回给 Amazon。 WorkMail
3. Amazon WorkMail 使用纯文本邮箱密钥和高级加密标准 (AES) 算法对外部的邮件密钥进行加密。AWS KMS
4. Amazon 将加密消息密钥 WorkMail 存储在加密消息的元数据中，以便可以对其进行解密。

解密邮箱消息

要解密消息，Amazon WorkMail 使用以下流程。

1. Amazon WorkMail 调用 “AWS KMS解密” 操作并传入加密的邮箱密钥。 AWS KMS使用组织的 KMS 密钥解密邮箱密钥，然后将纯文本邮箱密钥返回给 Amazon。 WorkMail
2. Amazon WorkMail 使用纯文本邮箱密钥和高级加密标准 (AES) 算法来解密外部的加密邮件密钥。AWS KMS
3. Amazon WorkMail 使用明文消息密钥来解密加密的消息。

缓存邮箱密钥

为了提高性能并最大限度地减少对的呼叫AWS KMS，Amazon 在本地 WorkMail 缓存每个客户端的每个纯文本邮箱密钥最多一分钟。在缓存期结束时，将删除邮箱密钥。如果在缓存期间需要该客户端的邮箱密钥，Amazon WorkMail 可以从缓存中获取该密钥，而不必调用AWS KMS。邮箱密钥在缓存中受保护，并且永远不会以明文形式写入磁盘中。

授权使用 KMS 密钥

当 Amazon WorkMail 使用加密操作时，它代表邮箱管理员行事。AWS KMS key

要代表您将 AWS KMS key 用于密钥，管理员必须拥有以下权限。您可以在 IAM policy 或密钥政策中指定这些所需的权限。

- `kms:Encrypt`
- `kms:Decrypt`
- `kms:CreateGrant`

要允许 KMS 密钥仅用于来自亚马逊的请求 WorkMail，您可以将 kms: ViaService 条件密钥与`workmail.<region>.amazonaws.com`值一起使用。

您还可以在加密上下文中将密钥或值用作将 KMS 密钥用于加密操作的条件。例如，可在 IAM 或密钥策略文档中使用字符串条件运算符，或在授权中使用授权约束。

密钥策略，适用于 AWS 托管式密钥

只有当亚马逊 WorkMail 代表用户提出请求时，Ama WorkMail zon 的密钥策略才允许用户使用 KMS 密钥进行指定操作。AWS 托管式密钥密钥策略不允许任何用户直接使用 KMS 密钥。

此密钥策略与所有 AWS 托管式密钥 策略类似，均由该服务来建立。您无法更改密钥策略，但可以随时查看。有关更多信息，请参阅 查看密钥策略。

密钥策略中的策略语句具有以下影响：

- 允许账户和地区的用户使用 KMS 密钥进行加密操作和创建授权，但前提是请求来自亚马逊 WorkMail 代表他们。`kms:ViaService` 条件密钥可强制实施此限制。
- 允许 AWS 账户 创建 IAM policy 以允许用户查看 KMS 密钥属性和撤销授权。

以下是 Amazon 示例AWS 托管式密钥的关键政策 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" : "*"
  } ]
}
```

使用赠款授权 Amazon WorkMail

除了密钥策略外，Amazon 还 WorkMail 使用授权为每个组织添加对 KMS 密钥的权限。要查看您账户中 KMS 密钥的授权，请使用ListGrants操作。

Amazon WorkMail 使用授权向组织的 KMS 密钥添加以下权限。

- 添加`kms:Encrypt`允许 Amazon WorkMail 加密邮箱密钥的权限。
- 添加`kms:Decrypt`允许 Amazon WorkMail 使用 KMS 密钥解密邮箱密钥的权限。Amazon 在授权中 WorkMail 需要此权限，因为阅读邮箱消息的请求使用的是正在阅读邮件的用户的安全上下文。该请求不使用 AWS 账户 的凭证。当您为组织选择 KMS 密钥时，Amazon WorkMail 会创建此授权。

为了创建授权，Amaz CreateGranton 代表创建该组织的用户致 WorkMail 电。用于创建授权的权限来自密钥策略。当亚马逊 WorkMail 代表授权用户提出请求时，该政策允许账户用户调用`CreateGrant`组织的 KMS 密钥。

该密钥策略还允许账户根用户撤销对 AWS 托管式密钥 的授权。但是，如果您撤销授权，Amazon 将 WorkMail 无法解密您邮箱中的加密数据。

Amazon WorkMail 加密环境

加密上下文是一组包含任意非机密数据的键值对。在请求中包含加密上下文以加密数据时，AWS KMS 以加密方式将加密上下文绑定到加密的数据。要解密数据，您必须传入相同的加密上下文。

Amazon 在所有加密操作中 WorkMail 使用相同的AWS KMS加密上下文格式。您可以使用加密上下文在审计记录和日志中标识加密操作（例如 AWS CloudTrail），并将加密上下文用作在策略和授权中进行授权的条件。

在对的加密和解密请求中，AWS KMSAmazon WorkMail 使用加密环境，其中密钥为`aws:workmail:arn`，值为组织的亚马逊资源名称 (ARN)。

```
"aws:workmail:arn":"arn:aws:workmail:region:account ID:organization/organization ID"
```

例如，以下加密上下文将示例组织 ARN 包含在美国东部（俄亥俄）(`us-east-2`) 区域中。

```
"aws:workmail:arn":"arn:aws:workmail:us-east-2:111122223333:organization/
m-68755160c4cb4e29a2b2f8fb58f359d7"
```

监控亚马逊与之的 WorkMail 互动 AWS KMS

您可以使用AWS CloudTrail和 Amaz CloudWatch on Logs 来跟踪亚马逊AWS KMS代表您 WorkMail 发送的请求。

Encrypt

当您创建新邮箱时，Amazon WorkMail 会生成邮箱密钥并调用AWS KMS对邮箱密钥进行加密。亚马逊 WorkMail 向发送加密请求，AWS KMS其中包含明文邮箱密钥和亚马逊 WorkMail 组织的 KMS 密钥标识符。

记录 `Encrypt` 操作的事件与以下示例事件类似。用户是 Amazon WorkMail 服务。这些参数包括 KMS 密钥 ID (`keyId`) 和 Amazon WorkMail 组织的加密上下文。Amazon WorkMail 还会传入邮箱密钥，但该密钥不会记录在 CloudTrail 日志中。

```
{
    "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

当您添加、查看或删除邮箱消息时，Amazon WorkMail 会要求AWS KMS解密邮箱密钥。亚马逊 WorkMail 向发送解密请求，其中包含加密AWS KMS的邮箱密钥和亚马逊 WorkMail组织的 KMS 密钥的标识符。

记录 Decrypt 操作的事件与以下示例事件类似。用户是 Amazon WorkMail 服务。这些参数包括未记录在日志中的加密邮箱密钥（作为密文 blob）和 Amazon 组织的加密上下文。 WorkMail AWS KMS从密文中获取 KMS 密钥的 ID。

```
{
```

```
    "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"
}
```


如何 WorkSpaces 使用 AWS KMS

您可以使用WorkSpaces为每个最终用户配置基于云的桌面 (a WorkSpace)。启动新版本时 WorkSpace，您可以选择加密其卷并决定使用哪个卷AWS KMS key进行加密。您可以选择 for WorkSpaces（aws/workspaces）或对称客户托管密钥。AWS 托管式密钥

> **Important**
>
> WorkSpaces 仅支持对称加密 KMS 密钥。您不能使用非对称 KMS 密钥对中的卷进行加密。WorkSpaces要获取确定 KMS 密钥是对称还是非对称的帮助，请参阅 识别非对称 KMS 密钥。

有关 WorkSpaces 使用加密卷创建的更多信息，请参阅《Amazon WorkSpaces 管理指南》WorkSpace中的 “加密”。

主题

- 使用 WorkSpaces 加密概述 AWS KMS
- WorkSpaces 加密上下文
- WorkSpaces 授予代表您使用 KMS 密钥的权限

使用 WorkSpaces 加密概述 AWS KMS

使用加密卷创建 WorkSpaces 时， WorkSpaces 使用亚马逊弹性区块存储 (Amazon EBS) Elastic Block Store 来创建和管理这些卷。这两种服务都使用 AWS KMS key 来处理加密卷。有关 EBS 卷加密的更多信息，请参阅以下文档：

- 本指南中的Amazon Elastic Block Store (Amazon EBS) 如何使用 AWS KMS
- 适用于 Windows 实例的 Amazon EC2 用户指南中的 Amazon EBS 加密

当您 WorkSpaces 使用加密卷启动时， end-to-end 过程如下所示：

1. 您可以指定用于加密的 KMS 密钥以及 WorkSpace的用户和目录。此操作会创建一项授权，该授权仅 WorkSpaces 允许为此使用您的 KMS 密钥 WorkSpace，也就是说，仅允许与指定用户和目录 WorkSpace 关联的用户使用您的 KMS 密钥。
2. WorkSpaces 为创建加密的 EBS 卷 WorkSpace 并指定要使用的 KMS 密钥以及该卷的用户和目录（与您在中指定的信息相同Step 1）。此操作将创建一项授权，允许 Amazon EBS 仅将您的 KMS 密钥用于此卷 WorkSpace 和卷，也就是说，仅适用于与指定用户和目录 WorkSpace 关联的，并且仅用于指定的卷。
3. Amazon EBS 请求使用您的 KMS 密钥加密的卷数据密钥，并将 WorkSpace 用户`Sid`和目录 ID 以及卷 ID 指定为加密上下文。
4. AWS KMS 创建新的数据密钥，使用您的 KMS 密钥对其进行加密，然后将加密的数据密钥发送到 Amazon EBS。

5. WorkSpaces 使用 Amazon EBS 将加密卷附加到您的 WorkSpace。Amazon EBS AWS KMS 通过Decrypt请求将加密的数据密钥发送到，并指定 WorkSpace 用户的Sid、其目录 ID 和卷 ID，后者用作加密上下文。
6. AWS KMS 使用您的 KMS 密钥解密数据密钥，然后将纯文本数据密钥发送到 Amazon EBS。
7. Amazon EBS 使用纯文本数据密钥加密所有传入和传出加密卷的数据。Amazon EBS 会将纯文本数据密钥保存在内存中，直至该卷连接到。 WorkSpace
8. Amazon EBS 将加密的数据密钥（接收于Step 4）与卷元数据一起存储，以备将来重启或重建时使用。 WorkSpace
9. 当您使用删除 WorkSpace （或使用 WorkSpaces API 中的TerminateWorkspaces操作）时，WorkSpaces Amazon EBS 会停用允许他们使用您的 KMS 密钥进行此 WorkSpace操作的赠款。AWS Management Console

WorkSpaces 加密上下文

WorkSpaces 不AWS KMS key直接使用你的进行加密操作（例如Encrypt、DecryptGenerateDataKey、等），这意味着 WorkSpaces 不向包含加密上下文的请求发送请求。AWS KMS但是，当 Amazon EBS 请求您的加密卷的加密数据密钥时 WorkSpaces（Step 3在使用 WorkSpaces 加密概述 AWS KMS）以及请求该数据密钥的纯文本副本（Step 5）时，它会在请求中包含加密上下文。加密上下文提供 AWS KMS 用于确保数据完整性而使用的额外的身份验证数据 (AAD)。加密上下文也将写入您的 AWS CloudTrail 日志文件，这有助于您了解为什么使用给定的 AWS KMS key。Amazon EBS 会对加密上下文使用以下内容：

- 与关联的AWS Directory Service用户的 `sid` WorkSpace
- 与之关联的AWS Directory Service目录的目录 ID WorkSpace
- 加密卷的卷 ID

以下示例显示了 Amazon EBS 使用的加密上下文的 JSON 表示形式：

```
{
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

WorkSpaces 授予代表您使用 KMS 密钥的权限

您可以在 for WorkSpaces (aws/workspaces) 或客户托管密钥下保护您的工作空间数据。如果您使用客户托管密钥，则需要授予代表账户 WorkSpaces管理员使用 KMS 密钥的 WorkSpaces 权限。AWS 托管式密钥默认情况下 WorkSpaces ，for 具有所需的权限。AWS 托管式密钥

要准备您的客户托管密钥以供使用 WorkSpaces，请按以下步骤操作。

1. 将 WorkSpaces 管理员添加到 KMS 密钥的密钥策略中的密钥用户列表中
2. 通过 IAM 策略为 WorkSpaces 管理员提供额外权限

WorkSpaces 管理员还需要获得使用权限 WorkSpaces。有关这些权限的更多信息，请参阅《Amazon WorkSpaces 管理指南》中的 “控制 WorkSpaces资源访问权限”。

第 1 部分：向 KMS 密钥的密钥用户添加 WorkSpaces 管理员

要向 WorkSpaces 管理员授予他们所需的权限，您可以使用AWS Management Console或 AWS KMS API。

将 WorkSpaces 管理员添加为 KMS 密钥的密钥用户（控制台）

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择首选客户托管密钥的密钥 ID 或别名。
5. 选择 Key policy (密钥策略) 选项卡。在 Key users（密钥用户）下，选择 Add（添加）。
6. 在 IAM 用户和角色列表中，选择与您的 WorkSpaces 管理员对应的用户和角色，然后选择附加。

将 WorkSpaces 管理员添加为 KMS 密钥的密钥用户 (AWS KMSAPI)

1. 使用GetKeyPolicy操作获取现有密钥策略，然后将策略文档保存到文件中。
2. 在您的首选文本编辑器中打开策略文档。将与您的 WorkSpaces 管理员对应的 IAM 用户和角色添加到向关键用户授予权限的策略声明中。然后保存文件。
3. 使用PutKeyPolicy操作将密钥策略应用于 KMS 密钥。

第 2 部分：为 WorkSpaces 管理员提供额外权限

如果您使用客户托管密钥来保护 WorkSpaces 数据，则除了默认密钥策略的 “密钥用户” 部分中的权限外，WorkSpaces 管理员还需要权限才能对 KMS 密钥创建授权。此外，如果 WorkSpaces 管理员使用使用加密卷AWS Management Console WorkSpaces 进行创建，则需要列出别名和列出密钥的权限。有关创建和编辑 IAM 用户策略的信息，请参阅 IAM 用户指南中的托管策略与内联策略。

要将这些权限授予您的 WorkSpaces 管理员，请使用 IAM 策略。在每位 WorkSpaces管理员的 IAM 策略中添加与以下示例类似的策略声明。将示例 IAM 密钥 ARN (*arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab*) 替换为有效值。如果您的 WorkSpaces 管理员仅使用 WorkSpaces API（不使用控制台），则可以省略第二条具有"kms:ListAliases"和"kms:ListKeys"权限的策略声明。

```
{
  "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": "*"
    }
  ]
}
```

使用 AWS KMS API 进行编程

您可以使用 AWS KMS API 来创建和管理 KMS 密钥和特殊功能，如自定义密钥存储，并在加密操作中使用 KMS 密钥。有关详细信息，请参阅 AWS Key Management Service API 引用。

以下主题中的示例代码显示如何使用 AWS 开发工具包调用 AWS KMS API。

有关使用 AWS KMS 控制台执行其中某些任务的信息，请参阅管理 密钥。

主题

创建客户端

要使用 Node.js 中的AWS SDK for Java、AWS SDK for .NET、the AWS SDK for Ruby、the AWS SDK for PHP、the 或 AWS SDK 来编写使用 AWS Key Management Service(AWS KMS) API 的代码，请先创建一个AWS KMS客户端。AWS SDK for Python (Boto3) JavaScript

后面的主题中会在示例代码中使用您创建的客户端对象。

Java

要在 Java 中创建 AWS KMS 客户端，请使用客户端生成器。

```
AWSKMS kmsClient = AWSKMSClientBuilder.standard().build();
```

有关使用 Java 客户端生成器的更多信息，请参阅以下资源。

- 开发人员博客上的 Fluent Client BuildersAWS

- AWS SDK for Java 开发人员指南中的创建服务客户端
- 《AWS SDK for Java API 参考》中的 AWSKMSClientBuilder

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

要在 PHP 中创建 AWS KMS 客户端，请使用 AWS KMS 客户端对象，并指定版本 2014-11-01。有关更多信息，请参阅 AWS SDK for PHP API 参考中的 KMSClient 类。

```
// 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();
```

使用密钥

本主题中的示例使用 AWS KMS API 创建、查看、启用和禁用 AWS KMS AWS KMS keys 并生成数据密钥。

主题

创建 KMS 密钥

要创建 AWS KMS key（KMS 密钥），请使用CreateKey操作。本节中的示例创建一个对称加密 KMS 密钥。这些示例中使用的 `Description` 参数是可选的。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

有关在 AWS KMS 控制台中创建 KMS 密钥的帮助，请参阅 创建密钥。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 createKey 方法。

```
// Create a KMS key
//
String desc = "Key for protecting critical data";

CreateKeyRequest req = new CreateKeyRequest().withDescription(desc);
CreateKeyResult result = kmsClient.createKey(req);
```

C#

有关详细信息，请参阅 AWS SDK for .NET 中的 CreateKey 方法。

```
// Create a KMS key
//
String desc = "Key for protecting critical data";

CreateKeyRequest req = new CreateKeyRequest()
{
    Description = desc
```

```
};
CreateKeyResponse response = kmsClient.CreateKey(req);
```

Python

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 create_key 方法。

```
# Create a KMS key

desc = 'Key for protecting critical data'

response = kms_client.create_key(
    Description=desc
)
```

Ruby

有关详细信息，请参阅 AWS SDK for Ruby 中的 create_key 实例方法。

```
# Create a KMS key

desc = 'Key for protecting critical data'

response = kmsClient.create_key({
  description: desc
})
```

PHP

有关详细信息，请参阅 AWS SDK for PHP 中的 CreateKey 方法。

```
// Create a KMS key
//
$desc = "Key for protecting critical data";

$result = $KmsClient->createKey([
    'Description' => $desc
]);
```

Node.js

有关详细信息，请参阅 Node.js 软件开发工具包中的 create AWS Key 属性 JavaScript 。

```
// Create a KMS key
//
const Description = 'Key for protecting critical data';

kmsClient.createKey({ Description }, (err, data) => {
  ...
});
```

PowerShell

要在中创建 KMS 密钥 PowerShell，请使用 New-KmsKey cmdlet。

```
# Create a KMS key

$desc = 'Key for protecting critical data'
New-KmsKey -Description $desc
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

生成数据密钥

要生成对称数据密钥，请使用GenerateDataKey操作。此操作将返回一个明文数据密钥以及以您指定的对称加密 KMS 密钥加密的该数据密钥的副本。您必须在每个命令中指定 KeySpec 或 NumberOfBytes（但不能同时指定这两者）。

在使用数据密钥加密数据如需帮助，请参阅 AWS Encryption SDK。您还可以使用数据密钥进行 HMAC 操作。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅《AWS SDK for JavaAPI 参考》中的generateDataKey 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 GenerateDataKey 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 generate_data_key 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 generate_data_key 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 GenerateDataKey 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS 软件开发工具包 JavaScript 中的generateDataKey 属性。

```
// 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

要生成对称数据密钥，请使用 new-DataKey KMS cmdlet。

在输出中，纯文本密钥（在Plaintext属性中）和加密密钥（在CiphertextBlob属性中）是MemoryStream对象。要将它们转换为字符串，请使用MemoryStream类的方法，或者使用将MemoryStream对象转换为字符串的 cmdlet 或函数，例如 Convert 模块中的 ConvertFrom-MemoryStream 和 ConvertFrom-Base64 函数。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

查看 AWS KMS key

要获取有关（包括 KMS 密钥 ARN 和密钥状态）的详细信息，请使用操作。AWS KMS key DescribeKey

DescribeKey 未获得别名。要获取别名，请使用ListAliases操作。有关示例，请参阅使用别名。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

有关在 AWS KMS 控制台中查看 KMS 密钥的帮助，请参阅 查看密钥。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 describeKey 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 DescribeKey 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 describe_key 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 describe_key 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 DescribeKey 方法。

```
// 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

有关详细信息，请参阅 Node.js 软件开发工具包中的 AWS describe K JavaScript ey 属性。

```
// 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

要获取有关 KMS 密钥的详细信息，请使用 Get-KmsKey cmdlet。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

获取 KMS 密钥的密钥 ID 和密钥 ARN

要获取的密钥 ID 和密钥 ARNAWS KMS keys，请使用ListKeys操作。这些示例使用可选 `Limit` 参数，该参数设置在每个调用中返回的最大 KMS 密钥数。有关在 AWS KMS 操作中识别 KMS 密钥的帮助信息，请参阅 密钥标识符 (KeyId)。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

有关在 AWS KMS 控制台中查找密钥 ID 和密钥 ARN 的帮助，请参阅查找密钥 ID 和密钥 ARN。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 listKeys 方法。

```
// List KMS keys in this account
```

```
//
Integer limit = 10;

ListKeysRequest req = new ListKeysRequest().withLimit(limit);
ListKeysResult result = kmsClient.listKeys(req);
```

C#

有关详细信息，请参阅 AWS SDK for .NET 中的 ListKeys 方法。

```
// List KMS keys in this account
//
int limit = 10;

ListKeysRequest listKeysRequest = new ListKeysRequest()
{
    Limit = limit
};
ListKeysResponse listKeysResponse = kmsClient.ListKeys(listKeysRequest);
```

Python

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 list_keys 方法。

```
# List KMS keys in this account

response = kms_client.list_keys(
    Limit=10
)
```

Ruby

有关详细信息，请参阅 AWS SDK for Ruby 中的 list_keys 实例方法。

```
# List KMS keys in this account

response = kmsClient.list_keys({
  limit: 10
})
```

PHP

有关详细信息，请参阅 AWS SDK for PHP 中的 ListKeys 方法。

```
// List KMS keys in this account
//
$limit = 10;

$result = $KmsClient->listKeys([
    'Limit' => $limit,
]);
```

Node.js

有关详细信息，请参阅 Node.js 软件开发工具包中的 list AWS Keys 属性 JavaScript 。

```
// List KMS keys in this account
//
const Limit = 10;
kmsClient.listKeys({ Limit }, (err, data) => {
  ...
});
```

PowerShell

要获取账户和区域中所有 KMS 密钥的密钥 ID 和密钥 ARN，请使用 Get -KmsKeyList cmdlet。

为限制输出对象的数量，此示例使用 Select-Object cmdlet，而不是 `Limit` 参数，该参数在列表 cmdlet 中将被弃用。有关在 AWS Tools for PowerShell 中分页输出的帮助，请参阅使用 AWS Tools for PowerShell 的输出分页。

```
# List KMS keys in this account

$limit = 10
Get-KmsKeyList | Select-Object -First $limit
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

启用 AWS KMS keys

要启用已禁用AWS KMS key，请使用EnableKey操作。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

有关在 AWS KMS 控制台中启用和禁用 KMS 密钥的帮助，请参阅 启用和禁用密钥。

Java

有关 Java 实施的详细信息，请参阅 AWS SDK for Java API 参考中的 enableKey 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 EnableKey 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 enable_key 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 enable_key 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 EnableKey 方法。

```
// 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

有关详细信息，请参阅 Node.js 软件开发工具包中的 AWSenable K JavaScript ey 属性。

```
// 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

要启用 KMS 密钥，请使用 En able-KmsKey cmdlet。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

禁用 AWS KMS key

要禁用 KMS 密钥，请使用DisableKey操作。禁用 KMS 密钥可防止其在加密操作中使用。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

有关在 AWS KMS 控制台中启用和禁用 KMS 密钥的帮助，请参阅 启用和禁用密钥。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 disableKey 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 DisableKey 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 disable_key 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 disable_key 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 DisableKey 方法。

```
// 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

有关详细信息，请参阅 Node.js 软件开发工具包中的 AWS d isable K JavaScript ey 属性。

```
// 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

要禁用 KMS 密钥，请使用禁用-KmsKey cmdlet。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

使用别名

本主题中的示例使用 AWS KMS API 创建、查看、更新和删除别名。有关别名的信息，请参阅 the section called “使用别名”。

主题

创建别名

在 AWS Management Console 中创建 AWS KMS key 时，您必须创建它的别名。但是，创建 KMS 密钥的CreateKey操作不会创建别名。

要创建别名，请使用CreateAlias操作。别名在账户和 区域中必须是唯一的。您无法创建以 aws/ 开头的别名。aws/ 前缀被 Amazon Web Services 保留用于 AWS 托管式密钥。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 createAlias 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 CreateAlias 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 create_alias 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 create_alias 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 CreateAlias 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS软件开发工具包中的 createAlias 属性 JavaScript 。

```
// 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

要创建别名，请使用 New-KMSAlias cmdlet。别名名称区分大小写。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

列出别名

要列出账户和区域中的别名，请使用ListAliases操作。

默认情况下，ListAliases 命令会返回账户和区域中的所有别名。这包括您创建的与您的客户托管密钥关联的别名，以及 AWS 创建并与您的 AWS 托管式密钥 关联的别名。该响应可能还包括没有 `TargetKeyId` 字段的别名。这些是 AWS 已创建但尚未与 KMS 密钥关联的预定义别名。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关 Java 实施的详细信息，请参阅中的 AWS SDK for Java API 参考中的 listAliases 方法。

```
// List the aliases in this AWS ##
//
Integer limit = 10;

ListAliasesRequest req = new ListAliasesRequest().withLimit(limit);
ListAliasesResult result = kmsClient.listAliases(req);
```

C#

有关详细信息，请参阅 AWS SDK for .NET 中的 ListAliases 方法。

```
// List the aliases in this AWS ##
//
int limit = 10;

ListAliasesRequest listAliasesRequest = new ListAliasesRequest()
{
    Limit = limit
};
ListAliasesResponse listAliasesResponse = kmsClient.ListAliases(listAliasesRequest);
```

Python

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 `list_aliases` 方法。

```
# List the aliases in this AWS ##

response = kms_client.list_aliases(
    Limit=10
)
```

Ruby

有关详细信息，请参阅 AWS SDK for Ruby 中的 `list_aliases` 实例方法。

```
# List the aliases in this AWS ##

response = kmsClient.list_aliases({
  limit: 10
})
```

PHP

有关详细信息，请参阅 https://docs.aws.amazon.com/sdk-for-php/latest/reference/api-kms-2014-11-01.html#listaliases 中的 AWS SDK for PHPList Aliases 方法。

```
// List the aliases in this AWS ##
//
$limit = 10;

$result = $KmsClient->listAliases([
    'Limit' => $limit,
]);
```

Node.js

有关详细信息，请参阅 Node.js 软件开发工具包 JavaScript 中的 AWSlistAliases 属性。

```
// List the aliases in this AWS ##
//
const Limit = 10;
kmsClient.listAliases({ Limit }, (err, data) => {
  ...
});
```

PowerShell

要列出账户和区域中的别名，请使用 get-KMS cmdlet AliasList。

为限制输出对象的数量，此示例使用 Select-Object cmdlet，而不是 Limit 参数，该参数在列表 cmdlet 中将被弃用。有关在 AWS Tools for PowerShell 中分页输出的帮助，请参阅使用 AWS Tools for PowerShell 的输出分页。

```
# List the aliases in this AWS ##
$limit = 10

$result = Get-KMSAliasList | Select-Object -First $limit
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

要仅列出与特定 KMS 密钥关联的别名，请使用 KeyId 参数。其值可以是区域中任何 KMS 密钥的密钥 ID 或密钥 ARN。您不能指定别名名称或别名 ARN。

Java

有关 Java 实施的详细信息，请参阅中的 AWS SDK for Java API 参考中的 listAliases 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 ListAliases 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 list_aliases 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 list_aliases 实例方法。

```
# 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

有关详细信息，请参阅 https://docs.aws.amazon.com/sdk-for-php/latest/reference/api-kms-2014-11-01.html#listaliases 中的 AWS SDK for PHPList Aliases 方法。

```
// 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

有关详细信息，请参阅 Node.js 软件开发工具包 JavaScript 中的 AWSlistAliases 属性。

```
// 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

要列出 KMS 密钥的别名，请使用 get-KMS cmdlet AliasList 的KeyId参数。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

更新别名

要将现有别名与其他 KMS 密钥关联，请使用UpdateAlias操作。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关 Java 实施的详细信息，请参阅中的 AWS SDK for Java API 参考中的 updateAlias 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 UpdateAlias 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 update_alias 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 update_alias 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 UpdateAlias 方法。

```
// 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

有关详细信息，请参阅 Node.js 软件开发工具包 JavaScript 中的 AWSupdateAlias 属性。

```
// 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

若要更改与别名关联的 KMS 密钥，请使用 Update-KMSAlias cmdlet。别名名称区分大小写。

`Update-KMSAlias` cmdlet 不返回任何输出。要验证该命令是否有效，请使用 get-KMS cmdlet AliasList。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

删除别名

要删除别名，请使用DeleteAlias操作。删除别名不会影响关联的 KMS 密钥。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 deleteAlias 方法。

```
// Delete an alias for a KMS key
//
String aliasName = "alias/projectKey1";

DeleteAliasRequest req  = new DeleteAliasRequest().withAliasName(aliasName);
kmsClient.deleteAlias(req);
```

C#

有关详细信息，请参阅 AWS SDK for .NET 中的 DeleteAlias 方法。

```
// Delete an alias for a KMS key
//
String aliasName = "alias/projectKey1";

DeleteAliasRequest deleteAliasRequest = new DeleteAliasRequest()
{
    AliasName = aliasName
};
kmsClient.DeleteAlias(deleteAliasRequest);
```

Python

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 delete_alias 方法。

```
# Delete an alias for a KMS key

alias_name = 'alias/projectKey1'

response = kms_client.delete_alias(
    AliasName=alias_name
)
```

Ruby

有关详细信息，请参阅 AWS SDK for Ruby 中的 delete_alias 实例方法。

```
# Delete an alias for a KMS key
```

```
alias_name = 'alias/projectKey1'

response = kmsClient.delete_alias({
  alias_name: alias_name
})
```

PHP

有关详细信息，请参阅 AWS SDK for PHP 中的 DeleteAlias 方法。

```
// Delete an alias for a KMS key
//
$aliasName = "alias/projectKey1";

$result = $KmsClient->deleteAlias([
    'AliasName' => $aliasName,
]);
```

Node.js

有关详细信息，请参阅 Node.js 软件开发工具包 JavaScript 中的 AWSdeleteAlias 属性）。

```
// Delete an alias for a KMS key
//
const AliasName = 'alias/projectKey1';
kmsClient.deleteAlias({ AliasName }, (err, data) => {
  ...
});
```

PowerShell

要删除别名，请使用 Remove-KMSAlias cmdlet。别名名称区分大小写。

由于此 cmdlet 会永久删除别名，因此 PowerShell 会提示您确认该命令。`ConfirmImpact` 是 `High`，因此您不能使用 `ConfirmPreference` 禁止显示此提示。如果必须禁止显示确认提示，请添加值为 `$false` 的 `Confirm` 公共参数，例如：`-Confirm:$false`。

`Remove-KMSAlias` cmdlet 不返回任何输出。要验证该命令是否有效，请使用 get-KMS cmdlet AliasList。

```
# Delete an alias for a KMS key
```

```
$aliasName = 'alias/projectKey1'
Remove-KMSAlias -AliasName $aliasName
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

加密和解密数据密钥

本主题中的示例使用 API 中的加密、解密和ReEncrypt操作。AWS KMS

这些操作专用于加密和解密数据密钥。它们在加密操作中使用 AWS KMS keys，而且它们无法接受 4KB（4096 字节）以上的数据。尽管您可以使用它们来加密少量数据，例如密码或 RSA 密钥，但它们不用于加密应用程序数据。

要加密应用程序数据，请使用 AWS 服务的服务器端加密功能或客户端加密库，例如 AWS Encryption SDK 或 Amazon S3 加密客户端。

主题

- 加密数据密钥
- 解密数据密钥
- 在不同的 AWS KMS key 下重新加密数据密钥

加密数据密钥

Encrypt 操作专用于加密数据密钥，但并不常用。GenerateDataKey和GenerateDataKeyWithoutPlaintext操作返回加密的数据密钥。在将加密的数据移动到不同区域并希望在新区域中使用 KMS 密钥加密其数据密钥时，可以使用此方法。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 encrypt 方法。

```
// 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#

有关详细信息，请参阅 https://docs.aws.amazon.com/sdkfornet/v3/apidocs/items/KeyManagementService/MKeyManagementServiceEncryptEncryptRequest.html 中的 AWS SDK for .NETEncrypt 方法。

```
// 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

有关详细信息，请参阅 中的 encrypt 方法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

有关详细信息，请参阅 https://docs.aws.amazon.com/sdk-for-ruby/v3/api/Aws/KMS/Client.html#encrypt-instance_method 中的 AWS SDK for Rubyencrypt 实例方法。

```
# 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

有关详细信息，请参阅 https://docs.aws.amazon.com/aws-sdk-php/v3/api/api-kms-2014-11-01.html#encrypt 中的 AWS SDK for PHPEncrypt 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS 软件开发工具包中的 en crypt 属性。 JavaScript

```
// 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

要使用 KMS 密钥加密数据密钥，请使用 Invoke-KMSEncrypt cmdlet。它将密文作为 MemoryStream (system.io. MemoryStream) 对象。您可以使用 MemoryStream 对象作为 Invoke-KMSDecrypt cmdlet 的输入。

AWS KMS 也将数据密钥作为 MemoryStream 对象返回。在这个例子中，为了模拟明文数据密钥，我们创建一个字节数组并将其写入 MemoryStream 对象。

请注意，Invoke-KMSEncrypt 的 Plaintext 参数采用字节数组 (byte[])；它不需要 MemoryStream 对象。从 4.0 AWSPowerShell 版开始，所有采用字节数组和MemoryStream对象的 AWSPowerShell 模块中的参数都接受字节数组、MemoryStream对象、字符串、字符串数组和 FileInfo (System.io. FileInfo) 对象。您可以将这些类型中的任何一种传递给 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

解密数据密钥

要解密数据密钥，请使用 Decrypt 操作。

您指定的必须ciphertextBlob是GenerateDataKey、GenerateDataKeyWithoutPlaintext或 Encrypt 响应中的CiphertextBlob字段值，或者是GenerateDataKeyPairWithoutPlaintext响应中的PrivateKeyCiphertextBlob字段值。GenerateDataKeyPair您还可以使用 Decrypt 操作解密由非对称 KMS 密钥中的公有密钥在 AWS KMS 外部加密的数据。

使用对称加密 KMS 密钥进行解密时不需要 KeyId 参数。AWS KMS 可以获取用于加密密文 Blob 中的元数据中的数据的 KMS 密钥。但是，指定您正在使用的 KMS 密钥始终是最佳实践。此做法可确保您使用预期的 KMS 密钥，并防止您意外使用不信任的 KMS 密钥解密密文。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 decrypt 方法。

```
// 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#

有关详细信息，请参阅 https://docs.aws.amazon.com/sdkfornet/v3/apidocs/items/KeyManagementService/MKeyManagementServiceDecryptDecryptRequest.html 中的 AWS SDK for .NETDecrypt 方法。

```
// 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

有关详细信息，请参阅 中的 decrypt 方法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

有关详细信息，请参阅 https://docs.aws.amazon.com/sdk-for-ruby/v3/api/Aws/KMS/Client.html#decrypt-instance_method 中的 AWS SDK for Rubydecrypt 实例方法。

```
# 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

有关详细信息，请参阅 https://docs.aws.amazon.com/aws-sdk-php/v3/api/api-kms-2014-11-01.html#decrypt 中的 AWS SDK for PHPDecrypt 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS软件开发工具包中的解密属性 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

要解密数据密钥，请使用 Invoke-KMSEncrypt cmdlet。

此 cmdlet 以 (System.io.) 的形式返回纯文本 MemoryStream MemoryStream) 对象。要将其转换为字节数组，请使用将 MemoryStream 对象转换为字节数组的 cmdlet 或函数，例如 Convert 模块中的函数。

由于此示例使用 AWS KMS 加密 cmdlet 返回的密文，因此它使用 MemoryStream 对象作为 CiphertextBlob 参数的值。但是，Invoke-KMSDecrypt 的 CiphertextBlob 参数采用字节数组 (byte[])；它不需要 MemoryStream 对象。从 4.0 AWSPowerShell 版开始，所有采用字节数组和MemoryStream对象的 AWSPowerShell 模块中的参数都接受字节数组、MemoryStream对象、字符串、字符串数组和 FileInfo (System.io. FileInfo) 对象。您可以将这些类型中的任何一种传递给 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

在不同的 AWS KMS key 下重新加密数据密钥

要解密加密的数据密钥，然后立即在不同的数据密钥下重新加密该数据密钥AWS KMS key，请使用该操作。ReEncrypt这些操作全部都在 AWS KMS 内的服务器端执行，因此它们永远不会将您的明文在 AWS KMS 外公开。

您指定的必须ciphertextBlob是GenerateDataKey、GenerateDataKeyWithoutPlaintext或 Encrypt 响应中的CiphertextBlob字段值，或者是GenerateDataKeyPairWithoutPlaintext响应中的PrivateKeyCiphertextBlob字段值。GenerateDataKeyPair您还可以使用 ReEncrypt 操作重新加密由非对称 KMS 密钥中的公有密钥在 AWS KMS 外部加密的数据。

使用对称加密 KMS 密钥进行重新加密时不需要 SourceKeyId 参数。AWS KMS 可以获取用于加密密文 Blob 中的元数据中的数据的 KMS 密钥。但是，指定您正在使用的 KMS 密钥始终是最佳实践。此做法可确保您使用预期的 KMS 密钥，并防止您意外使用不信任的 KMS 密钥解密密文。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 reEncrypt 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 ReEncrypt 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 re_encrypt 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 re_encrypt 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 ReEncrypt 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS软件开发工具包中的 reEncrypt 属性 JavaScript 。

```
// 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

要使用相同或不同的 KMS 密钥重新加密密文，请使用 invoke-KMS cmdlet。ReEncrypt

由于此示例使用 AWS KMS 加密 cmdlet 返回的密文，因此它使用 MemoryStream 对象作为 CiphertextBlob 参数的值。但是，Invoke-KMSReEncrypt 的 CiphertextBlob 参数采用字节数组 (byte[])；它不需要 MemoryStream 对象。从 4.0 AWSPowerShell 版开始，所有采用字节数组和MemoryStream对象的 AWSPowerShell 模块中的参数都接受字节数组、MemoryStream对象、字符串、字符串数组和 FileInfo (System.io. FileInfo) 对象。您可以将这些类型中的任何一种传递给 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

使用密钥策略

本主题中的示例使用 AWS KMS API 查看和更改 AWS KMS keys 的密钥策略。

有关如何使用密钥政策、IAM policy 管理和授权对您的 KMS 密钥的访问的详细信息，请参阅 AWS KMS 的身份验证和访问控制。有关编写和格式化 JSON 策略文档的帮助，请参阅 IAM 用户指南中的 IAM JSON 策略参考。

主题

- 列出密钥策略名称
- 获取密钥策略
- 设置密钥策略

列出密钥策略名称

要获取的密钥策略的名称AWS KMS key，请使用ListKeyPolicies操作。它返回的唯一密钥策略名称是default。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关 Java 实现的详细信息，请参阅《AWS SDK for JavaAPI 参考》中的listKeyPolicies 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 ListKeyPolicies 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 list_key_policies 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 list_key_policies 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 ListKeyPolicies 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS 软件开发工具包 JavaScript 中的listKeyPolicies 属性。

```
// 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

要列出默认密钥策略的名称，请使用 get-KMS cmdlet 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

获取密钥策略

要获取的密钥策略AWS KMS key，请使用GetKeyPolicy操作。

GetKeyPolicy 需要策略名称。唯一有效的策略名称是 default。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅《AWS SDK for JavaAPI 参考》中的getKeyPolicy 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 GetKeyPolicy 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 get_key_policy 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 get_key_policy 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 GetKeyPolicy 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS 软件开发工具包 JavaScript 中的getKeyPolicy 属性。

```
// 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

要获取 KMS 密钥的密钥策略，请使用 get-KMS cmdlet KeyPolicy。此 cmdlet 以字符串（System.String）的形式返回密钥策略，您可以在 Wr it KeyPolicy e-KMS () 命令中使用该字符串。PutKeyPolicy要将 JSON 字符串中的策略转换为PSCustomObject对象，请使用 ConvertFrom-JSON cmdle t。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

设置密钥策略

要创建或替换 KMS 密钥的密钥策略，请使用PutKeyPolicy操作。

PutKeyPolicy 需要策略名称。唯一有效的策略名称是 default。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅《AWS SDK for JavaAPI 参考》中的putKeyPolicy 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 PutKeyPolicy 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 put_key_policy 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 put_key_policy 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 PutKeyPolicy 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS 软件开发工具包 JavaScript 中的putKeyPolicy 属性。

```
// 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

要为 KMS 密钥设置密钥策略，请使用 Write-KMS KeyPolicy cmdlet。此 cmdlet 不返回任何输出。要验证该命令是否有效，请使用 get-KMS cmdlet KeyPolicy。

Policy 参数接受一个字符串。用单引号将字符串括起来，使其成为文本字符串。您不必在文本字符串中使用延续字符或转义字符。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

处理授权

本主题中的示例使用 AWS KMS API 创建、查看、停用和撤销对 AWS KMS keys 的授权。有关在 AWS KMS 中使用授权的更多详细信息，请参阅AWS KMS 中的授权。

主题

- 创建授予
- 查看授予
- 停用授予
- 撤销授予

创建授予

要为创建授权AWS KMS key，请使用CreateGrant操作。响应仅包括授权 ID 和授权令牌。要获取有关拨款的详细信息，请使用ListGrants操作，如所示查看授予。

这些示例创建了一个授权，允许能够担任该`ExampleKeyUser`角色的用户对`KeyId`参数标识的 KMS 密钥调用GenerateDataKey操作。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 createGrant 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 CreateGrant 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 create_grant 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 `create_grant` 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 CreateGrant 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS软件开发工具包中的 createGrant 属性 JavaScript 。

```
// 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

要创建授权，请使用 New-KMSGrant cmdlet。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

查看授予

要获取有关 KMS 密钥授权的详细信息，请使用ListGrants操作。

> **Note**
>
> `ListGrants` 响应中的 `GranteePrincipal` 字段通常包含授权的被授权者委托人。但是，当授权中的被授权者委托人是 AWS 服务时，`GranteePrincipal` 字段包含服务委托人，该委托人可能表示多个不同的被授权者委托人。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

这些示例使用可选 `Limits` 参数，该参数确定操作返回的授权数量。

Java

有关 Java 实施的详细信息，请参阅中的 AWS SDK for Java API 参考中的 listGrants 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 ListGrants 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 list_grants 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 list_grants 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 ListGrants 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS软件开发工具包中的 listGrants 属性 JavaScript 。

```
// 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

要查看 KMS 密钥的所有AWS KMS授权的详细信息，请使用 get-KMS cmdlet GrantList。

为限制输出对象的数量，此示例使用 Select-Object cmdlet，而不是 `Limit` 参数，该参数在列表 cmdlet 中将被弃用。有关在 AWS Tools for PowerShell 中分页输出的帮助，请参阅使用 AWS Tools for PowerShell 的输出分页。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

您必须在每个 `ListGrants` 运算中指定 KMS 密钥。但是，您可以通过指定授权 ID 或被授权者委托人来进一步筛选授权列表。以下示例仅获取 KMS 密钥的授权，其中 `test-engineer` 角色是被授予者承担者。

Java

有关 Java 实施的详细信息，请参阅中的 AWS SDK for Java API 参考中的 listGrants 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 ListGrants 方法。

```
// 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

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 `list_grants` 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 `list_grants` 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 ListGrants 方法。

```
// 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

有关详细信息，请参阅 Node.js AWS软件开发工具包中的 listGrants 属性 JavaScript 。

```
// 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

要查看 KMS 密钥的所有AWS KMS授权的详细信息，请使用 get-KMS cmdlet GrantList。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

停用授予

要取消对 KMS 密钥的授权，请使用RetireGrant操作。在使用完授予后，您应停用它，以将其清除。

要停用授权，请提供授权令牌，或同时提供授权 ID 和 KMS 密钥 ID。对于此操作，KMS 密钥 ID 必须是 KMS 密钥的 Amazon Resource Name (ARN)。CreateGrant操作返回授权令牌。授权 ID 由 CreateGrant 和ListGrants操作返回。

RetireGrant 不返回响应。要验证其是否有效，请使用该ListGrants操作。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 retireGrant 方法。

```
// Retire a grant
//
String grantToken = Place your grant token here;

RetireGrantRequest req = new RetireGrantRequest().withGrantToken(grantToken);
kmsClient.retireGrant(req);
```

C#

有关详细信息，请参阅 AWS SDK for .NET 中的 RetireGrant 方法。

```
// Retire a grant
//
String grantToken = "Place your grant token here";

RetireGrantRequest retireGrantRequest = new RetireGrantRequest()
{
    GrantToken = grantToken
};
kmsClient.RetireGrant(retireGrantRequest);
```

Python

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 retire_grant 方法。

```
# Retire a grant

grant_token = Place your grant token here

response = kms_client.retire_grant(
    GrantToken=grant_token
)
```

Ruby

有关详细信息，请参阅 AWS SDK for Ruby 中的 retire_grant 实例方法。

```
# Retire a grant
```

```
grant_token = Place your grant token here

response = kmsClient.retire_grant({
  grant_token: grant_token
})
```

PHP

有关详细信息，请参阅 AWS SDK for PHP 中的 RetireGrant 方法。

```
// Retire a grant
//
$grantToken = 'Place your grant token here';

$result = $KmsClient->retireGrant([
    'GrantToken' => $grantToken,
]);
```

Node.js

有关详细信息，请参阅 Node.js 软件开发工具包 JavaScript 中的 AWSretiRegrant 属性。

```
// Retire a grant
//
const GrantToken = 'Place your grant token here';
kmsClient.retireGrant({ GrantToken }, (err, data) => {
  ...
});
```

PowerShell

要停用授权，请使用 Disable-KMSGrant cmdlet。要获取授予令牌，请使用 New-KMSGrant cmdlet。`GrantToken` 参数接受一个字符串，因此您不需要转换 Read-Host cmdlet 返回的输出。

```
# Retire a grant

$grantToken = Read-Host -Message Place your grant token here
Disable-KMSGrant -GrantToken $grantToken
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

撤销授予

要撤消对 KMS 密钥的授权，请使用RevokeGrant操作。您可以撤销授予，以显式拒绝依赖它的操作。

在需要客户端对象的语言中，这些示例使用您在 创建客户端 中创建的 AWS KMS 客户端对象。

Java

有关详细信息，请参阅 AWS SDK for Java API 参考中的 revokeGrant 方法。

```
// 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#

有关详细信息，请参阅 AWS SDK for .NET 中的 RevokeGrant 方法。

```
// 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);
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

Python

有关详细信息，请参阅 AWS SDK for Python (Boto3) 中的 revoke_grant 方法。

```
# 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

有关详细信息，请参阅 AWS SDK for Ruby 中的 revoke_grant 实例方法。

```
# 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

有关详细信息，请参阅 AWS SDK for PHP 中的 RevokeGrant 方法。

```
// 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

有关详细信息，请参阅 Node.js 软件开发工具包 JavaScript 中的 AWSrevokeGrant 属性。

```
// 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

要撤销授权，请使用 Revoke-KMSGrant cmdlet。

```
# 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
```

要使用 AWS KMS PowerShell cmdlet，请安装 aws.Tools。 KeyManagementService模块。有关更多信息，请参阅 AWS Tools for Windows PowerShell 用户指南。

测试您的 AWS KMS API 调用

要使用 AWS KMS，您必须拥有 AWS 可以用来验证您的 API 请求的凭证。此凭证必须包括访问 KMS 密钥和别名的权限。权限由密钥政策、IAM policy、授权和跨账户存取控制决定。除了控制对 KMS 密钥的访问外，您还可以控制对 CloudHSM 和自定义密钥存储的访问权限。

您可以指定 DryRun API 参数来确认您具有使用 AWS KMS 密钥的所需权限。您还可以使用 DryRun 来验证 AWS KMS API 调用中的请求参数指定是否正确。

主题

DryRun 参数是什么？

DryRun 是一个可选的 API 参数，您可以指定该参数来验证 AWS KMS API 调用是否成功。在实际调用 AWS KMS 之前，请使用 DryRun 测试您的 API 调用。您可以验证如下内容。

- 您具有使用 AWS KMS 密钥的所需权限。
- 您已正确指定调用中的参数。

AWS KMS 支持在某些 API 操作中使用 DryRun 参数：

- CreateGrant
- Decrypt
- Encrypt
- GenerateDataKey
- GenerateDataKeyPair
- GenerateDataKeyPairWithoutPlaintext
- GenerateDataKeyWithoutPlaintext
- GenerateMac

- ReEncrypt
- RetireGrant
- RevokeGrant
- Sign
- 验证
- VerifyMac

使用 DryRun 参数将产生费用，并将按标准 API 请求计费。有关 AWS KMS 定价的更多信息，请参阅 AWS Key Management Service 定价。

使用 DryRun 参数的所有 API 请求都适用于 API 的请求限额，如果您超过 API 请求限额，则可能会导致节流异常。例如，无论使用 DryRun 还是不使用 DryRun 调用 Decrypt，都将计入相同的加密操作限额。请参阅限制请求 AWS KMS，了解更多信息。

对 AWS KMS API 操作的每次调用都被捕获为事件并记录在 AWS CloudTrail 日志中。任何指定DryRun参数的操作的输出都会出现在您的 CloudTrail 日志中。有关更多信息，请参阅 使用记录 AWS KMS API 调用 AWS CloudTrail。

使用 API DryRun 进行指定

要使用 DryRun，请在支持该参数的 AWS CLI 命令和 AWS KMS API 调用中指定 –dry-run 参数。当您这样做时，AWS KMS 将验证您的调用是否会成功。使用 DryRun 的 AWS KMS 调用将始终失败并返回一条消息，其中包含有关调用失败原因的信息。消息可能包括以下例外情况：

- DryRunOperationException - 如果 DryRun 未指定，则请求会成功。
- ValidationException - 请求因指定错误的 API 参数而失败。
- AccessDeniedException - 您无权在 KMS 资源上执行指定的 API 操作。

例如，以下命令使用该CreateGrant操作并创建授权，允许有权担任该keyUserRole角色的用户对指定的对称 KMS 密钥调用 Decry pt 操作。DryRun 参数已指定。

```
$  aws kms create-grant \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/keyUserRole \
    --operations Decrypt \
    --dry-run
```

AWS KMS 最终一致性

由于系统的分布式特性，AWS KMS API 遵循最终一致性模型。因此，对 AWS KMS 资源的更改可能不会立即对您运行的后续命令可见。

当您执行 AWS KMS API 调用时，可能会出现短暂的延迟，才能使更改在整个 AWS KMS 中可用。更改通常需要不到几秒钟的时间即可在整个系统中传播，但在某些情况下，可能需要几分钟。在这段时间内，您可能会遇到意外错误，例如 `NotFoundException` 或 `InvalidStateException`。例如，如果您在调用 `CreateKey` 后立即调用 `GetParametersForImport`，则 AWS KMS 可能会返回 `NotFoundException`。

我们建议您在 AWS KMS 客户端上配置重试策略，以便在短暂的等待时间后自动重试操作。有关更多信息，请参阅《AWS SDKs and Tools Reference Guide》中的 Retry behavior。

对于与授权相关的 API 调用，您可以使用授权令牌来避免任何潜在的延迟，并立即在授权中使用权限。有关更多信息，请参阅最终一致性（用于授权）。

参考信息

以下引用提供了有关使用和管理 KMS 密钥的有用信息。

- 密钥类型引用。列出支持每个 AWS KMS API 操作的 KMS 密钥类型。

  查找：我能否启用和禁用 RSA 签名 KMS 密钥？
- 密钥状态表。显示 KMS 密钥的密钥状态如何影响其在 AWS KMS API 操作中的使用。

  查找：我能否更改待删除的 KMS 密钥的别名？
- AWS KMS API 权限引用。提供有关各个 AWS KMS API 操作所需权限的信息。

  查找：我能否使用其他AWS账户中的密钥运行 GetKeyPolicy？ 我能否在 IAM policy 中允许 `kms:Decrypt` 权限？
  - ViaService 参考。列出支持 `kms:ViaService` 条件键的 AWS 服务。

    查找：我能否使用`kms:ViaService`条件密钥仅允许来自亚马逊的许可 ElastiCache？ Amazon Neptune 怎么样？
- AWS KMS 定价。列出并解释 KMS 密钥的价格。

  查找：使用我的非对称密钥如何收费？
- AWS KMS 请求配额。列出每个账户和区域中 AWS KMS API 请求的每秒配额。

  查找：我每秒可以运行多少 Decrypt 请求？ 在自定义密钥存储中的 KMS 密钥上，我可以运行多少个 Decrypt 请求？
- AWS KMS 资源配额。列出 AWS KMS 资源上的配额。

  查找：我可以在账户的各个区域拥有多少 KMS 密钥？ 在每个 KMS 密钥上我可以拥有多少个别名？
- 与 AWS KMS 集成的 AWS 服务。列出使用 KMS 密钥来保护其所创建、存储和管理的资源的 AWS 服务。

  查找：Amazon Connect 是否使用 KMS 密钥来保护我的 Connect 资源？

文档历史记录

本主题介绍了有关 AWS Key Management Service 开发人员指南的重要更新。

主题

最近的更新

下表介绍了自 2018 年 1 月起对此文档的一些重要更改。除了此处列出的主要更改以外，我们还会经常更新文档，以改进说明和示例以及处理您发送给我们的反馈意见。要获得有关重要更改的通知，请订阅 RSS 源。

您可能需要水平或垂直滚动才能查看此表中的所有数据。

变更	说明	日期
密钥轮换更新	增加了对自定义轮换周期的支持，包括自动按键轮换、按需密钥轮换以及对密钥材料轮换的可见性。	2024 年 4 月 12 日
托管式策略的更新	添加了新的权限`AWSKeyManagementServiceCustomKeyStoresServiceRolePolicy`，AWS KMS 允许监控包含您的 AWS CloudHSM 集群的 VPC 中的更改，以便在出现故障时 AWS KMS 可以提供清晰的错误消息。	2023 年 11 月 10 日
功能更新	添加了对 `DryRun` API 参数的支持。	2023 年 7 月 5 日

功能更新	增加了对导入所有类型密钥材料的支持，自定义 AWS KMS 密钥库除外。	2023 年 6 月 5 日
功能更新	Nitro En AWS KMS claves 的 API 更新	2023 年 3 月 10 日
功能更新	RSAES_PKCS1_V1_5 包装算法已被弃用。 AWS KMS 根据美国国家标准与技术研究院 (NIST) 的加密密钥管理指南，将在 2023 年 10 月 1 日RSAES_PKCS1_V1_5 之前终止所有支持。我们建议您立即开始使用不同的包装算法。	2023 年 2 月 28 日
功能更新	增加了对外部密钥存储的支持，该功能允许您使用外部的加密密钥来保护您的 AWS 资源。 AWS	2022 年 11 月 29 日
配额更改	将每个账户和地区的 AWS KMS keys 资源配额增加到 100,000 个 KMS 密钥。	2022 年 7 月 8 日
功能更新	在更多内容中增加了对 HMAC KMS 密钥的支持 AWS 区域	2022 年 7 月 8 日
新主题	在《 AWS KMS 开发者指南》的 “安全” 一章中添加了 AWS Key Management Service 主题中的弹性。	2022 年 6 月 14 日
新功能	增加了对生成和验证 HMAC 代码的 AWS KMS 密钥和 API 操作的支持。	2022 年 4 月 19 日

文档更改	将术语客户主密钥 (CMK) 替换为 AWS KMS key 和 KMS 密钥。	2021 年 8 月 30 日
新功能	添加了对多区域密钥的支持，这是一组具有相同密钥 ID 和密钥材料的不同区域中的可互操作 KMS 密钥。您可以使用多区域密钥加密一个区域中的数据，并解密不同区域中的数据。	2021 年 6 月 8 日
新功能	添加了对基于属性的访问控制 (ABAC) 的支持。您可以使用标签和别名来控制对您的 AWS KMS keys访问权限。	2020 年 12 月 17 日
新功能	增加了对 VPC 终端节点策略的支持。	2020 年 7 月 9 日
新增内容	解释的安全属性 AWS KMS。	2020 年 6 月 18 日
新功能	增加了对非对称 AWS KMS keys 和非对称数据密钥的支持。	2019 年 11 月 25 日
更新功能	您可以在 AWS KMS 控制台 AWS 托管式密钥 中查看的密钥策略。此功能过去仅限于客户托管密钥。	2019 年 11 月 15 日
新功能	说明如何在 TLS 中使用混合后量子密钥交换算法来调用 AWS KMS。	2019 年 11 月 4 日
配额更改	提升了管理 KMS 密钥的某些 API 的资源配额。	2019 年 9 月 18 日

配额更改	更改了 KMS 密钥、别名和每个 KMS 密钥的授权数的资源配额。	2019 年 3 月 27 日
配额更改	更改了使用自定义密钥存储中的 AWS KMS keys 的加密操作的每秒请求配额。	2019 年 3 月 7 日
新功能	说明如何创建和管理 AWS KMS 自定义密钥库。每个密钥库都由您拥有和控制的 AWS CloudHSM 集群提供支持。	2018 年 11 月 26 日
新控制台	说明如何使用独立于 IAM AWS KMS 控制台的新控制台。原始控制台及其使用说明将在短时间内保持可用状态，以便您有时间熟悉新控制台。	2018 年 11 月 7 日
配额更改	已更改共享请求配额以供使用 AWS KMS keys。	2018 年 8 月 21 日
新增内容	说明如何 AWS Secrets Manager 使用 AWS KMS密钥加密密钥中的密钥值。	2018 年 7 月 13 日
新增内容	介绍 DynamoDB 如何使用 AWS KMS AWS KMS keys 支持其服务器端加密选项。	2018 年 5 月 23 日
新功能	说明如何使用您的 VPC 中的私有终端节点直接连接 AWS KMS，而不是通过互联网进行连接。	2018 年 1 月 22 日

早期更新

下表描述了 2018 年之前对《 AWS Key Management Service 开发者指南》所做的重要更改。

您可能需要水平或垂直滚动才能查看此表中的所有数据。

更改	描述	日期
新增内容	添加了有关标记密钥的文档。	2017 年 2 月 15 日
新增内容	添加了有关 监控 AWS KMS keys 和 使用 Amazon 进行监控 CloudWatch 的文档。	2016 年 8 月 31 日
新增内容	添加了有关导入的密钥材料的文档。	2016 年 8 月 11 日
新增内容	添加了以下文档：IAM 策略、权限参考 和 条件键。	2016 年 7 月 5 日
更新	更新了 身份验证和访问控制 一章中的文档部分。	2016 年 7 月 5 日
更新	更新了配额页面，在其中说明新的默认配额。	2016 年 5 月 31 日
更新	更新了 配额 页面，在其中说明新的默认配额，并更新了授权令牌文档以提高清晰性和准确性。	2016 年 4 月 11 日
新增内容	添加了有关 允许多个 IAM 主体访问 KMS 密钥 和 使用 IP 地址条件 的文档。	2016 年 2 月 17 日
更新	更新了 中的关键政策 AWS KMS 和 更改密钥策略 页面以提高清晰性和准确性。	2016 年 2 月 17 日
更新	更新了 管理 密钥 主题页面以提高清晰性。	2016 年 1 月 5 日

更改	描述	日期
新增内容	添加了有关AWS CloudTrail 如何使用 AWS KMS的文档。	2015 年 11 月 18 日
新增内容	添加了有关 更改密钥策略 的说明。	2015 年 11 月 18 日
更新	更新了有关Amazon Relational Database Service (Amazon RDS) 如何使用 AWS KMS的文档。	2015 年 11 月 18 日
新增内容	添加了有关如何 WorkSpaces 使用 AWS KMS的文档。	2015 年 11 月 6 日
更新	更新了 中的关键政策 AWS KMS 页面以提高清晰性。	2015 年 10 月 22 日
新增内容	增加了有关 删除 AWS KMS keys 的文档，包括有关 创建警报 和 确定 KMS 密钥的过去使用情况 的支持文档。	2015 年 10 月 15 日
新增内容	添加了有关确定对 AWS KMS keys 的访问权限的文档。	2015 年 10 月 15 日
新增内容	添加了有关密 AWS KMS 钥的关键状态的文档。	2015 年 10 月 15 日
新增内容	添加了有关Amazon Simple Email Service (Amazon SES) 如何使用 AWS KMS的文档。	2015 年 10 月 1 日
更新	更新了 配额 页面，在其中解释新的请求配额。	2015 年 8 月 31 日

更改	描述	日期
新增内容	添加了有关使用费用的信息 AWS KMS。请参阅 AWS KMS 定价。	2015 年 8 月 14 日
新增内容	向中添加了请求配额 AWS KMS 配额。	2015 年 6 月 11 日
新增内容	添加了演示 `UpdateAlias` 操作用法的新 Java 代码示例。请参阅 更新别名。	2015 年 6 月 1 日
更新	将 AWS Key Management Service 区域表移至 AWS 一般参考。	2015 年 5 月 29 日
新增内容	添加了有关Amazon EMR 如何使用 AWS KMS的文档。	2015 年 1 月 28 日
新增内容	添加了有关亚马逊如何 WorkMail 使用 AWS KMS的文档。	2015 年 1 月 28 日
新增内容	添加了有关Amazon Relational Database Service (Amazon RDS) 如何使用 AWS KMS的文档。	2015 年 1 月 6 日
新增内容	添加了有关Amazon Elastic Transcoder 如何使用 AWS KMS的文档。	2014 年 11 月 24 日
新指南	介绍了 AWS Key Management Service 开发人员指南。	2014 年 11 月 12 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。