



AWS Key Management Service 最佳实践

AWS 规范性指导



AWS 规范性指导: AWS Key Management Service 最佳实践

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

简介	1
目标业务成果	1
关于 AWS KMS keys	2
管理密钥	3
选择管理模式	3
选择密钥类型	4
选择密钥库	5
删除和禁用 KMS 密钥	6
数据保护	7
加密	7
加密日志数据	8
默认加密	8
数据库加密	9
PCI DSS 数据加密	10
将 KMS 密钥与 Amazon EC2 Auto Scaling 一起使用	11
密钥轮换	11
对称密钥轮换	11
亚马逊 EBS 的密钥轮换	12
亚马逊 RDS 的密钥轮换	13
亚马逊 S3 的密钥轮换	13
使用进口材料旋转钥匙	14
使用 AWS Encryption SDK	14
身份和访问管理	15
密钥策略和 IAM policy	15
最低权限许可	17
基于角色的访问控制	18
基于属性的访问控制	19
加密上下文	19
排除权限故障	20
检测和监控	21
监控 AWS KMS 操作	21
监控密钥访问权限	22
监控加密设置	23
配置 CloudWatch 警报	24

自动回复	24
成本和账单	26
密钥存储成本	26
Amazon S3 存储桶密钥	26
缓存数据密钥	27
替代方案	27
管理日志成本	27
资源	28
AWS KMS 文档	28
工具	28
AWS 规范性指导	28
策略	28
指南	28
模式	28
贡献者	29
编写	29
正在审阅	29
技术写作	29
文档历史记录	30
.....	xxxi

AWS Key Management Service 最佳实践

亚马逊 Web Services ([贡献者](#))

2025 年 3 月 ([文档历史记录](#))

[AWS Key Management Service \(AWS KMS\)](#) 是一项托管服务，可让您轻松创建和控制用于保护数据的加密密钥。本指南描述了如何有效使用 AWS KMS 并提供了最佳实践。它可以帮助您比较配置选项并选择最适合您需求的设置。

本指南包含有关您的组织如何使用 AWS KMS 来保护敏感信息以及为多个用例实施签名的建议。它考虑了使用以下维度的当前建议：

- 管理密钥-管理和密钥存储选项的委派选项
- 数据保护 — 加密您自己的应用程序中的数据，而不是代表您 AWS 服务 进行加密
- 访问管理 — 使用 AWS KMS 密钥策略和 AWS Identity and Access Management (IAM) 策略实施基于角色的访问控制 (RBAC) 或基于属性的访问控制 (ABAC)。
- 多账户和多区域架构-针对大规模部署的建议。
- 账单和成本管理 — 了解您的成本和使用情况，并就降低成本的方法提出建议。
- Detective 控件 — 监控 KMS 密钥的状态、加密设置和加密数据。
- 事件响应-更正导致不遵守数据保护策略的错误配置。

目标业务成果

您的数据是企业的重要敏感资产。使用 AWS KMS，您可以管理用于保护和验证数据的加密密钥。您可以控制数据的使用方式、谁有权访问数据以及如何对其进行加密。本指南旨在帮助开发人员、系统管理员和安全专业人员实施加密最佳实践，以帮助您保护存储或传输的敏感数据 AWS 服务。通过理解和实施本指南中的建议，您可以提高整个 AWS 环境中的数据机密性和完整性。无论这些要求是在内部制定的，还是针对合规性或验证计划的特定要求，您都可以满足您的数据保护要求。有关 AWS KMS 如何帮助您保护 AWS 环境中数据的更多信息，请参阅 AWS KMS 文档中的[将 AWS KMS 加密与一起 AWS 服务使用](#)。

关于 AWS KMS keys

AWS Key Management Service (AWS KMS) 允许您创建可用于传递给服务的数据的加密密钥。主要资源类型是 KMS 密钥，其中有[三种类型](#)：

- 高级加密标准 (AES) 对称密钥 — 这些是在 AES 的 Galois 计数器模式 (GCM) 模式下使用的 256 位密钥。这些密钥为大小小于 4 KB 的数据提供经过身份验证的加密和解密。这是最常见的密钥类型。它用于保护其他数据密钥，例如您的应用程序中使用的数据密钥或代表 AWS 服务 您加密数据的密钥。
- RSA 或椭圆曲线非对称密钥 — 这些密钥有各种大小可供选择，并支持多种算法。根据算法的不同，它们可用于加密和解密以及签名和验证操作。
- 用于执行基于哈希的消息身份验证码 (HMAC) 操作的对称密钥-这些密钥是 256 位密钥，用于签名和验证操作。

无法以明文形式从服务中导出 KMS 密钥。它们由服务使用的硬件安全模块 (HSMs) 生成，并且只能在其中使用。这是防止密钥泄露的基本安全属性。AWS KMS 在中国（北京）和中国（宁夏）地区，HSMs 它们已获得OSCCA [认证](#)。在所有其他地区，中 HSMs 使用的内容 AWS KMS 均在 [NIST 的 FIPS 140 计划](#)下进行安全级别为 3 的验证。有关中有助于保护密钥 AWS KMS 的设计和控件的更多信息，请参阅[AWS Key Management Service 加密详细信息](#)。

您可以使用各种加密 APIs 方法向提交数据，以便使用 KMS 密钥执行加密、解密、签名或验证操作。AWS KMS 您也可以选择让 KMS 密钥充当密钥加密密钥，以保护称为数据密钥的密钥类型。可以从导出数据密钥 AWS KMS 以在本地应用程序中使用 AWS 服务，也可以导出代表您保护数据的应用程序。数据密钥的使用在所有密钥管理系统中都很常见，通常被称为[信封加密](#)。信封加密允许在处理您的敏感数据的远程系统上使用数据密钥，而不必将您的敏感数据直接发送到 KMS 密钥下 AWS KMS 进行加密。

有关更多信息 [AWS KMS keys](#)，请参阅 AWS KMS 文档中的[AWS KMS 密码学基础知识](#)。

的密钥管理最佳实践 AWS KMS

使用 AWS Key Management Service (AWS KMS) 时，必须做出一些基本的设计决策。其中包括使用集中式还是分散式模式进行密钥管理和访问、要使用的密钥类型以及要使用的密钥存储类型。以下各节可帮助您做出适合您的组织和用例的决策。本节最后介绍禁用和删除 KMS 密钥的重要注意事项，包括为帮助保护数据和密钥而应采取的措施。

本节包含以下主题：

- [选择集中式或分散式模式](#)
- [选择客户托管密钥、AWS 托管密钥或 AWS 自有密钥](#)
- [选择密 AWS KMS 钥库](#)
- [删除和禁用 KMS 密钥](#)

选择集中式或分散式模式

AWS 建议您在多帐户 AWS 账户，并将这些帐户作为单个组织进行管理[AWS Organizations](#)。在多帐户环境中，有两种 AWS KMS keys 主要的管理方法。

第一种方法是去中心化方法，即在使用这些密钥的每个帐户中创建密钥。将 KMS 密钥存储在与其保护的资源相同的帐户中时，可以更轻松地将权限委托给了解其 AWS 委托人和密钥访问要求的本地管理员。您可以仅使用密钥[策略来授权密钥](#)的使用，也可以在 AWS Identity and Access Management (IAM) 中将密钥策略和[基于身份的策略](#)结合使用。

第二种方法是集中式方法，即在一个或几个指定的密钥中维护 KMS 密钥 AWS 账户。您允许其他账户仅使用密钥进行加密操作。您可以通过集中式账户管理密钥、密钥的生命周期和权限。您 AWS 账户允许其他人使用密钥，但不允许其他权限。外部账户无法管理有关密钥生命周期或访问权限的任何内容。这种集中式模式可以帮助最大限度地降低被授权的管理员或用户意外删除密钥或权限升级的风险。

您选择的选项取决于几个因素。选择方法时，请考虑以下几点：

1. 您是否有自动或手动配置密钥和资源访问权限的流程？这包括部署管道和基础设施即代码 (IaC) 模板等资源。这些工具可以帮助您部署和管理多个资源（例如 KMS 密钥、密钥策略、IAM 角色和 IAM 策略）AWS 账户。如果您没有这些部署工具，那么集中式密钥管理方法对您的企业来说可能更易于管理。
2. 您是否可以管理所有 AWS 账户 包含使用 KMS 密钥的资源的资源？如果是这样，集中式模式可以简化管理，无需切换 AWS 账户 到管理密钥。但请注意，仍然必须按账户管理 IAM 角色和用户使用密钥的权限。

3. 您是否需要向拥有自己 AWS 账户 和资源的客户或合作伙伴提供使用您的 KMS 密钥的权限？对于这些密钥，集中式方法可以减轻客户和合作伙伴的管理负担。
4. 您是否有通过集中访问或本地访问方法更好地解决的 AWS 资源访问权限要求？例如，如果不同的应用程序或业务部门负责管理其自身数据的安全性，则最好采用分散的密钥管理方法。
5. 您是否超过了服务[资源配额](#) AWS KMS？由于这些配额是按比例设置的 AWS 账户，因此分散式模型会将负载分配给各个账户，从而有效地乘以服务配额。

Note

在考虑[请求配额](#)时，密钥的管理模式无关紧要，因为这些配额适用于针对密钥提出请求的账户委托人，而不是拥有或管理密钥的账户。

一般而言，我们建议您从去中心化方法开始，除非您可以明确表示需要集中式 KMS 密钥模型。

选择客户托管密钥、AWS 托管密钥或 AWS 自有密钥

您创建和管理的、用于自己的加密应用程序的 KMS 密钥称为客户托管密钥。AWS 服务 可以使用客户管理的密钥来加密服务代表您存储的数据。如果您想完全控制密钥的生命周期和使用情况，建议使用客户托管密钥。账户中拥有客户托管密钥将按月收费。此外，使用或管理密钥的请求会产生使用成本。有关更多信息，请参阅[AWS KMS 定价](#)。

如果您想对数据进行加密，但又不想承担管理密钥的开销或成本，则可以使用 AWS 托管密钥。AWS 服务 这种类型的密钥存在于您的账户中，但只能在某些情况下使用。它只能在您正在操作的 AWS 服务 上下文中使用，并且只能由包含密钥的账户中的委托人使用。您无法对这些密钥的生命周期或权限进行任何管理。有些 AWS 服务 使用 AWS 托管密钥。AWS 托管密钥别名的格式为 `aws/<service code>`。例如，`aws/ebs` 密钥只能用于加密与密钥相同的账户中的亚马逊弹性区块存储 (Amazon EBS) 卷，并且只能由该账户中的 IAM 委托人使用。AWS 托管密钥只能由该账户中的用户以及该账户中的资源使用。您不能与其他账户共享使用 AWS 托管密钥加密的资源。如果这是您的用例的限制，我们建议您改用客户托管密钥；您可以与任何其他账户共享该密钥的使用。您无需为账户中存在 AWS 托管密钥而付费，但分配给该密钥的使用将 AWS 服务 向您收取任何使用此类密钥的费用。

AWS 托管密钥是一种传统密钥类型，自 2021 年起不再 AWS 服务 为新密钥创建。取而代之的是，新的（和传统 AWS 服务 的）默认使用 AWS 自有密钥来加密您的数据。AWS 拥有的密钥是 AWS 服务 拥有并管理的 KMS 密钥的集合，用于多个密钥 AWS 账户。尽管这些密钥不在您的账户中 AWS 账户，但 AWS 服务 可以使用这些密钥来保护您账户中的资源。

我们建议您在精细控制最重要的时候使用客户托管的密钥，并在最重要的便利性时使用 AWS 自有密钥。

下表描述了每种密钥类型之间的密钥策略、日志记录、管理和定价差异。有关密钥类型的更多信息，请参阅[AWS KMS 概念](#)。

考虑因素	客户自主管理型密钥	AWS 托管密钥	AWS 拥有的密钥
密钥策略	完全由客户控制	由服务控制；客户可以查看	独家控制，只能由加密您的数据 AWS 服务的人查看
日志记录	AWS CloudTrail 客户跟踪或事件数据存储	CloudTrail 客户跟踪或事件数据存储	客户无法查看
生命周期管理	客户管理轮换、删除和 AWS 区域	AWS 服务 管理轮换（每年）、删除和区域	AWS 服务 管理轮换（每年）、删除和区域
定价	密钥存在的月费（按小时按比例收费）；调用者需支付 API 使用费	密钥存在不收费；调用者需支付 API 使用费	不向客户收费

选择密 AWS KMS 钥库

密钥库是存储和使用加密密钥材料的安全位置。密钥库的行业最佳实践是使用一种名为硬件安全模块 (HSM) 的设备，该设备已通过 [NIST 联邦信息处理标准 \(FIPS\) 140 加密模块验证计划的验证](#)，安全级别为 3 级。还有其他计划可以支持用于处理付款的密钥存储。[AWS Payment Cryptography](#) 是一项可用于保护与支付工作负载相关的数据的服务。

AWS KMS 支持多种密钥存储类型，可在用于创建和管理加密密钥 AWS KMS 时帮助保护您的密钥材料。提供的所有密钥存储选项 AWS KMS 均在 FIPS 140 下持续通过安全等级 3 的验证。它们旨在防止任何人（包括 AWS 操作员）访问您的明文密钥或在未经您许可的情况下使用它们。有关可用密钥库类型的更多信息，请参阅 AWS KMS 文档中的[密钥存储](#)。

[AWS KMS 标准密钥存储库](#) 是大多数工作负载的最佳选择。如果您需要选择其他类型的密钥存储，请仔细考虑监管或其他要求（例如内部）是否要求做出此选择，并仔细权衡成本和收益。

删除和禁用 KMS 密钥

删除 KMS 密钥可能会产生重大影响。在删除不再打算使用的 KMS 密钥之前，请考虑将密钥状态设置为“已禁用”是否足够。当密钥被禁用时，它不能用于加密操作。它仍然存在于中 AWS，如果需要，您可以将来重新启用它。禁用的密钥将继续产生存储费用。我们建议您禁用密钥而不是将其删除，直到您确信密钥无法保护任何数据或数据密钥。

Important

删除密钥时必须谨慎计划。如果相应的密钥已被删除，则无法解密数据。AWS 已删除的密钥在被删除后无法恢复。与中的其他关键操作一样 AWS，您应应用一项政策，限制谁可以安排密钥删除，并要求使用多重身份验证 (MFA) 才能删除密钥。

为帮助防止意外删除密钥，AWS KMS 在DeleteKey调用执行后，默认的最短等待时间为七天，然后才会删除密钥。您可以[将等待时间的最大值设置为 30 天](#)。在等待期间，密钥仍以“待删除”状态存储。AWS KMS 它不能用于加密或解密操作。任何使用处于“待删除”状态的密钥进行加密或解密的尝试都将被记录到。AWS CloudTrail您可以在 CloudTrail 日志中为这些事件[设置 Amazon CloudWatch 警报](#)。如果您收到有关这些事件的警报，则可以根据需要选择取消删除过程。在等待期到期之前，您可以将密钥从“待删除”状态恢复，然后将其恢复为“已禁用”或“启用”状态。

要删除多区域密钥，必须先删除副本，然后再删除原始副本。有关更多信息，请参阅[删除多区域密钥](#)。

如果您使用的是包含已导入密钥材料的密钥，则可以立即删除导入的密钥材料。这与删除 KMS 密钥有多种不同之处。执行DeleteImportedKeyMaterial操作时，AWS KMS 会删除密钥材料，密钥状态更改为“待导入”。删除密钥材料后，密钥将立即无法使用。没有等待期。要再次启用密钥的使用，您需要再次导入相同的密钥材料。KMS 密钥删除的等待期也适用于已导入密钥材料的 KMS 密钥。

如果数据密钥受到 KMS 密钥的保护并且正在被积极使用 AWS 服务，则如果其关联的 KMS 密钥被禁用或其导入的密钥材料被删除，则这些密钥不会立即受到影响。例如，假设使用带有导入材料的密钥通过 [SSE- KMS](#) 加密对象。您正在将对象上传到亚马逊简单存储服务 (Amazon S3) 存储桶。在将对象上传到存储桶之前，您需要将材料导入到您的密钥中。上传对象后，您可以从该密钥中删除导入的密钥材料。该对象在存储桶中仍处于加密状态，但在已删除的密钥材料重新导入到密钥中之前，任何人都无法访问该对象。尽管此流程需要精确的自动化才能从密钥中导入和删除密钥材料，但它可以在环境中提供额外的控制级别。

AWS 提供了规范性指导，可帮助您监控和修复 (如有必要) KMS 密钥的计划删除。有关更多信息，请参阅[监控和修复 AWS KMS 密钥的计划删除](#)。

的数据保护最佳实践 AWS KMS

本节可帮助您选择用于数据保护的 AWS Key Management Service (AWS KMS) 密钥用法，例如每种数据类型使用哪些密钥。它还提供了 AWS KMS 与不同的使用方法的示例 AWS 服务。这些建议和示例可帮助您了解可能需要多少密钥以及哪些委托人需要权限才能使用这些密钥。

本节还讨论了密钥轮换。密钥轮换是将现有 KMS 密钥替换为新密钥或用新材料替换与现有 KMS 密钥关联的加密材料的做法。本指南提供了有关如何轮换常用的 KMS 密钥的示例和说明 AWS 服务。这些建议和示例旨在帮助您对密钥轮换策略做出明智的选择。

最后，本节就如何使用该工具提出了建议 AWS Encryption SDK，该工具用于在应用程序中实现客户端加密。本节包括您可以根据的功能集和功能做出的设计选择 AWS Encryption SDK。

本节讨论以下加密主题：

- [使用加密 AWS KMS](#)
- [密钥轮换 AWS KMS 和影响范围](#)
- [使用建议 AWS Encryption SDK](#)

使用加密 AWS KMS

加密是保护敏感信息的机密性和完整性的一般最佳做法。您应该使用现有的数据分类级别，并且每个级别至少有一个 AWS Key Management Service (AWS KMS) 密钥。例如，您可以为分类为“机密”的数据定义一个 KMS 密钥，一个用于仅限内部的数据和一个用于敏感数据的 KMS 密钥。这可以帮助您确保只有经过授权的用户才有权使用与每个保密级别关联的密钥。

Note

单个客户托管的 KMS 密钥可以在存储特定类别数据的任意组合 AWS 服务 或您自己的应用程序中使用。在多个工作负载中使用密钥的限制因素 AWS 服务 是控制一组用户对数据的访问所需的使用权限有多复杂。AWS KMS 密钥策略 JSON 文档必须小于 32 KB。如果此大小限制成为限制，请考虑使用[AWS KMS 授权](#)或创建多个密钥以最大限度地减少密钥策略文档的大小。

您还可以选择在单个密钥中分配用于数据分类的 KMS 密钥，而不是仅依靠数据分类对 KMS 密钥进行分区 AWS 服务。例如，Sensitive在亚马逊简单存储服务 (Amazon S3) Simple Service 中标记的所有数据都应使用名称类似的 KMS 密钥进行加密。S3-Sensitive您可以在定义的数据分类和 AWS 服务 /或应用程序中将数据进一步分发到多个 KMS 密钥中。例如，您可以删除特定时间段内的某些数据

集，在不同的时间段内删除其他数据集。您可以使用资源标签来帮助您识别和排序使用特定 KMS 密钥加密的数据。

如果您为 KMS 密钥选择去中心化管理模式，则应设置防护措施，确保创建具有给定分类的新资源，并使用具有正确权限的预期 KMS 密钥。有关如何使用自动化强制执行、检测和管理资源配置的更多信息，请参阅本指南的[检测和监控](#)部分。

本节讨论以下加密主题：

- [使用日志数据加密 AWS KMS](#)
- [默认加密](#)
- [使用数据库加密 AWS KMS](#)
- [PCI DSS 数据加密使用 AWS KMS](#)
- [将 KMS 密钥与 Amazon EC2 Auto Scaling 一起使用](#)

使用日志数据加密 AWS KMS

许多 AWS 服务公司（例如 [Amazon GuardDuty](#) 和 [AWS CloudTrail](#)）都提供了加密发送到 Amazon S3 的日志数据的选项。将[结果从导出 GuardDuty 到 Amazon S3](#)时，必须使用 KMS 密钥。我们建议您加密所有日志数据，并仅向授权委托人（例如安全团队、事件响应人员和审计员）授予解密访问权限。

AWS 安全参考架构建议创建一个[日志中心 AWS 账户](#)。这样做还可以减少密钥管理开销。例如，使用 CloudTrail，您可以创建[组织跟踪](#)或[事件数据存储](#)以记录整个组织中的事件。配置组织跟踪或事件数据存储时，可以在指定的日志账户中指定单个 Amazon S3 存储桶和 KMS 密钥。此配置适用于组织中的所有成员帐户。然后，所有账户都将其 CloudTrail 日志发送到日志账户中的 Amazon S3 存储桶，并使用指定的 KMS 密钥对日志数据进行加密。您需要更新此 KMS 密钥的密钥策略，以授予使用 CloudTrail 该密钥所需的权限。有关更多信息，请参阅 CloudTrail 文档[CloudTrail 中的为其配置 AWS KMS 密钥策略](#)。

为了帮助保护 GuardDuty 和 CloudTrail 日志，Amazon S3 存储桶和 KMS 密钥必须相同 AWS 区域。[AWS 安全参考架构](#)还提供了有关日志和多账户架构的指导。在汇总多个区域和账户的日志时，请查看 CloudTrail 文档中的[为组织创建跟踪](#)，以了解有关选择加入区域的更多信息，并确保您的集中式日志按设计运行。

默认加密

AWS 服务 存储或处理数据通常提供静态加密。此安全功能可在不使用数据时对其进行加密，从而帮助保护您的数据。授权用户仍然可以在需要时访问它。

实现和加密选项各不相同 AWS 服务。默认情况下，许多都提供加密。了解您使用的每项服务的加密工作原理非常重要。下面是一些示例：

- Amazon Elastic Block Store (Amazon EBS) — 默认启用加密后，所有新的亚马逊 EBS 卷和快照副本都将加密。AWS Identity and Access Management (IAM) 角色或用户无法启动具有未加密卷或不支持加密的卷的实例。此功能可确保存储在 Amazon EBS 卷上的所有数据都经过加密，从而有助于实现安全、合规和审计。有关此服务中加密的更多信息，请参阅 [Amazon EBS 文档中的 Amazon EBS 加密](#)。
- 亚马逊简单存储服务 (Amazon S3) Simple Service — 默认情况下，所有新对象均已加密。除非您指定不同的加密选项，否则 Amazon S3 会自动对每个新对象应用使用 Amazon S3 托管密钥 (SSE-S3) 的服务器端加密。通过在 API 调用中明确说明，IAM 委托人仍然可以将未加密的对象上传到 Amazon S3。在 Amazon S3 中，要强制执行 SSE-KMS 加密，您必须使用带有需要加密条件的存储桶策略。有关策略示例，请参阅 Amazon [S3 文档中的所有写入存储桶的对象都需要 SSE-KMS](#)。某些 Amazon S3 存储桶会接收和提供大量对象。如果使用 KMS 密钥对这些对象进行加密，则大量 Amazon S3 操作会导致对的大量 GenerateDataKey 和 Decrypt 调用 AWS KMS。这可能会增加您因 AWS KMS 使用而产生的费用。您可以配置 Amazon S3 [存储桶密钥](#)，这样可以显著降低 AWS KMS 成本。有关此服务中加密的更多信息，请参阅 Amazon S3 文档中的 [使用加密保护数据](#)。
- Amazon DynamoDB — DynamoDB 是一项完全托管的 NoSQL 数据库服务，它默认启用服务器端静态加密，您无法将其禁用。我们建议您使用客户托管密钥来加密您的 DynamoDB 表。这种方法可帮助您通过在 AWS KMS 密钥策略中定位特定的 IAM 用户和角色来实现最小权限，实现精细权限和职责分离。在为 DynamoDB 表配置加密设置时，您也可以选择 AWS 托管密钥或 AWS 自有密钥。对于需要高度保护的数据（其中数据只能以明文形式对客户端可见），请考虑使用 [AWS 数据库加密 SDK 的客户端加密](#)。有关此服务中加密的更多信息，请参阅 DynamoDB 文档中的 [数据保护](#)。

使用数据库加密 AWS KMS

您实施加密的级别会影响数据库的功能。以下是您必须考虑的权衡：

- 如果您仅使用 AWS KMS 加密，则 [支持表的存储将针对 DynamoDB 和亚马逊关系数据库服务 \(Amazon RDS\) 进行加密](#)。这意味着运行数据库的操作系统将存储的内容视为明文。所有数据库函数，包括索引生成和其他需要访问明文数据的高阶函数，都将继续按预期运行。
- 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。当您使用 Amazon RDS 创建加密数据库实例时，Amazon RDS 会代表您创建一个加密的 Amazon EBS 卷来存储数据库。存储在卷上的静态数据、数据库快照、自动备份和只读副本都使用您在创建数据库实例时指定的 KMS 密钥进行加密。

- Amazon Redshift 集成 AWS KMS 并创建了四层密钥层次结构，这些密钥用于通过数据级别对集群级别进行加密。启动集群时，您可以[选择使用 AWS KMS 加密](#)。在内存中打开（和解密）表时，只有 Amazon Redshift 应用程序和具有适当权限的用户才能看到明文。这与某些商业数据库中提供的透明或基于表的数据加密 (TDE) 功能大致相似。这意味着所有数据库函数，包括索引生成和其他需要访问明文数据的高阶函数，都将按预期运行。
- 通过[AWS 数据库加密 SDK（和类似工具）实现的客户端数据级加密](#)意味着操作系统和数据库都只能看到密文。只有当用户从安装了数据库加密 SDK 的客户端访问 AWS 数据库并且有权访问相关密钥时，他们才能查看明文。需要访问明文才能按预期工作的高阶数据库函数（例如索引生成）如果被指示对加密字段进行操作，则将无法运行。选择使用客户端加密时，请确保使用强大的加密机制，以帮助防止针对加密数据的常见攻击。这包括使用强大的加密算法和适当的技术（例如[盐](#)）来帮助缓解密文攻击。

我们建议对 AWS 数据库服务使用 AWS KMS 集成加密功能。对于处理敏感数据的工作负载，应考虑对敏感数据字段进行客户端加密。使用客户端加密时，应考虑对数据库访问的影响，例如 SQL 查询中的联接或索引创建。

PCI DSS 数据加密使用 AWS KMS

中的安全和质量控制 AWS KMS 已经过验证和认证，符合[支付卡行业数据安全标准 \(PCI DSS\)](#) 的要求。这意味着您可以使用 KMS 密钥加密主账号 (PAN) 数据。使用 KMS 密钥加密数据可以减轻管理加密库的部分负担。此外，无法从中导出 KMS 密钥 AWS KMS，这减少了人们对加密密钥以不安全的方式存储的担忧。

还有其他方法可以 AWS KMS 用来满足 PCI DSS 的要求。例如，如果您使用 AWS KMS 的是 Amazon S3，则可以将 PAN 数据存储在 Amazon S3 中，因为每项服务的访问控制机制彼此不同。

与往常一样，在审查您的合规要求时，请务必从经验丰富、合格且经过验证的各方那里获得建议。在设计直接使用密钥来保护 PCI DSS 范围内的信用卡交易数据的应用程序时，请注意[AWS KMS 请求配额](#)。

由于所有 AWS KMS 请求都已登录 AWS CloudTrail，因此您可以通过查看 CloudTrail 日志来审核密钥使用情况。但是，如果您使用 Amazon S3 存储桶密钥，则没有与每个 Amazon S3 操作相对应的条目。这是因为存储桶密钥会加密您用来加密 Amazon S3 中对象的数据密钥。虽然使用存储桶密钥并不能消除对的所有 API 调用 AWS KMS，但它会减少调用的数量。因此，Amazon S3 对象访问尝试与对的 API 调用之间不再存在 one-to-one 匹配 AWS KMS。

将 KMS 密钥与 Amazon EC2 Auto Scaling 一起使用

[Amazon EC2 Auto Scaling](#) 是一项推荐的服务，用于自动扩展您的亚马逊 EC2 实例。它可以帮助您确保有正确数量的可用实例来处理应用程序的负载。Amazon EC2 Auto Scaling 使用[服务相关角色](#)，该角色为服务提供适当的权限，并在您的账户中授权其活动。要将 KMS 密钥与 Amazon EC2 Auto Scaling 配合使用，您的密 AWS KMS 策略必须允许服务关联角色在某些 API 操作中使用您的 KMS 密钥 Decrypt，例如，这样自动化才能发挥作用。如果 AWS KMS 密钥策略未授权执行操作的 IAM 委托人执行操作，则该操作将被拒绝。有关如何正确应用密钥策略中的权限以允许访问的更多信息，请参阅 Amazon EC2 Auto Scaling 文档中的[Amazon EC2 Auto Scaling 中的数据保护](#)。

密钥轮换 AWS KMS 和影响范围

除非为了合规要求您轮换密钥，否则我们不建议 AWS Key Management Service (AWS KMS) 密钥轮换。例如，由于业务政策、合同规则或政府法规，您可能需要轮换 KMS 密钥。的设计 AWS KMS 大大减少了通常使用密钥轮换来缓解的风险类型。如果您必须轮换 KMS 密钥，我们建议您使用自动密钥轮换，并且仅在不支持自动密钥轮换时才使用手动密钥轮换。

本节讨论以下密钥轮换主题：

- [AWS KMS 对称密钥轮换](#)
- [亚马逊 EBS 卷的密钥轮换](#)
- [亚马逊 RDS 的密钥轮换](#)
- [Amazon S3 和同区域复制的密钥轮换](#)
- [使用导入的材料轮换 KMS 密钥](#)

AWS KMS 对称密钥轮换

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[自动密钥轮换](#)。对于客户托管的 KMS 密钥，自动轮换是可选的。每年 AWS KMS 轮换 AWS 托管 KMS 密钥的密钥材料。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。此外，当您使用解密对象时 AWS KMS，服务会确定用于解密操作的正确支持材料；无需提供其他输入参数。

由于 AWS KMS 保留了加密密钥材料的先前版本，并且您可以使用该材料来解密数据，因此密钥轮换不会提供任何额外的安全优势。如果您在监管或其他要求要求的环境中操作工作负载，则密钥轮换机制可以更轻松地轮换密钥。

亚马逊 EBS 卷的密钥轮换

您可以使用以下方法之一轮换亚马逊 Elastic Block Store (Amazon EBS) 数据密钥。方法取决于您的工作流程、部署方法和应用程序架构。从托管密钥更改为客户 AWS 托管密钥时，您可能需要这样做。

使用操作系统工具将数据从一个卷复制到另一个卷

1. 创建新的 KMS 密钥。有关说明，请参阅[创建 KMS 密钥](#)。
2. 创建一个大小与原始卷相同或大于原始卷的新 Amazon EBS 卷。要进行加密，请指定您创建的 KMS 密钥。有关说明，请参阅[创建 Amazon EBS 卷](#)。
3. 将新卷挂载到与原始卷相同的实例或容器上。有关说明，请参阅[将 Amazon EBS 卷附加到亚马逊 EC2 实例](#)。
4. 使用您首选的操作系统工具，将数据从现有卷复制到新卷。
5. 同步完成后，在预先安排的维护时段内，停止流向实例的流量。有关说明，请参阅[手动停止和启动您的实例](#)。
6. 卸载原始卷。有关说明，请参阅[将 Amazon EBS 卷与亚马逊 EC2 实例分离](#)。
7. 将新卷装载到原始装入点。
8. 验证新卷是否运行正常。
9. 删除原始卷。有关说明，请参阅[删除 Amazon EBS 卷](#)。

使用 Amazon EBS 快照将数据从一个卷复制到另一个卷

1. 创建新的 KMS 密钥。有关说明，请参阅[创建 KMS 密钥](#)。
2. 创建原始卷的 Amazon EBS 快照。有关说明，请参阅[创建 Amazon EBS 快照](#)。
3. 从快照创建一个新卷。要进行加密，请指定您创建的新 KMS 密钥。有关说明，请参阅[创建 Amazon EBS 卷](#)。

Note

根据您的工作负载，您可能需要使用 [Amazon EBS 快速快照还原](#) 来最大限度地减少卷上的初始延迟。

4. 创建一个新的 Amazon EC2 实例。有关说明，请参阅[启动 Amazon EC2 实例](#)。
5. 将您创建的卷附加到 Amazon EC2 实例。有关说明，请参阅[将 Amazon EBS 卷附加到亚马逊 EC2 实例](#)。

6. 将新实例轮换到生产环境中。
7. 将原始实例退出生产环境并将其删除。有关说明，请参阅[删除 Amazon EBS 卷](#)。

Note

可以复制快照并修改用于目标副本的加密密钥。在复制快照并使用首选 KMS 密钥对其进行加密后，您还可以使用快照创建 Amazon 系统映像 (AMI)。有关更多信息，请参阅[亚马逊 EC2 文档中的亚马逊 EBS 加密](#)。

亚马逊 RDS 的密钥轮换

对于某些服务，例如亚马逊关系数据库服务 (Amazon RDS)，数据加密是在服务中进行的，由提供 AWS KMS。按照以下说明轮换 Amazon RDS 数据库实例的密钥。

轮换 Amazon RDS 数据库的 KMS 密钥

1. 创建原始加密数据库的快照。有关说明，请参阅 Amazon RDS 文档中的[管理手动备份](#)。
2. 将快照复制到新快照。要进行加密，请指定新的 KMS 密钥。有关说明，请参阅[复制 Amazon RDS 的数据库快照](#)。
3. 使用新快照创建新的 Amazon RDS 集群。有关说明，请参阅 Amazon RDS 文档中的[恢复到数据库实例](#)。默认情况下，集群使用新的 KMS 密钥。
4. 验证新数据库及其中的数据运行情况。
5. 将新数据库转入生产环境。
6. 将旧数据库从生产环境中淘汰出来并将其删除。有关说明，请参阅[删除数据库实例](#)。

Amazon S3 和同区域复制的密钥轮换

对于亚马逊简单存储服务 (Amazon S3) Simple Service，要更改对象的加密密钥，您需要读取和重写该对象。重写对象时，您可以在写入操作中明确指定新的加密密钥。要对许多对象执行此操作，您可以使用[Amazon S3 批量操作](#)。在作业设置中，为复制操作指定新的加密设置。例如，您可以选择 SSE-KMS 并输入 keyID。

或者，您可以使用[Amazon S3 同区域复制 \(SSR\)](#)。SSR 可以对传输中的对象进行重新加密。

使用导入的材料轮换 KMS 密钥

AWS KMS 不会恢复或轮换您[导入的密钥材料](#)。要使用导入的密钥材料轮换 KMS 密钥，必须[手动轮换密钥](#)。

使用建议 AWS Encryption SDK

[AWS Encryption SDK](#)是在应用程序中实现客户端加密的强大工具。库可用于 Java、JavaScript、C、Python 和其他编程语言。它与 AWS Key Management Service (AWS KMS) 集成。您也可以将其用作独立的 SDK，而无需引用 KMS 密钥。

使用此工具的建议做法包括仔细考虑应用程序的要求。在这些要求与某些配置可能引入的风险之间取得平衡，例如在应用程序中引入密钥缓存。有关数据密钥缓存的更多信息，请参阅 AWS Encryption SDK 文档中的[数据密钥缓存](#)。

在决定是否使用时，请考虑以下问题 AWS Encryption SDK：

- 是否存在客户端加密要求，而服务器端加密无法通过与集成的服务来满足？AWS KMS
- 你能否充分保护用于在客户端加密数据的密钥，你将如何做到这一点？
- 还有其他 fit-for-purpose加密库可能更适合你的用例吗？考虑其他 AWS 产品，例如 [Amazon S3 客户端加密](#)和[AWS 数据库加密软件开发工具包](#)。

要了解有关为您的用例选择合适服务的更多信息，请参阅 [AWS Crypto Tools 文档](#)。

的身份和访问管理最佳实践 AWS KMS

要使用 AWS Key Management Service (AWS KMS)，您必须拥有 AWS 可用于对您的请求进行身份验证和授权的证书。除非明确提供了 KMS 密钥的权限，否则任何 AWS 委托人均无权访问 KMS 密钥，并且从不被拒绝。没有使用或管理 KMS 密钥的隐式或自动权限。本节中的主题定义了安全最佳实践，以帮助您确定应使用哪些 AWS KMS 访问管理控制来保护基础架构。

本节讨论以下身份和访问管理主题：

- [AWS KMS 密钥策略和 IAM 策略](#)
- [的最低权限权限 AWS KMS](#)
- [基于角色的访问控制 AWS KMS](#)
- [基于属性的访问控制 AWS KMS](#)
- [的加密上下文 AWS KMS](#)
- [AWS KMS 权限疑难解答](#)

AWS KMS 密钥策略和 IAM 策略

管理 AWS KMS 资源访问权限的主要方法是使用策略。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 AWS Identity and Access Management (IAM) 身份（用户、用户组或角色）的策略称为[基于身份的策略](#)。附加到资源的 IAM 策略称为[基于资源的策略](#)。AWS KMS KMS 密钥的资源策略称为[密钥策略](#)。除了 IAM 策略和 AWS KMS 密钥策略外，还 AWS KMS 支持[授权](#)。授权提供了一种灵活而强大的权限委托方式。您可以使用授权向您 AWS 账户 或其他的 IAM 委托人发放有时限的 KMS 密钥访问权限。AWS 账户

所有 KMS 密钥都具有密钥策略。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，具体取决于您是使用 AWS KMS 控制台还是使用 AWS KMS API 创建密钥。我们建议您编辑默认密钥策略，使其符合贵组织对[最低权限](#)的要求。这也应与您将 IAM 策略与关键策略结合使用的策略保持一致。有关将 IAM 策略与一起使用的更多建议 AWS KMS，请参阅 AWS KMS 文档[中的 IAM 策略最佳实践](#)。

您可以使用密钥策略将 IAM 委托人的授权委托给基于身份的策略。您还可以将密钥策略与基于身份的策略结合使用来完善授权。无论哪种情况，均由密钥策略和基于身份的策略决定访问权限，以及任何其他适用于访问范围的适用策略，例如[服务控制策略 \(SCPs\)](#)、[资源控制策略 \(RCPs\)](#) 或[权限边界](#)。如果委托人与 KMS 密钥位于不同的账户中，则基本上只支持加密和授权操作。有关这种跨账户场景的更多信息，请参阅 AWS KMS 文档[中的允许其他账户中的用户使用 KMS 密钥](#)。

您必须将基于 IAM 身份的策略与密钥策略结合使用，以控制对您的 KMS 密钥的访问。授权也可以与这些策略结合使用，以控制对 KMS 密钥的访问权限。要使用基于身份的策略来控制对 KMS 密钥的访问，密钥策略必须允许账户使用基于身份的策略。您可以指定[启用 IAM 策略的密钥策略语句](#)，也可以在密钥策略中明确[指定允许的主体](#)。

在编写策略时，请确保您有严格的控制措施，以限制谁可以执行以下操作：

- 更新、创建和删除 IAM 策略和 KMS 密钥策略
- 为用户、角色和群组附加和分离基于身份的策略
- 从 KMS AWS KMS 密钥中附加和分离密钥策略
- 为您的 KMS 密钥创建授权 — 无论您是仅通过密钥策略控制对 KMS 密钥的访问权限，还是将密钥策略与 IAM 策略结合使用，都应限制修改策略的能力。实施批准流程以更改任何现有政策。批准流程可以帮助防止以下情况：
 - 意外丢失 IAM 委托人权限 — 可以进行更改，从而阻止 IAM 委托人管理密钥或将其用于加密操作。在极端情况下，可以撤消所有用户的密钥管理权限。如果发生这种情况，您需要联系[AWS 支持](#)以重新获得对密钥的访问权限。
 - 对 KMS 密钥策略的未经批准的更改-如果未经授权的用户获得了对密钥策略的访问权限，他们可以对其进行修改以将权限委托给非预期用户 AWS 账户 或委托人。
 - 对 IAM 策略的未经批准的更改 — 如果未经授权的用户获得了一组有权管理群组成员资格的证书，则他们可以提升自己的权限并更改您的 IAM 策略、密钥策略、KMS 密钥配置或其他 AWS 资源配置。

仔细查看与被指定为您的 KMS 密钥管理员的 IAM 委托人关联的 IAM 角色和用户。这可以帮助防止未经授权的删除或更改。如果您需要更改有权访问您的 KMS 密钥的委托人，请确认新的管理员委托人已添加到所有必需的密钥策略中。在删除之前的管理委托人之前，请先测试他们的权限。我们强烈建议遵循所有 [IAM 安全最佳实践](#)，使用临时证书而不是长期证书。

如果您在创建策略时不知道委托人的姓名，或者需要访问权限的委托人经常发生变化，我们建议您通过授权来发放有时限的访问权限。[被授权者委托人](#)可以与 KMS 密钥位于同一个账户中，也可以位于不同的账户中。如果委托人和 KMS 密钥位于不同的账户中，则除了授权外，您还必须指定基于身份的策略。授权需要额外的管理，因为您必须调用 API 来创建授权，并在不再需要时停用或撤销授权。

任何 AWS 委托人（包括账户根用户或密钥创建者）都没有对 KMS 密钥的任何权限，除非在密钥策略、IAM 策略或授权中明确允许且未明确拒绝这些权限。推而广之，你应该考虑如果用户获得使用 KMS 密钥的意外访问权限会发生什么，以及会产生什么影响。要降低此类风险，请考虑以下几点：

- 您可以为不同类别的数据维护不同的 KMS 密钥。这可以帮助您分离密钥并维护更简洁的密钥策略，这些策略包含专门针对该数据类别的委托人访问权限的策略声明。这也意味着，如果无意中访问了相关的 IAM 证书，则与该访问相关的身份只能访问 IAM 策略中指定的密钥，并且前提是密钥策略允许访问该委托人。
- 您可以评估意外访问密钥的用户是否可以访问数据。例如，使用亚马逊简单存储服务 (Amazon S3) Simple Service，用户还必须具有访问亚马逊 S3 中加密对象的相应权限。或者，如果用户意外访问了使用 KMS 密钥加密的卷的 Amazon EC2 实例（使用 RDP 或 SSH），则该用户可以使用操作系统工具访问数据。

Note

AWS 服务 这种用途 AWS KMS 不会向用户公开密文（大多数当前的密码分析方法都需要访问密文）。此外，密文不能在 AWS 数据中心之外进行体检，因为根据 N SP8 IST 00-88 的要求，所有存储介质在停用时都会被物理销毁。

的最低权限权限 AWS KMS

由于您的 KMS 密钥可以保护敏感信息，因此我们建议遵循最低权限访问的原则。在定义密钥策略时，请委派执行任务所需的最低权限。仅当您计划使用其他基于身份的策略进一步限制权限时，才允许对 KMS 密钥策略执行所有操作 (kms:*)。如果您计划使用基于身份的策略管理权限，请限制谁能够创建 IAM 策略并将其附加到 IAM 委托人，并[监控策略的变化](#)。

如果您允许在密钥策略和基于身份的策略中执行所有操作 (kms:*)，则委托人同时拥有 KMS 密钥的管理权限和使用权限。作为安全最佳实践，我们建议仅将这些权限委托给特定的委托人。考虑一下如何向负责管理您的密钥的委托人和将使用您的密钥的委托人分配权限。为此，您可以通过在密钥策略中明确命名委托人或限制基于身份的策略所关联的委托人来实现。您也可以使用[条件键](#)来限制权限。例如，如果发出 API 调用的委托人具有条件规则中指定的标签，则可以使用 aws: [PrincipalTag](#) 来允许所有操作。

要帮助了解中如何评估策略声明 AWS，请参阅 IAM 文档中的[策略评估逻辑](#)。我们建议您在撰写策略之前先阅读此主题，以帮助减少您的策略产生意外影响的可能性，例如向本不应拥有访问权限的委托人提供访问权限。

Tip

在非生产环境中测试应用程序时，请使用 [AWS Identity and Access Management Access Analyzer \(IAM Access Analyzer\)](#) 来帮助您在 IAM 策略中应用最低权限权限。

如果您使用 IAM 用户而不是 IAM 角色，我们强烈建议您使用[AWS 多因素身份验证 \(MFA\)](#) 来缓解长期证书的漏洞。您可使用 MFA 执行以下操作：

- 要求用户在执行特权操作（例如安排密钥删除）前先使用 MFA 验证其凭证。
- 将管理员账户密码和 MFA 设备的所有权分配给不同个人，进行授权拆分。

有关可帮助您配置最低权限权限的示例策略，请参阅文档[中的 IAM 策略示例](#)。AWS KMS

基于角色的访问控制 AWS KMS

基于角色的访问控制 (RBAC) 是一种授权策略，它仅为用户提供履行其工作职责所需的权限，仅此而已。这种方法可以帮助您实现最小权限原则。

AWS KMS 支持 RBAC。它允许您通过在密钥[策略中指定精细权限来控制对密钥](#)的访问。密钥政策指定授予密钥访问权限的资源、操作、效果、主体和可选条件。要在中实现 RBAC AWS KMS，我们建议将密钥用户和密钥管理员的权限分开。

对于密钥用户，仅分配用户所需的权限。使用以下问题来帮助您进一步完善权限：

- 哪些 IAM 委托人需要访问密钥？
- 每位主体需要使用密钥来执行哪些操作？例如，委托人是否只需要Encrypt和Sign权限？
- 委托人需要访问哪些资源？
- 这个实体是人类还是 AWS 服务？如果是服务，则可以使用 `kms: ViaService` 条件密钥将密钥的使用限制在特定服务范围内。

对于密钥管理员，仅分配管理员所需的权限。例如，管理员的权限可能会有所不同，具体取决于密钥是在测试环境还是生产环境中使用。如果您在某些非生产环境中使用限制较少的权限，请在策略发布到生产环境之前实施一个流程来对其进行测试。

有关可帮助您为关键用户和管理员配置基于角色的访问控制的策略示例，请参阅相关的 [RBAC](#)。AWS KMS

基于属性的访问控制 AWS KMS

[基于属性的访问控制 \(ABAC\)](#) 是一种基于属性定义权限的授权策略。与 RBAC 一样，它是一种可以帮助您实现最小权限原则的方法。

AWS KMS 支持 ABAC，允许您根据与目标资源关联的标签（例如 KMS 密钥）以及与进行 API 调用的委托人关联的标签来定义权限。在中 AWS KMS，您可以使用标签和别名来控制对客户托管密钥的访问权限。例如，您可以定义使用标签条件密钥的 IAM 策略，以便在委托人的标签与与 KMS 密钥关联的标签匹配时允许操作。有关教程，请参阅 AWS KMS 文档中的[基于标签定义访问 AWS 资源的权限](#)。

作为最佳实践，使用 ABAC 策略来简化 IAM 策略管理。借助 ABAC，管理员可以使用标签来允许访问新资源，而不必更新现有策略。ABAC 需要的策略更少，因为您不必为不同的工作职能创建不同的策略。有关更多信息，请参阅 IAM 文档中的[ABAC 与传统 RBAC 模型的比较](#)。

将最低权限权限的最佳实践应用于 ABAC 模型。仅向 IAM 委托人提供他们执行任务所需的权限。谨慎控制对标签的访问权限 APIs，这将允许用户修改角色和资源的标签。如果您使用密钥别名条件键来支持 ABAC AWS KMS，请确保您还有强大的控制来限制谁可以创建密钥和修改别名。

您还可以使用标签将特定密钥链接到业务类别，并验证给定操作是否使用了正确的密钥。例如，您可以使用 AWS CloudTrail 日志来验证用于执行特定 AWS KMS 操作的密钥是否与正在使用的资源属于相同的业务类别。

Warning

不要在标签键或标签值中包含机密或敏感信息。标签未加密。许多人都可以访问它们 AWS 服务，包括计费。

在实施 ABAC 访问控制方法之前，请考虑您使用的其他服务是否支持这种方法。有关确定哪些服务支持 ABAC 的帮助，请参阅 AWS 服务 IAM 文档中的[“与 IAM 配合使用”](#)。

有关为实现 ABAC AWS KMS 以及可以帮助您配置策略的条件密钥的更多信息，请参阅[ABAC](#) 的。AWS KMS

的加密上下文 AWS KMS

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。加密上下文是一组可选的非秘密密钥值对，可以包含有关数据的其他上下文信息。作为最佳实践，您可以在 Encrypt 操作中插入加密上下文，AWS KMS 以增强对的解密 API 调用的授权和可审计性。AWS KMS AWS KMS 使用加密

上下文作为额外的身份验证数据 (AAD) 来支持[经过身份验证的加密](#)。加密上下文以加密方式绑定到加密文字，以便需要使用相同的加密上下文解密数据。

加密上下文不是密钥，且没有加密。它以纯文本形式出现在 AWS CloudTrail 日志中，因此您可以使用它来识别和分类您的加密操作。由于加密上下文不是秘密的，因此您应该只允许授权委托人访问您的 CloudTrail 日志数据。

您还可以使用 `kms::context-key EncryptionContext` 和 `kms:条件EncryptionContextKeys` 密钥根据[加密上下文](#)控制对对称加密 KMS 密钥的访问权限。您也可以使用这些条件密钥来要求在加密操作中使用加密上下文。对于这些条件密钥，请查看有关使用 `ForAnyValue` 或 `ForAllValues` 设置运算符的指南，以确保您的策略反映了您的预期权限。

AWS KMS 权限疑难解答

在为 KMS 密钥编写访问控制策略时，请考虑 IAM 策略和密钥策略是如何协同工作的。委托人的有效权限是所有有效策略授予（但未明确拒绝）的权限。在账户内，KMS 密钥的权限可能会受基于 IAM 身份的策略、密钥策略、权限边界、服务控制策略或会话策略的影响。例如，如果您同时使用基于身份的策略和密钥策略来控制对 KMS 密钥的访问，则会评估与委托人和资源相关的所有策略，以确定委托人是否有权执行给定操作。有关更多信息，请参阅 IAM 文档中的[策略评估逻辑](#)。

有关详细信息和排除密钥访问故障的流程图，请参阅 AWS KMS 文档中的[密钥访问疑难解答](#)。

对拒绝访问错误消息进行故障排除

1. 确认基于 IAM 身份的策略和 KMS 密钥策略允许访问。
2. 确认 IAM 中的[权限边界](#)没有限制访问。
3. 确认中的[服务控制策略 \(SCP\)](#) 或[资源控制策略 \(RCP\)](#) AWS Organizations 未限制访问。
4. 如果您使用的是 VPC 终端节点，请确认[终端节点策略](#)是否正确。
5. 在基于身份的策略和密钥策略中，删除任何限制访问密钥的条件或资源引用。取消这些限制后，确认委托人可以成功调用之前失败的 API。如果成功，请逐一重新应用条件和资源引用，然后验证委托人是否仍具有访问权限。这可以帮助您确定导致错误的条件或资源参考。

有关更多信息，请参阅 IAM 文档中的[对拒绝访问错误消息进行故障排除](#)。

的检测和监控最佳实践 AWS KMS

检测和监控是了解 AWS Key Management Service (AWS KMS) 密钥的可用性、状态和使用情况的重要组成部分。监控有助于维护 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您的 KMS 密钥和 AWS KMS 操作的工具。本节介绍如何配置和使用这些工具来更好地了解您的环境并监控 KMS 密钥的使用情况。

本节讨论以下检测和监控主题：

- [使用监控 AWS KMS 操作 AWS CloudTrail](#)
- [使用 IAM 访问分析器监控 KMS 密钥的访问权限](#)
- [使用监视其他 AWS 服务 人的加密设置 AWS Config](#)
- [使用 Amazon CloudWatch 警报监控 KMS 密钥](#)
- [使用 Amazon 自动回复 EventBridge](#)

使用监控 AWS KMS 操作 AWS CloudTrail

AWS KMS 与[AWS CloudTrail](#)一项服务集成，该服务可以记录用户、角色和其他人的所有呼叫 AWS 服务。AWS KMS 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 APIs、AWS CloudFormation、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。它还会记录管理 KMS 密钥的操作，例如 CreateKey 和 PutKeyPolicy, and cryptographic operations, such as GenerateDataKey 和 Decrypt。它还会记录 AWS KMS 需要您的内部操作，例如 DeleteExpiredKeyMaterial、DeleteKeySynchronizeMultiRegionKey、和 RotateKey。

CloudTrail 在你创建 AWS 账户 时已在你上启用。默认情况下，[事件历史记录](#)提供过去 90 天中记录的管理事件 API 活动的可查看、可搜索、可下载且不可变的记录。AWS 区域要监控或审计 90 天后您的 KMS 密钥的使用情况，我们建议您[创建 CloudTrail 跟踪](#) AWS 账户。如果您在中创建了组织 AWS Organizations，则可以[创建组织跟踪](#)或[事件数据存档](#)，用于记录该组织 AWS 账户 中所有人的事件。

为您的账户或组织建立跟踪后，您可以使用其他 AWS 服务 来存储、分析并自动响应跟踪中记录的事件。例如，您可以执行以下操作：

- 您可以设置 Amazon CloudWatch 警报，通知您跟踪中的某些事件。有关更多信息，请参阅本指南中的[使用 Amazon CloudWatch 警报监控 KMS 密钥](#)。
- 您可以创建 Amazon EventBridge 规则，以便在跟踪中发生事件时自动执行操作。有关更多信息，请参阅本指南 EventBridge 中的[使用 Amazon 自动回复](#)。
- 您可以使用 Amazon Security Lake 收集和存储多个日志 AWS 服务，包括 CloudTrail。有关更多信息，请参阅 Amazon [安全湖文档 AWS 服务 中的从安全湖中收集数据](#)。
- 为了增强对运营活动的分析，您可以使用 Amazon Athena 查询 CloudTrail 日志。有关更多信息，请参阅 Amazon Athena 文档中的[查询 AWS CloudTrail 日志](#)。

有关使用监控 AWS KMS 操作的更多信息 CloudTrail，请参阅以下内容：

- [使用记录 AWS KMS API 调用 AWS CloudTrail](#)
- [AWS KMS 日志条目示例](#)
- [使用 Amazon 监控 KMS 密钥 EventBridge](#)
- [CloudTrail 与亚马逊集成 EventBridge](#)

使用 IAM 访问分析器监控 KMS 密钥的访问权限

[AWS Identity and Access Management Access Analyzer \(IAM Access Analyzer\)](#) 可帮助您识别组织中的资源以及与外部实体共享的账户（例如 KMS 密钥）。该服务可以帮助您识别对您的资源和数据的意外访问或过于宽泛的访问权限，这存在安全风险。IAM Access Analyzer 使用基于逻辑的推理来分析环境中基于资源的策略，从而识别与外部委托人共享的资源。AWS

您可以使用 IAM 访问分析器来识别哪些外部实体有权访问您的 KMS 密钥。启用 IAM Access Analyzer 时，您可以为整个组织或目标账户创建分析器。您选择的组织或账户被称为分析器的信任区域。分析器监视信任区域内支持的资源。委托人在信任区域内对资源的任何访问都被视为可信。

对于 KMS 密钥，IAM Access Analyzer 会分析[应用于密钥的密钥策略和授权](#)。它会生成密钥策略或授权是否允许外部实体访问密钥的结果。使用 IAM Access Analyzer 来确定外部实体是否有权访问您的 KMS 密钥，然后验证这些实体是否应该拥有访问权限。

有关使用 IAM 访问分析器监控 KMS 密钥访问的更多信息，请参阅以下内容：

- [使用 AWS Identity and Access Management Access Analyzer](#)
- [用于外部访问的 IAM 访问分析器资源类型](#)

- [IAM 访问分析器资源类型：AWS KMS keys](#)
- [外部访问和未使用访问权限的调查结果](#)

使用监视其他 AWS 服务 人的加密设置 AWS Config

[AWS Config](#) 提供了中 AWS 资源配置的详细视图 AWS 账户。您可以使用 AWS Config 来验证使用您的 KMS 密钥的用户是否已正确配置其加密设置。AWS 服务 例如，您可以使用[加密卷](#) AWS Config 规则来验证您的 Amazon Elastic Block Store (Amazon EBS) 卷是否已加密。

AWS Config 包括托管规则，可帮助您快速选择评估资源的规则。请查看 AWS Config 您的 AWS 区域，以确定该区域是否支持您需要的托管规则。可用的托管规则包括检查亚马逊关系数据库服务 (Amazon RDS) 快照的配置、CloudTrail 跟踪加密、亚马逊简单存储服务 (Amazon S3) 存储桶的默认加密、Amazon DynamoDB 表加密等。

您还可以创建自定义规则并应用业务逻辑来确定您的资源是否符合您的要求。许多托管规则的开源代码可在上的“[AWS Config 规则存储库](#)”中找到 GitHub。这些可以成为开发自己的自定义规则的有用起点。

当资源不符合规则时，您可以启动响应操作。AWS Config 包括[AWS Systems Manager 自动化](#)执行的补救措施。例如，如果您应用了[cloud-trail-encryption-enabled](#)规则并且规则返回了NON_COMPLIANT结果，则 AWS Config 可以启动自动化文档，通过为您加密 CloudTrail 日志来修复问题。

AWS Config 允许您在配置资源之前主动检查是否符合 AWS Config 规则。在[主动模式下](#)应用规则可以帮助您在创建或更新云资源之前对其进行评估。在部署管道中以主动模式应用规则可以让您在部署资源之前测试资源配置。

您也可以通过控制来实现 AWS Config 规则[AWS Security Hub CSPM](#)。Security Hub CSPM 提供了可以应用于自己的安全标准。AWS 账户这些标准可帮助您根据建议的做法评估您的环境。[AWS 基础安全最佳实践](#)标准包括[保护控制类别](#)中的控件，用于验证静态加密是否已配置以及 KMS 密钥策略是否遵循建议的实践。

有关使用 AWS Config 监控中的加密设置的更多信息 AWS 服务，请参阅以下内容：

- [AWS Config入门](#)
- [AWS Config 托管规则](#)
- [AWS Config 自定义规则](#)
- [使用修复不合规的资源 AWS Config](#)

使用 Amazon CloudWatch 警报监控 KMS 密钥

[Amazon](#) 会实时 CloudWatch 监控您的 AWS 资源和您运行 AWS 的应用程序。您可以使用 CloudWatch 来收集和跟踪指标，这些指标是您可以衡量的变量。

如果导入的密钥材料过期或密钥的删除是意外的，或者计划不当，则可能是灾难性事件。我们建议您配置 [CloudWatch 警报](#)，以便在这些事件发生之前提醒您注意这些事件。我们还建议您配置 AWS Identity and Access Management (IAM) 策略或 AWS Organizations [服务控制策略 \(SCPs\)](#)，以防止删除重要密钥。

CloudWatch 警报可帮助您采取纠正措施，例如取消密钥删除，或采取补救措施，例如重新导入已删除或过期的密钥材料。

使用 Amazon 自动回复 EventBridge

您还可以使用 [Amazon EventBridge](#) 将影响您的 KMS 密钥的重要事件通知您。EventBridge AWS 服务 是一种提供近乎实时的系统事件流，这些事件描述了 AWS 资源的变化。EventBridge 自动接收来自 CloudTrail 和 Security Hub CSPM 的事件。在中 EventBridge，您可以创建用于响应所记录的事件的规则 CloudTrail。

AWS KMS 事件包括以下内容：

- KMS 密钥中的密钥材料已自动轮换
- KMS 密钥中导入的密钥材料已过期
- 原定删除的 KMS 密钥已删除

这些事件可以在您的中启动其他操作 AWS 账户。这些操作与上一节中描述的 CloudWatch 警报不同，因为只有事件发生后才能对它们采取行动。例如，您可能想在删除特定密钥后删除与该密钥关联的资源，或者您可能想通知合规或审计团队该密钥已被删除。

您还可以筛选使用登录的任何其他 API 事件 EventBridge。CloudTrail 这意味着，如果与关键策略相关的 API 操作存在特定问题，则可以对其进行筛选。例如，您可以筛选出 EventBridge PutKeyPolicy API 操作。更广泛地说，您可以筛选以自动响应开头 Disable* 或 Delete* 启动自动响应的任何 API 操作。

使用 EventBridge，您可以监控（这是侦探控件），并对意外事件或选定事件进行调查和响应（响应控件）。例如，如果创建 IAM 用户或角色、创建 KMS 密钥或更改密钥策略，您可以提醒安全团队并采取具体措施。您可以创建筛选您指定的 API 操作 EventBridge 的事件规则，然后将目标与该规则相

关联。示例目标包括 AWS Lambda 函数、亚马逊简单通知服务 (Amazon SNS) Simple Notification 通知、亚马逊简单队列服务 (Amazon SQS) Simple Queue Service 队列等。有关向目标发送事件的更多信息，请参阅 [Amazon 中的事件总线目标 EventBridge](#)。

有关 AWS KMS 使用监控 EventBridge 和自动响应的更多信息，请参阅 AWS KMS 文档 EventBridge 中的使用 [Amazon 监控 KMS 密钥](#)。

的成本和账单管理最佳实践 AWS KMS

从广度和深度上讲，AWS 服务 您可以灵活地管理成本，同时满足业务需求。本节介绍了 AWS Key Management Service (AWS KMS) 中密钥存储的定价，并提供了降低成本的建议，例如通过密钥缓存。您还可以查看 KMS 密钥的使用情况，以确定是否还有其他降低成本的机会。

本节讨论以下成本和账单管理主题：

- [AWS KMS 密钥存储的定价](#)
- [采用默认加密功能的 Amazon S3 存储桶密钥](#)
- [使用缓存数据密钥 AWS Encryption SDK](#)
- [密钥缓存和 Amazon S3 存储桶密钥的替代方案](#)
- [管理 KMS 密钥使用的日志成本](#)

AWS KMS 密钥存储的定价

你 AWS KMS key 在其中创建的每一个都会 AWS KMS 产生冲锋。对称密钥、非对称密钥、HMAC 密钥、多区域密钥（每个主密钥和每个副本多区域密钥）、具有导入密钥材料的密钥以及密钥来源为其中一个 AWS CloudHSM 或外部密钥存储的 KMS 密钥的月度费用相同。

对于自动或按需轮换的 KMS 密钥，密钥的第一次和第二次轮换会增加额外的月度费用（按小时按比例分配）。第二次轮换后，该月的任何后续轮换均不计费。请查看[AWS KMS 定价](#)以获取最新的定价信息。

您可以使用[AWS Budgets](#)来配置使用预算。AWS Budgets 当您的账户内的支出超过特定阈值时，可以提醒您。对于与之相关的费用 AWS KMS，您可以[创建使用预算](#)，以便根据 KMS 密钥或请求提醒。这可以提高您对 AWS KMS 密钥存储和使用成本的可见性。

采用默认加密功能的 Amazon S3 存储桶密钥

在某些用例中，在 Amazon Simple Storage Service (Amazon S3) 中访问或生成大量对象的工作负载可能会 AWS KMS 向其生成大量请求，从而增加您的成本。配置 [Amazon S3 存储桶密钥](#) 可以帮助您将成本降低多达 99%。这是禁用加密的推荐替代方案，以帮助降低与之相关的成本 AWS KMS。

使用缓存数据密钥 AWS Encryption SDK

使用执行[AWS Encryption SDK](#)客户端加密时，[数据密钥缓存](#)可以帮助提高应用程序的性能，降低应用程序请求 AWS KMS 受[限](#)的风险，并帮助您降低成本。有关如何入门的更多信息，请参阅[如何使用数据密钥缓存](#)。

密钥缓存和 Amazon S3 存储桶密钥的替代方案

如果由于您的数据处理要求而无法选择密钥缓存，您也可以使用 AWS 管理控制台 或 Service AWS KMS [Quotas API 请求增加配额](#)。考虑一下您可能进行的 API 调用量。您进行的 API 调用次数是[AWS KMS 定价](#)的重要因素。如果您增加请求速率配额以扩展性能，则请求数量的增加会 AWS KMS 产生额外成本。

管理 KMS 密钥使用的日志成本

所有 AWS KMS API 调用都记录到 AWS CloudTrail。应用程序和服务可以生成大量 AWS KMS API 调用（例如用于加密操作，包括加密和解密）。如果没有可帮助您整理数据、调查趋势和搜索异常 API 活动的工具，就很难查看 CloudTrail 日志。[Amazon](#) Athena 提供预定义的数据结构，可帮助您快速设置日志表 CloudTrail 并开始分析日志数据。它对于事件响应期间的临时分析或进一步调查特别有用。有关更多信息，请参阅 Athena 文档中的[查询 AWS CloudTrail 日志](#)。

由于您按查询为 Athena 付费，因此您可以免费提前设置表格。数据定义语言语句不收取任何费用。当您应对事件时，这可以帮助你确保已经满足了许多先决条件。为了帮助您做好准备，最佳做法是在创建表之后编写查询，对其进行测试，并确保它们产生了您想要的结果。您可以将查询保存在 Athena 中以备将来使用。有关如何开始使用 Athena 的更多信息，[请参阅亚马逊 Athena 入门](#)。

[通过数据事件](#)，可以查看在资源上或资源内部执行的操作。这些也称为数据层面操作。示例包括 Amazon S3 PutObject 事件或 Lambda 函数操作 API 调用。数据事件通常是高容量活动，记录这些事件会产生费用。为了帮助控制记录到跟踪或事件数据存储中的数据事件量 CloudTrail，您可以通过配置高级事件选择器来限制要登录的数据事件 CloudTrail AWS KMS，从而优化日志记录以降低、和 Amazon S3 的成本。CloudTrail 有关更多信息，请参阅[如何使用高级事件选择器优化 AWS CloudTrail 成本](#)（AWS 博客文章）。

资源

AWS Key Management Service (AWS KMS) 文档

- [AWS KMS 开发人员指南](#)
- [AWS KMS API 参考](#)
- [AWS KMS 在 AWS CLI 参考文献中](#)

工具

- [AWS Encryption SDK](#)

AWS 规范性指导

策略

- [为静态数据创建加密策略](#)

指南

- [的加密最佳实践和功能 AWS 服务](#)
- [AWS 隐私参考架构 \(AWS PRA\)](#)

模式

- [自动加密 Amazon EBS 卷](#)
- [Automatically remediate unencrypted Amazon RDS DB instances and clusters](#)
- [监控并修复计划删除的 AWS KMS keys](#)

贡献者

编写

- Frank Phillis，高级 GTM 专家解决方案架构师，AWS
- Ken Beer AWS KMS，加密图书馆主任，AWS
- 迈克尔·米勒，高级解决方案架构师 AWS
- 杰里米·斯蒂格利茨，首席产品经理 AWS
- 首席解决方案架构师扎克·米勒 AWS
- Peter M. O'Donnell，首席解决方案架构师 AWS
- 帕特里克·帕尔默，首席解决方案架构师 AWS
- 首席解决方案架构师戴夫·沃克 AWS

正在审阅

- Manigandan Shri，高级交付顾问，AWS

技术写作

- Lilly AbouHarb，高级技术撰稿人，AWS
- Kimberly Garmoe，高级技术作家，AWS

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 [RSS 源](#)。

变更	说明	日期
初次发布	—	2025 年 3 月 24 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。