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

Table of Contents

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。
- D@@ etective 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。可以从中导出数据密钥 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

AWS 建议您在中使用多个帐户 AWS 账户 ，并将这些帐户作为单个组织进行管理AWS Organizations。在多账户环境中，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账户中创建密钥。将 KMS 密钥存储在与其保护的资源相同的账户中时，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. 您是否超过了的服务资源配额 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具体示例 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) S imple 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 D ynamoDB — 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，都将继续按预期运行。
- 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 钥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 R DS 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的运行情况。
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 (SRR)。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 策略的密钥政策语句，也可以在密钥政策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。在定义密钥政策时，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 k ms: 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储，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，因为只有在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。当你应对事件时，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

AWS 规范性指导词汇表

以下是 AWS 规范性指导提供的策略、指南和模式中的常用术语。若要推荐词条，请使用术语表末尾的提供反馈链接。

数字

7 R

将应用程序迁移到云中的 7 种常见迁移策略。这些策略以 Gartner 于 2011 年确定的 5 R 为基础，包括以下内容：

- 重构/重新架构：充分利用云原生功能来提高敏捷性、性能和可扩展性，以迁移应用程序并修改其架构。这通常涉及到移植操作系统和数据库。示例：将本地 Oracle 数据库迁移到 Amazon Aurora PostgreSQL 兼容版。
- 更换平台：将应用程序迁移到云中，并进行一定程度的优化，以利用云功能。示例：将本地 Oracle 数据库迁移到 AWS 云中的 Amazon Relational Database Service（Amazon RDS）for Oracle。
- 重新购买：转换到其他产品，通常是从传统许可转向 SaaS 模式。示例：将客户关系管理（CRM）系统迁移到 Salesforce.com。
- 重新托管（直接迁移）：将应用程序迁移到云中，无需进行任何更改即可利用云功能。示例：将本地 Oracle 数据库迁移到 AWS 云中 EC2 实例上的 Oracle。
- 重新放置（虚拟机监控器级直接迁移）：将基础设施迁移到云中，无需购买新硬件、重写应用程序或修改现有操作。您将服务器从本地平台迁移到同一平台的云服务中。示例：将Microsoft Hyper-V应用程序迁移到 AWS。
- 保留（重访）：将应用程序保留在源环境中。其中可能包括需要进行重大重构的应用程序，并且您希望将工作推迟到以后，以及您希望保留的遗留应用程序，因为迁移它们没有商业上的理由。
- 停用：停用或删除源环境中不再需要的应用程序。

A

ABAC

请参阅基于属性的访问控制。

抽象服务

请参阅托管服务。

ACID

请参阅原子性、一致性、隔离性、持久性。

主动-主动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步（通过使用双向复制工具或双写操作），两个数据库都在迁移期间处理来自连接应用程序的事务。这种方法支持小批量、可控的迁移，而不需要一次性割接。它比主动-被动迁移更灵活，但工作量更大。

主动-被动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步，但在将数据复制到目标数据库时，只有源数据库处理来自连接应用程序的事务。目标数据库在迁移期间不接受任何事务。

聚合函数

一种 SQL 函数，它对一组行进行操作并计算该组的单个返回值。聚合函数的示例包括 SUM 和 MAX。

AI

请参阅人工智能。

AIOps

请参阅人工智能运营。

匿名化

永久删除数据集中个人信息的过程。匿名化可以帮助保护个人隐私。匿名化数据不再被视为个人数据。

反模式

一种用于解决反复出现的问题的常用解决方案，而在这类问题中，此解决方案适得其反、无效或不如替代方案有效。

应用程序控制

一种安全方法，仅允许使用经批准的应用程序，以帮助保护系统免受恶意软件的侵害。

应用程序组合

有关组织使用的每个应用程序的详细信息的集合，包括构建和维护该应用程序的成本及其业务价值。这些信息是产品组合发现和分析过程的关键，有助于识别需要进行迁移、现代化和优化的应用程序并确定其优先级。

人工智能（AI）

计算机科学领域致力于使用计算技术执行通常与人类相关的认知功能，例如学习、解决问题和识别模式。有关更多信息，请参阅什么是人工智能？

人工智能操作 (AIOps)

使用机器学习技术解决运营问题、减少运营事故和人为干预以及提高服务质量的过程。有关如何在 AIOps AWS 迁移策略中使用的更多信息，请参阅操作集成指南。

非对称加密

一种加密算法，使用一对密钥，一个公钥用于加密，一个私钥用于解密。您可以共享公钥，因为它不用于解密，但对私钥的访问应受到严格限制。

原子性、一致性、隔离性、持久性（ACID）

一组软件属性，即使在出现错误、电源故障或其他问题的情况下，也能保证数据库的数据有效性和操作可靠性。

基于属性的访问权限控制（ABAC）

根据用户属性（如部门、工作角色和团队名称）创建精细访问权限的做法。有关更多信息，请参阅 AWS Identity and Access Management (I AM) 文档 AWS中的 AB AC。

权威数据来源

存储主要数据版本的位置，被认为是最可靠的信息源。您可以将数据从权威数据来源复制到其他位置，以便处理或修改数据，例如对数据进行匿名化、编辑或假名化。

可用区

中的一个不同位置 AWS 区域 ，不受其他可用区域故障的影响，并向同一区域中的其他可用区提供低成本、低延迟的网络连接。

AWS 云采用框架 (AWS CAF)

该框架包含指导方针和最佳实践 AWS ，可帮助组织制定高效且有效的计划，以成功迁移到云端。AWS CAF将指导分为六个重点领域，称为视角：业务、人员、治理、平台、安全和运营。业务、人员和治理角度侧重于业务技能和流程；平台、安全和运营角度侧重于技术技能和流程。例如，人

员角度针对的是负责人力资源（HR）、人员配置职能和人员管理的利益相关者。从这个角度来看，AWS CAF 为人员发展、培训和沟通提供了指导，以帮助组织为成功采用云做好准备。有关更多信息，请参阅 AWS CAF 网站和 AWS CAF 白皮书。

AWS 工作负载资格框架 (AWS WQF)

一种评估数据库迁移工作负载、推荐迁移策略和提供工作估算的工具。 AWS WQF 包含在 AWS Schema Conversion Tool (AWS SCT) 中。它用来分析数据库架构和代码对象、应用程序代码、依赖关系和性能特征，并提供评测报告。

B

恶意机器人

一种旨在扰乱或伤害个人或组织的机器人。

BCP

请参阅业务连续性计划。

行为图

一段时间内资源行为和交互的统一交互式视图。您可以使用 Amazon Detective 的行为图来检查失败的登录尝试、可疑的 API 调用和类似的操作。有关更多信息，请参阅 Detective 文档中的行为图中的数据。

大端序系统

一个先存储最高有效字节的系统。另请参阅字节顺序。

二进制分类

一种预测二进制结果（两个可能的类别之一）的过程。例如，您的 ML 模型可能需要预测诸如“该电子邮件是否为垃圾邮件？”或“这个产品是书还是汽车？”之类的问题

bloom 筛选条件

一种概率性、内存高效的数据结构，用于测试元素是否为集合的成员。

蓝/绿部署

一种部署策略，您可以创建两个独立但完全相同的环境。在一个环境中运行当前应用程序版本（蓝色），在另一个环境中运行新应用程序版本（绿色）。此策略可帮助您在影响最小的情况下快速回滚。

自动程序

一种通过互联网运行自动任务并模拟人类活动或交互的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的 Web 爬网程序。还有一些被称为恶意机器人的机器人，其目的是扰乱或伤害个人或组织。

僵尸网络

被恶意软件感染并受单方（称为僵尸网络控制者或僵尸网络操作者）控制的僵尸网络。僵尸网络是最著名的扩展机器人及其影响力的机制。

分支

代码存储库的一个包含区域。在存储库中创建的第一个分支是主分支。您可以从现有分支创建新分支，然后在新分支中开发功能或修复错误。为构建功能而创建的分支通常称为功能分支。当功能可以发布时，将功能分支合并回主分支。有关更多信息，请参阅关于分支（GitHub 文档）。

紧急（break-glass）访问

在特殊情况下，通过批准的流程，用户 AWS 账户 可以快速访问他们通常没有访问权限的内容。有关更多信息，请参阅 AWS Well-Architected Guidance 中的 Implement break-glass procedures 指示器。

棕地策略

您环境中的现有基础设施。在为系统架构采用棕地策略时，您需要围绕当前系统和基础设施的限制来设计架构。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

缓冲区缓存

存储最常访问的数据的内存区域。

业务能力

企业如何创造价值（例如，销售、客户服务或营销）。微服务架构和开发决策可以由业务能力驱动。有关更多信息，请参阅在 AWS上运行容器化微服务白皮书中的围绕业务能力进行组织部分。

业务连续性计划（BCP）

一项计划，旨在应对大规模迁移等破坏性事件对运营的潜在影响，并使企业能够快速恢复运营。

C

CAF

请参阅 AWS 云采用框架。

金丝雀部署

缓慢而渐进地向最终用户发布版本。当您确信无误后，即可部署新版本，并完全替换当前版本。

CCoE

请参阅云卓越中心。

CDC

请参阅更改数据捕获。

更改数据捕获（CDC）

跟踪数据来源（如数据库表）的更改并记录有关更改的元数据的过程。您可以将 CDC 用于各种目的，例如审计或复制目标系统中的更改以保持同步。

混沌工程

故意引入故障或破坏性事件来测试系统的韧性。您可以使用 AWS Fault Injection Service (AWS FIS) 来执行实验，对您的 AWS 工作负载施加压力并评估其响应。

CI/CD

请参阅持续集成和持续交付。

分类

一种有助于生成预测的分类流程。分类问题的 ML 模型预测离散值。离散值始终彼此不同。例如，一个模型可能需要评估图像中是否有汽车。

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心 (CCoE)

一个多学科团队，负责推动整个组织的云采用工作，包括开发云最佳实践、调动资源、制定迁移时间表、领导组织完成大规模转型。有关更多信息，请参阅 AWS 云 企业战略博客上的 CCoE 帖子。

云计算

通常用于远程数据存储和 IoT 设备管理的云技术。云计算通常连接到边缘计算技术。

云运营模型

在 IT 组织中，一种用于构建、完善和优化一个或多个云环境的运营模型。有关更多信息，请参阅构建您的云运营模型。

云采用阶段

组织迁移到 AWS 云中时通常会经历四个阶段：

- 项目 - 出于概念验证和学习目的，开展一些与云相关的项目
- 基础 — 进行基础投资以扩大云采用率（例如，创建着陆区、定义 CCo E、建立运营模型）
- 迁移 - 迁移单个应用程序
- 重塑 - 优化产品和服务，在云中创新

Stephen Orban在 AWS 云 企业战略博客的博客文章《云优先之旅和采用阶段》中定义了这些阶段。有关它们与 AWS 迁移策略的关系的信息，请参阅迁移准备指南。

CMDB

请参阅配置管理数据库。

代码存储库

通过版本控制过程存储和更新源代码和其他资产（如文档、示例和脚本）的位置。常见的云存储库包括 GitHub 或 Bitbucket Cloud。每个版本的代码都称为一个分支。在微服务结构中，每个存储库都专门用于一个功能。单个 CI/CD 管线可以使用多个存储库。

冷缓存

一种空的、填充不足或包含过时或不相关数据的缓冲区缓存。这会影响性能，因为数据库实例必须从主内存或磁盘读取，这比从缓冲区缓存读取要慢。

冷数据

很少访问的数据，且通常是历史数据。查询此类数据时，通常可以接受慢速查询。将这些数据转移到性能较低且成本更低的存储层或类别可以降低成本。

计算机视觉（CV）

一种 AI 领域，它使用机器学习来分析和提取数字图像和视频等视觉格式中的信息。例如，Amazon SageMaker AI 为 CV 提供了图像处理算法。

配置偏移

对于工作负载而言，一种偏离预期状态的配置更改。这可能会导致工作负载变得不合规，且通常是渐进的，不是故意的。

配置管理数据库（CMDB）

一种存储库，用于存储和管理有关数据库及其 IT 环境的信息，包括硬件和软件组件及其配置。您通常在迁移的产品组合发现和分析阶段使用来自 CMDB 的数据。

合规性包

一系列 AWS Config 规则和补救措施，您可以汇编这些规则和补救措施，以自定义您的合规性和安全性检查。您可以使用 YAML 模板将一致性包作为单个实体部署在 AWS 账户 和区域或整个组织中。有关更多信息，请参阅 AWS Config 文档中的一致性包。

持续集成和持续交付（CI/CD）

自动执行软件发布过程的源代码、构建、测试、暂存和生产阶段的过程。 CI/CD 通常被描述为管道。 CI/CD 可以帮助您实现流程自动化、提高生产力、提高代码质量和更快地交付。有关更多信息，请参阅持续交付的优势。CD 也可以表示持续部署。有关更多信息，请参阅持续交付与持续部署。

CV

请参阅计算机视觉。

D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

根据网络中数据的关键性和敏感性对其进行识别和分类的过程。它是任何网络安全风险管理策略的关键组成部分，因为它可以帮助您确定对数据的适当保护和保留控制。数据分类是 Well-Architecte AWS d Framework 中安全支柱的一个组成部分。有关详细信息，请参阅数据分类。

数据漂移

生产数据与用来训练机器学习模型的数据之间的有意义差异，或者输入数据随时间推移的有意义变化。数据漂移可能降低机器学习模型预测的整体质量、准确性和公平性。

传输中数据

在网络中主动移动的数据，例如在网络资源之间移动的数据。

数据网格

一种架构框架，可提供分布式、去中心化的数据所有权以及集中式管理和治理。

数据最少化

仅收集并处理绝对必要数据的原则。在中进行数据最小化 AWS 云 可以降低隐私风险、成本和分析碳足迹。

数据边界

AWS 环境中的一组预防性防护措施，可帮助确保只有可信身份才能访问来自预期网络的可信资源。有关更多信息，请参阅在上构建数据边界。 AWS

数据预处理

将原始数据转换为 ML 模型易于解析的格式。预处理数据可能意味着删除某些列或行，并处理缺失、不一致或重复的值。

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

一种支持商业智能（例如分析）的数据管理系统。数据仓库通常包含大量历史数据，通常用于查询和分析。

数据库定义语言（DDL）

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言（DML）

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

请参阅数据库定义语言。

深度融合

组合多个深度学习模型进行预测。您可以使用深度融合来获得更准确的预测或估算预测中的不确定性。

深度学习

一个 ML 子字段使用多层人工神经网络来识别输入数据和感兴趣的目标变量之间的映射。

defense-in-depth

一种信息安全方法，经过深思熟虑，在整个计算机网络中分层实施一系列安全机制和控制措施，以保护网络及其中数据的机密性、完整性和可用性。当你采用这种策略时 AWS，你会在 AWS

Organizations 结构的不同层面添加多个控件来帮助保护资源。例如，一种 defense-in-depth方法可以结合多因素身份验证、网络分段和加密。

委派管理员

在中 AWS Organizations，兼容的服务可以注册 AWS 成员帐户来管理组织的帐户并管理该服务的权限。此账户被称为该服务的委托管理员。有关更多信息和兼容服务列表，请参阅 AWS Organizations 文档中使用 AWS Organizations的服务。

部署

使应用程序、新功能或代码修复在目标环境中可用的过程。部署涉及在代码库中实现更改，然后在应用程序的环境中构建和运行该代码库。

开发环境

请参阅环境。

侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出提醒。这些控制是第二道防线，提醒您注意绕过现有预防性控制的安全事件。有关更多信息，请参阅在 AWS上实施安全控制中的侦测性控制。

开发价值流映射（DVSM）

用于识别对软件开发生命周期中的速度和质量产生不利影响的限制因素并确定其优先级的流程。DVSM 扩展了最初为精益生产实践设计的价值流映射流程。其重点关注在软件开发过程中创造和转移价值所需的步骤和团队。

数字孪生

真实世界系统的虚拟再现，如建筑物、工厂、工业设备或生产线。数字孪生支持预测性维护、远程监控和生产优化。

维度表

星型架构中的一种较小的表，其中包含事实表中定量数据的数据属性。维度表属性通常是文本字段或行为类似于文本的离散数字。这些属性通常用于查询约束、筛选和结果集标注。

灾难

阻止工作负载或系统在其主要部署位置实现其业务目标的事件。这些事件可能是自然灾害、技术故障或人为操作的结果，例如无意的配置错误或恶意软件攻击。

灾难恢复（DR）

您用来最大程度地减少由灾难造成的停机时间和数据丢失的策略和流程。有关更多信息，请参阅 Well-Architected Fr ame AWS work 中的 “工作负载灾难恢复：云端 AWS 恢复”。

DML

请参阅数据库操作语言。

领域驱动设计

一种开发复杂软件系统的方法，通过将其组件连接到每个组件所服务的不断发展的领域或核心业务目标。Eric Evans 在其著作领域驱动设计：软件核心复杂性应对之道（Boston: Addison-Wesley Professional, 2003）中介绍了这一概念。有关如何将领域驱动设计与 strangler fig 模式结合使用的信息，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

DR

请参阅灾难恢复。

偏差检测

跟踪与基准配置的偏差。例如，您可以使用 AWS CloudFormation 来检测系统资源中的偏差，也可以使用 AWS Control Tower 来检测着陆区中可能影响监管要求合规性的变化。

DVSM

请参阅开发价值流映射。

E

EDA

请参阅探索性数据分析。

EDI

请参阅电子数据交换。

边缘计算

该技术可提高位于 IoT 网络边缘的智能设备的计算能力。与云计算比较时，边缘计算可以减少通信延迟并缩短响应时间。

电子数据交换（EDI）

组织之间业务文件的自动交换。有关更多信息，请参阅什么是电子数据交换。

加密

一种将人类可读的纯文本数据转换为加密文字的计算流程。

加密密钥

由加密算法生成的随机位的加密字符串。密钥的长度可能有所不同，而且每个密钥都设计为不可预测且唯一。

字节顺序

字节在计算机内存中的存储顺序。大端序系统先存储最高有效字节。小端序系统先存储最低有效字节。

端点

请参阅服务端点。

端点服务

一种可以在虚拟私有云（VPC）中托管，与其他用户共享的服务。您可以使用其他 AWS 账户 或 AWS Identity and Access Management (IAM) 委托人创建终端节点服务， AWS PrivateLink 并向其授予权限。这些账户或主体可通过创建接口 VPC 端点来私密地连接到您的端点服务。有关更多信息，请参阅 Amazon Virtual Private Cloud（Amazon VPC）文档中的创建端点服务。

企业资源规划（ERP）

一种自动化和管理企业关键业务流程（例如会计、MES 和项目管理）的系统。

信封加密

用另一个加密密钥对加密密钥进行加密的过程。有关更多信息，请参阅 AWS Key Management Service (AWS KMS) 文档中的信封加密。

环境

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

- 开发环境 — 正在运行的应用程序的实例，只有负责维护应用程序的核心团队才能使用。开发环境用于测试更改，然后再将其提升到上层环境。这类环境有时称为测试环境。
- 下层环境 — 应用程序的所有开发环境，比如用于初始构建和测试的环境。

- 生产环境 — 最终用户可以访问的正在运行的应用程序的实例。在 CI/CD 管道中，生产环境是最后一个部署环境。
- 上层环境 — 除核心开发团队以外的用户可以访问的所有环境。这可能包括生产环境、预生产环境和用户验收测试环境。

epic

在敏捷方法学中，有助于组织工作和确定优先级的功能类别。epics 提供了对需求和实施任务的总体描述。例如， AWS CAF 安全史诗包括身份和访问管理、侦探控制、基础设施安全、数据保护和事件响应。有关 AWS 迁移策略中 epics 的更多信息，请参阅计划实施指南。

ERP

请参阅企业资源规划。

探索性数据分析（EDA）

分析数据集以了解其主要特征的过程。您收集或汇总数据，并进行初步调查，以发现模式、检测异常并检查假定情况。EDA 通过计算汇总统计数据和创建数据可视化得以执行。

F

事实表

星型架构中的中心表。它存储有关业务运营的定量数据。通常，事实表包含两种类型的列：包含度量的列和包含维度表外键的列。

快速失效机制

一种使用频繁且增量式的测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

在中 AWS 云，诸如可用区 AWS 区域、控制平面或数据平面之类的边界，它限制了故障的影响并有助于提高工作负载的弹性。有关更多信息，请参阅 AWS 故障隔离边界。

功能分支

请参阅分支。

特征

您用来进行预测的输入数据。例如，在制造环境中，特征可能是定期从生产线捕获的图像。

特征重要性

特征对于模型预测的重要性。这通常表示为数值分数，可以通过各种技术进行计算，例如 Shapley 加法解释（SHAP）和积分梯度。有关更多信息，请参阅使用机器学习模型的可解释性 AWS。

功能转换

为 ML 流程优化数据，包括使用其他来源丰富数据、扩展值或从单个数据字段中提取多组信息。这使得 ML 模型能从数据中获益。例如，如果您将“2021-05-27 00:15:37”日期分解为“2021”、“五月”、“星期四”和“15”，则可以帮助学习与不同数据成分相关的算法学习精细模式。

少样本提示

在要求 LLM 执行类似任务之前，先向其提供少量示例，以演示任务和预期输出。此技术是上下文内学习的一种应用，其中模型可以从提示中嵌入的示例（样本）中学习。对于需要特定格式、推理或领域知识的任务，少样本提示可能非常有效。另请参阅零样本提示。

FGAC

请参阅精细访问控制。

精细访问控制（FGAC）

使用多个条件允许或拒绝访问请求。

快闪迁移

一种数据库迁移方法，通过更改数据捕获使用连续数据复制，在极短的时间内迁移数据，而非使用分阶段方法。目标是将停机时间降至最低。

FM

请参阅基础模型。

基础模型（FM）

一个大型深度学习神经网络，一直在广义和未标记数据的大量数据集上进行训练。 FMs 能够执行各种各样的一般任务，例如理解语言、生成文本和图像以及用自然语言进行对话。有关更多信息，请参阅什么是基础模型。

G

生成式人工智能

AI 模型的一个子集，这些模型已经过大量数据训练，可以使用简单的文本提示来创建新的内容和构件，例如图像、视频、文本和音频。有关更多信息，请参阅什么是生成式人工智能。

地理阻止

请参阅地理限制。

地理限制（地理阻止）

在 Amazon 中 CloudFront，一种阻止特定国家/地区的用户访问内容分发的选项。您可以使用允许列表或阻止列表来指定已批准和已禁止的国家/地区。有关更多信息，请参阅 CloudFront 文档中的限制内容的地理分布。

GitFlow 工作流程

一种方法，在这种方法中，下层和上层环境在源代码存储库中使用不同的分支。Gitflow 工作流程被认为是传统的工作流程，而基于中继的工作流程则是现代的、首选的方法。

黄金映像

系统或软件的快照，用作部署该系统或软件的新实例的模板。例如，在制造业中，黄金映像可用于在多个设备上预调配软件，并有助于提高设备制造操作的速度、可扩展性和生产效率。

全新策略

在新环境中缺少现有基础设施。在对系统架构采用全新策略时，您可以选择所有新技术，而不受对现有基础设施（也称为棕地）兼容性的限制。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

防护机制

帮助管理各组织单位的资源、策略和合规性的高级规则 (OUs)。预防性防护机制会执行策略以确保符合合规性标准。它们是使用服务控制策略和 IAM 权限边界实现的。侦测性护栏会检测策略违规和合规性问题，并生成提醒以进行修复。它们通过使用 AWS Config、、Amazon、 AWS Security Hub CSPM GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

H

HA

请参阅高可用性。

异构数据库迁移

将源数据库迁移到使用不同数据库引擎的目标数据库（例如，从 Oracle 迁移到 Amazon Aurora）。异构迁移通常是重新架构工作的一部分，而转换架构可能是一项复杂的任务。AWS 提供了 AWS SCT 来帮助实现架构转换。

高可用性（HA）

在遇到挑战或灾难时，工作负载无需干预即可连续运行的能力。HA 系统旨在自动进行故障转移、持续提供良好性能，并以最小的性能影响处理不同负载和故障。

历史数据库现代化

一种用于实现运营技术（OT）系统现代化和升级以更好满足制造业需求的方法。历史数据库是一种用于收集和存储工厂中各种来源数据的数据库。

保留数据

从用于训练机器学习模型的数据集中保留的一部分标注的历史数据。通过将模型预测与保留数据进行比较，您可以使用保留数据来评估模型性能。

同构数据库迁移

将源数据库迁移到共享同一数据库引擎的目标数据库（例如，从 Microsoft SQL Server 迁移到 Amazon RDS for SQL Server）。同构迁移通常是更换主机或更换平台工作的一部分。您可以使用本机数据库实用程序来迁移架构。

热数据

经常访问的数据，例如实时数据或近期的转化数据。这些数据通常需要高性能存储层或存储类别才能提供快速的查询响应。

修补程序

针对生产环境中关键问题的紧急修复。由于其紧迫性，修补程序通常是在典型的 DevOps 发布工作流程之外进行的。

hypercare 周期

割接之后，迁移团队立即管理和监控云中迁移的应用程序以解决任何问题的时间段。通常，这个周期持续 1-4 天。在 hypercare 周期结束时，迁移团队通常会将应用程序的责任移交给云运营团队。

我

IaC

请参阅基础设施即代码。

基于身份的策略

附加到一个或多个 IAM 委托人的策略，用于定义他们在 AWS 云 环境中的权限。

空闲应用程序

90 天内平均 CPU 和内存使用率在 5% 到 20% 之间的应用程序。在迁移项目中，通常会停用这些应用程序或将其保留在本地。

IIoT

请参阅工业物联网。

不可变基础设施

一种模型，可为生产工作负载部署新的基础设施，而不是更新、修补或修改现有基础设施。不可变基础设施本质上比可变基础设施更一致、更可靠、更可预测。有关更多信息，请参阅 AWS Well-Architected Framework 中的使用不可变基础设施进行部署最佳实践。

入站（入口）VPC

在 AWS 多账户架构中，一种接受、检查和路由来自应用程序外部的网络连接的 VPC。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查， VPCs 以保护您的应用程序与更广泛的互联网之间的双向接口。

增量迁移

一种割接策略，在这种策略中，您可以将应用程序分成小部分进行迁移，而不是一次性完整割接。例如，您最初可能只将几个微服务或用户迁移到新系统。在确认一切正常后，您可以逐步迁移其他微服务或用户，直到停用遗留系统。这种策略降低了大规模迁移带来的风险。

工业 4.0

该术语由 Klaus Schwab 在 2016 年提出，指的是通过连接、实时数据、自动化、分析和 AI/ML 的进步来实现制造流程的现代化。

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码（IaC）

通过一组配置文件预调配和管理应用程序基础设施的过程。IaC 旨在帮助您集中管理基础设施、实现资源标准化和快速扩展，使新环境具有可重复性、可靠性和一致性。

工业物联网 (IIoT)

在工业领域使用联网的传感器和设备，例如制造业、能源、汽车、医疗保健、生命科学和农业。有关更多信息，请参阅制定工业物联网 (IIoT) 数字化转型战略。

检查 VPC

在 AWS 多账户架构中，一种集中式 VPC，用于管理对 VPCs（相同或不同 AWS 区域）、互联网和本地网络之间的网络流量的检查。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查， VPCs 以保护您的应用程序与更广泛的互联网之间的双向接口。

物联网（IoT）

由带有嵌入式传感器或处理器的连接物理对象组成的网络，这些传感器或处理器通过互联网或本地通信网络与其他设备和系统进行通信。有关更多信息，请参阅什么是 IoT？

可解释性

它是机器学习模型的一种特征，描述了人类可以理解模型的预测如何取决于其输入的程度。有关更多信息，请参阅使用机器学习模型的可解释性 AWS。

物联网

请参阅物联网。

IT 信息库（ITIL）

提供 IT 服务并使这些服务符合业务要求的一套最佳实践。ITIL 是 ITSM 的基础。

IT 服务管理（ITSM）

为组织设计、实施、管理和支持 IT 服务的相关活动。有关将云运营与 ITSM 工具集成的信息，请参阅运营集成指南。

ITIL

请参阅 IT 信息库。

ITSM

请参阅 IT 服务管理。

L

基于标签的访问控制（LBAC）

强制访问控制（MAC）的一种实施方式，其中明确为用户和数据本身分配了安全标签值。用户安全标签和数据安全标签之间的交集决定了用户可以看到哪些行和列。

登录区

landing zone 是一个架构精良的多账户 AWS 环境，具有可扩展性和安全性。这是一个起点，您的组织可以从这里放心地在安全和基础设施环境中快速启动和部署工作负载和应用程序。有关登录区的更多信息，请参阅设置安全且可扩展的多账户 AWS 环境。

大语言模型（LLM）

一种基于大量数据进行预训练的深度学习 AI 模型。LLM 可以执行多项任务，例如回答问题、总结文档、将文本翻译成其他语言以及完成句子。有关更多信息，请参阅什么是 LLMs。

大规模迁移

迁移 300 台或更多服务器。

LBAC

请参阅基于标签的访问控制。

最低权限

授予执行任务所需的最低权限的最佳安全实践。有关更多信息，请参阅 IAM 文档中的应用最低权限许可。

直接迁移

请参阅 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参阅字节顺序。

LLM

请参阅大型语言模型。

下层环境

请参阅环境。

M

机器学习（ML）

一种使用算法和技术进行模式识别和学习的人工智能。ML 对记录的数据（例如物联网（IoT）数据）进行分析和学习，以生成基于模式的统计模型。有关更多信息，请参阅机器学习。

主分支

请参阅分支。

恶意软件

旨在危害计算机安全或隐私的软件。恶意软件可能会破坏计算机系统、泄露敏感信息或获得未经授权的访问权限。恶意软件的示例包括病毒、蠕虫、勒索软件、木马、间谍软件和键盘记录器。

托管式服务

AWS 服务 它 AWS 运行基础设施层、操作系统和平台，您可以访问端点来存储和检索数据。Amazon Simple Storage Service（Amazon S3）和 Amazon DynamoDB 就是托管服务的示例。这些服务也称为抽象服务。

制造执行系统（MES）

一种软件系统，用于跟踪、监控、记录和控制在车间将原材料转化为成品的生产过程。

MAP

请参阅迁移加速计划。

机制

一个完整的过程，您可以在其中创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运作过程中自我强化和改善的循环。有关更多信息，请参阅在 Well-Architect AWS ed 框架中构建机制。

成员账户

AWS 账户 除属于组织中的管理账户之外的所有账户 AWS Organizations。一个账户一次只能是一个组织的成员。

MES

请参阅制造执行系统。

消息队列遥测传输（MQTT）

一种基于发布/订阅模式的轻量级 machine-to-machine (M2M) 通信协议，适用于资源受限的物联网设备。

微服务

一种小型的独立服务，通过明确的定义进行通信 APIs ，通常由小型的独立团队拥有。例如，保险系统可能包括映射到业务能力（如销售或营销）或子域（如购买、理赔或分析）的微服务。微服务

的好处包括敏捷、灵活扩展、易于部署、可重复使用的代码和恢复能力。有关更多信息，请参阅使用 AWS 无服务器服务集成微服务。

微服务架构

一种使用独立组件构建应用程序的方法，这些组件将每个应用程序进程作为微服务运行。这些微服务使用轻量级通过定义明确的接口进行通信。 APIs该架构中的每个微服务都可以更新、部署和扩展，以满足对应用程序特定功能的需求。有关更多信息，请参阅在上实现微服务。 AWS

迁移加速计划（MAP）

AWS 该计划提供咨询支持、培训和服务，以帮助组织为迁移到云奠定坚实的运营基础，并帮助抵消迁移的初始成本。MAP 提供了一种以系统的方式执行遗留迁移的迁移方法，以及一套用于自动执行和加速常见迁移场景的工具。

大规模迁移

将大部分应用程序组合分波迁移到云中的过程，在每一波中以更快的速度迁移更多应用程序。本阶段使用从早期阶段获得的最佳实践和经验教训，实施由团队、工具和流程组成的迁移工厂，通过自动化和敏捷交付简化工作负载的迁移。这是 AWS 迁移策略的第三阶段。

迁移工厂

跨职能团队，通过自动化、敏捷的方法简化工作负载迁移。迁移工厂团队通常包括运营、业务分析师和所有者、迁移工程师、开发人员和冲刺 DevOps 领域的专业人员。20% 到 50% 的企业应用程序组合由可通过工厂方法优化的重复模式组成。有关更多信息，请参阅本内容集中有关迁移工厂的讨论和云迁移工厂指南。

迁移元数据

有关完成迁移所需的应用程序和服务器的信息。每种迁移模式都需要一套不同的迁移元数据。迁移元数据的示例包括目标子网、安全组和 AWS 账户。

迁移模式

一种可重复的迁移任务，详细列出了迁移策略、迁移目标以及所使用的迁移应用程序或服务。示例：使用 AWS 应用程序迁移服务重新托管向 Amazon EC2 的迁移。

迁移组合评测（MPA）

一种在线工具，提供了用于验证迁移到 AWS 云的业务案例的信息。MPA 提供了详细的组合评测（服务器规模调整、定价、TCO 比较、迁移成本分析）以及迁移计划（应用程序数据分析和数据收集、应用程序分组、迁移优先级排序和波次规划）。所有 AWS 顾问和 APN 合作伙伴顾问均可免费使用 MPA 工具（需要登录）。

迁移准备情况评测（MRA）

使用 AWS CAF 深入了解组织的云就绪状态、确定优势和劣势以及制定行动计划以缩小已发现差距的过程。有关更多信息，请参阅迁移准备指南。MRA 是 AWS 迁移策略的第一阶段。

迁移策略

将工作负载迁移到 AWS 云的方法。有关更多信息，请参见术语表中的 7 R 词条，以及动员您的组织以加快大规模迁移。

ML

请参阅机器学习。

现代化

将过时的（原有的或单体）应用程序及其基础设施转变为云中敏捷、弹性和高度可用的系统，以降低成本、提高效率和利用创新。有关更多信息，请参阅在 AWS 云中实现应用程序现代化的策略。

现代化准备情况评估

一种评估方式，有助于确定组织应用程序的现代化准备情况；确定收益、风险和依赖关系；确定组织能够在多大程度上支持这些应用程序的未来状态。评估结果是目标架构的蓝图、详细说明现代化进程发展阶段和里程碑的路线图以及解决已发现差距的行动计划。有关更多信息，请参阅在 AWS 云中评估应用程序的现代化准备情况。

单体应用程序（单体式）

作为具有紧密耦合进程的单个服务运行的应用程序。单体应用程序有几个缺点。如果某个应用程序功能的需求激增，则必须扩展整个架构。随着代码库的增长，添加或改进单体应用程序的功能也会变得更加复杂。若要解决这些问题，可以使用微服务架构。有关更多信息，请参阅将单体分解为微服务。

MPA

请参阅迁移组合评测。

MQTT

请参阅消息队列遥测传输。

多分类器

一种帮助为多个类别生成预测（预测两个以上结果之一）的过程。例如，ML 模型可能会询问“这个产品是书、汽车还是手机？”或“此客户最感兴趣什么类别的产品？”

可变基础设施

一种用于更新和修改生产工作负载的现有基础设施的模型。为了提高一致性、可靠性和可预测性，Well-Architect AWS ed Framework 建议使用不可变基础设施作为最佳实践。

O

OAC

请参阅来源访问控制。

OAI

请参阅来源访问身份。

OCM

请参阅组织变革管理。

离线迁移

一种迁移方法，在这种方法中，源工作负载会在迁移过程中停止运行。这种方法会延长停机时间，通常用于小型非关键工作负载。

OI

请参阅运营集成。

OLA

请参阅运营级别协议。

在线迁移

一种迁移方法，在这种方法中，源工作负载无需离线即可复制到目标系统。在迁移过程中，连接工作负载的应用程序可以继续运行。这种方法的停机时间为零或最短，通常用于关键生产工作负载。

OPC-UA

请参阅开放流程通信 – 统一架构。

开放流程通信 – 统一架构（OPC-UA）

一种用于工业自动化的 machine-to-machine（M2M）通信协议。OPC-UA 提供了一个包含数据加密、身份验证和授权方案的互操作性标准。

运营级别协议（OLA）

一项协议，阐明了 IT 职能部门承诺相互交付的内容，以支持服务水平协议（SLA）。

运营准备情况审查（ORR）

一份问题核对清单和关联的最佳实践，可帮助您了解、评估、预防或缩小事件和可能的故障的范围。有关更多信息，请参阅 AWS Well-Architected Framework 中的运营准备情况审查（ORR）。

运营技术（OT）

与物理环境配合使用以控制工业运营、设备和基础设施的硬件和软件系统。在制造业中，OT 和信息技术（IT）系统的集成是工业 4.0 转型的关键重点。

运营整合（OI）

在云中实现运营现代化的过程，包括就绪计划、自动化和集成。有关更多信息，请参阅运营整合指南。

组织跟踪

由 AWS CloudTrail 此创建的跟踪记录组织 AWS 账户 中所有人的所有事件 AWS Organizations。该跟踪是在每个 AWS 账户 中创建的，属于组织的一部分，并跟踪每个账户的活动。有关更多信息，请参阅 CloudTrail文档中的为组织创建跟踪。

组织变革管理（OCM）

一个从人员、文化和领导力角度管理重大、颠覆性业务转型的框架。OCM 通过加快变革采用、解决过渡问题以及推动文化和组织变革，帮助组织为新系统和战略做好准备和过渡。在 AWS 迁移策略中，该框架被称为人员加速，因为云采用项目需要变更的速度。有关更多信息，请参阅 OCM 指南。

来源访问控制（OAC）

在中 CloudFront，一个增强的选项，用于限制访问以保护您的亚马逊简单存储服务 (Amazon S3) 内容。OAC 全部支持所有 S3 存储桶 AWS 区域、使用 AWS KMS (SSE-KMS) 进行服务器端加密，以及对 S3 存储桶的动态PUT和DELETE请求。

来源访问身份（OAI）

在中 CloudFront，一个用于限制访问权限以保护您的 Amazon S3 内容的选项。当您使用 OAI 时，CloudFront 会创建一个 Amazon S3 可以对其进行身份验证的委托人。经过身份验证的委托人只能通过特定 CloudFront 分配访问 S3 存储桶中的内容。另请参阅 OAC，其中提供了更精细和增强的访问控制。

ORR

请参阅运营准备情况审查。

OT

请参阅运营技术。

出站（出口）VPC

在 AWS 多账户架构中，一种处理从应用程序内部启动的网络连接的 VPC。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查， VPCs 以保护您的应用程序与更广泛的互联网之间的双向接口。

P

权限边界

附加到 IAM 主体的 IAM 管理策略，用于设置用户或角色可以拥有的最大权限。有关更多信息，请参阅 IAM 文档中的权限边界。

个人身份信息（PII）

直接查看其他相关数据或与之配对时可用于合理推断个人身份的信息。PII 的示例包括姓名、地址和联系信息。

PII

请参阅个人身份信息。

playbook

一套预定义的步骤，用于捕获与迁移相关的工作，例如在云中交付核心运营功能。playbook 可以采用脚本、自动化运行手册的形式，也可以是操作现代化环境所需的流程或步骤的摘要。

PLC

请参阅可编程逻辑控制器。

PLM

请参阅产品生命周期管理。

policy

一个对象，可以定义权限（请参阅基于身份的策略）、指定访问条件（请参阅基于资源的策略）或定义 AWS Organizations 的组织中所有账户的最大权限（请参阅服务控制策略）。

多语言持久性

根据数据访问模式和其他要求，独立选择微服务的数据存储技术。如果您的微服务采用相同的数据存储技术，它们可能会遇到实现难题或性能不佳。如果微服务使用最适合其需求的数据存储，则可以更轻松地实现微服务，并获得更好的性能和可扩展性。

组合评测

一个发现、分析和确定应用程序组合优先级以规划迁移的过程。有关更多信息，请参阅评估迁移准备情况。

谓词

返回 `true` 或 `false` 的查询条件，通常位于 `WHERE` 子句中。

谓词下推

一种数据库查询优化技术，可在传输之前筛选查询中的数据。这将减少从关系数据库检索和处理的数据量，并提高查询性能。

预防性控制

一种安全控制，旨在防止事件发生。这些控制是第一道防线，帮助防止未经授权的访问或对网络的意外更改。有关更多信息，请参阅在 AWS上实施安全控制中的预防性控制。

主体

中 AWS 可以执行操作和访问资源的实体。此实体通常是 IAM 角色的根用户或用户。 AWS 账户有关更多信息，请参阅 IAM 文档中角色术语和概念中的主体。

隐私设计

一种在整个开发过程中都考虑隐私的系统工程方法。

私有托管区

一个容器，其中包含有关您希望 Amazon Route 53 如何响应针对一个或多个 VPCs域名及其子域名的 DNS 查询的信息。有关更多信息，请参阅 Route 53 文档中的私有托管区的使用。

主动控制

一种安全控制，旨在防止部署不合规资源。这些控制会在资源预置之前对其进行扫描。如果资源与控制不兼容，则不会预置它。有关更多信息，请参阅 AWS Control Tower 文档中的控制参考指南，并参见在上实施安全控制中的主动控制 AWS。

产品生命周期管理（PLM）

对产品在其整个生命周期内的数据和流程的管理，从设计、开发和发布，到增长和成熟，再到衰退和淘汰。

生产环境

请参阅环境。

可编程逻辑控制器（PLC）

在制造业中，一种高度可靠、适应性强的计算机，用于监控机器并实现制造过程自动化。

提示串接

使用一个 LLM 提示的输出作为下一个提示的输入，以生成更好的响应。该技术用于将复杂的任务分解为子任务，或者迭代地完善或扩展初步响应。它有助于提高模型响应的准确性和相关性，并允许获得更精细的个性化结果。

假名化

用占位符值替换数据集中个人标识符的过程。假名化可以帮助保护个人隐私。假名化数据仍被视为个人数据。

publish/subscribe (pub/sub)

一种支持微服务间异步通信的模式，可提高可扩展性和响应能力。例如，在基于微服务的 MES 中，微服务可以将事件消息发布到其他微服务可以订阅的频道。系统可以在不更改发布服务的情况下添加新的微服务。

Q

查询计划

一系列用于访问 SQL 关系数据库系统中的数据的步骤，类似于指令。

查询计划回归

当数据库服务优化程序选择的最佳计划不如数据库环境发生特定变化之前时。这可能是由统计数据、约束、环境设置、查询参数绑定更改和数据库引擎更新造成的。

R

RACI 矩阵

请参阅责任、问责、咨询和知情（RACI）。

RAG

请参阅检索增强生成。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI 矩阵

请参阅责任、问责、咨询和知情（RACI）。

RCAC

请参阅行列访问控制。

只读副本

用于只读目的的数据库副本。您可以将查询路由到只读副本，以减轻主数据库的负载。

重新架构

请参阅 7 R。

恢复点目标（RPO）

自上一个数据恢复点以来可接受的最长时间。这决定了从上一个恢复点到服务中断之间可接受的数据丢失情况。

恢复时间目标（RTO）

服务中断和服务恢复之间可接受的最大延迟。

重构

请参阅 7 R。

Region

地理区域内的 AWS 资源集合。每一个 AWS 区域 都相互隔离，相互独立，以提供容错、稳定性和弹性。有关更多信息，请参阅指定您的账户可以使用的 AWS 区域。

回归

一种预测数值的 ML 技术。例如，要解决“这套房子的售价是多少？”的问题 ML 模型可以使用线性回归模型，根据房屋的已知事实（如建筑面积）来预测房屋的销售价格。

重新托管

请参阅 7 R。

版本

在部署过程中，推动生产环境变更的行为。

重新放置

请参阅 7 R。

更换平台

请参阅 7 R。

重新购买

请参阅 7 R。

韧性

应用程序抵御中断或从中断中恢复的能力。在 AWS 云中规划韧性时，高可用性和灾难恢复是常见的考虑因素。有关更多信息，请参阅 AWS 云 韧性。

基于资源的策略

一种附加到资源的策略，例如 AmazonS3 存储桶、端点或加密密钥。此类策略指定了允许哪些主体访问、支持的操作以及必须满足的任何其他条件。

责任、问责、咨询和知情（RACI）矩阵

定义参与迁移活动和云运营的所有各方的角色和责任的矩阵。矩阵名称源自矩阵中定义的责任类型：负责（R）、问责（A）、咨询（C）和知情（I）。支持（S）类型是可选的。如果包括支持，则该矩阵称为 RASCI 矩阵，如果将其排除在外，则称为 RACI 矩阵。

响应性控制

一种安全控制，旨在推动对不良事件或偏离安全基线的情况进行修复。有关更多信息，请参阅在AWS上实施安全控制中的响应性控制。

保留

请参阅 7 R。

停用

请参阅 7 R。

检索增强生成（RAG）

一种生成式人工智能技术，其中 LLM 在生成响应之前引用其训练数据来源之外的权威数据来源。例如，RAG 模型可以对组织的知识库或自定义数据执行语义搜索。有关更多信息，请参阅什么是 RAG。

轮换

定期更新密钥以使攻击者更难访问凭证的过程。

行列访问控制（RCAC）

使用已定义访问规则的基本、灵活的 SQL 表达式。RCAC 由行权限和列掩码组成。

RPO

请参阅恢复点目标。

RTO

请参阅恢复时间目标。

运行手册

执行特定任务所需的一套手动或自动程序。它们通常是为了简化重复性操作或高错误率的程序而设计的。

S

SAML 2.0

许多身份提供商 (IdPs) 使用的开放标准。此功能支持联合单点登录 (SSO)，因此用户无需在 IAM 中为组织中的所有人创建用户即可登录 AWS 管理控制台 或调用 AWS API 操作。有关基于 SAML 2.0 的联合身份验证的更多信息，请参阅 IAM 文档中的关于基于 SAML 2.0 的联合身份验证。

SCADA

请参阅监督控制和数据采集。

SCP

请参阅服务控制策略。

机密密钥

在中 AWS Secrets Manager，您以加密形式存储的机密或受限信息，例如密码或用户凭证。它由密钥值及其元数据组成。密钥值可以是二进制、单个字符串或多个字符串。有关更多信息，请参阅 Secrets Manager 文档中的什么是 Amazon Secrets Manager 密钥？。

安全设计

一种在整个开发过程中都考虑安全的系统工程方法。

安全控制

一种技术或管理防护机制，可防止、检测或降低威胁行为体利用安全漏洞的能力。安全控制有以下四种类型：预防性、检测性、响应性和主动性。

安全固化

缩小攻击面，使其更能抵御攻击的过程。这可能包括删除不再需要的资源、实施授予最低权限的最佳安全实践或停用配置文件中不必要的功能等操作。

安全信息和事件管理（SIEM）系统

结合了安全信息管理（SIM）和安全事件管理（SEM）系统的工具和服务。SIEM 系统会收集、监控和分析来自服务器、网络、设备和其他来源的数据，以检测威胁和安全漏洞，并生成警报。

安全响应自动化

一种预定义的程序化操作，旨在自动响应或修复安全事件。这些自动化可作为侦探或响应式安全控制措施，帮助您实施 AWS 安全最佳实践。自动响应操作的示例包括修改 VPC 安全组、修补 Amazon EC2 实例或轮换凭证。

服务器端加密

由接收数据的人在目的地对数据 AWS 服务 进行加密。

服务控制策略（SCP）

一种策略，用于集中控制组织中所有账户的权限 AWS Organizations。 SCPs 定义防护措施或限制管理员可以委托给用户或角色的操作。您可以使用 SCPs 允许列表或拒绝列表来指定允许或禁止哪些服务或操作。有关更多信息，请参阅 AWS Organizations 文档中的服务控制策略。

服务端点

的入口点的 URL AWS 服务。您可以使用端点，通过编程方式连接到目标服务。有关更多信息，请参阅 AWS 一般参考 中的 AWS 服务 端点。

服务水平协议（SLA）

一份协议，阐明了 IT 团队承诺向客户交付的内容，比如服务正常运行时间和性能。

服务水平指示器（SLI）

对服务性能方面的衡量，例如错误率、可用性或吞吐量。

服务水平目标（SLO）

代表服务运行状况的目标指标，由服务水平指示器衡量。

责任共担模式

描述您在云安全与合规方面共同承担 AWS 的责任的模型。 AWS 负责云的安全，而您则负责云中的安全。有关更多信息，请参阅责任共担模式。

SIEM

请参阅安全信息和事件管理系统。

单点故障（SPOF）

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

请参阅服务水平协议。

SLI

请参阅服务水平指示器。

SLO

请参阅服务水平目标。

split-and-seed 模型

一种扩展和加速现代化项目的模式。随着新功能和产品发布的定义，核心团队会拆分以创建新的产品团队。这有助于扩展组织的能力和服务，提高开发人员的工作效率，支持快速创新。有关更多信息，请参阅在 AWS 云中实现应用程序现代化的分阶段方法。

SPOF

请参阅单点故障。

星型架构

一种数据库组织结构，它使用一个大型事实表来存储事务数据或测量数据，并使用一个或多个较小的维度表来存储数据属性。此结构专为在数据仓库中使用或用于商业智能目的而设计。

strangler fig 模式

一种通过逐步重写和替换系统功能直至可以停用原有的系统来实现单体系统现代化的方法。这种模式用无花果藤作为类比，这种藤蔓成长为一棵树，最终战胜并取代了宿主。该模式是由 Martin Fowler 提出的，作为重写单体系统时管理风险的一种方法。有关如何应用此模式的示例，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

监督控制和数据采集（SCADA）

在制造业中，一种使用硬件和软件来监控实物资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

以模拟用户交互的方式测试系统，以检测潜在问题或监控性能。你可以使用 Amazon S CloudWatch ynthetics 来创建这些测试。

系统提示

一种为 LLM 提供上下文、说明或准则以指导其行为的技术。系统提示有助于设置上下文并制定与用户交互的规则。

T

标签

键值对，用作组织资源的元数据。 AWS 标签有助于您管理、识别、组织、搜索和筛选 资源。有关更多信息，请参阅标记您的 AWS 资源。

目标变量

您在监督式 ML 中尝试预测的值。这也被称为结果变量。例如，在制造环境中，目标变量可能是产品缺陷。

任务列表

一种通过运行手册用于跟踪进度的工具。任务列表包含运行手册的概述和要完成的常规任务列表。对于每项常规任务，它包括预计所需时间、所有者和进度。

测试环境

请参阅环境。

训练

为您的 ML 模型提供学习数据。训练数据必须包含正确答案。学习算法在训练数据中查找将输入数据属性映射到目标（您希望预测的答案）的模式。然后输出捕获这些模式的 ML 模型。然后，您可以使用 ML 模型对不知道目标的新数据进行预测。

中转网关

一个网络传输中心，可用于将您的网络 VPCs 和本地网络互连。有关更多信息，请参阅 AWS Transit Gateway 文档中的什么是公交网关。

基于中继的工作流程

一种方法，开发人员在功能分支中本地构建和测试功能，然后将这些更改合并到主分支中。然后，按顺序将主分支构建到开发、预生产和生产环境。

可信访问权限

向您指定的服务授予权限，该服务可代表您在其账户中执行任务。 AWS Organizations 当需要服务相关的角色时，受信任的服务会在每个账户中创建一个角色，为您执行管理任务。有关更多信息，请参阅 AWS Organizations 文档中的AWS Organizations 与其他 AWS 服务一起使用。

优化

更改训练过程的各个方面，以提高 ML 模型的准确性。例如，您可以通过生成标签集、添加标签，并在不同的设置下多次重复这些步骤来优化模型，从而训练 ML 模型。

双披萨团队

一个小 DevOps 团队，你可以用两个披萨来喂食。双披萨团队的规模可确保在软件开发过程中充分协作。

U

不确定性

这一概念指的是不精确、不完整或未知的信息，这些信息可能会破坏预测式 ML 模型的可靠性。不确定性有两种类型：认知不确定性是由有限的、不完整的数据造成的，而偶然不确定性是由数据中固有的噪声和随机性导致的。有关更多信息，请参阅量化深度学习系统中的不确定性指南。

无差别任务

也称为繁重工作，即创建和运行应用程序所必需的工作，但不能为最终用户提供直接价值或竞争优势。无差别任务的示例包括采购、维护和容量规划。

上层环境

请参阅环境。

V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC 对等连接

两者之间的连接 VPCs ，允许您使用私有 IP 地址路由流量。有关更多信息，请参阅 Amazon VPC 文档中的什么是 VPC 对等连接。

漏洞

损害系统安全的软件缺陷或硬件缺陷。

W

热缓存

一种包含经常访问的当前相关数据的缓冲区缓存。数据库实例可以从缓冲区缓存读取，这比从主内存或磁盘读取要快。

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

一种对与当前记录有某种关联的一组行执行计算的 SQL 函数。窗口函数对于处理任务很有用，例如计算移动平均值或根据当前行的相对位置访问行的值。

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

迁移项目中负责一组特定任务的职能小组。每个工作流都是独立的，但支持项目中的其他工作流。例如，组合工作流负责确定应用程序的优先级、波次规划和收集迁移元数据。组合工作流将这些资产交付给迁移工作流，然后迁移服务器和应用程序。

WORM

请参阅一次写入多次读取。

WQF

请参阅 AWS 工作负载资格鉴定框架。

一次写入多次读取（WORM）

一种存储模型，可一次写入数据并防止数据被删除或修改。授权用户可以根据需要多次读取数据，但无法对其进行更改。此数据存储基础设施被认为不可变。

Z

零日漏洞利用

一种利用零日漏洞的攻击，通常为恶意软件。

零日漏洞

生产系统中不可避免的缺陷或漏洞。威胁主体可能利用这种类型的漏洞攻击系统。开发人员经常因攻击而意识到该漏洞。

零样本提示

为 LLM 提供执行任务的说明，但没有可以帮助指导的示例（样本）。LLM 必须使用预先训练的知识来处理任务。零样本提示的有效性取决于任务的复杂性和提示的质量。另请参阅少样本提示。

僵尸应用程序

平均 CPU 和内存使用率低于 5% 的应用程序。在迁移项目中，通常会停用这些应用程序。

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。