



为静态数据创建企业加密策略

AWS 规范性指导



AWS 规范性指导: 为静态数据创建企业加密策略

Copyright © 2024 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

介绍	1
目标受众	1
有针对性的业务成果	1
限制	2
关于数据加密	3
关于加密密钥	3
关于加密算法	3
关于信封加密	3
加密策略阶段	5
策略	5
标准	6
成本和性能	7
密钥访问	7
加密类型	7
加密密钥规范	7
密钥存储位置	8
框架	8
数据分类	8
环境分类	9
变更事件和流程	9
实现	10
成本、便利性和控制	11
性能和加密类型	11
密钥存储位置	12
访问控制	12
审计和日志记录	13
常见问题	14
我什么时候需要对称加密？	14
我什么时候需要非对称加密？	14
我什么时候需要信封加密？	14
何时需要使用 HSM？	14
为什么要集中管理加密密钥？	15
我需要专门构建的加密基础设施吗？	15
怎么能AWS KMS帮上忙？	15

资源	16
AWS 服务 文档	16
AWS 营销	16
AWS Well-Architected	16
哈希和标记化	16
视频	17
文档历史记录	18
术语表	19
#	19
A	19
B	22
C	23
D	26
E	29
F	31
G	32
H	32
I	33
L	35
M	36
O	39
P	42
Q	44
R	44
S	47
T	49
U	51
V	51
W	51
Z	52
.....	liii

为静态数据创建企业加密策略

Amazon Web Services 的 Venki Srivatsav、Andrea Di Fabio 和 Vikramaditya Bhatnagar (AWS)

2022 年 9 月 ([文件历史记录](#))

许多企业担心数据泄露的网络安全威胁。发生数据泄露时，未经授权的人会访问您的网络并窃取企业数据。防火墙和反恶意软件服务可以帮助抵御这种威胁。您可以实现的另一种保护是数据加密。在本指南的“关于数据加密”部分中，您可以详细了解数据加密的工作原理和可用类型。

一般来说，当你讨论加密时，有两种类型的数据。传输中的数据是指在网络中主动传输的数据，例如在网络资源之间。静态数据是静止和休眠的数据，例如存储中的数据。该策略侧重于静态数据。有关加密传输中的数据的更多信息，请参阅[保护传输中的数据 \(Well-AWS Architected 框架 \)](#)。

加密策略由四个部分组成，您按顺序开发这些部分。加密策略由高级管理层确定，概述了加密的法规、合规性和业务要求。加密标准可帮助实施该政策的人员理解并遵守该政策。标准可以是技术性的，也可以是程序性的。该框架是支持标准实施的标准操作程序、结构和护栏。最后，架构是加密标准的技术实现，例如您使用的环境、服务和工具。本文档的目标是帮助您创建适合您的业务、安全性和合规性需求的加密策略。它包括有关如何审查和实施静态数据安全标准的建议，以便您可以全面满足合规性和业务需求。

此策略使用AWS Key Management Service (AWS KMS) 来帮助您创建和管理有助于保护数据的加密密钥。AWS KMS集成了许多AWS服务，可以加密所有静态数据。即使您选择了其他加密服务，您仍然可以采用本指南中的建议和阶段。

目标受众

该策略旨在面向以下受众：

- 为企业制定政策的执行官员，例如首席执行官、首席技术官 (CTO)、首席信息官 (CIO) 和首席信息安全官 (CISO)
- 负责制定技术标准的技术官员，例如技术副总裁和总监
- 合规和治理官员，负责监督合规政策的遵守情况，包括法定和自愿合规制度

有针对性的业务成果

- Data-at-rest 加密策略 — 决策者和政策制定者可以创建加密策略并了解影响策略的关键因素。

- Data-at-rest 加密标准 — 技术主管可以开发基于加密策略的加密标准。
- 加密框架 — 技术领导者和实施者可以创建一个框架，作为政策制定者和标准制定者之间的桥梁。在这种情况下，框架意味着确定适当的流程和工作流程，以帮助您在政策的范围内实施标准。框架类似于用于更改政策或标准的标准操作程序或变更管理流程。
- 技术架构和实现 — 开发人员和架构师等亲身实践的实施者知道可以帮助他们实施加密策略的可用架构参考资料。

限制

本文档旨在帮助您制定最适合企业需求的自定义加密策略。它本身不是加密策略，也不是合规清单。本文档不包括以下主题：

- 传输中传输加密
- 令牌化
- 哈希
- 合规性和数据治理
- 为您的加密程序编列预算

有关某些主题的更多信息，请参阅小[资源](#)节。

关于数据加密

本部分高度概括加密概念和术语。有关更多详细信息，请参阅[密码学概念](#)（AWS加密服务和工具指南）。数据加密可帮助您加强数据机密性。通过实施加密和访问控制，您可以帮助保护企业中的数据。

关于加密密钥

加密服务使用加密密钥来加密数据。加密密钥是由加密算法生成的由随机位组成的加密字符串。按键的长度可以不同，每个密钥的设计都是不可预测和唯一的。加密的强度通常取决于两个因素：密钥的长度和所使用的算法。一般来说，较长的密钥可提供更强的加密。

关于加密算法

生成加密密钥有两种算法，对称算法和非对称算法。

对称加密使用相同的密钥为数据加密和解密。这种类型的加密通常更快，因此对大量数据非常有效。这种类型的加密已被广泛使用，并且被普遍认为是安全的。由于加密和解密都使用单个密钥，因此最佳做法是经常更改密钥，以防止未经授权的人员获取密钥。有关何时推荐使用对称加密的更多信息，请参阅[我什么时候需要对称加密？](#)常见问题解答部分。

非对称加密使用一对密钥，一个用于加密的公钥和一个用于解密的私钥。您可以共享公钥，因为它不用于解密，但是对私钥的访问应受到严格限制。人们普遍认为非对称加密比对称加密更安全，但速度较慢，因为它使用更长的密钥长度并且需要更复杂的加密计算。有关何时建议使用非对称加密的更多信息，请参阅[我什么时候需要非对称加密？](#)常见问题解答部分。

关于信封加密

当您加密数据时，只有当您的加密密钥保持机密时，数据才会受到保护。用于加密数据的密钥称为数据密钥。信封加密是使用另一种加密密钥（称为密钥加密密钥）对数据密钥进行加密的做法。您甚至可以使用另一个加密密钥加密该密钥，依此类推。最终，一个密钥必须保留在明文中，这样您才能解密密钥和数据。此顶级明文密钥加密密钥称为根密钥。

信封加密可提供以下多种优势：

- 方便 — 由于您的数据密钥已加密，因此您可以将其与加密数据一起存储。
- 效率 — 加密操作可能很耗时，尤其是在数据量大的情况下。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。这使您可以提供两层或多层加密保护，而无需重新加密数据。

- 性能-您可以组合加密算法。例如，您可以对原始数据使用对称加密，但对数据密钥使用非对称加密，这结合了两种加密算法的优势。

有关信封加密的更多信息，请参阅[信封加密](#) (AWS Key Management Service文档)。有关决定是否需
要信封加密的更多信息，请参阅[我什么时候需要信封加密？](#)常见问题解答部分。

建立加密策略的各个阶段

建立企业级加密策略需要多阶段方法。每个阶段都定义了一组控制措施，以帮助您实现预期的切实成果。本文档指导您完成这些阶段，并询问您一些具体问题，以帮助您自定义加密策略。

为静态数据构建加密策略包括以下连续阶段：

1. [加密策略](#)— 制定策略，为您的企业定义 data-at-rest 加密目标。
2. [加密标准](#)— 定义可帮助您实现企业政策的技术和程序标准。
3. [加密框架](#)— 构建框架，帮助所有利益相关者理解、更改和实施您的加密标准。
4. [实现](#)— 部署您的加密基础架构。

加密策略

加密策略的目的是在高级管理层建立组织需要满足的业务和合规性期望。该策略是定义合适加密策略的起点。该政策应足够抽象，以便为实施提供自由和灵活性。同时，它必须足够具体，以界定符合组织目标的可接受实施的范围。通常，策略与技术无关，很少更改，因为它们定义了企业加密策略的基本特征。

通常，加密策略包含但不限于以下内容：

- 您的企业必须遵守的任何监管或合规制度
- 对数据加密的任何业务承诺或期望
- 必须加密的数据类型
- 何时使用加密以外的数据保护技术（例如哈希或令牌化）的标准

组织的最高管理级别，例如 CIO、CTO 和 CISO，通常会定义和批准加密策略。

创建加密策略时，请注意以下事项：

- 您的业务范围决定了您需要遵守的合规和监管制度。这些制度规定了数据加密要求。管理层将业务扩展到新地区或扩大产品供应的决策可能会影响适用于您的数据的法规。例如，如果银行决定向其客户提供信用卡，则他们可能需要遵守[支付卡行业数据安全标准 \(PCI-DSS\)](#)，该标准要求数据加密。
- 您的策略应指定需要加密的数据类型。这因企业的合规性要求和数据处理目标而异。例如，您的政策可能规定，企业捕获或拥有的任何数据都必须静态加密。

- 您的加密策略必须符合您的内部数据分类标准。要制定有效的加密策略，需要在元数据级别确定数据类别。例如，您的类别可能包括公共数据、内部数据、机密数据、机密数据或客户数据。
- 包括如何确定哪些数据应加密以及哪些数据应使用另一种技术（例如令牌化或哈希）保护的标准。例如，您的策略可能会规定审计、跟踪或应用程序日志中的任何个人身份信息 (PII) 都必须进行标记化。

加密标准

标准源于您的政策。它们的范围较窄，有助于定义实施的框架和架构。例如，如果贵组织的政策是加密静态数据，则标准将定义所需的加密类型，并提供有关如何遵守该策略的一般指导。

加密标准通常规定以下内容：

- 应使用的加密类型
- 加密密钥的最低规格
- 谁有权访问加密密钥
- 应将加密密钥存储在哪里
- 选择加密或哈希技术时选择适当密钥强度的标准
- 密钥轮换频率

尽管您很少需要更新加密策略，但加密标准可能会发生变化。网络安全行业不断发展，以应对不断变化的威胁格局。因此，您的标准应更改以采用最新的技术和最佳实践，以便为您的企业数据提供最佳保护。

在企业组织中，副总裁、主管或数据管理员通常定义加密标准，合规官员通常会审查和批准这些标准。

在组织中定义和维护加密标准时，请考虑以下几类因素：

- [成本和性能注意事项](#)
- [密钥访问](#)
- [加密类型](#)
- [加密密钥规范](#)
- [密钥存储位置](#)

成本和性能注意事项

在确定静态数据的加密标准时，请考虑以下操作因素：

- 可用的硬件资源必须能够大规模支持您的标准。
- 加密成本因密钥长度、数据量和执行加密所需的时间而异。例如，与对称加密相比，非对称加密使用更长的密钥并花费更多时间。
- 考虑企业应用程序的性能要求。如果您的应用程序需要低延迟和高吞吐量，则可能需要使用对称加密。

密钥访问

根据最小权限原则确定加密密钥的访问控制策略。最低权限是授予用户执行工作职能所需的最低访问权限的安全最佳实践。在您的标准中，定义一个访问控制策略，该策略：

- 确定管理密钥加密密钥和数据密钥的角色。
- 定义密钥权限并将其映射到角色。例如，它定义了谁拥有密钥管理员权限以及谁拥有密钥用户权限。密钥管理员可以创建或修改密钥加密密钥，密钥用户可以加密和解密数据并生成数据密钥。

加密类型

在您的标准中，定义哪些加密类型和功能适合您的组织：

- 记录何时使用对称加密算法。有关更多信息，请参阅常见问题解答部分[我什么时候需要非对称加密？](#)中的[我什么时候需要对称加密？](#)和。
- 决定是否应使用信封加密，并定义具体情况。有关更多信息，请参阅常见[我什么时候需要信封加密？](#)问题解答部分。
- 定义何时使用加密替代方案（例如令牌化和哈希）的标准。

加密密钥规范

为您的加密密钥定义所需的规范，例如密钥强度和算法。这些规范必须符合政策中定义的监管和合规制度。考虑定义以下规范：

- 为对称和非对称加密类型定义最低密钥强度和算法。关键优势因素包括长度、随机性和唯一性。

- 定义何时要实现新版本的加密算法。例如，您的标准可能会声明“在发布后 30 天内实施最新版本的算法”或“始终使用比最新版本早一个版本”。
- 定义轮换加密密钥的间隔。

密钥存储位置

在您的标准中，在决定将加密密钥存储在何处时，请考虑以下几点：

- 合规性和监管要求可能会决定您的加密密钥可以存储在何处。
- 决定是要将密钥存储在集中位置还是与相应的数据一起存储。有关更多信息，请参阅常见[为什么要集中管理加密密钥？](#)问题解答部分。
- 如果您选择集中存储，请决定是将密钥存储在企业管理的基础架构（例如硬件安全模块 (HSM)）中，还是将密钥存储在托管服务提供商（例如）中AWS Key Management Service。有关更多信息，请参阅常见[何时需要使用硬件安全模块 \(HSM\)？](#)问题解答部分。

加密框架

在这种情况下，框架是指修改加密标准或策略时需要遵循的一组标准操作程序。框架是帮助您实施标准的脚手架。它有助于将言语转化为行动。该框架将定义标准的人员与实施标准的人联系起来。

框架通常包括以下主题：

- [数据分类](#)
- [环境分类](#)
- [变更事件和流程](#)

数据分类

数据分类在创建加密策略中起着至关重要的作用。数据分类是指根据数据的敏感度将数据分配给某个类别的过程。以下是常见的数据分类类别，按敏感度递增顺序排列：公开、私有、内部、机密和受限。

您的加密框架应包括以下有关数据分类的信息：

- 企业的分类类别。
- 用于将数据分类为相应类别的分类标准。例如，公司的交易秘诀可以归类为受限，员工个人身份信息可以是机密的，员工之间通过官方渠道进行的内部沟通可能是内部的。

- 该过程用于在类别之间提升和降级数据。
- 每个数据分类类别的访问标准。
- 每个类别所需的加密密钥类型。

环境分类

您的企业可能有多个环境，如开发、测试、沙盒、预生产和生产。每个环境可以包含不同类型的数据，并且有不同的加密要求。

加密框架应包含有关环境的以下信息：

- 定义您的企业环境。
- 为每个环境定义加密要求。例如，您可以对开发环境中的所有数据类别使用单个加密密钥，而在生产环境中，您可以为每个业务应用程序或数据分类类别使用不同的加密密钥。

变更事件和流程

加密标准经常发生变化，因此您可以跟上最新的技术、最佳实践和创新。以下是可能引发加密标准修订的常见变更事件：

- 加密密钥最小长度的变化
- 加密算法强度的变化
- 更改谁可以访问加密密钥或如何访问加密密钥
- 更改按键的旋转间隔
- 密钥删除流程的更改
- 密钥存储位置或策略的更改
- 更改备份和还原密钥的流程

您的加密框架应包括以下内容，以帮助您的组织做好管理、实施和传达加密标准或策略变更的准备：

- 变更控制流程-此过程的目的是为即将到来的变更做好计划和准备。当您需要更改加密标准或策略时，这个可重复且可扩展的过程旨在定义：
 - 您的组织如何评估更改的影响
 - 谁可以发起更改
 - 谁负责实施变更

- 谁负责批准变更
- 如有必要，您的组织将如何撤消变更
- 变更可审计性和可追溯性流程 — 此流程定义了您的组织如何在元数据级别和数据级别上审计和跟踪变更。它应该定义如何保存和访问以下记录：
 - 什么改变了
 - 当它被改变的时候
 - 谁发起、批准和实施了变更

例如，如果您的组织更改了最低加密密钥强度，则您应该能够确定原始要求和新要求、更改何时生效以及谁参与了变更过程。

- 变更发布流程 — 此流程的目的是定义您的组织在您决定进行变更后如何实施变更。此过程定义了：
 - 谁是利益相关者
 - 您是应该完成试点还是概念验证
 - 您应该如何以及何时传达变更状态
 - 如有必要，如何撤消更改。
 - 实施变更后的观察期应该是多少。
 - 监测变更影响的观察过程将是什么，包括如何收集有关变更的反馈和评估有效性
- 报废流程 — 此流程的目的是定义您的组织如何处理与加密相关的资源和信息的报废。它包括有关实际退休的说明以及退休的沟通流程。

实现

在此策略中，架构是指您的加密标准的技术实现。本部分包含有关如何AWS 服务帮助您根据策略和[AWS CloudHSM](#)标准实施 data-at-rest 加密策略的信息，例如 [AWS Key Management Service\(AWS KMS\)](#) 和。

AWS KMS是一项托管服务，可以帮助您创建和控制用于保护数据的加密密钥。这些 KMS 密钥绝不会让该服务处于未加密状态。要使用或管理您的 KMS 密钥，您需要与之交互AWS KMS，并且许多密钥AWS 服务都与之集成AWS KMS。

AWS CloudHSM是一项加密服务，用于在您的AWS环境中创建和维护硬件安全模块 (HSM)。HSM 是处理加密操作并为加密密钥提供安全存储的计算设备。如果你的标准要求你使用 FIPS 140-2 3 级验证的硬件，或者如果你的标准要求使用行业标准的 API，例如 PKCS #11、Java 加密扩展 (JCE) 和微软 CryptonG (CNG)，那么你可以考虑使用AWS CloudHSM。

您可以将配置AWS CloudHSM为的自定义密钥库AWS KMS。该解决方案将的便利性和服务集成AWS KMS与在您的集群中使用AWS CloudHSM集群所带来的额外控制和合规性优势相结合AWS 账户。有关更多信息，请参阅[自定义密钥库](#) (AWS KMS文档)。

本文档从较高的层面讨论了AWS KMS功能，并解释了AWS KMS如何满足您的政策和标准。

成本、便利性和控制

AWS KMS提供不同类型的密钥。有些由客户拥有或管理AWS，而另一些则由客户创建和管理。您可以根据自己想要对密钥和成本考虑因素的控制级别在这些选项之间进行选择：

- **AWS拥有的密钥** — AWS 拥有和管理这些密钥，它们用于多个密钥AWS 账户。有些AWS 服务支持AWS自有密钥。您可以免费使用这些密钥。这种密钥类型使您免于管理密钥生命周期和密钥访问的成本和管理开销。有关此类密钥的更多信息，请参阅[AWS自有密钥](#) (AWS KMS文档)。
- **AWS托管密钥** — 如果与集成AWS KMS，AWS 服务则它可以代表您创建、管理和使用此类密钥，以保护您在该服务中的资源。这些密钥是在您的中创建的AWS 账户，AWS 服务只能使用。AWS托管密钥没有月度费用。超出免费套餐的使用量可能会收取费用，但有些可以为您AWS 服务支付这些费用。您可以使用身份策略来控制这些密钥的查看和审计访问权限，但可以AWS管理密钥生命周期。有关此类密钥的更多信息，请参阅[AWS托管密钥](#) (AWS KMS文档)。有关与集成的完整列表AWS 服务AWS KMS，请参阅[AWS 服务集成](#) (AWS营销)。
- **客户管理的密钥** — 您可以创建、拥有和管理此类密钥，并且可以完全控制密钥生命周期。为实现职责分离，您可以使用基于身份的策略来控制对密钥的访问。您还可设置自动[轮换的密钥](#)。客户托管密钥会产生月费用，如果您超过免费套餐，还会产生使用费用。有关此类密钥的更多信息，请参阅[客户管理的密钥](#) (AWS KMS文档)。

有关密钥存储和使用的更多信息，请参阅[AWS Key Management Service定价](#) (AWS营销)。

性能和加密类型

根据标准中选择的加密类型，您可以使用两种类型的 KMS 密钥。

- **对称** — 所有AWS KMS key类型都支持对称加密。加密客户管理的密钥时，您可以使用单强度密钥对 AES-256-GCM 进行加密和解密。
- **非对称** — 客户管理的密钥支持非对称加密。您可以根据自己的预期用途在不同的关键优势和算法之间进行选择。非对称密钥可以使用 RSA 进行加密和解密，也可以使用 RSA 或 ECC 签署和验证操作。非对称密钥算法本质上提供了角色分离并简化了密钥管理。使用非对称加密时AWS KMS，不支持某些操作，例如轮换密钥和导入外部密钥材料。

有关对称和非对称密钥支持的AWS KMS操作的更多信息，请参阅[密钥类型参考](#)（AWS KMS文档）。

信封加密

内置信封加密AWS KMS。在中AWS KMS，您可以生成纯文本或加密格式的数据密钥。加密数据密钥使用KMS密钥加密。您可以将KMS密钥存储在AWS CloudHSM集群的自定义密钥存储中。有关信封加密优势的更多信息，请参阅[关于信封加密](#)。

密钥存储位置

您可以使用策略来管理对AWS KMS资源的访问。策略用于描述谁可以访问什么资源。附加到AWS Identity and Access Management (IAM) 委托人的策略称为基于身份的策略或IAM策略。附加到其他类型资源的策略称为资源策略。AWS KMS的资源策略AWS KMS keys称为密钥策略。每个KMS密钥都有密钥策略。

密钥策略可以灵活地将加密密钥存储在中心位置或以分布式方式将其存储在离数据更近的地方。在决定将KMS密钥存储在何处时，请考虑以下AWS KMS功能AWS账户：

- 单区域基础设施支持 — 默认情况下，KMS密钥是特定区域的，它们永远不会处于AWS KMS未加密状态。如果您的标准对控制特定地理位置的密钥有严格要求，请使用单区域密钥进行探索。
- 多区域基础设施支持-AWS KMS还支持称为多区域密钥的特殊用途密钥类型。将数据分成多个存储AWS区域是灾难恢复的常见配置。通过使用多区域密钥，您可以在区域之间传输数据而无需对其进行重新加密，并且可以像在每个区域中拥有相同的密钥一样管理数据。如果您的标准要求您的加密基础设施在主动-主动配置中跨越多个区域，则此功能非常有用。有关更多信息，请参阅[多区域密钥](#)（AWS KMS文档）。
- 集中管理-如果您的标准要求您将密钥存储在集中位置，则可以使用AWS KMS将所有加密密钥存储在单个位置AWS账户。您可以使用密钥策略向其他应用程序授予访问权限，这些应用程序可以位于同一区域的不同账户中。集中式密钥管理可以减少管理密钥生命周期和密钥访问控制的管理开销。
- 外部密钥材料-您可以将外部生成的密钥材料导入AWS KMS。单区域和多区域对称密钥Support此功能。由于对称密钥的材料是在外部生成的，因此您有责任保护生成的密钥材料。有关更多信息，请参阅[导入的密钥材料](#)（AWS KMS文档）。

访问控制

在中AWS KMS，您可以使用以下策略机制实施精细级别的访问控制：[密钥策略](#)、[IAM策略](#)和[授权](#)。使用这些控件，您可以根据角色设置职责分工，例如管理员、可以加密数据的密钥用户、可以解密数据的密钥用户以及可以加密和解密数据的密钥用户。有关更多信息，请参阅[身份验证和访问控制](#)（AWS KMS文档）。

审计和日志记录

AWS KMS与AWS CloudTrail Amazon 集成 EventBridge ，用于记录和监控。所有AWS KMS API 操作都记录在 CloudTrail 日志中并可审计。您可以使用 Amazon CloudWatch EventBridge、和AWS Lambda设置自定义监控解决方案来配置通知和自动修复。有关更多信息，请参阅[记录和监控](#) (AWS KMS文档)。

常见问题

本节提供了在定义加密标准或在实施阶段创建加密基础架构时常见问题的答案。

我什么时候需要对称加密？

在以下情况下，您可以使用对称加密：

- 速度、成本和更低的计算开销是当务之急。
- 需要加密大量数据。
- 加密的数据不会离开组织网络的边界。

我什么时候需要非对称加密？

在以下情况下，您可以使用非对称加密：

- 您需要在组织外部共享数据。
- 法规或治理禁止共享密钥。
- 需要使用不可否认性。（不可否认性可防止用户拒绝先前的承诺或行动。）
- 您需要根据组织角色严格隔离对加密密钥的访问权限。

我什么时候需要信封加密？

如果您的加密策略需要密钥轮换，则需要支持和实施信封加密。某些治理和合规制度要求密钥轮换，或者您的策略可能会强制轮换密钥以满足业务需求。

何时需要使用硬件安全模块 (HSM)？

如果您的策略规定符合以下条件，则可能需要使用 HSM：

- 联邦信息处理标准 (FIPS) 140-2 3 级加密标准 有关更多信息，请参阅 [FIPS 验证](#) (AWS CloudHSM 文档)。
- 行业标准 API，例如 PKCS #11、Java 密码学扩展 (JCE) 或微软密码学 API：下一代 (CNG)

为什么要集中管理加密密钥？

以下是集中式密钥管理的常见好处：

- 由于密钥在不同的位置使用和管理，因此您可以重复使用密钥，这样可以降低成本。
- 您可以更好地控制加密密钥的访问权限。
- 将密钥存储在单一位置可以更轻松地在标准发生变化时查看、审计和更新密钥。

我是否需要为静态数据使用专门构建的加密基础架构？

如果满足以下任一条件，业务需要加密基础架构：

- 您的企业处理和存储除公共以外的任何分类的数据。
- 您的企业捕获和存储有关员工或客户的数据。
- 您的企业处理 PII 数据。
- 您的企业必须遵守要求对数据进行加密的监管或治理制度。
- 您的企业管理层已强制对所有静态数据进行加密。

如何AWS KMS帮助我的组织实现静态数据的加密目标？

除了许多其他功能外，AWS Key Management Service还可以帮助您：

- 使用信封加密。
- 控制加密密钥的访问，例如将密钥管理与密钥使用分开。
- 在多个AWS 区域和之间共享密钥AWS 账户。
- 集中管理密钥。
- 自动执行并强制密钥轮换。

资源

AWS 服务 文档

- [AWS KMS加密细节](#)
- [AWS KMS 开发人员指南](#)
 - [AWS KMS 概念](#)
 - [特殊用途按键](#)
 - [身份验证和访问控制AWS KMS](#)
 - [的安全AWS KMS](#)
 - [如何AWS 服务使用AWS KMS](#)
- [AWS CloudHSM 用户指南](#)
- [AWS加密服务和工具指南](#)
 - [如何选择加密工具或服务](#)
 - [密码学概念](#)

AWS营销

- [AWS KMS 定价](#)
- [AWS KMS与其他整合AWS 服务](#)

AWSWell-Architected

- [保护传输中的数据](#)
- [保护静态数据](#)

哈希和标记化

- [如何使用标记化来提高数据安全性并缩小审计范围](#) (AWS博客文章)
- [对使用经批准的哈希算法的应用程序的建议](#) (NIST 出版物)

视频

- [加密的工作原理AWS](#)
- [保护您的区块存储AWS](#)
- [通过以下方式实现安全目标AWS CloudHSM](#)
- [实现的最佳实践AWS Key Management Service](#)
- [深入探讨AWS加密服务](#)

文档历史记录

下表描述了本指南的重大更改。如果您想收到有关future 更新的通知，可以订阅 [RSS feed](#)。

变更	说明	日期
首次出版	—	2022 年 9 月 15 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：将您的本地 Oracle 数据库迁移到兼容 Amazon Aurora PostgreSQL 的版本。
- **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：在中将您的本地 Oracle 数据库迁移到适用于 Oracle 的亚马逊关系数据库服务 (Amazon RDS) AWS Cloud。
- **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：将您的客户关系管理 (CRM) 系统迁移到 Salesforce.com。
- **更换主机 (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：在中的 EC2 实例上将您的本地 Oracle 数据库迁移到 Oracle AWS Cloud。
- **重新定位 (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。您可以将服务器从本地平台迁移到同一平台的云服务。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

参见[托管服务](#)。

酸

参见[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。与[主动-被动迁移](#)相比，它更灵活，但需要更多的工作。

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

一个 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

参见[人工智能](#)。

AIOps

参见[人工智能操作](#)。

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？](#)

人工智能运营 (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 AWS 迁移策略中使用 AIOps 的更多信息，请参阅[运营集成指南](#)。

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 (IAM) 文档 [AWS 中的 AB AC](#)。

权威数据源

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

坏机器人

旨在破坏个人或组织或对其造成伤害的[机器人](#)。

BCP

参见[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。另请参见[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的应用程序版本（蓝色），在另一个环境中运行新的应用程序版本（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互动的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的网络爬虫。其他一些被称为恶意机器人的机器人旨在破坏个人或组织或对其造成伤害。

僵尸网络

被[恶意软件](#)感染并受单方（称为[机器人](#)牧民或机器人操作员）控制的机器人网络。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）。

破碎的玻璃通道

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 [Well -Architected 指南](#) 中的“[实施破碎玻璃程序](#)”指示 AWS 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

参见[AWS 云采用框架](#)。

金丝雀部署

向最终用户缓慢而渐进地发布版本。当你有信心时，你可以部署新版本并全部替换当前版本。

CCoE

参见[云卓越中心](#)。

CDC

参见[变更数据捕获](#)。

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弹性。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

查看[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 Cloud 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。云计算通常与[边缘计算](#)技术相关。

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

组织迁移到以下阶段时通常会经历四个阶段 AWS Cloud：

- 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，创建登录区、定义 CCoE、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 Cloud 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

参见 [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 AWS CodeCommit。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 管道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)

[人工智能](#) 领域，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，AWS Panorama 提供将 CV 添加到本地摄像机网络的设备，而 Amazon 则为 CV SageMaker 提供图像处理算法。

配置偏差

对于工作负载，配置会从预期状态发生变化。这可能会导致工作负载变得不合规，而且通常是渐进的，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、提高工作效率、改善代码质量并加快交付速度。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

参见[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-Architected 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 Cloud 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

参见[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。

委托管理员

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。此帐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

参见[环境](#)。

侦测性控制

一种安全控制，在事件发生后进行检测、记录日志和发出警报。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

在[星型架构](#)中，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)

您用来最大限度地减少[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 Framework AWS work 中的[“工作负载灾难恢复：云端 AWS 恢复”](#)。

DML

参见[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

参见[灾难恢复](#)。

漂移检测

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

参见[开发价值流映射](#)。

E

EDA

参见[探索性数据分析](#)。

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](#)相比，边缘计算可以减少通信延迟并缩短响应时间。

加密

一种将人类可读的纯文本数据转换为密文的计算过程。

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

参见[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](#)。

environment

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

参见[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

[星形架构](#)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。

失败得很快

一种使用频繁和增量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 Cloud，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

参见[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[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。

FGAC

请参阅[精细的访问控制](#)。

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，它使用连续的数据复制，通过[更改数据捕获](#)在尽可能短的时间内迁移数据，而不是使用分阶段的方法。目标是将停机时间降至最低。

G

地理封锁

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，而[基于主干的工作流程](#)是现代的首选方法。

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

一种高级规则，用于跨组织单位 (OU) 管理资源、策略和合规性。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。侦测性防护机制会检测策略违规和合规性问题，并生成警报以进行修复。它们通过使用 AWS Config、Amazon、AWS Security Hub GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

H

HA

参见[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。

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。

|

laC

参见[基础架构即代码](#)。

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 Cloud 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。

IloT

参见[工业物联网](#)。

不可变的基础架构

一种为生产工作负载部署新基础架构，而不是更新、修补或修改现有基础架构的模型。[不可变基础架构本质上比可变基础架构更一致、更可靠、更可预测](#)。有关更多信息，请参阅 Well-Architected Framework 中的[使用不可变基础架构 AWS 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](#)建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与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[克劳斯·施瓦布 \(Klaus Schwab \)](#)于2016年推出，指的是通过连接、实时数据、自动化、分析和人工智能/机器学习的进步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置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 (IloT)

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 \(IloT \) 数字化转型策略](#)。

检查 VPC

在 AWS 多账户架构中，一种集中式 VPC，用于管理 VPC（相同或不同 AWS 区域）、互联网和本地网络之间的网络流量检查。[AWS 安全参考架构](#)建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与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 AWS 实现机器学习模型的可解释性](#)。

IoT

参见[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](#)。

大规模迁移

迁移 300 台或更多服务器。

LBAC

参见[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

见 [7 R](#)。

小端序系统

一个先存储最低有效字节的系统。另请参见[字节顺序](#)。

下层环境

参见[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

参见[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。恶意软件的示例包括病毒、蠕虫、勒索软件、特洛伊木马、间谍软件和键盘记录器。

托管服务

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。亚马逊简单存储服务 (Amazon S3) Service 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、记录和控制车间将原材料转化为成品的生产过程。

MAP

参见[迁移加速计划](#)。

机制

一个完整的过程，在此过程中，您可以创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运行过程中自我增强和改进的循环。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

参见[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

一种小型独立服务，通过明确定义的 API 进行通信，通常由小型独立团队拥有。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 API 通过明确定义的接口进行通信。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 DevOps 人员和冲刺专业人员。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，可提供信息，用于验证迁移到的业务案例。AWS Cloud 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

用于将工作负载迁移到的方法 AWS Cloud。有关更多信息，请参阅此词汇表中的 [7 R](#) 条目和[动员组织以加快大规模迁移](#)。

ML

参见[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[中的应用程序现代化策略](#)。AWS Cloud

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[中的评估应用程序的现代化准备情况](#) AWS Cloud。

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

参见[迁移组合评估](#)。

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？”

可变基础架构

一种用于更新和修改现有生产工作负载基础架构的模型。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[源站访问控制](#)。

OAI

参见[源访问身份](#)。

OCM

参见[组织变更管理](#)。

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

参见[运营集成](#)。

OLA

参见[运营层协议](#)。

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

参见[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)

一份问题清单和相关的最佳实践，可帮助您理解、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 Well-Architecte AWS d Frame [work 中的运营准备情况评估 \(ORR\)](#)。

操作技术 (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 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。

或者

参见[运营准备情况审查](#)。

OT

参见[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](#)建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与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

查看[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

参见[可编程逻辑控制器](#)。

PLM

参见[产品生命周期管理](#)。

策略

一个对象，可以在中定义权限（参见[基于身份的策略](#)）、指定访问条件（参见[基于资源的策略](#)）或定义组织中所有账户的最大权限 AWS Organizations（参见[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。有关更多信息，请参阅[在微服务中实现数据持久性](#)。

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或的查询条件false，通常位于子WHERE句中。

谓词下推

一种数据库查询优化技术，可在传输前筛选查询中的数据。这减少了必须从关系数据库检索和处理的数据量，并提高了查询性能。

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

一种贯穿整个工程化过程考虑隐私的系统工程方法。

私有托管区

私有托管区就是一个容器，其中包含的信息说明您希望 Amazon Route 53 如何响应一个或多个 VPC 中的某个域及其子域的 DNS 查询。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](#)措施，旨在防止部署不合规的资源。这些控件会在资源置备之前对其进行扫描。如果资源与控件不兼容，则不会对其进行配置。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)

在产品的整个生命周期中，从设计、开发和上市，到成长和成熟，再到衰落和移除，对产品进行数据和流程的管理。

生产环境

参见[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。

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。

发布/订阅 (发布/订阅)

一种支持微服务间异步通信的模式，以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

一系列步骤，例如指令，用于访问 SQL 关系数据库系统中的数据。

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

参见“[负责任、负责、咨询、知情](#)” (RACI)。

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

参见“[负责任、负责、咨询、知情](#)” (RACI)。

RCAC

请参阅[行和列访问控制](#)。

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。

重新架构师

见 [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

见 [7 R](#)。

区域

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

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

见 [7 R](#)。

版本

在部署过程中，推动生产环境变更的行为。

搬迁

见 [7 R](#)。

更换平台

见 [7 R](#)。

回购

见 [7 R](#)。

故障恢复能力

应用程序抵御中断或从中断中恢复的能力。在中规划弹性时，[高可用性](#)和[灾难恢复](#)是常见的考虑因素。AWS Cloud有关更多信息，请参阅[AWS Cloud 弹性](#)。

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

见 [7 R](#)。

退休

见 [7 R](#)。

旋转

定期更新[密钥](#)以使攻击者更难访问凭据的过程。

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

参见[恢复点目标](#)。

RTO

参见[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 Management Console 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

参见[监督控制和数据采集](#)。

SCP

参见[服务控制政策](#)。

secret

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 密钥中有什么？](#) 在 Secrets Manager 文档中。

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。安全控制主要有四种类型：[预防性](#)、[侦测](#)、[响应式](#)和[主动式](#)。

安全加固

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

一种预定义和编程的操作，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 实例或轮换证书。

服务器端加密

在目的地对数据进行加密，由接收数据 AWS 服务的人加密。

服务控制策略 (SCP)

一种策略，用于集中控制 AWS Organizations 的组织中所有账户的权限。SCP 为管理员可以委托给用户或角色的操作定义了防护机制或设定了限制。您可以将 SCP 用作允许列表或拒绝列表，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。

服务级别指示器 (SLI)

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 (SLO)

代表服务运行状况的目标指标，由服务[级别指标](#)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](#)。

暹粒

参见[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

参见[服务级别协议](#)。

SLI

参见[服务级别指标](#)。

SLO

参见[服务级别目标](#)。

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[中的分阶段实现应用程序现代化的方法](#)。 [AWS Cloud](#)

恶作剧

参见[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交易数据或测量数据，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。

监控和数据采集 (SCADA)

在制造业中，一种使用硬件和软件来监控有形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 ynthetic](#) 来创建这些测试。

T

标签

键值对，充当用于组织资源的元数据。AWS 标签可帮助您管理、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

参见[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

中转网关是网络中转中心，您可用它来互连 VPC 和本地网络。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，该服务可以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

参见[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

两个 VPC 之间的连接，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

一个 SQL 函数，用于对一组以某种方式与当前记录相关的行进行计算。窗口函数对于处理任务很有用，例如计算移动平均线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。

蠕虫

参见 [一次写入，多读](#)。

WQF

请参阅 [AWS 工作负载资格框架](#)。

一次写入，多次读取 (WORM)

一种存储模型，它可以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，但他们无法对其进行更改。这种数据存储基础架构被认为是 [不可变的](#)。

Z

零日漏洞利用

一种利用未修补 [漏洞](#) 的攻击，通常是恶意软件。

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。

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。