的加密最佳实践和功能 AWS 服务

AWS 规范性指导

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 规范性指导: 的加密最佳实践和功能 AWS 服务

Copyright © 2025 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
目标受众 1
算法和 AWS 服务 3
AWS 密码学服务 3
加密算法 3
一般加密最佳实践 7
数据分类 7
传输中数据加密 7
静态数据加密 8
AWS 服务的加密最佳实践 9
AWS CloudTrail 9
Amazon DynamoDB 10
亚马逊 EC2 和亚马逊 EBS 11
Amazon ECR 12
Amazon ECS 13
Amazon EFS 14
Amazon EKS 15
AWS Encryption SDK 16
AWS KMS 17
AWS Lambda 19
Amazon RDS 20
AWS Secrets Manager 21
Amazon S3 22
Amazon VPC 23
资源 25
文档历史记录 26
术语表 27
..... 27
A 27
B 30
C 31
D 34
E 37
F 39

G 40
H 41
我 42
L 44
M 45
O 49
P 51
Q 53
R 54
S 56
T 59
U 60
V 61
W 61
Z 62
..... lxiii

AWS 服务的加密最佳实践和功能

Kurt Kumar，亚马逊 Web Services

2025 年 6 月（文档历史记录）

加密是在数字时代保护敏感数据的基本网络安全工具。随着组织越来越依赖数据来推动其运营，包括生成式人工智能部署，通过强大的加密实践来保护这些有价值的信息已成为全面数据保护策略的重要组成部分。本指南可以帮助您了解加密原理和所 AWS 提供的加密功能。

现代网络安全威胁包括数据泄露的风险，即未经授权访问您的信息资产会导致数据丢失。数据是一种业务资产，对每个组织来说都是独一无二的。它可以包括客户信息、业务计划、设计文档或代码。保护业务意味着保护其数据。

即使发生泄露事件，数据加密也可以帮助保护您的业务数据。它为防止意外泄露提供了一层防御。要访问 AWS 云中的加密数据，用户需要拥有使用密钥解密的权限，以及使用数据所在的服务的权限。如果没有这两个权限，用户就无法解密和查看数据。

通常，您可以加密三种类型的数据。传输中数据是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。静态数据是静止和休眠的数据，例如存储中的数据。例如，块存储、对象存储、数据库、档案和物联网（IoT）设备。使用中的数据是指应用程序或服务正在积极处理或使用的数据。通过在使用时保护数据，组织可以帮助降低意外泄露的风险。

本指南讨论了加密传输中的数据和静态数据的注意事项和最佳实践。它还回顾了许多版本中可用的加密功能和控件 AWS 服务。您可以在 AWS 云 环境中的服务级别实施这些加密建议。

目标受众

本指南可供公共和私营部门的小型、中型和大型组织使用。无论您的组织处于评测和实施数据保护策略的初始阶段，还是以加强现有安全控制为目标，本指南中所列的建议都非常适合以下受众：

- 为企业制定政策的执行官，例如首席执行官 (CEOs)、首席技术官 (CTOs)、首席信息官 (CIOs) 和首席信息安全官 (CISOs)
- 负责制定技术标准的技术官员，如技术副总裁和总监
- 业务利益相关者和应用程序所有者，他们负责：
  - 评估风险状况、数据分类和保护要求
  - 监控对既定组织标准的遵守情况

- 负责监督合规政策（包括法定和自愿合规制度）遵守情况的合规、内部审计和治理官员

密码算法和 AWS 服务

加密算法是将纯文本消息转换为加密文字的公式或过程。如果您不熟悉加密或其术语，我们建议您在继续阅读本指南之前先阅读关于数据加密。

AWS 密码学服务

AWS 加密服务依赖于安全的开源加密算法。这些算法经过公共标准机构和学术研究机构审查。一些 AWS 工具和服务强制使用特定算法。在其他服务中，您可以在多种可用算法和密钥长度之间进行选择，也可以使用推荐的默认值。

本节介绍 AWS 工具和服务支持的一些算法。根据密钥的功能，它们分为对称和非对称两类：

- 对称加密使用相同的密钥来加密和解密数据。 AWS 服务 支持高级加密标准 (AES) 和三重数据加密标准（3DES 或 TDES），这是两种广泛使用的对称算法。
- 非对称加密使用一对密钥，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，但应严格限制对私钥的访问。 AWS 服务 通常支持 RSA 和椭圆曲线加密 (ECC) 非对称算法。

AWS 加密服务符合各种加密安全标准，因此您可以遵守政府或专业法规。有关 AWS 服务 符合的数据安全标准的完整列表，请参阅AWS 合规性计划。

加密算法

密码学是安全的重要组成部分。 AWS AWS 服务 支持对传输中、静态或内存中的数据进行加密。许多还支持使用无法访问的客户托管密钥进行 AWS加密。您可以在AWS 数字主权 AWS 承诺（AWS 博客文章）中详细了解对创新的承诺以及对主权和加密功能的额外控制措施进行投资。

AWS 致力于使用最安全的可用加密算法来满足您的安全和性能要求。 AWS 默认使用高保障度的算法和实现，并且更喜欢速度更快、安全性更高、能效更高的硬件优化解决方案。有关经过优化、高保证、经过正式验证的恒定时间AWS 加密算法，请参阅 Crypto Lib rary。 AWS 遵循责任共担模式，并提供加密选项，以满足您的个人安全、合规和性能要求，同时仍能满足行业认可的安全级别。例如，Elastic Load Balancing 提供的应用程序负载均衡器为传输层安全 (TLS) 协议提供各种安全策略。

AWS 服务 使用符合行业标准并促进互操作性的可信加密算法。这些标准已被政府、业界和学术界广泛接受。一种算法需要全球社会的大量分析才能被广泛接受。它还需要一段时间才能在业内广泛使用。缺

乏分析和可用性会给互操作性、复杂性和部署风险带来挑战。 AWS 继续部署新的加密选项，以满足安全性和性能的高标准。

下表总结了为保护您的数据而在其服务中 AWS 部署的加密算法、密码、模式和密钥大小。不应将它们视为中所有可用加密选项的详尽列表。 AWS算法分为两类：

- 首选符合 AWS 安全和性能标准的算法。
- 为了兼容某些应用程序，可以使用可@@ 接受的算法，但不是首选。

非对称加密	状态
模量为 2048 或 3072 位的 RSA-OAEP	可接受
HPKE 带有 P-256 或 P-384、HKDF 和 AES-GCM	可接受

非对称密钥协议	状态
带有 P-384 的 ECDH (E)	首选
使用 P-256、P-521 或 X25519 的 ECDH (E)	可接受
使用 Brainpoolp256r1、brainpoolp384r1 或 brainpoolp512r1 的 ECDH (E)	可接受
ML-KEM-768 与 ECDH (E) 结合使用（在 PQ-Hybrid 密钥交换中）	首选（用于量子电阻）

分组密码和模式	状态
AES-GCM-256	首选
AES-XTS-256	可接受
AES-GCM-128	可接受

分组密码和模式	状态
ChaCha20/Poly1305	可接受
CBC/CTR/CCM 模式（使用 AES-128 或 AES-256）	可接受

哈希	状态
SHA2-384	首选
SHA2-256	可接受
SHA3	可接受

密钥推导	状态
HKDF_expand 或者用 -256 的 HKDF SHA2	首选
带有 HMAC 的计数器模式 KDF--256 SHA2	可接受

钥匙包装	状态
AES-GCM-256	首选
带有 256 位密钥的 AES-KW 或 AES-KWP	可接受

消息验证码 (MAC)	状态
HMAC--384 SHA2	首选
HMAC--256 SHA2	可接受
KMAC	可接受

密码哈希	状态
用 scrypt SHA384	首选
PBKDF2	可接受

Signatures	状态
带 P-384 的 ECDSA	首选
带有 P-256、P-521 或 Ed25519 的 ECDSA	可接受
RSA-2048 或 RSA-3072	可接受
SLH-DSA	首选（用于抗量子签名） software/firmware

AWS 密切跟踪密码学的发展、安全问题和研究结果。当发现不推荐使用的算法和安全问题后，这些问题就会得到解决。有关更多信息，请参阅AWS 安全博客。 AWS 继续致力于识别与使用传统安全算法的客户的兼容性问题，并帮助客户迁移到更安全的选项。 AWS 还继续参与新的密码学领域，包括后量子密码学和密码计算。

一般加密最佳实践

本节提供了在中加密数据时适用的建议。 AWS 云这些一般加密最佳做法并非特定于 AWS 服务。本节包括以下主题：

- 数据分类
- 传输中数据加密
- 静态数据加密

数据分类

数据分类是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 Wel l-Architecte AWS d Framework 中安全支柱的一个组成部分。类别可能包括高度机密、机密、非机密和公开，但是分类层及其名称可能因组织而异。有关数据分类过程、注意事项和模型的更多信息，请参阅数据分类（AWS 白皮书）。

对数据进行分类后，您可以根据每个类别所需的保护级别为组织创建加密策略。例如，您的组织可能决定高度机密的数据应使用非对称加密，而公共数据不需要加密。有关设计加密策略的更多信息，请参阅 Creating an enterprise encryption strategy for data at rest。尽管该指南中的技术注意事项和建议特定于静态数据，但您也可以使用分阶段方法为传输中数据创建加密策略。

传输中数据加密

通过 AWS 全球网络之间 AWS 区域 传输的所有数据在离开 AWS 安全设施之前都会在物理层自动加密。可用区之间的所有流量都是加密的。

以下是对 AWS 云中传输中数据进行加密的一般最佳实践：

- 根据您的数据分类、组织要求以及任何适用的监管或合规标准，为传输中数据定义组织加密策略。我们强烈建议您对归类为高度机密或机密的传输中数据进行加密。您的策略还可能根据需要指定其他类别的加密，例如，非机密或公共数据。
- 对传输中数据进行加密时，我们建议使用批准的加密算法、数据块密码模式和密钥长度，如加密策略中定义。
- 使用以下方法之一对企业网络和 AWS 云 基础架构内的信息资产和系统之间的流量进行加密：
  - AWS Site-to-Site VPN 连接

  - AWS Site-to-Site VPN 和AWS Direct Connect连接的组合，提供 IPsec加密的私有连接
  - AWS Direct Connect 支持 MAC Security (MACsec) 的连接，用于加密从公司网络到该 AWS Direct Connect 地点的数据
- 根据最低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其工作职能所需的最低访问权限的安全最佳实践。有关应用最低权限的更多信息，请参阅 Security best practices in IAM 和 Best practices for IAM policies。

静态数据加密

所有 AWS 数据存储服务，例如亚马逊简单存储服务 (Amazon S3) 和亚马逊弹性文件系统 (Amazon EFS)，都提供加密静态数据的选项。使用 256 位高级加密标准 (AES-256) 分组 AWS 密码和加密服务执行加密，例如 () 或。AWS Key Management ServiceAWS KMSAWS CloudHSM

您可以根据数据分类、加密需求或阻止您使用加密的技术限制等因素，使用 end-to-end客户端 end-to-end加密或服务器端加密来加密数据：

- 客户端加密是在目标应用程序或服务接收数据之前对数据进行本地加密的行为。 AWS 服务 接收加密数据，但不会影响对其加密或解密。对于客户端加密，您可以使用 AWS KMS、AWS Encryption SDK 或其他第三方加密工具或服务。
- 服务器端加密是由接收数据的应用程序或服务在目标位置对数据进行加密的行为。对于服务器端加密，您可以使用 AWS KMS 加密整个存储块。您还可以使用其他第三方加密工具或服务，如 LUKS，在操作系统（OS）级别对 Linux 文件系统进行加密。

以下是对 AWS 云中静态数据进行加密的一般最佳实践：

- 根据您的数据分类、组织要求以及任何适用的监管或合规标准，为静态数据定义组织加密策略。有关详细信息，请参阅Creating an enterprise encryption strategy for data at rest。我们强烈建议您对归类为高度机密或机密的静态数据进行加密。您的策略还可能根据需要指定其他类别的加密，例如，非机密或公共数据。
- 对静态数据进行加密时，我们建议使用批准的加密算法、数据块密码模式和密钥长度。
- 根据最低权限原则确定加密密钥的访问控制策略。

AWS 服务的加密最佳实践

本节包括以下方面的最佳实践和建议 AWS 服务：

- AWS CloudTrail
- Amazon DynamoDB
- 亚马逊弹性计算云（亚马逊 EC2）和亚马逊弹性区块存储（亚马逊 EBS）
- Amazon Elastic Container Registry（Amazon ECR）
- Amazon Elastic Container Service（Amazon ECS）
- Amazon Elastic File System（Amazon EFS）
- Amazon Elastic Kubernetes Service（Amazon EKS）
- AWS Encryption SDK
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- Amazon Relational Database Service（Amazon RDS）
- AWS Secrets Manager
- Amazon Simple Storage Service（Amazon S3）
- Amazon Virtual Private Cloud（Amazon VPC）

的加密最佳实践 AWS CloudTrail

AWS CloudTrail 可帮助您审计 AWS 账户的治理、合规性、运营和风险。

考虑下面针对该服务的加密最佳实践：

- CloudTrail 应使用客户管理的日志进行加密 AWS KMS key。选择与接收日志文件的 S3 存储桶位于同一个区域的 KMS 密钥。有关更多信息，请参阅 Updating a trail to use your KMS key。
- 作为额外的安全层，为跟踪启用日志文件验证。这可以帮助您确定日志文件在 CloudTrail 传送后是被修改、删除还是未更改。有关说明，请参阅启用日志文件完整性验证 CloudTrail。
- 使用接口 VPC 终端节点 CloudTrail ， VPCs 无需通过公共 Internet 即可与其他资源进行通信。有关更多信息，请参阅 Using AWS CloudTrail with interface VPC endpoints。
- 向 KMS 密钥策略添加`aws:SourceArn`条件密钥，以确保该策略仅对一个或多个特定的跟踪 CloudTrail 使用 KMS 密钥。有关更多信息，请参阅为配置 AWS KMS key 策略 CloudTrail。

- 在中 AWS Config，实施cloud-trail-encryption-enabled AWS 托管规则以验证和强制执行日志文件加密。
- 如果配置 CloudTrail 为通过亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题发送通知，请在策略声明中添加`aws:SourceArn`（或`aws:SourceAccount`可选）条件密钥，以防止账户未经授权访问该 SNS 主题。 CloudTrail 有关更多信息，请参阅 Amazon SNS 主题政策。 CloudTrail
- 如果您正在使用 AWS Organizations，请创建记录该组织 AWS 账户 中所有事件的组织跟踪。这包括组织中的管理账户和所有成员账户。有关更多信息，请参阅 Creating a trail for an organization。
- 创建一条适用于您存储公司数据的所有 AWS 区域位置的跟踪，以记录这些地区的 AWS 账户 活动。 AWS 启动新区域时， CloudTrail 会自动包含新区域并记录该区域中的事件。

亚马逊 DynamoDB 的加密最佳实践

Amazon DynamoDB 是一项完全托管的 NoSQL 数据库服务，可提供快速、可预测和可扩展的性能。如果数据存储在耐用介质中，DynamoDB 静态加密可保护加密表中的数据，包括主键、本地和全局二级索引、流、全局表、备份和 DynamoDB Accelerator（DAX）集群。

根据数据分类要求，可以通过实施服务器端或客户端加密来保持数据的机密性和完整性：

对于服务器端加密，在创建新表时，可以使用 AWS KMS keys 对表进行加密。您可以使用 AWS 自有密钥、 AWS 托管密钥或客户托管密钥。我们建议使用客户管理的密钥，因为您的组织可以完全控制密钥，并且当您使用这种密钥类型时，表级加密密钥、DynamoDB 表、本地和全局二级索引以及流都使用相同的密钥加密。有关这些密钥类型的更多信息，请参阅客户密钥和 AWS 密钥。

> **Note**
>
> 您可以随时在 AWS 自有密钥、 AWS 托管密钥和客户管理密钥之间切换。

要对静态和传输中的数据进行客户端加密和 end-to-end保护，您可以使用 Amazon DynamoDB 加密客户端。除了保护项目属性值机密性的加密之外，DynamoDB 加密客户端还会对项目签名。它允许检测对项目的未授权更改，包括添加或删除属性，或用一个加密值替换另一个，来提供完整性保护。

考虑下面针对该服务的加密最佳实践：

- 将禁用或计划删除密钥的权限仅授予需要执行这些任务的用户。这些状态会阻止所有用户和 DynamoDB 服务对数据进行加密或解密，以及对表执行读写操作。

- 虽然 DynamoDB 默认使用 HTTPS 对传输中数据进行加密，但建议采取额外的安全控制措施。您可以使用以下任意选项：
  - AWS Site-to-Site VPN 连接 IPsec 用于加密。
  - AWS Direct Connect 连接以建立私有连接。
  - AWS Direct Connect 带连接的 AWS Site-to-Site VPN 连接用于 IPsec加密的私有连接。
  - 如果只需从虚拟私有云（VPC）中访问 DynamoDB，可使用 VPC 网关端点，只允许 VPC 中的资源访问它。这样可以防止流量遍历公共互联网。
- 如果您使用的是 VPC 端点，则将与端点关联的端点策略和 IAM policy 仅限于授权用户、资源和服务使用。有关更多信息，请参阅 Control access to DynamoDB endpoints by using IAM policies 和 Control access to services using endpoint policies。
- 根据您的加密策略，您可以在应用程序级别对需要加密的数据实施列级数据加密。
- 将 DAX 集群配置为在设置集群时加密静态数据，比如缓存中数据、配置数据和日志文件。您无法在现有集群上启用静态加密。这种服务器端加密有助于防止数据免遭通过底层存储进行未经授权的访问。DAX 静态加密会自动与 AWS KMS 集成，用于管理用于加密集群的单一服务默认密钥。如果创建加密的 DAX 集群时不存在服务默认密钥，则 AWS KMS 会自动创建新的 AWS 托管密钥。有关更多信息，请参阅 DAX encryption at rest。

  > **Note**
  >
  > 客户管理的密钥不能用于 DAX 集群。

- 将 DAX 集群配置为在设置集群时对传输中数据进行加密。您无法在现有集群上启用传输中加密。DAX 使用 TLS 来加密应用程序和集群之间的请求和响应，并使用集群的 x509 证书对集群进行身份验证。有关更多信息，请参阅 DAX encryption in transit。
- 在中 AWS Config，实施dax-encryption-enabled AWS 托管规则以验证和维护 DAX 集群的加密。

Amazon EC2 和 Amazon EBS 的加密最佳实践

亚马逊弹性计算云 (Amazon EC2) 在中提供可扩展的计算容量 AWS 云。您可以根据需要启动任意数量的虚拟服务器，并快速扩展或缩减它们。Amazon Elastic Block Store (Amazon EBS) 提供用于实例的块级存储卷。 EC2

考虑下面针对这些服务的加密最佳实践：

- 用适当的数据分类键和值标记所有 EBS 卷。这可以帮助您根据您的策略确定和实施适当的安全和加密要求。

- 根据您的加密策略和技术可行性，为实例之间或 EC2 实例与本地网络之间 EC2 传输的数据配置加密。
- 对 EC2 实例的启动卷和数据 EBS 卷进行加密。加密 EBS 卷可保护以下数据：
  - 卷中的静态数据
  - 在卷和实例之间移动的所有数据
  - 从卷创建的所有快照
  - 从这些快照创建的所有卷

  有关更多信息，请参阅 How EBS encryption works。
- 默认情况下，对当前 AWS 区域账户的 EBS 卷启用加密。这将强制对任何新的 EBS 卷和快照副本进行加密。加密对现有 EBS 卷或快照没有影响。有关更多信息，请参阅 Enable encryption by default。
- 对 Amazon EC2 实例的实例存储根卷进行加密。这有助于保护与操作系统一起存储的配置文件和数据。有关更多信息，请参阅如何使用 Amazon EC2 实例存储加密保护静态数据（AWS 博客文章）
- 在中 AWS Config，对自动检查实施加密卷规则，以验证和强制执行适当的加密配置。

Amazon ECR 的加密最佳实践

Amazon Elastic Container Registry（Amazon ECR）是一项安全、可扩展且可靠的托管容器映像注册表服务。

Amazon ECR 将映像存储在 Amazon ECR 管理的 Amazon S3 存储桶中。每个 Amazon ECR 存储库都有一个加密配置，该配置是在创建存储库时设置的。默认情况下，Amazon ECR 使用具有 Amazon S3 托管的（SSE-S3）加密密钥的服务器端加密。有关更多信息，请参阅 Encryption at rest（Amazon ECR 文档）。

考虑下面针对该服务的加密最佳实践：

- 使用 AWS KMS中存储的客户管理的 KMS 密钥，而不是使用具有 Amazon S3 托管的（SSE-S3）加密密钥的默认服务器端加密。这种密钥类型提供了最精细的控制选项。

  > **Note**
  > KMS 密钥必须与存储库位于同一 AWS 区域 位置。

- 在预置存储库时，请勿撤销 Amazon ECR 默认创建的授权。这可能会影响功能，比如访问数据、对推送到存储库的新图像进行加密或在提取时对其进行解密。

- AWS CloudTrail 用于记录 Amazon ECR 向其发送的 AWS KMS请求。日志条目包含加密上下文密钥，以便更容易识别它们。
- 配置 Amazon ECR 策略以控制来自特定亚马逊 VPC 终端节点或特定 VPCs终端节点的访问。实际上，这隔离了对特定 Amazon ECR 资源的网络访问，仅允许从特定 VPC 访问。通过与 Amazon VPC 端点建立虚拟专用网络（VPN）连接，您可以对传输中数据进行加密。
- Amazon ECR 支持基于资源的策略。使用这些策略，您可以根据源 IP 地址或具体地址来限制访问权限 AWS 服务。

Amazon ECS 的加密最佳实践

Amazon Elastic Container Service（Amazon ECS）是一项快速且可扩展的容器管理服务，可帮助运行、停止和管理集群上的容器。

借助 Amazon ECS，您可以使用以下任何一种方法对传输中数据进行加密：

- 创建服务网格。使用 AWS App Mesh在已部署的 En voy 代理和网状端点（例如虚拟节点或虚拟网关）之间配置 TLS 连接。您可以使用来自的 TLS 证书 AWS Private Certificate Authority 或客户提供的证书。有关更多信息和演练，请参阅AWS App Mesh 使用 AWS Certificate Manager (ACM) 或客户提供的证书（AWS 博客文章）启用服务之间的流量加密。
- 如果支持，请使用 AWS Nitro Enclaves。 AWS Nitro Enclaves 是一项亚马逊 EC2 功能，允许您从亚马逊实例创建隔离的执行环境，称为安全区。 EC2它们旨在帮助保护您最敏感的数据。此外，ACM for Nitro Enclaves 允许您在带有 Nitro Enclaves 的亚马逊 EC2 实例上运行的 Web 应用程序和网络服务器上使用公有和私有 SSL/TLS 证书。 AWS 有关更多信息，请参阅 AWS Nitro Enclaves — 用于处理机密数据的隔离 EC2 环境（AWS 博客文章）。
- 将服务器名称指示 (SNI) 协议与应用程序负载均衡器配合使用。您可以在 Application Load Balancer 的单个 HTTPS 侦听器后面部署多个应用程序。每个侦听器都有自己的 TLS 证书。您可以使用 ACM 提供的证书，也可以使用自签名证书。应用程序负载均衡器和网络负载均衡器都支持 SNI。有关更多信息，请参阅应用程序负载均衡器现在支持多个 TLS 证书，并使用 SNI 进行智能选择（AWS 博客文章）。
- 为了提高安全性和灵活性，请使用 AWS Private Certificate Authority 在 Amazon ECS 任务中部署 TLS 证书。有关更多信息，请参阅一直维护容器的 TLS 第 2 部分：使用 AWS Private CA（AWS 博客文章）。
- 使用密钥发现服务 (Envoy) 或 ACM () 中托管的证书，在 App Mesh 中实现双向 TLS (GitHubm TL)。

考虑下面针对该服务的加密最佳实践：

- 在技术上可行的情况下，为了增强安全性，请在 AWS PrivateLink中配置 Amazon ECS 接口 VPC 端点。通过 VPN 连接访问这些端点可对传输中数据进行加密。
- 安全存储敏感材料，比如 API 密钥或数据库凭证。您可以将它们作为加密参数存储在 Parameter Store 中，这是 AWS Systems Manager的一项功能。但是，我们建议您使用， AWS Secrets Manager 因为此服务允许您自动轮换密钥、生成随机密钥以及共享密钥 AWS 账户。
- 如果您的数据中心中的用户或应用程序或网络上的外部第三方直接向发出 HTTPS API 请求 AWS 服务，请使用从 AWS Security Token Service (AWS STS) 获得的临时安全证书签署这些请求。

Amazon EFS 的加密最佳实践

Amazon Elastic File System（Amazon EFS）可帮助您在 AWS 云中创建和配置共享文件系统。

考虑下面针对该服务的加密最佳实践：

- 在中 AWS Config，实施efs-encrypted-check AWS 托管规则。此规则检查 Amazon EFS 是否配置为使用加密文件数据 AWS KMS。
- 通过创建 Amazon 警报来强制加密 Amazon EFS 文件系统，该 CloudWatch 警报监控`CreateFileSystem`事件 CloudTrail 日志，并在创建未加密文件系统时触发警报。有关更多信息，请参阅 Walkthrough: Enforcing Encryption on an Amazon EFS File System at Rest。
- 使用 EFS 挂载帮助程序挂载文件系统。这将在客户端和 Amazon EFS 服务之间建立和维护 TLS 1.2 隧道，并通过这个加密隧道路由所有网络文件系统（NFS）流量。以下命令实现了使用 TLS 进行传输中加密。

  ```
  sudo mount -t efs  -o tls file-system-id:/ /mnt/efs
  ```

  有关更多信息，请参阅 Using EFS mount helper to mount EFS file systems。
- 使用 AWS PrivateLink、实现接口 VPC 终端节点，在 VPCs 和 Amazon EFS API 之间建立私有连接。通过 VPN 连接传入和传出端点的传输中数据会被加密。有关更多信息，请参阅 Access an AWS 服务 using an interface VPC endpoint。
- 在基于 IAM 身份的策略中使用 `elasticfilesystem:Encrypted` 条件键可防止用户创建未加密的 EFS 文件系统。有关更多信息，请参阅 Using IAM to enforce creating encrypted file systems。
- 使用基于资源的密钥政策将用于 EFS 加密的 KMS 密钥配置为最低权限访问。

- 在 EFS 文件系统策略中使用 `aws:SecureTransport` 条件键，强制 NFS 客户端在连接 EFS 文件系统时使用 TLS。有关更多信息，请参阅使用 Amazon Elastic File System 加密文件数据中的传输数据加密（AWS 白皮书）。

Amazon EKS 的加密最佳实践

亚马逊 Elastic Kubernetes Service（亚马逊 EKS）可帮助你在上面运行 AWS Kubernetes，而无需安装或维护自己的 Kubernetes 控制平面或节点。在 Kubernetes 中，密钥可帮助您管理敏感信息，比如用户证书、密码或 API 密钥。默认情况下，这些密钥以未加密方式存储在 API 服务器的底层数据存储中（称为 etcd）。在亚马逊 EKS 上，节点的亚马逊弹性区块存储 (Amazon EBS) 卷`etcd`使用亚马逊 EBS 加密进行加密。任何具有 API 访问权限或 `etcd` 访问权限的用户都可以检索或修改密钥。此外，任何有权在命名空间中创建 pod 的人都可以使用该访问权限读取该命名空间中的任何密钥。您可以使用托管密钥或客户 AWS 托管密钥在 Amazon EKS 中对这些秘密进行 AWS KMS keys静态加密。另一种使用方法`etcd`是使用 S AWS ecrets and Config Provider (ASCP)（GitHub 存储库）。ASCP 与 IAM 和基于资源的策略集成，可限制对密钥的访问，且仅限于集群内特定 Kubernetes pod。

你可以在 Kubernetes 中使用以下 AWS 存储服务：

- 对于 Amazon EBS，您可以使用树内存储驱动程序或 A mazon EBS CSI 驱动程序。两者都包含用于加密卷和提供客户管理密钥的参数。
- 对于 Amazon Elastic File System（Amazon EFS），您可以使用支持动态和静态预置的 Amazon EFS CSI 驱动程序。

考虑下面针对该服务的加密最佳实践：

- 如果使用 `etcd` 来存储默认未加密的密钥对象，请执行以下操作以帮助保护密钥：
  - 加密静态密钥数据（Kubernetes 文档）。
  - AWS KMS 用于对 Kubernetes 机密进行信封加密。这允许您使用唯一的数据密钥加密您的机密。您可以使用 AWS KMS 密钥加密密钥来加密数据密钥。您可以定期自动轮换密钥加密密钥。使用适用于 Kubernetes 的 AWS KMS 插件，所有 Kubernetes 机密都存储在密文中。`etcd`它们只能由 Kubernetes API 服务器解密。有关更多信息，请参阅使用 Amazon EKS 加密提供商支持进行深度防御和使用现有集群加密 Kubernetes 密钥。 AWS KMS
  - 通过基于角色的访问控制（RBAC）规则启用或配置授权，来限制读写密钥。限制创建新密钥或替换现有密钥的权限。有关更多信息，请参阅 Authorization overview（Kubernetes 文档）。
  - 如果您要在一个 Pod 中定义多个容器，并且其中只有一个容器需要访问密钥，请定义卷挂载，使其他容器无法访问该密钥。作为卷挂载的密钥将实例化为 `tmpfs` 卷，并在删除 pod 时自动从节点

中删除。您也可以使用环境变量，但我们不建议使用这种方法，因为环境变量的值可能会出现在日志中。有关更多信息，请参阅 Secrets（Kubernetes 文档）。

  - 如果可能，避免授予对命名空间中密钥的 `watch` 和 `list` 请求的访问权限。在 Kubernetes API 中，这些请求非常强大，因为它们允许客户端检查该命名空间中每个密钥的值。
  - 仅允许集群管理员访问 `etcd`，包括只读访问权限。
  - 如果有多个 `etcd` 实例，确保 `etcd` 使用 TLS 在 `etcd` 对等机之间进行通信。
- 如果您使用的是 ASCP，请执行以下操作来帮助保护密钥：
  - 使用服务账户的 IAM 角色，限制只有经过授权的 pod 才能访问密钥。
  - 使用加密提供商（GitHub 存储库）使用客户托管的 KMS 密钥实现信封AWS 加密，从而启用 Kubernetes 密钥的加密。
- 为了帮助降低环境变量造成数据泄露的风险，我们建议您使用AWS Secrets Manager 和 Config Provider for Secret Store CSI 驱动程序 (GitHub)。该驱动程序允许您使存储在 Secrets Manager 中的密钥和存储在 Parameter Store 中的参数显示为挂载在 Kubernetes Pod 中的文件。

> **Note**
>
> AWS Fargate 不支持。

- 创建 Amazon CloudWatch 指标筛选器和警报，以针对管理员指定的操作发送警报，例如删除密钥或在等待删除期间使用密钥版本。有关更多信息，请参阅 Creating an alarm based on anomaly detection。

的加密最佳实践 AWS Encryption SDK

AWS Encryption SDK 是一个开源的客户端加密库。它使用行业标准和最佳实践来支持多种编程语言的实现和互操作性。 AWS Encryption SDK 使用安全、经过身份验证的对称密钥算法对数据进行加密，并提供符合加密最佳实践的默认实现。有关更多信息，请参阅 Supported algorithm suites in the AWS Encryption SDK。

的关键功能之一 AWS Encryption SDK 是支持对正在使用的数据进行加密。通过采用某种 encrypt-then-use方法，您可以在应用程序逻辑处理敏感数据之前对其进行加密。即使应用程序本身受到安全事件的影响，这也有助于保护数据免遭潜在的泄露或篡改。

考虑下面针对该服务的最佳实践：

- 遵守 AWS Encryption SDK最佳实践中的所有建议。

- 选择一个或多个包装密钥，帮助保护您的数据密钥。有关更多信息，请参阅 Select wrapping keys。
- 将`KeyId`参数传递给ReEncrypt操作以帮助防止使用不受信任的 KMS 密钥。有关更多信息，请参阅改进的客户端加密：显式 KeyIds 和密钥承诺（AWS 博客文章）。
- 使用 with 时 AWS Encryption SDK AWS KMS，请使用本地`KeyId`筛选。有关更多信息，请参阅改进的客户端加密：显式 KeyIds 和密钥承诺（AWS 博客文章）。
- 对于需要加密或解密的大量流量的应用程序，或者如果您的账户超出了 AWS KMS 请求配额，则可以使用的数据密钥缓存功能。 AWS Encryption SDK请注意以下数据密钥缓存的最佳实践：
  - 配置缓存安全阈值限制每个缓存数据密钥的使用时间长度，以及每个数据密钥保护的数据量。有关配置这些阈值的建议，请参阅 Setting cache security thresholds。
  - 将本地缓存限制为最少数量的数据密钥，以便在特定应用程序用例情况下实现性能改进。有关配置本地缓存限制的说明和示例，请参阅使用数据密钥缓存： Step-by-step。

  有关更多信息，请参阅 AWS Encryption SDK：如何确定数据密钥缓存是否适合您的应用程序（AWS 博客文章）。

的加密最佳实践 AWS Key Management Service

AWS Key Management Service (AWS KMS) 可帮助您创建和控制加密密钥以帮助保护您的数据。AWS KMS 与大多数其他 AWS 服务 可以加密您的数据的软件集成。有关完整列表，请参阅与AWS 服务 集成 AWS KMS。 AWS KMS 还与集成 AWS CloudTrail 以记录您的 KMS 密钥的使用情况，以满足审计、监管和合规需求。

KMS 密钥是中的主要资源 AWS KMS，也是加密密钥的逻辑表示形式。KMS 密钥主要分为三种类型：

- 客户管理的密钥是您创建的 KMS 密钥。
- AWS 托管密钥是代表您在账户中 AWS 服务 创建的 KMS 密钥。
- AWS 拥有的密钥是 AWS 服务 拥有和管理的 KMS 密钥，用于多个密钥 AWS 账户。

有关密钥类型的更多信息，请参阅 Customer keys and AWS keys。

在中 AWS 云，策略用于控制谁可以访问资源和服务。例如，在 AWS Identity and Access Management (IAM) 中，基于身份的策略定义用户、用户组或角色的权限，基于资源的策略附加到资源（例如 S3 存储桶），并定义允许访问哪些委托人、支持的操作以及必须满足的任何其他条件。与 IAM 策略类似， AWS KMS 使用密钥策略来控制对 KMS 密钥的访问。每个 KMS 密钥必须有一个密钥政策，并且每个密钥只能有一个密钥政策。在定义允许或拒绝访问 KMS 密钥的策略时，请注意以下几点：

- 您可以控制客户托管密钥的密钥策略，但不能直接控制 AWS 托管密钥或 AWS 自有密钥的密钥策略。
- 密钥策略允许在中授予对 AWS KMS API 调用的精细访问权限。 AWS 账户除非密钥政策明确允许，否则您不能使用 IAM policy 允许访问 KMS 密钥。未经密钥政策许可，允许权限的 IAM policy 无效。有关更多信息，请参阅 Allow IAM policies to allow access to the KMS key。
- 您可以使用 IAM policy 拒绝访问客户管理的密钥，而无需密钥政策的相应权限。
- 为多区域密钥设计密钥政策和 IAM policy 时，请考虑以下方面：
  - 密钥政策不是多区域密钥的共享属性，也不会在相关的多区域密钥之间复制或同步。
  - 使用 `CreateKey` 和 `ReplicateKey` 操作创建多区域密钥时，除非在请求中指定了密钥政策，否则将应用默认密钥政策。
  - 您可以实现条件键，例如 aws: RequestedRegion，将权限限制为特定的权限 AWS 区域。
  - 您可以使用授权来允许对多区域主密钥或副本密钥的权限。但是，不能使用单个授权来允许对多个 KMS 密钥的权限，即使它们是相关的多区域密钥。

在使用 AWS KMS 和创建密钥策略时，请考虑以下加密最佳做法和其他安全最佳实践：

- 请遵循以下资源中的建议以获取 AWS KMS 最佳实践：
  - AWS KMS 拨款最佳实践（AWS KMS 文档）
  - IAM policy 最佳实践（AWS KMS 文档）
- 根据职责分离最佳实践，为管理密钥的人员和使用密钥的人员维护不同的身份：
  - 创建和删除密钥的管理员角色不能使用密钥。
  - 某些服务可能只需要加密数据，不应被授予使用密钥解密数据的能力。
- 密钥政策应始终遵循最低权限模式。请勿将 `kms:*` 用于 IAM 或密钥政策中的操作，因为这会授予主体管理和使用密钥的权限。
- 使用密钥策略中的 k ms: ViaService 条件密钥，将客户托管密钥的使用限制在特定 AWS 服务 范围内。
- 如果您可以在密钥类型之间进行选择，则首选客户管理的密钥，因为它们提供了最精细的控制选项，包括以下选项：
  - 管理身份验证和访问控制
  - 启用和禁用密钥
  - 轮换 AWS KMS keys
  - 标记密钥

  - 创建别名
  - 删除 AWS KMS keys
- AWS KMS 必须明确拒绝向未经批准的委托人授予管理和 AWS KMS 修改权限，并且允许语句中不应存在任何未经授权的委托人的修改权限。有关更多信息，请参阅用于 AWS Key Management Service的操作、资源和条件键。
- 为了检测未经授权使用的 KMS 密钥，请在中实现-kms-acti AWS Config ons 和 iam-customer-policy-blockediam-inline-policy-blocked-kms-actions 规则。这可以防止委托人对所有 AWS KMS 资源使用解密操作。
- 在中实施服务控制策略 (SCPs) AWS Organizations ，以防止未经授权的用户或角色直接通过命令或通过控制台删除 KMS 密钥。有关更多信息，请参阅 SCPs 用作预防性控制措施（AWS 博客文章）。
- 将 AWS KMS API 调用 CloudTrail 记录在日志中。这会记录相关的事件属性，例如，发出了哪些请求、发出请求的源 IP 地址以及发出请求的人。有关更多信息，请参阅使用记录 AWS KMS API 调用 AWS CloudTrail。
- 如果您使用加密上下文，则它不应包含任何敏感信息。 CloudTrail 将加密上下文存储在纯文本 JSON 文件中，任何有权访问包含该信息的 S3 存储桶的人都可以查看这些文件。
- 在监控客户管理的密钥的使用情况时，配置事件以在检测到特定操作时通知您，如密钥创建、更新客户管理的密钥政策或导入密钥材料。此外，还建议您实施自动响应，例如禁用密钥的 AWS Lambda 函数，或者根据您的组织策略执行任何其他事件响应操作。
- 对于特定方案，如合规性、灾难恢复或备份，建议使用多区域密钥。多区域密钥的安全属性与单区域密钥有很大不同。授权创建、管理和使用多区域密钥时，以下建议适用：
  - 只允许主体将多区域密钥复制到需要它们的 AWS 区域 中。
  - 仅对需要多区域密钥的主体授予权限，并且仅对需要多区域密钥的任务授予权限。

的加密最佳实践 AWS Lambda

AWS Lambda 是一项计算服务，可帮助您运行代码，无需预置或管理服务器。为了保护环境变量，您可以使用服务器端加密来保护静态数据，使用客户端加密来保护传输中数据。

考虑下面针对该服务的加密最佳实践：

- Lambda 始终通过 AWS KMS key提供服务器端静态加密。默认情况下，Lambda 使用 AWS 托管密钥。我们建议您使用客户管理的密钥，因为您可以完全控制密钥，包括管理、轮换和审计。

- 对于需要加密的传输中数据，启用帮助程序，以确保使用首选 KMS 密钥对环境变量进行客户端加密，从而保护传输中数据。有关更多信息，请参阅 Securing environment variables 中的 Security in transit。
- 应在传输过程中对包含敏感数据或关键数据的 Lambda 函数环境变量进行加密，以保护动态传递给函数的数据（通常是访问信息）免遭未经授权的访问。
- 要防止用户查看环境变量，请在 IAM policy 或密钥政策中的用户权限中添加一条语句，以拒绝用户访问默认密钥、客户管理的密钥或所有密钥。有关更多信息，请参阅使用 AWS Lambda 环境变量。

Amazon RDS 的加密最佳实践

Amazon Relational Database Service（Amazon RDS）可帮助您在 AWS 云中设置、操作和扩展关系数据库（DB）。静态加密的数据包括数据库实例的底层存储、自动备份、只读副本和快照。

以下是用于加密 RDS 数据库实例中静态数据的方法：

- 您可以使用托管密钥或客户 AWS 托管密钥加密 Amazon RDS 数据库实例。 AWS KMS keys有关更多信息，请参阅本指南中的AWS Key Management Service。
- Amazon RDS for Oracle 和 Amazon RDS for SQL Server 支持使用透明数据加密（TDE）加密数据库实例。有关更多信息，请参阅 Oracle Transparent Data Encryption 或 Transparent Data Encryption in SQL Server 支持。

  您可以使用 TDE 和 KMS 密钥来加密数据库实例。但是，这会对数据库的性能造成轻微影响，因此必须单独管理这些密钥。

以下是用于加密传入或传出 RDS 数据库实例的传输中数据的方法：

- 对于运行 MariaDB、Microsoft SQL Server、MySQL、Oracle 或 PostgreSQL 的 Amazon RDS 数据库实例，您可以使用 SSL 对连接进行加密。有关更多信息，请参阅 SSL/TLS 使用加密与数据库实例的连接。
- Amazon RDS for Oracle 还支持 Oracle 本机网络加密（NNE），在数据传入和传出数据库实例时对数据进行加密。不能同时使用 NNE 和 SSL 加密。有关更多信息，请参阅 Oracle 本机网络加密。

考虑下面针对该服务的加密最佳实践：

- 连接到 Amazon RDS for SQL Server 或 Amazon RDS for PostgreSQL 数据库实例以处理、存储或传输需要加密的数据时，请使用 RDS 传输加密功能对连接进行加密。您可以在参数组中将

`rds.force_ssl` 参数设置为 1 来实现这一点。有关更多信息，请参阅 Working with parameter groups。Amazon RDS for Oracle 使用 Oracle 数据库本机网络加密。

- 用于 RDS 数据库实例加密的客户管理密钥只能用于此目的，不得与任何其他 AWS 服务一起使用。
- 在加密 RDS 数据库实例之前，请确定 KMS 密钥要求。实例使用的密钥无法在以后进行更改。例如，在您的加密策略中，根据您的业务需求定义 AWS 托管密钥或客户托管密钥的使用和管理标准。
- 在授权访问客户托管的 KMS 密钥时，请在 IAM 策略中使用条件密钥来遵循最低权限原则。例如，要允许客户托管密钥仅用于源自 Amazon RDS 的请求，请使用带有`rds.<region>.amazonaws.com`值的 k m ViaService s: 条件密钥。此外，您可以使用 Amazon RDS 加密环境中的密钥或值作为使用客户托管密钥的条件。
- 强烈建议您为加密的 RDS 数据库实例启用备份。Amazon RDS 可能会失去对数据库实例的 KMS 密钥的访问权限，例如当未启用 KMS 密钥或撤销 RDS 对 KMS 密钥的访问权限时。如果发生这种情况，加密的数据库实例将进入可恢复状态，并持续 7 天。如果数据库实例在 7 天后仍未重新获得对密钥的访问权限，数据库将永久无法访问，必须从备份中还原。有关更多信息，请参阅 Encrypting a DB instance。
- 如果只读副本与其加密的数据库实例相同 AWS 区域，则必须使用相同的 KMS 密钥对两者进行加密。
- 在中 AWS Config，实施rds-storage-encrypted AWS 托管规则以验证和强制执行 RDS 数据库实例的加密，以及对 RDS 数据库快照进行验证和强制加密的rds-snapshots-encrypted规则。
- AWS Security Hub 用于评估您的 Amazon RDS 资源是否遵循安全最佳实践。有关更多信息，请参阅 Amazon RDS 的 Security Hub 控件。

的加密最佳实践 AWS Secrets Manager

AWS Secrets Manager 有助于您通过对 Secrets Manager 的 API 调用来替换代码中的硬编码凭证（包括密码），以编程方式检索密钥。Secrets Manager 与 AWS KMS 集成，使用受保护的唯一数据密钥对每个密钥值的每个版本进行加密 AWS KMS key。这种集成使用永远不会保持 AWS KMS 未加密状态的加密密钥来保护存储的机密。您还可以对 KMS 密钥定义自定义权限，以审计生成、加密和解密用于保护存储密钥的数据密钥的操作。有关更多信息，请参阅 Secret encryption and decryption in AWS Secrets Manager。

考虑下面针对该服务的加密最佳实践：

- 在大多数情况下，我们建议使用`aws/secretsmanager` AWS 托管密钥来加密机密。使用它不产生任何费用。

- 为了能够从其他账户访问密钥或将密钥政策应用于加密密钥，请使用客户自主管理型密钥对密钥进行加密。
  - 在密钥策略中，为 k m secretsmanager.<region>.amazonaws.com s: ViaService 条件密钥分配值。这会将密钥的使用限制为仅限来自 Secrets Manager 的请求。
  - 为了进一步将密钥的使用限制为仅来自 Secrets Manager 且具有正确上下文的请求，请通过创建以下项将 Secrets Manager 加密上下文中的键或值用作使用 KMS 密钥的条件：
    - IAM 策略或密钥政策中的字符串条件运算符
    - 在授权中创建授权约束

Amazon S3 的加密最佳实践

Amazon Simple Storage Service（Amazon S3） 是一项基于云的对象存储服务，可帮助您存储、保护和检索任意数量的数据。

对于 Amazon S3 的服务器端加密，有三个选项：

- 使用 Amazon S3 托管加密密钥（SSE-S3）进行服务器端加密
- 使用 AWS Key Management Service (SSE-KMS) 进行服务器端加密
- 使用客户提供的加密密钥（SSE-C）进行服务器端加密

Amazon S3 应用服务器端加密，将亚马逊 S3 托管密钥 (SSE-S3) 作为亚马逊 S3 中每个存储桶的基本加密级别。从 2023 年 1 月 5 日起，上传到 Amazon S3 的所有新对象都将自动加密，不会产生额外费用，也不会影响性能。S3 存储桶默认加密配置和新对象上传的自动加密状态可在 AWS CloudTrail 日志、S3 清单、S3 存储镜头、Amazon S3 控制台中找到，并在 AWS Command Line Interface (AWS CLI) 和 AWS SDKs中作为其他 Amazon S3 API 响应标头提供。有关更多信息，请参阅默认加密常见问题解答。

如果在上传时使用服务器端加密来加密对象，请将 `x-amz-server-side-encryption` 标头添加到请求中，以通知 Amazon S3 使用 SSE-S3、SSE-KMS 或 SSE-C 加密对象。以下是 `x-amz-server-side-encryption` 标头的可能值：

- `AES256`，通知 Amazon S3 使用 Amazon S3 托管的密钥。
- `aws:kms`，它告诉 Amazon S3 使用 AWS KMS 托管密钥。
- 对于 SSE-C，将值设置为 `True` 或 `False`

有关更多信息，请参阅 “如何使用存储桶策略和申请 Defense-in-Depth帮助保护您的 Amazon S3 数据”（AWS 博客文章）中的Defense-in-depth 要求 1：静态数据和传输期间必须对数据进行加密。

对于 Amazon S3 中的客户端加密，有两个选项：

- 密钥存储在 AWS KMS
- 存储在应用程序中的密钥

考虑下面针对该服务的加密最佳实践：

- 在中 AWS Config，实施bucket-server-side-encryption启用 s3 的 AWS 托管规则来验证和实施 S3 存储桶加密。
- 部署 Amazon S3 存储桶策略，验证所有上传的对象是否都已使用 `s3:x-amz-server-side-encryption` 条件进行加密。有关更多信息，请参阅 Protecting data using SSE-S3 中的示例存储桶策略以及 Adding a bucket policy 中的说明。
- 使用 S3 存储桶策略中的 `aws:SecureTransport` 条件仅允许通过 HTTPS（TLS）的加密连接。有关更多信息，请参阅我应该使用哪个 S3 存储桶策略来遵守 AWS Config 规则 s3-bucket-ssl-requests-only？
- 在中 AWS Config，实现 s3 bucket-ssl-requests-only AWS 托管规则，要求请求使用 SSL。
- 如果您需要授予对 Amazon S3 对象的跨账户访问权限，请使用客户管理的密钥。配置密钥政策以允许来自另一个 AWS 账户的访问。

亚马逊 VPC 的加密最佳实践

Amazon Virtual Private Cloud（亚马逊 VPC）可帮助您将 AWS 资源启动到您定义的虚拟网络中。该虚拟网络类似于您在数据中心中运行的传统网络，并具有使用 AWS的可扩展基础设施的优势。

考虑下面针对该服务的加密最佳实践：

- 使用以下方法之一对企业网络内信息资产和系统之间的流量 VPCs 进行加密：
  - AWS Site-to-Site VPN 连接
  - AWS Site-to-Site VPN 和 AWS Direct Connect 连接的组合，提供 IPsec加密的私有连接
  - AWS Direct Connect 支持 MAC Security (MACsec) 的连接，用于加密从公司网络到该 AWS Direct Connect 地点的数据
- 使用中的 VPC 终端节点将您私密 AWS PrivateLink VPCs 连接到受支持的， AWS 服务 而无需使用 Internet 网关。您可以使用我们的 AWS VPN 服务 AWS Direct Connect 来建立此连接。您的

VPC 与其他服务之间的流量不会离开 AWS 网络。有关更多信息，请参阅AWS 服务 通过访问 AWS PrivateLink。

- 配置安全组规则，仅允许来自与安全协议关联的端口的流量，例如 HTTPS over TCP/443。定期审计安全组及其规则。

资源

- 为静态数据创建企业加密策略（AWS 规范性指南）
- AWS Key Management Service（AWS KMS 文档）的安全最佳实践
- 如何 AWS 服务 使用 AWS KMS（AWS KMS 文档）
- 安全支柱：数据保护（Well-Architect AWS ed Framework）

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
密码算法	我们在 “密码算法和 AWS 服务” 部分中添加了有关密码学算法的信息。	2025年6月18日
亚马逊 EKS 更新	我们更新了亚马逊 Elastic Kubernetes Service（亚马逊 EKS）的加密最佳实践。	2025 年 1 月 7 日
Secrets Manager 更新	我们更新了的信息和建议 AWS Secrets Manager。	2024 年 9 月 9 日
AWS 服务 更新	我们更新了亚马逊 EKS AWS Encryption SDK、亚马逊关系数据库服务 (Amazon RDS) 和亚马逊简单存储服务 (Amazon S3) 的信息和建议。	2024 年 9 月 4 日
初次发布	—	2022 年 12 月 2 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 云。
- 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 云。
- 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。

ACID

参见原子性、一致性、隔离性、耐久性。

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

请参阅变更数据捕获。

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 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 云：

- 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

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的信息。例如，Amazon SageMaker AI 为 CV 提供了图像处理算法。

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 is commonly described as a pipeline. 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

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-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

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。

后

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，其中包含事实表中有关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 Fr ame 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。

EDI

参见电子数据交换。

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。与云计算相比，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)

组织之间自动交换业务文档。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。

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

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 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

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。

少量提示

在要求法学硕士执行类似任务之前，向其提供少量示例，以演示该任务和所需的输出。这种技术是情境学习的应用，模型可以从提示中嵌入的示例（镜头）中学习。对于需要特定格式、推理或领域知识的任务，Few-shot 提示可能非常有效。另请参见零镜头提示。

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。

FM

参见基础模型。

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

人工智能模型的一个子集，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工件，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 AI。

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。

金色影像

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配置软件，并有助于提高设备制造运营的速度、可扩展性和生产力。

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

一项高级规则，可帮助管理各组织单位的资源、策略和合规性 (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。

抵制数据

从用于训练机器学习模型的数据集中扣留的一部分带有标签的历史数据。通过将模型预测与抵制数据进行比较，您可以使用抵制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

参见基础设施即代码。

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

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 (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。

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。

大型语言模型 (LLM)

一种基于大量数据进行预训练的深度学习 AI 模型。法学硕士可以执行多项任务，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

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。

LLM

参见大型语言模型。

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、记录和控制在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 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： EC2 使用 AWS 应用程序迁移服务重新托管向 Amazon 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 云 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 云。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 云

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 云。

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

由此创建的跟踪 AWS CloudTrail ，用于记录组织 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

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

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。

policy

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。

通过设计保护隐私

一种在整个开发过程中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

一种安全控制措施，旨在防止部署不合规的资源。这些控件会在资源配置之前对其进行扫描。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。

提示链接

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，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) 。

RAG

请参见检索增强生成。

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

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 云有关更多信息，请参阅AWS 云 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。

检索增强生成（RAG）

一种生成式人工智能技术，其中法学硕士在生成响应之前引用其训练数据源之外的权威数据源。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 Secret s Manager 密钥中有什么？ 在 Secrets Manager 文档中。

安全性源于设计

一种在整个开发过程中考虑安全性的系统工程方法。

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，由接收方 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。

SIEM

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 云

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 ynthetics 来创建这些测试。

系统提示符

一种向法学硕士提供上下文、说明或指导方针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

tags

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

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

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

参见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。

零镜头提示

向法学硕士提供执行任务的说明，但没有示例（镜头）可以帮助指导任务。法学硕士必须使用其预先训练的知识来处理任务。零镜头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 few-shot 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。