实施 AWS CAF 安全功能的推荐安全控制措施

AWS 规范性指导

AWS 规范性指导: 实施 AWS CAF 安全功能的推荐安全控制措施

Table of Contents

实施 AWS CAF 安全功能的推荐安全控制措施

Rishi Singla 和 Rovan Omar，Amazon Web Services（AWS）

2023 年 11 月（文档历史记录）

安全是重中之重 AWS。为了帮助减轻您的运营负担，您需要共同承担云安全和合规责任 AWS。 AWS负责云的安全，这意味着要保护运行云中提供的服务的基础架构 AWS Cloud。您负责云内安全，例如您的数据和应用程序。本指南提供的安全控制措施可以帮助您履行 AWS Cloud中的安全责任。

AWS 云采用框架 (AWS CAF) 提供了最佳实践，旨在提高您的云就绪性。 AWS CAF将这些最佳实践分为六个方面：业务、人员、治理、平台、安全和运营。本指南从安全角度重点介绍以下功能：

- 身份和访问管理：大规模管理人类和计算机身份及其权限。
- 威胁检测：配置日志记录和监控功能，以检测和调查潜在的安全配置错误、威胁或意外行为。
- 保护基础设施：保护系统和服务免受意外或未经授权的访问以及潜在漏洞的侵害。
- 保护数据：根据敏感度级别对数据进行分类。保持对数据及其在组织中的访问和使用方式的可见性和控制。
- 事件响应：建立机制来响应安全事件并减轻其潜在影响。

未能对这些 AWS CAF 安全功能实施预防性、侦测性和响应性安全控制措施可能会对您的云环境构成重大风险，并可能中断您的业务。实施本指南中的安全控制措施可以帮助您的组织保护其云环境。

> **Note**
>
> AWS 提供服务、工具和框架，可帮助您在中安全运行 AWS Cloud。本指南与 Well-Ar AWS chitected 框架AWS 、云采用框架AWS (CAF)、安全参考架构AWS (SRA) 以及AWS 由发布的其他安全建议保持一致并对其进行了补充。 AWS本指南中的控制措施并未全面涵盖所有云安全注意事项，且本指南并非旨在替代这些框架。

管理身份和访问权限的安全控制措施建议

您可以在中创建身份 AWS，也可以连接外部身份源。通过 AWS Identity and Access Management (IAM) 策略，您可以向用户授予必要的权限，以便他们可以访问或管理 AWS 资源和集成应用程序。有效的身份和访问管理有助于验证合适的人员和计算机是否能够在合适的条件下访问合适的资源。Well AWS -Architected Fram ework 提供了管理身份及其权限的最佳实践。最佳实践的示例包括依赖集中式身份提供者和使用强大的登录机制，例如多重身份验证（MFA）。本节中的安全控制措施可以帮助您实施这些最佳实践。

本节中的控制措施：

- 监控和配置根用户活动的通知
- 请勿为根用户创建访问密钥
- 为根用户启用 MFA
- 遵循 IAM 安全最佳实践
- 授予最低权限许可
- 在工作负载级别定义权限护栏
- 定期轮换 IAM 访问密钥
- 识别与外部实体共享的资源

监控和配置根用户活动的通知

首次创建时 AWS 账户，您首先会使用名为 root 用户的单一登录身份。默认情况下，根用户拥有对该账户中所有 AWS 服务 和资源的完全访问权限。您应该严格控制和监控根用户，并且应仅将其用于需要根用户凭证的任务。

有关更多信息，请参阅以下资源：

- 在 Well-Architect@@ ed Framework 中授予最低权限访问权限 AWS
- 在《 AWS 规范性指南》中@@ 监控 IAM 根用户活动

请勿为根用户创建访问密钥

根用户是 AWS 账户中权限最高的用户。禁用对根用户的编程访问有助于降低无意中暴露用户凭证以及随后云环境遭到破坏的风险。我们建议您创建并使用 IAM 角色作为访问 AWS 账户 和资源的临时凭证。

有关更多信息，请参阅以下资源：

- AWS Security Hub CSPM 文档中@@ 不应有 IAM 根用户访问密钥
- IAM 文档中的删除根用户的访问密钥
- IAM 文档中的 IAM 角色

为根用户启用 MFA

我们建议您为根用户和 IAM 用户启用多重身份验证 (MFA) 设备。 AWS 账户 这将提高 AWS 账户 中的安全门槛，并可以简化访问管理。由于根用户是能够执行特权操作的高权限用户，因此对根用户要求 MFA 至关重要。您可以使用基于时间的一次性密码（TOTP）算法生成数字代码的硬件 MFA 设备、FIDO 硬件安全密钥或虚拟身份验证器应用程序。

2024 年，将需要 MFA 才能访问任何根用户。 AWS 账户有关更多信息，请参阅安全博客中的设计安全：在 2024 年 AWS 提高 MFA 要求。 AWS 我们强烈建议您扩展这种安全措施，并要求您 AWS 环境中的所有用户类型都必须采用 MFA。

如果可能，我们建议您对根用户使用硬件 MFA 设备。虚拟 MFA 无法提供与硬件 MFA 设备相同的安全水平。您可以在等待硬件购买批准或交付时使用虚拟 MFA。

在管理数百个账户的情况下 AWS Organizations，根据组织的风险承受能力，可能无法扩展为对组织单位 (OU) 中每个账户的根用户使用基于硬件的 MFA。在这种情况下，您可以在 OU 中选择一个账户充当 OU 管理账户，然后禁用该 OU 中其他账户的根用户。默认情况下，OU 管理账户无权访问其他账户。通过提前设置跨账户访问，您可以在紧急情况下从 OU 管理账户访问其他账户。要设置跨账户访问，您可在成员账户中创建一个 IAM 角色，然后定义策略，以便只有 OU 管理账户中的根用户才能担任此角色。有关更多信息，请参阅 IAM 文档中的教程： AWS 账户 使用 IAM 角色委派访问权限。

我们建议您为根用户凭证启用多台 MFA 设备。您最多可以注册 8 台任意组合的 MFA 设备。

有关更多信息，请参阅以下资源：

- IAM 文档中的启用硬件 TOTP 令牌

- IAM 文档中的启用虚拟多重身份验证（MFA）设备
- IAM 文档中的启用 FIDO 安全密钥
- IAM 文档中的使用多重身份验证（MFA）保护您的根用户登录安全

遵循 IAM 安全最佳实践

IAM 文档包含一系列最佳实践，旨在帮助您保护 AWS 账户 和资源。其包括关于根据最低权限原则配置访问权限和权限的建议。IAM 安全最佳实践的示例包括配置身份联合验证、要求 MFA 和使用临时凭证。

有关更多信息，请参阅以下资源：

- IAM 文档中的 IAM 的安全防御最佳实操
- 将临时证书与 IAM 文档中的 AWS 资源配合使用

授予最低权限许可

最低权限是仅授予执行任务所需最低权限的实践。为此，您可以定义在特定条件下可以对特定资源执行的操作。

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于其标签等属性来定义权限。您可以使用组、身份和资源属性来大规模动态定义权限，而不是为单个用户定义权限。例如，您可以使用 ABAC 允许一组开发人员仅访问具有与其项目关联的特定标签的资源。

有关更多信息，请参阅以下资源：

- IAM 文档中的应用最低权限许可
- IAM 文档中的什么是适用于 AWS的 ABAC

在工作负载级别定义权限护栏

最佳实践是使用多账户策略，因为该策略提供了在工作负载级别定义护栏的灵活性。 AWS 安全参考架构提供了有关如何构建账户的规范性指导。这些帐户在中作为一个组织进行管理 AWS Organizations，并将这些帐户分组为组织单位 (OUs)。

AWS Control Tower 等AWS 服务服务可以帮助您集中管理整个组织的控制措施。我们建议您为组织内的每个账户或 OU 定义明确的用途，并根据该目的应用控制措施。 AWS Control Tower 实施预防性、

侦查性和主动控制措施，帮助您管理资源并监控合规性。预防性控制措施旨在防止事件发生。侦测性控制措施用于在事件发生后进行检测、记录日志和发出提醒。主动性控制措施旨在通过在资源预调配之前对其进行扫描来防止部署不合规的资源。

有关更多信息，请参阅以下资源：

- 使用 Well-Architecte AWS d Framework 中的账户来分离工作负载
- AWS AWS 规范性指南中的@@ 安全参考架构 (AWS SRA)
- 关于 AWS Control Tower 文档 AWS Control Tower中的控件
- 在《 AWS 规范性@@ 指南》 AWS中实施安全控制
- 使用服务控制策略在安全博客中为 AWS 组织中的账户设置权限护栏 AWS

定期轮换 IAM 访问密钥

对于需要长期凭证的使用案例，最佳实践是更新访问密钥。我们建议每 90 天或更短时间轮换一次访问密钥。轮换访问密钥可减少他人使用遭盗用账户或已终止账户关联的访问密钥的风险。它还可以防止使用可能已丢失、泄露或被盗的旧密钥进行访问。轮换访问密钥后，请务必更新应用程序。

有关更多信息，请参阅以下资源：

- IAM 文档中的对于需要长期凭证的用例，应在需要时更新访问密钥
- 使用规范性指导@@ AWS Organizations 和在 “ AWS 规范性指南” AWS Secrets Manager中自动轮换 IAM 用户访问密钥
- IAM 文档中的更新访问密钥

识别与外部实体共享的资源

外部实体是指 AWS 组织之外的资源、应用程序、服务或用户，例如另一个用户、根用户 AWS 账户、IAM 用户或角色、联合用户、或匿名（或未经身份验证）的用户。 AWS 服务安全最佳实践是使用 IAM Access Analyzer 识别组织和账户中与外部实体共享的资源，例如 Amazon Simple Storage Service（Amazon S3）存储桶或 IAM 角色。这可以帮助您识别对资源和数据的意外访问，此类访问会带来安全风险。

有关更多信息，请参阅以下资源：

- IAM 文档中的使用 IAM Access Analyzer 验证对资源的公共和跨账户存取

- 在 Well-Ar AWS chitected Frame@@ work 中分析公共和跨账户访问权限
- IAM 文档中的使用 AWS Identity and Access Management Access Analyzer

日志记录和监控的安全控制措施建议

日志记录和监控是威胁检测的重要方面。威胁检测是AWS 云采用框架 (AWS CAF) 中的安全视角功能之一。通过使用日志数据，您的组织可以监控您的环境，以了解和识别潜在的安全错误配置、威胁和意外行为。了解潜在威胁可以帮助您的组织确定安全控制措施的优先级，而有效的威胁检测可以帮助您更快地应对威胁。

本节中的控制措施：

- 在中配置至少一条多区域跟踪 CloudTrail
- 在服务和应用程序级别配置日志记录
- 建立分析日志和响应安全事件的集中式位置
- 防止未经授权访问包含 CloudTrail 日志文件的 S3 存储桶
- 配置安全组或网络变更警报 ACLs
- 为进入警报状态的 CloudWatch 警报配置警报

在中配置至少一条多区域跟踪 CloudTrail

AWS CloudTrail帮助您审计您的治理、合规和运营风险 AWS 账户。用户、角色或执行的操作将作为事件记录 AWS 服务 在中 CloudTrail。事件包括在 AWS 管理控制台、 AWS Command Line Interface (AWS CLI) AWS SDKs 和中采取的操作 APIs。此事件历史记录可帮助您分析安全状况、跟踪资源变更及审计合规性。

要持续记录您的事件 AWS 账户，必须创建跟踪。应将每个跟踪配置为记录所有 AWS 区域中的事件。通过全部记录事件 AWS 区域，可以确保记录发生在您的中的所有事件，无论 AWS 账户 这些事件发生在哪个 AWS 区域 事件中。多区域跟踪可确保记录全球服务事件。

有关更多信息，请参阅以下资源：

- CloudTrail CloudTrail文档中的@@ 侦探安全最佳实践
- 将@@ 应用于一个区域的跟踪转换为应用于 CloudTrail 文档中的所有区域
- 在 CloudTrail文档中@@ 启用和禁用全局服务事件记录

在服务和应用程序级别配置日志记录

Well AWS -Architected Framework 建议您保留来自服务和应用程序的安全事件日志。这是审计、调查和运营使用案例的基本安全原则。服务和应用程序日志保留是一个由治理、风险与合规性（GRC）标准、策略和程序驱动的常见安全要求。

安全运营团队依靠日志和搜索工具来发现可能需要关注的事件，这些事件可能指示未经授权的活动或意外更改。您可以根据使用案例为不同的服务启用日志记录。例如，您可以记录 Amazon S3 存储桶访问权限、 AWS WAF Web ACL 流量、网络层的 Amazon API Gateway 流量或亚马逊 CloudFront 分配。

有关更多信息，请参阅以下资源：

- 在 AWS 架构博客中@@ 将 Amazon CloudWatch 日志流式传输到中央账户进行审计和分析
- AWS Well-Architected Framework 中的配置服务和应用程序日志记录

建立分析日志和响应安全事件的集中式位置

手动分析日志和处理信息不足以应对与复杂架构相关的海量信息。仅靠分析和报告无法及时将事件分配给正确的资源。Wel AWS l-Architected Framework 建议您将安全事件和发现 AWS 集成到通知和工作流程系统中，例如票务、错误或安全信息和事件管理 (SIEM) 系统。这些系统可帮助您分配、路由和管理安全事件。

有关更多信息，请参阅以下资源：

- AWS Well-Architected Framework 中的集中分析日志、调查发现和指标
- 在@@ 安全博客中使用和 Amazon Athena 分析安全、合规 CloudTrail 和运营活动 AWS
- AWS 在合作伙伴组合中提供威胁检测和响应服务的 AWS 合作伙伴

防止未经授权访问包含 CloudTrail 日志文件的 S3 存储桶

默认情况下， CloudTrail 日志文件存储在 Amazon S3 存储桶中。这是一种最佳安全实践，可以防止未经授权访问任何包含 CloudTrail 日志文件的 Amazon S3 存储桶。这可帮助您维护这些日志的完整性、完全性和可用性，对于进行取证和审计至关重要。如果您想记录包含 CloudTrail 日志文件的 S3 存储桶的数据事件，可以为此目的创建 CloudTrail 跟踪。

有关更多信息，请参阅以下资源：

- Amazon S3 文档中的为 S3 存储桶配置屏蔽公共访问权限设置

- CloudTrail 文档中的@@ 预防性安全最佳实 CloudTrail践
- 在 CloudTrail 文档中@@ 创建跟踪

配置安全组或网络变更警报 ACLs

Amazon Virtual Private Cloud（Amazon VPC）中的安全组控制允许到达和离开与其关联资源的流量。网络访问控制列表（ACL）在 VPC 子网级别允许或拒绝特定的入站或出站流量。这些资源对于管理 AWS 环境中的访问权限至关重要。

创建并配置 Amazon CloudWatch 警报，以便在安全组或网络 ACL 配置发生变化时通知您。将此告警配置为在每次执行 AWS API 调用以更新安全组时提醒您。您还可以使用诸如 Amazon EventBridge 和AWS Config之类的服务来自动响应这些类型的安全事件。

有关更多信息，请参阅以下资源：

- 在安全博客中@@ 自动恢复并接收有关您的 Amazon VPC 安全组变更的 AWS 通知
- 在 CloudWatch 文档中@@ 使用 Amazon CloudWatch 警报
- 在 Well-Ar AWS chitec@@ ted Framework 中实施可操作的安全事件
- 自动响应 Well-Architected Fram AWS ework 中的事件

为进入警报状态的 CloudWatch 警报配置警报

在中 CloudWatch，您可以指定警报在`OKALARM`、和`INSUFFICIENT_DATA`状态之间更改状态时会采取哪些操作。最常见的告警操作类型是通过向 Amazon Simple Notification Service（Amazon SNS）主题发送消息来通知一个或多个人员。您还可以配置要创建的警报OpsItems或事件 AWS Systems Manager。

我们建议激活告警操作，以便在监控的指标超出定义的阈值时自动向您发出提醒。监控告警可帮助您识别异常活动并快速响应安全和操作问题。

有关更多信息，请参阅以下资源：

- 在 Well-Ar AWS chitec@@ ted Framework 中实施可操作的安全事件
- CloudWatch 文档中的@@ 警报操作

保护基础设施的安全控制措施建议

基础设施保护是任何安全计划的一个关键组成部分。它包括可帮助您保护网络和计算资源的控制方法。基础设施保护的示例包括信任边界、 defense-in-depth方法、安全加固、补丁管理以及操作系统身份验证和授权。有关更多信息，请参阅 Well-Architecte AWS d Framework 中的基础设施保护。本节中的安全控制措施可以帮助您实施基础设施保护的最佳实践。

本节中的控制措施：

- 为 CloudFront 分布指定默认根对象
- 扫描应用程序代码以识别常见安全问题
- 使用专用网 VPCs 和子网创建网络层
- 将传入流量限制为仅使用授权的端口
- 阻止对 Systems Manager 文档的公开访问
- 阻止对 Lambda 函数的公开访问
- 限制默认安全组的入站和出站流量
- 扫描软件漏洞和意外网络暴露
- 设置 AWS WAF
- 配置针对 DDo S 攻击的高级防护
- 使用一种 defense-in-depth方法来控制网络流量

为 CloudFront 分布指定默认根对象

Amazon 通过全球数据中心网络交付您的网页内容，从而降低延迟并提高性能，从而 CloudFront加快网络内容的分发。如果您不定义默认根对象，对分配的根请求则传递到源服务器。如果您使用的是 Amazon Simple Storage Service（Amazon S3）来源，则该请求可能会返回 S3 存储桶中的内容列表或来源的私有内容列表。指定一个默认根对象，可帮助您避免公开分配的内容。

有关更多信息，请参阅以下资源：

- 在 CloudFront 文档中指定默认根对象

扫描应用程序代码以识别常见安全问题

Well AWS -Architected Framework 建议您扫描库和依赖项以查找问题和缺陷。您可以使用许多源代码分析工具来扫描源代码。例如，Amazon CodeGuru 可以扫描Java或Python应用程序中的常见安全问题，并提供补救建议。

有关更多信息，请参阅以下资源：

- CodeGuru 文档
- OWASP Foundation 网站上的 Source code analysis tools
- 在 Well-Architecte AWS d Framework 中@@ 执行漏洞管理

使用专用网 VPCs 和子网创建网络层

Well- AWS Architected Framework 建议您将具有相同敏感度要求的组件分组为多个层。这样可以最大限度地减少未经授权访问的潜在影响范围。例如，应将不需要互联网访问的数据库集群放在其 VPC 的私有子网中，以确保没有进出互联网的路由。

AWS 提供了许多服务，可以帮助您测试和确定公众可访问性。例如，Reachability Analyzer 是一种配置分析工具，可帮助您测试中源资源和目标资源之间的连接。 VPCs此外，网络访问分析器可帮助您识别对资源的意外网络访问。

有关更多信息，请参阅以下资源：

- 在 Well-Architecte AWS d Framework 中@@ 创建网络层
- Reachability Analyzer 文档
- 网络访问分析器文档
- Amazon Virtual Private Cloud （ Amazon VPC ）文档中的创建子网

将传入流量限制为仅使用授权的端口

不受限制的访问（例如来自0.0.0.0/0源 IP 地址的流量）会增加恶意活动的风险，例如黑客攻击、denial-of-service (DoS) 攻击和数据丢失。安全组为资源的入口和出口网络流量提供状态过滤。 AWS 任何安全组都不应允许对 SSH 和 Windows 远程桌面协议（ RDP ）等已知端口进行不受限制的入口访问。对于入站流量，在您的安全组中，仅允许授权端口上的 TCP 或 UDP 连接。要连接到 Amazon

Elastic Compute Cloud（Amazon EC2）实例，请使用会话管理器或运行命令，而不是直接访问 SSH 或 RDP。

有关更多信息，请参阅以下资源：

- Amazon EC2 文档中的使用安全组
- 使用 Amazon VPC 文档中的安全组控制您的 AWS 资源的流量

阻止对 Systems Manager 文档的公开访问

除非您的用例要求开启公开共享，否则 AWS Systems Manager 最佳做法建议您屏蔽 Systems Manager 文档的公开共享。公开共享可能会导致他人意外访问文档。公开的 Systems Manager 文档可能会公开有关账户、资源和内部流程的宝贵敏感信息。

有关更多信息，请参阅以下资源：

- Systems Manager 文档中的共享 Systems Manager 文档的最佳做法
- Systems Manager 文档中的修改共享 Systems Manager 文档的权限

阻止对 Lambda 函数的公开访问

AWS Lambda 是一项计算服务，可帮助您运行代码，无需预调配或管理服务器。Lambda 函数应不可公开访问，因为这可能会导致意外访问函数代码。

我们建议您为 Lambda 函数配置基于资源的策略，以拒绝来自账户外部的访问。您可以通过移除权限或在允许访问的语句中添加 `AWS:SourceAccount` 条件来实现此目的。您可以通过 Lambda API 或 AWS Command Line Interface（AWS CLI）更新 Lambda 函数基于资源的策略。

我们还建议您在 AWS Security Hub CSPM中启用 [Lambda.1] Lambda 函数策略应禁止公开访问控制措施。此控制措施可验证 Lambda 函数基于资源的策略是否禁止公开访问。

有关更多信息，请参阅以下资源：

- AWS Lambda Security Hub CSPM 文档中的@@ 控件
- Lambda 文档中的为 Lambda 使用基于资源的策略
- Lambda 文档中的 Lambda 操作的资源和条件

限制默认安全组的入站和出站流量

如果您在配置资源时未关联自定义安全组，则该 AWS 资源将与 VPC 的默认安全组关联。该安全组的默认规则允许来自分配给该安全组的所有资源的所有入站流量，并且允许所有出站 IPv6 流量 IPv4 和流量。这可能会允许资源接收意外流量。

AWS 建议您不要使用默认安全组。相反，可以为特定资源或资源组创建自定义安全组。

由于无法删除默认安全组，我们建议您更改默认安全组规则设置以限制入站和出站流量。配置安全组规则时，请遵循最低权限原则。

我们还建议您启用 [EC2.2] VPC 默认安全组不应允许 Security Hub CSPM 中的入站或出站流量控制。此控制措施验证 VPC 的默认安全组是否拒绝入站和出站流量。

有关更多信息，请参阅以下资源：

- 使用 Amazon VPC 文档中的安全组控制您的 AWS 资源的流量
- 亚马逊 VPC 文档 VPCs中@@ 您的默认安全组
- Security Hub CSPM 文档中的@@ 亚马逊 EC2 控件

扫描软件漏洞和意外网络暴露

我们建议您在所有账户中启用 Amazon Inspector。Amazon Inspector 是一项漏洞管理服务，可持续扫描 Amazon EC2 实例、Amazon Elastic Container Registry（Amazon ECR）容器映像和 Lambda 函数，以查找软件漏洞和意外网络暴露。它还支持深度检查 Amazon EC2 实例。当 Amazon Inspector 发现漏洞或开放的网络路径时，其会生成可供您调查的调查发现。如果您的账户中同时设置了 Amazon Inspector 和 Security Hub CSPM，则亚马逊检查员会自动将安全调查结果发送给 Security Hub CSPM 进行集中管理。

有关更多信息，请参阅以下资源：

- Amazon Inspector 文档中的 Scanning resources with Amazon Inspector
- Amazon Inspector 文档中的 Amazon Inspector Deep inspection for Amazon EC2
- AMIs 使用 AWS 安全博客中的 Amazon Inspector 扫描 EC2
- AWS 规范指引中的 Building a scalable vulnerability management program on AWS
- 在 Well-Architecte AWS d Framework 中@@ 自动保护网络
- 在 Well-Architecte AWS d Framework 中@@ 自动保护计算

设置 AWS WAF

AWS WAF是一种 Web 应用程序防火墙，可帮助您监控和阻止转发到受保护的 Web 应用程序资源（例如 Amazon API Gat APIs eway、Amazon CloudFront 分配或应用程序负载均衡器）的 HTTP 或 HTTPS 请求。根据您指定的标准，服务使用请求的内容、HTTP 403 状态代码（禁止）或自定义响应来响应请求。 AWS WAF 可以帮助保护 Web 应用程序或 APIs 防范可能影响可用性、危及安全性或消耗过多资源的常见 Web 漏洞。考虑 AWS WAF 在您的中进行设置， AWS 账户 并结合使用 AWS 托管规则、自定义规则和合作伙伴集成，以帮助保护您的应用程序免受应用程序层（第 7 层）攻击。

有关更多信息，请参阅以下资源：

- 在 AWS WAF 文档@@ AWS WAF中开始使用
- AWS WAF AWS 网站上的@@ 配送合作伙伴
- AWS 解决方案库 AWS WAF中的@@ 安全自动化
- 在 Well-Architecte AWS d 框架中@@ 实施检查和保护

配置针对 DDo S 攻击的高级防护

AWS Shield为网络和传输层（第 3 层和第 4 层）以及应用层（第 7 层）的 AWS 资源提供保护，抵御分布式拒绝服务 (DDoS) 攻击。此服务有两个选项： AWS Shield Standard 和 AWS Shield Advanced。Shield Standard 可自动保护支持的 AWS 资源，无需额外付费。

我们建议您订阅 Shield Advanced，它为受保护的资源提供扩展的 DDo S 攻击保护。根据您的架构和配置选择，您从 Shield Advanced 获得的保护会有所不同。考虑为需要以下任何一项的应用程序实施 Shield Advanced 保护：

- 保证应用程序用户的可用性。
- 如果应用程序受到 DDo S 攻击的影响，可以快速联系 DDo S 缓解专家。
- AWS 意识到应用程序可能受到 DDo S 攻击的影响，并收到来自 AWS 的攻击通知并上报给您的安全或运营团队。
- 云成本的可预测性，包括 DDo S 攻击何时影响您的使用 AWS 服务。

有关更多信息，请参阅以下资源：

- Shield 文档中的 AWS Shield Advanced overview
- AWS Shield Advanced Shield 文档中的@@ 受保护资源

- AWS Shield Advanced Shield 文档中的@@ 功能和选项
- 在 Sh@@ ield 文档中响应 DDo S 事件
- 在 Well-Architecte AWS d 框架中@@ 实施检查和保护

使用一种 defense-in-depth方法来控制网络流量

AWS Network Firewall 是针对虚拟私有云 (VPCs) 中的状态托管网络防火墙以及入侵检测和防御服务 ()。 AWS Cloud它可以帮助您在 VPC 边界部署基本的网络保护。这包括筛选进出互联网网关、NAT 网关或者通过 VPN 或 AWS Direct Connect的流量。Network Firewall 包含有助于抵御常见网络威胁的功能。Network Firewall 中的状态防火墙可以整合来自流量的上下文（例如连接和协议）来强制执行策略。

有关更多信息，请参阅以下资源：

- AWS Network Firewall 文档
- 在 Well-Architecte AWS d Framework 中控制所有层的流量

保护数据的安全控制措施建议

Wel AWS l-Architected Framework 将保护数据的最佳做法分为三类：数据分类、保护静态数据和保护传输中的数据。本节中的安全控制措施可以帮助您实施数据保护的最佳实践。在云架构任何工作负载之前，应先落实这些基础最佳实践。它们可以防止数据处理不当，并帮助您履行组织、监管与合规义务。使用本节中的安全控制措施以实施数据保护的最佳实践。

本节中的控制措施：

- 在工作负载级别识别并分类数据
- 建立每个数据分类级别的控制措施
- 加密静态数据
- 加密传输中数据
- 阻止对 Amazon EBS 快照的公开访问
- 阻止对 Amazon RDS 快照的公开访问
- 阻止公众访问亚马逊 RDS、Amazon Redshift 和资源 AWS DMS
- 阻止对 Amazon S3 存储桶的公开访问
- 需要 MFA 才能删除关键 Amazon S3 存储桶中的数据
- 在 VPC 中配置亚马逊 OpenSearch 服务域
- 配置 AWS KMS key 删除警报
- 阻止公众访问 AWS KMS keys
- 配置负载均衡器侦听器以使用安全协议

在工作负载级别识别并分类数据

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。它是所有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。数据分类通常会降低数据重复的频率。这可以降低存储和备份成本并加快搜索速度。

我们建议您了解工作负载正在处理的数据类型和分类、相关业务流程、数据存储位置以及数据所有者。数据分类可帮助工作负载所有者识别存储敏感数据的位置，并确定应如何访问和共享这些数据。标签是键值对，用作组织资源的元数据。 AWS 标签可帮助管理、识别、组织、搜索和筛选资源。

有关更多信息，请参阅以下资源：

- AWS 白皮书中的@@ 数据分类
- 在 Well-Architecte AWS d Framework 中识别工作负载中的数据

建立每个数据分类级别的控制措施

定义每个分类级别的数据保护控制措施。例如，使用建议的控制措施来保护归类为公开的数据，使用其他控制措施来保护敏感数据。使用减少或消除直接访问或手动处理数据需求的相关机制和工具。自动化数据识别和分类可降低错误分类、处理不当、修改或人为错误的风险。

例如，考虑使用 Amazon Macie 扫描 Amazon Simple Storage Service（Amazon S3）存储桶中的敏感数据，如个人身份信息（PII）。此外，您还可以使用 Amazon Virtual Private Cloud（Amazon VPC）中的 VPC 流日志自动检测意外数据访问。

有关更多信息，请参阅以下资源：

- 在 Well-Architecte AWS d Framework 中定义数据保护控制
- AWS Well-Architected Framework 中的自动识别和分类
- AWS AWS 规范性指南中的@@ 隐私参考架构 (AWS PRA)
- Macie 文档中的 Discovering sensitive data with Amazon Macie
- Amazon VPC 文档中的使用 VPC 流日志记录 IP 流量
- 在 for In@@ dustries 博客 AWS 服务中使用的检测 PHI 和 PII 数据的常 AWS 用技术

加密静态数据

静态数据是网络中静止的数据，例如存储中的数据。对静态数据实施加密和适当的访问控制有助于降低未经授权访问的风险。加密是一种将人类可读的明文数据转换为加密文字的计算过程。您需要一个加密密钥才能将内容解密回明文以供使用。在中 AWS Cloud，您可以使用 AWS Key Management Service (AWS KMS) 来创建和控制有助于保护数据的加密密钥。

如建立每个数据分类级别的控制措施中所述，我们建议创建一个策略来指定需要加密的数据类型。包括如何确定应加密哪些数据以及应使用令牌化或哈希等其他技术保护哪些数据的标准。

有关更多信息，请参阅以下资源：

- Amazon S3 文档中的配置默认加密
- Amazon EBS 文档中的 Encryption by default for new EBS volumes and snapshot copies

- Amazon Aurora 文档中的加密 Amazon Aurora 资源
- AWS KMS 文档中的 Introduction to the cryptographic details of AWS KMS
- AWS 规范指引中的 Creating an enterprise encryption strategy for data at rest
- 在 Well-@@ Architected Framework 中强制执行静 AWS 态加密
- 有关特定加密的更多信息 AWS 服务，请参阅该服务的AWS 文档

加密传输中数据

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。使用安全的 TLS 协议和密码套件加密所有传输中数据。必须对资源和互联网之间的网络流量进行加密，以帮助防止未经授权的数据访问。如果可能，请使用 TLS 对内部 AWS 环境中的网络流量进行加密。

有关更多信息，请参阅以下资源：

- 需要使用 HTTPS 才能在观众之间以及 CloudFront在 Amazon CloudFront 文档中进行通信
- AWS PrivateLink 文档
- 在 Well-Architecte AWS d Framework 中强制执行传输中的加密
- 有关特定加密的更多信息 AWS 服务，请参阅该服务的AWS 文档

阻止对 Amazon EBS 快照的公开访问

Amazon Elastic Block Store (Amazon EBS) 提供了块级存储卷，以与 Amazon Elastic Compute Cloud (Amazon EC2) 实例一起使用。您可以通过拍摄 point-in-time快照将 Amazon EBS 卷上的数据备份到 Amazon S3。您可以与其他所有人公开共享快照 AWS 账户，也可以与您指定的个人 AWS 账户 私下共享快照。

我们建议您不要公开共享 Amazon EBS 快照。这可能会无意中暴露敏感数据。当您共享快照时，您将允许其他人访问快照中的数据。只能与您信任且可访问所有数据的人共享快照。

有关更多信息，请参阅以下资源：

- Amazon EC2 文档中的共享快照
- AWS Security Hub CSPM 文档中的 Amazon EBS snapshots should not be publicly restorable
- ebs-snapshot-public-restorable-查看文档 AWS Config

阻止对 Amazon RDS 快照的公开访问

Amazon Relational Database Service（Amazon RDS）可帮助您在 AWS Cloud中设置、操作和扩展关系数据库。在数据库实例的备份时段中，Amazon RDS 创建并保存数据库（DB）实例或多可用区数据库集群的自动备份。Amazon RDS 创建数据库实例的存储卷快照，并备份整个数据库实例而不仅仅是单个数据库。您可以共享手动快照，以便复制快照或从中恢复数据库实例。

如果您将快照设置为公开共享，请确保快照中不包含任何私有或敏感数据。公开共享快照时，它会授予所有 AWS 账户 访问数据的权限。这可能会导致 Amazon RDS 实例中的数据意外泄露。

有关更多信息，请参阅以下资源：

- Amazon RDS 文档中的共享数据库快照
- rds-snapshots-public-prohibited在 AWS Config 文档中
- 在 Security Hub CSP@@ M 文档中，RDS 快照应该是私有的

阻止公众访问亚马逊 RDS、Amazon Redshift 和资源 AWS DMS

您可以将 Amazon RDS 数据库实例、Amazon Redshift 集群和 AWS Database Migration Service (AWS DMS) 复制实例配置为可公开访问。如果 `publiclyAccessible` 字段值为 `true`，则这些资源可公开访问。允许公开访问可能会导致不必要的流量、暴露或数据泄露。我们建议您不要允许公开访问这些资源。

我们建议您启用 AWS Config 规则或 Security Hub CSPM 控件，以检测 Amazon RDS 数据库实例、AWS DMS 复制实例或 Amazon Redshift 集群是否允许公开访问。

> **Note**
>
> 预配置实例后，无法修改 AWS DMS 复制实例的公共访问设置。要更改公开访问设置，请删除当前实例，然后重新创建实例。重新创建时，请不要选择可公开访问选项。

有关更多信息，请参阅以下资源：

- AWS DMS 复制实例不应在 Security Hub CSPM 文档中公开
- RDS 数据库实例应在 Security Hub CSPM 文档中禁止公众访问
- Amazon Redshift 集群应在 Security Hub CSPM 文档中禁止公众访问

- rds-instance-public-access-查看文档 AWS Config
- dms-replication-not-public在 AWS Config 文档中
- redshift-cluster-public-access-查看文档 AWS Config
- Amazon RDS 文档中的修改 Amazon RDS 数据库实例
- Amazon Redshift 文档中的修改集群

阻止对 Amazon S3 存储桶的公开访问

这是一项 Amazon S3 安全最佳实践，用于确保您的存储桶不可公开访问。除非您明确要求互联网上的任何人都能读写您的存储桶，否则请确保存储桶不是公有的。这有助于保护数据的完整性和安全性。您可以使用 AWS Config 规则和 Security Hub CSPM 控件来确认您的 Amazon S3 存储桶是否符合此最佳实践。

有关更多信息，请参阅以下资源：

- Amazon S3 文档中的 Amazon S3 安全最佳实践
- 应在 Security Hub CSPM 文档中启用 S3 阻止公共访问设置
- S3 存储桶应在 Security Hub CSPM 文档中禁止公共读取权限
- S3 存储桶应在 Security Hub CSPM 文档中禁止公共写入权限
- s3- AWS Config 文档中的bucket-public-read-prohibited 规则
- AWS Config 文档@@ 中的 s3-bucket-public-write-prohibited

需要 MFA 才能删除关键 Amazon S3 存储桶中的数据

在 Amazon S3 存储桶中使用 S3 版本控制时，您可以选择通过将存储桶配置为启用 MFA（多重身份验证）删除来添加另一层安全保护。执行此操作时，存储桶拥有者必须在任何请求中包含两种形式的身份验证，以删除版本或更改存储桶的版本控制状态。我们建议您为包含组织关键数据的存储桶启用此功能。这可以防止意外删除存储桶和数据。

有关更多信息，请参阅以下资源：

- Amazon S3 文档中的配置 MFA 删除

在 VPC 中配置亚马逊 OpenSearch 服务域

Amazon OpenSearch Service 是一项托管服务，可帮助您在中部署、操作和扩展OpenSearch集群 AWS Cloud。亚马逊 OpenSearch 服务支持OpenSearch和传统的Elasticsearch开源软件 (OSS)。部署在 VPC 内的 Amazon Serv OpenSearch ice 域可以通过私有 AWS 网络与 VPC 资源通信，无需穿越公共互联网。此配置通过限制对传输中数据的访问来提升安全状况。我们建议您不要将 Amazon Serv OpenSearch ice 域附加到公有子网，并且应根据最佳实践配置 VPC。

有关更多信息，请参阅以下资源：

- 在@@ 亚马逊 OpenSearch 服务文档中的 VPC 内启动您的亚马逊 OpenSearch 服务域
- opensearch-in-vpc-only在 AWS Config 文档中
- OpenSearch在 Security Hub CSPM 文档中，域名应位于 VPC 中

配置 AWS KMS key 删除警报

AWS Key Management Service (AWS KMS) 密钥被删除后无法恢复。如果删除 KMS 密钥，则仍使用该密钥加密的数据将永久无法恢复。如果您需要保留对数据的访问权限，则在删除该密钥之前，必须解密该数据或使用新的 KMS 密钥对其进行重新加密。只有当您确定不再需要使用 KMS 密钥时，才能将其删除。

我们建议您配置 Amazon CloudWatch 警报，以便在有人发起删除 KMS 密钥时通知您。由于删除 KMS 密钥具有破坏性和潜在危险， AWS KMS 因此要求您设置等待期并计划在 7-30 天内删除。这提供了查看计划删除并在必要时取消的机会。

有关更多信息，请参阅以下资源：

- AWS KMS 文档中的 Scheduling and canceling key deletion
- 在 AWS KMS 文档@@ 中创建警报，检测到有待删除的 KMS 密钥的使用情况
- AWS KMS keys 不应在 Security Hub CSPM 文档中无意中删除

阻止公众访问 AWS KMS keys

密钥策略是控制对 AWS KMS keys访问的主要方法。每个 KMS 密钥都有且只有一个密钥策略。允许匿名访问 KMS 密钥可能会导致敏感数据泄露。我们建议您识别所有可公开访问的 KMS 密钥并更新其访问策略，以防止向这些资源发出未签名的请求。

有关更多信息，请参阅以下资源：

- AWS KMS 文档 AWS Key Management Service中的@@ 安全最佳实践
- 在 AWS KMS 文档中更改密钥策略
- 在 AWS KMS 文档@@ AWS KMS keys中确定访问权限

配置负载均衡器侦听器以使用安全协议

弹性负载均衡将传入的应用程序流量自动分配到多个目标。您可通过指定一个或多个侦听器将您的负载均衡器配置为接受传入流量。侦听器是一个使用您配置的协议和端口检查连接请求的进程。每种类型的负载均衡器支持不同的协议和端口：

- 应用程序负载均衡器在应用层进行路由决策并使用 HTTP 或 HTTPS 协议。
- 网络负载均衡器在传输层进行路由决策并使用 TCP、TLS、UDP 或 TCP_UDP 协议。
- 经典负载均衡器在传输层（使用 TCP 或 SSL 协议）或应用层（使用 HTTP 或 HTTPS 协议）进行路由决策。

我们建议您始终使用 HTTPS 或 TLS 协议。这些协议确保负载均衡器负责加密和解密客户端和目标之间的流量。

有关更多信息，请参阅以下资源：

- 弹性负载均衡文档中的 Listeners for your Application Load Balancers
- 弹性负载均衡文档中的 Listeners for your Classic Load Balancer
- 弹性负载均衡文档中的 Listeners for your Network Load Balancers
- 确保 AWS 负载均衡器使用 AWS 规范指南中的安全侦听器协议
- elb-tls-https-listeners-仅在文档中 AWS Config
- 应在 Security Hub CSPM 文档中将 Classic Load Balancer 侦听器配置为 HTTPS 或 TLS 终止
- 应在 Security Hub CSPM 文档中将 Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS

响应事件的安全建议

当组织中发生安全事件时，您的用户必须做好应对问题的准备。所有用户都应基本了解组织的安全响应流程。规划、培训和经验对于成功的事件响应计划至关重要。理想情况下，应在潜在的安全事件发生之前为组织做好准备。Wel AWS l-Architected Framework 确定了在云端成功实施事件响应计划所需的三个基础：准备、运营和事后活动。有关更多信息，请参阅 Well-Archit ecte AWS d Framework 中的 AWS 事件响应方面。

除了就事件通知您或自动响应事件的安全控制措施外，您可以为事件响应建立的控制措施非常有限。强大的事件响应态势主要通过您在组织中使用的计划、流程、运行手册、行动手册和培训计划来建立。您可以使用本节中的控制措施和建议为事件响应计划实施最佳实践。有关事件响应最佳实践和实施指南的更多信息，请参阅 Well-Architecte AWS d Framework 中的事件响应。

本节中的建议：

- 定义事件响应计划
- 创建和维护事件响应运行手册和行动手册
- 实施事件驱动型安全自动化
- 记录运营团队应如何参与 支持
- 配置安全事件提醒

定义事件响应计划

制定明确定义的事件响应计划（IRP）。事件响应计划旨在为您的事件响应计划奠定基础。此计划必须自定义以满足每个组织的需求。

有关更多信息，请参阅以下资源：

- 《AWS 安全事件响应指南》中的制定并测试事件响应计划
- 在 Well-Architecte AWS d Framework 中制定事件管理计划
- AWS Well-Architected Framework 中的确定关键人员和外部资源

创建和维护事件响应运行手册和行动手册

准备事件响应流程的关键环节是制定行动手册。事件响应行动手册提供了一系列建议步骤，供用户在发生安全事件时遵循。清晰的结构和步骤可简化响应，减少发生人为错误的可能性。

有关更多信息，请参阅以下资源：

- 《AWS 安全事件响应指南》中的应针对哪些事件场景创建行动手册
- AWS 事件响应手册样本已启用 GitHub
- AWS Well-Architected Framework 中的制定和测试安全事件响应行动手册

实施事件驱动型安全自动化

安全响应自动化是一种预定义且编程的操作，旨在自动响应或修复安全事件。这些自动化可作为检测性或响应性安全控制措施，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。

许多 AWS 服务 支持自动回复。例如，您可以为特定指标配置 Amazon CloudWatch 警报，警报可以在警报状态发生变化时启动操作。通过亚马逊 EventBridge，您还可以针对和 Amazon Inspector 中的发现配置自动响应 AWS Security Hub CSPM 和补救措施。

有关更多信息，请参阅下面的资源：

- AWS 安全博客中的 Remediate Amazon Inspector security findings automatically
- 在@@ 安全博客 AWS中开始使用 AWS 安全响应自动化
- 在 AWS 解决方案库 AWS中@@ 开启自动安全响应
- 在 CloudWatch 文档中@@ 使用 Amazon CloudWatch 警报
- Security Hub CSPM 文档中的@@ 自动响应和补救
- 在 Amazon Inspector 文档 EventBridge中与亚马逊一起创建对亚马逊 Inspector 发现的自定义回复

记录运营团队应如何参与 支持

您可以为自己 AWS 账户定义一个主要联系人和三个备用联系人。我们建议您为每位 AWS 账户 或您的组织提供一名安全联系人。

AWS 支持 提供了一系列计划，可提供工具和专业知识，以支持 AWS 解决方案的成功和运行健康。另外，请考虑使用 AWS Managed Services 代替 支持 计划是否会使您的组织受益。 AWS Managed Services (AMS) 通过提供对 AWS 基础设施的持续管理，包括监控、事件管理、安全指导、补丁支持和 AWS 工作负载备份，帮助您更高效、更安全地运营。AMS 支持模型可能更适合云运营团队资源有限的组织。我们建议您比较这些模型和计划，以选择最适合组织使用案例和云成熟程度的方案。

有关更多信息，请参阅以下资源：

- 在《AWS 安全事件 AWS 响应指南》中了解响应团队和支持
- 《AWS Account Management Guide》中的 Update the alternate contacts for your AWS 账户
- 在 AWS 网站上@@ 比较 支持 套餐
- AWS 规范性指导中@@ AWS Managed Services 用于实现目标业务成果的策略

配置安全事件提醒

检测异常与为控制该异常而实施的措施同样重要。警报是检测阶段的主要组成部分。它会根据感兴趣的 AWS 账户 活动生成通知，以启动事件响应流程。请确保提醒中包含团队采取行动所需的相关信息。

有关更多信息，请参阅以下资源：

- 《AWS 安全事件响应指南》中的检测
- 在 Well-Architecte AWS d Framework 中@@ 准备取证能力
- 在 Well-Ar AWS chitec@@ ted Framework 中实施可操作的安全事件

后续步骤

在继续云之旅的过程中，务必应用这些记录的控制措施、指引和修复选项。这些建议有助于提升云安全状况，并帮助您在 AWS Cloud中履行如 AWS 责任共担模式所定义的安全责任。

对于后续步骤，我们建议如下：

- 有关最佳实践和实施指引的更多信息，请查看 AWS Well-Architected Framework 的六个支柱。
- 对于组织使用的 AWS 服务，请查看可用 AWS Security Hub CSPM 控制措施列表，并评估是否应在您的环境中启用任何控制措施。
- 对于组织使用的 AWS 服务，请查看可用 AWS Config 托管规则列表，并评估是否应在您的环境中启用任何规则。

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
根用户的 MFA	我们更新了建议，并在根用户的 MFA 一节提供了更多信息。	2023 年 11 月 9 日
初次发布	—	2023 年 10 月 27 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 Cloud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 Cloud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 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 Cloud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 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

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 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

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 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

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 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。

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 Cloud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 Cloud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 Cloud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 Cloud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，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 Cloud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 Cloud 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 Cloud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。

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。