采用零信任：一种安全和敏捷的业务转型策略

AWS 规范性指导

AWS 规范性指导: 采用零信任：一种安全和敏捷的业务转型策略

Table of Contents

采用零信任：一种安全和敏捷的业务转型策略

Greg Gooden，Amazon Web Services（AWS）

2023 年 12 月（文档历史记录）

如今，各组织比以往任何时候均更加关注安全这一关键优先事项。这样会带来广泛的优势，从维护客户的信任，到提高员工的移动性，再到开启新的数字化商机。在此过程中，他们继续提出一个老生常谈的问题：确保我的系统和数据具有适当级别的安全性和可用性的最佳模式是什么？ 零信任已日益成为用来描述此问题的现代答案的术语。

零信任架构（ZTA）是一种概念模型和一组相关的机制，侧重于为数字资产提供安全控件，这些资产不仅仅或并非从根本上依赖于传统的网络控制或网络边界。相反，网络控制通过身份、设备、行为和其他丰富的上下文和信号进行增强，以做出更精细、智能、自适应和持续的访问决策。通过实施 ZTA 模型，您可以在网络安全的持续成熟中实现有意义的下一次迭代，特别是深度防御概念。

决策流程

实施 ZTA 策略需要仔细规划和决策。它涉及到评估各种因素并使它们与组织目标保持一致。开启 ZTA 之旅的关键决策流程包括：

1. 利益相关者参与 – 与其他首席高管、副总裁和高级管理人员接触，了解其优先事项、顾虑以及对组织安全状况的愿景，是至关重要的。通过从一开始就让关键利益相关者参与进来，您可以使 ZTA 的实施与总体战略目标保持一致，并获得必要的支持和资源。
2. 风险评测 – 开展全面的风险评测有助于识别问题、过大的表面面积和关键资产，从而帮助您在安全控件和投资方面做出明智的决策。评估组织的现有安全状况，找出潜在的弱点，并根据您所在行业和运营环境的特定风险状况确定需要改进的领域的优先级。
3. 技术评估 – 评测组织现有的技术发展趋势并找出差距，有助于选择符合 ZTA 原则的适当工具和解决方案。该评估应包括对以下内容的全面分析：
    - 网络架构
    - 身份和访问管理系统
    - 身份验证和授权机制
    - 统一端点管理
    - 资源所有权工具和流程
    - 加密技术

- 监控和日志记录功能
- 选择合适的技术堆栈对于构建强大的 ZTA 模型至关重要。

4. 变革管理 – 认识到采用 ZTA 模型的文化和组织影响至关重要。实施变革管理实践有助于确保平稳过渡和在整个组织中被接受。它涉及到教导员工了解 ZTA 原则和优势、提供有关新安全实践的培训，以及培养可鼓励问责制和持续学习的安全意识文化。

该规范性指导旨在为首席高管、副总裁和高级管理人员提供实施 ZTA 的全面策略。它将深入探讨 ZTA 的关键方面，包括以下内容：

- 组织就绪性
- 分阶段采用方法
- 利益相关者协作
- 实现安全、敏捷业务转型的最佳实践

通过遵循本指导，您的组织可以驾驭 ZTA 环境，并在 Amazon Web Services（AWS）Cloud 的安全之旅中取得成功结果。AWS 提供了可用于实施 ZTA 的各种服务，例如 AWS Verified Access、AWS Identity and Access Management（IAM）、Amazon Virtual Private Cloud（Amazon VPC）、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway 和 Amazon GuardDuty。这些服务可以帮助保护 AWS 资源免受未经授权的访问。

目标业务成果

本节将讨论与在您的整个组织中定义和实施零信任架构相关的预期结果。

改善安全状况

通过采用零信任原则，您的组织可以增强其安全状况，降低安全风险，并保护您的云基础设施和数据。零信任的基本原则是在必要时授予访问权限，再加上严格的控制措施，可显著减少表面面积，并限制安全事件的潜在影响。这种主动式方法可以帮助组织防范新出现的安全风险，并有助于确保资产的机密性、完整性和可用性。

无缝云采用

开发明确定义的零信任架构（ZTA）采用计划可帮助确保顺利成功地过渡到云环境。ZTA 原则通过为组织安全地获得云计算优势提供坚实的基础，从而与云安全最佳实践紧密结合。从一开始就采用零信任架构原则有助于您的组织设计以安全性为核心元素的云架构。

合规性与监管一致

实施零信任架构原则实践可以帮助您的组织满足行业和监管要求及标准。零信任架构本质上提倡最低权限原则，并实施严格的访问控制。访问控制通常由如下法规强制执行：

- 联邦风险与授权管理项目 (FedRAMP)
- 健康保险流通与责任法案 (HIPAA)
- 支付卡行业数据安全标准 (PCI DSS)。

通过采用零信任，您的组织可以帮助展示其对数据保护、隐私和监管合规性的承诺，同时最大限度地减小处罚或名誉受损的可能性。

增强数据保护

组织通过实施数据加密、访问控制和定期安全评测，可以在整个云采用过程中保护敏感数据。您的组织可以采取以下具体步骤：

- 数据加密 – 数据加密是将明文数据加密成加密文字的过程，这种方式需要密钥才能将数据解密回原始的明文形式。这使得未经授权的个人更难访问敏感数据，即使他们能够获得数据的副本也是如此。

- 访问控制 – 访问控制可限制谁可以访问敏感数据，以及他们可以对敏感数据执行哪些操作。这一点可以通过分配用户角色和权限，以及使用多重身份验证或其他方法来验证用户身份来实现。
- 定期安全评测 – 定期安全评测可以帮助组织识别和解决安全问题，并主动修复问题。可以由内部安全团队或外部安全公司开展这些评测。

零信任架构通过实施一系列安全措施来采取全面的数据保护方法。这些措施包括强力身份验证、数据加密和精细访问控制。此方法可以最大限度地降低与数据相关的安全事件风险，并保护敏感信息免遭未经授权的访问。

高效事件响应

组织通过在云环境中建立监控和事件响应框架，可以更快、更高效地检测和响应安全事件。零信任架构强调持续监控、威胁情报集成以及对用户活动、网络流量和系统行为的实时可见性。然后，安全团队可以主动识别和缓解安全事件。这种方法可缩短检测和响应潜在问题所需的时间，并将对业务运营的影响降至最低。关键点包括：

- 测试 – 无论您的组织采用何种事件响应框架或方法，您均应该定期测试事件响应计划。桌面演练、模拟和红队研判提供了机会，在现实环境中练习事件响应、发现工具和功能差距，并建立事件响应者的经验和信心。
- 监控 – 持续监控您的云环境中是否有异常活动的迹象。为此，您可以使用各种工具和技术，例如日志分析、网络监控和脆弱性扫描。
- 威胁情报集成 – 将威胁情报集成到您的监控和事件响应框架中。这样将帮助您的组织更快、更高效地识别和响应威胁。
- 实时可见性 – 为了快速识别和响应安全事件，您的组织需要实时了解用户活动、网络流量和系统行为。
- 主动识别和缓解 – 通过主动识别和缓解安全事件，您的组织可以缩短检测和响应潜在威胁的时间，从而最大限度地减少对业务运营的影响。

提高员工的工作效率

现代员工需要灵活性，以便可在地点、设备和时间组合日益增多的情况下完成工作。通过实施 ZTA，您可以支持这些要求并提高员工的移动性、工作效率和满意度，同时维护或改善组织的安全状况。

实现数字化转型

作为数字化转型的一部分，组织越来越多地寻求传统网络边界之外的设备、计算机、设施、基础设施和流程的互连。物联网（IoT）和运营技术 [OT，也称为工业物联网（IIoT）] 设备通常将遥测和预测性维护信息直接传输到云端。为了保护工作负载，这就需要应用超出传统边界方法的安全控件。

章节摘要

通过专注于这些目标业务成果，您的组织可以充分发挥 ZTA 的潜力，并加强您在云中的安全状况。重要的是要使这些成果与特定的组织目标保持一致，根据您的独特业务需求对其进行量身定制，并定期评测其有效性，以推动持续改善。

了解零信任原则

零信任架构（ZTA）基于构成其安全模型基础的一组核心原则。了解这些原则对于希望有效采用 ZTA 策略的组织具有至关重要的意义。本节介绍了 ZTA 的核心原则。

验证和身份验证

验证和身份验证原则强调了对所有类型的主体（包括用户、计算机和设备）执行严格的识别和身份验证的重要性。ZTA 要求在整个会话中持续验证身份和身份验证状态，最好是针对每个请求进行验证。它不单单依赖于传统的网络位置或控制。这一点包括实施现代严格的多重身份验证（MFA），以及在身份验证过程中评估其他环境和上下文信号。组织通过采用这一原则，可以帮助确保资源授权决策具有尽可能最佳的身份输入。

最低权限访问

最低权限原则涉及到授予主体执行其任务所需的最低级别的访问权限。组织通过采用最低权限访问原则，可以执行精细的访问控制，这样主体只能访问履行其角色和职责所需的资源。这包括实施即时访问预置、基于角色的访问控制（RBAC）和定期访问审核，以最大限度地减少表面面积和未经授权访问的风险。

微分段

微分段是一种网络安全策略，它将网络划分为更小的隔离分段，用于授权特定的流量。您可以通过创建工作负载边界并在不同分段之间实施严格的访问控制来实现微分段。

可以通过网络虚拟化、软件定义网络（SDN）、基于主机的防火墙、网络访问控制列表（NACL）和 AWS 特定功能 [如 Amazon Elastic Compute Cloud（Amazon EC2）安全组或 AWS PrivateLink] 来实施微分段。分段网关可控制不同分段之间的流量，以明确授权访问权限。微分段和分段网关可帮助组织限制通过网络的不必要路径，尤其是那些通往关键系统和数据的路径。

持续监控和分析

持续监控和分析涉及到在整个组织的环境中收集、分析和关联与安全相关的事件和数据。您的组织通过实施可靠的监控和分析工具，从而能够以融合的方式评估安全数据和遥测数据。

该原则强调了解用户行为、网络流量和系统活动以识别异常和潜在安全事件的重要性。安全信息和事件管理（SIEM）、用户和实体行为分析（UEBA）以及威胁情报平台等高级技术在实现持续监控和主动威胁检测方面发挥着至关重要的作用。

自动化和编排

自动化和编排可帮助组织简化安全流程，减少人工干预，并缩短响应时间。您的组织通过自动执行日常安全任务和使用编排功能，可以实施一致的安全策略并快速响应安全事件。该原则还包括自动执行访问预置和取消预置流程，以帮助确保及时、准确地管理用户权限。通过采用自动化和编排，您的组织可以提高运营效率，减少人为错误，并将资源集中在更具战略性的安全计划上。

授权

在 ZTA 中，访问资源的每个请求均应由门控实施点明确授权。除了经过身份验证的身份外，授权策略还应考虑其他上下文，例如设备运行状况和状态、行为模式、资源分类和网络因素。授权流程应根据与正在访问的资源相关的相应访问策略来评估这种融合的上下文。最理想的情况是，机器学习模型可以为声明性策略提供动态补充。使用时，这些模型应仅关注其他限制，且不应授予未明确指定的访问权限。

章节摘要

通过遵守 ZTA 的这些核心原则，组织可以建立与现代企业环境的多样性保持一致的强大安全模型。实施这些原则需要采用综合方法，将技术、流程和人员结合起来，以实现零信任思维方式并构建弹性安全状况。

零信任架构的关键组件

为了有效实施零信任架构（ZTA）策略，您的组织必须了解构成 ZTA 的关键组件。这些组件协同工作，以持续改进符合零信任原则的全面安全模型。本节介绍了 ZTA 的这些关键组件。

Identity and Access Management

身份和访问管理通过提供可靠的用户身份验证和粗略访问控制机制，构成了 ZTA 的基础。它包括诸如单点登录（SSO）、多重身份验证（MFA）以及身份治理和管理解决方案等技术。身份和访问管理可提供高级别的身份验证保障和重要上下文，这些对于做出零信任授权决策是不可或缺的。同时，ZTA 是一种安全模型，在这种模型中，对应用程序和资源的访问权限是按用户、按设备和按会话授予的。这样有助于保护组织免受未经授权的访问，即使用户的凭证遭到泄露也是如此。

安全访问服务边缘

安全访问服务边缘（SASE）是一种新的网络安全方法，它将网络和安全功能虚拟化、组合和分发到一个基于云的单一服务中。无论用户身在何处，SASE 都可以提供对应用程序和资源的安全访问。

SASE 包括各种安全功能，例如安全 Web 网关、防火墙即服务和零信任网络访问（ZTNA）。这些功能协同工作，以保护组织免受各种威胁，包括恶意软件、网络钓鱼和勒索软件。

数据丢失防护

数据丢失防护（DLP）技术可以帮助组织保护敏感数据免遭未经授权的信息泄露。DLP 解决方案监视和控制动态数据和静态数据。这样可以帮助组织定义和实施可防止与数据相关的安全事件的策略，从而帮助确保敏感信息在整个网络中受到保护。

安全信息和事件管理

安全信息和事件管理（SIEM）解决方案从组织基础设施中的各种来源收集、聚合和分析安全事件日志。您可以使用此数据来检测安全事件，促进事件响应，并提供对潜在威胁和脆弱性的洞察。

特别是对于 ZTA，SIEM 解决方案关联和理解来自不同安全系统的相关遥测数据的能力对于改进对异常模式的检测和响应至关重要。

企业资源所有权目录

为了正确授予对企业资源的访问权限，组织必须有一个可靠的系统来对这些资源进行编目，更重要的是，要知道谁拥有这些资源。此事实来源需要提供工作流，以促进访问请求、相关审批决策及其定期认证。随着时间的推移，此事实来源将包含组织内部“谁可以访问什么？”的答案。您可以将答案用于授权、审核和合规性。

统一端点管理

除了对用户进行强制身份验证外，ZTA 还必须考虑用户设备的运行状况、状况和状态，以评测公司数据和资源访问是否安全。统一端点管理（UEM）平台提供以下功能：

- 设备预调配
- 持续的配置和补丁管理
- 安全基线
- 遥测报告
- 设备清理和停用

基于策略的执行点

在 ZTA 中，对每个资源的访问应由基于门控策略的执行点明确授权。最初，这些执行点可以基于现有网络和身份系统中的现有执行点。通过考虑由 ZTA 提供的更广泛的上下文和信号，可以逐步提高执行点的功能。从长远来看，您的组织应实施特定于 ZTA 的执行点，这些执行点在融合上下文上运行，始终如一地集成信号提供程序，维护全面的策略集，并通过从组合遥测中收集的情报进行增强。

章节摘要

了解这些关键组件对于计划采用 ZTA 的组织具有至关重要的意义。通过实施这些组件并将其集成到一个内聚安全模型中，您的组织可以基于零信任原则建立强大的安全状况。以下各节探讨了组织就绪性、分阶段采用方法和最佳实践，以帮助您在组织内成功实施 ZTA。

评测组织就绪性以采用零信任

采用新的架构策略是一项艰巨的任务，需要仔细规划并考虑组织因素。本节重点介绍在整个企业中采用零信任的关键组织就绪性注意事项。通过因应这些注意事项，您的组织可以为实现更强大、更成功的安全状况铺平道路。

领导层的协调和沟通

领导层的协调和沟通对于成功实施零信任具有至关重要的意义。领导层必须了解零信任的优势和所需的资源。领导者还必须愿意变革组织的文化和流程。要建立信任和认同，就必须与员工进行沟通。员工需要了解组织为何要实施零信任，这对他们意味着什么，以及他们如何能够提供帮助。沟通应该是公开、透明和持续的。

领导层的支持和认同

要成功实施零信任架构（ZTA），在架构的目标、优势和成功的衡量标准方面与关键利益相关者和高管保持一致，这一点是至关重要的。分享零信任原则在增强安全性和实现业务敏捷性方面的重要性，方法为：从传统的基于边界的安全性转向更精细的、以用户为中心的方法。您的组织通过切换到这种方法，可以更快地适应变革和威胁。高管协调为组织定下了基调，并有助于克服潜在的变革阻力。

透明的沟通

在实施零信任的整个过程中，与员工保持开放、透明的沟通。解释采用零信任的理由、优势和预期结果，并及时解决顾虑问题。定期提供有关实施进展的更新信息。这样将会增加认同、减少阻力并建立信任。

技能开发和培训

在领导层协调一致、开放沟通之后，重要的是培养要实施零信任的员工掌握相关技能和知识。这些技能和知识包括了解零信任原则、如何在工作中实施这些原则，以及如何应对安全事件。提供培训和发展机会，帮助员工掌握这些技能。

云知识和技能

评测组织在云技术和零信任原则方面的技能和知识差距。提供培训和发展计划，以提高员工的技能，让他们具备必要的专业知识，以便在以云为中心的零信任环境中高效地工作。为了跟上不断发展的技术和安全实践的步伐，要培养持续学习的文化。

安全文化和意识

评测组织的安全文化。评估员工的安全意识水平、他们对安全最佳实践的理解以及他们对政策和程序的遵守情况。确定在安全知识方面的任何差距。考虑开展安全意识培训计划，教导员工了解零信任的重要性及其在维护安全环境方面的作用。

组织结构和角色

要成功实施零信任，请建立有效的组织结构和角色。这包括创建云卓越中心（CCoE）、审查和修改安全操作，以及分配脆弱性管理、事件响应和安全监控的角色和职责。

云卓越中心

建立 CCoE（云卓越中心），以便针对云运营提供指导、最佳实践和监督。CCoE 是负责创建和实施与云相关的最佳实践、指南和治理策略的团队或群体。CCoE 应包括来自不同业务部门和 IT 团队的代表，以帮助确保协作和协调一致。CCoE 在推动云托管工作负载中采用零信任原则方面发挥着至关重要的作用。CCoE 还促进了整个组织的知识共享。

安全运营

要满足零信任环境的需求，请查看和修改当前的安全运营组织。要提高监控、事件响应和威胁情报功能，请考虑实施安全运营中心（SOC）或托管安全服务提供商（MSSP）。确定脆弱性管理、事件响应和安全监控的角色和职责。运转良好的事件响应流程对于确保能够快速检测和修复微小的安全事件以中断事件序列具有至关重要的意义。这有助于防止微小的事件演变为更具影响力的事件。

IT 基础设施和架构

检查贵公司的 IT 架构和基础设施，找出可能影响采用零信任方法的任何限制或依赖项。确定当前的应用程序和系统是否与必要的零信任架构组件兼容。分析是否需要对基础设施进行任何改进或调整，以支持零信任原则的成功部署。对于每个应用程序或系统，请考虑零信任在原地实施效果最好，还是通过更大的现代化工作来实施效果最好。

风险管理、治理和变更控制

要成功实施零信任，请建立有效的风险管理、治理和变更控制流程。这一点包括使风险管理与零信任原则保持一致，制定事件响应计划，与法律和合规性部门合作，以及建立变更控制流程。

风险管理

检查贵公司实施的风险管理策略，并确定其对零信任原则的遵循程度。分析当前事件响应系统、安全措施和风险评测程序的效率。确定需要改进哪些领域以符合零信任策略。开始开发自动化事件响应系统或持续监控和分析框架，以加快解决问题的速度。

变更控制流程

为了帮助确保所有与云相关的修改均符合安全性和合规性要求，请建立有效的变更控制方法。建立系统性变更管理程序，包括安全配置分析、风险评估、审批和文档。经常审查和审计更新，以保持零信任架构的完整性。

监控和评估

要成功实施零信任，您的组织必须持续监控和评估其安全状况。这一点包括制定关键绩效指标（KPI）、监控和评估关键绩效指标，以及培养持续改进的文化。通过遵循这些步骤，组织可以确保成功实施零信任并始终努力提高其安全性。

关键绩效指标

建立相关的关键绩效指标（KPI），以衡量零信任部署的成功和有效性。这些 KPI 可以衡量用户满意度、设备和推出进度、成本降低、合规性遵守情况以及安全事件的数量。要跟踪整体发展情况并寻找改进机会，请定期监控和评估这些关键绩效指标。

持续改进

建立系统以征求利益相关者的意见和洞察将有助于培养持续改进的文化。鼓励员工为改善云环境的安全性、有效性和用户体验而提供想法和提议。使用此输入来简化程序、改进安全措施并刺激创新。

章节摘要

通过应对这些组织和文化方面的注意事项，您的组织可以为零信任安全模型的云采用营造一个支持性环境。下一节将探讨分阶段采用方法，并就如何以实用且可管理的方式逐步实施零信任原则提供指导。

培养零信任心态

实现零信任不仅限于技术实现。这需要您的组织内部进行文化转变。培养零信任心态涉及强调以下关键方面。

零信任教育和培训

教育员工了解零信任架构 (ZTA) 的价值和优势。通过培训课程、研讨会和其他资源提供 ZTA 概念和方法的技术和非技术性解释。鼓励工作人员意识到自己在建立和维护零信任安全模式方面的责任。

协作和沟通

促进参与 ZTA 实施的所有团队和部门的协作和透明度。为了确保每个人都对计划有透彻的了解，促进跨职能沟通、知识共享和信息交流。营造一种分担责任的文化，让每个人都认识到自己对企业整体安全所做贡献的重要性。

持续学习和改进

在零信任的背景下，优先考虑持续学习和改进。鼓励员工及时了解最新的安全趋势、技术和最佳实践。培育创新和实验文化，鼓励员工探索新的解决方案和方法，以加强组织的安全态势。

指标和问责制

建立明确的指标和问责机制，以衡量零信任战略的有效性。定义与组织安全目标一致的关键绩效指标 (KPI)，并定期跟踪进度。要求个人和团队为实施和维护零信任原则所做的贡献负责。

章节摘要

通过解决这些问题并培养零信任心态，组织可以为成功采用和实施零信任奠定坚实的基础。这种文化转变对于帮助组织中的每个人了解零信任的重要性并为其成功做出积极贡献至关重要。

下一节探讨分阶段采用的方法，为如何以切实可行和可管理的方式逐步实施零信任原则提供指导。

分阶段实现零信任的方法

采用零信任架构（ZTA）需要仔细地进行规划和实施。我们建议利用分阶段采用方法，以实现平稳过渡并最大限度地减少对业务运营的干扰。本节就采用 ZTA 所涉及的关键阶段提供指导。

阶段 1：评测和规划

零信任实施的第一阶段是评测和规划。此阶段对于整体实施的成功至关重要，因为它涉及到识别和弥合您的组织当前安全状况中的任何差距。通过花时间评测您的当前状态并定义安全目标，您可以为成功实施零信任奠定基础。

同时，完全完整和准确的评测可能并非总是现实的。为避免分析瘫痪导致您无法继续进入后续阶段，做好权限分离或接受某种程度的缺陷的准备。

1. 评测当前状态 – 对现有的安全基础设施、策略和控制措施开展评测。确定潜在的脆弱性、安全差距，以及零信任原则的实施可以提供改进的领域。
2. 定义安全目标 – 根据当前状态评测调查发现，定义符合零信任原则的安全目标。这些安全目标还应与组织的总体安全策略保持一致，并解决已发现的脆弱性和差距。
3. 设计架构 – 制定一个支持组织的安全目标的 ZTA。该架构应包括必要的组件，例如身份和访问管理解决方案、网络分段机制和持续监控系统。该架构还应具有可扩展性、较强的适应性，并能够适应未来的增长和技术进步。理想情况下，这种架构应以一种易于由负责实施的团队使用的格式来表示，例如 AWS CloudFormation 模板，而不仅仅是文档或图表。
4. 让利益相关者参与 – 让所有利益相关者（包括业务部门、IT 团队和安全团队）参与进来，以获得洞察并使其目标与 ZTA 实施计划保持一致。鼓励协作和沟通，以建立对零信任方法的优势和要求的共识。

阶段 2：试点和实施

零信任实施的第二个阶段是试点和实施。此阶段涉及到在小规模、受控的环境中测试 ZTA，然后在整个组织中对其进行迭代部署。教导员工了解新的安全措施以及他们在维护零信任环境方面的角色非常重要。

1. 试点部署 – 在小规模、受控的环境中测试 ZTA。实施在架构设计阶段定义的必要组件和安全控件。密切监控试点部署、收集反馈并进行必要的调整。当零信任从一种假设的练习转变为您正在积累真实体验的实操时，请做好在过程的早期保持灵活性的准备。

2. 迭代部署 – 根据从试点部署中吸取的经验教训，开始在整个组织中迭代部署零信任。通过飞轮效应建立势头，该方法无需广泛的活动即可实现关键的部署量。在可能需要的地方，为推出的余尾部分保留领导层授权或升级。
3. 提供用户培训并提高意识 – 教导员工了解新的安全措施及其在维护零信任环境方面的角色。强调安全实践的重要性，例如强密码、多重身份验证和定期安全更新。
4. 管理变更 – 创建全面的变更管理计划，以应对与采用零信任相关的组织和文化变革。向员工传达采用背后的优势和理由，并应对任何顾虑或阻力。提供持续的支持和指导，以促进平稳过渡。

阶段 3：监控和持续改进

零信任实施的第三个（也是最后一个）阶段是监控和持续改进。此阶段涉及到制定全面的监控和分析计划，创建全面的事件响应计划，并定期征求利益相关者和用户的反馈。

1. 持续监控 – 建立全面的监控和分析计划，以持续评测安全状况并检测任何潜在的异常情况。使用高级安全工具和技术监控用户行为、网络流量和系统活动。
2. 规划事件响应和补救 – 创建符合零信任原则的全面事件响应计划。建立明确的上报途径，定义角色和职责，并在可能的情况下实施自动化事件响应机制。定期测试和更新事件响应计划。
3. 获取反馈和评估 – 定期征求利益相关者和用户的反馈，以收集对零信任架构（ZTA）有效性的洞察。定期开展评估和评测，以衡量对安全状况、运营效率和用户体验的影响。使用反馈和评估结果来确定需要改进的领域。预计您的 ZTA 会随着时间的推移而发生变化，并考虑开发团队将如何以极小的工作量或中断来实施这些更新。

章节摘要

组织通过遵循这种分阶段采用方法，可以有效地过渡到 ZTA，同时最大限度地减少风险和中断。下一节将讨论实现成功实施零信任的最佳实践，涵盖面向首席高管、副总裁和高级管理人员的关键注意事项和建议。

利用零信任取得成功的最佳实践

成功采用零信任架构（ZTA）需要采取战略方法并遵循最佳实践。本节介绍了一套最佳实践，用于指导首席高管、副总裁和高级管理人员成功采用零信任。通过遵循以下建议，您的组织可以建立强大的安全基础，并实现零信任方法的优势：

- 定义明确的目标和业务成果 – 明确定义云运营的目标和预期的业务成果。将这些目标与零信任原则保持一致，以在实现业务增长和创新的同时，奠定坚实的安全基础。
- 开展全面评测 – 对当前的 IT 基础设施、应用程序和数据资产执行全面评估。确定依赖项、技术债务和潜在的兼容性问题。此评估将为采用计划提供信息，并帮助根据重要性、复杂性和业务影响来确定工作负载的优先级。
- 制定采用计划 – 纳入详细的采用计划，该计划概述了将工作负载、应用程序和数据迁移到云端的分步方法。定义采用阶段、时间表和依赖项。吸引关键利益相关者并相应地分配资源。
- 尽早开始构建 – 在您开始构建和部署零信任（而不是分析和讨论它）之后，您在组织中真实地呈现零信任状态的能力将显著提高。
- 获取高管赞助 – 确保高管对实施零信任的赞助和支持。让其他首席级高管参与进来，以支持相应计划并分配必要的资源。领导层承诺对于推动成功实施所需的文化和组织变革具有至关重要的意义。
- 实施治理框架 – 创建治理框架，用于定义零信任实施的角色、责任和决策流程。明确定义安全控件、风险管理和合规性的问责和所有权。定期审核和更新治理框架，以适应不断变化的安全要求。
- 支持跨职能协作 – 鼓励不同业务部门、IT 团队和安全团队之间进行协作和沟通。营造一种责任共担文化，以在整个零信任实施过程中促进一致性和协调性。鼓励频繁互动、知识共享和共同解决问题。
- 保护您的数据和应用程序 – 零信任所涉及的不只是最终用户访问资源和应用程序。零信任原则还应在工作负载内部和工作负载之间实施。通过同样使用数据中心内的所有可用上下文，从而应用相同的技术原则，即强身份、微分段和授权。
- 提供深度防御 – 通过使用多层安全控件来实施深度防御策略。将多重身份验证（MFA）、网络分段、加密和异常检测等各种安全技术相结合，以提供全面的保护。确保每一层均相互补充，以创建强大的防御系统。
- 需要强力身份验证 – 对访问所有资源的所有用户强制使用强力身份验证机制，例如 MFA。理想情况下，可以考虑现代 MFA，例如 FIDO2 硬件支持的安全密钥，它为零信任提供了高水平的身份验证保障，并具有广泛的安全优势（例如，防范网络钓鱼）。
- 集中和改进授权 – 对每一次访问尝试提供专门授权。根据协议的具体信息，应根据每个连接或根据每个请求执行此操作。根据每个请求执行此操作为理想之选。使用所有可用上下文（包括身份、设备、行为和网络信息），做出更精细、更自适应和更高级的授权决策。

- 使用最低权限原则 – 实施最低权限原则，向用户授予履行其工作职责所需的最低访问权限。根据工作角色、职责和业务需求定期审核和更新访问权限。实施即时访问预置。
- 使用特权访问管理 – 实施特权访问管理（PAM）解决方案来保护特权账户并降低未经授权访问关键系统的风险。PAM 解决方案可以提供特权访问控制、会话记录和审计功能，帮助您的组织保护其最敏感的数据和系统。
- 使用微分段 – 将您的网络划分为更小、更隔离的分段。使用微分段，根据用户角色、应用程序或数据敏感度在不同分段之间强制实施严格的访问控制。努力消除所有不必要的网络路径，尤其是那些通向数据的路径。
- 监控和响应安全警报 – 在云环境中实施全面的安全监控和事件响应计划。使用云原生安全工具和服务实时检测威胁、分析日志并自动执行事件响应。建立明确的事件响应程序、定期开展安全评测，并持续监控异常或可疑活动。
- 使用持续监控 – 要快速有效地检测和响应安全事件，请实施持续监控。使用高级安全分析工具监控用户行为、网络流量和系统活动。自动发出警报和通知，以确保事件得到及时响应。
- 倡导安全性和合规性文化 – 在整个组织中倡导安全性和合规性文化。教导员工安全最佳实践、遵守零信任原则的重要性以及员工在维护安全云环境中的作用。定期开展安全意识培训，以帮助确保员工警惕社交工程，并了解自己在数据保护和隐私方面的责任。
- 使用社交工程模拟 – 执行社交工程模拟，以评测用户对社交工程攻击的敏感性。使用模拟结果量身定制培训计划，以提高用户对潜在威胁的认知和响应。
- 倡导持续教育 – 通过提供持续的安全培训和资源，建立持续教育和学习的文化。让用户随时了解不断演变的安全最佳实践。鼓励用户保持警惕，及时举报任何可疑活动。
- 持续评测和优化 – 定期评测云环境以了解需要改进的领域。使用云原生工具监控资源使用情况和性能，并开展脆弱性评测和渗透测试，以识别和解决任何弱点。
- 建立治理和合规性框架 – 建立治理和合规性框架，以帮助确保您的组织符合行业标准和监管要求。在该框架中，定义策略、程序和控制措施，以保护数据和系统免遭未经授权的访问、使用、披露、中断、修改或破坏。实施跟踪和报告合规性指标的机制，定期执行审计，并及时解决任何不合规问题。
- 鼓励协作和知识共享 – 鼓励参与 ZTA 采用的团队之间的协作和知识共享。为此，您可以促进 IT、安全和业务部门之间的跨职能沟通与协作。您的组织还可以建立论坛、研讨会和知识共享会话，以促进了解、应对挑战并分享在整个采用过程中吸取的经验教训。

关键要点

本指南探讨了成功制定零信任架构（ZTA）策略的重要方面。本节总结了所提供的规范性指导的关键要点：

- 了解零信任原则 – 零信任是一种概念模型和一组相关的机制，侧重于为数字资产提供安全控件，这些资产不仅仅或并非从根本上依赖于传统的网络控制或网络边界。相反，网络控制通过身份、设备、行为和其他丰富的上下文和信号进行增强，以做出更精细、智能、自适应和持续的访问决策。让自己熟悉零信任的核心原则，例如最低权限、微分段、持续身份验证和自适应授权。
- 定义明确的目标 – 明确定义 ZTA 采用的目标和预期业务成果。将这些目标与零信任原则保持一致，以在实现业务增长和创新的同时，帮助确保奠定坚实的安全基础。
- 开展全面评测 – 对您现有的 IT 基础设施、应用程序和数据资产执行全面评测。确定依赖项、技术债务和兼容性问题，以便为您的采用策略提供信息。
- 制定 ZTA 采用计划 – 创建详细的计划，该计划概述了将工作负载、应用程序和数据迁移到云端的分步方法。考虑合规性要求和应用程序现代化等因素。
- 实施强大的 ZTA – 设计和实施可实施精细访问控制、强力身份验证机制和持续监控的 ZTA。为了更高效地采用 ZTA，请使用云原生零信任服务，例如 AWS Verified Access 和 Amazon VPC Lattice。
- 确定数据和应用程序安全性的优先级 – 应用零信任原则（强身份、微分段和授权）来提供所有可用的上下文。将此上下文用于用户访问系统和资源，以及后端组件内部及其之间的通信和数据流。
- 建立监控和事件响应框架 – 在云环境中实施强大的安全监控和事件响应功能。使用云原生安全工具进行实时威胁检测、日志分析和事件响应自动化，例如 Amazon Inspector、AWS Security Hub 和 Amazon GuardDuty。
- 培养安全性和合规性文化 – 在整个组织中倡导安全意识和合规性文化。教导员工了解安全最佳实践及其在维护安全云环境方面的作用。
- 持续评测和优化 – 定期评测云环境、安全控件和运营流程。要收集洞察并优化资源利用率、成本管理和性能，请使用云原生分析和监控工具，例如 Amazon CloudWatch 和 AWS Security Hub。
- 建立治理和合规性框架 – 制定符合行业标准和监管要求的治理和合规性框架。定义策略、程序和控制措施，以帮助确保遵守安全性、隐私和合规性标准。

后续步骤

采用零信任架构（ZTA）是改善组织状况和降低风险的最安全方法之一。本规范性指导为您提供了实施零信任的全面路线图，从了解原则到评测您的就绪性，再到实施必要的组件，不一而足。

此工作流或域中的后续步骤涉及以下内容：

- 实施采用计划
- 实施 ZTA
- 定期开展安全评测
- 持续优化云环境和安全控件

ZTA 是一个持续的过程，需要持续的监测、评估和调整，以确保奠定坚实的安全基础。通过遵循本指导中概述的最佳实践，您的组织可以增强其安全状况，确保遵守法规，并保护敏感数据。

常见问题

本节提供有关设计和实施零信任架构（ZTA）的常见问题的解答。

什么是零信任？

零信任是一种概念模型和一组相关的机制，侧重于为数字资产提供安全控件，这些资产不仅仅或并非从根本上依赖于传统的网络控制或网络边界。相反，网络控制通过身份、设备、行为和其他丰富的上下文和信号进行增强，以做出更精细、智能、自适应和持续的访问决策。

哪些 AWS 服务可以帮助我实施零信任架构？

AWS 提供了多种有助于实施零信任的服务，例如 AWS Verified Access、AWS Identity and Access Management（IAM）、Amazon Virtual Private Cloud（Amazon VPC）、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway 和 Amazon GuardDuty。

如何能够使用 AWS 确保数据安全？

AWS 提供 AWS Key Management Service（AWS KMS）等服务用于静态和传输中的数据加密，提供 Amazon Virtual Private Cloud（Amazon VPC）用于网络隔离，还提供 AWS Secrets Manager 用于安全存储和检索凭证。

AWS 能否帮助满足零信任环境中的合规性要求？

能，AWS 提供合规计划和服务，以帮助满足各种监管要求。AWS Artifact 提供对 AWS 合规性报告的访问权限，而 AWS Config 支持对合规性的持续监控和评测。

是否有任何 AWS 工具或服务可用于在零信任环境中自动执行安全性？

AWS 提供用于集中和自动化安全调查发现的 AWS Security Hub 等服务，以及用于定义和实施安全策略的 AWS Config 规则。

如何利用 AWS 确保在零信任云环境中进行持续监控和事件响应

AWS 提供用于实时监控的 Amazon CloudWatch 等服务，以及用于日志记录和分析的 AWS CloudTrail 等服务。有关事件响应最佳实践，您可以使用《AWS Security Incident Response Guide》。

资源

参考信息

- What is a cloud center of excellence and why should your organization create one? – 这篇博文概述了云卓越中心（CCoE）、有关如何创建有效的 CCoE 的最佳实践等。
- AWS 上的零信任 – 本页概述了 AWS 环境中的零信任安全原则和最佳实践。
- Zero Trust architecture: An AWS perspective – 这篇博文分享了 AWS 实施零信任方式的定义和指导原则。
- AWS Identity and Access Management（IAM）用户指南 – 本指南提供了有关在 IAM 中管理用户访问和权限的综合性文档，而 IAM 是零信任架构的关键组件。
- AWS Security Hub – 了解 Security Hub，该服务可让您全面了解跨 AWS 账户 的安全警报和合规性状态。
- AWS Well-Architected Framework – 探索 Well-Architected Framework，它提供了有关在 AWS 上构建安全、高性能、弹性和高效架构的指导。
- AWS Security Incident Response Guide – 该指南概述了在组织的 AWS Cloud 环境中响应安全事件的基础知识。它概述了云安全和事件响应概念，并确定了响应安全问题的客户可以使用的云功能、服务和机制。

工具

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- AWS Verified Access

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
添加了更新	向零信任架构的关键组件一节添加了信息，在评测组织就绪性以采用零信任一节中进行了更改，向最佳实践部分添加了信息，并对常见问题进行了更改。	2023 年 12 月 4 日
初次发布	—	2023 年 6 月 19 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SQL兼容 Amazon Aurora Postgre 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：将您的本地 Oracle 数据库迁移到适用于 Oracle 的 Amazon Relational Database Service (AmazonRDS) AWS Cloud。
- 重新购买 - 转换到其他产品，通常是从传统许可转向 SaaS 模式。示例：将您的客户关系管理 (CRM) 系统迁移到 Salesforce.com。
- 更换主机（直接迁移）- 将应用程序迁移到云中，无需进行任何更改即可利用云功能。示例：在中的EC2实例上将您的本地 Oracle 数据库迁移到 Oracle AWS Cloud。
- 重新定位（虚拟机监控器级直接迁移）：将基础设施迁移到云中，无需购买新硬件、重写应用程序或修改现有操作。您可以将服务器从本地平台迁移到同一平台的云服务。示例：迁移 Microsoft Hyper-V 申请到 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

对一组行进行操作并计算该组的单个返回值的SQL函数。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？

人工智能运营 (AIOps)

使用机器学习技术解决运营问题、减少运营事故和人为干预以及提高服务质量的过程。有关如何在 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、耐久性 () 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，ABAC请参阅 AWS Identity and Access Management (IAM) 文档 AWS中的。

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。您可以在 Amazon Detective 中使用行为图来检查登录尝试失败、可疑API呼叫和类似操作。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。当您确信时，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CDC用于各种用途，例如审计或复制目标系统中的更改以保持同步。

混沌工程

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

CI/CD

查看持续集成和持续交付。

分类

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

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心 (CCoE)

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

云计算

通常用于远程数据存储和 IoT 设备管理的云技术。云计算通常与边缘计算技术相关。

云运营模型

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

云采用阶段

组织迁移到以下阶段时通常会经历四个阶段 AWS Cloud：

- 项目 - 出于概念验证和学习目的，开展一些与云相关的项目
- 基础 — 进行基础投资以扩大云采用率（例如，创建着陆区、定义CCoE、建立运营模型）

- 迁移 - 迁移单个应用程序
- 重塑 - 优化产品和服务，在云中创新

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

CMDB

参见配置管理数据库。

代码存储库

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

冷缓存

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

冷数据

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

计算机视觉 (CV)

人工智能领域，使用机器学习来分析和提取数字图像和视频等视觉格式中的信息。例如， AWS Panorama 提供将 CV 添加到本地摄像机网络的设备，而 Amazon 则为 CV SageMaker 提供图像处理算法。

配置偏差

对于工作负载，配置会从预期状态发生变化。这可能会导致工作负载变得不合规，而且通常是渐进的，不是故意的。

配置管理数据库 (CMDB)

一种存储库，用于存储和管理有关数据库及其 IT 环境的信息，包括硬件和软件组件及其配置。您通常使用来自投资组合CMDB中的迁移发现和分析阶段的数据。

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模板将合规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 Cloud 可以降低隐私风险、成本和分析碳足迹。

数据边界

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

数据预处理

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

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

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

数据库定义语言 (DDL)

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言 (DML)

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

参见数据库定义语言。

深度融合

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

深度学习

一个 ML 子字段使用多层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。

部署

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

开发环境

参见环境。

侦测性控制

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

开发价值流映射 (DVSM)

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

数字孪生

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

维度表

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

灾难

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

灾难恢复 (DR)

您用来最大限度地减少灾难造成的停机时间和数据丢失的策略和流程。有关更多信息，请参阅 Well-Architected 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。有关如何使用带有 strangler fig 模式的域驱动设计的信息，请参阅对旧版 Microsoft 进行现代化改造。ASP NET(ASMX) 通过使用容器和 Amazon API Gateway 逐步提供网络服务。

DR

参见灾难恢复。

漂移检测

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

DVSM

参见开发价值流映射。

E

EDA

参见探索性数据分析。

边缘计算

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

加密

一种将人类可读的纯文本数据转换为密文的计算过程。

加密密钥

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

字节顺序

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

端点

参见服务端点。

端点服务

您可以托管在虚拟私有云 (VPC) 中以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。这些账户或委托人可以通过创建接口终端节点私密连接到您的终VPC端节点服务。有关更多信息，请参阅 Amazon Vir tual Private Cloud (AmazonVPC) 文档中的创建终端节点服务。

企业资源规划 (ERP)

一种自动化和管理企业关键业务流程（例如会计和项目管理）的系统。MES

信封加密

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

environment

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

- 开发环境 — 正在运行的应用程序的实例，只有负责维护应用程序的核心团队才能使用。开发环境用于测试更改，然后再将其提升到上层环境。这类环境有时称为测试环境。
- 下层环境 — 应用程序的所有开发环境，比如用于初始构建和测试的环境。
- 生产环境 — 最终用户可以访问的正在运行的应用程序的实例。在 CI/CD 管道中，生产环境是最后一个部署环境。
- 上层环境 — 除核心开发团队以外的用户可以访问的所有环境。这可能包括生产环境、预生产环境和用户验收测试环境。

epic

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

ERP

参见企业资源规划。

探索性数据分析 () EDA

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

F

事实表

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

失败得很快

一种使用频繁和增量测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

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

功能分支

参见分支。

特征

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

特征重要性

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

功能转换

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

FGAC

请参阅精细的访问控制。

精细的访问控制 () FGAC

使用多个条件允许或拒绝访问请求。

快闪迁移

一种数据库迁移方法，它使用连续的数据复制，通过更改数据捕获在尽可能短的时间内迁移数据，而不是使用分阶段的方法。目标是将停机时间降至最低。

G

地理封锁

请参阅地理限制。

地理限制（地理阻止）

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

GitFlow 工作流程

一种方法，在这种方法中，下层和上层环境在源代码存储库中使用不同的分支。Gitflow 工作流程被认为是传统的，而基于主干的工作流程是现代的首选方法。

全新策略

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

防护机制

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。它们通过使用服务控制策略和IAM权限边界来实现。侦测性防护机制会检测策略违规和合规性问题，并生成警报以进行修复。它们通过使用 AWS Config、、Amazon、 AWS Security Hub GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

H

HA

参见高可用性。

异构数据库迁移

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

高可用性 (HA)

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

历史数据库现代化

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

同构数据库迁移

将您的源数据库迁移到共享相同数据库引擎的目标数据库（例如，将 Microsoft SQL Server 迁移到 Amazon fo RDS r 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。

I

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 Cloud 环境中的权限。

空闲应用程序

一种在 90 天内平均使用率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VPC，接受、检查和路由来自应用程序外部的网络连接。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，请参阅构建工业物联网 (IIoT) 数字化转型战略。

检查 VPC

在 AWS 多账户架构中，VPC一种集中式管理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为... 提供了基础ITSM。

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。有关将云操作与ITSM工具集成的信息，请参阅操作集成指南。

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) 的实现，其中明确为用户和数据本身分配了安全标签值。用户安全标签和数据安全标签之间的交集决定了用户可以看到哪些行和列。

登录区

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

大规模迁移

迁移 300 台或更多服务器。

LBAC

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，请参阅文档中的应用最低权限权限。IAM

直接迁移

见 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参见字节顺序。

下层环境

参见环境。

M

机器学习（ML）

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

主分支

参见分支。

恶意软件

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

托管服务

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

制造执行系统 (MES)

一种软件系统，用于跟踪、监控、记录和控制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

Migration Acceleration P MAP rog

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包括一种以有条不紊的方式执行遗留迁移的迁移方法，以及一组用于自动化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。

迁移组合评估 (MPA)

一种在线工具，可提供信息，用于验证迁移到的业务案例。 AWS Cloud MPA提供详细的产品组合评估（服务器规模调整、定价、TCO比较、迁移成本分析）以及迁移规划（应用程序数据分析和数据收集、应用程序分组、迁移优先级划分和波浪规划）。所有 AWS 顾问和APN合作伙伴顾问均可免费使用该MPA工具（需要登录）。

迁移准备情况评估 (MRA)

使用以下方法获取有关组织云就绪状态的见解、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 AWS CAF。有关更多信息，请参阅迁移准备指南。MRA是AWS 迁移策略的第一阶段。

迁移策略

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

ML

参见机器学习。

现代化

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

现代化准备情况评估

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

单体应用程序（单体式）

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

MPA

参见迁移组合评估。

MQTT

请参阅消息队列遥测传输。

多分类器

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

可变基础架构

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

O

OAC

请参阅源站访问控制。

OAI

参见源访问身份。

OCM

参见组织变更管理。

离线迁移

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

OI

参见运营集成。

OLA

参见运营层协议。

在线迁移

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

OPC-UA

参见开放流程通信-统一架构。

开放流程通信-统一架构 (OPC-UA)

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

运营层协议 () OLA

一项协议，阐明 IT 职能部门承诺相互提供哪些服务，以支持服务级别协议 () SLA。

操作准备情况审查 (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 ORRwork 中的运营准备情况评估 ()。

操作技术 (OT)

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

运营整合（OI）

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

组织跟踪

由 AWS CloudTrail 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并过渡到新系统和战略。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。

源站访问控制 (OAC)

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。

源站访问身份 (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。使用时OAI，CloudFront 会创建 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，它提供了更精细和更增强的访问控制。

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VPC，用于处理从应用程序内部启动的网络连接。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委托人的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。的示例PII包括姓名、地址和联系信息。

PII

查看个人身份信息。

playbook

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

PLC

参见可编程逻辑控制器。

PLM

参见产品生命周期管理。

策略

一个对象，可以在中定义权限（参见基于身份的策略）、指定访问条件（参见基于资源的策略）或定义组织中所有账户的最大权限 AWS Organizations （参见服务控制策略）。

多语言持久性

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

组合评测

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

谓词

返回`true`或的查询条件`false`，通常位于子`WHERE`句中。

谓词下推

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

预防性控制

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

主体

中 AWS 可以执行操作和访问资源的实体。该实体通常是 AWS 账户、IAM角色或用户的 root 用户。有关更多信息，请参见IAM文档中的角色承担者术语和概念。

隐私设计

一种贯穿整个工程化过程考虑隐私的系统工程方法。

私有托管区

一个容器，其中包含有关您希望 Amazon Route 53 如何响应对一个或多个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。这些控件会在资源置备之前对其进行扫描。如果资源与控件不兼容，则不会对其进行配置。有关更多信息，请参阅 AWS Control Tower 文档中的控制参考指南，并参见在上实施安全控制中的主动控制 AWS。

产品生命周期管理 (PLM)

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

生产环境

参见环境。

可编程逻辑控制器 (PLC)

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

假名化

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

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，在基于微服务的微服务中MES，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

见负责任、负责、咨询、知情（RACI）。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI矩阵

见负责任、负责、咨询、知情（RACI）。

RCAC

请参阅行和列访问控制。

只读副本

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

重新架构师

见 7 R。

恢复点目标 (RPO)

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

恢复时间目标 (RTO)

服务中断和服务恢复之间可接受的最大延迟。

重构

见 7 R。

区域

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

回归

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

重新托管

见 7 R。

版本

在部署过程中，推动生产环境变更的行为。

搬迁

见 7 R。

更换平台

见 7 R。

回购

见 7 R。

故障恢复能力

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

基于资源的策略

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

负责、负责、咨询、知情 (RACI) 矩阵

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

响应性控制

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

保留

见 7 R。

退休

见 7 R。

旋转

定期更新密钥以使攻击者更难访问凭据的过程。

行和列访问控制 (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

SAML2.0

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)，因此用户无需为组织中的IAM所有人创建用户即可登录 AWS Management Console 或调用 AWS API操作。有关SAML基于 2.0 的联合身份验证的更多信息，请参阅文档中的关于SAML基于 2.0 的联合。IAM

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 AWS Organizations的组织中所有账户的权限。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

URL的入口点的 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。

服务级别协议 () 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 Cloud

SPOF

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，请参阅对旧版 Microsoft ASP 进行现代化改造。 NET(ASMX) 通过使用容器和 Amazon API Gateway 逐步提供网络服务。

子网

您的 IP 地址范围VPC。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。

T

标签

键值对，充当用于组织资源的元数据。 AWS 标签可帮助您管理、识别、组织、搜索和筛选资源。有关更多信息，请参阅标记您的 AWS 资源。

目标变量

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

任务列表

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

测试环境

参见环境。

训练

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

中转网关

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

优化

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

双披萨团队

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

U

不确定性

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

无差别任务

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

上层环境

参见环境。

V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC凝视

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对等互连。

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

一种对一组以某种方式与当前记录相关的行进行计算的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。

WORM

参见一次写入，多读。

WQF

参见AWS工作负载资格框架。

写一次，读多次 (WORM)

一种存储模型，它可以一次写入数据并防止数据被删除或修改。授权用户可以根据需要多次读取数据，但他们无法对其进行更改。这种数据存储基础架构被认为是不可变的。

Z

零日漏洞利用

一种利用未修补漏洞的攻击，通常是恶意软件。

零日漏洞

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

僵尸应用程序

平均值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。