在上构建可扩展的漏洞管理程序 AWS

AWS 规范性指导

AWS 规范性指导: 在上构建可扩展的漏洞管理程序 AWS

Table of Contents

简介 1
目标受众 2
目标 2
准备 3
定义计划 3
分配所有权 4
制定披露计划 5
准备好您的环境 5
AWS 账户 结构 6
标签 6
监控公告 7
配置安全服务 7
Amazon Inspector 7
AWS Security Hub 8
准备分配调查结果 10
使用现有工具 11
使用 Security Hub 12
分类和修复 13
分配调查结果 13
评估结果并确定其优先顺序 14
修复调查结果 15
示例 16
安全团队示例 16
云团队示例 17
应用程序团队示例 18
举报并改进 20
安全运营会议 20
Security Hub 见解 20
结论及后续步骤 21
资源 23
AWS 服务文档 23
其他 AWS 资源 23
文档历史记录 24
术语表 25

..... 25
A 25
B 28
C 29
D 32
E 35
F 37
G 38
H 38
I 39
L 41
M 42
O 45
P 48
Q 50
R 50
S 53
T 55
U 57
V 57
W 57
Z 58
..... lix

在上构建可扩展的漏洞管理程序 AWS

Anna McAbee 和 Megan O'Neil，Amazon Web Services ()AWS

2023 年 10 月（文档历史记录）

根据您使用的底层技术，各种工具和扫描可以在云环境中生成安全发现。如果没有处理这些发现的流程，它们就会开始积累，通常会在短时间内产生成千上万的发现。但是，通过结构化的漏洞管理计划和工具的适当运行，您的组织可以处理和分类来自不同来源的大量发现。

漏洞管理侧重于发现漏洞、确定其优先级、评估、修复和报告漏洞。另一方面，补丁管理侧重于修补或更新软件以删除或修复安全漏洞。补丁管理只是漏洞管理的一个方面。通常，我们建议既建立一个patch-in-place 流程（也称为mitigate-in-place流程）来解决关键的、立即修补的情况，也建议您建立一个定期运行的标准流程，以便发布经过修补的 Amazon 系统映像 (AMI)、容器或软件包。这些流程有助于您的组织做好准备，以快速响应未修补的漏洞。对于生产环境中的关键系统，使用 patch-in-place 流程比在机群中部署新的 AMI 更快、更可靠。对于定期安排的补丁，例如操作系统 (OS) 和软件补丁，我们建议您像处理任何软件级别的更改一样，使用标准开发流程进行构建和测试。这为标准操作模式提供了更好的稳定性。您可以使用 Patch Manager AWS Systems Manager、的功能或其他第三方产品作为 patch-in-place 解决方案。有关使用 Patch Manager 的更多信息，请参阅《AWS 云采用框架：运营视角》中的补丁管理。此外，您还可以使用 EC2 Image Builder 自动创建、管理和部署自定义镜像和 up-to-date 服务器映像。

构建可扩展的漏洞管理程序除了云配置风险外，还 AWS 涉及管理传统软件和网络漏洞。云配置风险，例如未加密的亚马逊简单存储服务 (Amaz on S3) 存储桶，应遵循与软件漏洞类似的分类和修复流程。在这两种情况下，应用程序团队都必须拥有其应用程序（包括底层基础架构）并对其安全负责。这种所有权分配是有效且可扩展的漏洞管理计划的关键。

本指南讨论了如何简化漏洞的识别和修复以降低总体风险。使用以下部分来构建和迭代您的漏洞管理程序：

1. 准备 — 让您的人员、流程和技术做好准备，以识别、评估和修复环境中的漏洞。
2. 分类和补救-将安全调查结果发送给相关利益相关者，确定适当的补救措施，然后采取补救措施。
3. 报告和改进-使用报告机制来识别改进机会，然后对漏洞管理计划进行迭代。

构建云漏洞管理程序通常涉及迭代。对本指南中的建议进行优先排序，并定期重新审视待办事项，以了解最新的技术变化和业务需求。

目标受众

本指南适用于拥有三个主要团队负责安全相关发现的大型企业：安全团队、卓越云中心 (CCoE) 或云团队，以及应用程序（或开发人员）团队。本指南使用最常见的企业运营模型，并在这些运营模型的基础上再接再厉，以便更有效地响应安全发现并改善安全成果。使用的组织 AWS 可能具有不同的结构和不同的运营模式；但是，您可以修改本指南中的许多概念，以适应不同的运营模式和较小的组织。

目标

本指南可以帮助您和您的组织：

- 制定政策以简化漏洞管理并确保问责制
- 建立机制，将安全责任分配给应用团队
- AWS 服务 根据可扩展漏洞管理的最佳实践进行相关配置
- 分配安全发现的所有权
- 建立报告漏洞管理计划并对其进行迭代的机制
- 提高安全发现的可见性并改善整体安全状况

准备您的可扩展漏洞管理计划

准备构建可扩展的漏洞管理计划包括教育人员、开发流程和根据最佳实践实施适当的技术。人员、流程和技术对于有效的漏洞管理计划同样重要，您必须将其紧密整合，才能大规模管理漏洞。

本指南的这一部分回顾了在准备可扩展漏洞管理计划时可以采取的基本措施。 AWS

主题

- 定义漏洞管理计划
- 分配安全所有权
- 制定漏洞披露计划
- 准备好您的 AWS 环境
- 监控 AWS 安全公告
- 配置 AWS 安全服务
- 准备分配安全调查结果

定义漏洞管理计划

准备云漏洞管理计划的第一步是定义漏洞管理计划。该计划包括您的组织所遵循的政策和流程。该计划应记录在案，供所有利益攸关方查阅。漏洞管理计划是一份高级文档，通常包括以下部分：

- 目标和范围-概述漏洞管理的目标、功能和范围。
- 角色和职责-列出漏洞管理利益相关者并详细说明他们的职责。
- 漏洞严重性和优先级定义-确定如何对漏洞的严重性进行分类以及如何确定漏洞的优先级。
- 补救服务级别协议 (SLA)-对于每个严重性级别，定义补救所有者解决安全发现的最长时间。由于 SLA 合规性是制定有效且可扩展的漏洞管理计划不可或缺的一部分，因此请考虑如何跟踪您是否符合这些 SLA。
- 例外流程-详细说明提交、批准和更新例外情况的流程。此过程应确保例外情况是合法的、有时限的、可跟踪的。
- 漏洞信息来源-列出生成安全发现的来源或工具。有关 AWS 服务 这可能是安全发现来源的更多信息，请参阅本指南配置 AWS 安全服务中的。

虽然这些部分在不同规模和行业的公司中很常见，但每个组织的漏洞管理计划都是独一无二的。您需要制定最适合您的组织的漏洞管理计划。期望随着时间的推移对您的计划进行迭代，以纳入吸取的经验教训和不断发展的技术。

分配安全所有权

责任AWS 共担模型定义了云安全和合规性责任的分担方式 AWS 及其客户。在此模型中 AWS ，保护运行中提供的所有服务的基础架构 AWS Cloud， AWS 客户负责保护其数据和应用程序。

您可以在组织内部反映这种模式，并在云和应用程序团队之间分配责任。这可以帮助您更有效地扩展云安全计划，因为应用程序团队对其应用程序的某些安全方面拥有所有权。对分担责任模型的最简单解释是，如果您有权配置资源，则您应对该资源的安全性负责。

将安全责任分配给应用程序团队的一个关键部分是构建自助服务安全工具，帮助您的应用程序团队实现自动化。最初，这可能是一项共同努力。安全团队可以将安全要求转化为代码扫描工具，然后应用程序团队可以使用这些工具来构建解决方案，并与其内部开发人员社区共享解决方案。这有助于提高其他需要满足类似安全要求的团队的效率。

下表概述了向应用程序团队分配所有权的步骤并提供了示例。

步骤	操作	示例
1	定义您的安全要求 — 您想要实现什么？ 这可能来自安全标准或合规性要求。	例如，安全要求是应用程序身份的最低权限访问权限。
2	列举安全要求的控制措施 — 从控制的角度来看，此要求实际上意味着什么？ 我需要做些什么才能实现这一目标？	为了实现应用程序身份的最低权限，以下是两个示例控件： • 使用 AWS Identity and Access Management (IAM) 角色 • 请勿在 IAM 策略中使用通配符
3	控件文档指南 — 有了这些控件，您可以向开发人员提供哪	首先，您可以先记录简单的示例策略，包括安全和不安全的 IAM 策略以及亚马逊简单存储

步骤	操作	示例
	些指导来帮助他们遵守控制规定？	服务 (Amazon S3) 存储桶策略。接下来，您可以在持续集成和持续交付 (CI/CD) 管道中嵌入策略扫描解决方案，例如使用AWS Config 规则进行主动评估。
4	开发可重复使用的工件 — 在指导下，你能否让它变得更简单，为开发者开发可重复使用的工件？	您可以创建基础设施即代码 (IaC) 来部署遵循最低权限原则的 IAM 策略。您可以将这些可重复使用的构件存储在代码存储库中。

自助服务可能无法满足所有安全要求，但它可以适用于标准场景。通过遵循这些步骤，组织可以授权其应用程序团队以可扩展的方式处理自己的更多安全职责。总体而言，分布式责任模型在许多组织中带来了更具协作性的安全实践。

制定漏洞披露计划

要想获得漏洞管理defense-in-depth方法，请创建漏洞披露计划，以便组织内部或外部的人员可以报告安全漏洞或风险。

对于组织内部人员，请制定提交风险或漏洞的流程。这可以通过票务系统或电子邮件完成。无论您选择哪种流程，都必须让您的员工了解流程并能够轻松提交他们遇到的任何漏洞或风险。

对于组织外部人员，请创建一个外部网页，用于提交潜在的安全漏洞。例如，请参阅AWS 漏洞报告网页。该网页还应包含披露指南，以帮助保护贵组织的数据和资产。漏洞披露计划不应鼓励潜在的有害活动，因此制定明确的政策以及指导方针至关重要。随着计划的成熟，制定成熟、负责任的披露计划是一个需要努力实现的目标。大多数都不是从外部披露计划开始的，需要时间才能把它做好。

准备好您的 AWS 环境

在实施任何漏洞管理工具之前，请确保您的 AWS 环境架构支持可扩展的漏洞管理计划。您 AWS 账户和您的组织的标签策略结构可以简化构建可扩展漏洞管理计划的过程。

开发一个 AWS 账户 结构

AWS Organizations随着业务的增长和 AWS 资源的扩展，可以帮助集中管理和治理 AWS 环境。中的组织 AWS 账户 将您 AWS Organizations 整合到逻辑组或组织单位中，这样您就可以将其作为一个单元进行管理。您可以通过一个 AWS Organizations 名为管理账户的专用账户进行管理。有关更多信息，请参阅 AWS Organizations 术语和概念。

我们建议您在中管理您的 AWS 多账户环境。 AWS Organizations这有助于创建贵公司的账户和资源的完整清单。完整的资产清单是漏洞管理的关键方面。应用程序团队不应使用组织之外的帐户。

AWS Control Tower按照规范性最佳实践，帮助您设置和管理 AWS 多账户环境。如果您尚未建立多账户环境，那么 AWS Control Tower 这是一个不错的起点。

我们建议使用AWS 安全参考架构 (AWS SRA) 中描述的专用账户结构和最佳实践。安全工具账户应充当您的安全服务的委托管理员。本指南稍后将提供有关在此账户中配置漏洞管理工具的更多信息。在工作负载组织单元 (OU) 的专用账户中托管应用程序。这为每个应用程序建立了强大的工作负载级别隔离和明确的安全边界。有关使用多账户方法的设计原则和优势的信息，请参阅使用多个账户组织 AWS 环境（AWS 白皮书）。

建立有针对性的账户结构并通过专用账户集中管理安全服务是可扩展漏洞管理计划的关键方面。

定义、实施和强制执行标签

标签是键值对，可充当用于组织资源的元数据。 AWS 有关更多信息，请参阅标记您的 AWS 资源。您可以使用标签来提供业务背景，例如业务部门、应用程序所有者、环境和成本中心。下表显示了一组示例标签。

键	值
BusinessUnit	HumanResources
CostCenter	CC101
ApplicationTeam	HumanResourcesTechnology
环境	生产

标签可以帮助您确定发现结果的优先顺序。例如，它可以帮助你：

- 确定负责修补漏洞的资源所有者

- 跟踪哪些应用程序或业务部门有大量调查结果
- 提高某些数据分类的调查结果的严重性，例如个人身份信息 (PII) 或支付卡行业 (PCI) 数据
- 确定环境中的数据类型，例如较低级别开发环境中的测试数据或生产数据

为了帮助您实现大规模的有效标记，请按照《标记 AWS 资源的最佳实践》（AWS 白皮书）中构建标签策略中的说明进行操作。

监控 AWS 安全公告

我们强烈建议定期和频繁地监控AWS 安全公告。安全公告可以通知您任何新的安全相关漏洞、受影响的服务和适用的更新。作为漏洞管理计划的一部分，您还可以订阅安全公告的 RSS 提要，并构建一个流程来接收和处理这些公告。

配置 AWS 安全服务

AWS 提供各种安全服务，旨在帮助保护您的 AWS 环境。对于您的漏洞管理程序，我们建议您在每个账户 AWS 服务 中启用以下选项：

- Amazon GuardDuty 可帮助检测您环境中的活跃威胁。 GuardDuty发现可以帮助您识别在您的环境中被利用的未知漏洞。它还可以帮助您了解未修补漏洞的影响。
- AWS Health提供对您的资源绩效以及 AWS 服务 和账户可用性的持续可见性。
- AWS Identity and Access Management Access Analyzer分析您 AWS 环境中基于资源的策略，以确定与外部实体共享的资源。这可以帮助您识别与意外访问您的资源和数据相关的漏洞。对于在您的账户外共享的资源的每个实例，IAM Access Analyzer 都会生成一个调查结果。
- Amazon Inspector 是一项漏洞管理服务，可持续扫描您的 AWS 工作负载，以查找软件漏洞和意外网络泄露。
- AWS Security Hub帮助您根据安全行业标准检查您的 AWS 环境，并可以识别云配置风险。它还通过汇总来自其他 AWS AWS 安全服务和第三方安全工具的调查结果，全面了解您的安全状态。

本节讨论如何启用和配置 Amazon Inspector 和 Security Hub，以帮助您建立可扩展的漏洞管理计划。

在漏洞管理程序中使用 Amazon Inspector

Amazon Inspector 是一项漏洞管理服务，可持续扫描您的亚马逊弹性计算云 (Amazon EC2) 实例、亚马逊弹性容器注册表 (Amazon ECR) Elastic Registry 容器映像 AWS Lambda 和函数中是否存在软件

漏洞和意外网络泄露。您可以使用 Amazon Inspector 来了解您的 AWS 环境中的软件漏洞，并确定解决这些漏洞的优先顺序。

Amazon Inspector 会在资源的整个生命周期中持续评估您的环境。它会自动重新扫描资源，以应对可能引入新漏洞的更改。例如，当您在 EC2 实例上安装新软件包、安装补丁或发布影响资源的新常见漏洞和漏洞 (CVE) 时，它会重新扫描。当 Amazon Inspector 发现漏洞或开放的网络路径时，它会生成一个可供您调查的发现。该发现提供了有关该漏洞的全面信息，包括以下内容：

- 亚马逊 Inspector 风险评分
- 通用漏洞评分系统 (CVSS) 分数
- 受影响的资源
- Amazon 提供的有关 CVE 的漏洞情报数据 Recorded Future，以及 Cybersecurity and Infrastructure Security Agency (CISA)
- 补救建议

有关设置 Amazon Inspector 的说明，请参阅 Ama zon Inspector 入门。本教程中的激活 Amazon Inspector 步骤提供了两个配置选项：独立账户环境和多账户环境。如果您想监控多个属于组织成员的用户 AWS 账户 ，我们建议您使用多账户环境选项。 AWS Organizations

在为多账户环境设置 Amazon Inspector 时，您可以将组织中的一个账户指定为 Amazon Inspector 的委托管理员。授权的管理员可以管理组织成员的调查结果和某些设置。例如，授权管理员可以查看所有成员账户的汇总结果的详细信息，启用或禁用对成员账户的扫描，以及查看扫描的资源。 AWS SRA 建议您创建一个安全工具账户，并将其作为 Amazon Inspector 的委托管理员使用。

AWS Security Hub 在您的漏洞管理程序中使用

构建可扩展的漏洞管理程序除了云配置风险外，还 AWS 涉及管理传统软件和网络漏洞。 AWS Security Hub帮助您根据安全行业标准检查您的 AWS 环境，并可以识别云配置风险。Security Hub 还 AWS 通过汇总来自其他 AWS 安全服务和第三方安全工具的安全发现，全面了解您的安全状态。

在以下各节中，我们提供了设置 Security Hub 以支持您的漏洞管理计划的最佳实践和建议：

- 设置 Security Hub
- 启用 Security Hub 标准
- 管理 Security Hub 的调查结果
- 汇总来自其他安全服务和工具的调查结果

设置 Security Hub

有关设置说明，请参阅设置 AWS Security Hub。要使用 Security Hub，必须启用AWS Config。有关更多信息，请参阅 Security Hub 文档 AWS Config中的启用和配置。

如果您已与组织管理账户集成 AWS Organizations，则可以从组织管理账户中指定一个账户作为 Security Hub 授权管理员。有关说明，请参阅指定 Security Hub 的委托管理员。 AWS SRA 建议您创建一个安全工具帐户，并将其用作 Security Hub 的委托管理员。

授权的管理员自动有权为组织中的所有成员账户配置 Security Hub，并查看与这些账户关联的调查结果。我们建议您全部启用 Sec AWS Config urit AWS 区域 y Hub AWS 账户。您可以将 Security Hub 配置为自动将新的组织帐户视为 Security Hub 成员帐户。有关说明，请参阅管理属于组织的成员账户。

启用 Security Hub 标准

Security Hub 通过对安全控制进行自动和持续的安全检查来生成调查结果。这些控件与一个或多个安全标准相关联。这些控件可帮助您确定是否满足标准中的要求。

当你在 Security Hub 中启用标准时，Security Hub 会自动启用适用于该标准的控件。Security Hub 使用 AWS Config 规则对控件执行大部分安全检查。您可以随时启用或禁用 Security Hub 标准。有关更多信息，请参阅中的安全控制和标准 AWS Security Hub。有关标准的完整列表，请参阅 Sec urity Hub 标准参考。

如果您的组织还没有首选安全标准，我们建议使用AWS 基础安全最佳实践 (FSBP) 标准。该标准旨在检测何时 AWS 账户 出现资源偏离安全最佳实践。 AWS 策划本标准并定期对其进行更新，以涵盖新的功能和服务。对 FSBP 的调查结果进行分类后，可以考虑启用其他标准。

管理 Security Hub 的调查结果

Security Hub 提供了多项功能，可帮助您处理来自整个组织的大量发现，并了解 AWS 环境的安全状态。为了帮助您管理调查结果，我们建议启用以下两个 Security Hub 功能：

- 使用跨区域聚合将多个聚合区域的调查结果、查找更新、见解、控制合规性状态和安全评分汇总 AWS 区域 到单个聚合区域。
- 使用整合的控制结果，通过删除重复的发现来减少发现噪音。在账户中启用整合的控件调查发现后，Security Hub 会为控件的每项安全检查生成一个新调查发现或调查发现更新，即使某项控件适用于多个启用的标准。

汇总来自其他安全服务和工具的调查结果

除了生成安全调查结果外，您还可以使用 Security Hub 汇总来自多个 AWS 服务 受支持的第三方安全解决方案的查找数据。本节重点介绍向 Security Hub 发送安全调查结果。下一节将讨论如何将 Security Hub 与可以从 Security Hub 接收发现结果的产品集成。准备分配安全调查结果

有许多 AWS 服务第三方产品和开源解决方案可供您与 Security Hub 集成。如果您刚刚起步，我们建议您执行以下操作：

1. 启用集成 AWS 服务-在您同时启用 S AWS 服务 ecurity Hub 和集成服务后，大多数将发现结果发送到 Security Hub 的集成都会自动激活。对于您的漏洞管理计划，我们建议在每个账户中启用 Amazon Inspector GuardDuty AWS Health、Amazon 和 IAM Access Analyzer。这些服务会自动将其发现结果发送到 Security Hub。有关支持的 AWS 服务 集成的完整列表，请参阅将发现结果发送 AWS 服务 到 Security Hub。

   > **Note**
   >
   > AWS Health 如果满足以下条件之一，则会将发现结果发送到 Security Hub：
   > - 该发现与 AWS 安全部门有关
   > - 查找结果类型码包含单词、或 `security` `abuse` `certificate`
   > - 查找 AWS Health 服务是`risk`或 `abuse`

2. 设置第三方集成-有关当前支持的集成列表，请参阅可用的第三方合作伙伴产品集成。选择可以向 Security Hub 发送调查结果或从 Security Hub 接收调查结果的任何其他工具。您可能已经拥有了其中一些第三方工具。按照产品说明配置与 Security Hub 的集成。

准备分配安全调查结果

在本节中，您将设置团队用来管理和分配安全调查结果的工具。本节包括以下选项：

- 在现有工具和工作流程中管理调查结果— 此选项可 AWS Security Hub 与您的团队用来管理日常任务（例如产品待办事项）的现有系统集成。对于已建立管理工作流程的工具的团队，建议使用此选项。
- 在 Security Hub 中管理调查结果— 此选项配置 Security Hub 事件的通知，以便相应的团队收到警报并可以在 Security Hub 中处理发现的问题。

确定哪种工作流程最适合您的团队，并确保安全调查结果能够迅速传达给各自的所有者。

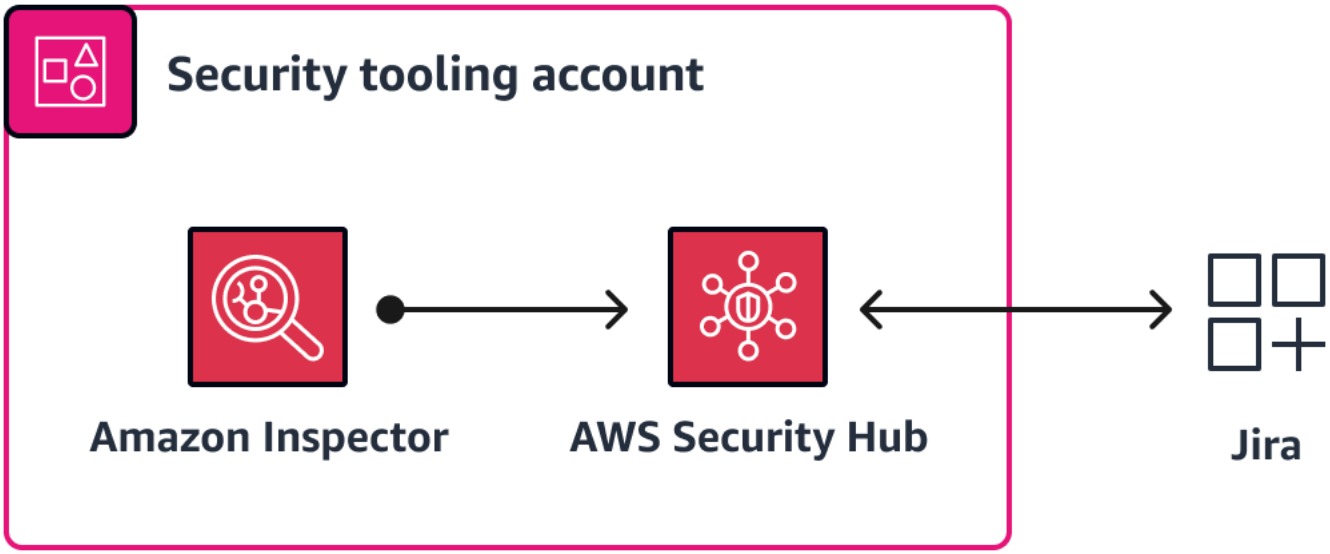
在现有工具和工作流程中管理调查结果

对于已建立工具供团队管理或执行日常任务的企业组织，我们建议他们使用其他 Security Hub 集成。您可以将 Security Hub 查找数据导入多个技术平台。示例包括：

- 安全信息和事件管理 (SIEM) 系统可帮助安全团队对运营安全事件进行分类。SIEM 系统可对应用程序和网络硬件生成的安全警报进行实时分析。
- 治理、风险和合规 (GRC) 系统可帮助合规和治理团队监控和报告风险管理数据。GRC 工具是企业可以用来管理政策、评估风险、控制用户访问和简化合规的软件应用程序。您可以使用 GRC 工具来整合业务流程、降低成本和提高效率。
- 产品待办事项和工单系统可帮助应用程序和云团队管理功能并确定开发任务的优先顺序。 Atlassian Jira并且Microsoft Azure DevOps是这些系统的例子。

将 Security Hub 的发现结果直接与这些现有企业系统集成，可以缩短平均恢复时间 (MTTR) 和安全结果，因为日常操作工作流程不必改变。由于团队不必使用单独的工作流程和工具，因此他们可以更快地做出响应并从安全发现中吸取教训。集成使处理安全发现成为正常、标准工作流程的一部分。

Security Hub 可与多个第三方合作伙伴产品集成。有关完整列表和说明，请参阅 Security Hub 文档中可用的第三方合作伙伴产品集成。常见的集成包括 Atlassian - Jira Service Management，AWS Security Hub 与Jira软件双向集成，以及。ServiceNow – ITSM下图显示了如何将 Amazon Inspector 配置为将调查结果发送到 Security Hub，然后将 Security Hub 配置为将所有调查结果发送到Jira。



在 Security Hub 中管理调查结果

您可以使用亚马逊 EventBridge规则和亚马逊简单通知服务 (Amazon SNS) Service 主题为 Security Hub 的发现构建基于云的通知系统。该系统会在创建发现时通知相应的团队。对于这种方法，中描述的多账户策略开发一个 AWS 账户 结构至关重要，因为应用程序被分成专用账户。这可以帮助你将每项发现通知正确的团队。

安全团队或云团队可能会选择接收来自所有人的事件 AWS 账户。在这种情况下，请在 Security Hub 委托管理员账户中制定 EventBridge 规则，并订阅通知这些团队的 Amazon SNS 主题。对于应用程序团队，请在各自的应用程序帐户中配置 EventBridge 规则和 SNS 主题。当 Security Hub 发现出现在应用程序帐户中时，负责团队会收到有关该发现的通知。

Security Hub 已经自动将所有新发现和现有发现的所有更新 EventBridge 作为 Sec urity Hub 调查结果-导入的事件发送到。每个 S ecurity Hub 调查结果-导入的事件都包含一个发现。您可以对 EventBridge 规则应用过滤器，这样，只有当查找结果与筛选条件匹配时，查找结果才会启动规则。有关说明，请参阅为自动发送的调查结果配置 EventBridge 规则。有关创建和订阅 Amazon SNS 主题的更多信息，请参阅配置 Amazon S NS。

使用此方法时，请考虑以下几点：

- 对于应用程序团队，请在每个团队 AWS 账户 以及应用程序的托管 AWS 区域 位置中创建 EventBridge 规则。
- 对于安全和云团队，请在 Security Hub 委托管理员帐户中创建 EventBridge 规则。这会通知团队成员账户中的所有发现。
- 如果安全发现的状态为，Amazon SNS 每天都会发送通知。`NEW`如果您想关闭每日通知，可以创建一个自定义 AWS Lambda 函数，在 Amazon SNS 订阅者收到通知`NOTIFIED`后，`NEW`将发现的状态从更改为。

对环境中的安全发现进行分类和修复 AWS

对安全发现进行分类包括将发现传送给相应的利益相关者，对发现进行评估并确定其优先顺序，然后对其进行补救。本节详细介绍了每个步骤，并就可扩展性和效率提供了建议。它还包括一些示例，以帮助说明分类和补救过程。

主题

- 定义安全发现的所有权
- 评估安全发现并确定其优先级
- 修复安全发现
- 对安全发现进行分类和补救的示例

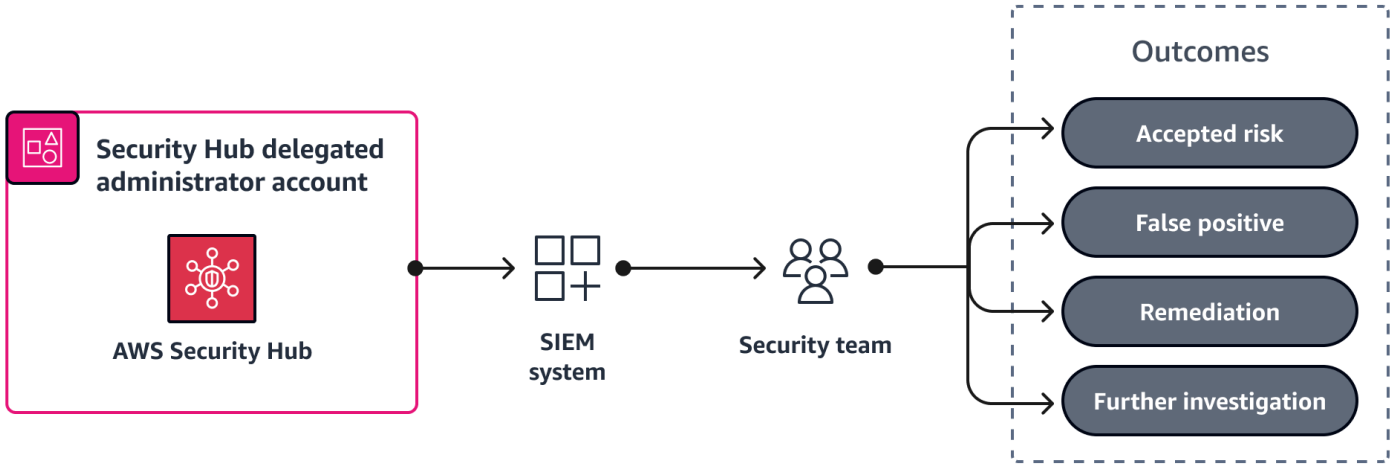
定义安全发现的所有权

定义所有权模式来对安全发现进行分类可能具有挑战性，但事实并非如此。安全格局不断变化，从业人员必须灵活地适应这些变化。采用灵活的方法来开发安全发现的所有权模型。您的初始模型应使您的团队能够立即采取行动。我们建议从基本的所有权逻辑入手，并随着时间的推移完善该逻辑。如果您延迟定义完美的所有权标准，则安全发现的数量将继续增加。

为了便于将调查结果分配给适当的团队和资源，我们建议 AWS Security Hub 与您的团队用来管理其日常任务的任何现有系统集成。例如，您可以将 Security Hub 与安全信息和事件管理 (SIEM) 系统或产品待办事项和票务系统集成。有关更多信息，请参阅本指南中的准备分配安全调查结果。

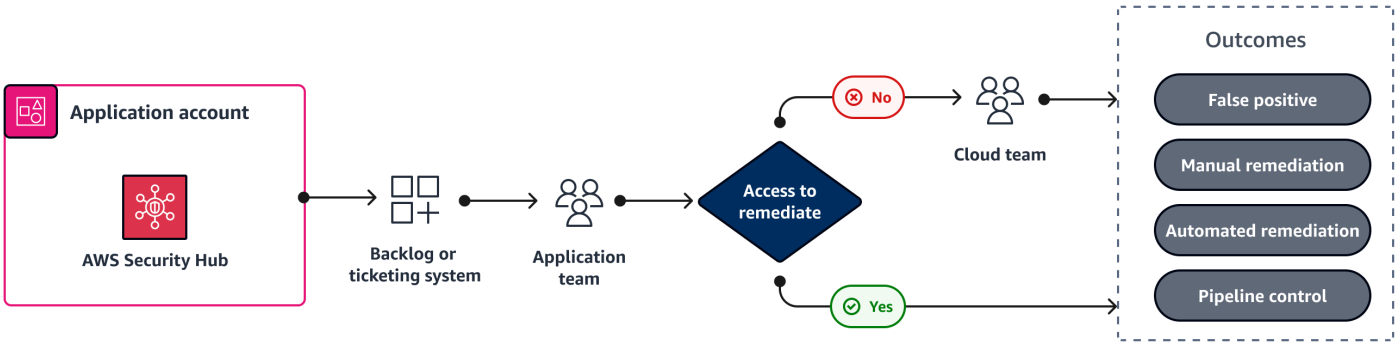
以下是所有权模型的示例，您可以将其用作起点：

- 安全团队会审查潜在的活跃威胁，并帮助评估安全发现并确定其优先级。安全团队拥有正确评估背景的专业知识和工具。他们了解其他与安全相关的数据，这些数据可以帮助他们评估漏洞并确定其优先级，并调查威胁检测事件。如果需要查找严重性或进行其他调整，请参阅本指南中的评估安全发现并确定其优先级部分。有关示例，请参阅本指南安全团队示例中的。



- 在@@ 云和应用程序团队之间分发安全调查结果 — 如分配安全所有权本节所述，有权配置资源的团队负责其安全配置。应用程序团队负责与其构建和配置的资源相关的安全调查结果，而云团队则负责与广泛配置相关的安全调查结果。在大多数情况下，应用团队无权更改范围广泛的配置，例如 AWS Control Tower中的服务控制策略 (SCP) AWS 服务、与网络相关的 VPC 配置和 IAM Identity Center AWS 。 AWS Organizations

  对于将应用程序分成专用账户的多账户环境，您通常可以将账户中与安全相关的调查结果集成到应用程序的待办事项或工单系统中。通过该系统，云团队或应用团队可以解决这一发现。有关示例，请参阅本指南应用程序团队示例中的云团队示例或。



- 将剩余的、未解决的发现分配给云团队 — 剩余的发现可能与默认设置或云团队可以解决的广泛配置有关。该团队可能拥有最多的历史知识和解决这一发现的机会。总体而言，这通常在总发现中所占的子集要小得多。

评估安全发现并确定其优先级

有效的漏洞管理计划的一个关键组成部分是能够评估安全发现并确定其优先顺序。这就是上下文拉动、组织历史和调整检测系统的用武之地。确定安全发现的优先顺序有助于确定响应级别的适当速度。

对于 Amazon Inspector 和 Amazon GuardDuty，调查结果包含严重性标签或分数。 AWS Security Hub我们建议优先调查Security Hub中的所有关键和高严重性发现，包括与基础安全最佳实践 (FSBP) 标准、Amazon Inspector 和。 GuardDuty查找严重性标签是按以下方式确定分数：

- Amazon Inspector 分数是每项发现的高度情境化分数。它是通过将通用漏洞评分系统 (CVSS) 基本分数信息与网络可访问性结果和可利用性数据关联来计算的。使用此分数，您可以对发现结果进行优先排序，将重点放在最关键的发现和脆弱的资源上。除了分数外，Amazon Inspector 还提供了有关常见漏洞和风险敞口 (CVE) 的增强型漏洞情报。这是亚马逊提供的有关CVE的现有情报以及行业标准的安全情报来源（例如记录的未来和网络安全与基础设施安全局（CISA））的摘要。例如，Amazon Inspector 可以提供用于利用漏洞的已知恶意软件包的名称。有关更多信息，请参阅漏洞情报。
- 每个 GuardDuty 发现都有指定的严重级别和值，以反映该发现对您的环境的潜在风险。此级别和值由 AWS 安全工程师确定。例如，`High`严重性级别表示资源已被泄露并被积极用于未经授权的目的。我们建议您将`High`严重性 GuardDuty 发现作为优先事项，并立即采取补救措施，以防止进一步未经授权的使用。
- Security Hub 控制发现的严重性取决于漏洞利用的难度和入侵的可能性。难度取决于利用弱点执行威胁场景所需的复杂程度。泄露的可能性表明威胁情景导致您的 AWS 服务 或资源中断或泄露的可能性有多大。

要调整调查结果，您可以直接在相应的服务控制台中或使用服务的 API 来抑制或存档特定的调查结果。此外，您还可以使用自动化规则对 Security Hub 中的搜索结果进行更改。 GuardDuty Amazon Inspector 的调查结果会自动发送到 Security Hub。您可以使用自动化规则根据您定义的标准近乎实时地自动更新（例如更改严重性）或隐藏搜索结果。在创建自动化规则时，我们建议在规则描述中添加上下文，例如创建或修改日期、谁创建了规则以及为什么需要规则。这些信息通常有助于将来参考。

修复安全发现

在对发现进行评估并确定其优先顺序之后，下一步行动是纠正调查结果。您可以采取许多不同的措施来补救发现。对于软件漏洞，您可以更新操作系统或应用补丁。对于云配置的发现，您可以更新资源配置。通常，您为补救而采取的措施可以分为以下结果之一：

- 手动修复- 您可以手动修复漏洞，例如修改 AWS 资源的属性以启用加密。如果发现来自 Security Hub 中的托管支票，则该发现包括一个指向手动修复发现的说明的链接。
- 可重复使用的构件 — 您更新基础设施即代码 (IaC) 以修复漏洞，并知道其他人可以从类似的解决方案中受益。考虑将更新后的 IaC 和解决方案的简要摘要上传到内部共享代码存储库。
- 自动修复- 通过您创建的机制自动修复漏洞。

- 管道控制 — 在持续集成和持续交付 (CI/CD) 管道中应用控制措施，如果存在漏洞，则可以阻止部署。
- 可接受的风险 — 您不采取任何措施或实施补偿性控制，并且您接受漏洞带来的风险。在风险登记处等专用位置跟踪可接受的风险。
- 误报-您没有采取任何行动，因为您已确定发现未正确识别漏洞。

您可以采取的各种操作以及可用于修复漏洞的工具的完整列表不在本指南的范围之内。但是，有一些值得注意的服务和工具可以帮助您大规模修复漏洞，包括：

- Patch Manager 是一项功能 AWS Systems Manager，它可以自动使用与安全相关的更新和其他类型的更新来修补托管节点。您可以使用 Patch Manager 来应用操作系统和应用程序的补丁。
- AWS Firewall Manager可帮助您在中的账户和应用程序中集中配置和管理防火墙规则 AWS Organizations。随着新应用程序的创建，Firewall Manager 通过强制执行一组通用的安全规则，可以更轻松地使新的应用程序和资源合规。
- 开@@ 启自动安全响应 AWS是一种与 Security Hub 配合使用的 AWS 解决方案，可根据行业合规标准和安全威胁最佳实践提供预定义的响应和补救措施。

对安全发现进行分类和补救的示例

本节提供了安全、云和应用程序团队的分类流程示例。它讨论了每个团队通常处理的调查结果类型，并提供了如何应对的示例。还包括高级补救指南。

本节包含以下示例：

- 安全团队示例：创建 Security Hub 自动化规则
- 云团队示例：更改 VPC 配置
- 应用程序团队示例：创建 AWS Config 规则

安全团队示例：创建 Security Hub 自动化规则

安全团队会收到与威胁检测相关的发现，包括 Amazon 的 GuardDuty 发现。有关按 AWS 资源类型分类的 GuardDuty 查找类型的完整列表，请参阅 GuardDuty 文档中的查找类型。安全团队必须熟悉所有这些发现类型。

在此示例中，安全团队接受安全发现的相关风险级别 AWS 账户 ，该级别仅用于学习目的，不包括重要或敏感数据。此账户的名称是sandbox，账户 ID 是123456789012。安全团队可以创建 AWS

Security Hub 自动化规则，禁止从该账户中 GuardDuty发现的所有结果。他们可以根据涵盖许多常见用例的模板创建规则，也可以创建自定义规则。在 Security Hub 中，我们建议预览标准的结果，以确认该规则是否返回了预期的结果。

> **Note**
>
> 此示例重点介绍自动化规则的功能。我们不建议隐瞒账户的所有搜索 GuardDuty 结果。背景很重要，每个组织都必须根据数据类型、分类和缓解控制来选择要抑制哪些发现。

以下是用于创建此自动化规则的参数：

- 规则：
  - 规则名称是 `Suppress findings from Sandbox account`
  - 规则描述是 `Date: 06/25/23 Authored by: John Doe Reason: Suppress GuardDuty findings from the sandbox account`
- 标准：
  - `AwsAccountId` = `123456789012`
  - `ProductName` = `GuardDuty`
  - `WorkflowStatus` = `NEW`
  - `RecordState` = `ACTIVE`
- 自动操作：
  - `Workflow.status` 是 `SUPPRESSED`

有关更多信息，请参阅 Security Hub 文档中的自动化规则。安全团队有多种方法可以调查和修复检测到的威胁的发现。如需详细指导，请参阅《AWS 安全事件响应指南》。我们建议您查看本指南，以确认您已经建立了强有力的事件响应流程。

云团队示例：更改 VPC 配置

云团队负责对具有共同趋势的安全发现进行分类和修复，例如对可能不适合您的用例的 AWS 默认设置的更改。这些发现往往会影响许多 AWS 账户 资源，例如 VPC 配置，或者它们包含应在整个环境中施加的限制。在大多数情况下，云团队会手动进行一次性更改，例如添加或更新策略。

在您的组织使用 AWS 环境一段时间后，您可能会发现一组反模式正在形成。反模式是经常使用的解决方案，用于解决反复出现的问题，在这种问题中，该解决方案适得其反、无效或不如替代方案有效。作

为这些反模式的替代方案，您的组织可以使用更有效的环境范围限制，例如 AWS Organizations 服务控制策略 (SCP) 或 IAM Identity Center 权限集。SCP 和权限集可以为资源类型提供额外的限制，例如阻止用户配置公共的亚马逊简单存储服务 (Amazon S3) Service 存储桶。尽管限制所有可能的安全配置可能很诱人，但是 SCP 和权限集存在策略大小限制。我们建议采取平衡的方法进行预防和侦查控制。

以下是云团队可能负责 AWS Security Hub 的基础安全最佳实践 (FSBP) 标准中的一些控制措施：

- [EC2.2] VPC 默认安全组不应允许入站和出站流量
- [EC2.6] 应在所有 VPC 中启用 VPC 流量记录
- [EC2.23] Amazon EC2 传输网关不应自动接受 VPC 连接请求
- [CloudTrail.1] CloudTrail 应启用并配置至少一条包含读写管理事件的多区域跟踪
- AWS Config 应启用 [Config.1]

在此示例中，云团队正在解决FSBP控制EC2.2的发现。此控件的文档建议不要使用默认安全组，因为它允许通过默认的入站和出站规则进行广泛访问。由于无法删除默认安全组，因此建议更改规则设置以限制入站和出站流量。为了有效地解决此问题，云团队应使用已建立的机制来修改所有 VPC 的安全组规则，因为每个 VPC 都有此默认安全组。在大多数情况下，云团队使用AWS Control Tower自定义项或基础设施即代码 (IaC) 工具（例如HashiCorp Terraform或）来管理 VPC 配置。AWS CloudFormation

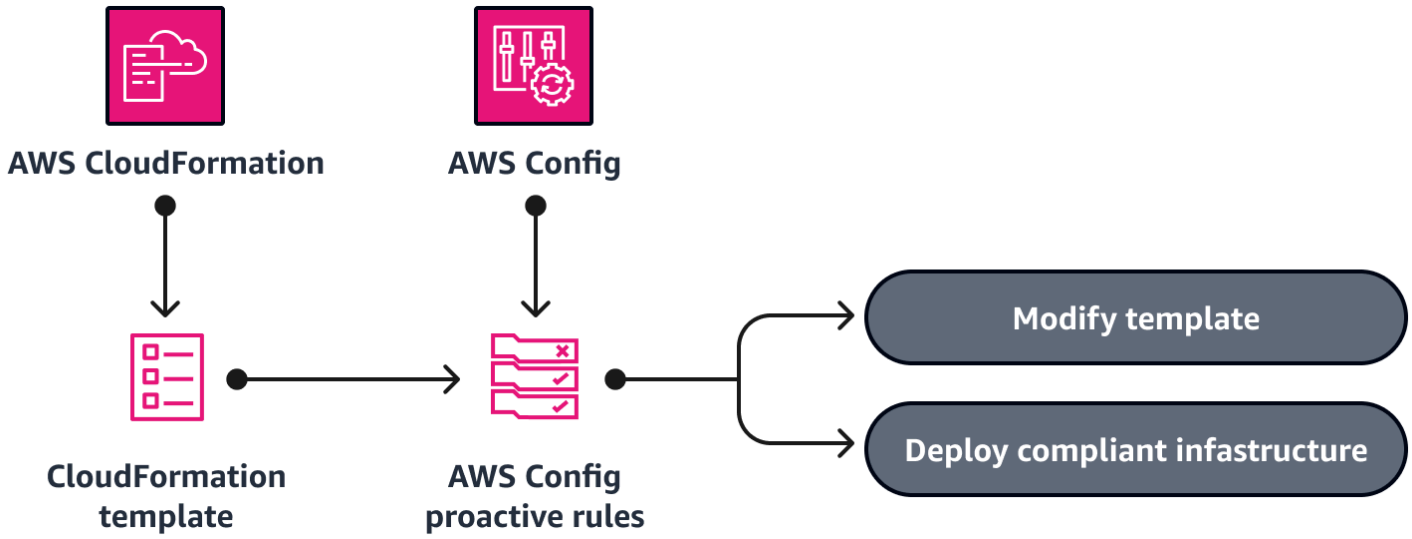
应用程序团队示例：创建 AWS Config 规则

以下是应用或开发团队可能负责的 Security Hub 基础安全最佳实践 (FSBP) 安全标准中的一些控制措施：

- [CloudFront.1] CloudFront 发行版应配置默认根对象
- [EC2.19] 安全组不应允许不受限制地访问高风险端口
- [CodeBuild.1] CodeBuild GitHub 或 Bitbucket 源存储库网址应使用 OAuth
- [ECS.4] ECS 容器应以非特权身份运行
- [ELB.1] 应将 Application Load Balancer 配置为将所有 HTTP 请求重定向到 HTTPS

在此示例中，应用团队正在解决FSBP控制EC2.19的发现。此控件检查风险最高的指定端口是否可以访问安全组的不受限制的传入流量。如果安全组中的任何规则允许来自`0.0.0.0/0`或`::/0`流向这些端口的入口流量，则此控制失败。此控件的文档建议删除允许此流量的规则。

除了解决单个安全组规则外，这也是一个很好的例子，说明了应该会产生新 AWS Config 规则的发现。通过使用主动评估模式，您可以帮助防止将来部署有风险的安全组规则。主动模式会在资源部署之前对其进行评估，这样您就可以防止资源配置错误及其相关的安全发现。在实施新服务或新功能时，应用程序团队可以在主动模式下运行规则，将其作为持续集成和持续交付 (CI/CD) 管道的一部分，以识别不合规的资源。下图显示了如何使用主动 AWS Config 规则来确认 AWS CloudFormation 模板中定义的基础架构是否合规。



在此示例中可以获得另一个重要的效率。当应用程序团队创建主动 AWS Config 规则时，他们可以在公共代码存储库中共享该规则，以便其他应用程序团队可以使用。

与 Security Hub 控件关联的每个发现都包含有关该发现的详细信息以及修复问题的说明的链接。尽管云团队可能会遇到需要手动进行一次性补救的发现，但我们建议在开发过程中尽早进行主动检查，以尽早发现问题。

报告并改进您的漏洞管理计划

有效的漏洞管理报告包括审查数据、监控趋势和共享知识。这提供了可见性，并帮助团队改善其组织的安全状况 AWS Cloud。

每月召开安全运营会议

每月一次的安全运营会议是促进团队持续自主权、问责制和协调一致的有效机制。在会议中，来自安全、云和应用程序团队的利益相关者将审查数据，以了解未完成的安全调查结果、服务级别协议 (SLA) 之外的调查结果以及发现最多的团队。

这些会议可以帮助您的团队识别反模式，例如增加更多限制的机会。还可以发现和分享预防性控制和自动化机会。这些会议还有助于确定漏洞管理计划中哪些行之有效，哪些不起作用，以便您可以做出改进。

通过审查数据、识别反模式和问题以及共享有关控制和自动化的信息，团队可以获得宝贵的见解并进行持续改进，从而增强其安全态势并降低与安全相关的服务水平协议。

使用 Security Hub 见解来识别反模式

AWS Security Hub 见解还可以帮助您识别反模式并跟踪修复发现的进度。Security Hub 见解是相关发现的集合。它确定了需要注意和干预的安全区域。Security Hub 见解可以帮助您确定具体需求并制定报告。Security Hub 提供了多种内置的托管见解。要跟踪您的 AWS 环境和使用情况所特有的安全问题，您可以创建自定义见解。

结论及后续步骤

总而言之，有效的漏洞管理计划需要充分的准备，并要求您启用正确的工具和集成，微调这些工具，高效地对问题进行分类，并持续报告和改进。通过遵循本指南中的最佳实践，组织可以在此基础上构建可扩展的漏洞管理计划 AWS ，以帮助保护其云环境。

您可以对该计划进行扩展，以包括其他与安全相关的漏洞和发现，例如应用程序安全漏洞。 AWS Security Hub 支持自定义产品集成。考虑使用 Security Hub 作为其他安全工具和产品的集成点。这种集成使您可以利用在漏洞管理计划中已经建立的流程和工作流程，例如与产品积压的直接集成以及每月的安全审查会议。

下表汇总了本指南中描述的阶段和操作项目。

阶段	操作项
准备	• 定义漏洞管理计划。 • 分配调查结果的所有权。 • 制定漏洞披露计划。 • 开发一个 AWS 账户 结构。 • 定义、实施和强制执行标签。 • 监控 AWS 安全公告。 • 使用授权管理员启用 Amazon Inspector。 • 使用委派管理员启用 Security Hub。 • 启用 Security Hub 标准。 • 设置 Security Hub 跨区域聚合。 • 在 Security Hub 中启用整合控制结果。 • 设置和管理 Security Hub 集成，包括与 SIEM、GRC、产品待办事项或票务系统的相应下游集成
分类和修复	• 基于多账户策略路由调查结果。 • 将调查结果发送给安全、云和应用程序或开发人员团队。 • 调整安全调查结果，确保它们适用于您的特定环境。

阶段	操作项
	• 尽可能开发自动补救机制。 • 尽可能实施有助于防止安全发现的 CI/CD 管道控制或其他护栏。 • 使用 Security Hub 自动化规则来上报或隐藏搜索结果。
举报并改进	• 每月举行安全运营会议。 • 使用 Security Hub 见解来识别反模式。

资源

AWS 服务文档

- 产品集成 ()AWS Security Hub
- 集成 AWS Security Hub 到 Jira Service Management Cloud (AWS Security Hub)
- 自动化规则 (AWS Security Hub)
- 主动评估规则 (AWS Config)
- 补丁管理器 (AWS Systems Manager)

其他 AWS 资源

- 标记 AWS 资源的最佳实践（AWS 白皮书）
- 开@@ 启自动安全响应 AWS（AWS 解决方案库）
- AWS 安全事件响应指南（AWS 技术指南）
- AWS 安全公告

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
初次发布	—	2023 年 10 月 12 日

AWS 规范性指导词汇表

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

数字

7 R

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

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

A

ABAC

请参阅基于属性的访问控制。

抽象服务

参见托管服务。

酸

参见原子性、一致性、隔离性、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？

人工智能运营（AIOps）

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

非对称加密

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

原子性、一致性、隔离性、持久性（ACID）

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

基于属性的访问权限控制（ABAC）

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

参见变更数据捕获。

更改数据捕获（CDC）

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

混沌工程

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

CI/CD

查看持续集成和持续交付。

分类

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

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心（CCoE）

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

云计算

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

云运营模型

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

云采用阶段

组织迁移到以下阶段时通常会经历四个阶段 AWS Cloud：

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

- 迁移 - 迁移单个应用程序
- 重塑 - 优化产品和服务，在云中创新

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

CMDB

参见配置管理数据库。

代码存储库

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

冷缓存

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

冷数据

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

计算机视觉 (CV)

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

配置偏差

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

配置管理数据库（CMDB）

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

合规性包

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

持续集成和持续交付（CI/CD）

自动执行软件发布过程的源代码、构建、测试、暂存和生产阶段的过程。CI/CD 通常被描述为管道。CI/CD 可以帮助您实现流程自动化、提高工作效率、改善代码质量并加快交付速度。有关更多信息，请参阅持续交付的优势。CD 也可以表示持续部署。有关更多信息，请参阅持续交付与持续部署。

CV

参见计算机视觉。

D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

根据网络中数据的关键性和敏感性对其进行识别和分类的过程。它是任何网络安全风险管理策略的关键组成部分，因为它可以帮助您确定对数据的适当保护和保留控制。数据分类是 Well-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。有关如何将领域驱动设计与 strangler fig 模式结合使用的信息，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

DR

参见灾难恢复。

漂移检测

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

DVSM

参见开发价值流映射。

E

EDA

参见探索性数据分析。

边缘计算

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

加密

一种将人类可读的纯文本数据转换为密文的计算过程。

加密密钥

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

字节顺序

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

端点

参见服务端点。

端点服务

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

企业资源规划 (ERP)

一种自动化和管理企业关键业务流程（例如会计、MES 和项目管理）的系统。

信封加密

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

environment

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

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

epic

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

ERP

参见企业资源规划。

探索性数据分析（EDA）

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

F

事实表

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

失败得很快

一种使用频繁和增量测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

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

功能分支

参见分支。

特征

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

特征重要性

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

功能转换

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

FGAC

请参阅精细的访问控制。

精细访问控制 (FGAC)

使用多个条件允许或拒绝访问请求。

快闪迁移

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

G

地理封锁

请参阅地理限制。

地理限制（地理阻止）

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

GitFlow 工作流程

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

全新策略

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

防护机制

一种高级规则，用于跨组织单位（OU）管理资源、策略和合规性。预防性防护机制会执行策略以确保符合合规性标准。它们是使用服务控制策略和 IAM 权限边界实现的。侦测性防护机制会检测策略违规和合规性问题，并生成警报以进行修复。它们通过使用 AWS Config、、Amazon、 AWS Security Hub GuardDuty AWS Trusted Advisor、Amazon Inspector 和自定义 AWS Lambda 支票来实现。

H

HA

参见高可用性。

异构数据库迁移

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

高可用性 (HA)

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

历史数据库现代化

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

同构数据库迁移

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

热数据

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

修补程序

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

hypercare 周期

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

I

IaC

参见基础架构即代码。

基于身份的策略

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

空闲应用程序

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

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 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

增量迁移

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

工业 4.0

该术语由克劳斯·施瓦布（Klaus Schwab）于2016年推出，指的是通过连接、实时数据、自动化、分析和人工智能/机器学习的进步实现制造流程的现代化。

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码（IaC）

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

工业物联网（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）数字化转型策略。

检查 VPC

在 AWS 多账户架构中，一种集中式 VPC，用于管理 VPC（相同或不同 AWS 区域）、互联网和本地网络之间的网络流量检查。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

物联网（IoT）

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

可解释性

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

IoT

参见物联网。

IT 信息库（ITIL）

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

IT 服务管理（ITSM）

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

ITIL

请参阅 IT 信息库。

ITSM

请参阅 IT 服务管理。

L

基于标签的访问控制 (LBAC)

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

登录区

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

大规模迁移

迁移 300 台或更多服务器。

LBAC

参见基于标签的访问控制。

最低权限

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

直接迁移

见 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参见字节顺序。

下层环境

参见环境。

M

机器学习（ML）

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

主分支

参见分支。

恶意软件

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

托管服务

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

制造执行系统 (MES)

一种软件系统，用于跟踪、监控、记录和控制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

一种小型独立服务，通过明确定义的 API 进行通信，通常由小型独立团队拥有。例如，保险系统可能包括映射到业务能力（如销售或营销）或子域（如购买、理赔或分析）的微服务。微服务的好处包括敏捷、灵活扩展、易于部署、可重复使用的代码和恢复能力。有关更多信息，请参阅使用 AWS 无服务器服务集成微服务。

微服务架构

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

迁移加速计划（MAP）

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

大规模迁移

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

迁移工厂

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

迁移元数据

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

迁移模式

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

迁移组合评测（MPA）

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

迁移准备情况评测（MRA）

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

迁移策略

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

ML

参见机器学习。

现代化

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

现代化准备情况评估

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

单体应用程序（单体式）

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

MPA

参见迁移组合评估。

MQTT

请参阅消息队列遥测传输。

多分类器

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

可变基础架构

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

O

OAC

请参阅源站访问控制。

OAI

参见源访问身份。

OCM

参见组织变更管理。

离线迁移

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

OI

参见运营集成。

OLA

参见运营层协议。

在线迁移

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

OPC-UA

参见开放流程通信-统一架构。

开放流程通信-统一架构 (OPC-UA)

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

运营级别协议（OLA）

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

运营准备情况审查 (ORR)

一份问题清单和相关的最佳实践，可帮助您理解、评估、预防或缩小事件和可能的故障的范围。有关更多信息，请参阅 Well-Architecte AWS d Frame work 中的运营准备情况评估 (ORR)。

操作技术 (OT)

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

运营整合（OI）

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

组织跟踪

由 AWS CloudTrail 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。

或者

参见运营准备情况审查。

OT

参见运营技术。

出站（出口）VPC

在 AWS 多账户架构中，一种处理从应用程序内部启动的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

P

权限边界

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

个人身份信息 (PII)

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

PII

查看个人身份信息。

playbook

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

PLC

参见可编程逻辑控制器。

PLM

参见产品生命周期管理。

策略

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

多语言持久性

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

组合评测

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

谓词

返回`true`或的查询条件`false`，通常位于子`WHERE`句中。

谓词下推

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

预防性控制

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

主体

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

隐私设计

一种贯穿整个工程化过程考虑隐私的系统工程方法。

私有托管区

私有托管区就是一个容器，其中包含的信息说明您希望 Amazon Route 53 如何响应一个或多个 VPC 中的某个域及其子域的 DNS 查询。有关更多信息，请参阅 Route 53 文档中的私有托管区的使用。

主动控制

一种安全控制措施，旨在防止部署不合规的资源。这些控件会在资源置备之前对其进行扫描。如果资源与控件不兼容，则不会对其进行配置。有关更多信息，请参阅 AWS Control Tower 文档中的控制参考指南，并参见在上实施安全控制中的主动控制 AWS。

产品生命周期管理 (PLM)

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

生产环境

参见环境。

可编程逻辑控制器 (PLC)

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

假名化

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

发布/订阅（发布/订阅）

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

Q

查询计划

一系列步骤，例如指令，用于访问 SQL 关系数据库系统中的数据。

查询计划回归

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

R

RACI 矩阵

参见 “负责任、负责、咨询、知情”（RACI）。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI 矩阵

参见 “负责任、负责、咨询、知情”（RACI）。

RCAC

请参阅行和列访问控制。

只读副本

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

重新架构师

见 7 R。

恢复点目标 (RPO)

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

恢复时间目标 (RTO)

服务中断和服务恢复之间可接受的最大延迟。

重构

见 7 R。

区域

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

回归

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

重新托管

见 7 R。

版本

在部署过程中，推动生产环境变更的行为。

搬迁

见 7 R。

更换平台

见 7 R。

回购

见 7 R。

故障恢复能力

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

基于资源的策略

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

责任、问责、咨询和知情（RACI）矩阵

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

响应性控制

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

保留

见 7 R。

退休

见 7 R。

旋转

定期更新密钥以使攻击者更难访问凭据的过程。

行列访问控制 (RCAC)

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

RPO

参见恢复点目标。

RTO

参见恢复时间目标。

运行手册

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

S

SAML 2.0

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

SCADA

参见监督控制和数据采集。

SCP

参见服务控制政策。

secret

在中 AWS Secrets Manager，您以加密形式存储的机密或受限信息，例如密码或用户凭证。它由密钥值及其元数据组成。密钥值可以是二进制、单个字符串或多个字符串。有关更多信息，请参阅 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 AWS Organizations的组织中所有账户的权限。SCP 为管理员可以委托给用户或角色的操作定义了防护机制或设定了限制。您可以将 SCP 用作允许列表或拒绝列表，指定允许或禁止哪些服务或操作。有关更多信息，请参阅 AWS Organizations 文档中的服务控制策略。

服务端点

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

服务水平协议（SLA）

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

服务级别指示器 (SLI)

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 (SLO)

代表服务运行状况的目标指标，由服务级别指标衡量。

责任共担模式

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

暹粒

参见安全信息和事件管理系统。

单点故障 (SPOF)

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

参见服务级别协议。

SLI

参见服务级别指标。

SLO

参见服务级别目标。

split-and-seed 模型

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

恶作剧

参见单点故障。

星型架构

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

strangler fig 模式

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

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

监控和数据采集 (SCADA)

在制造业中，一种使用硬件和软件来监控有形资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

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

中转网关是网络中转中心，您可用它来互连 VPC 和本地网络。有关更多信息，请参阅 AWS Transit Gateway 文档中的什么是公交网关。

基于中继的工作流程

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

可信访问权限

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

优化

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

双披萨团队

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

U

不确定性

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

无差别任务

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

上层环境

参见环境。

V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC 对等连接

两个 VPC 之间的连接，允许您使用私有 IP 地址路由流量。有关更多信息，请参阅 Amazon VPC 文档中的什么是 VPC 对等连接。

漏洞

损害系统安全的软件缺陷或硬件缺陷。

W

热缓存

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

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

一个 SQL 函数，用于对一组以某种方式与当前记录相关的行进行计算。窗口函数对于处理任务很有用，例如计算移动平均线或根据当前行的相对位置访问行的值。

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

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

蠕虫

参见一次写入，多读。

WQF

请参阅 AWS 工作负载资格框架。

一次写入，多次读取 (WORM)

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

Z

零日漏洞利用

一种利用未修补漏洞的攻击，通常是恶意软件。

零日漏洞

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

僵尸应用程序

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

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。