aws

达到基本八大成熟度 AWS

AWS 规范性指导

AWS 规范性指导: 达到基本八大成熟度 AWS

Table of Contents

简介 1
澳大利亚安全性和合规性 2
信息安全注册评估员计划 2
托管认证框架 2
AWS 分担责任模型 2
AWS Well-Architected 框架 3
重新解读八大要点策略 4
使用主题 4
重新解读云的八大要点策略 5
您正在使用哪些服务？ 5
您使用的是哪种部署模式？ 5
主题 1：托管服务 7
相关最佳实践 8
实现此主题 8
启用修补 8
扫描漏洞 8
监控此主题 8
实施治理检查 8
监控 Amazon Inspector 8
实施以下 AWS Config 规则 8
主题 3：不可变基础设施 10
相关最佳实践 10
实现此主题 11
实施 AMI 和容器构建管线 11
实施安全的应用程序构建管线 11
实施漏洞扫描 12
监控此主题 12
持续监控 IAM 和日志 12
实施以下 AWS Config 规则 12
主题 3：可变基础设施 13
相关最佳实践 13
实现此主题 13
自动修补 13
使用自动化而不是手动流程 13

使用自动化在 EC2 实例上安装以下项 14
发布任何版本之前都应进行同行审查，以确保变更符合最佳实践。 14
使用身份级别的控件 14
实施漏洞扫描 14
监控此主题 14
持续监控补丁合规性 14
持续监控 IAM 和日志 15
实施以下 AWS Config 规则 15
主题 4：身份 16
相关最佳实践 16
实现此主题 17
实施身份联合验证 17
应用最低权限许可 17
轮换凭证 17
强制执行 MFA 18
监控此主题 18
监控最低访问权限 18
实施以下 AWS Config 规则 18
主题 5：数据边界 19
相关最佳实践 19
实现此主题 19
实施身份控制 19
实施资源控制 20
实施网络控制 20
监控此主题 20
监控策略 20
实施以下 AWS Config 规则 20
主题 6：备份 21
Well-Architecte AWS d Framework 中的相关最佳实践 21
实现此主题 22
自动执行数据备份和恢复 22
相关最佳实践 22
监控此主题 22
实施以下 AWS Config 规则 22
主题 7：记录和监控 24
相关最佳实践 24

实现此主题 24
启用日志记录 24
实施日志记录安全最佳实践 25
集中日志 25
监控此主题 25
实施机制 25
实施以下 AWS Config 规则 25
主题 8：手动流程机制 27
相关最佳实践 27
实现此主题 27
监控此主题 28
案例研究 29
概述 29
核心架构 29
无服务器数据湖 30
容器化 Web 服务 31
COTS 软件 33
资源 35
AWS 文档 35
其他 AWS 资源 35
澳大利亚网络安全中心资源 35
贡献者 36
附录：控制矩阵 37
应用程序控制 37
修补应用程序 41
配置 Microsoft Office 宏设置 45
用户应用程序固化 46
限制管理权限 48
修补操作系统 54
多重身份验证 57
定期备份 61
版权声明 63
文档历史记录 64
术语表 65
..... 65
A 65

B 68
C 69
D 72
E 75
F 77
G 78
H 79
我 80
L 82
M 83
O 87
P 89
Q 91
R 92
S 94
T 97
U 98
V 99
W 99
Z 100
..... ci

在以下方面达到基本八项的成熟度 AWS：澳大利亚组织的安全与合规性

Amazon Web Services（贡献者）

2024 年 11 月（文档历史记录）

澳大利亚信号局（ASD）已制定并确定战略的优先顺序，以帮助组织降低网络安全威胁的风险。从中选取了八种策略，形成了八大要点框架。根据八大要点框架，澳大利亚的许多公共和私营部门组织都必须达到成熟度。

澳大利亚网络安全中心（ACSC）创建了八大要点框架，来帮助保护基于 Microsoft 的互联网连接网络。但是，许多组织都必须在其所有环境（包括本地环境和云）达到八大要点成熟度。

八大要点框架还包含一个成熟度模型，旨在帮助组织通过渐进式迭代来实施该框架。该模型概述了从零到三的成熟度级别。成熟度三级代表对高级网络安全策略和高度针对性攻击的抵御能力。本指南提供了具体、自以为是的指导，可帮助您达到基本八级成熟度三级。 AWS

澳大利亚组织的安全性和合规性

澳大利亚的许多组织都使用 AWS Cloud 来存储机密数据、处理敏感交易和构建关键服务。

虽然本指南讨论了如何调整八大要点框架以适应云，但 AWS 也提供了以下认证和模型来帮助您满足组织的安全性和合规性要求：

- 信息安全注册评估员计划
- 托管认证框架
- AWS 分担责任模型
- AWS Well-Architected 框架

信息安全注册评估员计划

AWS 服务 已根据澳大利亚网络安全中心 (ACSC) 信息安全注册评估员计划 (IRAP) 进行了受保护级别的评估。澳大利亚信号局（ASD）认证的独立IRAP评估员完成了对IRAP的评估。 AWS该评估可确保在 AWS 产品和服务方面，对受保护级别的工作负载实施了适用的控制措施。

AWS IRAP PROTECTED 软件包可通过以下方式AWS Artifact获得。IRAP 报告是使用 ACSC 云安全指引（ACSC 网站）编写的。有关范围内 AWS 服务 的完整列表，请参阅范围内的AWS 服务 ：IRAP。

托管认证框架

澳大利亚托管认证框架的制定是为了支持政府系统和数据的安全管理。该框架旨在帮助组织降低供应链和数据中心所有权风险。 AWS 已获得认证战略级别的认证。这有助于政府机构继续快速创新，因为他们知道这 AWS 符合政府要求。

AWS 分担责任模型

责任AWS 共担模型定义了您如何分担云端安全与 AWS 合规责任。 AWS 保护运行中提供的所有服务的基础架构 AWS Cloud，并且您有责任保护您对这些服务（例如您的数据和应用程序）的使用。

此共担模式可以帮助减轻您的合规性和运营负担，因为 AWS 运行、管理和控制从主机操作系统和虚拟化层到运行各种服务的设施的物理安全性等许多组件。您负责管理来宾操作系统（包括更新和安全补丁程序）及其他关联应用程序软件。您还负责配置 AWS 提供的安全组防火墙。

当你临近 Essential Eight 成熟度时，了解 AWS 分担责任模式至关重要 AWS。您的责任因使用的服务、这些类服务与您的 IT 环境的集成以及适用的法律和法规而异。

AWS Well-Architected 框架

AWS Well-Architected 帮助云架构师为各种应用程序和工作负载构建安全、高性能、弹性和高效的基础架构。Well AWS -Architected Framework 提供了架构最佳实践，可帮助您设计、构建和操作系统。AWS此框架基于以下六个支柱而构建：卓越运营、安全性、可靠性、性能效率、成本优化及可持续性。

AWS 还提供用于审查您的工作负载的服务。AWS Well-Architected Tool它可以帮助你使用 Well-Architecte AWS d Framework 来审查和评估你的架构。为您提供建议，以使您的工作负载变得更可靠、安全、高效且经济有效。

重新解读云的八大要点策略

以下是最初为基于 Microsoft 的互联网连接网络设计的八大要点缓解策略：

- 应用程序控制
- 修补应用程序
- 配置 Microsoft Office 宏设置
- 用户应用程序固化
- 限制管理权限
- 修补操作系统
- 多重身份验证
- 定期备份

需要再次强调的是，八大要点框架并非为云环境而设计。但是，基本原则是适用的，基本八大策略和Well-Architecte AWS d Framework最佳实践之间存在重叠之处。

各种云原生方法可以提高安全性并显著减轻您的合规负担。在本地环境中，您对安全的各个方面负责，并且不存在继承的控制措施。在云中运行工作负载 AWS 时，负责保护运行我们服务的基础架构。您还可以通过使用自动化和托管服务来减轻合规负担。托管服务，也称为抽象服务， AWS 服务 用于 AWS 运营基础设施层、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。有关更多信息，请参阅本指南的主题 1：使用托管服务部分。

因此，需要进行一些重新解释，才能使八大要点策略适合 AWS上的工作负载。本指南将基本八大策略转换为 AWS 主题。

使用主题

本指南分为八个主题。每个 Essential Eight 策略都映射到以下一个或多个主题，每个主题都映射到 Well-Architecte AWS d Framework 中的一个或多个最佳实践：

- 主题 1：使用托管服务
- 主题 2：通过安全管线管理不可变基础设施
- 主题 3：通过自动化管理可变基础设施
- 主题 4：管理身份

- 主题 5：建立数据边界
- 主题 6：自动备份
- 主题 7：集中记录和监控
- 主题 8：实施手动流程机制

每个主题都包括该主题的概述、相关的Well-Architect AWS ed Framework最佳实践，以及有关如何实现基本八项成熟度和监控合规性的说明。这些说明提供了手动步骤或帮助您使用 AWS Config 规则配置自动化。手动步骤需要相应的机制，来确保发现的问题得到解决。有关更多信息，请参阅主题 8：实施手动流程机制。 AWS Config 规则需要类似的监督或自动化，才能补救不合规的资源。通过遵循与这些主题一致的指引，您可以采用一种能够最大限度地发挥云优势的方法，达到八大要点成熟度。

重新解读云的八大要点策略

由于八大要点框架不是为云环境设计的，因此在解决每个八大要点策略的基本原则时，必须采用云原生方法。方法因两个关键问题而异。

您正在使用哪些服务？

AWS 分担责任模型可以帮助您减轻合规和运营负担。托管服务将更多责任转移到 AWS 维护已部署服务的可用性、性能和安全优化上。托管服务还消除了维护服务的运营和管理负担，让您的团队有更多时间专注于创新。

托管服务包括无服务器服务，例如 Amazon API Gateway、AWS Lambda 和 DynamoDB。与 Amazon Elastic Compute Cloud（Amazon EC2）上的数据库相比，Amazon Relational Database Service（Amazon RDS）上的数据库所需的运营责任更少。

例如，如果您正在调整云端操作系统的 Essential Eight 策略，则需要考虑正在使用哪些服务，以及是否负责修补这些资源。 AWS 负责修补完全托管的服务，例如 Lambda 和 DynamoDB。对于其他服务，例如 Amazon RDS 或 Amazon Redshift，您可能需要在维护时段内管理补丁。

您使用的是哪种部署模式？

您的组织是否在使用可变或不可变的基础设施方法？

可变基础设施模型更新和修改生产工作负载的现有基础设施。这是云之前的标准部署方法，当时更换服务器基础设施成本高昂且耗时，因此最实用的方法是将更改应用于已在生产环境中运行的服务器。云中可变方法的一个示例是将应用程序更改直接部署到正在运行的 EC2 实例上，可以手动部署或使用软件部署服务，例如 AWS Systems Manager Run Command 或 AWS CodeDeploy。

不可变基础设施模型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。不可变方法的一个示例是在 AWS CloudFormation 或 AWS Cloud Development Kit (AWS CDK) 中定义应用程序堆栈。您可以使用这些服务通过持续集成和持续交付（CI/CD）管线部署应用程序堆栈。此方法使用滚动或蓝绿等部署方法。有关此方法的更多信息，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。

例如，如果您要为云调整修补操作系统八大要点策略，则需要考虑如何将补丁应用于部署模型。对于可变基础设施，您可以手动修补资源，或者通过自动化提高运营效率。如果你使用的是不可变的基础架构，那么你需要使用 CI/CD 管道来部署带有最新版本操作系统的新基础架构。实际上，在这种模式下，修补一词用词不当，因为基础设施将被替换而不是修补。

主题 1：使用托管服务

涵盖八大要点策略

修补应用程序、限制管理权限、修补操作系统

托管服务允许 AWS 您管理一些安全任务，例如修补和漏洞管理，从而帮助您减少合规义务。

如AWS 分担责任模型本节所述，您与您共同 AWS 负责云安全与合规性。这可以减轻您的运营负担，因为可以 AWS 操作、管理和控制组件，从主机操作系统和虚拟化层到服务运行设施的物理安全。

您的职责可能包括管理托管服务（例如亚马逊关系数据库服务 (Amazon RDS) 或 Amazon Redshift）的维护窗口，以及扫描 AWS Lambda 代码或容器映像中的漏洞。与本指南中的所有主题一样，您也保留监控和合规报告的责任。您可以使用 Amazon Inspector 报告您的所有 AWS 账户中的漏洞。您可以使用中的规则 AWS Config 来确保诸如 Amazon RDS 和 Amazon Redshift 之类的服务已启用次要更新和维护窗口。

例如，如果您运行 Amazon EC2 实例，则您的责任包括：

- 应用程序控制
- 修补应用程序
- 将管理权限限制在 Amazon EC2 控制面板和操作系统（OS）
- 修补操作系统
- 强制执行多因素身份验证 (MFA) 以访问控制平面 AWS 和操作系统
- 备份数据和配置

而如果您运行 Lambda 函数，则您的责任就会减少，包括：

- 应用程序控制
- 确认图书馆是 up-to-date
- 将管理权限限制为 Lambda 控制面板
- 强制 MFA 访问控制平面 AWS
- 备份 Lambda 函数代码和配置

Well-Architecte AWS d Framework 中的相关最佳实践

- SEC01-BP05 缩小安全管理范围

实现此主题

启用修补

- 应用 Amazon RDS 更新
- 在中启用托管更新 AWS Elastic Beanstalk
- 注意 Amazon Redshift 集群维护时段

扫描漏洞

- 使用 Amazon Inspector 扫描 Amazon Elastic Container Registry（Amazon ECR）容器映像
- 使用 Amazon Inspector 扫描 Lambda 函数

监控此主题

实施治理检查

- 在 ACSC Essential 8 一致性包中启用《运营最佳实践》 AWS Config

监控 Amazon Inspector

- 评测账户级别的覆盖率
- 管理多个账户

实施以下 AWS Config 规则

- `RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED`
- `ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED`
- `REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK`

- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EKS_CLUSTER_SUPPORTED_VERSION

主题 2：通过安全管线管理不可变基础设施

涵盖八大要点策略

应用程序控制、修补应用程序、修补操作系统

对于不可变的基础架构，您必须保护部署管道以进行系统更改。 AWS 杰出工程师Colm MacCárthaigh在2022年re: Invent会议上的 “零权限操作：在不访问数据的情况下运行服务”（YouTube视频）演示中解释了这一原则。 AWS

通过限制对配置 AWS 资源的直接访问，您可以要求通过经批准的、安全的自动化管道来部署或更改所有资源。通常，您可以创建 AWS Identity and Access Management（IAM）策略以允许用户仅访问托管部署管线的账户。您还可以配置 IAM 策略，以允许有限数量的用户进行紧急访问。为防止手动更改，您可以使用安全组阻止对服务器的 SSH 和 Windows 远程桌面协议（RDP）访问。会话管理器是一项功能 AWS Systems Manager，可以提供对实例的访问权限，而无需打开入站端口或维护堡垒主机。

亚马逊机器映像（AMI）和容器映像必须安全且可重复构建。对于 Amazon EC2 实例，您可以使用 EC2 Image Builder 来构建 AMIs 具有内置安全功能（例如实例发现、应用程序控制和日志记录）的实例。有关应用程序控制的更多信息，请参阅 ACSC 网站上的实现应用程序控制。您也可以使用 Image Builder 来构建容器映像，且可以使用 Amazon Elastic Container Registry（Amazon ECR）跨账户共享这些映像。中央安全团队可以批准构建这些镜像 AMIs 和容器镜像的自动流程，以便应用程序团队批准使用生成的任何 AMI 或容器映像。

必须使用 AWS CloudFormation 或 AWS Cloud Development Kit (AWS CDK) 等服务在基础设施即代码（IaC）中定义应用程序。代码分析工具 AWS CloudFormation Guard，例如 cfn-nag 或 cdk-nag，可以根据您批准的管道中的安全最佳实践自动测试代码。

与主题 1：使用托管服务一样，Amazon Inspector 可以报告您 AWS 账户中的漏洞。集中的云和安全团队可以使用此信息，来验证应用程序团队是否满足安全性和合规性要求。

要监控和报告合规性，请持续审查 IAM 资源和日志。使用 AWS Config 规则确保只使用经批准 AMIs 的资源，并确保将 Amazon Inspector 配置为扫描 Amazon ECR 资源中是否存在漏洞。

Well-Architecte AWS d Framework 中的相关最佳实践

- OPS05-BP04 使用构建和部署管理系统

- REL08-使用不可变基础架构进行BP04 部署
- SEC06-BP03 减少手动管理和交互式访问

实现此主题

实施 AMI 和容器构建管线

- 使用 EC2 Image Builder 并将以下内容构建到您的 AMIs：
  - AWS Systems Manager 代理（SSM 代理），用于实例发现和管理
  - 用于应用程序控制的安全工具，例如安全增强型 Linux (SELinux) (GitHub)、文件访问策略守护程序 (fapolicyd) (GitHub) 或 OpenSCAP
  - Amazon A CloudWatch gent，用于记录
- 对于所有 EC2 实例，请在实例配置文件或 Systems Manager 用于访问实例的 IAM 角色中包含 `CloudWatchAgentServerPolicy` 和 `AmazonSSMManagedInstanceCore` 策略。
- AMIs 与整个组织共享
- 共享 EC2 Image Builder 资源
- 确保应用团队参考的是最新的 AMIs
- 使用您的 AMI 管线进行补丁管理
- 实施容器构建管线：
  - 使用 EC2 Image Builder 控制台向导创建容器映像管线
  - 使用 Amazon ECR 作为来源，为您的容器镜像构建持续交付渠道（AWS 博客文章）
- 通过多账户和多区域架构在组织中共享 ECR 容器映像

实施安全的应用程序构建管线

- 为 IaC 实施构建管道，例如使用 EC2 Image Builder 和 AWS CodePipeline（AWS 博客文章）
- 在 CI/CD 管道中使用代码分析工具 AWS CloudFormation Guard，例如 cfn-nag (GitHub) 或 cdk-nag (GitHub)，来帮助检测违反最佳实践的行为，例如：
  - 过于宽松的 IAM 策略，例如使用通配符的策略
  - 过于宽松的安全组规则，例如使用通配符或允许 SSH 访问的规则
  - 未启用的访问日志
  - 未启用的加密

  - 密码文本
- 在管道中实现扫描工具（AWS 博客文章）
- AWS Identity and Access Management Access Analyzer 在管道中使用（AWS 博客文章）来验证 CloudFormation 模板中定义的 IAM 策略
- 配置 IAM 策略和服务控制策略，以获得使用管线或对其进行任何修改的最低权限访问权限

实施漏洞扫描

- 在您组织的所有账户中启用 Amazon Inspector
- 使用 Amazon Inspector AMIs 在你的 AMI 构建管道中进行扫描：
  - 在 EC2 Image Builder 中管理 AMI 的生命周期 () GitHub
- 使用 Amazon Inspector 为 Amazon ECR 存储库配置增强扫描
- 构建漏洞管理程序，对安全调查发现进行分类和修复

监控此主题

持续监控 IAM 和日志

- 定期查看您的 IAM 策略，以确保：
  - 只有部署管线可以直接访问资源
  - 只有经批准的服务才能直接访问数据
  - 用户没有直接访问资源或数据的权限。
- 监控 AWS CloudTrail 日志以确认用户正在通过管道修改资源，而不是直接修改资源或访问数据
- 定期查看 IAM 访问权限分析器调查发现
- 设置提醒，以便在 AWS 账户 的根用户凭证被使用时通知您。

实施以下 AWS Config 规则

- `APPROVED_AMIS_BY_ID`
- `APPROVED_AMIS_BY_TAG`
- `ECR_PRIVATE_IMAGE_SCANNING_ENABLED`

主题 3：通过自动化管理可变基础设施

涵盖八大要点策略

应用程序控制、修补应用程序、修补操作系统

与不可变基础设施类似，您可以将可变基础设施作为 IaC 来管理，并通过自动化流程修改或更新此基础设施。不可变基础设施的许多实现步骤也适用于可变基础设施。但是，对于可变基础设施，您还必须实施手动控制，以确保修改的工作负载仍遵循最佳实践。

对于可变基础架构，您可以使用 Patch Manager（一项功能）来自动管理补丁。 AWS Systems Manager在 AWS 组织的所有账户中启用补丁管理器。

防止直接访问 SSH 和 RDP，并要求用户使用会话管理器或运行命令，这也是 Systems Manager 的功能。与 SSH 和 RDP 不同，这些功能可以记录系统访问和更改。

要监控和报告合规性，您必须持续审查补丁合规性。您可以使用 AWS Config 规则来确保所有 Amazon EC2 实例均由 Systems Manager 管理，拥有所需的权限和已安装的应用程序，并且符合补丁合规性。

Well-Architecte AWS d Framework 中的相关最佳实践

- SEC06-BP03 减少手动管理和交互式访问
- SEC06-BP05 自动计算保护

实现此主题

自动修补

- 实施在 AWS 组织的所有账户中启用补丁管理器
- 对于所有 EC2 实例，请在实例配置文件或 Systems Manager 用于访问实例的 IAM 角色中包含 `CloudWatchAgentServerPolicy` 和 `AmazonSSMManagedInstanceCore`。

使用自动化而不是手动流程

- 在 主题 2：通过安全管线管理不可变基础设施 中遵循实施 AMI 和容器构建管线中的指引

- 使用会话管理器或运行命令而不是直接访问 SSH 或 RDP

使用自动化在 EC2 实例上安装以下项

- AWS Systems Manager 代理（SSM 代理），用于实例发现和管理
- 用于应用程序控制的安全工具，例如安全增强型 Linux (SELinux) (GitHub)、文件访问策略守护程序 (fapolicyd) (GitHub) 或 OpenSCAP
- Amazon A CloudWatch gent，用于记录

发布任何版本之前都应进行同行审查，以确保变更符合最佳实践。

- 过于宽松的 IAM 策略，例如使用通配符的策略
- 过于宽松的安全组规则，例如使用通配符或允许 SSH 访问的规则
- 未启用的访问日志
- 未启用的加密
- 密码文本
- 安全的 IAM 策略

使用身份级别的控件

- 为了要求用户通过自动化流程修改资源并防止手动配置，请允许用户对可代入的角色授予只读权限。
- 仅向服务角色授予修改资源的权限，例如 Systems Manager 使用的角色

实施漏洞扫描

- 遵循 主题 2：通过安全管线管理不可变基础设施 中的实施漏洞扫描中的指引
- 使用 Amazon Inspector 扫描您的 EC2 实例

监控此主题

持续监控补丁合规性

- 使用自动化和控制面板报告补丁合规性

- 实施一种机制来审查控制面板的补丁合规性

持续监控 IAM 和日志

- 定期查看您的 IAM 策略，以确保：
  - 只有部署管线可以直接访问资源
  - 只有经批准的服务才能直接访问数据
  - 用户没有直接访问资源或数据的权限。
- 监控 AWS CloudTrail 日志，确保用户通过管道修改资源，而不是直接修改资源或访问数据
- 定期审查 AWS Identity and Access Management Access Analyzer 调查结果
- 设置提醒，以便在 AWS 账户 的根用户凭证被使用时通知您。

实施以下 AWS Config 规则

- EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK
- EC2_INSTANCE_MANAGED_BY_SSM
- EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED - SELinux/fapolicyd/OpenSCAP, CW Agent
- EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED - any unsupported apps
- IAM_ROLE_MANAGED_POLICY_CHECK - CW Logs, SSM
- EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK
- REQUIRED_TAGS
- RESTRICTED_INCOMING_TRAFFIC - 22, 3389

主题 4：管理身份

涵盖八大要点策略

限制管理权限，多重身份验证

稳健的身份和权限管理是管理云安全的关键方面。强大的身份实践如何在必要的访问权限和最低权限之间取得平衡。这有助于开发团队在不影响安全性的情况下快速行动。

使用身份联合验证来集中管理身份。这样一来，由于可以从一个位置管理访问权限，因此更容易管理跨多个应用程序和服务的访问权限。这也可以帮助您实现临时权限和多重身份验证（MFA）。

仅向用户授予他们执行任务所需的权限。 AWS Identity and Access Management Access Analyzer 可以验证策略并验证公共和跨账户访问。 AWS Organizations 服务控制策略 (SCPs)、IAM 策略条件、IAM 权限边界和 AWS IAM Identity Center 权限集等功能可以帮助您配置精细访问控制 (F GAC)。

进行任何类型的身份验证时，最好使用临时凭证来减少或消除风险，例如凭证被无意泄露、共享或被盗。使用 IAM 角色而不是 IAM 用户。

使用强大的登录机制（例如 MFA）来减小登录凭证被无意泄露或很容易猜到的风险。根用户需要 MFA，您也可以在联合身份验证级别要求 MFA。如果不可避免地使用 IAM 用户，请强制执行 MFA。

要监控和报告合规性，您必须不断努力减少权限，监控来自 IAM 访问权限分析器的调查发现，并删除未使用的 IAM 资源。使用 AWS Config 规则来确保强制使用强大的登录机制、证书的有效期以及使用 IAM 资源。

Well-Architecte AWS d Framework 中的相关最佳实践

- SEC02-BP01 使用强大的登录机制
- SEC02-BP02 使用临时证书
- SEC02-安全地BP03 存储和使用机密
- SEC02-BP04 依赖集中式身份提供商
- SEC02-定期BP05 审核和轮换证书
- SEC02-BP06 使用用户组和属性
- SEC03-BP01 定义访问要求

- SEC03-BP02 授予最低权限访问权限
- SEC03-BP03 建立紧急访问流程
- SEC03-持续BP04 减少权限
- SEC03-BP05 为您的组织定义权限护栏
- SEC03-基于生命周期BP06 管理访问权限
- SEC03-BP07 分析公开和跨账户访问权限
- SEC03-在组织内安全BP08 共享资源

实现此主题

实施身份联合验证

- 要求人类用户通过与身份提供者联合身份验证，并使用临时凭证访问 AWS
- Implement temporary elevated access to your AWS environments

应用最低权限许可

- 保护您的 root 用户凭证，不要将其用于日常任务
- 使用 IAM Access Analyzer 根据访问活动生成最低权限策略
- 使用 IAM Access Analyzer 验证公共和跨账户对资源的访问权限
- 使用 IAM 访问权限分析器验证您的 IAM 策略，以确保权限的安全性和功能性
- 跨多个账户建立权限防护栏
- 使用权限边界设置基于身份的策略可以授予的最大权限
- 使用 IAM 策略中的条件进一步限制访问权限
- 定期审查并删除未使用的用户、角色、权限、策略和证书
- 开始使用 AWS 托管策略，转向最低权限权限
- 使用 IAM Identity Center 中的权限集功能

轮换凭证

- 要求工作负载使用 IAM 角色进行访问 AWS
- 自动删除未使用的 IAM 角色

- 对于需要长期凭证的用例，定期轮换访问密钥

强制执行 MFA

- 根用户需要 MFA
- 要求通过 IAM Identity Center 进行 MFA
- 考虑要求对特定于服务的 API 操作进行 MFA

监控此主题

监控最低访问权限

- 将 IAM 访问分析器的调查结果发送至 AWS Security Hub CSPM
- 考虑为关键 IAM Identity Center 调查发现设置通知
- 定期查看您的证书报告 AWS 账户

实施以下 AWS Config 规则

- ACCESS_KEYS_ROTATED
- IAM_ROOT_ACCESS_KEY_CHECK
- IAM_USER_MFA_ENABLED
- IAM_USER_UNUSED_CREDENTIALS_CHECK
- IAM_PASSWORD_POLICY
- ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

主题 5：建立数据边界

涵盖八大要点策略

限制管理权限

数据边界是 AWS 环境中的一组预防性护栏，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。这些护栏充当了永远在线的边界，有助于保护您在各种资源中的数据。 AWS 账户 这些组织范围的护栏并不能取代现有的精细访问控制。相反，它们通过确保所有 AWS Identity and Access Management (IAM) 用户、角色和资源都遵守一组定义的安全标准来帮助改善您的安全策略。

您可以使用禁止从组织边界之外进行访问的策略（通常是在 AWS Organizations中创建的）来建立数据边界。用于建立数据边界的三个主要边界授权条件是：

- 可信身份 — 您内部的委托人（IAM 角色或用户） AWS 账户，或代表您 AWS 服务 行事。
- 可信资源 — 属于您的资源 AWS 账户 或代表您管理的资源。 AWS 服务
- 预期的网络 — 您的本地数据中心和虚拟私有云 (VPCs)，或者代表您 AWS 服务 行事的网络。

考虑在不同数据分类（例如 `OFFICIAL:SENSITIVE` 或 `PROTECTED`）或不同风险级别（例如开发、测试或生产）的环境之间实施数据边界。有关更多信息，请参阅 AWS（AWS 白皮书）上的 “构建数据边界” 和 “建立数据边界 AWS：概述”（AWS 博客文章）。

Well-Architecte AWS d Framework 中的相关最佳实践

- SEC03-BP05 为您的组织定义权限护栏
- SEC07-根据数据敏感度BP02 应用数据保护控制

实现此主题

实施身份控制

- 仅允许可信身份访问您的资源：使用带有条件密钥 `aws:PrincipalOrgID` 和 `aws:PrincipalIsAWSService` 的基于资源的策略。这只允许您所在 AWS 组织和来自的委托 AWS 人访问您的资源。

- 仅允许来自您的网络的可信身份：使用带有条件键 `aws:PrincipalOrgID` 和 `aws:PrincipalIsAWSService` 的 VPC 端点策略。这只允许来自您的组织和来自您的 AWS 组织的委托人通过 VPC 终端节点访问服务。 AWS

实施资源控制

- 仅允许您的身份访问可信资源- 使用带有条件密钥的服务控制策略 (SCPs) `aws:ResourceOrgID`。这允许您的身份仅访问 AWS 组织中的资源。
- 允许仅从您的网络访问可信资源：使用带有条件键 `aws:ResourceOrgID` 的 VPC 端点策略。此设置允许您的身份仅通过属于您的 AWS 组织的 VPC 端点来访问服务。

实施网络控制

- 允许身份仅从预期的网络访问资源- SCPs 与条件密钥`aws:SourceIp`、`aws:SourceVpc`和`aws:SourceVpce`、和一起使用`aws:ViaAWSService`。这允许您的身份仅从预期的 IP 地址、、 VPCs、VPC 终端节点以及通过访问资源 AWS 服务。
- 允许仅从预期的网络访问您的资源：使用带有条件键 `aws:SourceIp`、`aws:SourceVpc`、`aws:SourceVpce`、`aws:ViaAWSService` 和 `aws:PrincipalIsAWSService` 的基于资源的策略。这仅允许从预期的、从预期的 IPs、从预期 VPCs的 VPC 终端节点 AWS 服务、通过或当主叫身份为时访问您的资源 AWS 服务。

监控此主题

监控策略

- 实施审查机制 SCPs、IAM 策略和 VPC 终端节点策略

实施以下 AWS Config 规则

- `SERVICE_VPC_ENDPOINT_ENABLED`

主题 6：自动备份

涵盖八大要点策略

定期备份

“如果故障在所难免，那么一切操作会在一段时间后全部失败：从路由器到硬盘，从操作系统到内存单元 TCP 数据包损坏，从暂时性错误到永久性故障。不管使用的是最高质量的硬件还是最低成本的组件，必然会出现故障。” – Werner Vogels，Amazon 首席技术官，其博客名为 All Things Distributed

数据备份和恢复是系统可靠性的关键部分。 AWS 旨在更轻松地创建备份，保持备份数据的持久性，并确保备份的数据保持可恢复状态。

AWS Backup 是一项完全托管服务，可集中并自动执行跨 AWS 服务的数据备份。它支持多种 AWS 资源类型，可帮助您为使用多种 AWS 资源且必须集体备份的工作负载实施和维护备份策略。 AWS Backup 还可以帮助您共同监视多个 AWS 资源的备份和还原操作。

AWS Backup 文件库锁定是备份保管库的一项可选功能，它可以提供额外的安全性和控制力。当锁在合规模式下处于活跃状态并且宽限期结束时，用户、账户或数据所有者或者 AWS无法更改或删除保管库配置。每个保管库可以有一个保管库锁。这提供了一次写入多次读取（WORM）配置和保留期的强制执行。

如果您遵循当前的配置指南，则 AWS Backup 可以提供 99.999999999% 的年度耐久性，也称为 11 9。它使用 AWS 全球基础架构跨多个可用区复制您的备份。有关更多信息，请参阅 AWS Backup中的韧性。

AWS Backup 帮助您自动恢复和测试备份数据，以验证备份的完整性和流程。

Well-Architecte AWS d Framework 中的相关最佳实践

- SEC09-BP01 实施安全密钥和证书管理
- SEC09-在传输过程中BP02 强制加密
- SEC09-BP03 验证网络通信

实现此主题

自动执行数据备份和恢复

- 在上实施数据备份 AWS
- 大规模自动备份数据（AWS 博客文章）
- 使用 AWS Backup（AWS 博客文章）自动验证数据恢复

在所有 AWS Backup 结果中实施治理

- 保护备份的十大安全最佳实践 AWS（AWS 博客文章）
- 使用 AWS Backup Vault Lock 来提高备份存储库的安全性
- 使用 AWS Backup Audit Manager 审计 AWS Backup 策略的合规性

监控此主题

实施以下 AWS Config 规则

- RDS_IN_BACKUP_PLAN
- RDS_LAST_BACKUP_RECOVERY_POINT_CREATED
- RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- REDSHIFT_BACKUP_ENABLED
- AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED
- AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
- BACKUP_RECOVERY_POINT_ENCRYPTED
- BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
- BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
- DB_INSTANCE_BACKUP_ENABLED
- DYNAMODB_IN_BACKUP_PLAN
- DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED
- DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

- EBS_IN_BACKUP_PLAN
- EBS_LAST_BACKUP_RECOVERY_POINT_CREATED
- EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- EC2_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_LAST_BACKUP_RECOVERY_POINT_CREATED
- S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED
- STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN
- VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED
- VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

主题 7：集中记录和监控

> **涵盖八大要点策略**
>
> 应用程序控制、修补应用程序、限制管理权限、多因素身份验证

AWS 提供的工具和功能使您能够查看 AWS 环境中正在发生的事情。这些方法包括：

- AWS CloudTrail通过为您的账户创建 AWS API AWS 调用的历史记录（包括通过、和命令行工具进行的 API 调用） AWS 管理控制台 AWS SDKs，帮助您监控部署。对于支持的服务 CloudTrail，您还可以识别哪些用户和账户调用了该服务的 API、发出呼叫的源 IP 地址以及调用的发生时间。
- Amazon CloudWatch 可帮助您实时监控您的 AWS 资源和运行的应用程序 AWS 的指标。
- Amazon CloudWatch Lo gs 可帮助您集中所有系统和应用程序的日志， AWS 服务 这样您就可以监控它们并安全地将其存档。
- Amazon GuardDuty 是一项持续的安全监控服务，可分析和处理日志，以识别您的 AWS 环境中意外和可能未经授权的活动。 GuardDuty 与 Amazon EventBridge 集成，以便开始自动回复或通知人类。
- AWS Security Hub CSPM提供了您的安全状态的全面视图 AWS。它还可以帮助您根据安全行业标准和最佳实践检查您的 AWS环境。

这些工具和功能旨在提高可见性，且可帮助您在问题对您的环境产生负面影响之前解决问题。这可以帮助您改善组织在云中的安全状况，并降低环境的风险概况。

Well-Architecte AWS d Framework 中的相关最佳实践

- SEC04-BP01 配置服务和应用程序日志
- SEC04-在标准化位置BP02 捕获日志、发现结果和指标

实现此主题

启用日志记录

- 使用 CloudWatch 代理将系统级日志发布到 Logs CloudWatch

- 为 GuardDuty 调查结果设置警报
- 在中创建组织跟踪 CloudTrail

实施日志记录安全最佳实践

- 实施 CloudTrail 安全最佳实践
- 用于 SCPs 防止用户禁用安全服务（AWS 博客文章）
- 使用加密日志中的 CloudWatch 日志数据 AWS Key Management Service

集中日志

- 接收来自多个账户的 CloudTrail 日志
- 向日志归档账户发送日志
- 将 CloudWatch 日志集中到账户中以进行审计和分析（AWS 博客文章）
- 集中管理 Amazon Inspector
- 在 AWS Config（博客文章）AWS 中创建组织范围的聚合器
- 集中管理 Security Hub CSPM
- 集中管理 GuardDuty
- 考虑使用 Amazon Security Lake

监控此主题

实施机制

- 建立审查日志调查发现的机制
- 建立审查 Security Hub CSPM 调查结果的机制
- 建立回应 GuardDuty 调查结果的机制

实施以下 AWS Config 规则

- `CLOUDTRAIL_SECURITY_TRAIL_ENABLED`
- `GUARDDUTY_ENABLED_CENTRALIZED`

- SECURITYHUB_ENABLED
- ACCOUNT_PART_OF_ORGANIZATIONS

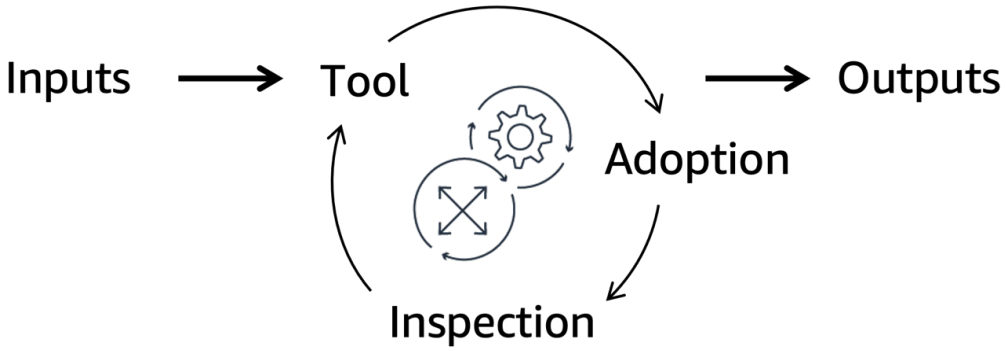
主题 8：实施手动流程机制

涵盖八大要点策略

应用程序控制，修补应用程序

在亚马逊，我们有句话：良好的意图行不通，机制行不通（AWS 博客文章）。这意味着您必须使用自动化、可重复、可扩展的流程和工具取代最大努力，以实现预期的结果。

如下图所示，机制是一个完整的过程，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。这是一个在运作过程中自我强化和改善的循环。它采用可控的输入并将其转化为持续的输出，以应对反复出现的业务挑战。有关更多信息，请参阅在 Well-Architect AWS ed 框架中构建机制。



Well-Architecte AWS d Framework 中的相关最佳实践

- OPS02-BP01 资源已确定所有者
- OPS02-BP02 流程和程序已确定所有者
- OPS02-BP03 运营活动已确定了对其绩效负责的所有者
- OPS02-存在管理责任和所有权的BP04 机制
- OPS03-BP01 提供高管赞助
- OPS03-鼓励BP03 升级

实现此主题

- 建立审查和解决合规差距的机制

- 建立更新安全策略的机制
- 删除不支持的应用程序，然后将其添加到 AWS Config 规则拒绝列表中
- 使用验证访问策略 AWS Identity and Access Management Access Analyzer
- 启用 Amazon Inspector，它会自动保存漏洞登记册 up-to-date
- 至少每年审查应用程序控制规则集
- 考虑实施自动化（例如 AWS Config 规则），以减轻手动流程的负担
- 考虑使用 AWS Systems Manager 清单来了解哪些实例正在运行软件策略要求的软件

监控此主题

- 对执行发起人进行监督，以跟踪实现目标的进展情况，包括合规、检查差距和评估机制。

关于达到基本八大成熟度的指示性案例研究 AWS

本章提供了政府机构达到 AWS上的八大要点成熟度的典型案例研究。

本章中的章节：

- 场景和架构概述
- 工作负载示例：无服务器数据湖
- 工作负载示例：容器化 Web 服务
- 工作负载示例：Amazon EC2 上的 COTS 软件

场景和架构概述

该政府机构在 AWS Cloud中有三项工作负载：

- 使用亚马逊简单存储服务 (Amazon S3) 进行存储以及提取、转换 AWS Lambda 和加载 (ETL) 操作的无服务器数据湖
- 一种容器化 Web 服务，在 Amazon Elastic Container Service（Amazon ECS）上运行并使用 Amazon Relational Database Service（Amazon RDS）中的数据库
- 在亚马逊 EC2 上运行的商用 off-the-shelf (COTS) 软件

云团队为组织提供集中式平台，为 AWS 环境运行核心服务。云团队为 AWS 环境提供核心服务。每个工作负载都由不同的应用程序团队拥有，也称为开发者团队或交付团队。

核心架构

云团队已经在 AWS Cloud中建立了以下功能：

- 身份联合链接 AWS IAM Identity Center 到他们的 E Microsoft ntra ID（以前是 Azure 活动目录）实例。联合会强制执行 MFA、用户账户自动到期以及 AWS Identity and Access Management 通过 (IAM) 角色使用短期证书。
- 使用集中式 AMI 管线，通过 EC2 Image Builder 修补操作系统和核心应用程序。
- Amazon Inspector 可以识别漏洞，所有安全发现都将发送到亚马逊 GuardDuty 进行集中管理。
- 使用既定机制来更新应用程序控制规则、响应网络安全事件，及审查合规差距。
- AWS CloudTrail 用于记录和监控。

- 安全事件（例如根用户登录）会触发提醒。
- SCPs 而且 VPC 终端节点策略会为您的 AWS 环境建立数据边界。
- SCPs 防止应用程序团队禁用安全和日志服务，例如 CloudTrail 和 AWS Config。
- AWS Config AWS 账户 为了安全起见，将整个 AWS 组织的调查结果汇总到一个单一的调查结果中。
- AWS Config ACSC Essential 8 一致性包已 AWS 账户 在您的组织中启用。

工作负载示例：无服务器数据湖

此工作负载是主题 1：使用托管服务的一个示例。

数据湖使用 Amazon S3 进行存储和 AWS Lambda ETL。这些资源是在 AWS Cloud Development Kit (AWS CDK) 应用程序中定义的。对系统的更改是通过部署的 AWS CodePipeline。此管线仅限应用程序团队使用。当应用程序团队对代码存储库提出拉取请求时，将使用双人规则。

对于此工作负载，应用程序团队采取以下措施来解决八大要点策略。

应用程序控制

- 应用程序团队在 A mazon Inspector 中启用 Lambda 保护和在 GuardDuty Lambda 扫描中启用 Lambda 扫描。
- 应用程序团队实施用于检查和管理 Amazon Inspector 调查发现的机制。

修补应用程序

- 应用程序团队在 Amazon Inspector 中启用 Lambda 扫描，并为已弃用或易受攻击的库配置提醒。
- 应用程序团队可以跟踪 AWS 资源 AWS Config 以进行资产发现。

限制管理权限

- 如核心架构部分所述，应用程序团队已通过部署管线上的批准规则限制了对生产部署的访问权限。
- 应用程序团队依赖核心架构部分所述的集中式身份联合验证和集中式日志记录解决方案。
- 应用程序团队创建 AWS CloudTrail 跟踪和 Amazon CloudWatch 筛选器。
- 应用程序团队为部署 AWS CloudFormation 和堆栈删除设置亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 警报 CodePipeline 。

修补操作系统

- 应用程序团队在 Amazon Inspector 中启用 Lambda 扫描，并为已弃用或易受攻击的库配置提醒。

多重身份验证

- 应用程序团队依赖核心架构部分所述的集中式身份联合验证解决方案。此解决方案可强制执行 MFA，记录身份验证，并在出现可疑的 MFA 事件时发出提醒或自动做出响应。

定期备份

- 应用程序团队将代码（例如 AWS CDK 应用程序和 Lambda 函数和配置）存储在代码存储库中。
- 应用程序团队启用版本控制和 Amazon S3 对象锁定，来帮助防止对象被删除或修改。
- 应用程序团队依赖内置的 Amazon S3 持久性，而不是将其整个数据集复制到另一个 AWS 区域。
- 应用程序团队在满足其数据主权要求的另一个 AWS 区域 工作负载中运行工作负载的副本。他们使用 Amazon DynamoDB 全局表和 Amazon S3 跨区域复制将数据从主区域自动复制到辅助区域。

工作负载示例：容器化 Web 服务

此工作负载是主题 2：通过安全管线管理不可变基础设施的一个示例。

Web 服务在 Amazon ECS 上运行，并使用 Amazon RDS 中的数据库。应用团队在 CloudFormation 模板中定义这些资源。容器使用 EC2 Image Builder 创建并存储在 Amazon ECR 中。应用程序团队通过 AWS CodePipeline将更改部署到系统。此管线仅限应用程序团队使用。当应用程序团队对代码存储库提出拉取请求时，将使用双人规则。

对于此工作负载，应用程序团队采取以下措施来解决八大要点策略。

应用程序控制

- 应用程序团队支持在 Amazon Inspector 中扫描 Amazon ECR 容器镜像。
- 应用程序团队在 EC2 Image Builder 管线中构建文件访问策略进程守护程序（fapolicyd）安全工具。有关更多信息，请参阅 ACSC 网站上的实现应用程序控制。
- 应用程序团队将 Amazon ECS 任务定义配置为将输出记录到 Amazon CloudWatch 日志。
- 应用程序团队实施用于检查和管理 Amazon Inspector 调查发现的机制。

修补应用程序

- 应用程序团队在 Amazon Inspector 中启用扫描 Amazon ECR 容器映像，并为已弃用或易受攻击的库配置提醒。
- 应用程序团队自动对 Amazon Inspector 调查发现做出响应。新发现通过Amazon EventBridge 触发器启动其部署渠道，并且 CodePipeline 是目标。
- 应用程序团队可以跟踪 AWS 资源 AWS Config 以进行资产发现。

限制管理权限

- 应用程序团队已通过部署管线上的批准规则限制对生产部署的访问权限。
- 应用程序团队依赖集中式云团队的身份联合验证来轮换凭证和集中式日志记录。
- 应用团队创建 CloudTrail 跟踪和 CloudWatch 过滤器。
- 应用程序团队为 CodePipeline 部署和 CloudFormation堆栈删除设置 Amazon SNS 警报。

修补操作系统

- 应用程序团队在 Amazon Inspector 中启用扫描 Amazon ECR 容器映像，并为操作系统补丁更新配置提醒。
- 应用程序团队自动对 Amazon Inspector 调查发现做出响应。新发现通过 EventBridge 触发器启动其部署管道，并且 CodePipeline 是目标。
- 应用程序团队订阅 Amazon RDS 事件通知，以便及时了解更新。他们与企业主一起做出基于风险的决定，决定是手动应用这些更新，还是让 Amazon RDS 自动应用这些更新。
- 应用程序团队将 Amazon RDS 实例配置为多可用区集群，以减少维护事件的影响。

多重身份验证

- 应用程序团队依赖核心架构部分所述的集中式身份联合验证解决方案。此解决方案可强制执行 MFA，记录身份验证，并在出现可疑的 MFA 事件时发出提醒或自动做出响应。

定期备份

- 应用程序团队配置 AWS Backup 为自动备份其 Amazon RDS 集群的数据。
- 应用团队将 CloudFormation 模板存储在代码存储库中。

- 应用程序团队开发了一个自动化管道，用于在另一个区域创建其工作负载的副本并运行自动测试（AWS 博客文章）。自动测试运行后，管线会销毁堆栈。此管线每月自动运行一次，并验证恢复过程的有效性。

工作负载示例：Amazon EC2 上的 COTS 软件

此工作负载是主题 3：通过自动化管理可变基础设施的一个示例。

在 Amazon EC2 上运行的工作负载是使用 AWS 管理控制台手动创建的。开发者通过登录 EC2 实例并更新软件来手动更新系统。

对于此工作负载，云和应用程序团队采取以下措施来解决八大要点策略。

应用程序控制

- 云团队配置其集中式 AMI 管道，以安装和配置 AWS Systems Manager 代理（SSM 代理）、CloudWatch 代理和。 SELinux他们跨组织中的所有账户共享生成的 AMI。
- 云团队使用 AWS Config 规则来确认所有正在运行的 EC2 实例均由 Systems Manager 管理，并且已安装 SSM 代理、 CloudWatch 代理并 SELinux 已安装。
- 云团队将 Amazon CloudWatch Logs 输出发送到在亚马逊 OpenSearch 服务上运行的集中式安全信息和事件管理 (SIEM) 解决方案。
- 应用程序团队实施机制来检查和管理来自 AWS Config、 GuardDuty和 Amazon Inspector 的调查结果。云团队实施自己的机制来捕获应用程序团队错过的任何调查发现。有关创建漏洞管理程序以处理调查发现的更多指引，请参阅在 AWS上构建可扩展的漏洞管理程序。

修补应用程序

- 应用程序团队根据 Amazon Inspector 调查发现修补实例。
- 云团队修补基本 AMI，当该 AMI 发生更改时，应用程序团队会收到提醒。
- 应用程序团队通过配置安全组规则来限制对其 EC2 实例的直接访问，仅允许工作负载所需的端口上的流量。
- 应用程序团队使用补丁管理器来修补实例，而不是登录单个实例。
- 要对 EC2 实例组运行任意命令，应用程序团队可以使用 Run Command。
- 在极少数情况下，当应用程序团队需要直接访问实例时，他们会使用会话管理器。此访问方法使用联合身份并记录任何会话活动以供审计。

限制管理权限

- 应用程序团队配置安全组规则，仅允许工作负载所需的端口上的流量。这限制了对 Amazon EC2 实例的直接访问，并要求用户通过会话管理器访问 EC2 实例。
- 应用程序团队依赖集中式云团队的身份联合验证来轮换凭证和集中式日志记录。
- 应用团队创建 CloudTrail 跟踪和 CloudWatch 过滤器。
- 应用程序团队为 CodePipeline 部署和 CloudFormation堆栈删除设置 Amazon SNS 警报。

修补操作系统

- 云团队修补基本 AMI，当该 AMI 发生更改时，应用程序团队会收到提醒。应用程序团队使用此 AMI 部署新实例，然后使用状态管理器（Systems Manager 的功能）来安装所需的软件。
- 应用程序团队使用补丁管理器来修补实例，而不是登录单个实例。
- 要对 EC2 实例组运行任意命令，应用程序团队可以使用 Run Command。
- 在极少数情况下，当应用程序团队需要直接访问时，他们会使用会话管理器。

多重身份验证

- 应用程序团队依赖核心架构部分所述的集中式身份联合验证解决方案。此解决方案可强制执行 MFA，记录身份验证，并在出现可疑的 MFA 事件时发出提醒或自动做出响应。

定期备份

- 应用程序团队为其 EC2 实例和亚马逊弹性区块存储 (Amazon EBS) 卷 AWS Backup 制定计划。
- 应用程序团队实施了一种机制，每月手动执行一次备份恢复。

资源

AWS 文档

- AWS 安全参考架构（AWS SRA）
- AWS 安全性文档
- AWS Well-Architected Framework 的安全性支柱

其他 AWS 资源

- AWS 云安全性
- AWS Cloud Adoption Framework（安全视角）

澳大利亚网络安全中心资源

- 八大要点说明
- 八大要点成熟度模型
- 八大要点评估流程指南

贡献者

本文档的贡献者包括：

- James Kingsmill，AWS 解决方案架构高级解决方案架构师
- Chris Harding，AWS 解决方案架构高级解决方案架构师
- Jess Modini，AWS 解决方案架构咨询解决方案架构师
- Justin Bowden，AWS 安全保障的安全保障负责人
- Rob Powell，AWS 解决方案架构高级解决方案架构师
- Tony Mihaljevic，AWS 专业服务团队高级云架构师
- Volker Rath，AWS 全球服务安全首席安全顾问

附录：八大要点控制矩阵

下表将基本八大策略与 Well-Architecte AWS d Framework 中的 AWS 实施指南和相关最佳实践联系起来。对于不适用于的 Essential Eight 控制措施 AWS Cloud，该表包含指向澳大利亚网络安全中心 (ACSC) 其他指南的链接。

控制矩阵：

- 应用程序控制
- 修补应用程序
- 配置 Microsoft Office 宏设置
- 用户应用程序固化
- 限制管理权限
- 修补操作系统
- 多重身份验证
- 定期备份

应用程序控制

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
在工作站和服务器上实施应用程序控制，以将可执行文件、软件库、脚本、安装程序、编译的 HTML、HTML 应用程序、控制面板小程序和驱动程序的执行限制在组织批准的集合内。	主题 2：通过安全管线管理不可变基础设施：实施 AMI 和容器构建管线	使用 EC2 Image Builder 并内置： • AWS Systems Manager 代理（SSM 代理） • 用于应用程序控制的安全工具，例如安全增强型 Linux (SELinux) (GitHub)、文件访问策略守护程序	SEC06-从经过强化的映像BP02 配置计算

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
		(fapolicyd) (GitHub) 或 OpenSCAP 亚马逊 CloudWatch 代理 AMIs 与整个组织共享 确保应用团队参考的是最新的 AMIs 使用您的 AMI 管线进行补丁管理	
已实施 Microsoft 的“推荐的阻止规则”。	请参阅实现应用程序控制（ACSC 网站）	不适用	不适用
已实施 Microsoft 的“推荐的驱动程序阻止规则”。			
应用程序控制规则集每年或更频繁地进行一次验证。	主题 8：实施手动流程机制：实施更新安全策略的机制	不可用	SEC01-定期BP08 评估和实施新的安全服务和功能

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
工作站和服务器上允许和阻止的执行会集中记录，防止未经授权的修改和删除，监控泄露迹象，并在检测到网络安全事件时采取行动。	主题 7：集中记录和监控：启用日志记录	使用 CloudWatch 代理将系统级日志发布到 Logs CloudWatch 为 GuardDuty 发现设置警报 在中创建组织跟踪 CloudTrail 使用版本控制和 S3 对象锁定来保护存储在 Amazon S3 中的数据	SEC04-BP01 配置服务和应用程序日志 SEC04-在标准化位置 BP02 捕获日志、发现结果和指标
	主题 7：集中记录和监控：实施日志记录安全最佳实践	实施 CloudTrail 安全最佳实践 用于 SCPs 防止用户禁用安全服务（AWS 博客文章） 使用加密日志中的 CloudWatch 日志数据 AWS Key Management Service	SEC04-BP01 配置服务和应用程序日志 SEC04-在标准化位置 BP02 捕获日志、发现结果和指标

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
	主题 7：集中记录和监控：集中日志	接收来自多个账户的 CloudTrail 日志 向日志归档账户发送日志 将 CloudWatch 日志集中到账户中以进行审计和分析（AWS 博客文章） 集中管理 Amazon Inspector 在 AWS Config（博客文章）AWS 中创建组织范围的聚合器 集中管理 Security Hub CSPM 集中管理 GuardDuty 考虑使用 Amazon Security Lake	SEC04-在标准化位置 BP02 捕获日志、发现结果和指标
	主题 8：实施手动流程机制：实施审查和解决合规差距的机制	考虑实施自动化（例如 AWS Config 规则），以减轻手动流程的负担	OPS02-BP02 流程和程序已确定所有者 OPS02-BP03 运营活动已确定了对其绩效负责的所有者 OPS02-存在管理责任和所有权的BP04 机制

修补应用程序

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
每两周至少使用一次自动化资产发现方法，以支持对资产的检测，从而进行后续的漏洞扫描活动。	主题 1：使用托管服务：扫描漏洞 主题 2：通过安全管线管理不可变基础设施：实施漏洞扫描 主题 3：通过自动化管理可变基础设施：实施漏洞扫描	在您组织的所有账户中启用 Amazon Inspector 使用 Amazon Inspector 为 Amazon ECR 存储库配置增强扫描 构建漏洞管理程序，对安全调查发现进行分类和修复	SEC06-BP01 执行漏洞管理 SEC06-BP05 自动计算保护
	主题 7：集中记录和监控：集中日志	接收来自多个账户的 CloudTrail 日志 向日志归档账户发送日志 将 CloudWatch 日志集中到账户中以进行审计和分析（AWS 博客文章） 集中管理 Amazon Inspector Create an organisation-wide aggregator in AWS Config（AWS 博客文章） 集中管理 Security Hub CSPM	SEC04-在标准化位置 BP02 捕获日志、发现结果和指标

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
		集中管理 GuardDuty 考虑使用 Security Lake	
带有漏洞数据库的 up-to-date漏洞扫描程序用于漏洞扫描活动。 每天至少使用一次漏洞扫描程序，以识别面向互联网的服务中安全漏洞缺少的补丁或更新。	主题 1：使用托管服务：扫描漏洞 主题 2：通过安全管线管理不可变基础设施：实施漏洞扫描 主题 3：通过自动化管理可变基础设施：实施漏洞扫描	在您组织的所有账户中启用 Amazon Inspector 使用 Amazon Inspector 为 Amazon ECR 存储库配置增强扫描 构建漏洞管理程序，对安全调查发现进行分类和修复	SEC06-BP01 执行漏洞管理 SEC06-BP05 自动计算保护
每周至少使用一次漏洞扫描程序，以识别办公生产力套件、Web 浏览器及其扩展、电子邮件客户端、PDF 软件和安全产品中安全漏洞缺少的补丁或更新。	请参阅技术示例：补丁应用程序（ACSC 网站）	不适用	不适用

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
每两周至少使用一次漏洞扫描程序，以识别其他应用程序中安全漏洞缺少的补丁或更新。	主题 1：使用托管服务：扫描漏洞 主题 2：通过安全管线管理不可变基础设施：实施漏洞扫描 主题 3：通过自动化管理可变基础设施：实施漏洞扫描	在您组织的所有账户中启用 Amazon Inspector 使用 Amazon Inspector 为 Amazon ECR 存储库配置增强扫描 构建漏洞管理程序，对安全调查发现进行分类和修复	SEC06-BP01 执行漏洞管理 SEC06-BP05 自动计算保护
针对面向互联网的服务中的安全漏洞，补丁、更新或供应商缓解措施将在发布后两周内应用；如果存在漏洞，则将在 48 小时内应用。	主题 1：使用托管服务：扫描漏洞 主题 2：通过安全管线管理不可变基础设施：实施漏洞扫描 主题 3：通过自动化管理可变基础设施：实施漏洞扫描	在您组织的所有账户中启用 Amazon Inspector 使用 Amazon Inspector 为 Amazon ECR 存储库配置增强扫描 构建漏洞管理程序，对安全调查发现进行分类和修复	SEC06-BP01 执行漏洞管理
	主题 3：通过自动化管理可变基础设施：自动修补	在 AWS 组织的所有账户中启用补丁管理器	SEC06-BP01 执行漏洞管理 SEC06-BP05 自动计算保护

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
针对办公生产力套件、Web 浏览器及其扩展、电子邮件客户端、PDF 软件和安全产品中的安全漏洞的补丁、更新或供应商缓解措施将在发布后的两周内应用；如果存在漏洞，则将在 48 小时内应用。	请参阅技术示例：补丁应用程序（ACSC 网站）	不适用	不适用
针对其他应用程序中安全漏洞的补丁、更新或供应商缓解措施将在发布后的一个月内应用。	主题 1：使用托管服务：扫描漏洞 主题 2：通过安全管线管理不可变基础设施：实施漏洞扫描 主题 3：通过自动化管理可变基础设施：实施漏洞扫描	在您组织的所有账户中启用 Amazon Inspector 使用 Amazon Inspector 为 Amazon ECR 存储库配置增强扫描 构建漏洞管理程序，对安全调查发现进行分类和修复	SEC06-BP01 执行漏洞管理
	主题 3：通过自动化管理可变基础设施：自动修补	在 AWS 组织的所有账户中启用补丁管理器	SEC06-BP01 执行漏洞管理 SEC06-BP05 自动计算保护
供应商不再支持的应用程序将删除。	主题 8：实施手动流程机制：实施审查和解决合规差距的机制	考虑使用 AWS Systems Manager 清单来了解哪些实例正在运行软件策略要求的软件	SEC06-从经过强化的映像BP02 配置计算

配置 Microsoft Office 宏设置

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
对于没有演示业务需求的用户，将禁用 Microsoft Office 宏。	请参阅技术示例：配置宏设置（ACSC 网站）	不适用	不适用
只有在沙盒环境、可信位置或由可信发布者进行数字签名的 Microsoft Office 宏才允许执行。			
只有负责验证 Microsoft Office 宏是否不含恶意代码的特权用户才能写入和修改可信位置中的内容。			
通过消息栏或后台视图无法启用由不可信发布者进行数字签名的 Microsoft Office 宏。			
Microsoft Office 的可信发布者列表每年或更频繁地进行验证。			
来自互联网的文件中的 Microsoft Office 宏已阻止。			
Microsoft Office 宏防病毒扫描已启用。			

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
Microsoft Office 宏被阻止进行 Win32 API 调用。			
用户无法更改 Microsoft Office 宏安全设置。			
允许和阻止的 Microsoft Office 宏执行会集中记录，防止未经授权的修改和删除，监控泄露迹象，并在检测到网络安全事件时采取行动。			

用户应用程序固化

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
Web 浏览器不会处理来自互联网的 Java。	请参阅技术示例：用户应用程序固化（ACSC 网站）	不适用	不适用
Web 浏览器不会处理来自互联网的 Web 广告。			
Internet Explorer 11 已禁用或删除。			
Microsoft Office 被阻止创建子进程。			

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
Microsoft Office 被阻止创建可执行内容。			
Microsoft Office 被阻止向其他进程注入代码。			
Microsoft Office 配置为防止激活 OLE 软件包。			
PDF 软件被阻止创建子进程。			
已实施针对 Web 浏览器、Microsoft Office 和 PDF 软件的 ACSC 或供应商固化指引。			
用户无法更改 Web 浏览器、Microsoft Office 和 PDF 软件安全设置。			
.NET Framework 3.5（包括 .NET 2.0 和 3.0）已禁用或删除。			
Windows PowerShell 2.0 已禁用或删除。			
PowerShell 配置为使用受限语言模式。			

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
允许的 PowerShell 脚本执行会集中记录，防止未经授权的修改和删除，监控泄露迹象，并在检测到网络安全事件时采取行动。			

限制管理权限

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
对系统和应用程序的特权访问请求会在首次请求时进行验证。	主题 4：管理身份：实施身份联合验证	要求人类用户通过与身份提供者联合身份验证，并使用临时凭证访问 AWS	SEC02-BP04 依赖集中式身份提供商 SEC03-BP01 定义访问要求
除非重新验证，否则对系统和应用程序的特权访问权限将在 12 个月后自动禁用。	主题 4：管理身份：实施身份联合验证	要求人类用户通过与身份提供者联合身份验证，并使用临时凭证访问 AWS	SEC02-BP04 依赖集中式身份提供商
	主题 4：管理身份：轮换凭证	要求工作负载使用 IAM 角色进行访问 AWS 自动删除未使用的 IAM 角色 对于需要长期凭证的用例，定期轮换访问密钥	SEC02-定期BP05 审核和轮换证书

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
		AWS 2023 年澳新银行峰会：您的云端临时证书之旅（YouTube视频）	
对系统和应用程序的特权访问权限将在 45 天非活动状态后自动禁用。	主题 4：管理身份：实施身份联合验证 主题 4：管理身份：轮换凭证	要求人类用户与身份提供商联合使用临时 AWS 证书进行访问 要求工作负载使用 IAM 角色进行访问 AWS 自动删除未使用的 IAM 角色 对于需要长期凭证的用例，定期轮换访问密钥 AWS 2023 年澳新银行峰会：您的云端临时证书之旅（YouTube视频）	SEC02-BP04 依赖集中式身份提供商 SEC02-定期BP05 审核和轮换证书

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
对系统和应用程序的特权访问权限仅限于用户和服务履行职责所需的权限。	主题 4：管理身份：应用最低权限许可	保护您的 root 用户凭证，不要将其用于日常任务 使用 IAM 访问分析器根据访问活动生成最低权限策略 使用 IAM Access Analyzer 验证公共和跨账户对资源的访问权限 使用 IAM 访问权限分析器验证您的 IAM 策略，以确保权限的安全性和功能性 跨多个账户建立权限防护栏 使用权限边界设置基于身份的策略可以授予的最大权限 使用 IAM 策略中的条件进一步限制访问权限 定期审查并删除未使用的用户、角色、权限、策略和证书 开始使用 AWS 托管策略，转向最低权限权限	SEC01-BP02 安全账户 root 用户和属性 SEC03-BP02 授予最低权限访问权限

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
		使用 IAM Identity Center 中的权限集功能	
禁止特权账户访问互联网、电子邮件和 Web 服务。	请参阅技术示例：限制管理权限（ACSC 网站）	考虑实施 SCP，以阻止还没有互联网访问权的任何 VPC 获取它	不适用
特权用户使用不同的特权和非特权操作环境。 特权操作环境不会在非特权操作环境中进行虚拟化。 非特权账户无法登录到特权操作环境。 特权账户（不包括本地管理员账户）无法登录到非特权操作环境。	主题 5：建立数据边界	建立数据边界。考虑在不同数据分类（例如 OFFICIAL: SENSITIVE 或 PROTECTED ）或不同风险级别（例如开发、测试或生产）的环境之间实施数据边界。	SEC06-BP03 减少手动管理和交互式访问
Just-in-time 管理用于管理系统和应用程序。	主题 4：管理身份：实施身份联合验证	要求人类用户与身份提供商联合使用临时 AWS 证书进行访问 对您的 AWS 环境实施临时提升访问权限（AWS 博客文章）	SEC02-BP04 依赖集中式身份提供商

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
管理活动通过跳转服务器进行。	主题 1：使用托管服务 主题 3：通过自动化管理可变基础设施：使用自动化而不是手动流程	使用会话管理器或运行命令而不是直接访问 SSH 或 RDP	SEC01-BP05 缩小安全管理范围 SEC06-BP03 减少手动管理和交互式访问
本地管理员账户和服务账户的凭证是唯一的、不可预测的和托管的。	请参阅技术示例：限制管理权限（ACSC 网站）	不适用	不适用
Windows Defender Credential Guard 和 Windows Defender Remote Credential Guard 已启用。			

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
特权访问的使用情况会集中记录并受到保护，防止未经授权的修改和删除，监控泄露迹象，并在检测到网络安全事件时采取行动。	主题 7：集中记录和监控：启用日志记录 主题 7：集中记录和监控：集中日志	使用 CloudWatch 代理将操作系统级别的日志发布到日志 CloudWatch CloudTrail 为您的组织启用 将 CloudWatch 日志集中到账户中以进行审计和分析（AWS 博客文章） 集中管理 Amazon Inspector 集中管理 Security Hub CSPM Create an organisation-wide aggregator in AWS Config（AWS 博客文章） 集中管理 GuardDuty 考虑使用 Amazon Security Lake 接收来自多个账户的 CloudTrail 日志 向日志归档账户发送日志	SEC04-BP01 配置服务和应用程序日志 SEC04-在标准化位置 BP02 捕获日志、发现结果和指标
对特权账户和组的更改会集中记录并受到保护，防止未经授权的修改和删除，监控泄露迹象，并在检测到网络安全事件时采取行动。			

修补操作系统

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
针对面向互联网的服务的操作系统中的安全漏洞，补丁、更新或供应商缓解措施将在发布后两周内应用；如果存在漏洞，则将在 48 小时内应用。	主题 2：通过安全管线管理不可变基础设施：实施 AMI 和容器构建管线	使用 EC2 Image Builder 并内置： • AWS Systems Manager 代理（SSM 代理） • 用于应用程序控制的安全工具，例如安全增强型 Linux (SELinux) (GitHub)、文件访问策略守护程序 (fapolicyd) (GitHub) 或 OpenSCAP • 亚马逊 CloudWatch 代理 AMIs 与整个组织共享 确保应用团队参考的是最新的 AMIs 使用您的 AMI 管线进行补丁管理	SEC01-BP05 缩小安全管理范围 SEC06-BP01 执行漏洞管理 SEC06-BP03 减少手动管理和交互式访问
	主题 1：使用托管服务：启用修补 主题 3：通过自动化管理可变基础设施：自动修补	在 AWS 组织的所有账户中启用补丁管理器	SEC06-BP01 执行漏洞管理 SEC06-BP05 自动计算保护

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
针对工作站、服务器和网络设备的操作系统中安全漏洞的补丁、更新或供应商缓解措施将在发布后两周内应用；如果存在漏洞，则将在 48 小时内应用。	主题 2：通过安全管线管理不可变基础设施：实施 AMI 和容器构建管线	使用 EC2 Image Builder 并内置： • AWS Systems Manager 代理（SSM 代理） • 用于应用程序控制的安全工具，例如安全增强型 Linux (SELinux) (GitHub)、文件访问策略守护程序 (fapolicyd) (GitHub) 或 OpenSCAP • 亚马逊 CloudWatch 代理 AMIs 与整个组织共享 确保应用团队参考的是最新的 AMIs 使用您的 AMI 管线进行补丁管理	SEC01-BP05 缩小安全管理范围 SEC06-BP01 执行漏洞管理 SEC06-从经过强化的映像BP02 配置计算
	主题 1：使用托管服务：启用修补 主题 3：通过自动化管理可变基础设施：自动修补	在 AWS 组织的所有账户中启用补丁管理器	SEC06-BP01 执行漏洞管理 SEC06-BP05 自动计算保护

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
每天至少使用一次漏洞扫描程序，以识别面向互联网的服务的操作系统中安全漏洞缺少的补丁或更新。 每周至少使用一次漏洞扫描程序，以识别工作站、服务器和网络设备的操作系统中安全漏洞的缺少的补丁或更新。	主题 1：使用托管服务：扫描漏洞 主题 2：通过安全管线管理不可变基础设施：实施漏洞扫描 主题 3：通过自动化管理可变基础设施：实施漏洞扫描	在您组织的所有账户中启用 Amazon Inspector 使用 Amazon Inspector 为 Amazon ECR 存储库配置增强扫描 构建漏洞管理程序，对安全调查发现进行分类和修复	SEC01-BP05 缩小安全管理范围 SEC06-BP01 执行漏洞管理 SEC06-从经过强化的映像BP02 配置计算

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
最新版本或上一版本的操作系统用于工作站、服务器和网络设备。 供应商不再支持的操作系统将被替换。	主题 2：通过安全管线管理不可变基础设施：实施漏洞扫描	使用 EC2 Image Builder 并内置： • AWS Systems Manager 代理（SSM 代理） • 用于应用程序控制的安全工具，例如安全增强型 Linux (SELinux) (GitHub)、文件访问策略守护程序 (fapolicyd) (GitHub) 或 OpenSCAP • 亚马逊 CloudWatch 代理 AMIs 与整个组织共享 确保应用团队参考的是最新的 AMIs 使用您的 AMI 管线进行补丁管理	SEC01-BP05 缩小安全管理范围 SEC06-BP01 执行漏洞管理 SEC06-从经过强化的映像BP02 配置计算

多重身份验证

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
如果组织的用户向其组织面向互联网的服	主题 4：管理身份：实施身份联合验证	要求人类用户与身份提供商联合使用临时 AWS 证书进行访问	SEC02-BP04 依赖集中式身份提供商

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
务进行身份验证，则使用多重身份验证。		Implement temporary elevated access to your AWS environments	
	主题 4：管理身份：强制执行 MFA	根用户需要 MFA 要求通过 MFA AWS IAM Identity Center 考虑要求对特定于服务的 API 操作进行 MFA	SEC02-BP01 使用强大的登录机制
如果组织的用户向处理、存储或传输其组织敏感数据的面向互联网的第三方服务进行身份验证，则他们将使用多重身份验证。	请参阅实现多重身份验证（ACSC 网站）	不适用	不适用
如果组织的用户向处理、存储或传输其组织非敏感数据的面向互联网的第三方服务进行身份验证，则他们将使用多重身份验证（可用时）。			

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
如果非组织用户向组织面向互联网的服务进行身份验证，则默认情况下会启用多重身份验证（但用户可以选择退出）。			
多重身份验证用于对系统的特权用户进行身份验证。	主题 4：管理身份：实施身份联合验证	要求人类用户与身份提供商联合使用临时 AWS 证书进行访问 Implement temporary elevated access to your AWS environments	SEC02-BP04 依赖集中式身份提供商
	主题 4：管理身份：强制执行 MFA	根用户需要 MFA 要求通过 IAM Identity Center 进行 MFA 考虑要求对特定于服务的 API 操作进行 MFA	SEC02-BP01 使用强大的登录机制
多重身份验证用于对访问重要数据存储库的用户进行身份验证。	主题 4：管理身份：强制执行 MFA	考虑要求对特定于服务的 API 操作进行 MFA	SEC02-BP01 使用强大的登录机制

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
多重身份验证可以抵抗验证者冒充攻击，它使用以下两种方式之一：一种是用户拥有的东西与用户知晓的信息相结合，或者是一种用户拥有的、但需要通过用户知晓的信息或用户固有的生物特征来解锁的东西	请参阅实现多重身份验证（ACSC 网站）	不适用	不适用

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
成功和失败的多重身份验证会集中记录，防止未经授权的修改和删除，监控泄露迹象，并在检测到网络安全事件时采取行动。	主题 7：集中记录和监控：启用日志记录 主题 7：集中记录和监控：集中日志	将 CloudWatch 日志集中到账户中以进行审计和分析（AWS 博客文章） 集中管理 Amazon Inspector 集中管理 Security Hub CSPM Create an organisation-wide aggregator in AWS Config（AWS 博客文章） 集中管理 GuardDuty 考虑使用 Security Lake 接收来自多个账户的 CloudTrail 日志 向日志归档账户发送日志	SEC04-BP01 配置服务和应用程序日志 SEC04-在标准化位置 BP02 捕获日志、发现结果和指标

定期备份

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
根据业务连续性要求，以协调和弹性的方式执行和保留重要数	主题 6：自动备份：自动执行数据备份和恢复	在上实施数据备份 AWS	REL09-BP01 识别并备份所有需要备份的

八大要点控制	实施指导	AWS 资源	AWS Well-Architected 指南
据、软件和配置设置的备份。		大规模自动备份数据（AWS 博客文章）	数据，或从源中复制数据 REL09-BP02 保护和加密备份 REL09-自动BP03 执行数据备份
作为灾难恢复练习的一部分，以协调的方式测试从备份中恢复系统、软件和重要数据。	主题 6：自动备份：自动执行数据备份和恢复 主题 6：自动备份：对所有 AWS Backup 结果实施治理	Automate data recovery validation with AWS Backup（AWS 博客文章） 使用 A AWS Backup udit Manager 来审计您的 AWS Backup 策略的合规性	REL09-BP04 定期恢复数据，以验证备份的完整性和流程
非特权账户和特权账户（不包括备份管理员）无法访问备份。 禁止非特权账户和特权账户（不包括备份 break glass 账户）修改或删除备份。	主题 6：自动备份: 在所有 AWS Backup 结果中实施治理	保护备份的十大安全最佳实践 AWS（AWS 博客文章） 使用 AWS Backup Vault Lock 来提高备份存储库的安全性 使用 A AWS Backup udit Manager 来审计您的 AWS Backup 策略的合规性	SEC08-BP04 强制执行访问控制

版权声明

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
最佳实践更新	我们更新了本指南，以反映 AWS Well-Architected Framework 安全性支柱中的最新最佳实践。	2024 年 11 月 6 日
初次发布	—	2023 年 10 月 20 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。