aws

美国国防部启用安全云计算架构 (SCCA) AWS

# AWS 规范性指导

# AWS 规范性指导: 美国国防部启用安全云计算架构 (SCCA) AWS

# Table of Contents

# 美国国防部启用安全云计算架构 (SCCA) AWS

Rob Higareda 和 Rughved Gadgil，Amazon Web Services ()AWS

2024 年 3 月（文档历史记录）

美国国防部 (DoD) 将云信息划分为影响级别 (iL)。影响级别与信息的敏感性以及失去该信息的机密性、完整性或可用性的风险有关。IL4 容纳国防部控制的非机密信息 (CUI)，IL5 容纳国防部 CUI 和国家安全系统 (NSS) 信息。本指南旨在帮助您构建支持 IL4 和 IL5 信息的着陆区。

要构建符合 IL4 或 IL5 标准的云基础架构，必须构建特定的组件。国防信息系统局 (DISA) 安全云计算架构 (SCCA) 是一系列云安全和管理服务。它为创建云边界提供了一种标准化的方法。SCCA 还包括云端托管的 IL4 和 IL5 信息的应用程序级安全组件。

本指南通过使用着陆区加速器 (LZA) 来帮助您满足 SCCA 要求。 AWS LZA 解决方案部署了一组基础功能，旨在与 AWS 最佳实践和多个全球合规框架保持一致。LZA 可以帮助您创建遵守国防部 SCCA 所需的许多组件。本指南还建议如何添加其他组件以实现 SCCA 合规性，并为您的云环境奠定安全的基础。 AWS尽管本指南并未包括所有潜在情况，但它提供了有关如何入门以及哪些 AWS 服务 可以帮助您满足 SCCA 要求的指导。

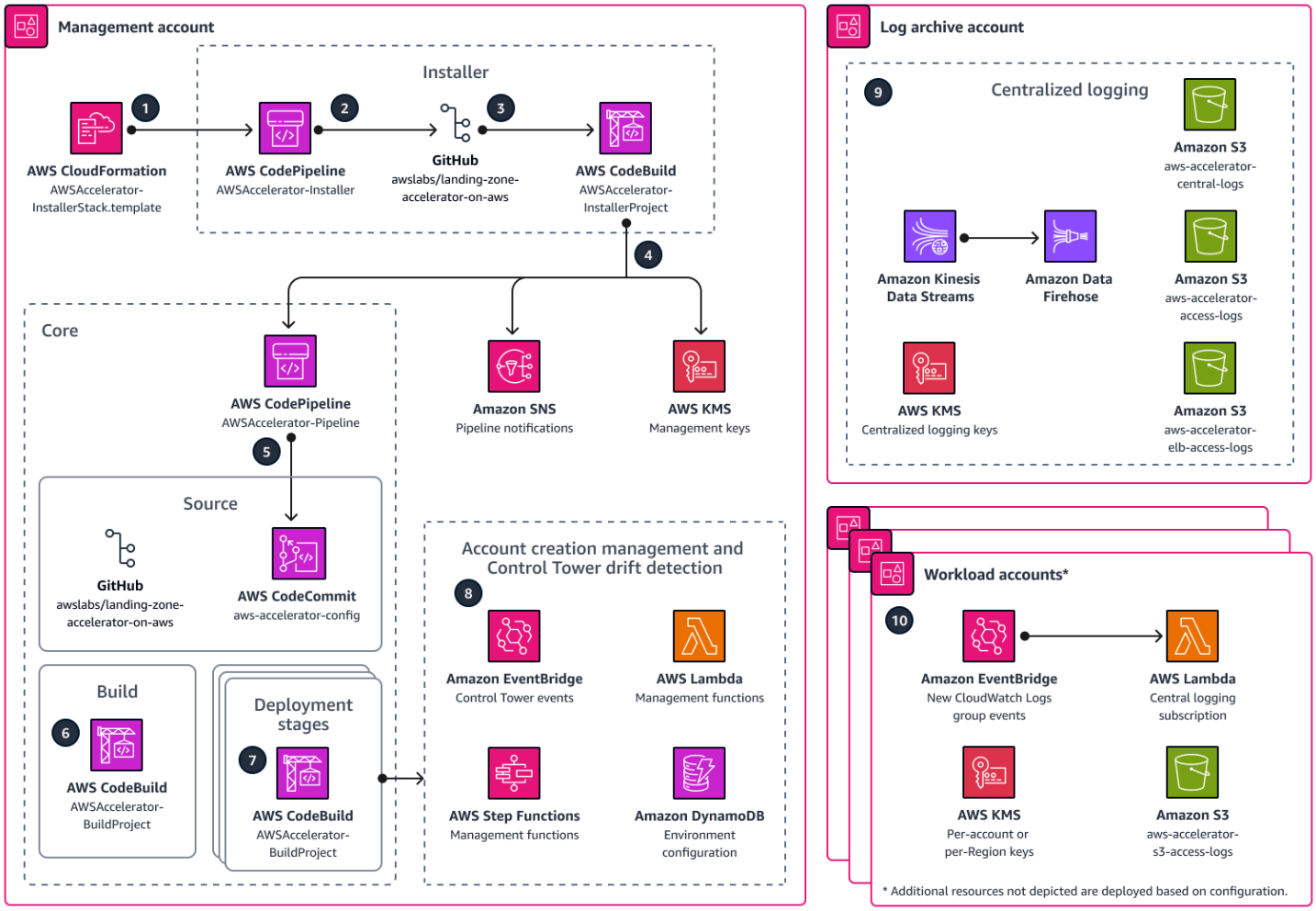
## 目标受众

本指南适用于需要遵守国防部安全云计算架构以帮助保护其中的IL4和IL5信息的个人。 AWS Cloud如果您尚未这样做，请在阅读本指南之前查看《迪砂云计算安全要求指南》。

# 着陆区加速器概述

为了在其中建立 AWS 符合国防信息系统局 (DISA) 安全云计算架构 (SCCA) 的着陆区，您必须具备某些要素来帮助您满足最低要求。 AWS 创建了着陆区加速器 (LZA)，以帮助您部署符合必要要求的着陆区。使用 LZA 解决方案，您可以使用一组配置文件来部署环境。这些配置文件可帮助您专注于环境的交付，而不是学习每个人 AWS 服务 以及如何部署环境。

下图显示了 LZA 部署中涉及的服务。这些数字表示工作流程，从修改配置文件到在工作负载帐户 AWS 服务 中进行配置。




该解决方案旨在与 AWS 最佳实践保持一致，并符合多个全球合规框架。当与诸如之类的服务配合使用时 AWS Control Tower，该解决方案可提供涵盖超过 35 AWS 服务 个功能的全面、低代码解决方案。具体而言，此解决方案可帮助您管理和治理多账户环境，该环境专为支持高度监管的工作负载和复杂的合规性要求而构建。LZA 通过安全性、合规性和运营能力帮助您建立平台就绪状态。本指南包括有关使用此解决方案来支持与美国 (US) 联邦和国防部 (DoD) 指导方针保持一致的具体说明。

AWS 将 LZA 解决方案作为开源项目提供，该项目是使用. AWS Cloud Development Kit (AWS CDK) 您可以将其直接安装到您的环境中，从而完全访问基础设施即代码 (IaC) 解决方案。

通过一组简化的配置文件，您可以：

- 配置其他功能、护栏和安全服务，例如AWS Config托管规则和。AWS Security Hub
- 通过诸如亚马逊虚拟私有云（Amazon VPC）和AWS Network Firewall之类的服务管理您的基础网络拓扑。AWS Transit Gateway
- 使用帐户工厂生成其他工作负载AWS Control Tower 帐户。

使用着陆区加速器无需支付额外费用或预付款。 AWS您只需为设置平台和操作护栏而开启的费用 AWS 服务 即可。该解决方案还可以支持非标准 AWS 分区，包括 AWS GovCloud (US)、AWS Secret 和 AWS 绝密区域。

> **Important**
>
> LZA 解决方案本身并不能使您合规。它提供了基础架构，您可以从中集成其他补充解决方案。LZA 实施指南中包含的信息并不详尽。您必须根据贵组织的特定安全功能、工具和配置来审查、评估、评估和批准该解决方案。确定哪些监管要求适用并确保您遵守所有要求是您和您的组织的全部责任。尽管此解决方案同时讨论了技术和管理要求，但该解决方案并不能帮助您遵守非技术管理要求。

# 计划您的 LZA 部署 AWS

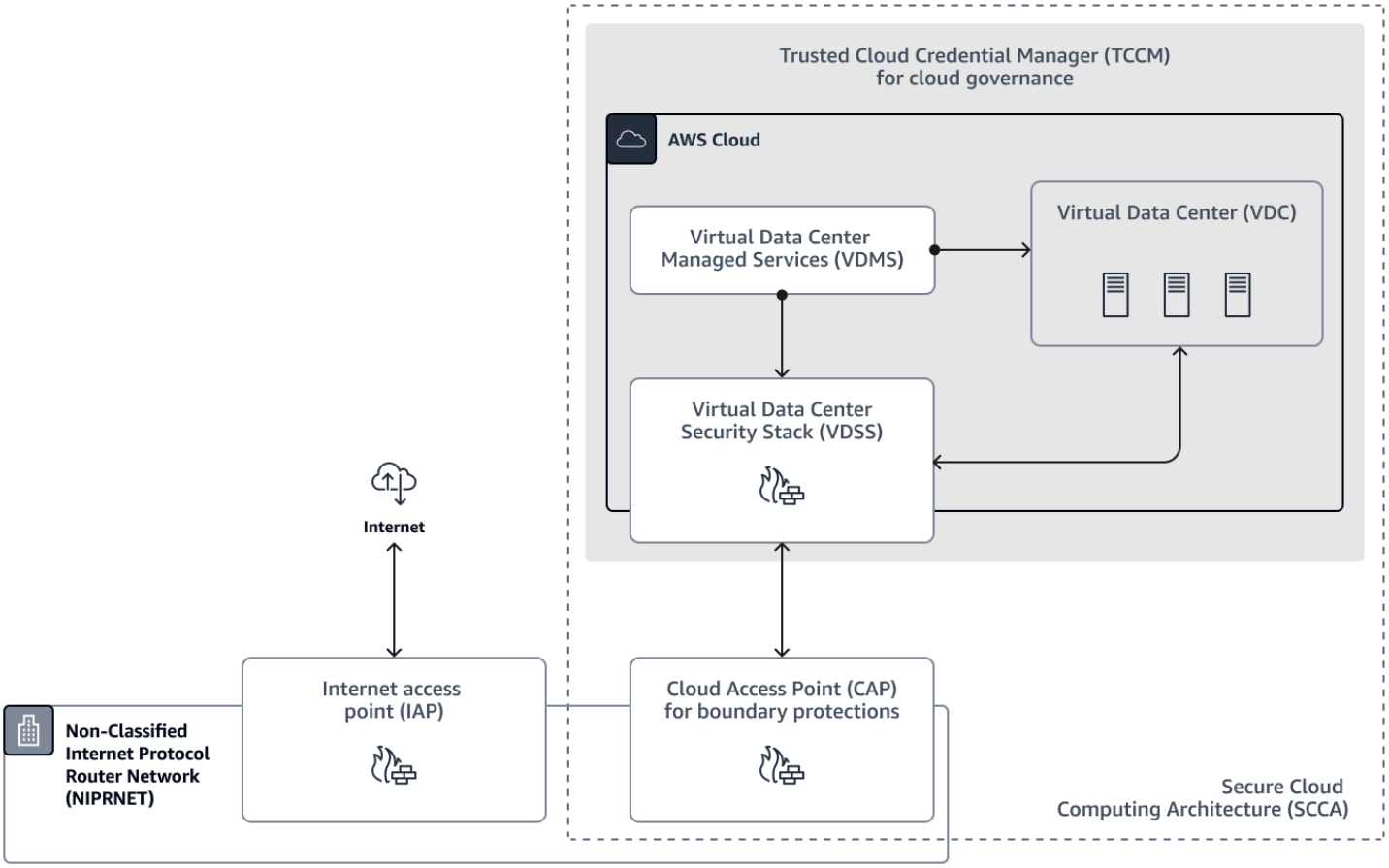
AWS 已为在上部署着陆区加速器 (LZA) 解决方案创建了详细的AWS实施指南。有关架构图和部署步骤概述，请参阅《 AWS 实施指南》上的《着陆区加速器》中的架构图。在部署解决方案之前，您的环境必须满足先决条件。使用本指南中 SCCA 组件和要求一章中的要求，您可以在 LZA 实施指南中描述的部署选项之间进行选择。

# SCCA 组件和要求

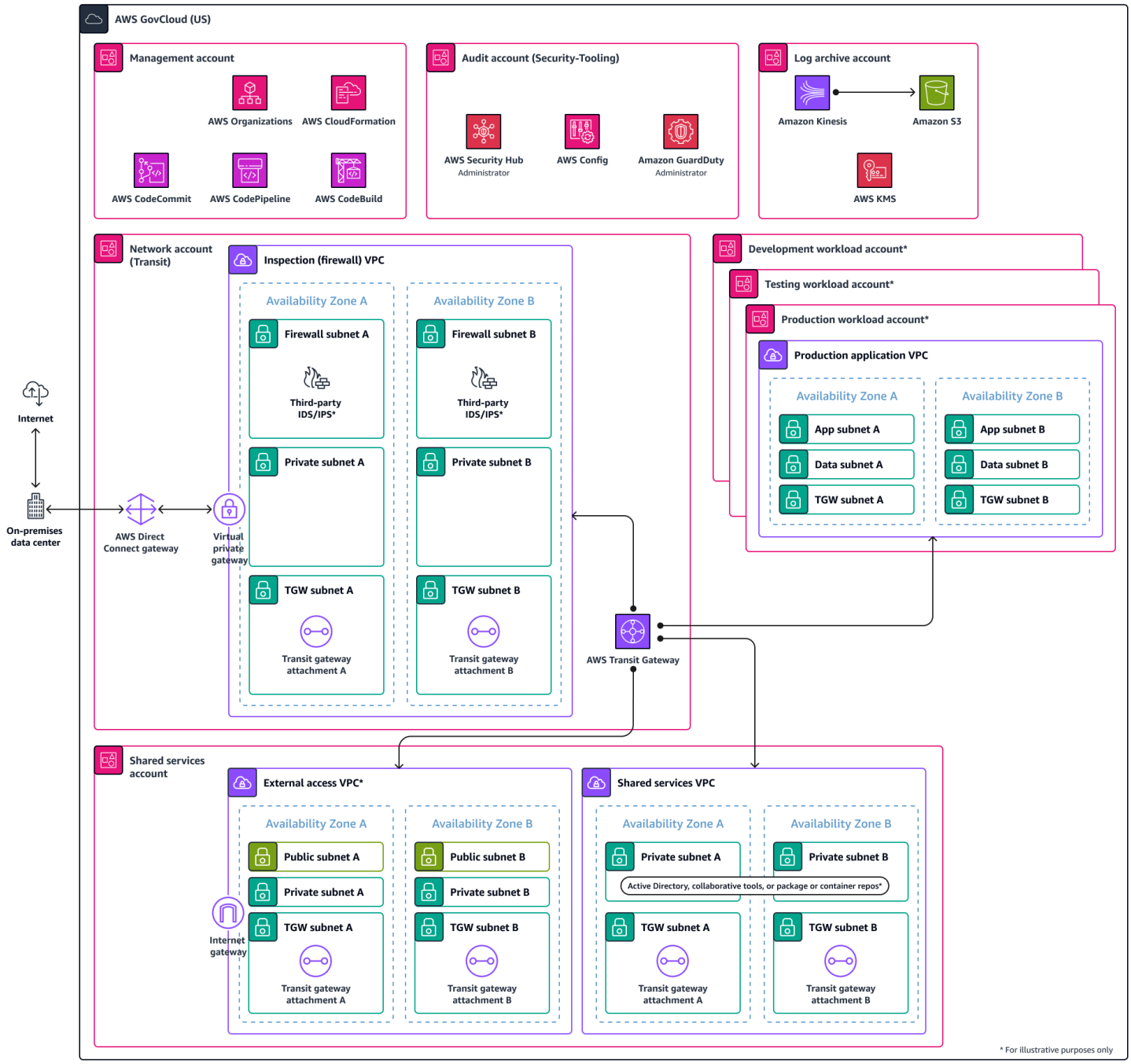
美国国防部 (DoD) 采用的国防信息系统局 (DISA) 安全云计算架构 (SCCA) 旨在成为一种可扩展、经济高效的方法，用于在通用安全架构下保护基于云的应用程序。它提供了一种在云环境中保护 IL4 和 IL5 数据的标准方法。正如 DISA SCCA 情况说明书中所述，SCCA 的总体组成部分包括：

- 云接入点 (CAP)- 提供对云的访问并保护国防部网络免受云端侵害。简化的保护措施侧重于保护网络边界。
- 虚拟数据中心安全堆栈 (VDSS) — 虚拟网络飞地安全，用于保护商业云产品中的应用程序和数据。
- Virt@@ ual Data Center Managed Services (VDMS) — 为商业环境中的特权用户提供访问权限的应用程序主机安全。
- 可信云凭证管理器 (TCCM) — 云凭证管理器，用于实施基于角色的访问控制 (RBAC) 和最低权限访问权限。

下图显示了 SCCA 的这些组件。



本节详细讨论了每个组件以及 LZA 中可以帮助您遵守国防信息系统局 (DISA) 标准的相应组件。下图显示了在中构建 SCCA 组件的 LZA 多账户结构。 AWS Cloud这种 LZA 多账户结构是帮助您实现完全符合 DISA SCCA 要求的架构的基础。有关帮助您完全满足合规性要求的架构示例，请参阅 SCCA on AWS GovCloud 架构图。



# 云接入点

边界云接入点 (BCAP) 或云接入点 (CAP) 由您的组织预先确定。因此，它不在本指南的范围内。CAP 允许从国防信息系统网络 (DISN) 访问商业云环境。CAP 还为云端的 DISN 提供边界保护。在 DISN 边界，它包括网络防御功能，例如防火墙、入侵检测系统 (IDS) 和入侵防御系统 (IPS)。组织通常使用国防部云原生接入点参考设计进行访问。 AWS

# 虚拟数据中心安全堆栈

虚拟数据中心安全堆栈 (VDSS) 的目的是保护托管在中的国防部任务所有者应用程序。 AWS VDSS 为安全服务提供了一个飞地。VDSS 在 SCCA 中执行大部分安全操作。此组件包含安全和网络服务，例如入站连接访问控制和外围保护服务，包括 Web 应用程序防火墙、DDOS 保护、负载均衡器和网络路由资源。VDSS 可以驻留在云基础架构中，也可以驻留在您的数据中心内部。 AWS 或者第三方供应商可以通过基础架构即服务 (IaaS) 提供 VDSS 功能， AWS 也可以通过软件即服务 (SaaS) 解决方案提供这些功能。有关 VDSS 的更多信息，请参阅美国国防部云计算安全要求指南。

下表包含 VDSS 的最低要求。它解释了 LZA 是否满足了每项要求，以及 AWS 服务 您可以使用哪些要求来满足这些要求。

| ID | VDSS 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
|---|---|---|---|---|
| 2.1.2.1 | VDSS 应将所有管理、用户和数据流量保持虚拟隔离。 | AWS Network Firewall<br>网络访问控制列表 (ACL)<br>弹性网络接口的安全组 | 隔离 VPC | 已覆盖 |
| 2.1.2.2 | VDSS 应允许使用加密对管理流量进行分段。 | Amazon VPC（加密实例之间的流量） | 亚马逊 VPC 的加密最佳实践 | 已覆盖 |
| 2.1.2.3 | VDSS 应提供反向代理功能来处理来自客户端系统的访问请求。 | 不适用 | 使用完全托管的反向代理提供内容 | 未覆盖 |

| ID | VDSS 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
| --- | --- | --- | --- | --- |
| 2.1.2.4 | VDSS 应提供基于一组预定义的规则（包括 HTTP）检查和过滤应用层对话的功能，以识别和阻止恶意内容。 | AWS WAF<br>Network 防火墙 | Web 请求正文检查<br>使用网络防火墙进行 TLS 流量检查 | 已部分覆盖 |
| 2.1.2.5 | VDSS 应提供一种能够区分和阻止未经授权的应用层流量的功能。 | AWS WAF | 如何使用 Amazon GuardDuty 和 AWS WAF 自动屏蔽可疑主机 | 未覆盖 |
| 2.1.2.6 | VDSS 应提供监控网络和系统活动的功能，以检测和报告进出任务所有者虚拟专用网络/飞地的流量的恶意活动。 | VPC 流日志<br>亚马逊 GuardDuty<br>AWS 硝基飞地 | AWS Nitro Enclaves 车间 | 已部分覆盖 |
| 2.1.2.7 | VDSS 应提供监控网络和系统活动的功能，以阻止或阻止检测到的恶意活动。 | Network 防火墙<br>AWS WAF | 不适用 | 已部分覆盖 |
| 2.1.2.8 | VDSS 应检查和过滤任务所有者虚拟专用网络/飞地之间穿越的流量。 | Network 防火墙 | 部署集中式流量过滤 | 已覆盖 |

| ID | VDSS 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
|---|---|---|---|---|
| 2.1.2.9 | VDSS 应对 SSL/TLS 通信流量进行中断和检查，支持对发往 CSE 中托管系统的流量进行单一和双重身份验证。 | Network 防火墙 | Network Firewall 的部署模型 | 已覆盖 |
| 2.1.2.10 | VDSS 应提供用于执行端口、协议和服务管理 (PPSM) 活动的接口，以便为 MCD 运营商提供控制。 | Network 防火墙 | Network Firewall 的部署模型 | 已覆盖 |
| 2.1.2.11 | VDSS 应提供监控功能，用于捕获日志文件和事件数据以进行网络安全分析。 | 亚马逊 CloudWatch<br><br>AWS CloudTrail | 记录安全事件响应 | 已覆盖 |
| 2.1.2.12 | VDSS 应向分配的存档系统提供或馈送安全信息和事件数据，以便执行边界和任务 CND 活动的特权用户共同收集、存储和访问事件日志。 | 亚马逊 CloudWatch 日志 | CloudWatch 日志中的安全性 | 已覆盖 |

| ID | VDSS 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
| --- | --- | --- | --- | --- |
| 2.1.2.13 | VDSS 应提供符合 FIPS-140-2 标准的加密密钥管理系统，用于存储国防部生成和分配的服务器私有加密密钥凭据，供 Web 应用程序防火墙 (WAF) 在执行 SSL/TLS 中断和检查加密通信会话时访问和使用。 | AWS Secrets Manager<br><br>AWS Key Management Service(AWS KMS) | 使用 AWS WAF 和 Secrets Manager 增强亚马逊 CloudFront 原产地安全<br><br>AWS KMS 使用 FIPS 140-2 进行密钥管理 | 未覆盖 |
| 2.1.2.14 | VDSS 应提供检测和识别应用程序会话劫持的能力。 | 不适用 | 不适用 | 未覆盖 |
| 2.1.2.15 | VDSS 应提供国防部 DMZ 扩展，以支持面向互联网的应用程序 (IFA)。 | 不适用 | 不适用 | 未覆盖 |
| 2.1.2.16 | VDSS 应提供完整的数据包捕获 (FPC) 或等同于云服务的 FPC 功能，用于记录和解释穿越通信。 | Network 防火墙<br><br>VPC 流日志 | 不适用 | 已覆盖 |

| ID | VDSS 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
| --- | --- | --- | --- | --- |
| 2.1.2.17 | VDSS 应为所有穿越通信提供网络数据包流指标和统计数据。 | CloudWatch | 使用监控接口 VPC 终端节点的网络吞吐量 CloudWatch | 已覆盖 |
| 2.1.2.18 | VDSS 应规定对进出每个任务所有者虚拟专用网络的流量进行检查。 | Network 防火墙 | 部署集中式流量过滤 | 已覆盖 |

CAP 的某些组成部分由您定义，但本指南未涵盖这些组件，因为每个机构都有自己的 CAP 连接 AWS。您可以用 LZA 补充 VDSS 的组件，以帮助检查进入的流量。 AWS LZA 中使用的服务提供边界和内部流量扫描，以帮助保护您的环境。为了继续构建 VDSS，LZA 中未包含一些其他基础架构组件。

通过使用虚拟私有云 (VPC)，您可以在每个虚拟私有云 (VPC) 中建立边界 AWS 账户 ，以帮助遵守 SCCA 标准。这不是作为 LZA 的一部分进行配置的，因为 VPC、IP 寻址和路由是您必须根据需要为基础架构设置的组件。您可以在 A mazon Rou te 53 中实现诸如域名系统安全扩展 (DNSSEC) 之类的组件。您 AWS WAF 也可以添加第三方商用 WAF 来帮助您达到必要的标准。

此外，为了支持 DISA SCCA 中的 2.1.2.7 要求，您可以使用和 Network Fi GuardDutyrew all 来帮助保护和监控环境中是否存在恶意流量。

## 虚拟数据中心 Managed Services

虚拟数据中心管理服务 (VDMS) 的目的是提供主机安全和共享数据中心服务。VDMS 的功能可以在你的 SCCA 中心运行，也可以由任务所有者自己部署其中的一部分。 AWS 账户可以在您的 AWS 环境中提供此组件。有关 VDMS 的更多信息，请参阅美国国防部云计算安全要求指南。

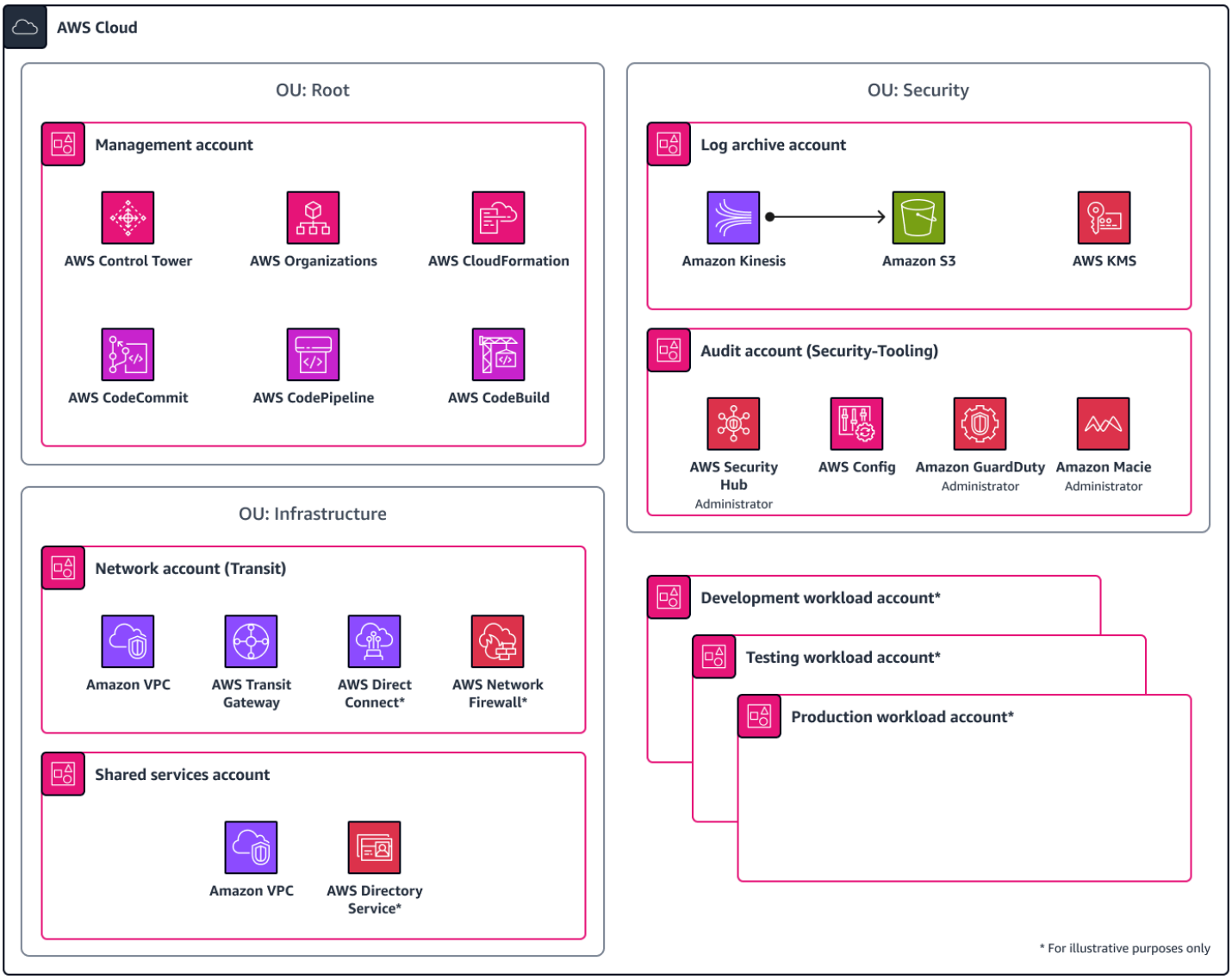
下表包含 VDMS 的最低要求。它解释了 LZA 是否满足了每项要求，以及 AWS 服务 您可以使用哪些要求来满足这些要求。

| ID | VDMS 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
| --- | --- | --- | --- | --- |
| 2.1.3.1 | VDMS应提供有保障的合规评估解决方案（ACAS）或经批准的同等解决方案，以对CSE内的所有飞地进行持续监测。 | AWS Config<br><br>AWS Security Hub<br><br>AWS Audit Manager<br><br>Amazon Inspector | 使用亚马逊 Inspector 进行漏洞扫描 | 已部分覆盖 |
| 2.1.3.2 | VDMS 应提供基于主机的安全系统 (HBSS) 或经批准的等效系统，以管理 CSE 内所有飞地的端点安全。 | 不适用 | 不适用 | 未覆盖 |
| 2.1.3.3 | VDMS 应提供身份服务，包括在线证书状态协议（oCloud Workload Security）响应器，用于远程系统国防部通用访问卡 (CAC) 对国防部特权用户向 CSE 中实例化的系统进行双因素身份验证。 | 多因素身份验证 (MFA) 可通过以下方式获得：<br><br>AWS Identity and Access Management (IAM)<br><br>AWS IAM Identity Center<br><br>AWS Directory Service for Microsoft Active Directory | 为亚马逊配置 CAC 卡 WorkSpaces | 已部分覆盖 |

| ID | VDMS 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
|---|---|---|---|---|
| | | AWS Private Certificate Authority | | |
| 2.1.3.4 | VDMS 应提供配置和更新管理系统，为 CSE 内所有飞地的系统和应用程序提供服务。 | AWS Systems Manager Patch Manager<br>AWS Config | 使用 AWS Systems Manager（YouTube 视频）实现补丁管理自动化 | 已部分覆盖 |
| 2.1.3.5 | VDMS 应为 CSE 内的所有安全区提供逻辑域服务，包括目录访问、目录联合、动态主机配置协议 (DHCP) 和域名系统 (DNS)。 | AWS Managed Microsoft AD<br>Amazon Virtual Private Cloud (Amazon VPC)<br>Amazon Route 53 | 为您的 VPC 配置 DNS 属性 | 已部分覆盖 |
| 2.1.3.6 | VDMS 应提供一个网络，用于管理 CSE 内的系统和应用程序，该网络在逻辑上与用户和数据网络分开。 | Amazon VPC<br>Amazon VPC 子网 | 不适用 | 已覆盖 |

| ID | VDMS 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
| --- | --- | --- | --- | --- |
| 2.1.3.7 | VDMS 应提供系统、安全、应用程序和用户活动事件记录和存档系统，供执行 BCP 和 MCP 活动的特权用户共同收集、存储和访问事件日志。 | AWS Security Hub<br>AWS CloudTrail<br>亚马逊 CloudWatch 日志<br>Amazon Simple Storage Service (Amazon S3) | 使用集中式日志记录 OpenSearch | 已覆盖 |
| 2.1.3.8 | VDMS 应规定将国防部特权用户身份验证和授权属性与 CSP 的身份和访问管理系统交换，以实现云系统的配置、部署和配置。 | AWS Managed Microsoft AD | 增强您的 AWS Managed Microsoft AD 安全配置 | 未覆盖 |
| 2.1.3.9 | VDMS 应具备必要的技术能力，以执行 TCCM 角色的使命和目标。 | AWS Managed Microsoft AD<br>IAM<br>IAM Identity Center | 不适用 | 已部分覆盖 |

如下图所示，LZA 奠定了满足 VDMS 基本要求的基础组件。部署 LZA 后，还需要配置一些其他组件，以帮助您满足 VDMS 标准。在上表中，请务必查看其他资源列中的链接。这些链接可以帮助您配置这些附加项目，也可以提供进一步的安全增强。




## 补充服务集成

上表中的其他资源列列出了可帮助您扩展 LZA 以满足 VDMS 要求的资源。 AWS 此外，还提供了一些研讨会材料来帮助您配置安全的云架构。无需修改，LZA 即可满足 IL4/IL5 要求，但您可以部署其他服务来增强环境的安全性。 AWS

例如，Amazon Inspector 是一项漏洞管理服务，它可以持续扫描您的 AWS 工作负载中是否存在软件漏洞和意外网络泄露。您可以使用它来识别和调查主机操作系统（例如 Windows 和 Linux）中的漏洞。尽管 Amazon Inspector 可能没有完全纳入基于主机的安全系统 (HBSS) 的所有必要要求，但它至少提供了对实例的基本漏洞评估。

## 操作系统修补

操作系统补丁是运营安全环境的核心组件。 AWS 提供并推荐使用 Patch Manager（一项功能）来维护一致的 AWS Systems Manager补丁基准并自动部署补丁。Patch Manager 通过与安全相关的更新和其他类型的更新自动修补托管节点。

您可以使用 Patch Manager 来应用操作系统和应用程序的补丁。（在 Windows 服务器上，应用程序支持仅限于微软发布的应用程序的更新。）有关更多信息，请参阅 AWS 云运营和迁移博客上的 “使用补丁管理器编排多步骤、自定义的 AWS Systems Manager 补丁流程”。

有关使用 Patch Manager 的 step-by-step 说明，请参阅AWS 管理和治理工具研讨会。

有关保护微软 Windows 工作负载的更多信息 AWS，请参阅AWS 研讨会上的保护 Windows 工作负载。

## 可信云凭证管理器

可信云凭证管理器 (TCCM) 是 SCCA 的组成部分。它负责凭证管理。在建立 TCCM 时，允许最低权限访问 SCCA 非常重要。这可以通过使用 AWS 身份和访问管理服务来实现。TCCM 的另一个组成部分是与虚拟数据中心托管服务 (VDMS) 的连接。您可以根据需要使用此连接来访问 AWS Management Console 以管理 TCCM。

TCCM 是管理访问的技术和标准的组合。 AWS TCCM 被认为对大多数实现至关重要，因为它可以控制访问权限。TCCM 功能并不是为了向商业云服务提供商 (CSP) 提出独特的身份管理要求。TCCM 也不禁止使用国防部 CSP 联盟或第三方身份代理解决方案来提供预期的身份控制。

TCCM 策略组件基于这样的普遍理解，即 CSP 提供允许控制对云系统的访问的身份和访问管理系统。此类系统可以包括 CSP 的访问控制台、API 和命令行接口 (CLI) 服务组件。在基本级别，TCCM 必须锁定可用于创建未经授权的网络和其他资源的凭证。TCCM 由负责监督信息技术系统的授权官员 (AO) 任命。TCCM 策略规定了对最低权限访问模式的需求。这些政策负责在商用云中提供和控制特权用户凭证。这是为了与国防部云计算安全要求指南保持一致，该指南涉及管理门户账户凭证的政策、计划和程序的实施。在连接到国防信息系统网络 (DISN) 之前，DISA 将验证云凭证管理计划 (CCMP) 的存在，这是《连接流程指南》中定义的连接批准流程的一部分。

下表包含 TCCM 的最低要求。它解释了 LZA 是否满足了每项要求，以及 AWS 服务 您可以使用哪些要求来满足这些要求。

| ID | TCCM 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
|---|---|---|---|---|
| 2.1.4.1 | TCCM 应制定和维护云凭证管理计划 (CCMP)，以解决适用于任务所有者客户门户网站账户凭证管理的政策、计划和程序的实施问题。 | 不适用 | 不适用 | 未覆盖 |
| 2.1.4.2 | TCCM 应收集、审计和存档所有客户门户活动日志和警报。 | AWS CloudTrail<br>亚马逊 CloudWatch 日志 | 不适用 | 已覆盖 |
| 2.1.4.3 | TCCM 应确保与参与 MCP 和 BCP 活动的国防部特权用户共享、转发给或检索活动日志警报。 | AWS CloudTrail<br>CloudWatch 日志<br>Amazon Simple Notification Service (Amazon SNS)<br>CloudWatch 日志见解 | 不适用 | 已覆盖 |
| 2.1.4.4 | 根据信息共享的需要，TCCM 应创建日志存储库访问帐户，以便同时执行 MCP 和 BCP 活动的特 | AWS CloudTrail<br>CloudWatch 日志<br>Amazon SNS | 不适用 | 已覆盖 |

| ID | TCCM 安全要求 | AWS 技术 | 其他 资源 | 由 LZA 承保 |
|---|---|---|---|---|
| | 权用户访问活动日志数据。 | CloudWatch 日志见解 | | |
| 2.1.4.5 | 在任务应用程序连接到DISN之前，TCCM应恢复并安全地控制客户门户网站的账户凭证。 | AWS IAM Identity Center | 不适用 | 已覆盖 |
| 2.1.4.6 | TCCM 应根据需要为任务所有者应用程序和系统管理员（即国防部特权用户）创建、颁发和撤销基于角色的访问权限最低的客户门户凭证。 | AWS Identity and Access Management (IAM)<br><br>AWS Directory Service for Microsoft Active Directory | 不适用 | 已覆盖 |

为了使 TCCM 能够满足要求，LZA 通过 IAM 服务对资源进行编程控制。此外，您还可以将 IAM 与结合使用 AWS Managed Microsoft AD 以实现对另一个目录的单点登录。这会通过 Active Directory 信任将您的 AWS 环境与本地基础设施联系起来。 在 LZA 中，实施是使用 IAM 角色部署的，用于临时的、基于会话的访问权限 IAM 角色是短期证书，可帮助您的组织满足必要的 TCCM 要求。

尽管 LZA 实施了最低权限访问权限和编程短期 AWS 资源访问权限，但请查看 IAM 最佳实践，确保您遵循推荐的安全指南。

有关实施的更多信息 AWS Managed Microsoft AD，请参阅 AWS Immersion Day 活动目录研讨会的AWS Managed Microsoft AD部分。

分AWS 担责任模式适用于TCCM和LZA。LZA 建立了访问控制的基本方面，但每个组织都负责配置其安全控制。

# 结论

对于美国国防部 (DoD)，本指南解释了国防信息系统局 (DISA) 部署安全云计算架构 (SCCA) 的要求。通过使用着陆区加速器 (LZA) AWS，您可以实施 AWS 产品并消除无差别的繁重工作。这可以帮助您专注于构建符合 IL4 或 IL5 标准的云基础架构的使命。

# 资源

## AWS 文档

- AWS 按合规计划划分的范围内的服务（AWS 合规性）
- 国防部云计算安全要求指南（AWS 合规性）
- 着陆区加速器已开启 AWS（AWS 解决方案库）
- AWS 《实施指南》中的着陆区域加速器
- AWS GovCloud 架构图上的 SCCA

## 其他资源

- 云计算安全要求指南（DISA 网站）
- 国防部 (DoD) 云原生接入点 (CNAP) 参考设计（国防部网站）
- 国防部安全云计算架构情况说明书（DISA 网站）

# 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 | — | 2024 年 3 月 12 日 |

# AWS Prescriptive

以下是 Prescript AWS ive Guidance 提供的策略、指南和模式中常用的术语。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 Postgre SQL 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 Amazon Relational Database Service（AmazonRDS）for Oracle 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：将本地 Oracle 数据库迁移到中的EC2实例上的 Oracle AWS Cloud。
- 重新定位（虚拟机监控器级直接迁移）：将基础设施迁移到云中，无需购买新硬件、重写应用程序或修改现有操作。您可以将服务器从本地平台迁移到同一平台的云服务。示例：迁移 Microsoft Hyper-V 申请到 AWS。
- 保留（重访）- 将应用程序保留在源环境中。其中可能包括需要进行重大重构的应用程序，并且您希望将工作推迟到以后，以及您希望保留的遗留应用程序，因为迁移它们没有商业上的理由。
- 停用 - 停用或删除源环境中不再需要的应用程序。

## A

ABAC

请参阅基于属性的访问控制。

抽象服务

参见托管服务。

ACID

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，但需要更多的工作量。

主动-被动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步，但在将数据复制到目标数据库时，只有源数据库处理来自连接应用程序的事务。目标数据库在迁移期间不接受任何事务。

聚合函数

对一组行进行操作并计算该组的单个返回值的SQL函数。聚合函数的示例包括SUM和MAX。

AI

参见人工智能。

AIOps

参见人工智能运营。

匿名化

永久删除数据集中个人信息的过程。匿名化可以帮助保护个人隐私。匿名化数据不再被视为个人数据。

反模式

一种用于解决反复出现的问题的常用解决方案，而在这类问题中，此解决方案适得其反、无效或不如替代方案有效。

应用程序控制

一种安全方法，仅允许使用经批准的应用程序，以帮助保护系统免受恶意软件的侵害。

应用程序组合

有关组织使用的每个应用程序的详细信息的集合，包括构建和维护该应用程序的成本及其业务价值。这些信息是产品组合发现和分析过程的关键，有助于识别需要进行迁移、现代化和优化的应用程序并确定其优先级。

人工智能（AI）

计算机科学领域致力于使用计算技术执行通常与人类相关的认知功能，例如学习、解决问题和识别模式。有关更多信息，请参阅什么是人工智能？

人工智能运营（AIOps）

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

基于属性的访问控制（）ABAC

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

权威数据源

存储主要数据版本的位置，被认为是最可靠的信息源。您可以将数据从权威数据源复制到其他位置，以便处理或修改数据，例如对数据进行匿名化、编辑或假名化。

可用区

一个中的不同位置 AWS 区域 ，用于与其他可用区的故障隔离，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)

的指导原则和最佳实践框架 AWS ，旨在帮助组织制定高效且有效的计划来成功迁移到云。 AWS CAF将指导原则分为六个重点领域（角度）：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，为人员发展、培训和沟通 AWS CAF提供了指导，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、推荐迁移策略并提供工作量估算的工具。 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

Bad 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呼叫和类似的操作。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。当您确信时，可以部署新版本并全部替换当前版本。

CCoE

参见云卓越中心。

CDC

请参阅变更数据捕获。

更改数据捕获（CDC）

跟踪数据来源（如数据库表）的更改并记录有关更改的元数据的过程。您可以CDC用于各种目的，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

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 接收数据之前，在本地对数据进行加密。

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

组织迁移到中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 企业战略博客上发表的博客文章云优先之旅和采用阶段中对这些阶段进行了定义。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。您通常使用来CMDB自产品组合发现和分析阶段的数据。

合规性包

一系列 AWS Config 规则和修复操作，您可以将其组合起来以自定义合规性和安全性检查。您可以使用YAML模板，将合规性包作为单个实体部署到区域中，或者跨组织部署。 AWS 账户 有关更多信息，请参阅 AWS Config 文档中的合规性包。

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。在中践行数据最少化 AWS Cloud 可以降低隐私风险、成本和您的分析碳足迹。

数据边界

AWS 环境中的一组预防性防护机制，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。当您在上采用此策略时 AWS，您可以在 AWS Organizations 结构的不同层添加多种控制措施，来保护资源。例如，一种 defense-in-depth 方法可能将多因素身份验证、网络分段和加密结合起来。

委托管理员

在中 AWS Organizations，兼容服务可以注册 AWS 成员账户来管理组织的账户，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，请参阅上工作负载的灾难恢复 AWS：Well-Architected Framework 中的云中 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，请参阅将原有的 Microsoft 现代化。ASP NET(ASMX) 通过使用容器和 Amazon API Gateway 逐步提供网络服务。

DR

参见灾难恢复。

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

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端点来私密地连接到您的VPC端点服务。有关更多信息，请参阅 Amazon Vir tual Private Cloud（AmazonVPC）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（例如会计和项目管理）的系统。MES

信封加密

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

environment

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

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

epic

在敏捷方法学中，有助于组织工作和确定优先级的功能类别。epics 提供了对需求和实施任务的总体描述。例如， AWS CAF安全史诗包括身份和访问管理、侦测性控制、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。

快速失败

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，请参阅使用:AWS实现机器学习模型的可解释性。

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

参见精细访问控制。

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，通过使用连续数据复制，在极短的时间内迁移数据，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。

# G

地理封锁

请参阅地理限制。

地理限制（地理阻止）

Amazon 中的一个选项 CloudFront，用于阻止特定国家/地区的用户访问内容分发。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发。

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，而基于主干的工作流程是现代的、首选的方法。

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

# H

HA

参见高可用性。

异构数据库迁移

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

高可用性 (HA)

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

历史数据库现代化

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

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 fo RDS r SQL Server）。同构迁移通常是更换主机或更换平台工作的一部分。您可以使用本机数据库实用程序来迁移架构。

热数据

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

修补程序

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

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主体的策略，用于定义它们在 AWS Cloud 环境中的权限。

空闲应用程序

90 天内平均CPU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-Arch AWS itected Framework 中的使用不可变基础设施部署的最佳实践。

入站（入口）VPC

在 AWS 多账户架构中，VPC一种用于接受、检查和路由来自应用程序外部的网络连接。AWS 安全参考架构建议使用入站、出站和检查VPCs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，请参阅构建工业物联网（IIoT）数字化转型策略。

检查 VPC

在 AWS 多账户架构中，VPC一种用于管理VPCs（相同或不同的 AWS 区域）互联网和本地网络之间的网络流量检查的集中式。AWS 安全参考架构建议使用入站、出站和检查VPCs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，请参阅使用实现机器学习模型的可AWS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为... 提供了基础ITSM。

IT 服务管理 (ITSM)

为组织设计、实施、管理和支持 IT 服务的相关活动。有关将云运营与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 是一个架构完善、可扩展且 AWS 安全的多账户环境。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，请参阅文档中的应用最低权限许可。IAM

直接迁移

见 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参见字节顺序。

下层环境

参见环境。

# M

机器学习（ML）

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

主分支

参见分支。

恶意软件

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

托管式服务

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) 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 Well-Architecte AWS d Framework 中的构建机制。

成员账户

AWS 账户 除管理账户外，属于中的组织的所有 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，通过明确定义进行通信APIs，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通过明确定义的接口进行通信。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

Migrative Accriptive（MAP）

一项提供咨询支持、培训和服务的 AWS 计划，旨在帮助组织为迁移到云奠定坚实的运营基础，并抵消迁移的初始成本。MAP包括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、开发人员和从事 sprint 工作的 DevOps 专业人员。20% 到 50% 的企业应用程序组合由可通过工厂方法优化的重复模式组成。有关更多信息，请参阅本内容集中有关迁移工厂的讨论和云迁移工厂指南。

迁移元数据

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

迁移模式

一种可重复的迁移任务，详细列出了迁移策略、迁移目标以及所使用的迁移应用程序或服务。示例：EC2使用 App AWS lication Service 将主机迁移到 Amazon。

迁移组合评测（MPA）

一种在线工具，提供了用于验证迁移到的业务用例的信息。 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）。该MPA工具（需要登录）向所有 AWS 顾问和APN合作伙伴顾问免费提供。

迁移准备情况评测（MRA）

使用使用。深入了解组织的云就绪状态、找出优势和劣势、并制定行动计划来弥补发现的差距 AWS CAF。有关更多信息，请参阅迁移准备指南。MRA是AWS 迁移策略的第一阶段。

迁移策略

将工作负载迁移到中的方法 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的策略。 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现代化的准备情况 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？”

可变基础设施

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

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M2M machine-to-machine （M2M）通信协议。OPC-UA 提供数据加密、身份验证和授权方案的互操作性标准。

运营级别协议（ ）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。

操作准备情况审查 (ORR)

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

操作技术 (OT)

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

运营整合（OI）

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

组织跟踪

由创建的跟踪 AWS CloudTrail ，用于记录 AWS 账户 中的组织的所有事件 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，这个框架称为人员加速，因为云采用项目需要快速的变革。有关更多信息，请参阅OCM指南。

源访问控制（OAC）

中的一个增强选项 CloudFront，用于限制访问以保护您的 Amazon Simple Storage Service Service（Amazon S3）内容。OAC全部支持所有 S3 存储桶 AWS 区域、使用 AWS KMS (SSE-KMS) 的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）

中 CloudFront，一个选项，用于限制访问以保护您的 Amazon S3 内容。当您使用时OAI，CloudFront 会创建一个主体，供 Amazon S3 进行身份验证。经过身份验证的主体只能通过特定 CloudFront 分发访问 S3 存储桶中的内容。另OAC请参阅其中提供了更精细和增强的访问控制。

ORR

参见运营准备情况审查。

OT

参见运营技术。

出站（出口）VPC

在 AWS 多账户架构中，VPC一种用于处理从应用程序内部启动的网络连接的。AWS 安全参考架构建议使用入站、出站和检查VPCs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。示例PII包括姓名、地址和联系信息。

PII

查看个人身份信息。

playbook

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

PLC

参见可编程逻辑控制器。

PLM

参见产品生命周期管理。

策略

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

多语言持久性

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

组合评测

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

谓词

返回true或的查询条件false，通常位于子WHERE句中。

谓词下推下

一种数据库查询优化技术，可在传输前筛选查询中的数据。这将减少必须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 可执行操作并访问资源的实体。该实体通常是 AWS 账户、IAM角色或用户的根用户。有关更多信息，请参见IAM文档中的角色承担者术语和概念。

隐私设计

一种贯穿整个工程化过程考虑隐私的系统工程方法。

私有托管区

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VPCs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

一种旨在防止部署不合规的资源的安全控制。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，在基于微服务的微服务中MES，微服务可以将事件消息发布到其他微服务可以订阅的频道。系统可以在不更改发布服务的情况下添加新的微服务。

# Q

查询计划

一系列步骤，例如指令，用于访问SQL关系数据库系统中的数据。

查询计划回归

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

# R

RACI矩阵

请参阅责任、问责、咨询和知情（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

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。

重构

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

地理区域中的 AWS 资源集合。每个 AWS 区域 是孤立的，独立于其他的区域，以提供容错能力、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

定期升级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

SAML2.0

众多身份提供者（IdPs）使用的开放标准。此功能可实现联合单点登录（SSO），因此用户可以登录 AWS Management Console 或调用 AWS API操作，而不必IAM为企业中的每个人都创建用户。有关SAML基于 2.0 的联合身份验证的更多信息，请参阅文档中的关于基SAML于 2.0 的联合身份验证。IAM

SCADA

参见监督控制和数据采集。

SCP

参见服务控制政策。

secret

在中 AWS Secrets Manager，您以加密形式存储的机密或受限信息，例如密码或用户凭证。它由密钥值及其元数据组成。密钥值可以是二进制、单个字符串或多个字符串。有关更多信息，请参阅 Secret s Manager 密钥中有什么？ 在 Secrets Manager 文档中。

安全控制

一种技术或管理防护机制，可防止、检测或降低威胁行为体利用安全漏洞的能力。安全控制主要有四种类型：预防性、侦测、响应式和主动式。

安全加固

缩小攻击面，使其更能抵御攻击的过程。这可能包括删除不再需要的资源、实施授予最低权限的最佳安全实践或停用配置文件中不必要的功能等操作。

安全信息和事件管理（SIEM）系统

结合了安全信息管理（SIM）和安全事件管理（SEM）系统的工具和服务。SIEM系统会收集、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

由接收数据的在目的地对数据 AWS 服务 进行加密。

服务控制策略（SCP）

一种策略，用于集中控制 AWS Organizations的组织中所有账户的权限。SCPs为管理员可以委托给用户或角色的操作定义防护机制或设定限制。您可以SCPs将其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

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

服务水平协议（ ）SLA

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

服务级别指示器 () SLI

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 () SLO

代表服务运行状况的目标指标，由服务级别指标衡量。

责任共担模式

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

SIEM

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

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，请参阅中的分阶段将应用程序现代化的分阶段方法。 AWS Cloud

SPOF

参见单点故障。

star

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，请参阅将原有的 Microsoft ASP 现代化。 NET(ASMX) 通过使用容器和 Amazon API Gateway 逐步提供网络服务。

子网

您的 IP 地址范围VPC。子网必须位于单个可用区中。

监督控制和数据采集 (SCADA)

在制造业中，一种使用硬件和软件来监控有形资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

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

# T

标签

充当元数据的键值对，用于组织资源。 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。VPCs有关更多信息，请参阅 AWS Transit Gateway 文档中的什么是中转网关。

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

为您指定的服务授予权限，让其代表您在的组织中 AWS Organizations 及其账户中执行任务。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，两个披萨就能养活。双披萨团队的规模可确保在软件开发过程中充分协作。

# U

不确定性

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

无差别任务

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

上层环境

参见环境。

# V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC凝视

两者之间的连接VPCs，允许您使用私有 IP 地址路由流量。有关更多信息，请参阅 Amazon VPC 文档中的 VPC Peering。

漏洞

损害系统安全的软件缺陷或硬件缺陷。

# W

热缓存

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

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

一种对一组以某种方式与当前记录相关的行进行计算的SQL函数。窗口函数对于处理任务很有用，例如计算移动平均线或根据当前行的相对位置访问行的值。

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

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

WORM

参见一次写入，多读。

WQF

参见AWS工作负载资格框架。

写一次，读多次 (WORM)

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

# Z

零日漏洞利用

一种利用未修补漏洞的攻击，通常为恶意软件。

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。

僵尸应用程序

平均值CPU且内存使用率低于 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。