为可持续发展用例构建数据空间

AWS 规范性指导

AWS 规范性指导: 为可持续发展用例构建数据空间

Table of Contents

为可持续发展用例构建数据空间

Malte Gasseling 和 Ramy Hcini（Think-it）

2024 年 1 月（文件历史记录）

该策略的主要目标是为您提供如何设计、运营和维护数据空间的明确起点。该文件解释了数据空间的好处和潜力，特别是在环境、社会和公司治理 (ESG) 数据交换计划背景下。它展示了构建块，并提供了有关如何加入数据空间的信息。它还提供了在 Amazon Web Services (AWS) 云上构建数据空间的选项示例。该战略文件以技术模式为依据，该模式将具体模块和材料与 step-by-step 技术指导相结合，使该战略成为现实。

通过联合技术交换有关环境影响及其他方面的数据

数据空间是用于可信数据交换的联合网络，其核心原则是控制自己的数据。它们通过提供经济实惠且与技术无关的解决方案，使组织能够大规模共享、交换和协作处理数据。

数据空间有可能通过一种让所有相关利益相关者参与的 end-to-end 方法来支持实证问题的解决，从而极大地推动实现可持续未来的努力。这可以通过协作、数据驱动的创新来激发新想法和发现新机会，并有助于建立数据价值链。

通过打破数据壁垒并实现多种数据来源的交换，您的组织可以利用同行的综合知识，从而实现新的解决方案和突破。因此，数据空间通过支持大规模共享ESG数据、促进协作计划和行业标准，为可持续发展举措做出了贡献。这在供应链尽职调查和合规要求不断演变的背景下尤其重要，包括《非财务报告指令》（NFRD）、《企业可持续发展报告指令》（CSRD）和类似举措等法规。

此外，数据空间可以帮助您做出明智的决策，从而支持可持续发展并减少对环境的影响。通过为ESG数据创建可信且可访问的交换网络，数据空间可以帮助您的组织更好地跟踪其实现可持续发展目标的进展，从参与性的角度确定需要改进的领域，并更有效地证明其对监管要求的合规性。

在本决策者和企业高管指南的背景下，数据空间是支持实施欧洲议会和欧盟理事会最近就欧洲数据法达成的政治协议的技术之一。《欧洲数据法》旨在解锁工业数据，改善数据可访问性，培育竞争激烈的欧洲云市场，最终促进数据驱动的解决方案和协作，以符合更广泛的欧洲数据战略。这符合数据空间在促进可持续发展的数据交换和协作方面的原则，因为这两项举措都旨在通过数据驱动的解决方案增强组织能力。

要详细了解云技术对数据空间的好处以及其作用 AWS，请参阅博客文章 “通过数据空间实现数据共享” 和 AWS。

通过数据空间创造积极的环境影响

从设计上讲，参与数据空间的组织拥有并控制其在此类网络中的参与和协作。这可能会成为进入壁垒，但它也被视为您的组织学习如何更好地控制其数据并增加从数据资产中捕获的价值的潜在机会。

对于构建新数据空间或加入现有数据空间的组织来说，观察到的好处包括以下几点：

- 提高数据质量和完整性-使用标准化数据格式、验证数据源和实施数据验证规则
- 提高效率 — 自动化数据交换流程，减少手动错误，简化工作流程
- 增强协作 — 促进跨组织协作，加速创新，创造新的商机

数据空间作为 ESG 报告的支持

Organizations 和城市使用数据空间来做出明智的决策，从而支持可持续发展并减少对环境的影响。可持续发展目标几乎在所有行业中无处不在。以下示例重点介绍了数据空间计划如何推动ESG的目标和具体目标：

- 智慧城市 — 数据空间可以帮助优化能源消耗、交通管理、废物管理和城市基础设施，从而减少环境足迹并改善市民的生活质量。城市数据空间和智能停车等举措通过减少交通拥堵和促进资源的高效利用来促进可持续发展。有关更多信息，请参阅 “国际数据空间：数据空间雷达” 页面。
- 医疗保健和公共卫生 — 通过数据空间交换的数据有助于改善疾病监测、疫情防范和资源分配。这些改进带来了更高效、更可持续的医疗保健系统。
- 可再生能源优化 — 数据驱动的技术可以优化太阳能和风能等可再生能源的发电、分配和消费，以提高其效率并整合到能源网中。诸如sMart E nergy数据空间（DARE）和可再生能源后平台之类的举措旨在减少能源消耗，最大限度地减少浪费，促进可持续的经济增长。有关 “后可再生能源平台” 计划的更多信息，请参阅 “国际数据空间：数据空间雷达” 页面。

建立在 AWS 服务之上的数据空间示例

AWS 在塑造各行各业的数据空间和协作生态系统的周围格局方面发挥了关键作用。通过提供强大且可扩展的云原生服务，AWS 使组织能够创建和管理数据空间，从而促进数据共享、协作和创新。

本节介绍了两个基于 AWS 基础设施的持续数据空间的示例，展示了如何利用该技术来促进数据驱动的计划、简化信息交换以及推动不同领域的进步。这些真实的例子说明了促进数据空间和协作网络发展的多功能性和潜力。 AWS

证监会物流业交易所网络

智能货运中心（SFC）交换网络是一个协作网络，致力于在物流领域创建数据空间，其主要目标是通过促进活动和物流排放数据交换和报告来提高运输链的透明度和脱碳。该项目涉及各种利益相关者，包括物流服务提供商、托运人、承运人和工具提供商，他们在强调数据主权和安全的共享治理框架下进行协作。

为了实现证监会交易所网络的目标，已经根据参与者的意见和需求起草了几个主要用例的路线图。最初的用例是 “企业目标监控和报告”。该用例侧重于评估准确报告碳排放的参与公司的百分比，从而确保碳减排工作的透明度和问责制。

适用于汽车行业的 Catena-X

Catena-X 是迄今为止最先进的数据空间之一，由汽车行业推动，旨在应对可追溯性、可持续性、循环经济和高效供应链方面的挑战和机遇。数据领域表现出对可持续发展的巨大承诺，特别是在测量和减少汽车行业供应链中的碳排放，以及其标准化和改善碳数据管理的努力方面。

Catena-X承诺在整个产品生命周期中减少碳排放。为了实现这一目标，该协会已确定需要在价值链上进行标准化测量，准确记录真实的碳数据，并在汽车行业内进行可比性。其中一项举措侧重于制定《产品碳足迹规则手册》，该手册为记录和比较碳数据提供了统一的方法。

该协会与包括世界可持续发展商业理事会（WBCSD）在内的技术、行业和协会的利益相关者合作制定了这些标准和程序。Catena-X成功的一个关键目标是将整个供应链，尤其是中小型企业（SME）纳入数据交换，从而使他们的计划取得成功。

构建数据空间

正如AWS 博客中所解释的那样，以数据空间为核心 “有助于克服跨异构技术堆栈、环境和地理位置的组织间数据集成问题。” 该技术使组织能够保持对数据的控制，同时促进创新、协作和与他人共享见解。

数据空间为传统的集中式数据管理系统（例如数据湖和数据湖房）提供了分布式替代方案，后者通常依赖单一信任点。这使得数据空间比传统系统更具弹性和稳定性。它还鼓励协作和分担责任，从而在利益相关者之间建立信任，因为他们遵循开放标准和兼容的数据交换规则。控制与合作之间的平衡可确保敏感数据的安全，并鼓励创新。

数据空间中的核心角色

构建数据空间涉及以下三个核心角色：

- 数据空间管理局 — 根据国际数据空间协会的定义，数据空间管理局管理一个或多个数据空间，其中包括参与者注册，可能需要强制性的业务或技术要求。例如，数据空间管理局可能会要求参与者获得某种形式的商业认证。数据空间管理机构还可能施加技术要求，例如为特定使用政策的技术执行提供支持。
- 数据提供者-提供者管理要共享的数据资产。提供商帮助确保数据资产质量并确定使用政策。
- 数据使用者-消费者通常与提供者交互以获取所需的数据。消费者可能会将这些数据用于分析、决策、研究或其他应用。

提供者以结构化和可访问的方式提供数据，而消费者则根据约定的合同访问和使用数据。随着数据空间的发展和成熟，可以引入额外的角色和职责。例如，以下角色很常见：

- 应用程序提供商 — 负责开发和提供使用数据空间内数据的软件应用程序的实体。
- 定位合作伙伴 — 促进将新数据源、数据生成者或数据使用者整合到数据空间中的实体。它们在扩大和丰富数据空间生态系统方面发挥着至关重要的作用。
- 值得信赖的技术合作伙伴 — 在与数据空间内数据共享和协作相关的技术问题上充当中介机构或促进者的实体。它们涵盖了广泛的职责，包括：
  - 数据治理
  - 数据质量
  - 安全性
  - 促进数据集成和兼容性

- 技术支持和故障排除
- 监控数据空间运行状况
- 遵守法规

数据空间通常是如何构造和管理的

参与者之间的关系及其数据准备情况都定义了数据空间中治理和信任的基本规则。为了在参与者之间建立信任，数据空间管理机构可以采用三种典型模式之一：

- 集中式数据空间管理机构-数据空间管理机构制定参与规则并管理数据空间参与者的注册表。核心数据空间服务通过这个中央实体进行管理和访问，这促进了数据共享并有助于确保一致的治理。这种方法提供了简单性和统一性，但可能会引起人们对数据控制以及潜在的单点故障或信任的担忧。
- 联邦数据空间管理机构 — 在联合（或分布式）模型中，数据空间管理机构保留了一定程度的集中控制，但改进了技术和安全挑战。多个实体共同负责提供核心服务，而不仅仅是一个实体。Federation 促进了自主性、可扩展性和灵活性，同时有助于确保对数据的控制并解决隐私问题。
- 去中心化的数据空间管理机构 — 完全分散的机构消除了对中心信任点的需求，并且治理在参与组织之间分配。去中心化促进自主权、隐私和弹性，但它可能会带来与协调、共识和治理相关的挑战。

建立数据空间的关键步骤

数据空间管理局通过拥有或委托涵盖业务、法律、运营、功能和技术考虑因素的几个关键步骤来领导和推动数据空间的建设。

Data Space Support Center (DSSC) 提供了一个入门套件，其中包括在每个维度内需要回答的一组基础问题。入门套件问题包含在以下注意事项中：

1. 定义数据空间的范围和用途 — 确定数据空间中将包含哪些类型的数据、谁将使用数据以及数据空间将满足哪些业务需求。随着数据空间采用率的提高，数据类型和用例可能会随着时间的推移而发生变化。
2. 确定初始参与者、源系统和数据集 — 确定相关利益相关者的初始要求和期望。确定将在数据空间中交换的第一组数据源，并确定哪些数据集与预期用例最相关。
3. 制定治理原则和流程 — 定义数据管理和使用的角色和责任。制定数据标准、数据交换策略和安全协议。为协作环境提供激励措施。
4. 测试和验证数据空间用例 — 测试数据空间以确保其满足预期用例的要求，并验证是否实现了关键绩效指标 (KPI) 目标。

5. 部署和运营数据空间技术基础架构 — 在生产环境中部署数据空间，并监控其服务的性能和使用情况，以确定需要改进的领域。有关更多信息，请参阅技术模式。
6. 持续改善数据空间 — 通过更新政策并改善开发者和参与者的生态系统，根据用户和利益相关者的反馈随着时间的推移完善生态系统。
7. 向@@ 上扩展 — 通过更多参与者、更多、更高质量的数据、集成的数据分析和其他服务来扩展数据空间。要成功扩大规模，必须确保 IT 与业务部门之间的密切合作。

财务状况良好的商业模式对于确保数据空间的成功和增长至关重要。但是，收入优化和商业模式设计不属于本文档的范围。该策略侧重于为基于并由 AWS 服务其提供支持的具有成本效益的架构提供蓝图。

数据空间的核心技术组件

在构建数据空间时，以下组件是必不可少的：

- 信任框架 — 一组指导方针、标准和原则，用于定义数据空间内的信任和安全措施。信任框架概述了确保参与者之间安全交换数据的规则、政策和最佳实践。
- 数据空间协议 — 一组规则和规范，规定了如何在数据空间内传输、交换和访问数据。数据空间协议概述了数据共享、保持对数据的控制、互操作性和参与者之间高效通信的技术标准和方法。
- Ident@@ ity Hub — 对参与者的身份和身份验证方法进行集中管理。
- 发现服务-一种搜索数据并与他人共享数据的方式。
- 数据空间连接器 — 一种提供和管理数据空间策略（也称为数据交换规则）的连接器的实现。

信任框架

信任框架定义了数据空间内的信任和安全方法和措施。信任框架是构建数据空间的基础层。两个常用的框架为数据空间的实施和采用做出了贡献。

国际数据空间协会和 IDS 信任框架

国际数据空间协会（IDSA）是一家总部位于德国的非营利组织，成立于2016年。其目的是提供一种安全、保护隐私和值得信赖的数据交换方案，即国际数据空间 (IDS)。

IDS Trust Fram ework 为组织和个人之间的数据交换提供了解决方案，实现了安全高效的数据共享、处理和使用。该框架包括参考架构、开源构建块以及用于创建和运营数据空间的认证流程。IDSA致力于促进IDS信任框架的使用，并将其确立为数据交换和数据主权的全球标准。

Gaia-X 信任框架

Gaia-X Trust Fram ework 通过解决传统技术难以克服的挑战，代表了数据管理的重大进步。它在两个关键方面表现出色：数据主权和互操作性。Gaia-X Trust Framework 有助于确保组织即使在共享数据时也能保持对数据的控制权，这为数据安全和隐私建立了强大的框架。这种控制级别类似于敏感信息的安全数字保管库。

此外，Gaia-X Trust Framework在互操作性治理方面表现出色，它集成了不同的计算机系统并使它们能够进行有效的通信。它为各种数字组件和谐协作的环境提供了便利。这种创新的方法增强了数据共享，同时降低了成本，使更广泛的组织可以访问这些数据。与可能限制灵活性的旧技术不同，Gaia-X Trust Framework提供了更大的选择自由，为数据管理提供了一个现代开放的生态系统。

数据空间协议

数据空间协议是一组规则和标准，用于定义如何在数据空间内共享和使用数据。它的发展由国际数据空间协会（IDSA）推动和支持，旨在为不同领域和行业的数据交换提供共同的语言和结构。

数据空间协议定义了作为数据交换标准化和互操作性基础的关键概念和组件：

- 数据表示和编目-定义共享数据的结构和格式。
- 数据资产-发布到数据空间的单个数据。可以对资源进行版本控制，其元数据可以包含时间戳、作者和描述等信息。
- 数据服务-数据空间提供的功能，用于对资产执行操作，例如查询、筛选或转换数据。可以使用 REST API 或消息队列调用服务。
- Exchange 策略 — 管理如何访问、修改或删除数据的规则。数据使用和数据控制策略可以在多个层面进行定义，包括组织、数据集或资产级别。这些策略通过连接器附加到每项资产。违反策略可以启动警报和操作以强制执行数据治理。

数据空间的连接器技术

连接器是一种软件工具，允许在各种系统、应用程序和数据源之间共享和集成数据。在数据空间的背景下，连接器在符合数据空间协议预定义标准和交换策略的不同平台、系统和组织之间的通信和数据交换中起着关键作用。

基于 Eclipse 数据空间组件的连接器

Eclipse 数据空间组件 (EDC) 框架由 Eclipse 基金会作为免费开源软件开发。EDC框架的目标是创建一个高效实用的数据传输组件，该组件实现IDS标准的协议并追求与Gaia-X项目要求的兼容性。

作为核心组件，该连接器允许通过定义的数据主权合同进行数据交换，这些合同是自动协商的，以管理对数据资产的访问权限。EDC的架构以可扩展性和适应性为重点，是根据IDS和Gaia-X计划的反馈开发的。

EDC 框架的设计和构建基于以下四个支柱：

- 身份 — 每个参与者仍然可以控制自己的身份。
- 信任 — 每个参与者都决定信任谁。
- 主权 — 每个参与者决定根据什么政策共享他们的数据。
- 互操作性 — 每个参与者都可以控制自己的部署。

FIWARE 真连接器

FIWARE TRUE Connector 提供了一个规范，您的组织可以使用该规范在国际数据空间 (IDS) 生态系统中安全高效地共享数据。它提供了一种安全且可追溯的方式交换数据的标准化方式。该工具由三个主要组件组成：

- 执行核心容器
- FIWARE 数据应用程序
- 使用控制数据应用程序

这些组件协同工作，可实现数据交换、与身份提供商的通信以及使用控制策略的执行。通过使用 FIWARE TRUE Connector，您的组织可以参与 IDS 生态系统，并从安全、高效和可互操作的数据共享中受益。

简单

Simpl 是一个智能中间件平台，它代表了朝着创建欧洲共同数据空间迈出的重要一步。它旨在应对资源共享的挑战，同时保持控制和安全，促进利益相关者之间的信任。它在促进互操作性和资源共享，同时确保控制和安全方面的作用使其成为公共和私营部门实体的有前途的解决方案。协作是必不可少的，而且 Simpl 起着通用粘合剂的作用，可确保不同容量的互操作性，而无需昂贵的接口。

随着生态系统的不断发展，Simpl有望适应并成为欧洲数据空间的重要连接器。但是，有关其去中心化身份系统的考虑以及进一步整合的必要性仍然是需要解决的重要问题。Simpl有可能被欧盟委员会推荐或授权，这凸显了该项目在欧洲数据领域中的持续重要性。

以最小可行数据空间为起点

最小可行数据空间 (MVDS) 是数据空间的基本版本，它仅包含足够的组件来满足特定的业务需求。它通常包括少数参与者，其数据集对于特定用例或价值证明至关重要。它通常只包含最少的元数据和治理结构。

MVDS 的目的是为数据共享和协作提供一个起点，然后可以随着时间的推移对其进行扩展和完善。通常，MVDS 将包括许多集中式组件，以加快参与者对数据的采用和交换。

MVDS 工作流程示例

MVDS 的示例可能包含以下内容：

- 提供商
- 消费者
- 证书颁发机构
- 集中式身份服务

证书颁发机构颁发数字证书，作为参与者的加密凭证。身份服务使用这些证书来验证参与数据交换的实体的身份。

身份服务负责管理与数据空间参与者相关的动态属性。这些属性可能包括诸如访问权限、角色和其他与参与者关联的元数据之类的信息。

数据交换使用以下基本工作流程：

1. 证书颁发机构向消费者连接器和提供商连接器颁发证书。
2. 当消费者向提供者请求数据时，集中式身份服务会向消费者和提供者提供数据访问令牌 (DAT)。
3. 提供者应要求向消费者发送数据。

要在上部署和运行这样的 MVDS AWS，你可以使用 Amazon Elastic Kubernetes Service (Amazon EKS) 中的容器以及其他托管服务，例如亚马逊关系数据库服务 (Amazon RDS)，用于数据库和机密管理。AWS Secrets Manager

操作和维护数据空间

数据空间管理机构负责操作和维护任务。通常，它将这些任务委托给值得信赖的技术合作伙伴。这些任务可以包括但不限于以下内容：

- 优先考虑标准化、性能和可扩展性 — 确保标准化得到维持，以实现顺畅的数据交换和协作。决策者应承诺采用通用数据格式、命名惯例和协议。
- 强调用户友好的设计和可访问性 — 创建用户友好且现有和新参与者均可访问的界面和流程至关重要。提供清晰的文档、培训资源和支持服务，以促进快速采用，并确保参与者能够有效利用数据空间。
- 建立关键成功标准并定期将其作为绩效基准进行评估 — 评估与系统使用情况、数据合规性、效率、用户满意度和入职时间相关的指标。积极寻求正面反馈和参与者满意度作为成功的指标，并根据这些意见进行持续改进。
- 建立扩展和故障转移机制 — 这对于确保数据空间不间断的功能和可靠的性能至关重要，尤其是在面对不断变化的需求和意想不到的挑战的情况下。
- 仔细研究为数据空间的稳定发布提出的里程碑和路线图 ——这些时间表和目标应与组织的战略目标和承诺保持一致，确保数据空间开发步入正轨。
- 与参与者的目标保持一致 — 确保数据空间的设计和实施与参与者的更广泛的战略目标保持一致。这尤其适用于可持续性、效率和数据驱动决策等领域。
- 持续监控系统性能、用户满意度和标准合规性 — 准备好根据反馈和不断变化的要求进行必要的调整。
- 评估成本影响 — 跟踪拟议路线图的预计成本以及要完成的技术或开发工作。努力在数据空间开发投资与预期收益和回报之间取得平衡。
- 考虑潜在风险并制定缓解策略 — 这尤其涉及技术挑战、可扩展性问题和面向参与者的困难。采取积极措施应对这些风险，并确保数据空间的长期成功。
- 确保持续的支持和维护 — 在初始部署后，制定流程和机制，以保持数据空间的健康和最新。

加入数据空间

加入现有的数据空间为组织提供了一个极具吸引力的机会，使其成为完善的协作生态系统的一部分。通过加入数据空间而不是从头开始构建数据空间，您可以使用已经存在的基础架构、数据资源和参与者网络。

准备加入数据空间

面向数据空间的初始阶段侧重于了解数据空间的核心使命、目标和优势。这个基本的指导过程可以采取各种形式，例如参加网络研讨会、查看全面的文档或参加动手指导会议。

准备阶段是至关重要的基础。你需要清楚地了解数据空间的目的以及对有效协作和数据共享的支持与组织的目标一致。研究并考虑以下几点：

- 数据空间格局和核心使命 ——数据空间的类型、其重点领域及其所服务的社区
- 组织是否准备好有效地加入数据空间并在其中做出贡献 — 贵组织的数据成熟度级别和参与范围
- 参与的商业案例 — 通过明确的关键绩效指标和成功标准加入数据空间的好处，例如提高数据质量、提高效率和加强协作
- 角色和职责 — 明确的数据所有权、访问控制和争议解决机制

要帮助做好准备，请使用 Think-it 提供的数据空间就绪清单。

加入并参与数据空间

成功的准备阶段可以帮助参与者与数据空间集成，安全地交换数据，并协作探索共享信息在特定用例中的潜力。

定向过程的细节和复杂性各不相同，具体取决于特定的数据空间及其目标。方向可能包括以下常见步骤和注意事项。

成员资格和协议

- 根据数据空间的不同，您的组织可能需要提交成员资格申请。
- 审查并签署法律协议，概述数据共享的条款、数据治理、安全性和责任。

技术集成和高可用性

- 为控制平面（例如亚马逊 EKS）和数据平面（例如亚马逊简单存储服务 (Amazon S3)、Amazon Redshift AWS Gluehttps://aws.amazon.com/glue/ 和 AmazonKinesis）选择合适的技术。
- 将贵组织的系统与数据空间的连接器技术和数据服务集成。
- 制定适当的服务级别协议 (SLA) 并建立有效的流程，以确保联合服务和数据提供商端点的可靠性和可用性。
- 确定是否需要进行数据标准化和转换，以确保与数据空间标准的兼容性。
- 执行数据质量和合规性检查。
- 进行严格的测试，以验证数据是否可以安全无中断地流动。

数据共享、协作和创新

- 您的组织开始将相关数据共享到数据空间。对数据进行验证，并采用质量控制措施来维护数据的完整性。
- 您的组织可以访问其他人提供的数据，从而使数据与您的特定用例保持一致。对使用情况进行监控，以确保遵守数据治理和安全政策。
- 我们鼓励您探索创新的用例，并使用共享数据来实现互惠互利。
- 网络和协作机会可以带来伙伴关系和增值服务。

合规与治理

- 定期的合规性检查和审计有助于确保遵守数据治理标准。
- 随着规则执行、策略和数据交换标准的治理框架的演变而得到遵守。

扩展和增长

- 数据标准、安全协议和治理政策在适应不断变化的需求和挑战时得到遵守。
- 随着信任和参与度的提高，数据空间可能会扩大其生态系统，包括更多的参与者和数据源。
- 随着数据空间生态系统的发展，您的组织必须增强其以主权方式使用数据的能力，以实现目标并建立以数据为导向的文化和业务实践。这需要培训和技能提升。

挑战和局限性

根据多种因素，在设计和连接数据空间时需要考虑一些挑战和限制，包括以下十个最常观察到的挑战和限制：

- 技术复杂性 — 设置和维护数据空间需要一定的技术专业知识，尤其是在数据集成、数据治理和网络安全等领域。缺乏熟练专业人员来管理这些任务的组织可能很难从构建数据空间中获得全部收益。
- 数据质量问题 — 数据空间依赖于高质量的数据才能有效运行。但是，数据质量仍然是一项重大挑战，尤其是在处理遗留系统、不同的数据源和人为错误时。确保所有数据集的数据准确性、完整性和一致性至关重要，但通常很难实现。
- 集成挑战 — 将来自多个来源的数据整合到一个统一的视图中可能是一项复杂的任务。不同的数据格式、架构和语义可能会带来集成难题，需要大量时间和资源才能解决。
- 数据隐私和安全问题 — 数据空间必须确保敏感信息的隐私和安全，尤其是在医疗保健或金融等受严格监管的行业。实施强有力的安全措施和维护数据机密性至关重要，但并不总是那么简单。
- 文化和采用障碍 — 鼓励不同部门或组织之间的协作和数据共享可能具有挑战性。一些团队或组织可能对共享数据犹豫不决，理由是担心知识产权、竞争或过去的负面经历。
- 可扩展性限制 — 随着数据量的持续增长，数据空间必须进行扩展以适应增长。但是，扩展可能会带来新的挑战，例如管理大量数据、确保性能和维护数据质量。这些限制可能发生在治理层面，也可能出现在参与者层面。
- 成本和投资回报率 — 实施和维护数据空间确实会产生一些成本，包括基础架构、人员和软件费用。请务必预测并展示建设数据空间的明确投资回报率 (ROI)，尤其是在实施的早期阶段。
- 缺乏标准化 — 数据格式、架构和本体缺乏标准化会使不同的系统难以有效地通信和共享数据。建立共同的标准和框架可以帮助应对这些挑战。
- 变更管理 — 设计或加入数据空间需要对现有的工作流程、流程和文化进行重大更改。管理这种变化可能具有挑战性，尤其是在习惯根深蒂固或抵制新技术的组织中。
- 道德考量 ——随着人们越来越重视数据驱动的决策以及基于数据的创新商业模式，人们越来越担心偏见。这包括交换的数据和在数据空间内提供的服务中的偏见。确保数据空间的公平性、问责制和透明度至关重要，但这需要仔细考虑和努力。

通过承认并解决这些挑战和局限性，您的组织可以更好地了解构建或加入数据空间时的潜在障碍，并制定克服这些障碍的策略。

结论

本战略文件探讨了数据空间的动态格局及其作为可信数据交换联合网络的变革潜力。数据空间不仅仅是技术解决方案。它们也是积极的环境影响和可持续发展的催化剂。它们在打破壁垒、促进协作和促进大规模共享ESG数据方面发挥着重要作用。SFC Data Exchange Network和Catena-X的例子说明了跨行业数据空间的适应性，突显了数据空间的多功能性。

对构建和运营数据空间的不同方面的探索，加上对信任框架、连接器技术和最小可行数据空间 (MVDS) 概念的见解，为决策者提供了实用指南。然而，必须强调必须对交换后的数据使用进行周到的规划。这需要设想如何将共享数据用于决策、创新和价值创造。

全面的数据策略必须包括数据治理、分析和集成到现有工作流程中的注意事项。这种战略远见可确保交换的数据不仅可以满足即时的协作需求，还可以与长期组织目标保持一致。

从本质上讲，这份战略文件不仅可以作为实施数据空间的指南，还可以作为决策者考虑数据的整个生命周期（从交换到战略利用）的行动呼吁。在利用数据空间的变革力量时，要培养一种前瞻性的方法。除了协作，还包括明智而负责任地使用共享数据，以实现持续的积极影响和创新。

后续步骤

要踏上贵组织的数据空间之旅，请联系 Partn AWS er Think-i t。

Think-it 是一个软件工程团体。他们的使命是利用技术来再生我们的星球并提高人类的潜力。他们是数据空间连接器运营的先驱，使主权数据交换成为现实。他们尖端的跨学科方法正在推动更可持续的未来。

Think-it 的初始免费产品包括以下内容：

- 用于构建最小可行数据空间 (MVDS) 的技术模块，以便您可以尝试一下、构思并亲眼看到可以创造的价值。有关更多信息，请参阅 Think-it 技术模式指南。
- 免费咨询，指导您完成整个流程并了解您的业务需求。然后，顾问将为您提供准备清单，并确定下一步的范围，无论您是要针对现有数据空间进行定向，还是要构建一个新的、可扩展的数据空间试点。

资源

参考

- 通过数据空间和 AWS（AWS 公共部门博客文章）启用数据共享
- 《数据法》：委员会欢迎就公平和创新的数据经济规则达成政治协议
- 《欧洲数据法》
- 智能能源 (DARE) 的数据空间
- Catena-X：可持续发展
- Catena-X 如何加强汽车供应链？（西门子博客文章）
- 国际数据空间：数据空间雷达
- Gaia-x.eu
- 数字技术：Gaia-X生态系统——欧洲的主权数据基础设施
- TNO 终身创新：Gaia-X，一项旨在增强数字主权的欧洲计划
- Eclipse 数据空间组件
- 欧盟委员会：采购开源 cloud-to-edge 中间件平台的准备工作
- SIMPL：安全的物联网管理平台
- 后平台基金会

AWS 伙伴

- Think-it

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 2 月 15 日

AWS 规范性指导词汇表

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

数字

7 R

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

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

A

ABAC

请参阅基于属性的访问控制。

抽象服务

参见托管服务。

酸

参见原子性、一致性、隔离性、耐久性。

主动-主动迁移

一种数据库迁移方法，在这种方法中，源数据库和目标数据库保持同步（通过使用双向复制工具或双写操作），两个数据库都在迁移期间处理来自连接应用程序的事务。这种方法支持小批量、可控的迁移，而不需要一次性割接。与主动-被动迁移相比，它更灵活，但需要更多的工作。

主动-被动迁移

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

聚合函数

一个 SQL 函数，它对一组行进行操作并计算该组的单个返回值。聚合函数的示例包括SUM和MAX。

AI

参见人工智能。

AIOps

参见人工智能操作。

匿名化

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

反模式

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

应用程序控制

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

应用程序组合

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

人工智能（AI）

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

人工智能运营（AIOps）

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

非对称加密

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

原子性、一致性、隔离性、持久性（ACID）

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

基于属性的访问权限控制（ABAC）

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

权威数据源

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

可用区

中的一个不同位置 AWS 区域 ，不受其他可用区域故障的影响，并向同一区域中的其他可用区提供低成本、低延迟的网络连接。

AWS 云采用框架 (AWS CAF)

该框架包含指导方针和最佳实践 AWS ，可帮助组织制定高效且有效的计划，以成功迁移到云端。AWS CAF将指导分为六个重点领域，称为视角：业务、人员、治理、平台、安全和运营。业务、人员和治理角度侧重于业务技能和流程；平台、安全和运营角度侧重于技术技能和流程。例如，人员角度针对的是负责人力资源（HR）、人员配置职能和人员管理的利益相关者。从这个角度来看，AWS CAF 为人员发展、培训和沟通提供了指导，以帮助组织为成功采用云做好准备。有关更多信息，请参阅 AWS CAF 网站和 AWS CAF 白皮书。

AWS 工作负载资格框架 (AWS WQF)

一种评估数据库迁移工作负载、推荐迁移策略和提供工作估算的工具。 AWS WQF 包含在 AWS Schema Conversion Tool (AWS SCT) 中。它用来分析数据库架构和代码对象、应用程序代码、依赖关系和性能特征，并提供评测报告。

B

坏机器人

旨在破坏个人或组织或对其造成伤害的机器人。

BCP

参见业务连续性计划。

行为图

一段时间内资源行为和交互的统一交互式视图。您可以使用 Amazon Detective 的行为图来检查失败的登录尝试、可疑的 API 调用和类似的操作。有关更多信息，请参阅 Detective 文档中的行为图中的数据。

大端序系统

一个先存储最高有效字节的系统。另请参见字节顺序。

二进制分类

一种预测二进制结果（两个可能的类别之一）的过程。例如，您的 ML 模型可能需要预测诸如“该电子邮件是否为垃圾邮件？”或“这个产品是书还是汽车？”之类的问题

bloom 筛选条件

一种概率性、内存高效的数据结构，用于测试元素是否为集合的成员。

蓝/绿部署

一种部署策略，您可以创建两个独立但完全相同的环境。在一个环境中运行当前的应用程序版本（蓝色），在另一个环境中运行新的应用程序版本（绿色）。此策略可帮助您在影响最小的情况下快速回滚。

自动程序

一种通过互联网运行自动任务并模拟人类活动或互动的软件应用程序。有些机器人是有用或有益的，例如在互联网上索引信息的网络爬虫。其他一些被称为恶意机器人的机器人旨在破坏个人或组织或对其造成伤害。

僵尸网络

被恶意软件感染并受单方（称为机器人牧民或机器人操作员）控制的机器人网络。僵尸网络是最著名的扩展机器人及其影响力的机制。

分支

代码存储库的一个包含区域。在存储库中创建的第一个分支是主分支。您可以从现有分支创建新分支，然后在新分支中开发功能或修复错误。为构建功能而创建的分支通常称为功能分支。当功能可以发布时，将功能分支合并回主分支。有关更多信息，请参阅关于分支（GitHub 文档）。

破碎的玻璃通道

在特殊情况下，通过批准的流程，用户 AWS 账户 可以快速访问他们通常没有访问权限的内容。有关更多信息，请参阅 Well -Architected 指南中的 “实施破碎玻璃程序” 指示 AWS 器。

棕地策略

您环境中的现有基础设施。在为系统架构采用棕地策略时，您需要围绕当前系统和基础设施的限制来设计架构。如果您正在扩展现有基础设施，则可以将棕地策略和全新策略混合。

缓冲区缓存

存储最常访问的数据的内存区域。

业务能力

企业如何创造价值（例如，销售、客户服务或营销）。微服务架构和开发决策可以由业务能力驱动。有关更多信息，请参阅在 AWS上运行容器化微服务白皮书中的围绕业务能力进行组织部分。

业务连续性计划（BCP）

一项计划，旨在应对大规模迁移等破坏性事件对运营的潜在影响，并使企业能够快速恢复运营。

C

CAF

参见AWS 云采用框架。

金丝雀部署

向最终用户缓慢而渐进地发布版本。当你有信心时，你可以部署新版本并全部替换当前版本。

CCoE

参见云卓越中心。

CDC

参见变更数据捕获。

更改数据捕获（CDC）

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

混沌工程

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

CI/CD

查看持续集成和持续交付。

分类

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

客户端加密

在目标 AWS 服务 收到数据之前，对数据进行本地加密。

云卓越中心（CCoE）

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

云计算

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

云运营模型

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

云采用阶段

组织迁移到以下阶段时通常会经历四个阶段 AWS Cloud：

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

- 迁移 - 迁移单个应用程序
- 重塑 - 优化产品和服务，在云中创新

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

CMDB

参见配置管理数据库。

代码存储库

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

冷缓存

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

冷数据

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

计算机视觉 (CV)

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

配置偏差

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

配置管理数据库（CMDB）

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

合规性包

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

持续集成和持续交付（CI/CD）

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

CV

参见计算机视觉。

D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

根据网络中数据的关键性和敏感性对其进行识别和分类的过程。它是任何网络安全风险管理策略的关键组成部分，因为它可以帮助您确定对数据的适当保护和保留控制。数据分类是 Well-Architecte AWS d Framework 中安全支柱的一个组成部分。有关详细信息，请参阅数据分类。

数据漂移

生产数据与用来训练机器学习模型的数据之间的有意义差异，或者输入数据随时间推移的有意义变化。数据漂移可能降低机器学习模型预测的整体质量、准确性和公平性。

传输中数据

在网络中主动移动的数据，例如在网络资源之间移动的数据。

数据网格

一种架构框架，可提供分布式、去中心化的数据所有权以及集中式管理和治理。

数据最少化

仅收集并处理绝对必要数据的原则。在中进行数据最小化 AWS Cloud 可以降低隐私风险、成本和分析碳足迹。

数据边界

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

数据预处理

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

数据溯源

在数据的整个生命周期跟踪其来源和历史的过程，例如数据如何生成、传输和存储。

数据主体

正在收集和处理其数据的个人。

数据仓库

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

数据库定义语言（DDL）

在数据库中创建或修改表和对象结构的语句或命令。

数据库操作语言（DML）

在数据库中修改（插入、更新和删除）信息的语句或命令。

DDL

参见数据库定义语言。

深度融合

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

深度学习

一个 ML 子字段使用多层人工神经网络来识别输入数据和感兴趣的目标变量之间的映射。

defense-in-depth

一种信息安全方法，经过深思熟虑，在整个计算机网络中分层实施一系列安全机制和控制措施，以保护网络及其中数据的机密性、完整性和可用性。当你采用这种策略时 AWS，你会在 AWS Organizations 结构的不同层面添加多个控件来帮助保护资源。例如，一种 defense-in-depth 方法可以结合多因素身份验证、网络分段和加密。

委托管理员

在中 AWS Organizations，兼容的服务可以注册 AWS 成员帐户来管理组织的帐户并管理该服务的权限。此账户被称为该服务的委托管理员。有关更多信息和兼容服务列表，请参阅 AWS Organizations 文档中使用 AWS Organizations的服务。

部署

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

开发环境

参见环境。

侦测性控制

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

开发价值流映射 (DVSM)

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

数字孪生

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

维度表

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

灾难

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

灾难恢复 (DR)

您用来最大限度地减少灾难造成的停机时间和数据丢失的策略和流程。有关更多信息，请参阅 Well-Architected Fr ame AWS work 中的 “工作负载灾难恢复：云端 AWS 恢复”。

DML

参见数据库操作语言。

领域驱动设计

一种开发复杂软件系统的方法，通过将其组件连接到每个组件所服务的不断发展的领域或核心业务目标。Eric Evans 在其著作领域驱动设计：软件核心复杂性应对之道（Boston: Addison-Wesley Professional, 2003）中介绍了这一概念。有关如何将领域驱动设计与 strangler fig 模式结合使用的信息，请参阅使用容器和 Amazon API Gateway 逐步将原有的 Microsoft ASP.NET（ASMX）Web 服务现代化。

DR

参见灾难恢复。

漂移检测

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

DVSM

参见开发价值流映射。

E

EDA

参见探索性数据分析。

边缘计算

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

加密

一种将人类可读的纯文本数据转换为密文的计算过程。

加密密钥

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

字节顺序

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

端点

参见服务端点。

端点服务

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

企业资源规划 (ERP)

一种自动化和管理企业关键业务流程（例如会计、MES 和项目管理）的系统。

信封加密

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

environment

正在运行的应用程序的实例。以下是云计算中常见的环境类型：

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

epic

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

ERP

参见企业资源规划。

探索性数据分析（EDA）

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

F

事实表

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

失败得很快

一种使用频繁和增量测试来缩短开发生命周期的理念。这是敏捷方法的关键部分。

故障隔离边界

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

功能分支

参见分支。

特征

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

特征重要性

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

功能转换

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

FGAC

请参阅精细的访问控制。

精细访问控制 (FGAC)

使用多个条件允许或拒绝访问请求。

快闪迁移

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

G

地理封锁

请参阅地理限制。

地理限制（地理阻止）

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

GitFlow 工作流程

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

全新策略

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

防护机制

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

H

HA

参见高可用性。

异构数据库迁移

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

高可用性 (HA)

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

历史数据库现代化

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

同构数据库迁移

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

热数据

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

修补程序

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

hypercare 周期

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

I

IaC

参见基础架构即代码。

基于身份的策略

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

空闲应用程序

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

IIoT

参见工业物联网。

不可变的基础架构

一种为生产工作负载部署新基础架构，而不是更新、修补或修改现有基础架构的模型。不可变基础架构本质上比可变基础架构更一致、更可靠、更可预测。有关更多信息，请参阅 Well-Architected Framework 中的使用不可变基础架构 AWS 部署最佳实践。

入站（入口）VPC

在 AWS 多账户架构中，一种接受、检查和路由来自应用程序外部的网络连接的 VPC。AWS 安全参考架构建议使用入站、出站和检查 VPC 设置网络账户，保护应用程序与广泛的互联网之间的双向接口。

增量迁移

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

工业 4.0

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

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码（IaC）

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

工业物联网（IIoT）

在工业领域使用联网的传感器和设备，例如制造业、能源、汽车、医疗保健、生命科学和农业。有关更多信息，请参阅制定工业物联网（IIoT）数字化转型策略。

检查 VPC

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

物联网（IoT）

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

可解释性

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

IoT

参见物联网。

IT 信息库（ITIL）

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

IT 服务管理（ITSM）

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

ITIL

请参阅 IT 信息库。

ITSM

请参阅 IT 服务管理。

L

基于标签的访问控制 (LBAC)

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

登录区

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

大规模迁移

迁移 300 台或更多服务器。

LBAC

参见基于标签的访问控制。

最低权限

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

直接迁移

见 7 R。

小端序系统

一个先存储最低有效字节的系统。另请参见字节顺序。

下层环境

参见环境。

M

机器学习（ML）

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

主分支

参见分支。

恶意软件

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

托管服务

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

制造执行系统 (MES)

一种软件系统，用于跟踪、监控、记录和控制在车间将原材料转化为成品的生产过程。

MAP

参见迁移加速计划。

机制

一个完整的过程，在此过程中，您可以创建工具，推动工具的采用，然后检查结果以进行调整。机制是一种在运行过程中自我增强和改进的循环。有关更多信息，请参阅在 Well-Architect AWS ed 框架中构建机制。

成员账户

AWS 账户 除属于组织中的管理账户之外的所有账户 AWS Organizations。一个账户一次只能是一个组织的成员。

MES

参见制造执行系统。

消息队列遥测传输 (MQTT)

一种基于发布/订阅模式的轻量级 machine-to-machine (M2M) 通信协议，适用于资源受限的物联网设备。

微服务

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

微服务架构

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

迁移加速计划（MAP）

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

大规模迁移

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

迁移工厂

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

迁移元数据

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

迁移模式

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

迁移组合评测（MPA）

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

迁移准备情况评测（MRA）

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

迁移策略

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

ML

参见机器学习。

现代化

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

现代化准备情况评估

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

单体应用程序（单体式）

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

MPA

参见迁移组合评估。

MQTT

请参阅消息队列遥测传输。

多分类器

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

可变基础架构

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

O

OAC

请参阅源站访问控制。

OAI

参见源访问身份。

OCM

参见组织变更管理。

离线迁移

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

OI

参见运营集成。

OLA

参见运营层协议。

在线迁移

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

OPC-UA

参见开放流程通信-统一架构。

开放流程通信-统一架构 (OPC-UA)

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

运营级别协议（OLA）

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

运营准备情况审查 (ORR)

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

操作技术 (OT)

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

运营整合（OI）

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

组织跟踪

由 AWS CloudTrail 此创建的跟踪记录组织 AWS 账户 中所有人的所有事件 AWS Organizations。该跟踪是在每个 AWS 账户 中创建的，属于组织的一部分，并跟踪每个账户的活动。有关更多信息，请参阅 CloudTrail文档中的为组织创建跟踪。

组织变革管理（OCM）

一个从人员、文化和领导力角度管理重大、颠覆性业务转型的框架。OCM 通过加快变革采用、解决过渡问题以及推动文化和组织变革，帮助组织为新系统和战略做好准备和过渡。在 AWS 迁移策略中，该框架被称为人员加速，因为云采用项目需要变更的速度。有关更多信息，请参阅 OCM 指南。

来源访问控制（OAC）

在中 CloudFront，一个增强的选项，用于限制访问以保护您的亚马逊简单存储服务 (Amazon S3) 内容。OAC 全部支持所有 S3 存储桶 AWS 区域、使用 AWS KMS (SSE-KMS) 进行服务器端加密，以及对 S3 存储桶的动态PUT和DELETE请求。

来源访问身份（OAI）

在中 CloudFront，一个用于限制访问权限以保护您的 Amazon S3 内容的选项。当您使用 OAI 时，CloudFront 会创建一个 Amazon S3 可以对其进行身份验证的委托人。经过身份验证的委托人只能通过特定 CloudFront 分配访问 S3 存储桶中的内容。另请参阅 OAC，其中提供了更精细和增强的访问控制。

或者

参见运营准备情况审查。

OT

参见运营技术。

出站（出口）VPC

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

P

权限边界

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

个人身份信息 (PII)

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

PII

查看个人身份信息。

playbook

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

PLC

参见可编程逻辑控制器。

PLM

参见产品生命周期管理。

策略

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

多语言持久性

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

组合评测

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

谓词

返回`true`或的查询条件`false`，通常位于子`WHERE`句中。

谓词下推

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

预防性控制

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

主体

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

隐私设计

一种贯穿整个工程化过程考虑隐私的系统工程方法。

私有托管区

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

主动控制

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

产品生命周期管理 (PLM)

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

生产环境

参见环境。

可编程逻辑控制器 (PLC)

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

假名化

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

发布/订阅（发布/订阅）

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

Q

查询计划

一系列步骤，例如指令，用于访问 SQL 关系数据库系统中的数据。

查询计划回归

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

R

RACI 矩阵

参见 “负责任、负责、咨询、知情”（RACI）。

勒索软件

一种恶意软件，旨在阻止对计算机系统或数据的访问，直到付款为止。

RASCI 矩阵

参见 “负责任、负责、咨询、知情”（RACI）。

RCAC

请参阅行和列访问控制。

只读副本

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

重新架构师

见 7 R。

恢复点目标 (RPO)

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

恢复时间目标 (RTO)

服务中断和服务恢复之间可接受的最大延迟。

重构

见 7 R。

区域

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

回归

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

重新托管

见 7 R。

版本

在部署过程中，推动生产环境变更的行为。

搬迁

见 7 R。

更换平台

见 7 R。

回购

见 7 R。

故障恢复能力

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

基于资源的策略

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

责任、问责、咨询和知情（RACI）矩阵

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

响应性控制

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

保留

见 7 R。

退休

见 7 R。

旋转

定期更新密钥以使攻击者更难访问凭据的过程。

行列访问控制 (RCAC)

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

RPO

参见恢复点目标。

RTO

参见恢复时间目标。

运行手册

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

S

SAML 2.0

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

SCADA

参见监督控制和数据采集。

SCP

参见服务控制政策。

secret

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

安全控制

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

安全加固

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

安全信息和事件管理（SIEM）系统

结合了安全信息管理（SIM）和安全事件管理（SEM）系统的工具和服务。SIEM 系统会收集、监控和分析来自服务器、网络、设备和其他来源的数据，以检测威胁和安全漏洞，并生成警报。

安全响应自动化

一种预定义和编程的操作，旨在自动响应或修复安全事件。这些自动化可作为侦探或响应式安全控制措施，帮助您实施 AWS 安全最佳实践。自动响应操作的示例包括修改 VPC 安全组、修补 Amazon EC2 实例或轮换证书。

服务器端加密

在目的地对数据进行加密，由接收数据 AWS 服务 的人加密。

服务控制策略（SCP）

一种策略，用于集中控制 AWS Organizations的组织中所有账户的权限。SCP 为管理员可以委托给用户或角色的操作定义了防护机制或设定了限制。您可以将 SCP 用作允许列表或拒绝列表，指定允许或禁止哪些服务或操作。有关更多信息，请参阅 AWS Organizations 文档中的服务控制策略。

服务端点

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

服务水平协议（SLA）

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

服务级别指示器 (SLI)

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 (SLO)

代表服务运行状况的目标指标，由服务级别指标衡量。

责任共担模式

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

暹粒

参见安全信息和事件管理系统。

单点故障 (SPOF)

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

参见服务级别协议。

SLI

参见服务级别指标。

SLO

参见服务级别目标。

split-and-seed 模型

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

恶作剧

参见单点故障。

星型架构

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

strangler fig 模式

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

子网

您的 VPC 内的一个 IP 地址范围。子网必须位于单个可用区中。

监控和数据采集 (SCADA)

在制造业中，一种使用硬件和软件来监控有形资产和生产操作的系统。

对称加密

一种加密算法，它使用相同的密钥来加密和解密数据。

综合测试

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

T

标签

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

目标变量

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

任务列表

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

测试环境

参见环境。

训练

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

中转网关

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

基于中继的工作流程

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

可信访问权限

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

优化

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

双披萨团队

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

U

不确定性

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

无差别任务

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

上层环境

参见环境。

V

vacuum 操作

一种数据库维护操作，包括在增量更新后进行清理，以回收存储空间并提高性能。

版本控制

跟踪更改的过程和工具，例如存储库中源代码的更改。

VPC 对等连接

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

漏洞

损害系统安全的软件缺陷或硬件缺陷。

W

热缓存

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

暖数据

不常访问的数据。查询此类数据时，通常可以接受中速查询。

窗口函数

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

工作负载

一系列资源和代码，它们可以提供商业价值，如面向客户的应用程序或后端过程。

工作流

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

蠕虫

参见一次写入，多读。

WQF

请参阅 AWS 工作负载资格框架。

一次写入，多次读取 (WORM)

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

Z

零日漏洞利用

一种利用未修补漏洞的攻击，通常是恶意软件。

零日漏洞

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

僵尸应用程序

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

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