



为物联网设备制造商采用 Matter 标准

AWS 规范性指导



AWS 规范性指导: 为物联网设备制造商采用 Matter 标准

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

简介	1
目标	1
理解物质	2
物质协议	2
Matter 工作原理概述	2
认证的优势	4
对消费者的好处	4
简化设置和统一管理	4
改善了语音控制的选择和灵活性	4
为设备制造商带来的好处	5
跨生态系统的单一认证	5
降低了开发成本	5
简化的客户支持	5
认证注意事项	7
非 IP 连接协议	7
硬件限制	7
客户生态系统	8
设备类型尚未定义	8
另一种选择：在网关上代理	8
使用 Matter 实现云连接	10
通过云连接为物质端点启用高级设备功能	10
需要云连接的用例	10
支持云连接的架构	11
架起 Matter 和制造商云平台的桥梁	11
安全性	12
设备认证	12
加密通信	12
Over-the-air 更新	12
用物质发展	13
使用 Alexa	13
AWS 私有 CA 对 Matter 的支持	13
常见问题解答	15
Matter 的会员等级是多少？	15
智能家居消费者如何从 Matter 中受益？	15

设备制造商如何从 Matter 中受益？	16
Matter 会取代 Wi-Fi、蓝牙还是 Thread？	16
什么是供应商 ID 和产品 ID？	17
哪些设备需要通过 Matter 认证？	17
我的产品类型目前未在 Matter 中定义。为了让 Matter 产品获得认证，我还应该为哪些其他任务 预留时间？	17
我的一些设备直接连接到家庭 Wi-Fi 网络。这些设备需要通过 Matter 认证吗？	17
资源	18
AWS 资源	18
物联网连接标准联盟 (CSA)	18
文档历史记录	19
术语表	20
#	20
A	20
B	23
C	24
D	27
E	30
F	32
G	33
H	34
我	35
L	37
M	38
O	42
P	44
Q	46
R	47
S	49
T	52
U	53
V	54
W	54
Z	55
.....	lvi

为物联网设备制造商采用 Matter 标准

Tushar Patel、Vijay Ujjain 和 Amazon Web Services 的大卫·沃尔特斯 (AWS)

2024 年 2 月 ([文档历史记录](#))

根据 [Statista](#) 的数据，预计到2028年，全球智能家居家庭的数量将达到7.8亿。这种快速增长给运营和管理带来了挑战。从消费者的角度来看，每个设备供应商都有不同的方法，通过特定于该设备供应商的应用程序将智能家居设备接入家庭网络。这使得管理来自不同供应商的越来越多的不同类型的设备变得具有挑战性。同样，从设备制造商的角度来看，通过各种生态系统认证其智能家居产品会增加其业务流程的成本和复杂性。例如，这可能需要为同一设备型号使用不同的 SKU。维护一款引人注目的用户体验应用程序并提供定期更新会带来额外的开销，从而使资源无法专注于构建和交付更好的产品。消费者和设备制造商都将受益于通用的智能家居互操作性标准。该标准允许来自多个供应商的设备以无缝、安全和可靠的方式相互操作。

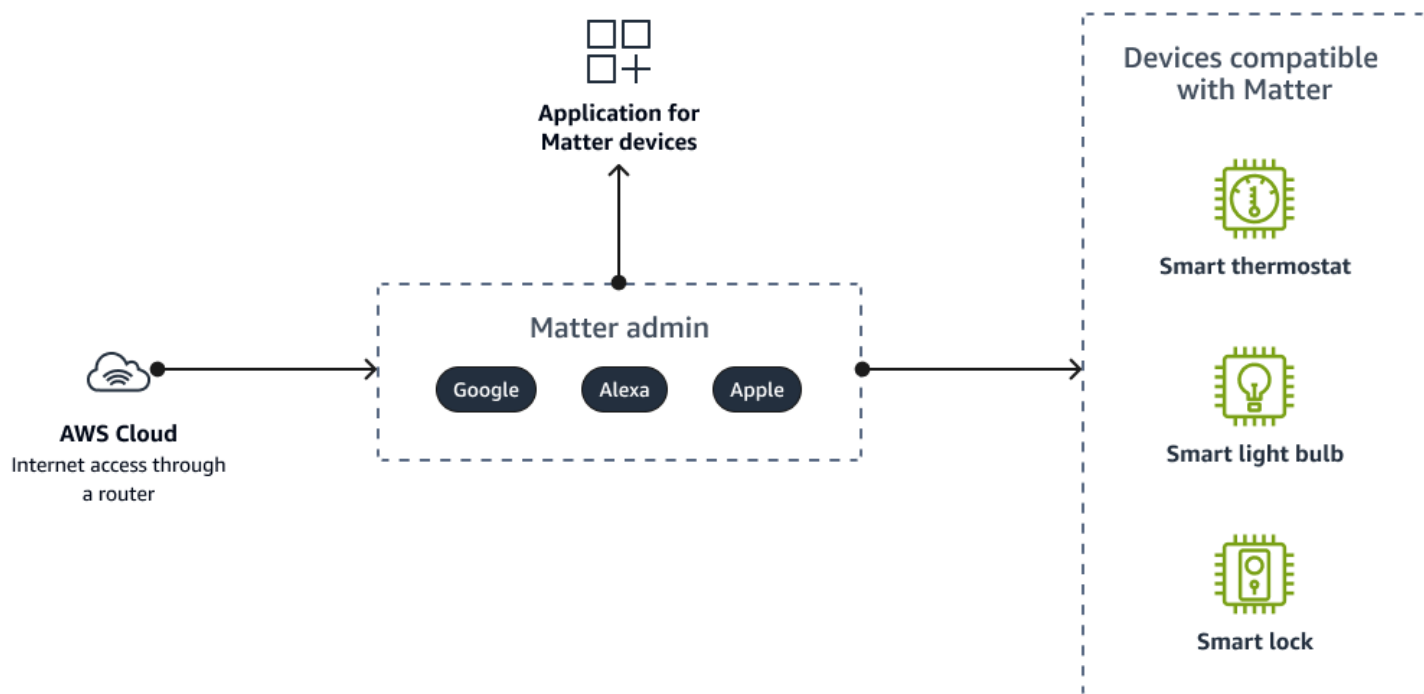
新的 [Matter](#) 标准为智能家居领域的物联网 (IoT) 设备制造商提供了一个激动人心的机会。该标准旨在提高不同制造商设备之间的兼容性和互操作性。Matter 是一种开放的智能家居连接协议，支持物联网设备、移动应用程序和云服务之间的通信。

目标

在将 Matter 标准集成到其产品中时，物联网设备制造商在开始开发之前必须解决几个挑战。与专有物联网协议相比，Matter 具有许多优势，包括设备的互操作性、安全性、简单性、可靠性和面向未来。但是，将 Matter 集成到新的和现有的物联网部署中需要仔细的规划和策略。制造商希望获得有关 Matter 合规流程的指导，以便在避免陷阱的同时利用好处。本指南为物联网设备制造商提供了有关 Matter 采用的全面指导。它包括从战略到实施的清晰路线图。本指南简化了向 Matter 的过渡，帮助您构建在智能家居生态系统中蓬勃发展的安全、可互操作且面向未来的产品。通过正确的战略方法，组织可以克服 Matter 采用的障碍，开发采用开放标准的创新物联网设备。

本指南为设备制造商全面概述了 Matter 以及实现 Matter 兼容所需的步骤。它概述了规划 Matter 采用策略的利弊。该指南还提出了在继续分阶段支持现有无线协议的同时利用 Matter 的最佳实践。对于探索智能家居解决方案的物联网设备制造商，本指南可以为您的连接策略提供信息。

了解 Matter 标准



物质协议

Matter 是一种开放的智能家居连接协议，可实现设备、移动应用程序和云服务之间的通信。Matter 由连接标准联盟 (CSA) 开发，可简化消费者和制造商的连接和互操作性。Matter 支持各种智能家居类别。对于消费者，Matter 提供了跨生态系统的入门培训、统一管理和控制。对于制造商而言，Matter 通过单一认证和应用程序开发来降低开发和支持成本。许多大公司，例如亚马逊、苹果和谷歌，都在推动 Matter 的采用。CSA 根据组织参与情况提供四种[会员级别](#)：发起人、参与者、采用者和同事。在强大的行业支持下，Matter 旨在为消费者提供跨品牌的无缝连接，并简化制造商的开发。

Matter 工作原理概述

Matter 是一种基于 IP 的应用程序级协议，适用于跨供应商生态系统的智能家居设备。它适用于使用 IPv6 的设备。从概念上讲，Matter 被组织为网络节点的集合，这些节点是 Matter 端点。以下是 Matter 术语的简要摘要：

- M@@@ atter 设备是智能家居产品，例如灯泡、开关、恒温器或锁。
- M atter 结构是连接所有设备的虚拟网络。所有设备共享同一个可信根目录。该结构形成星形网络拓扑。

- Matter 管理员创建、维护和管理结构上所有设备的安全和权限。管理员可以是集线器或应用程序。Matter 具有多管理员功能，其中 Matter 设备可以同时成为多个结构的一部分。例如，一台 Matter 设备可以由一台 Amazon Alexa 设备和 Google Home 设备进行管理，两者都可以是同一个物理网络上的 Matter 管理员。
- Matter 专员是一种将新 Matter 设备委托（或加载）到结构中的设备。这可能是手机上的应用程序、智能家居网关或 Matter 管理员。
- Matter 桥将非 IP 协议设备连接到 Matter 结构。

有关硬件和软件可以在 Matter 中扮演的不同角色的信息，请参阅 [Peeking Of Your Matter Smart Home](#)（CSA 博客文章）。

使用 Matter 进行认证的优势

Matter 的推出有望为智能家居消费者和为他们服务的制造商带来显著的优势。通过为智能设备建立通用语言，Matter 旨在通过简化的设置、跨平台的统一管理以及扩大的语音控制选择和灵活性来打破当今分散的市场。

对于消费者来说，这种统一的体验应该可以大大降低建造和扩展智能家居的复杂性和艰巨性。设备制造商还可以通过简化认证、降低开发成本和简化客户支持获得有意义的收益。由于 Matter 推动了更高的互操作性并降低了采用智能家居的门槛，这两个群体都将从中受益。总体而言，Matter 标准的认证有望通过解决迄今为止阻碍智能家居市场发展的市场问题，加速智能家居市场的增长。

主题

- [Matter 认证对智能家居消费者的好处](#)
- [Matter 认证对设备制造商的好处](#)

Matter 认证对智能家居消费者的好处

Matter 的推出有望为消费者带来显著的好处。Matter 为智能家居设备提供了一种通用语言，可以在主要平台上无缝协作。通过使用 Matter 对设备进行认证，消费者可以更轻松地设置和管理智能家居，并在如何控制设备方面获得更大的灵活性和选择性。

简化设置和统一管理

消费者面临的挫折之一是操作不同的智能家居设备并使它们协同工作所需的复杂设置和入门流程。每台设备可能需要自己的专有应用程序和单独的帐户。为了解决这个问题，Matter 为经过认证的设备启用了 plug-and-play 功能。入门 Matter 认证的设备非常简单，只需将设备连接到本地家庭网络，然后使用 Matter 管理员（例如 Alexa 应用程序）读取设备上的二维码即可。

这种通过单个应用程序实现的统一设置体验意味着消费者不再需要兼顾多个单独的应用程序来管理不同品牌的设备。他们可以通过单一界面查看和控制所有经过 Matter 认证的灯光、锁、传感器等。苹果 HomeKit、亚马逊 Alexa 和 Google Assistant 用户都受益于无需下载单独的制造商应用程序即可发现和控制在 Matter 设备。通过统一的系统简化了对智能家居设备的管理，降低了消费者的复杂性，并使构建和扩展设置变得不那么艰巨。

改善了语音控制的选择和灵活性

语音控制已成为消费者与智能家居设备互动的一种流行方式。但是，如今，语音助手的选择通常决定了你可以用语音控制哪些品牌的设备。Matter 通过启用跨生态系统的语音控制来改变这种状况。

消费者可以灵活地选择最适合其需求的语音助手生态系统，而不必担心设备兼容性。熟悉 Google Assistant 的用户可以用自己的语音控制他们的 Matter 认证设备，即使这些设备最初是为 Alexa 或市场制造的。HomeKit

语音控制的这种交叉兼容性创造了一个更加开放的环境，为用户提供了更多选择。他们可以根据功能和定价而不是与单一生态系统的兼容性来选择设备。如果用户将来想更换语音助手，他们现有的智能家居设置可以轻松随之移动，因为所有设备都使用通用的 Matter 语言。

Matter 认证对设备制造商的好处

除了帮助消费者外，Matter 认证还为智能设备制造商提供了有意义的好处。通过采用 Matter 标准，组织可以获得降低成本和扩大客户覆盖范围的优势。

跨生态系统的单一认证

目前，为了确保 Alexa HomeKit 和 Google Home 等生态系统的兼容性，制造商需要与每个组织进行多个漫长而昂贵的认证流程。Matter 通过建立单一的通用认证来改变这种状况。

设备制造商只需按照 Matter 标准对其产品进行一次认证，即可与所有主要的智能家居生态系统和语音助手兼容。与现状相比，这简化了开发并大大降低了认证成本。随着产品的更新，不再需要将资源花在维护单独的认证上。单一的 Matter 认证还可以使产品经得起未来考验，即使在新的生态系统出现时也能确保兼容性。

降低了开发成本

Matter 还有助于降低制造商的开发成本。通过采用通用的连接和安全标准，组织可以从共享基础设施组件中受益，这些组件为整个 Matter 项目做出了贡献。

例如，制造商不再需要在产品中加入自己的专有 Thread 边界路由器，从而将这一责任移交给了集线器制造商。共享的开源驱动程序和库进一步减少了冗余的工程工作。通用的服务发现和设备设置机制意味着需要更少的定制应用程序开发。基础设施和应用程序开发成本的降低可以以更实惠的智能家居设备的形式传递给消费者。

简化的客户支持

当前智能家居市场的分散给制造商带来了沉重的客户支持负担。消费者经常遇到连接、设置和兼容性方面的问题，需要进行故障排除。Matter 旨在通过标准化核心功能来减少这些问题。

当问题确实发生时，常见的底层 Matter 协议意味着公司可以更轻松地诊断和解决连接问题，而不必考虑多个生态系统。这简化了支持流程。借助单一应用程序和通用的语音兼容性，客户还可以更轻松地学

习使用设备，从而在许多情况下减少对支持的需求。Matter 提供的简化客户体验和故障排除有助于降低制造商的长期支持成本。

Matter 认证策略的注意事项

Matter 支持不同智能家居设备和平台之间的互操作性。但是，使用 Matter 进行认证可能并不总是设备制造商的最佳选择。实施和认证的成本可能不具有实际意义或财务意义，具体取决于设备类型和用例。本节探讨了制造商可能选择不通过 Matter 对某些设备进行认证的一些关键原因。

虽然 Matter 标准旨在简化开发并实现通用兼容性，但某些类型的智能家居设备在认证方面可能面临实际障碍，这些障碍大于好处。对于具有严格限制、非 IP 协议、受众有限或 Matter 中未定义设备类型的产品，最初寻求 Matter 认证可能不是最佳策略。这些可能是制造商可能避免采用 Matter 的原因。但是，Matter 确实允许启用 IP 的网关设备代理非 IP 端点。对于某些传统设备，网关方法可能是实现 Matter 兼容性的可行途径，同时可以避免对设备进行全面的重新设计。

随着 Matter 标准的发展及其范围扩大到涵盖更多用例，认证的理由可能会随着时间的推移而得到加强，即使对于这些产品类别也是如此。设备制造商需要评估其具体情况和路线图，以确定与 Matter 合规性有关的最佳方法。在许多情况下，选择退出认证可能有充分的技术或商业理由，至少是暂时的。

非 IP 连接协议

为了采用 Matter 标准，设备必须在 IP 网络上运行，例如 Wi-Fi、以太网和 Thread。非 IP 无线协议，例如 Zigbee、Z-Wave 和蓝牙 LE，通常用于低带宽设备。这些协议需要额外的非 IP 到基于 IP 的协议转换器才能与 Matter 兼容。升级通信模块或引入转换网关通常会增加设备的硬件成本。

添加 IP 堆栈支持意味着为网络处理分配更多的内存和处理能力。这可能会超出极低成本和低功耗设备的能力。添加额外的内存或闪存来支持 IP 还会增加制造成本并缩短电池寿命。对于只需要开启和关闭电源或传感器数据的用例，非 IP 协议可以提供有效的解决方案。

Matter 基本上排除了对任何依赖专有非 IP 无线标准的设备进行认证的可能性。这可能会限制想要为其低端产品使用替代连接方法的制造商。虽然基于 IP 的协议（如 Wi-Fi 和以太网）是连接不同的生态系统所必需的，但在某些应用中，非 IP 标准对于传感器和交换机的基本连接仍然有其优点。

硬件限制

另一个挑战是，Matter 需要最低水平的设备端处理能力和内存来支持必要的软件堆栈。但是，由于成本和尺寸限制，最基本的智能家居设备的嵌入式芯片功能通常非常有限。

例如，一个简单的门窗传感器可能只包含一个闪存小于 100 KB、RAM 小于 10 KB 的微控制器。这无法为完整的 Matter 实施提供足够的存储空间和处理空间。添加更强大、更昂贵的硅片将大大增加物料清单。

在成本和尺寸是重中之重的情况下，制造商可能会发现 Matter 要求与他们的硬件预算不一致。使用 Matter 认证非常基本的传感器、开关或控制器可能会强制进行不必要的硬件升级，从而影响可负担性。

客户生态系统

另一个需要考虑的因素是，制造商的目标客户群是否使用与 Matter 兼容的智能家居平台。如果该细分市场中的大多数消费者不使用 Matter 控制器或支持 Matter 的集线器和应用程序，那么可能就没有动力对产品进行认证。

例如，一家专注于满足老年用户需求的公司可能会发现他们的客户设置简单，没有 Matter 管理员。或者 do-it-yourself (DIY) 家庭自动化爱好者可能更喜欢定制解决方案，并且不需要 Matter plug-and-play 跨品牌的经验。

在目标人群不使用 Matter 基础设施的情况下，认证会增加复杂性，但没有明显的好处。最好将资源花在优化相关平台内的用户体验上，而不是将精力转移到 Matter 合规性上。

设备类型尚未定义

Matter 目前仅定义常见智能家居类别的设备配置文件和规格，例如照明、暖通空调、锁、百叶窗和娱乐。在设备类型标准化之前，这些定义区域之外的任何利基产品类型都必须使用自定义配置文件。所列垂直领域之外的设备类别，例如灌溉控制器、泳池设备和利基电器，尚无法使用 Matter。

如果公司开发了现有 Matter 配置文件未涵盖的独特设备类型，则在起草新的配置文件之前，无法进行认证。这可能会在等待 Matter 扩大其范围的同时推迟新产品的发布。

一些制造商可能宁愿通过专有手段更快地将利基解决方案推向市场，而不是推迟发布创新。在相关配置文件成熟后，仍然可以选择稍后进行认证。为了获得先发优势，在某些 direct-to-consumer 情况下，不使用 Matter 可能更可取。

另一种选择：在网关上代理

如果端点设备存在限制，无法直接通过 Matter 认证，则另一种方法是在网关上代理设备的 Matter 功能。网关充当在端点的本地无线协议和基于 IP 的 Matter 协议之间进行转换的桥梁。

例如，通过专有无线电标准进行通信的基本温度传感器仍然可以作为 Matter 设备显示给 Matter 管理员。网关在非 IP 接口上接收传感器数据，但通过 IP 向控制器公开表示该数据的虚拟 Matter 实体。这使您可以使用现有硬件，并通过网关获得一些互操作性优势。

当然，这会增加开发人员的复杂性，并且需要网关来支持必要的翻译层。但是，在直接认证对设备本身来说太具有挑战性的情况下，这可能是一个可行的折衷方案。代理可以帮助低功耗或利基解决方案在不进行全面硬件改革的情况下参与 Matter 生态系统。

使用 Matter 实现云连接

虽然 Matter 支持基本的本地设备互操作性，但还需要额外的云连接才能提供强大的 over-the-air 更新、遥测数据、远程管理以及与专有供应商服务的集成。设备制造商可以选择，例如运送 Matter 网关中心，使用家庭的 Matter 认证中心，或者将直接的云连接集成到端点中。Matter-to-cloud 连接标准正在出现，但制造商仍需要将其他连接软件堆栈集成到 Matter 设备中。要在诊断和新功能更新等领域提供智能家居设备的全部价值，Matter 制造商必须考虑云集成，而不仅仅是基本的本地运营。

通过云连接为物质端点启用高级设备功能

Matter 标准承诺通过通用协议统一来自不同供应商的物联网设备。它规定了智能家居设备如何使用基于 IP 的网络技术（例如以太网、Wi-Fi 和 Thread）在本地网络上进行发现、通信和互操作。这种本地互操作性使来自不同供应商的 Matter 认证设备能够无缝协作，进行自动场景和语音控制等活动。但是，Matter 不定义云接口，也不要求设备端点连接互联网。

如今，许多智能设备依赖额外的云连接来实现关键功能，例如 over-the-air（OTA）更新、远程访问以及与制造商平台的集成。希望构建符合 Matter 标准的产品，同时保留高级功能的设备制造商在为 Matter 补充云连接方面面临一些设计上的考虑。虽然基本的本地控制和语音助手集成适用于简单的 Matter 设备，但需要额外的云连接才能实现更高级的功能。

需要云连接的用例

尽管 Matter 可以处理本地设备互操作性，但额外的云连接可实现多项重要的智能家居设备功能：

- **Over-the-air (OTA) 更新** — 通过互联网提供固件和软件更新使供应商能够轻松增强已经部署的设备。如果没有 OTA，则将手动处理更新。虽然 Matter 标准描述了如何处理 OTA 更新并将其交付给 Matter 认证的端点，但它取决于端点所连接的 Matter 中心支持的功能。此外，对于向终端节点提供哪些更新，也存在限制。例如，当终端节点请求更新时，仅提供最新的可用更新。所有相同类型的设备都提供该单次更新。无法进行顺序更新，甚至无法选择 OTA 回滚或删除更新。在端点上启用云连接可以缓解 OTA 更新缺乏精细管理的情况。
- **远程访问和控制**-从家庭网络之外远程访问和控制设备需要云端点。按照目前的定义，Matter 仅支持本地访问。虽然可以通过本地网络内的用户应用程序控制 Matter 端点，但只有在 Matter Hub 支持的情况下，远程控制才可用。即便如此，通常也只能使用基本的遥控器。
- **遥测和诊断** — 将现场数据（例如错误日志和传感器流）聚合到云中，使供应商能够监控设备运行状况并识别问题。虽然 Matter 通过通用诊断集群支持与无线电和协议相关的诊断，但任何针对该设备的详细诊断都需要云连接，以便制造商可以从设备中检索数据。

- 供应商特定的集成 — 任何未在 Matter 规范中定义的自定义功能和数据类型都需要连接到供应商云平台。
- 外部集成 — 链接到第三方服务，例如不在 Matter 生态系统中的语音助手或第三方支付网关（视用例而定），需要与 Matter 管理员以外的互联网连接。

由于这些关键功能依赖于云连接，Matter 端点通常需要额外的互联网访问选项。

支持云连接的架构

对于 Matter 设备，有三种一般方法可以在满足本地操作规范的同时提供必要的云连接。

带有内置网关的智能家居集线器

一些设备制造商可能会选择推出一个专有的家庭中心，其中包含 Matter 管理员和通往其云服务的网关。这个家庭中心将按照标准在本地管理连接的 Matter 端点，同时还可以为高级功能的云连接提供便利。该中心可以支持端点的 OTA 更新、远程访问和遥测收集。

将云连接卸载到现有的 Matter 中心

与其捆绑自定义集线器，不如将设备设计为与 Amazon Echo 或 Google Home 等 Matter 集线器连接以进行互联网连接。在这种情况下，现有的 Matter Hub 会根据标准处理本地设备通信，它还还为需要它的端点提供了通往云端的网关。这利用了消费者可能已经拥有的基础设施。但是，这种方法取决于 Matter 中心为标准中未指定为 Matter Hub 规范的功能提供的支持级别。

端点中的直接云连接

具有直接互联网连接的设备（例如 Wi-Fi）可以为 Matter 本地网络和供应商云服务集成单独的连接。这使设备可以充当自己的云端网关。但是，依赖于 Thread 等协议的非 Wi-Fi 端点需要解决方案。这允许设备独立连接到云端，但对于简单、低成本、电池供电的设备来说，这可能不可行。

架起 Matter 和制造商云平台的桥梁

虽然 Matter 简化了本地互操作性，但要顺利连接 Matter 管理系统和制造商云平台，还需要付出额外的努力。诸如连接标准联盟 (CSA) 之类的组织正在努力标准化 Matter 设备与云端接口以获取 OTA 更新等功能的方式。广泛采用这种云连接标准将使设备制造商的开发变得容易。

最佳路径取决于特定产品的用例、价位和商业模式。很明显，要解锁智能家居消费者所期望的全部功能，即使对于注重本地互操作性的符合 Matter 标准的设备也是如此，对云服务的强大访问权限也是如此。设备制造商有机会使用 Matter 实现互操作性，同时仍然通过精心设计的云连接提供高级功能。

安全性

通过设计实现安全性是在设备设计阶段整合安全功能的做法，而不是在开发的后期阶段将其作为事后才想到的做法。加密通信和 over-the-air (OTA) 更新是安全设计的示例。Matter 从值得信赖、安全的制造工厂开始，通过设计实现安全性，为智能家居设备奠定了坚实的基础。Matter 设备只能由已知的可信产品认证机构 (PAA) 证书颁发机构 (CA) 的所有者制造和配置。

设备认证

Matter 设备必须相互进行身份验证并向控制器进行身份验证，然后才能进行通信。只有经过授权的设备才能连接到 Matter 结构。在制造过程中，设备会配置唯一的身份和 X.509 证书，即设备认证证书 (DAC)。当设备首次尝试连接到 Matter 结构时，专员设备会检查 DAC 的有效性，以及它是否由已知且值得信赖的产品认证中间体 (PAI) CA 签名。专员设备还会检查尝试连接到网络的设备是否符合 Matter 的规范、协议和安全标准。只有当所有检查都成功时，设备才有权访问 Matter 结构。

加密通信

在设备获得 Matter 结构的访问权限后，设备之间传递的所有数据都将通过高度加密进行保护。使用多层方法可以保持数据的完整性。事务专员使用 ECC-256 secp256r1 曲线进行密钥交换和签名验证。交换密钥后，Matter 设备使用 AES-256 对传输中的数据进行加密。对于每条消息，设备都使用 SHA-256 算法来验证数据在传输过程中没有被篡改。

Over-the-air 更新

Matter 标准还要求设备为 over-the-air (OTA) 更新实现强大的安全状态。OTA 是智能家居生态系统的重要组成部分，因此设备可以接收安全更新和新功能。Matter 设备的每次固件更新都必须由制造商的私钥签名。设备使用相应的非对称公钥来验证有效载荷签名。验证有效负载的签名后，设备可以将映像提交到其引导加载程序并进行重置。在启动过程中，设备必须再次验证镜像以确保其未被篡改，并且设备还会验证其运行的是最新的已知版本。

用物质发展

使用 Alexa

亚马逊为 Matter 开发提供了一套全面的工具。这些工具为构建与所有主要生态系统兼容并与 Amazon Alexa 无缝配合的 Matter 产品提供了快速途径。

节目：与 Alexa 配合使用

该计划可确保您连接到 Alexa 的设备提供卓越的客户体验。Works with Alexa (WWA) 徽章可增强客户的信心，这有助于提高对认证设备的偏好。有关更多信息，请参阅[宣布 Matter 发布和在 Matter 设备上推出与 Alexa \(WWA\) 配合使用](#)（亚马逊博客文章）。

SDK：使用 Alexa 开发 Matter

此 SDK 允许您为设备添加本地 Matter 连接，同时还包括托管云连接、商业智能和 OTA 支持。有关更多信息，请参阅使用[Alexa 充分利用 Matter](#)。

套件：Alexa Ambient Home 开发

该套件可帮助您跨协议与设备集成，从而使用 Alexa 构建环境统一的智能家居。有关更多信息，请参阅[Amazon Alexa](#)。

终端：可获得佣金的端点

对于与技能相关的 Matter 设备，Commissionable Endpoint API 可以创建与 Alexa 设备的本地基于 Matter 的连接，无需客户在获得许可后采取任何步骤。欲了解更多信息，请参阅[Alexa.Commissable Interface 1.0](#)（Alexa 技能套件）。

AWS 私有 CA 对 Matter 的支持

AWS Private Certificate Authority (AWS 私有 CA) 提供有关使用 Matter 标准的指导。

物质 DAC

Matter 需要设备认证证书 (DAC)，该证书必须由符合 Matter 公钥基础设施 (PKI) 证书政策 (CP) 的设备认证机构颁发。设备供应商可以 AWS 私有 CA 用来执行以下操作：

- 托管产品认证机构 (PAA) 证书颁发机构 (CA)

- 主持产品认证中级 (PAI) CA
- 发放、签名和维护每台设备的 DAC

有关更多信息，请参阅 AWS 安全博客中的[用于 AWS Private Certificate Authority 为 Matter 颁发设备认证证书](#)。

物质基础设施

AWS 提供了一个示例，演示了如何使用为 M[AWS Cloud Development Kit \(AWS CDK\)](#)atter 设置 PKI 基础架构。你 AWS 私有 CA 用来满足 Matter PKI CP 的要求。有关更多信息，请参阅上的 Mat[ter PKI CDK 项目](#)。GitHub

Java 示例

AWS 私有 CA 提供了用于创建符合 Matter 的产品认证机构 (PAA) 证书、产品认证中级 (PAI) 证书和设备认证证书 (DAC) 的 Java 示例。有关更多信息，请参阅 AWS Private Certificate Authority 文档[中的使用 AWS 私有 CA API 实现 Matter 标准 \(Java 示例\)](#)。

Matter PKI 合规指南

本[Matter PKI 合规指南](#)解释了如何实施和证明符合 CSA Matter PKI CP 要求。它提供了有关如何使用 AWS 私有 CA 来创建和操作符合 Matter 的证书颁发机构 (CA) 的信息。

常见问题解答

Matter 的会员等级是多少？

截至 2023 年 1 月，Matter 的成员级别分为以下四个级别。

成员类型	年度会员费（美元）	描述
发起人	105,000 美元	领导联盟，最终批准所有标准，拥有董事会席位，并参与董事会委员会
参与者	20,000 美元	为标准做出贡献并获取规范草案，以更快地推向市场
采用者	7,000	使用经批准的规格来制造和认证产品
助理	0美元*	通过认证转移计划为认证产品贴标签

*对于为产品贴上白标或品牌重塑的准会员，每件产品每年的初始费用为2,500美元，每件产品每年的持续费用为500美元。

您选择的会员级别取决于您对认证产品（采用者）或在标准中定义产品类型（参与者）的兴趣。有关会员级别的更多信息，请参阅 CSA 网站上的[“影响物联网的未来”](#)。

智能家居消费者如何从 Matter 中受益？

消费者通过以下方式从 Matter 中受益：

- 在家中简化了 Matter 设备的入门流程
- 通过单个应用程序统一管理所有智能家居设备
- 通过不同生态系统的一个或多个语音助手进行设备控制

有关更多信息，请参阅本指南中的[Matter 认证对智能家居消费者的好处](#)。

设备制造商如何从 Matter 中受益？

设备制造商通过以下方式从 Matter 中受益：

- 为设备提供单一认证，而不是每个生态系统（例如亚马逊 Alexa 或 Google Home）的多项认证。
- 不再需要开发该应用程序
- 由于无需运送基础设施组件（例如 Thread Border Router），因此降低了材料成本
- 降低了为有基础设施和连接问题的客户提供支持的成本

有关更多信息，请参阅本指南中的[Matter 认证对设备制造商的好处](#)。

Matter 会取代 Wi-Fi、蓝牙还是 Thread？

不是，Matter 是一种在 IP 网络上运行的应用程序级协议。使用 Wi-Fi、以太网或 Thread 进行连接的设备可以获得 Matter 认证。下表总结了 Matter 与 Wi-Fi、蓝牙和 Thread 的对比。

功能	问题	Wi-Fi	蓝牙	Thread
用途	智能家居通信	互联网接入和数据传输	短距离无线通信	低功耗无线网状网络
Range	因底层协议而异	最远可达 300 英尺	最远可达 30 英尺	最远可达 300 英尺
带宽	因底层协议而异	每秒高达 10 千兆比特	最高每秒 2 兆比特	高达每秒 250 千比特
功耗	因底层协议而异	相对较高	相对较低	非常低
安全性	因底层协议而异	WPA2、WPA3	AES、BLE 安全连接	AES
费用	因设备而异	相对便宜	相对便宜	相对昂贵

什么是供应商 ID 和产品 ID？

CSA 成员可以申请将他们识别为供应商的供应商 ID。此后，该公司的产品将分配给此 ID，并且可以追溯到其来源。此外，他们还会收到一个唯一的商品编码。16 位数的数字代码与护照号码等产品一起出现，使它们与供应商一样清晰明了。

哪些设备需要通过 Matter 认证？

任何需要进行身份验证并成为 Matter 结构一部分的设备都需要获得 Matter 认证。但是，那些设计为仅通过非标准（专有）协议与供应商指定的集线器交互的设备将无法从 Matter 认证流程中受益。例如，智能家居安全系统集线器必须通过 Matter 认证，但是与集线器通信的门窗传感器无需通过 Matter 合规认证。选择产品获得 Matter 认证主要是出于这种考虑。

我的产品类型目前未在 Matter 中定义。为了让 Matter 产品获得认证，我还应该为哪些其他任务预留时间？

案件规格并不支持所有类型的设备。如果您的设备类型不受支持，则第一步是以参与者身份加入 CSA。这需要您在 CSA 上投入财务和时间。作为参与者成员，您可以领导设备类型的定义，并可以访问规范草案，从而更快地 go-to-market 制定策略。有关会员级别的更多信息，请参阅 CSA 网站上的[“影响物联网的未来”](#)。

我的一些设备直接连接到家庭 Wi-Fi 网络。这些设备需要通过 Matter 认证吗？

Matter 认证可以使直接连接到智能家居网络的设备受益，因为它们可以连接到 Matter 结构。这使消费者能够通过同一 Matter 架构上的虚拟助手控制设备。但是，消费者必须使用特定于设备的应用程序来执行任何特定于供应商且未在 Matter 规范中定义的操作。

资源

AWS 资源

- [使用 Alexa 充分利用 Matter](#)
- [宣布 Matter 发布并推出适用于 Matter 设备的 Alexa \(WWA\)](#) (亚马逊 Alexa 博客)

物联网连接标准联盟 (CSA)

- [CSA 网站](#)
- [CSA 认证流程概述](#)
- [CSA 授权的测试提供商](#)
- [案件规格](#)

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5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](#)。

ACID

参见[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。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](#)。

AI Ops

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 (IAM) [文档](#) [AWS 中的 ABAC](#)。

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

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

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的信息。例如，Amazon SageMaker AI 为 CV 提供了图像处理算法。

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 is commonly described as a pipeline. CI/CD可以帮助您实现流程自动化、提高生产力、提高代码质量和更快地交付。有关更多信息，请参阅[持续交付的优势](#)。CD 也可以表示持续部署。有关更多信息，请参阅[持续交付与持续部署](#)。

CV

参见[计算机视觉](#)。

D

静态数据

网络中静止的数据，例如存储中的数据。

数据分类

根据网络中数据的关键性和敏感性对其进行识别和分类的过程。它是任何网络安全风险管理策略的关键组成部分，因为它可以帮助您确定对数据的适当保护和保留控制。数据分类是 Well-Architected 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](#)。

后

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，其中包含事实表中有关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 Framework 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](#)。

EDI

参见[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](#)相比，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)

组织之间自动交换业务文档。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](#)。

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

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。

少量提示

在要求[法学硕士](#)执行类似任务之前，向其提供少量示例，以演示该任务和所需的输出。这种技术是情境学习的应用，模型可以从提示中嵌入的示例 (镜头) 中学习。对于需要特定格式、推理或领域知识的任务，Few-shot 提示可能非常有效。另请参见[零镜头提示](#)。

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。

FM

参见[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

[人工智能](#)模型的子集，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工件，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 AI](#)。

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。

金色影像

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配置软件，并有助于提高设备制造运营的速度、可扩展性和生产力。

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

一项高级规则，可帮助管理各组织单位的资源、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。

抵制数据

从用于训练[机器学习](#)模型的数据集中扣留的一部分带有标签的历史数据。通过将模型预测与抵制数据进行比较，您可以使用抵制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。

hypercure 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 hypercure 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

laC

参见[基础设施即代码](#)。

基于身份的策略

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

空闲应用程序

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](#)建议设置您的网络帐户，包括入站、出站和检查，VPCs 以保护您的应用程序与更广泛的互联网之间的双向接口。

增量迁移

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

工业 4.0

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

基础设施

应用程序环境中包含的所有资源和资产。

基础设施即代码 (IaC)

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

工业物联网 (IIoT)

在工业领域使用联网的传感器和设备，例如制造业、能源、汽车、医疗保健、生命科学和农业。有关更多信息，请参阅[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](#)。

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](#)。

大型语言模型 (LLM)

一种基于大量数据进行预训练的深度学习 [AI](#) 模型。法学硕士可以执行多项任务，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

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](#)。

LLM

参见[大型语言模型](#)。

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、记录和控制将原材料转化为成品的生产过程。

MAP

参见[迁移加速计划](#)。

机制

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

成员账户

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

MES

参见[制造执行系统](#)。

消息队列遥测传输 (MQTT)

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

微服务

一种小型的独立服务，通过明确的定义进行通信 APIs，通常由小型的独立团队拥有。例如，保险系统可能包括映射到业务能力（如销售或营销）或子域（如购买、理赔或分析）的微服务。微服务

的好处包括敏捷、灵活扩展、易于部署、可重复使用的代码和恢复能力。有关更多信息，请参阅[使用 AWS 无服务器服务集成微服务](#)。

微服务架构

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

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信息。每种迁移模式都需要一套不同的迁移元数据。迁移元数据的示例包括目标子网、安全组和 AWS 账户。

迁移模式

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

迁移组合评测 (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

由此创建的跟踪 AWS CloudTrail，用于记录组织 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

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

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](#)。

policy

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。

通过设计保护隐私

一种在整个开发过程中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](#)措施，旨在防止部署不合规的资源。这些控件会在资源配置之前对其进行扫描。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。

提示链接

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，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” \(RACI \)](#)。

RAG

请参见[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

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](#)。

检索增强生成 (RAG)

一种[生成式人工智能](#)技术，其中[法学硕士](#)在生成响应之前引用其训练数据源之外的权威数据源。

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 [Secrets Manager 密钥中有什么？](#) 在 Secrets Manager 文档中。

安全性源于设计

一种在整个开发过程中考虑安全性的系统工程方法。

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。安全控制主要有四种类型：[预防性](#)、[侦测](#)、[响应式](#)和[主动式](#)。

安全加固

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

安全信息和事件管理 (SIEM) 系统

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

安全响应自动化

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

服务器端加密

在目的地对数据进行加密，由接收方 AWS 服务 进行加密。

服务控制策略 (SCP)

一种策略，用于集中控制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。

服务级别指示器 (SLI)

对服务性能方面的衡量，例如其错误率、可用性或吞吐量。

服务级别目标 (SLO)

代表服务运行状况的目标指标，由服务[级别指标](#)衡量。

责任共担模式

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

SIEM

参见[安全信息和事件管理系统](#)。

单点故障 (SPOF)

应用程序的单个关键组件出现故障，可能会中断系统。

SLA

参见[服务级别协议](#)。

SLI

参见[服务级别指标](#)。

SLO

参见[服务级别目标](#)。

split-and-seed 模型

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

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。您可以使用 [Amazon S CloudWatch ynthetic](#) 来创建这些测试。

系统提示符

一种向[法学硕士提供上下文、说明或指导方针](#)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

tags

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

目标变量

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

任务列表

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

测试环境

参见[环境](#)。

训练

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

中转网关

一个网络传输中心，可用于将您的网络 VPCs 和本地网络互连。有关更多信息，请参阅 AWS Transit Gateway 文档中的[什么是公交网关](#)。

基于中继的工作流程

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

可信访问权限

向您指定的服务授予权限，该服务可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

参见[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。

零镜头提示

向[法学硕士](#)提供执行任务的说明，但没有示例（镜头）可以帮助指导任务。法学硕士必须使用其预先训练的知识来处理任务。零镜头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[few-shot 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。