通过以下方式构建混合云架构的最佳实践 AWS 服务

AWS 规范性指导

AWS 规范性指导: 通过以下方式构建混合云架构的最佳实践 AWS 服务

Table of Contents

通过以下方式构建混合云架构的最佳实践 AWS 服务

亚马逊 Web Services（贡献者）

2025 年 6 月（文档历史记录）

许多企业和组织已将云计算作为其技术战略的关键方面。他们通常会将工作负载迁移到， AWS Cloud 以提高敏捷性、成本节约、性能、可用性、弹性和可扩展性。大多数应用程序都可以轻松迁移，但有些应用程序必须保留在本地，才能利用本地环境的低延迟和本地数据处理，以避免高昂的数据传输成本或合规性。此外，可能需要对一部分应用程序进行重新架构或现代化改造，然后才能将其迁移到云端。这促使许多组织寻求混合云架构来集成其本地和云端运营，以支持广泛的用例。这种混合方法可以提供本地计算和基于云的计算的优势，并且对边缘计算场景特别有用。

当您使用构建混合云时 AWS，我们建议您确定混合云策略和技术策略：

- 混合云战略提供了管理云和本地资源消耗的指导方针，以支持您的业务目标。本指南描述了构建混合云的常见用例，例如支持向云的持续迁移、确保灾难期间的业务连续性、将云基础架构扩展到本地环境以支持低延迟应用程序，或者扩大您的国际影响 AWS力。定义此策略可帮助您确定和定义构建混合云的业务目标，并提供在混合云上部署工作负载的指导方针。
- 混合云的技术策略确定了混合云架构的指导原则，并定义了实施框架。本指南概述了持续部署和管理的混合云架构的常见要求，以帮助您定义计划中的混合云实施原则。这些要求包括用于在云基础架构中进行资源配置和管理的标准化接口。

本指南描述了一种运营和管理框架，可帮助解决方案架构师和运营商确定用于实施 AWS 混合云的构建块、最佳实践以及混合云和区域内服务。 AWS

许多组织已使用本指南中描述的解决方案成功部署混合云环境，这些环境充分利用了该指南提供的规模、敏捷性、创新和全球足迹 AWS Cloud。（参见案例研究。）AWS 混合云服务可提供从云到本地和边缘的一致 AWS 体验。当 AWS Outposts 您需要在终端用户设备或现有本地数据中心和工作负载服务器之间实现低延迟时，计算、存储、数据库等服务将选择 AWS Local Zones 放在人口众多、行业中心 AWS 服务 附近。

在本指南中：

- 概述
- 先决条件和限制
- 混合云采用流程：

概览

本指南将混合云 AWS 建议分为五大支柱：网络、安全、弹性、容量规划和基础设施管理。它提供了指导方针，可帮助您提高准备状态，并使用 AWS 混合边缘服务（例如 AWS Outposts 或）制定迁移策略 AWS Local Zones。我们强烈建议您与您的 AWS 账户 团队合作 AWS Partner ，或者确保 AWS 混合云专家在您遵循本指南和开发流程时为您提供帮助。

> **Note**
>
> 尽管 AWS Outposts 和 Local Zones 可以解决类似的问题，但我们建议您查看用例以及可用的服务和功能，以确定哪种产品最适合您的需求。有关更多信息，请参阅 AWS 博客文章 AWS Outposts，AWS Local Zones 然后为您的边缘工作负载选择合适的技术。

混合云研讨会

在 AWS 混合云主题专家 (SME) 的协助下，您可以举办混合云研讨会，评估贵公司与本指南中讨论的五大支柱相关的成熟度。

研讨会侧重于组织内部领域，例如网络、安全、合规性 DevOps、虚拟化和业务部门。按照本指南混合云采用流程部分中的步骤，它可以帮助您设计满足组织要求的混合云架构，并定义实施细节。

PoCs

如果您有特定要求，则可以使用概念证明 (PoCs) 来验证 Local Zones 中的功能并根据这些要求 AWS Outposts 进行验证。

AWS 用于帮助您测试要移 PoCs 至 Outpost 或本地区域的工作负载，以确定这些工作负载在测试架构下是否可以正常运行。要访问本地区域进行测试，请按照 L ocal Zones 文档中的说明进行操作。要测试您的工作负载 AWS Outposts，请与您的 AWS 账户 团队合作或 AWS Partner 访问 AWS Outposts 测试实验室并接受 AWS 解决方案架构师的指导。在所有场景中，PoC 的开发都需要您生成一份包含以下内容的测试文档：

- AWS 服务 可供使用，例如亚马逊弹性计算云（亚马逊 EC2）、亚马逊弹性区块存储（亚马逊 EBS）、亚马逊虚拟私有云（亚马逊 VPC）和亚马逊 Elastic Kubernetes 服务（亚马逊 EKS）
- 要使用的实例的大小和数量（例如，`m5.xlarge`或`c5.2xlarge`）
- 测试架构图

- 测试成功标准
- 要运行的每项测试的详细信息和目标

支柱

下一节将介绍使用本指南中讨论的架构的先决条件和限制。之后的章节涵盖了每个支柱的详细信息，因此您在混合云研讨会期间创建的建议文档可以反映实施所需的设计细节。

- 边缘联网
- 边缘安全
- 边缘弹性
- 边缘容量规划
- 边缘基础设施管理

先决条件和限制

在遵循本指南之前，请与您的 AWS 账户 团队合作或 AWS Partner 查看使用和 Local Zones 实现边缘架构的先决条件 AWS Outposts 和限制。

先决条件

AWS Outposts

- 您现有的数据中心必须满足设施、网络和电力方面的AWS Outposts 要求。 AWS Outposts 设计用于在具有 5-15 kVA 冗余电源输入、每分钟 kVA 立方英尺 (CFM) 气流的 145.8 倍、环境温度介于 41°F (5°C) 和 95° F (35°C) 之间的数据中心环境中运行，以及其他要求。
- 咨询AWS Outposts 机架，确认该 AWS Outposts 服务在您所在的国家/地区可用 FAQs。看看问题：Outposts 机架在哪些国家和地区可用？
- 如果您的组织需要四个或更多AWS Outposts 机架，则您的数据中心必须满足聚合、核心、边缘 (ACE) 机架要求。
- 必须提供至少 500 Mbps（最好是 1 Gbps）的互联网或 AWS Direct Connect 链路才能连接AWS Outposts 到 AWS 区域，如果您的用例需要，还要有适当的备份连接。从该区域 AWS Outposts 到该地区的往返延迟最大值必须为 175 毫秒。
- 您必须拥有有效的AWS 企业支持或AWS 企业入门合同。

AWS Local Zones

- AWS 本地区域必须位于您的数据中心或用户附近。查看AWS Local Zones 地点。
- 确认您的本地基础设施与本地区域之间有网络连接：
  - 选项 1：从您的数据中心到离本地区域最近的AWS Direct Connect 接入点 (PoP) 的 AWS Direct Connect 链接。有关更多信息，请参阅 Local Zones 文档中的 Di rect Connect。
  - 选项 2：除本地虚拟专用网络 (VPN) 设备外，还需要互联网链接，并获得 EC2 在亚马逊本地区域启动基于软件的 VPN 设备所需的许可。有关更多信息，请参阅 Local Zones 文档中的 VPN 连接。

有关其他连接选项，请参阅 L ocal Zones 文档。

限制

AWS Outposts

- AWS Outposts 多可用区部署中的亚马逊关系数据库服务 (Amazon RDS) 需要客户拥有的 IP (CoIP) 地址池。有关更多信息，请参阅客户拥有的 Amazon AWS Outposts RDS 的 IP 地址。
- 在 Amazon R AWS Outposts DS 上，多可用区适用于所有支持的 MySQL 和 PostgreSQL 版本。AWS Outposts有关更多信息，请参阅 Amazon RDS on AWS Outposts 对 Amazon RDS 特征的支持。上的 Amazon RDS AWS Outposts 支持 SQL Server、适用于 MySQL 的亚马逊 RDS 和适用于 PostgreSQL 的 Amazon RDS 数据库。
- AWS Outposts 不是为在断开连接时运行而设计的 AWS 区域。有关更多信息，请参阅 AWS 白皮书《AWS Outposts 高可用性设计和架构注意事项》中的 “从故障模式角度思考” 部分。
- 上的亚马逊简单存储服务 (Amazon S3) Service 有 AWS Outposts 一些限制。《Outposts 上的亚马逊 S3 与亚马逊 S3 有何不同？》中讨论了这些问题 《O utposts 上的 Amazon S3 用户指南》部分。
- 开启的应用程序负载均衡器 AWS Outposts 不支持双向 TLS (mTLS) 或粘性会话。
- ACE 机架不是完全封闭的，不包括前门或后门。
- 实例容量工具仅适用于新订单。

AWS Local Zones

- Local Zones 没有 AWS Site-to-Site VPN 终端节点。取而代之的是在 Amazon EC2 上使用基于软件的 VPN。
- Local Zones 不支持 AWS Transit Gateway。而是使用 AWS Direct Connect 私有虚拟接口 (VIF) 连接到本地区域。
- 并非所有 Local Zones 都支持 Amazon RDS、Amazon FSx、Amazon EMR、Ama ElastiCache zon 或 NAT 网关等服务。有关更多信息，请参阅AWS Local Zones 功能。
- Local Zones 中的应用程序负载均衡器不支持 mTLS 或粘性会话。

混合云采用流程

以下各节讨论了 AWS 混合云各支柱的架构和设计细节：

- 边缘联网
- 边缘安全
- 边缘弹性
- 边缘容量规划
- 边缘基础设施管理

边缘联网

在设计使用 AWS 边缘基础设施（例如 AWS Outposts 或 Local Zones）的解决方案时，必须仔细考虑网络设计。网络是连接部署在这些边缘位置的工作负载的基础，对于确保低延迟至关重要。本节概述了混合边缘连接的各个方面。

VPC 架构

虚拟私有云 (VPC) 跨越其 AWS 区域中的所有可用区。您可以使用 AWS 控制台或 AWS Command Line Interface (AWS CLI) 添加 Outpost 或本地区域子网，将该区域中的任何 VPC 无缝扩展到 Outposts 或 Local Zones。以下示例说明如何使用以下方法在 Local Zones AWS Outposts 和 Local Zones 中创建子网： AWS CLI

- AWS Outposts：要向 VPC 添加前哨子网，请指定前哨基地的亚马逊资源名称 (ARN)。

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  有关更多信息，请参阅 AWS Outposts 文档。

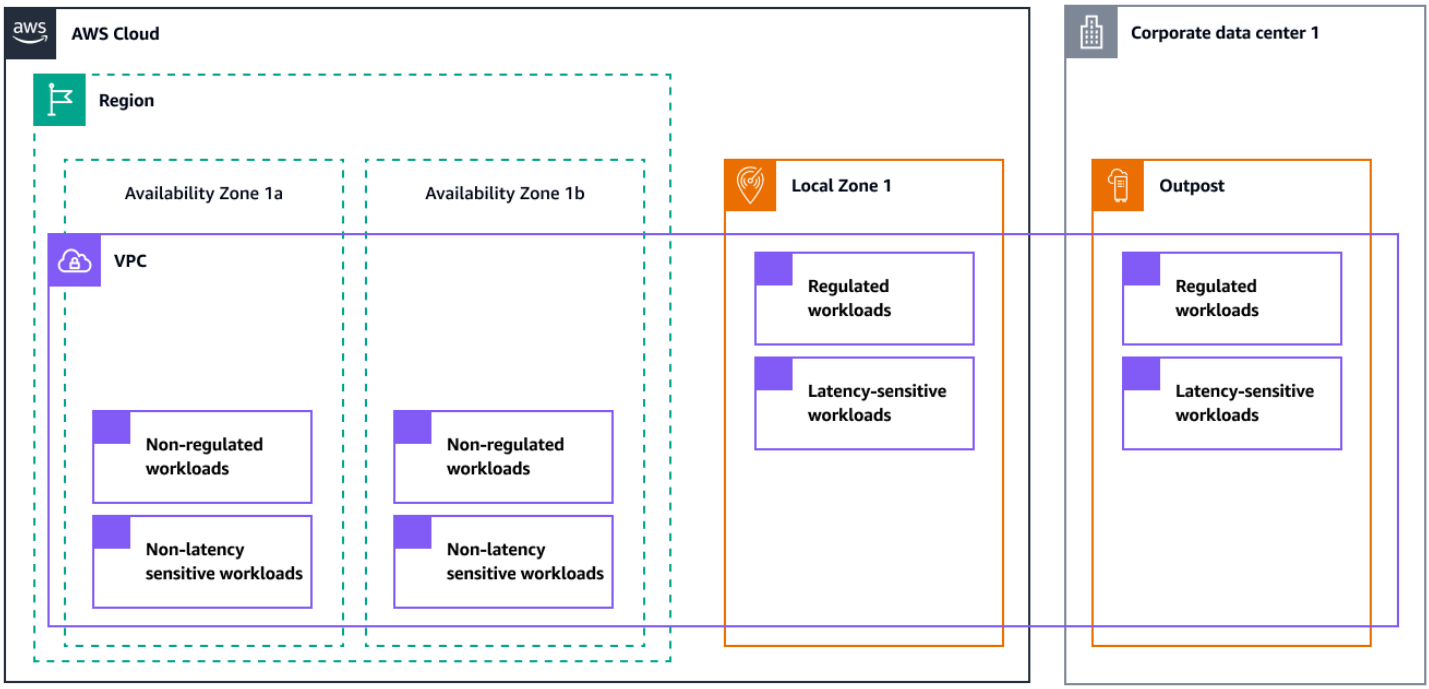
- L@@ oc al Zones：要向 VPC 添加本地区域子网，请按照与可用区域相同的步骤进行操作，但要指定本地区域 ID（<local-zone-name>在以下示例中）。

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
```

```
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

有关更多信息，请参阅 L ocal Zones 文档。

下图显示了包含 Outpost 和本地区域子网的 AWS 架构。



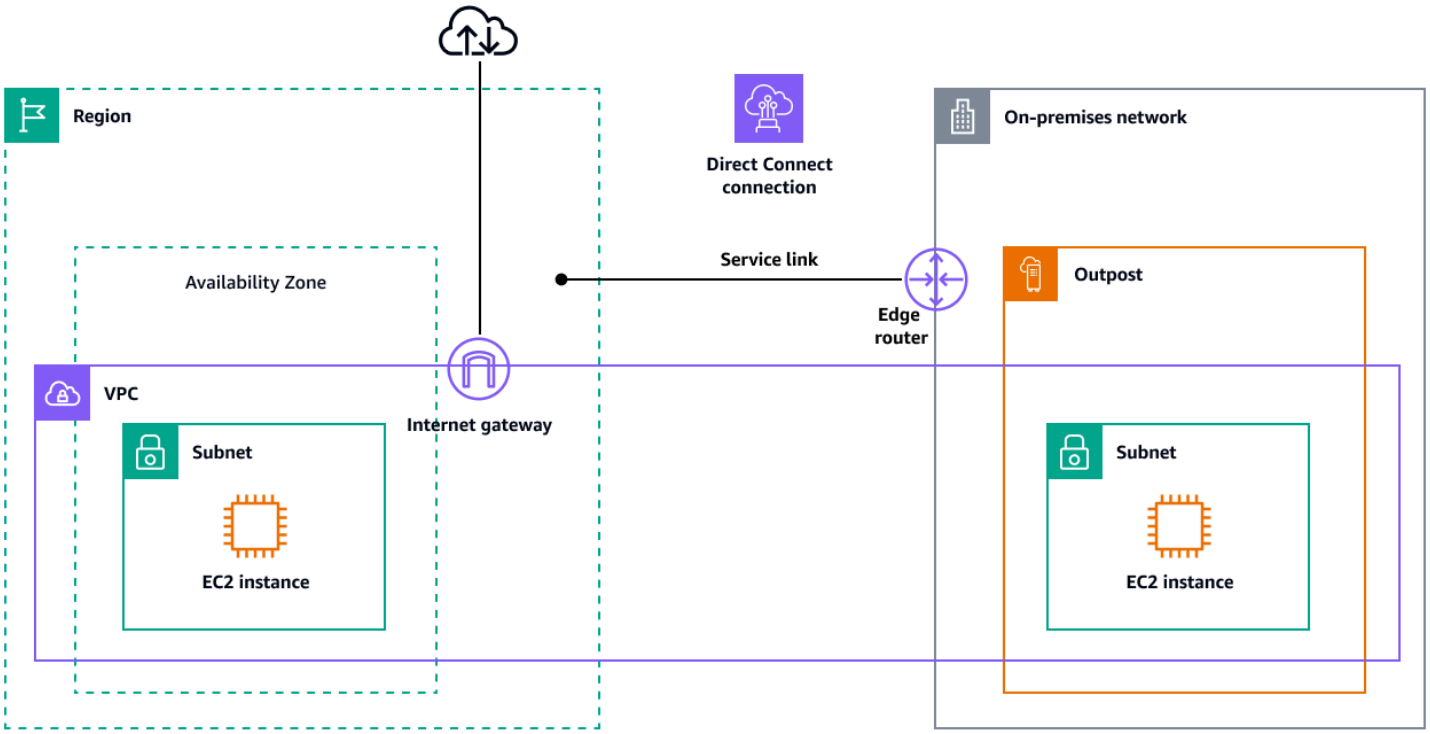
边缘到区域的流量

在使用诸如 Local Zones 和之类的服务设计混合架构时 AWS Outposts，请同时考虑边缘基础架构与之间的控制流和数据流量 AWS 区域。根据边缘基础设施的类型，您的责任可能会有所不同：有些基础设施要求您管理与父区域的连接，而另一些基础设施则通过 AWS 全球基础设施来处理此问题。本节探讨控制平面和数据平面连接对 Local Zones 和 AWS Outposts.

AWS Outposts 控制平面

AWS Outposts 提供了一种称为服务链路的网络结构。服务链接是 AWS Outposts 与选定区域 AWS 区域 或父区域（也称为主区域）之间的必需连接。它使前哨基地的管理以及前哨基地和之间的流量交换成为可能。 AWS 区域服务链接使用一组加密的 VPN 连接与本地区域进行通信。您必须通过互联网链接或 AWS Direct Connect 公共虚拟接口（公共 VIF）或私有虚拟接口（ AWS Direct Connect 私有 VIF）提供和之间的 AWS Outposts 连接。 AWS 区域 为了获得最佳体验和弹性， AWS 建议您使用至少 500 Mbps（更好 1 Gbps）的冗余连接来连接到。 AWS 区域至少 500 Mbps 的服务链接连接允许您启动亚马逊 EC2 实例、附加亚马逊 EBS 卷以及访问亚马逊 EKS AWS 服务 、亚马逊 EMR 和亚马逊

指标等。 CloudWatch 网络必须支持 Outpost 和父节点中的服务链路端点之间的最大传输单位 (MTU) 为 1,500 字节。 AWS 区域有关更多信息，请参阅 Outpo st AWS 区域 s 文档中的AWS Outposts 连接信息。



有关为使用 AWS Direct Connect 和公共 Internet 的服务链路创建弹性架构的信息，请参阅 AWS 白皮书《AWS Outposts 高可用性设计和架构注意事项》中的 Anchor 连接部分。

AWS Outposts 数据平面

AWS Outposts 和之间的数据平面由控制平面使用的相同服务链路架构支持。 AWS 区域 AWS Outposts 和之间的数据平面服务链路的带宽 AWS 区域 应与必须交换的数据量相关：数据依赖性越大，链路带宽应越大。

带宽要求因以下特征而异：

- AWS Outposts 机架数量和容量配置
- 工作负载特征，例如 AMI 大小、应用程序弹性和突发速度需求
- 发往该区域的 VPC 流量

中的实例 AWS Outposts 和 EC2 中的 EC2 实例之间的流量的 MTU AWS 区域 为 1,300 字节。我们建议您先与 AWS 混合云专家讨论这些要求，然后再提出在区域和之间具有相互依赖关系的架构。 AWS Outposts

Local Zones 数据平面

Local Zones 和 Local Zon AWS 区域 es 之间的数据平面通过 AWS 全球基础设施提供支持。数据平面通过 VPC 从扩展 AWS 区域 到本地区域。Local Zones 还提供高带宽 AWS 区域、安全的连接，使您能够通过相同 APIs 和工具集无缝连接到所有区域服务。

下表显示了连接选项和关联项 MTUs。

来自	至	MTU
该 EC2 地区的亚马逊	Local Zones EC2 中的亚马逊	1,300 字节
AWS Direct Connect	Local Zones	1,468 字节
互联网网关	Local Zones	1,500 字节
Local Zones EC2 中的亚马逊	Local Zones EC2 中的亚马逊	9,001 字节

Local Zones 使用 AWS 全球基础设施进行连接 AWS 区域。基础设施完全由管理 AWS，因此您不必设置此连接。我们建议您在设计任何在区域和本地区域之间存在相互依赖关系的架构之前，与 AWS 混合云专家讨论您的 Local Zones 要求和注意事项。

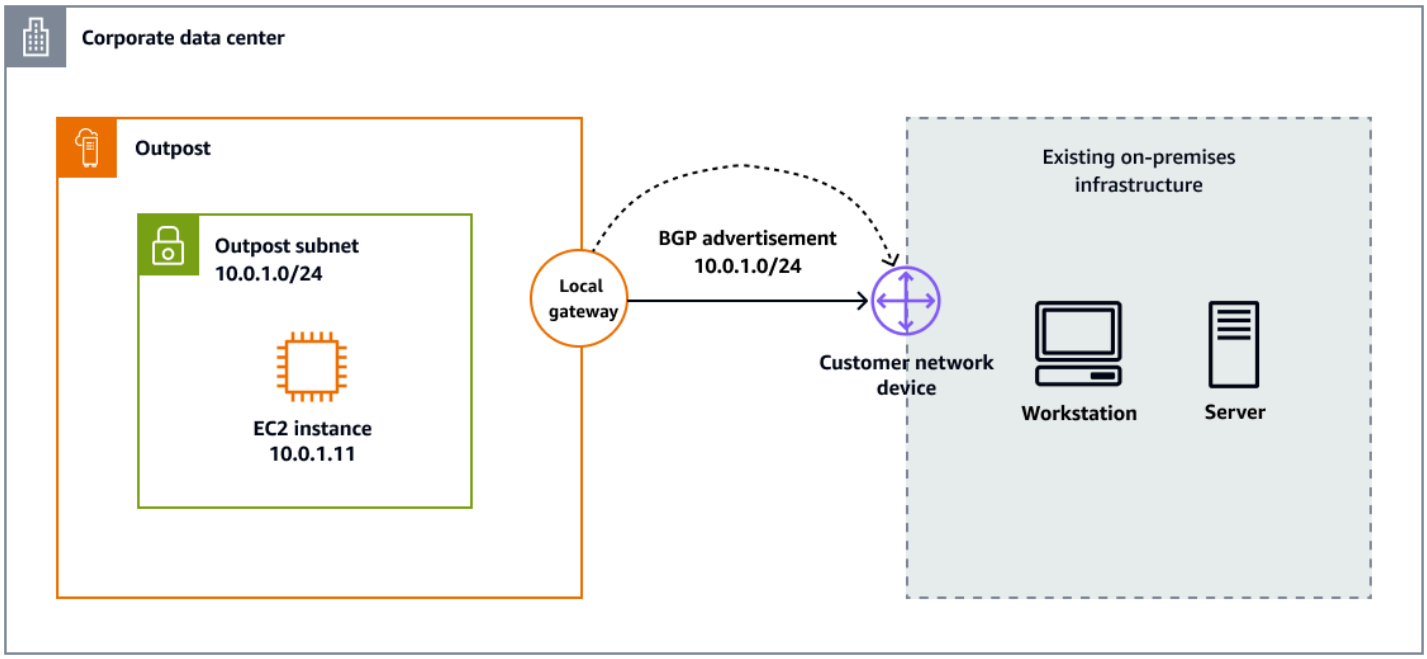
边缘到本地的流量

AWS 混合云服务旨在解决需要低延迟、本地数据处理或数据驻留合规性的用例。访问这些数据的网络架构很重要，这取决于您的工作负载是在还是 Local Zon AWS Outposts es 中运行。本地连接还需要明确定义的范围，如以下各节所述。

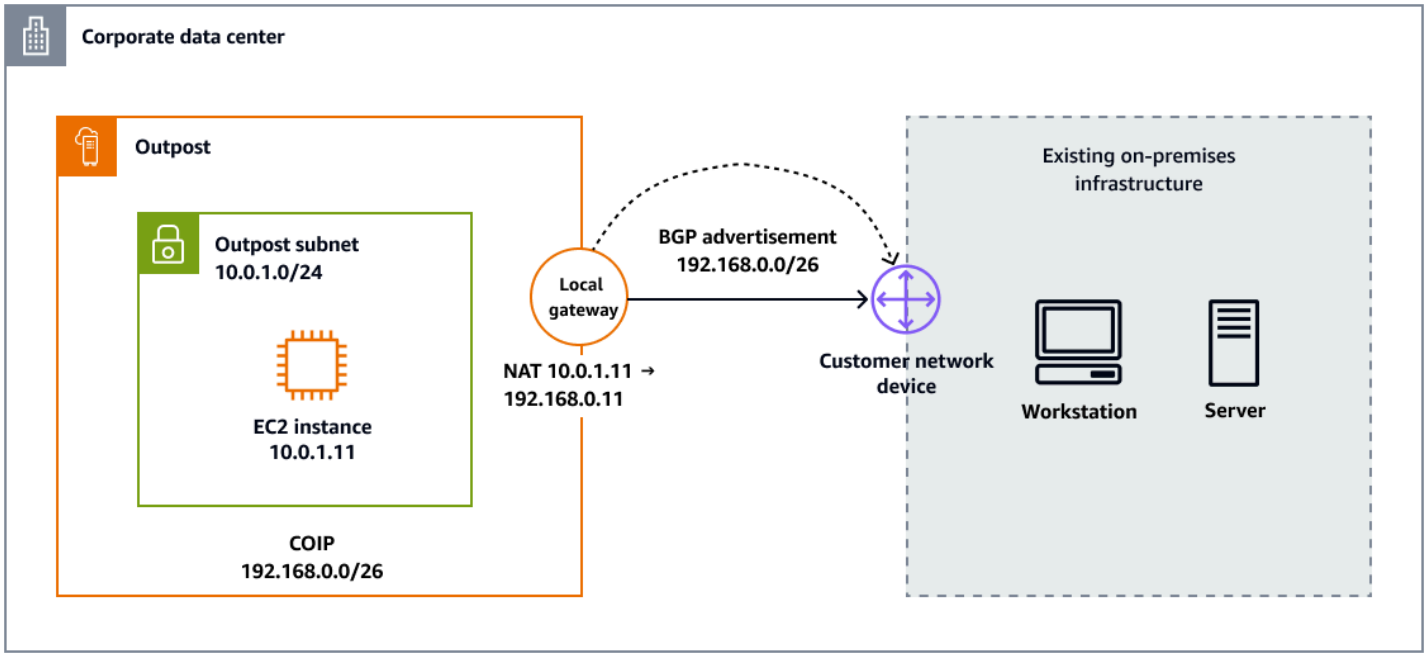
AWS Outposts 本地网关

本地网关 (LGW) 是 AWS Outposts 架构的核心组件。本地网关支持 Outpost 子网与本地网络之间的连接。LGW 的主要作用是提供从 Outpost 到本地本地网络的连接。它还通过直接 VPC 路由或客户拥有的 IP 地址，通过您的本地网络提供与互联网的连接。

- 直接 VPC 路由使用您的 VPC 中实例的私有 IP 地址来促进与本地网络的通信。这些地址通过边界网关协议 (BGP) 通告到您的本地网络。向 BGP 的通告仅适用于属于您的 Outpost 机架上子网的私有 IP 地址。这种类型的路由是的默认模式 AWS Outposts。在此模式下，本地网关不对实例执行 NAT，您也无需为 EC2 实例分配弹性 IP 地址。下图显示了使用直接 VPC 路由的 AWS Outposts 本地网关。



- 使用客户拥有的 IP 地址，您可以提供一个地址范围，即客户拥有的 IP (CoIP) 地址池，该地址池支持重叠的 CIDR 范围和其他网络拓扑。选择 CoIP 时，必须创建一个地址池，将其分配给本地网关路由表，然后通过 BGP 将这些地址通告回您的网络。CoIP 地址为本地网络中的资源提供本地或外部连接。您可以将这些 IP 地址分配给 Outpost 上的资源（例如 EC2实例），方法是从 CoIP 中分配新的弹性 IP 地址，然后将其分配给您的资源。下图显示了使用 CoIP 模式的 AWS Outposts 本地网关。



从本地网络 AWS Outposts 到本地网络的连接需要一些参数配置，例如启用 BGP 路由协议和在 BGP 对等体之间通告前缀。您的 Outpost 和本地网关之间可以支持的 MTU 为 1,500 字节。有关更多信息，请联系 AWS 混合云专家或查看AWS Outposts 文档。

Local Zones 和互联网

需要低延迟或本地数据驻留的行业（例如游戏、直播、金融服务和政府）可以使用 Local Zones 通过互联网向最终用户部署和提供应用程序。在部署本地区域期间，必须分配公有 IP 地址以供本地区域使用。在分配弹性 IP 地址时，您可以指定通告 IP 地址的位置。此位置称为网络边界组。网络边界组是可用区、Local Zon AWS es 或从中通告公有 IP 地址的 AWS Wavelength 区域的集合。这有助于确保 AWS 网络与访问这些区域中资源的用户之间的延迟或物理距离降至最低。要查看本地区域的所有网络边界组，请参阅 Local Zones 文档中的可用本地区域。

要将本地区域中的 EC2 Amazon 托管的工作负载暴露给互联网，您可以在启动实例时启用自动分配公有 IP 选项。 EC2 如果您使用 Application Load Balancer，则可以将其定义为面向互联网，这样分配给本地区域的公有 IP 地址就可以通过与本地区域关联的边界网络进行传播。此外，当您使用弹性 IP 地址时，您可以在 EC2 实例启动后将其中一个资源与其关联起来。当您通过 Local Zones 中的互联网网关发送流量时，将应用该区域使用的相同实例带宽规格。本地区域网络流量直接进入互联网或接入点 (PoPs)，无需穿过本地区域的父区域，从而可以访问低延迟计算。

Local Zones 通过互联网提供以下连接选项：

- 公共访问：通过互联网网关使用弹性 IP 地址，将工作负载或虚拟设备连接到互联网。
- 出站互联网访问：使资源能够通过网络地址转换 (NAT) 实例或具有关联弹性 IP 地址的虚拟设备访问公共终端节点，而不会直接暴露互联网。
- VPN 连接：使用互联网协议安全 (IPsec) VPN 通过具有关联弹性 IP 地址的虚拟设备建立私有连接。

有关更多信息，请参阅 L ocal Zones 文档中的本地区域的连接选项。

Local Zones 和 AWS Direct Connect

Local Zones 还支持 AWS Direct Connect，允许您通过专用网络连接路由流量。有关更多信息，请参阅 Local Zones 文档中的本地区域中的 Direct Connect。

Local Zones 和中转网关

AWS Transit Gateway 不支持将 VPC 直接连接到本地区域子网。但是，您可以通过在同一 VPC 的父可用区子网中创建 Transit Gateway 附件来连接到本地区域工作负载。此配置支持多个工作负载 VPCs

和您的本地区域工作负载之间的互连。有关更多信息，请参阅 Local Zones 文档中的本地区域之间的公交网关连接。

Local Zones 和 VPC 对等互连

通过创建新子网并将其分配给本地区域，您可以将任何 VPC 从父区域扩展到本地区域。可以在两者之间建立 VPC 对等互连 VPCs ，然后扩展到 Local Zones。当对等用户 VPCs 位于同一个本地区域时，流量将停留在本地区域内，不会通过父区域。

边缘安全

在中 AWS Cloud，安全是重中之重。随着组织采用云的可扩展性和灵活性， AWS 可以帮助他们将安全性、身份和合规性作为关键业务因素。 AWS 将安全性集成到其核心基础架构中，并提供服务来帮助您满足独特的云安全要求。当您将架构的范围扩展到时 AWS Cloud，您将受益于将 Local Zones 和 Outposts 等基础架构集成到中。 AWS 区域通过这种集成 AWS ，可以将一组精选的核心安全服务扩展到边缘。

安全是双方共同承担 AWS 的责任。责任AWS 共担模型区分了云的安全性和云端的安全性：

- 云安全 — AWS 负责保护在云 AWS 服务 中运行的基础架构 AWS Cloud。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划的一部分，第三方审计师定期测试和验证 AWS 安全的有效性。
- 云端安全 — 您的责任由您 AWS 服务 使用的内容决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

数据保护

分 AWS 担责任模型适用于 AWS Outposts 和中的数据保护 AWS Local Zones。如本模型所述 AWS ，负责保护运行 AWS Cloud （云安全）的全球基础架构。您有责任保持对托管在此基础架构上的内容的控制（云端安全）。此内容包括您 AWS 服务 使用的的安全配置和管理任务。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS Identity and Access Management (IAM) 或设置个人用户AWS IAM Identity Center。这仅为每位用户提供履行其工作职责所需的权限。

静态加密

在 EBS 卷中加密

使用 AWS Outposts，所有数据都处于静态加密状态。密钥材料用外部密钥 Nitro 安全密钥 (NSK) 包裹，该密钥存储在可移动设备中。需要使用 NSK 来解密 Outpost 机架上的数据。您可以对 EBS 卷和

快照使用 Amazon EBS 加密。Amazon EBS 加密使用 AWS Key Management Service (AWS KMS) 和 KMS 密钥。

就本地区域而言，默认情况下，所有本地区域中的所有 EBS 卷都经过加密，但AWS Local Zones 常见问题解答中记录的列表除外（参见问题：本地区域中 EBS 卷的默认加密行为是什么？），除非已为账户启用加密。

Outposts 上的 Amazon S3 中的加密

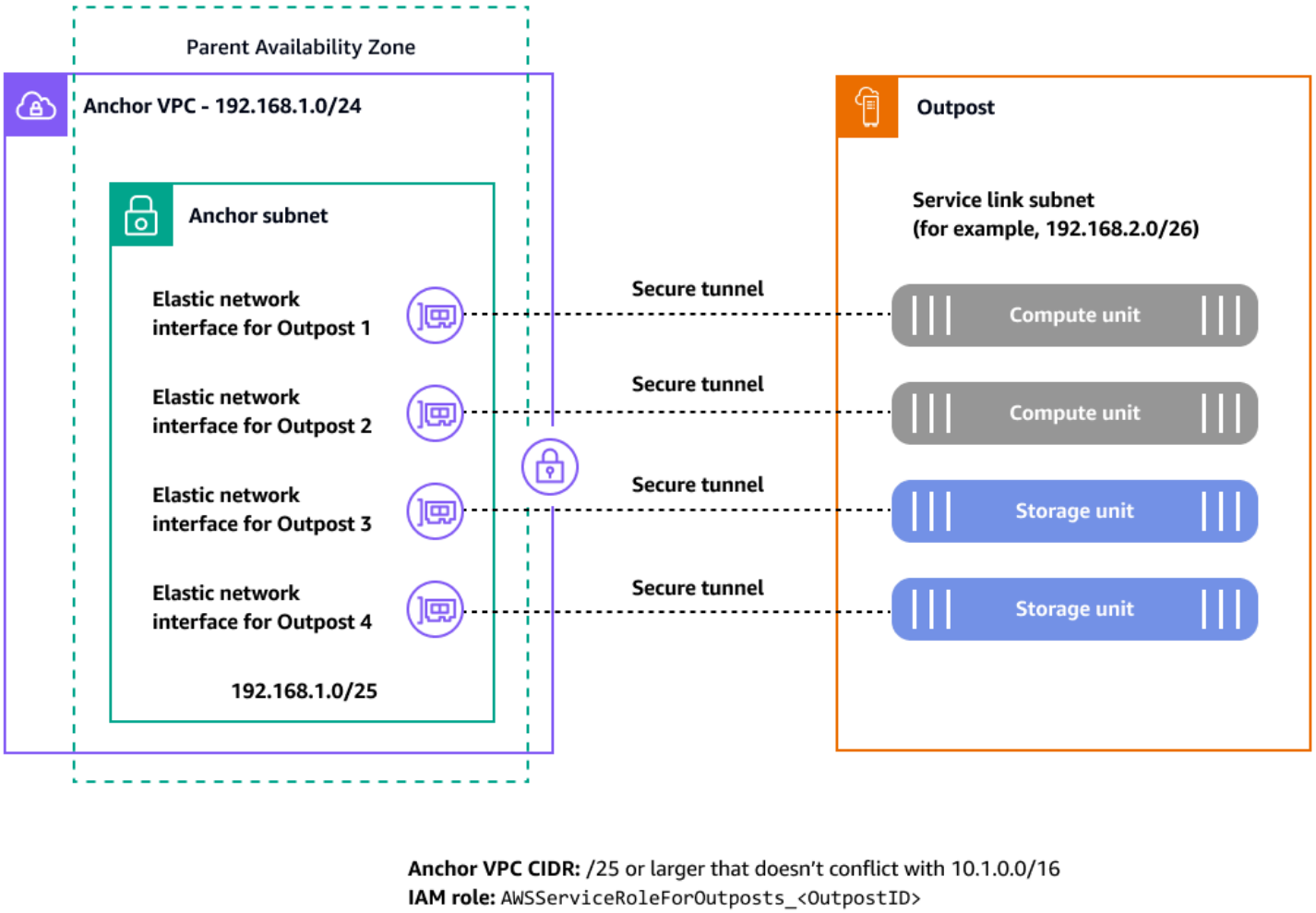
原定设置情况下，存储在 Amazon S3 on Outposts 中的所有数据都使用带 Amazon S3 托管式加密密钥 (SSE-S3) 的服务器端加密进行加密。您可以选择使用带客户提供的加密密钥的服务器端加密 (SSE-C)。要使用 SSE-C，请在对象 API 请求中指定加密密钥。服务器端加密仅加密对象数据而非加密对象元数据。

> **Note**
>
> Outposts 上的 Amazon S3 不支持使用 KMS 密钥 (SSE-KMS) 进行服务器端加密。

传输中加密

因为 AWS Outposts，服务链接是你的Outposts服务器和你选择的 AWS 区域 （或主区域）之间的必要连接，它允许管理前哨基地以及交换往返前哨的流量。 AWS 区域服务链接使用 AWS 托管 VPN 与本地区域通信。内部的每台主机都会 AWS Outposts 创建一组 VPN 隧道来分割控制平面流量和 VPC 流量。根据服务链路连接（互联网或 AWS Direct Connect）的不同 AWS Outposts，这些隧道需要打开防火墙端口，服务链路才能在其上创建叠加层。有关安全 AWS Outposts 性和服务链接的详细技术信息，请参阅 AWS Outposts 文档AWS Outposts中的通过服务链接连接和基础设施安全。

AWS Outposts 服务链路创建加密隧道，用于建立与父节点的控制平面和数据平面连接 AWS 区域，如下图所示。



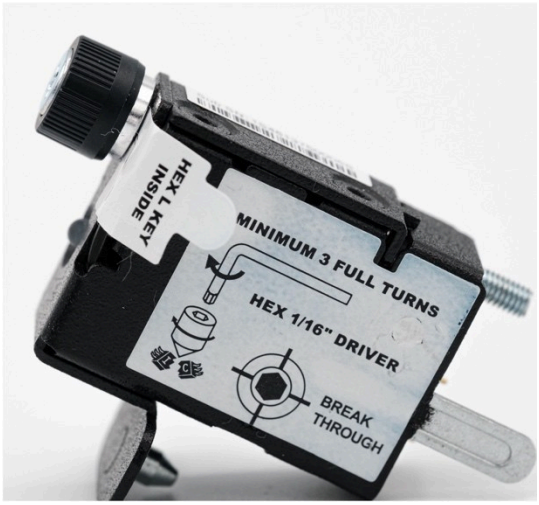
每 AWS Outposts 台主机（计算和存储）都需要这些通过众所周知的 TCP 和 UDP 端口的加密隧道才能与其父区域通信。下表显示了 UDP 和 TCP 协议的源和目标端口和地址。

协议	源端口	源地址	目的端口	目的地地址
UDP	443	AWS Outposts 服务链接 /26	443	AWS Outposts 区域的公共路由或锚点 VPC CIDR
TCP	1025-65535	AWS Outposts 服务链接 /26	443	AWS Outposts 区域的公共路由或锚点 VPC CIDR

Local Zones 还通过 Amazon 冗余且带宽极高的全球私有主干网连接到父区域。这种连接使在 Local Zones 中运行的应用程序可以快速、安全、无缝地访问其他应用程序 AWS 服务。只要 Local Zones 是 AWS 全球基础设施的一部分，所有流经 AWS 全球网络的数据都会在离开 AWS 安全设施之前在物理层自动加密。如果您对在本地位置之间传输的数据进行加密以及 AWS Direct Connect PoPs 访问本地区域有特定要求，则可以在本地路由器或交换机与 AWS Direct Connect 终端节点之间启用 MAC Security (MACsec)。有关更多信息，请参阅 AWS 博客文章为AWS Direct Connect 连接添加 MACsec 安全性。

数据删除

当您在中停止或终止 EC2 实例时 AWS Outposts，虚拟机管理程序会清理分配给该实例的内存（设置为零），然后再将其分配给新实例，并且每个存储块都会被重置。从 Outpost 硬件中删除数据需要使用专门的硬件。NSK是一种小型设备，如下图所示，它连接到前哨基地中每个计算或存储单元的正面。它旨在提供一种机制，防止您的数据从您的数据中心或托管站点暴露。Outpost 设备上的数据通过包装用于加密设备的密钥材料并将包装好的材料存储在 NSK 上来保护。当你返回 Outpost 主机时，你可以通过转动芯片上的小螺丝来摧毁 NSK，摧毁 NSK 并物理摧毁芯片。摧毁 NSK 会以加密方式粉碎你的前哨基地上的数据。



身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（拥有权限）使用 AWS Outposts 资源。如果您有 AWS 账户，则可以免费使用 IAM。

下表列出了您可以搭配使用的 IAM 功能 AWS Outposts。

IAM 功能	AWS Outposts 支持
基于身份的策略	是
基于资源的策略	是*
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
访问控制列表 (ACLs)	否
基于属性的访问控制 (ABAC)（策略中的标签）	是
临时凭证	是
主体权限	是
服务角色	否
服务相关角色	是

* 除了基于 IAM 身份的策略外，Outposts 上的 Amazon S3 还支持存储桶和接入点策略。这些是基于资源的政策，附在 Amazon S3 on Outposts 资源上。

有关中如何支持这些功能的更多信息 AWS Outposts，请参阅AWS Outposts 用户指南。

基础结构安全性

基础设施保护是信息安全计划的一个关键组成部分。它可确保工作负载系统和服务受到保护，防止意外和未经授权的访问以及潜在的漏洞。例如，您可以定义信任边界（例如，网络和帐户边界）、系统安全配置和维护（例如强化、最小化和修补）、操作系统身份验证和授权（例如用户、密钥和访问级别）以及其他相应的策略实施点（例如，Web 应用程序防火墙或 API 网关）。

AWS 提供了多种基础架构保护方法，如以下各节所述。

保护网络

您的用户可能是您的员工或客户的一员，并且可以位于任何地方。因此，您不能信任所有有权访问您的网络的人。当你遵循在所有层面应用安全的原则时，你就采用了零信任方法。在零信任安全模型中，应用程序组件或微服务被视为离散的，任何组件或微服务都不信任任何其他组件或微服务。要实现零信任安全，请遵循以下建议：

- 创建网络层。分层网络有助于对相似的网络组件进行逻辑分组。它们还缩小了未经授权的网络访问的潜在影响范围。
- 控制流量层。通过一种 defense-in-depth方法对入站和出站流量应用多种控制措施。这包括使用安全组（状态检查防火墙）、网络 ACLs、子网和路由表。
- 实施检查和保护。检查并过滤每层的流量。您可以使用网络访问分析器检查您的 VPC 配置是否存在潜在的意外访问。您可以指定您的网络访问要求并确定不符合这些要求的潜在网络路径。

保护计算资源

计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。每种计算资源类型都需要不同的安全方法。但是，这些资源确实共享您需要考虑的共同策略：深度防御、漏洞管理、减少攻击面、配置和操作自动化以及远距离执行操作。

以下是保护关键服务的计算资源的一般指南：

- 创建和维护漏洞管理程序。定期扫描和修补资源，例如 EC2 实例、亚马逊弹性容器服务 (Amazon ECS) 容器和亚马逊 Elastic Kubernetes Service (Amazon EKS) 工作负载。
- 自动计算保护。实现保护性计算机制的自动化，包括漏洞管理、减少攻击面和资源管理。这种自动化可以腾出时间来保护工作负载的其他方面，并有助于降低人为错误的风险。
- 减少攻击面。通过强化操作系统并最大限度地减少所使用的组件、库和外部可使用的服务，减少意外访问的风险。

此外，对于您 AWS 服务 使用的每种产品，请查看服务文档中的具体安全建议。

互联网访问

两者 AWS Outposts 和 Local Zones 都提供了架构模式，让您的工作负载可以访问和访问互联网。当你使用这些模式时，只有当你使用该区域来修补、更新、访问外部的 Git 存储库以及类似场景时，才将AWS该地区的互联网消费视为可行的选择。对于这种架构模式，集中式入站检查和集中式互联网出站

的概念适用。这些访问模式使用 AWS Transit Gateway NAT 网关、网络防火墙和其他组件，这些组件位于区域中 AWS 区域但通过区域和边缘之间的数据路径连接到 AWS Outposts 或 Local Zones。

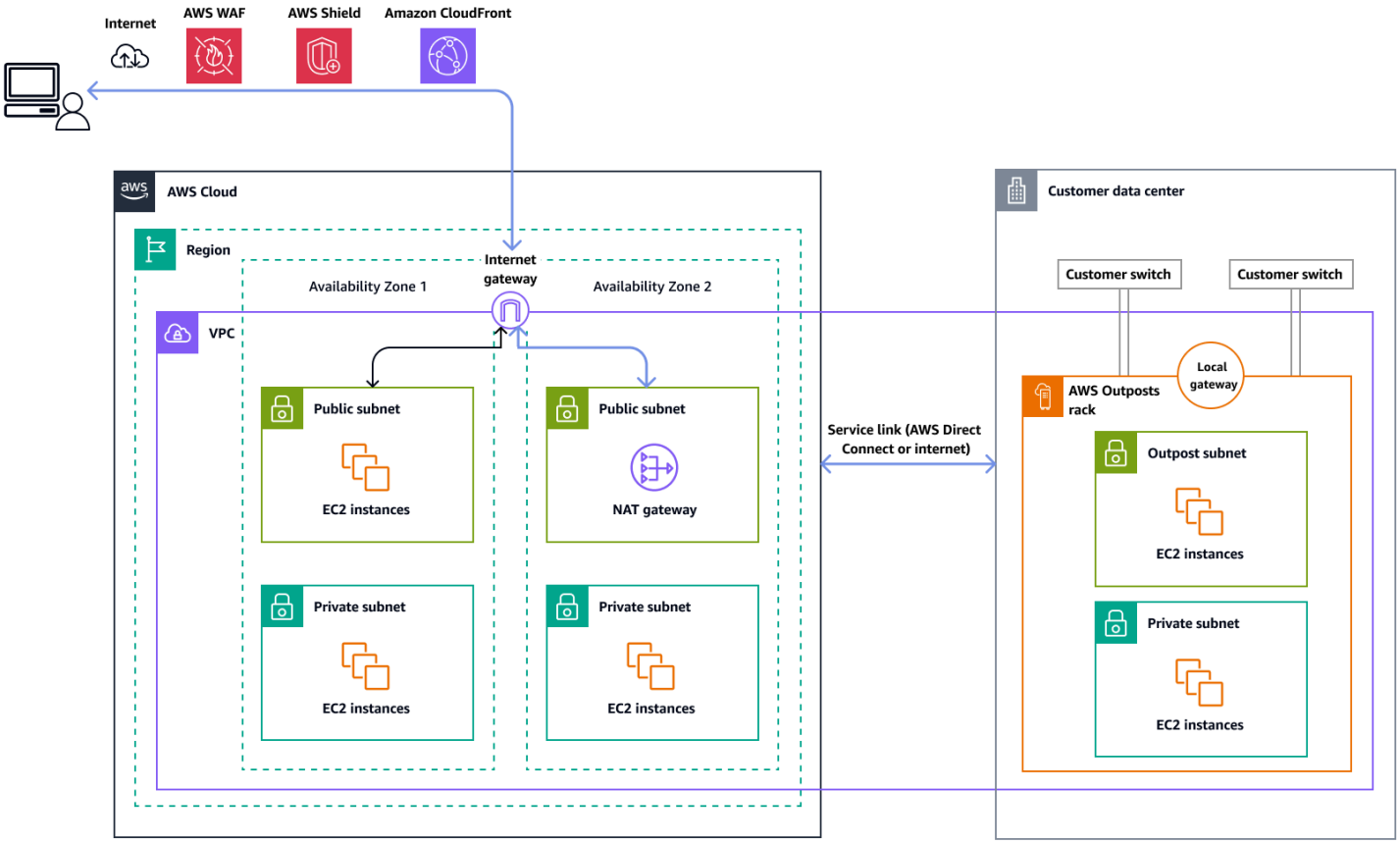
Local Zones 采用一种称为网络边界组的网络结构，用于 AWS 区域。 AWS 通告来自这些唯一群组的公有 IP 地址。网络边界组由可用区、Local Zones 或 Wavelength 区域组成。您可以明确分配公有 IP 地址池以用于网络边界组。您可以使用网络边界组将互联网网关扩展到 Local Zones，方法是允许该组提供弹性 IP 地址。此选项要求您部署其他组件来补充 Local Zones 中可用的核心服务。这些组件可能来自 ISVs 并帮助您在本地区域中构建检查层，如 AWS 博客文章《混合检查架构》中所述 AWS Local Zones。

在中 AWS Outposts，如果要使用本地网关 (LGW) 从您的网络访问 Internet，则必须修改与 AWS Outposts 子网关联的自定义路由表。路由表必须有一个使用 LGW 作为下一跳的默认路由条目 (0.0.0.0/0)。您负责在本地网络中实施其余的安全控制，包括外围防御，例如防火墙和入侵防御系统或入侵检测系统 (IPS/IDS)。这与责任共担模式一致，后者在您和云提供商之间划分安全职责。

通过家长上网 AWS 区域

在此选项中，Outpost 中的工作负载通过服务链接和父 AWS 区域站中的互联网网关访问互联网。互联网的出站流量可以通过在您的 VPC 中实例化的 NAT 网关进行路由。为了进一步保护您的入口和出口流量，您可以在 CloudFront 中使用 AWS 安全服务 AWS WAF，例如 AWS Shield、和 Amazon。AWS 区域

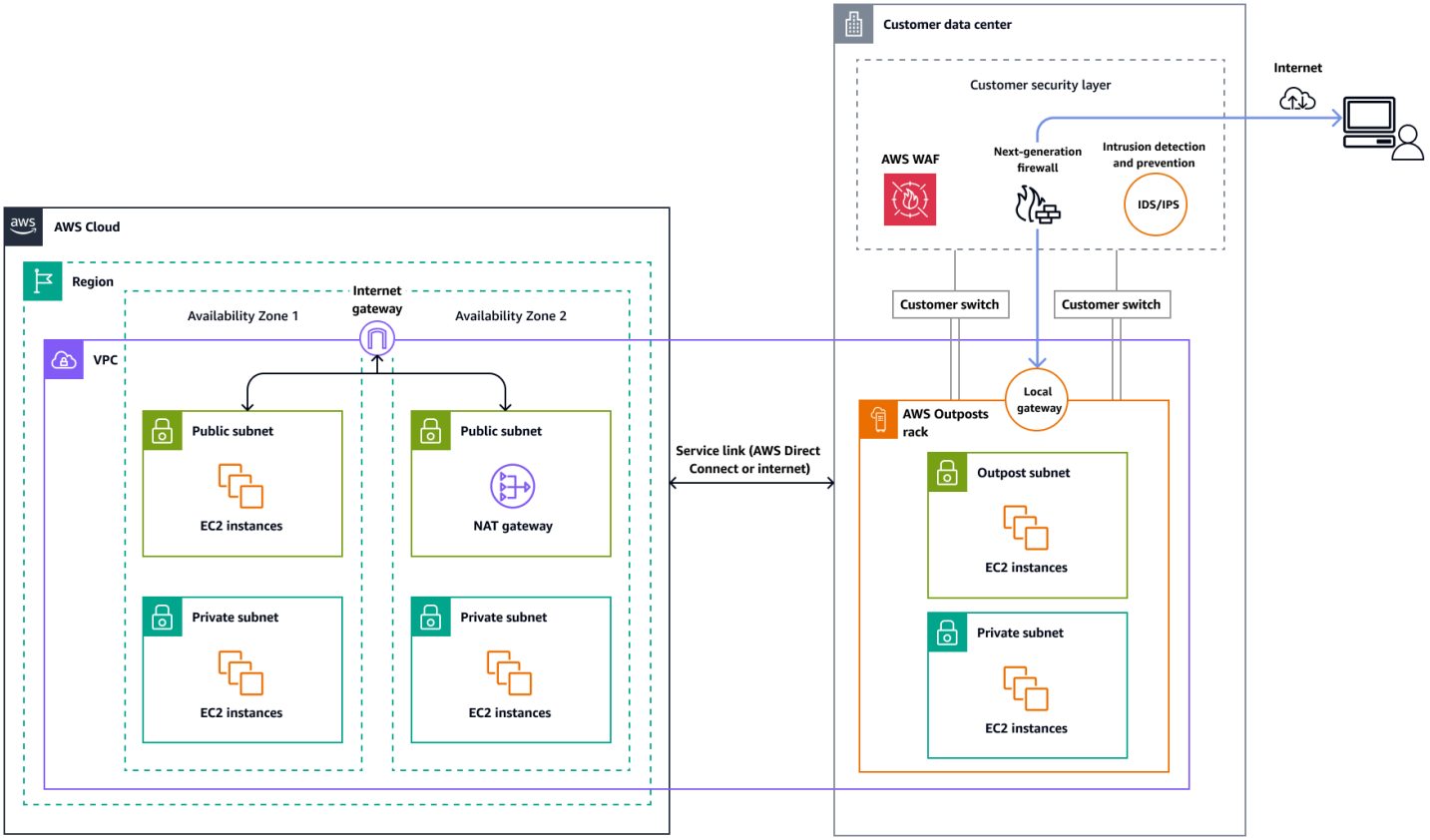
下图显示了实例中的工作负载与通过父 AWS Outposts 实例的 Internet 之间的流量 AWS 区域。



通过本地数据中心的网络访问互联网

在此选项中，Outpost 中的工作负载通过您的本地数据中心访问互联网。访问互联网的工作负载流量通过您的本地互联网接入点并在本地流出。在这种情况下，本地数据中心的网络安全基础设施负责保护 AWS Outposts 工作负载流量。

下图显示了 AWS Outposts 子网中的工作负载与通过数据中心的互联网之间的流量。



基础设施治理

无论您的工作负载是部署在 AWS 区域、本地区域还是 Outpost 中，您都可以使用它来 AWS Control Tower 管理基础架构。 AWS Control Tower 遵循规范性最佳实践，提供了一种设置和管理 AWS 多账户环境的简单方法。 AWS Control Tower 协调其他几项功能 AWS 服务，包括 AWS Organizations AWS Service Catalog、和 IAM Identity Center（查看所有集成服务），以便在不到一小时的时间内构建一个着陆区。资源是代表您设置和管理的。

AWS Control Tower 提供跨所有 AWS 环境的统一管理，包括区域、Local Zones（低延迟扩展）和 Outposts（本地基础架构）。这有助于确保整个混合云架构始终如一的安全性和合规性。有关更多信息，请参阅 AWS Control Tower 文档。

您可以配置护栏等功能，以符合政府 AWS Control Tower 和监管行业（如金融服务机构）的数据驻留要求（ ）FSIs。要了解如何为边缘数据驻留部署护栏，请参阅以下内容：

- AWS Local Zones 使用 landing zone 控件管理数据驻留的最佳实践（AWS 博客文章）
- 使用机架和 landing zone 护栏设计数据驻留 AWS Outposts 架构（AWS 博客文章）
- 混合云服务视角下的数据驻留（Well-Architect AWS ed Framework 文档）

共享 Outposts 资源

由于 Outpost 是一种有限的基础架构，位于您的数据中心或托管空间中，因此要进行集中管理 AWS Outposts，您需要集中控制与哪些账户共享 AWS Outposts 资源。

通过 Outpost 共享，Outpost 所有者可以与同一组织中的其他 AWS 账户 人共享他们的 Outposts 和 Outpost 资源，包括前哨基地和子网。 AWS Organizations作为 Outpost 所有者，您可以从一个中心位置创建和管理 Outpost 资源，并在组织 AWS 账户 内的多个位置共享资源。 AWS 这允许其他用户使用 Outpost 站点，在共享的 Outpost 上配置 VPCs、启动和运行实例。

中的可共享资源 AWS Outposts 有：

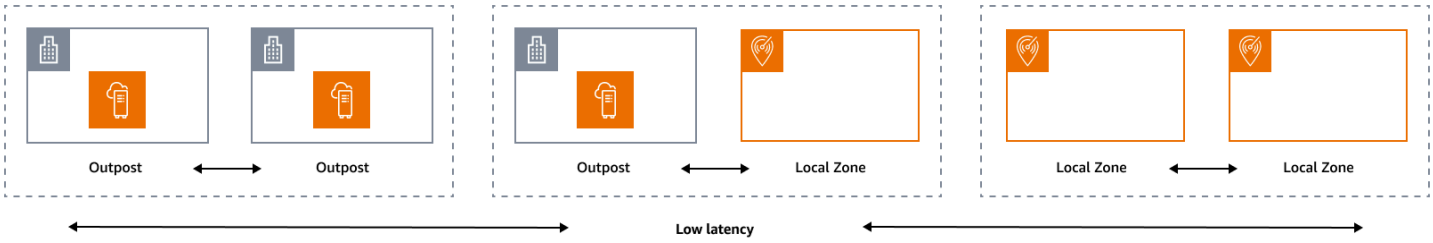
- 已分配的专用主机
- 容量预留
- 客户拥有的 IP (CoIP) 地址池
- 本地网关路由表
- Outposts
- Amazon S3 on Outposts
- 站点
- 子网

要遵循在多账户环境中共享 Outposts 资源的最佳做法，请参阅以下 AWS 博客文章：

- AWS Outposts 在多账户 AWS 环境中共享：第 1 部分
- AWS Outposts 在多账户 AWS 环境中共享：第 2 部分

边缘弹性

可靠性支柱包括工作负载在预期时正确、一致地执行其预期功能的能力。这包括能够在工作负载的整个生命周期中对其进行操作和测试。从这个意义上讲，在边缘设计弹性架构时，必须首先考虑将使用哪些基础架构来部署该架构。使用 AWS Local Zones 和可以实现三种可能的组合 AWS Outposts：前哨基地到前哨基地、前哨基地到本地区域以及本地区域到局域区域，如下图所示。尽管弹性架构还有其他可能性，例如将 AWS 边缘服务与传统的本地基础设施相结合 AWS 区域，或者，本指南重点介绍适用于混合云服务设计的这三种组合



基础架构注意事项

在 AWS，服务设计的核心原则之一是避免底层物理基础架构出现单点故障。由于这一原则， AWS 软件和系统使用多个可用区，并且能够抵御单个区域的故障。在边缘， AWS 提供基于 Local Zones 和 Outposts 的基础架构。因此，确保基础设施设计弹性的关键因素是定义应用程序资源的部署位置。

Local Zones

Local Zones 的作用与其中的可用区域类似 AWS 区域，因为可以选择它们作为子网和 EC2 实例等区域 AWS 资源的放置位置。但是，它们不在人口稠密 AWS 区域的工业和IT中心附近，而是在当今不 AWS 区域 存在的地方。尽管如此，它们仍然在本地区域中的本地工作负载与在本地区域中运行的工作负载之间保持高带宽的安全连接。 AWS 区域因此，您应该使用 Local Zones 将工作负载部署到离用户更近的地方，以满足低延迟要求。

Outposts

AWS Outposts 是一项完全托管的服务，可将 AWS 基础架构 AWS 服务 APIs、、和工具扩展到您的数据中心。您的数据中心安装的硬件基础设施与中 AWS Cloud 使用的硬件基础架构相同。然后，Outposts 与最近的哨所相连。 AWS 区域您可以使用 Outposts 来支持具有低延迟或本地数据处理要求的工作负载。

父可用区

每个本地区域或前哨基地都有一个父区域（也称为主区域）。父区域是 AWS 边缘基础设施（前哨基地或本地区域）的控制平面的锚定区域。就本地区域而言，父区域是本地区域的基本架构组件，客户无法对其进行修改。 AWS Outposts 将扩展 AWS Cloud 到您的本地环境，因此您必须在订购过程中选择特定的区域和可用区。此选项可将 Outposts 部署的控制平面锚定到所 AWS 选基础架构。

在边缘开发高可用性架构时，这些基础设施的父区域（例如 Outposts 或 Local Zones）必须相同，以便可以在它们之间扩展 VPC。这种扩展的 VPC 是创建这些高可用性架构的基础。在定义高弹性架构时，这就是为什么必须验证父区域和服务将（或已停靠）的区域的可用区。如下图所示，如果您想在两个 Outposts 之间部署高可用性解决方案，则必须选择两个不同的可用区来锚定 Outposts。这允许从控

制平面角度实现多可用区架构。如果要部署包含一个或多个 Local Zones 的高可用性解决方案，则必须首先验证基础架构所在的父可用区。为此，请使用以下 AWS CLI 命令：

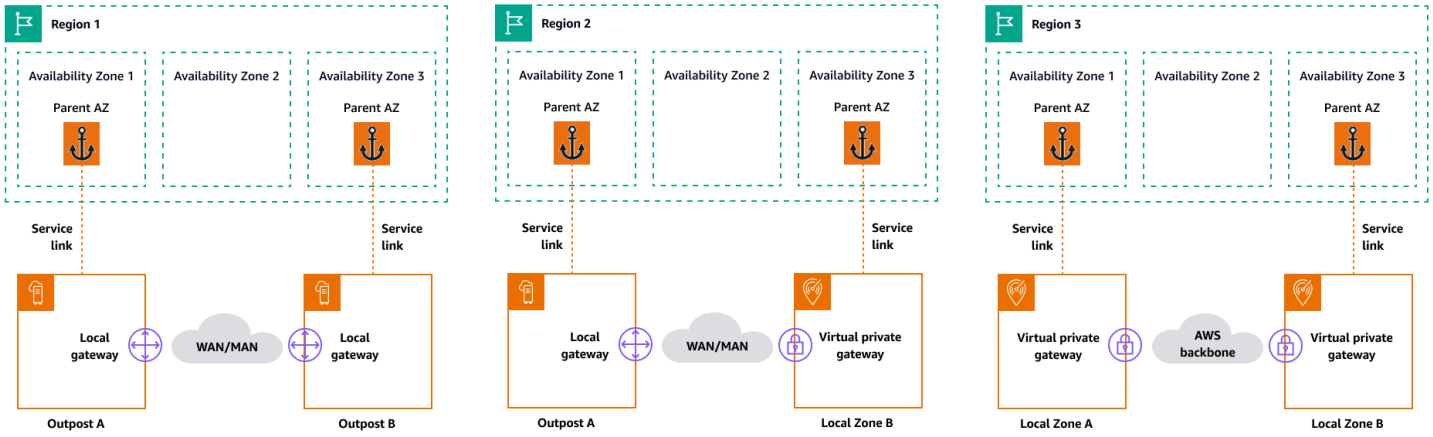
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

上一个命令的输出：

```
{     "AvailabilityZones": [
          {
              "State": "available",
              "OptInStatus": "opted-in",
              "Messages": [],
              "RegionName": "us-east-1",
              "ZoneName": "us-east-1-mia-1a",
              "ZoneId": "use1-mia1-az1",
              "GroupName": "us-east-1-mia-1",
              "NetworkBorderGroup": "us-east-1-mia-1",
              "ZoneType": "local-zone",
              "ParentZoneName": "us-east-1d",
              "ParentZoneId": "use1-az2"
          }
      ]
 }
```

在此示例中，迈阿密本地区域 (us-east-1d-mia-1a1) 锚定在us-east-1d-az2可用区中。因此，如果您需要在边缘创建弹性架构，则必须确保辅助基础架构（Outposts 或 Local Zones）锚定到除之外的可用区。**us-east-1d-az2**例如，us-east-1d-az1将是有效的。

下图提供了高可用性边缘基础设施的示例。



联网注意事项

本节讨论边缘联网的初步注意事项，主要是访问边缘基础设施的连接。它审查了为服务链路提供弹性网络的有效架构。

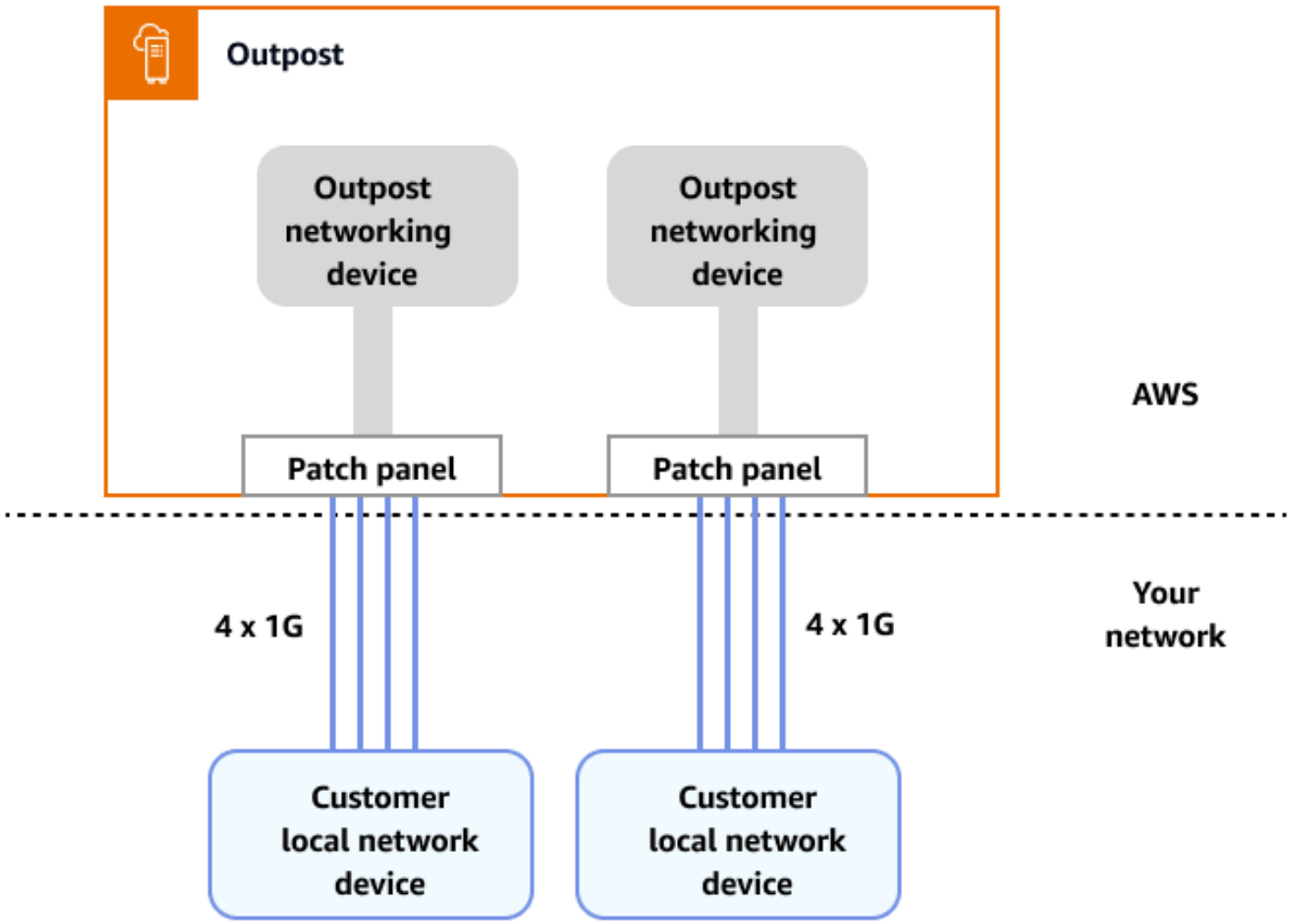
Local Zones 的弹性网络

Local Zones 通过多个冗余、安全、高速的链路连接到父区域，使您能够无缝使用任何区域服务，例如 Amazon S3 和 Amazon RDS。您负责提供从您的本地环境或用户到本地区域的连接。无论您选择哪种连接架构（例如，VPN 或 AWS Direct Connect），通过网络链路实现的延迟都必须相同，以避免在主链路出现故障时对应用程序性能产生任何影响。如果您正在使用 AWS Direct Connect，则适用的弹性架构与用于访问的弹性架构相同 AWS 区域，如AWS Direct Connect 弹性建议中所述。但是，有些场景主要适用于国际 Local Zones。在启用本地区域的国家/地区，只有一个 AWS Direct Connect PoP 就无法创建推荐的 AWS Direct Connect 弹性架构。如果您只能访问单个 AWS Direct Connect 位置或需要单一连接以外的弹性，则可以在 Amazon EC2 上创建 VPN 设备 AWS Direct Connect，如 AWS 博客文章启用从本地到 AWS Local Zones的高可用性连接中所说明和讨论的那样。

Outposts 的弹性网络

与 Local Zones 形成鲜明对比的是，Outposts 具有冗余连接，可以从本地网络访问部署在 Outposts 中的工作负载。这种冗余是通过两台 Outposts 网络设备实现的 () ONDs。每个 OND 需要至少两个 1 Gbps、10 Gbps、40 Gbps 或 100 Gbps 的光纤连接到您的本地网络。必须将这些连接配置为链路聚合组 (LAG)，以允许以可扩展的方式添加更多链路。

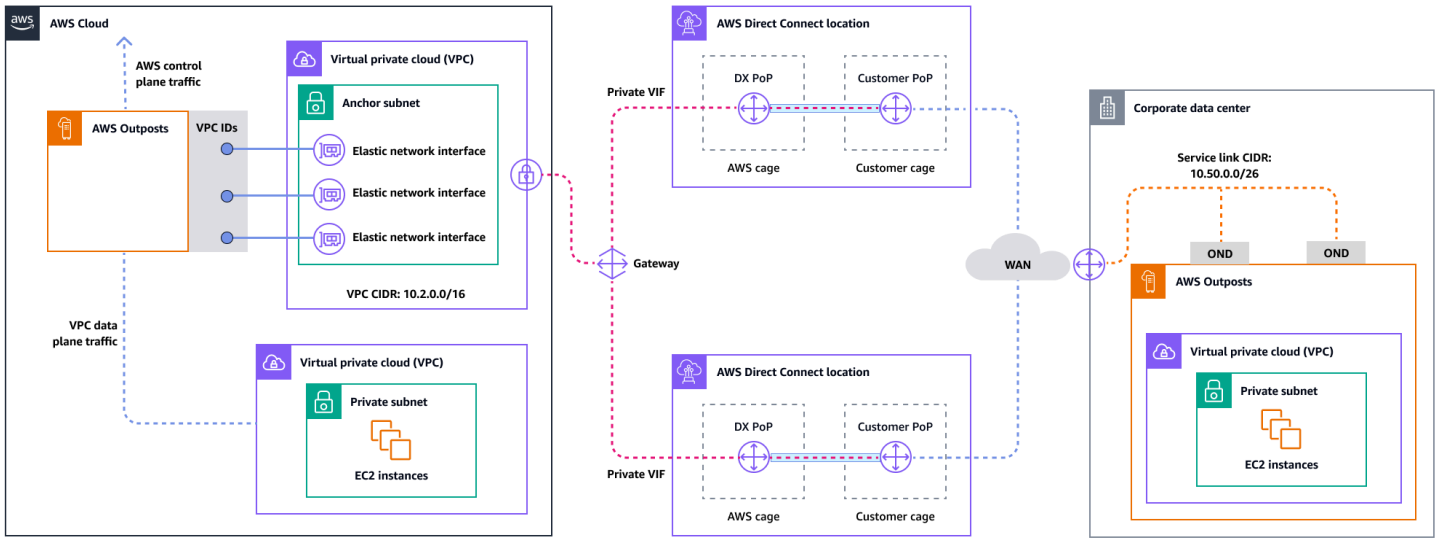
上行链路速度	上行链路数量
1 Gbps	1、2、4、6 或 8
10 Gbps	1、2、4、8、12 或 16
40 或 100 Gbps	1、2 或 4



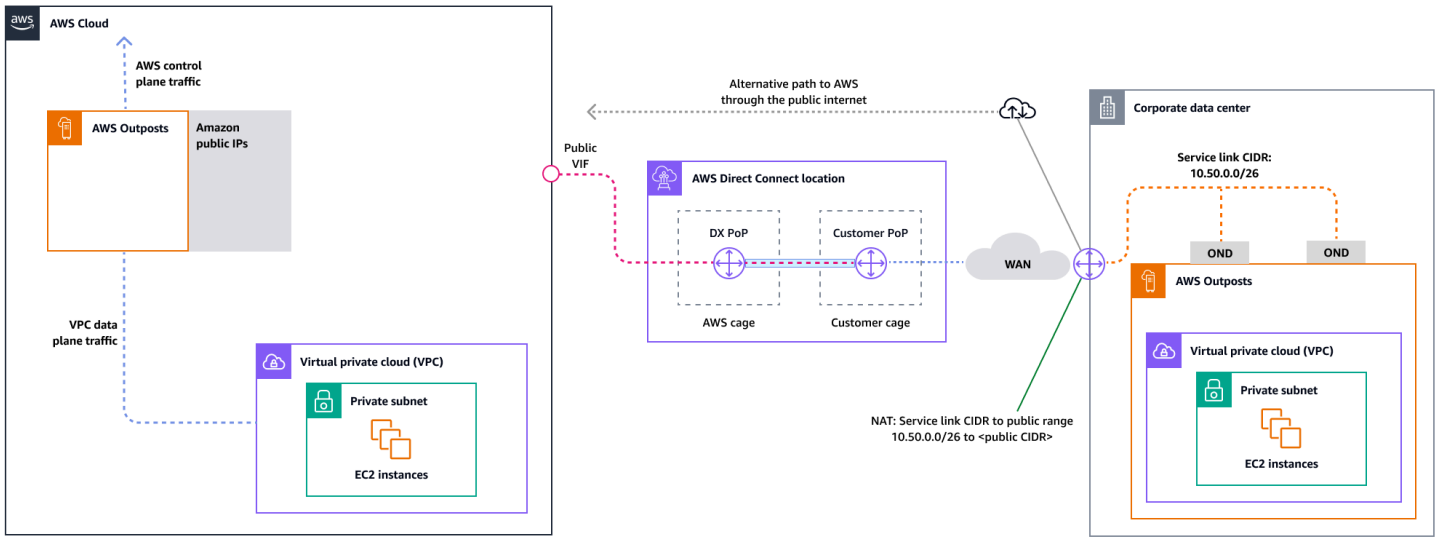
有关此连接的更多信息，请参阅文档中的 Outposts Racks 的本地网络连接。 AWS Outposts

为了获得最佳体验和弹性， AWS建议您使用至少 500 Mbps（更好 1 Gbps）的冗余连接来连接到。 AWS 区域您可以使用 AWS Direct Connect 或互联网连接来获取服务链接。此最低限度使您能够启动 EC2 实例、附加 EBS 卷和访问 AWS 服务，例如 Amazon EKS、Amazon EMR 和指标。 CloudWatch

下图说明了这种用于高可用性专用连接的架构。



下图说明了这种用于高可用性公共连接的架构。

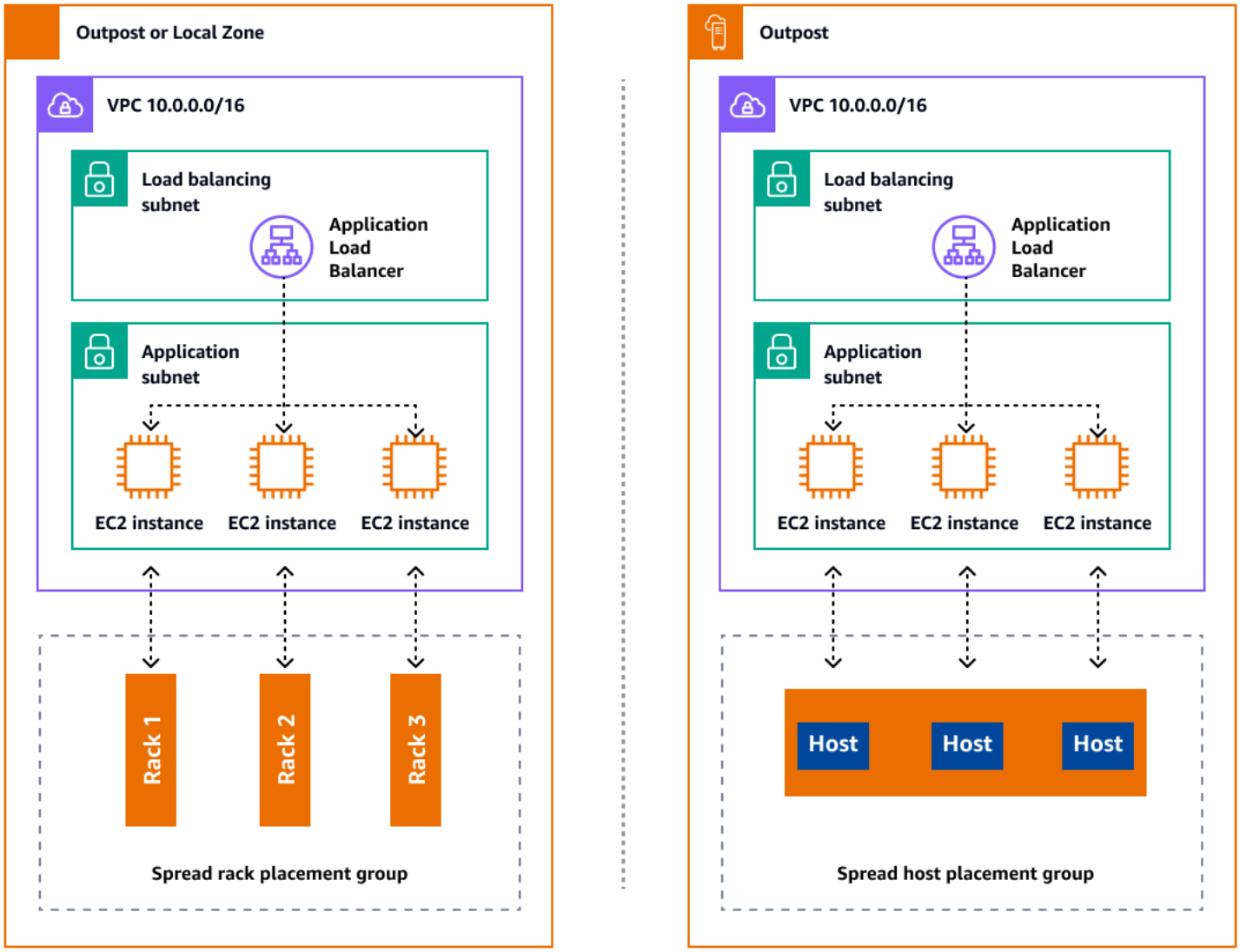


使用 ACE 机架扩展 Outposts 机架部署

聚合、核心、边缘 (ACE) 机架是 AWS Outposts 多机架部署的关键聚合点，主要推荐用于超过三个机架的安装或计划未来的扩展。每个 ACE 机架都有四台路由器，支持 10 Gbps、40 Gbps 和 100 Gbps 连接（100 Gbps 是最佳选择）。每个机架最多可连接四台上游客户设备，以实现最大冗余。ACE 机架消耗高达 10 kVA 的功率，重量可达 705 磅。主要优势包括降低物理网络需求、减少光纤布线上行链路以及减少 VLAN 虚拟接口。 AWS 通过 VPN 隧道通过遥测数据监控这些机架，并在安装过程中与客户密切合作，以确保适当的电源可用性、网络配置和最佳位置。随着部署规模的扩大，ACE 机架架构提供了不断增长的价值，并有效地简化了连接，同时降低了大型安装的复杂性和物理端口要求。 有关更多信息，请参阅 AWS 博客文章使用 ACE Rac AWS Outposts k 扩展机架部署。

在 Outposts 和 Local Zones 之间分配实例

Outposts 和 Local Zones 的计算服务器数量有限。如果您的应用程序部署了多个相关实例，则这些实例可能会部署在同一台服务器上或同一机架中的服务器上，除非它们的配置不同。除了默认选项外，您还可以跨服务器分配实例，以降低在同一基础架构上运行相关实例的风险。您还可以使用分区置放群组将实例分配到多个机架上。这称为展架分销模型。使用自动分配将实例分布到组中的各个分区，或者将实例部署到选定的目标分区。通过将实例部署到目标分区，您可以将选定的资源部署到同一个机架，同时在机架之间分配其他资源。Outpo sts 还提供了另一种名为 spre ad host 的选项，它允许你在主机级别分配工作负载。下图显示了分散机架和分散主机的分发选项。



Amazon RDS 中的多可用区 AWS Outposts

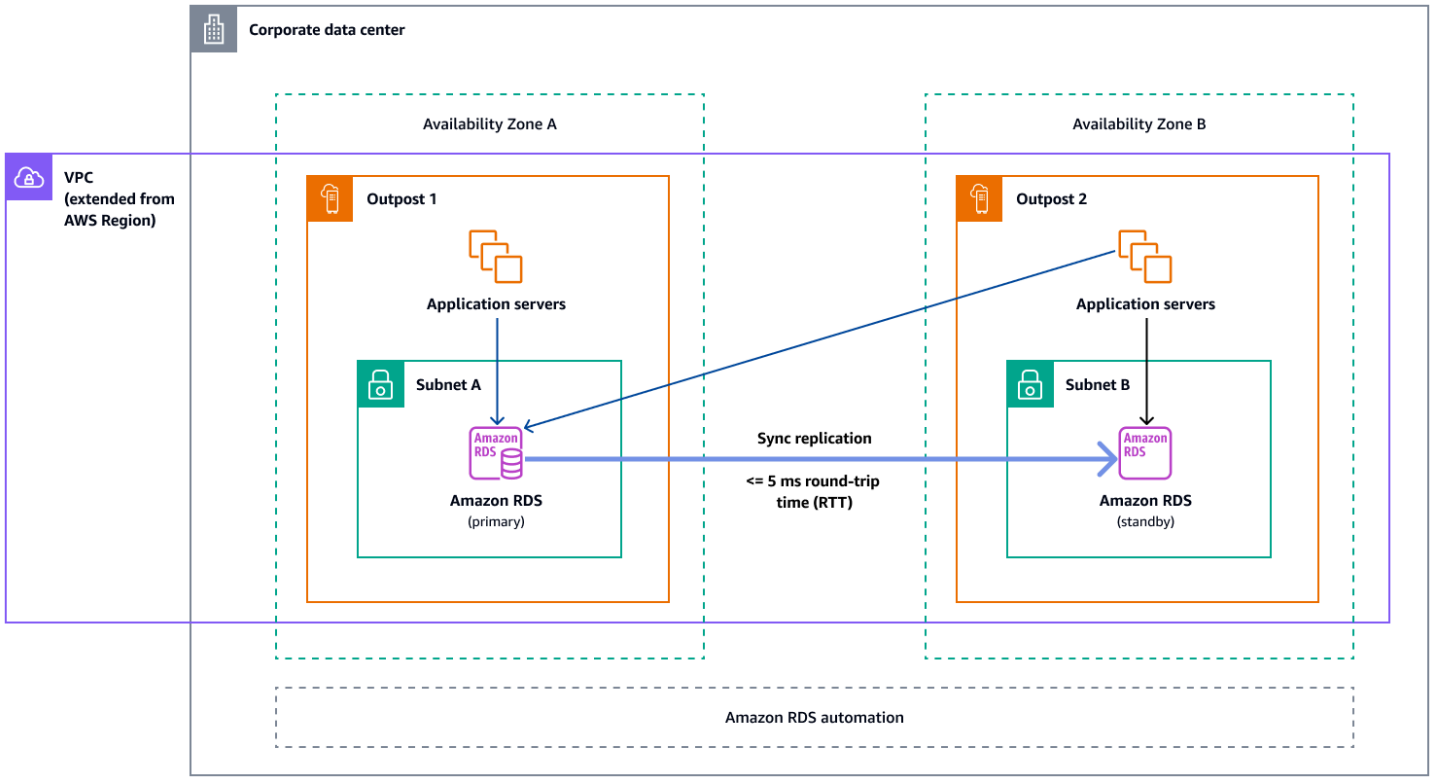
当您在 Outposts 上使用多可用区实例部署时，Amazon RDS 会在两个 Outposts 上创建两个数据库实例。每个 Outpost 都运行在自己的物理基础设施上，并连接到一个区域中的不同可用区以实现高可用

性。当两个 Outposts 通过客户管理的本地连接连接时，Amazon RDS 会管理主数据库实例和备用数据库实例之间的同步复制。如果软件或基础设施出现故障，Amazon RDS 会自动将备用实例提升为主角色，并更新 DNS 记录以指向新的主实例。对于多可用区部署，Amazon RDS 会在一个 Outpost 上创建主数据库实例，并将数据同步复制到不同 Outpost 上的备用数据库实例。Outposts 上的多可用区部署与 AWS 区域中的多可用区部署类似，但有以下区别：

- 它们需要两个或更多 Outposts 之间的本地连接。
- 它们需要客户拥有的 IP (CoIP) 地址池。有关更多信息，请参阅 Amazon RDS 文档 AWS Outposts 中的客户拥有的 Amazon RDS 的 IP 地址。
- 复制在您的本地网络上运行。

Outposts 上的 Amazon RDS 上所有支持的 MySQL 和 PostgreSQL 版本均支持多可用区部署。多可用区部署不支持本地备份。

下图显示了 Outposts 上的 Amazon RDS 多可用区配置的架构。

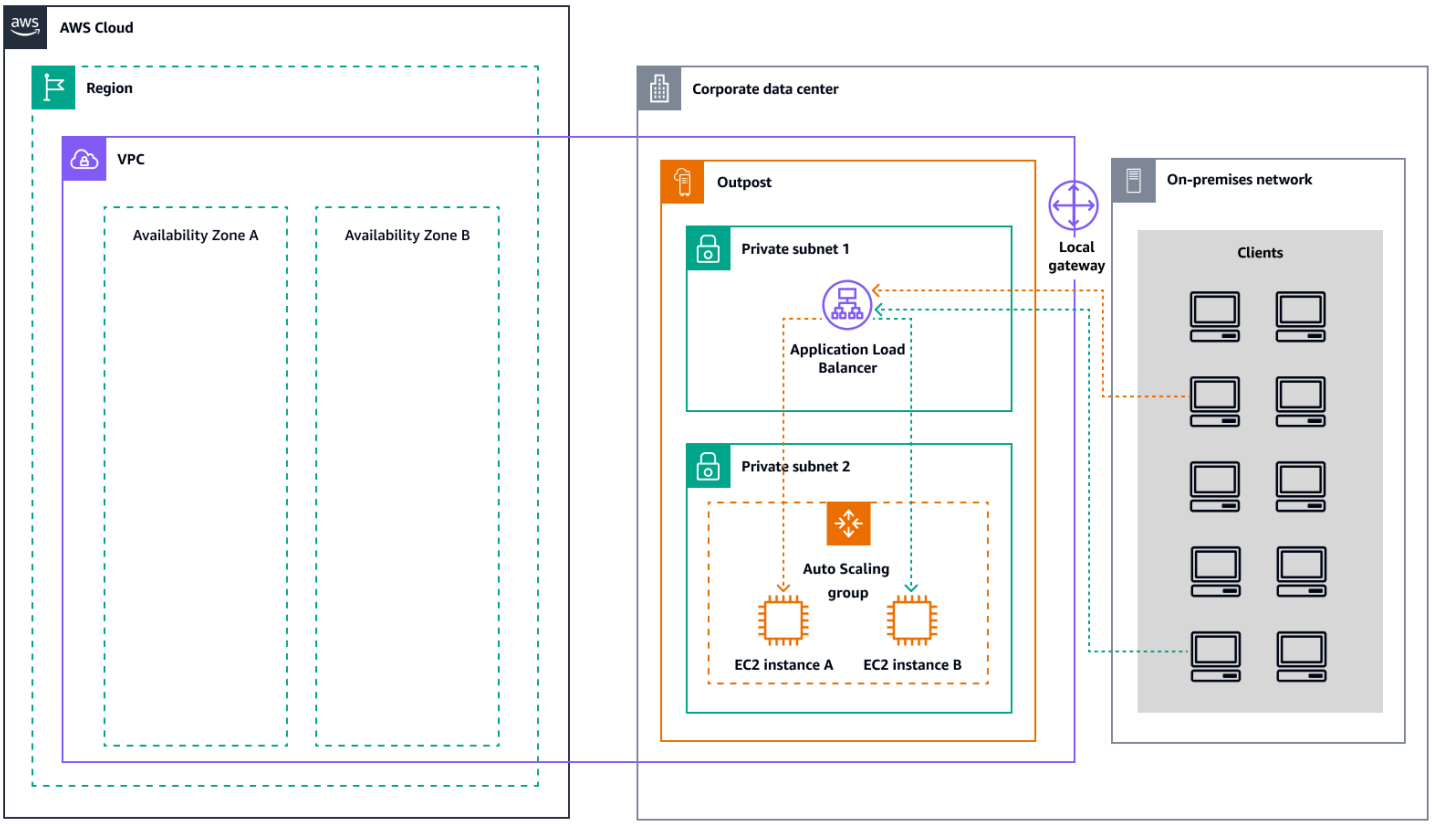


故障转移机制

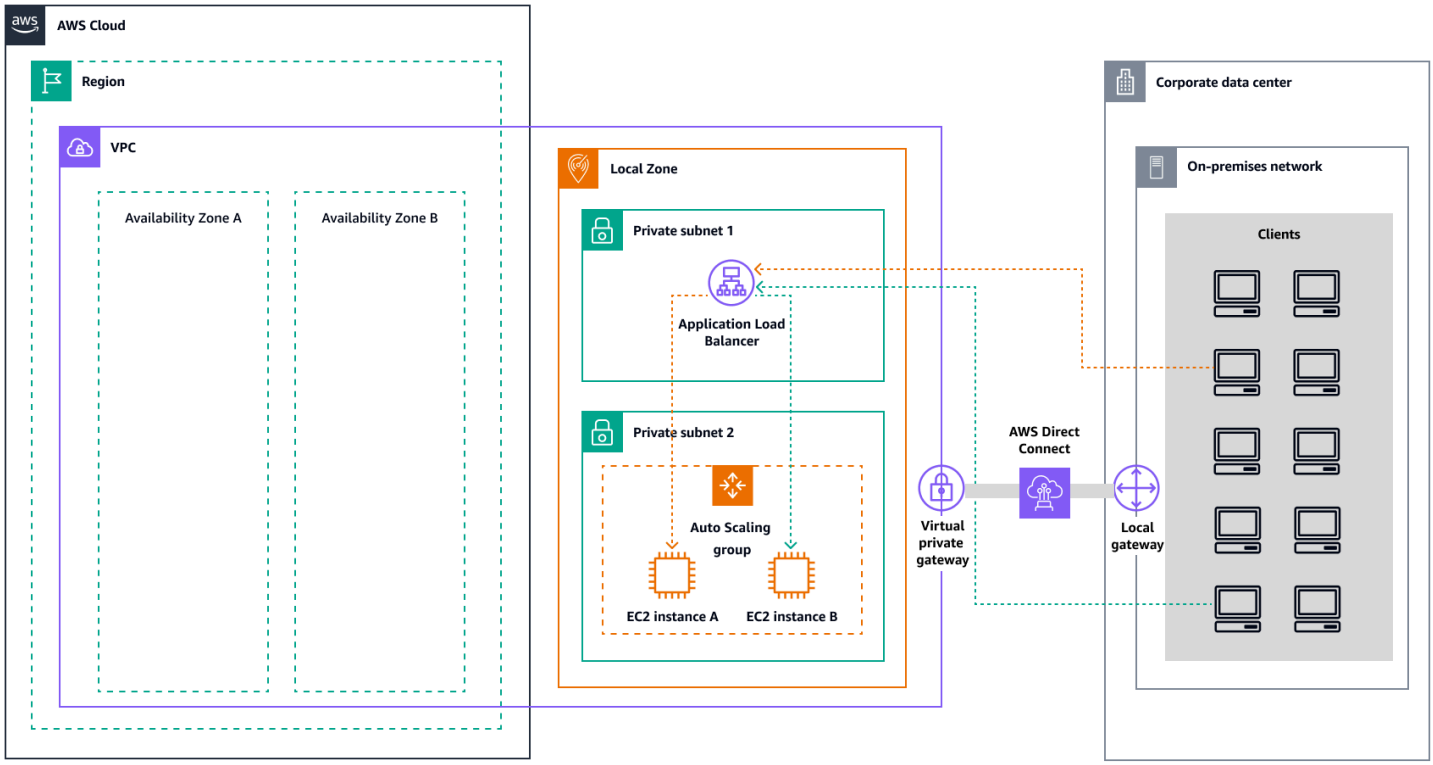
负载平衡和自动扩展

Elastic Load Balancing (ELB) 会自动将您的传入应用程序流量分配到您正在 EC2 运行的所有实例。ELB 通过优化流量路由来帮助管理传入的请求，这样就不会让单个实例不堪重负。要将 ELB 与您的 Amazon A EC2 uto Scaling 组一起使用，请将负载均衡器附加到您的 Auto Scaling 组。这会将群组注册到负载均衡器，负载均衡器充当您的群组所有传入 Web 流量的单一联系点。在 Auto Scaling 组中使用 ELB 时，无需向负载均衡器注册单个 EC2 实例。您的 Auto Scaling 组所启动的实例会自动注册到负载均衡器。同样，由您的 Auto Scaling 组终止的实例将自动从负载均衡器注销。将负载均衡器连接到 Auto Scaling 组后，您可以将您的组配置为使用 ELB 指标（例如每个目标的 Application Load Balancer 请求数）来根据需求波动扩展组中的实例数量。或者，您可以将 ELB 运行状况检查添加到您的 Auto Scaling 组中，这样 Amazon A EC2 uto Scaling 就可以根据这些运行状况检查识别和替换运行状况不佳的实例。您也可以创建一个 Amazon CloudWatch 警报，当目标组的健康主机数低于允许值时，该警报会通知您。

下图说明了 Application Load Balancer 如何在 EC2 中管理 Amazon 上的工作负载 AWS Outposts。



下图说明了 Local Zones EC2 中亚马逊的类似架构。

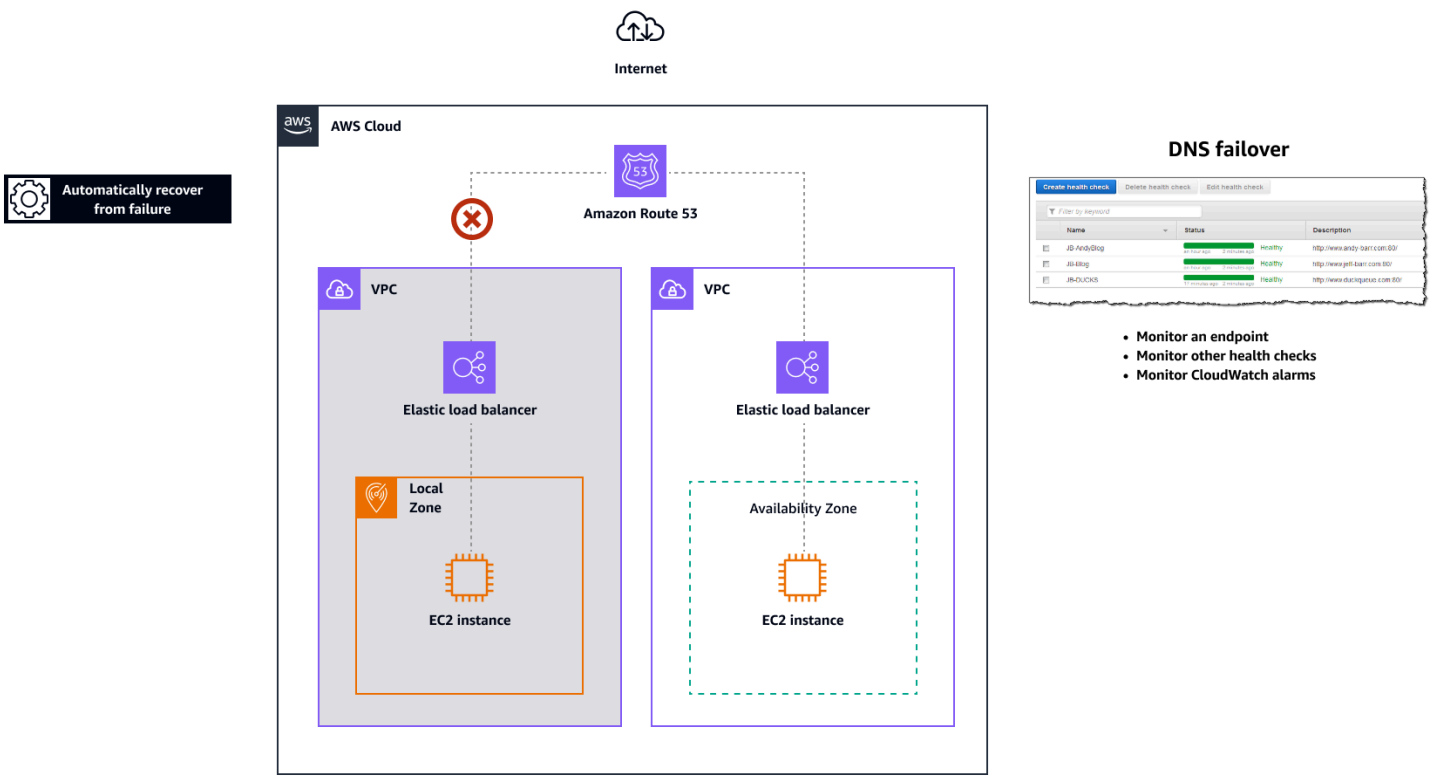


> **Note**
>
> 应用程序负载均衡器在 Local Zones AWS Outposts 和 Local Zones 中均可用。但是，要在中使用 Application Load Balancer AWS Outposts，您需要调整 Amazon EC2 容量的大小，以提供负载均衡器所需的可扩展性。有关调整负载均衡器大小的更多信息 AWS Outposts，请参阅上的 “配置 Application Load Balan cer” 的 AWS 博客文章 AWS Outposts。

用于 DNS 故障转移的亚马逊 Route 5

当您有多个资源执行相同的功能（例如多个 HTTP 或邮件服务器）时，您可以将 Amazon Rou te 53 配置为仅使用运行状况良好的资源来检查资源的运行状况并响应 DNS 查询。例如，假设您的网站托管在两台服务器上。`example.com`一台服务器在本地区域中，另一台服务器位于前哨基地。您可以将 Route 53 配置为仅使用当前运行状况的服务器来检查这些服务器的`example.com`运行状况并响应 DNS 查询。如果您使用别名记录将流量路由到选定 AWS 资源（例如 ELB 负载均衡器），则可以配置 Route 53 以评估资源的运行状况，并仅将流量路由到运行状况良好的资源。配置别名记录以评估资源的运行状况时，无需为该资源创建运行状况检查。

下图说明了 Route 53 的故障转移机制。



> **备注**
>
> - 如果您在私有托管区域中创建故障转移记录，则可以创建 CloudWatch 指标，将警报与指标相关联，然后根据警报的数据流创建运行状况检查。
> - 要使用 Application Load Balancer 在中 AWS Outposts 公开访问应用程序，请设置网络配置，启用从公共 IPs 到负载均衡器的完全限定域名 (FQDN) 的目标网络地址转换 (DNAT)，并使用指向暴露的公有 IP 的运行状况检查创建 Route 53 故障转移规则。这种组合可确保公众可靠地访问您的 Outposts 托管的应用程序。

Amazon Route 53 Resolver on AWS Outposts

Amazon Route 53 Resolver可在 Outposts 机架上使用。它直接从 Outposts 为您的本地服务和应用程序提供本地 DNS 解析。本地 Route 53 解析器端点还支持 Outposts 和你的本地 DNS 服务器之间的 DNS 解析。Outposts 上的 Route 53 Resolver 有助于提高本地应用程序的可用性和性能。

Outposts 的典型用例之一是部署需要低延迟访问本地系统的应用程序，例如工厂设备、高频交易应用程序和医疗诊断系统。

当你选择在 Outposts 上使用本地 Route 53 解析器时，应用程序和服务将继续受益于本地 DNS 解析来发现其他服务，即使与 AWS 区域 父级的连接中断。本地解析器还有助于缩短 DNS 解析的延迟，因为查询结果是从 Outposts 本地缓存和提供的，从而消除了前往父节点的不必要往返行程。 AWS 区域 Outposts 中使用私有 DNS 的应用程序 VPCs 的所有 DNS 解析都是在本地提供的。

除了启用本地解析器外，此次启动还启用了本地解析器端点。Route 53 解析器出站终端节点允许 Route 53 解析器将 DNS 查询转发给您管理的 DNS 解析器，例如在您的本地网络上。相比之下，Route 53 Resolver 入站终端节点会将他们从 VPC 外部收到的 DNS 查询转发给在 Outposts 上运行的解析器。它允许您从该私有 Outposts VPC 外部为部署在私有 Outposts VPC 上的服务发送 DNS 查询。有关入站和出站终端节点的更多信息，请参阅 Route 53 文档中的解析 VPCs 与您的网络之间的 DNS 查询。

边缘容量规划

容量规划阶段包括收集部署架构的 vCPU、内存和存储需求。在Well-Ar chitecte AWS d Framewor k的成本优化支柱中，调整规模是一个持续的过程，从规划开始。您可以使用 AWS 工具根据内部 AWS的资源消耗来定义优化。

Local Zones 中的边缘容量规划与中的相同 AWS 区域。您应该检查以确保您的实例在每个本地区域中都可用，因为某些实例类型可能与中的类型不同 AWS 区域。对于 Outposts，你应该根据自己的工作量要求来规划容量。Outposts 的插槽中每台主机的实例数是固定的，可以根据需要重新分配。如果您的工作负载需要备用容量，请在规划容量需求时将其考虑在内。

Outposts 的容量规划

AWS Outposts 容量规划需要为区域规模调整提供具体的投入，以及影响应用程序可用性、性能和增长的特定边缘因素。有关详细指导，请参阅 AWS 白皮书《AWS Outposts 高可用性设计和架构注意事项》中的容量规划。

Local Zones 的容量规划

本地区域是地理位置靠近您的用户的扩展。 AWS 区域 在本地区域中创建的资源可以为本地用户提供延迟极低的通信。要在您的中启用本地区域 AWS 账户，请查看 AWS 文档 AWS Local Zones中的入门指南。每个本地区域都有不同的插槽可供 EC2 实例系列使用。在使用这些实例之前，请先验证每个本地区域中的可用实例。要确认可用 EC2 实例，请运行以下 AWS CLI 命令：

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
--filters Name=location,Values=<local-zone-name>
```

预期输出：

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "availability-zone",
          "Location": "<local-zone-name>"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "availability-zone",
          "Location": "local.zone-name"
      },
      ...
  ]
}
```

边缘基础设施管理

AWS 提供完全托管的服务，可将 AWS 基础架构 APIs、服务和工具扩展到更靠近最终用户和数据中心的距离。Outposts 和 Local Zones 中提供的服务与中提供的服务相同 AWS 区域，因此您可以使用相同的 AWS 控制台 AWS CLI、或来管理这些服务。 AWS APIs有关支持的服务，请参阅AWS Outposts 功能比较表和AWS Local Zones 功能。

在边缘部署服务

您可以按照与配置相同的方式在 Local Zones 和 Outposts 中配置可用服务 AWS 区域：使用 AWS 控制台 AWS CLI、或。 AWS APIs区域部署和边缘部署之间的主要区别在于将在哪些子网中配置资源。边缘网络部分描述了如何在 Outposts 和 Local Zones 中部署子网。识别边缘子网后，您可以使用边缘子网 ID 作为参数在 Outposts 或 Local Zones 中部署服务。以下各节提供了部署边缘服务的示例。

EC2 处于边缘的亚马逊

以下`run-instances`示例在当前区域的边缘子网`m5.2xlarge`中启动同类型的单个实例。如果您不打算在 Linux 上使用 SSH 或在 Windows 上使用远程桌面协议 (RDP) 连接到您的实例，则密钥对是可选的。

```
aws ec2 run-instances \
```

```
    --image-id ami-id \
    --instance-type m5.2xlarge \
    --subnet-id <subnet-edge-id> \
    --key-name MyKeyPair
```

边缘应用程序负载均衡器

以下`create-load-balancer`示例创建内部应用程序负载均衡器，并为指定子网启用 Local Zones 或 Outposts。

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internal \
    --subnets <subnet-edge-id>
```

要将面向互联网的 Application Load Balancer 部署到 Outpost 上的子网，请在`--scheme`选项中设置`internet-facing`标志并提供 CoIP 池 ID，如以下示例所示：

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internet-facing \
    --customer-owned-ipv4-pool <coip-pool-id>
    --subnets <subnet-edge-id>
```

有关在边缘部署其他服务的信息，请访问以下链接：

服务	AWS Outposts	AWS Local Zones
Amazon EKS	在本地部署 Amazon EKS AWS Outposts	使用启动低延迟 EKS 集群 AWS Local Zones
Amazon ECS	Amazon ECS 已开启 AWS Outposts	共享子网、本地区域和波长区域中的 Amazon ECS 应用程序
Amazon RDS	亚马逊 RDS 开启 AWS Outposts	选择本地区域子网
Amazon S3	开始在 Outposts 上使用亚马逊 S3	不可用

服务	AWS Outposts	AWS Local Zones
Amazon ElastiCache	将 Outposts 与 ElastiCache	将 Local Zones 与 ElastiCache
Amazon EMR	EMR 集群已开启 AWS Outposts	EMR 集群已开启 AWS Local Zones
Amazon FSx	不可用	选择本地区域子网
AWS Elastic Disaster Recovery	使用 AWS Elastic Disaster Recovery 和 AWS Outposts	不可用
AWS Application Migration Service	不可用	选择本地区域子网作为暂存子网

前哨基地专用的 CLI 和 SDK

AWS Outposts 有两组命令，分别 APIs 用于创建服务订单或操纵本地网关和本地网络之间的路由表。

Outposts 订购流程

你可以使用AWS CLI或 Outposts APIs 来创建 Outp osts 站点、创建 Outposts 和创建 Outposts 订单。我们建议您在 AWS Outposts 订购过程中与混合云专家合作，以确保根据您的实施需求正确选择资源 IDs 和最佳配置。有关完整的资源 ID 列表，请参阅AWS Outposts 机架定价页面。

本地网关管理

管理和操作 Outposts 中的本地网关 (LGW) 需要了解可用于 AWS CLI 此任务的和 SDK 命令。除其他任务外， AWS CLI 您可以使用和创建和修改 LGW 路由。 AWS SDKs 有关管理 LGW 的更多信息，请参阅以下资源：

- AWS CLI 适用于亚马逊 EC2
- EC2.Client 在 AWS SDK for Python (Boto)
- Ec2Client 在 适用于 Java 的 AWS SDK

CloudWatch 指标和日志

为 AWS 服务 此，Outposts 和 Local Zones 均可用，指标和日志的管理方式与区域相同。亚马逊 CloudWatch 提供了专门用于监控 Outposts 的以下维度的指标：

维度	说明
Account	使用容量的账户或服务
InstanceFamily	实例系列
InstanceType	实例类型
OutpostId	前哨基地的 ID
VolumeType	EBS 卷类型
VirtualInterfaceId	本地网关或服务链路虚拟接口 (VIF) 的 ID
VirtualInterfaceGroupId	本地网关 VIF 的 VIF 组的 ID

有关更多信息，请参阅 Outp osts 文档中的 Outposts 机架CloudWatch 指标。

资源

AWS 参考文献

- 混合云与 AWS
- AWS Outposts Outposts 机架用户指南
- AWS Local Zones 用户指南
- AWS Outposts 家庭
- AWS Local Zones
- 将 VPC 扩展到本地区域、波长区域或前哨基地（Amazon VPC 文档）
- L@@ ocal Zones 中的 Linux 实例（亚马逊 EC2 文档）
- Outposts 中的 Linux 实例（亚马逊文档 EC2 ）
- 开始部署低延迟应用程序 AWS Local Zones（教程）

AWS 博客文章

- 使用 Amazon 在本地运行 AWS 基础设施 EC2
- 在亚马逊上使用 Amazon EKS 构建现代应用程序 EC2
- 如何在 Amazon EC2 机架上的 CoIP 和直接 VPC 路由模式之间进行选择
- 为您的 Amazon 选择网络交换机 EC2
- 在中维护数据的本地副本 AWS Local Zones
- 亚马逊上的 Amazon ECS EC2
- 使用 Amazon EKS 管理边缘感知服务网格 AWS Local Zones
- 在 Amazon 上部署本地网关入口路由 EC2
- 在中实现工作负载部署的自动化 AWS Local Zones
- 在多账户 AWS 环境 EC2 中共享亚马逊：第 1 部分
- 在多账户 AWS 环境 EC2 中共享亚马逊：第 2 部分
- AWS Direct Connect 和 AWS Local Zones 互操作性模式
- 在亚马逊上部署 Amazon RDS EC2 ，实现多可用区高可用性

贡献者

以下人员为本指南做出了贡献。

编写

- 首席混合云解决方案架构师莱昂纳多·索拉诺 AWS
- Len Gomes，合作伙伴解决方案架构师， AWS
- Matt Price，高级企业支持工程师， AWS
- 汤姆·加多姆斯基，解决方案架构师， AWS
- Obed Gutierrez，解决方案架构师， AWS
- Dionysios Kakaletris，技术客户经理， AWS
- Outposts 首席专家 Vamsi Krishna， AWS

正在审阅

- David Filiatrault，交付顾问， AWS

技术写作

- Handan Selamoglu，高级文档经理， AWS

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	—	2025 年 6 月 10 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、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？

人工智能操作 (AIOps)

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

非对称加密

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

原子性、一致性、隔离性、持久性（ACID）

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

基于属性的访问权限控制（ABAC）

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

权威数据源

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)

一种 AI 领域，它使用机器学习来分析和提取数字图像和视频等视觉格式中的信息。例如，Amazon SageMaker AI 为 CV 提供了图像处理算法。

配置偏差

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，以自定义您的合规性和安全性检查。您可以使用 YAML 模板将一致性包作为单个实体部署在 AWS 账户 和区域或整个组织中。有关更多信息，请参阅 AWS Config 文档中的一致性包。

持续集成和持续交付（CI/CD）

自动执行软件发布过程的源代码、构建、测试、暂存和生产阶段的过程。 CI/CD 通常被描述为管道。 CI/CD 可以帮助您实现流程自动化、提高生产力、提高代码质量和更快地交付。有关更多信息，请参阅持续交付的优势。CD 也可以表示持续部署。有关更多信息，请参阅持续交付与持续部署。

CV

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。

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。

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。

few-shot 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

人工智能模型的一个子集，这些模型已经过大量数据训练，可以使用简单的文本提示来创建新的内容和工件，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

帮助管理各组织单位的资源、策略和合规性的高级规则 (OUs)。预防性防护机制会执行策略以确保符合合规性标准。它们是使用服务控制策略和 IAM 权限边界实现的。侦测性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。

hypercare 周期

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

我

IaC

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 进行部署” 最佳实践。

入站（入口）VPC

在 AWS 多账户架构中，一种接受、检查和路由来自应用程序外部的网络连接的 VPC。AWS 安全参考架构建议设置您的网络帐户，包括入站、出站和检查， VPCs 以保护您的应用程序与更广泛的互联网之间的双向接口。

增量迁移

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

工业 4.0

该术语由克劳斯·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

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

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

微服务架构

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

迁移加速计划（MAP）

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

大规模迁移

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

迁移工厂

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

迁移元数据

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

迁移模式

一种可重复的迁移任务，详细列出了迁移策略、迁移目标以及所使用的迁移应用程序或服务。示例： 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，并参阅调动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。

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 Secret s 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。你可以使用 Amazon S CloudWatch ynthetics 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。