AWS 白皮书

AWS Outposts 高可用性设计和架构注意事项

AWS Outposts 高可用性设计和架构注意事项: AWS 白皮书

Table of Contents

AWS Outposts 高可用性设计和架构注意事项

发布日期：2021 年 8 月 12 日（文档历史记录）

本白皮书讨论了 IT 经理和系统架构师在构建高度可用的本地应用程序环境时可以采用的架构注意事项和推荐实践。 AWS Outposts

您的架构是否良好？

当您在云端构建系统时，AWS Well-Architected Framework 可助您了解所作决策的利弊。利用此框架的六个支柱，您可以了解到设计和运行可靠、安全、高效、经济有效且可持续的系统的架构最佳实践。您可以使用 AWS 管理控制台 免费提供的 AWS Well-Architected Tool，回答与每个支柱相关的一组问题，即可根据这些最佳实践检查自己的工作负载。

有关云架构的更多专家指导和最佳实践（参考架构部署、图表和白皮书），请参阅 AWS 架构中心。

简介

本 paper 适用于希望使用 AWS 云平台部署、迁移和操作应用程序，并在本地使用机架（42U AWS Outposts 机架外形规格为）运行这些应用程序的 IT 经理和系统架构师。AWS Outposts

它介绍了架构模式、反模式以及构建包括 AWS Outposts 机架在内的高可用性系统的推荐做法。您将学习如何管理 AWS Outposts 机架容量，以及如何使用网络和数据中心设施服务来设置高度可用的 AWS Outposts 机架基础设施解决方案。

AWS Outposts rack 是一项完全托管的服务，可提供云计算、存储和网络功能的逻辑池。借助 Outposts 机架，客户可以在本地环境中使用支持的 AWS 托管服务，包括：亚马逊弹性计算云（亚马逊）、亚马逊弹性区块存储（亚马逊 EBS EC2）、Outposts 上的亚马逊 S3、亚马逊弹性 Kubernetes 服务（亚马逊 EKS）、亚马逊弹性容器服务（亚马逊 ECS）、亚马逊关系数据库服务（亚马逊 RDS）），以及 O utpost s 上的其他服务。AWSOutpost 上的服务将在 AWS 区域内的相同 AWS Nitro 系统上提供。

通过利用 AWS Outposts 机架，您可以使用熟悉的 AWS 云服务和工具构建、管理和扩展高度可用的本地应用程序。 AWS Outposts rack 非常适合需要低延迟访问本地系统、本地数据处理、数据驻留以及迁移具有本地系统相互依赖关系的应用程序的工作负载。

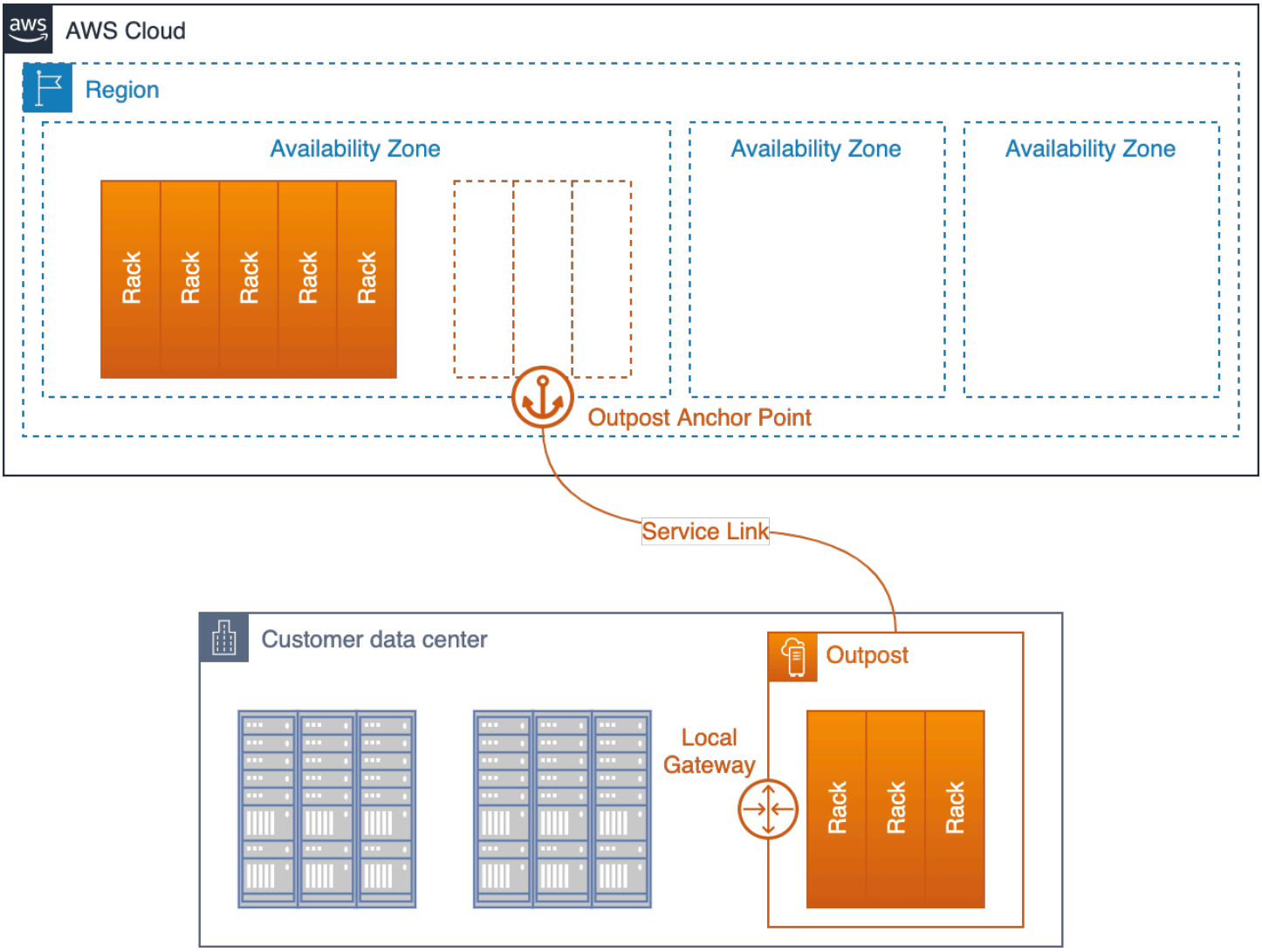
将 AWS 基础设施和服务扩展到本地位置

该 AWS Outposts 服务为 50多个国家和地区的本地位置提供 AWS 基础设施和服务，使客户能够将相同的 AWS 基础架构、 AWS APIs服务和工具部署到几乎任何数据中心、托管空间或本地设施，从而获得真正一致的混合体验。要了解如何使用 Outposts 进行设计，你应该了解构成云的不同等级。 AWS

AWS 区域是指世界上的一个地理区域。每个 AWS 区域 数据中心都是按逻辑分组为可用区 (AZs) 的数据中心的集合。 AWS 区域 提供多个（至少两个）物理分隔和隔离的可用区，这些可用区通过低延迟、高吞吐量和冗余网络连接相连。每个 AZ 包含一个或多个物理数据中心。

逻辑前哨（以下简称 Outpost）是部署一个或多个物理连接的 AWS Outposts 机架，作为单个实体进行管理。Outpost 在您的一个站点上提供 AWS 计算和存储容量池，作为 AWS 区域中可用区的私有扩展。

也许最好的概念模型 AWS Outposts 是考虑将一个或多个机架从可用区内的数据中心拔下电源 AWS 区域，然后将其安装在自己的数据中心或托管设施中。将这些机架从 AZ 数据中心部署到您的数据中心。然后，你用一根（非常）长的电缆将机架插入亚利桑那州数据中心的锚点，这样机架就可以继续作为其中的一部分运行 AWS 区域。您还可以将这些机架插入本地网络，以便在本地网络和这些机架上运行的工作负载之间提供低延迟连接。这为您提供了操作和 API 的一致性 AWS 云，同时将您的工作负载保持在本地。



部署在客户数据中心内并与其锚 AZ 和父级区域相连的 Outpost

前哨基地充当其停泊的AZ的延伸。 AWS 作为其中的一部分运营、监控和管理 AWS Outposts 基础架构 AWS 区域。Outpost 通过一组名为服务链接的加密 VPN 隧道（而非一条特别长的物理电缆）连接回其父级区域。

服务链接的终点位于 Outpost 父级区域的可用区（AZ）中的一组锚点上。

您可以选择内容的存储位置。您可以将您的内容复制并备份到 AWS 区域 或其他位置。未经您的同意，您的内容不会被转移或复制到您所选择的位置以外，除非为了遵守法律或政府机构具有约束力的命令必须如此。有关更多信息，请参阅 AWS 数据隐私 FAQ。

您在这些机架上部署的工作负载在本地运行。而且，虽然这些机架中可用的计算和存储容量是有限的，无法容纳运行的云规模服务 AWS 区域，但部署在机架上的资源（您的实例及其本地存储）可以获得在本地运行的好处，同时管理平面继续在中运行。 AWS 区域

要在 Outpost 上部署工作负载，您需要向虚拟私有云（VPC）环境中添加子网，并指定 Outpost 作为子网的位置。然后，在通过、CLI、 AWS 管理控制台 APIs、CDK 或基础设施即代码 (IaC) 工具部署支持的 AWS 资源时，您可以选择所需的子网。Outpost 子网中的实例通过 VPC 联网与 Outpost 或区域中的其他实例通信。

Outpost 服务链接可同时传输 Outpost 管理流量和客户 VPC 流量（Outpost 上的子网与区域中的子网之间的 VPC 流量）。

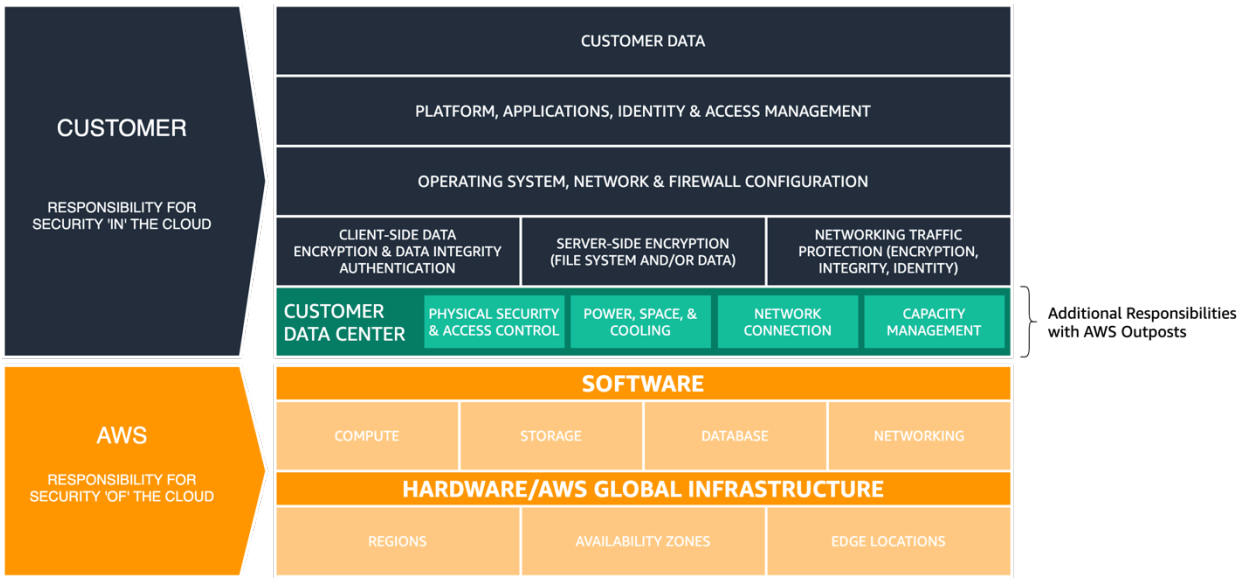
重要术语：

- AWS Outposts— 是一项完全托管的服务，可为几乎任何数据中心 APIs、托管空间或本地设施提供相同的 AWS 基础架构、 AWS 服务和工具，以实现真正一致的混合体验。
- Outpos t — 是一个或多个物理连接的 AWS Outposts 机架的部署，这些机架作为单个逻辑实体进行管理， AWS 计算、存储和网络池部署在客户现场。
- 父区域 — 为 Outpost 部署提供管理、控制平面 AWS 服务和区域服务。 AWS 区域
- 锚可用区（锚 AZ）：父级区域中的可用区，用于托管 Outpost 锚点。前哨基地充当其锚点 AZ 的延伸。在下达 Outposts 订单时，主要 AZ 由客户选择。选择锚可用区后，在 AWS Outposts 订阅期限内无法对其进行更改。
- 锚点：锚 AZ 中的端点，用于接收来自远程部署的 Outpost 的连接。
- 服务链接：一组加密的 VPN 隧道，用于将 Outpost 连接到其父级区域的锚可用区。
- 本地网关（LGW）：一种逻辑互连虚拟路由器，用于实现 Outpost 与本地网络之间的通信。

了解 AWS Outposts 分担责任模型

当您将 AWS Outposts 基础设施部署到数据中心或主机托管设施时，您将在责任AWS 共担模式中承担额外的责任。例如，在该地区 AWS 提供多种电源、冗余核心网络和弹性广域网 (WAN) 连接，以确保在一个或多个组件出现故障时提供服务。

使用 Outpost 时，您负责为 Outpost 机架提供弹性电源和网络连接，以满足 Outpost 上运行的工作负载的可用性需求。



AWS 已更新分担责任模型 AWS Outposts

使用 AWS Outposts，您负责数据中心环境的物理安全和访问控制。您必须提供足够的电源、空间和冷却能力以保持 Outpost 正常运行，并提供网络连接以使 Outpost 连接回区域。

由于 Outpost 的容量是有限的，由站点 AWS 安装的机架大小和数量决定，因此您必须决定运行初始工作负载、适应未来的增长以及提供额外容量来缓解服务器故障和维护事件所需的容量、EBS 和 S3 on Outposts 的容量。 EC2

AWS 负责 Outposts 基础设施的可用性，包括机架内的电源、服务器和网络设备。 AWS Outposts AWS 还管理在 Outposts 上运行的虚拟化虚拟机管理程序、存储系统和 AWS 服务。

每个 Outpost 机架中的中央电源架可以将交流电转换为直流电，并通过汇流排架构为机架中的服务器供电。借助汇流排架构，即使机架中有一半的电源出现故障，所有服务器仍将继续不间断地运行。

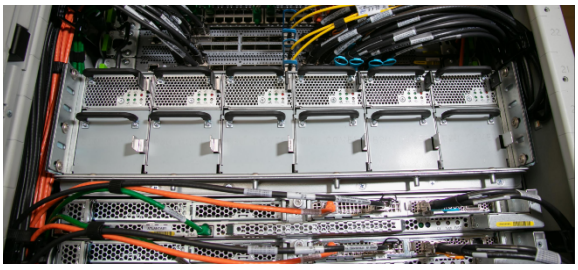


图 3- AWS Outposts AC-to-DC 电源和汇流条功率分布

Outpost 机架内和机架之间的网络交换和布线也采用完全冗余的配置。光纤配线架提供 Outpost 机架和本地网络之间的连接，并充当客户管理的数据中心环境与托管环境之间的分界点。 AWS Outposts

就像在该地区一样，负责Outpost AWS s上提供的云服务，并在您选择和部署更高级别的托管服务（例如Outposts上的Amazon RDS）时承担额外的责任。在考虑和选择要在 Outpost 上部署的服务时，应查看 AWS 责任共担模型和针对不同服务的常见问题 (FAQ) 页面。这些资源提供了有关您与之间的责任划分的更多详细信息 AWS。

从故障模式的角度进行思考

在设计高可用性应用程序或系统时，必须考虑哪些组件可能会出现故障，组件故障会对系统产生什么影响，以及您的应用程序 R PO/RTO 目标，以及可以实施哪些机制来缓解或消除组件故障的影响。应用程序是在单台服务器上、单个机架中还是单个数据中心中运行？ 当服务器、机架或数据中心出现临时或永久故障时会发生什么？ 当网络等关键子系统或应用程序本身出现故障时会发生什么？ 这些就是故障模式。

在规划 Outpost 和应用程序部署时，应考虑本部分所述的故障模式。以下各部分将介绍如何缓解这些故障模式，从而为应用程序环境提供更高级别的可用性。

故障模式 1：网络

Outpost 部署的管理和监控依赖于与其父级区域的弹性连接。网络中断可能是由各种故障引起的，例如操作员错误、设备故障和服务提供商的服务中断。Outpost 可能包含在站点连接在一起的一个或多个机架，如果其无法通过服务链接与区域通信，则被视为已断开连接。

冗余网络路径可以帮助降低发生断开连接事件的风险。您应该映射应用程序依赖关系和网络流量，以了解断开连接事件对工作负载操作的影响。规划足够的网络冗余以满足应用程序可用性需求。

在断开连接事件期间，在 Outpost 上运行的实例将继续运行，并且可通过 Outpost 本地网关（LGW）从本地网络进行访问。如果本地工作负载和服务依赖于区域的服务，则可能会受损或出现故障。当 Outpost 与区域断开连接时，变更请求（例如启动或停止前哨基地上的实例）、控制平面操作和服务遥测（例如 CloudWatch 指标）将失败。 CloudWatch 在网络断开短时间内，指标将在您的 Outpost 上进行本地后台处理，并在服务链接连接重新建立后发送到该地区进行审查。

故障模式 2：实例

如果运行的服务器出现问题，或者 EC2 实例出现操作系统或应用程序故障，Amazon 实例可能会受损或出现故障。应用程序处理这些类型故障的方式取决于应用程序架构。单片应用程序通常使用应用程序或系统功能进行恢复，而面向服务的模块化架构或微服务架构通常会替换故障组件以保持服务可用性。

您可以使用 Amazon A EC2 uto Scaling 群组等自动机制将失败的实例替换为新实例。Instance auto recovery 可以重启因服务器故障而失败的实例，前提是其余服务器上有足够的可用容量并且服务链路仍处于连接状态。

故障模式 3：计算

服务器可能会出现故障或受损，并且可能由于各种原因（例如组件故障和定期维护操作）而需要（临时或永久）停止运行。Outpost 机架上的服务处理服务器故障和受损问题的方式各不相同，可能取决于客户如何配置高可用性选项。

您应该订购充足的计算容量以支持 N+M 可用性模型，其中 N 是所需的容量，M 是为应对服务器故障而预置的备用容量。

作为完全托管 AWS Outposts 机架服务的一部分，将为出现故障的服务器提供硬件更换。 AWS 主动监控 Outpost 部署中所有服务器和网络设备的运行状况。如需进行物理维护， AWS 将安排时间前往您的站点以更换出现故障的组件。配置备用容量可以让您的工作负载保持弹性，抵御主机故障，同时将不健康的服务器停用并更换。

故障模式 4：机架或数据中心

机架故障可能是由于机架完全断电或环境故障（例如冷却中断或数据中心因洪水或地震而受到物理损坏）所致。数据中心的配电架构存在缺陷或标准数据中心电源维护期间出现错误，都可能导致一个或多个机架甚至整个数据中心断电。

通过将基础设施部署到多个数据中心楼层或者同一园区或城区内相互独立的地点，可以缓解上述情况。

在 AWS Outposts 机架上采用这种方法需要仔细考虑应用程序的架构和分布方式，使其在多个独立的逻辑 Outposts 上运行，以保持应用程序的可用性。

故障模式 5： AWS 可用区或区域

每个 Outpost 都锚定到某个 AWS 区域内的特定可用区（AZ）。锚 AZ 或父级区域内的故障可能会导致 Outpost 失去管理和可变性，并可能中断 Outpost 与区域之间的网络通信。

与网络故障类似，AZ 或区域故障可能会导致 Outpost 与区域断开连接。如前所述，在 Outpost 上运行的实例将继续运行，并且可以通过 Outpost 本地网关（LGW）从本地网络进行访问，如果这些实例依赖于区域内的服务，则可能会受损或失败。

为了减轻 AWS 可用区和区域故障的影响，您可以部署多个 Outposts，每个Outpost都锚定到不同的可用区或区域。然后，可以使用目前用于在 AWS 上进行设计和部署的许多类似机制和架构模式，将工作负载设计为在分布式多 Outpost 部署模型中运行。

运行的服务的控制平面位于其 AWS Outposts 所在的区域，从而产生了对亚马逊和 EC2 亚马逊 EBS 等区域服务以及区域服务（例如亚马逊 RDS、Elastic Load Balancing 和 Amazon EKS）的依赖。在 Outposts 中，可以在静态稳定概念下部署应用程序，以帮助提高控制飞机损伤的弹性。

使用 AWS Outposts 机架构建 HA 应用程序和基础设施解决方案

借 AWS Outposts 助 rack，您可以使用熟悉的 AWS 云服务和工具构建、管理和扩展高度可用的本地应用程序。云 HA 的架构和方法通常不同于当前可能在数据中心内运行的传统本地 HA，了解这一点非常重要。

使用传统的本地 HA 应用程序部署，应用程序部署在虚拟机中（VMs）。要保持这些虚拟机持续正常运行，则需要部署和维护复杂的 IT 系统和基础设施。它们 VMs 通常具有特定的身份，每个虚拟机都可能在整个应用程序架构中发挥关键作用。

架构角色与 VM 身份紧密耦合。系统架构师可以利用 IT 基础设施功能提供高度可用的 VM 运行时环境，使每台 VM 都能可靠地访问计算容量、存储卷和网络服务。如果 VM 出现故障，则会运行自动或手动恢复流程，以将出现故障的 VM 恢复到正常运行状态，恢复流程通常在其他基础设施上或完全在另一个数据中心内运行。

Cloud HA 架构采用不同的方法。 AWS 云服务提供可靠的计算、存储和联网功能。应用程序组件部署到 EC2实例、容器、无服务器函数或其他托管服务。

实例是指某个应用程序组件（可能是扮演该角色的众多组件之一）的实例化。应用程序组件彼此之间以及这些组件与其在整个应用程序架构中所扮演的角色之间为松耦合关系。实例的单个身份通常并不重要。可以创建或销毁其他实例，以根据需求进行扩展或缩减。只需将失败的实例或运行不正常的实例替换为运行正常的新实例即可。

AWS Outposts rack 是一项完全托管的服务，可将 AWS 计算、存储、网络、数据库和其他云服务扩展到本地位置，以提供真正一致的混合体验。您不应将 Outpost 机架服务视为采用传统本地 HA 机制的 IT 基础设施系统的简易替代。尝试使用 AWS 服务和 Outposts 来支持传统的本地 HA 架构是一种反模式。

在 AWS Outposts 机架上运行的工作负载使用云高可用性机制，例如 Amazon A EC2 uto Scaling（水平扩展以满足工作负载需求）、运行EC2 状况检查（检测和删除不健康的实例）和应用程序负载均衡器（将传入的工作负载流量重定向到扩展或替换的实例）。将应用程序迁移到云端时，无论是迁移到云 AWS 区域 还是 AWS Outposts 机架，都应更新高可用性应用程序架构，以开始利用托管云服务和云高可用性机制。

以下各节介绍了架构模式、反模式以及在本地环境中部署 AWS Outposts 机架以运行具有高可用性要求的工作负载的推荐实践。这些部分介绍了多种模式和实操；但是，其中并未提供配置和实现细节。

在为 Outposts AWS Outposts 机架 FAQs和应用程序迁移到服务做准备时，你应该阅读 FAQs 并熟悉 Outposts 机架上运行的服务的机架和用户指南以及和服务文档。 AWS

主题

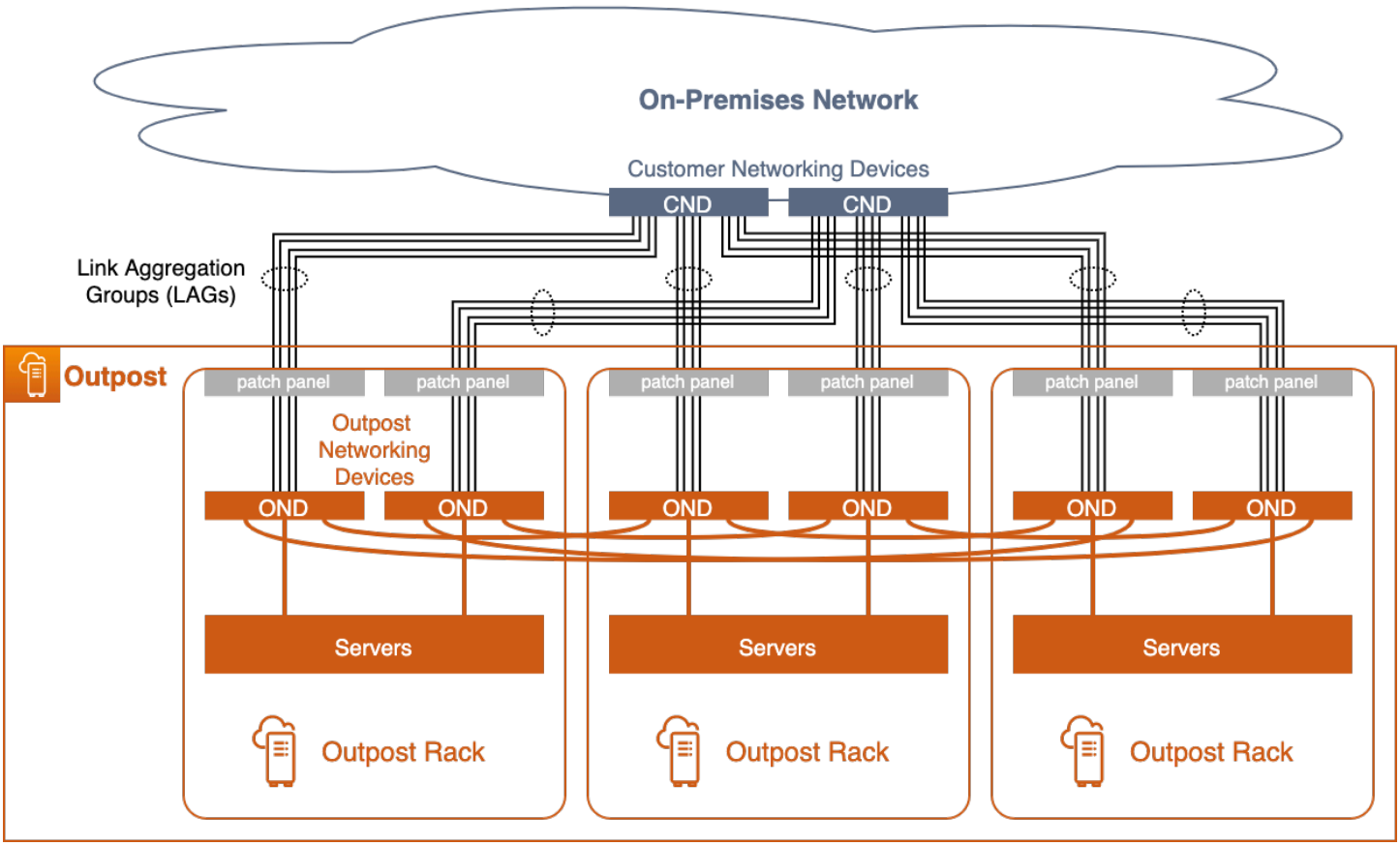
网络连接

Outpost 部署依赖于与其锚 AZ 的弹性连接，从而使管理、监控和服务操作正常运行。您应该配置本地网络，为每个 Outpost 机架提供冗余的网络连接，并提供与 AWS 云中锚点的可靠连接。此外，还要考虑在 Outpost 上运行的应用程序工作负载以及与之进行通信的其他本地系统和云系统之间的网络路径 – 您要如何在网络中路由这些流量呢？

主题

网络连接

每个 AWS Outposts 机架都配置了名为 Outpost 网络设备 (ONDs) 的冗余 top-of-rack交换机。每个机架中的计算和存储服务器都与两者相连 ONDs。您应该将每个 OND 连接到数据中心中一台名为客户网络设备 (CND) 的单独交换机，以便为每个 Outpost 机架提供不同的物理和逻辑路径。 ONDs 使用光纤电缆和光学收发器通过一个或多个物理连接连接到您 CNDs 的。物理连接是在逻辑链路聚合组（LAG）链路中配置的。



具有冗余网络连接的多机架 Outpost

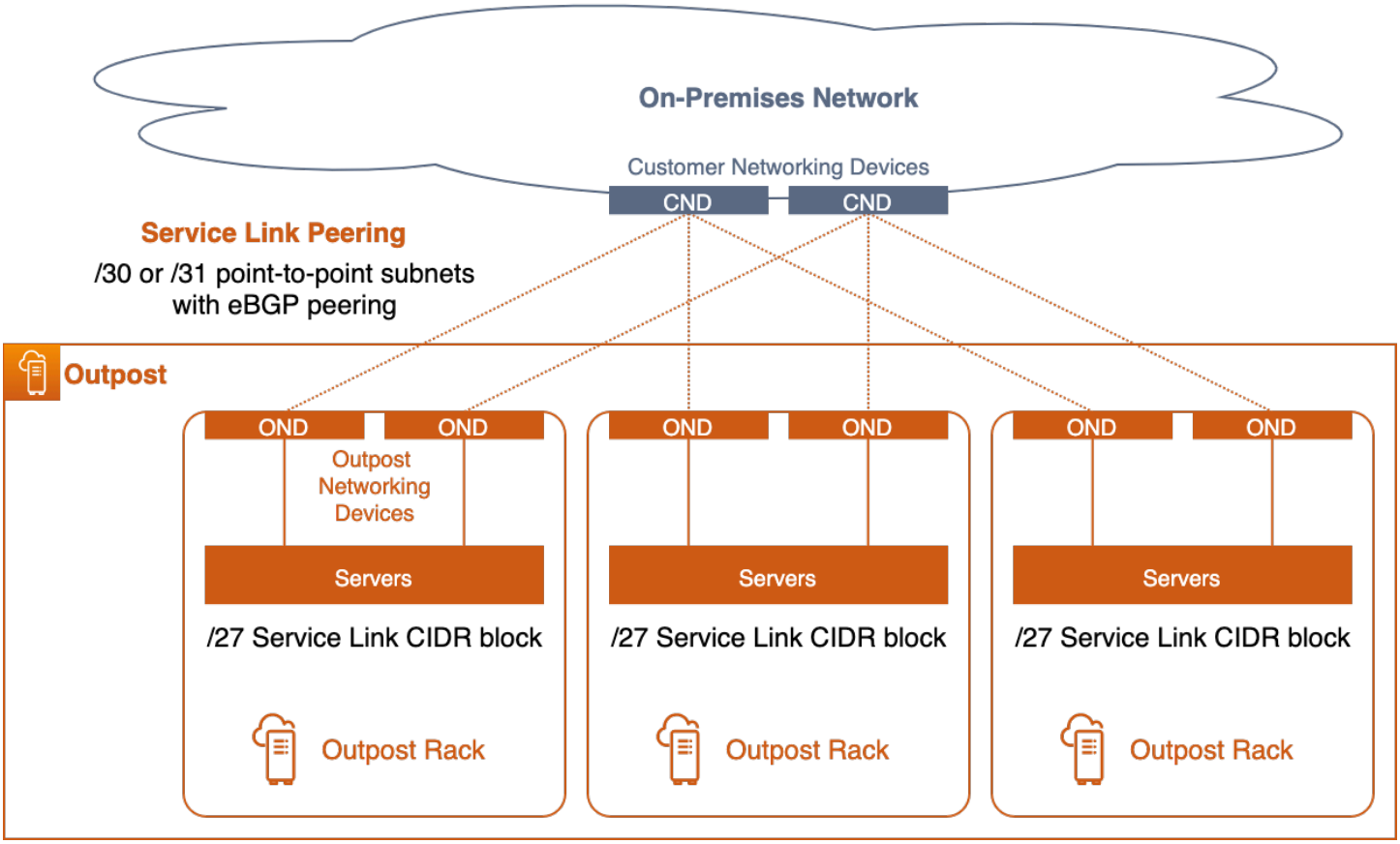
OND 到 CND 的链路始终在 LAG 中配置，即使物理连接是单根光纤电缆也是如此。若将链路配置为 LAG 组，则可以通过向逻辑组添加其他物理连接来增加链路带宽。将 LAG 链路配置为 IEEE 802.1q 以太网中继，以便实现 Outpost 和本地网络之间的网络隔离。

每个 Outpost 都有至少两个逻辑上隔离的网络，这些网络需要与客户网络进行通信或跨客户网络进行通信：

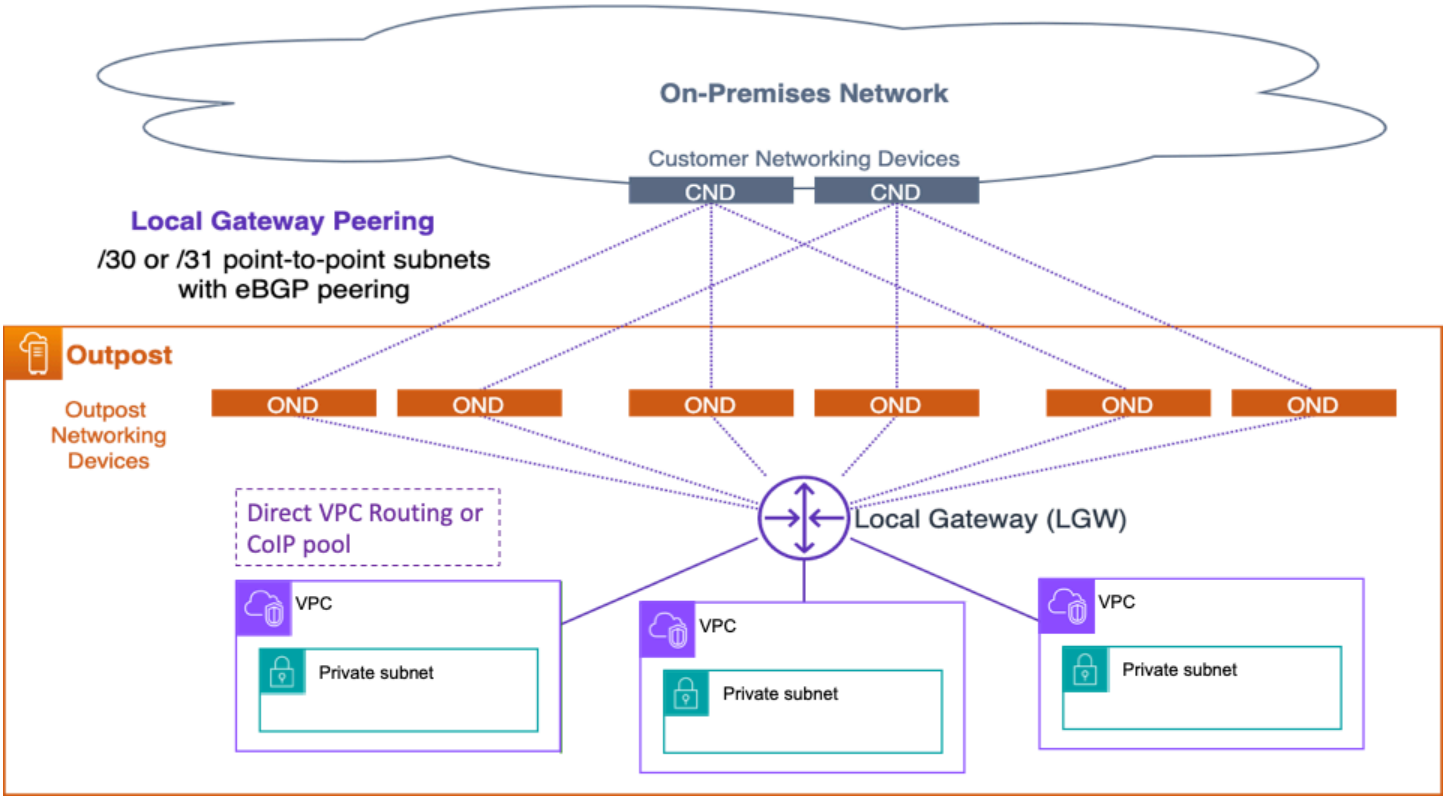
- 服务链接网络 — 将服务链路 IP 地址分配给 Outpost 服务器，并促进与本地网络的通信，从而允许服务器重新连接到该区域的 Outpost 锚点。当您在单个逻辑 Outposts 中有多个机架实现时，您需要为每个机架分配一个 Service Link /26 CIDR。
- 本地网关网络：通过 Outpost 本地网关（LGW）实现 Outpost 上的 VPC 子网与本地网络之间的通信。

这些隔离的网络通过一组 point-to-point IP 连接通过 LAG 链路连接到本地网络。每个 OND 到 CND LAG 链路都配置了 VLAN IDs、 point-to-point（/30 或 /31）IP 子网，以及每个隔离网络（服务链路和 LGW）的 eBGP 对等连接。您应该将 LAG 链路 point-to-point VLANs 及其子网视为第 2 层分段、路由

的第 3 层连接。路由的 IP 连接可提供冗余的逻辑路径，有利于 Outpost 上的隔离网络与本地网络之间的通信。



服务链接对等



本地网关对等

您应该终止直接连接的 CND 交换机上的第 2 层 LAG 链路（及其链路 VLANs），并在 CND 交换机上配置 IP 接口和 BGP 对等连接。您不应在数据中心交换机 VLANs 之间架起延迟。有关更多信息，请参阅《AWS Outposts 用户指南》中的网络层连接。

在逻辑多机架前哨基地内， ONDs 它们以冗余方式互连，从而在机架和服务器上运行的工作负载之间提供高度可用的网络连接。 AWS 负责前哨基地内的网络可用性。

不使用 ACE 进行高可用性网络连接的推荐做法

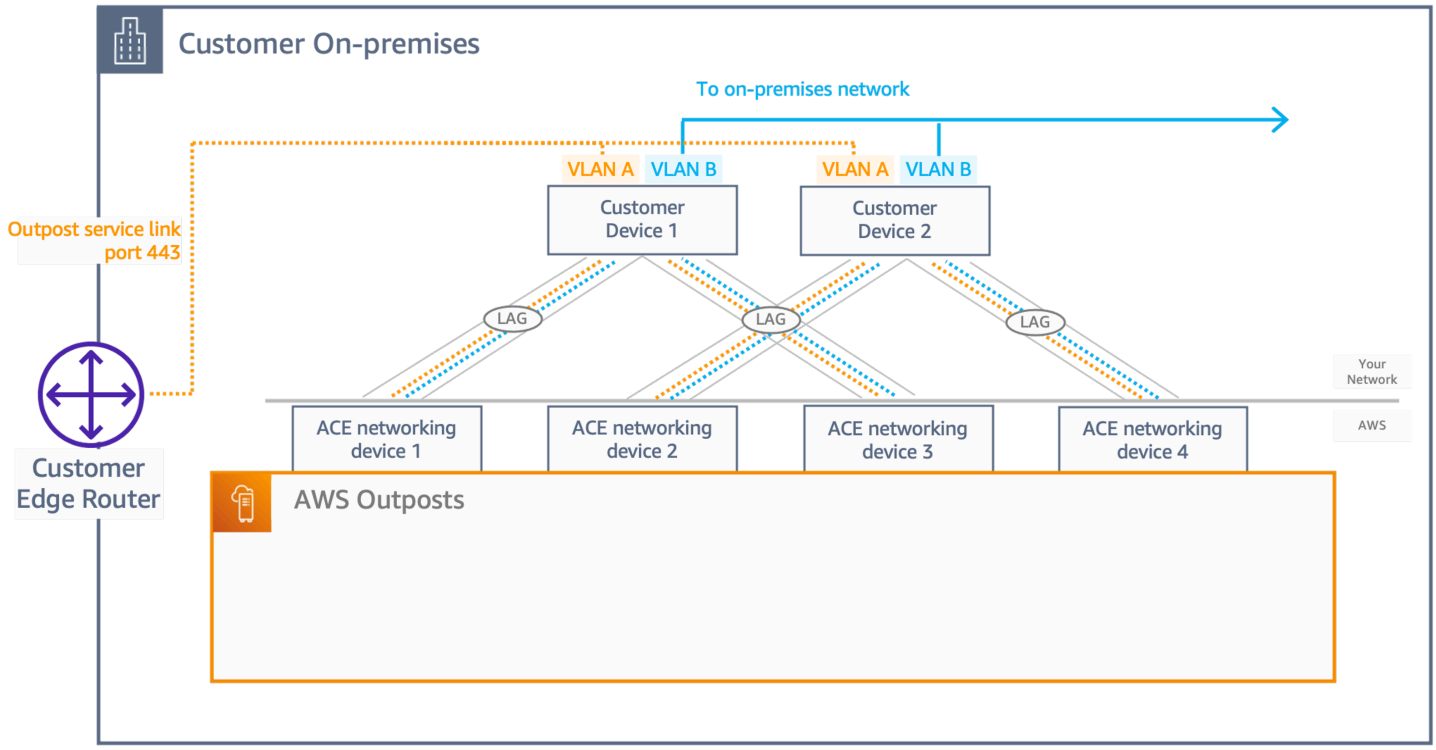
- 将 Outpost 机架中的每台 Outpost 网络设备（OND）连接到数据中心中的独立客户网络设备（CND）。
- 终止直接连接的客户网络设备 (CND) 交换机上的第 2 层链路 VLANs、第 3 层 IP 子网和 BGP 对等连接。请勿在本地网络 VLANs 之间 CNDs 或通过本地网络将 OND 桥接到 CND。
- 向链路聚合组 (LAGs) 添加链路，以增加前哨基地和数据中心之间的可用带宽。不要依赖通过两者的不同路径的总带宽 ONDs。
- 使用通过冗余 ONDs 的不同路径在 Outpost 网络和本地网络之间提供弹性连接。
- 为了实现最佳冗余并允许无中断的 OND 维护，我们建议客户按以下方式配置 BGP 通告和策略：

- 客户网络设备应在不更改 BGP 属性的情况下从 Outpost 接收 BGP 通告，并在需要维护时启用 BGP multipath/load-balancing to achieve optimal inbound traffic flows (from customer towards Outpost). AS-Path prepending is used for Outpost BGP prefixes to shift traffic away from a particular OND/uplink。客户网络应首选 Outpost 中 AS-Path 长度为 1 的路由，而不是 AS-Path 长度为 4 的路由，也就是说，应对 AS-Path 前置作出反应。
- 客户网络应在 Outpost 中向所有人通告具有相同属性的相等 BGP 前缀 ONDs 。默认情况下，Outpost 网络负载会均衡所有上行链路之间的出站流量（流向客户）。如果需要维护，可在 Outpost 端使用路由策略，以将流量从特定的 OND 转移出去。要执行此流量转移并以无中断的方式进行维护，客户端 ONDs 都需要使用相同的 BGP 前缀。当客户的网络需要维护时，我们建议使用 AS-Path 前置，以将来自特定上行链路或设备的流量暂时转移出去。

使用 ACE 进行高可用性网络连接的推荐做法

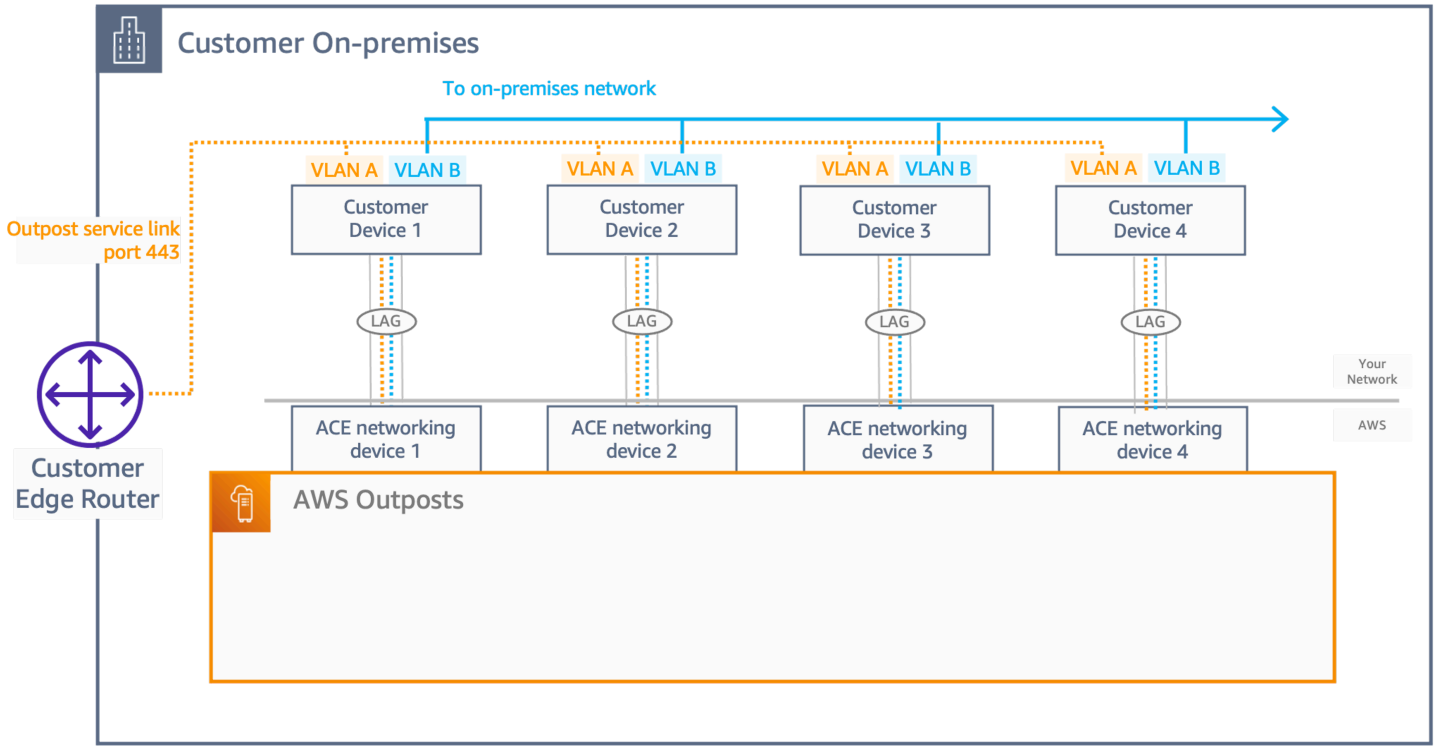
对于具有四个或更多计算机架的多机架部署，您必须使用聚合、核心、边缘 (ACE) 机架，它将充当网络聚合点，以减少与本地网络设备的光纤链路数量。ACE 机架提供与每个 Outposts 机架 ONDs 中的连接，因此 AWS 将拥有和 ACE 网络设备之间的 VLAN 接口分配 ONDs 和配置。

无论是否使用 ACE 机架，服务链路和本地网关网络仍然需要隔离的网络层，ACE 机架的目标是为每个隔离的网络提供 VLAN point-to-point（/30 或 /31）IP 子网和 eBGP 对等互连配置。建议的架构应遵循以下两种架构中的任何一种：



双客户网络设备

- 使用此架构，客户应有两台网络设备 (CND) 来互连 ACE 网络设备，从而提供冗余。
- 对于每个物理连接，您都必须启用 LAG（以增加 Outpost 和数据中心之间的可用带宽），即使它是单个物理端口，并且它将传输两个网段，有 2 point-to-point VLANs （/30 或 /31），以及和之间的 eBGP 配置。 ACEs CNDs
- 在稳定状态下，流量将在启用等价多路径 (ECMP) 模式平衡后进行负载to/from the customer network from the ACE layer, 25% traffic distribution across the ACE to customer. In order to allow this behavior, the eBGP peering's between ACEs and CNDs must have BGP multipath/load平衡，并在 4 个 eBGP 对等连接上宣布具有相同 BGP 指标的客户前缀。
- 为了实现最佳冗余并允许无中断的 OND 维护，我们建议客户遵循以下建议：
  - 客户网络设备应在 Outpost ONDs 中向所有设备通告具有相同属性的相等 BGP 前缀。
  - 客户网络设备应在不更改 BGP 属性的情况下从 Outpost 接收 BGP 通告，并启用 BGP 多路径/负载平衡。



四用户网络设备

使用此架构，客户将有四个网络设备 (CND) 用于互连 ACE 网络设备，从而提供冗余和相同的网络逻辑 VLANs，包括适用于 2 CND 架构的 eBGP 和 ECMP。

锚连接

O utpost 服务链接连接到 Outpost 父区域中特定可用区 (AZ) 中的公共锚点或私有锚点（不能两者兼而有之）。前哨服务器启动从其服务链接 IP 地址到锚点 AZ 中锚点的出站服务链接 VPN 连接。这些连接使用 UDP 和 TCP 端口 443。 AWS 负责区域内锚点的可用性。

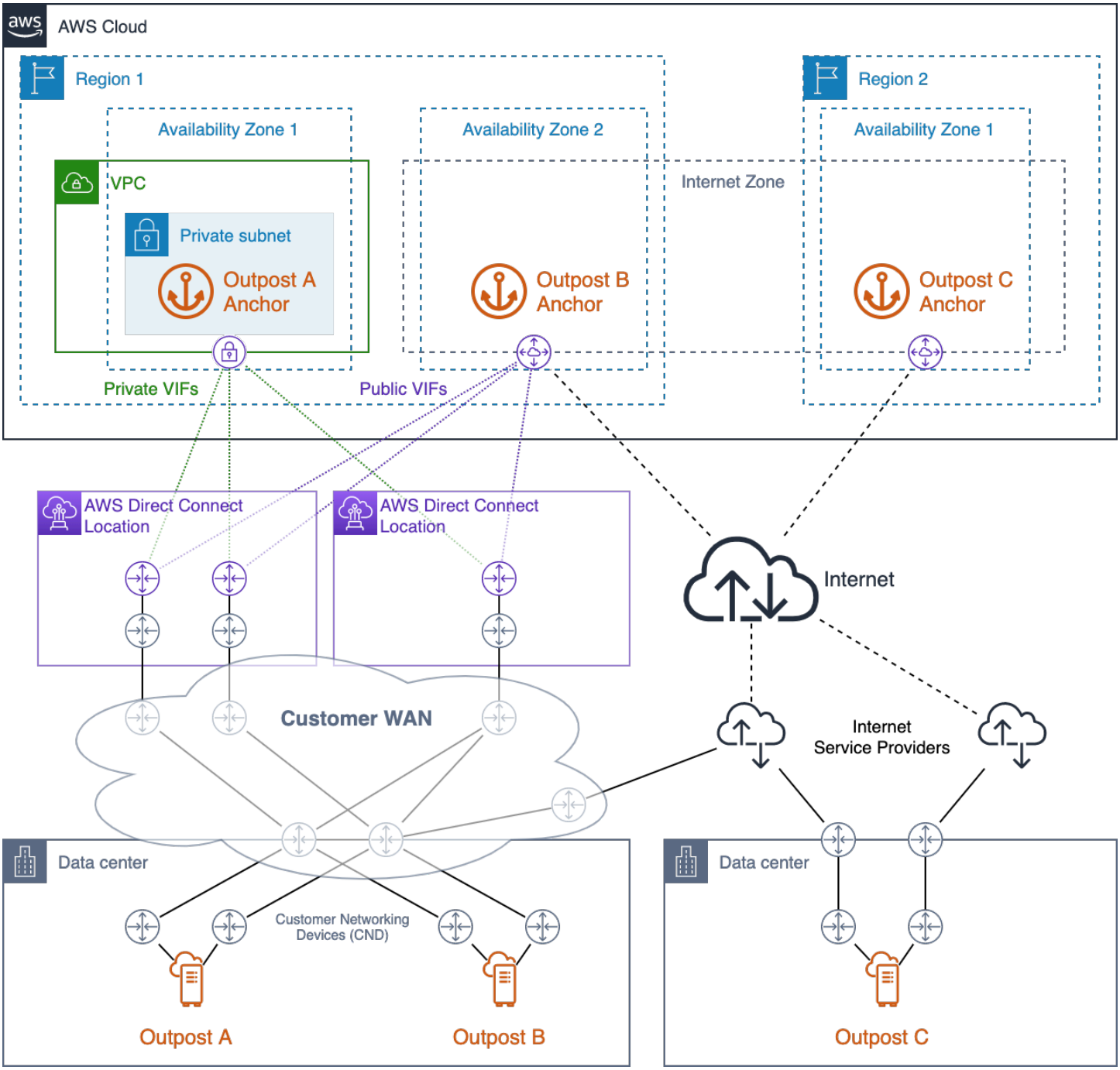
您必须确保 Outpost 服务链接 IP 地址可以通过您的网络连接到锚点 AZ 中的锚点。服务链接 IP 地址无需与本地网络上的其他主机通信。

公共锚点位于该地区的公有 IP 范围（在 EC2 服务 CIDR 块中），可以通过互联网或 AWS Direct Connect（DX）公共虚拟接口（ ）进行访问（VIFs）。使用公共锚点可以更灵活地选择路径，因为服务链路流量可以通过任何可以成功到达公共互联网上的锚点的可用路径进行路由。

私有锚点支持您使用自己的 IP 地址范围进行锚连接。私有锚点是使用客户分配的 IP 地址在专用 VPC 内的私有子网中创建的。VPC 是在拥有 Outpost 资源的中创建的，您负责确保 VPC 可用且配置正确。AWS 账户 在 Organizations 中 AWSOrigamiServiceGateway 使用安全控制策略 (SCP) 来防止用户删除该虚拟私有云 (VPC)。必须使用 Direct Connect private 访问私有锚点。 VIFs

您应该预置 Outpost 与区域内锚点之间的冗余网络路径，同时在多个位置的独立设备上终止连接。动态路由的配置应可实现以下功能：在连接或网络设备出现故障时，自动将流量重新路由到备用路径。您应该预置充足的网络容量，以确保一条 WAN 路径的故障不会使剩余路径不堪重负。

下图显示了三个Out AZs posts，这些Outposts具有通往其锚点的冗余网络路径 AWS Direct Connect 以及公共互联网连接。Outpost A 和 Outpost B 锚定到同一区域的不同可用区。Outpost A 连接到区域 1 的 AZ 1 中的私有锚点。Outpost B 连接到区域 1 的 AZ 2 中的公有锚点。Outpost C 连接到区域 2 的 AZ 1 的公有锚。



高度可用的锚点连接 AWS Direct Connect 和公共互联网接入

Outpost A 有三条冗余网络路径可以访问其私有锚点。其中两条路径通过单个 Direct Connect 位置的冗余 Direct Connect 线路实现。第三条路径通过位于另一个 Direct Connect 位置的 Direct Connect 线路实现。这种设计将 Outpost A 的服务链路流量保持在专用网络上，并提供路径冗余，允许任何一个 Direct Connect 电路出现故障或整个 Direct Connect 位置出现故障。

Outpost B 有四条冗余网络路径可以访问其公有锚点。有三条路径可通过公共 VIFs 配置的 Direct Connect 电路和 Outpost A 使用的位置获得。第四条路径可通过客户广域网和公共互联网获得。Outpost B 的服务链路流量可以通过任何可以成功到达公共互联网锚点的可用路径进行路由。使用 Direct Connect 路径可以提供更稳定的延迟和更高的带宽可用性，而公有互联网路径可用于灾难恢复（DR）或带宽增强方案。

Outpost C 有两条冗余的网络路径可以访问其公有锚点。Outpost C 部署在与 Outpost A 和 B 不同的数据中心中。Outpost C 的数据中心没有连接到客户 WAN 的专用线路。取而代之的是，数据中心有由两个不同的互联网服务提供商提供的冗余互联网连接（ISPs）。Outpost C 的服务链路流量可以通过任一 ISP 网络进行路由，以到达公共互联网上的锚点。这种设计允许灵活地通过任何可用的公共互联网连接路由服务链路流量。但是，该 end-to-end路径依赖于带宽可用性和网络延迟波动的公共第三方网络。

前哨基地与其服务链路锚点之间的网络路径必须符合以下带宽规范：

- 每个 Outpost 机架的可用带宽为 500 Mbps – 1 Gbps（例如，3 个机架：1.5 – 3 Gbps 可用带宽）

高可用性锚点连接的推荐做法

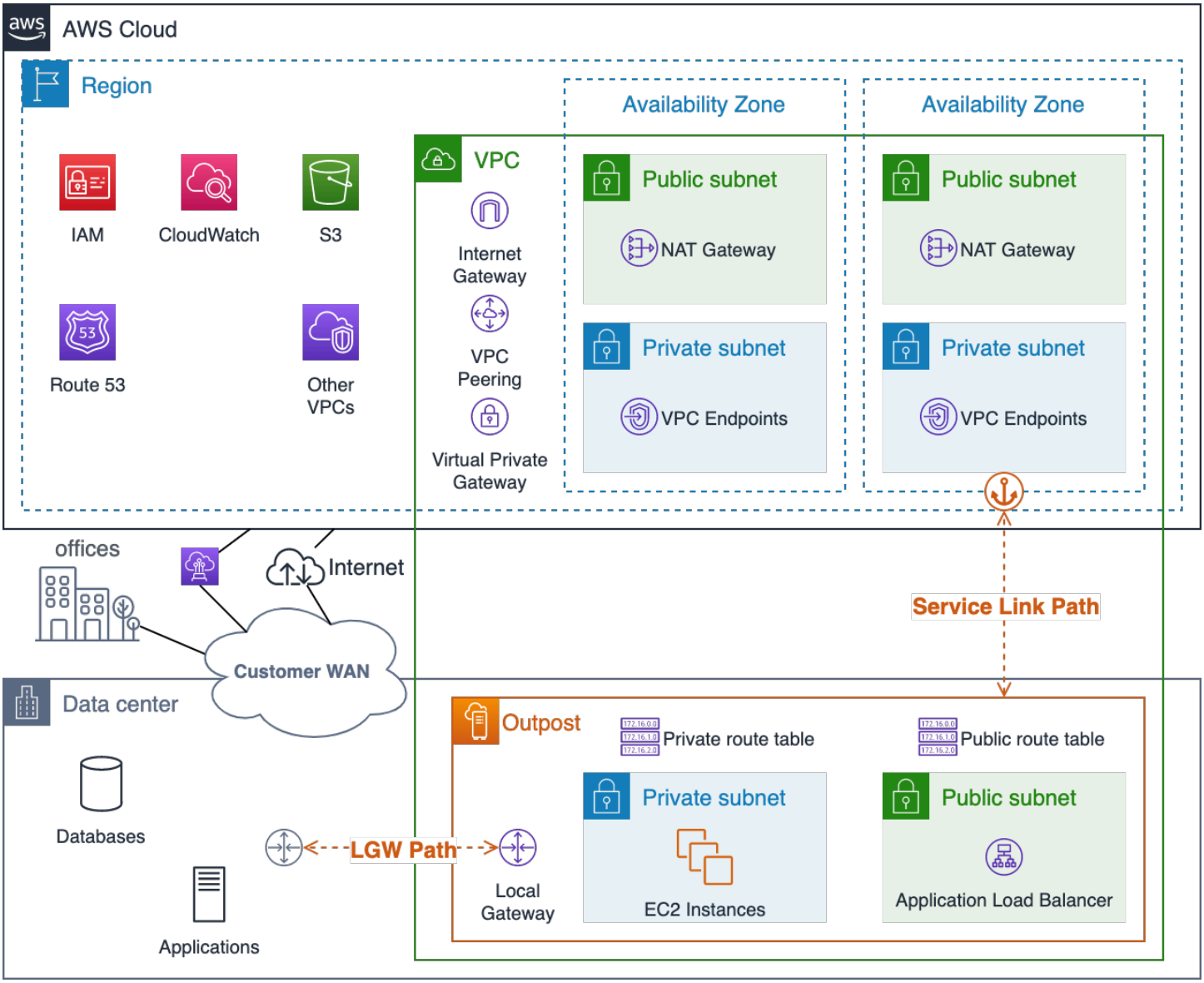
- 预置每个 Outpost 与其在区域内的锚点之间的冗余网络路径。
- 使用 Direct Connect（DX）路径来控制延迟和带宽可用性。
- 确保从前哨服务链路 CIDR 块到父区域的 EC2 IP 地址范围的 TCP 和 UDP 端口 443 处于打开状态（出站）。确保所有网络路径上的端口均处于打开状态。
- 如果您使用的是该地区的 CIDR 范围子集，请跟踪防火墙上的 Amazon EC2 IP 地址范围。
- 确保每条路径都满足带宽可用性和延迟需求。
- 使用动态路由，从而自动重定向流量以绕过网络故障。
- 测试在每条规划的网络路径上路由服务链路流量，以确保路径按预期运行。

应用程序/工作负载路由

应用程序工作负载有两条从 Outpost 传出的路径：

- 服务链接路径：除了将 MTU 限制为 1300 字节外，还要考虑应用程序流量将与 Outposts 控制平面流量竞争。
- 本地网关 (LGW) 路径：请考虑客户的本地网络允许访问本地和中的 AWS 区域应用程序。

您可以配置 Outpost 子网路由表，以控制通过哪条路径访问目标网络。指向 LGW 的路由会使流量从本地网关传出并将其定向到本地网络。指向该区域服务和资源的路由（例如 Internet Gateway、NAT Gateway、Virtual Private Gateway 和 TGW）将使用服务链接来到达这些目标。如果您在同一 Outpost VPCs 上与多个 VPC 对等连接，则两者之间的流量 VPCs 仍保留在 Outpost 上，并且不会使用返回该地区的服务链接。有关 VPC 对等的信息，请参阅 Amazon VPC 用户指南中的 VPCs 使用 VPC 对等连接进行连接。



Outpost 服务链接和 LGW 网络路径的可视化

在规划应用程序路由时，应保持谨慎，考虑到正常操作和网络故障期间的有限路由和服务可用性。如果 Outpost 与区域断开连接，则服务链接路径不可用。

您应该在 Outpost LGW 和关键本地应用程序、系统和用户之间预置不同的路径并配置动态路由。冗余网络路径允许网络绕过故障路由流量，并确保在部分网络出现故障期间，本地资源能够与 Outpost 上运行的工作负载进行通信。

Outpost VPC 路由配置是静态的。您可以通过 AWS 管理控制台 APIs、CLI 和其他基础设施即代码 (IaC) 工具配置子网路由表；但是，在断开连接事件期间，您将无法修改子网路由表。您必须重新建立 Outpost 和区域之间的连接才能更新路由表。正常操作时使用的路由与计划在断开连接事件期间使用的路由相同。

前哨基地上的资源可以通过服务链接和该地区的Internet Gateway（IGW）或通过本地网关（LGW）路径访问互联网。通过 LGW 路径和本地网络路由互联网流量允许您使用现有的本地 Internet 入口/出口点，与使用通往该地区的 IGW 的服务链路路径相比，延迟更低 MTUs、更高、 AWS 数据出站费用更低。

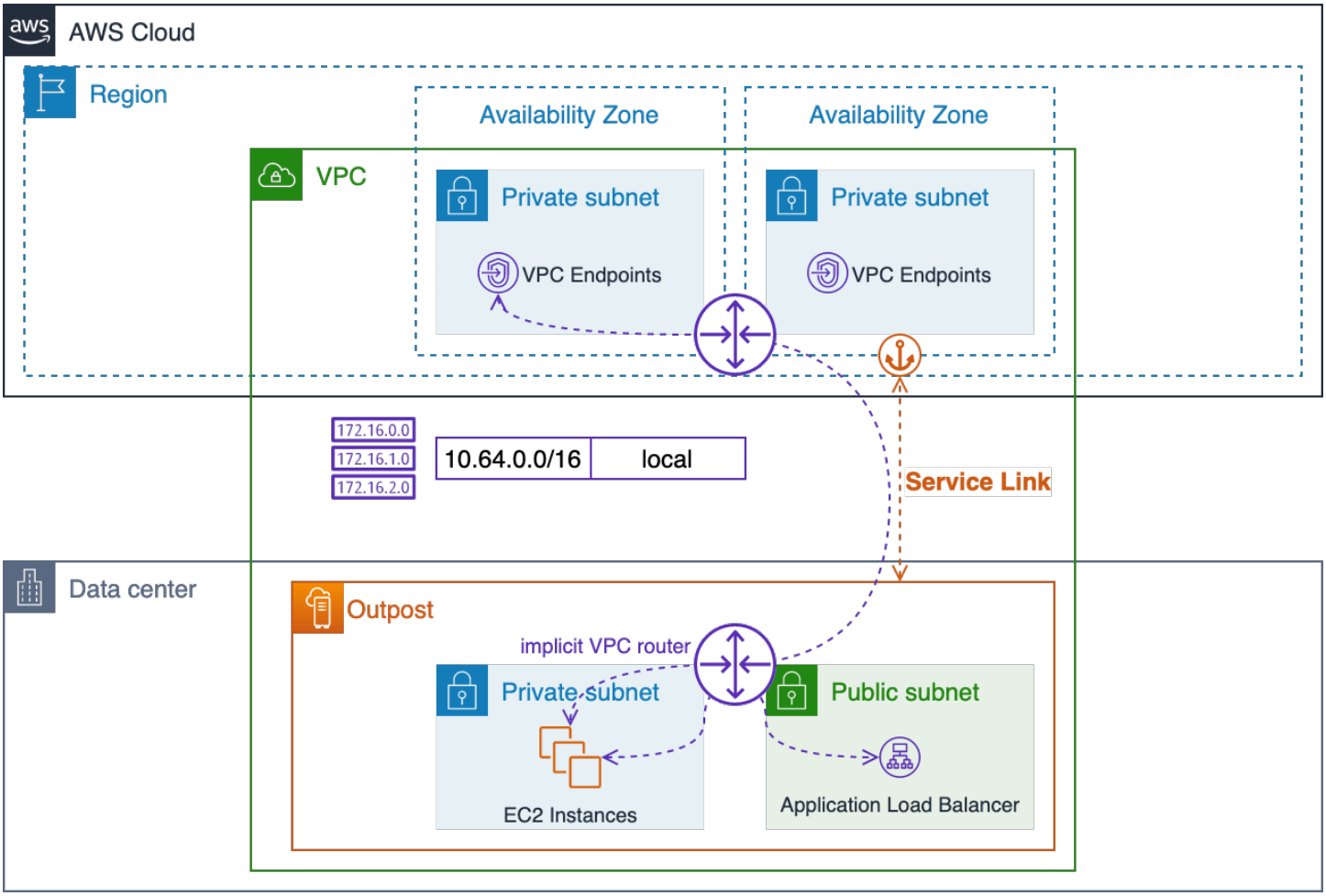
如果应用程序必须在本地运行且需要支持通过公有互联网进行访问，则应通过本地互联网连接将应用程序流量路由到 LGW，以访问 Outpost 上的资源。

虽然您可以用类似于配置区域内的公有子网的方式在 Outpost 上配置子网，但对于大多数使用场景来说，这可能是一种不良实操。入站互联网流量将通过进入， AWS 区域 并通过服务链接路由到前哨基地上运行的资源。

反过来，响应流量将通过服务链路路由，然后通过互联网连接返回。 AWS 区域在流量离开区域流向 Outpost 的过程中，以及在返回流量通过区域返回并传出到互联网的过程中，这种流量模式可能会增加延迟，并且会产生数据输出费用。如果应用程序可以在区域内运行，则区域是其最佳运行位置。

不同 VPC 资源（同一 VPC 内）之间的流量将始终由本地 VPC CIDR 路由，并由隐式 VPC 路由器在子网之间路由。

例如，在 Outpost 上运行的 EC2 实例与该地区的 VPC 终端节点之间的流量将始终通过服务链接进行路由。



通过隐式路由器进行的本地 VPC 路由

应用程序/工作负载路由的推荐做法

- 尽可能使用本地网关 (LGW) 路径而不是服务链接路径。
- 通过 LGW 路径路由互联网流量。
- 使用一组标准路由配置 Outpost 子网路由表，这些路由将用于正常操作和断开连接事件。
- 预置 Outpost LGW 和关键本地应用程序资源之间的冗余网络路径。使用动态路由，从而自动重定向流量以绕过本地网络故障。

计算

虽然亚马逊的 EC2 容量看似 AWS 区域 是无限的，但Outposts的容量是有限的。您负责规划和管理 Outpost 部署的计算容量。

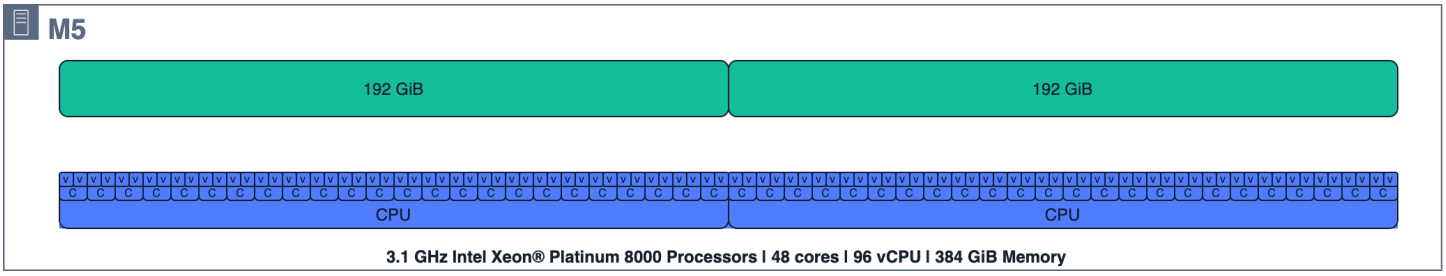
主题

容量规划

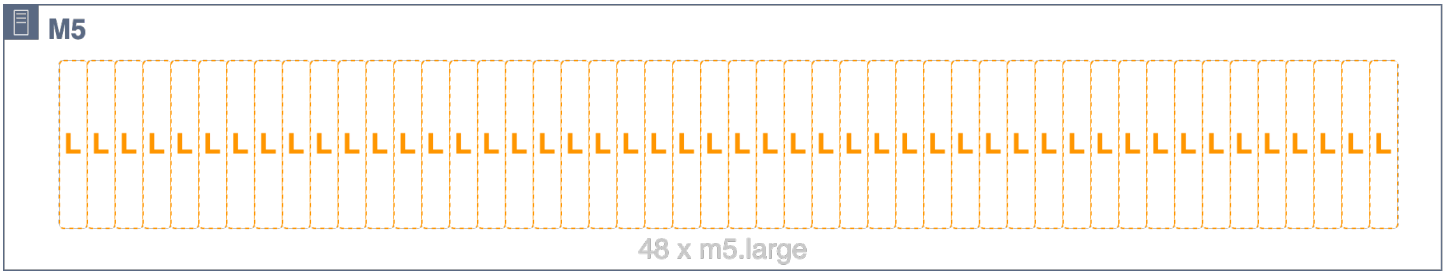
虽然亚马逊的 EC2 容量看似 AWS 区域 是无限的，但Outposts的容量是有限的——受订购的计算容量总量的限制。您负责规划和管理 Outpost 部署的计算容量。您应该订购充足的计算容量以支持 N+M 可用性模型，其中 N 是所需的服务器数量，M 是为应对服务器故障而预置的备用服务器数量。N+1 和 N+2 是最常见的可用性级别。

每台主机（C5M5R5、、等）都支持单一的 EC2 实例系列。在 EC2 计算服务器上启动实例之前，必须提供时段布局，指定您希望每台服务器提供的EC2 实例大小。 AWS 使用请求的时段布局配置每台服务器。

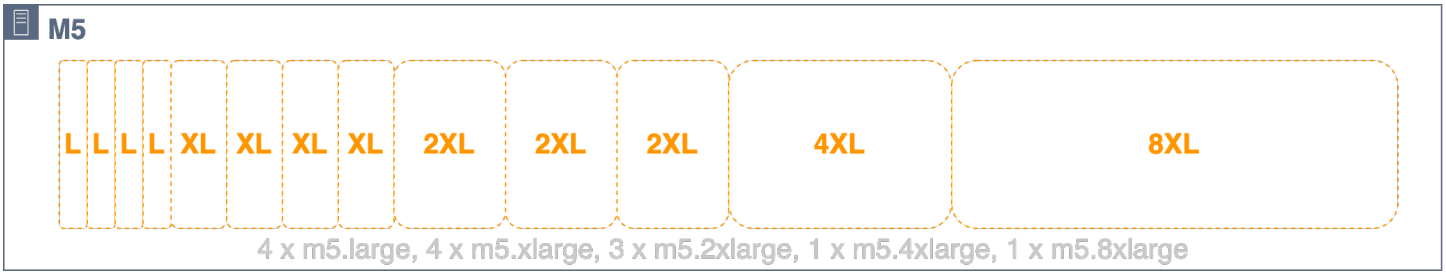
如果所有插槽的实例大小相同（例如，48 个插槽），则主机可以采用同质m5.large插槽，也可以使用混合实例类型（例如 4、4 m5.large、3 m5.2xlarge、1 和 1m5.8xlarge）进行异质插槽m5.xlarge，有关这些插槽配置的可视化效果m5.4xlarge，请参阅接下来的三个图。



*m5.24xlarge*主机计算资源



*m5.24xlarge*主机均匀地插入 48 个插槽 *m5.large*



*m5.24xlarge*主机异质插槽为 4 *m5.large*、4、3 *m5.xlarge* *m5.2xlarge* *m5.4xlarge*、1 和 1 个插槽 *m5.8xlarge*

不必为全部主机容量排定时段。可以将插槽添加到具有可用未分配容量的主机上。您可以使用容量管理修改时段布局， APIs 也可以 UIs 为 AWS Outposts 新容量任务创建新的容量任务。有关更多信息，请参阅机架AWS Outposts 用户指南 AWS Outposts中的容量管理。如果在某些插槽被正在运行的实例占用时无法应用新的时段布局，则可能需要关闭或重启某些实例才能完成新的容量任务。CreateCapacityTaskAPI 允许您表示所示的 Outpost ID 上应显示的每个实例大小的数量，如果由于正在运行的实例而无法完成任务，则会返回必须停止才能满足请求的实例。此时，如果您不想停止其中一个返回的实例，则可以选择性地指明要查看 “N” 个其他选项，也可以指明不应建议将其作为 EC2 实例关闭以满足容量任务请求的实例 ID、实例标签、账户或服务。 EC2 在选择了您想要使用的选项后，我们建议在实施之前使用 Dry Run 参数来验证提议的更改并了解其潜在影响。

所有主机都将其预配置的插槽贡献给 Outpost 上的 EC2 容量池，并且给定实例类型和大小的所有插槽都作为单个 EC2 容量池进行管理。例如，之前带有、、m5.largem5.xlargem5.2xlargem5.4xlarge、和m5.8xlarge插槽的异构插槽主机会将这些插槽贡献给五个 EC2 容量池，每种实例类型和大小各占一个池。这些池可能分布在多个主机上，为了实现工作负载的高可用性，应考虑放置实例。

在为 N+M 主机可用性规划备用 EC2 容量时，必须考虑主机插槽和容量池。 AWS 检测主机何时出现故障或降级，并安排现场访问以更换出现故障的主机。在设计容 EC2 量池时，应允许每个实例系列 (N+1) 中至少有一台服务器在 Outpost 中出现故障。有了这个最低的主机可用性级别，当一台主机出现故障或需要停止服务时，你可以在同一系列的其余主机的备用插槽上重启失败或已降级的实例。

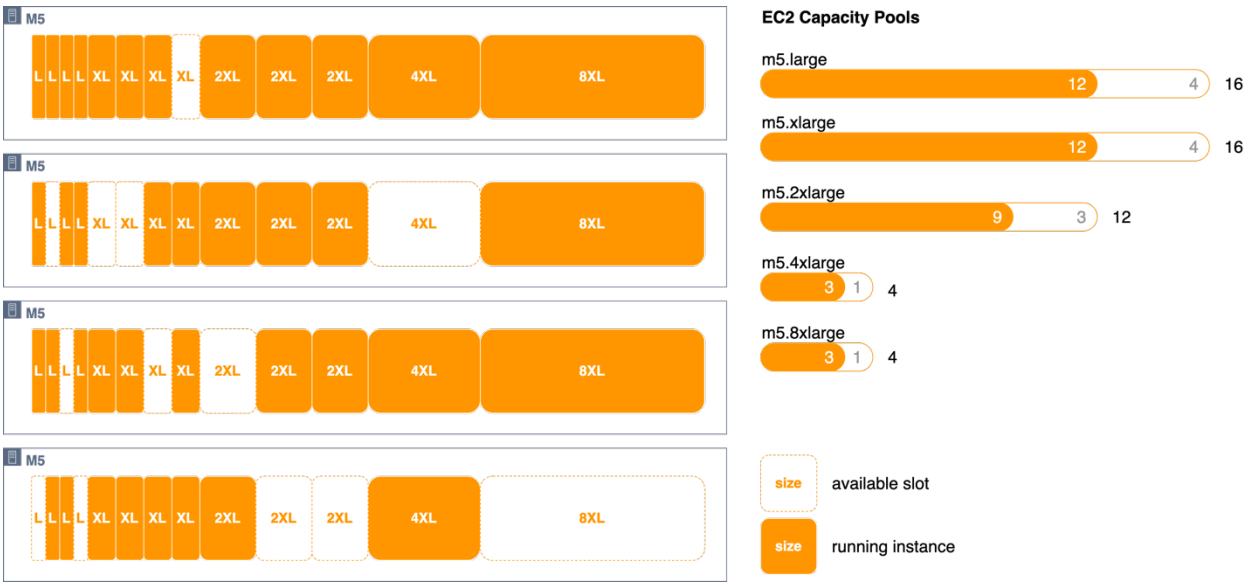
当您拥有同一个插槽的主机或一组具有相同插槽布局的异质插槽主机时，规划 N+M 可用性就很简单了。您只需计算运行所有工作负载所需的主机数量 (N)，然后再添加 (M) 台主机即可满足故障和维护事件期间服务器可用性的要求。

由于 NUMA 边界，以下插槽配置不可用：

- 3 m5.8xlarge
- 1 m5.16xlarge 和 1 m5.8xlarge

请咨询您的 AWS 账户 团队，以验证您计划的 AWS Outposts 机架插槽配置。

在下图中，四m5.24xlarge台主机采用异质开槽，时隙布局相同。四台主机创建了五个 EC2 容量池。每个池都以最大利用率 (75%) 运行，以保持在这四台主机上运行的实例的 N+1 可用性。如果任何主机出现故障，则有足够的空间在其余主机上重启失败的实例。



EC2 主机插槽、正在运行的实例和插槽池的可视化

对于更复杂的时段布局，即主机时段不完全相同，则需要计算每个容量池的 N+M 可用性。 EC2 您可以使用以下公式来计算有多少主机（为给定 EC2 容量池提供插槽）可能出现故障，但仍允许其余主机承载正在运行的实例：

$$M = \left\lceil \frac{poolSlots_{available}}{serverSlots_{max}} \right\rceil$$

其中：

- PoolSlot $_{available}$ s 是给定 EC2 容量池中可用插槽的数量（池中的插槽总数减去正在运行的实例数）
- ServerS $_{max}$ lot s 是任何主机为给定 EC2 容量池贡献的最大插槽数
- M 是可能出现故障但仍允许其余主机承载正在运行的实例的主机数量

示例：前哨基地有三台主机为m5.2xlarge容量池提供插槽。第一个提供4个插槽，第二个提供3个插槽，第三个主机贡献2个插槽。Outpost 上的m5.2xlarge实例池总容量为 9 个插槽（4 + 3 + 2）。前

哨基地有 4 个正在运行的`m5.2xlarge`实例。有多少主机可能出现故障，但仍允许其余主机承载正在运行的实例？

$$poolSlots_{available} = total\ capacity - running\ instances = 9 - 4 = 5$$

$$serverSlots_{max} = \max([4, 3, 2]) = 4$$

$$M = \left\lceil \frac{poolSlots_{available}}{serverSlots_{max}} \right\rceil = \left\lceil \frac{5}{4} \right\rceil = [1.25] = 1$$

答：您可能会丢失任何一台主机，但仍将正在运行的实例放在剩余的主机上。

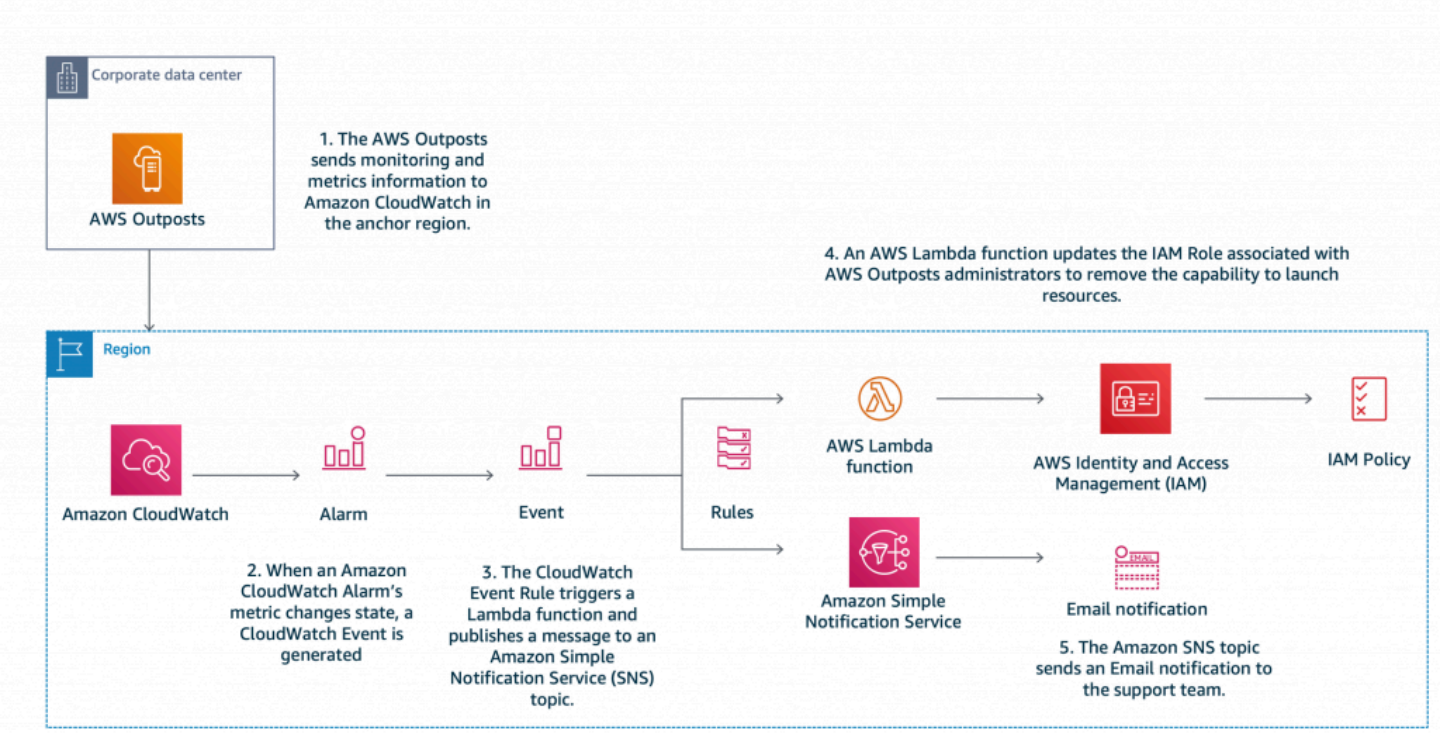
计算容量规划的推荐做法

- 调整计算容量，为前哨基地上的每个 EC2 容量池提供 N+M 冗余。
  - 为采用同构槽配置或具有相同布局的异构槽配置的服务器部署 N+M 服务器。
  - 计算每个容量池的 N+M 可用性，并确保每个 EC2 容量池都满足您的可用性要求。

容量管理

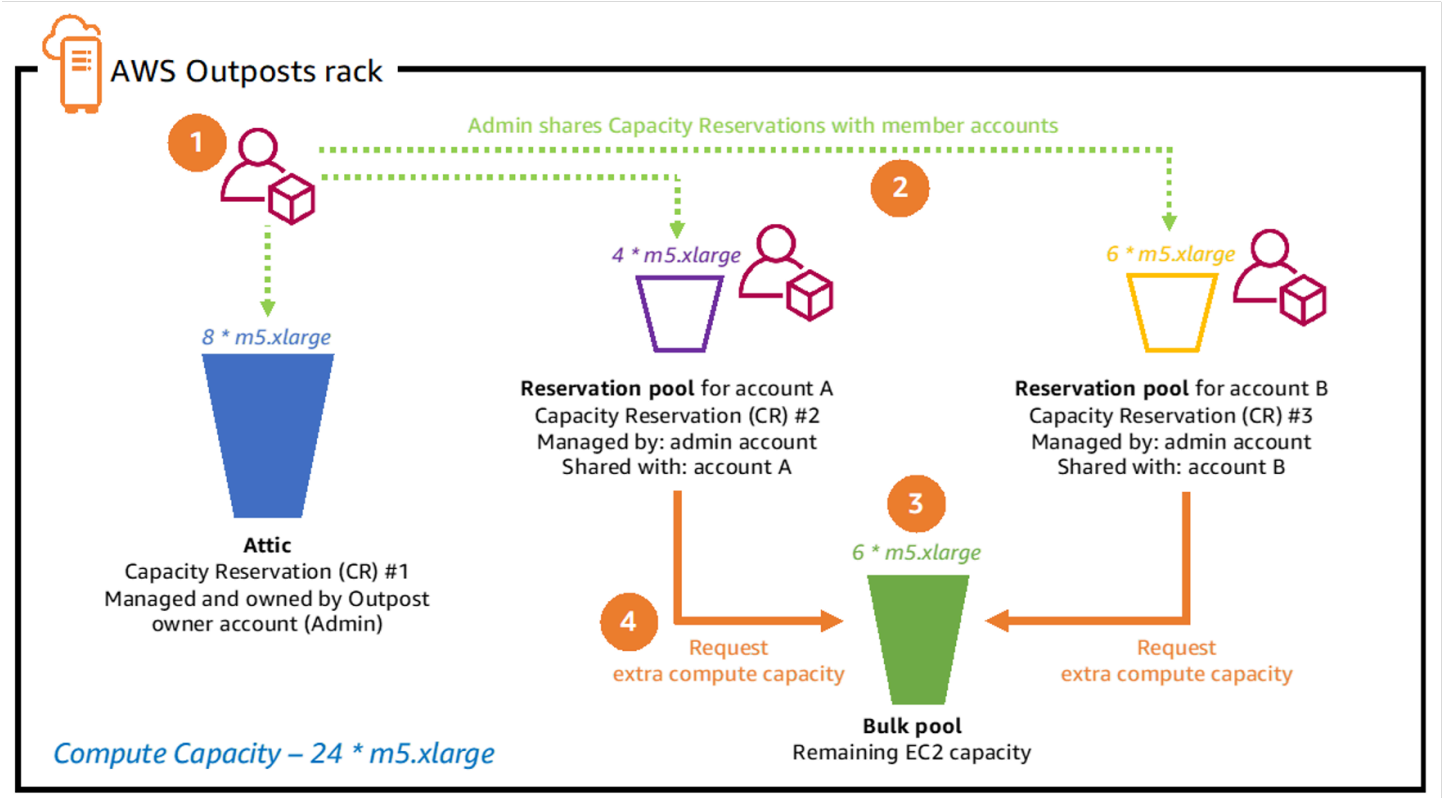
您可以通过亚马逊指标 AWS 管理控制台 和通过 Amazon CloudWatch 指标监控 Outpost EC2 实例池的利用率。请联系 Enterprise Support 以检索或更改 Outpost 的槽布局。

您可以使用相同的实例自动恢复和 EC2 Auto Scaling 机制来恢复或替换受服务器故障和维护事件影响的实例。您必须对 Outpost 容量进行监控和管理，以确保始终有充足的备用容量来应对服务器故障。使用 Amazon 管理 AWS Outposts 容量 CloudWatch 和 AWS Lambda博客文章提供了一个动手教程，向您展示了如何合并 AWS CloudWatch 和 AWS Lambda 管理 Outpost 容量以保持实例可用性。

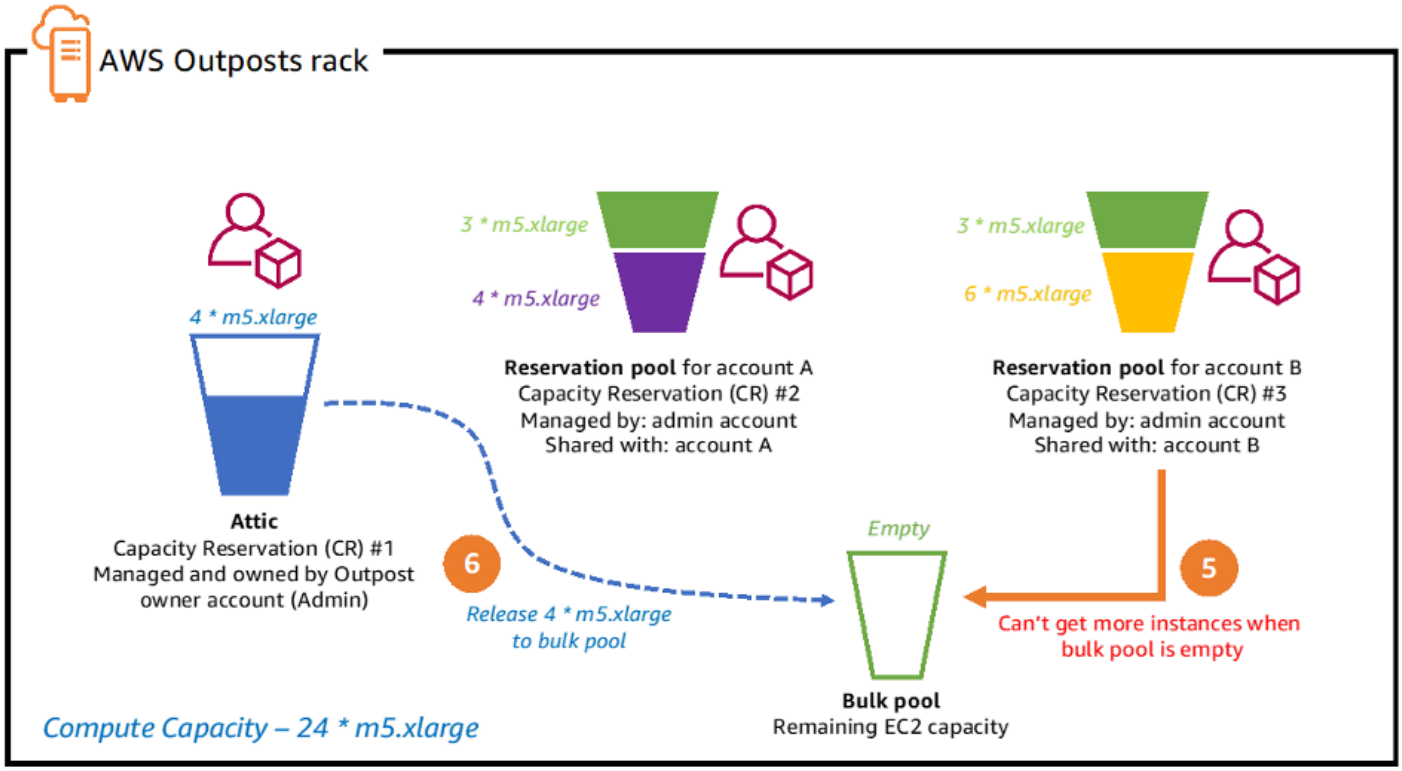


使用 Amazon 管理 AWS Outposts 容量 CloudWatch 和 AWS Lambda

容量预留可在多账户环境中使用，以控制单个账户或包含多个账户的 AWS 组织单位 (OU) 使用的 Outpost 计算容量。你可以在 Outposts EC2 上为亚马逊创建容量预留，也可以为受支持的 Outposts 创建容量预留， AWS 服务 例如亚马逊 Elastic Kubernetes Service (EKS)、亚马逊弹性容器服务 (ECS) 和亚马逊弹性地图缩减 (EMR)。 容量预留是通过 Outpost 所有者账户中的 AWS Resource Access Manager (AWS RAM) 创建并共享给账户的。“使用 EC2 容量预留在 AWS Outposts 机架上创建计算配额” 共享提供了动手教程和其他指导，说明如何为容量管理目的在 Outpost 中实现容量预留。



Capacity Reservation sharing process steps 1-4



Capacity Reservation sharing process steps 5-6

计算容量管理的推荐做法

- 在 Auto Scaling 组中配置您的 EC2 实例，或者使用实例自动恢复来重启失败的实例。
- 自动监控 Outpost 部署的容量，并配置容量警报的通知和（可选的）自动响应。
- 使用容量预留可以精细控制与 AWS 组织内其他账户共享的计算容量。

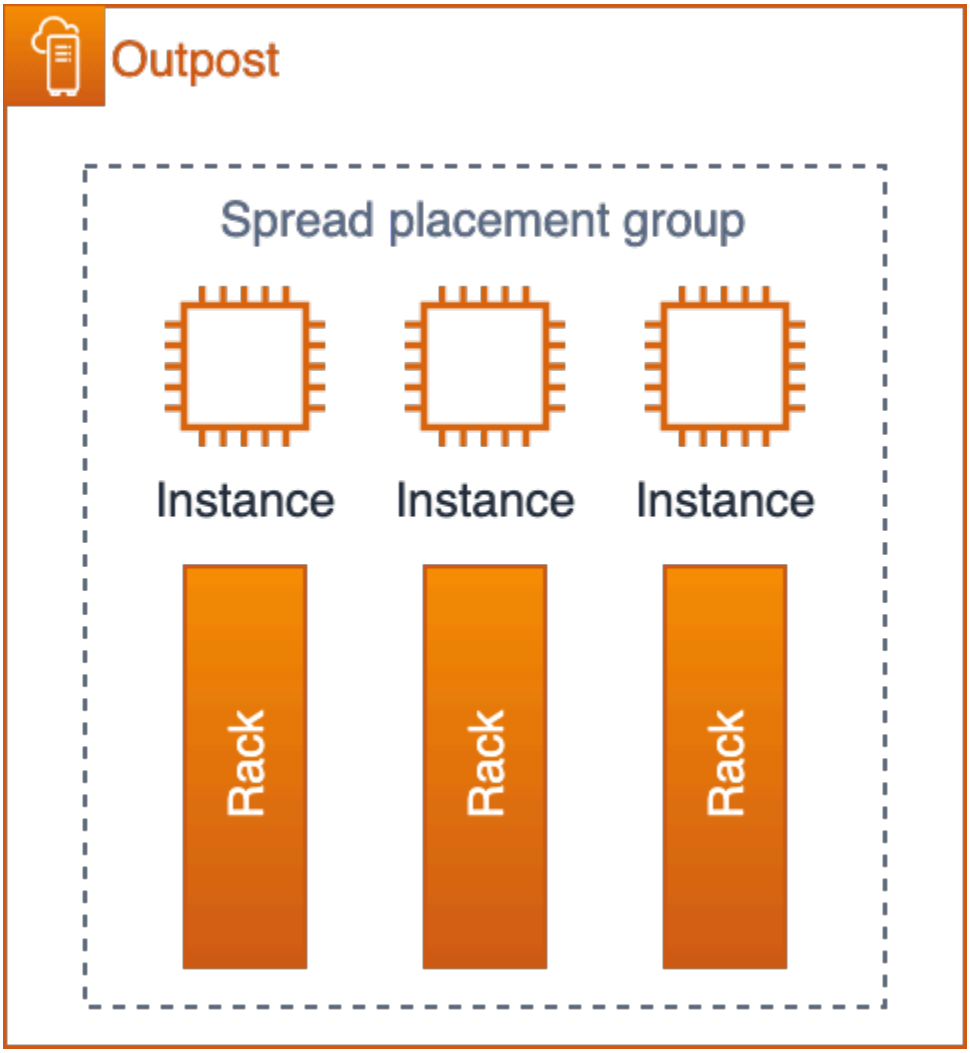
实例置放

Outposts 的计算主机数量有限。如果您的应用程序在 Outposts 上部署了多个相关实例；无需额外配置，则这些实例可能会部署在相同的主机上或同一机架的主机上。如今，您可以使用三种机制来分配实例，以降低在同一基础设施上运行相关实例的风险：

多 Outpost 部署：与区域内的多 AZ 策略类似，您可以将 Outpost 部署到单独的数据中心，并将应用程序资源部署到特定的 Outpost。这使您能够在所需的 Outpost（一组逻辑机架）上运行实例。使用直接 VPC 路由在多个前哨基地之间进行的 VPC 内部通信是另一种策略，它可以使用 Outpost 本地网关 (LGW) 在前哨基地的子网之间创建路由，在同一 VPC 内的多个前哨站之间分配工作负载。可以采用多前哨策略来防范机架和数据中心故障模式，如果Outposts固定在单独的区域 AZs 或区域，也可以提供针对可用区或区域故障模式的保护。有关多 Outpost 架构的更多信息，请参阅更大规模的故障模式。

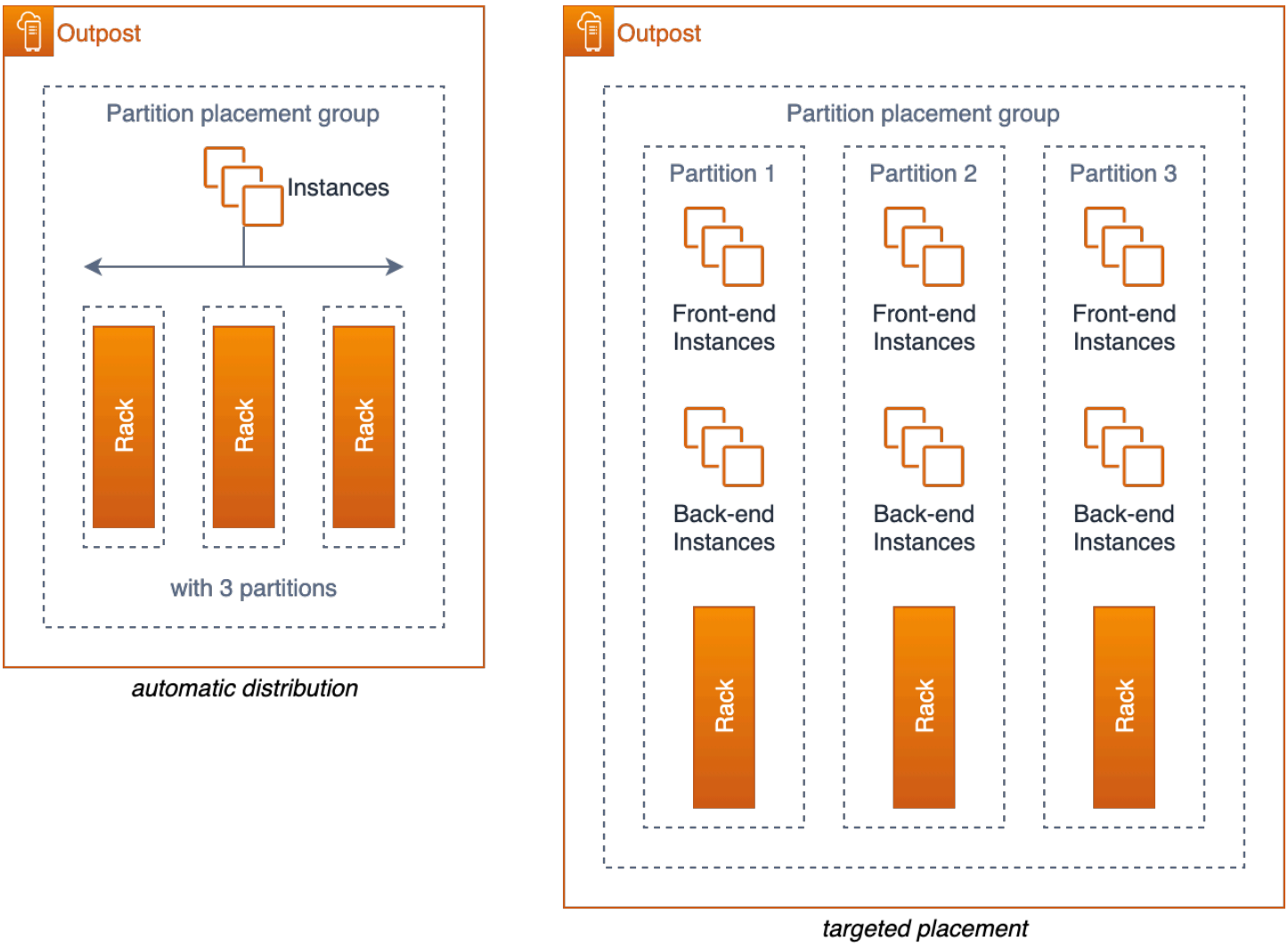
Outposts 上的亚马逊 EC2 置放群组（单个 Outpost 多机架实例放置）— 您可以在账户中创建的 Outposts 上创建置放群组。从而将实例分布在您站点中的 Outpost 上的底层硬件上。当您在 Outpost 上创建具有分布策略的置放群组时，您可以选择让置放群组跨主机或机架分布实例。

分布置放群组提供了一种在机架或主机之间分配单个实例的简单方法，以减少出现相关故障的可能性。在群组中部署的实例数量只能与前哨基地中的主机数量相同。



EC2 在有三个机架的前哨基地上分散放置组

您还可以使用分区置放群组跨多个机架分配实例。使用自动分配跨群组中的分区分布实例或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，同时跨机架分配其他资源。例如，如果您有一个具有三个机架的逻辑 Outpost，则通过创建一个包含三个分区的分区置放群组，您可以跨机架分配资源。



EC2 在带有三个机架的前哨基地上对放置组进行分区

富有创造性的服务器槽配置：如果您使用的是单机架 Outpost，或者您在 Outpost 上使用的服务不支持置放群组，则可以使用富有创造性的槽配置来确保实例不会部署在同一台物理服务器上。如果相关实例的 EC2 实例大小相同，则可以对服务器进行插槽以限制每台服务器上配置的该大小的插槽数量，从而将插槽分布在服务器上。服务器槽配置将限制可在单台服务器上运行的（该大小）实例的数量。

以前文中图 13 所示的槽布局为例。如果您的应用程序需要在配置了此时段布局的 Outpost 上部署三个`m5.4xlarge`实例，则可以 EC2 将每个实例放在单独的服务器上，并且这些实例不可能在同一台服务器上运行，前提是插槽配置不更改为在服务器上打开更多`m5.4xlarge`插槽。

计算实例放置的推荐做法

- 在 Outpo EC2 sts 上使用 Amazon 置放群组来控制实例在单个逻辑 Outpost 中跨机架的放置。

- 与其订购带有单个中型或大型 Outpost 机架的 Outpost，不如考虑将容量分成两个小型或中型机架，这样您就可以利用 EC2 置放组在机架之间分配实例的能力。
- Outposts 上的 Amazon EC2 置放群组可用于影响 EKS 节点组、EKS 本地集群的控制平面节点和 ECS 任务的放置。
- 使用 VPC 内部通信将工作负载分散到同一 VPC 内的多个 Outposts。

存储

机 AWS Outposts 架服务提供三种存储类型：

- 支持的@@ 实例类型上的 EC2 实例存储
- 用于持久块存储的 Amazon Elastic Block Store（EBS）gp2 卷
- 用于本地对象存储的 Amazon Simple Storage Service on Outposts（S3 on Outposts）

实例存储在支持的服务器（C5d、M5d、R5d、G4dn 和 I3en）上提供。就像在区域内一样，实例存储中的数据仅在实例的（运行）生命周期内保留。

Outposts EBS 卷和 S3 on Outposts 对象存储作为 AWS Outposts 机架托管式服务的一部分提供。客户负责管理 Outpost 存储池的容量。客户在订购 Outpost 时指定他们对 EBS 和 S3 存储的存储要求。AWS 使用提供请求的存储容量所需的存储服务器数量来配置 Outpost。 AWS 负责 Outposts 上的 EBS 和 S3 存储服务的可用性。预置足够数量的存储服务器，从而为 Outpost 提供高度可用的存储服务。丢失单个存储服务器时，服务不应中断，也不应导致数据丢失。

你可以使用 AWS 管理控制台 和CloudWatch 指标来监控 Outposts 上的 Outpost EBS 和 S3 的容量利用率。

数据保护

对于 EBS 卷： AWS Outposts 机架支持 EBS 卷快照，以提供一种简单而安全的数据保护机制来保护您的块存储数据。快照是 EBS 卷的 point-in-time增量备份。默认情况下，Outpost 上的 Amazon EBS 卷快照存储在区域内的 Amazon S3 上。如果已将 Outpost 配置为 S3 on Outposts 容量，则可以借助 EBS Local Snapshots on Outposts，将快照本地存储在使用 S3 on Outposts 存储的 Outpost 上。

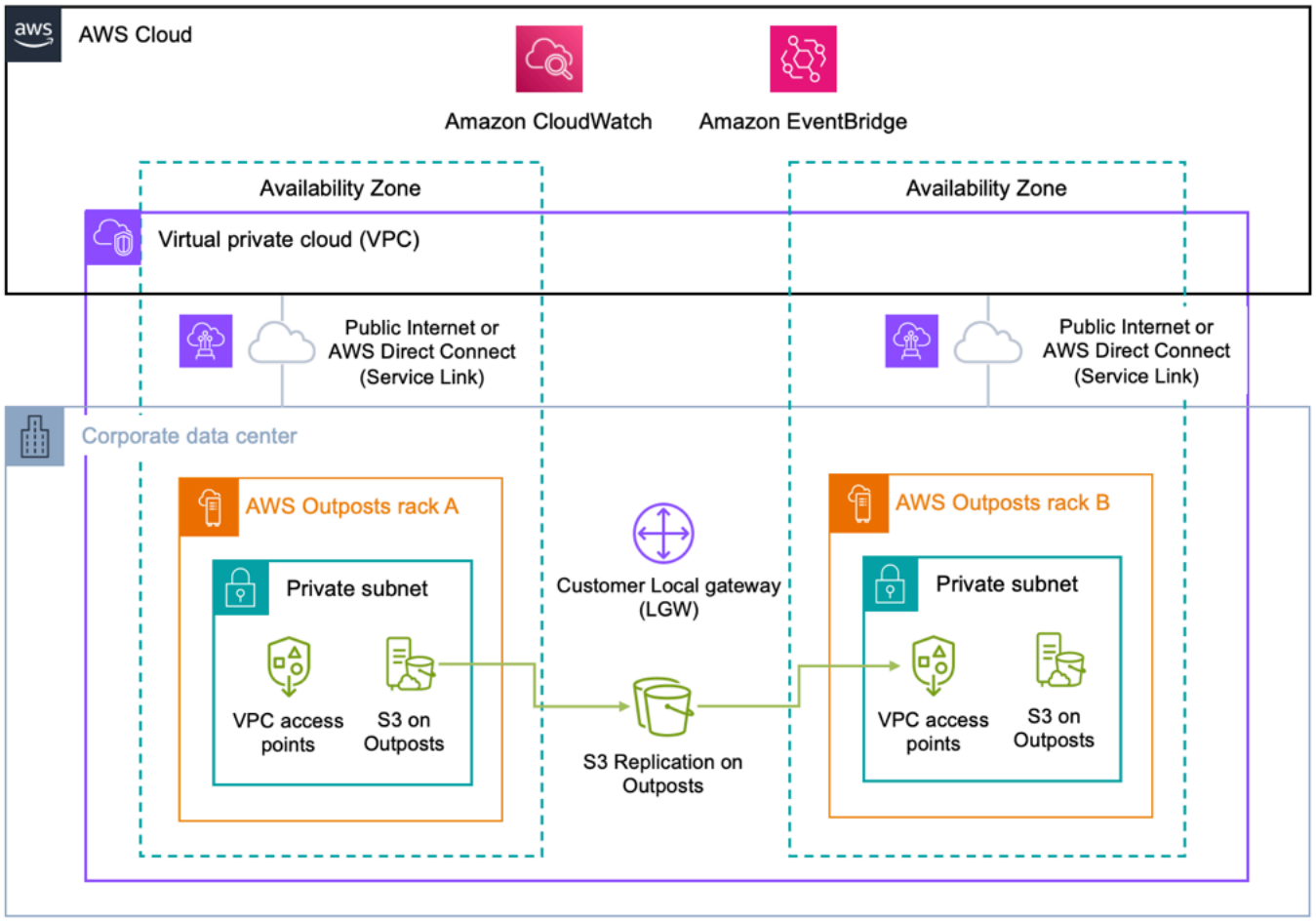
对于 S3 on Outposts 桶（数据驻留使用场景）：

- 您可以使用 Outpost 上的 S3 版本控制功能来保存所有更改和对象历史记录。启用后，S3 版本控制功能将对象的多个不同副本保存到同一个存储桶中。对于 Outpost 桶中存储的每个对象，您可以使

用 S3 版本控制功能来保留、检索和还原其每个版本。S3 版本控制功能可帮助您从用户意外操作和应用程序故障中恢复。

- 您可以使用 Outpost 上的 S3 复制功能来创建和配置复制规则，以将 S3 对象自动复制到其他 Outpost 或同一 Outpost 上的其他桶。在复制过程中，S3 on Outposts 对象通过客户的本地网关（LGW）发送，并且对象不会返回到 AWS 区域。Outposts 上的 S3 复制提供了一种简单灵活的方式，可以在特定的数据边界内自动复制数据，以满足数据冗余和合规性要求。

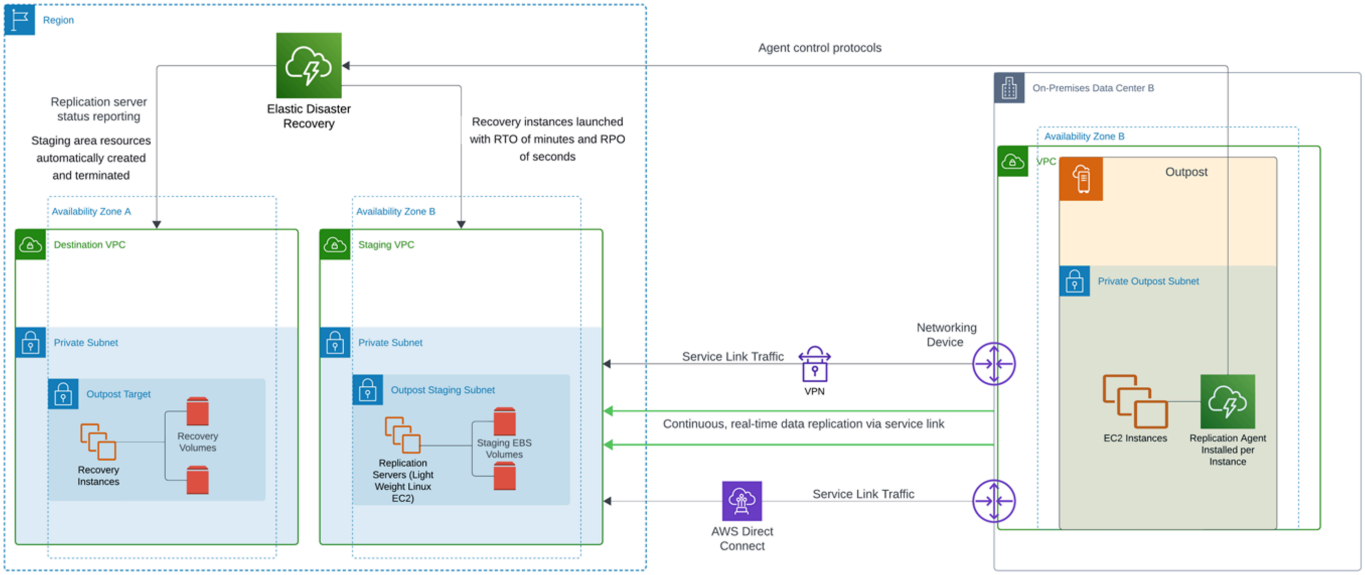
  Outpost 上的 S3 复制功能还提供了详细的指标和通知，以监控对象复制的状态。您可以使用 Amazon 跟踪源和目标 Outposts 存储桶之间的待处理字节、待处理操作以及复制延迟，从而监控复制进度。 CloudWatch您还可以设置 Amazon EventBridge 规则以接收复制失败事件，从而快速诊断和更正配置问题。有关如何配置的更多详细信息，请参阅 Outposts 上的 Amazon S3 复制 YouTube 视频。



对于 Outposts 上的 S3 存储桶（非数据驻留用例），可以 AWS 区域：您可以使用自动在 Outposts 上的AWS DataSync Amazon S3 在您的 Outpost s 和该地区之间传输数据。 DataSync 允许您选择要传输的内容、何时传输以及使用多少带宽。通过将本地 S3 on Outposts 桶备份到 AWS 区域 中的

S3 桶中，您可以利用 99.999999999%（11 个 9）的数据持久性和其他存储层（标准、不频繁访问和 Glacier）来优化区域 S3 服务的成本。

实例复制：您可以使用 AWS 弹性灾难恢复 (AWS DRS) 将单个实例和附加的块存储从本地系统复制到前哨基地、从前哨基地复制到区域、从区域复制到前哨基地，或者从一个前哨基地复制到另一个前哨基地。使用 AWS Elastic 灾难恢复在 AWS Outposts 机架上进行灾难恢复架构博客文章描述了每种场景以及如何使用 AWS DRS 设计解决方案。



从 Outpost 到区域的灾难恢复（DR）

使用 AWS Outposts 机架作为 AWS DRS 目标（复制目标）需要 Outposts 上的 S3 存储，该存储用于存储复制的 Amazon EBS 快照。还需要在源 Outposts 上使用 S3 存储空间进行故障恢复。Outposts 机架必须使用直接 VPC 路由 (DVR) 才能使用 DRS。 AWS AWS DRS 不能用于保护 Outposts 上的托管服务实例，仅支持 EC2实例及其连接的 EBS 卷的灾难恢复。

针对数据保护的建议实操：

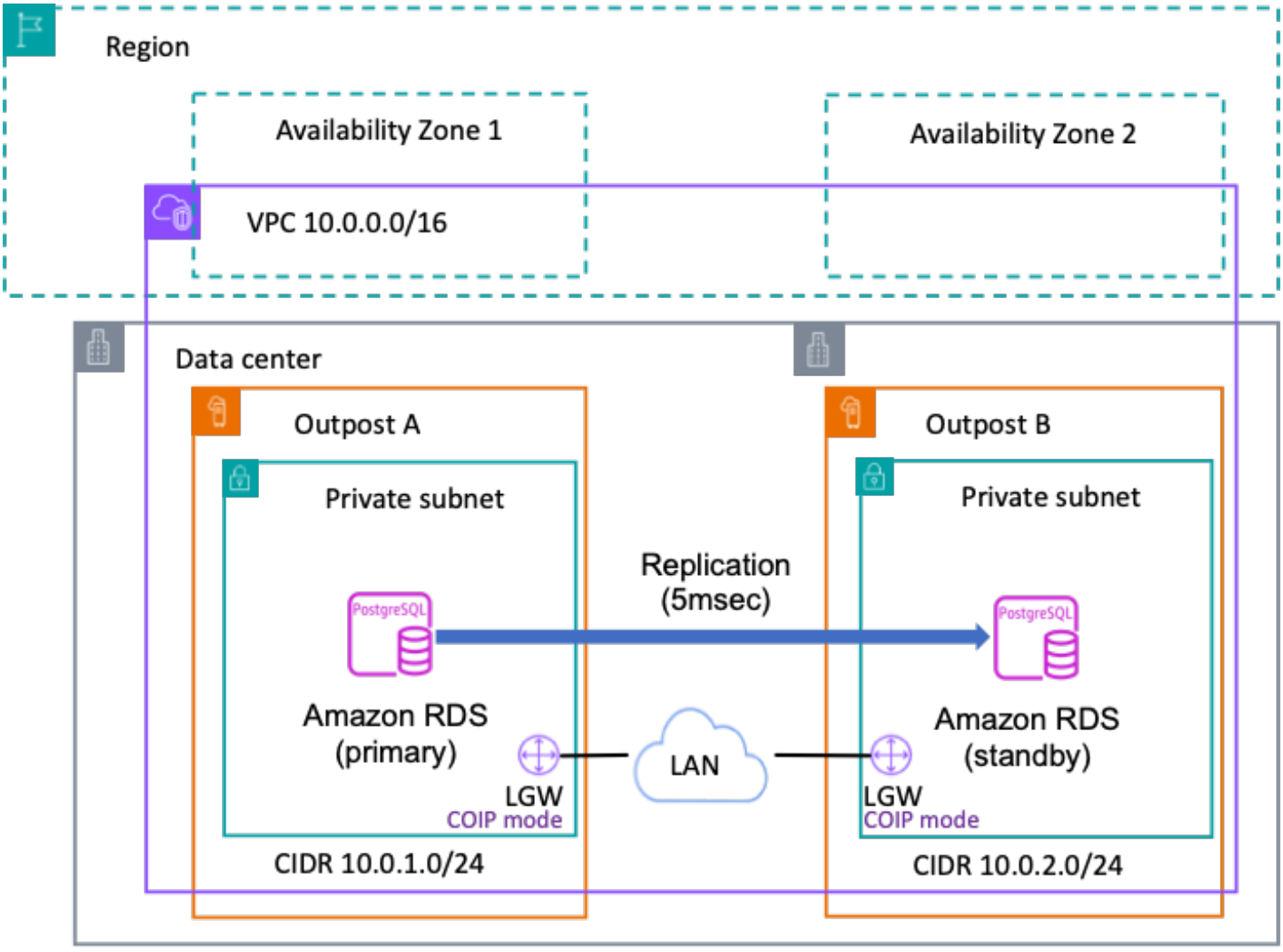
- 使用 EBS 快照将块存储卷 point-in-time备份到该区域的 Amazon S3 或 Outposts 上的 S3。
- 使用 S3 on Outposts 对象版本控制功能来保留对象的多个版本和历史记录。
- 使用 Outpost 上的 S3 复制功能将对象数据自动复制到其他 Outpost。
- 对于非数据驻留用例，请使用 AWS DataSync 将存储在 Outpost 上 S3 中的对象备份到该地区的 Amazon S3。
- 使用 AWS DRS 在本地系统、逻辑 Outposts 和区域之间复制实例。

数据库

亚马逊关系数据库服务 (RDS) 将适用于 SQL Server 的 RD AWS Outposts S、适用于 MySQL 的 RDS 和适用于 PostgreSQL 数据库的 RDS 扩展到部署。 AWS Outposts 对于那些必须提供高可用架构的部署，Amazon RDS 支持在 PostgreSQL 和 MySQL 上部署多可用区实例。 AWS Outposts

带多可用区的 Outposts 上的 Amazon RDS

在多可用区部署中，Amazon RDS 在一个可用区上创建主数据库实例， AWS Outposts 然后 RDS 将数据同步复制到不同 Outposts 上的备用数据库实例。为了提供弹性架构，两者 AWS Outposts 必须锚定在给定区域的不同可用区，并且必须以客户自有的 IP (CoIP) 模式运行。为了允许在主实例和备用实例之间进行复制，两个 Outposts 之间必须有网络链接，往返时间 (RTT) 延迟为个位数毫秒。我们建议 5 毫秒或更短。还要考虑用足够的带宽调整 Outposts 之间的复制链路，以避免将复制作业排队。



带有多可用区的 Outpost 上的 Amazon RDS

使用多可用区的 Outposts 上的 Amazon RDS 注意事项

查看在多可用区中部署 Amazon RDS on Outposts 的以下注意事项：

- 将至少两个 Outposts 部署锚定在同一个可用区的不同可用区。 AWS 区域
- 每个 Outposts 部署的主实例和备用实例都需要一个 VPC 和一个子网。
- 将数据库实例的 VPC 与所有本地网关路由表相关联。
- 确保你的 Outposts 使用客户拥有的 IP 路由。
- 您的本地网络必须允许使用 UPD 端口 500 的 Outposts for Internet 安全协会和密钥管理协议 (ISAKAMP) 和使用 UDP 端口 4500 的 IPsec 网络地址转换遍历 (NAT-T) 之间的出站和相关入站流量。
- 多可用区部署不支持本地 RDS 备份。
- 如果您的工作负载必须遵守您所在行业或地区的数据驻留规定，请咨询监管机构，以确定多可用区 RDS 能否满足您的要求。

有关更多详细信息，请参阅在 AWS Outposts 上使用 Amazon RDS 的多可用区部署。

只 AWS Outposts 读副本上的 Amazon RDS

Amazon RDS 只读副本为 Amazon RDS 数据库 (DB) 实例提供了增强的性能和耐久性。它们可以轻松地弹性地横向扩展，超越单个数据库实例的容量限制，以应对读取密集型数据库工作负载。Amazon RDS 上 AWS Outposts 使用 MySQL 和 PostgreSQL 数据库引擎的内置复制功能从源数据库实例创建只读副本。源数据库实例将成为主数据库实例。对主数据库实例进行的更新将异步复制到只读副本。只读副本使用客户拥有的 IP (CoIP) 模型，并且复制在您的本地网络上运行。

Outposts 只读副本上的 Amazon RDS 注意事项

查看以下针对只读副本部署 Amazon RDS on Outposts 的注意事项：

- 您无法为 RDS on Outposts 上的 RDS for SQL Server 数据库实例创建只读副本。
- RDS on Outposts 不支持跨区域只读副本。
- RDS on Outposts 不支持级联只读副本。
- 源 RDS on Outposts 数据库实例不能具有本地备份。源数据库实例的备份目标必须是您的 AWS 区域。确保您有至少 500 mbps 的冗余服务链路连接，以便将 RDS 备份发送到数据频繁变化或写入流量大的 AWS 区域 数据库。
- 只读副本需要客户拥有的 IP（CoIP）池。

- 只能在与源数据库实例相同的虚拟私有云（VPC）中，在 RDS on Outposts 上创建只读副本。
- RDS on Outposts 上的只读副本可以位于与源数据库实例相同的 Outpost 上或同一 VPC 中的另一个 Outpost 上。
- 您无法为使用 AWS KMS 外部密钥存储 (XKS) 加密的数据库实例创建只读副本。
- 创建您的只读副本作为多可用区数据库实例与源数据库是否为多可用区数据库实例无关。

Amazon RDS 存储自动扩缩功能已开启 AWS Outposts

如果您的工作负载是不可预测的，则可以为 Amazon RDS 数据库实例启用存储自动扩展。上的 Amazon Relational Database Service (Amazon RDS) AWS Outposts 支持手动和自动存储扩展。启用存储自动扩展后，当 Amazon RDS 检测到您的数据库实例的可用数据库空间用完时，它会根据您的 Outposts 部署的 EBS 容量大小自动扩展您的存储。该功能提供的功能与 A mazon RDS Autoscaling 指南中提供的功能相同，在这些区域存在一些适用于自动扩展的特定因素。请务必仔细管理在 Outposts 上为 RDS 实例分配的最大存储空间，因为 EBS 资源仅限于 Outpost 中配置的容量。Amazon RDS 存储自动扩展允许您设置最大存储限制，确保您的部署保持在可用的 EBS 容量之内。有关管理 Outposts 容量的更多信息，请参阅本白皮书的容量管理部分。

AWS Outposts 本地备份上的 Amazon RDS

AWS Outposts启用的 Amazon RDS 本地备份使您可以直接从本地存储在 Outposts 上的 S3 中恢复 RDS 数据库实例。与从中恢复相比，这使您能够满足数据驻留要求并减少延迟 AWS 区域。启用 Amazon RDS 后 AWS Outposts，您可以选择以下还原选项：

- 来自存储在父区域或本地的 Outposts 上的手动数据库快照。
- 自动备份（point-in-time 恢复）：
  - 如果从父级还原 AWS 区域，则可以将备份存储在Outposts AWS 区域 或Outposts上。
  - 如果从你的 Outposts 恢复，则备份必须存储在支持 S3 的 Outposts 本地。

上的 Amazon RDS 本地备份注意事项 AWS Outposts

要在上使用 Amazon RDS 本地备份，请参阅以下注意事项 AWS Outposts：

- 你需要 Outposts 上的 S3 容量才能在本地存储备份。
- MySQL 和 PostgreSQL 数据库实例支持本地备份。
- 多可用区实例部署或只读副本不支持本地备份。

导出和恢复 RDS 的快照 AWS Outposts

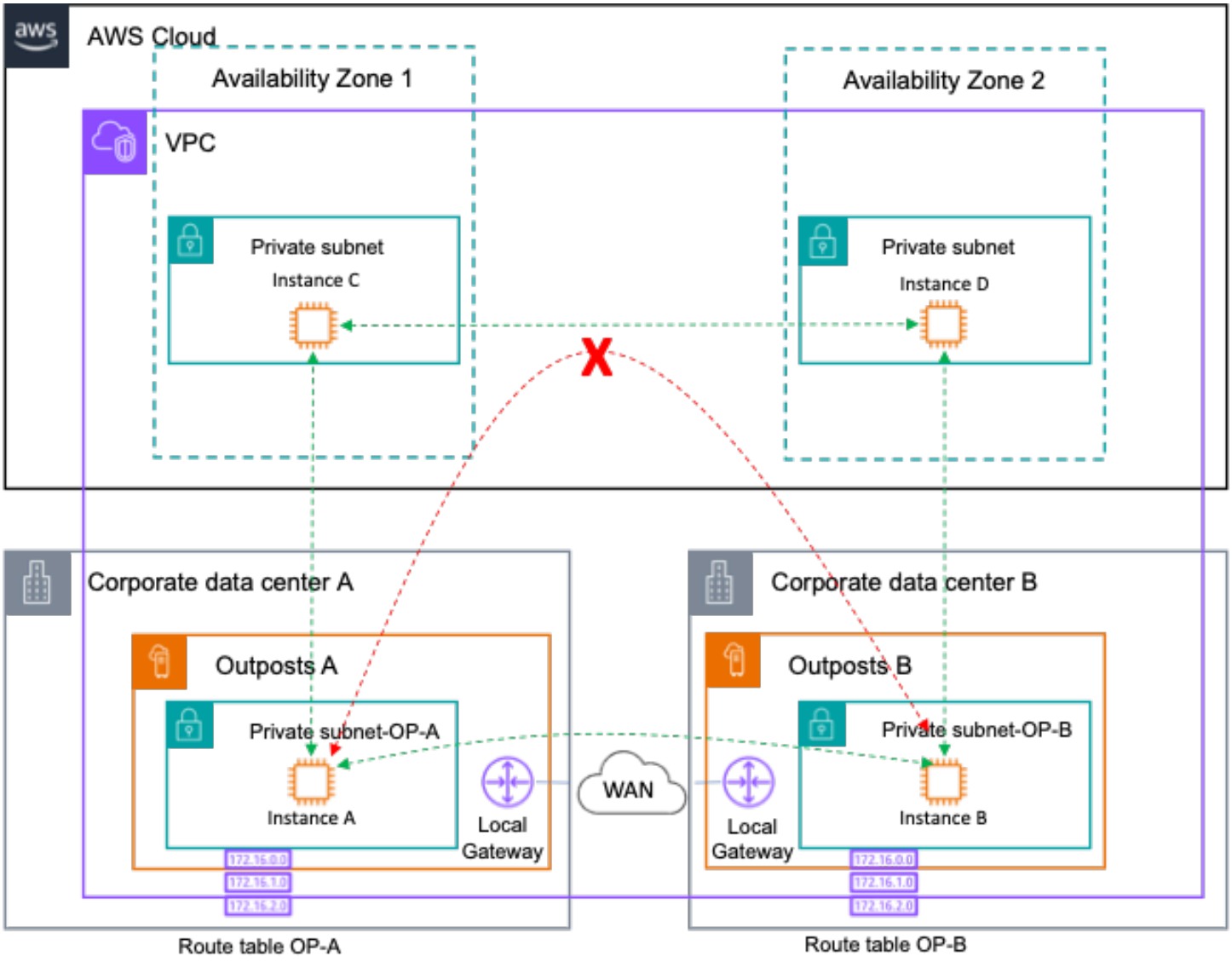
将快照导出到 S3 并从 Amazon S3 恢复数据库实例：虽然可以直接从 Amazon S3 中导出或恢复 RDS 快照 AWS 区域，但 AWS Outposts 环境中不支持这样做。

更大规模的故障模式

要设计 HA 架构以缓解更大规模的故障模式 [例如机架、数据中心、可用区（AZ）或区域故障]，您应该在配备独立电源和 WAN 连接的单独数据中心中部署具有充足基础设施容量的多个 Outpost。您可以将 Outposts 锚定到一个 AWS 区域 或多个区域内的不同可用区 (AZs)。您还应在位置之间配置弹性和足够的 site-to-site连接，以支持同步或异步数据复制以及工作负载流量重定向。根据您的应用程序架构，您可以在 Outpo sts 上使用全球可用的 Amazon R oute 53 DNS 和 Amazon Rout e 53 将流量引导到所需位置，并在发生大规模故障时自动将流量重定向到幸存的地点。

Outposts 机架 VPC 内部路由

AWS Outposts rack 支持跨多个 Outposts 的 VPC 内部通信。两个独立的逻辑 Outposts 上的资源可以使用 Outpost 本地网关 (LGW) 在同一 VPC 内的子网之间路由流量，从而相互通信。通过跨多个 Outposts 的 VPC 内部通信，您可以使用本地 LGW 作为下一跳向其他 Outposts 子网添加更具体的路由，从而覆盖与 Outposts 子网关联的路由表中的本地路由。它可以为架构需要在两个逻辑前哨之间跨一个 VPC 的应用程序提供优势，比如跨越两个 Outposts 机架的 Amazon ECS 或者跨越两个 Outposts 机架的 Amazon EKS 集群。 AWS Outposts

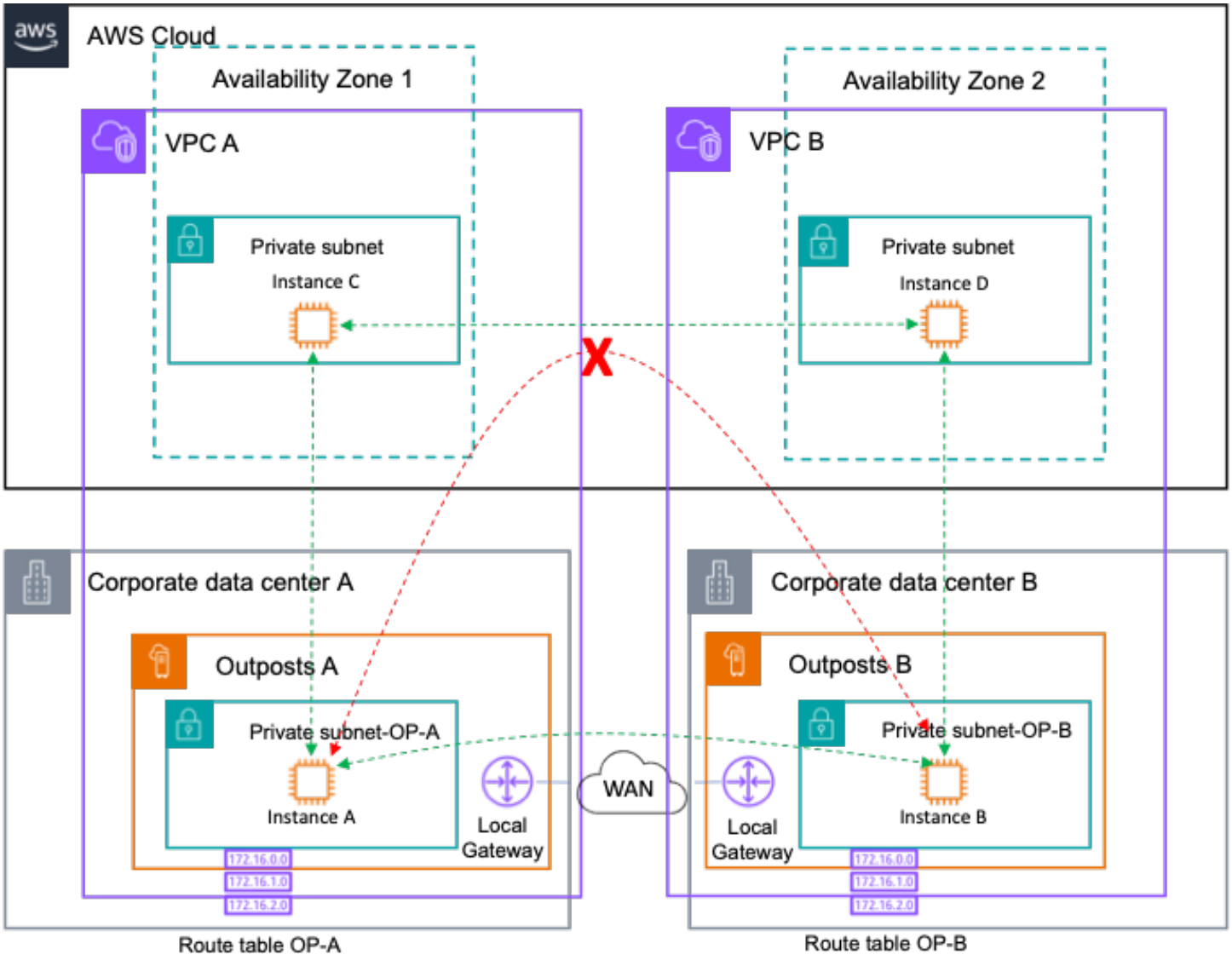


具有多个逻辑 Outposts 的单个 VPC 的网络路径

Outposts-to-Outposts 通过该区域的流量路由被阻止，因为这是一种反模式。与通过客户 WAN 路由流量相比，此类流量会产生双向出站费，并且延迟要高得多。

Outposts 机架 VPC 间路由

部署在不同位置的两个独立的 Outposts 上的资源 VPCs 可以在客户网络中相互通信。部署此架构使您能够 Outposts-to-Outposts通过本地本地和广域网路由流量，从而添加通往对应前哨/VPC 子网的路由。



具有多个逻辑 Outposts 的多个 VPC 的网络路径

针对防范更大规模的故障模式的建议实操：

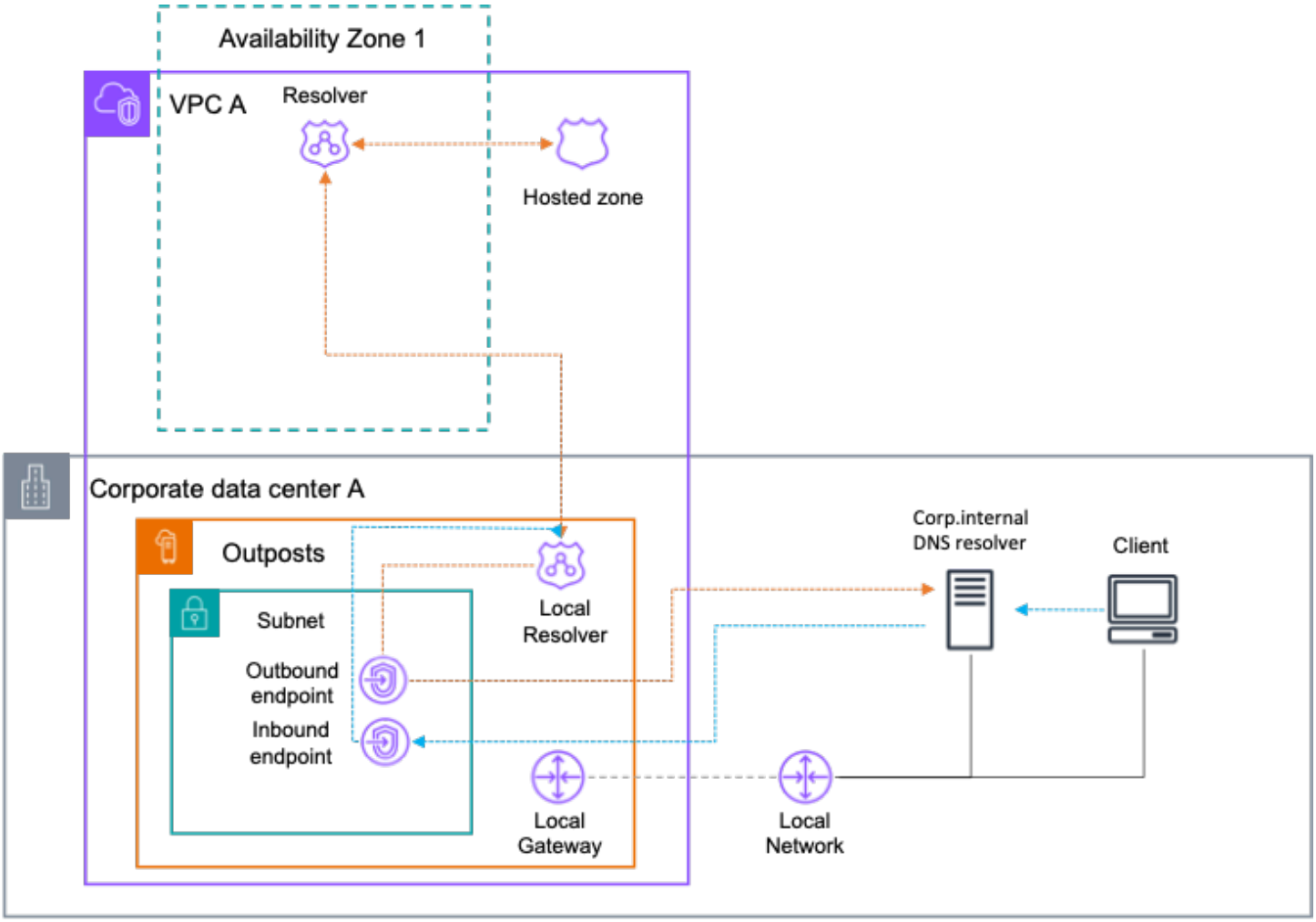
- 部署多个锚定在多个区域的 Outposts。 AZs
- 在多前哨基地部署中， VPCs 对每个前哨基地分别使用。

Outposts 上的 Route 53 本地解析器

当 AWS Outposts 服务链接受到暂时断开连接的影响时，本地 DNS 解析就会失败，这使得应用程序和服务很难发现其他服务，即使它们在同一 Outposts 机架上运行也是如此。但是，在 Route 53 Resolver 开启后 AWS Outposts，应用程序和服务将继续受益于本地 DNS 解析以发现其他服

务，即使在与父 AWS 区域服务器的连接中断的情况下也是如此。同时，对于本地主机名的 DNS 解析，Outposts 上的 Route 53 解析器有助于减少延迟，因为查询结果在本地缓存和提供，同时与 Route 53 解析器端点完全集成。

Route 53 解析器入站终端节点将他们从 VPC 外部收到的 DNS 查询转发给在 Outposts 中运行的解析器。相比之下，Route 53 Resolver Outbound 允许 Route 53 解析器将 DNS 查询转发给您在本地网络上管理的 DNS 解析器，如下图所示。



Outposts 上的 53 号公路解析器

Outposts 上的 Route 53 Resolver 注意事项

请考虑以下事项：

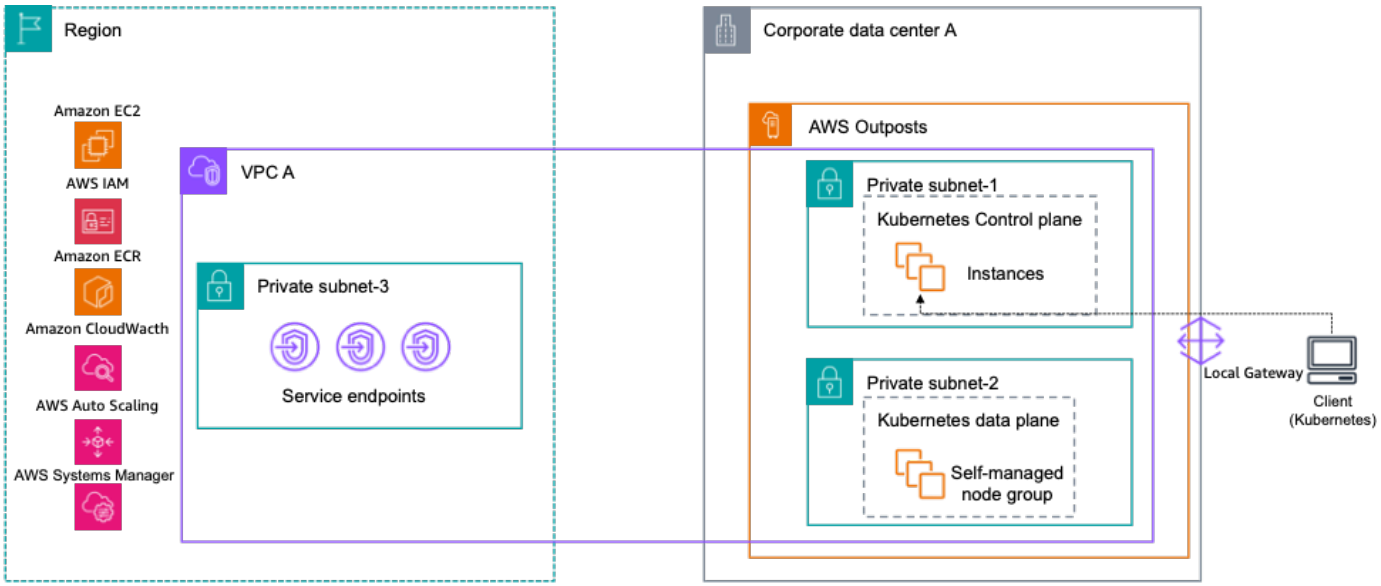
- 你必须在 Outposts 上启用 Route 53 Resolver，它适用于整个 Outposts 部署，即使这涉及单个 Outposts ID 下的多个计算机架。

- 要启用此功能，您的 Outposts 必须有足够的计算容量来部署本地解析器，其形式为任何 c5.xlarge、m5.large 或 m5.xlarge 的至少 4 个 EC2 实例。
- 如果您使用私有 DNS，则必须与所需的 Outposts 共享私有托管区域，以便将记录缓存在本地 VPCs 的 Outposts 上的 Route 53 解析器中。
- 为了通过入站和出站终端节点与本地 DNS 集成，您的 Outposts 必须具有足够的计算容量，以便每个 Route53 终端节点部署两个 EC2 实例。

Outposts 上的 EKS 本地集群

当 Outposts 服务链路与父区域断开连接时，控制平面位于该区域的 EKS Extended Cluster 等服务可能会遇到挑战。挑战之一是EKS控制平面和工作节点之间的通信中断，以及 PODs. 尽管工作节点和工作节点 PODs 都可以继续在本地运行，也可以为驻留在 Outposts 上的应用程序提供服务，但 Kubernetes 控制平面可能会认为它们不健康，并计划在与控制平面的连接恢复时更换它们。恢复连接后，这可能会导致应用程序停机。

为了简化这一点，可以选择在 Outposts 上托管整个 EKS 集群。在这种配置中，Kubernetes 控制平面和你的工作节点都使用你的 Outposts 计算容量在本地运行。这样，即使您的服务链接连接暂时中断以及恢复后，您的集群仍能继续运行。



Outposts 上的 Amazon EKS 本地集群

Outposts 上的 EKS 本地集群注意事项

在 Outposts 中部署 EKS 本地集群时，有一些注意事项：

- 在断开连接期间，没有选项可以对集群本身执行任何需要添加新工作节点或自动扩展节点组的更改，前提是它依赖于父区域 EC2 和 ASG API 调用。 AWS
- • e ksc AWS Outposts tl 支持中列出了本地集群上的一组不支持的功能。 。

结论

借助 r AWS Outposts ack，您可以使用熟悉的 AWS 工具和服务（例如亚马逊、亚马逊 EBS、Outposts 上的 Amazon S3 EC2、Amazon ECS、Amazon EKS 和 Amazon RDS）构建、管理和扩展高度可用的本地应用程序。工作负载可以在本地运行、为客户端提供服务、访问本地网络中的应用程序和系统，以及访问 AWS 区域中的全套服务。Outpost 机架非常适合需要低延迟访问本地系统、本地数据处理、数据驻留以及迁移具有本地系统相互依赖项的应用程序的工作负载。

当您为 Outpost 部署提供足够的电力、空间、冷却和弹性连接时 AWS 区域，您就可以构建高度可用的单一数据中心服务。而且，为了实现更高级别的可用性和弹性，可以部署多个 Outpost，并跨逻辑和地理边界分发应用程序。

Outposts rack 消除了构建本地计算、存储和应用程序网络池的无差别繁重的工作，并允许您将 AWS 全球基础设施的覆盖范围扩展到您的数据中心和托管设施。现在，您可以将时间和精力集中在实现应用程序现代化、简化应用程序部署和提高 IT 服务的业务影响上。

贡献者

本文档的贡献者包括：

- Jesus Federico，Amazon Web Services 电信公司首席解决方案架构师
- Mallory Gershenfeld，亚马逊云科技 S3 on Outposts 的 Product Manager
- Rob Goodwin，Amazon Web Services 混合云高级解决方案架构师
- Chris Lunsford，高级专业解决方案架构师 AWS Outposts，亚马逊 Web Services
- Rohan Mathews，Amazon Web Services AWS Outposts首席架构师
- Brianna Rosentrater，Amazon Web Services 混合边缘专家解决方案架构师
- 莱昂纳多·索拉诺，Amazon Web Services 首席混合边缘专家解决方案架构师
-

文档历史记录

如需获取有关该白皮书更新的通知，请订阅 RSS 信息源。

变更	说明	日期
主要更新	添加了有关联网、DRS 支持、Amazon EKS 本地集群、置放群组和 Amazon RDS 的更新 AWS Outposts	2024 年 11 月 24 日
次要更新	在容量规划中增加了额外的排档指导。	2024 年 2 月 9 日
次要更新	更新以体现自初次发布以来的功能发布。	2023 年 7 月 19 日
次要更新	更新了针对高度可用的网络连接的建议实操。	2023 年 6 月 29 日
初次发布	白皮书首次发布。	2021 年 8 月 12 日

> **Note**
>
> 要订阅 RSS 更新，您必须为当前使用的浏览器启用 RSS 插件。

版权声明

AWS 词汇表

有关最新 AWS 术语，请参阅《AWS 词汇表 参考资料》中的AWS 词汇表。

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。