



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

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

简介	1
概览	3
混合云研讨会	3
PoCs	3
支柱	4
先决条件和限制	5
先决条件	5
AWS Outposts	5
AWS Local Zones	5
限制	6
AWS Outposts	6
AWS Local Zones	6
混合云采用流程	7
边缘联网	7
VPC 架构	7
边缘到区域的流量	8
边缘到本地的流量	10
边缘安全	13
数据保护	13
Identity and access management	16
基础结构安全性	17
互联网访问	18
基础设施治理	21
边缘弹性	22
基础架构注意事项	23
联网注意事项	25
在 Outposts 和 Local Zones 之间分配实例	28
亚马逊 RDS Multi-AZ 在 AWS Outposts	28
故障转移机制	30
边缘容量规划	33
Outposts 的容量规划	33
Local Zones 的容量规划	33
边缘基础设施管理	34
在边缘部署服务	34

前哨基地专用的 CLI 和 SDK 36

资源 38

AWS 参考文献 38

AWS 博客文章 38

贡献者 39

编写 39

审阅 39

技术写作 39

文档历史记录 40

..... xli

通过以下方式构建混合云架构的最佳实践 AWS 服务

Amazon 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：

- [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](#)
- [资源](#)
- [贡献者](#)
- [文档历史记录](#)

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 [Local 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 E [AWS nterprise Supp](#) ort 合同或[AWS 统一运营](#)计划。

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[Direct Connect 接入点 \(PoP\)](#) 的 Direct Connect 链接。有关更多信息，请参阅 Local Zones 文档中的 [Direct 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，并在本地区域的 Amazon EC2 上启动基于软件的 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 [Local 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 Amazon 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 《Outposts 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。相反，请在 Amazon EC2 上使用基于软件的 VPN。
- Local Zones 不支持 AWS Transit Gateway。而是使用 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、Amazon ElastiCache 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-2:111111111111:outpost/op-0e32example1 \  
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

有关详情，请参阅 [AWS Outposts 文档](#)。

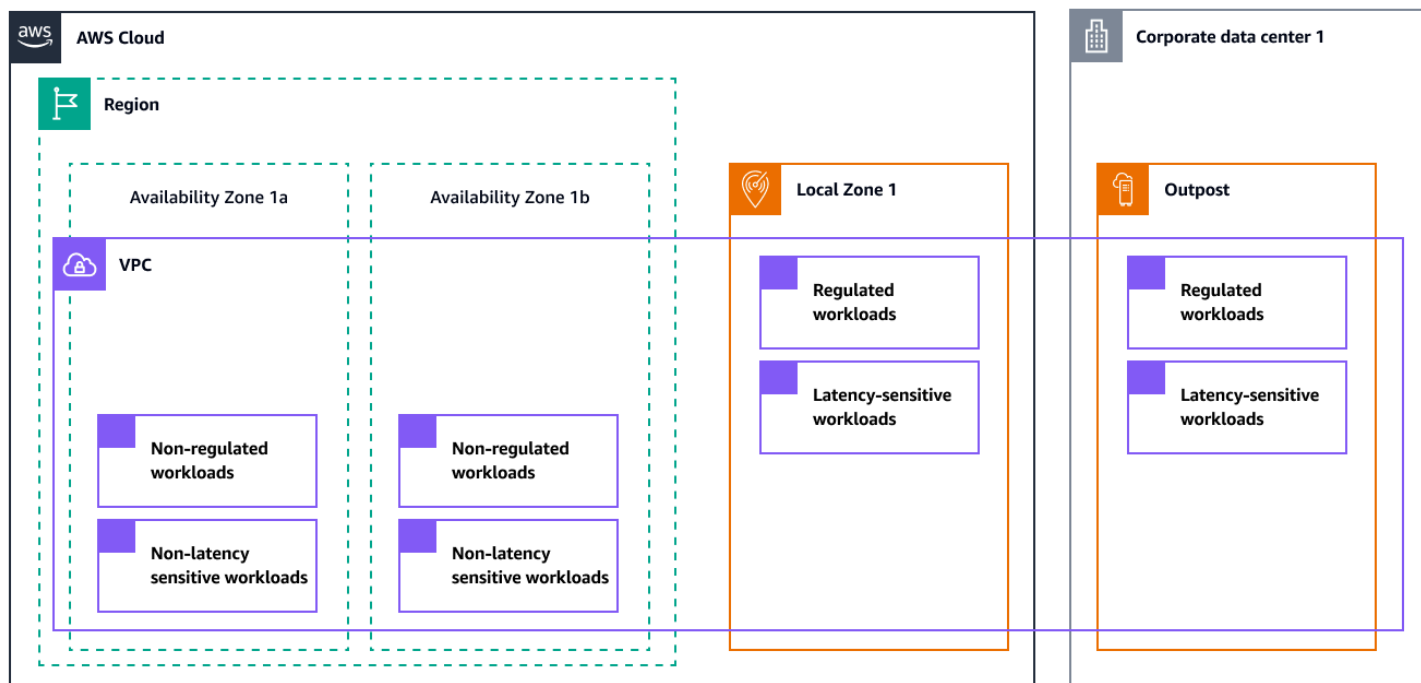
- Local Zones：要向 VPC 添加本地区域子网，请按照与可用区域相同的步骤进行操作，但要指定本地区域 ID（<local-zone-name>在以下示例中）。

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \  
--cidr-block 10.0.1.0/24 \  
--local-zone-id local-zone-1
```

```
--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 [Local Zones 文档](#)。

下图显示了包含 Outpost 和本地区域子网的 AWS 架构。



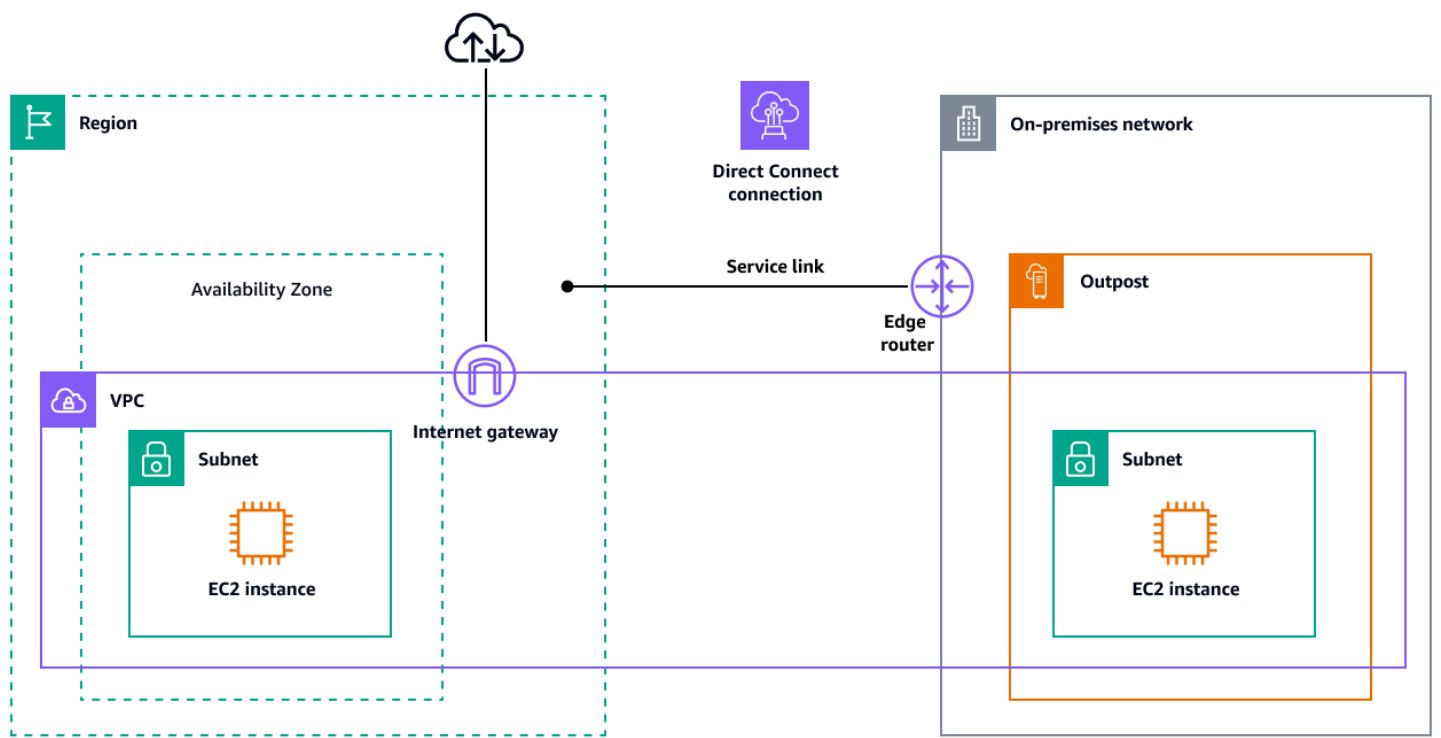
边缘到区域的流量

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。本节探讨了控制平面和数据平面连接对 Local Zones 和 AWS Outposts。

AWS Outposts 控制面板

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 Direct Connect 公共虚拟接口（公共 VIF）或私有虚拟接口（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、Amazon EMR 和亚马逊指标 AWS 服

务等。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 Outpost AWS 区域 s 文档中的AWS Outposts 连接信息。](#)



有关为使用 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 数据面板

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 EC2 实例与中的 EC2 实例之间的流量的 MTU AWS 区域 为 1,300 字节。AWS Outposts 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，使您能够通过相同的 API 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的 MTU。

来自	至	MTU
该地区的 Amazon EC2	Local Zones 中的亚马逊 EC2	1,300 字节
Direct Connect	Local Zones	1,468 字节
互联网网关	Local Zones	1,500 字节
Local Zones 中的亚马逊 EC2	Local Zones 中的亚马逊 EC2	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，先与 AWS 混合云专家讨论您的 Local Zones 要求和注意事项。

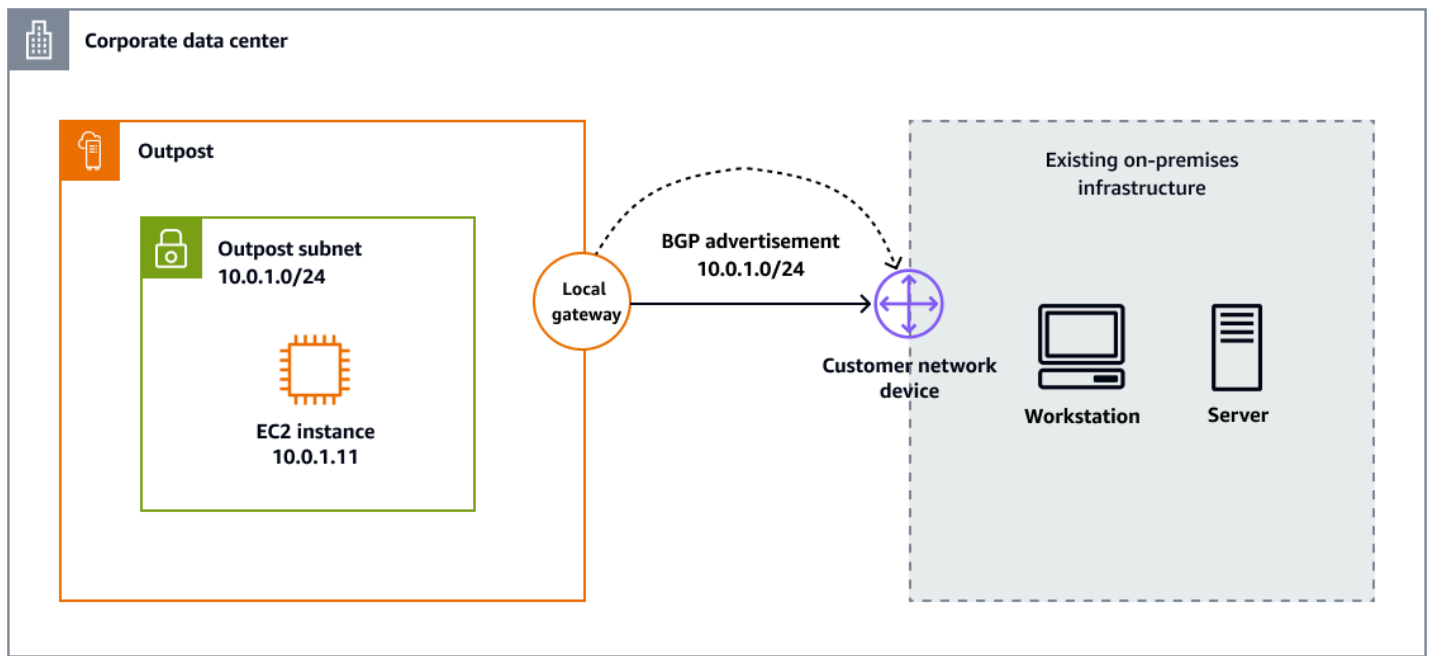
边缘到本地的流量

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。

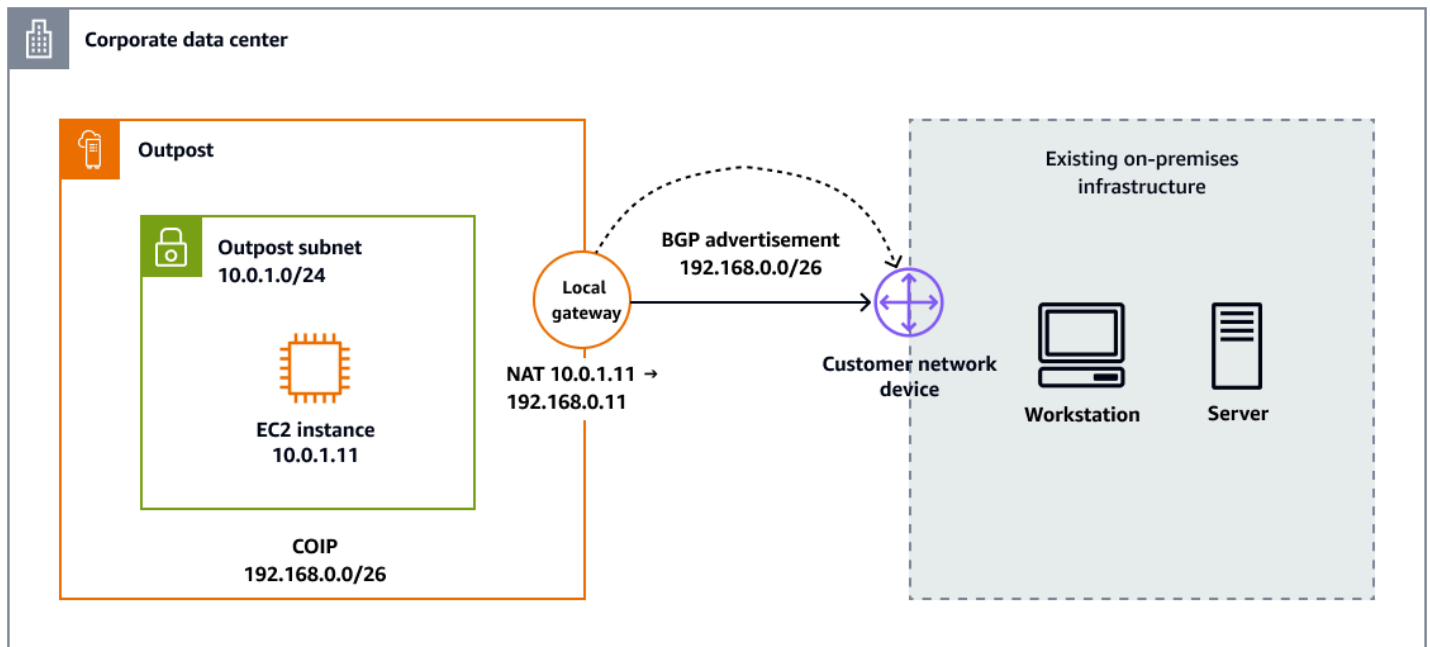
AWS Outposts 本地网关

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 Zones 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 Amazon EC2-hosted 工作负载暴露给互联网，您可以在启动 EC2 实例时启用 Auto-assign 公有 IP 选项。如果您使用 Application Load Balancer，则可以将其实例定义为面向互联网，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，您可以在启动后将其中一个资源与 EC2 实例相关联。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 [Local Zones 文档中的本地区域的连接选项](#)。

Local Zones 和 Direct Connect

Local Zones 还支持 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 VPC 与您的本

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。可以在扩展到 Local Zones 的 VPC 之间建立 VPC 对等关系。当对等互连的 VPC 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，并提供服务来帮助满足独特的云安全要求。当您扩展架构的范围到时 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。Third-party 作为[AWS 合规计划](#)的一部分，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

默认情况下，存储在 Outposts 上的 Amazon S3 中的所有数据都使用服务器端加密和 Amazon S3 托管加密密钥（）进行加密。SSE-S3 您可以选择将服务器端加密与客户提供的加密密钥一起使用（）SSE-C。要使用 SSE-C，请在对象 API 请求中指定加密密钥。Server-side 加密仅加密对象数据，不加密对象元数据。

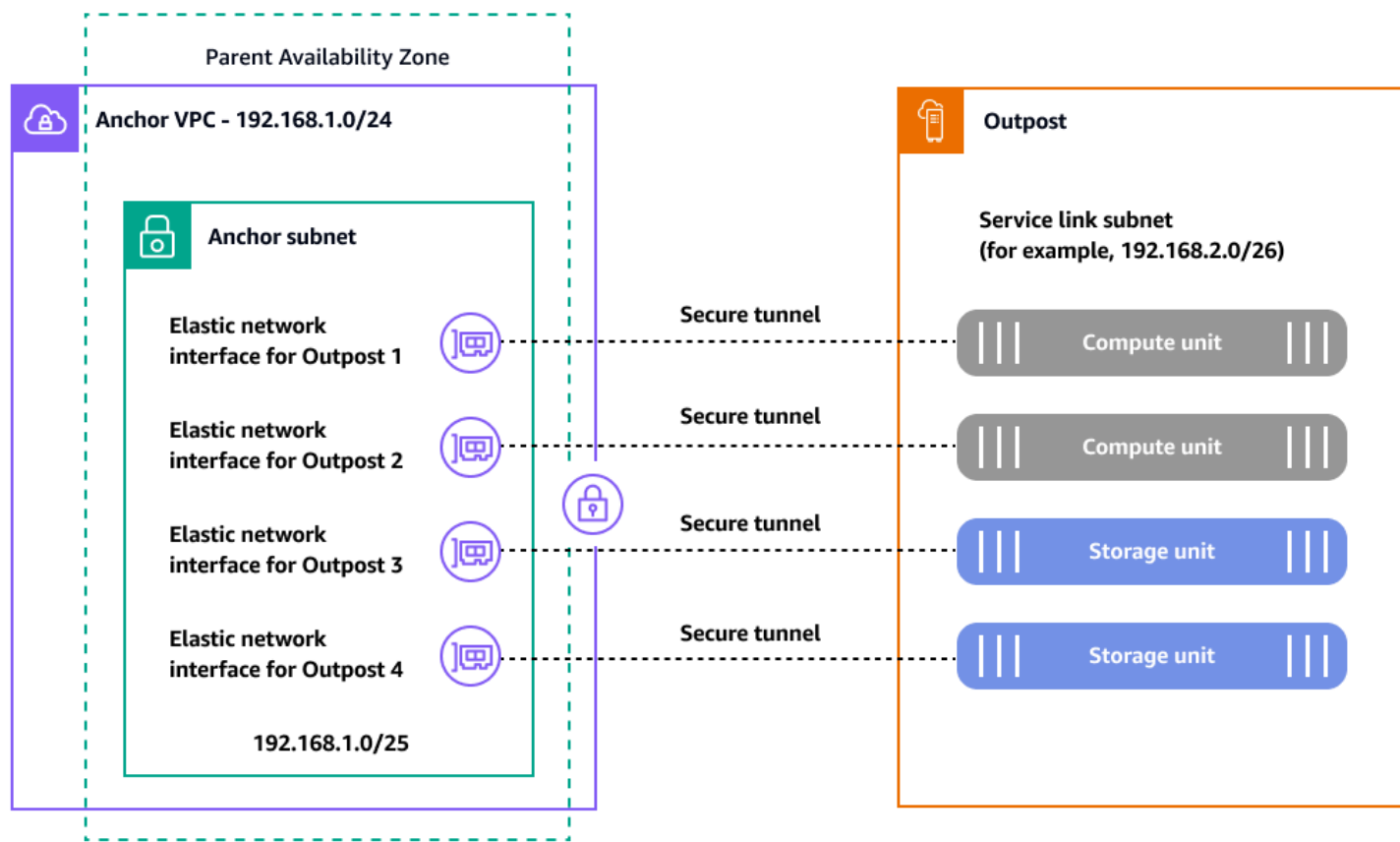
Note

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

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（Internet 或 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。



Anchor VPC CIDR: /25 or larger that doesn't conflict with 10.1.0.0/16
IAM role: `AWSServiceRoleForOutposts_<OutpostID>`

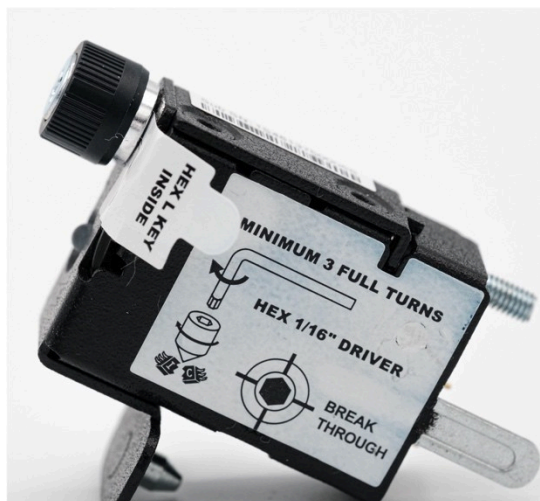
每 AWS Outposts 台主机（计算和存储）都需要这些通过众所周知的 TCP 和 UDP 端口的加密隧道才能与其父区域通信。下表显示了 UDP 和 TCP 协议的源和目标端口和地址。

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。如果您对本地理位置之间传输的数据进行加密和 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 Direct Connect 端点之间启用 MAC 安全 (MacSec)。有关更多信息，请参阅 AWS 博客文章为[Direct Connect 连接添加 MacSec 安全](#)。

数据删除

当您在中停止或终止某个 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。



Identity and access management

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（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
Identity-based 政策	是
Resource-based 政策	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 (ACL)	否
Attribute-based 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
Service-linked 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。当您遵循在所有层面应用安全的原则时，您就采用了[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](#)。使用深度防御方法对入站和出站流量应用多种控制。这包括使用安全组（状态检查防火墙）、网络 ACL、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](#)。自动化您的保护性计算机制，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。
- [缩小攻击面](#)。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。当您使用这些模式时，只有当您使用该区域来修补、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、网络防火墙以及位于 AWS 区域区域内但通过区域和边缘之间的数据路径连接到 AWS Outposts 或 Local Zones 的其他组件。

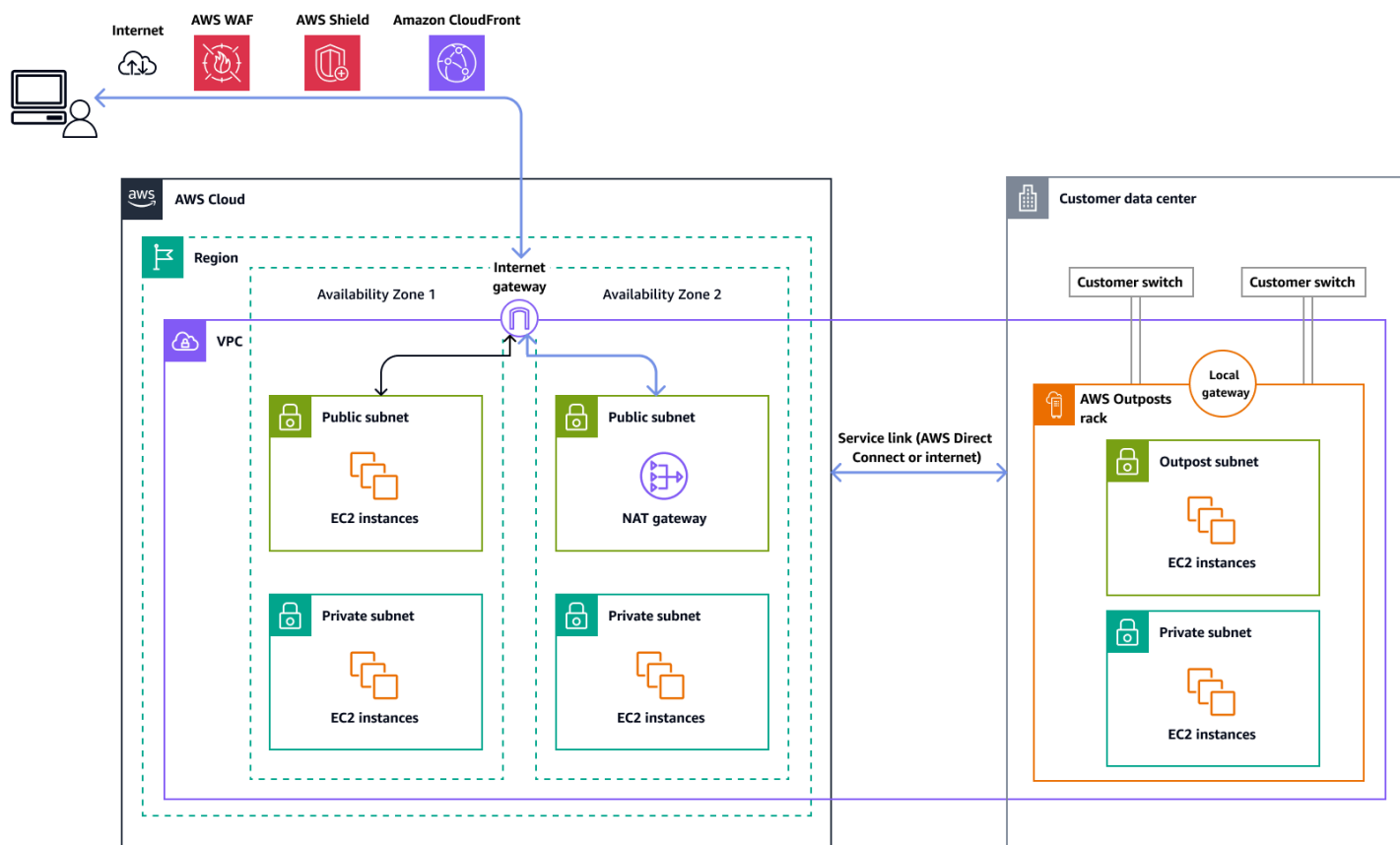
Local Zones 采用一种称为网络边界组的网络结构，用于 AWS 区域。AWS 通告来自这些唯一群组的公有 IP 地址。网络边界组由可用区、Local Zones 或 Wavelength 区域组成。您可以明确分配公有 IP 地址池以用于网络边界组。您可以使用网络边界组将互联网网关扩展到 Local Zones，方法是允许该组提供弹性 IP 地址。此选项要求您部署其他组件来补充 Local Zones 中提供的核心服务。这些组件可能来自 ISV，可帮助您在本地区域中构建检查层，如 AWS 博客文章[混合检查架构](#)中所述。AWS Local Zones

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。路由表必须有默认路由条目 (0.0.0.0/0) 它使用 LGW 作为下一跳。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

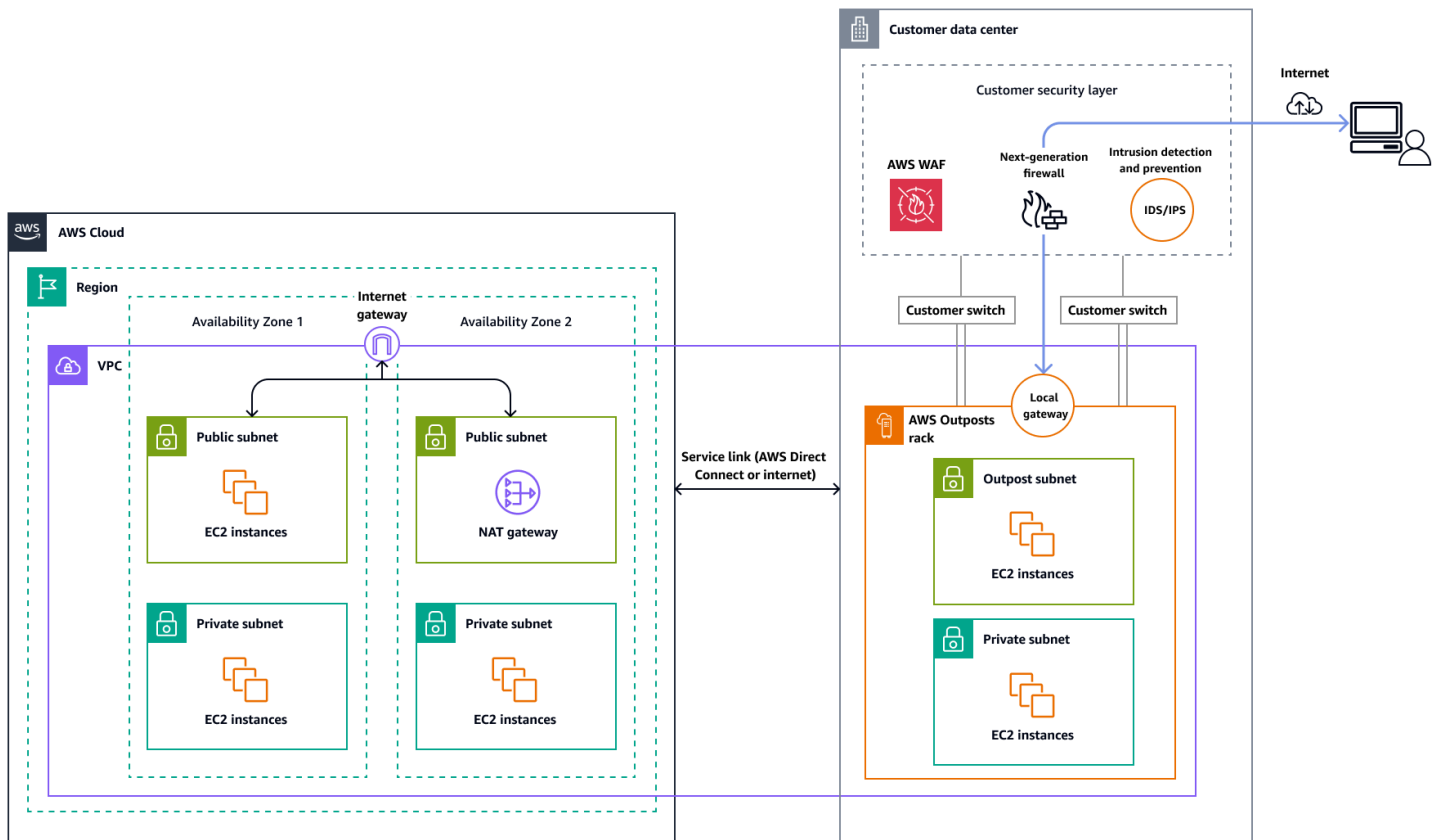
下图显示了实例中的工作负载与通过父 AWS Outposts 实例的 Internet 之间的流量 AWS 区域。



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。有关详情，请参阅[AWS Control Tower 文档](#)。

您可以配置护栏等功能，以满足政府 AWS Control Tower 和监管行业（如金融服务机构 (FSI)）的数据驻留要求。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](#)（AWS Well-Architected 框架文档）

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 这样，其他用户可以使用 Outpost 站点，配置 VPC 并且在共享的 Outpost 上启动和运行实例。

中的可共享资源 AWS Outposts 有：

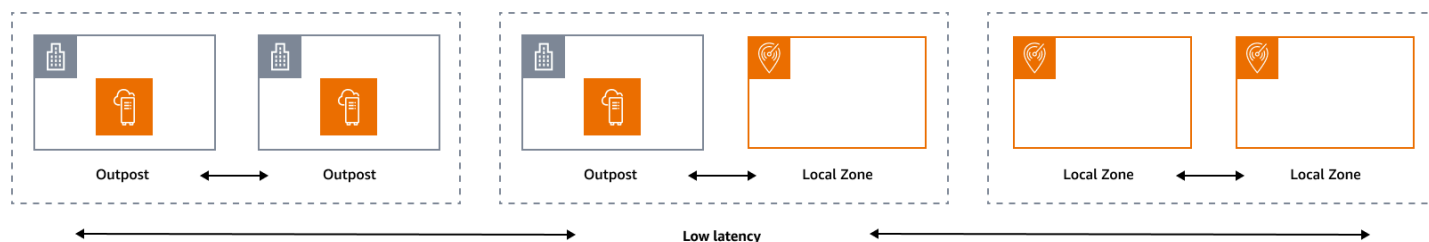
- 已分配的专用主机
- 容量预留
- Customer-owned IP (CoIP) 地址池
- 本地网关路由表
- Outposts
- Amazon S3 on Outposts
- 站点
- 子网

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、API 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 使用的硬件基础设施相同。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。此选择会将 Outposts 部署的控制平面锚定到选定的基础架构。AWS

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

制平面的角度进行架 Multi-AZ 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：

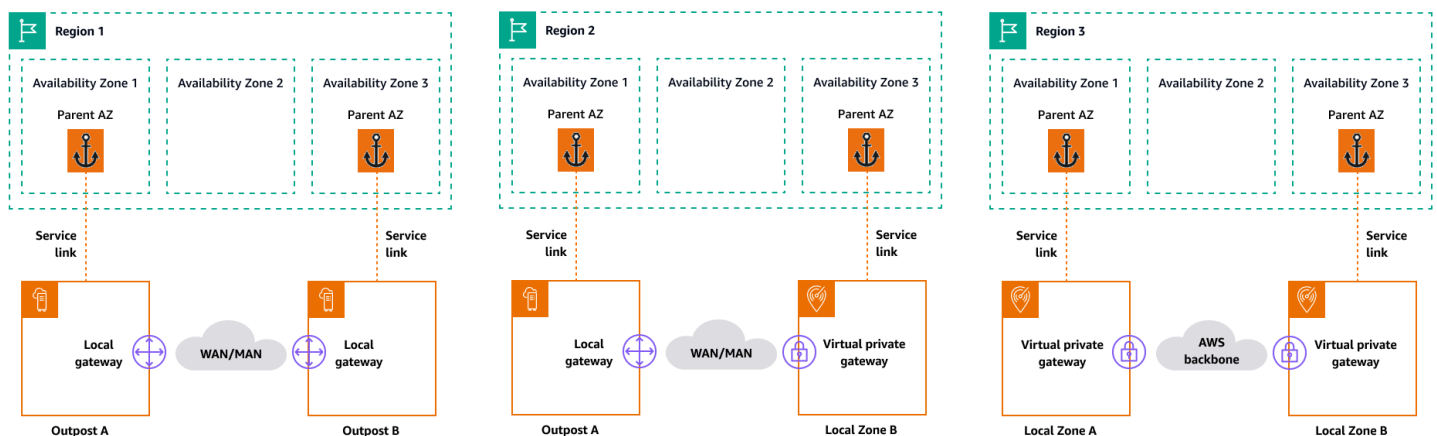
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

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。

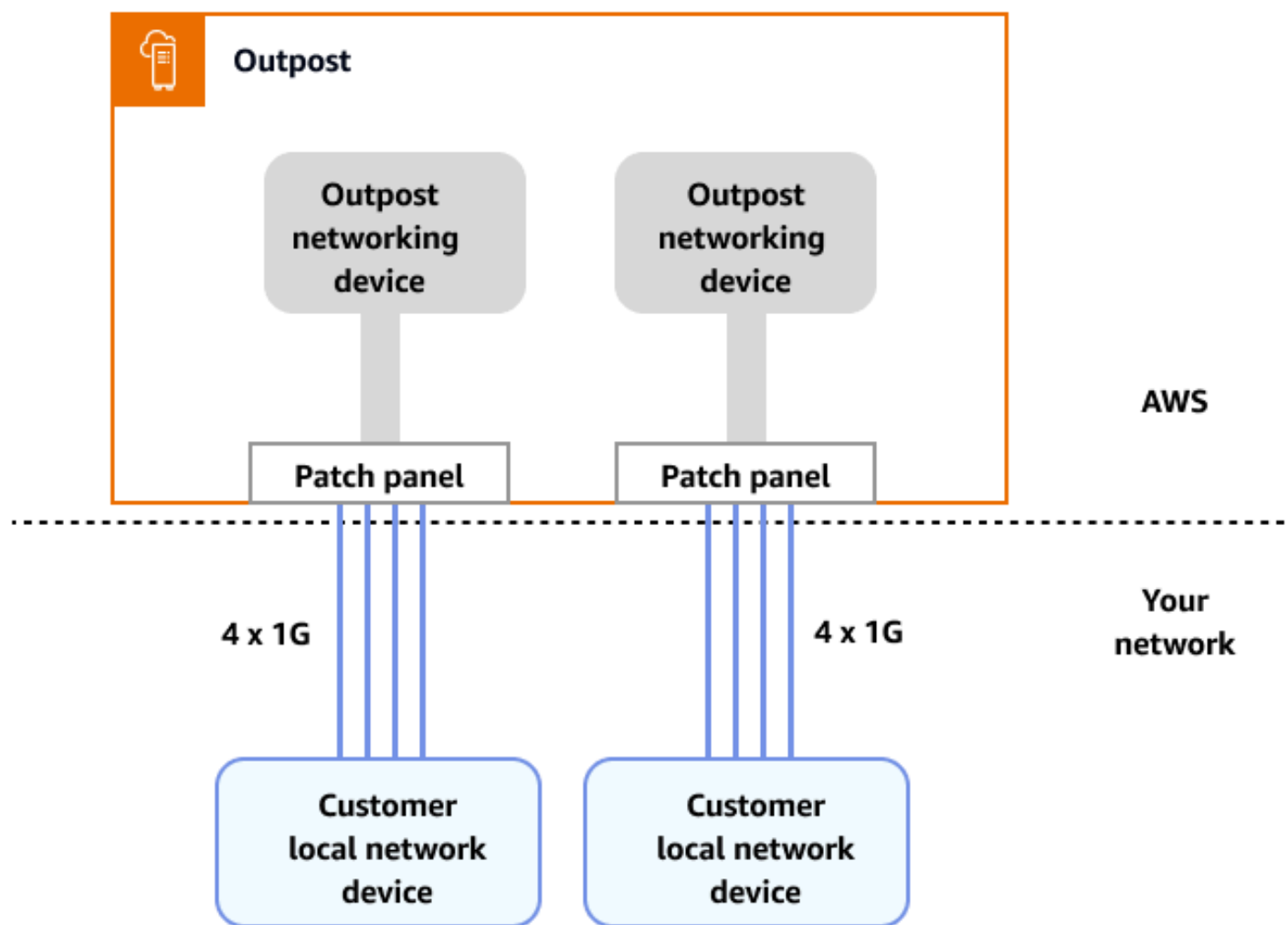
Local Zones 的弹性网络

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的连接。无论您选择哪种连接架构（例如，VPN 或 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 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[Direct Connect 弹性建议](#)中所述。但是，有些场景主要适用于国际 Local Zones。在启用本地区的国家/地区，只有一个 Direct Connect PoP 就无法创建推荐的 Direct Connect 弹性架构。如果您只能访问单个 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 Direct Connect，正如 AWS 博客文章中说明和讨论的那样，[启用从本地到 AWS Local Zones 的高可用性连接](#)。

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。这种冗余是通过两个 Outposts 网络设备 (OnD) 实现的。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。

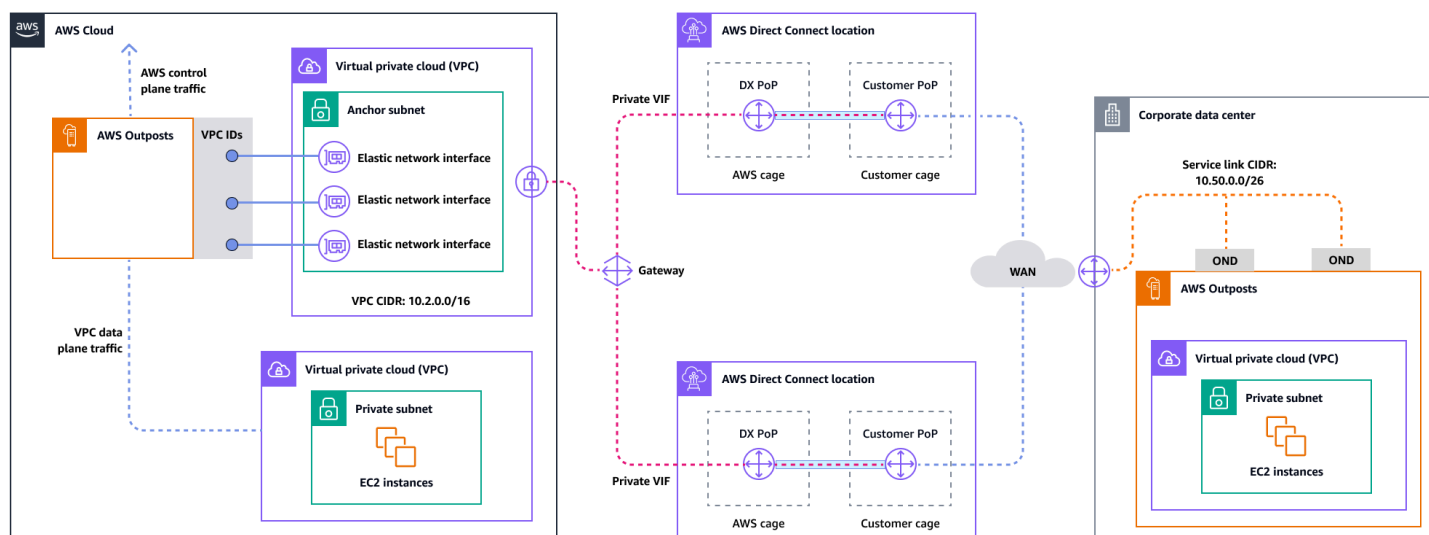
上行链路速度	上行链路数量
1 Gbps	1、2、4、6 或 8
10 Gbps	1、2、4、8、12 或 16
40 或 100 Gbps	1、2 或 4



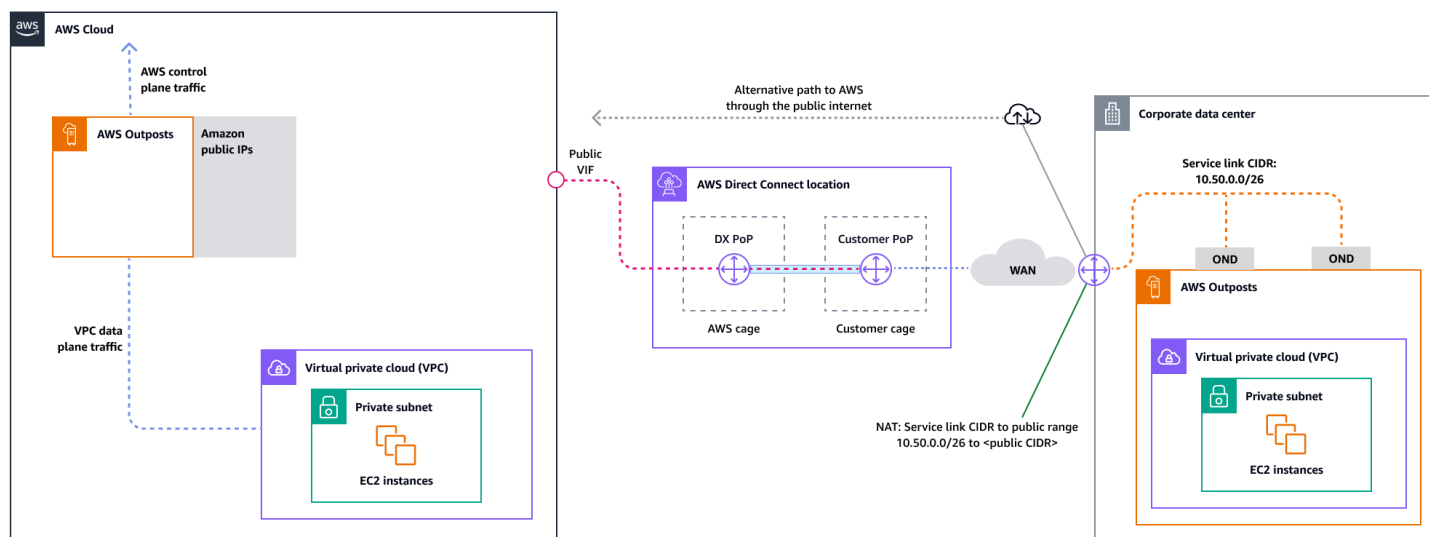
有关此连接的更多信息，请参阅文档中的 [Outposts Racks 的本地网络连接](#)。AWS Outposts

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 Direct Connect 或互联网连接获取服务链接。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。

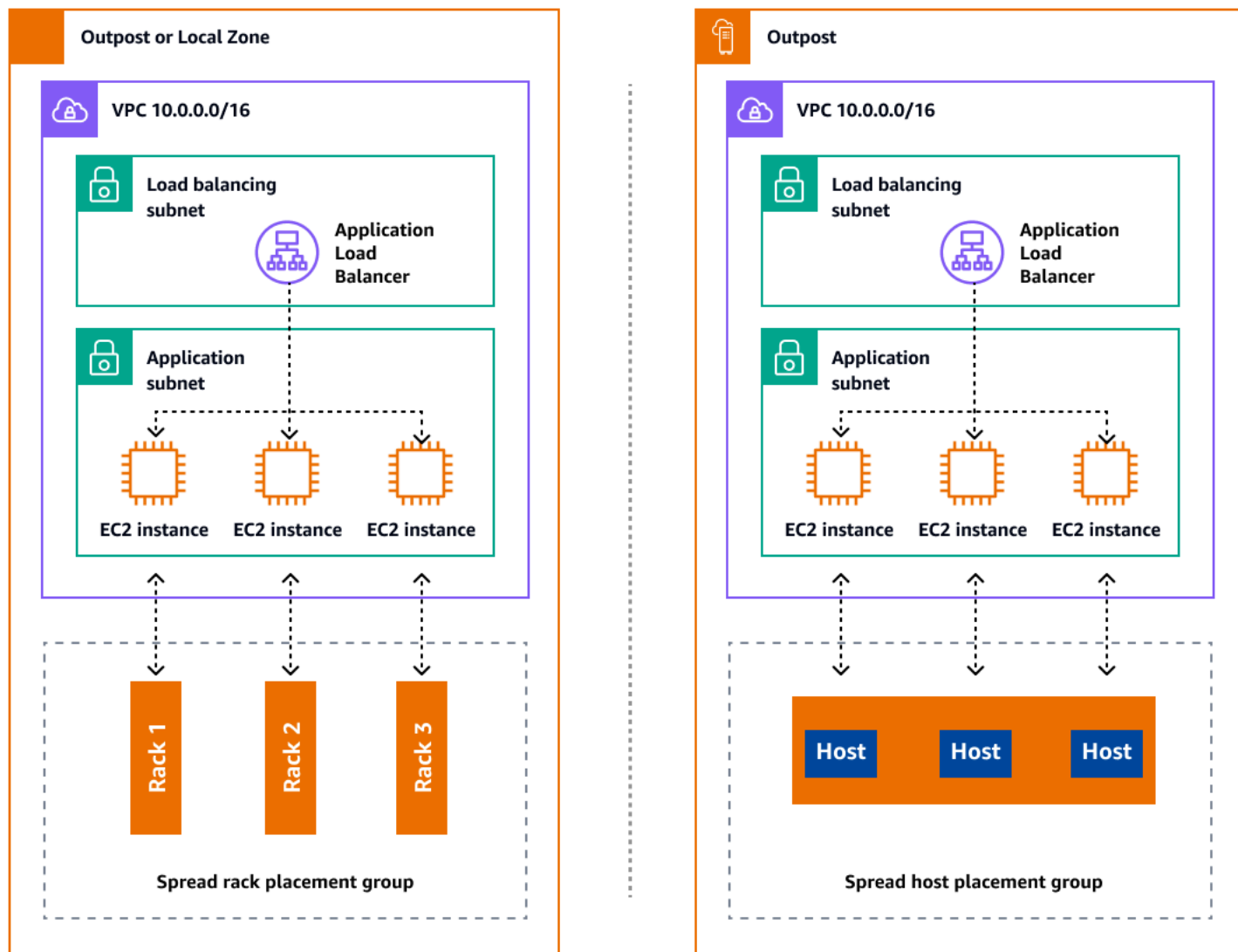


使用 ACE 机架扩展 Outposts 机架部署

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。Outposts 还提供了另一种名为 spread 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。



亚马逊 RDS Multi-AZ 在 AWS Outposts

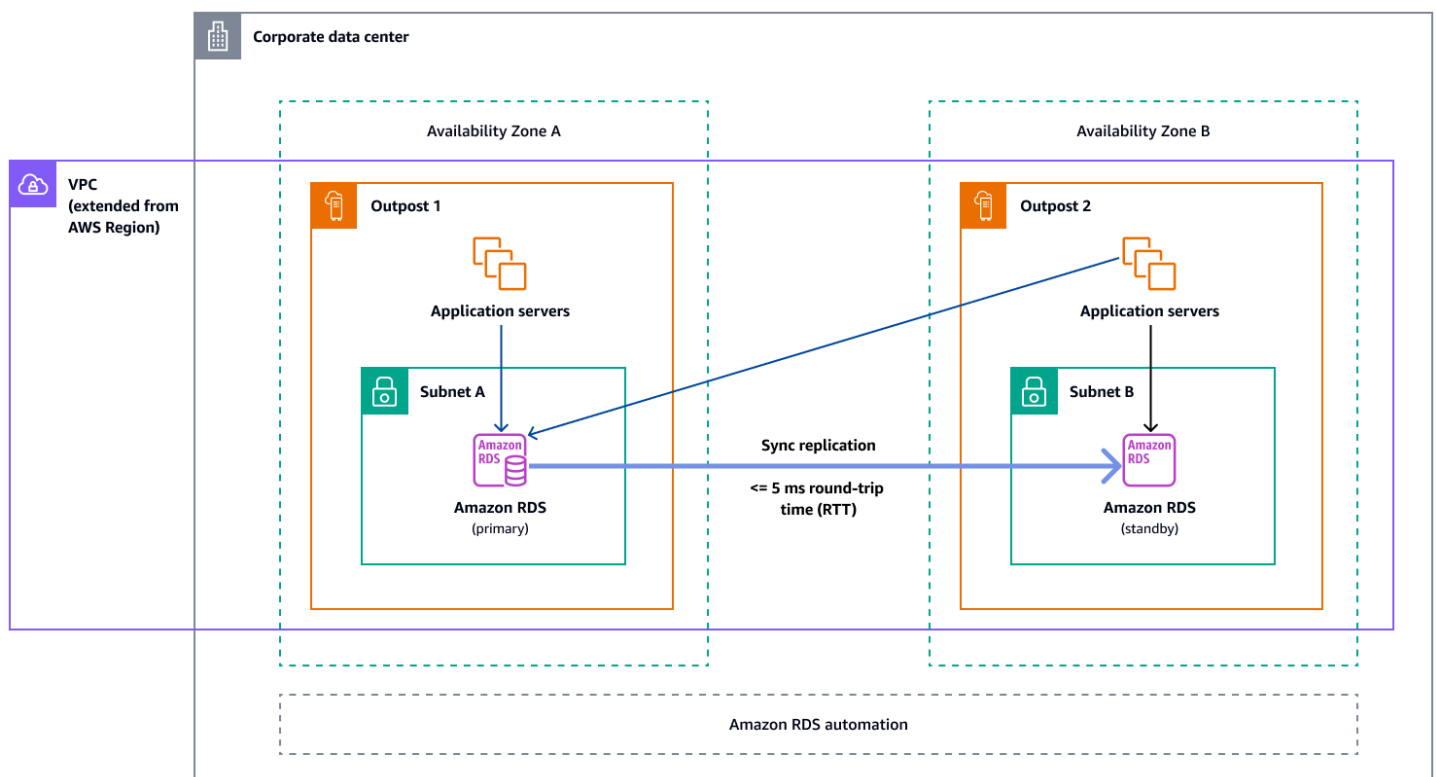
当你在 Outposts 上使用 Multi-AZ 实例部署时，Amazon RDS 会在两个 Outposts 上创建两个数据库实例。每个 Outpost 都运行在自己的物理基础设施上，并连接到一个区域中的不同可用区以实现高可用

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 Multi-AZ 部署，Amazon RDS 在一个 Outpost 上创建主数据库实例，并将数据同步复制到另一个 Outpost 上的备用数据库实例。Multi-AZ Outposts 上的部署与中的 Multi-AZ 部署类似 AWS 区域，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 中的亚马逊 RDS 的 Customer-owned IP 地址](#)。
- 复制在您的本地网络上运行。

Multi-AZ 在 Outposts 上的 Amazon RDS 上部署适用于所有支持的 MySQL 和 PostgreSQL 版本。Multi-AZ 部署不支持本地备份。

下图显示了 Out Multi-AZ posts 上的 Amazon RDS 配置架构。

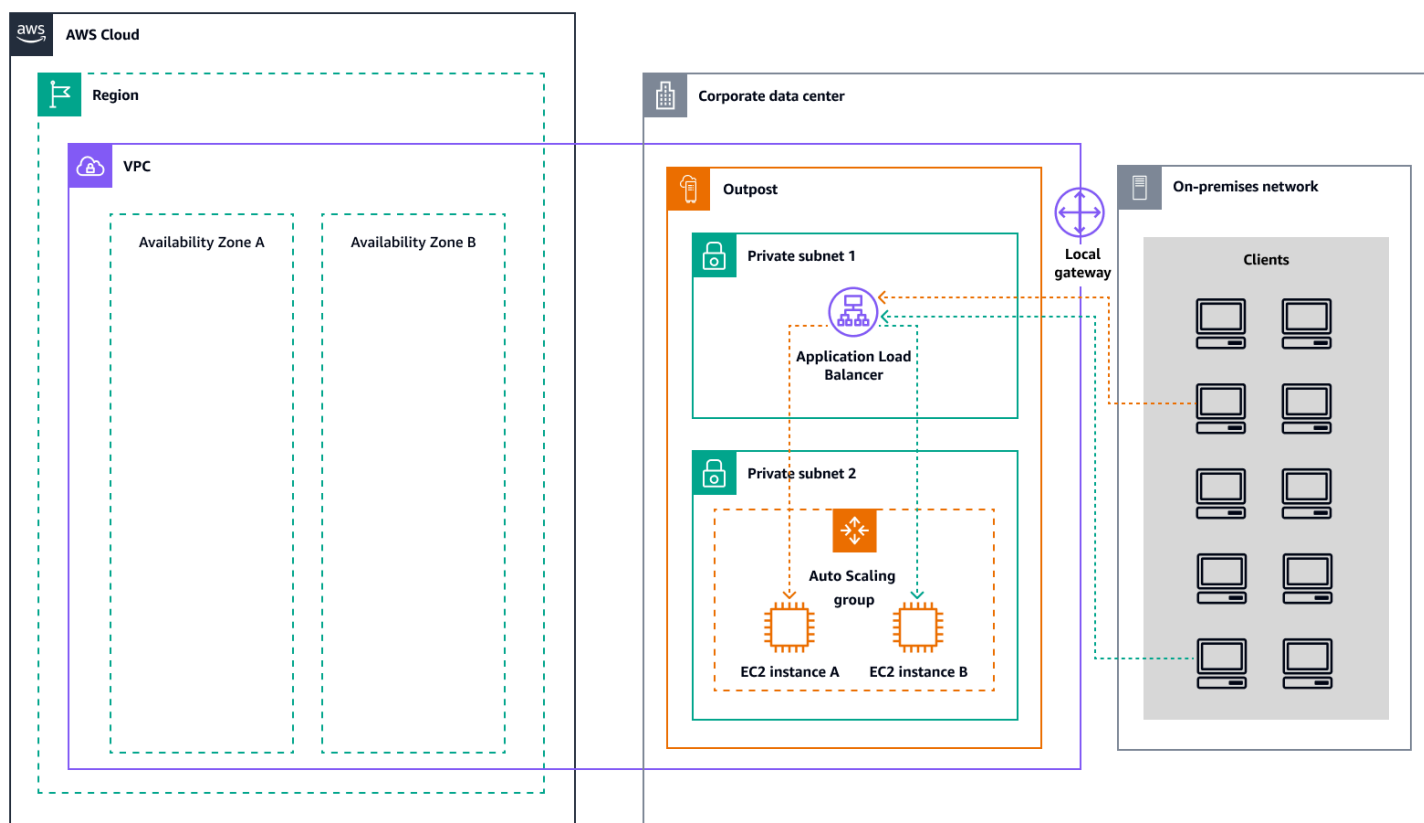


故障转移机制

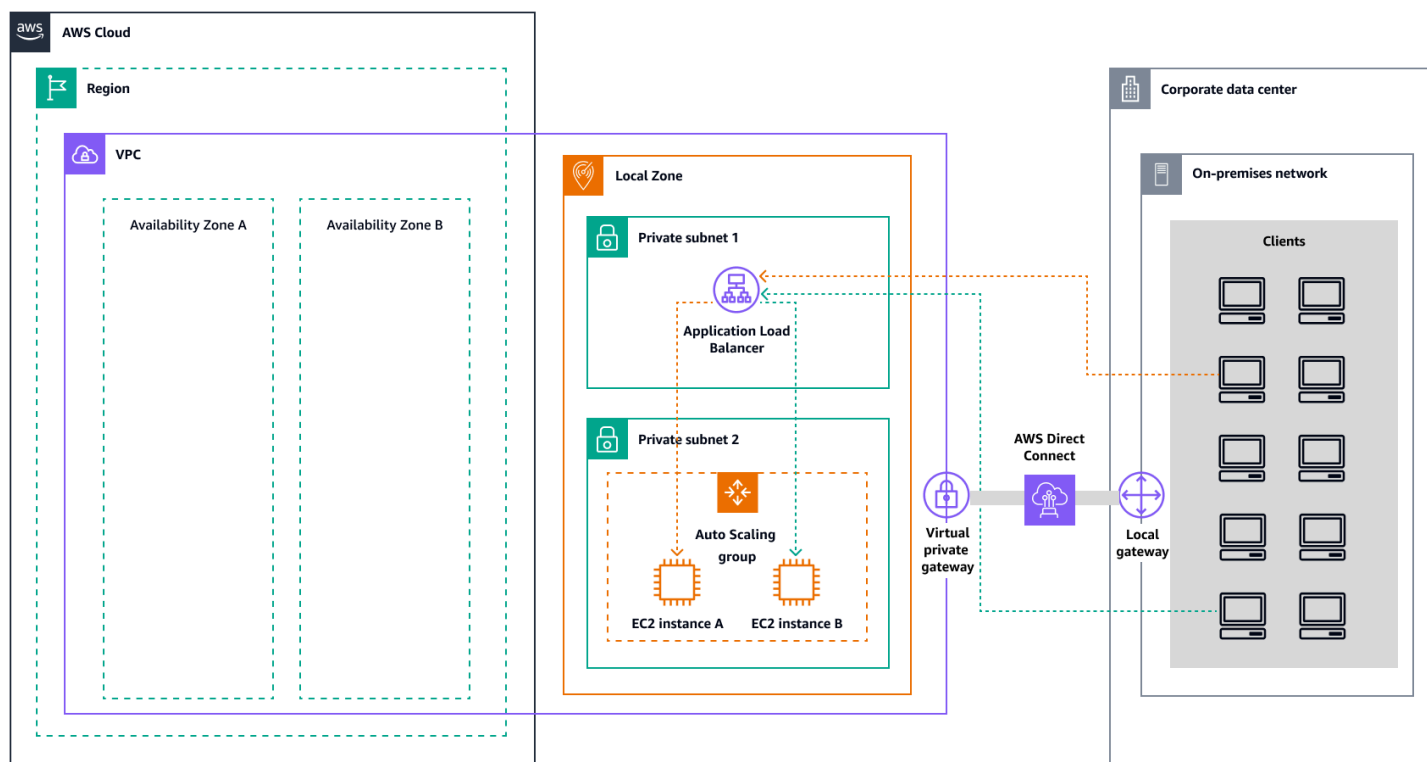
负载均衡和自动扩展

Elastic Load Balancing (ELB) 会自动将您的传入应用程序流量分配到您正在运行的所有 EC2 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 EC2 Auto 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网络流量的单一联系点。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 EC2 Auto 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 如何在中管理 Amazon EC2 上的工作负载 AWS Outposts。



下图说明了 Local Zones 中 Amazon EC2 的类似架构。



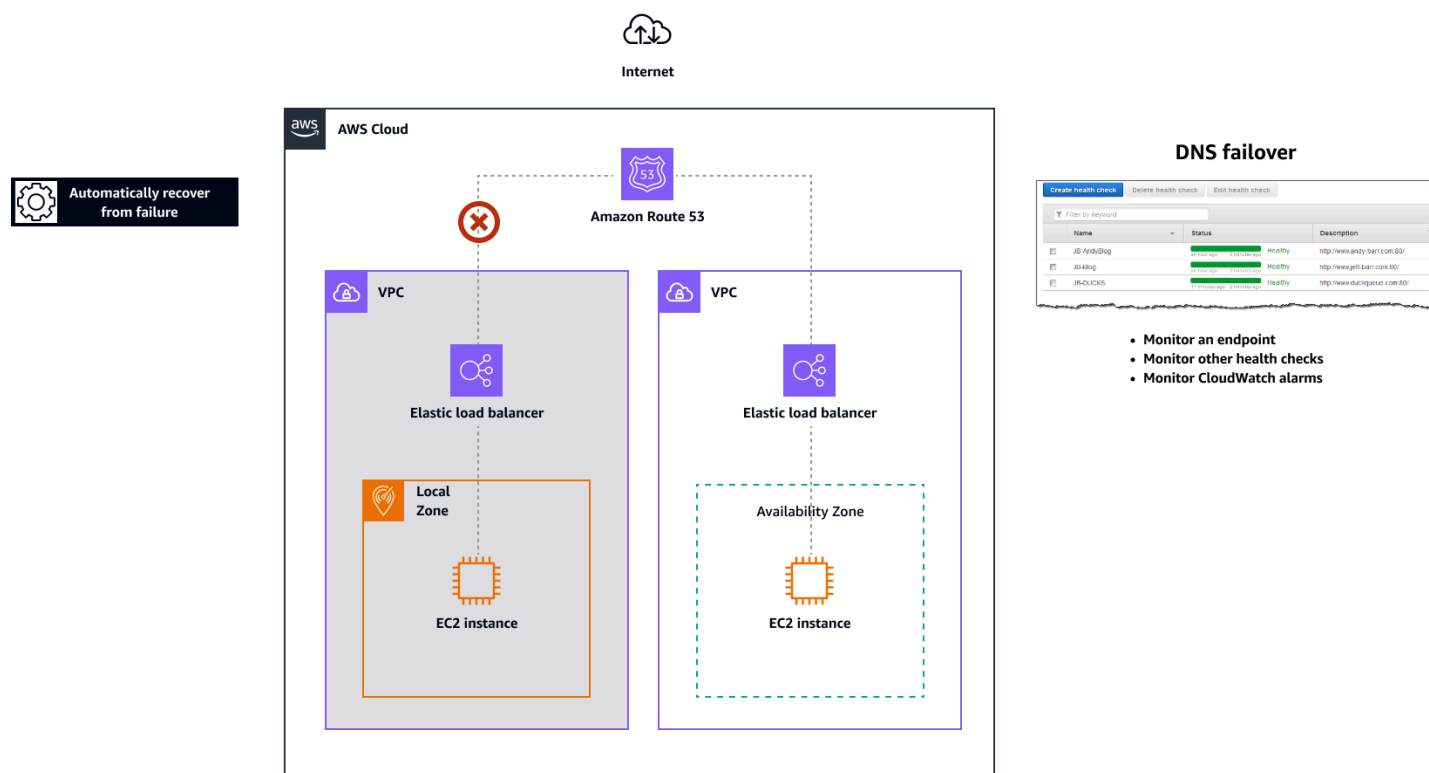
Note

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 Balancer](#)”的 AWS 博客文章 AWS Outposts。

用于 DNS 故障转移的亚马逊 Route 53

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 Route 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。



注意

- 如果您要在私有托管区域中创建故障转移记录，则可以创建 CloudWatch 指标，将警报与该指标相关联，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，启用从公有 IP 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。这种组合可确保对您的 Outposts-hosted 应用程序进行可靠的公开访问。

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 VPC 中使用[私有 DNS 的应用程序的所有 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[解决 VPC 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-Architected AWS Framework 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	选择本地区域网
AWS 弹性灾难恢复	使用 AWS 弹性灾难恢复 和 AWS Outposts	不可用
AWS Transform MGN	不可用	选择本地区域网作为暂存子网

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

您可以使用[AWS CLI](#)或 Outposts APIs 来创建 [Outposts](#) 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 [Outposts 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 \(Amazon VPC 文档 \)](#)
- [Local 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

以下个人参与了本指南的编撰。

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
- 技术客户经理 Dionysios Kakaletis AWS
- Outposts 首席专家 Vamsi Krishna AWS

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

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。