aws

机架用户指南

AWS Outposts

AWS Outposts: 机架用户指南

Table of Contents

什么是 AWS Outposts？

AWS Outposts 是一项完全托管的服务，可将 AWS 基础架构、服务、API 和工具扩展到客户驻地。通过提供对 AWS 托管基础设施的本地访问权限， AWS Outposts 使客户能够使用与 AWS 区域相同的编程接口在本地构建和运行应用程序，同时使用本地计算和存储资源来降低延迟和满足本地数据处理需求。

Outpost 是部署在客户现场的 AWS 计算和存储容量池。 AWS 将此容量作为 AWS 区域的一部分进行运营、监控和管理。您可以在 Outpost 上创建子网，并在创建 EC2 实例、EBS 卷、ECS 集群和 RDS 实例等 AWS 资源时指定子网。Outpost 子网中的实例使用私有 IP 地址与该 AWS 区域中的其他实例通信，所有实例都在同一 VPC 内。

> **Note**
>
> 您无法将 Outpost 连接到同一 VPC 内的其他 Outpost 或本地区域。

有关更多信息，请参阅AWS Outposts 产品页。

重要概念

这些是的关键概念 AWS Outposts。

- 前哨站点 — 客户管理的实体建筑 AWS 将安装你的前哨基地。站点必须满足 Outpost 的设施、网络和电力要求。
- Outpost 容量 — Outpost 上可用的计算和存储资源。您可以从 AWS Outposts 控制台查看和管理 Outpost 的容量。
- 前哨设备 — 提供 AWS Outposts 服务访问权限的物理硬件。硬件包括由其拥有和管理的机架、服务器、交换机和电缆 AWS。
- Outposts 机架 — Outpost 的外形规格，行业标准的 42U 机架。Outpost 机架包括可在机架上安装的服务器、交换机、网络配线架、电源架和空白面板。
- Outposts ACE 机架 — 聚合、核心、边缘 (ACE) 机架充当多机架 Outpost 部署的网络聚合点。ACE 机架通过在逻辑 Outposts 中的多个 Outpost 计算机架和本地网络之间提供连接，减少了物理网络端口的数量和逻辑接口要求。

  如果您有五个或更多计算机架，则必须安装 ACE 机架。如果您的计算机架少于五个，但计划将来扩展到五个或更多机架，我们建议您尽早安装 ACE 机架。

有关 ACE 机架的更多信息，请参阅使用 ACE AWS Outposts 机架扩展机架部署。

- Outpost 服务器 — Outpost 的外形规格，行业标准的 1U 或 2U 服务器，可以安装在符合 EIA-310D 19 标准的 4 柱机架中。Outpost 服务器为空间有限或容量要求较低的站点提供本地计算和网络服务。
- 服务链接 — 支持您的 Outpost 与其关联 AWS 区域之间进行通信的网络路由。每个 Outpost 都是可用区及其关联区域的扩展。
- 本地网关 (LGW) — 一种逻辑互连虚拟路由器，可在 Outpost 机架和您的本地网络之间进行通信。
- 本地网络接口 — 一种网络接口，可实现 Outpost 服务器与您的本地网络之间的通信。

AWS Outposts 上的资源

您可以在 Outpost 上创建以下资源，以支持低延迟工作负载（这些工作负载必须靠近本地数据和应用程序的位置运行）：

计算

资源类型	机架	服务器
Amazon EC2 实例	是	是
Amazon ECS 集群	是	是
Amazon EKS 节点	是	否

数据库和分析

资源类型	机架	服务器
亚马逊 ElastiCache 节点（Redis 集群、Memcached 集群）	 是	 否
Amazon EMR 集群	 是	 否
Amazon RDS 数据库实例	 是	 否

联网

资源类型	机架	服务器
App Mesh Envoy 代理	 是	 是
应用程序负载均衡器	 是	 否
Amazon VPC 子网	 是	 是
Amazon Route 53	 是	 否

存储

资源类型	机架	服务器
Amazon EBS 卷	是	否
Amazon S3 存储桶	是	否

其他 AWS 服务

服务	机架	服务器
AWS IoT Greengrass	是	是
亚马逊 SageMaker Edge 管理器	是	是

定价

您可以从各种 Outpost 配置中进行选择，每种配置都提供 EC2 实例类型和存储选项的组合。机架配置的价格包括安装、拆卸和维护。对于服务器，您必须安装和维护设备。

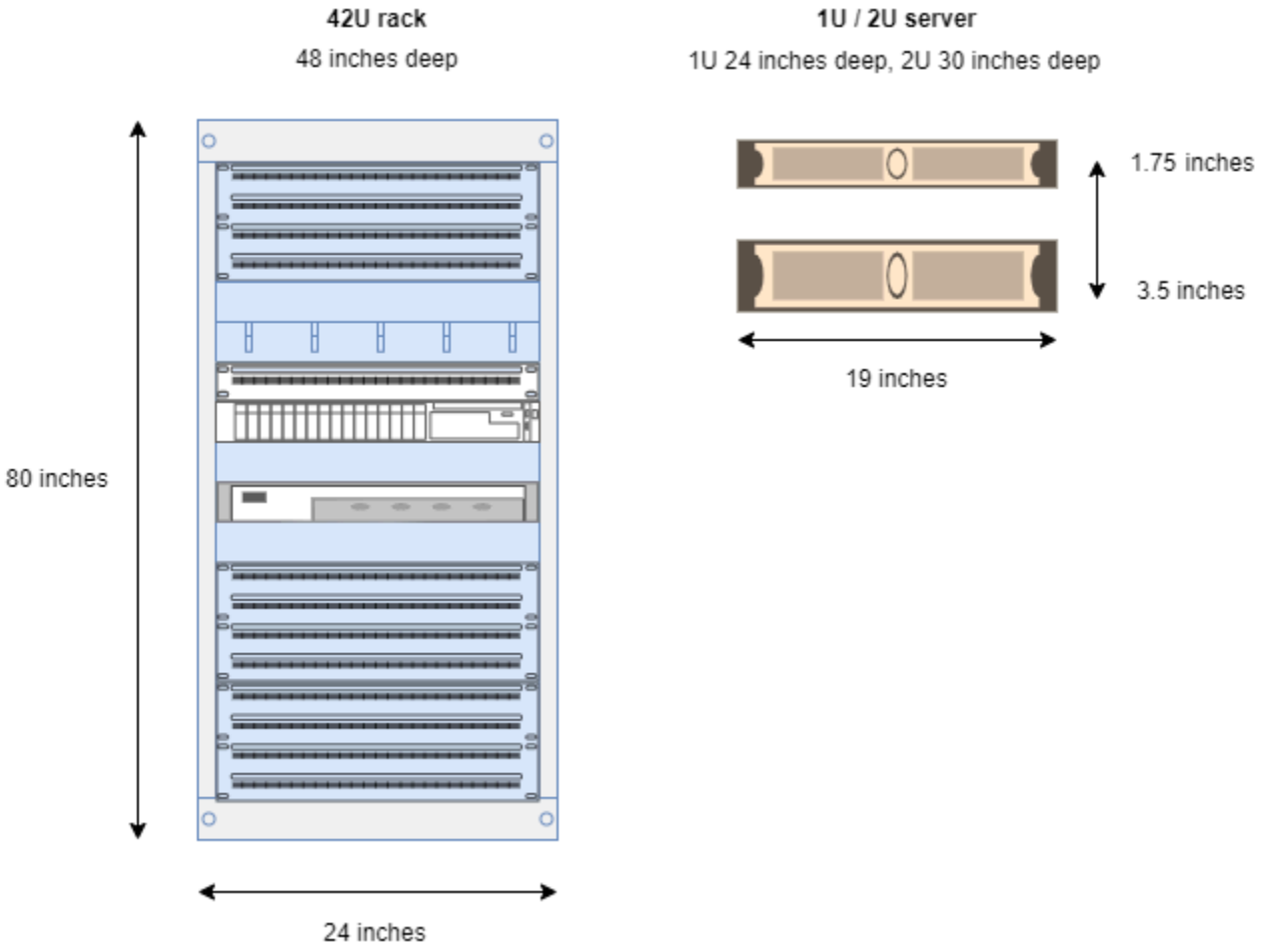
您购买的配置期限为 3 年，有三种付款选项可供选择：全额预付、部分预付和不预付。如果您选择“部分预付”或“不预付”付款选项，则将按月收费。任何预付费用都将在 Outpost 安装完毕且计算和存储容量可供使用的 24 小时后收取。有关更多信息，请参阅：

- AWS Outposts 机架定价
- AWS Outposts 服务器定价

如何 AWS Outposts 运作

AWS Outposts 旨在在你的前哨基地和 AWS 地区之间保持持续而稳定的连接下运行。要实现与该区域以及本地环境中的本地工作负载的连接，您必须将 Outpost 连接到本地网络。您的本地网络必须提供返回该区域和互联网的广域网 (WAN) 访问权限。它还必须提供对本地工作负载或应用程序所在的本地网络的 LAN 或 WAN 访问权限。

下图说明了 Outpost 的两种外形规格。



内容

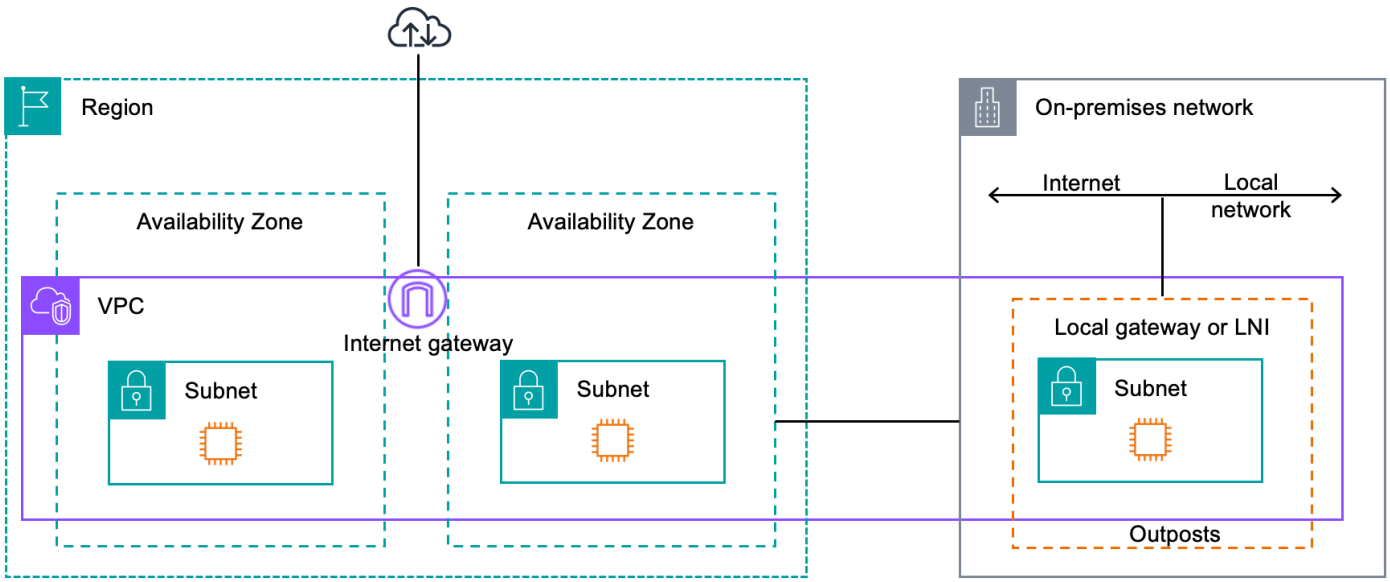
- 本地网关
- 本地网络接口

网络组件

AWS Outposts 使用可在 AWS 该区域访问的 VPC 组件（包括互联网网关、虚拟私有网关、Amazon VPC 传输网关和 VPC 终端节点）将 Amazon VPC 从一个区域扩展到前哨站。Outpost 位于该区域内的一个可用区中，是该可用区的延伸，让您可以用来实现弹性。

下图显示了您的 Outpost 的网络组件。

- AWS 区域 和本地网络
- 区域内有多个子网的 VPC
- 本地网络中的 Outpost
- Outpost 与本地网络之间的连接由本地网关（机架）或本地网络接口（服务器）提供



VPC 和子网

虚拟私有云 (VPC) 跨越其 AWS 区域内的所有可用区。您可以通过添加 Outpost 子网将区域中的任何 VPC 扩展到您的 Outpost。要将 Outpost 子网添加到 VPC，请在创建子网时指定 Outpost 的 Amazon Resource Name (ARN)。

Outpost 支持多个子网。在 Outpost 中启动 EC2 实例时，您可以指定 EC2 实例子网。您无法指定部署实例的底层硬件，因为 Outpost 是一个 AWS 计算和存储容量池。

每个 Outpost 可以支持多个 VPC，这些 VPC 可以有一个或多个 Outpost 子网。有关 VPC 配额的信息，请参阅 Amazon VPC 用户指南中的 Amazon VPC 配额。

您可以根据创建 Outpost 的 VPC 的 VPC CIDR 范围创建 Outpost 子网。您可以将 Outpost 地址范围用于资源，例如驻留在 Outpost 子网中的 EC2 实例。

路由

默认情况下，每个 Outpost 子网都会从其 VPC 继承主路由表。您可以创建自定义路由表，并将其与 Outpost 子网相关联。

Outpost 子网的路由表与可用区子网的路由表一样起作用。您可以指定 IP 地址、互联网网关、本地网关、虚拟私有网关和对等连接作为目标。例如，每个 Outpost 子网，无论是通过继承的主路由表还是自定义表，都继承 VPC 本地路由。这意味着 VPC 中的所有流量，包括目标为 VPC CIDR 的 Outpost 子网，仍在 VPC 中路由。

Outpost 子网路由表可以包括以下目的地：

- VPC CIDR 范围 — 在安装时 AWS 定义此范围。这是本地路由，适用于所有 VPC 路由，包括同一 VPC 中 Outpost 实例之间的流量。
- AWS 区域目标 — 这包括亚马逊简单存储服务 (Amazon S3) Simple Service、Amazon DynamoDB 网关终端节点 AWS Transit Gateway、虚拟私有网关、互联网网关和 VPC 对等互连的前缀列表。

  如果您与同一 Outpost 上的多个 VPC 建立了对等连接，则这些 VPC 之间的流量将保留在 Outpost 中，并且不会使用返回该地区的服务链路。
- 使用本地网关跨越 Outpost 的 VPC 内部通信 — 您可以使用直接 VPC 路由，跨越不同 Outpost 在同一 VPC 的子网与本地网关之间建立通信。有关更多信息，请参阅：
  - 直接 VPC 路由
  - 路由到 AWS Outposts 本地网关

DNS

对于连接 VPC 的网络接口，Outposts 子网中的 EC2 实例可以使用 Amazon Route 53 DNS 服务将域名解析为 IP 地址。Route 53 支持 DNS 功能，例如域注册、DNS 路由和对您的 Outpost 中运行的实例进行运行状况检查。支持公有和私有托管可用区将流量路由到特定域。该 AWS 地区托管了 Route 53

解析器。因此，从前哨基地返回该 AWS 地区的服务链路连接必须处于正常运行状态，这些 DNS 功能才能正常运行。

使用 Route 53 时，您可能会遇到更长的 DNS 解析时间，具体取决于您的前哨基地和 AWS 区域之间的路径延迟。在这种情况下，您可以使用在本地环境中以本地方式安装的 DNS 服务器。要使用自己的 DNS 服务器，必须为本地 DNS 服务器创建 DHCP 选项集并将其与 VPC 关联。您还必须确保这些 DNS 服务器有 IP 连接。您可能还需要将路由添加到本地网关路由表中以实现可访问性，但这仅适用于带有本地网关的 Outpost 机架。由于 DHCP 选项集具有 VPC 范围，因此 Outpost 子网和 VPC 的可用区子网中的实例都将尝试使用指定的 DNS 服务器进行 DNS 名称解析。

源自 Outpost 的 DNS 查询不支持查询日志记录。

服务链路

服务链接是从你的 Outpost 返回你选择的 AWS 地区或 Outposts 主区域的连接。服务链路是一组加密的 VPN 连接，每当 Outpost 与您选择的主区域通信时，都会使用这些连接。您可以使用虚拟 LAN (VLAN) 对服务链路上的流量进行分段。服务链路 VLAN 支持前哨基地和 AWS 区域之间的通信，用于管理前哨基地和 AWS 区域与前哨基地之间的 VPC 内部流量。

您的服务链路是在您的 Outpost 预置完毕时创建的。如果您有服务器外形，则可以创建连接。如果您有机架，则 AWS 创建服务链接。有关更多信息，请参阅：

- 前哨基地连接至 AWS 区域
- 《AWS Outposts 高可用性设计和架构注意事项》白皮书中的应用程序/工作负载路由 AWS

本地网关

Outpost 机架包括本地网关，用于连接到您的本地网络。如果您有 Outpost 机架，则可以将本地网关作为目标，目标为本地网络。本地网关仅适用于 Outpost 机架，并且只能在与 Outpost 机架关联的 VPC 和子网路由表中使用。有关更多信息，请参阅：

- 本地网关
- 《AWS Outposts 高可用性设计和架构注意事项》白皮书中的应用程序/工作负载路由 AWS

本地网络接口

Outpost 服务器包括本地网络接口，用于连接到您的本地网络。本地网络接口仅适用于在 Outpost 子网上运行的 Outpost 服务器。您不能在 Outpost 机架上或 AWS 该地区使用来自 EC2 实例的本地网络接

口。本地网络接口仅适用于本地位置。有关更多信息，请参阅适用于 Outpost 服务器的AWS Outposts用户指南中的本地网络接口。

Outpost 机架的站点要求

Outpost 站点是您的 Outpost 运行所在的物理位置。站点仅在部分国家和地区可用。有关更多信息，请参阅 AWS Outposts 机架常见问题。参考以下问题：Outpost 机架在哪些国家和地区可用？

本页介绍了 Outpost 机架的要求。如果要安装聚合、核心、边缘 (ACE) 机架，则您的站点还必须满足中列出的要求Outposts ACE 机架的场地要求。

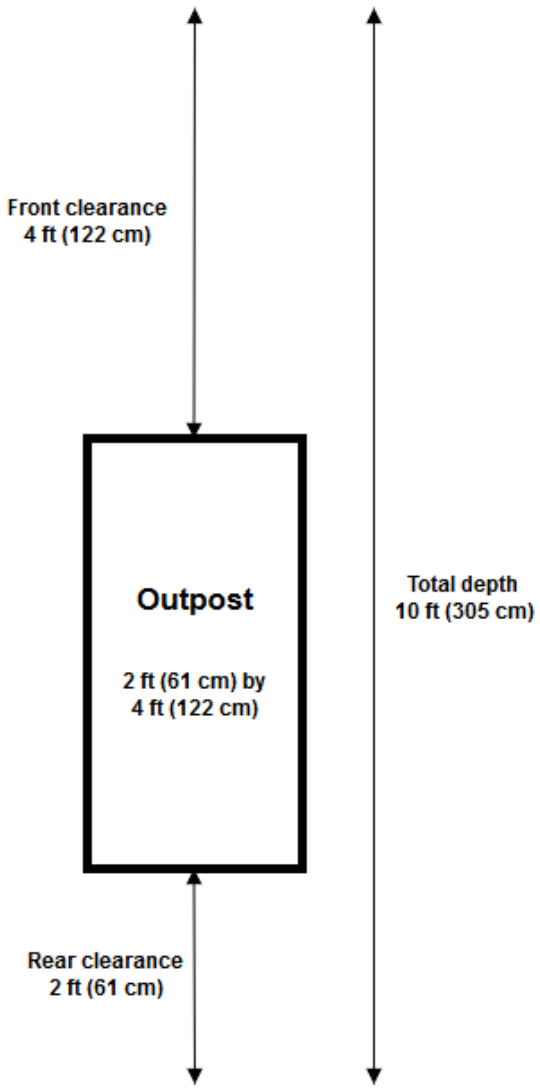
有关 Outpost 服务器的要求，请参阅 AWS Outposts 服务器用户指南中的 Outpost 服务器的站点要求。

设施

如下是机架的设施要求。

- 温度和湿度 - 环境温度必须介于 41°F (5°C) 到 95°F (35°C) 之间。相对湿度必须介于 8% 到 80% 之间，无冷凝。
- 气流 - 机架从前通道吸入冷空气，再将热空气排到后通道。机架位置上气流的每分钟立方英尺（CFM）数必须至少为 kVA 的 145.8 倍。
- 装载底座 - 装载底座必须能够容纳高 94 英寸（239 厘米）、宽 54 英寸（138 厘米）、深 51 英寸（130 厘米）的机架箱。
- 重量支撑 — 重量因配置而异。您可以在机架点负载上找到订单摘要中为您的配置指定的重量。机架安装位置和通往该处的路径必须能够支撑指定的重量。这包括沿途的任何货运和标准电梯。
- 间隙 - 机架高度为 80 英寸（203 厘米），宽度为 24 英寸（61 厘米），深度为 48 英寸（122 厘米）。任何门口、走廊、转弯、坡道和电梯都必须提供足够的间隙。在最后的静止位置上，Outpost 必须有一个 24 英寸（61 厘米）宽 x 48 英寸（122 厘米）深的区域，以及额外的 48 英寸（122 厘米）前部间隙和 24 英寸（61 厘米）后部间隙。Outpost 需要的最小总面积为 24 英寸（61 厘米）宽 x 10 英尺（305 厘米）深。

  下图显示了 Outpost 需要的最小总面积，包括间隙在内。



- 抗震支撑 — 在法规或法规要求的范围内，您将为机架在设施中安装和维护适当的抗震锚固和支撑。AWS 提供地板支架，可为所有 Outposts 机架提供高达 2.0G 的地震活动保护。
- 接合点 — 我们建议您在机架位置提供键合线/点，以便 AWS经过认证的技术人员可以在安装过程中粘合机架。
- 设施访问权限 — 您不得以对进入、维修或移除前哨基地 AWS 的能力产生负面影响的方式更改设施。
- 海拔高度 - 安装机架的房间的海拔高度必须低于 10,005 英尺（3,050 米）。

联网

如下是机架的网络要求。

- 提供速度为 1Gbps、10Gbps、40Gbps 或 100Gbps 的上行链路。

  有关服务链路连接的带宽建议，请参阅 Bandwidth recommendations。
- 提供配有 Lucent 连接器（LC）的单模光纤（SMF）、多模光纤（MMF）或配有 LC 的 MMF OM4。
- 提供一到两台上游设备，可以是交换机或路由器。我们建议提供两台设备来获得高可用性。

网络就绪性核对清单

在收集 Outpost 配置的信息时，您可以参考这份核对清单。这包括局域网、广域网、前哨基地和本地流量目的地之间的任何设备，以及该 AWS 地区的目的地。

上行链路速度、端口和光纤

上行链路速度和端口

一台 Outpost 具有两个 Outpost 网络设备，连接到您的本地网络上。每一设备能够支持的上行链路数量取决于您的带宽需求和路由器的支持能力。有关更多信息，请参阅 物理连接。

以下列表根据上行链路速度显示了每一 Outpost 网络设备支持的上行链路端口数量。

1 Gbps

1、2、4、6 或 8 个上行链路

10 Gbps

1、2、4、8、12 或 16 个上行链路

40 Gbps 或 100 Gbps

1、2 或 4 个上行链路

光纤

支持以下光纤类型：

- 配有 Lucent 连接器（LC）的单模光纤（SMF）
- 多模光纤（MMF）或装有 LC 的 MMF OM4

根据上行链路速度和您选择的光纤类型，支持以下光纤标准。

上行链路速度	光纤类型	光纤标准
1 Gbps	SMF	– 1000Base-LX
1 Gbps	MMF	– 1000Base-SX
10 Gbps	SMF	– 10GBASE-IR – 10GBASE-LR
10 Gbps	MMF	– 10GBASE-SR
40Gbps	SMF	– 40GBASE-IR4 (LR4L) – 40GBASE-LR4
4 x 10 Gbps 分路应用	MMF	– 40GBASE-ESR4 – 40GBASE-SR4
100 Gbps	SMF	– 100G PSM4 MSA – 100GBASE-CWDM4 — 100GBASE-LR4
4 x 25 Gbps 分路应用	MMF	– 100GBASE-SR4

Outpost 链路聚合和 VLAN

Outpost 和您的网络之间需要链路聚合控制协议（LACP）。您必须将动态 LAG 与 LACP 结合使用。

每台 Outpost 网络设备都需要以下 VLAN。有关更多信息，请参阅 虚拟 LAN。

Outpost 网络设备	服务链路 VLAN	本地网关 VLAN
#1	有效值：1-4094	有效值：1-4094
#2	有效值：1-4094	有效值：1-4094

对于每台 Outpost 网络设备，您可以选择是要将相同的 VLAN 还是不同的 VLAN 用于服务链路和本地网关。但是，我们建议每一台 Outpost 网络设备使用与其他 Outpost 网络设备不同的 VLAN。有关更多信息，请参阅链路聚合和虚拟 LAN。

另外，还建议您使用冗余的第 2 层连接。LACP 用于支持链路聚合，不用于提供高可用性。Outpost 网络设备之间不支持 LACP。

Outpost 网络设备 IP 连接

两台 Outpost 网络设备都需要一个 CIDR 和 IP 地址来用于服务链路和本地网关 VLAN。我们建议为每台网络设备分配一个 /30 或 /31 CIDR 的专用子网。指定要供 Outpost 使用的子网和子网 IP 地址。有关更多信息，请参阅 网络层连接。

Outpost 网络设备	服务链路要求	本地网关要求
#1	- 服务链路 CIDR (/30 或 /31) - 服务链路 IP 地址	- 本地网关 CIDR (/30 或 /31) - 本地网关 IP 地址
#2	- 服务链路 CIDR (/30 或 /31) - 服务链路 IP 地址	- 本地网关 CIDR (/30 或 /31) - 本地网关 IP 地址

服务链路最大传输单元 (MTU)

网络必须支持 Outpost 和父区域中的服务链接端点之间的 1500 字节的 MTU。 AWS 有关服务链路的更多信息，请参阅 AWS Outposts 与 AWS 区域的连接。

服务链路边界网关协议

Outpost 在每个 Outpost 网络设备和您的本地网络设备之间建立一个外部 BGP (eBGP) 对等会话，以便通过服务链路 VLAN 进行服务链路连接。有关更多信息，请参阅 服务链路 BGP 连接。

Outpost	服务链路 BGP 要求
您的 Outpost	- Outpost BGP 自治系统号（ASN）。2 字节（16 位）或 4 字节（32 位）。来自您的私有 ASN 范围（64512-65534 或 4200000000-4294967294）。 - 基础设施 CIDR（必须是 /26，通告为两个连续的 /27）。

本地网络设备	服务链路 BGP 要求
#1	- 服务链路 BGP 对等 IP 地址。 - 服务链路 BGP 对等 ASN。2 字节（16 位）或 4 字节（32 位）。
#2	- 服务链路 BGP 对等 IP 地址。 - 服务链路 BGP 对等 ASN。2 字节（16 位）或 4 字节（32 位）。

服务链路防火墙

UDP 和 TCP 443 必须在防火墙中以有状态的方式列出。

协议	源端口	源地址	目的地端口	目标地址
UDP	443	Outpost 服务链路 /26	443	Outpost 区域的公有路由
TCP	1025-65535	Outpost 服务链路 /26	443	Outpost 区域的公有路由

您可以使用连接或公共互联网 AWS Direct Connect 连接将 Outpost 连接回该 AWS 地区。对于 Outpost 服务链路连接，您可以在防火墙或边缘路由器上使用 NAT 或 PAT。服务链路的建立始终从 Outpost 发起。

本地网关边界网关协议

Outpost 建立从各个 Outpost 网络设备到本地网络设备的 eBGP 对等会话，以便从本地网络连接到本地网关。有关更多信息，请参阅 本地网关 BGP 连接。

Outpost	本地网关 BGP 要求
您的 Outpost	- Outpost BGP 自治系统号（ASN）。2 字节（16 位）或 4 字节（32 位）。来自您的私有 ASN 范围（64512-65534 或 4200000000-4294967294）。 - 要通告的 CoIP CIDR（公有或私有，最低 /26）。

本地网络设备	本地网关 BGP 要求
#1	- 本地网关 BGP 对等 IP 地址。 - 本地网关 BGP 对等 ASN。2 字节（16 位）或 4 字节（32 位）。
#2	- 本地网关 BGP 对等 IP 地址。 - 本地网关 BGP 对等 ASN。2 字节（16 位）或 4 字节（32 位）。

Power

Outpost 电源架支持以下三种电源配置：5 kVA、10 kVA 或 15 kVA。电源架的配置取决于 Outpost 容量的总功耗。例如，如果 Outpost 资源的最大功耗为 9.7 kVA，您必须提供 10 kVA 的电源配置：4 x L6-30P 或 IEC309，2 个连至 S1，2 个连至 S2，以获得冗余的单相电源。下方第二张表格中列出了三种电源配置。

要查看不同 Outpost 资源的功耗要求，请在 AWS Outposts 主机中选择 “浏览目录”，网址为 https://console.aws.amazon.com/outposts/。

要求	规范
交流线路电压	单相 208 至 277 VAC；50 或 60 Hz 三相： • 208 至 250 VAC（Delta）；50 到 60 Hz • 346 至 480 VAC (Wye)；50 到 60 Hz
功耗	5 kVA (4 kW)、10 kVA (9 kW) 或 15 kVA (13 kW)
交流保护（上游断路器）	对于 1N 输入（非冗余）和 2N 输入（冗余）：30 A、32 A 或 50 A，带 D 曲线或 K 曲线断路器。 仅限于 2N 输入（冗余）：C 曲线、D 曲线或 K 曲线断路器。 不支持 B 曲线或更低规格。
交流输入类型（插口）	单相 3xL6-30P，P+P+E，30A；或 3xIEC60309 P+N+E，IP67，32A 插头 三相 Wye 1xIEC60309，3P+N+E，IP67，时钟位置 7、30A 插头；或 1xIEC60309，3P+N+E，IP67，时钟位置 6，32A 插头 三相 Delta 1xNon-NEMA 扭锁式 Hubbell CS8365C，3P+E，中心接地，50A 插头 **Note** 最佳做法是将 IP67 插头与 IP67 插口搭配使用。如果无法做到，IP67 插头可与 IP44 插口搭配使用。插头与插座组合后的额定值将是其中较低的额定值 (IP44)。
电源线长度	10.25 英尺 (3 米)
电源线 - 机架布线输入	从机架上方或下方

电源架有两个输入，即 S1 和 S2，可以按如下方式进行配置。

	冗余，单相	冗余，三相	单相	三相
5 kVA	2 x L6-30P 或 IEC309；1 个掉到 S1，1 个掉到 S2	2 x AH530P7W、AH532P6W 或 CS8365C；1 个掉到 S1，1 个掉到 S2	1 x L6-30P 或 IEC309；1 掉到 S1	1 x AH530P7W、AH532P6W 或 CS8365C；1 掉到 S1
10 kVA	4 x L6-30P 或 IEC309；2 次掉落到 S1，2 次掉落到 S2		2 x L6-30P 或 IEC309；2 掉到 S1	
15 kVA	6 x L6-30P 或 IEC309；3 次掉落到 S1，3 次掉落到 S2		3 x L6-30P 或 IEC309；3 掉到 S1	

如果如前所述 AWS 提供的交流电鞭子必须安装备用电源插头，请考虑以下事项：

- 只有客户安排并经过认证的电工才能修改交流电源线来匹配新的插头类型。
- 安装应符合所有适用的国家、州/省和地方安全要求，并根据需要进行电气安全检查。
- 您（客户）应将交流鞭子插头的修改通知您的 AWS 代表。根据要求，您将向提供有关修改的信息 AWS。您还要附上拥有管辖权的机构签发的所有安全检查记录。要求 AWS 员工在设备上操作之前，必须满足这项安装安全验证要求。

订单配送

为了配送订单， AWS 将与您安排日期和时间。您还会收到一份安装前需要查验或提供的物品的核对清单。

AWS 安装团队将在预定的日期和时间到达您的现场。他们会将机架放在确定的位置。您和电工负责完成机架的电气连接和安装。

您必须确保电气安装以及这些安装的任何变更由经过认证的电工按照所有适用法律、法规和最佳实践来完成。 AWS 在对 Outpost 硬件或电气装置进行任何更改之前，您必须获得书面批准。您 AWS 同意提供证明任何变更的合规性和安全性的文件。 AWS 对前哨电气装置或设施电气线路或任何变更造成的任何风险概不负责。您不得对 Outposts 硬件进行任何其他变更。

团队将通过您提供的上行链路为 Outpost 机架建立网络连接，并配置机架的容量。

当您确认您的 AWS 账户中为 Outpost 机架提供的 Amazon EC2 和 Amazon EBS 容量可以使用时，安装即告完成。

Outposts ACE 机架的场地要求

> **Note**
>
> 如果您不需要 ACE 机架，请跳过本节。

聚合、核心、边缘 (ACE) 机架充当多机架 Outpost 部署的网络聚合点。如果您有五个或更多计算机架，则必须安装 ACE 机架。如果您的计算机架少于五个，但计划将来扩展到五个或更多机架，我们建议您尽早安装 ACE 机架。

要安装 ACE 机架，除了中列出的要求外，还必须满足本节中的要求Outpost 机架的站点要求。

设施

这些是 ACE 机架的设施要求。

- 电源 — 所有机架出厂时均配备 10kVA 单相（AA+BB；IEC60309 或 L6-30P Whip 连接器类型）。
- 承重 — 机架重量为 705 磅；320 千克。
- 间隙/尺寸尺寸 — 机架高度为 80 英寸；203 厘米。

> **Note**
>
> ACE 机架不是完全封闭的，不包括前门或后门。

联网

这些是 ACE 机架的网络要求。要了解 ACE 机架如何连接 Outposts 网络设备、您的本地网络设备和 Outpost 机架，请参阅。ACE 机架连接

- 机架网络要求 — 确保满足网络就绪性核对清单和机架的本地网络连接部分中列出的要求，但以下更改除外：

  - ACE 机架有四台连接到上游设备的网络设备，而不是像单个 Outposts 机架那样有两台。
  - ACE 机架不支持 1 Gbps 的上行链路。
- 上行链路速度 — 提供速度为 10 Gbps、40 Gbps 或 100 Gbps 的上行链路。有关服务链路连接的带宽建议，请参阅服务链路带宽建议。

> **Important**
>
> ACE 机架不支持 1 Gbps 的上行链路。

- 光纤 — 使用朗讯连接器 (LC) 提供单模光纤 (SMF)，或使用朗讯连接器 (LC) 提供多模光纤 (MMF)。有关支持的光纤类型和光学标准的完整列表，请参阅上行链路速度、端口和光纤。
- 上游设备-提供两到四个上游设备，可以是交换机或路由器。
- 服务 VLAN 和本地网关 VLAN — 对于四台 ACE 网络设备中的每台，您都必须提供一个服务 VLAN 和一个不同的本地网关 VLAN。您可以选择仅提供两个不同的 VLAN，一个用于服务 VLAN，一个用于本地网关 VLAN，或者在每个 ACE 网络设备中为服务 VLAN 和 LGW VLAN 提供不同的 VLAN，总共有 8 个不同的 VLAN。有关如何使用链路聚合组 (LAG) 和 VLAN 的更多信息，请参阅链路聚合和虚拟 LAN。
- 服务链路和本地网关 VLAN 的 CIDR 和 IP 地址 — 我们建议为每台带有 /30 或 /31 CIDR 的 ACE 网络设备分配一个专用子网。或者，可以在每个服务和本地网关 VLAN 中分配一个 /29 子网。在这两种情况下，都必须指定要使用的 ACE 网络设备的 IP 地址。有关更多信息，请参阅 网络层连接。
- 服务链路 VLAN 和本地网关 VLAN 的客户和 Outpost BGP 自治系统号 (ASN) — Outpost 在每个 ACE 机架设备和本地网络设备之间建立外部 BGP (eBGP) 对等会话，用于通过服务链路 VLAN 进行服务链路连接。此外，它还会建立从每台 ACE 网络设备到本地网络设备的 eBGP 对等会话，以便从您的本地网络连接到本地网关。有关更多信息，请参阅 服务链路 BGP 连接 和 本地网关 BGP 连接。

> **Important**
>
> 服务链路基础设施子网 — Outposts 安装中包含的每个计算机架都需要服务链路基础设施子网（必须为 /26）。

Power

这些是 ACE 机架的电源要求。

要求	规范
交流线路电压	单相 200 至 240 VAC；50 或 60 Hz
功耗	10 kVA 单相 (AA+BB)
交流保护（上游断路器）	仅限于 2N 输入（冗余）：C 曲线、D 曲线或 K 曲线断路器。 不支持 B 曲线或更低规格。
交流输入类型（插口）	IEC60309 或 L6-30P 鞭状连接器类型。

开始使用 AWS Outposts

订购 Outpost 以开始。安装 Outpost 设备后，启动 Amazon EC2 实例并访问您的本地网络。

任务

- 创建一个 Outpost 并订购 Outpost 容量
- 在你的 Outpost 机架上启动一个实例

创建一个 Outpost 并订购 Outpost 容量

要开始使用 AWS Outposts，您必须创建前哨基地并订购前哨站容量。

先决条件

- 查看您的 Outpost 机架的可用配置。
- Outpost 站点是存放 Outpost 设备的实际位置。在订购容量之前，请验证您的站点是否符合要求。有关更多信息，请参阅 Outpost 机架的站点要求。
- 您必须有 AWS 企业支持计划或 AWS 企业入口支持计划。
- 确定哪个 AWS 账户 将拥有前哨基地。使用此账户创建 Outposts 站点、创建 Outpost 并下订单。监控与此账户关联的电子邮件以获取来自的信息 AWS。

任务

- 步骤 1：创建站点
- 步骤 2：创建一个 Outpost
- 步骤 3：下订单
- 步骤 4：修改实例容量
- 后续步骤

步骤 1：创建站点

创建一个站点以指定运营地址。运营地址是您的 Outposts 机架的实际位置。

先决条件

- 确定运营地址。

创建站点

1. AWS 使用将拥有前哨基地 AWS 账户 的用户登录。
2. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
3. 要选择父级 AWS 区域，请使用页面右上角的区域选择器。
4. 在导航窗格中，选择 Sites (站点)。
5. 选择 Create site (创建站点)。
6. 对于支持的硬件类型，请选择机架和服务器。
7. 输入您的站点的名称、描述和运营地址。
8. 对于站点详细信息，请提供有关该站点的所需信息。
   - 最大重量 — 此站点可以承受的最大机架重量，以磅为单位。
   - 功耗 — 机架硬件放置位置的可用功耗，以 kVA 为单位。
   - 电源选项 — 您可以为硬件提供的电源选项。
   - 电源连接器 — AWS 应计划的电源连接器，以便为硬件提供连接。
   - 供电位置 — 指明电源是位于机架上方还是下方。
   - 上行链路速度 — 机架在连接区域时应支持的上行链路速度，以 Gbps 为单位。
   - 上行链路数量 — 您打算用于将机架连接到网络的每台 Outpost 网络设备的上行链路数量。
   - 光纤类型 — 用于将机架连接到网络的光纤类型。
   - 光纤标准 — 用于将机架连接到网络的光纤标准类型。
9. （可选）对于网站备注，请输入可能 AWS 有助于了解该网站的任何其他信息。
10. 阅读设施要求，然后选择我已阅读设施要求。
11. 选择 Create site (创建站点)。

步骤 2：创建一个 Outpost

为您的机架创建一个 Outpost。然后，在下单时指定此前哨基地。

先决条件

- 确定要与您的站点关联的 AWS 可用区。

创建 Outpost

1. 在导航窗格中，选择 Outposts。
2. 选择创建 Outpost。
3. 选择机架。
4. 为您的 Outpost 输入名称和描述。
5. 为您的 Outpost 选择可用区。
6. （可选）要配置私有连接，请选择使用私有连接。选择与您的 Outpost 位于同一个可用区的 VPC AWS 账户 和子网。有关更多信息，请参阅 the section called “先决条件”。
7. 对于站点 ID，请选择您的站点。
8. 选择创建 Outpost。

步骤 3：下订单

订购您需要的 Outpost 机架。提交订单后， AWS Outposts 代表将与您联系。

> **Important**
>
> 提交订单后，您将无法对其进行编辑，因此在提交之前请仔细查看所有详细信息。如果您需要更改订单，请联系您的 AWS 账户经理。

先决条件

- 确定您将如何支付订单。您可以在全部预付、部分预付或者不预付。如果您不选择预付所有费用，则需要在三年期限内按月支付费用。

  定价包括交付、安装、基础设施服务维护以及软件修补程序和升级。
- 确定收货地址是否与您为该站点指定的操作地址不同。

要下订单

1. 在导航窗格中，选择采购订单。
2. 选择下订单。
3. 对于支持的硬件类型，请选择机架。

4. 要添加容量，请选择配置。如果可用配置不能满足您的需求，您可以联系 AWS 申请自定义容量配置。
5. 选择下一步。
6. 选择使用现有 Outpost，然后选择您的 Outpost。
7. 选择下一步。
8. 选择合同期限和付款选项。
9. 指定收货地址。您可以指定新地址或选择站点的操作地址。如果您选择运营地址，请注意，将来对站点运营地址的任何更改都不会影响到现有订单。如果您需要更改现有订单的配送地址，请联系您的 AWS 账户经理。
10. 选择下一步。
11. 在查看和订购页面上，验证您的信息是否正确并根据需要进行编辑。提交订单后将无法编辑。
12. 选择下订单。

步骤 4：修改实例容量

Outpost 为您的站点提供 AWS 计算和存储容量池，作为 AWS 区域中可用区的私有扩展。由于 Outpost 中可用的计算和存储容量是有限的，由 AWS 安装在您站点的机架的大小和数量决定，因此您可以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以缓解服务器故障和维护事件所需的 AWS Outposts 容量 Amazon EC2、Amazon EBS 和 Amazon S3 的容量。

每个新的 Outpost 订单的容量均使用默认容量配置进行配置。您可以转换默认配置来创建各种实例以满足您的业务需求。为此，您需要创建容量任务，指定实例大小和数量，然后运行容量任务来实施更改。

> **Note**
>
> - 下单 Outposts 后，您可以更改实例大小的数量。
> - 实例的大小和数量是在前哨基地级别定义的。
> - 实例是根据最佳实践自动放置的。

修改实例容量

1. 在AWS Outposts 控制台的AWS Outposts 左侧导航窗格中，选择容量任务。

2. 在容量任务页面上，选择创建容量任务。
3. 在入门页面上，选择顺序。
4. 要修改容量，您可以使用控制台中的步骤或上传 JSON 文件。

Console steps

1. 选择修改新的 Outpost 容量配置。
2. 选择下一步。
3. 在配置实例容量页面上，每种实例类型都显示一个预先选择的最大实例大小。要添加更多实例大小，请选择添加实例大小。
4. 指定实例数量并记下针对该实例大小显示的容量。
5. 查看每个实例类型部分末尾的消息，该消息会告知您容量是否超出或不足。在实例大小或数量级别进行调整，以优化您的总可用容量。
6. 您也可以请求 AWS Outposts 针对特定实例大小优化实例数量。为此，请执行以下操作：
   a. 选择实例大小。
   b. 在相关实例类型部分的末尾选择自动平衡。
7. 对于每种实例类型，请确保至少为一种实例大小指定实例数量。
8. 选择下一步。
9. 在 “查看并创建” 页面上，验证您请求的更新。
10. 选择 “创建”。 AWS Outposts 创建容量任务。
11. 在容量任务页面上，监控任务的状态。

> **Note**
>
> - AWS Outposts 可能会要求您停止一个或多个正在运行的实例以允许运行容量任务。停止这些实例后， AWS Outposts 将运行任务。
> - 如果您在完成订单后需要更改容量，请联系 AWS Support 以进行更改。

Upload JSON file

1. 选择上传容量配置。
2. 选择下一步。

3. 在上传容量配置计划页面上，上传指定实例类型、大小和数量的 JSON 文件。

   Example

   示例 JSON 筛选条件

   ```
   {
       "RequestedInstancePools": [
           {
               "InstanceType": "c5.24xlarge",
               "Count": 1
           },
           {
               "InstanceType": "m5.24xlarge",
               "Count": 2
           }
       ]
   }
   ```

4. 在容量配置计划部分中查看 JSON 文件的内容。
5. 选择下一步。
6. 在 “查看并创建” 页面上，验证您请求的更新。
7. 选择 “创建”。 AWS Outposts 创建容量任务。
8. 在容量任务页面上，监控任务的状态。

> **Note**
>
> - AWS Outposts 可能会要求您停止一个或多个正在运行的实例以允许运行容量任务。停止这些实例后， AWS Outposts 将运行任务。
> - 如果您在完成订单后需要更改容量，请联系 AWS Support 以进行更改。

后续步骤

您可以使用 AWS Outposts 控制台查看订单状态。您的订单的初始状态为已收到订单。 AWS 代表将在三个工作日内与您联系。当您的订单状态更改为订单处理时，您将收到一封确认电子邮件。 AWS 代表可能会与您联系以获取 AWS 所需的任何其他信息。

如果您对订单有任何疑问，请联系 AWS Support。

为了配送订单， AWS 将与您安排日期和时间。

您还会收到一份安装前需要查验或提供的物品的核对清单。 AWS 安装团队将在预定的日期和时间到达您的现场。团队会将机架滚动到确定的位置，您的电工可以为机架供电。团队将通过您提供的上行链路为机架建立网络连接，并配置机架的容量。当您确认您的账户有可用的 Outpost 的 Amazon EC2 和 Amazon EBS 容量后，安装即告完成。 AWS

在你的 Outpost 机架上启动一个实例

安装 Outpost 并且可以使用计算和存储容量后，您便可以开始创建资源。启动 Amazon EC2 实例并使用 Outpost 子网在您的 Outpost 上创建 Amazon EBS 卷。您还可以在 Outpost 上创建 Amazon EBS 卷的快照。有关适用于 Linux 的更多信息，请参阅亚马逊 EC2 用户指南 AWS Outposts中的本地亚马逊 EBS 快照。有关适用于 Windows 的更多信息，请参阅亚马逊 EC2 用户指南 AWS Outposts中的本地亚马逊 EBS 快照。

先决条件

您的站点必须安装一个 Outpost。有关更多信息，请参阅 创建一个 Outpost 并订购 Outpost 容量。

任务

- 第 1 步：创建 VPC
- 步骤 2：创建子网和自定义路由表
- 步骤 3：配置本地网关连接
- 步骤 4：配置本地网络
- 第 5 步：在前哨基地启动实例
- 步骤 6：测试连通性

第 1 步：创建 VPC

您可以将 AWS 该地区的任何 VPC 扩展到您的前哨基地。如果您已经有可供使用的 VPC，请跳过此步骤。

为您的前哨基地创建 VPC

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 选择与 Outposts 机架相同的区域。
3. 在导航窗格上，选择您的 VPC，然后选择创建 VPC。

4. 仅选择 VPC。
5. （可选）在名称标签中输入 VPC 的名称。
6. 对于 IPv4 CIDR 块，选择 IPv4 CIDR 手动输入，然后在 IPv4 CIDR 文本框中输入 VPC 的 IPv4 地址范围。

> **Note**
>
> 如果要使用直接 VPC 路由，请指定与您在本地网络中使用的 IP 范围不重叠的 CIDR 范围。

7. 对于 IPv6 CIDR 块，请选择无 IPv6 CIDR 块。
8. 对于“租赁”，选择“默认”。
9. （可选）要向您的 VPC 添加标签，请选择添加标签，然后输入密钥和值。
10. 选择创建 VPC。

步骤 2：创建子网和自定义路由表

您可以为前哨基地所在 AWS 区域中的任何 VPC 创建和添加前哨子网。当你这样做时，VPC 将包括前哨基地。有关更多信息，请参阅 网络组件。

> **Note**
>
> 如果您要在 Outpost 子网中启动已由其他人共享的实例 AWS 账户，请跳至第 5 步：在前哨基地启动实例。

2a：创建前哨子网

创建 Outpost 子网

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 在导航窗格中，选择 Outposts。
3. 选择 Outpost，然后依次选择操作和创建子网。您将被重定向到在 Amazon VPC 控制台中创建子网。我们为您选择 Outpost 和 Outpost 所属的可用区。
4. 选择 VPC。
5. 在子网设置中，可以选择命名您的子网并为该子网指定 IP 地址范围。

6. 选择创建子网。
7. （可选）为了便于识别 Outpost 子网，请在 “子网” 页面上启用 Outpost ID 列。要启用该列，请选择 “首选项” 图标，选择 Outpost ID，然后选择 “确认”。

2b：创建自定义路由表

遵循以下过程创建自定义路由表，其中包含指向本地网关的路由。您不能使用与可用区子网相同的路由表。

创建自定义路由表

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择路由表。
3. 选择创建路由表。
4. （可选）对于 Name（名称），为您的路由表输入名称。
5. 对于 VPC，选择您的 VPC。
6. （可选）若要添加标签，请选择 Add new tag（添加新标签），然后输入标签键和标签值。
7. 选择创建路由表。

2c：关联 Outpost 子网和自定义路由表

若要对特定子网应用路由表路由，您必须将路由表与子网关联。一个路由表可以与多个子网关联。但是，子网一次只能与一个路由表关联。任何未与路由表显式关联的子网都默认与主路由表隐式关联。

关联 Outpost 子网和自定义路由表

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择路由表。
3. 在 Subnet associations (子网关联) 选项卡上，选择 Edit subnet associations (编辑子网关联)。
4. 选中要与路由表关联的子网的复选框。
5. 选择 Save associations (保存关联)。

步骤 3：配置本地网关连接

本地网关 (LGW) 支持您的 Outpost 子网和本地网络之间的连接。有关 LGW 的更多信息，请参阅本地网关。

要在 Outposts 子网中的实例与您的本地网络之间提供连接，您必须完成以下任务。

3a. 创建自定义本地网关路由表

您可以使用 AWS Outposts 控制台为本地网关 (LGW) 创建自定义路由表。

使用控制台创建自定义 LGW 路由表

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择创建本地网关路由表。
5. （可选）在“名称”中，输入 LGW 路由表的名称。
6. 对于本地网关，请选择您的本地网关。
7. 对于模式，请选择与本地网络通信的模式。
   - 选择直接 VPC 路由以使用实例的私有 IP 地址。
   - 选择 CoIP 以使用客户拥有的 IP 地址。
     - （可选）添加或移除 CoIP 池和其他 CIDR 块

       [添加 CoIP 池] 选择添加新标签，然后执行以下操作：
       - 对于名称，请为您的 CoIP 池输入名称。
       - 对于 CIDR，请输入由客户拥有的 IP 地址组成的 CIDR 块。
     - [添加 CIDR 块] 选择添加新 CIDR，然后输入客户拥有的 IP 地址范围。
     - [移除 CoIP 池或其他 CIDR 块] 选择 CIDR 块右侧或 CoIP 池下方的移除。

       您最多可以指定 10 个 CoIP 池和 100 个 CIDR 块。
8. （可选）添加或删除标签。

   [添加标签] 选择添加新标签，然后执行以下操作：
   - 对于 Key（键），输入键名称。
   - 对于值，输入键值。

   [删除标签] 选择标签的“键”和“值”右侧的删除。
9. 选择创建本地网关路由表。

3b：将 VPC 与自定义 LGW 路由表关联

您必须将 VPC 与您的 LGW 路由表关联。默认情况下，它们不会关联。

使用以下步骤将 VPC 与 LGW 路由表关联。

您可以选择性地标记您的关联，以帮助您识别它或根据组织的需要对其进行分类。

AWS Outposts console

将 VPC 与自定义 LGW 路由表关联

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择路由表，然后依次选择操作、关联 VPC。
5. 在 VPC ID 中，选择要与本地网关路由表关联的 VPC。
6. （可选）添加或删除标签。

   要添加标签，请选择添加新标签，然后执行以下操作：

   - 对于 Key（键），输入键名称。
   - 对于值，输入键值。

   要删除标签，请选择标签的“键”和“值”右侧的删除。
7. 选择 Associate VPC (关联 VPC)。

AWS CLI

将 VPC 与自定义 LGW 路由表关联

使用 create-local-gateway-route-table-vpc-association 命令。

示例

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

输出

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

3c：在 Outpost 子网路由表中添加路由条目

在 Outpost 子网路由表中添加路由条目，以启用 Outpost 子网和 LGW 之间的流量。

与 Outpost LGW 路由表关联的 VPC 内的前哨子网可以为其路由表添加其他目标类型，即 Outpost 本地网关 ID。假设您希望目的地址为 172.16.100.0/24 的流量通过 LGW 路由到客户网络。为此，请编辑 Outpost 子网路由表，并添加以下包含目标网络和 LGW 目标的路由 () `lgw-xxxx`。

目标位置	目标
172.16.100.0/24	`lgw-id`

要在 Outpost 子网路由表中添加以**`lgw-id`**为目标的路由条目，请执行以下操作：

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择路由表，然后选择您在中创建的路由表2b：创建自定义路由表。
3. 选择操作，然后选择编辑路线。
4. 要添加路由，请选择添加路由。
5. 对于目的地，输入客户网络的目标 CIDR 块。
6. 对于目标，选择 Outpost 本地网关 ID。
7. 选择保存更改。

3d：将自定义 LGW 路由表与 LGW VIF 组相关联

VIF 群组是虚拟接口 (VIF) 的逻辑分组。将本地网关路由表与 VIF 组关联。

将自定义 LGW 路由表与 LGW VIF 组相关联

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择路由表。
5. 在详细信息窗格中选择 VIF 群组关联选项卡，然后选择编辑 VIF 群组关联。
6. 对于 VIF 群组设置，选择关联 VIF 群组，然后选择一个 VIF 群组。
7. 选择保存更改。

3e：在 LGW 路由表中添加路由条目

编辑本地网关路由表，添加以 VIF 组为目标、本地子网 CIDR 范围（或 0.0.0.0/0）作为目的地的静态路由。

目标位置	目标
172.16.100.0/24	`VIF-Group-ID`

在 LGW 路由表中添加路由条目

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 在导航窗格中，选择本地网关路由表。
3. 选择本地网关路由表，然后选择操作、编辑路由。
4. 选择 Add route（添加路由）。
5. 对于目的地，请输入目的地 CIDR 块、单个 IP 地址或前缀列表的 ID。
6. 对于目标，选择本地网关的 ID。
7. 选择 Save routes（保存路由）。

3f：（可选）为实例分配客户拥有的 IP 地址

如果您在中将 Outposts 配置3a. 创建自定义本地网关路由表为使用客户拥有的 IP (CoIP) 地址池，则必须从 CoIP 地址池中分配一个弹性 IP 地址，并将该弹性 IP 地址与实例关联起来。有关 CoIP 的更多信息，请参阅 客户拥有的 IP 地址。

如果您将 Outposts 配置为使用直接 VPC 路由 (DVR)，请跳过此步骤。

Amazon VPC console

为实例分配 CoIP 地址

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Elastic IPs。
3. 选择 Allocate Elastic IP address (分配弹性 IP 地址)。
4. 对于网络边界组，选择通告 IP 地址的位置。
5. 对于公有 IPv4 地址池，选择客户拥有的 IPv4 地址池。
6. 对于客户拥有的 IPv4 地址池，请选择您配置的地址池。
7. 选择 Allocate。
8. 选择弹性 IP 地址，然后选择操作、关联弹性 IP 地址。
9. 从实例中选择实例，然后选择关联。

AWS CLI

为实例分配 CoIP 地址

1. 使用 describe-coip-pools 命令检索有关您的客户拥有的地址池的信息。

```
aws ec2 describe-coip-pools
```

下面是示例输出。

```
{
    "CoipPools": [
        {
            "PoolId": "ipv4pool-coip-0abcdef0123456789",
            "PoolCidrs":  [
                "192.168.0.0/16"
            ],
            "LocalGatewayRouteTableId": "lgw-rtb-0abcdef0123456789"
        }
    ]
}
```

2. 使用 allocate-address 命令分配弹性 IP 地址。使用上一步中返回的池 ID。

```
aws ec2 allocate-address--address 192.0.2.128 --customer-owned-ipv4-
pool ipv4pool-coip-0abcdef0123456789
```

下面是示例输出。

```
{
    "CustomerOwnedIp": "192.0.2.128",
    "AllocationId": "eipalloc-02463d08ceEXAMPLE",
    "CustomerOwnedIpv4Pool": "ipv4pool-coip-0abcdef0123456789",
}
```

3. 使用 associate-address 命令关联弹性 IP 地址与 Outpost 实例。使用上一步返回的分配 ID。

```
aws ec2 associate-address --allocation-id eipalloc-02463d08ceEXAMPLE --network-
interface-id eni-1a2b3c4d
```

下面是示例输出。

```
{
    "AssociationId": "eipassoc-02463d08ceEXAMPLE",
}
```

共享的客户拥有的 IP 地址池

如果要使用共享的客户拥有的 IP 地址池，则在开始配置之前必须共享该池。有关如何共享客户拥有的 IPv4 地址的信息，请参阅 AWS RAM 用户指南中的共享您的 AWS 资源。

步骤 4：配置本地网络

Outpost 建立从每个 Outpost 网络设备 (OND) 到客户本地网络设备 (CND) 的外部 BGP 对等连接，以发送和接收来自本地网络到 Outposts 的流量。有关更多信息，请参阅本地网关 BGP 连接。

要从本地网络向 Outpost 发送和接收流量，请确保：

- 在您的客户网络设备上，本地网关 VLAN 上的 BGP 会话在您的网络设备上处于活动状态。

- 对于从本地到Outposts的流量，请确保在CND中收到来自Outposts的BGP广告。这些 BGP 广告包含您的本地网络必须使用的路由，用于将流量从本地路由到 Outpost。因此，请确保您的网络在 Outposts 和本地资源之间有正确的路由。
- 对于从 Outposts 到本地网络的流量，请确保您的 CND 将本地网络子网的 BGP 路由广告发送到 Outposts（或 0.0.0.0/0）。或者，你可以向 Outposts 通告一条默认路由（例如 0.0.0.0/0）。CND 通告的本地子网的 CIDR 范围必须等于或包含在中配置的 CIDR 范围。3e：在 LGW 路由表中添加路由条目

示例：直接 VPC 模式下的 BGP 通告

考虑一下这样的场景：你有一个 Outpost，配置为直接 VPC 模式，两个 Outposts 机架式网络设备通过本地网关 VLAN 连接到两台客户的本地网络设备。配置了以下内容：

- VPC：CIDR 块为 10.0.0.0/16。
- VPC 中的前哨子网，网段为 10.0.3.0/24。
- 本地网络中带有 CIDR 块的子网 172.16.100.0/24
- Outposts 使用 Outpost 子网中实例的私有 IP 地址（例如 10.0.3.0/24）与您的本地网络进行通信。

在这种情况下，通过以下方式通告的路由：

- 您的客户设备的本地网关是 10.0.3.0/24。
- 您连接到 Outpost 本地网关的客户设备是 172.16.100.0/24。

因此，本地网关会将目标网络 172.16.100.0/24 的出站流量发送到您的客户设备。确保您的网络具有正确的路由配置，以便将流量传送到网络中的目标主机。

有关检查 BGP 会话状态以及这些会话中通告的路由所需的特定命令和配置，请参阅您的网络供应商提供的文档。有关故障排除，请参阅AWS Outposts 机架网络故障排除清单。

示例：CoIP 模式下的 BGP 通告

假设你有一个 Outpost，里面有两个 Outposts 机架网络设备，通过本地网关 VLAN 连接到两台客户的本地网络设备。配置了以下内容：

- VPC：CIDR 块为 10.0.0.0/16。
- VPC 中带有 CIDR 块的 10.0.3.0/24 的子网。
- 客户拥有的 IP 池 (10.1.0.0/26)。

- 一种将 10.0.3.112 关联到 10.1.0.2 的弹性 IP 地址关联。
- 本地网络中带有 CIDR 块的子网 172.16.100.0/24
- 您的 Outpost 和本地网络之间的通信将使用 CoIP 弹性 IP 来寻址 Outpost 中的实例，但不会使用 VPC CIDR 范围。

在这种情况下，通过以下方式通告的路由：

- 您的客户设备的本地网关是 10.1.0.0/26。
- 您连接到 Outpost 本地网关的客户设备是 172.16.100.0/24。

因此，本地网关会将目标网络 172.16.100.0/24 的出站流量发送到您的客户设备。确保您的网络具有正确的路由配置，以便将流量传送到网络中的目标主机。

有关检查 BGP 会话状态以及这些会话中通告的路由所需的特定命令和配置，请参阅您的网络供应商提供的文档。有关故障排除，请参阅AWS Outposts 机架网络故障排除清单。

第 5 步：在前哨基地启动实例

您可以在您创建的 Outpost 子网中启动 EC2 实例，也可以在与您共享的 Outpost 子网中启动。安全组控制 Outpost 子网中实例的入站和出站 VPC 流量，就像控制可用区子网中的实例一样。要连接到 Outpost 子网中的 EC2 实例，您可以在启动实例时指定密钥对，就像对待可用区子网中的实例一样。

注意事项

- 您可以创建置放群组来影响 Amazon EC2 应如何尝试在 Outposts 硬件上放置相互依赖的实例群组。您可以选择满足工作负载需求的置放群组策略。
- 如果您的 Outpost 已配置为使用客户拥有的 IP (CoIP) 地址池，那么您必须为自己启动的任何实例分配客户拥有的 IP 地址。

要在 Outpost 子网内启动实例

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 在导航窗格中，选择 Outposts。
3. 选择 Outpost，然后选择操作，查看详细信息。
4. 在 Outpost 摘要页面上，选择启动实例。您将会被重定向到 Amazon EC2 控制台中的实例启动向导。我们为您选择 Outpost 子网，并仅向您显示您的 Outposts 机架支持的实例类型。

5. 选择您的 Outposts 机架支持的实例类型。请注意，显示为灰色的实例不适用于你的前哨基地。
6. （可选）要将实例启动到置放群组，请展开高级详细信息并滚动至置放群组。您可以选择现有置放群组或创建新的置放群组。
7. 完成向导，以在您的 Outpost 子网中启动实例。有关更多信息，请参阅 Amazon EC2 用户指南中的以下内容：

   - Linux-使用新的启动实例向导启动实例
   - Windows — 使用新的启动实例向导启动实例

> **Note**
>
> 如果您要创建 Amazon EBS 卷，则必须使用 gp2 卷类型，否则向导将失败。

步骤 6：测试连通性

您可以使用适当的使用案例来测试连接。

测试从本地网络到 Outpost 的连接

在本地网络中的计算机上，向 Outpost 实例的私有 IP 地址运行`ping`命令。

```
ping 10.0.3.128
```

下面是示例输出。

```
Pinging 10.0.3.128

Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128
Reply from 10.0.3.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.3.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

测试从 Outpost 实例到本地网络的连接

根据您的操作系统，使用 ssh 或 rdp 连接到您的 Outpost 实例的私有 IP 地址。有关连接到 Linux 实例的信息，请参阅 Amazon EC2 用户指南中的连接到您的 Linux 实例。有关连接到 Windows 实例的信息，请参阅亚马逊 EC2 用户指南中的连接到您的 Windows 实例。

实例运行后，对本地网络中计算机的 IP 地址运行 ping 命令。在以下示例中，IP 地址为 172.16.0.130。

```
ping 172.16.0.130
```

下面是示例输出。

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

测试该 AWS 地区与前哨基地之间的连通性

AWS 在该区域的子网中启动实例。例如，使用 run-instances 命令。

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

在实例运行后，请执行以下操作：

1. 获取该 AWS 区域中实例的私有 IP 地址。Amazon EC2 控制台中的实例详细信息页面上提供了此信息。
2. 根据您的操作系统，使用 ssh 或 rdp 连接到您的 Outpost 实例的私有 IP 地址。
3. 从 Outpost 实例运行ping命令，指定该 AWS 区域中该实例的 IP 地址。

```
ping 10.0.1.5
```

下面是示例输出。

```
Pinging 10.0.1.5

Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.1.5:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.1.5
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

客户拥有的 IP 地址连接示例

测试从本地网络到 Outpost 的连接

在本地网络中的计算机上，向 Outpost 实例的客户拥有的 IP 地址运行 ping 命令。

```
ping 172.16.0.128
```

下面是示例输出。

```
Pinging 172.16.0.128

Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.128:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.128
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

测试从 Outpost 实例到本地网络的连接

根据您的操作系统，使用 ssh 或 rdp 连接到您的 Outpost 实例的私有 IP 地址。有关连接到 Linux 实例的信息，请参阅 Amazon EC2 用户指南中的连接到您的 Linux 实例。有关连接到 Windows 实例的信息，请参阅亚马逊 EC2 用户指南中的连接到您的 Windows 实例。

Outpost 实例运行后，对本地网络中计算机的 IP 地址运行 ping 命令。

```
ping 172.16.0.130
```

下面是示例输出。

```
Pinging 172.16.0.130

Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128
Reply from 172.16.0.130:  bytes=32 time=<1ms TTL=128

Ping statistics for 172.16.0.130
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

测试该 AWS 地区与前哨基地之间的连通性

AWS 在该区域的子网中启动实例。例如，使用 run-instances 命令。

```
aws ec2 run-instances \
    --image-id ami-abcdefghi1234567898 \
    --instance-type c5.large \
    --key-name MyKeyPair \
    --security-group-ids sg-1a2b3c4d123456787 \
    --subnet-id subnet-6e7f829e123445678
```

在实例运行后，请执行以下操作：

1. 获取 AWS 区域实例的私有 IP 地址，例如 10.0.0.5。Amazon EC2 控制台中的实例详细信息页面上提供了此信息。
2. 根据您的操作系统，使用 ssh 或 rdp 连接到您的 Outpost 实例的私有 IP 地址。
3. 将ping命令从您的 Outpost 实例运行到 AWS 区域实例 IP 地址。

```
ping 10.0.0.5
```

下面是示例输出。

```
Pinging 10.0.0.5

Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128
Reply from 10.0.0.5:  bytes=32 time=<1ms TTL=128

Ping statistics for 10.0.0.5
Packets:  Sent = 3,  Received = 3,  Lost = 0 (0% lost)

Approximate round trip time in milliseconds
Minimum = 0ms,  Maximum = 0ms,  Average = 0ms
```

AWS Outposts 与 AWS 区域的连接

AWS Outposts 支持通过服务链路连接进行广域网 (WAN) 连接。

内容

通过服务链路进行连接

服务链接是您的Outposts和您选择 AWS 的地区（或家乡）之间的必要连接，它允许管理Outposts以及交换进出该地区的流量。 AWS 服务链路利用一组加密的 VPN 连接与本地区域进行通信。

要设置服务链路连接，您或 AWS 必须在 Outpost 配置期间配置服务链路物理、虚拟 LAN (VLAN) 和网络层与本地网络设备的连接。有关更多信息，请参阅机架的本地网络连接和 Outposts 机架的站点要求。

对于与区域的广域网 (WAN) 连接， AWS Outposts 可以通过该 AWS 地区的公共连接建立服务链路 VPN 连接。 AWS 这要求Outposts能够通过公共互联网或 AWS Direct Connect 公共虚拟接口访问该地区的公共IP范围。有关当前 IP 地址范围，请参阅 A mazon VPC 用户指南中的 AWS IP 地址范围。可以通过在服务链路网络层路径中配置特定或默认 (0.0.0.0/0) 路由来启用此连接。有关更多信息，请参阅服务链路 BGP 连接和服务链路基础架构子网通告和 IP 范围。

或者，您可以为 Outpost 选择私有连接选项。有关更多信息，请参阅使用 VPC 的服务链接私有连接。

建立服务链接连接后，您的 Outpost 将开始运行并由 AWS管理。服务链路用于以下流量：

- 前哨基地与任何关联的 VPC 之间的客户 VPC 流量。
- Outposts 管理流量，例如资源管理、资源监控以及固件和软件更新。

服务链路最大传输单元 (MTU) 要求

网络连接的最大传输单位 (MTU) 是能够通过该连接传递的最大可允许数据包的大小（以字节为单位）。网络必须支持 Outpost 和父区域中的服务链接端点之间的 1500 字节的 MTU。 AWS 有关通过

服务链接在前哨基地中的实例与该 AWS 地区实例之间所需的 MTU 的信息，请参阅 Amazon EC2 用户指南中的 Amazon EC2 实例的网络最大传输单位 (MTU)。

服务链路带宽建议

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）的冗余连接来连接与该地区的服务链路。 AWS 您可以使用 AWS Direct Connect 或互联网连接获取服务链接。至少 500 Mbps 的服务链接连接允许您启动亚马逊 EC2 实例、连接亚马逊 EBS 卷以及访问 AWS 服务，例如亚马逊 EKS、Amazon EMR 和指标。 CloudWatch

您的 Outpost 服务相关带宽要求视以下特征而异：

- 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、突增速度需求以及到区域的 Amazon VPC 流量

要获得有关您的需求所需的服务链路带宽的定制建议，请联系您的 AWS 销售代表或 APN 合作伙伴。

防火墙和服务链路

本部分讨论防火墙配置和服务链路。

在下图中，该配置将 Amazon VPC 从该 AWS 区域扩展到前哨基地。 AWS Direct Connect 公共虚拟接口是服务链路连接。以下流量通过服务链路和 AWS Direct Connect 连接传送：

- 通过服务链路管理到 Outpost 的流量
- Outpost 和任何关联的 VPC 之间的流量

如果您在互联网连接中使用状态防火墙来限制从公共互联网到服务链路 VLAN 的连接，则可以阻止所有从互联网发起的入站连接。这是因为服务链路 VPN 仅从 Outpost 发起到该区域，而不是从该区域发起到 Outpost。

如果您使用防火墙限制来自服务链路 VLAN 的连接，则可以阻止所有入站连接。根据下表，您必须允许从该 AWS 地区返回前哨基地的出站连接。如果为状态防火墙，则应允许来自 Outpost 的出站连接（即这些连接是从 Outpost 发起的）返回入站。

协议	源端口	源地址	目的地端口	目标地址
UDP	443	AWS Outposts 服务链接 /26	443	AWS Outposts 该地区的公共路线
TCP	1025-65535	AWS Outposts 服务链接 /26	443	AWS Outposts 该地区的公共路线

> **Note**
>
> Outpost 中的实例不能使用服务链路与其他 Outpost 中的实例进行通信。利用通过本地网关或本地网络接口的路由在 Outpost 之间进行通信。
> AWS Outposts 机架还设计有冗余电源和网络设备，包括本地网关组件。有关更多信息，请参阅中的弹性 AWS Outposts。

使用 VPC 的服务链路私有连接

创建 Outpost 时，您可以在控制台中选择私有连接选项。执行此操作时，将在安装 Outpost 后使用您指定的 VPC 和子网建立服务链路 VPN 连接。这允许通过 VPC 进行私有连接，并最大限度地减少公共互联网暴露。

先决条件

在为 Outpost 配置私有连接之前，需要满足以下先决条件：

- 您必须为 IAM 实体（用户或角色）配置权限，以允许用户或角色创建服务链路的角色，以实现私有连接。IAM 实体需要权限才能访问以下操作：
  - `iam:CreateServiceLinkedRole`，发布时间：`arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `iam:PutRolePolicy`，发布时间：`arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*`
  - `ec2:DescribeVpcs`
  - `ec2:DescribeSubnets`

有关更多信息，请参阅 的身份和访问管理 (IAM) AWS Outposts 和 将服务相关角色用于 AWS Outposts。

- 在与您的 Outpost 相同的 AWS 账户和可用区中，创建一个专为 Outpost 私有连接而使用子网 /25 或更大且与 10.1.0.0/16 不冲突的 VPC。例如，您可以使用 10.2.0.0/16。
- 创建 AWS Direct Connect 连接、私有虚拟接口和虚拟专用网关，以允许您的本地 Outpost 访问 VPC。如果 AWS Direct Connect 连接位于与您的 VPC 不同的 AWS 账户中，请参阅AWS Direct Connect 用户指南中的跨账户关联虚拟私有网关。
- 向您的本地网络通告子网 CIDR。你可以用它 AWS Direct Connect 来做到这一点。有关更多信息，请参阅 AWS Direct Connect 用户指南中的AWS Direct Connect 虚拟接口和使用 AWS Direct Connect 网关。

在 AWS Outposts 控制台中创建 Outpost 时，您可以选择私有连接选项。有关说明，请参阅创建一个 Outpost 并订购 Outpost 容量。

> **Note**
>
> 要在 Outpost 处于待定状态时选择私有连接选项，请从控制台中选择 Outpost，然后选择您的 Outpost。选择操作和添加私有连接，然后按步骤操作。

为 Outpost 选择私有连接选项后，会在您的账户中 AWS Outposts 自动创建一个服务相关角色，使其能够代表您完成以下任务：

- 在您指定的子网和 VPC 中创建网络接口，并为网络接口创建安全组。
- 向 AWS Outposts 服务授予权限，以将网络接口连接到账户中的服务链接端点实例。
- 将网络接口附加到账户中的服务链路端点实例。

有关服务相关角色的更多信息，请参阅 将服务相关角色用于 AWS Outposts。

> **Important**
>
> 安装 Outpost 后，确认从 Outpost 连接到子网中的私有 IP。

冗余互联网连接

当您建立从 Outpost 到该 AWS 地区的连接时，我们建议您创建多个连接，以提高可用性和弹性。有关更多信息，请参阅 AWS Direct Connect 弹性建议。

如果您需要连接到公共互联网，则可以使用冗余互联网连接和各种互联网提供商，就像使用现有的本地工作负载一样。

Outpost 和站点

管理 Outposts 和网站. AWS Outposts

您可以对 Outpost 和站点进行标记，以帮助您识别资源或根据组织的需求进行分类。有关标记的更多信息，请参阅指南中的为AWS 资源添加标签。AWS 一般参考

主题

- 管理 Outpost
- 管理 Outpost 站点

管理 Outpost

AWS Outposts 包括名为 Outposts 的硬件和虚拟资源。此部分可用于创建和管理 Outpost，包括更改名称以及添加或查看详细信息或标签。

创建 Outpost

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Outposts。
4. 选择创建 Outpost。
5. 为这个 Outpost 选择一种硬件类型。
6. 为您的 Outpost 输入名称和描述。
7. 为您的 Outpost 选择可用区。
8. （可选）选择私有连接选项。对于 VPC 和子网，选择与您的 Outpost 处于同一 AWS 账户和可用区的 VPC 和子网。

   > **Note**
   >
   > 如果您需要撤消 Outpost 的私有连接，则必须联系 AWS 企业支持。

9. 对于站点 ID，执行下列操作之一：

   - 要选择现有站点，请选择这个站点。
   - 要创建新站点，请选择创建站点，单击下一步，然后在新窗口中输入您的站点的信息。

创建站点后，返回此窗口以选择站点。您可能需要刷新站点列表，才能看到新站点。要刷新数据，请选择刷新图标
()。

有关更多信息，请参阅 the section called “站点”。

10. 选择创建 Outpost。

> **Tip**
>
> 要为新的 Outpost 添加容量，您必须下单订购。

使用以下步骤，编辑 Outpost 的名称和描述。

编辑 Outpost 的名称和描述

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Outposts。
4. 选择 Outpost，然后依次选择操作和编辑 Outpost。
5. 修改名称和描述。

   对于名称，输入名称。

   对于说明，输入说明。
6. 选择 保存更改。

按照下面的步骤操作，以查看 Outpost 的详细信息。

查看 Outpost 详细信息

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Outposts。
4. 选择 Outpost，然后选择操作，查看详细信息。

您也可以使用 AWS CLI 来查看 Outpost 的详细信息。

要查看 Outpost 的详细信息，请使用 AWS CLI

- 使用 get-outpost 命令 AWS CLI 。

按照以下步骤管理 Outpost 上的标签。

管理 Outpost 标签

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择 Outposts。
4. 选择 Outpost，然后依次选择操作、管理标签。
5. 添加或删除标签。

   要添加标签，请选择添加新标签，然后执行以下操作：

   - 对于 Key（键），输入键名称。
   - 对于值，输入键值。

   要删除标签，请选择标签的“键”和“值”右侧的删除。
6. 选择 保存更改。

管理 Outpost 站点

客户管理的实体建筑 AWS 将安装你的前哨基地。站点必须满足 Outpost 的设施、网络和电力要求。有关更多信息，请参阅 Outposts 机架的要求。

创建 Outpost 站点

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择站点。
4. 选择 Create site (创建站点)。
5. 为该站点选择受支持的硬件类型。

6. 输入您的站点的名称、描述和运营地址。如果您选择在站点支持机架，请输入以下信息：
   - 最大重量 — 指定此站点可以承受的最大机架重量。
   - 功耗 — 指定机架硬件放置位置的可用功耗，以 kVA 为单位。
   - 电源选项 — 指定您可以为硬件提供的电源选项。
   - 电源连接器-指定计划 AWS 用于连接硬件的电源连接器。
   - 电源馈电点 — 指定电源馈电是位于机架上方还是下方。
   - 上行链路速度 — 指定机架在连接到所属区域时应支持的上行链路速度。
   - 上行链路数量 — 指定您打算用于将机架连接到网络的每台 Outpost 网络设备的上行链路数量。
   - 光纤类型 — 指定用于将 Outpost 连接到您的网络的光纤类型。
   - 光纤标准 — 指定用于将 Outpost 连接到网络的光纤标准类型。
   - 备注 — 指定有关网站的备注。
7. 阅读设施要求，然后选择我已阅读设施要求。
8. 选择 Create site (创建站点)。

按照以下步骤编辑 Outpost 站点。

编辑站点

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择站点。
4. 选择站点，然后选择操作和编辑站点。
5. 您可以修改名称、描述、运营地址和站点详细信息。

   如果您更改运营地址，请注意这些更改不会传播到现有订单。
6. 选择 保存更改。

按照以下步骤查看 Outpost 站点的详细信息。

要查看站点详细信息

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。

3. 在导航窗格中，选择站点。
4. 选择站点，然后依次选择操作、查看详细信息。

按照以下步骤管理 Outpost 站点上的标签。

管理站点标签

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择站点。
4. 选择站点，然后依次选择操作、管理标签。
5. 添加或删除标签。

   要添加标签，请选择添加新标签，然后执行以下操作：

   - 对于 Key（键），输入键名称。
   - 对于值，输入键值。

   要删除标签，请选择标签的“键”和“值”右侧的删除。
6. 选择保存更改。

本地网关

本地网关是 Outpost 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。如果本地基础设施提供互联网接入，则在Outpost 上运行的工作负载也可以利用本地网关与区域服务或区域工作负载进行通信。这种连接可以通过使用公共连接（互联网）或使用 Direct Connect 来实现。有关更多信息，请参阅 AWS Outposts 与 AWS 区域的连接。

内容

本地网关基础知识

每个 Outpost 都支持一个本地网关。本地网关包含下列组件：

- 路由表 — 用于创建本地网关路由表。有关更多信息，请参阅 the section called “本地网关路由表”。
- CoIP 池 —（可选）您可以使用自己的 IP 地址范围来促进本地网络与 VPC 中的实例之间的通信。有关更多信息，请参阅 the section called “客户拥有的 IP 地址”。
- 虚拟接口 (VIF)-为每个 LAG AWS 创建一个 VIF 并将两个 VIF 添加到 VIF 组中。本地网关路由表必须具有指向两个 VIF 的默认路由，才能实现本地网络连接。有关更多信息，请参阅 本地网络连接。
- VIF 群组关联 — 将其创建的 VIF AWS 添加到 VIF 群组。VIF 群组是 VIF 的逻辑分组。有关更多信息，请参阅 the section called “VIF 组关联”。
- VPC 关联 — 用于创建与您的 VPC 和本地网关路由表的 VPC 关联。与驻留在 Outpost 上的子网关联的 VPC 路由表可以使用本地网关作为路由目标。有关更多信息，请参阅 the section called “VPC 关联”。

在配置 AWS 您的 Outpost 机架时，我们会创建一些组件，而您则负责创建其他组件。

AWS 责任

- 交付硬件。
- 创建本地网关。

- 创建虚拟接口 (VIF) 和 VIF 组。

您的责任

- 创建本地网关路由表。
- 将 VPC 与本地网关路由表相关联。
- 将 VIF 组与本地网关路由表相关联。

路由

您的 Outpost 子网中的实例可以使用以下选项之一，以通过本地网关与您的本地网络进行通信：

- 私有 IP 地址 — 本地网关使用 Outpost 子网中实例的私有 IP 地址来促进与本地网络的通信。这是默认模式。
- 客户拥有的 IP 地址 — 本地网关对您分配给 Outpost 子网中实例的客户拥有的 IP 地址执行网络地址转换（NAT）。此选项支持重叠的 CIDR 范围和其他网络拓扑。

有关更多信息，请参阅 the section called “本地网关路由表”。

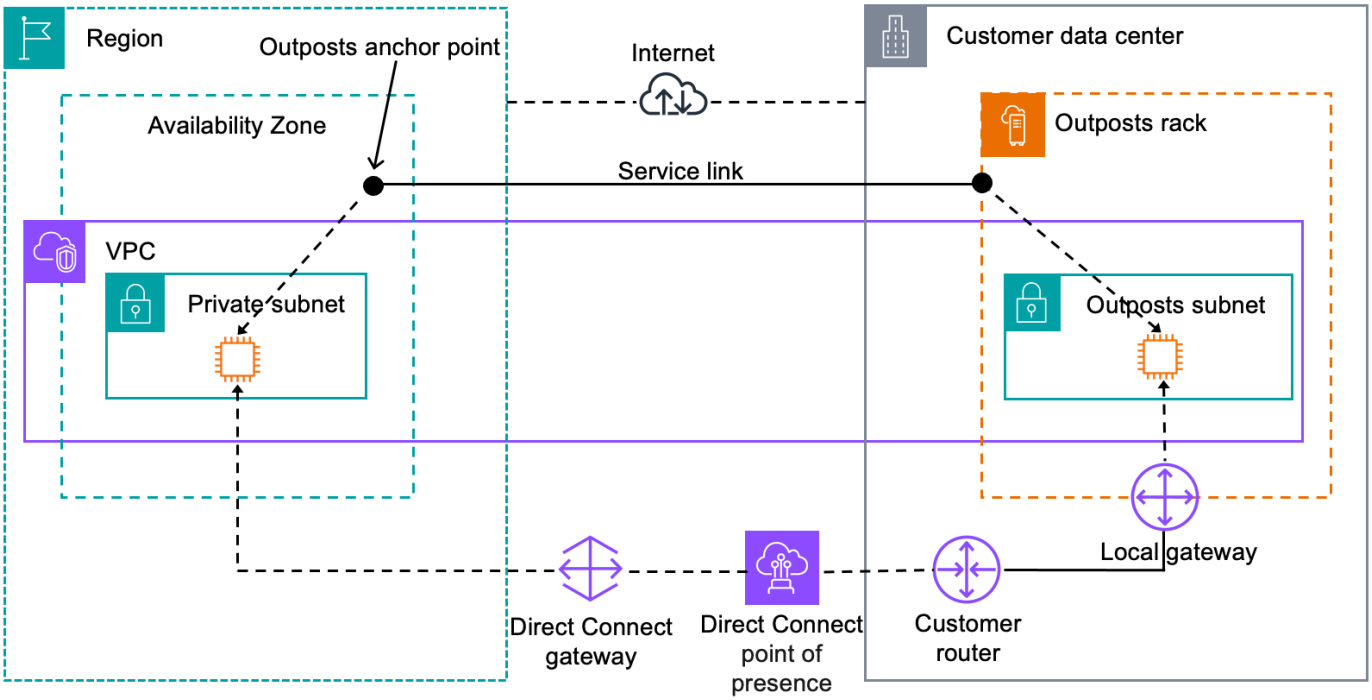
通过本地网关进行连接

本地网关的主要作用是提供从 Outpost 到本地网络的连接。它还通过您的本地网络提供与 Internet 的连接。有关示例，请参阅 the section called “直接 VPC 路由” 和 the section called “客户拥有的 IP 地址”。

本地网关还可以提供返回该 AWS 区域的数据平面路径。本地网关的数据面板路径从 Outpost 穿过本地网关，到达您的私有本地网关 LAN 段。然后沿着私有路径返回该区域的 AWS 服务端点。请注意，无论您使用何种数据面板路径，控制面板路径始终使用服务链路连接。

您可以通过私密方式将本地 Outposts 基础设施连接到该区域 AWS 服务 内。 AWS Direct Connect有关更多信息，请参阅AWS Outposts 私有连接。

下图显示了通过本地网关的连接：



本地网关路由表

机架上的 Outpost 子网路由表可以包括通往本地网络的路由。本地网关将此流量路由到本地网络，以实现低延迟路由。

默认情况下，Outpost 使用 Outpost 上实例的私有 IP 地址与您的本地网络进行通信。这称为 AWS Outposts直接 VPC 路由（或直接 VPC 路由）。但是，您可以提供一个地址范围，即客户拥有的 IP 地址池 (CoIP)，并让网络上的实例使用这些地址与您的本地网络通信。直接 VPC 路由和 CoIP 是互斥的选项，根据您的选择，路由的工作方式会有所不同。

内容

直接 VPC 路由

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 BGP 通告到本地网络。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。这种路由类型

是 Outpost 的默认模式。在此模式下，本地网关不对实例执行 NAT，您也无需为您的 EC2 实例分配弹性 IP 地址。您可以选择使用自己的地址空间而非直接 VPC 路由模式。有关更多信息，请参阅 客户拥有的 IP 地址。

仅实例网络接口支持直接 VPC 路由。对于代表您 AWS 创建的网络接口（称为请求者管理的网络接口），您的本地网络无法访问其私有 IP 地址。例如，VPC 端点无法从您的本地网络直接访问。

以下示例演示了直接 VPC 路由。

示例

- 示例：通过 VPC 连接互联网
- 示例：通过本地网络连接互联网

示例：通过 VPC 连接互联网

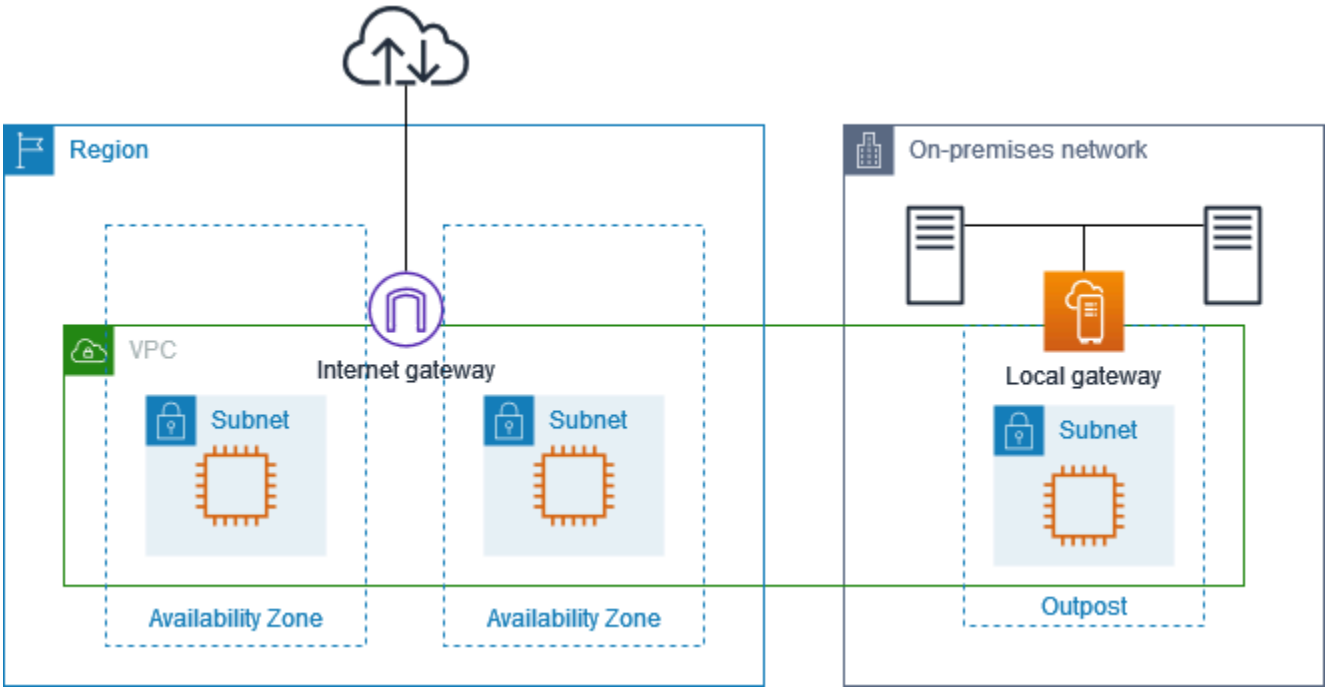
Outpost 子网中的实例可以通过连接到 VPC 的互联网网关访问互联网。

请考虑以下配置：

- 父 VPC 跨越两个可用区，且每个可用区都有一个子网。
- Outpost 有一个子网。
- 每个子网都有一个 EC2 实例。
- 本地网关使用 BGP 通告将 Outpost 子网的私有 IP 地址通告到本地网络。

> **Note**
>
> Outpost 上符合以下条件的子网才支持 BGP 通告：其路由是以逻辑网关作为目标。任何其他子网都不会通过 BGP 进行通告。

在下图中，来自 Outpost 子网中实例的流量可以使用 VPC 的互联网网关访问互联网。



要通过父区域实现互联网连接，Outpost 子网的路由表必须包含以下路由。

目标位置	目标	注释
VPC CIDR	本地	提供 VPC 中子网之间的连接。
0.0.0.0	*internet-gateway-id*	将发往互联网网关的流量发送到互联网网关。
#### CIDR	*local-gateway-id*	将发往本地网络的流量发送到本地网关。

示例：通过本地网络连接互联网

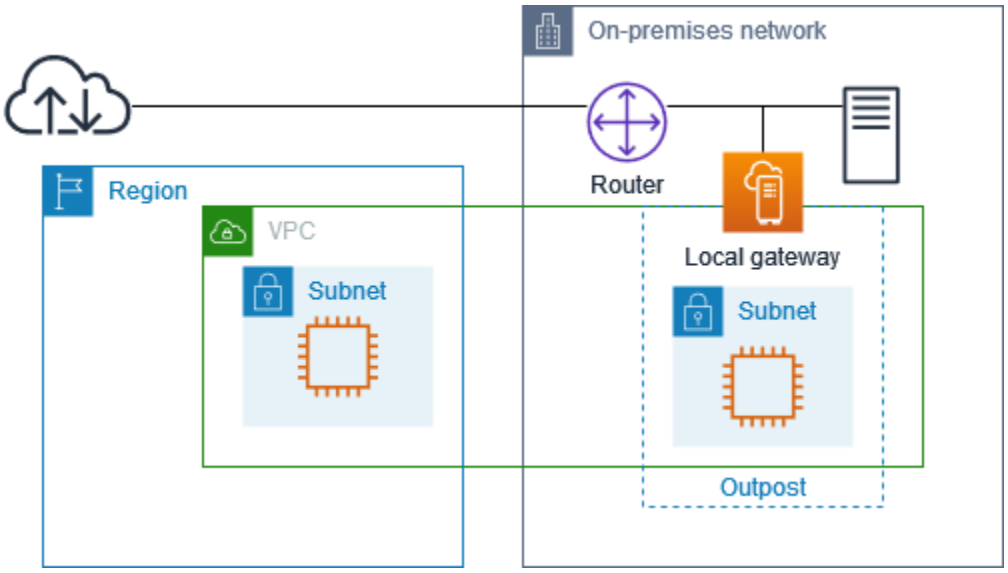
Outpost 子网中的实例可以通过本地网络访问互联网。Outpost 子网中的实例不需要公有 IP 地址或弹性 IP 地址。

请考虑以下配置：

- Outpost 子网有一个 EC2 实例。
- 本地网络中的路由器会执行网络地址转换（NAT）。
- 本地网关使用 BGP 通告将 Outpost 子网的私有 IP 地址通告到本地网络。

> **Note**
>
> Outpost 上符合以下条件的子网才支持 BGP 通告：其路由是以逻辑网关作为目标。任何其他子网都不会通过 BGP 进行通告。

在下图中，Outpost 子网中实例的流量可以使用本地网关访问互联网或本地网络。来自本地网络的流量使用本地网关访问 Outpost 子网中的实例。



要通过本地网络实现互联网连接，Outpost 子网的路由表必须包含以下路由。

目标位置	目标	注释
VPC CIDR	本地	提供 VPC 中子网之间的连接。
0.0.0.0/0	*local-gateway-id*	将发往互联网网关的流量发送到本地网关。

对互联网的出站访问

如果从 Outpost 子网中实例发起的流量以互联网为目的地，则使用 0.0.0.0/0 的路由将流量路由到本地网关。本地网关将流量发送到路由器。路由器使用 NAT 将私有 IP 地址转换为路由器上的公有 IP 地址，然后将流量发送至目的地。

对本地网络的出站访问

如果从 Outpost 子网中实例发起的流量以本地网络为目的地，则使用 0.0.0.0/0 的路由将流量路由到本地网关。本地网关将流量发送到本地网络中的目的地。

来自本地网络的入站访问

如果来自本地网络的流量以 Outpost 子网中的实例为目标，则会使用实例的私有 IP 地址。当流量到达本地网关时，本地网关会将流量发送到 VPC 中的目的地。

客户拥有的 IP 地址

默认情况下，本地网关使用 VPC 中实例的私有 IP 地址来促进与本地网络的通信。但是，您可以提供一个地址范围，即客户拥有的 IP 地址池 (CoIP)，它支持重叠的 CIDR 范围和其他网络拓扑。

如果您选择 CoIP，则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客户网络。与您的本地网关路由表关联的所有由客户拥有的 IP 地址在路由表中显示为传播路由。

客户拥有的 IP 地址为您的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，方法是从客户拥有的 IP 池中分配新的弹性 IP 地址，然后将其分配给您的资源。有关更多信息，请参阅 the section called “3f：（可选）为实例分配客户拥有的 IP 地址”。

以下要求适用于客户拥有的 IP 地址池：

- 您必须能够在您的网络中路由该地址
- CIDR 区块必须至少为 /26

当您从客户拥有的 IP 地址池中分配弹性 IP 地址时，您继续拥有客户拥有的 IP 地址池中的 IP 地址。您负责根据需要在内部网络或 WAN 上通告这些地址。

您可以选择使用 AWS Resource Access Manager与组织 AWS 账户 中的多个客户共享客户拥有的资源池。共享池后，参与者可以从客户拥有的 IP 地址池中分配弹性 IP 地址，然后将其分配给 Outpost 上的 EC2 实例。有关更多信息，请参阅《AWS RAM 用户指南》中的共享您的 AWS 资源。

示例

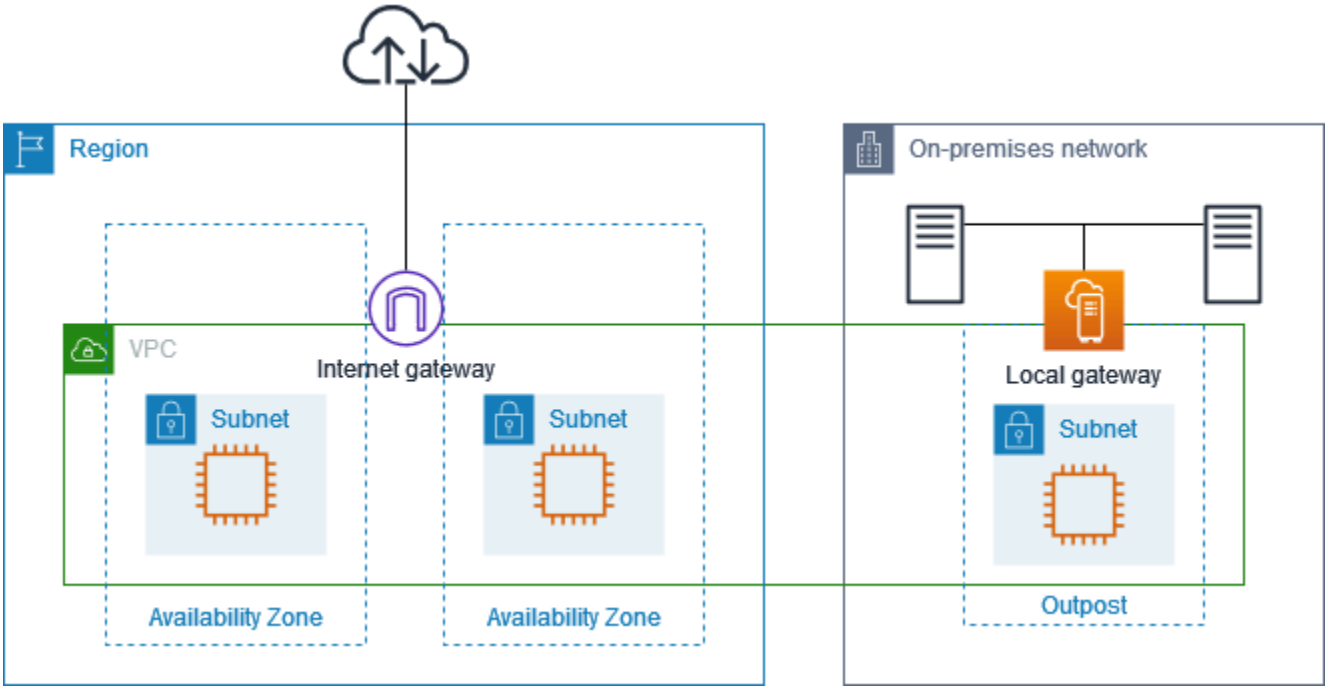
- 示例：通过 VPC 连接互联网
- 示例：通过本地网络连接互联网

示例：通过 VPC 连接互联网

Outpost 子网中的实例可以通过连接到 VPC 的互联网网关访问互联网。

请考虑以下配置：

- 父 VPC 跨越两个可用区，且每个可用区都有一个子网。
- Outpost 有一个子网。
- 每个子网都有一个 EC2 实例。
- 有一个客户拥有的 IP 地址池。
- Outpost 子网中的实例具有来自客户拥有的 IP 地址池的弹性 IP 地址。
- 本地网关使用 BGP 通告将客户拥有的 IP 地址池通告到本地网络。



要通过区域实现互联网连接，Outpost 子网的路由表必须包含以下路由。

目标位置	目标	注释
VPC CIDR	本地	提供 VPC 中子网之间的连接。
0.0.0.0	*internet-gateway-id*	将发往公共互联网的流量发送到互联网网关。

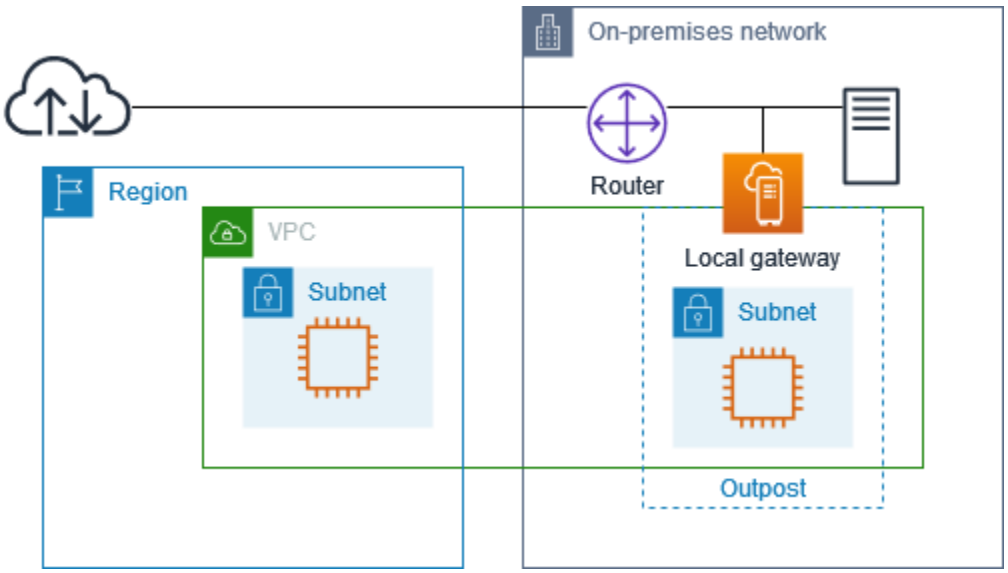
目标位置	目标	注释
#### CIDR	*local-gateway-id*	将发往本地网络的流量发送到本地网关。

示例：通过本地网络连接互联网

Outpost 子网中的实例可以通过本地网络访问互联网。

请考虑以下配置：

- Outpost 子网有一个 EC2 实例。
- 有一个客户拥有的 IP 地址池。
- 本地网关使用 BGP 通告将客户拥有的 IP 地址池通告到本地网络。
- 一种将 10.0.3.112 映射到 10.1.0.2 的弹性 IP 地址关联。
- 在客户本地网络中的路由器执行 NAT。



要通过本地网关实现互联网连接，Outpost 子网的路由表必须包含以下路由。

目标位置	目标	注释
VPC CIDR	本地	提供 VPC 中子网之间的连接。

目标位置	目标	注释
0.0.0.0/0	*local-gateway-id*	将发往互联网网关的流量发送到本地网关。

对互联网的出站访问

如果从 Outpost 子网中的 EC2 实例发起的流量以互联网为目的地，则使用 0.0.0.0/0 的路由将流量路由到本地网关。本地网关将实例的私有 IP 地址映射到客户拥有的 IP 地址，然后将流量发送到路由器。路由器使用 NAT 将客户拥有的 IP 地址转换为路由器上的公有 IP 地址，然后将流量发送到目的地。

对本地网络的出站访问

如果从 Outpost 子网中 EC2 实例发起的流量以本地网络为目的地，则使用 0.0.0.0/0 的路由将流量路由到本地网关。本地网关将 EC2 实例的 IP 地址转换为客户拥有的 IP 地址（弹性 IP 地址），然后将流量发送到目的地。

来自本地网络的入站访问

如果来自本地网络的流量以 Outpost 子网中的实例为目标，则会使用实例的客户拥有的 IP 地址（弹性 IP 地址）。当流量到达本地网关时，本地网关会将客户拥有的 IP 地址（弹性 IP 地址）映射到实例 IP 地址，然后将流量发送到 VPC 中的目的地。此外，本地网关路由表还会评估所有以弹性网络接口为目标的路由。如果目标地址与任何静态路由的目标 CIDR 匹配，则流量将发送到该弹性网络接口。当流量沿着静态路由到达弹性网络接口时，目的地地址会被保留，并且不会转换为网络接口的私有 IP 地址。

使用本地网关路由表

作为机架安装的一部分， AWS 创建本地网关、配置 VIF 和 VIF 组。您将创建本地网关路由表。本地网关路由表必须与 VIF 组和 VPC 建立关联。您可以创建和管理 VIF 组和 VPC 的关联。请考虑以下有关本地网关路由表的信息：

- VIF 组和本地网关路由表必须有关 one-to-one系。
- 本地网关归与 Outpost 关联的 AWS 账户所有，只有所有者才能修改本地网关路由表。
- 您可以使用与其他 AWS 账户或组织单位共享本地网关路由表 AWS Resource Access Manager。有关更多信息，请参阅使用共享的 AWS Outposts 资源。
- 本地网关路由表的模式决定在与本地网络通信时使用实例的私有 IP 地址（直接 VPC 路由）还是使用客户拥有的 IP 地址池 (CoIP)。直接 VPC 路由和 CoIP 是互斥的选项，根据您的选择，路由的工作方式会有所不同。有关更多信息，请参阅 ???。

- 直接 VPC 路由模式不支持重叠的 CIDR 范围。

任务

- 查看本地网关路由表详细信息
- 创建自定义本地网关路由表
- 管理本地网关路由表路由
- 管理本地网关路由表标签
- 切换本地网关路由表模式或删除本地网关路由表
- 管理 CoIP 池
- VIF 组关联
- VPC 关联

查看本地网关路由表详细信息

您可以使用控制台或 AWS CLI来查看本地网关路由表的详细信息。

AWS Outposts console

查看本地网关路由表详细信息

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择本地网关路由表，然后选择操作、查看详细信息。

AWS CLI

查看本地网关路由表详细信息

使用 describe-local-gat eway-route- AWS CLI tables 命令。

示例

```
aws ec2 describe-local-gateway-route-tables --region us-west-2
```

输出

```
{
    "LocalGatewayRouteTables": [
        {
            "LocalGatewayRouteTableId": "lgw-rtb-059615ef7deEXAMPLE",
            "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
            "OutpostArn": "arn:aws:outposts:us-west-2:111122223333:outpost/
op-0dc11b66edEXAMPLE",
            "State": "available",
            "Tags": []
        }
    ]
}
```

> **Note**
>
> 如果您正在查看的默认本地网关路由表使用 CoIP 模式，则本地网关路由表会配置指向每个 VIF 的默认路由，以及指向 CoIP 池中每个客户拥有的关联 IP 地址的传播路由。

创建自定义本地网关路由表

您可以使用 AWS Outposts 控制台为本地网关创建自定义路由表。

使用控制台创建自定义本地网关路由表

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择创建本地网关路由表。
5. （可选）对于名称，为您的本地网关路由表输入名称。
6. 对于本地网关，请选择您的本地网关。
7. （可选）选择关联 VIF 组，然后选择您的 VIF 组。
8. 对于模式，请选择与本地网络通信的模式。
   - 选择直接 VPC 路由以使用实例的私有 IP 地址。
   - 选择 CoIP 以使用客户拥有的 IP 地址。
     - （可选）添加或移除 CoIP 池和其他 CIDR 块

[添加 CoIP 池] 选择添加新标签，然后执行以下操作：

- 对于名称，请为您的 CoIP 池输入名称。
- 对于 CIDR，请输入由客户拥有的 IP 地址组成的 CIDR 块。

- [添加 CIDR 块] 选择添加新 CIDR，然后输入客户拥有的 IP 地址范围。
- [移除 CoIP 池或其他 CIDR 块] 选择 CIDR 块右侧或 CoIP 池下方的移除。

您最多可以指定 10 个 CoIP 池和 100 个 CIDR 块。

9. （可选）添加或删除标签。

[添加标签] 选择添加新标签，然后执行以下操作：

- 对于 Key（键），输入键名称。
- 对于值，输入键值。

[删除标签] 选择标签的“键”和“值”右侧的删除。

10. 选择创建本地网关路由表。

管理本地网关路由表路由

您可以在 Outpost 上创建通往弹性网络接口的本地网关路由表和入站路由。您也可以修改现有的本地网关入站路由，以更改目标弹性网络接口。

只有当路由的目标弹性网络接口连接到正在运行的实例时，路由才会处于活动状态。如果实例停止或接口已断开，则路由将从活动状态变为黑洞状态。

以下要求和限制适用于本地网关：

- 目标弹性网络接口必须属于您的 Outpost 上的子网，并且必须连接到该 Outpost 中的实例。本地网关路由不能以其他 Outpost 或父 AWS 区域中的 Amazon EC2 实例为目标。
- 子网必须属于与本地网关路由表关联的 VPC。
- 同一路由表中的弹性网络路由不得超过 100 条。
- AWS 优先考虑最具体的路由，如果路由匹配，我们将静态路由优先于传播路由。
- 不支持 接口 VPC 端点。
- BGP 通告仅适用于 Outpost 上符合以下条件的子网：路由表中的路由是以本地网关为目标。如果子网的路由表中没有以本地网关为目标的路由，则不会使用 BGP 通告这些子网。

- 只有连接到 Outpost 实例的 ENI 才能通过该 Outpost 的本地网关进行通信。属于 Outpost 子网但连接到区域中实例的 ENI 无法通过该 Outpost 的本地网关进行通信。
- 无法通过本地网关从本地网络访问托管接口，例如 VPCE 端点或接口。只能通过 Outpost 中的实例来访问托管接口。

以下 NAT 注意事项适用。

- 本地网关不对匹配弹性网络互联网路由的流量执行 NAT。目标 IP 地址会被保留。
- 关闭目标弹性网络接口的源/目标检查。有关更多信息，请参阅 Amazon EC2 用户指南中的网络接口基础知识。
- 将操作系统配置为允许网络接口接受来自目标 CIDR 的流量。

AWS Outposts console

编辑本地网关路由表路由

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择本地网关路由表，然后选择操作、编辑路由。
5. 要添加路由，请选择添加路由。对于目的地，请输入目的地 CIDR 块、单个 IP 地址或前缀列表的 ID。
6. 要修改现有路由，对于目的地，请替换目的地 CIDR 块或单个 IP 地址。对于目标，请选择一个目标。
7. 选择 Save routes (保存路由)。

AWS CLI

创建本地网关路由表路由

- 使用 create-local-gateway-route AWS CLI 命令。

示例

```
aws ec2 create-local-gateway-route \
```

```
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-03e612f0a1EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

输出

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-03e612f0a1EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

修改本地网关路由表路由

您可以修改现有路由所针对的弹性网络接口。要使用修改操作，路由表必须已经包含具有指定目标 CIDR 块的路由。

- 使用 m odify-local-gateway-route 命令 AWS CLI 。

示例

```
aws ec2 modify-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-12a345b6c7EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

输出

```
{
    "Route": {
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-12a345b6c7EXAMPLE",
        "Type": "static",
        "State": "active",
```

```
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

管理本地网关路由表标签

您可以对本地网关路由表进行标记，以帮助您识别它或根据组织的需要对其进行分类。

管理本地网关路由表标签

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择本地网关路由表，然后选择操作、管理标签。
5. 添加或删除标签。

   要添加标签，请选择添加新标签，然后执行以下操作：

   - 对于 Key（键），输入键名称。
   - 对于值，输入键值。

   要删除标签，请选择标签的“键”和“值”右侧的删除。
6. 选择保存更改。

切换本地网关路由表模式或删除本地网关路由表

您必须删除并重新创建本地网关路由表才能切换模式。删除本地网关路由表会导致网络流量中断。

要切换模式或删除本地网关路由表

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 请验证您的输入是否正确 AWS 区域。

   要更改区域，请使用页面右上角的区域选择器。

3. 在导航窗格中，选择本地网关路由表。
4. 验证本地网关路由表是否与 VIF 组关联。如果已关联，则必须删除本地网关路由表和 VIF 组之间的关联。
   a. 选择本地网关路由表的 ID。
   b. 选择 VIF 组关联选项卡。
   c. 如果一个或多个 VIF 组与本地网关路由表关联，请选择编辑 VIF 组关联。
   d. 清除 “关联 VIF 组” 复选框。
   e. 选择保存更改。
5. 选择删除本地网关路由表。
6. 在确认对话框中，键入 **delete**，然后选择删除。
7. （可选）使用新模式创建本地网关路由表。
   a. 在导航窗格中，选择本地网关路由表。
   b. 选择创建本地网关路由表。
   c. 使用新模式配置本地网关路由表。有关更多信息，请参阅创建自定义本地网关路由表。

管理 CoIP 池

您可以提供 IP 地址范围，以促进本地网络与 VPC 中的实例之间的通信。有关更多信息，请参阅客户拥有的 IP 地址。

客户拥有的 IP 池可用于 CoIP 模式下的本地网关路由表。要在本地网关路由表模式之间切换，请参阅切换本地网关路由表模式。

要创建 CoIP 池，请按照以下过程操作。

创建 CoIP 池

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择路由表。
5. 在详细信息窗格中选择 CoIP 池选项卡，然后选择创建 CoIP 池。
6. （可选）对于名称，请为您的 CoIP 池输入名称。

7. 选择添加新 CIDR，然后输入客户拥有的 IP 地址范围。
8. （可选）添加或删除 CIDR 块

   [添加 CIDR 块] 选择添加新 CIDR，然后输入客户拥有的 IP 地址范围。

   [移除 CIDR 块] 选择 CIDR 块右侧的移除。
9. 选择创建 CoIP 池。

可以按照以下步骤编辑 CoIP 池。

编辑 CoIP 池

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择路由表。
5. 在详细信息窗格中选择 CoIP 池选项卡，然后选择 CoIP 池。
6. 依次选择操作、编辑 CoIP 池。
7. 选择添加新 CIDR，然后输入客户拥有的 IP 地址范围。
8. （可选）添加或删除 CIDR 块

   [添加 CIDR 块] 选择添加新 CIDR，然后输入客户拥有的 IP 地址范围。

   [移除 CIDR 块] 选择 CIDR 块右侧的移除。
9. 选择保存更改。

使用以下步骤以管理标签或向 CoIP 池添加名称标签。

管理 CoIP 池上的标签

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择路由表。
5. 在详细信息窗格中选择 CoIP 池选项卡，然后选择 CoIP 池。

6. 选择操作、管理标签。
7. 添加或删除标签。

   要添加标签，请选择添加新标签，然后执行以下操作：

   - 对于 Key（键），输入键名称。
   - 对于值，输入键值。

   要删除标签，请选择标签的“键”和“值”右侧的删除。
8. 选择保存更改。

要删除 CoIP 池，请按照以下过程操作。

删除 CoIP 池

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择路由表。
5. 在详细信息窗格中选择 CoIP 池选项卡，然后选择 CoIP 池。
6. 选择操作、删除 CoIP 池。
7. 在确认对话框中，键入 **delete**，然后选择删除。

VIF 组关联

VIF 群组是虚拟接口 (VIF) 的逻辑分组。您可以更改与 VIF 群组关联的本地网关路由表。解除 VIF 群组与本地网关路由表的关联后，将从路由表中删除所有路由并中断网络流量。

更改 VIF 群组的关联

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择路由表。
5. 在详细信息窗格中选择 VIF 群组关联选项卡，然后选择编辑 VIF 群组关联。

6. 对于 VIF 组设置，执行以下操作之一：

   - 要将 VIF 群组与本地网关路由表关联，请选择关联 VIF 群组，然后选择一个 VIF 群组。
   - 要解除 VIF 群组与本地网关路由表的关联，请清除关联 VIF 群组。

   > **Important**
   > 解除 VIF 组与本地网关路由表的关联会自动删除所有路由并中断网络流量。

7. 选择保存更改。

VPC 关联

您必须将 VPC 与本地网关路由表关联。默认情况下，它们不会关联。

创建 VPC 关联

遵循以下过程将 VPC 与本地网关路由表相关联。

您可以选择性地标记您的关联，以帮助您识别它或根据组织的需要对其进行分类。

AWS Outposts console

关联 VPC

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择路由表，然后依次选择操作、关联 VPC。
5. 在 VPC ID 中，选择要与本地网关路由表关联的 VPC。
6. （可选）添加或删除标签。

   要添加标签，请选择添加新标签，然后执行以下操作：

   - 对于 Key（键），输入键名称。
   - 对于值，输入键值。

   要删除标签，请选择标签的“键”和“值”右侧的删除。

7. 选择 Associate VPC (关联 VPC)。

AWS CLI

关联 VPC

使用 create-local-gateway-route-table-vpc-association 命令。

示例

```
aws ec2 create-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

输出

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

删除 VPC 关联

遵循以下过程取消 VPC 与本地网关路由表的关联。

AWS Outposts console

解除 VPC 关联

1. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择本地网关路由表。
4. 选择路由表，然后选择操作、查看详细信息。
5. 在 VPC 关联中，选择要取消关联的 VPC，然后选择取消关联。

6. 选择取消关联。

AWS CLI

解除 VPC 关联

使用 delete-local-gateway-route-table-vpc-association 命令。

示例

```
aws ec2 delete-local-gateway-route-table-vpc-association \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --vpc-id vpc-07ef66ac71EXAMPLE
```

输出

```
{
    "LocalGatewayRouteTableVpcAssociation": {
        "LocalGatewayRouteTableVpcAssociationId": "lgw-vpc-assoc-0ee765bcc8EXAMPLE",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayId": "lgw-09b493aa7cEXAMPLE",
        "VpcId": "vpc-07ef66ac71EXAMPLE",
        "State": "associated"
    }
}
```

机架的本地网络连接

您需要以下组件才能将 Outpost 机架连接到本地网络：

- 从 Outpost 配线架到客户的本地网络设备的物理连接。
- 链路聚合控制协议 (LACP)，用于与 Outpost 网络设备和本地网络设备建立两个链路聚合组 (LAG) 连接。
- Outpost 和您的客户本地网络设备之间的虚拟局域网 (VLAN) 连接。
- 每个 VLAN 的第 3 层 point-to-point 连接。
- 边界网关协议 (BGP)，用于在 Outpost 和您的本地服务链路之间进行路由通告。
- BGP 用于在 Outpost 和您的本地网络设备之间进行路由公告，用于连接到本地网关。

内容

物理连接

一台 Outpost 机架具有两个物理网络设备，连接到您的本地网络上。

Outpost 要求这些 Outpost 网络设备和您的本地网络设备之间至少有两条物理链路。对于每台 Outpost 网络设备，Outpost 支持下列上行链路速度和数量。

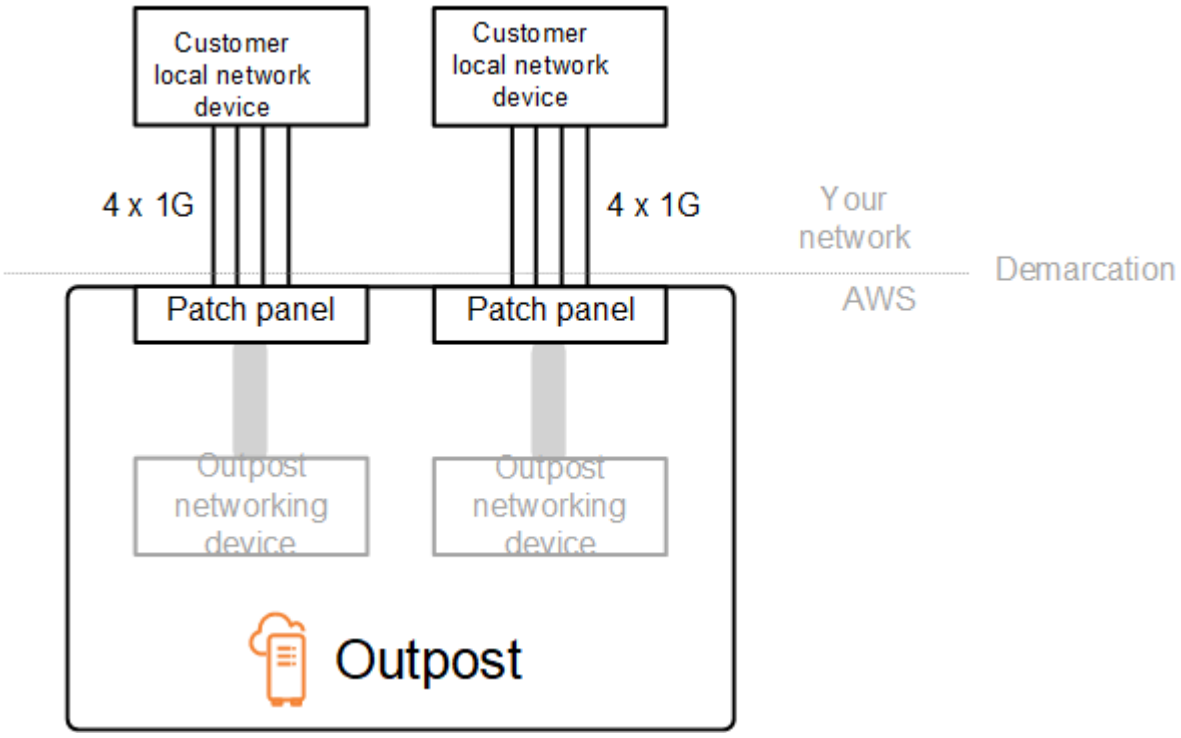
上行链路速度	上行链路数量
1 Gbps	1、2、4、6 或 8

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

每台 Outpost 网络设备上的上行链路速度和数量是对称的。如果使用 100 Gbps 作为上行链路速度，则必须为链路配置前向纠错 (FEC CL91)。

前哨机架可以支持带朗讯连接器 (LC) 的单模光纤 (SMF)、多模光纤 (MMF) 或带有 LC 的 MMF OM4。AWS 提供与您在机架位置提供的光纤兼容的光学元件。

在下图中，物理分界线是每个 Outpost 中的光纤配线架。您需要提供将 Outpost 连接到配线架所需的光缆。



链路聚合

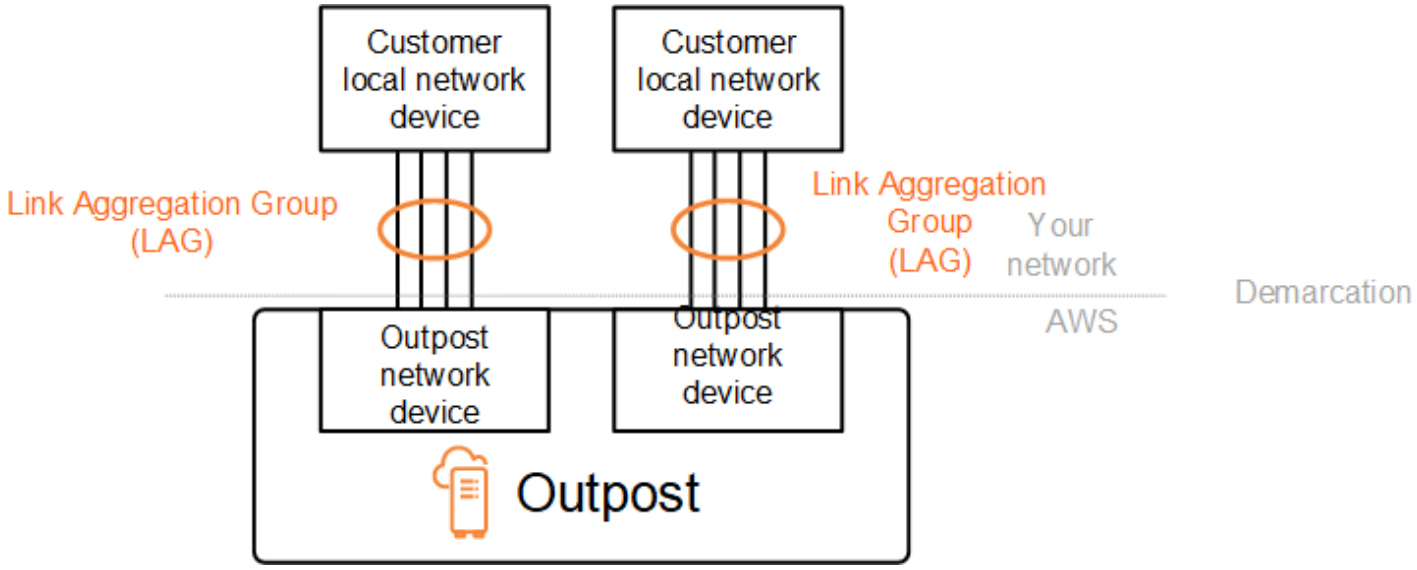
AWS Outposts 使用链路聚合控制协议 (LACP) 建立两个链路聚合组 (LAG) 连接，分别从每个 Outpost 网络设备连接到每台本地网络设备。来自每个 Outpost 网络设备的链路聚合到以太网 LAG 中，以表示单个网络连接。这些 LAG 使用 LACP 和标准快速计时器。您无法将 LAG 配置为使用慢速计时器。

要在您的站点上启用 Outpost 安装，您必须在网络设备上配置您的 LAG 连接。

从逻辑的角度来看，请忽略 Outpost 配线板作为分界点，请使用 Outpost 网络设备。

对于具有多个机架的部署，Outpost 必须在 Outpost 网络设备的聚合层和您的本地网络设备之间有四个 LAG。

下图显示了每个 Outpost 网络设备与其连接的本地网络设备之间的四个物理连接。我们使用以太网 LAG 来聚合连接 Outpost 网络设备和客户本地网络设备的物理链路。



虚拟 LAN

Outpost 网络设备和本地网络设备之间的每个 LAG 都必须配置为 IEEE 802.1q 以太网中继。这允许使用多个 VLAN 在数据路径之间进行网络分割。

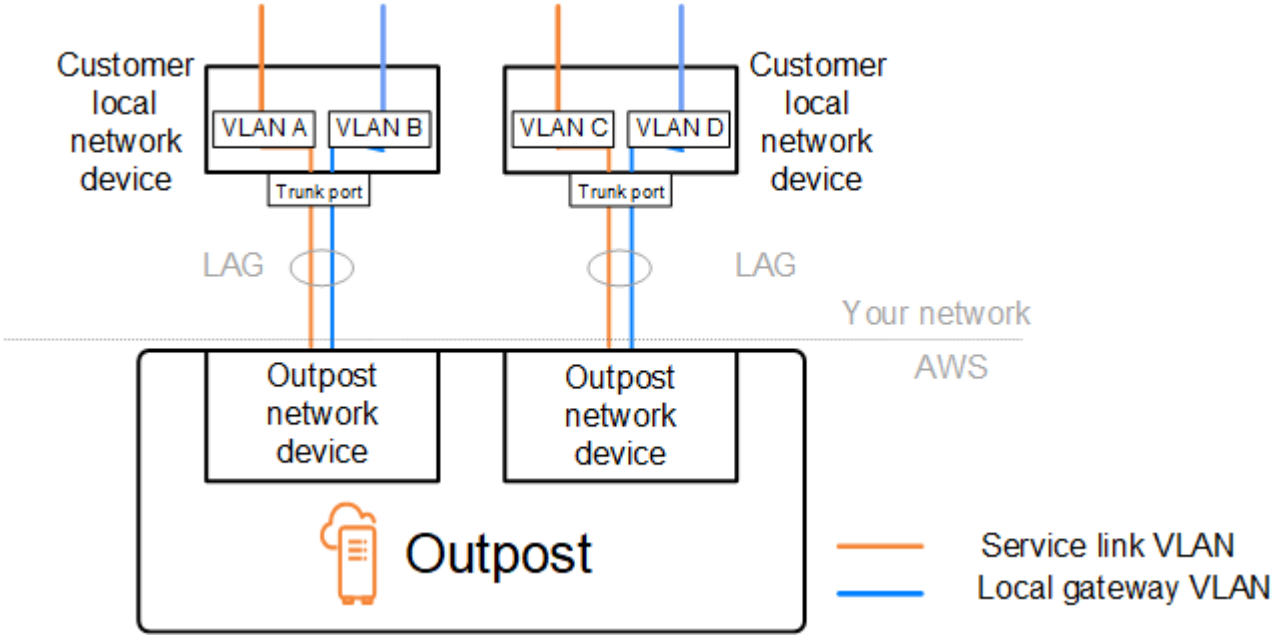
每个 Outpost 都有以下 VLAN 来与您的本地网络设备通信：

- 服务链路 VLAN — 启用 Outpost 与本地网络设备之间的通信，以便为服务链路连接建立服务链路路径。有关更多信息，请参阅与 AWS 区域的AWS Outposts 连接。
- 本地网关 VLAN — 启用 Outpost 与本地网络设备之间的通信，以便建立本地网关路径来连接您的 Outpost 子网和局域网。Outpost 本地网关利用此 VLAN 为您的实例提供与本地网络的连接，其中可能包括通过您的网络访问互联网。有关更多信息，请参阅本地网关。

您只能在 Outpost 和客户的本地网络设备之间配置服务链路 VLAN 和本地网关 VLAN。

Outpost 旨在将服务链路和本地网关数据路径分成两个隔离的网络。这使您可以选择哪些网络可以与 Outpost上运行的服务进行通信。它还允许您在客户本地网络设备（通常称为虚拟路由和转发实例

(VRF)) 上使用多个路由表，使服务链路成为与本地网关网络隔离的网络。分界线位于前哨网络设备的端口。 AWS 管理连接 AWS 侧的任何基础架构，并管理线路边的任何基础架构。



要在安装和持续运行期间将 Outpost 与本地网络集成，您必须在 Outpost 网络设备和客户本地网络设备之间分配使用的 VLAN。在安装 AWS 之前，您需要向提供此信息。有关更多信息，请参阅 the section called “网络就绪性核对清单”。

网络层连接

为了建立网络层连接，每台 Outpost 网络设备都要配置虚拟接口 (VIF)，其中包括每个 VLAN 的 IP 地址。通过这些 VIF， AWS Outposts 网络设备可以与您的本地网络设备建立 IP 连接和 BGP 会话。

我们建议执行下列操作：

- 使用带有 /30 或 /31 CIDR 的专用子网来表示这种逻辑连接。 point-to-point
- 请勿在本地网络设备之间桥接 VLAN。

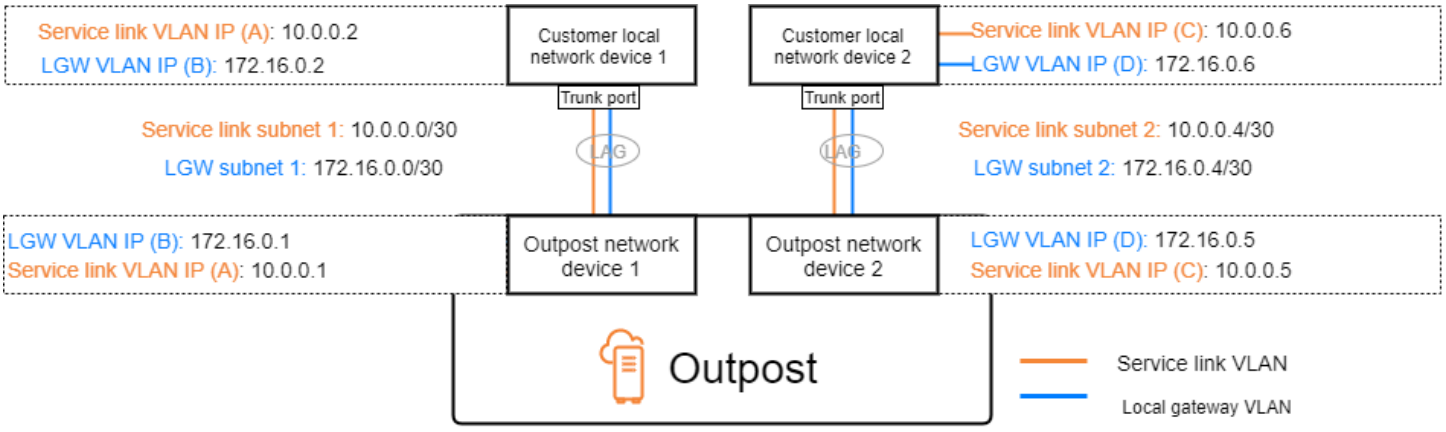
要实现网络层连接，必须建立两条路径：

- 服务链路路径-要建立此路径，请指定一个范围为 /30 或 /31 的 VLAN 子网，并为 AWS Outposts 网络设备上的每个服务链路 VLAN 指定一个 IP 地址。服务链路虚拟接口 (VIF) 用于此路径，用于在您的 Outpost 和本地网络设备之间建立 IP 连接和 BGP 会话，以实现服务链路连接。有关更多信息，请参阅与 AWS 区域的AWS Outposts 连接。

- 本地网关路径-要建立此路径，请在 AWS Outposts 网络设备上指定一个范围为 /30 或 /31 的 VLAN 子网以及本地网关 VLAN 的 IP 地址。此路径上使用本地网关 VIF 在您的 Outpost 和本地网络设备之间建立 IP 连接和 BGP 会话，以实现本地资源连接。

下图显示了从每个 Outpost 网络设备到客户本地网络设备的连接（对于服务链路路径和本地网关路径）。此示例有四个 VLAN：

- VLAN A 用于连接 Outpost 网络设备 1 和客户本地网络设备 1 的服务链路路径。
- VLAN B 用于连接 Outpost 网络设备 1 和客户本地网络设备 1 的本地网关路径。
- VLAN C 用于连接 Outpost 网络设备 2 和客户本地网络设备 2 的服务链路路径。
- VLAN D 用于连接 Outpost 网络设备 2 和客户本地网络设备 2 的本地网关路径。



下表显示了将 Outpost 网络设备 1 与客户本地网络设备 1 连接起来的子网的示例值。

VLAN	子网	客户设备 1 IP	AWS OND 1 IP
A	10.0.0.0/30	10.0.0.2	10.0.0.1
B	172.16.0.0/30	172.16.0.2	172.16.0.1

下表显示了将 Outpost 网络设备 2 与客户本地网络设备 2 连接起来的子网的示例值。

VLAN	子网	客户设备 2 IP	AWS OND 2 IP
C	10.0.0.4/30	10.0.0.6	10.0.0.5

VLAN	子网	客户设备 2 IP	AWS OND 2 IP
D	172.16.0.4/30	172.16.0.6	172.16.0.5

ACE 机架连接

> **Note**
>
> 如果您不需要 ACE 机架，请跳过本节。

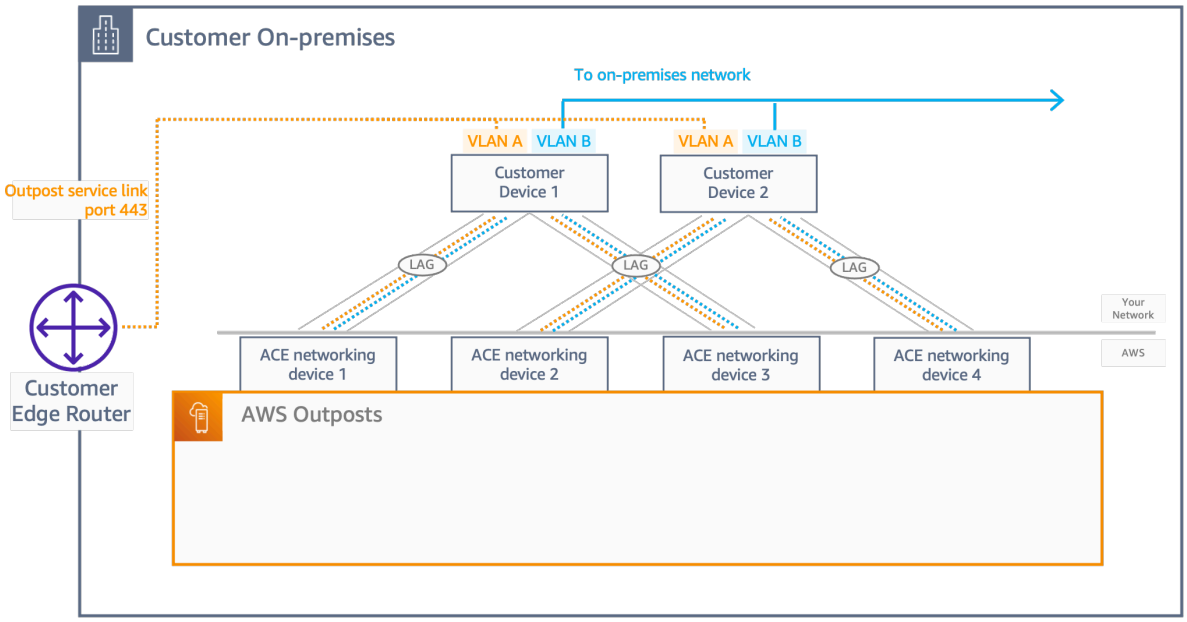
聚合、核心、边缘 (ACE) 机架充当多机架 Outpost 部署的网络聚合点。如果您有五个或更多计算机架，则必须使用 ACE 机架。如果您的计算机架少于五个，但计划将来扩展到五个或更多机架，我们建议您尽早安装 ACE 机架。

使用 ACE 机架，Outposts 网络设备不再直接连接到您的本地网络设备。相反，它们连接到 ACE 机架，ACE 机架提供与 Outpost 机架的连接。在此拓扑中， AWS 拥有 Outposts 网络设备和 ACE 网络设备之间的 VLAN 接口分配和配置。

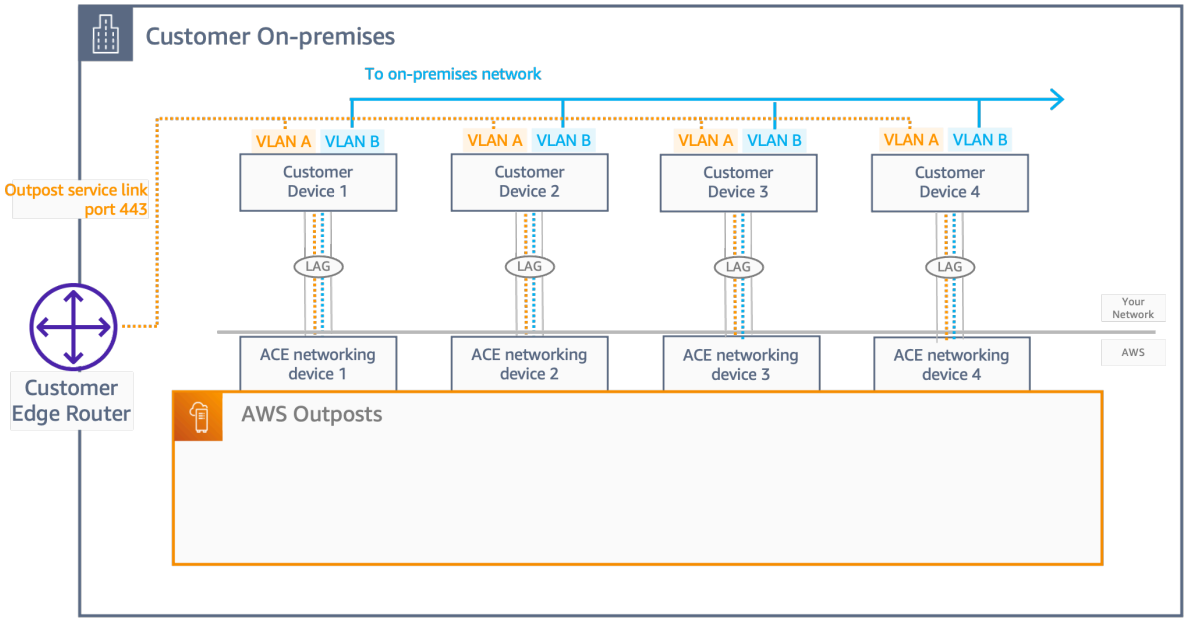
ACE 机架包括四台网络设备，这些设备可以连接到客户本地网络中的两台上游客户设备或四台上游客户设备，以实现最大的弹性。

下图显示了两种网络拓扑。

下图显示了连接到两台上游客户设备的 ACE 机架中的四台 ACE 网络设备：



下图显示了连接到四台上游客户设备的 ACE 机架上的四台 ACE 网络设备：

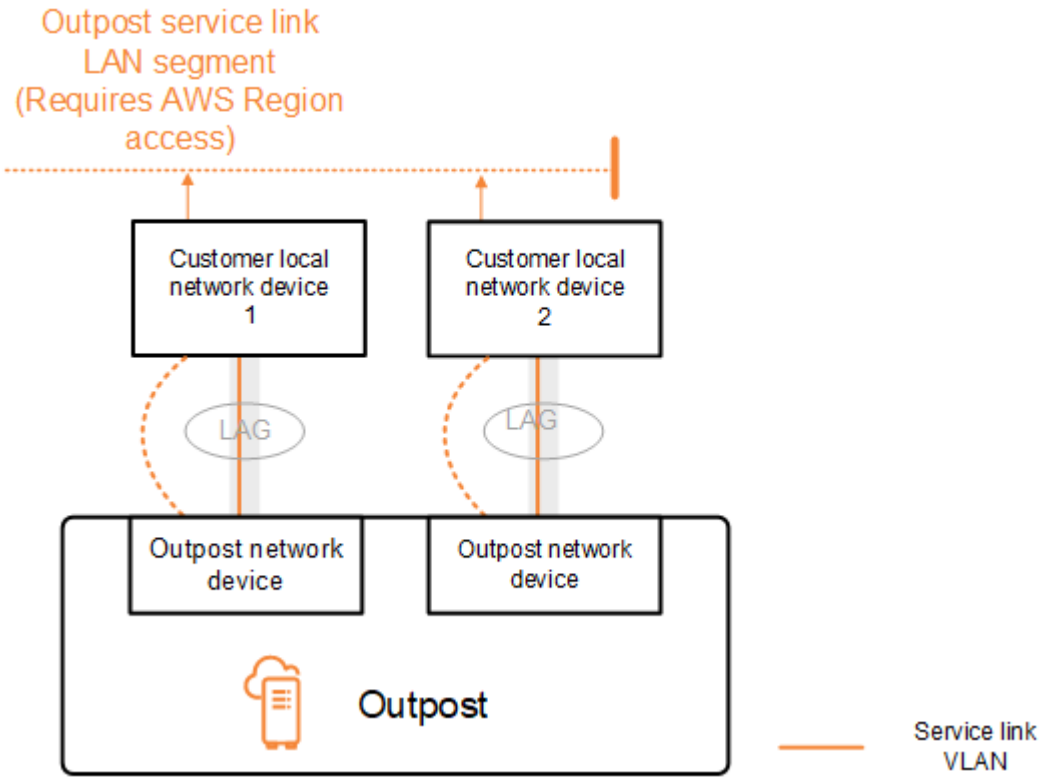


服务链路 BGP 连接

Outpost 在每个 Outpost 网络设备和客户本地网络设备之间建立一个外部 BGP 对等会话，以便通过服务链路 VLAN 进行服务链路连接。BGP 对等会话是在为 VLAN 提供的 /30 或 /31 IP 地址之间建立的。point-to-point 每个 BGP 对等会话都在 Outpost 网络设备上使用私有自治系统号 (ASN) 以及您为客户本地网络设备选择的 ASN。 AWS 提供属性作为安装过程的一部分。

考虑一下这样的场景：您的 Outpost 有两台 Outpost 网络设备，通过服务链路 VLAN 连接到两台客户本地网络设备。您可以为每个服务链路配置以下基础架构和客户本地网络设备 BGP ASN 属性：

- 服务链路 BGP ASN。2 字节（16 位）或 4 字节（32 位）。有效值为 64512-65535 或 4200000000-4294967294。
- 基础设施 CIDR。这必须是每个机架的 /26 CIDR。
- 客户本地网络设备 1 服务链路 BGP 对等 IP 地址。
- 客户本地网络设备 1 服务链路 BGP 对等 ASN。有效值为 1-4294967294。
- 客户本地网络设备 2 服务链路 BGP 对等 IP 地址。
- 客户本地网络设备 2 服务链路 BGP 对等 ASN。有效值为 1-4294967294。有关更多信息，请参阅 RFC4893。



Outpost 使用以下过程通过服务链路 VLAN 建立外部 BGP 对等会话：

1. 每个 Outpost 网络设备都使用 ASN 与其连接的本地网络设备建立 BGP 对等会话。
2. Outpost 网络设备将 /26 CIDR 范围通告为两个 /27 CIDR 范围，以支持链路和设备故障。每个 OND 都通告自己的 /27 前缀，AS-path 长度为 1，再加上 AS 路径长度为 4 的所有其他 OD 的 /27 前缀（作为备份）。

3. 子网用于从前哨基地到该 AWS 地区的连接。

我们建议您将客户网络设备配置为在不更改 BGP 属性的情况下接收来自 Outposts 的 BGP 通告。客户网络应首选 AS-Path 长度为 1 的 Outpost 路由，而不是 AS-Path 长度为 4 的路由。

客户网络应向所有 OND 通告具有相同属性的同等 BGP 前缀。默认情况下，Outpost 网络对所有上行链路之间的出站流量执行负载均衡。如果需要维护，Outpost 一侧使用路由策略将流量从 OND 转移出去。这种流量转移需要客户端在所有 OND 上使用相同的 BGP 前缀。如果客户网络需要维护，建议您使用 AS-Path 预置来临时转移特定上行链路的流量组。

服务链路基础架构子网通告和 IP 范围

在服务链路基础架构子网的预安装过程中，您可以提供 /26 CIDR 范围。Outpost 基础架构使用该范围通过服务链路与该地区建立连接。服务链路子网是 Outpost 源，后者启动连接。

Outpost 网络设备将 /26 CIDR 范围通告为两个 /27 CIDR 区块，以支持链路和设备故障。

您必须为 Outpost 提供服务链路 BGP ASN 和基础设施子网 CIDR (/26)。对于每台 Outpost 网络设备，需提供本地网络设备的 VLAN 上的 BGP 对等 IP 地址和本地网络设备的 BGP ASN。

如果您采用多机架部署，则每个机架必须有一个 /26 子网。

本地网关 BGP 连接

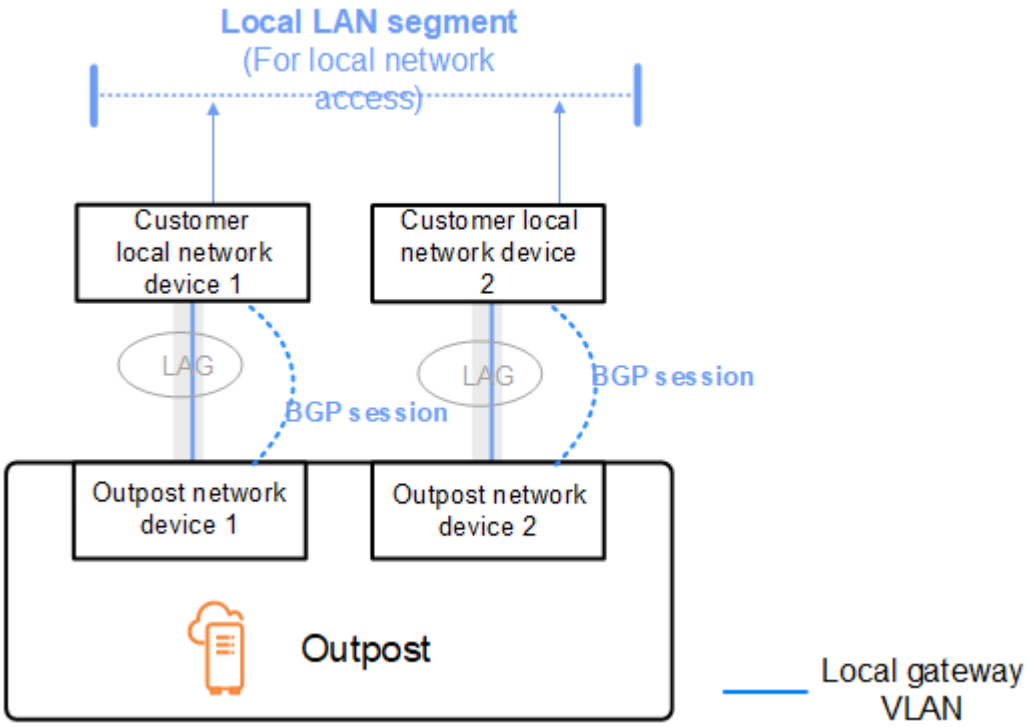
Outpost 建立从每个 Outpost 网络设备到本地网络设备的外部 BGP 对等连接，以连接到本地网关。Outpost 使用您分配的私有自治系统号 (ASN) 来建立外部 BGP 会话。每个 Outpost 网络设备都有一个外部 BGP，通过其本地网关 VLAN 与本地网络设备对等。

Outpost 通过本地网关 VLAN 在每台 Outpost 网络设备与其连接的客户本地网络设备之间建立外部 BGP 对等会话。对等会话是在您在设置网络连接时提供的 /30 或 /31 IP 之间建立的，并使用 Outpost 网络设备和客户本地网络设备之间的 point-to-point 连接。有关更多信息，请参阅 the section called “网络层连接”。

每个 BGP 会话都使用 Outpost 网络设备端的私有 ASN，以及您在客户本地网络设备端选择的 ASN。AWS 在预安装过程中提供了这些属性。

考虑一下这样的场景：您的 Outpost 有两台 Outpost 网络设备，通过服务链路 VLAN 连接到两台客户本地网络设备。您可以为每个服务链路配置以下本地网关和客户本地网络设备 BGP ASN 属性：

- AWS 提供本地网关 BGP ASN。2 字节（16 位）或 4 字节（32 位）。有效值为 64512-65535 或 4200000000-4294967294。
- （可选）您提供将进行通告的客户拥有的 CIDR（公共或私有，最低 /26）。
- 您为客户本地网络设备 1 提供本地网关 BGP 对等 IP 地址。
- 您为客户本地网络设备 1 提供本地网关 BGP 对等 SAN。有效值为 1-4294967294。有关更多信息，请参阅 RFC4893。
- 您为客户本地网络设备 2 提供本地网关 BGP 对等 IP 地址。
- 您为客户本地网络设备 2 提供本地网关 BGP 对等 SAN。有效值为 1-4294967294。有关更多信息，请参阅 RFC4893。



建议您对客户网络设备进行相应配置，以便在不更改 BGP 属性的情况下接收 Outpost 的 BGP 通告，并启用 BGP 多路径/负载均衡来实现最佳的入站流量。AS-Path 预置用于本地网关前缀，以便在需要维护时将流量从 OND 转移出去。客户网络应首选 AS-Path 长度为 1 的 Outpost 路由，而不是 AS-Path 长度为 4 的路由。

客户网络应向所有 OND 通告具有相同属性的同等 BGP 前缀。默认情况下，Outpost 网络对所有上行链路之间的出站流量执行负载均衡。如果需要维护，Outpost 一侧使用路由策略将流量从 OND 转移出去。这种流量转移需要客户端在所有 OND 上使用相同的 BGP 前缀。如果客户网络需要维护，建议您使用 AS-Path 预置来临时转移特定上行链路的流量组。

本地网关客户拥有的 IP 子网通告

默认情况下，本地网关使用 VPC 中实例的私有 IP 地址来促进与本地网络的通信。但是，您可以提供客户拥有的 IP 地址池 (CoIP)。

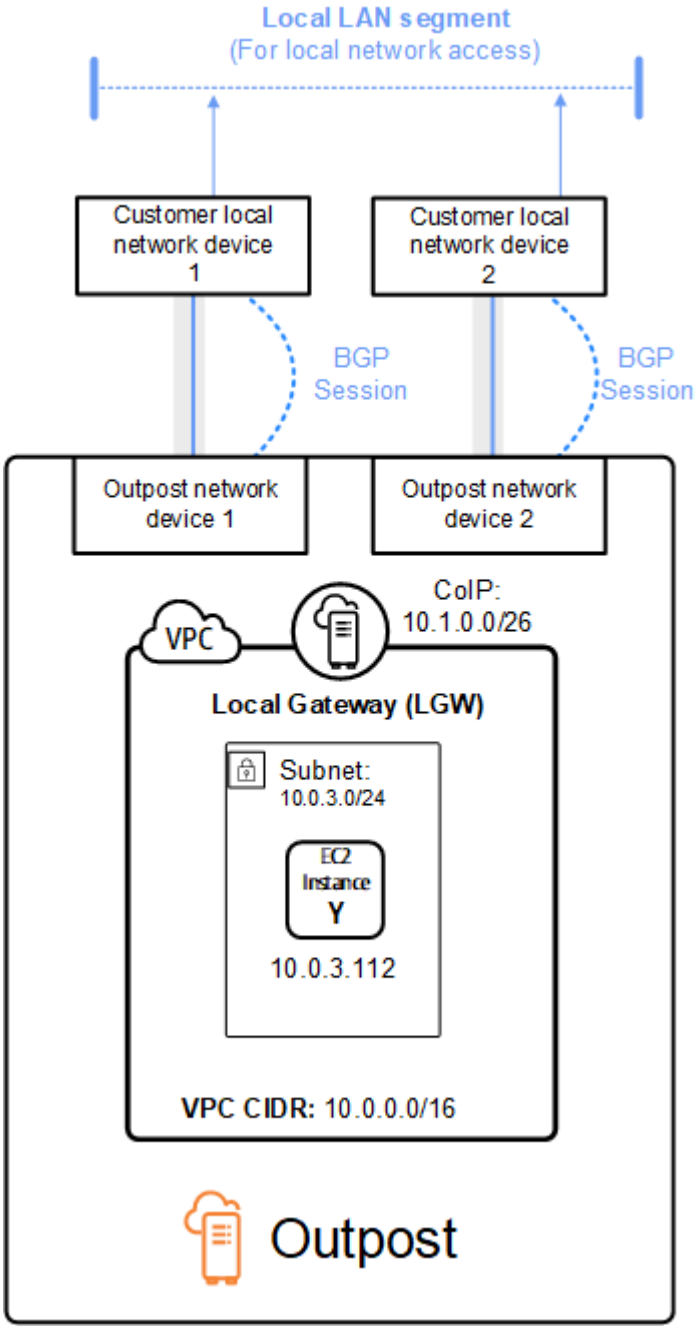
如果您选择 CoIP，则会根据您在安装过程中提供的信息 AWS 创建池。您可以从该池中创建弹性 IP 地址，然后将这些地址分配给您的 Outpost 上的资源，例如 EC2 实例。

本地网关将弹性 IP 地址转换为客户拥有的池中的地址。本地网关会将转换后的地址通告到您的本地网络以及与 Outpost 通信的任何其他网络。这些地址将在这两个本地网关 BGP 会话中通告给本地网络设备。

> **Tip**
>
> 如果您未使用 CoIP，则 BGP 会通告您的 Outpost 上所有符合以下条件的子网的私有 IP 地址：其路由表中包含以本地网关为目标的路由。

考虑一下这样的场景：您的 Outpost 有两台 Outpost 网络设备，通过服务链路 VLAN 连接到两台客户本地网络设备。配置了以下内容：

- VPC：CIDR 块为 10.0.0.0/16。
- VPC 中带有 CIDR 块的 10.0.3.0/24 的子网。
- 子网中的一个 EC2 实例，其私有 IP 地址为 10.0.3.112。
- 客户拥有的 IP 池 (10.1.0.0/26)。
- 一种将 10.0.3.112 关联到 10.1.0.2 的弹性 IP 地址关联。
- 一种本地网关，其使用 BGP 通过本地设备向本地网络通告 10.1.0.0/26。
- 您的 Outpost 和本地网络之间的通信将使用 CoIP 弹性 IP 来寻址 Outpost 中的实例，但不会使用 VPC CIDR 范围。


Local LAN segment
(For local network access)
Customer local network device 1
Customer local network device 2
BGP Session
BGP Session
Outpost network device 1
Outpost network device 2
CoIP: 10.1.0.0/26
VPC
Local Gateway (LGW)
Subnet: 10.0.3.0/24
EC2 Instance Y
10.0.3.112
VPC CIDR: 10.0.0.0/16
Outpost

使用共享的 AWS Outposts 资源

通过 Outpost 共享，Outpost 所有者可与同一 AWS 组织下的其他 AWS 账户共享他们的 Outpost 和 Outpost 资源，包括 Outpost 站点和子网。作为 Outpost 所有者，您可以集中创建和管理 Outpost 资源，并在 AWS 组织内的多个 AWS 账户之间共享资源。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。

在此模型中，拥有 Outpost 资源的 AWS 账户（所有者）与同一组织中的其他 AWS 账户（使用者）共享资源。使用者可以在共享的 Outpost 上创建资源，操作方式与他们在自己的账户中所创建的 Outpost 上创建资源一样。所有者负责管理 Outpost 以及他们在其上创建的资源。拥有者可以随时更改或撤销共享访问权限。所有者还可以查看、修改和删除使用者在共享的 Outpost 上创建的资源，但使用容量预留的实例除外。拥有者无法修改使用者启动到已共享的容量预留中的实例。

使用者负责管理他们在与其共享的 Outpost 上创建的资源，包括使用容量预留的任何资源。使用者无法查看或修改由其他使用者或 Outpost 拥有者拥有的资源。他们也无法修改别人共享给他们的 Outpost。

Outpost 所有者可以与以下人员共享 Outpost 资源：

- AWS Organizations 中其组织内部的特定 AWS 帐户。
- AWS Organizations 中其组织内部的组织单元。
- AWS Organizations 中的整个组织。

目录

- 限制

可共享的 Outpost 资源

Outpost 所有者可以与使用者共享本部分中列出的 Outpost 资源。

这些资源可供 Outpost 机架使用。对于服务器资源，请参阅适用于 Outpost 服务器的 AWS Outposts 用户指南中的使用共享的 AWS Outposts 资源。

- 分配的专属主机 — 有权访问此资源的使用者可以：
  - 在专属主机上启动和运行 EC2 实例。
- 容量预留 — 有权访问此资源的使用者可以：
  - 确定其他人共享给他们的容量预留。
  - 启动和管理使用容量预留的实例。
- 客户拥有的 IP 地址 (CoIP) 池 — 有权访问此资源的使用者可以：
  - 分配客户拥有的 IP 地址并将其与实例关联。
- 本地网关路由表 — 有权访问此资源的使用者可以：
  - 创建和管理与本地网关的 VPC 关联。
  - 查看本地网关路由表和虚拟接口的配置。
- Outpost — 有权访问此资源的使用者可以：
  - 在 Outpost 上创建和管理子网。
  - 在 Outpost 上创建和管理 EBS 卷。
  - 使用 AWS Outposts API 查看 Outpost 的相关信息。
- S3 on Outposts — 有权访问此资源的使用者可以：
  - 在 Outpost 上创建和管理 S3 存储桶、接入点和端点。
- 站点 — 有权访问此资源的使用者可以：
  - 在站点上创建、管理和控制 Outpost。
- 子网 — 有权访问此资源的使用者可以：
  - 查看子网的相关信息。
  - 在子网中启动和运行 EC2 实例。

  使用 Amazon VPC 控制台共享 Outpost 子网。有关更多信息，请参阅 Amazon VPC 用户指南中的共享子网。

共享 Outpost 资源的先决条件

- 要与您的组织或 AWS Organizations 内的组织单元共享 Outpost 资源，您必须允许与 AWS Organizations 共享。有关更多信息，请参阅《AWS RAM 用户指南》中的允许与 AWS Organizations 共享。
- 要共享 Outpost 资源，您必须在您的 AWS 账户拥有该资源。您无法共享已与您共享的 Outpost 资源。
- 要共享 Outpost 资源，您必须与所在组织内的账户共享该资源。

相关服务

Outpost 资源共享与 AWS Resource Access Manager (AWS RAM) 集成。AWS RAM 是一项服务，允许您与任何 AWS 账户或通过 AWS Organizations 共享 AWS 资源。利用 AWS RAM，您可通过创建资源共享来共享您拥有的资源。资源共享指定要共享的资源以及与之共享资源的使用者。使用者可以是单个 AWS 账户、组织单位或 AWS Organizations 中的整个组织。

有关 AWS RAM 的更多信息，请参阅 AWS RAM 用户指南。

跨可用区共享

为确保资源分配到区域的各可用区，我们将可用区独立映射到每个账户的名称。这可能会导致账户之间的可用区命名差异。例如，您的 `us-east-1a` 账户的可用区 AWS 可能与另一 `us-east-1a` 账户的 AWS 不在同一位置。

要确定相对于账户的 Outpost 资源位置，您必须使用可用区 ID (AZ ID)。AZ ID 是跨所有 AWS 账户的可用区的唯一且一致的标识符。例如，`use1-az1` 是 `us-east-1` 区域的 AZ ID，它在每个 AWS 账户中的位置均相同。

查看账户中的可用区的 AZ ID

1. 通过以下网址打开 AWS RAM 控制台：https://console.aws.amazon.com/ram。
2. 当前区域的 AZ ID 显示在屏幕右侧的 Your AZ ID (您的 AZ ID) 面板中。

> **Note**
>
> 本地网关路由表与其 Outpost 位于同一个可用区，因此您无需为路由表指定可用区 ID。

共享 Outpost 资源

所有者与使用者共享 Outpost 后，使用者可以在这个 Outpost 上创建资源，如同他们在自己的账户中所创建的 Outpost 上创建资源一样。有权访问共享的本地网关路由表的使用者可以创建和管理 VPC 关联。有关更多信息，请参阅 可共享的 Outpost 资源。

要共享 Outpost 资源，必须将它添加到资源共享。资源共享是一项 AWS RAM 资源，可让您跨 AWS 账户共享资源。资源共享指定要共享的资源以及与之共享资源的使用者。在使用 AWS Outposts 控制台共享 Outpost 资源时，必须将它添加到现有资源共享。要将 Outpost 资源添加到新的资源共享，必须首先使用 AWS RAM 控制台创建资源共享。

如果您属于 AWS Organizations 组织内的某个组织，并启用了组织内共享，则您可以授予组织中的使用者从 AWS RAM 控制台访问共享 Outpost 资源的权限。否则，使用者将会收到加入资源共享的邀请，并在接受邀请后为其授予共享的 Outpost 资源的访问权限。

您可以使用 AWS Outposts 控制台、AWS RAM 控制台或 AWS CLI 共享您拥有的 Outpost 资源。

使用 AWS Outposts 控制台共享您拥有的 Outpost

1. 打开 AWS Outposts 控制台 (https://console.aws.amazon.com/outposts/)。
2. 在导航窗格中，选择 Outposts。
3. 选择 Outpost，然后选择操作，查看详细信息。
4. 在 Outpost 摘要页面上，选择资源共享。
5. 选择 Create resource share（创建资源共享）。

您将被重定向到 AWS RAM 控制台，然后按照以下步骤完成 Outpost 共享。要共享您拥有的本地网关路由表，也可以按以下步骤操作。

使用 AWS RAM 控制台共享您拥有的 Outpost 或本地网关路由表

请参阅 AWS RAM 用户指南中的创建资源共享。

使用 AWS CLI 共享您拥有的 Outpost 或本地网关路由表

使用 create-resource-share 命令。

取消共享已共享的 Outpost 资源

取消共享的 Outpost 后，使用者将无法再在 AWS Outposts 控制台中查看此 Outpost。他们无法在 Outpost 上创建新子网，或在 Outpost 上创建新的 EBS 卷，也无法通过 AWS Outposts 控制台或 AWS CLI 查看 Outpost 的详细信息和实例类型。由使用者创建的现有子网、卷或实例不会被删除。使用者在 Outpost 上创建的任何现有子网仍然可用于启动新实例。

取消共享已共享的本地网关路由表后，使用者无法再为其创建新的 VPC 关联。使用者创建的任何现有 VPC 关联仍然与该路由表关联。这些 VPC 中的资源可以继续将流量路由到本地网关。

要取消共享您拥有的共享的 Outpost 资源，必须从资源共享中将其删除。您可以使用 AWS RAM 控制台或 AWS CLI 以执行该操作。

使用 AWS RAM 控制台取消共享您拥有的共享的 Outpost 资源

请参阅 AWS RAM 用户指南中的更新资源共享。

使用 AWS CLI 取消共享您拥有的共享的 Outpost 资源

使用 disassociate-resource-share 命令。

识别共享的 Outpost 资源

拥有者和使用者可以使用 AWS Outposts 控制台和 AWS CLI 标识共享的 Outpost。他们可以使用 AWS CLI 来识别共享的本地网关路由表。

使用 AWS Outposts 控制台标识共享的 Outpost

1. 打开 AWS Outposts 控制台 (https://console.aws.amazon.com/outposts/)。
2. 在导航窗格中，选择 Outposts。
3. 选择 Outpost，然后选择操作，查看详细信息。
4. 在 Outpost 摘要页面上，查看所有者 ID 以识别 Outpost 所有者的 AWS 账户 ID。

使用 AWS CLI 标识共享的 Outpost 资源

使用 list-outposts 和 describe-local-gateway-route-tables 命令。这些命令返回您拥有的 Outpost 资源以及与您共享的 Outpost 资源。`OwnerId` 显示 Outpost 资源所有者的 AWS 帐户 ID。

共享的 Outpost 资源权限

拥有者的权限

所有者负责管理 Outpost 以及他们在其上创建的资源。拥有者可以随时更改或撤销共享访问权限。他们可以使用 AWS Organizations 查看、修改和删除使用者在共享的 Outpost 上创建的资源。

使用者的权限

使用者可以在共享的 Outpost 上创建资源，操作方式与他们在自己的账户中所创建的 Outpost 上创建资源一样。使用者负责管理他们在与其共享的 Outpost 上发布的资源。使用者无法查看或修改其他使用者或 Outpost 拥有者所拥有的资源，也无法修改与其共享的 Outpost。

计费和计量

所有者需要为他们共享的 Outpost 和 Outpost 资源支付费用。还需要为与来自 AWS 区域的 Outpost 服务链接 VPN 流量相关的任何数据传输支付费用。

共享本地网关路由表不会产生额外费用。对于共享的子网，VPC 所有者需要为 VPC 级别的资源（例如 AWS Direct Connect 和 VPN 连接、NAT 网关以及私有链路连接）支付费用。

使用者需要为他们在共享的 Outpost 上创建的应用程序资源（例如负载均衡器和 Amazon RDS 数据库）支付费用。还需要为来自 AWS 区域的收费数据传输支付费用。

限制

以下限制适用于 AWS Outposts 共享的使用：

- 使用 AWS Outposts 共享时适用共享子网的限制。有关 VPC 共享限制的更多信息，请参阅 Amazon Virtual Private Cloud 用户指南中的限制。
- 服务配额按各个账户应用。

安全性 AWS Outposts

安全性 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将此描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用的合规计划 AWS Outposts，请参阅按合规计划划分的范围内的AWSAWS 服务按合规计划。
- 云端安全-您的责任由您使用的 AWS 服务决定。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。

有关安全性和合规性的更多信息 AWS Outposts，请参阅AWS Outposts 机架常见问题解答AWS Outposts 服务器常见问题。

本文档可帮助您了解在使用时如何应用分担责任模型 AWS Outposts。它说明了如何实现您的安全性和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的资源。

内容

中的数据保护 AWS Outposts

分 AWS 担责任模型适用于中的数据保护 AWS Outposts。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。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 IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。

有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

静态加密

使用 AWS Outposts，所有数据都处于静态加密状态。密钥材料封装在外部密钥中，而该外部密钥存储可移动设备中，即 Nitro 安全密钥 (NSK)。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。有关更多信息，请参阅《Amazon EC2 用户指南》中的 Amazon EBS 加密。

传输中加密

AWS 加密您的 Outpost 与其所在地区之间的传输数据。 AWS 有关更多信息，请参阅 通过服务链路进行连接。

您可以使用传输层安全性协议 (TLS) 等加密协议来加密通过本地网关传输到本地网络的传输中敏感数据。

数据删除

在停止或终止 EC2 实例时，管理程序将清理分配给实例的内存（设置为零），然后再将内存分配给新实例并重置每个存储块。

销毁 Nitro 安全密钥会以加密方式粉碎您的 Outpost 上的数据。

的身份和访问管理 (IAM) AWS Outposts

AWS Identity and Access Management (IAM) 是一项 AWS 服务，可帮助管理员安全地控制对 AWS 资源的访问。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。使用 IAM 不会产生额外的费用。

内容

- AWS Outposts 如何与 IAM 配合使用
- AWS Outposts 政策示例
- 将服务相关角色用于 AWS Outposts
- AWS 的托管策略 AWS Outposts

AWS Outposts 如何与 IAM 配合使用

在使用 IAM 管理对 AWS Outposts 的访问权限之前，请先了解有哪些 IAM 功能可用于 Out AWS posts。

你可以在 O AWS utposts 中使用的 IAM 功能

IAM 功能	AWS Outposts 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACL	否
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

Outposts 基于身份的政策 AWS

支持基于身份的策略	是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅 IAM 用户指南中的创建 IAM 策略。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Outposts 基于身份的策略示例 AWS

要查看 AWS Outposts 基于身份的政策示例，请参阅。AWS Outposts 政策示例

Outposts 内部 AWS 基于资源的政策

支持基于资源的策略	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。

AWS Outposts 的政策行动

支持策略操作	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 AWS Outposts 操作列表，请参阅《服务授权参考》 AWS Outposts中定义的操作。

AWS Outposts 中的策略操作在操作前使用以下前缀：

```
outposts
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
    "outposts:action1",
    "outposts:action2"
]
```

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 List 开头的所有操作，包括以下操作：

```
"Action": "outposts:List*"
```

AWS Outposts 的政策资源

支持策略资源	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

某些 AWS Outposts API 操作支持多种资源。要在单个语句中指定多个资源，请使用逗号分隔 ARN。

```
"Resource": [
    "resource1",
    "resource2"
```

```
]
```

要查看 AWS Outposts 资源类型及其 ARN 的列表，请参阅《服务授权参考》 AWS Outposts中定义的资源类型。要了解可以在哪些操作中指定每个资源的 ARN，请参阅 AWS Outposts定义的操作。

AWS Outposts 的策略条件密钥

支持特定于服务的策略条件键	是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 AWS Outposts 条件键列表，请参阅《服务授权参考》 AWS Outposts中的条件密钥。要了解可以使用条件键的操作和资源，请参阅由定义的操作 AWS Outposts。

要查看 AWS Outposts 基于身份的政策示例，请参阅。AWS Outposts 政策示例

Outposts 中的 AWS ACL

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC with Outposts AWS

支持 ABAC（策略中的标签）	是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

在 O AWS utposts 中使用临时证书

支持临时凭证	是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Outposts 的跨服务主体 AWS 权限

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

AWS Outpost 的服务角色

支持服务角色	否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

Outposts 的 AWS 服务相关角色

支持服务相关角色	是

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理 AWS Outposts 服务相关角色的详细信息，请参阅。将服务相关角色用于 AWS Outposts

AWS Outposts 政策示例

默认情况下，用户和角色无权创建或修改 AWS Outposts 资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM 策略。

有关 AWS Outposts 定义的操作和资源类型（包括每种资源类型的 ARN 格式）的详细信息，请参阅《服务授权参考》 AWS Outposts中的操作、资源和条件密钥。

内容

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 O AWS utposts 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

示例：使用资源级权限

以下示例使用资源级权限来授予权限，以获取有关指定 Outpost 的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": "outposts:GetOutpost",
      "Resource": "arn:aws:outposts:region:12345678012:outpost/op-1234567890abcdef0"
    }
  ]
}
```

以下示例使用资源级权限来授予权限，以获取有关指定站点的信息。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "outposts:GetSite",
      "Resource": "arn:aws:outposts:region:12345678012:site/os-0abcdef1234567890"
    }
  ]
}
```

将服务相关角色用于 AWS Outposts

AWS Outposts 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 AWS Outposts服务相关角色由服务预定义 AWS Outposts ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色可以提高您的设置 AWS Outposts 效率，因为您不必手动添加必要的权限。 AWS Outposts 定义其服务相关角色的权限，除非另有定义，否则 AWS Outposts 只能担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

只有在先删除相关资源后，才能删除服务相关角色。这样可以保护您的 AWS Outposts 资源，因为您不能无意中删除访问资源的权限。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务相关角色文档。

AWS Outposts的服务相关角色权限

AWS Outposts 使用名为 AWSServiceRoleForOutposts_ ***outpostID ####### – ## O*** utposts 代表你访问私有连接 AWS 资源。此服务相关角色允许配置私有连接、创建网络接口并将其附加到服务链路端点实例。

AWSServiceRoleForOutposts_ *outpostID* 服务相关角色信任以下服务来代入该角色：

- outposts.amazonaws.com

AWSServiceRoleForOutposts_ ***OutpostID*** 服务相关角色包括以下策略：

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ ***out*** postID

该AWSOutpostsServiceRolePolicy策略是一个与服务相关的角色策略， AWS 用于允许访问由管理的 AWS Outposts资源。

此策略 AWS Outposts 允许对指定资源完成以下操作：

- 操作：all AWS resources 上的 ec2:DescribeNetworkInterfaces
- 操作：ec2:DescribeSecurityGroups 上的 all AWS resources
- 操作：ec2:CreateSecurityGroup 上的 all AWS resources
- 操作：ec2:CreateNetworkInterface 上的 all AWS resources

AWSOutpostsPrivateConnectivityPolicy_ ***outpostID*** 策略 AWS Outposts 允许对指定资源完成以下操作：

- 操作：all AWS resources that match the following Condition: 上的 ec2:AuthorizeSecurityGroupIngress

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- 操作：ec2:AuthorizeSecurityGroupEgress 上的 all AWS resources that match the following Condition:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- 操作：ec2:CreateNetworkInterfacePermission 上的 all AWS resources that match the following Condition:

```
{ "StringLike" : { "ec2:ResourceTag/outposts:private-connectivity-resourceId" :
 "OutpostID" }} and { "StringEquals" : { "ec2:Vpc" : "vpcArn" }}
```

- 操作：`all AWS resources that match the following Condition:` 上的 `ec2:CreateTags`

```
{ "StringLike" : { "aws:RequestTag/outposts:private-connectivity-resourceId" :
 "{{OutpostId}}*"}}
```

必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为 AWS Outposts创建服务相关角色

您无需手动创建服务相关角色。在中为 Outpost 配置私有连接时 AWS Management Console， AWS Outposts 会为您创建服务相关角色。

有关更多信息，请参阅 使用 VPC 的服务链路私有连接。

为 AWS Outposts编辑服务相关角色

AWS Outposts 不允许您编辑 AWSServiceRoleForOutposts _ *outpostID* 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

删除 AWS Outposts的服务相关角色

如果您不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样，您就可以避免使用当前未监控或维护的未使用实体。但是，您必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果您尝试删除资源时 AWS Outposts 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

> **Warning**
>
> 必须先删除 Outpost，然后才能删除 AWSServiceRoleForOutposts _ *Outpost* ID 服务相关角色。以下步骤将删除您的 Outpost。

在开始之前，请确保没有使用 AWS Resource Access Manager (AWS RAM) 共享您的前哨基地。有关更多信息，请参阅 取消共享已共享的 Outpost 资源。

删除 AWSServiceRoleForOutposts _ ***ou*** tpostId 使用的 AWS Outposts 资源

- 请联系 AWS Enterprise Support 删除你的前哨基地。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForOutposts _ *outpostID* 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务相关角色。

AWS Outposts 服务相关角色的受支持区域

AWS Outposts 支持在提供服务的所有区域中使用服务相关角色。有关更多信息，请参阅 AWS Outposts 终端节点和限额。

AWS 的托管策略 AWS Outposts

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略： AWSOutpostsServiceRolePolicy

此策略附加到允许代表您执行操作 AWS Outposts 的服务相关角色。有关更多信息，请参阅 使用服务相关角色。

AWS 托管策略： AWSOutpostsPrivateConnectivityPolicy

此策略附加到允许代表您执行操作 AWS Outposts 的服务相关角色。有关更多信息，请参阅 使用服务相关角色。

AWS OutpostsAWS 托管策略的更新

查看 AWS Outposts 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。

更改	描述	日期
AWS Outposts 开始跟踪更改	AWS Outposts 开始跟踪其 AWS 托管策略的更改。	2019 年 12 月 3 日

中的基础设施安全 AWS Outposts

作为一项托管服务， AWS Outposts受到 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 AWS Outposts。客户端必须支持以下内容：

- 传输层安全性协议 (TLS)。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

有关为 Outpost 上运行的 EC2 实例和 EBS 卷提供的基础设施安全的更多信息，请参阅 Amazon EC2 中的基础设施安全。

VPC 流日志的功能与在 AWS 区域中的功能相同。这意味着它们可以发布到 CloudWatch 日志、Amazon S3 或亚马逊 GuardDuty 进行分析。需要将数据发送回该地区以发布到这些服务，因此，当 Outpost 处于断开连接状态时，这些数据无法从 CloudWatch 或其他服务中看到。

对设备进行篡改监 AWS Outposts 控

确保没有人对设备进行修改、改动、逆向工程或篡改。 AWS Outposts AWS Outposts 设备可能配备防篡改监控功能，以确保遵守AWS 服务条款。

韧性在 AWS Outposts

AWS Outposts 被设计为具有高可用性。Outpost 机架采用冗余电源和网络设备设计。为了提高弹性，建议您为 Outpost 提供双电源和冗余网络连接。

要获得高可用性，您可以在 Outpost 机架上预配置始终处于活动状态的额外内置容量。Outpost 容量配置专为在生产环境中运行而设计，并且在您为每个实例系列预配置容量后，每个实例系列均支持 N+1 个实例。 AWS 建议您为任务关键型应用程序分配足够的额外容量，以便在出现潜在主机问题时进行恢复和失效转移。您可以使用 Amazon CloudWatch 容量可用性指标和设置警报来监控应用程序的运行状况，创建 CloudWatch 操作来配置自动恢复选项，并监控 Outposts 随时间推移的容量利用率。

创建 Outpost 时，您可以从一个 AWS 区域中选择一个可用区。此可用区支持控制面板操作，例如响应 API 调用、监控 Outpost 和更新 Outpost 等。要从可用区提供的弹性中受益，您可以将应用程序部署到多个 Outpost 上，并将每个 Outpost 关联到不同的可用区。这样，您既能增强应用程序的弹性，又可避免依赖于单个可用区。有关区域和可用区的更多信息，请参阅AWS 全球基础设施。

您可以使用具有分布策略的置放群组来确保将实例放置到不同的 Outpost 机架上。这样做可以帮助减少相关的故障。有关更多信息，请参阅 Outpost 上的置放群组。

您可以使用 Amazon EC2 Auto Scaling 在 Outpost 中启动实例，并通过创建应用程序负载均衡器在实例之间分配流量。有关更多信息，请参阅在 AWS Outposts中配置应用程序负载均衡器。

合规性验证 AWS Outposts

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。

- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规性 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

AWS Outposts 工作负载的互联网接入

本节介绍 AWS Outposts 工作负载如何通过以下方式访问互联网：

- 通过父 AWS 区域
- 通过本地数据中心的网络

通过父 AWS 区域访问互联网

在此选项中，Outposts 中的工作负载通过服务链接访问互联网，然后通过父区域的互联网网关 (IGW) 访问互联网。 AWS 互联网的出站流量可以通过在您的 VPC 中实例化的 NAT 网关传输。为了进一步保护您的入口和出口流量，您可以 CloudFront 在该地区使用 AWS 安全服务 AWS WAF，例如 AWS Shield、和 Amazon。 AWS

有关 Outposts 子网上的路由表设置，请参阅本地网关路由表。

注意事项

- 在以下情况下使用此选项：
  - 您需要灵活地通过该 AWS 地区的多种 AWS 服务来保护互联网流量。
  - 您的数据中心或主机托管设施中没有互联网接入点。
- 在此选项中，流量必须穿过父 AWS 区域，这会带来延迟。
- 与 AWS 区域中的数据传输费用类似，从父可用区传输到前哨基地的数据会产生费用。要了解有关数据传输的更多信息，请参阅 Amazon EC2 按需定价。
- 服务链路带宽的利用率将提高。

下图显示了 Outposts 实例中的工作负载与通过父 AWS 区域的互联网之间的流量。

通过本地数据中心的网络访问互联网

在此选项中，驻留在 Outposts 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和本地出口。本地数据中心网络的安全层负责保护 Outposts 工作负载流量。

有关 Outposts 子网上的路由表设置，请参阅本地网关路由表。

注意事项

- 在以下情况下使用此选项：
  - 您的工作负载需要低延迟访问互联网服务。
  - 您希望避免产生数据传出 (DTO) 费用。
  - 您想为控制平面流量保留服务链路带宽。
- 你的安全层负责保护 Outposts 的工作负载流量。
- 如果您选择直接 VPC 路由 (DVR)，则必须确保 Outposts 的 CIDR 不会与本地 CIDR 冲突。
- 如果默认路由 (0/0) 通过本地网关 (LGW) 传播，则实例可能无法到达服务终端节点。或者，您可以选择 VPC 终端节点来访问所需的服务。

下图显示了 Outposts 实例中的工作负载与通过本地数据中心的互联网之间的流量。

监控您的 Outpost

AWS Outposts 与以下提供监控和日志记录功能的服务整合：

CloudWatch 指标

使用 Amazon CloudWatch 以一组有序的时间序列数据（称为指标）的形式检索有关您的 Outposts 数据点的统计数据。您可使用这些指标来验证您的系统是否按预期运行。有关更多信息，请参阅 CloudWatch 的指标 AWS Outposts。

CloudTrail 日志

使用 AWS CloudTrail 捕获有关向 AWS API 发出的调用的详细信息。您可以将这些调用作为日志文件存储在 Amazon S3 中。您可以使用这些 CloudTrail 日志来确定拨打了哪个电话、呼叫来自哪个源 IP 地址、谁拨打了电话以及何时拨打了呼叫等信息。

CloudTrail 日志包含有关调用 API 操作的信息AWS Outposts。它们还包含从 Outpost 上的服务（例如 Amazon EC2 和 Amazon EBS）调用 API 操作的信息。有关更多信息，请参阅 AWS Outposts信息在 CloudTrail。

Amazon VPC 流日志

使用 VPC 流日志来捕获有关往来于您的 Outpost 以及您的 Outpost 内的流量的详细信息。有关更多信息，请参阅《Amazon VPC 用户指南》中的 VPC 流日志。

流量镜像

使用流量镜像将网络流量从 Outpost 复制并转发到 Outpost 中的 out-of-band安全和监控设备。您可以使用镜像流量进行内容检查、威胁监控或故障排除。有关更多信息，请参阅 Amazon Virtual Private Cloud 的流量镜像指南。

AWS Health Dashboard

AWS Health Dashboard 会显示相关信息以及因 AWS 资源的运行状况变化所触发的通知。信息会以两种方式显示：在显示按类别组织的最近和未来事件的控制面板上，以及在显示过去 90 天内所有事件的完整事件日志中。例如，服务链路上的连接问题将引发一个事件，该事件将显示在控制面板和事件日志中，并在事件日志中保留 90 天。作为 AWS Health 服务的一部分，AWS Health Dashboard 不需要设置，您的账户中通过身份验证的任何用户都可以查看。有关更多信息，请参阅 AWS Health Dashboard 入门。

CloudWatch 的指标 AWS Outposts

AWS Outposts向亚马逊发布你的 Outp CloudWatch osts 的数据点。 CloudWatch 允许您以一组有序的时间序列数据（称为指标）的形式检索有关这些数据点的统计信息。可将指标视为要监控的变量，而将数据点视为该变量随时间变化的值。例如，您可以在指定时间段内监控 Outpost 的可用实例容量。每个数据点都有关联的时间戳和可选的测量单位。

您可使用指标来验证系统是否正常运行。例如，您可以创建 CloudWatch 警报来监控`ConnectedStatus`指标。如果平均指标小于`1`，则 CloudWatch 可以启动操作，例如向电子邮件地址发送通知。然后，您可以调查可能影响 Outpost 运行的本地或上行链路潜在网络问题。常见问题包括最近对防火墙和 NAT 规则的本地网络配置更改，或者互联网连接问题。对于 `ConnectedStatus` 问题，我们建议您在本地网络中验证与该 AWS 区域的连接；如果问题仍然存在，请联系 AWS 支持。

有关创建 CloudWatch 警报的更多信息，请参阅亚马逊 CloudWatch 用户指南中的使用亚马逊 CloudWatch警报。有关的更多信息 CloudWatch，请参阅 Amazon CloudWatch 用户指南。

内容

Outpost 指标

`AWS/Outposts` 命名空间包括以下指标。

`ConnectedStatus`

Outpost 服务链路连接的状态。如果平均统计数据小于 1，则连接受损。

单位：计数

最大分辨率：1 分钟

统计数据：最有用的统计工具是 `Average`。

维度：`OutpostId`

`CapacityExceptions`

实例启动时出现的容量不足错误数量。

单位：计数

最大分辨率：5 分钟

统计数据：最有用的统计工具为 Maximum 和 Minimum。

尺寸：InstanceType和 OutpostId

IfTrafficIn

Outposts 虚拟接口 (VIF) 从连接的本地网络设备接收的数据比特率。

单位：每秒比特数

最大分辨率：5 分钟

统计数据：最有用的统计工具为 Max 和 Min。

本地网关 VIF (lgw-vif) 的尺寸：、和 OutpostsId VirtualInterfaceGroupId VirtualInterfaceId

服务链接 VIF 的尺寸 (sl-vi f)：和 OutpostsId VirtualInterfaceId

IfTrafficOut

Outposts 虚拟接口 (VIF) 传输到连接的本地网络设备的数据比特率。

单位：每秒比特数

最大分辨率：5 分钟

统计数据：最有用的统计工具为 Max 和 Min。

本地网关 VIF (lgw-vif) 的尺寸：、和 OutpostsId VirtualInterfaceGroupId VirtualInterfaceId

服务链接 VIF 的尺寸 (sl-vi f)：和 OutpostsId VirtualInterfaceId

InstanceFamilyCapacityAvailability

可用实例容量的百分比。该指标不包括在 Outpost 上配置的任何专属主机的容量。

单位：百分比

最大分辨率：5 分钟

Statistics：最有用的统计工具是 Average 和 pNN.NN（百分比）。

尺寸：InstanceFamily和 OutpostId

InstanceFamilyCapacityUtilization

使用中实例容量的百分比。该指标不包括在 Outpost 上配置的任何专属主机的容量。

单位：百分比

最大分辨率：5 分钟

Statistics：最有用的统计工具是 Average 和 pNN.NN（百分比）。

维度：Account、InstanceFamily、和 OutpostId

InstanceTypeCapacityAvailability

可用实例容量的百分比。该指标不包括在 Outpost 上配置的任何专属主机的容量。

单位：百分比

最大分辨率：5 分钟

Statistics：最有用的统计工具是 Average 和 pNN.NN（百分比）。

尺寸：InstanceType和 OutpostId

InstanceTypeCapacityUtilization

使用中实例容量的百分比。该指标不包括在 Outpost 上配置的任何专属主机的容量。

单位：百分比

最大分辨率：5 分钟

Statistics：最有用的统计工具是 Average 和 pNN.NN（百分比）。

维度：Account、InstanceType、和 OutpostId

UsedInstanceType_Count

当前正在使用的实例类型数量，包括 Amazon Relational Database Service (Amazon RDS) 或应用程序负载均衡器等托管服务使用的任何实例类型。该指标不包括在 Outpost 上配置的任何专属主机的容量。

单位：计数

最大分辨率：5 分钟

维度：Account、InstanceType、和 OutpostId

`AvailableInstanceType_Count`

可用实例类型的数量。该指标不包括在 Outpost 上配置的任何专属主机的容量。

单位：计数

最大分辨率：5 分钟

尺寸：InstanceType和 OutpostId

`AvailableReservedInstances`

Outpost 上按需容量预留 (ODCR) 可用的实例数量。该指标不能衡量 Amazon EC2 预留实例。

单位：计数

最大分辨率：5 分钟

尺寸：InstanceType和 OutpostId

`UsedReservedInstances`

Outpost 上按需容量预留 (ODCR) 可用的实例数量。该指标不能衡量 Amazon EC2 预留实例。

单位：计数

最大分辨率：5 分钟

尺寸：InstanceType和 OutpostId

`TotalReservedInstances`

Outpost 上按需容量预留 (ODCR) 可用的实例数量。该指标不能衡量 Amazon EC2 预留实例。

单位：计数

最大分辨率：5 分钟

尺寸：InstanceType和 OutpostId

EBSVolumeTypeCapacityUtilization

使用中的 EBS 卷类型容量的百分比。

单位：百分比

最大分辨率：5 分钟

Statistics：最有用的统计工具是 Average 和 pNN.NN（百分比）。

尺寸：VolumeType和 OutpostId

EBSVolumeTypeCapacityAvailability

可用的 EBS 卷类型容量的百分比。

单位：百分比

最大分辨率：5 分钟

Statistics：最有用的统计工具是 Average 和 pNN.NN（百分比）。

尺寸：VolumeType和 OutpostId

EBSVolumeTypeCapacityUtilizationGB

用于 EBS 卷类型的千兆字节数。

单位：千兆字节

最大分辨率：5 分钟

Statistics：最有用的统计工具是 Average 和 pNN.NN（百分比）。

尺寸：VolumeType和 OutpostId

EBSVolumeTypeCapacityAvailabilityGB

EBS 卷类型的可用容量的千兆字节数。

单位：千兆字节

最大分辨率：5 分钟

Statistics：最有用的统计工具是 Average 和 pNN.NN（百分比）。

尺寸：VolumeType和 OutpostId

Outpost 指标维度

要筛选您的 Outpost 的指标，可以使用以下维度。

维度	描述
Account	使用容量的账户或服务。
InstanceFamily	实例系列。
InstanceType	实例类型。
OutpostId	Outpost 的 ID。
VolumeType	EBS 卷的类型。
VirtualInterfaceId	本地网关或服务链路虚拟接口 (VIF) 的 ID。
VirtualInterfaceGroupId	本地网关虚拟接口 (VIF) 的虚拟接口组的 ID。

查看前哨基地的 CloudWatch 指标

您可以使用 CloudWatch 控制台查看负载均衡器的 CloudWatch 指标。

使用 CloudWatch 控制台查看指标

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择指标。
3. 选择 Outpost 命名空间。
4. （可选）要跨所有维度查看某个指标，请在搜索框中输入其名称。

使用 AWS CLI 查看指标

使用以下 list-metrics 命令列出可用指标。

```
aws cloudwatch list-metrics --namespace AWS/Outposts
```

使用 AWS CLI 获取指标的统计数据

使用以下get-metric-statistics命令获取指定指标和维度的统计信息。 CloudWatch 将每个唯一的维度组合视为一个单独的指标。您无法使用未专门发布的维度组合检索统计数据。您必须指定创建指标时使用的同一维度。

```
aws cloudwatch get-metric-statistics --namespace AWS/Outposts \
--metric-name InstanceTypeCapacityUtilization --statistics Average  --period 3600 \
--dimensions Name=OutpostId,Value=op-01234567890abcdef \
Name=InstanceType,Value=c5.xlarge \
--start-time 2019-12-01T00:00:00Z --end-time 2019-12-08T00:00:00Z
```

使用 AWS CloudTrail 记录 AWS Outposts API 调用

AWS Outposts与AWS CloudTrail一项服务集成，该服务提供用户、角色或AWS服务在中执行的操作的记录AWS Outposts。 CloudTrail 将所有 API 调用捕获AWS Outposts为事件。捕获的调用包含来自 AWS Outposts 控制台和代码的 AWS Outposts API 操作调用。如果您创建了跟踪，则可以启用向 S3 存储桶持续传输事件，包括的事件AWS Outposts。 CloudTrail 如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向哪个请求发出AWS Outposts、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

有关的更多信息 CloudTrail，请参阅《AWS CloudTrail用户指南》。

AWS Outposts信息在 CloudTrail

CloudTrail 在您创建AWS账户时已在您的账户上启用。当活动发生在中时AWS Outposts，该活动会与其他AWS服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史查看 CloudTrail 事件。

要持续记录 AWS 账户中的事件（包括 AWS Outposts 的事件），请创建跟踪。跟踪允许 CloudTrail 将日志文件传送到父存储桶中的 S3 存储桶AWS 区域。默认情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 S3 存储桶。此外，您可以配置其他AWS服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- Overview for creating a trail
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail

- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail日志文件

所有AWS Outposts操作都由记录 CloudTrail。它们记录在 AWS Outposts API 参考中。例如，对CreateOutpostGetOutpostInstanceTypes、和ListSites操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于确定发出的请求是否：

- 使用根或用户凭证。
- 使用角色或联合身份用户的临时安全凭证。
- 由另一 AWS 服务 发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 AWS Outposts 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件表示来自任何源的单个请求。它包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该CreateOutpost操作的 CloudTrail 日志条目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AKIAIOSFODNN7EXAMPLE:jdoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/example/jdoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AKIAIOSFODNN7EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/example",
                "accountId": "111122223333",
                "userName": "example"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-08-14T16:28:16Z"
            }
        }
    },
    "eventTime": "2020-08-14T16:32:23Z",
    "eventSource": "outposts.amazonaws.com",
    "eventName": "SetSiteAddress",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "SiteId": "os-123ab4c56789de01f",
        "Address": "***"
    },
    "responseElements": {
        "Address": "***",
        "SiteId": "os-123ab4c56789de01f"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Outpost 维护

这适用于区域 AWS Outposts，就像适用于 AWS 区域一样。例如， AWS 管理安全补丁、更新固件和维护 Outpost 设备。 AWS 还可以监控 Outpost 的性能、运行状况和指标，并确定是否需要进行任何维护。

> **Warning**
>
> 如果底层磁盘驱动器出现故障，或者实例停止、休眠或终止，则实例存储卷上的数据将会丢失。为防止数据丢失，我们建议您将实例存储卷上的长期数据备份到持久性存储上，例如 Amazon S3 存储桶、Amazon EBS 卷或本地网络中的网络存储设备。

内容

硬件维护

如果 AWS 检测到托管在您的 Outpost 上运行的 Amazon EC2 实例的硬件存在无法弥补的问题，我们将通知前哨的所有者和实例的所有者，受影响的实例已计划停用。有关更多信息，请参阅 Amazon EC2 用户指南中的实例停用。

Outpost 所有者和实例所有者可以协同解决问题。实例所有者可以停止和启动受影响的实例，以将其迁移到可用容量。实例所有者可以在方便时停止和启动受影响的实例。否则，将在实例 AWS 停用日期停止并启动受影响的实例。如果 Outpost 上没有额外的容量，则实例将保持已停止状态。Outpost 所有者可以尝试腾出已用容量或请求为 Outpost 增加容量，以便顺利完成迁移。

如果需要硬件维护， AWS 将联系Outpost站点的经理，以确认 AWS 安装团队访问的日期和时间。最快可以在站点经理与 AWS 团队沟通后两个工作日内安排上门服务。

当 AWS 安装团队到达现场时，他们将更换运行状况不佳的主机、交换机或机架元件，并将新容量联机。他们不会在现场进行任何硬件诊断或维修。如果要更换主机，他们将移除并销毁符合 NIST 要求的物理安全密钥，有效地粉碎硬件上可能遗留的所有数据。如此可确保没有数据离开您的站点。如果要更换 Outpost 网络设备，则当设备从站点移走时，其上可能会存在网络配置信息。这些信息可能包括 IP 地址和 ASN，它们用于建立虚拟接口以配置通往本地网络或返回区域的路径。

固件更新

更新 Outpost 固件通常不会影响您的 Outpost 上的实例。在极少数情况下，我们需要重启 Outpost 设备才能安装更新。对于使用该容量运行的任何实例，您将收到相应的实例停用通知。

网络设备维护

Outpost 网络设备 (OND) 的维护不会影响 Outpost 的常规运营和流量。如果需要维护，则流量将从 OND 转移出去。您可能会注意到 BGP 通告中出现临时变化，例如 AS-Path 预置，也可能会发现 Outpost 上行链路上的流量模式出现相应变化。发生 OND 固件更新时，您可能会注意到 BGP 抖动。

建议您对客户网络设备进行相应配置，以便在不更改 BGP 属性的情况下接收 Outpost 的 BGP 通告，并启用 BGP 多路径/负载均衡来实现最佳的入站流量。AS-Path 预置用于本地网关前缀，以便在需要维护时将流量从 OND 转移出去。客户网络应首选 AS-Path 长度为 1 的 Outpost 路由，而不是 AS-Path 长度为 4 的路由。

客户网络应向所有 OND 通告具有相同属性的同等 BGP 前缀。默认情况下，Outpost 网络对所有上行链路之间的出站流量执行负载均衡。如果需要维护，Outpost 一侧使用路由策略将流量从 OND 转移出去。这种流量转移需要客户端在所有 OND 上使用相同的 BGP 前缀。如果客户网络需要维护，建议您使用 AS-Path 预置来临时转移特定上行链路的流量组。

AWS Outposts 电源和网络事件的最佳实践

正如 AWS Outposts 客户AWS 服务条款中所述，Outposts设备所在的设施必须满足最低的电力和网络要求，以支持Outposts设备的安装、维护和使用。只有在电源和网络连接不间断的情况下，Outposts机架式才能正常运行。

电源事件

在完全停电的情况下，存在 AWS Outposts 资源无法自动恢复服务的固有风险。除了部署冗余电源和备用电源解决方案外，我们还建议您提前完成以下步骤，以减轻某些恶劣情况的影响：

- 使用基于 DNS 或机架外负载均衡更改，以受控方式将您的服务和应用程序从 Outpost 设备上移出。

- 以有序的增量方式停止容器、实例和数据库，并在恢复服务时使用相反的顺序。
- 测试受控地移动或停止服务的计划。
- 备份关键的数据和配置，并将其存储在 Outpost 之外。
- 尽可能减少停电时间。
- 在维护期间，避免重复开关电源（关-开-关-开）。
- 在维护时段内留出额外时间来处理意外情况。
- 通过传达比您通常需求更长的维护时段来管理用户和客户的期望。

网络连接事件

网络维护完成后，您的 Outpost 和 Region 或 Outposts 主区域之间的服务链接连接通常会自动从您的上游公司网络设备或任何第三方连接提供商的网络中可能发生的网络中断或问题中恢复。 AWS 在服务链路连接中断期间，您的 Outpost 操作仅限于本地网络活动。

有关更多信息，请参阅 AWS Outposts 机架常见问题页面上的以下问题：当我的设施的网络连接中断时会发生什么？。

如果由于现场电源问题或网络连接中断而导致服务链路中断，则会向拥有 Outposts 的账户 AWS Health Dashboard 发送通知。即使预计会出现中断，您也 AWS 无法抑制服务链路中断的通知。有关更多信息，请参阅 AWS Health 用户指南中的开始使用 AWS Health Dashboard。

如果计划中的服务维护会影响网络连接，请采取以下主动措施来限制潜在问题情景的影响：

- 如果您的 Outposts 机架通过 Internet 或公共 Direct Connect 连接到父 AWS 区域，则在计划维护之前，请捕获一条跟踪路线。获得正常运行（网络维护前）的网络路径和存在问题（网络维护后）的网络路径以识别差异，将有助于进行故障排除。如果您将维护后问题上报给 AWS 或您的 ISP，则可以包含此信息。

  捕获以下地址之间的 trace-route：

  - Outpost 位置的公有 IP 地址和 `outposts.region.amazonaws.com` 返回的 IP 地址。将`##`替换为父 AWS 区域的名称。
  - 父区域中具有公共互联网连接的实例和 Outpost 位置上的公有 IP 地址。
- 如果网络维护由您掌控，请限制服务链路的停机时间。在维护过程中加入一个步骤，以验证网络是否已恢复。
- 如果网络维护不由您掌控，请监控与通告的维护时段相关的服务链路停机时间。如果在通告的维护时段结束时服务链路还未恢复，请尽早上报给负责计划网络维护的一方。

资源

以下是一些与监控相关的资源，可以确保 Outpost 在发生计划内或计划外的电力或网络事件后正常运行：

- AWS 博客监控最佳实践 AWS Outposts涵盖了Out posts特有的可观察性和事件管理最佳实践。
- Amazon VPC 网络连接调试工具 AWS博客解释了 AWSSupport-setuPip MonitoringFrom VPC 工具。此工具是一个 AWS Systems Manager 文件（SSM 文件），可用于在您指定的子网中创建 Amazon EC2 监控实例并监控目标 IP 地址。该文档运行 ping、MTR、TCP 跟踪路径和跟踪路径诊断测试，并将结果存储在 Amazon CloudWatch Logs 中，这些结果可以在 CloudWatch 控制面板中可视化（例如延迟、丢包）。对于 Outposts 监控，监控实例应位于父 AWS 区域的一个子网中，并配置为使用其私有 IP 监控您的一个或多个 Outpost 实例，这将提供与父区域之间的 AWS Outposts 丢包图表和延迟。 AWS
- 部署自动化 Amazon CloudWatch 控制面板以供 AWS Outposts 使用的 AWS博客 AWS CDK描述了部署自动控制面板所涉及的步骤。
- 如果您有任何疑问或需要更多信息，请参阅 AWS 支持用户指南中的创建支持案例。

优化 Amazon EC2 AWS Outposts

与之形成鲜明对比的是 AWS 区域，前哨基地上的亚马逊弹性计算云 (Amazon EC2) 容量是有限的。您受到所订购计算容量总额的限制。本主题提供了最佳实践和优化策略，以帮助您充分利用您在 AWS Outposts中的 Amazon EC2 容量。

内容

Outpost 上的专属主机

Amazon EC2 专属主机是指 EC2 实例容量完全转供您专用的物理服务器。Outpost 为您提供了专属硬件，但有了专属主机，即使现有的软件许可证存在针对单一主机的按插槽、核心或虚拟机许可的限制，您也利用这些许可证。有关更多信息，请参阅 Amazon EC2 用户指南 AWS Outposts中的专用主机。对于 Windows，请参阅 Amazon EC2 用户指南 AWS Outposts中的开启专用主机。

除了许可外，Outpost 所有者还可以通过两种方式使用专属主机来优化其 Outpost 部署中的服务器：

- 更改服务器的容量布局
- 在硬件级别上控制实例置放

更改服务器的容量布局

专用主机使您无需联系 AWS Support即可更改 Outpost 部署中的服务器布局。为 Outpost 购买容量时，您需要指定每台服务器提供的 EC2 容量布局。每台服务器支持单个实例类型系列。一种布局可以提供单个或多个实例类型。专属主机允许您更改为初始布局选定的任何内容。如果您分配一台主机来支持将单一实例类型用于全部容量，则只能从该主机启动一种实例类型。下图显示了一台具有同构布局的 m5.24xlarge 服务器：

您可以分配相同容量来支持多个实例类型。当您分配一台主机以支持多种实例类型时，您会得到一个不需要明确容量布局的异构布局。下图显示了一台采用异构布局来支持全部容量的 m5.24xlarge 服务器：

有关更多信息，请参阅 Amazon EC2 用户指南中的分配专用主机或分配专用主机 Amazon EC2 用户指南。

在硬件级别上控制实例置放

您可以使用专属主机在硬件级别控制实例置放。通过对专属主机使用自动置放，您可以管理启动的实例是在特定主机上启动，还是在具有匹配配置的任何可用主机上启动。使用主机关联在实例和专属主机之间建立关系。如果您有 Outpost 机架，则可以使用这些专属主机功能来最大限度地减少相关硬件故障的影响。有关实例恢复的更多信息，请参阅 Amazon EC2 用户指南中的了解自动放置和关联性或了解自动放置和关联性 Amazon EC2 用户指南。

您可以使用共享专用主机 AWS Resource Access Manager。通过共享专属主机，您可以在 AWS 账户范围内分配 Outpost 部署中的主机。有关更多信息，请参阅 使用共享的资源。

设置实例恢复

Outpost 上的实例由于硬件故障而进入运行不正常状态时，必须迁移到运行正常的主机上。您可以设置自动恢复，以根据实例状态检查来自动完成迁移。有关更多信息，请参阅恢复您的 Linux 实例或恢复您的 Windows 实例。

Outpost 上的置放群组

AWS Outposts 支持置放群组。使用置放群组来影响 Amazon EC2 应如何尝试将您启动的彼此依赖的实例群组放置到底层硬件上。您可以使用不同的策略（集群、分区或分布）来满足不同工作负载的需求。如果您有单机架 Outpost，则可以使用分布策略将实例放置到主机上，而不是机架上。

分布置放群组

使用分布置放群组，在不同的硬件上分配单个实例。通过在分布置放群组中启动实例，可以降低在实例位于同一设备中时同时出现故障的风险。置放群组可以跨机架或主机分布实例。您只能将主机级别的分布置放群组与一起使用 AWS Outposts。

机架级别分布置放群组

您的机架分布级置放群组可以容纳与 Outpost 部署中机架数量一样多的实例。下图显示了一个三机架 Outpost 部署，该部署在一个机架分布级置放群组中运行三个实例。

主机分布级别置放群组

您的主机分布级置放群组可以容纳与 Outpost 部署中的主机数量一样多的实例。下图显示了一个单机架 Outpost 部署，该部署在一个主机分布级置放群组中运行三个实例。

分区置放群组

使用分区置放群组，在含有分区的机架上分配多个实例。每个分区可以容纳多个实例。您可以使用自动分配将实例分布到各个分区，或将实例部署到目标分区。下图显示了采用自动分配的分区置放群组。

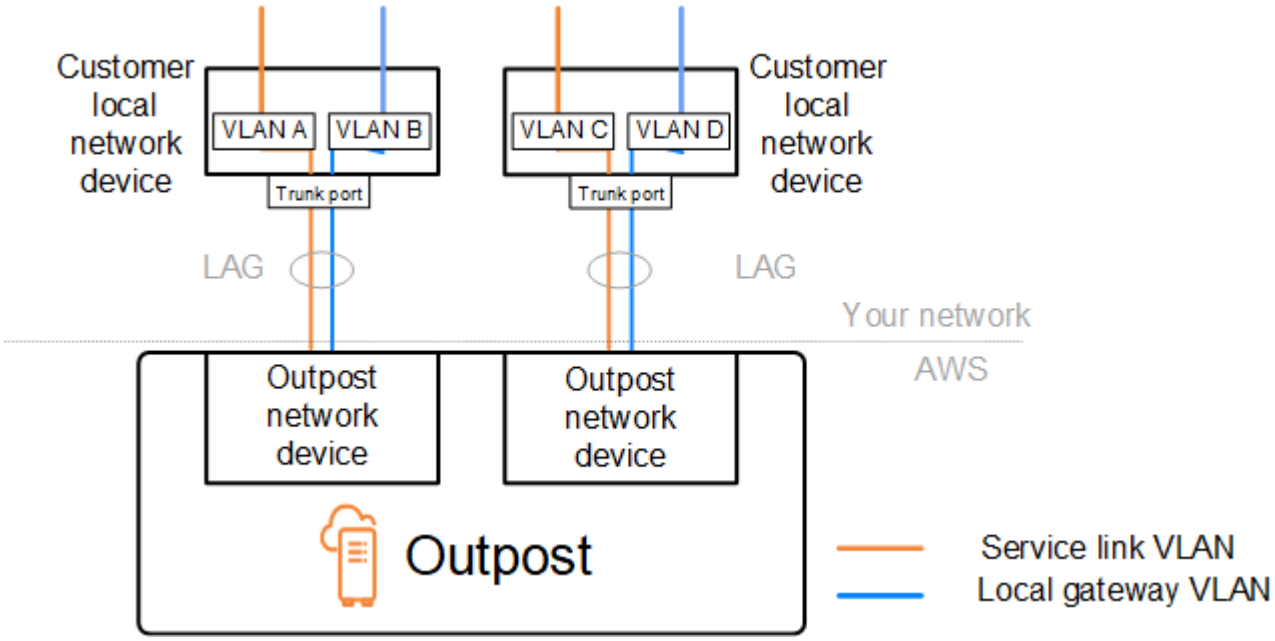
您也可以将实例部署到目标分区。下图显示了具有目标分配的分区置放群组。

有关使用置放群组的更多信息，请参阅 Amazon EC2 用户指南 AWS Outposts中的置放群组和置放群组。对于 Windows，请参阅 Amazon EC2 用户指南 AWS Outposts中的置放群组和置放群组。

有关 AWS Outposts 高可用性的更多信息，请参阅AWS Outposts 高可用性设计和架构注意事项。

AWS Outposts 机架网络故障排除清单

利用这份核对清单来帮助对 DOWN 状态的服务链路进行故障排除。



与 Outpost 网络设备的连接

检查连接到 Outpost 网络设备的客户本地网络设备上的 BGP 对等互连状态。如果 BGP 对等互连状态为 DOWN，请按照以下步骤操作：

1. 从客户设备上 ping Outpost 网络设备上的远程对等 IP 地址。您可以在设备的 BGP 配置中找到对等 IP 地址。还可以参阅安装时提供给您的 网络就绪性核对清单。
2. 如果 ping 失败，请检查物理连接并确保连接状态为 UP。
   a. 确认客户本地网络设备的 LACP 状态。
   b. 检查设备上的接口状态。如果状态为 UP，请跳到第 3 步。
   c. 检查客户的本地网络设备，并确认光纤模块工作正常。
   d. 更换有问题的光纤，并确保指示灯 (Tx/Rx) 在可接受的范围内。
3. 如果 ping 成功，请检查客户的本地网络设备，并确保以下 BGP 配置正确无误。
   a. 确认本地自治系统号（客户 ASN）配置正确无误。
   b. 确认远程自治系统号（Outpost ASN）配置正确无误。
   c. 确认接口 IP 和远程对等 IP 地址配置正确无误。
   d. 确认通告和接收的路由正确无误。
4. 如果您的 BGP 会话在活动状态和连接状态之间抖动，请确认客户本地网络设备上的 TCP 端口 179 和其他相关的临时端口均未被阻止。
5. 如果需要进一步排除故障，请在客户的本地网络设备上检查以下几项：

a. BGP 和 TCP 调试日志

b. BGP 日志

c. 数据包捕获

6. 如果问题仍然存在，请执行从 Outpost 连接的路由器到 Outpost 网络设备对等 IP 地址的 MTR/traceroute/数据包捕获。使用您的企业 AWS 支持计划与 Support 共享测试结果。

如果客户本地网络设备和 Outpost 网络设备之间的 BGP 对等互连状态为 UP，但服务链路仍然是 DOWN 状态，您可以通过检查客户本地网络设备上的以下设备来进一步排除故障。根据服务链路链接的预配置方式，参考以下核对清单之一。

- 连接的边缘路由器 AWS Direct Connect — 用于服务链路连接的公共虚拟接口。有关更多信息，请参阅 AWS Direct Connect 与 AWS 区域的公共虚拟接口连接。
- 连接的边缘路由器 AWS Direct Connect -用于服务链路连接的私有虚拟接口。有关更多信息，请参阅 AWS Direct Connect 与 AWS 区域的私有虚拟接口连接。
- 与互联网服务提供商 (ISP) 连接的边缘路由器 — 用于服务链路连接的公共互联网。有关更多信息，请参阅 与 AWS 区域的 ISP 公共互联网连接。

AWS Direct Connect 与 AWS 区域的公共虚拟接口连接

使用公共虚拟接口进行服务链路连接 AWS Direct Connect 时，使用以下清单对与之连接的边缘路由器进行故障排除。

1. 确认直接与 Outpost 网络设备连接的设备是通过 BGP 接收服务链路 IP 地址范围的。
   a. 确认通过 BGP 从您的设备接收的路由。
   b. 检查服务链路虚拟路由和转发实例 (VRF) 的路由表。路由表应该显示正在使用 IP 地址范围。
2. 为确保区域连接，请检查路由表中的服务链路 VRF。它应包括 AWS 公有 IP 地址范围或默认路由。
3. 如果您未在服务链接 VRF 中收到 AWS 公有 IP 地址范围，请检查以下各项。
   a. 检查来自边缘路由器或的 AWS Direct Connect 链路状态 AWS Management Console。
   b. 如果物理链路是 UP，请从边缘路由器检查 BGP 对等互连状态。
   c. 如果 BGP 对等互连状态为DOWN，则 ping 对等 AWS IP 地址并检查边缘路由器中的 BGP 配置。有关更多信息，请参阅AWS Direct Connect 用户指南 AWS Direct Connect中的故障排除和AWS 控制台中我的虚拟接口 BGP 状态已关闭。我应该怎么办？。
   d. 如果 BGP 已建立，但您在 VRF 中看不到默认路由或 AWS 公有 IP 地址范围，请使用您的企业 AWS 支持计划与 Support 联系。

4. 如果您有本地防火墙，请检查以下各项。
   a. 确认网络防火墙中允许使用服务链路连接所需要的端口。对端口 443 运行 traceroute 或使用任何其他网络故障排除工具，确认通过防火墙和您的网络设备的连接。您需要在防火墙策略中为服务链路连接配置以下端口。
      - TCP 协议 — 源端口：TCP 1025-65535；目标端口：443。
      - UDP 协议 — 源端口：TCP 1025-65535；目标端口：443。
   b. 如果防火墙处于状态状态，请确保出站规则允许 Outpost 的服务链接 IP 地址范围指向 AWS 公有 IP 地址范围。有关更多信息，请参阅 AWS Outposts 与 AWS 区域的连接。
   c. 如果防火墙不是状态的，请确保也允许入站流（从 AWS 公有 IP 地址范围到服务链接 IP 地址范围）。
   d. 如果您在防火墙中配置了虚拟路由器，请确保为 Outpost 和 AWS 区域之间的流量配置了适当的路由。
5. 如果您在本地网络中配置了 NAT 以将 Outpost 的服务链路 IP 地址范围转换为您自己的公有 IP 地址，请检查以下各项。
   a. 确认 NAT 设备没有过载，并且有可用端口可以分配给新会话。
   b. 确认 NAT 设备已正确配置了地址转换。
6. 如果问题仍然存在，请执行从边缘路由器到对 AWS Direct Connect 等 IP 地址的 MTR/traceroute / 数据包捕获。使用您的企业 AWS 支持计划与 Support 共享测试结果。

AWS Direct Connect 与 AWS 区域的私有虚拟接口连接

当使用私有虚拟接口进行服务链路连接 AWS Direct Connect 时，使用以下清单对与之连接的边缘路由器进行故障排除。

1. 如果 Outpost 机架和 AWS 区域之间的连接使用 AWS Outposts 私有连接功能，请检查以下各项。
   a. 从边缘路由器 Ping 远程对等 AWS IP 地址并确认 BGP 对等互连状态。
   b. 确保您的服务链路终端节点 VPC 和本地安装的 Outpost 之间的 AWS Direct Connect 私有虚拟接口上的 BGP 对等是。UP有关更多信息，请参阅《AWS Direct Connect 用户指南》 AWS Direct Connect中的故障排除，AWS 控制台中我的虚拟接口 BGP 状态已关闭。我应该怎么办？，以及如何通过 Direct Connect 解决 BGP 连接问题？。
   c. AWS Direct Connect 私有虚拟接口是与您所选 AWS Direct Connect 位置的边缘路由器的私有连接，它使用 BGP 交换路由。您的私有虚拟私有云 (VPC) CIDR 范围将通过此 BGP 会话通告到边缘路由器。同样，Outpost 服务链路的 IP 地址范围也将通过 BGP 从边缘路由器通告到该区域。

d. 确认与 VPC 中的服务链路私有端点关联的网络 ACL 允许相关的流量。有关更多信息，请参阅 网络就绪性核对清单。

e. 如果您有本地防火墙，请确保防火墙制定了相应的出站规则，来允许服务链路 IP 地址范围以及位于 VPC 或 VPC CIDR 中的 Outpost 服务端点（网络接口 IP 地址）。确保 TCP 1025-65535 和 UDP 443 端口未被阻止。有关更多信息，请参阅AWS Outposts 私有连接简介。

f. 如果防火墙不是有状态的，请确保防火墙制定了相应的规则和策略，允许从 VPC 中的 Outpost 服务端点到 Outpost 的入站流量。

2. 如果您的本地网络中有 100 个以上的网络，则可以通过 BGP 会话将默认路由通告到 AWS 您的私有虚拟接口。如果您不想通告默认路由，请通过汇总路由来使通告的路由数少于 100。

3. 如果问题仍然存在，请执行从边缘路由器到对 AWS Direct Connect 等 IP 地址的 MTR/traceroute / 数据包捕获。使用您的企业 AWS 支持计划与 Support 共享测试结果。

与 AWS 区域的 ISP 公共互联网连接

使用公共互联网实现服务链路连接时，请参考以下核对清单对通过 ISP 连接的边缘路由器进行故障排除。

- 确认互联网链路已连通。
- 确认可以从通过 ISP 连接的边缘设备访问公共服务器。

如果无法通过 ISP 链路访问互联网或公共服务器，请完成以下步骤。

1. 检查与 ISP 路由器的 BGP 对等互连状态是否是已建立。

   a. 确认 BGP 没有抖动。

   b. 确认 BGP 正在接收并通告来自 ISP 的必要路由。

2. 如果是静态路由配置，请检查边缘设备上的默认路由配置是否正确。

3. 确认您是否可以使用其他 ISP 连接来连入互联网。

4. 如果问题仍然存在，请在边缘路由器上执行 MTR/traceroute/数据包捕获。将结果分享给 ISP 的技术支持团队，以便进一步排除故障。

如果无法通过 ISP 链路访问互联网和公共服务器，请完成以下步骤。

1. 确认是否可以从边缘设备访问您在 Outpost 主区域中的任何可公开访问的 EC2 实例或负载均衡器。您可以使用 ping 或 telnet 来确认连接，然后使用 traceroute 来确认网络路径。

2. 如果您使用 VRF 来分隔网络中的流量，请确认服务链路 VRF 是否有路由或策略可以定向传入和传出 ISP（互联网）和 VRF 的流量。请参阅以下检查点。
   a. 与 ISP 连接的边缘路由器。检查边缘路由器的 ISP VRF 路由表，以确认服务链路 IP 地址范围是否存在。
   b. 与 Outpost 连接的客户本地网络设备。检查 VRF 的配置，以确保正确配置了服务链路 VRF 和 ISP VRF 之间连接所需的路由和策略。通常，从 ISP VRF 向服务链路 VRF 发送一条默认路由，来用于传输到互联网的流量。
   c. 如果您在连接到 Outpost 的路由器中配置了基于来源的路由，请确认配置是否正确。
3. 确保将本地防火墙配置为允许从 Outpost 服务链接 IP 地址范围到公有 IP 地址范围的出站连接（TCP 1025-65535 和 UDP 443 端口）。 AWS 如果防火墙不是有状态的，请确保还配置了与 Outpost 的入站连接。
4. 确保在本地网络中配置 NAT，以将 Outpost 的服务链路 IP 地址范围转换为公有 IP 地址。此外，也请确认以下各项。
   a. NAT 设备没有过载，并且有可用端口可以分配给新会话。
   b. NAT 设备已正确配置了地址转换。

如果问题仍然存在，请执行 MTR/traceroute/数据包捕获。

- 如果结果显示数据包在本地网络中丢失或被阻止，请联系您的网络或技术团队以获取更多指导。
- 如果结果显示数据包在 ISP 的网络中丢失或被阻止，则请与 ISP 的技术支持团队联系。
- 如果结果未显示任何问题，请收集所有测试的结果（例如 MTR、telnet、traceroute、数据包捕获和 BGP 日志），然后使用您的企业支持计划联系 AWS 支持部门。

Outposts 位于两台防火墙设备后面

如果您将 Outpost 置于一对高可用性的同步防火墙或两个独立防火墙后面，则可能会出现服务链路的非对称路由。这意味着入站流量可能通过防火墙 1，而出站流量可以通过 firewall-2。使用以下清单来识别服务链路的潜在非对称路由，尤其是在服务链路之前运行正常的情况下。

- 验证公司网络的路由设置最近是否有任何更改或持续维护，这些更改或维护可能导致服务链路通过防火墙进行非对称路由。
  - 使用防火墙流量图表来检查流量模式的变化，这些变化是否与服务链接问题开始时一致。
  - 检查是否存在部分防火墙故障或防火墙对分裂的情况，这些情况可能导致您的防火墙不再相互同步其连接表。

  - 检查公司网络中是否出现链路中断或最近的路由更改（OSPF/ISIS/EIGRP 指标更改、BGP 路由映射更改），这些更改与服务链路问题的开始一致。
- 如果您使用公共 Internet 连接作为通往本区域的服务链接，则服务提供商的维护可能会导致服务链路通过防火墙进行非对称路由。
  - 查看流量图表中是否有指向您的 ISP 的链接，以了解与服务链接问题开始时相应的流量模式变化。
- 如果您使用服务链路的 AWS Direct Connect 连接，则 AWS 计划维护可能会触发服务链路的非对称路由。
  - 查看您的 AWS Direct Connect 服务是否有计划维护的通知。
  - 请注意，如果您有冗余 AWS Direct Connect 服务，则可以在维护条件下主动测试 Outposts 服务链接在每条可能的网络路径上的路由。这使您可以测试某项服务的中断是否会导致 AWS Direct Connect 服务链路的非对称路由。 end-to-end 网络连接 AWS Direct Connect 部分的弹性可以通过 “弹性与 AWS Direct Connect 弹性” 工具包进行测试。有关更多信息，请参阅使用 AWS Direct Connect 弹性工具包测试弹性-故障转移测试。

在仔细阅读了前面的清单并确定了服务链路的非对称路由可能是根本原因之后，您可以采取许多进一步的措施：

- 恢复对称路由，方法是恢复对称路由，方法是恢复对称路由，方法是恢复对称路由。
- 登录到一个或两个防火墙，并从命令行清除所有流的所有流状态信息（如果防火墙供应商支持）。
- 通过其中一个防火墙临时过滤掉 BGP 公告，或者关闭一个防火墙上的接口，以强制对称路由通过另一个防火墙。
- 依次重新启动每个防火墙，以消除防火墙内存中服务链路流量的流量状态跟踪中可能出现的损坏。
- 请您的防火墙供应商验证或放松对源自端口 443 且目的地为端口 443 的 UDP 连接的 UDP 流状态的跟踪。

AWS Outposts end-of-term 选项

在任 AWS Outposts 期结束时，你有三种选择：

- 续订订阅并保留现有的 Outpost。
- 结束订阅并准备归还您的 Outpost 机架。
- 转换为 month-to-month 订阅并保留您现有的 Outpost。

主题

续订订阅

要续订订阅并保留现有的 Outpost，请执行以下操作：

在 Outpost 期限结束前至少 30 天完成以下步骤：

1. 登录 AWS Support 服务中心控制台。
2. 选择创建案例。
3. 选择账户和账单。
4. 对于服务，选择账单。
5. 对于类别，选择其他账单问题。
6. 对于严重性，选择重要问题。
7. 选择 Next step: Additional information（下一步：其他信息）。
8. 在其他信息页面的主题中，输入您的续订请求，例如 **`Renew my Outpost subscription`**。
9. 在描述中，输入以下付款选项之一：
    - 无预付款
    - 预付部分费用
    - 预付全部费用

有关定价，请参阅 AWS Outposts 机架定价。您也可以请求报价。

10. 选择下一步：立即解决或联系我们。
11. 在 Contact us（联系我们）页面上，选择您的首选语言。
12. 选择您的首选联系方式。
13. 检查工单详细信息，然后选择 Submit（提交）。此时将显示您的案例 ID 号和摘要。

AWS Customer Support 将启动订阅续订流程。新的订阅将在当前订阅结束后的第二天开始。

如果您没有表示要续订订阅或退还Outpost机架，则系统将自动转换为订 month-to-month 阅。您的 Outpost 将按与您的 AWS Outposts 配置相对应的 “无预付款” 付款选项的费率每月续订。新的月度订阅将在当前订阅结束后的第二天开始。

结束订阅并准备归还机架

> **Important**
>
> AWS 在您完成以下步骤之前，无法开始退货流程。在您提交支持案例以终止订阅后，我们无法停止归还流程。

要结束订阅：

在 Outpost 期限结束前至少 30 天完成以下步骤：

1. 登录 AWS Support 服务中心控制台。
2. 选择创建案例。
3. 选择账户和账单。
4. 对于服务，选择账单。
5. 对于类别，选择其他账单问题。
6. 对于严重性，选择重要问题。
7. 选择 Next step: Additional information（下一步：其他信息）。
8. 在其他信息页面的主题中，输入明确的请求，例如 **`End my Outpost subscription`**。
9. 在描述中，输入您希望归还 Outpost 的日期。
10. 选择下一步：立即解决或联系我们。

11. 在 Contact us（联系我们）页面上，选择您的首选语言。
12. 选择您的首选联系方式。
13. 检查工单详细信息，然后选择 Submit（提交）。此时将显示您的案例 ID 号和摘要。

AWS Customer Support 将与您联系以协调取回事宜。

要准备好退 AWS Outposts 货架，请执行以下操作：

> **Important**
>
> 在到达现场进行定期检索之前，请勿关闭 Out AWS post 机架的电源。

1. 如果 Outpost 的资源已共享，则必须取消共享这些资源。

   您可以通过以下方式之一取消共享 Outpost 资源：

   - 使用控制 AWS RAM 台。有关更多信息，请参阅 AWS RAM 用户指南中的更新资源共享。
   - 使用运行 AWS CLI 取消关联资源共享命令。

   有关可共享的 Outpost 资源列表，请参阅可共享的 Outpost 资源。
2. 终止与 Outpost 上的子网关联的活动实例。要终止实例，请按照 Amazon EC2 用户指南中终止您的实例中的说明进行操作。

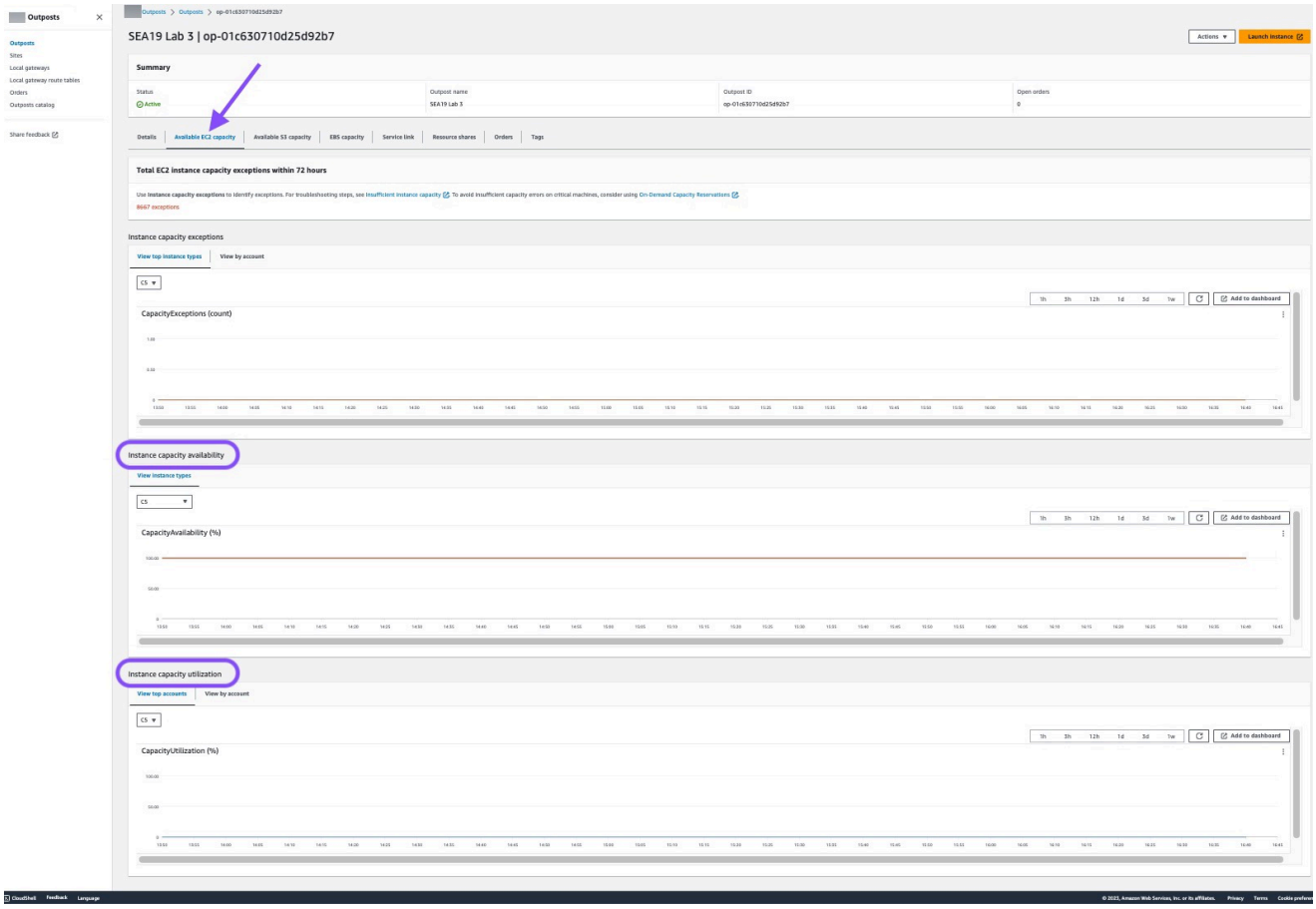
   > **Note**
   >
   > 在您的 Out AWS post 上运行的某些托管服务，例如应用程序负载均衡器或 Amazon 关系数据库服务 (RDS) Service，会消耗 EC2 容量。但是，它们的关联实例在 Amazon EC2 控制面板上不可见。您必须终止与这些服务相关的资源以释放容量。有关更多信息，请参阅为什么我的 Outpost 上缺少某些 EC2 实例容量？ 。
3. 在您的 AWS 账户 instance-capacity-availability 中验证您的 Amazon EC2 实例。

   a. 打开 AWS Outposts 控制台，网址为 https://console.aws.amazon.com/outposts/。
   b. 选择 Outpost。
   c. 选择您要归还的特定 Outpost。
   d. 在 Outpost 页面上，选择可用 EC2 容量选项卡。

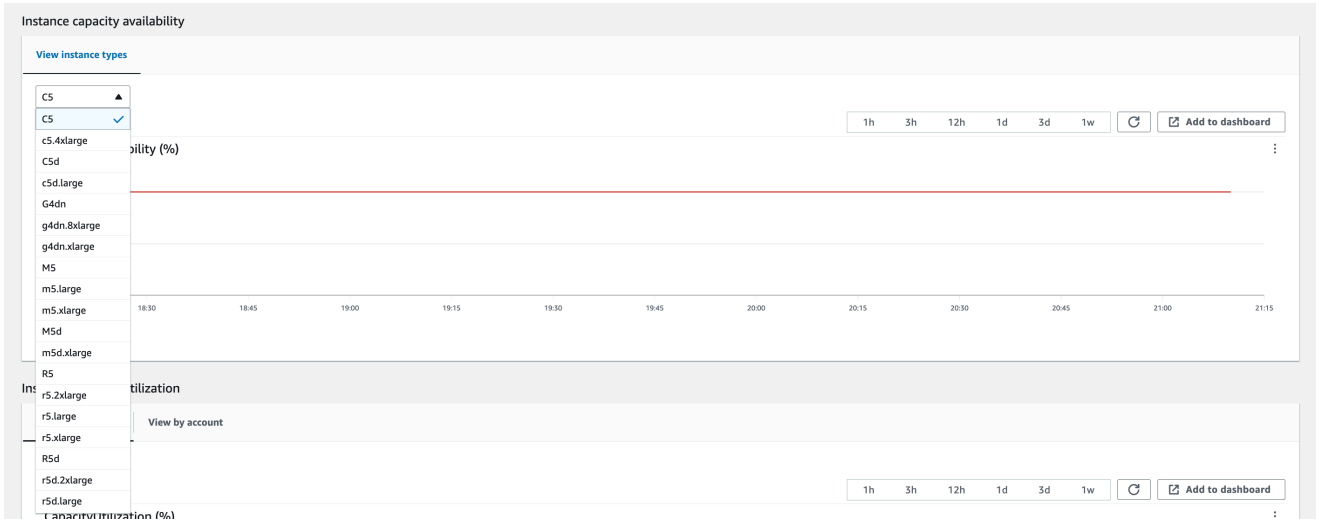
e. 确保每个实例系列的实例容量可用性均为 100%。

f. 确保每个实例系列的实例容量利用率均为 0%。

下图显示了可用 EC2 容量选项卡上的实例容量可用性和实例容量利用率图表。



下图显示了实例类型的列表。



4. 为您的 Amazon EC2 实例和服务器卷创建备份。要创建备份，请按照 AWS 规范性指南中使用 EBS 卷备份和恢复 Amazon EC2 中的说明进行操作。
5. 删除与您的 Outpost 关联的 Amazon EBS 卷。
   a. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
   b. 在导航窗格中，选择卷。
   c. 选择操作和删除卷。
   d. 在确认对话框中，选择删除。
6. 如果在 Outpost 拥有 Amazon S3，请删除 Outpost 上的所有本地快照。
   a. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
   b. 在导航窗格中，选择快照。
   c. 选择带有 Outpost ARN 的快照。
   d. 选择操作和删除快照。
   e. 在确认对话框中，选择删除。
7. 删除与您的 Outpost 关联的所有 Amazon S3 存储桶。要删除存储桶，请参照 Amazon Simple Storage Service 用户指南中删除 Outpost 存储桶上的 Amazon S3的说明。
8. 删除与您的 Outposts 关联的所有 VPC 关联和客户拥有的 IP 地址池 (CoIP) CIDR。

救 AWS 援小组将关闭机架的电源。Nitro 安全密钥关闭后，你可以销毁 AWS Nitro 安全密钥，也可以由 AWS 检索小组代表你销毁。

转换为订 month-to-month 阅

要转换为 month-to-month 订阅并保留现有的 Outpost，无需采取任何行动。如果您有任何疑问，请打开账单支持案例。

您的 Outpost 将按与您的 AWS Outposts 配置相对应的 “无预付款” 付款选项的费率每月续订。新的月度订阅将在当前订阅结束后的第二天开始。

AWS Outposts 的配额

对于每个 AWS 服务，您的 AWS 账户 都具有默认配额（以前称为“限制”）。除非另有说明，否则，每个配额是区域特定的。您可以请求增加某些配额，但并非所有配额都能增加。

要查看 AWS Outposts 的限额，请打开服务限额控制台。在导航窗格中，选择 AWS 服务，然后选择 AWS Outposts。

要请求提高配额，请参阅 Service Quotas 用户指南中的请求增加配额。

您的 AWS 账户 具有以下与 AWS Outposts 相关的配额。

资源	默认值	可调整	注释
Outpost 站点	100	是	Outpost 站点是客户管理的物理建筑，您可以在其中为 Outpost 设备供电并将其附加到网络。 AWS 账户的每个区域可以拥有 100 个 Outpost 站点。
每个站点的 Outpost	10	是	AWS Outposts 包括硬件和虚拟资源，统称为 Outpost。此配额限制了您的 Outpost 虚拟资源。 每个 Outpost 站点可以包含 10 个 Outpost。

AWS Outposts 和其他服务的配额

AWS Outposts 依赖于其他服务的资源，这些服务可能有自己的默认配额。例如，您的本地网络接口配额来自网络接口的 Amazon VPC 配额。

文档历史记录

下表介绍了 AWS Outposts 用户指南 的重要更改。

变更	说明	日期
容量管理	您可以修改新 Outposts 订单的默认容量配置。	2024年4月16日
AWS Outposts rack 支持服务链路接口吞吐量指标	现在，您可以通过利用`IfTrafficIn` 和指标来监控 Outpost 机架服务链路虚拟接口 (VIF) 和本地网络设备之间的吞吐量使用情况。`IfTrafficOut` Amazon CloudWatch	2023 年 11 月 17 日
AWS Outposts 通过本地网关进行 VPC 内部通信	您可以使用本地网关，在不同 Outpost 的同一 VPC 中的子网之间建立通信。	2023 年 8 月 30 日
AWS Outposts 机架的 E nd-of-term 选项	在 AWS Outposts 期限结束时，您可以续订、终止或转换您的订阅。	2023 年 8 月 1 日
Outposts 上的 Amazon Route 53 已在机架上 AWS Outposts 线。	Outpost 上的 Amazon Route 53 包括一个解析程序，用于缓存来自 AWS Outposts 的所有 DNS 查询。在部署入站和出站端点时，您还可以在 Outpost 和本地 DNS 解析程序之间设置混合连接。	2023 年 7 月 20 日
本地网关入站路由	您可以在 Outpost 上创建和修改通往弹性网络接口的本地网关入站路由。	2022 年 9 月 15 日

引入直接 VPC 路由 AWS Outposts	使用 VPC 中实例的私有 IP 地址来促进与本地网络的通信。	2022 年 9 月 14 日
为 Outposts 机架创建了 AWS Outposts 用户指南	AWS Outposts 《用户指南》针对机架和服务器分成了单独的指南。	2022 年 9 月 14 日
创建和管理本地网关路由表	创建和修改本地网关路由表和 CoIP 池。管理 VIF 群组关联。	2022 年 9 月 14 日
置放群组已开启 AWS Outposts	采用分布策略的置放群组可以在主机之间分配实例。	2022 年 6 月 30 日
开启专用主机 AWS Outposts	您现在可以在 Outpost 上使用专属主机了。	2022 年 5 月 31 日
共享的 Outpost 站点	创建和管理 Outpost 网站，并与组织中的其他 AWS 账号共享。	2021 年 10 月 18 日
新 CloudWatch 维度	AWS Outposts 命名空间中指标的新 CloudWatch 维度。	2021 年 10 月 13 日
共享 S3 存储桶	在您的 Outpost 上共享和管理 S3 存储桶。	2021 年 8 月 5 日
支持某些置放群组	您可以如同在区域中一样使用集群、分区或分布放置策略。	2021 年 7 月 28 日
其他 CloudWatch 指标	预留实例还有其他 CloudWatch 指标可用。	2021 年 5 月 24 日
网络故障排除核对清单	提供了一份网络故障排除核对清单。	2021 年 2 月 22 日
其他 CloudWatch 指标	还提供了 EBS 卷的其他 CloudWatch 指标。	2021 年 2 月 2 日
控制台订购更新	更新了控制台订购流程。	2021 年 1 月 14 日

私有连接	在 AWS Outposts 控制台中创建 Outpost 时，您可以为其配置私有连接。	2020 年 12 月 21 日
网络就绪性核对清单	在收集 Outpost 配置的信息时，您可以使用网络就绪性核对清单。	2020 年 10 月 28 日
共享 AWS Outposts 资源	通过 Outpost 共享，Outpost 所有者可以与同一组织下的其他 AWS 账户共享他们的 Outposts 和 Outpost 资源，包括本地网关路由表。 AWS	2020 年 10 月 15 日
其他 CloudWatch 指标	实例类型计数的其他 CloudWatch 指标可用。	2020 年 9 月 21 日
其他 CloudWatch 指标	还有一个服务链路连接状态的额外 CloudWatch 指标可用。	2020 年 9 月 11 日
支持共享客户拥有的 IPv4 地址	AWS Resource Access Manager 用于共享客户拥有的 IPv4 地址。	2020 年 4 月 20 日
其他 CloudWatch 指标	还提供了 EBS 卷的其他 CloudWatch 指标。	2020 年 4 月 4 日
初始版本	这是的初始版本 AWS Outposts。	2019 年 12 月 3 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。