适用于 Outposts 服务器的用户指南

AWS Outposts

AWS Outposts: 适用于 Outposts 服务器的用户指南

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 APIs、服务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 实例和子网等 AWS 资源时指定子网。Outpost 子网中的实例使用私有 IP 地址与 AWS 区域中的其他实例通信，全部都在相同 VPC 内进行。

> **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。你可以从 AWS Outposts 控制台查看和管理前哨基地的容量。 AWS Outposts 支持自助服务容量管理，您可以在 Outposts 级别进行定义，以重新配置 Outposts 中的所有资产，或者专门针对每项资产重新配置。Outpost 资产可以是 Outposts 机架中的一台服务器，也可以是 Outposts 服务器。
- 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。Outposts 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。
- 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。Outposts 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。

- 前哨站所有者-下 AWS Outposts 订单的账户的账户所有者。在与 AWS 客户互动后，所有者可能会包括其他联系人。 AWS 将与联系人沟通，以明确订单、安装预约以及硬件维护和更换。如果联系信息发生变化，请联系 AWS 支持 Center。
- 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，可实现 Outposts 机架与您的本地网络之间的通信。
- 本地网络接口 – 一种网络接口，可实现 Outposts 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

资源类型	机架	服务器
Amazon EMR 集群	 是	 否
Amazon RDS 数据库实例	 是	 否

Networking

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

仓储服务

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

定价

定价基于您的订单详情。下订单时，您可以从各种 Outpost 配置中进行选择，每种配置都提供 Amazon EC2 实例类型和存储选项的组合。您还可以选择合同期限和付款方式。定价包括以下内容：

- Outposts 机架 – 交付、安装、基础设施服务维护、软件补丁和升级以及机架拆除。
- Outposts 服务器 – 交付、基础设施服务维护以及软件补丁和升级。您负责服务器的安装和包装以备退货。

您需要为共享资源以及从 AWS 该地区传输到前哨基地的任何数据付费。您还需要为维护可用性和安全 AWS 性的数据传输付费。

有关基于地点、配置和付款方式的定价，请参阅：

- Outposts 机架定价
- 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地区的广域网 (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。

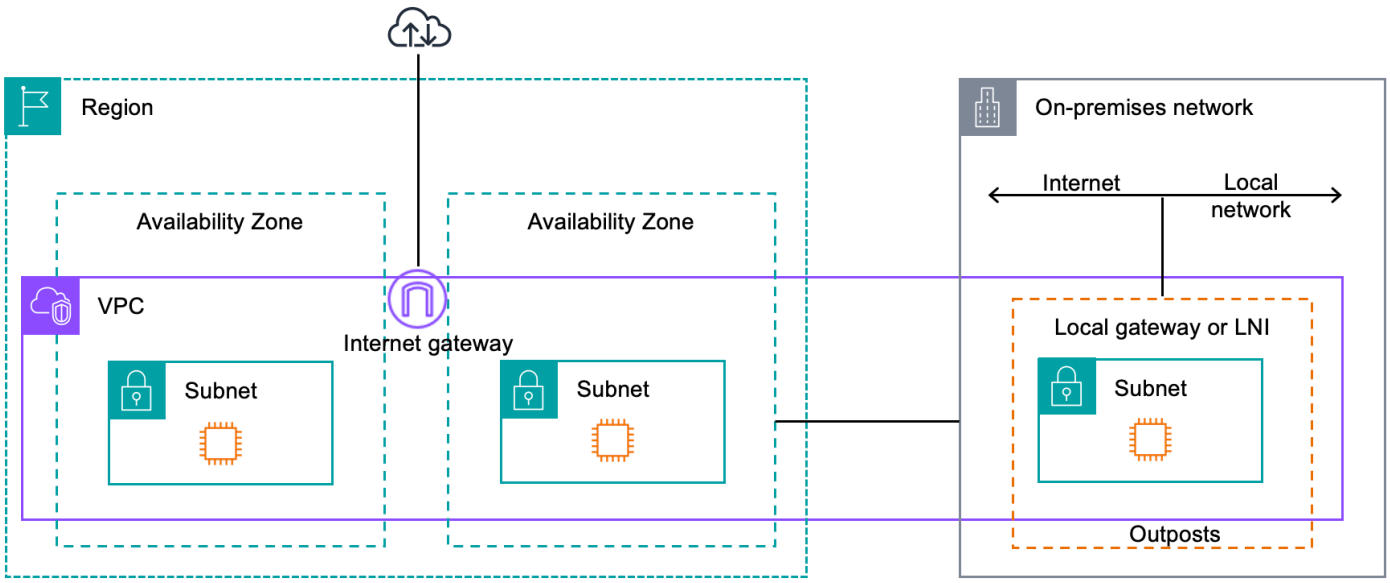
内容

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
- 前哨基地和本地网络之间的连接提供：
  - 对于 Outposts 机架：本地网关
  - 对于 Outposts 服务器：本地网络接口 (LNI)



VPCs 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。

每个前哨基地可以支持多个 VPCs 可以有一个或多个前哨子网。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。

  如果您在同一个前哨站 VPCs 上与多个前哨站建立了对等连接，则两者之间的流量 VPCs 仍保留在前哨基地中，并且不会使用返回该地区的服务链接。

DNS

对于连接到 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 Outposts 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：

-

- 《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

Outposts 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。你不能使用来自 Outposts 机架或区域内 EC2 实例的本地网络接口。AWS 本地网络接口仅适用于本地位置。有关更多信息，请参阅 Outposts 服务器的本地网络接口。

Outposts 服务器的站点要求

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 服务器 FAQs。参考以下问题：Outpost 服务器在哪些国家和地区可用？

本页介绍了 Outpost 服务器的要求。有关 Outposts 机架的要求，请参阅《适用于 Outposts 机架的 AWS Outposts 用户指南》中的 Outposts 机架的站点要求。

内容

设施

如下是服务器的设施要求。

> **Note**
>
> 这些规格适用于正常运行条件下的服务器。例如，初始安装过程中的噪音可能会比较大，但在安装完毕后会以额定声功率运行。

- 温度 — 环境温度必须介于 41 到 95°F（5 到 35°C）之间。

  温度超出此范围时服务器会关机，温度回到此范围内时服务器会重启。
- 湿度 — 相对湿度必须介于 8% 到 80% 之间，且无冷凝。
- 空气质量-必须使用 MERV8 （或更高的）过滤器过滤空气。
- 气流 — 服务器所在位置必须确保服务器与前后墙壁之间至少有 6 英寸（15 厘米）的间隙，以留出足够的气流间隙。
- 重量 — 1U 服务器的重量为 26 磅，2U 服务器则为 36 磅。确认您打算放置服务器的位置可以承受服务器的重量。

  要查看不同 Outposts 资源的重量要求，请在 AWS Outposts 控制台中选择浏览目录，网址为。https://console.aws.amazon.com/outposts/

- 导轨套件兼容性 — 运输包装中包含的导轨套件与符合 EIA-310-D 标准的 19 英寸机架的标准 L 形安装支架兼容。导轨套件与 U 形安装支架不兼容，如下图所示。

- 机架放置 – 我们建议使用标准的 19 英寸 EIA-310D 机架，其深度至少为 36 英寸（914 毫米）。AWS 提供用于机架式安装服务器的导轨套件。
  - Outposts 2U 服务器需要以下尺寸的空间：高 3.5 英寸（88.9 毫米），宽 17.5 英寸（447 毫米），深 30 英寸（762 毫米）
  - Outposts 1U 服务器需要以下尺寸的空间：高 1.75 英寸（44.45 毫米），宽 17.5 英寸（447 毫米），深 24 英寸（610 毫米）
  - 不支持垂直安装 AWS Outposts 服务器。
  - Outposts 1U 服务器的宽度与 Outposts 2U 服务器相同，但高度只有其一半，深度小一些

  如果不将服务器放置在机架上，则仍必须满足其他站点要求。
- 可维修性 — Outpost 服务器可在前通道上进行维修。
- 声学 — 温度 80°F（27°C）时的额定声功率低于 78 dBA，符合 GR-63 CORE NEBS 标准。
- 抗震支撑 — 在法律或法规要求的范围内，您应当安装和维护适当的抗震锚固和支撑，确保服务器在您的设施中的安全。
- 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）。
- 清洁 — 使用含有经批准的防静电清洁化学品的湿巾来擦拭表面。

Networking

每个 Outposts 服务器包括非冗余的物理上行链路端口。每个端口有自己的速度和连接器要求，具体如下方所示。

端口标签	Speed	上游网络设备上的连接器	交通
端口 3	10Gbe	SFP+	服务和 LNI 链路流量 — QSFP+ 分支线缆（10 英尺/3 米）分段流量。

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	1024-65535	服务链路 IP	53	DNS 服务器
UDP	443, 1024-65535	服务链路 IP	443	Outposts 服务链路端点
TCP	1024-65535	服务链路 IP	443	Outposts 注册端点

您可以使用连接或公共互联网 Direct Connect 连接将 Outpost 连接回该 AWS 地区。对于 Outposts 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。

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 服务器用户指南》中的 AWS Outposts 与 AWS 区域的连接。

服务链路带宽建议

为了获得最佳体验和弹性， AWS 要求您使用至少 500 Mbps 的冗余连接和最大 175 毫秒的往返延迟来回延迟，用于与该地区的服务链路连接。 AWS 每个 Outposts 服务器的最大利用率为 500 Mbps。要提高连接速度，请使用多个 Outposts 服务器。例如，如果您有三台 AWS Outposts 服务器，则最大连接速度会增加到 1.5 Gbps (1,500 Mbps)。有关更多信息，请参阅《AWS Outposts 服务器用户指南》中的服务器的服务链路流量。

您的 AWS Outposts 服务链路带宽要求因工作负载特征而异，例如 AMI 大小、应用程序弹性、突发速度需求以及流向该地区的 Amazon VPC 流量。请注意， AWS Outposts 服务器不进行缓存 AMIs。AMIs 每次启动实例时都会从该地区下载。

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。

电源

如下是 Outpost 服务器的电源要求。

要求

- 电源支持
- 功耗
- 电源线
- 电源冗余

电源支持

服务器的额定规格为最高 1600W 90-264 VaC 47/63 Hz 交流电。

功耗

要查看不同 Outposts 资源的功耗要求，请在 AWS Outposts 控制台中选择浏览目录，网址为。https://console.aws.amazon.com/outposts/

电源线

服务器随附一条 IEC C14-C13 电源线。

从服务器到机架的电源线连接

使用随附的 IEC C14-C13 电源线将服务器连接到机架。

从服务器到墙壁插座的电源线连接

要将服务器连接到标准墙壁插座上，必须使用适用于 C14 插座的适配器或特定于国家/地区的电源线。

确保您拥有适合所在地区的适配器或电源线，以节省服务器安装时间。

- 在美国，您需要一条 IEC C13 转 NEMA 5-15P 电源线。
- 在欧洲部分地区，您可能需要一条 IEC C13 转 CEE 7/7 的电源线。
- 在印度，你需要一根 IEC C13 来连接 IS1293 电线。

电源冗余

服务器配备多路电源连接，并随附相应电缆来实现电源冗余运行。我们建议部署电源冗余，但冗余不是强制要求。

服务器不附带不间断电源 (UPS)。

订单配送

为了履行订单， AWS 我们会将 Outposts 服务器设备（包括导轨支架以及所需的电源和网络电缆）运送到您提供的地址。服务器的装运箱子具有以下尺寸：

- 装有 2U 服务器的包装箱：
  - 长度：44 英寸/111.8 厘米
  - 高度：26.5 英寸/67.3 厘米
  - 宽度：17 英寸/43.2 厘米
- 装有 1U 服务器的包装箱：
  - 长度：34.5 英寸/87.6 厘米
  - 高度：24 英寸/61 厘米
  - 宽度：9 英寸/22.9 厘米

您的团队或第三方提供商必须安装设备。有关更多信息，请参阅《AWS Outposts 服务器用户指南》中的服务器的服务链路流量。

当您确认您的 AWS 账户中为 Outposts 服务器提供的 Amazon EC2 容量可以使用时，安装即告完成。

开始使用 Outposts 服务器

订购 Outposts 服务器以开始使用。安装 Outpost 设备后，启动 Amazon EC2 实例并配置与本地网络的连接。

任务

- 创建一个 Outpost 并订购 Outpost 容量
- 在 Outposts 服务器上启动实例

创建一个 Outpost 并订购 Outpost 容量

要开始使用 AWS Outposts，请使用您的 AWS 帐户登录。创建一个站点和一个 Outpost。然后，订购您需要的 Outpost 服务器。

先决条件

- 查看您的 Outpost 服务器的可用配置。
- 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 Outposts 服务器的站点要求。
- 您必须有 AWS 企业支持计划或 AWS 企业入口支持计划。
- 确定 AWS 账户 您将使用哪个网站来创建 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。操作地址是您安装和运行 Outpost 服务器的位置。创建网站后，为您的网站 AWS Outposts 分配一个 ID。在您创建 Outpost 时必须指定此站点。

先决条件

- 确定运营地址。

创建站点

1. 登录到 AWS。
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，选择仅限服务器。
7. 输入您的站点的名称、描述和运营地址。
8. （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。
9. 选择 Create site (创建站点)。

步骤 2：创建一个 Outpost

为每台服务器创建一个 Outpost。一个 Outpost 只能与一台服务器关联。您将在下订单时指定此 Outpost。

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 Servers (服务器)。
4. 输入 Outpost 的名称和说明。
5. 为您的 Outpost 选择可用区。
6. 对于站点 ID，请选择您的站点。
7. 选择创建 Outpost。

> **Note**
>
> 完成订单后，您将无法修改前哨基地的AZ锚点或实际位置。

步骤 3：下订单

订购所需的 Outposts 服务器。

> **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 AWS 支持 Center。

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。如果您选择部分预付或不预付的付款选项，您将在整个期限内按月支付费用。

  定价包括交付、基础设施服务维护以及软件修补程序和升级。
- 确定送货地址是否与您为网站指定的运营地址不同。

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，请选择服务器。
4. 要添加容量，请选择配置。
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

每个新 Outpost 订单的容量都配置了默认容量配置。您可以转换默认配置，创建各种实例来满足您的业务需求。为此，您需要创建一个容量任务，指定实例大小和数量，然后运行容量任务来执行更改。

> **Note**
>
> - 下单购买 Outposts 后，您可以更改实例的大小和数量。
> - 实例的大小和数量是在 Outpost 级别定义的。
> - 自动根据最佳实践下单实例。

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. 在开始使用页面上，选择订单。
4. 要修改容量，可使用控制台中的步骤或上传 JSON 文件。

Console steps

1. 选择修改新 Outpost 的容量配置。
2. 选择下一步。
3. 在配置实例容量页面上，每种实例类型都会显示一个预选了最大数量的实例大小。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，该消息会告知您是否超出或低于容量。在实例大小或数量级别进行调整，以优化总可用容量。
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末尾选择自动平衡。

7. 对于每种实例类型，确保至少为一种实例大小指定了实例数量。
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。

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。

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。如果您对订单有任何疑问，请联系 AWS 支持 Center。

为了配送订单， AWS 将安排交货日期。

您负责所有安装任务，包括物理安装和网络配置。您可以与第三方签订合同，让第三方替您完成这些任务。无论您是自己安装还是与第三方签订合同，安装都需要 AWS 账户 中的 IAM 凭证，其中包含 Outpost，用于验证新设备的身份。您负责提供和管理此访问权限。有关更多信息，请参阅服务器安装指南。

当 Outpost 的 Amazon EC2 容量可以通过您的 AWS 账户使用时，安装即告完成。容量可用后，您可以在 Outposts 服务器上启动 Amazon EC2 实例。有关更多信息，请参阅 the section called “启动实例”。

> **Note**
>
> 完成订单后，您将无法修改服务链接配置。

在 Outposts 服务器上启动实例

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。例如，您可以启动 Amazon EC2 实例。

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

- 步骤 1：创建子网
- 步骤 2：在 Outpost 上启动实例
- 步骤 3：配置连接
- 步骤 4：测试连接

步骤 1：创建子网

您可以将 Outpost 子网添加到 AWS 该区域的任何 VPC 作为前哨基地。执行此操作时，VPC 也会跨越 Outpost。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，请跳至步骤 2：在 Outpost 上启动实例。

创建一个 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 并为该子网指定 IP 地址范围。
5. 选择创建。
6. 创建子网后，必须为本地网络接口启用子网。在 AWS CLI中是 modify-subnet-attribute 命令。您必须在设备索引中指定网络接口的位置。在启用的 Outpost 子网中启动的所有实例都会使用此设备位置作为本地网络接口。下面的示例使用值 1 指定辅助网络接口。

```
aws ec2 modify-subnet-attribute \
    --subnet-id subnet-1a2b3c4d \
    --enable-lni-at-device-index 1
```

步骤 2：在 Outpost 上启动实例

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

- Outpost 服务器上的实例包括实例存储卷，但不包括 EBS 卷。选择具有足够实例存储空间的实例大小来满足应用程序需求。有关更多信息，请参阅《Amazon EC2 用户指南》中的实例存储卷和创建实例存储支持的 AMI。
- 您必须使用由亚马逊 EBS 支持的 AMI，且仅包含一个 EBS 快照。 AMIs 不支持多个 EBS 快照。
- 实例重启后会保留实例存储卷上的数据，但实例终止后不会保留这些数据。要在实例停用之后保留实例存储卷上的长期数据，请确保将数据备份到持久性存储中，例如 Amazon S3 存储桶或本地网络中的网络存储设备。
- 要使用由兼容的第三方存储支持的块数据或启动卷，您必须预配置和配置这些卷以与 Outposts 上的 EC2 实例配合使用。有关更多信息，请参阅 第三方块存储。
- 要将 Outpost 子网中的实例连接到您的本地网络，您必须添加本地网络接口，如以下过程所述。

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 服务器支持的实例类型。
5. 选择您的 Outposts 服务器支持的实例类型。请注意，显示为灰色的实例不可用。
6. （可选）您可以立即添加本地网络接口，也可以在创建实例之后添加。要立即添加，请展开高级网络配置并选择添加网络接口。选择 Outpost 子网。这将使用设备索引 1 为实例创建网络接口。如果指定 1 作为 Outpost 子网的本地网络接口设备索引，则此网络接口就是实例的本地网络接口。或者，要稍后添加，请参阅添加本地网络接口。
7. （可选）您可以添加第三方数据卷。
   a. 展开配置存储。在 “外部存储卷” 旁边，选择 “编辑”。
   b. 对于存储网络协议，请选择 iSCSI。

c. 输入启动器 IQN，然后添加外部存储阵列的目标 IP 地址、端口和 IQN。

8. 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》中的启动 EC2 实例。

步骤 3：配置连接

如果您在实例启动期间没有向实例添加本地网络接口，则必须立即这样做。有关更多信息，请参阅 添加本地网络接口。

您必须使用本地网络中的 IP 地址为实例配置本地网络接口。有关信息，请参阅实例上运行的操作系统的文档。您可以搜索有关配置其他网络接口和辅助 IP 地址的信息。

步骤 4：测试连接

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 实例的本地网络接口 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 EC2 实例的信息，请参阅《Amazon EC2 用户指南》中的连接到您的 EC2 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
```

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。

> **Note**
>
> 您不能将私有连接用于将 Outposts 服务器连接到您的 AWS 地区或 AWS Outposts 家乡地区的服务链接连接。

内容

通过服务链路进行连接

在 AWS Outposts 配置期间，您或 AWS 创建一个服务链接连接，将您的 Outposts 服务器连接到您选择的 AWS 地区或主区域。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。

Outpost 能够通过公共区域连接创建返回 AWS 区域的服务链路 VPN。为此，前哨基地需要通过公共互联网或 AWS Direct Connect 公共虚拟接口连接到该 AWS 地区的公共 IP 范围。这种连接可以通过服务链路 VLAN 中的特定路由或通过 0.0.0.0/0 的默认路由实现。有关公共范围的更多信息 AWS，请参阅 Amazon VPC 用户指南中的 AWS IP 地址范围。

建立服务链接后，前哨基地将投入使用并由其 AWS管理。服务链路用于以下流量：

- 通过服务链路管理 Outpost 的流量，包括内部控制面板流量、内部资源监控以及固件和软件更新。
- 前哨基地与任何相关人员之间的流量 VPCs，包括客户数据平面流量。

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）。

注意以下几点：

- 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
- 从 Outposts 中的实例到该区域实例的流量的 MTU 为 1300 字节，由于数据包开销，低于所需的 MTU（1500 字节）。

服务链路带宽建议

为了获得最佳体验和弹性， AWS 要求您使用至少 500 Mbps 的冗余连接和最大 175 毫秒的往返延迟来回连接与该地区的服务链路。 AWS 每个 Outposts 服务器的最大利用率为 500 Mbps。要提高连接速度，请使用多个 Outposts 服务器。例如，如果您有三 AWS Outposts 台服务器，则最大连接速度会增加到 1.5 Gbps（1,500 Mbps）。有关更多信息，请参阅服务器的服务链路流量。

您的 AWS Outposts 服务链路带宽要求因工作负载特征而异，例如 AMI 大小、应用程序弹性、突发速度需求以及流向该地区的 Amazon VPC 流量。请注意， AWS Outposts 服务器不进行缓存 AMIs。AMIs 每次启动实例时都会从该地区下载。

我们强烈建议您咨询您的 AWS 销售代表或 APN 合作伙伴，评估您所在地区可用的主区域选项，并就您的工作负载的服务链路带宽和延迟要求寻求定制建议。

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 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。

更新和服务链路

AWS 维护您的 Outposts 服务器与其父 AWS 区域之间的安全网络连接。这种网络连接称为服务链接，通过在前哨基地和地区之间提供VPC内部流量，对于管理前哨基地至关重要。 AWS AWS Well-Architected 最佳实践建议在两个 Outposts（位于采用主动-主动设计的不同可用区）上部署应用程序。有关更多信息，请参阅 AWS Outposts 高可用性设计和架构注意事项。

服务链路定期更新，以保持运行质量和性能。在维护期间，您可能会在该网络上看到短暂的延迟和数据包丢失，从而对依赖 VPC 连接到区域内托管资源的工作负载造成影响。不过，通过本地网络接口（LNI）的流量不会受到影响。您可以遵循 AWS Well-Architected 最佳实践，并确保您的应用程序能够抵御影响单个 Outposts 服务器的故障或维护活动，从而避免应用程序受到影响。

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。 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 Direct Connect 连接传送：

- 通过服务链路管理到 Outpost 的流量
- 前哨基地与任何相关联地点之间的交通 VPCs

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。

如果您使用同时支持 UDP 和 TCP 的状态防火墙来限制服务链路 VLAN 的连接，则可以拒绝所有入站连接。如果防火墙以状态方式运行，则从 Outposts 服务链接允许的出站连接应自动允许回复流量返回，而无需明确配置规则。只有从 Outpost 服务链接启动的出站连接才需要配置为允许。

协议	源端口	源地址	目的地端口	目标地址
UDP	1024-65535	服务链路 IP	53	DNS 服务器
UDP	443, 1024-65535	服务链路 IP	443	AWS Outposts 服务链接端点
TCP	1024-65535	服务链路 IP	443	AWS Outposts 注册端点

如果您使用非状态防火墙来限制服务链路 VLAN 的连接，则必须允许从 Outposts 服务链接启动的出站连接至该 AWS Outposts 地区的公共网络。您还必须明确允许回复流量从 Outposts 区域的公共网络进入服务链接 VLAN。连接始终从 Outposts 服务链路出站启动，但必须允许回复流量返回服务链接 VLAN。

协议	源端口	源地址	目的地端口	目标地址
UDP	1024-65535	服务链路 IP	53	DNS 服务器
UDP	443, 1024-65535	服务链路 IP	443	AWS Outposts 服务链接端点
TCP	1025-65535	服务链路 IP	443	AWS Outposts 服务链接端点
UDP	53	DNS 服务器	1025-65535	服务链路 IP
UDP	443	AWS Outposts 服务链接端点	443, 1024-65535	服务链路 IP
TCP	443	AWS Outposts 服务链接端点	1025-65535	服务链路 IP

> **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。

Outposts 服务器网络疑难解答

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。

初步评测

通过 Amazon CloudWatch 指标验证服务链接的状态：

1. 监控命 AWS Outposts 名空间中的ConnectedStatus指标。
2. 如果平均值小于 1，则确认服务链路受损。
3. 如果服务链路受损，请完成以下各节中的步骤以解决并重新建立连接。

步骤 1：检查物理连接

1. 确认您使用的是提供的 QSFP 分支电缆。如果问题仍然存在，请使用另一根 QSFP 分支电缆（如果有）进行测试。
2. 确认 Outposts 服务器中的 QSFP 分支电缆是否已牢固固定。
3. 验证电缆 1 (LNI) 是否已牢固地固定在交换机中。
4. 验证电缆 2（服务链路）是否牢固地安装在交换机中。
5. 完成一般交换机健全性检查，例如检查链路指示灯。

步骤 2：测试 Outposts 服务器与的连接 AWS

创建与 Outposts 服务器的串行连接并执行以下测试：

1. 测试链接。
   a. 如果成功，请继续下一次测试。
   b. 如果失败了，验证网络配置.
2. 测试 DNS 解析度。
   a. 如果成功，请继续下一次测试。
   b. 如果失败了，检查防火墙规则.
3. 测试该 AWS 地区的访问权限。
   a. 如果成功，请继续重新建立连接。
   b. 如果失败了，验证 MTU.

验证网络配置

确保您的交换机符合以下规格：

- 基本配置 — 服务链路端口必须是通往 VLAN 的未标记接入端口，该端口具有网关和通往 AWS 终端节点的路由。
- 链路速度-交换机端口必须将链路速度设置为 10 Gb，并且必须关闭自动协商。

验证 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 有关服务链接的更多信息，请参阅与AWS 区域的AWS Outposts 连接。

检查防火墙规则

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	1024-65535	服务链路 IP	53	DNS 服务器
UDP	443, 1024-65535	服务链路 IP	443	AWS Outposts 服务链接端点
TCP	1024-65535	服务链路 IP	443	AWS Outposts 注册端点

步骤 3：重新建立连接

如果之前的检查通过，但服务链接仍然存在DOWN（小ConnectedStatus于 1 英寸 CloudWatch），则按照使用 Outpost 配置工具授权 Outposts 服务器中的步骤重新建立连接。

> **Note**
>
> 如果服务链接仍然处于关闭状态，请在AWS 支持 中心创建案例。

归还 Outposts 服务器

> **Note**
>
> 如果您收到的服务器在运输过程中损坏，请参阅服务器安装指南中的步骤 2：检查 Outposts AWS Outposts 服务器设备。
> 要退回正在使用且要更换的服务器或订阅已结束的服务器，请查看本节。

如果 AWS Outposts 检测到服务器存在缺陷，我们会通知您，开始更换流程以向您发送一台新服务器，并通过 AWS Outposts 控制台为您提供退货标签。当您退回 Outposts 服务器时，您无需支付运费。但是，如果您退回的服务器已损坏，则可能会产生费用。

要开始归还，请完成以下步骤。

任务

- 步骤 1：为服务器做归还准备
- 第 2 步：打印退货标签
- 步骤 3：打包服务器
- 步骤 4：通过快递归还服务器

步骤 1：为服务器做归还准备

要为服务器做好归还准备，请取消共享资源、备份数据、删除本地网络接口并终止活动实例。

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。
   - AWS CLI 使用运行disassociate-resource-share命令。

   有关可共享的 Outpost 资源列表，请参阅可共享的 Outpost 资源。
2. 为存储在 AWS Outposts 服务器上运行的 Amazon 实例的 EC2 实例存储中的数据创建备份。
3. 删除与服务器上运行的实例关联的本地网络接口。

4. 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。
5. 销毁 Nitro 安全密钥 (NSK)，以加密方式粉碎服务器上的数据。要销毁 NSK，请按照加密方式粉碎服务器数据中的说明进行操作。

第 2 步：打印退货标签

> **Important**
>
> 您只能使用 AWS 提供的返回标签，因为它包含有关您要返回的服务器的特定信息，例如资产 ID。请勿创建自己的退货标签。

要获取退货标签，请执行以下操作：

1. 打开 AWS Outposts 控制台，网址为https://console.aws.amazon.com/outposts/。
2. 在导航窗格上，选择订单。
3. 选择要退回的服务器的顺序。
4. 在订单详情页面的订单状态部分，选择打印退货标签。

> **Note**
>
> 在当前订阅结束之前归还您的 Outposts 服务器不会终止与此 Outpost 相关的任何未付费用。

步骤 3：打包服务器

要打包服务器，请使用提供的包装盒和包装材料 AWS。

1. 用下面一种包装盒来打包服务器：

   - 服务器最初随附的包装盒和包装材料。
   - 更换服务器随附的包装盒和包装材料。

   或者，请联系 AWS 支持 中心申请包装盒。

2. 将 AWS 提供的退货标签粘贴在箱子外面。

> **Important**
>
> 验证退货标签上的资产 ID 是否与您要返回的服务器上的资产 ID 相匹配。
> 资产 ID 位于服务器正面的拉出式标签上。示例：1203779889 或 9305589922

3. 牢牢封住包装盒。

步骤 4：通过快递归还服务器

您必须通过您所在国家的指定快递公司归还服务器。您可以将服务器交付给快递员，也可以安排您希望快递员取货的日期和时间。 AWS 提供的退货标签包含返回服务器的正确地址。

下表显示了发货国家/地区的联系人：

Country	联系人
阿根廷	联络 AWS 支持 中心。在您的请求中，包含以下信息： • AWS提供的退货标签上的追踪编码 • 您希望快递员取件的日期和时间 • 联系人姓名 • 电话号码 • 电子邮件地址
巴林	
巴西	
文莱	
加拿大	
智利	
哥伦比亚	
中国香港	
印度	
印度尼西亚	
日本	

Country	联系人
马来西亚	
尼日利亚	
阿曼	
巴拿马	
秘鲁	
菲律宾	
塞尔维亚	
新加坡	
南非	
韩国	
中国台湾	
泰国	
阿拉伯联合酋长国	
越南	
墨西哥	AWS 联系德铁信可并请求从您所在地取件。然后，德铁信可与您联系以安排取货的日期和时间。

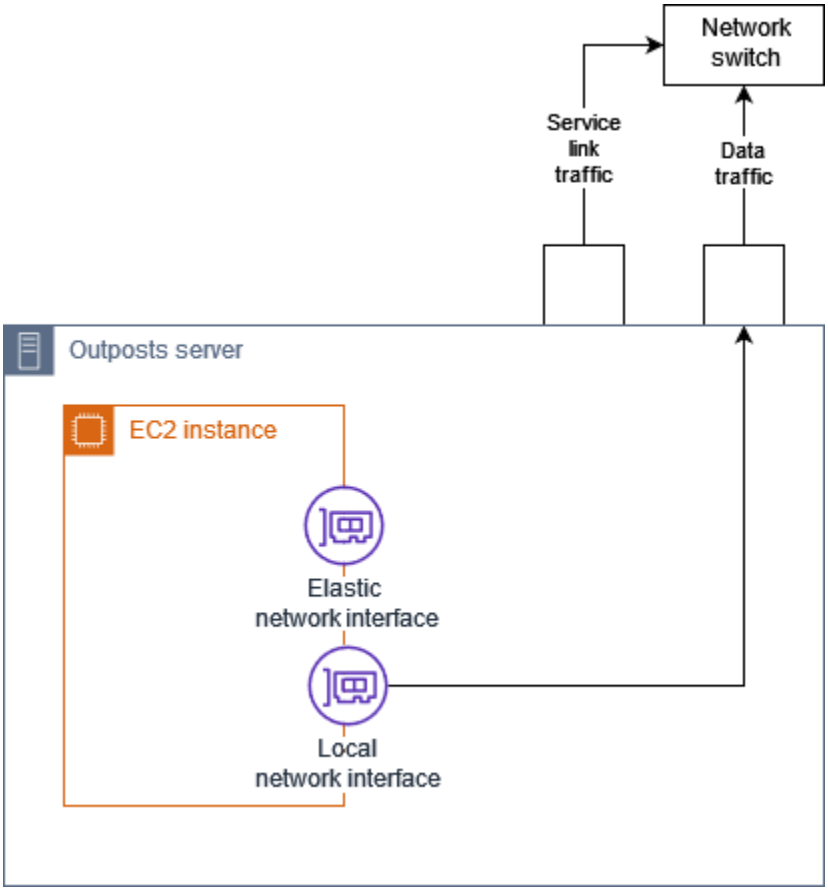
Country	联系人
United States of America	请联系 UPS。 您可以通过以下方式归还服务器： • 在所在地的 UPS 例行取件期间归还服务器。 • 将服务器送到 UPS 地点。 • 在您希望的日期和时间安排取件。输入 AWS 提供的退货标签上的追踪编码，即可享受免费配送。
所有其他国家	请联系 DHL。 您可以通过以下方式归还服务器： • 将服务器送到 DHL 地点。 • 在您希望的日期和时间安排取件。输入 AWS 提供的退货标签上的 DHL 运单编号，即可享受免费配送。 如果您收到以下错误 `Courier pickup can't be scheduled for an import shipment`，则通常意味着您选择的取件国家/地区与归还运输标签上的取件国家/地区不匹配。请选择发货的国家/地区，然后重试。

Outposts 服务器的本地网络接口

对于 Outposts 服务器，本地网络接口是一种逻辑网络组件，可将 Outposts 子网中的 Amazon EC2 实例连接到您的本地网络。

本地网络接口直接在您的局域网上运行。使用这种本地连接时，您无需路由器或网关即可与本地设备通信。本地网络接口的命名与网络接口或弹性网络接口类似。在提及本地网络接口时，我们始终使用本地接口来区分这两种接口。

在 Outpost 子网上启用本地网络接口后，您可以对 Outpost 子网中的 EC2 实例进行配置，使其除了弹性网络接口之外还包括本地网络接口。本地网络接口连接到本地网络，网络接口则连接到 VPC。下图显示了 Outpost 服务器上的 EC2 实例，该实例同时就有弹性网络接口和本地网络接口。



您必须配置操作系统，使本地网络接口能够在局域网上进行通信，就如您对待任何其他本地设备一样。您不能使用 VPC 中的 DHCP 选项集来配置本地网络接口，因为本地网络接口是在您的局域网上运行的。

弹性网络接口的工作方式与用于可用区子网中的实例的接口完全相同。例如，您可以使用 VPC 网络连接访问的公共区域终端节点 AWS 服务，也可以使用接口 VPC 终端节点 AWS 服务 进行访问 AWS PrivateLink。有关更多信息，请参阅 AWS Outposts 与 AWS 区域的连接。

内容

本地网络接口基础知识

本地网络接口提供对第二层物理网络的访问。VPC 是虚拟化的第三层网络。本地网络接口不支持 VPC 网络组件。这些组件包括安全组、网络访问控制列表、虚拟路由器或路由表以及流日志。本地网络接口不向 Outposts 服务器提供对 VPC 第三层流的可见性。实例的主机操作系统确实可以完全洞悉来自物理网络的帧。您可以将标准的防火墙逻辑应用于这些帧中的信息。但是，这种通信发生在实例内部，但超出了虚拟化结构的范围。

注意事项

- 本地网络接口支持 ARP 和 DHCP 协议。不支持常规的 L2 广播消息。
- 本地网络接口的配额来自您的网络接口配额。有关更多信息，请参阅《Amazon VPC 用户指南》中的网络接口配额。
- 每个 EC2 实例可以有一个本地网络接口。
- 本地网络接口不能使用实例的主网络接口。
- Outpost 服务器可以托管多个 EC2 实例，各自具有一个本地网络接口。

> **Note**
>
> 同一服务器内的 EC2 实例可以直接通信，无需将数据发送到 Outpost 服务器外面。这种通信包括通过本地网络接口或弹性网络接口传送的流量。

- 本地网络接口仅适用于在 Outposts 服务器上的 Outposts 子网中运行的实例。
- 本地网络接口不支持混杂模式或 MAC 地址欺骗。

性能

每个实例大小的本地网络接口提供部分 10 GbE 物理可用带宽。下表列出了每种实例类型的网络性能：

实例类型	基准带宽 (Gbps)	突增带宽（Gbps）
c6id.large	0.15625	2.5
c6id.xlarge	0.3125	2.5
c6id.2xlarge	0.625	2.5
c6id.4xlarge	1.25	2.5
c6id.8xlarge	2.5	2.5
c6id.12xlarge	3.75	3.75
c6id.16xlarge	5	5
c6id.24xlarge	7.5	7.5
c6id.32xlarge	10	10
c6gd.medium	0.15625	4
c6gd.large	0.3125	4
c6gd.xlarge	0.625	4
c6gd.2xlarge	1.25	4
c6gd.4xlarge	2.5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7.5	7.5
c6gd.16xlarge	10	10

安全组

根据设计，本地网络接口不使用 VPC 中的安全组。安全组控制入站和出站 VPC 流量。本地网络接口不连接到 VPC。本地网络接口连接到您的本地网络。要控制本地网络接口上的入站和出站流量，请使用防火墙或类似策略，如果您对待其他的本地设备一样。

监控

CloudWatch 为每个本地网络接口生成指标，就像为弹性网络接口生成指标一样。有关更多信息，请参阅《Amazon EC2 用户指南》中的监控 EC2 实例上 ENA 设置的网络性能。

MAC 地址

AWS 为本地网络接口提供 MAC 地址。本地网络接口使用本地管理的地址 (LAA) 作为其 MAC 地址。本地网络接口使用同一个 MAC 地址，直到您删除该接口为止。删除本地网络接口后，请从本地配置中删除 MAC 地址。 AWS 可以重复使用不再使用的 MAC 地址。

向 Outposts 子网中的 EC2 实例添加本地网络接口

您可以在启动期间或之后，向 Outposts 子网上的 Amazon EC2 实例添加本地网络接口。为此，您可以使用您在为本地网络接口启用 Outpost 子网时指定的设备索引向实例添加辅助网络接口。

考虑因素

使用控制台指定辅助网络接口时，将使用设备索引 1 来创建网络接口。如果这不是您在为本地网络接口启用 Outpost 子网时指定的设备索引，则可以改用 AWS CLI 或 AWS SDK 来指定正确的设备索引。例如，使用 AWS CLI:create-network-interface和中的以下命令attach-network-interface。

启动实例后，使用以下步骤添加本地网络接口。有关在实例启动过程中进行添加的信息，请参阅在 Outpost 上启动实例。

向 EC2 实例添加本地网络接口

1. 打开位于 https://console.aws.amazon.com/ec2/ 的 Amazon EC2 控制台。
2. 在导航窗格中，依次选择网络与安全、网络接口。
3. 创建网络接口
    a. 选择创建网络接口。
    b. 选择与实例相同的 Outpost 子网。

c. 确认私有 IPv4 地址已设置为自动分配。

d. 选择安全组 安全组不适用于本地网络接口，因此您选择的安全组无关紧要。

e. 选择创建网络接口。

4. 将网络接口连接至实例

a. 选中与新创建的网络接口对应的复选框。

b. 依次选择操作、附加。

c. 选择实例。

d. 选择 附加。网络接口已连接到设备索引 1。如果指定 1 作为 Outpost 子网本地网络接口的设备索引，则此网络接口就是实例的本地网络接口。

查看本地网络接口

当实例处于运行状态时，您可以使用 Amazon EC2 控制台来查看 Outpost 子网中实例的弹性网络接口和本地网络接口。选择实例，再选择网络选项卡。

控制台显示来自子网 CIDR 的本地网络接口的私有 IPv4 地址。该地址不是本地网络接口的 IP 地址，因此无法使用。但是，此地址是从子网 CIDR 中分配的，因此您必须在子网大小调整中将其考虑在内。您必须在来宾操作系统中以静态方式或通过 DHCP 服务器为本地网络接口设置 IP 地址。

配置操作系统

启用本地网络接口后，Amazon EC2 实例将有两个网络接口，其中之一就是本地网络接口。确保将启动的 Amazon EC2 实例的操作系统配置为支持多宿主联网配置。

Outposts 服务器的本地网络连接

使用本主题了解托管 Outposts 服务器的网络布线和拓扑要求。有关更多信息，请参阅 Outposts 服务器的本地网络接口。

内容

- 服务器 IP 地址分配
- 服务器注册

网络上的服务器拓扑

Outposts 服务器需要与网络设备进行两种不同的连接。每个连接使用一条不同的线缆，承载不同类型的流量。多条线缆仅用于流量级隔离，而不用于冗余。这两条线缆不需要连接到公共网络。

下表描述了 Outposts 服务器流量类型和标签。

流量标签	说明
2	服务链路流量 — 此流量允许前哨基地和 AWS 地区之间进行通信，以管理前哨基地以及 AWS 区域与前哨基地之间的 VPC 内部流量。服务链路流量包括从 Outpost 到该区域的服务链路连接。服务链接是自定义 VPN 或 VPNs 从前哨基地到该地区。Outpost 连接到您在购买时选择的区域中的可用区。
1	本地网络接口链路流量 – 此流量支持通过本地网络接口从您的 VPC 与本地 LAN 进行通信。本地链路流量包括在 Outpost 上运行并与您的本地网络通信的实例。本地链路流量还可能包括通过您的本地网络与互联网通信的实例。

服务器物理连接

每个 Outposts 服务器包括非冗余的物理上行链路端口。每个端口有自己的速度和连接器要求，如下所示：

- 10Gbe — 连接器类型 QSFP+

QSFP+ 线缆

QSFP+ 线缆有一个连接器，可以将其连接到 Outposts 服务器上的端口 3。QSFP+ 线缆的另一端有四个 SFP+ 接口，可以将其连接到交换机上。交换机一端的两个接口被标记为 1和 2。这两个接口都

是 Outposts 服务器正常运行所必需的。2 接口用于服务链路流量，1 接口则用于本地网络接口链路流量。其余接口没有用到。

服务器的服务链路流量

将交换机上的服务链路端口配置为 VLAN 的无标记接入端口，使其具通往以下区域端点的网关和路由：

- 服务链路端点
- Outpost 注册端点

服务链接连接必须具有公有 DNS，Outpost 才能发现其在该 AWS 地区的注册端点。该连接可在 Outposts 服务器和注册端点之间使用 NAT 设备。有关公有地址范围的更多信息 AWS，请参阅 Amazon VPC 用户指南中的 AWS IP 地址范围和中的AWS Outposts 终端节点和配额AWS 一般参考。

要注册服务器，请打开以下网络端口：

- TCP 443
- UDP 443
- UDP 53

本地网络接口链路流量

配置上游网络设备上的本地网络接口链路端口，作为本地网络 VLAN 的标准接入端口。如果您有多个 VLAN，请将上游网络设备上的所有端口配置为中继端口。将上游网络设备上的端口配置为需要多个 MAC 地址。在服务器上启动的每个实例都要使用一个 MAC 地址。某些网络设备提供端口安全功能，这些功能会关闭报告多个 MAC 地址的端口。

> **Note**
>
> AWS Outposts 服务器不标记 VLAN 流量。如果您将本地网络接口配置为中继，则必须确保操作系统标记 VLAN 流量。

以下示例演示了如何在 Amazon Linux 2023 上为本地网络接口配置 VLAN 标记。如果您正在使用其他 Linux 分配，请参阅有关配置 VLAN 标记的 Linux 发行版文档。

示例：在 Amazon Linux 2023 和 Amazon Linux 2 上为本地网络接口配置 VLAN 标记

1. 确保 8021q 模块已加载到内核中。如果没有，请使用 modprobe 命令来加载。

```
modinfo 8021q
modprobe --first-time 8021q
```

2. 创建 VLAN 设备。在本示例中：

   - 本地网络接口的接口名称是 ens6
   - VLAN ID 是 59
   - 为 VLAN 设备分配的名称是 ens6.59

```
ip link add link ens6 name ens6.59 type vlan id 59
```

3. 可选。如果您要手动分配 IP，请完成此步骤。在本例中，我们将分配 IP 192.168.59.205，其中子网 CIDR 是 192.168.59.0/24。

```
ip addr add 192.168.59.205/24 brd 192.168.59.255 dev ens6.59
```

4. 激活链路。

```
ip link set dev ens6.59 up
```

要在操作系统级别配置网络接口，并使 VLAN 标记更改持续有效，请参阅以下资源：

- 如果你使用的是 Amazon Linux 2，请参阅亚马逊 Linux 2 用户指南中的 AL2使用 ec2-net-utils 配置网络接口。
- 如果您使用的是 Amazon Linux 2023，请参阅 Amazon Linux 2023 用户指南中的网络服务。

服务器 IP 地址分配

您不需要为 AWS Outposts 服务器的服务链路和实例上的本地网络接口分配公有 IP 地址。对于服务链接，您可以手动分配 IP 地址或使用动态主机控制协议 (DHCP)。要配置服务链接连接，请参阅AWS Outposts 服务器安装指南中的配置和测试连接。

要配置本地网络接口链接，请参阅the section called “配置操作系统”。

> **Note**
>
> 确保为 Outposts 服务器使用稳定的 IP 地址。IP 地址更改可能会导致 Outpost 子网上的服务暂时中断。

服务器注册

当 Outposts 服务器在本地网络上建立连接时，它们会使用服务链路连接来连接到 Outpost 注册端点并自行完成注册。注册需要公有 DNS。当服务器注册时，它们会创建一条通往该区域中服务链路端点的安全隧道。Outposts 服务器使用 TCP 端口 443 来协助通过公共互联网与区域进行通信。Outposts 服务器不支持通过 VPC 进行私有连接。

的容量管理 AWS Outposts

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 安装在您站点上的资产的大小和数量决定，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。

主题

查看 AWS Outposts 容量

您可以在实例或 Outpost 级别查看容量配置。

使用控制台查看前哨基地的容量配置

1. 打开 AWS Outposts 控制台，网址为https://console.aws.amazon.com/outposts/。
2. 从左侧导航窗格中选择 Out posts。
3. 选择前哨基地。
4. 在 Outpost 详细信息页面上，选择实例视图或机架视图。
    - 实例视图-提供有关在 Outposts 上配置的实例以及按大小和系列划分的实例分布的信息。
    - 机架视图-提供每个 Outpost 中每项资产上实例的可视化，并允许您选择 “修改实例容量” 来更改实例容量。

修改 AWS Outposts 实例容量

每个新 Outpost 订单的容量都配置了默认容量配置。您可以转换默认配置，创建各种实例来满足您的业务需求。为此，您可以创建容量任务，选择 Outposts 或单个资产，指定实例大小和数量，然后运行容量任务来实施更改。

注意事项

修改实例容量之前，请考虑以下几点：

- 容量任务只能由拥有 Outpost 资源的 AWS 账户（所有者）运行。消费者无法运行容量任务。有关所有者和消费者的更多信息，请参阅共享您的 AWS Outposts 资源。
- 实例的大小和数量可以在 Outpost 级别或单个资产级别定义。
- 容量是根据可能的配置和最佳实践在前哨基地中的一项资产或所有资产中自动配置的。
- 在容量任务运行时，与所选前哨基地关联的资产可能会被隔离。因此，我们建议仅在您不希望在 Outposts 上启动新实例时才创建容量任务。
- 您可以选择立即运行容量任务，也可以在接下来的 48 小时内继续定期尝试。选择立即运行所需的资产隔离时间更短，但是如果需要停止实例才能运行任务，则任务可能会失败。选择定期运行可以让更多时间在任务失败之前停止实例，但资产隔离的时间可能会更长。
- 有效的容量配置可能无法利用资产上的所有可用 vCPU。在这种情况下，实例类型部分末尾会显示一条消息，告知您容量不足，但允许您按要求应用配置。
- 当您在控制台中修改 Outpost 时，不会显示所有支持的实例，因为控制台不完全支持将磁盘支持的non-disk-backed实例与实例混合使用。要访问所有可能的实例，请使用 StartCapacityTaskAPI。
- 您只能修改现有 Outposts 容量配置，以使用相应资产模型支持的实例系列中的有效 Amazon EC2 实例大小。
- 如果您的 Outpost 上有不想停止运行容量任务的实例，请在 “保持原样实例” 部分下选择它们各自的实例 ID（可选），并确保在更新的容量配置中保留该实例大小的必要数量。这将在容量任务运行时保留用于支持生产工作负载的实例。
- 在一个实例系列中配置具有多个实例大小的资产时，请使用自动平衡，以确保您不会试图过度配置或不足预置您的液滴。不支持过度配置，这会导致容量任务失败。
- 多个容量任务可以并行运行，前提是它们适用于相互排斥的资产集IDs。例如，您可以同时为不同的资产创建多个资产IDs 级别的容量任务。但是，如果有正在运行的 Outpost 级别任务，则无法同时创建另一个 Outpost 或资产级任务。同样，如果有正在运行的资产级任务，则不能同时在同一 assetID 上创建 OutPost 级别任务或资产级任务。

使用控制台修改前哨基地的容量配置

1. 打开 AWS Outposts 控制台，网址为https://console.aws.amazon.com/outposts/。
2. 在左侧导航窗格中，选择容量任务。
3. 在容量任务页面上，选择创建容量任务。
4. 在入门页面上，选择要配置的顺序、Outpost 或资产。
5. 要修改容量，请在 “修改方法：控制台中的步骤” 中指定一个选项或上传 JSON 文件。

    - 修改容量配置计划以使用控制台中的步骤

- 上传容量配置计划以上传 JSON 文件

> **Note**
>
> - 要防止容量管理建议停止特定实例，请指定不应停止的实例。这些实例将从要停止的实例列表中排除。

Console steps

1. 选择实例视图或机架视图。
2. 选择 “修改 Outpost 容量配置” 或 “修改单个资产”。
3. 如果前哨基地或资产与当前选择不同，请选择前哨基地或资产。
4. 选择立即运行此容量任务，或者在 48 小时内定期运行此容量任务。
5. 选择下一步。
6. 在配置实例容量页面上，每种实例类型都会显示一个预选了最大数量的实例大小。要添加更多实例大小，请选择添加实例大小。
7. 指定实例数量并记下针对该实例大小显示的容量。
8. 查看每个实例类型部分末尾的消息，该消息会告知您是否超出或低于容量。在实例大小或数量级别进行调整，以优化总可用容量。
9. 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末尾选择自动平衡。
10. 对于每种实例类型，确保至少为一种实例大小指定了实例数量。
11. （可选）选择要保持原状的实例。
12. 选择下一步。
13. 在查看并创建页面上，验证您请求的更新。
14. 选择 “创建”。 AWS Outposts 创建容量任务。
15. 在容量任务页面上，监控任务的状态。

Upload a 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。或者，您可以在 JSON 文件中指定InstancesToExclude、和TaskActionOnBlockingInstances参数。

   Example

   示例 JSON 筛选条件

```
{
  "InstancePools": [
    {
      "InstanceType": "c5.24xlarge",
      "Count": 1
    },
    {
      "InstanceType": "m5.24xlarge",
      "Count": 2
    }
  ],
  "InstancesToExclude": {
    "AccountIds": [
      "111122223333"
    ],
    "Instances": [
      "i-1234567890abcdef0"
    ],
    "Services": [
      "ALB"
    ]
  },
  "TaskActionOnBlockingInstances": "WAIT_FOR_EVACUATION"
}
```

4. 在容量配置计划部分查看 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。

容量任务问题疑难解答

查看以下已知问题，以按新顺序解决与容量管理有关的问题。如果您的问题未列出，请联系 支持。

订单与 *oo-xxxxxx* Outpost ID 无关 *op-xxxxx*

当您使用 AWS CLI 或 API 运行`StartCapacityTask`并且请求中的前哨站 ID 与订单中的前哨站 ID 不匹配时，就会出现此问题。

要解决此问题，请执行以下操作：

1. 登录到 AWS。
2. 打开 AWS Outposts 控制台，网址为https://console.aws.amazon.com/outposts/。
3. 从导航窗格中选择 “订单”。
4. 选择订单并验证订单状态是否为以下状态之一：`PREPARINGIN_PROGRESS`、或`ACTIVE`。
5. 请记下订单中的前哨基地 ID。
6. 在 `StartCapacityTask` API 请求中输入正确的 Outpost ID。

容量计划包括不支持的实例类型

当您使用 AWS CLI 或 API 创建或修改容量任务并且请求包含不支持的实例类型时，就会出现此问题。

要解决此问题，请使用控制台或 CLI。

使用控制台

1. 登录到 AWS。
2. 打开 AWS Outposts 控制台，网址为https://console.aws.amazon.com/outposts/。
3. 在导航窗格中，选择容量任务。
4. 使用上传容量配置选项上传具有相同实例类型列表的 JSON。
5. 控制台会显示一条错误消息，其中包含支持的实例类型列表。
6. 更正移除不支持的实例类型的请求。
7. 使用更正后的 JSON 在控制台上创建或修改容量任务，或者使用包含此更正后的实例类型列表的 CLI 或 API。

使用 CLI

1. 使用GetOutpostSupportedInstanceTypes命令查看支持的实例类型列表。
2. 使用正确的实例类型列表创建或修改容量任务。

没有带有前哨基地ID的前哨基地 *op-xxxxx*

当您使用 AWS CLI 或 API 运行StartCapacityTask并且请求中包含由于以下原因之一而无效的 Outpost ID 时，就会出现此问题：

- 前哨基地位于不同的 AWS 区域。
- 你没有访问这个前哨基地的权限。
- 前哨基地ID不正确。

要解决此问题，请执行以下操作：

1. 记下您在 StartCapacityTask API 请求中使用的 AWS 区域。
2. 使用 ListOutpostsAPI 操作获取您在该地区拥有的 Outposts 列表。 AWS
3. 检查前哨基地ID是否已列出。
4. 在StartCapacityTask请求中输入正确的前哨基地 ID。
5. 如果您找不到前哨基地 ID，请再次使用 ListOutposts API 操作来检查前哨基地是否存在于其他 AWS 区域。

Oppost 的激活 CapacityTask 上限—— *XXXX* 已经找到了 Op-*XXXX*

当您使用 AWS Outposts 控制台或 API 在 Outpost StartCapacityTask上运行并且前哨基地已经有运行容量任务时，就会出现此问题。如果容量任务处于以下任一状态，则该任务被视为正在运行：REQUESTED、IN_PROGRESSWAITING_FOR_EVACUATION、或CANCELLATION_IN_PROGRESS。

要解决此问题，请使用 AWS Outposts 控制台或 CLI。

使用控制台

1. 登录到 AWS。
2. 打开 AWS Outposts 控制台，网址为https://console.aws.amazon.com/outposts/。

3. 在导航窗格中，选择容量任务。
4. 确保没有正在运行的容量任务 OutpostId。
5. 如果有正在运行的容量任务 OutpostId，请等待它们终止，或者根据需要将其取消。
6. 当请求的容量任务没有正在运行时 OutpostId，请重试您的请求以创建容量任务。

使用 CLI

1. 使用ListCapacityTasks命令查找 Outpost 的运行容量任务。
2. 等待所有正在运行的容量任务终止，或者根据需要将其取消。
3. 当请求的容量任务没有正在运行时 OutpostId，请重试您的请求以创建容量任务。

*XXXX*已在 Outpost op-xxxx *XXXX* 上找到资产的活跃上 CapacityTask 限

当您使用 AWS Outposts 控制台或 API 在资产StartCapacityTask上运行并且该资产已有正在运行的容量任务时，就会出现此问题。如果容量任务处于以下任一状态，则该任务被视为正在运行：REQUESTED、IN_PROGRESSWAITING_FOR_EVACUATION、或CANCELLATION_IN_PROGRESS。

要解决此问题，请使用 AWS Outposts 控制台或 CLI。

使用控制台

1. 登录到 AWS。
2. 打开 AWS Outposts 控制台，网址为https://console.aws.amazon.com/outposts/。
3. 在导航窗格中，选择容量任务。
4. 确保没有正在运行的容量任务 OutpostId ，也没有正在运行的资产级容量任务。 AssetId
5. 如果有正在运行的容量任务，请等待它们终止，或者根据需要将其取消。
6. 如果没有正在运行的容量任务，请重试创建容量任务的请求。

使用 CLI

1. 使用ListCapacityTasks命令查找 OutpostID 和 assetID 的运行容量任务。
2. 确保没有正在运行的 OutPost 级别容量任务 OutpostId，也没有正在运行的资产级容量任务。AssetId
3. 如果有正在运行的容量任务，请等待它们终止，或者根据需要将其取消。

4. 重试创建容量任务的请求。

AssetId= *XXXX* 对于 outpost=op-无效 *XXXX*

当您使用 AWS Outposts 控制台或 API 在资产StartCapacityTask上运行时，由于以下原因之一，assetId 无效，就会出现此问题：

- 该资产与前哨基地无关。
- 资产是隔离的。

要解决此问题，请使用 AWS Outposts 控制台或 CLI。

使用控制台

1. 登录到 AWS。
2. 打开 AWS Outposts 控制台，网址为https://console.aws.amazon.com/outposts/。
3. 为前哨基地选择机架视图。
4. 确认请求的请求 AssetId 与 Outpost 相关联，并且未将其标记为隔离主机。
    a. 如果资产处于隔离状态，则可能是因为正在其上运行容量任务。您可以导航到容量任务面板，检查和是否有任何正在运行的 Outpost 或资产级任务。 OutpostId AssetId如果有，则等待任务终止并等待资产再次可用。
    b. 如果隔离的资产没有运行容量任务，则该资产可能会降级。
5. 验证资产存在且处于有效状态后，请重试创建容量任务的请求。

使用 CLI

1. 使用ListAssets命令查找与 OutpostID 关联的资产。
2. 验证请求的对象 AssetId 是否与前哨基地相关联，以及其状态是否`ACTIVE`与 Outpost 关联。
    a. 如果资产状态未处于活动状态，则可能是因为正在其上运行容量任务。使用ListCapacityTasks命令确定和是否有正在运行的 Outpost 或资产级任务。 OutpostId AssetId如果有，则等待任务终止并等待资产再次变为活动状态。
    b. 如果隔离的资产没有运行容量任务，则该资产可能会降级。
3. 验证资产存在且处于有效状态后，请重试创建容量任务的请求。

共享您的 AWS Outposts 资源

通过 Outpost 共享，Outpost 所有者可以与同一组织下的其他账户共享他们的 Outposts 和 Outpost 资源，包括前哨基地和子网。 AWS AWS 作为 Outpost 所有者，您可以集中创建和管理 Outpost 资源，并在组织内的多个 AWS 账户之间共享资源。 AWS 这允许其他用户使用 Outpost 站点，在共享的 Outpost 上配置 VPCs、启动和运行实例。

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（消费者）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：

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

内容

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。

有关 Outposts 服务器资源，请参阅使用共享 AWS Outposts资源。

这些资源可供 Outposts 服务器使用。有关 Outposts 机架资源，请参阅 Out posts 机架 AWS Outposts 用户指南中的使用共享 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。
- Outpost — 有权访问此资源的使用者可以：
  - 在 Outpost 上创建和管理子网。
  - 使用 AWS Outposts API 查看有关前哨基地的信息。
- 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》中的在 AWS Organizations中启用资源共享。
- 要共享 Outpost 资源，您必须在自己的 AWS 账户中拥有该资源。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

前哨资源共享与 AWS Resource Access Manager (AWS RAM) 集成。 AWS RAM 是一项服务，可让您与任何 AWS 账户或通过任何账户共享 AWS 资源 AWS Organizations。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。消费者可以是个人 AWS 帐户、组织单位或中的整个组织 AWS Organizations。

有关的更多信息 AWS RAM，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 AWS 账户的可用区`us-east-1a`可能与其他 AWS 账户的可用区不同。`us-east-1a`

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)。可用区 ID 是所有 AWS 账户中可用区的唯一且一致的标识符。例如，`use1-az1`是该`us-east-1`区域的可用区 ID，它在每个 AWS 账户中的位置都相同。

查看您 IDs 账户中可用区域的

1. 在AWS RAM 控制台中导航到 AWS RAM 控制台。
2. 当前区域 IDs 的可用区显示在屏幕右侧的您的可用区 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。资源共享是一种 AWS RAM 允许您跨 AWS 账户共享资源的资源。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 AWS Outposts 控制台

共享 Outpost 资源时，可以将其添加到现有资源共享中。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。

如果您是组织中的一员， AWS Organizations 并且启用了组织内部共享，则可以向组织中的消费者授予从 AWS RAM 控制台访问共享的 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 AWS RAM 台、主机或，共享您拥有的 Outpost 资源。 AWS CLI

使用主机共享您拥有的前哨基地 AWS Outposts

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，选择资源共享。
5. 选择创建资源共享。

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

使用控制台共享您拥有的 Outpost 或本地网关路由表 AWS RAM

请参阅《AWS RAM 用户指南》中的创建资源共享。

要共享您拥有的 Outpost 或本地网关路由表，请使用 AWS CLI

使用 create-resource-share 命令。

取消共享已共享的 Outpost 资源

当您取消与使用者共享您的 Outpost 时，使用者就不能再进行以下操作：

- 在 AWS Outposts 控制台中查看前哨基地。
- 在 Outpost 上创建新的子网。
- 在 Outpost 上创建新的 Amazon EBS 卷。
- 使用 AWS Outposts 控制台或，查看 Outpost 的详细信息和实例类型。 AWS CLI

使用者在共享期内创建的子网、卷或实例不会被删除，使用者可以继续执行以下操作：

- 访问和修改这些资源。
- 在使用者创建的现有子网上启动新实例。

为了防止使用者访问他们的资源并在您的 Outpost 上启动新实例，请让使用者删除其资源。

取消共享已共享的本地网关路由表后，使用者就不能再为其创建新的 VPC 关联。使用者创建的任何现有 VPC 关联仍与路由表相关联。这些资源 VPCs 可以继续将流量路由到本地网关。为防止出现这种情况，请使用者删除 VPC 关联。

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.

使用控制台取消共享您拥有的 Outpost 共享资源 AWS RAM

请参阅《AWS RAM 用户指南》中的更新资源共享。

要取消共享您拥有的共享 Outpost 资源，请使用 AWS CLI

使用 disassociate-resource-share 命令。

识别共享的 Outpost 资源

所有者和消费者可以使用 AWS Outposts 控制台识别共享的Outposts，然后. AWS CLI他们可以使用AWS CLI来识别共享的本地网关路由表。

使用控制台识别共享的前哨基地 AWS Outposts

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，查看所有者 ID 以识别 Outpost 所有者的 AWS 账户 ID。

要识别共享的前哨资源，请使用 AWS CLI

使用 list-outposts 和 describe-local-gateway-route-table s 命令。这些命令会返回您拥有的前哨基地资源和与您共享的前哨资源。 `OwnerId`显示了 Outpost 资源所有者的 AWS 账户 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、修改和删除消费者在共享 Outposts 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。他们还需要支付与来自该地区的 Outpost 服务链接 VPN 流量相关的任何数据传输费用。 AWS

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

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。消费者还需要为来自 AWS 该地区的收费数据传输付费。

限制

以下限制适用于使用共 AWS Outposts 享：

- 共享子网的限制适用于使用 AWS Outposts 共享。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。

借助 Outposts 服务器，您可以利用存储在第三方存储阵列上的现有数据。您可以在 Outposts 上为您的 EC2 实例指定外部块数据卷和外部块启动卷。通过这种集成，您可以使用由第三方供应商（例如戴尔、HPE Alletra Storage MP B10000 PowerStore、 NetApp 本地企业存储阵列和纯 FlashArray 存储系统）支持的外部块数据和启动卷。

注意事项

- 在 Outposts 机架和 Outposts 2U 服务器上可用。在 Outposts 1U 服务器上不可用。
- 适用于所有支持 Outposts 2U 服务器的 AWS 区域。
- 不收取额外费用。
- 您负责存储阵列的配置和 day-to-day管理。您还可以在存储阵列上创建和管理外部块卷。如果您在存储阵列的硬件、软件或连接方面遇到问题，请联系第三方存储供应商。

> **Note**
>
> 存储在外部存储阵列上的块卷包含将启动到 Outposts 上的 EC2 实例中的操作系统。不支持启动由外部存储阵列支持的 AMI。要启动 AMI，需要使用 Outposts 服务器上的实例存储。

外部区块数据量

在配置和配置由兼容的第三方存储系统支持的块数据卷后，您可以在启动 EC2 实例时将这些卷连接到 EC2 实例。如果您在存储阵列上将卷配置为多重连接，则可以将一个卷连接到多个 EC2 实例。

关键步骤

- 您负责通过本地网络接口在 Outpost 子网和本地网络之间建立连接。
- 您可以使用外部存储阵列的管理界面来创建卷。然后，您将通过创建新的启动器组并将目标 EC2 实例的 iSCSI 限定名称 (IQN) 添加到该组来配置启动器映射。这会将外部块数据卷与 EC2 实例相关联。
- 您在启动实例时添加外部数据量。您需要外部存储阵列的启动器 IQN、目标 IP 地址、端口和 IQN。有关更多信息，请参阅在 Outpost 上启动实例。

有关更多信息，请参阅通过简化第三方块存储的使用 AWS Outposts。

外部块启动卷

从外部存储阵列在 Outposts 上启动 EC2 实例为依赖第三方存储的本地工作负载提供了一种集中、经济实惠且高效的解决方案。可以选择以下选项：

iSCSI SAN 启动

提供从外部存储阵列直接启动的功能。利用 AWS提供的 iPXE 助手 AMI，以便实例可以从网络位置启动。当 iPXE 与 iSCSI 结合使用时，EC2 实例会将远程 iSCSI 目标（存储阵列）视为本地磁盘。操作系统的所有读取和写入操作都是在外部存储阵列上执行的。

iSCSI 或 NVMe-over-TCP LocalBoot

使用从存储阵列中检索的启动卷副本启动 EC2 实例，原始源映像保持不变。我们使用 LocalBoot AMI 启动帮助器实例。此帮助程序实例将启动卷从存储阵列复制到 EC2 实例的实例存储，并充当 iSCSI 启动器或 NVMe-over-TCP主机。最后，EC2 实例使用本地实例存储卷重新启动。

由于实例存储是临时存储，因此 EC2 实例终止时，启动卷将被删除。因此，此选项适用于只读启动卷，例如虚拟桌面基础架构 (VDI) 中使用的启动卷。

你无法使用启动 EC2 Windows 实例 NVMe-over-TCP LocalBoot。这仅在使用 EC2 Linux 实例时才受支持。

有关更多信息，请参阅部署外部启动卷以与一起使用 AWS Outposts。

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 AWS 的共同责任。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，请参阅解答。

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结构上的内容的控制。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 Security Blog 上的 AWS Shared Responsibility Model and 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 Outposts 服务器上的数据。

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。

数据删除

在终止 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。有关更多信息，请参阅以加密方式粉碎服务器数据。

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（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

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。

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
ACLs	否
ABAC（策略中的标签）	是
临时凭证	是
主体权限	是
服务角色	否
服务关联角色	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》中的使用客户管理型策略定义自定义 IAM 权限。

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。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

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。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。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，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 ARNs 用逗号分隔。

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

要查看 AWS Outposts 资源类型及其列表 ARNs，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。

`Condition` 元素根据定义的条件指定语句何时执行。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。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

ABAC with Outposts AWS

支持 ABAC（策略中的标签）：是

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

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》中的使用 ABAC 授权定义权限。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

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。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 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

Outposts 的跨服务主体 AWS 权限

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Outposts 的 AWS 服务相关角色

支持服务关联角色：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关联角色的权限。

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

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（控制台）。

有关 AWS Outposts 定义的操作和资源类型（包括每种资源类型的格式）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。 ARNs

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，请遵循以下指南和建议：

- 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 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》中的使用 IAM Access Analyzer 验证策略。
- 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》中的使用 MFA 保护 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 中的安全最佳实践。

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。

JSON

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

```
            "Action": "outposts:GetOutpost",
            "Resource": "arn:aws:outposts:us-east-1:111122223333: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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "outposts:GetSite",
            "Resource": "arn:aws:outposts:us-east-1:111122223333:site/
os-0abcdef1234567890"
        }
    ]
}
```

的服务相关角色 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直接链接到 AWS Outposts的服务角色。 AWS Outposts 定义服务相关角色，包括代表您调用其他 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，以及不能附加到任何其他 IAM 实体的权限策略。

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。

的服务相关角色权限 AWS Outposts

AWS Outposts 使用名为 AWSServiceRoleForOutposts_ ***OutpostID*** 的服务相关角色。此角色授予 Outposts 管理网络资源的权限，从而代表您启用私有连接。此角色还允许 Outposts 创建和配置网络接口、管理安全组以及将接口附加到服务链接端点实例。这些权限是建立和维护本地 Outpost 与 AWS 服务之间的安全、私密连接所必需的，从而确保 Outpost 部署的可靠运行。

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

- `outposts.amazonaws.com`

服务相关角色策略

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

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_*OutpostID*

AWSOutpostsServiceRolePolicy

该`AWSOutpostsServiceRolePolicy`策略允许访问由管理的 AWS 资源 AWS Outposts。

此策略 AWS Outposts 允许对指定资源完成以下操作：

- 操作：`ec2:DescribeNetworkInterfaces`对所有 AWS 资源采取行动
- 操作：`ec2:DescribeSecurityGroups`对所有 AWS 资源采取行动
- 操作：`ec2:CreateSecurityGroup`对所有 AWS 资源采取行动
- 操作：`ec2:CreateNetworkInterface`对所有 AWS 资源采取行动

AWSOutpostsPrivateConnectivityPolicy_OutpostID

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

- 操作：`ec2:AuthorizeSecurityGroupIngress`对符合以下条件的所有 AWS 资源执行操作：

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

- 操作：ec2:AuthorizeSecurityGroupEgress对符合以下条件的所有 AWS 资源执行操作：

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

- 操作：ec2:CreateNetworkInterfacePermission对符合以下条件的所有 AWS 资源执行操作：

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

- 操作：ec2:CreateTags对符合以下条件的所有 AWS 资源执行操作：

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

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

为创建服务相关角色 AWS Outposts

您无需手动创建服务关联角色。在中为 Outpost 配置私有连接时 AWS 管理控制台，AWS Outposts 会为您创建服务相关角色。

编辑服务相关角色 AWS Outposts

AWS Outposts 不允许您编辑 AWSService RoleForOutposts _ *OutpostID* 服务相关角色。在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。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的更新服务相关角色。

删除的服务相关角色 AWS Outposts

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。

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。

必须先删除 Outpost，然后才能删除 AWSService RoleForOutposts _ *OutpostID* 服务相关角色。

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，请参阅取消共享的 Outpost 资源。

删除 AWSService RoleForOutposts _ 使用的 AWS Outposts 资源 ***OutpostID***

联系 AWS Enterprise Support 删除你的 Outpost

使用 IAM 手动删除服务关联角色

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 服务相关角色支持的区域

AWS Outposts 支持在提供服务的所有区域中使用服务相关角色。欲了解更多信息，请参阅 Outp FAQs osts 服务器的。

AWS AWS Outposts 的托管政策

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使用案例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

此政策附属于服务相关角色，该角色允许 Outpo AWS sts 代表您执行操作。有关更多信息，请参阅 服务关联角色。

AWS 托管策略： AWSOutpostsAuthorizeServerPolicy

此策略可用于授予在本地网络中授权 Outposts 服务器硬件所需的权限。

该策略包含以下权限。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "outposts:StartConnection",
        "outposts:GetConnection"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Outposts 对托管政策的 AWS 更新

查看自该服务开始跟踪这些变更以来 AWS Outposts AWS 托管政策更新的详细信息。

更改	描述	日期
AWSOutpostsAuthorizeServerPolicy - 新策略	AWS Outposts 添加了一项策略，该策略授予在您的本地网络中授权 Outposts 服务器硬件的权限。	2023 年 1 月 4 日
AWS Outposts 开始追踪变更	AWS Outposts 开始跟踪其 AWS 托管政策的变更。	2019 年 12 月 3 日

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。

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。

韧性在 AWS Outposts

要获得高可用性，您可以订购额外的 Outpost 服务器。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。

Outpost 服务器包括实例存储卷，但不支持 Amazon EBS 卷。实例重启后会保留实例存储卷上的数据，但实例终止后不会保留这些数据。要在实例停用之后保留实例存储卷上的长期数据，请确保将数据备份到持久性存储中，例如 Amazon S3 存储桶或本地网络中的网络存储设备。

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。有关您在使用时的合规责任的更多信息 AWS 服务，请参阅AWS 安全文档。

监控 Outposts 服务器

AWS Outposts 与以下提供监控和记录功能的服务集成：

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 服务器数据点的统计信息。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 。

CloudTrail 日志

AWS CloudTrail 用于捕获有关拨打的呼叫的详细信息 AWS APIs。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 使用记录 API 调用 CloudTrail。

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 posts 机架服务器复制并转发 out-of-band到安全和监控设备。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 VPC Traffic Mirroring 指南》。

AWS Health Dashboard

Health Dashboard 显示由 AWS 资源运行状况的变化所启动的信息和通知。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， Health Dashboard 无需设置，任何在您的账户中经过身份验证的用户都可以查看。有关更多信息，请参阅 AWS Health Dashboard入门。

CloudWatch

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 Su AWS pport。

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

指标

`AWS/Outposts`命名空间包括以下类别的指标。

内容

实例指标

以下指标可用于 Amazon EC2 实例。

指标	维度	说明
InstanceFamilyCapacityAvailability	InstanceFamily 和 OutpostId	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）。
InstanceFamilyCapacityUtilization	Account、InstanceFamily 和 OutpostId	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）。
InstanceTypeCapacityAvailability	InstanceType 和 OutpostId	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）。

指标	维度	说明
InstanceTypeCapacityUtilization	Account、InstanceType 和 OutpostId	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）。
UsedInstanceType_Count	Account、InstanceType 和 OutpostId	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

指标	维度	说明
AvailableInstanceType_Count	InstanceType 和 OutpostId	可用实例类型的数量。此指标包括 AvailableReservedInstances 计数。 要确定您可以预留的实例数量，请从 AvailableInstanceType_Count 计数中减去 AvailableReservedInstances 计数。 `Number of instances that you can reserve = AvailableInstanceType_Count - AvailableReservedInstances` 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

指标	维度	说明
AvailableReservedInstances	InstanceType 和 OutpostId	在使用容量预留功能预留的计算容量中可启动的实例数量。 此指标不包括 Amazon EC2 预留实例。 此指标不包括您可以预留的实例数量。要确定可以预留多少实例，请从 AvailableInstanceType_Count 计数中减去 AvailableReservedInstances 计数。 `Number of instances that you can reserve = AvailableInstanceType_Count - AvailableReservedInstances` 单位：计数 最大分辨率：5 分钟
UsedReservedInstances	InstanceType 和 OutpostId	在使用容量预留功能预留的计算容量中运行的实例数量。此指标不包括 Amazon EC2 预留实例。 单位：计数 最大分辨率：5 分钟

指标	维度	说明
TotalReservedInstances	InstanceType 和 OutpostId	使用容量预留功能预留的计算容量所提供的正在运行且可供启动的实例总数。此指标不包括 Amazon EC2 预留实例。 单位：计数 最大分辨率：5 分钟

Outposts 指标

以下指标适用于你的 Outposts。

指标	维度	说明
ConnectedStatus	OutpostId	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 Statistics：最有用的统计工具是 Average。
CapacityExceptions	InstanceType 和 OutpostId	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。

指标维度

要筛选您的 Outpost 的指标，可以使用以下维度。

维度	说明
Account	使用容量的账户或服务。
InstanceFamily	实例系列。
InstanceType	实例类型。
OutpostId	Outpost 的 ID。

您可以使用控制台查看 Outposts 服务器的 CloudWatch 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，请在搜索字段中输入其名称。

要查看指标，请使用 AWS CLI

使用以下 list-metrics 命令列出可用指标。

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

要获取指标的统计数据，请使用 AWS CLI

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
```

使用记录 AWS Outposts API 调用 AWS CloudTrail

AWS Outposts 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务所执行操作的记录。 CloudTrail 将发出的 API 调用捕获 AWS Outposts 为事件。捕获的调用包括来自 AWS Outposts 控制台的调用和对 AWS Outposts API 操作的代码调用。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、发出请求的时间以及其他详细信息。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是否代表 IAM Identity Center 用户发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

CloudTrail 在您创建 AWS 账户时在您的账户中处于活动状态，并且您可以自动访问 CloudTrail 活动历史记录。 CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查看、可搜索、可下载且不可变的记录。 AWS 区域有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 “使用 CloudTrail 事件历史记录”。查看活动历史记录不 CloudTrail 收取任何费用。

要持续记录 AWS 账户 过去 90 天内的事件，请创建跟踪或 CloudTrail Lake 事件数据存储。

CloudTrail 步道

跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。使用创建的所有跟踪 AWS 管理控制台 都是多区域的。您可以通过使用 AWS CLI创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可以捕获账户 AWS 区域 中的所有活动。如果您创建单区域跟踪，则只能查看跟踪的 AWS 区域中记录的事件。有关跟踪的更多信息，请参阅《AWS CloudTrail 用户指南》中的为您的 AWS 账户创建跟踪和为组织创建跟踪。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到您的 Amazon S3 存储桶，但是，会收取 Amazon S3 存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail 湖泊事件数据存储

CloudTrail L@@ ak e 允许你对自己的事件运行基于 SQL 的查询。 CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅AWS CloudTrail 用户指南中的使用 AWS CloudTrail Lake。

CloudTrail 湖泊事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

AWS Outposts 中的管理事件 CloudTrail

管理事件提供有关对中的资源执行的管理操作的信息 AWS 账户。这些也称为控制面板操作。默认情况下， CloudTrail 记录管理事件。

AWS Outposts 将所有 O AWS utposts 控制平面操作记录为管理事件。有关 Outposts 记录的 AWS Outposts 控制平面操作列表， CloudTrail请参阅 AWS Outposts API 参考。AWS

AWS Outposts 事件示例

以下示例显示了一个演示该SetSiteAddress操作 CloudTrail 的事件。

```
{
    "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"
}
```

Outposts 服务器维护

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 Outposts 服务器的性能、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实例终止，则实例存储卷上的数据将丢失。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永久性存储，例如 Amazon S3 存储桶或本地网络中的网络存储设备。

内容

更新联系人详细信息

如果 Outpost 拥有者发生变化，请联系 AWS 支持 Center，提供新拥有者的名称和联系信息。

硬件维护

如果在服务器配置过程中或托管在您的 Outposts 服务器上运行的 Amazon EC2 实例时 AWS 检测到硬件存在无法弥补的问题，我们将通知实例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。

AWS 在实例停用日期终止受影响的实例。实例终止后不会保留实例存储卷上的数据。因此，请务必在实例停用日期之前采取措施。首先，将您的长期数据从各个受影响实例的实例存储卷传输到持久性存储上，例如 Amazon S3 存储桶或您的网络中的网络存储设备。

替换服务器将运往 Outpost 站点。然后执行以下操作：

- 从无法修复的服务器上拔下网络电缆和电源线，并根据需要将服务器从机架上拆下。
- 将替换服务器安装到原位。按照 Outposts 服务器安装中的安装说明进行操作。
- 将无法修复的服务器装 AWS 入与更换服务器相同的包装中。
- 使用预付费退货运输标签，该标签可在订单配置详细信息或替换服务器订单附带的控制台中找到。
- 将服务器返回到 AWS。有关更多信息，请参阅退回 AWS Outposts 服务器。

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。

电源和网络事件最佳实践

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中断的情况下，Outposts服务器才会正常运行。

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。
- 维护期间避免重复切换电源 (off-on-off-on)。
- 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。
- 恢复供电后，在 Cent AWS 支持 er 创建一个案例 AWS Outposts ，请求验证相关服务是否正在运行。

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。

Outposts 服务器上的 Amazon EC2 实例、LNI 网络和实例存储卷将继续正常运行，并可通过本地网络和 LNI 进行本地访问。同样，诸如 Amazon ECS 工作节点之类的 AWS 服务资源继续在本地运行。但是，API 可用性将降低。例如，运行、启动、停止和终止 APIs 可能不起作用。实例指标和日志将继续在本地缓存长达 7 天，并在连接恢复后推送到该 AWS 区域。断开连接超过 7 天可能会导致指标和日志丢失。

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 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 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博客对该AWSSupport-SetupIPMonitoringFromVPC工具进行了介绍。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。

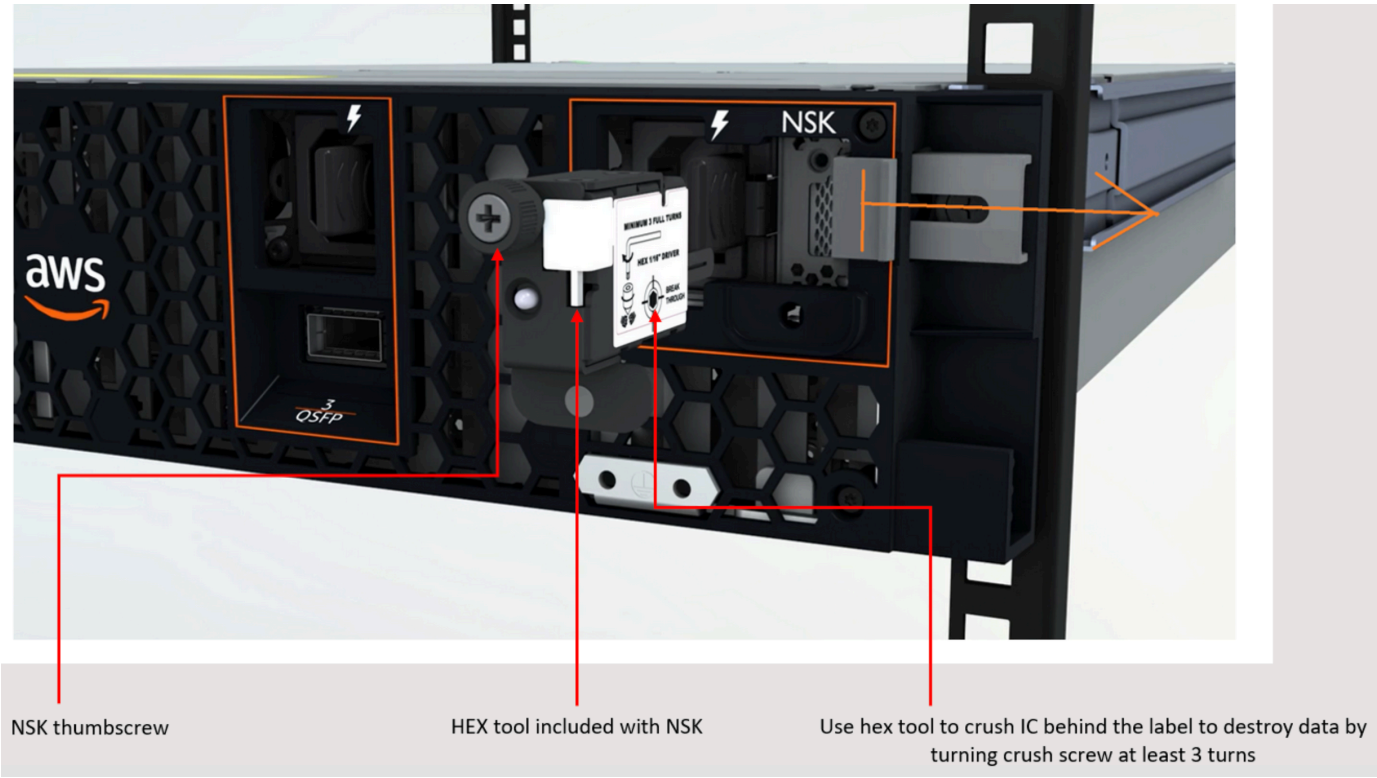
- 如果您有任何疑问或需要更多信息，请参阅 AWS 支持用户指南中的创建支持案例。

以加密方式粉碎服务器数据

需要使用 Nitro 安全密钥 (NSK) 来解密服务器上的数据。当您因为要更换服务器或停止服务而将 AWS 服务器返回到时，您可以销毁 NSK 以加密方式粉碎服务器上的数据。

以加密方式粉碎服务器上的数据

1. 在将服务器运回服务器之前，请先从服务器上删除 NSK。 AWS
2. 请确保您持有服务器随附的正确 NSK。
3. 取出贴纸下方的小六角工具/内六角扳手。
4. 使用六角工具，将贴纸下方的小螺丝转动整整三圈。此操作会销毁 NSK，并以加密方式粉碎服务器上的所有数据。



Outposts 服务器选项 end-of-term

在 AWS Outposts 任期结束时，您必须在以下选项中进行选择：

- 续订订阅并保留现有的 Outposts 服务器。
- 归还你的 Outposts 服务器。
- 转换为 month-to-month订阅并保留现有的 Outposts 服务器。

续订订阅

您必须在 Outposts 服务器的当前订阅到期前至少 5 个工作日完成以下步骤。未能在当前订阅结束前至少 5 个工作日完成这些步骤可能会导致意想不到的费用。

续订订阅并保留现有的 Outposts 服务器

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. 选择操作。
4. 选择 “续订前哨基地”。
5. 选择订阅期限和付款选项。

   有关定价，请参阅 AWS Outposts 服务器定价。您也可以请求报价。
6. 选择 “提交支持请求”。

> **Note**
>
> 如果您在Outposts服务器的当前订阅到期之前续订，则将立即向您收取任何预付费用。

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Outposts服务器，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。

返回 Outposts 服务器

要因为服务器已到合同期限而退回服务器，您必须首先在当前Outposts服务器的订阅到期前至少 5 个工作日完成停用流程。 AWS 除非你这样做，否则无法启动退货流程。未能在当前订阅结束前至少 5 个工作日完成停用流程可能会导致停用延迟和意外收费。

完成停用过程后，您必须为服务器做好退货准备，获取运输标签，然后将服务器打包并退回。 AWS

当您退回 Outposts 服务器时，您无需支付运费。但是，如果您退回的服务器已损坏，则可能会产生费用。

任务

- 步骤 1：为服务器做归还准备
- 步骤 2：停用服务器
- 第 3 步：获取退货货件标签
- 第 4 步：打包服务器
- 第 5 步：通过快递归还服务器

步骤 1：为服务器做归还准备

要为服务器做好归还准备，请取消共享资源、备份数据、删除本地网络接口并终止活动实例。

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。
   - AWS CLI 使用运行disassociate-resource-share命令。

   有关可共享的 Outpost 资源列表，请参阅可共享的 Outpost 资源。
2. 为存储在 AWS Outposts 服务器上运行的 Amazon 实例的 EC2 实例存储中的数据创建备份。
3. 删除与服务器上运行的实例关联的本地网络接口。
4. 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。
5. 销毁 Nitro 安全密钥 (NSK)，以加密方式粉碎服务器上的数据。要销毁 NSK，请按照加密方式粉碎服务器数据中的说明进行操作。

步骤 2：停用服务器

在您的 Outposts 服务器当前订阅到期前至少 5 个工作日完成以下步骤。

> **Important**
>
> AWS 在您提交退役申请后，无法停止退货流程。

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. 选择操作。
4. 选择 “停用 Outpos t”，然后按照工作流程删除资源。
5. 选择 Submit request (提交请求)。

> **Note**
>
> 在当前订阅结束之前归还您的 Outposts 服务器不会终止与此 Outpost 相关的任何未付费用。

第 3 步：获取退货货件标签

> **Important**
>
> 您只能使用 AWS 提供的发货标签，因为它包含有关您要退回的服务器的特定信息，例如资产 ID。请勿创建自己的运输标签。

要获取您的货件标签，请执行以下操作：

1. 打开 AWS Outposts 控制台，网址为https://console.aws.amazon.com/outposts/。
2. 在导航窗格上，选择订单。
3. 选择要退回的服务器的顺序。
4. 在订单详情页面的订单状态部分，选择打印退货标签。

> **Note**
>
> 在当前订阅结束之前归还您的 Outposts 服务器不会终止与此 Outpost 相关的任何未付费用。

第 4 步：打包服务器

要打包服务器，请使用提供的包装盒和包装材料 AWS。

1. 用下面一种包装盒来打包服务器：
   - 服务器最初随附的包装盒和包装材料。
   - 更换服务器随附的包装盒和包装材料。

   或者，请联系 AWS 支持 中心申请包装盒。
2. 将 AWS 提供的货件标签粘贴在箱子外面。

   > **Important**
   >
   > 验证运输标签上的资产 ID 是否与您要归还的服务器上的资产 ID 相匹配。
   > 资产 ID 位于服务器正面的拉出式标签上。示例：1203779889 或 9305589922
3. 牢牢封住包装盒。

第 5 步：通过快递归还服务器

您必须通过您所在国家的指定快递公司归还服务器。您可以将服务器交付给快递员，也可以安排您希望快递员取货的日期和时间。 AWS 提供的运输标签包含退回服务器的正确地址。

下表显示了发货国家/地区的联系人：

国家/地区	联系人
阿根廷	联络 AWS 支持 中心。在您的请求中，包含以下信息： • AWS提供的发货标签上的追踪编码
巴林	
巴西	

国家/地区	联系人
文莱	• 您希望快递员取件的日期和时间 • 联系人姓名 • 电话号码 • 电子邮件地址
加拿大	
智利	
哥伦比亚	
中国香港	
印度	
印度尼西亚	
日本	
马来西亚	
尼日利亚	
阿曼	
巴拿马	
秘鲁	
菲律宾	
塞尔维亚	
新加坡	
南非	
韩国	
中国台湾	
泰国	

国家/地区	联系人
阿拉伯联合酋长国	
越南	
United States of America	请联系 UPS。 您可以通过以下方式归还服务器： • 在所在地的 UPS 例行取件期间归还服务器。 • 将服务器送到 UPS 地点。 • 在您希望的日期和时间安排取件。输入 AWS 提供的运输标签上的追踪号码，即可享受免费运输。
所有其他国家	请联系 DHL。 您可以通过以下方式归还服务器： • 将服务器送到 DHL 地点。 • 在您希望的日期和时间安排取件。输入 AWS 提供的货件标签上的 DHL 运单编号，即可享受免费配送。 如果您收到以下错误 `Courier pickup can't be scheduled for an import shipment`，则通常意味着您选择的取件国家/地区与归还运输标签上的取件国家/地区不匹配。请选择发货的国家/地区，然后重试。

转换为订 month-to-month阅

要转换为 month-to-month订阅并保留现有的 Outposts 服务器，无需执行任何操作。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次日开始。

的配额 AWS Outposts

您的每个配额 AWS 账户 都有默认配额，以前称为限制 AWS 服务。除非另有说明，否则，每个配额是区域特定的。您只能请求提高某些配额，并非所有。

要查看的配额 AWS Outposts，请打开 S ervice Quotas 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《服务配额用户指南》中的请求提高配额。

您的 AWS 账户 配额与以下有关 AWS Outposts。

资源	默认	可调整	评论
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。 你可以在账户的每个区域拥有 100 个 Outposts AWS 站点。
每个站点的 Outpost	10	是	AWS Outposts 包括硬件和虚拟资源，称为 Outposts。此限额限制了您的 Outpost 虚拟资源。 每个 Outpost 站点可以包含 10 个 Outpost。

AWS Outposts 以及其他服务的配额

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。

Outposts 服务器的文档历史记录

下表介绍 Outposts 服务器的文档更新。

变更	说明	日期
AWS Outposts 支持来自戴尔和慧与存储阵列的外部块卷	您可以使用由第三方供应商（例如戴尔和HPE Alletra Storage MP B10000）支持的外部块数据 PowerStore 和启动卷。	2025年9月30日
续订您的订阅并为服务器退货做好准备	要续订订阅或退回服务器，您必须在当前订阅结束前至少 10 个工作日完成该流程。	2025 年 7 月 16 日
对服务链路连接进行故障排除	如果您的 Outposts 服务器和 AWS 地区之间的连接中断，请按照以下步骤进行故障排除和解决。	2025 年 5 月 5 日
静态稳定性更新	如果您的网络中断，实例指标和日志将在本地缓存最多 7 天。以前，Outposts只能将日志缓存几个小时。	2025 年 5 月 1 日
资产层面的容量管理	您可以在资产级别修改容量配置。	2025 年 3 月 31 日
由第三方存储器支持的外部块卷	现在，您可以在 Outpost 的实例启动过程中连接由兼容的第三方块存储系统支持的块数据卷。	2024 年 12 月 1 日
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

End-of-term AWS Outposts 服务器选项	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
为 Outposts 服务器创建了 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
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
引入 Outposts 服务器	添加了 Outposts 服务器，这是一种全新的外 AWS Outposts 形。	2021 年 11 月 30 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。