服务器用户指南

AWS Outposts

AWS Outposts: 服务器用户指南

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。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。
- 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

资源类型	机架	服务器
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。

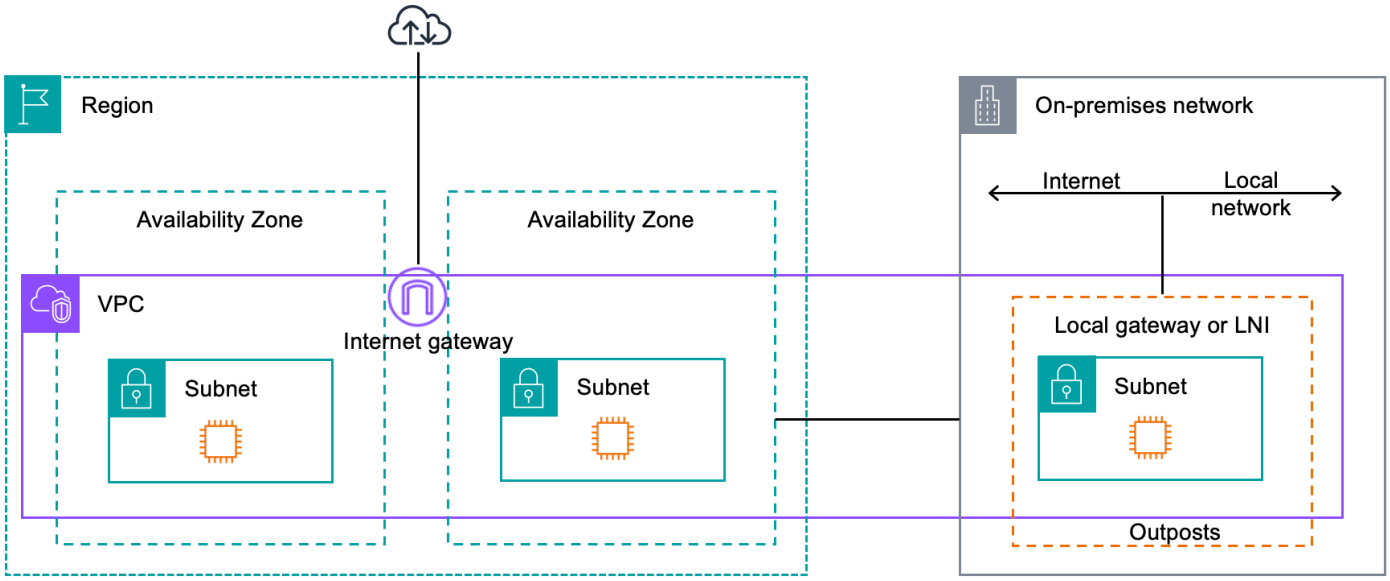
内容

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。

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 本地网络接口。

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 服务器常见问题。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 Outpost 机架的要求，请参阅适用于 Outpost 机架的AWS Outposts 用户指南中的 Outpost 机架站点要求。

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）的过滤器来过滤空气。
- 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。

  > **Important**
  >
  > 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）。

- 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）、30 英寸深（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）、24 英寸深（610 毫米）

> **Note**
>
> - 不支持垂直安装 AWS Outposts 服务器。
> - Outposts 1U 服务器的宽度与 Outposts 2U 服务器的宽度相同，但高度只有一半，深度也更小

AWS 提供了用于在机架上安装服务器的导轨套件。有关更多信息，请参阅 步骤 3：机架安装。

如果不将服务器安放在机架中，则仍然必须满足本部分中列出的其他要求。

- 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。

联网

每台 Outposts 服务器都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	流量
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。有关更多信息，请参阅 配置 QSFP 网络。

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	DHCP 提供的 DNS 服务器
UDP	443、1024-65535	服务链路 IP	443	Outposts 服务链接端点
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 AWS Direct Connect 连接将 Outpost 连接回该 AWS 地区。对于 Outposts 服务链路连接，你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 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连接与该地区的服务链路。 AWS 每台 Outpost 服务器的最大利用率为 500 Mbps。要提高连接速度，请使用多台 Outpost 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 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 服务器不缓存 AMI。每次启动实例时，都会从该区域下载 AMI。

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。

服务链路需要 DHCP 响应

服务链路需要 IPv4 DHCP 响应才能配置网络设置。

服务链路最大延迟

服务链路可以支持服务器与其可用区之间最长 250 ms 的网络延迟。

Power

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 主机中选择 “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，您需要一条 IEC C13 转 IS1293 电源线。

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 Outpost 服务器安装。

当您确认您的账户中有 Outposts 服务器的 Amazon EC2 容量可用时，安装即告完成。 AWS

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
- Outpost 服务器安装
- 在你的 Outpost 服务器上启动一个实例

创建一个 Outpost 并订购 Outpost 容量

要开始使用 AWS Outposts，请使用将拥有 Outpost 的 AWS 账号登录。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 。
- 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。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. 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，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。

步骤 3：下订单

订购你需要的 Outposts 服务器。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。如果您选择部分预付或不预付的付款选项，则需要在三年期内按月支付费用。

  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。

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。

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 Su AWS pport。

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 the section called “Outpost 服务器安装”。

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 Outpost 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”。

Outpost 服务器安装

订购 Outpost 服务器后，您需要负责安装，可以是您自己安装，也可以与第三方签订安装合同。安装方需要特定的权限才能验证新设备的身份。有关更多信息，请参阅授予权限。

先决条件

您的站点必须符合 Outpost 服务器外形规范。有关更多信息，请参阅 创建一个 Outpost 并订购 Outpost 容量。

> **Note**
>
> 我们建议您在安装之前和安装过程中观看安装 AWS Outposts 服务器培训视频。要访问培训，你必须登录 AWS Skill Builder 或在其中创建一个账户。

任务

- 步骤 1：授予权限
- 步骤 2：检查
- 步骤 3：机架安装
- 步骤 4：开机
- 步骤 5：连接网络
- 步骤 6：授权服务器
- Outpost 配置工具命令参考

步骤 1：授予权限

要验证新设备的身份，你必须在包含 Outpost 的 AWS 账户 中具有 IAM 凭据。AWSOutpostsAuthorizeServerPolicy 策略可授予安装 Outpost 服务器所需的权限。有关更多信息，请参阅 the section called “Identity and Access Management”。

注意事项

- 如果您使用的第三方无法访问您的 AWS 账户，则必须提供临时访问权限。
- AWS Outposts 支持使用临时证书。您可以配置有效期最长为 36 小时的临时证书。确保给安装程序足够的时间来执行服务器安装的所有步骤。有关更多信息，请参阅 the section called “临时凭证”。

步骤 2：检查

要完成对 Outposts 设备的检查，您应该检查运输包裹是否损坏，拆开运输包装，并找到 Nitro 安全密钥（NSK）。请考虑以下有关检查服务器的信息：

- 运输包裹有冲击传感器，位于包装箱最大的两个侧面。
- 运输包裹的内侧翻盖包含有关如何拆开服务器包装和找到 NSK 的说明。
- NSK 是一个加密模块。要完成检查，您需要找到 NSK。您可在稍后的步骤中将 NSK 连接到服务器。

检查配送包裹

要检查配送包裹

- 在打开包装之前，请观察两个冲击传感器，并观察它们是否已激活。如果冲击传感器已激活，则设备可能已损坏。继续安装，花点时间记录服务器或配件是否有任何进一步的损坏。如果系统的任何部分明显损坏或安装无法按预期进行，请联系 Su AWS pport 获取有关更换 Outposts 服务器的指导。

如果传感器中间的条为红色，则表示传感器已激活。

拆开配送包裹

要拆开配送包裹

- 打开包装，确保其中包含以下物品：
  - Server
  - Nitro 安全密钥（加密模块）— 包装上标有红色的“NSK”。有关更多信息，请参阅以下从配送包装中找到 NSK 的程序。

- 机架安装套件（2 个内部导轨、2 个外部导轨和螺钉）
- 安装手册
- 附件套装
  - 一对 C13/14 电源线 — 10 英尺（3 米）
  - QSFP 分支电缆 — 10 英尺（3 米）
  - USB 电缆，micro-USB 转 USB-C — 10 英尺（3 米）
  - 刷子防护罩

找到 NSK

NSK 位于标有 A 的盒子里，其中装有服务器的附件。

> **Important**
>
> 在安装过程中，请勿使用 NSK 销毁服务器上的数据。

需要使用 NSK 才能激活服务器。NSK 还用于在您寄回服务器时销毁服务器上的数据。在此安装步骤中，请忽略 NSK 主体上的说明，因为这些说明是为了销毁数据。

步骤 3：机架安装

要完成此步骤，必须将内导轨连接到服务器，将外导轨连接到机架，然后将服务器安装在机架上。您需要一把十字螺丝刀才能完成这些步骤。

机架安装替代方案

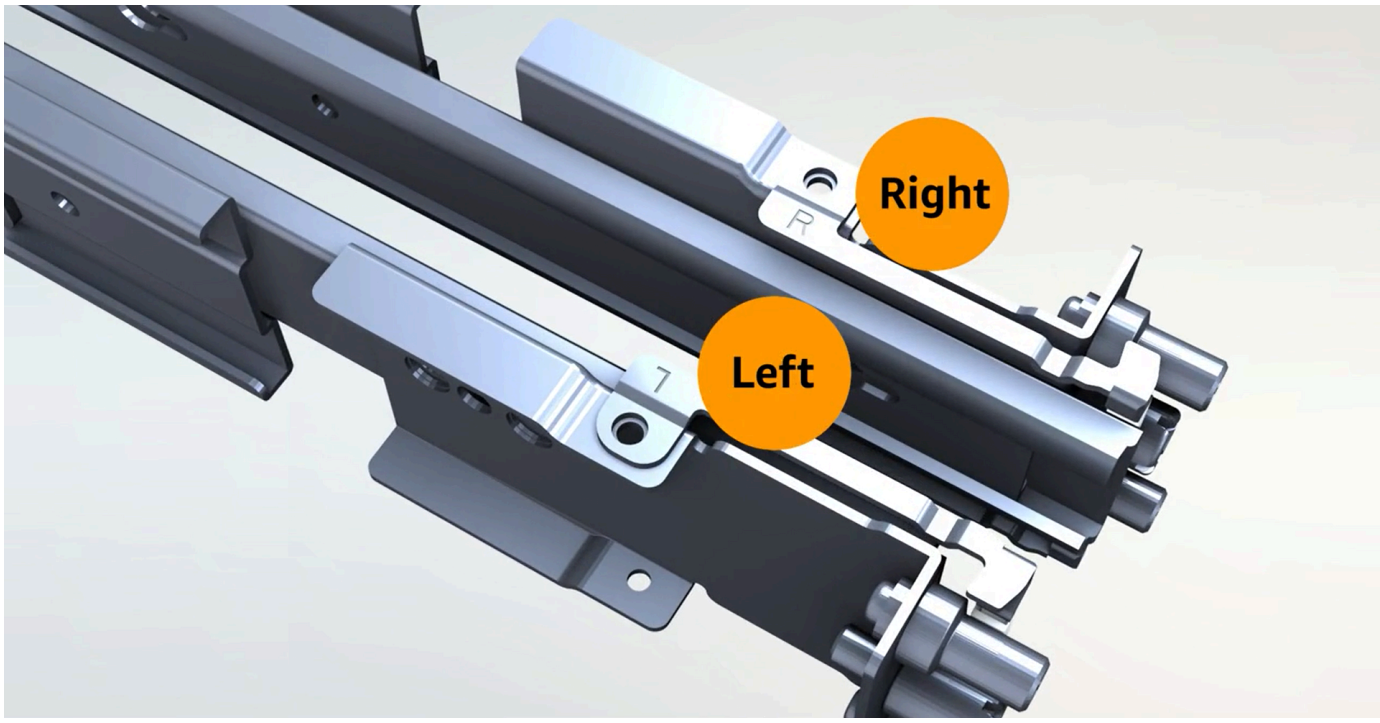
您无需将服务器安装在机架中。如果您没有将服务器安装在机架中，请考虑以下信息：

- 确保服务器与服务器前后的墙壁之间至少留出 6 英寸（15 厘米）的间隙，以使热空气流通。
- 将服务器放在稳定的表面上，避免潮湿或掉落物体等机械危险。
- 要使用服务器随附的网络电缆，必须将服务器放置在距离上游网络设备 10 英尺（3 米）以内。
- 按照当地的指导进行抗震支撑和粘接。

识别侧面和末端

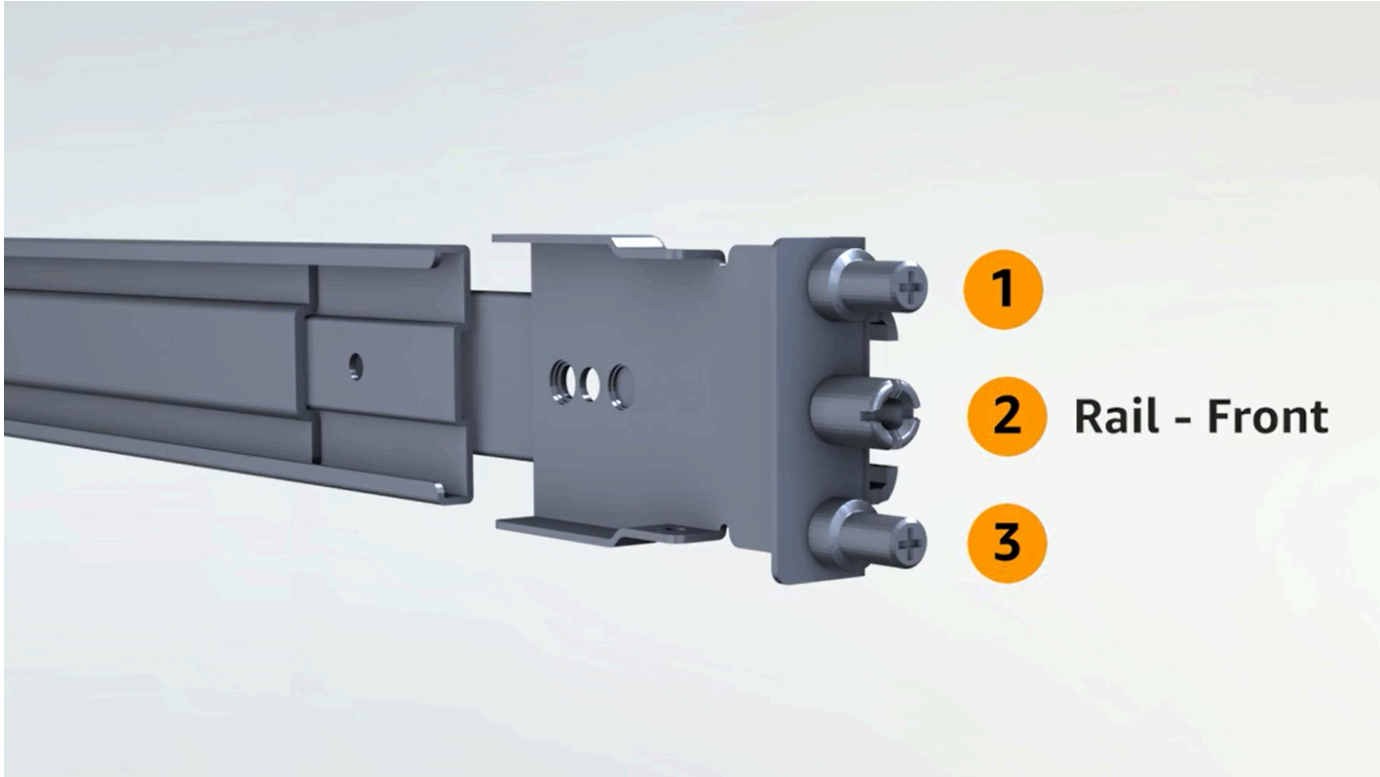
识别前后左右

1. 定位并打开服务器随附的机架导轨盒。
2. 查看导轨上的标记，确定左边和右边。这些标记决定了每个导轨附加到服务器的哪一侧。

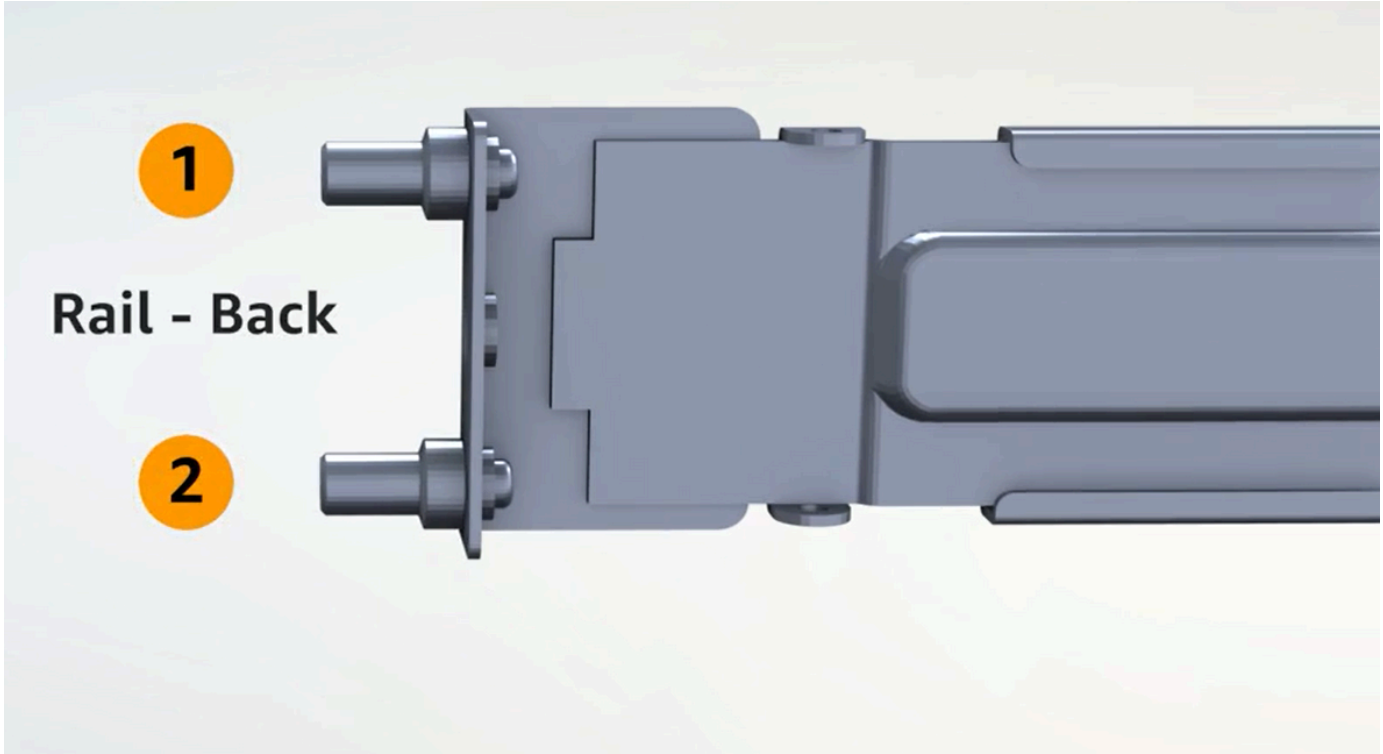


3. 查看导轨两端的柱子，确定前面和后面。

   前端有三个柱子。



后端有两个柱子。



连接内部导轨

要将内部导轨连接到服务器

1. 将两根导轨的内部导轨与外部导轨分开。您应该有四个导轨。
2. 将右侧内部导轨固定在服务器的右侧，然后用螺丝固定导轨。确保导轨与服务器的方向正确。将导轨的正面指向服务器的正面。
3. 将左侧的内部导轨固定在服务器的左侧，然后用螺丝固定导轨。

连接外部导轨

要将外部导轨固定在机架上

1. 面对机架并使用机架右侧标有 R 的导轨。先将导轨的背面安装到机架上，然后延长导轨以将其连接到机架正面。

   > **Tip**
   >
   > 请注意导轨的方向。如有必要，请使用随附的插销连接器。

2. 对位于左侧的左侧导轨重复以上步骤。

安装服务器

将服务器安装到机架中

- 将服务器滑入上一步中安装在机架上的外部导轨，然后用提供的两颗螺钉将服务器固定在正面。

  > **Tip**
  >
  > 由两个人将服务器滑入机架。

步骤 4：开机

要完成开机，您需要连接 NSK，将服务器连接到电源，然后验证服务器是否已开机。请考虑以下有关服务器开机的信息：

- 服务器使用一个电源即可运行，但 AWS 建议您使用两个电源来实现冗余。

- 在连接网络电缆之前，请先连接电源线。
- 使用一对 C13 插座/C14 插座电源线将服务器连接到机架上的电源。如果您不使用 C14 插座电源线将服务器连接到机架上的电源，则必须为连接到电源的 C14 插座提供适配器。

连接 NSK

您必须将 NSK 连接到服务器，这样它才能在运行期间解密服务器上的数据。

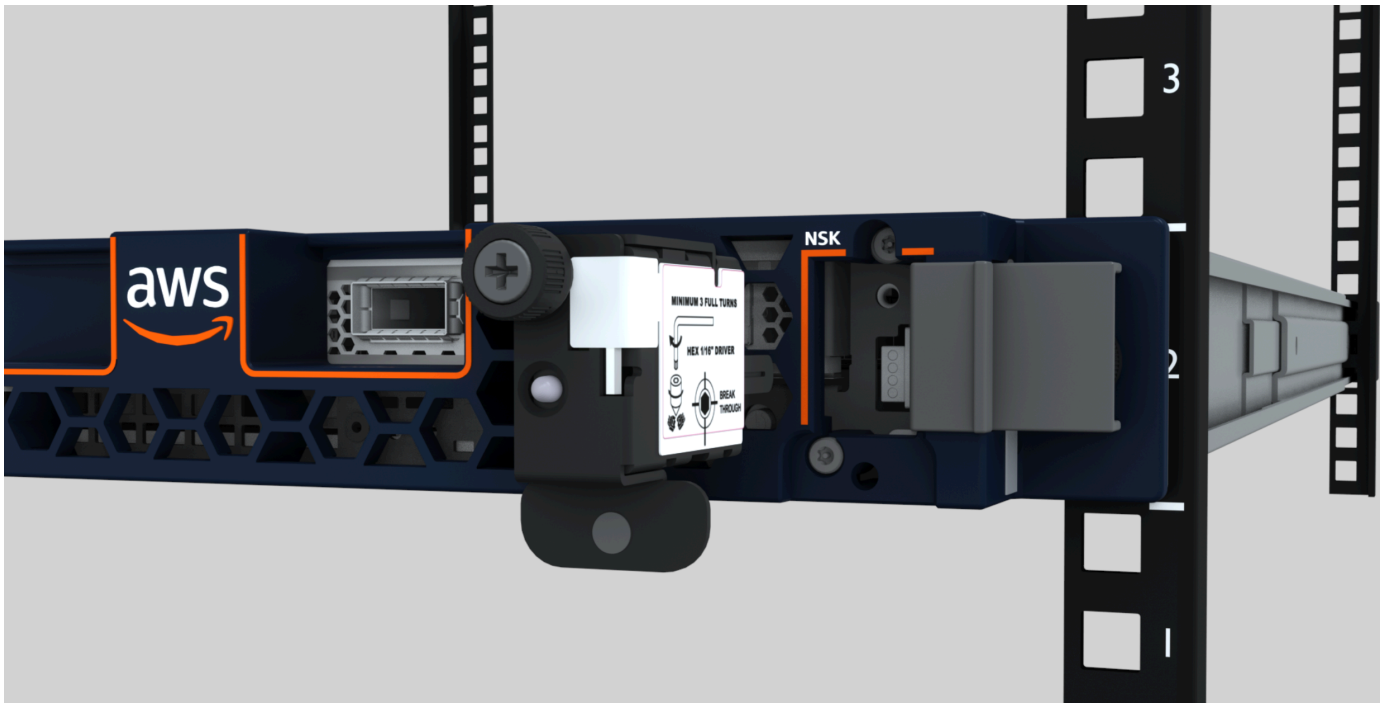
> **Important**
>
> - NSK 的侧面包含关于如何销毁 NSK 的说明。现在不要按照这些说明进行操作。只有在将服务器寄回给 AWS时才按照这些说明进行操作，目的是以加密方式粉碎服务器上的数据。
> - 如果要同时安装多台服务器，请确保不要混淆这些 NSK。您必须将 NSK 连接到配套的服务器。如果您使用其他 NSK，则服务器将无法启动。

要连接 NSK

1. 在服务器的右前方，打开 NSK 隔间。

   下图显示了连接到 2U 服务器的 NSK。

下图显示了连接到 1U 服务器的 NSK。

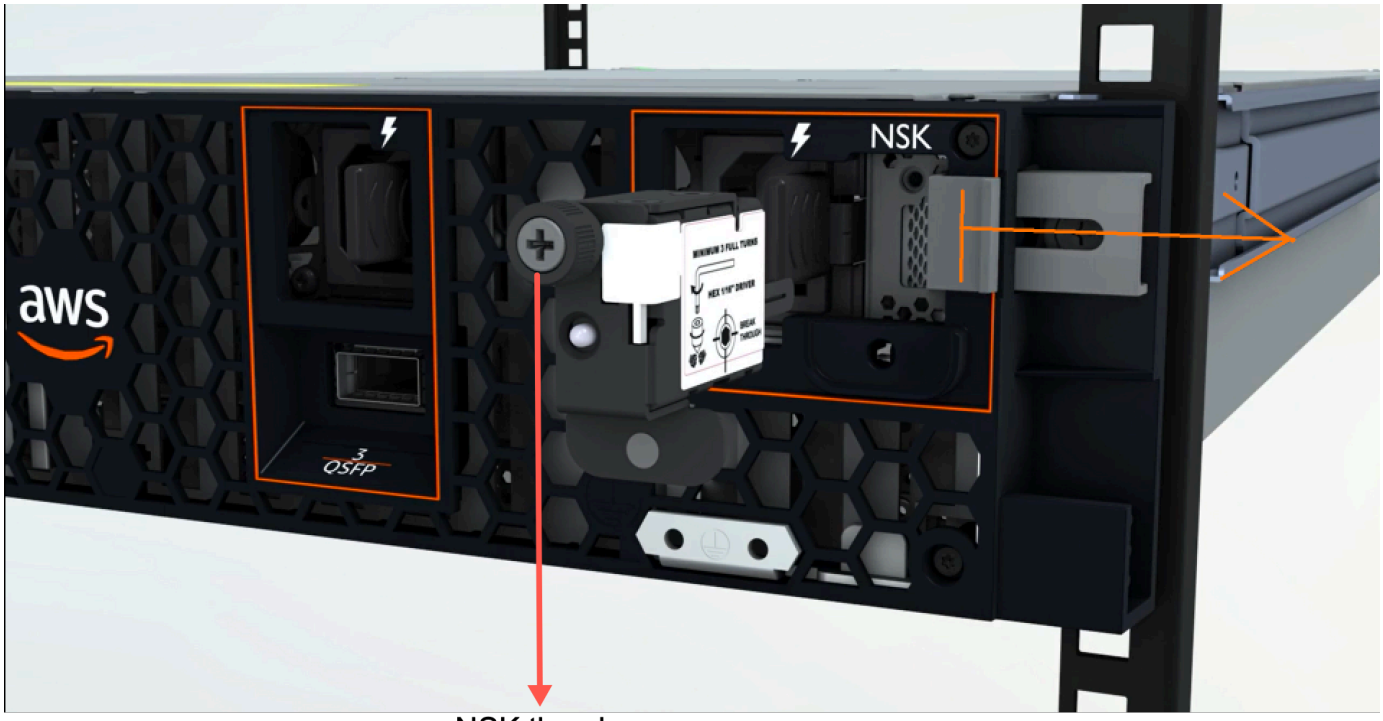


2. 确保 NSK 上的序列号 (SN) 与服务器 NSK 隔间挡板外拉手上的 SN 相匹配。

   下图显示了 NSK 和挡板外拉手上的 SN 号：

3. 将 NSK 放入插槽中。
4. 使用指旋螺丝用手拧紧或用螺丝刀 (0.7 Nm/0.52 lb-ft) 拧紧直至紧固。请勿使用电动工具，因为可能会产生过大扭矩并损坏 NSK。

   下图显示了指旋螺丝的位置。



NSK thumbscrew

下图显示了可用于将 NSK 附加到服务器的螺丝刀类型。

开机

将连接到服务器电源

1. 找到服务器附带的 C13/C14 电源线。

2. 将两根电缆的 C14 端连接到电源。
3. 将两根电缆的 C13 端连接到服务器正面的端口。

验证服务器电源

验证服务器是否已通电

1. 确认您能听到服务器运行的声音。

> **Tip**
>
> 服务器自行配置后，噪音水平会降低。

2. 验证电源端口上方的 LED 电源指示灯是否亮起。

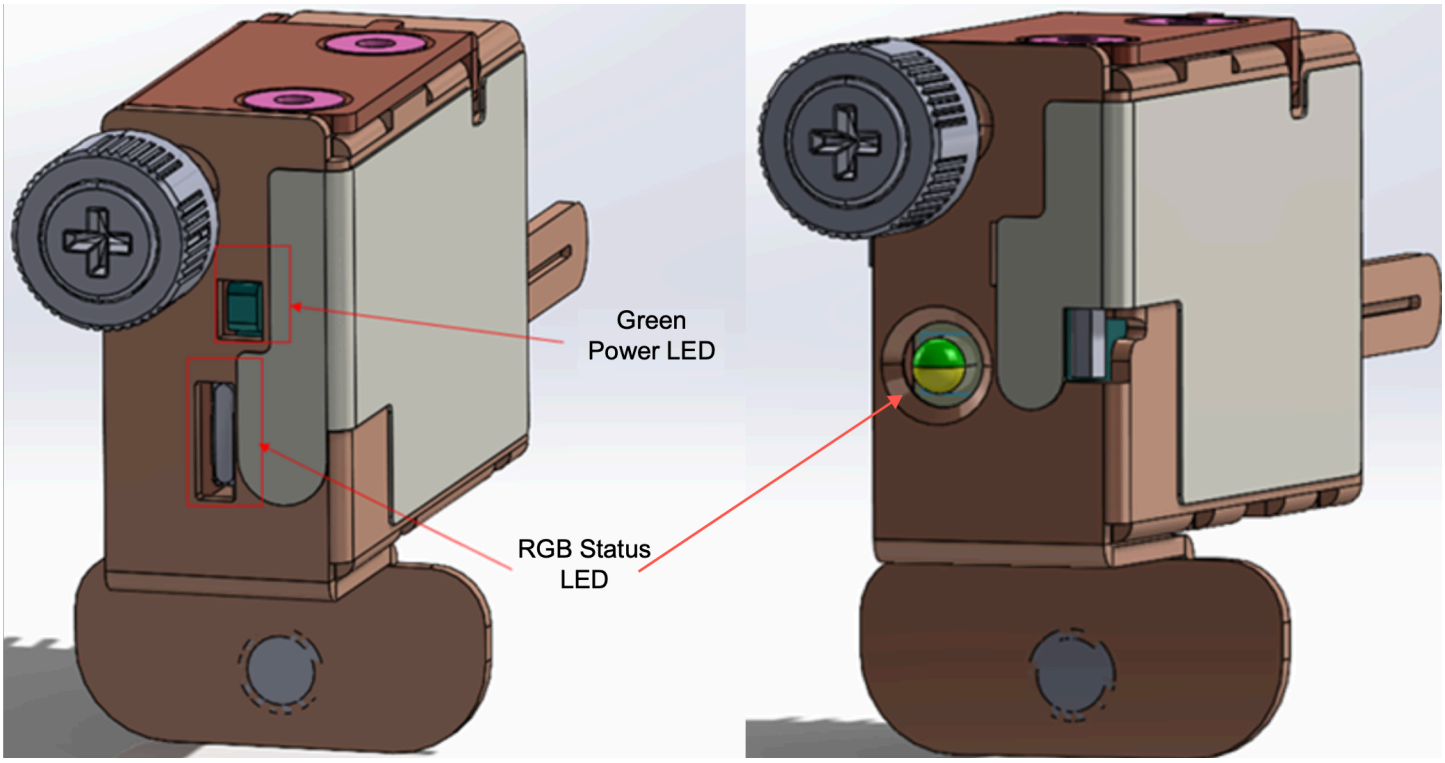
   下图显示了 2U 服务器上的 LED 电源指示灯

   下图显示了 1U 服务器上的 LED 电源指示灯

检查 Atlas 3.0 上的电源指示灯。NSK

AWS Outposts 支持 NSK 的两个版本：Atlas 2.0 和 Atlas 3.0。两个 NSK 版本都有 RGB 状态指示灯。此外，Atlas 3.0 还有一个绿色的电源 LED。此步骤仅适用于 Atlas 3.0 NSK。

下图显示了 Atlas 2.0 和 Atlas 3.0 NSK 上 LED 的位置：



Atlas 3.0 Atlas 2.0

如果你有 Atlas 2.0 NSK，请跳到下一步，步骤 5：连接网络因为这个版本的 NSK 只有 RGB 状态 LED，你必须在配置和激活 Outpost 服务器后检查它。

如果你有 Atlas 3.0 NSK，请检查绿色的电源 LED：

- 如果绿灯亮起，则表示 NSK 已正确连接到主机并已通电。您可以继续下一步。
- 如果绿灯熄灭，则表示 NSK 未正确连接到主机或/且无法通电。联系我们 AWS Support。

步骤 5：连接网络

要完成网络设置，请使用网络电缆将服务器连接到上游网络设备。

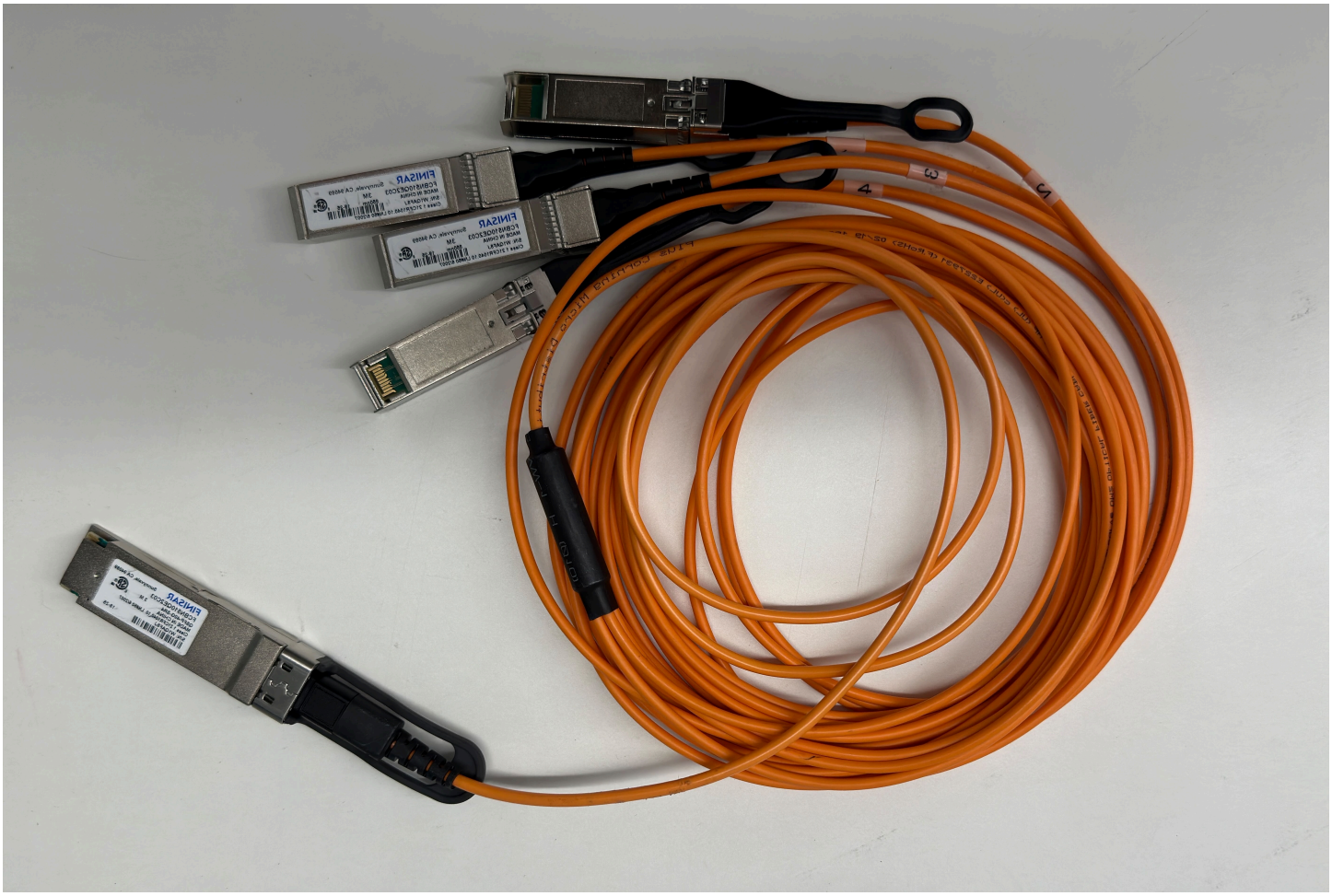
请考虑以下有关连接到网络的信息：

- 服务器需要连接两种类型的流量：服务链路流量和本地网络接口 (LNI) 链路流量。下一节中的说明描述了在服务器上使用哪些端口来分段流量。请咨询您的 IT 小组，以确定上游网络设备上的哪个端口应传输每种类型的流量。
- 确保服务器已连接到您的上游网络设备并已被分配一个 IP 地址。有关更多信息，请参阅 服务器 IP 地址分配。
- AWS Outposts 服务器上的光纤连接仅支持 10 Gbits，不支持端口速度的自动协商。如果主机端口尝试协商端口速度（例如，在 10 到 25 Gb 之间），则可能会遇到问题。在这种情况下，建议执行以下操作：
  - 将交换机端口上的端口速度设置为 10 Gb。
  - 请与您的交换机供应商合作以支持静态配置。

配置 QSFP 网络

使用 QSFP 分支电缆，您可以使用分支来分段流量。

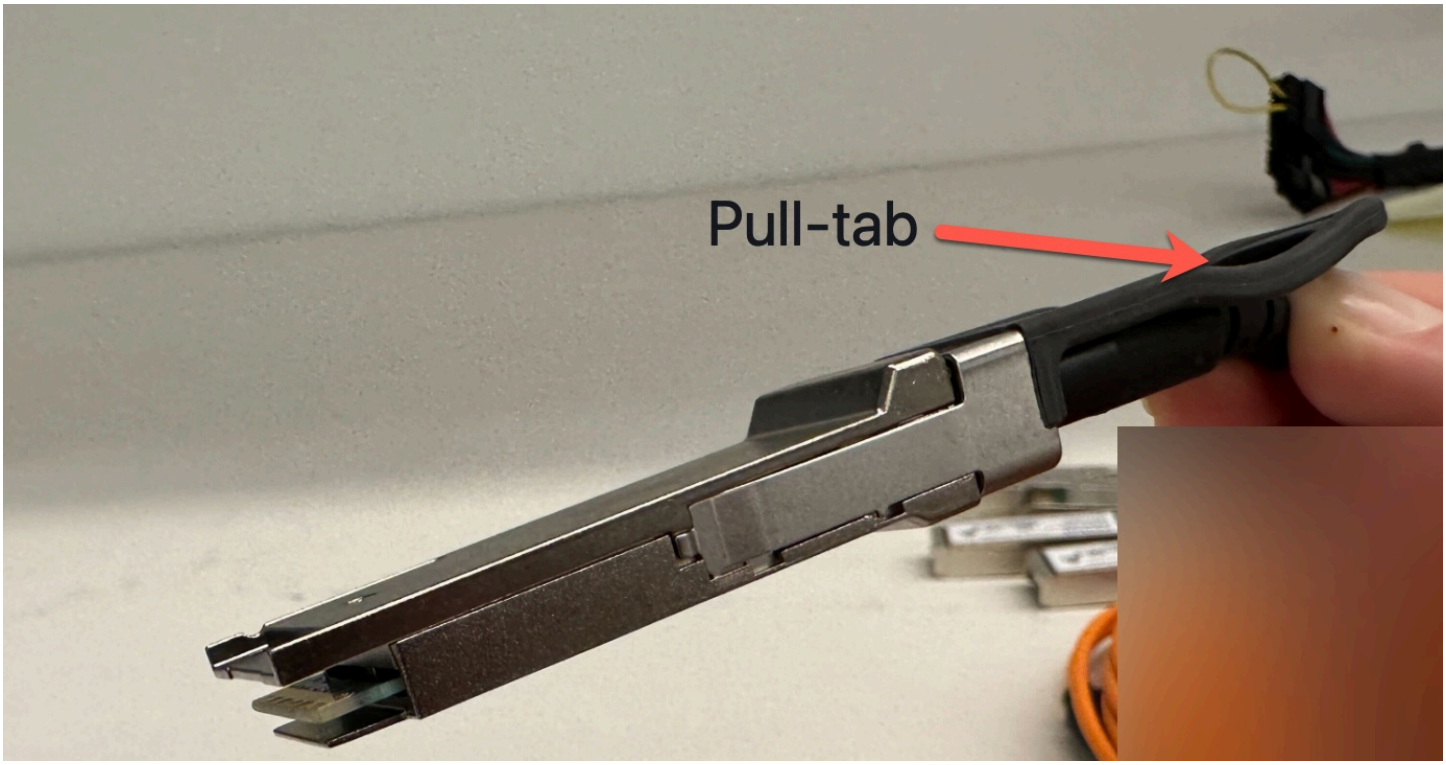
下图显示了 QSFP 分支电缆：



> **Note**
>
> AWS Outposts 服务器在 QSFP 端口旁边有一个物理 RJ45 端口。但是，未启用此 RJ45 端口供任何客户使用。如果你需要 RJ45 1Gbe 连接，请使用随附的 QSFP 电缆将 10GBASE-X SFP+ 连接到 1Gbase RJ45 媒体转换器。

QSFP 电缆的一端只有一个接头。将这一端连接到服务器。

下图显示了带有单个连接器的电缆的末端：



QSFP 电缆的另一端有 4 根分支电缆，标有 1 到 4。使用标有 1 的电缆传输 LNI 链接流量，使用标有 2 的电缆传输服务链路流量。

下图显示了带有 4 根分支电缆的电缆末端：

要使用 QSFP 分支电缆将服务器连接到网络

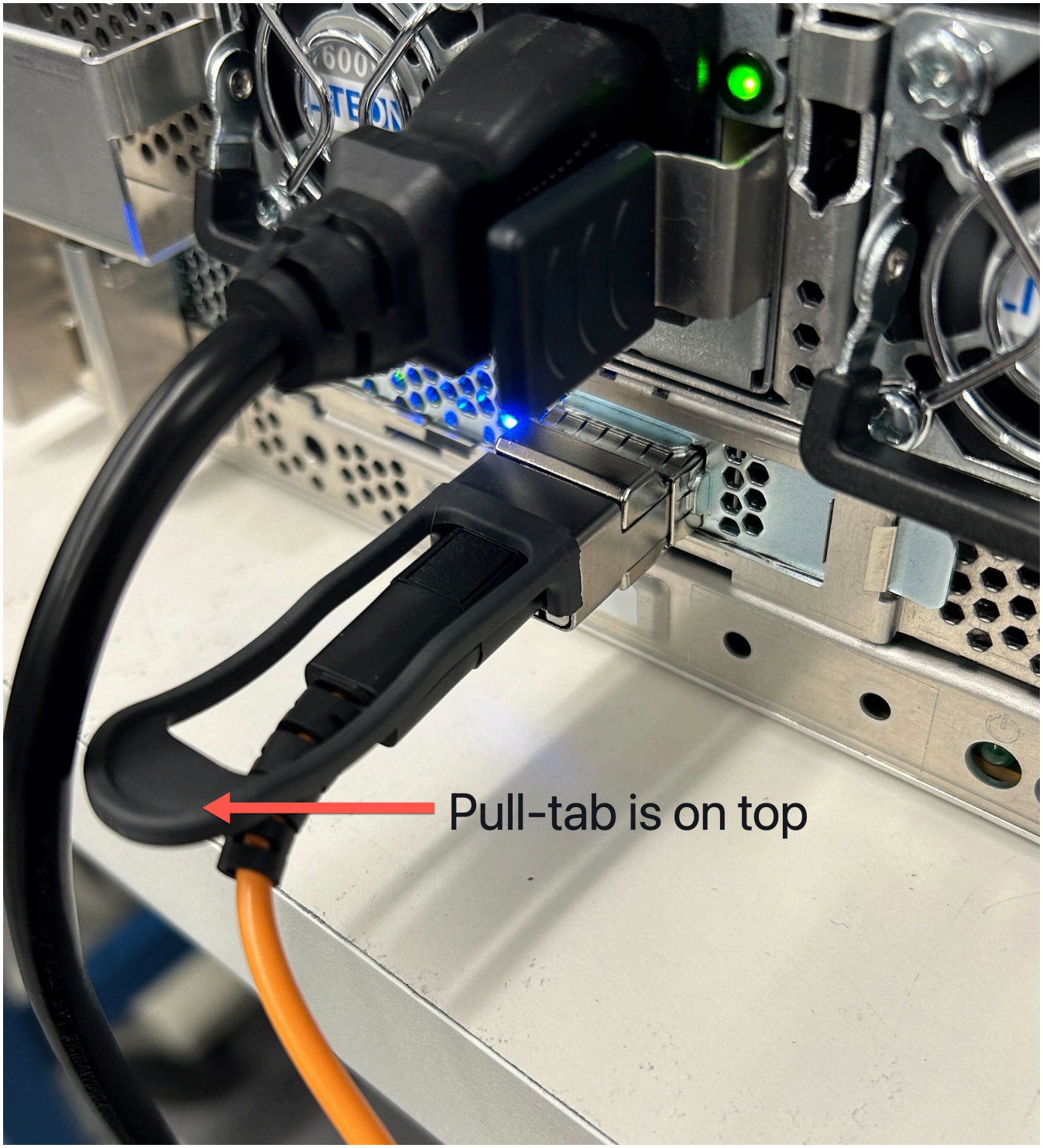
1. 找到服务器附带的 QSFP 分支电缆。
2. 将 QSFP 分支电缆的单端连接到服务器上的 QSFP 端口。
   1. 找到 QSFP 端口。

      下图显示了 2U 服务器上 QSFP 端口的位置。

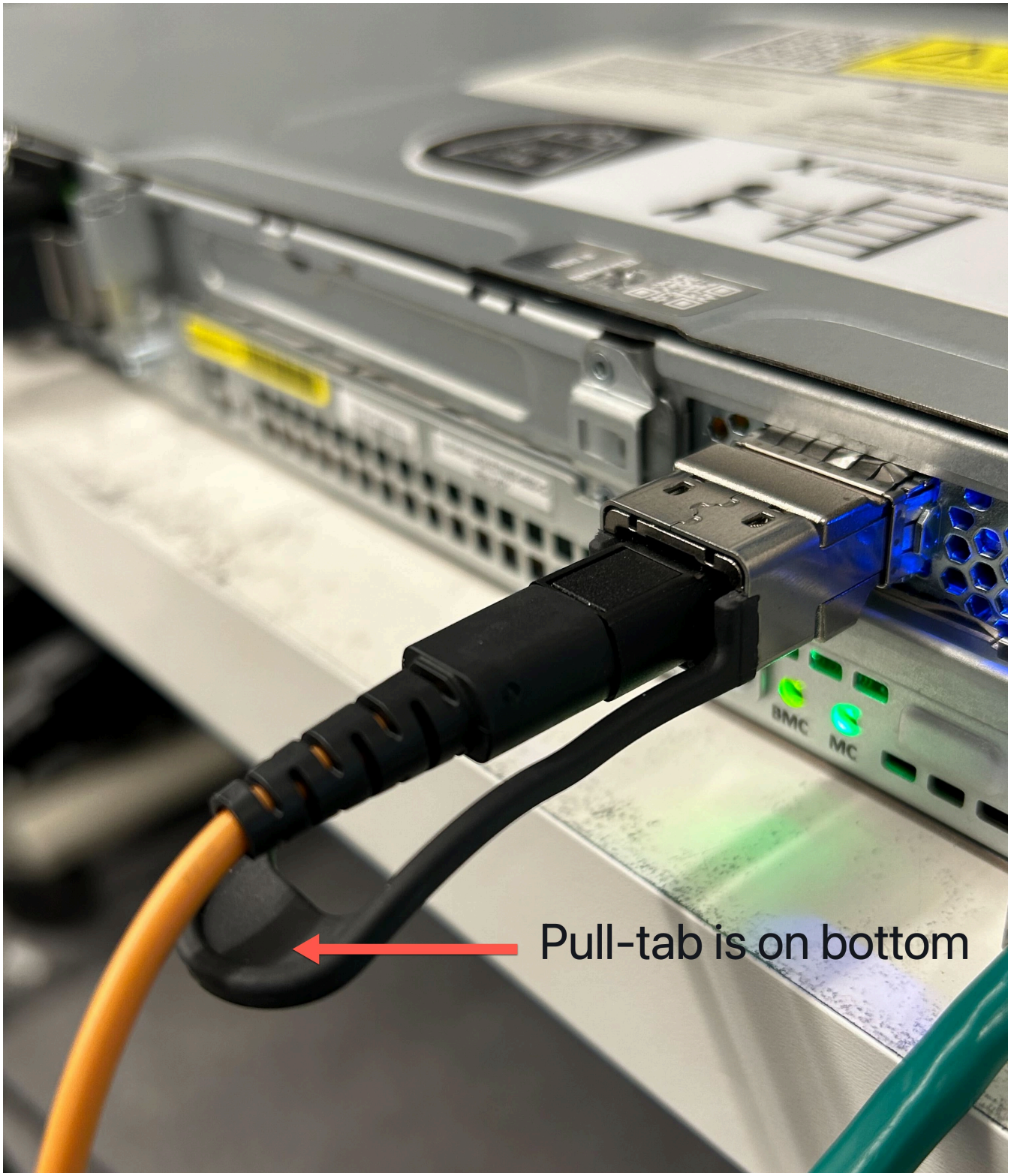
下图显示了 1U 服务器上 QSFP 端口的位置。

2. 插入 QSFP，拉片朝正确的方向移动。

   对于 2U 服务器，插入顶部有拉片的 QSFP，如下图所示。



对于 1U 服务器，插入底部有拉片的 QSFP，如下图所示。



3. 确保在插入电缆时感觉到或听到咔嗒声。这表明您已正确插入电缆。

3. 将 QSFP 电缆的分支 1 和 2 连接到上游网络设备。

> **Important**
>
> 要让 Outpost 服务器正常运行，需要以下两条电缆。
>
> - 使用标有 1 的电缆传输 LNI 链路流量。
> - 使用标有 2 的电缆传输服务链路流量。

步骤 6：授权服务器

要授权服务器，必须使用 USB 电缆将笔记本电脑连接到服务器，然后使用基于命令的串行协议测试连接并授权服务器。除了 IAM 凭证外，您还需要一根 USB 电缆、一台笔记本电脑和串行终端软件（例如 Putty 或 screen）才能完成这些步骤。

或者，如果您的安卓手机或平板电脑带有 USB-C 或微型 USB 接口，支持 USB On The Go (OTG)，那么您可以使用 Outposts Server Activator 应用程序引导您完成服务器授权流程。你可以从 Google Play 下载该应用程序

请考虑以下有关授权服务器的信息：

- 要对服务器进行授权，您或安装服务器的一方需要在包含 Outpost AWS 账户 的 IAM 证书。有关更多信息，请参阅 the section called “步骤 1：授予权限”。
- 测试您的连接时您无需使用 IAM 凭证进行身份验证。
- 在使用导出命令将 IAM 凭证设置为环境变量之前，请考虑先测试连接。
- 为了保护您的账户，Outpost 配置工具永远不会保存您的 IAM 凭证。
- 要将笔记本电脑连接到服务器，请务必先将 USB 电缆一端插入笔记本电脑，另一端插入服务器。

任务

- 将您的笔记本电脑连接到服务器
- 创建与服务器的串行连接
- 测试连接
- 对服务器进行授权
- 验证 NSK 指示灯

将您的笔记本电脑连接到服务器

将 USB 电缆一端连接到笔记本电脑，另一端连接到服务器。该服务器包括一个 USB 芯片，可在笔记本电脑上创建虚拟串行端口。您可以使用此虚拟串行端口通过串行终端仿真软件连接到服务器。您只能使用此虚拟串行端口来运行 Outpost 配置工具命令。

要将笔记本电脑连接到服务器

将 USB 电缆一端插入笔记本电脑，另一端插入服务器。

> **Note**
>
> USB 芯片需要驱动程序来创建虚拟串行端口。如果所需的驱动程序尚不存在，则您的操作系统应自动安装。要下载和安装驱动程序，请参阅 FTDI 的安装指南。

创建与服务器的串行连接

本部分包含使用常用串行终端程序的说明，但您无需使用这些程序。使用您喜欢的串行终端程序，连接速度为 `115200` 波特。

示例

- Windows 串行连接
- Mac 串行连接

Windows 串行连接

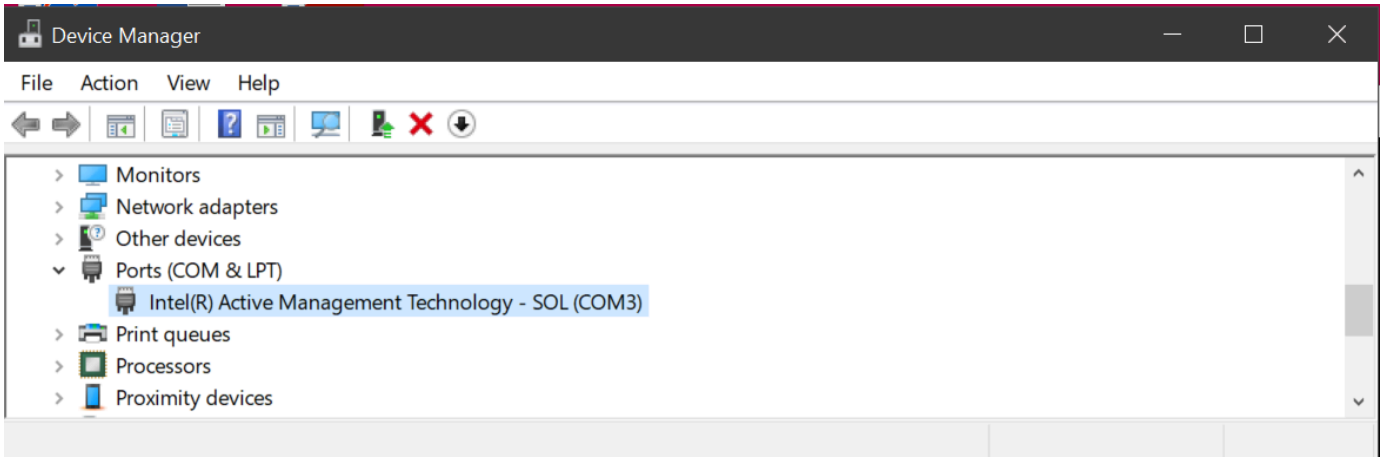
以下说明适用于 Windows 上的 PuTTY。PuTTY 是免费的，但您可能需要下载。

下载 PuTTY

从 PuTTY 下载页面下载 PuTTY 并安装。

要使用 PuTTY 在 Windows 上创建串行终端

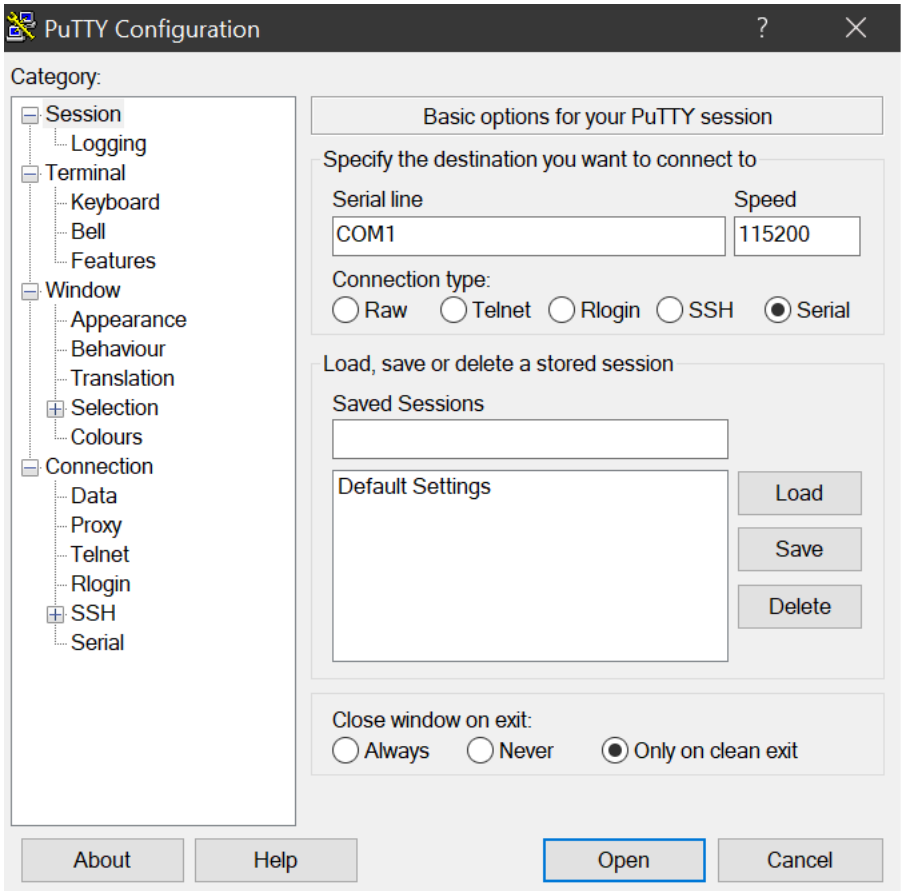
1. 将 USB 电缆一端插入 Windows 笔记本电脑，另一端插入服务器。
2. 在桌面上，右键单击开始，然后选择设备管理器。
3. 在设备管理器中，展开端口（COM 和 LPT）以确定 USB 串行连接的 COM 端口。您将看到一个名为 USB 串行端口 (COM #) 的节点。COM 端口的值取决于您的硬件。



4. 在 PuTTY 中，从会话中选择串行作为连接类型，然后输入以下信息：

   - 在串行线路下，输入设备管理器中显示的 COM#。
   - 在速度下输入：115200

   下图显示 PuTTY 配置页面上的示例：



5. 选择打开。

此时显示一个空的控制台窗口。可能需要 1 到 2 分钟才会出现以下内容之一：

- `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
- `Outpost>` 提示。

Mac 串行连接

以下说明适用于 macOS 上的 screen。您可以找到操作系统中包含的 screen。

要在 macOS 上使用 screen 创建串行终端

1. 将 USB 电缆一端插入 Mac 笔记本电脑，另一端插入服务器。
2. 在终端中，列出 `/dev` 并使用 `*usb*` 条件来筛选输出，以查找虚拟串行端口。

```
ls -ltr /dev/*usb*
```

串行设备显示为 `tty`。例如，请考虑以下上一个列表命令的示例输出。

```
ls -ltr /dev/*usb*
crw-rw-rw-  1 root  wheel   21,   3 Feb  8 15:48 /dev/cu.usbserial-EXAMPLE1
crw-rw-rw-  1 root  wheel   21,   2 Feb  9 08:56 /dev/tty.usbserial-EXAMPLE1
```

3. 在终端中，将 screen 用于串行设备和串行连接的波特率来设置串行连接。在以下命令中，将 *EXAMPLE1* 替换为您的笔记本电脑中的值。

```
screen /dev/tty.usbserial-EXAMPLE1 115200
```

此时显示一个空的控制台窗口。可能需要 1 到 2 分钟才会出现以下内容之一：

- `Please wait for the system to stabilize. This can take up to 900 seconds, so far x seconds have elapsed on this boot.`
- `Outpost>` 提示。

测试连接

本部分介绍如何使用 Outpost 配置工具测试连接。您不需要 IAM 凭证即可测试连接。您的连接需要能够解析 DNS 才能访问 AWS 区域。

1. 测试链接并收集有关连接的信息
2. 测试 DNS 解析器
3. 测试是否可以访问 AWS 区域

要测试链路

1. 先将 USB 电缆一端插入笔记本电脑，另一端插入服务器。
2. 使用串行终端程序（例如 PuTTY 或 screen）连接到服务器。有关更多信息，请参阅 the section called “创建与服务器的串行连接”。
3. 按下 Enter 可访问 Outpost 配置工具命令提示符。

```
Outpost>
```

> **Note**
>
> 如果您在开机后在左侧看到服务器机箱内持续出现红灯，并且无法连接到 Outpost 配置工具，则可能需要关闭服务器电源并耗尽服务器电量才能继续。要耗尽服务器电量，请断开所有网络和电源线，等待五分钟，然后开机并重新连接网络。

4. 使用 describe-links 可返回有关服务器上网络链接的信息。Outpost 服务器必须有一个服务链路和一个本地网络接口 (LNI) 链路。

```
Outpost>describe-links
---
service_link_connected: True
local_link_connected: False
links:
-
  name: local_link
  connected: False
  mac: 00:00:00:00:00:00
-
  name: service_link
```

```
  connected: True
  mac: 0A:DC:FE:D7:8E:1F
checksum: 0x46FDC542
```

如果任一链路返回了 `connected: False`，请对硬件上的网络连接进行故障排除。

5. 使用 describe-ip 可返回服务链路的 IP 分配状态和配置。

```
Outpost>describe-ip
---
links:
-
  name: service_link
  configured: True
  ip: 192.168.0.0
  netmask: 255.255.0.0
  gateway: 192.168.1.1
  dns: [ "192.168.1.1" ]
  ntp: [ ]
checksum: 0x8411B47C
```

NTP 值可能缺失，因为 NTP 在 DHCP 选项集中是可选的。不能缺少任何其他值。

要测试 DNS

1. 先将 USB 电缆一端插入笔记本电脑，另一端插入服务器。
2. 使用串行终端程序（例如 PuTTY 或 screen）连接到服务器。有关更多信息，请参阅 the section called “创建与服务器的串行连接”。
3. 按下 Enter 可访问 Outpost 配置工具命令提示符。

```
Outpost>
```

> **Note**
>
> 如果您在开机后在左侧看到服务器机箱内持续出现红灯，并且无法连接到 Outpost 配置工具，则可能需要关闭服务器电源并耗尽服务器电量才能继续。要耗尽服务器电量，请断开所有网络和电源线，等待五分钟，然后开机并重新连接网络。

4. 使用 export 输入 Outpost 服务器的父区域作为 `AWS_DEFAULT_REGION` 的值。

AWS_DEFAULT_REGION=##

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: 0xB2A945RE
```

- 请勿在等号 (=) 前后添加空格。
- 不会保存任何环境值。 AWS 区域 每次运行 Outpost 配置工具时都必须导出。
- 如果您聘请第三方安装服务器，则必须向第三方提供父区域。

5. 使用 describe-resolve 确定 Outpost 服务器能否访问 DNS 解析器以及能否解析该区域中 Outpost 配置端点的 IP 地址。至少需要一条带有 IP 配置的链路。

```
Outpost>describe-resolve
---
dns_responding: True
dns_resolving: True
dns: [ "198.xx.xxx.xx", "198.xx.xxx.xx" ]
query: outposts.us-west-2.amazonaws.com
records: [ "18.xxx.xx.xxx", "44.xxx.xxx.xxx", "44.xxx.xxx.xxx" ]
checksum: 0xB6A961CE
```

测试访问权限 AWS 区域

1. 先将 USB 电缆一端插入笔记本电脑，另一端插入服务器。
2. 使用串行终端程序（例如 PuTTY 或 screen）连接到服务器。有关更多信息，请参阅 the section called “创建与服务器的串行连接”。
3. 按下 Enter 可访问 Outpost 配置工具命令提示符。

```
Outpost>
```

> **Note**
>
> 如果您在开机后在左侧看到服务器机箱内持续出现红灯，并且无法连接到 Outpost 配置工具，则可能需要关闭服务器电源并耗尽服务器电量才能继续。要耗尽服务器电量，请断开所有网络和电源线，等待五分钟，然后开机并重新连接网络。

4. 使用 export 输入 Outpost 服务器的父区域作为 `AWS_DEFAULT_REGION` 的值。

   `AWS_DEFAULT_REGION=##`

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: 0xB2A945RE
```

   - 请勿在等号 (=) 前后添加空格。
   - 不会保存任何环境值。 AWS 区域 每次运行 Outpost 配置工具时都必须导出。
   - 如果您聘请第三方安装服务器，则必须向第三方提供父区域。

5. 使用 describe-reachability 确定 Outpost 服务器能否访问该区域中的 Outpost 配置端点。需要有效的 DNS 配置，您可以使用 describe-resolve 来确定该配置。

```
Outpost>describe-reachability
---
is_reachable: True
src_ip: 10.0.0.0
dst_ip: 54.xx.x.xx
dst_port: xxx
checksum: 0xCB506615
```

   - `is_reachable` 表示测试结果
   - `src_ip` 是服务器的 IP 地址。
   - `dst_ip` 是该区域中 Outpost 配置端点的 IP 地址
   - `dst_port` 是服务器用于连接 `dst_ip` 的端口

对服务器进行授权

本部分介绍如何使用 Outpost 配置工具和包含 Outpost 的 AWS 账户中的 IAM 凭证来授权服务器。

要对服务器进行授权

1. 先将 USB 电缆一端插入笔记本电脑，另一端插入服务器。
2. 使用串行终端程序（例如 PuTTY 或 screen）连接到服务器。有关更多信息，请参阅 the section called “创建与服务器的串行连接”。

3. 按下 Enter 可访问 Outpost 配置工具命令提示符。

```
Outpost>
```

> **Note**
>
> 如果您在开机后在左侧看到服务器机箱内持续出现红灯，并且无法连接到 Outpost 配置工具，则可能需要关闭服务器电源并耗尽服务器电量才能继续。要耗尽服务器电量，请断开所有网络和电源线，等待五分钟，然后开机并重新连接网络。

4. 使用 export 在 Outpost 配置工具中输入您的 IAM 凭证。如果您聘请第三方安装服务器，则必须向第三方提供 IAM 凭证。

   要进行身份验证，必须导出以下四个变量。一次导出一个变量。请勿在等号 (=) 前后添加空格。

   - `AWS_ACCESS_KEY_ID=`*`access-key-id`*
   - `AWS_SECRET_ACCESS_KEY=`*`secret-access-key`*
   - `AWS_SESSION_TOKEN=`*`session-token`*
     - 使用 AWS CLI `GetSessionToken`命令获取`AWS_SESSION_TOKEN`。有关更多信息，请参阅AWS CLI 命令参考中的 get-session-token。

       > **Note**
       >
       > 您必须将AWSOutpostsAuthorizeServerPolicy附加到您的 IAM 角色才能获得`AWS_SESSION_TOKEN`。

     - 要安装 AWS CLI，请参阅版本 2 AWS CLI 用户指南中的安装或更新最新版本的 AWS CLI。
   - `AWS_DEFAULT_REGION=`*`##`*

     使用 Outpost 服务器的父区域作为 `AWS_DEFAULT_REGION` 的值。如果您聘请第三方安装服务器，则必须向第三方提供父区域。

   以下示例中的输出显示了成功的导出。

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
```

```
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

5. 使用 start-connection 创建与该区域的安全连接。

   以下示例中的输出显示连接已成功启动。

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connection-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

6. 等待大约 5 分钟。
7. 使用 get-connection 检查是否已建立与该区域的连接。

   以下示例中的输出显示连接已成功。

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

   `keys_exchanged` 和 `connection_established` 更改为 `True` 后，会自动预置 Outpost 服务器并更新为最新的软件和配置。

> **Note**
>
> 请注意以下有关配置过程的信息：
>
> - 激活完成后，您的 Outpost 服务器最多可能要在 10 个小时后才能使用。
> - 在此过程中，您必须保持 Outpost 服务器的电源和网络连接并保持稳定。
> - 在此过程中，服务链路出现波动是正常情况。
> - 如果 `exchange_active` 为 `True`，则表示连接仍在建立中。请 5 分钟后重试。

- 如果 `keys_exchanged` 或 `connection_established` 为 `False` 并且如果 `exchange_active` 为 `True`，则表示连接仍在建立中。请 5 分钟后重试。
- 如果在 1 小时后 `keys_exchanged` 或 `connection_established` 仍为 `False`，请联系 AWS Support 服务中心。
- 如果`primary_status: No such asset id found.`出现该消息，请确认以下内容：
  - 您指定了正确的区域。
  - 您使用的帐户与订购 Outpost 服务器时使用的帐户相同。

  如果区域正确，并且您使用的帐户与订购 Outpost 服务器时使用的帐户相同，请联系 C AWS Support en ter。
- Outpost 的 `LifeCycleStatus` 属性将从 `Provisioning` 变为 `Active`。然后，您将收到一封电子邮件，告知您的 Outpost 服务器已配置并激活。
- 激活 Outposts 服务器后，您无需重新授权 Outposts 服务器。

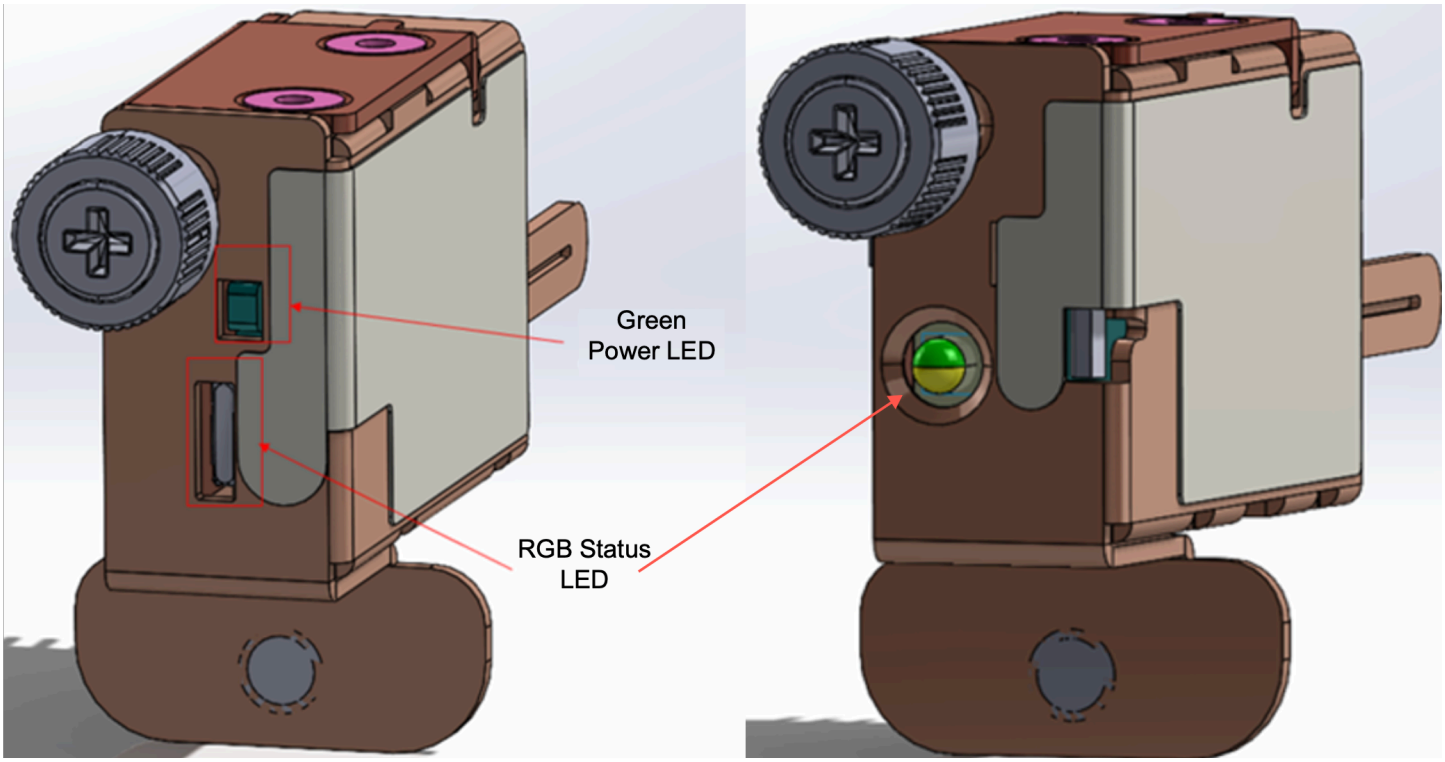
8. 连接成功后，可以断开笔记本电脑与服务器的连接。

验证 NSK 指示灯

配置过程完成后，检查 NSK LED。

AWS Outposts 支持 NSK 的两个版本：Atlas 2.0 和 Atlas 3.0。两个 NSK 版本都有 RGB 状态指示灯。此外，Atlas 3.0 还有一个绿色的电源 LED。

下图显示了 Atlas 2.0 和 Atlas 3.0 上 LED 的位置：



Atlas 3.0 Atlas 2.0

验证 NSK 上的状态和电源指示灯

1. 检查 RGB 状态指示灯的颜色。如果颜色为绿色，则表示NSK是健康的。如果颜色不是绿色，请联系 AWS Support。
2. 如果你有 Atlas 3.0 NSK，请检查绿色的电源 LED。如果绿灯亮起，则表示 NSK 已正确连接到主机并已通电。如果绿灯未亮，请联系 AWS Support。

Outpost 配置工具命令参考

Outpost 配置工具提供以下命令。

命令

- 导出
- Echo
- 描述链路
- 描述 IP
- 描述解析

- 描述可达性
- 开始连接
- 获取连接

导出

导出

使用 export 可将 IAM 凭证设置为环境变量。

语法

```
Outpost>export variable=value
```

export 采用变量赋值语句。

必须采用以下格式：*variable*=*value*

要进行身份验证，必须导出以下四个变量。一次导出一个变量。请勿在等号 (=) 前后添加空格。

- AWS_ACCESS_KEY_ID=*access-key-id*
- AWS_SECRET_ACCESS_KEY=*secret-access-key*
- AWS_SESSION_TOKEN=*session-token*
- AWS_DEFAULT_REGION=*##*

  使用 Outpost 服务器的父区域作为 AWS_DEFAULT_REGION 的值。

Example ：成功导入凭证

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_SESSION_TOKEN=MIICiTCCAfICCQD6m7oRw0uXOjANBgk
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=

result: OK
checksum: example-checksum
```

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum
```

Echo

echo

使用 echo 可显示您使用 export 命令为变量设置的值。

语法

```
Outpost>echo $variable-name
```

####可以是以下之一：

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN
- AWS_DEFAULT_REGION

Example ：成功

```
Outpost>export AWS_DEFAULT_REGION=us-west-2

result: OK
checksum: example-checksum

---

Outpost>echo $AWS_DEFAULT_REGION

variable name: AWS_DEFAULT_REGION
variable value: us-west-2
checksum: example-checksum
```

Example ：由于未使用 export 命令设置变量值而失败

```
Outpost> echo $AWS_ACCESS_KEY_ID

error_type: execution_error
error_attributes:
  AWS_ACCESS_KEY_ID: no value set
error_message: No value set for AWS_ACCESS_KEY_ID using export.
checksum: example-checksum
```

Example ：由于变量名无效而失败

```
Oupost>echo $foo

error_type: invalid_argument
error_attributes:
  foo: invalid variable name
error_message: Variables can only be AWS credentials.
checksum: example-checksum
```

Example ：由于语法问题而失败

```
Outpost>echo AWS_SECRET_ACCESS_KEY

error_type: invalid_argument
error_attributes:
  AWS_SECRET_ACCESS_KEY: not a variable
```

```
error_message: Expecting $ before variable name.
checksum: example-checksum
```

描述链路

describe-links

使用 describe-links 可返回有关服务器上网络链接的信息。Outpost 服务器必须有一个服务链路和一个本地网络接口 (LNI) 链路。

语法

```
Outpost>describe-links
```

describe-links 不包含参数。

描述 IP

describe-ip

使用 describe-ip 可返回每个已连接链路的 IP 分配状态和配置。

语法

```
Outpost>describe-ip
```

describe-ip 不包含参数。

描述解析

describe-resolve

使用 describe-resolve 确定 Outpost 服务器能否访问 DNS 解析器以及能否解析该区域中 Outpost 配置端点的 IP 地址。至少需要一条带有 IP 配置的链路。

语法

```
Outpost>describe-resolve
```

describe-resolve 不包含参数。

描述可达性

describe-reachability

使用 describe-reachability 确定 Outpost 服务器能否访问该区域中的 Outpost 配置端点。需要有效的 DNS 配置，您可以使用 describe-resolve 来确定该配置。

语法

```
Outpost>describe-reachability
```

describe-reachability 不包含参数。

开始连接

start-connection

使用 start-connection 可启动与该区域的 Outpost 服务的连接。此命令从您使用 export 加载的环境变量中获取签名版本 4 (SigV4) 凭证。连接异步运行并立即返回。要检查连接状态，请使用 get-connection。

语法

```
Outpost>start-connection [0|1]
```

start-connection 使用可选的连接索引来启动另一个连接。有效值仅为 `0` 和 `1`。

Example ：连接已开始

```
Outpost>start-connection

is_started: True
asset_id: example-asset-id
connection_id: example-connecdtion-id
timestamp: 2021-10-01T23:30:26Z
checksum: example-checksum
```

获取连接

get-connection

使用 get-connection 可返回连接的状态。

语法

```
Outpost>get-connection [0|1]
```

get-connection 使用可选的连接索引来返回另一个连接的状态。有效值仅为 `0` 和 `1`。

Example ：连接成功

```
Outpost>get-connection


---
keys_exchanged: True
connection_established: True
exchange_active: False
primary_peer: xx.xx.xx.xx:xxx
primary_status: success
primary_connection_id: a1b2c3d4567890abcdefEXAMPLE11111
primary_handshake_age: 1111111111
primary_server_public_key: AKIAIOSFODNN7EXAMPLE
primary_client_public_key: AKIAI44QH8DHBEXAMPLE
primary_server_endpoint: xx.xx.xx.xx:xxx
secondary_peer: xx.xxx.xx.xxx:xxx
secondary_status: success
secondary_connection_id: a1b2c3d4567890abcdefEXAMPLE22222
secondary_handshake_age: 1111111111
secondary_server_public_key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
secondary_client_public_key: je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
secondary_server_endpoint: xx.xxx.xx.xxx:xxx
timestamp: 2023-02-22T22:19:28Z
checksum: 0x83FA0123
```

注意：

- 如果 `exchange_active` 为 `True`，则表示连接仍在建立中。请 5 分钟后重试。

- 如果 `keys_exchanged` 或 `connection_established` 为 `False` 并且如果 `exchange_active` 为 `True`，则表示连接仍在建立中。请 5 分钟后重试。

如果 1 小时后问题仍然存在，请联系 AWS Support 服务中心。

在你的 Outpost 服务器上启动一个实例

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。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，为本地网络接口启用子网。

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，以满足您的应用程序的需求。有关更多信息，请参阅 Amazon EC2 用户指南中的实例存储卷。
- 您必须指定仅包含单个快照的 AMI。不支持具有多个快照的 AMI。
- 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。
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。如果您指定 1 作为 Outpost 子网的 LNI 设备索引，则此网络接口将成为该实例的本地网络接口。
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

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，请参阅启动后添加 LNI。

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。通常，您可以使用 DHCP 来执行此操作。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，对 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 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
```

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您的 Outpost 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 Outpost 连接到您选择的 AWS 地区或 AWS Outposts 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 AWS公共范围的更多信息，请参阅 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。
- Outpost 与任何关联的 VPC 之间的流量，包括客户数据面板流量。

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）。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 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 每台 Outpost 服务器的最大利用率为 500 Mbps。要提高连接速度，请使用多台 Outpost 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 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 服务器不缓存 AMI。每次启动实例时，都会从该区域下载 AMI。

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	1024-65535	服务链路 IP	53	DHCP 提供的 DNS 服务器
UDP	443、1024-65535	服务链路 IP	443	AWS Outposts 服务链接终端节点
TCP	1024-65535	服务链路 IP	443	AWS Outposts 注册端点

> **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。

更新和服务链路

AWS 维护您的 Outpost 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 W ell-Architected 最佳实践建议使用主动-主动设计在两个父级为不同可用区域的 Outposts 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。

服务链接会定期更新，以保持运营质量和性能。在维护期间，您可能会观察到该网络存在短暂的延迟和丢包，这会影响依赖于区域内托管资源的 VPC 连接的工作负载。但是，通过本地网络接口 (LNI) 的流量不会受到影响。您可以遵循Well-Architect AWS ed 最佳实践，并确保您的应用程序能够抵御影响单个Outpost服务器的故障或维护活动，从而避免对应用程序造成影响。

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

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 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。

返回 AWS Outposts 服务器

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 控制台为您提供发货标签。

如果您因为服务器已到合同期限或任何其他原因而想要归还服务器，请联系 AWS Support 中心。

主题

以下步骤说明了如何将服务器归还给 AWS。

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。
   - 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. 为存储在 AWS Outposts 服务器上运行的 Amazon EC2 实例的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。

2. 获取归还运输标签

> **Important**
> 您只能使用 AWS 提供的发货标签。请勿创建自己的运输标签。

根据归还原因获取运输标签。

Shipping label for a server that is being replaced

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. 在替换订单摘要下，选择打印归还标签，然后选择您计划归还的服务器的配置 ID。

Shipping label for a server that is not being replaced

1. 联络 AWS Support 中心。
2. 为您要归还的服务器申请运输标签。

3. 打包服务器

要打包服务器，请使用服务器最初随附的包装盒和包装材料。您也可以使用替换服务器随附的包装盒。或者，请联系 AWS Support 中心申请包装盒。包装好服务器后，贴上 AWS 提供的运输标签。

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：

Country	联系人
阿根廷	联络 AWS Support 中心。在您的请求中，包含以下信息：
巴林	

Country	联系人
巴西	• AWS提供的发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
文莱	
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	

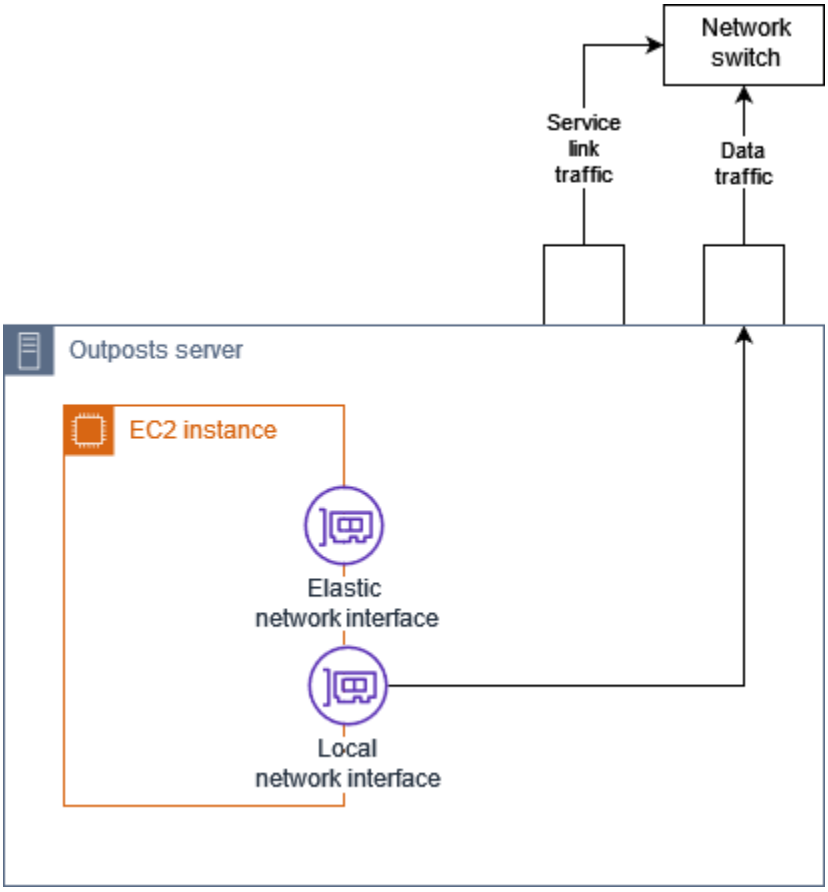
Country	联系人
泰国	
阿拉伯联合酋长国	
越南	
United States of America	请联系 UPS。 您可以通过以下方式归还服务器： • 在所在地的 UPS 例行取件期间归还服务器。 • 将服务器送到 UPS 地点。 • 在您希望的日期和时间安排取件。输入 AWS 提供的发货标签上的追踪编码，即可享受免费配送。
所有其他国家	请联系 DHL。 您可以通过以下方式归还服务器： • 将服务器送到 DHL 地点。 • 在您希望的日期和时间安排取件。输入 AWS 提供的货件标签上的 DHL 运单编号，即可享受免费配送。 如果您收到以下错误 `Courier pickup cannot 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。

本地网络接口

对于 AWS Outposts 服务器，本地网络接口 (LNI) 是一种逻辑网络组件，用于将 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 Outpost 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。
- 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 (eth0)。
- 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 Outpost 服务器上的 Outpost 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。

Performance

每种实例大小的 LNI 提供物理 10 GbE LNI 可用带宽的一部分。下表列出了每种实例类型的 LNI 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 Linux 实例的更多信息，请参阅 Amazon EC2 用户指南中的监控 EC2 实例的网络性能。对于 Windows 实例，请参阅亚马逊 EC2 用户指南中的监控 EC2 实例的网络性能。

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。

在 Outpost 服务器上为本地网络接口启用子网

使用中的modify-subnet-attribute命令 AWS CLI 为本地网络接口启用 Outpost 子网。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。例如，值为 1 表示 Outpost 子网中实例的辅助网络接口 (eth1) 是本地网络接口。

为本地网络接口启用 Outpost 子网

在命令提示符处，运行以下命令来指定本地网络接口的设备位置。

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

使用本地网络接口

此部分可用来了解如何使用本地网络接口。

任务

- 添加本地网络接口
- 查看本地网络接口

- 配置操作系统

添加本地网络接口

您可以在启动期间或之后，向 Outpost 子网上的 Amazon EC2 实例添加本地网络接口 (LNI)。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。

在实例启动期间添加 LNI

1. 在启动实例向导中，选择网络设置旁边的编辑。
2. 展开高级网络配置。
3. 选择添加网络接口。这将使用设备索引 1 来创建一个网络接口。如果您指定 1 作为 Outpost 子网的 LNI 设备索引，则此网络接口将成为该实例的本地网络接口。
4. 选择 Outpost 子网，再根据需要更新网络接口的配置。
5. 完成向导以启动实例。

在实例启动之后添加 LNI

1. 在导航窗格中，依次选择网络与安全、网络接口。
2. 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 LNI，因此您选择的安全组是不相关的。
   e. 选择创建网络接口。
3. 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。如果您指定 1 作为 Outpost 子网的 LNI 设备索引，则此网络接口是该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。

控制台将显示来自子网 CIDR 的 LNI 私有 IPv4 地址。此地址不是 LNI 的 IP 地址，因此是不可用的。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。您必须在客户机操作系统中设置 LNI 的 IP 地址，可以静态方式或通过 DHCP 服务器来设置。

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。

服务器的本地网络连接

本主题可用来了解承载 Outpost 服务器的网络布线和拓扑要求。有关更多信息，请参阅 本地网络接口。

内容

网络上的服务器拓扑

Outpost 服务器需要两个不同的连接来连接您的网络设备。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 Outpost 服务器流量类型和标签。

流量标签	描述
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。服务链路是从 Outpost 到区域的自定义 VPN 或多个 VPN。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 (LNI) 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

每台 Outpost 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 Outpost 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 Outpost 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 LNI 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 Outpost 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

上行链路速度

每台 Outpost 服务器需要至少以上行速度 20 Mbps 连接到 AWS 区域。

根据 LNI 链路和服务链路利用率，您可能需要速度更快的上行链路。有关更多信息，请参阅服务链路带宽建议。

本地网络接口 (LNI) 链路流量

配置上游网络设备上的 LNI 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 LNI 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 LNI 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 LNI 配置 VLinux 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：

   - LNI 接口的名称是 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 EC2 用户指南中的使用适用于亚马逊 Linux 的 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 Outpost 服务器分配公有 IP 地址。

动态主机控制协议 (DHCP) 是一种网络管理协议，用于自动化完成 IP 网络上的设备配置过程。在 Outpost 服务器的上下文中，您可以通过两种方式使用 DHCP：

- 服务器上的网卡
- 实例上的本地网络接口

对于服务链路，Outpost 服务器使用 DHCP 连接到本地网络。DHCP 必须返回 DNS 域名服务器和默认网关。Outpost 服务器不支持服务链路的静态 IP 分配。

对于 LNI 链路，请使用 DHCP 来配置要连接到本地网络的实例。有关更多信息，请参阅 the section called “配置操作系统”。

> **Note**
>
> 确保为 Outpost 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 Outpost 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。Outpost 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。当前， AWS Outposts 服务器不支持通过 VPC 进行私有连接。有关更多信息，请参阅 the section called “步骤 6：授权服务器”。

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

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 服务器使用。对于机架资源，请参阅适用于 Outpost 机架的 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。
- 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 Outpost 的相关信息。
- 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架构上的内容的控制。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 Outpost 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（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

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 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 中的跨账户资源访问。

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密钥：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

支持临时证书：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 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，因为您不会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策略是一个服务相关角色策略， AWS 用于允许访问由 AWS Outposts管理的资源。

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。

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 托管策略： AWSOutpostsAuthorizeServerPolicy

此策略可用于授予在本地网络中授权 Outpost 服务器硬件所需的权限。有关更多信息，请参阅授予权限。

该策略包含以下权限。

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

```
  ]
}
```

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
AWSOutpostsAuthorizeServerPolicy - 新策略	AWS Outposts 添加了一项策略，该策略授予在本地网络中授权 Outpost 服务器硬件的权限。	2023 年 1 月 4 日
AWS Outposts 已开始跟踪更改	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 主体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，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。 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 安全与合规架构 — 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AWS 规资源 — 此工作簿和指南集可能适用于您的行业和所在地区。

- 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 可以全面了解您的安全状态 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。

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

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`

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`CreateOutpost``GetOutpostInstanceTypes`、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。

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 Outpost 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。

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服务器才能正常运行。

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。
- 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。

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。

Outpost 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，并且可以通过本地网络和 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 API 可能不起作用。实例指标和日志将继续在本地缓存几个小时，并在连接恢复后推送到该 AWS 区域。但是，断开连接超过几个小时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 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：

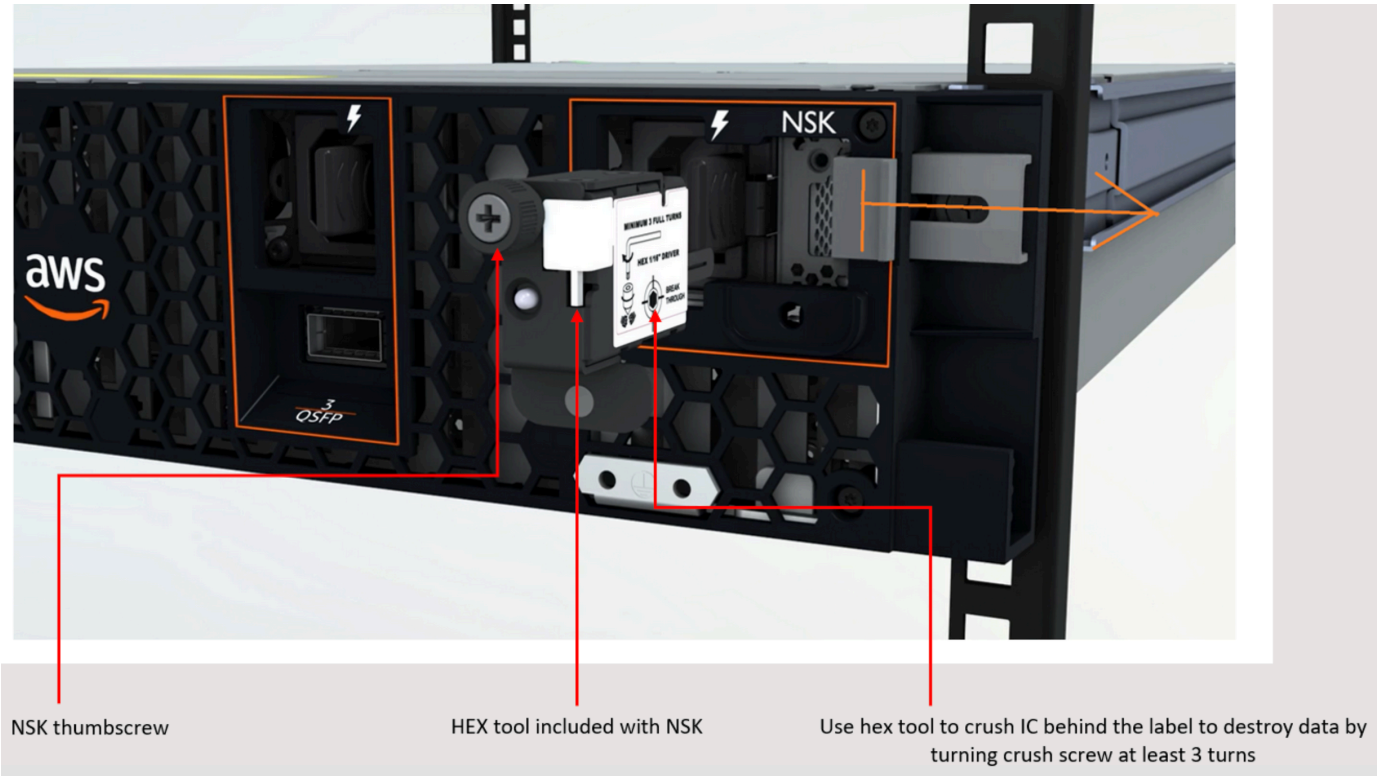
- AWS 博客监控最佳实践 AWS Outposts涵盖了Out posts特有的可观察性和事件管理最佳实践。
- Amazon VPC 网络连接调试工具 AWS博客解释了 AWSSupport-setuPip MonitoringFrom VPC 工具。此工具是一个 AWS Systems Manager 文件（SSM 文件），可用于在您指定的子网中创建 Amazon EC2 监控实例并监控目标 IP 地址。该文档运行 ping、MTR、TCP 跟踪路径和跟踪路径诊断测试，并将结果存储在 Amazon CloudWatch Logs 中，这些结果可以在 CloudWatch 控制面板中可视化（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。

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。



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。
- 结束订阅并归还您的 Outpost 服务器。
- 转换为 month-to-month 订阅并保留现有的 Outpost 服务器。

主题

续订订阅

要续订订阅并保留现有的 Outpost 服务器，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 服务器定价。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服务器，则系统会自动将您转换为订 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。

结束订阅并归还服务器

> **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，输入您希望终止订阅的日期。

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. 如有必要，请备份服务器上存在的所有实例和实例数据。
14. 终止在您的服务器上启动的实例。
15. 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。
16. 在支持案例中指示关闭服务器或断开服务器与网络的连接之前，请勿关闭服务器电源或断开服务器与网络的连接。

要退回 AWS Outposts 服务器，请按照 “返回 AWS Outposts 服务器” 中的步骤进行操作。

转换为订 month-to-month 阅

要转换为 month-to-month 订阅并保留现有的 Outpost 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第二天开始。

AWS Outposts 的配额

对于每项 AWS 服务，您的 AWS 账户 都具有默认配额（以前被称为限制）。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 服务器的 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
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
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
引入 Outpost 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。