機架使用者指南

AWS Outposts

AWS Outposts: 機架使用者指南

Table of Contents

什麼是 AWS Outposts？

AWS Outposts 是一項全受管服務，可將 AWS 基礎架構、服務、API 和工具延伸至客戶場所。透過提供 AWS 受管理基礎架構的本機存取權， AWS Outposts 讓客戶能夠使用與 Region 相同的程式設計介面在 AWS 內部部署建置和執行應用程式，同時使用本機運算和儲存資源來降低延遲和本機資料處理需求。

Outpost 是部署在客戶站點的 AWS 計算和儲存容量集區。 AWS 作為 AWS 區域的一部分來操作、監控和管理此容量。您可以在 Outpost 上建立子網路，並在建立 EC2 執行個體、EBS 磁碟區、ECS 叢集和 RDS 執行個體等 AWS 資源時指定子網路。Outpost 子網路中的執行個體會使用私有 IP 位址與 AWS 區域中的其他執行個體進行通訊，全部位於相同的 VPC 內。

> **Note**
>
> 您無法將 Outpost 連線到同一 VPC 內的另一個 Outpost 或本機區域。

如需詳細資訊，請參閱 AWS Outposts 產品頁面。

重要概念

這些是 AWS Outposts.

- 前哨站點 — 客戶管理的實體建築物， AWS 將在其中安裝您的前哨站。站點必須符合 Outpost 的設施、網路和電源要求。
- Outpost 容量 – Outpost 上可用的運算和儲存資源。您可以從 AWS Outposts 主控台檢視和管理 Outpost 的容量。
- 前哨設備 — 提供 AWS Outposts 服務存取權的實體硬體。硬體包括所擁有和管理的機架、伺服器、交換器，以及接線 AWS。
- Outpost 機架 – 業界標準 42U 機架的 Outpost 形式規格。Outpost 機架包括機架式伺服器、交換器、網路配線面板、電源機箱和空面板。
- Outposts ACE 機架 — 聚合、核心、邊緣 (ACE) 機架可作為多機架前哨部署的網路聚合點。ACE 機架可在邏輯 Outposts 中的多個 Outpost 運算機架與內部部署網路之間提供連線，減少實體網路連接埠數量和邏輯介面的需求。

  如果您有五個以上的運算機架，則必須安裝 ACE 機架。如果您的運算機架少於五個，但計劃 future 擴充至五個以上的機架，我們建議您儘早安裝 ACE 機架。

如需 ACE 機架的詳細資訊，請參閱使用 ACE AWS Outposts 機架調整機架部署。

- Outpost 伺服器：業界標準 1U 或 2U 伺服器的 Outpost 形式規格，可安裝在符合 EIA-310D 19 標準的 4 支桿機架中。Outpost 伺服器為空間有限或容量要求較小的站台提供本機運算和網路服務。
- 服務連結 — 可讓您的前哨站及其相關 AWS 區域之間進行通訊的網路路由。每個 Outpost 都是可用區域及其相關聯區域的延伸。
- 本機閘道 (LGW) — 邏輯互連虛擬路由器，可在 Outpost 機架與內部部署網路之間進行通訊。
- 本機網路介面 – 一種網路介面，可從 Outpost 伺服器和您的內部部署網路進行通訊。

AWS Outposts 資源

您可以在 Outpost 上建立下列資源，以支援必須在內部部署資料和應用程式附近執行的低延遲工作負載：

運算

資源類型	機架	伺服器
Amazon EC2 執行個體	 是	 是
Amazon ECS 叢集	 是	 是
Amazon EKS 節點	 是	 否

資料庫與分析

資源類型	機架	伺服器
Amazon ElastiCache 節點（Redis 集群，內存緩存集群）	 是	 否
Amazon EMR 叢集	 是	 否
Amazon RDS 資料庫執行個體	 是	 否

聯網

資源類型	機架	伺服器
App Mesh Envoy 代理	 是	 是
Application Load Balancer	 是	 否
Amazon VPC 子網路	 是	 是

資源類型	機架	伺服器
Amazon Route 53	是	否

儲存

資源類型	機架	伺服器
Amazon EBS 磁碟區	是	否
Amazon S3 儲存貯體	是	否

其他 AWS 服務

服務	機架	伺服器
AWS IoT Greengrass	是	是
Amazon SageMaker 邊緣經理	是	是

定價

您可以從各種 Outpost 配置中進行選擇，每種配置都提供 EC2 執行個體類型和儲存選項的組合。機架配置的價格包括安裝、拆卸和維護。對於伺服器，您必須安裝和維護設備。

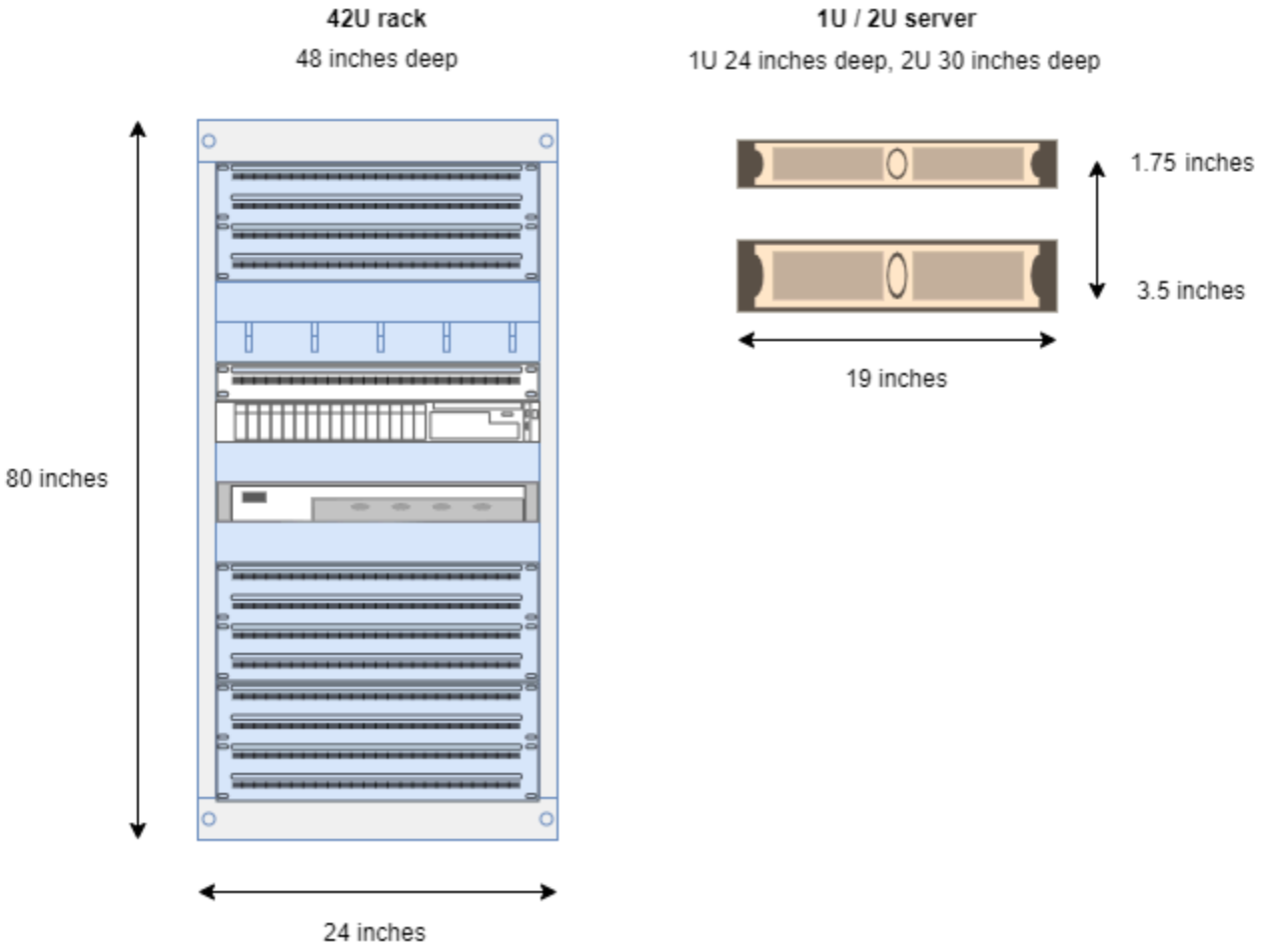
您可以購買 3 年期的配置，並從三種付款選項中進行選擇：全額預付、部分預付和不預付。如果您選擇「部分預付」或「不預付」付款選項，則會每月支付費用。任何預付費用都須在安裝 Outpost 並可使用運算和儲存容量後 24 小時內支付。如需詳細資訊，請參閱：

- AWS Outposts 機架定價
- AWS Outposts 伺服器定價

如何 AWS Outposts 工作

AWS Outposts 旨在在您的前哨站和 AWS 區域之間保持恆定且一致的連接運行。若要與區域以及內部部署環境中的本機工作負載實現此連線，您必須將 Outpost 連線到內部部署網路。您的內部部署網路必須提供連回區域和網際網路的廣域網路 (WAN) 存取。其也必須提供對內部部署工作負載或應用程式所在本機網路的 LAN 或 WAN 存取。

下圖說明兩種 Outpost 形式規格。



目錄

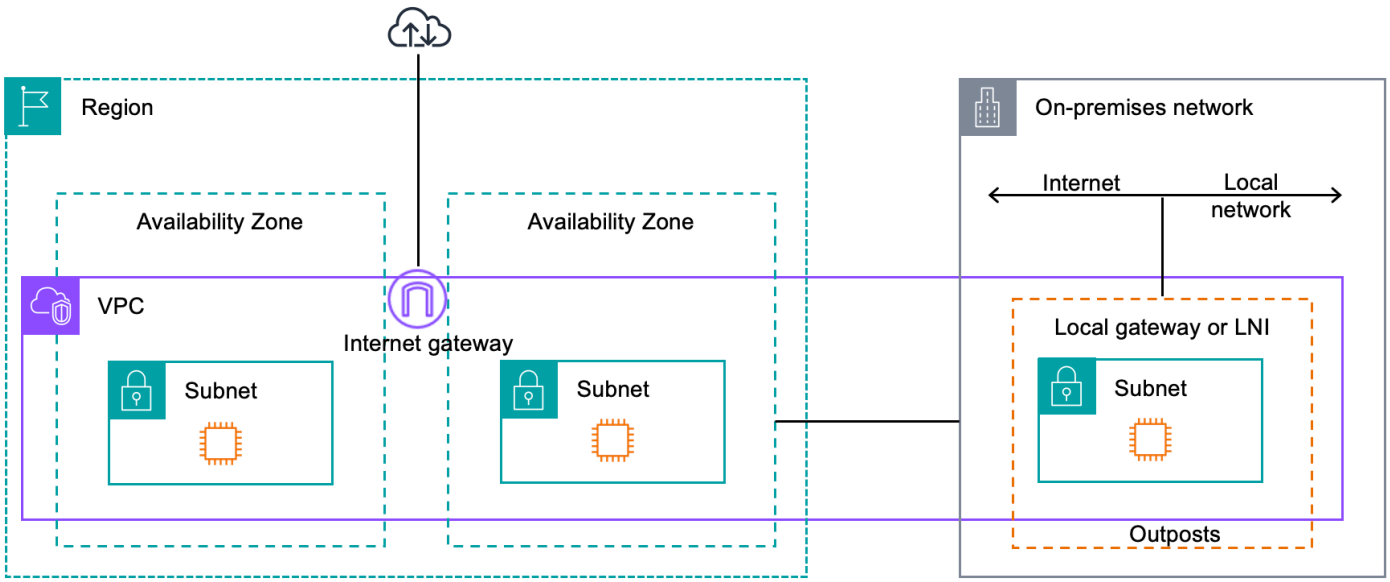
- 本機閘道
- 本機網路介面

網路元件

AWS Outposts 使用該 AWS 區域可存取的 VPC 元件 (包括網際網路閘道、虛擬私有閘道、Amazon VPC 傳輸閘道和 VPC 端點)，將 Amazon VPC 從某個區域延伸到前哨站。Outpost 位於區域中的可用區域，且為該可用區域的延伸，可用於復原。

下圖顯示 Outpost 的網路元件。

- AWS 區域 和內部部署網路
- 在區域中具有多個子網路的 VPC
- 內部部署網路中的 Outpost
- Outpost 與本機網路之間由本機閘道 (機架) 或本機網路介面 (伺服器) 提供的連線



VPC 和子網路

虛擬私有雲 (VPC) 橫跨其 AWS 區域中的所有可用區域。您可新增 Outpost 子網路，以將 區域中的任何 VPC 延伸至 Outpost。若要將 Outpost 子網路新增至 VPC，請在建立子網路時指定 Outpost 的 Amazon Resource Name (ARN)。

Outpost 支援多個子網路。當您在 Outpost 中啟動 EC2 執行個體時，您可以指定 EC2 執行個體子網路。您無法指定部署執行個體的基礎硬體，因為 Outpost 是 AWS 運算和儲存容量的集區。

每個 Outpost 可支援多個 VPC，其中可能包含一或多個 Outpost 子網路。如需 VPC 配額的資訊，請參閱《Amazon VPC 使用者指南》中的《Amazon VPC 配額》。

您可以從建立 Outpost 之 VPC 的 VPC CIDR 範圍建立 Outpost 子網路。您可以針對資源 (例如位於 Outpost 子網路中的 EC2 執行個體) 使用 Outpost 地址範圍。

路由

根據預設，每個 Outpost 子網路都會從其 VPC 繼承主路由表。您可以建立自訂路由表，並建立其與 Outpost 子網路的關聯。

Outpost 子網路中路由表的運作方式與可用區域子網路中路由表的運作方式相同。您可以指定 IP 地址、網際網路閘道、本機閘道、虛擬私有閘道和對等互連作為目的地。例如，每個 Outpost 子網路都會透過繼承的主路由表或自訂資料表繼承 VPC 本機路由。這表示 VPC 中的所有流量 (包括具有 VPC CIDR 中目的地的 Outpost 子網路) 都會在 VPC 中保持路由。

Outpost 子網路路由表可以包含下列目的地：

- VPC CIDR 範圍 — 在安裝時 AWS 定義此範圍。這是本機路由，適用於所有 VPC 路由，包括相同 VPC 中 Outpost 執行個體之間的流量。
- AWS 區域目的地 — 這包括 Amazon AWS Transit Gateway Simple Storage Service (Amazon S3)、Amazon DynamoDB 閘道端點、虛擬私有閘道、網際網路閘道和 VPC 對等的前置詞清單。

  如果您與相同 Outpost 上的多個 VPC 對等互連，則 VPC 之間的流量會保留在 Outpost 中，而不會使用連回區域的服務連結。
- 透過本機閘道跨 Outpost 進行 VPC 內部通訊 – 您可以使用直接 VPC 路由，在不同 Outpost 的相同 VPC 中的子網路之間建立通訊。如需詳細資訊，請參閱：
  - 直接 VPC 路由
  - 路由至 AWS Outposts 本機閘道

DNS

對於連線到 VPC 的網路介面，Outpost 子網路中的 EC2 執行個體可以使用 Amazon Route 53 DNS 服務將網域名稱解析為 IP 地址。Route 53 支援 DNS 功能，例如網域註冊、DNS 路由，以及執行於 Outpost 中之執行個體的運作狀態檢查。公有和私有託管的可用區域都支援將流量路由至特定網域。路

線 53 解析器在區域中託管。 AWS 因此，必須啟動並執行從 Outpost 返回該 AWS 區域的服務連結連線，這些 DNS 功能才能運作。

使用 Route 53 時，您可能會遇到較長的 DNS 解析時間，具體取決於前哨站和 AWS 區域之間的路徑延遲。在這種情況下，您可以使用內部部署環境中本機安裝的 DNS 伺服器。若要使用自己的 DNS 伺服器，您必須為內部部署 DNS 伺服器建立 DHCP 選項組，並建立其與 VPC 的關聯。您也必須確保具有這些 DNS 伺服器的 IP 連線。您可能還需要將路由新增至本機閘道路由表以進行連線，但僅具有本機閘道的 Outpost 機架才有此選項。由於 DHCP 選項組具有 VPC 範圍，因此 Outpost 子網路和 VPC 之可用區域子網路中的執行個體都會嘗試使用指定的 DNS 伺服器進行 DNS 名稱解析。

不支援對來自 Outpost 的 DNS 查詢進行查詢日誌記錄。

服務連結

服務鏈接是從您的前哨返回您選擇的 AWS 地區或 Outposts 所在地區的連接。服務連結是一組加密的 VPN 連線，會在每次 Outpost 與您選擇的主要區域進行通訊時使用。您可以使用虛擬 LAN (VLAN) 來分段服務連結上的流量。服務連結 VLAN 可讓前哨站和區域之間的通訊，以便管理 AWS 區域與前哨站之間的前哨和 VPC 內部流量。 AWS

您的服務連結是在佈建 Outpost 時所建立。如果您具有伺服器形式規格，請建立連線。如果您有機架，請 AWS 建立服務連結。如需詳細資訊，請參閱：

- 前哨連接到 AWS 區域
- AWS Outposts 高可用性設計與架構考量白皮書中的應用程式/工作負載路由 AWS

本機閘道

Outpost 機架包含本機閘道，可讓您連線到內部部署網路。如果您有 Outpost 機架，則可包含本機閘道作為目標，其目的地是內部部署網路。本機閘道僅適用於 Outpost 機架，而且只能在與 Outpost 機架相關聯的 VPC 和子網路路由表中使用。如需詳細資訊，請參閱：

- 本機閘道
- AWS Outposts 高可用性設計與架構考量白皮書中的應用程式/工作負載路由 AWS

本機網路介面

Outpost 伺服器包含本機網路介面，可讓您連線到內部部署網路。本機網路介面僅供在 Outpost 子網路上執行的 Outpost 伺服器使用。您無法在 Outpost 機架或 AWS 區域中使用 EC2 執行個體的本機網路

界面。本機網路介面僅適用於內部部署位置。如需詳細資訊，請參閱《AWS Outposts Outpost 伺服器使用者指南》中的《本機網路介面》。

Outpost 機架的站點要求

Outpost 站點是 Outpost 運行的實體位置。只有特定國家和地區才提供這些站點。如需詳細資訊，請參閱《AWS Outposts 機架常見問答集》。請參閱《在哪些國家和地區提供 Outpost 機架》問題。

本頁面涵蓋 Outpost 機架的要求。如果您要安裝聚合、核心、邊緣 (ACE) 機架，您的站台也必須符合中列出的需求Outposts ACE 機架的站點需求。

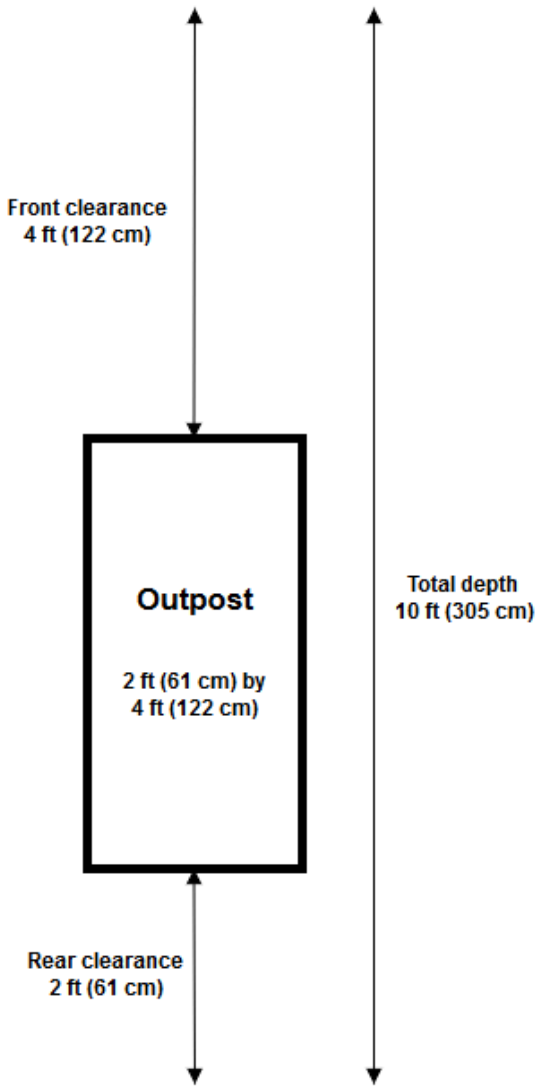
如需 Outpost 伺服器的要求，請參閱《AWS Outposts Outpost 伺服器使用者指南》中的《Outpost 伺服器的站點要求》。

設施

以下是機架的設施要求。

- 溫度和濕度 – 環境溫度必須介於 41°F (5°C) 和 95°F (35°C) 之間。相對濕度必須介於 8% 和 80% 之間，且無冷凝。
- 氣流 – 機架會從前通道吸入冷空氣，並將熱空氣排出到後通道。機架位置必須至少提供 145.8 x 每分鐘立方英呎 (CFM) kVA 的氣流。
- 裝卸碼頭 – 您的裝卸碼頭必須能夠容納 94 英吋(239 公分) 高 x 54 英吋 (138 公分) 寬 x 51 英吋 (130 公分) 深的機架箱。
- 支撐重量 – 重量因配置而異。您可以在訂單摘要中找到機架點負載所指定配置的重量。機架的安裝位置及通往該位置的途徑必須能夠支撐指定的重量。這包括沿途的任何貨物和標準升降梯。
- 間隙 – 機架為 80 英吋 (203 公分) 高 x 24 英吋 (61 公分) 寬 x 48 英吋 (122 公分) 深。任何門口、走廊、轉角、坡道和升降梯都必須提供足夠的間隙。在最終安放位置，必須有 24 英吋 (61 公分) 寬 x 48 英吋 (122 公分) 深的面積容納 Outpost，且前後各有額外的 48 英吋 (122 公分) 和 24 英吋 (61 公分) 間隙。Outpost 所需的最小總面積為 24 英吋 (61 公分) 寬 x 10 英呎 (305 公分) 深。

  下圖顯示 Outpost 所需的最小總面積 (包括間隙)。



- 抗震支撐 — 在法規或法規要求的範圍內，您將在設施中安裝和維護適當的抗震錨固和支撐機架。AWS 提供地板支架，可在所有 Outposts 支架上為高達 2.0G 的地震活動提供保護。
- 接合點 — 我們建議您在機架位置提供接合線/點，以便 AWS獲得認證的技術人員可以在安裝期間將機架固定在機架上。
- 設施通道 — 您不會以對訪問，維修或刪除前哨站能力產生負面影響的 AWS 方式更改設施。
- 海拔高度 – 安裝機架的機房海拔高度必須低於 10,005 英呎 (3,050 公尺)。

聯網

以下是機架的網路要求。

- 提供 1 Gbps、10 Gbps、40 Gbps 或 100 Gbps 速度的上行鏈路。

  如需服務連結連線的頻寬建議，請參閱《頻寬建議》。
- 提供單模光纖 (SMF) 搭配 Lucent 連接器 (LC)、多模光纖 (MMF) 或 MMF OM4 搭配 LC。
- 提供一或兩部上游裝置，可以是交換器或路由器。建議使用兩部裝置以提供高可用性。

網路整備檢查清單

當您收集 Outpost 組態的資訊時，請使用此檢查清單。這包括 LAN、WAN 以及前哨站和當地交通目的地之間的任何裝置，以及該地 AWS 區的目的地。

上行鏈路速度、連接埠和光纖

上行鏈路速度和連接埠

Outpost 有兩部連接至您本機網路的 Outpost 網路裝置。每部裝置可支援的上行鏈路數量取決於您的頻寬需求以及路由器可支援的內容。如需詳細資訊，請參閱 實體連線。

下列清單顯示根據上行鏈路速度，每部 Outpost 網路裝置支援的上行鏈路連接埠數量。

1 Gbps

1、2、4、6 或 8 個上行鏈路

10 Gbps

1、2、4、8、12 或 16 個上行鏈路

40 Gbps 或 100 Gbps

1、2 或 4 個上行鏈路

光纖

支援下列光纖類型：

- 單模光纖 (SMF) 搭配 Lucent 連接器 (LC)
- 多模光纖 (MMF) 或 MMF OM4 搭配 LC

根據上行鏈路速度和您選擇的光纖類型，支援下列光學標準。

上行鏈路速度	光纖類型	光學標準
1 Gbps	SMF	– 1000Base-LX
1 Gbps	MMF	– 1000Base-SX
10 Gbps	SMF	– 10GBASE-IR – 10GBASE-LR
10 Gbps	MMF	– 10GBASE-SR
40Gbps	SMF	– 40GBASE-IR4 (LR4L) – 40GBASE-LR4
4 部 10 Gbps 中斷應用裝置	MMF	– 40GBASE-ESR4 – 40GBASE-SR4
100 Gbps	SMF	– 100G PSM4 MSA – 100GBASE-CWDM4 – 100GBASE-LR4
4 部 25 Gbps 中斷應用裝置	MMF	– 100GBASE-SR4

Outpost 連結彙總和 VLAN

Outpost 與您的網路之間需要連結彙總控制通訊協定 (LACP)。您必須搭配 LACP 使用動態 LAG。

每部 Outpost 網路裝置都需要下列 VLAN。如需詳細資訊，請參閱 虛擬 LAN。

Outpost 網路裝置	服務連結 VLAN	本機閘道 VLAN
#1	有效值：1-4094	有效值：1-4094
#2	有效值：1-4094	有效值：1-4094

對於每部 Outpost 網路裝置，您可以選擇服務連結和本機閘道要使用相同的 VLAN 還是不同的 VLAN。不過，建議每部 Outpost 網路裝置使用與其他 Outpost 網路裝置不同的 VLAN。如需詳細資訊，請參閱《連結彙總》和《虛擬 LAN》。

我們也建議使用備援 Layer 2 連線。LACP 用於連結彙總，而不是用於提高可用性。Outpost 網路裝置之間不支援 LACP。

Outpost 網路裝置 IP 連線

兩部 Outpost 網路裝置針對服務連結和本機閘道 VLAN 各需要一個 CIDR 和 IP 地址。建議為每部具有 /30 或 /31 CIDR 的網路裝置配置專用子網路。指定 Outpost 要使用的子網路以及該子網路中的 IP 地址。如需詳細資訊，請參閱 網路層連線。

Outpost 網路裝置	服務連結要求	本機閘道要求
#1	– 服務連結 CIDR (/30 或 /31) – 服務連結 IP 地址	– 本機閘道 CIDR (/30 或 /31) – 本機閘道 IP 地址
#2	– 服務連結 CIDR (/30 或 /31) – 服務連結 IP 地址	– 本機閘道 CIDR (/30 或 /31) – 本機閘道 IP 地址

服務連結最大傳輸單位 (MTU)

網路必須在父區域中的 Outpost 和服務連結端點之間支援 1500 位元組的 MTU。 AWS 如需服務連結的詳細資訊，請參閱《AWS Outposts 連線至 AWS 區域》。

服務連結邊界閘道協定

Outpost 會在每部 Outpost 網路裝置與您的本機網路裝置之間建立外部 BGP (eBGP) 對等互連工作階段，以透過服務連結 VLAN 進行服務連結連線。如需詳細資訊，請參閱 服務連結 BGP 連線。

Outpost	服務連結 BGP 要求
您的 Outpost	– Outpost BGP 自治系統編號 (ASN)。2 個位元組 (16 位元) 或 4 個位元組 (32 位元)。來自您的私有 ASN 範圍 (64512-65534 或 4200000000-4294967294)。

Outpost	服務連結 BGP 要求
	– 基礎設施 CIDR (需要 /26，已公告為兩個連續 /27)。

本機網路裝置	服務連結 BGP 要求
#1	– 服務連結 BGP 對等 IP 地址。 – 服務連結 BGP 對等 ASN。2 個位元組 (16 位元) 或 4 個位元組 (32 位元)。
#2	– 服務連結 BGP 對等 IP 地址。 – 服務連結 BGP 對等 ASN。2 個位元組 (16 位元) 或 4 個位元組 (32 位元)。

服務連結防火牆

必須在防火牆中以具狀態方式列出 UDP 和 TCP 443。

通訊協定	來源連接埠	來源地址	目標連接埠	目的地地址
UDP	443	Outpost 服務連結 /26	443	Outpost 區域的公有路由
TCP	1025-65535	Outpost 服務連結 /26	443	Outpost 區域的公有路由

您可以使用 AWS Direct Connect 連接或公共互聯網連接將 Outpost 連接回該 AWS 地區。對於 Outpost 服務連結連線，您可以在防火牆或邊緣路由器上使用 NAT 或 PAT。一律會從 Outpost 起始建立服務連結。

本機閘道邊界閘道協定

Outpost 會建立從每部 Outpost 網路裝置到本機網路裝置的 eBGP 對等互連工作階段，以從您的本機網路連線到本機閘道。如需詳細資訊，請參閱 本機閘道 BGP 連線。

Outpost	本機閘道 BGP 要求
您的 Outpost	– Outpost BGP 自治系統編號 (ASN)。2 個位元組 (16 位元) 或 4 個位元組 (32 位元)。來自您的私有 ASN 範圍 (64512-65534 或 4200000000-4294967294)。 – 要公告的 CoIP CIDR (公有或私有且至少為 /26)。

本機網路裝置	本機閘道 BGP 要求
#1	– 本機閘道 BGP 對等 IP 地址。 – 本機閘道 BGP 對等 ASN。2 個位元組 (16 位元) 或 4 個位元組 (32 位元)。
#2	– 本機閘道 BGP 對等 IP 地址。 – 本機閘道 BGP 對等 ASN。2 個位元組 (16 位元) 或 4 個位元組 (32 位元)。

電源

Outpost 電源機箱支援三種電源配置：5 kVA、10 kVA 或 15 kVA。電源機箱的配置取決於 Outpost 容量的總耗電量。例如，如果 Outpost 資源的最大耗電量為 9.7 kVA，則必須提供 10 kVA 的電源配置：4 個 L6-30P 或 IEC309，其中 2 個接至 S1，2 個接至 S2 (適用於備援、單相電源)。下面的第二個表格描述了這三種電源配置。

若要查看不同前哨資源的耗電需求，請在 AWS Outposts 主控台中選擇 https://console.aws.amazon.com/outposts/ 的「瀏覽目錄」。

需求	規格
AC 電源線電壓	單相 208 至 277 空調; 50 或 60 赫茲 三相： • 208 至 250 空調 (三角洲) ; 50 至 60 赫茲 • 346 至 480 空調 (瓦伊); 50 至 60 赫茲
耗電量	5 kVA (4 kW)、10 kVA (9 kW) 或 15 kVA (13 kW)
AC 保護裝置 (上游斷路器)	對於 1N 輸入（非備援）和 2N 輸入（備援）：30 A、32 A 或 50 A，具有 D 曲線或 K 曲線斷路器。 僅限 2N 輸入 (備援)：C 曲線、D 曲線或 K 曲線斷路器。 不支援 B 曲線或更低規格。
AC 電源插座類型 (插座)	單相：3 個 L6-30P、P+P+E、30A 插頭，或 3 個 IEC60309 P+N+E、IP67、32A 插頭 三相、星形接法：1 個 IEC60309、3P+N+E、IP67、7 點鐘位置、30A 插頭，或 1 個 IEC60309、3P+N+E、IP67、6 點鐘位置、32A 插頭 三相、三角形接法：1 個非 NEMA 扭鎖式 Hubbell CS8365C、3P+E、中央接地、50A 插頭 **Note** 最好使用 IP67 插頭搭配 IP67 插座。如果不可行，請使用 IP67 插頭搭配 IP44 插座。插頭和插座組合的額定值將成為額定值下限 (IP44)。
電源線長度	10.25 英呎 (3 公尺)
電源線 - 機架佈線輸入	從機架上方或下方

電源機箱具有兩個輸入 S1 和 S2，可依照下列方式配置。

	備援、單相	備援、三相	單相	三相
5 kVA	2 x L6-30P 或 IEC309; 一個下降到中一，一個下降到第二	2 x AH530P7W、AH532P6W 或 CS8365C；1 個下降到中一，一個下降到第二季	1 x L6-30P 或 IEC309；1 次下降至中一	1 x AH530P7W、AH532P6W 或 CS8365C；1 次下降至中一
10 kVA	4 x L6-30P 或 IEC309；2 次下降至第一季，2 滴到第二階段		2 x L6-30P 或 IEC309; 2 滴到中一	
15 kVA	6 倍 L6-30P 或 IEC309；3 滴到中一，3 滴到第二階段		3 x L6-30P 或 IEC309；3 次下降至中一	

如果先前所述 AWS 提供的 AC 鞭子必須安裝備用電源插頭，請考慮下列事項：

- 只有經認證客戶提供的電工才能修改 AC 電源線來配合新的插頭類型。
- 安裝時應符合所有適用的國家、州和地方安全要求，並根據電氣安全要求進行檢查。
- 您（客戶）應通知您的 AWS 代表有關 AC 鞭形插頭的修改。根據要求，您將提供有關修改的資訊 AWS。您也必須包含具有管轄權的主管機關所核發的任何安全檢查記錄。必須驗證安裝安全無虞，才能讓 AWS 員工使用設備執行工作。

訂單履行

為了完成訂單， AWS 將與您安排一個日期和時間。您也會收到安裝之前要確認或提供的項目檢查清單。

AWS 安裝團隊將在預定的日期和時間到達您的現場。他們會將機架放置在指定的位置。您和您的電工必須負責執行機架的電氣連接和安裝。

您必須確保電氣裝置以及這些裝置的任何變更，均由經認證的電工根據所有適用法律、法規和最佳實務來執行。 AWS 在對 Outpost 硬體或電氣裝置進行任何變更之前，您必須取得書面核准。您同意提供文件， AWS 以驗證合規性和任何變更的安全性。 AWS 對於前哨電氣裝置或設施電線或任何更改造成的任何風險概不負責。您不得對 Outpost 硬體進行任何其他變更。

團隊會透過您提供的上行鏈路為 Outpost 機架建立網路連線，並設定機架的容量。

當您確認 AWS 帳戶可以使用 Outpost 機架的 Amazon EC2 和 Amazon EBS 容量時，安裝即完成。

Outposts ACE 機架的站點需求

> **Note**
>
> 如果您不需要 ACE 機架，請略過本節。

聚合、核心、邊緣 (ACE) 機架可作為多機架 Outpost 部署的網路聚合點。如果您有五個以上的運算機架，則必須安裝 ACE 機架。如果您的運算機架少於五個，但計劃 future 擴充至五個以上的機架，我們建議您最早安裝 ACE 機架。

若要安裝 ACE 機架，除了中列出的需求之外，您還必須符合本節中的需求Outpost 機架的站點要求。

設施

這些是 ACE 機架的設施需求。

- 電源 — 所有機架均隨附 10 千伏安單相 (AA+BB；IEC60309 或 L6-30P 鞭連接器類型)。
- 重量支撐 — 機架重量為 705 磅；320 公斤。
- 間隙/大小尺寸 — 機架高度為 80 英吋；203 公分。

> **Note**
>
> ACE 機架未完全封閉，且不包括前門或後門。

聯網

這些是 ACE 機架的網路需求。若要瞭解 ACE 機架如何連接 Outposts 網路裝置、您的內部部署網路裝置和 Outpost 機架，請參閱。ACE 機架連線能力

- 機架網路需求 — 請確定您符合以下變更以外的網路整備檢查清單和機架的本機網路連線章節中列出的需求：
  - ACE 機架具有四個連接到上游設備的網絡設備，而不是像單個 Outposts 機架一樣連接兩個。

  - ACE 機架不支援 1 Gbps 上行鏈路。
- 上行鏈路速度 — 為上行鏈路提供 10 Gbps、40 Gbps 或 100 Gbps 的速度。如需服務連結連線的頻寬建議，服務連結頻寬建議.

> **Important**
>
> ACE 機架不支援 1 Gbps 上行鏈路。

- 光纖 — 提供含朗訊連接器 (LC) 的單模光纖 (SMF)，或搭配朗訊連接器 (LC) 的多模光纖 (MMF)。如需支援光纖類型和光學標準的完整清單，請參閱上行鏈路速度、連接埠和光纖。
- 上游裝置 — 提供兩或四個上游裝置，可以是交換器或路由器。
- 服務 VLAN 和本機閘道 VLAN — 對於四個 ACE 網路裝置中的每一個，您必須提供服務 VLAN 和不同的本機閘道 VLAN。您可以選擇僅提供兩個不同的 VLAN，一個用於服務 VLAN，一個用於本地閘道 VLAN，或在每個 ACE 網絡設備中為服務 VLAN 和 LGW VLAN 提供不同的 VLAN，總共 8 個不同的 VLAN。如需如何使用連結彙總群組 (LAG) 和 VLAN 的詳細資訊，請參閱連結彙總和。虛擬 LAN
- 服務連結和本機閘道 VLAN 的 CIDR 和 IP 位址 — 建議您為每個具有 /30 或 /31 CIDR 的 ACE 網路裝置配置專用子網路。或者，您也可以在每個服務和本機閘道 VLAN 中配置單一 /29 子網路。在這兩種情況下，您都必須指定要使用之 ACE 網路裝置的 IP 位址。如需詳細資訊，請參閱 網路層連線。
- 服務連結 VLAN 和本機閘道 VLAN 的客戶與前哨 BGP 自主系統編號 (ASN) — 前哨站會在每個 ACE 機架裝置與您的區域網路裝置之間建立外部 BGP (EBGP) 對等工作階段，以透過服務連結 VLAN 進行服務連結。此外，它還會建立從每個 ACE 網路裝置到本機網路裝置的 EBGP 對等工作階段，以便從您的區域網路連線到本機閘道。如需詳細資訊，請參閱 服務連結 BGP 連線 及 本機閘道 BGP 連線。

> **Important**
>
> 服務連結基礎架構子網路 — Outposts 安裝中包含的每個運算機架都需要服務連結基礎結構子網路 (必須為 /26)。

電源

這些是 ACE 機架的電源需求。

需求	規格
AC 電源線電壓	單相二百至四十空調；50 或 60 赫茲
耗電量	10 千伏安單相 (AA+BB)
AC 保護裝置 (上游斷路器)	僅限 2N 輸入 (備援)：C 曲線、D 曲線或 K 曲線斷路器。 不支援 B 曲線或更低規格。
AC 電源插座類型 (插座)	IEC60309 或 L6-30P 鞭型連接器類型。

開始使用 AWS Outposts

訂購 Outpost 以開始使用。安裝 Outpost 設備之後，請啟動 Amazon EC2 執行個體並存取內部部署網路。

任務

- 建立 Outpost 並訂購 Outpost 容量
- 在前哨機架上啟動執行個體

建立 Outpost 並訂購 Outpost 容量

要開始使用 AWS Outposts，您必須創建一個前哨並訂購前哨容量。

必要條件

- 檢閱 Outpost 機架的可用配置。
- Outpost 站點是 Outpost 設備的實體位置。訂購容量之前，請確認您的站點是否符合要求。如需詳細資訊，請參閱 Outpost 機架的站點要求。
- 您必須擁有 AWS 企業 Support 計劃或 AWS 企業上線支 Support 計劃。
- 確定哪個 AWS 帳戶 將擁有前哨。使用此帳戶建立 Outpost 站點、建立 Outpost，並下訂單。監視與此帳戶關聯的電子郵件，以取得來自的資訊 AWS。

任務

- 步驟 1：建立站點
- 步驟 2：建立 Outpost
- 步驟 3：下訂單
- 步驟 4：修改執行個體容量
- 後續步驟

步驟 1：建立站點

建立站點以指定操作地址。操作地址是 Outpost 機架的實體位置。

必要條件

- 確定操作地址。

建立網站

1. 登錄以 AWS 使用擁 AWS 帳戶 有前哨站的。
2. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
3. 若要選取父項 AWS 區域，請使用頁面右上角的「區域」選取器。
4. 在導覽窗格中，選擇 Sites (網站)。
5. 選擇 Create site (建立網站)。
6. 針對 支援的硬體類型，選擇 機架和伺服器。
7. 輸入站點的名稱、描述和營運地址。
8. 針對 站點詳細資訊，提供要求的站點資訊。
    - 最大重量 – 此站點可支撐的最大機架重量，以 lbs 為單位。
    - 耗電量 – 機架硬體放置位置可用的耗電量，以 kVA 為單位。
    - 電源選項 – 您可以為硬體提供的電源選項。
    - 電源接頭 – AWS 應計畫提供以連接到硬體的電源接頭。
    - 供電位置 – 指出是從機架上方或下方供電。
    - 上行鏈路速度 – 機架連線到區域時應支援的上行鏈路速度，以 Gbps 為單位。
    - 上行鏈路數目 – 您要用來將機架連線到網路之每部 Outpost 網路裝置的上行鏈路數目。
    - 光纖類型 – 您要用來將機架連線到網路的光纖類型。
    - 光學標準 – 您要用來將機架連線到網路的光學標準類型。
9. (選擇性) 對於網站備註，請輸入任何其他有助於瞭 AWS 解網站的資訊。
10. 閱讀設施要求，然後選取 我已閱讀設施要求。
11. 選擇 Create site (建立網站)。

步驟 2：建立 Outpost

為您的機架建立 Outpost。然後，在下訂單時指定此前哨。

必要條件

- 決 AWS 定要與您的網站建立關聯的可用區域。

建立 Outpost

1. 在導覽窗格中，選擇 Outposts。
2. 選擇 建立 Outpost。
3. 選擇 機架。
4. 輸入 Outpost 的名稱和描述。
5. 選擇 Outpost 的可用區域。
6. (選擇性) 若要設定私有連線，請選取 使用私有連線。在與前哨站相同的可用區域中選擇 VPC AWS 帳戶 和子網路。如需詳細資訊，請參閱 the section called “必要條件”。
7. 針對 站點 ID，選擇您的站點。
8. 選擇 建立 Outpost。

步驟 3：下訂單

為您需要的 Outpost 機架下訂單。提交訂單之後， AWS Outposts 代表將與您聯絡。

> **Important**
>
> 提交訂單之後即無法編輯訂單，因此請在提交之前仔細檢閱所有詳細資訊。如果您需要變更訂單，請聯絡您的 AWS 客戶經理。

必要條件

- 確定訂單的支付方式。您可以預付所有費用、預付部分費用或不預付任何費用。如果您未選擇預付所有費用，您將分三年期每月支付費用。

  定價包括運輸、安裝、基礎設施服務維護，以及軟體修補和升級。
- 確定交付地址是否與您為站點指定的操作地址不同。

下訂單

1. 在導覽窗格中，選擇 訂單。
2. 選擇 下訂單。
3. 針對 支援的硬體類型，選擇 機架。
4. 若要新增容量，請選擇一種配置。如果可用的組態不符合您的需求，您可以聯絡 AWS 要求自訂容量組態。
5. 選擇下一步。
6. 選擇 使用現有的 Outpost，然後選取您的 Outpost。
7. 選擇下一步。
8. 選取合約期限和付款選項。
9. 指定運送地址。您可以指定新的地址或選取站點的操作地址。如果您選取操作地址，請注意對站點操作地址的任何未來變更都不會傳播到現有訂單。如果您需要變更現有訂單上的運送地址，請聯絡您的 AWS 客戶經理。
10. 選擇下一步。
11. 在 檢閱和訂購 頁面上，確認您的資訊正確，並視需要進行編輯。提交訂單之後，您就無法編輯訂單。
12. 選擇 下訂單。

步驟 4：修改執行個體容量

Outpost 在您的站點提供 AWS 運算和儲存容量集區，作為區 AWS 域中可用區域的私有擴充功能。由於 Outpost 中可用的運算和儲存容量是有限的，並且取決於您站點上 AWS 安裝的機架大小和數量，因此您可以決定執行初始工作負載、因應 future 成長並提供額外 AWS Outposts 容量以減輕伺服器故障和維護事件所需的 Amazon EC2、Amazon EBS 和 Amazon S3。

每個新的 Outpost 訂單的容量都設定為預設容量組態。您可以轉換預設組態以建立各種執行個體，以滿足您的業務需求。若要這麼做，您可以建立容量工作、指定執行個體大小和數量，然後執行容量工作以實作變更。

> **Note**
>
> - 您可以在為 Outposts 下訂單後變更執行個體大小的數量。
> - 例證大小和數量是在「前哨」層級定義的。

- 會根據最佳實踐自動放置例證。

修改執行個體容量

1. 從AWS Outposts 主控台的AWS Outposts 左側導覽窗格中，選擇 [容量工作]。
2. 在 [容量工作] 頁面上，選擇 [建立容量工作]。
3. 在 [開始使用] 頁面上，選擇順序。
4. 若要修改容量，您可以使用主控台中的步驟或上傳 JSON 檔案。

Console steps

1. 選擇修改新的前哨容量組態。
2. 選擇下一步。
3. 在 [設定執行個體容量] 頁面上，每個執行個體類型都會顯示一個執行個體大小，其中預先選取的 若要新增更多執行個體大小，請選擇 [新增執行個體
4. 指定執行個體數量，並記下針對該執行個體大小顯示的容量。
5. 檢視每個執行處理類型區段結尾的訊息，通知您容量超過或不足。在執行個體大小或數量層級進行調整，以最佳化您的總可用容量。
6. 您也可以 AWS Outposts 要求針對特定執行個體大小最佳化執行個體數量。若要這麼做：

   a. 選擇執行個體大小。

   b. 在相關執行個體類型區段的結尾選擇「自動平衡」。
7. 對於每個例證類型，請確保至少指定了一個例證大小的例證數量。
8. 選擇下一步。
9. 在 [檢閱並建立] 頁面上，確認您要求的更新。
10. 選擇 [建立]。 AWS Outposts 建立容量工作。
11. 在容量工作頁面上，監視工作的狀態。

> **Note**
>
> - AWS Outposts 可能會要求您停止一或多個執行中的執行個體，以啟用執行容量工作。停止這些實例後， AWS Outposts 將運行任務。

- 如果您需要在完成訂單後變更容量，請聯絡 AWS Support 以進行變更。

Upload JSON file

1. 選擇 [上傳容量組態]。
2. 選擇下一步。
3. 在 [上傳容量設定計劃] 頁面上，上傳指定執行個體類型、大小和數量的 JSON 檔案。

   Example

   範例 JSON 檔案：

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

4. 在 [容量設定計劃] 區段中檢閱 JSON 檔案的內容。
5. 選擇下一步。
6. 在 [檢閱並建立] 頁面上，確認您要求的更新。
7. 選擇 [建立]。 AWS Outposts 建立容量工作。
8. 在容量工作頁面上，監視工作的狀態。

> **Note**
>
> - AWS Outposts 可能會要求您停止一或多個執行中的執行個體，以啟用執行容量工作。停止這些實例後， AWS Outposts 將運行任務。
> - 如果您需要在完成訂單後變更容量，請聯絡 AWS Support 以進行變更。

後續步驟

您可以使用 AWS Outposts 主控台檢視訂單狀態。訂單的初始狀態為 訂單已收到。 AWS 代表將在三個工作日內與您聯繫。當您的訂單狀態變更為 訂單處理中 時，您將收到一封確認電子郵件。 AWS 代表可能會與您聯絡，以取得任何 AWS 需要的其他資訊。

如果您對訂單有任何疑問，請聯繫 AWS Support。

為了完成訂單， AWS 將與您安排一個日期和時間。

您也會收到安裝之前要確認或提供的項目檢查清單。 AWS 安裝團隊將在預定的日期和時間到達您的現場。團隊會將機架移至指定的位置，而您的電工可以為機架供電。團隊會透過您提供的上行鏈路為機架建立網路連線，並設定機架的容量。當您確認前哨站的 Amazon EC2 和 Amazon EBS 容量可從您的帳戶取得時，即表示安裝完成。 AWS

在前哨機架上啟動執行個體

安裝 Outpost 並可使用運算和儲存容量之後，即可開始建立資源。使用 Outpost 子網路在 Outpost 上啟動 Amazon EC2 執行個體，並建立 Amazon EBS 磁碟區。您也可以在 Outpost 上建立 Amazon EBS 磁碟區的快照。如需適用於 Linux 的詳細資訊，請參閱 Amazon EC2 使用者指南 AWS Outposts 中的本機亞馬遜 EBS 快照。如需適用於 Windows 的詳細資訊，請參閱 Amazon EC2 使用者指南 AWS Outposts中的本機亞馬遜 EBS 快照。

先決條件

您的站點必須安裝 Outpost。如需詳細資訊，請參閱 建立 Outpost 並訂購 Outpost 容量。

任務

- 步驟 1：建立 VPC
- 步驟 2：建立子網路和自訂路由表
- 步驟 3：設定本機閘道連線
- 步驟 4：設定內部部署網路
- 步驟 5：在前哨上啟動實例
- 步驟 6：測試連線

步驟 1：建立 VPC

您可以將該 AWS 地區中的任何 VPC 擴展到您的前哨站。如果您已經擁有可以使用的 VPC，請略過此步驟。

為您的前哨建立 VPC

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選擇與 Outposts 機架相同的區域。
3. 在功能窗格中，選擇 [您的 VPC]，然後選擇 [建立 V PC]。
4. 僅選擇 VPC。
5. (選擇性) 對於名稱標籤，請輸入 VPC 的名稱。
6. 對於 IPv4 CIDR 區塊，請選擇 IPv4 CIDR 手動輸入，然後在 IPv4 CIDR 文字方塊中輸入 VPC 的 IPv4 位址範圍。

   > **Note**
   >
   > 如果您想要使用直接 VPC 路由，請指定與您在內部部署網路中使用的 IP 範圍不重疊的 CIDR 範圍。

7. 對於 IPv6 CIDR 區塊，請選擇「無 IPv6 CIDR 封鎖」。
8. 對於「租賃」，選擇「預設」
9. (選擇性) 若要將標籤新增至 VPC，請選擇 [新增標籤]，然後輸入金鑰和值。
10. 選擇建立 VPC。

步驟 2：建立子網路和自訂路由表

您可以建立 Outpost 子網路，並將其新增至前哨所在 AWS 地區的任何 VPC。當您這樣做時，VPC 會包含前哨站。如需詳細資訊，請參閱 網路元件。

> **Note**
>
> 如果您要在 Outpost 子網路中啟動另一個與您共用的執行個體 AWS 帳戶，請跳至步驟 5：在前哨上啟動實例。

2a：建立前哨子網路

建立前哨子網路

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 在導覽窗格中，選擇 Outpost。
3. 選取 Outpost，然後選擇 動作、建立子網路。系統會將您重新導向以在 Amazon VPC 主控台中建立子網路。我們會為您選取 Outpost，以及 Outpost 所在的可用區域。
4. 選取 VPC。
5. 在子網路設定中，選擇性地為子網路命名，並指定子網路的 IP 位址範圍。
6. 選擇 Create subnet (建立子網路)。
7. (選擇性) 若要更容易識別 Outpost 子網路，請啟用「子網路」頁面上的「前哨 ID」欄。若要啟用欄，請選擇「偏好設定」圖示，選取「前哨 ID」，然後選擇「確認」。

2b：創建自定義路由表

使用下列程序建立具有以本機閘道為目標之路由的自訂路由表。您無法使用相同的路由表作為可用區域子網路。

建立自訂路由表

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇路由表。
3. 選擇 Create route table (建立路由表)。
4. (選用) 針對 Name (名稱)，輸入路由表的名稱。
5. 在 VPC 中，選擇您的 VPC。
6. (選用) 若要新增標籤，請選擇 Add new tag (新增標籤)，然後輸入標籤鍵和標籤值。
7. 選擇 Create route table (建立路由表)。

2c：關聯前哨子網路和自訂路由表

若要將路由表路由套用至特定子網，您必須將路由表與子網建立關聯。路由表可以和多個子網建立關聯。不過，子網一次只能與一個路由表相關聯。根據預設，所有未與表明確建立關聯的子網都會與主路由表隱含建立關聯。

建立前哨子網路與自訂路由表的關聯

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇「路由表」。
3. 在 Subnet associations (子網關聯) 標籤上，選擇 Edit subnet associations (編輯子網關聯)。
4. 選取子網路的核取方塊以和路由表建立關聯。
5. 選擇 Save associations (儲存關聯)。

步驟 3：設定本機閘道連線

本機閘道 (LGW) 可讓 Outpost 子網路與內部部署網路之間的連線能力。如需 LGW 的詳細資訊，請參閱本機閘道。

若要在 Outposts 子網路中的執行個體與區域網路之間提供連線，您必須完成下列工作。

三. 建立自訂本機閘道路由表

您可以使用 AWS Outposts 主控台為本機閘道 (LGW) 建立自訂路由表。

使用控制台建立自訂 LGW 路由表

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選擇 建立本機閘道路由表。
5. (選擇性) 在名稱中，輸入 LGW 路由表的名稱。
6. 針對 本機閘道，選擇您的本機閘道。
7. 針對 模式，選擇與您內部部署網路通訊的模式。

    - 選擇 直接 VPC 路由 以使用執行個體的私有 IP 地址。
    - 選擇 CoIP 以使用客戶擁有的 IP 地址。
        - (選擇性) 新增或移除 CoIP 集區和其他 CIDR 區塊

          [新增 CoIP 集區] 選擇 新增集區，然後執行下列動作：
            - 針對 名稱，輸入您的 CoIP 集區名稱。
            - 針對 CIDR，輸入客戶擁有 IP 地址的 CIDR 區塊。

- [新增 CIDR 區塊] 選擇 新增 CIDR，然後輸入客戶擁有的 IP 地址範圍。
- [移除 CoIP 集區或其他 CIDR 區塊] 選擇 CIDR 區塊右側或 CoIP 集區下方的 移除。

  您最多可以指定 10 個 CoIP 集區和 100 個 CIDR 區塊。

8. (選用) 新增或移除標籤。

   [新增標籤] 選擇新增標籤，並執行下列動作：

   - 對於 Key (金鑰)，輸入金鑰名稱。
   - 對於 Value (值)，進入金鑰值。

   [移除標籤] 選擇標籤金鑰和值右側的 移除。

9. 選擇 建立本機閘道路由表。

3b：將 VPC 與自訂 LGW 路由表建立關聯

您必須將 VPC 與 LGW 路由表建立關聯。這兩者預設沒有關聯。

使用下列程序將 VPC 與 LGW 路由表建立關聯。

您可選擇性地為關聯新增標籤，以便根據組織需求進行識別或分類。

AWS Outposts console

將 VPC 與自訂 LGW 路由表建立關聯

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選取路由表，然後選擇 動作、關聯 VPC。
5. 針對 VPC ID，選取要與本機閘道路由表建立關聯的 VPC。
6. (選用) 新增或移除標籤。

   若要新增標籤，請選擇 新增標籤，然後執行下列動作：

   - 在索引鍵中，輸入索引鍵名稱。
   - 對於 Value (值)，進入金鑰值。

若要移除標籤，請選擇標籤索引鍵和值右側的 移除。

7. 選擇 Associate VPC (關聯 VPC)。

AWS CLI

將 VPC 與自訂 LGW 路由表建立關聯

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

範例

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

輸出

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

3c：在前哨子網路路由表中添加路由條目

在 Outpost 子網路路由表中新增路由項目，以啟用 Outpost 子網路和 LGW 之間的流量。

VPC 內的 Outpost 子網路 (與 Outpost LGW 路由表相關聯) 可以為其路由表具有一個額外的前哨本機閘道 ID 目標類型。考慮您希望通過 LGW 將目標地址為 172.16.100.0/24 的流量路由到客戶網絡的情況。若要這麼做，請編輯 Outpost 子網路路由表，並在目的地網路和 LGW () `lgw-xxxx` 目標中新增以下路由。

目的地	目標
172.16.100.0/24	`lgw-id`

若要在 Outpost 子網路路由表中新增路由項目**`lgw-id`**做為目標：

1. 前往 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇「路由表」(Route table)，然後選取您在中建立的路由表格2b：創建自定義路由表。
3. 選擇動作，然後選擇編輯路由。
4. 若要新增路由，請選擇 Add route (新增路由)。
5. 針對目的地，輸入目的地 CIDR 區塊至客戶網路。
6. 針對「目標」，選擇「前哨本機閘道 ID」。
7. 選擇儲存變更。

3d：將自訂 LGW 路由表與 LGW VIF 群組建立關聯

VIF 群組是虛擬介面 (VIF) 的邏輯分組。將本機閘道路由表與 VIF 群組建立關聯。

將自訂 LGW 路由表與 LGW VIF 群組建立關聯

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選擇路由表。
5. 在詳細資訊窗格中選擇 VIF 群組關聯 標籤，然後選擇 編輯 VIF 群組關聯。
6. 對於 VIF 群組設定，選取關聯 VIF 群組，然後選擇 VIF 群組。
7. 選擇儲存變更。

3e：在 LGW 路線表中添加路線條目

編輯本機閘道路由表，以新增以 VIF 群組做為目標的靜態路由，並新增內部部署子網路 CIDR 範圍 (或 0.0.0.0/0) 做為目的地的靜態路由。

目的地	目標
172.16.100.0/24	`VIF-Group-ID`

在 LGW 路由表中新增路線條目

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 在導覽窗格中，選擇 本機閘道路由表。
3. 選取本機閘道路由表，然後選擇 [動作]、[編輯路由]。
4. 選擇 Add route (新增路由)。
5. 針對 目的地，輸入目的地 CIDR 區塊、單一 IP 地址或字首清單的 ID。
6. 針對 目標，選取本機閘道的 ID。
7. 選擇 Save routes (儲存路由)。

3f：(選擇性) 指派客戶擁有的 IP 位址給執行個體

如果您在中設定 Outposts 三. 建立自訂本機閘道路由表 以使用客戶擁有的 IP (CoIP) 位址集區，則必須從 CoIP 位址集區配置彈性 IP 位址，並將彈性 IP 位址與執行個體建立關聯。如需 CoIP 的詳細資訊，請參閱《客戶擁有的 IP 地址》。

如果您將 Outposts 設定為使用直接 VPC 路由 (DVR)，請略過此步驟。

Amazon VPC console

指派 CoIP 位址給執行個體

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇 Elastic IPs (彈性 IP)。
3. 選擇 Allocate Elastic IP address (配置彈性 IP 地址)。
4. 針對 網路邊界群組，選取要從中公告 IP 地址的位置。
5. 針對 公有 IPv4 地址集區，選擇 客戶擁有的 IPv4 地址集區。
6. 針對 客戶擁有的 IPv4 地址集區，選取您已設定的集區。
7. 選擇 Allocate (配置)。
8. 選取彈性 IP 地址，然後選擇 動作、與彈性 IP 地址建立關聯。
9. 從 執行個體 選取執行個體，然後選擇 關聯。

AWS CLI

指派 CoIP 位址給執行個體

1. 使用 describe-coip-pools 命令擷取客戶擁有的地址集區相關資訊。

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

下列為範例輸出。

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

2. 使用 allocate-address 命令配置彈性 IP 地址。使用在上一個步驟中傳回的集區 ID。

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

下列為範例輸出。

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

3. 使用 associate-address 命令，建立彈性 IP 地址與 Outpost 執行個體的關聯。https://docs.aws.amazon.com/cli/latest/reference/ec2/associate-address.html使用在上一個步驟中傳回的配置 ID。

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

下列為範例輸出。

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

共用的客戶擁有 IP 地址集區

如果您想要使用共用的客戶擁有 IP 地址集區，則必須先共用該集區，然後才能開始設定。如需如何共用客戶擁有 IPv4 地址的資訊，請參閱《 指南》中的《AWS RAM 共用您的 AWS 資源》。

步驟 4：設定內部部署網路

前哨建立了從每個前哨網路裝置 (OND) 到客戶本地網路裝置 (CND) 的外部 BGP 對等，以便將流量從您的內部部署網路傳送和接收到 Outposts。如需詳細資訊，請參閱本機閘道 BGP 連線。

若要從內部部署網路傳送和接收流量至 Outpost，請確定：

- 在您的客戶網路裝置上，本機閘道 VLAN 上的 BGP 工作階段從您的網路裝置處於作用中狀態。
- 對於從內部部署到 Outposts 的流量，請確保您在 CND 中收到來自 Outposts 的 BGP 廣告。這些 BGP 廣告包含內部部署網路必須使用的路由，才能將流量從內部部署路由到 Outpost。因此，請確保您的網路在 Outposts 和內部部署資源之間具有正確的路由。
- 對於從 Outposts 傳送到內部部署網路的流量，請確定您的 CND 正在將內部部署網路子網路的 BGP 路由廣告傳送至 Outposts (或 0.0.0.0/0)。作為替代方案，您可以向 Outposts 宣傳默認路由（例如 0.0.0.0/0 ）。CND 通告的內部部署子網路必須具有等於或包含在中設定的 CIDR 範圍內的 CIDR 範圍。3e：在 LGW 路線表中添加路線條目

範例：直接 VPC 模式下的 BGP 廣告

假設您有一個以直接 VPC 人雲端模式設定的前哨站，其中兩個 Outposts 機架式網路裝置透過本機閘道 VLAN 連接至兩個客戶的區域網路裝置。設定了下列項目：

- 具有 CIDR 區塊 10.0.0.0/16 的 VPC。
- VPC 中具有 CIDR 區塊 10.0.3.0/24 的前哨子網路。
- 內部部署網路中具有 CIDR 區塊的子網路
- Outposts 會使用 Outpost 子網路上執行個體的私人 IP 位址，例如 10.0.3.0/24，與您的內部部署網路通訊。

在這種情況下，通告的路由：

- 通往客戶裝置的本機閘道是 10.0.3.0/24。
- 您通往前哨本地閘道的客戶裝置是 172.16.100.0/24。

因此，本機閘道會將目標網路 172.16.100.0/24 的輸出流量傳送至您的客戶裝置。確定您的網路具有正確的路由組態，可將流量傳遞至網路內的目的地主機。

如需檢查 BGP 工作階段狀態以及這些工作階段中公告路由所需的特定命令和組態，請參閱網路廠商的說明文件。如需疑難排解，請參閱AWS Outposts 機架式網路疑難排解

範例：CoIP 模式下的 BGP 廣告

考慮一下，您有一個前哨，其中包含兩個 Outposts 機架式網路裝置，透過本機閘道 VLAN 連接至兩個客戶本機網路裝置的案例。設定了下列項目：

- 具有 CIDR 區塊 10.0.0.0/16 的 VPC。
- VPC 中具有 CIDR 區塊 10.0.3.0/24 的子網路。
- 客戶擁有的 IP 集區 (10.1.0.0/26)。
- 將 10.0.3.112 關聯到 10.1.0.2 的彈性 IP 地址關聯。
- 內部部署網路中具有 CIDR 區塊的子網路
- Outpost 與內部部署網路之間的通訊將使用 CoIP 彈性 IP 來定址 Outpost 中的執行個體，而不是使用 VPC CIDR 範圍。

在這種情況下，通告的路由：

- 通往客戶裝置的本機閘道是 10.1.0.0/26。
- 您通往前哨本地閘道的客戶裝置是 172.16.100.0/24。

因此，本機閘道會將目標網路 172.16.100.0/24 的輸出流量傳送至您的客戶裝置。確定您的網路具有正確的路由組態，可將流量傳遞至網路內的目的地主機。

如需檢查 BGP 工作階段狀態以及這些工作階段中公告路由所需的特定命令和組態，請參閱網路廠商的說明文件。如需疑難排解，請參閱AWS Outposts 機架式網路疑難排解

步驟 5：在前哨上啟動實例

您可以在建立的 Outpost 子網路中，或在與您共用的 Outpost 子網路中，啟動 EC2 執行個體。安全群組可控制 Outpost 子網路中執行個體的傳入與傳出 VPC 流量，就像可用區域子網路中的執行個體一樣。若要連線到 Outpost 子網路中的 EC2 執行個體，您可以在啟動執行個體時指定金鑰對，就像可用區域子網路中的執行個體一樣。

考量事項

- 您可以建立放置群組來影響 Amazon EC2 應嘗試將相互依存的執行個體群組放在 Outpost 硬體上的方式。您可以選擇符合工作負載需求的放置群組策略。
- 如果您的 Outpost 已設定為使用客戶擁有的 IP (CoIP) 地址集區，則必須為您啟動的任何執行個體指派客戶擁有的 IP 地址。

在 Outpost 子網路中啟動執行個體

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 在導覽窗格中，選擇 Outpost。
3. 選取 Outpost，然後選擇 動作、檢視詳細資訊。
4. 在 Outpost 摘要 頁面上，選擇 啟動執行個體。系統會將您重新導向至 Amazon EC2 主控台中的執行個體啟動精靈。我們會為您選取 Outpost 子網路，並僅顯示 Outposts 機架支援的執行個體類型。
5. 選擇您的 Outposts 機架支援的執行個體類型。請注意，顯示為灰色的執行個體不適用於您的 Outpost。
6. (選擇性) 若要將執行個體啟動到放置群組中，請展開 進階詳細資訊，然後捲動至 放置群組。您可以選取現有的放置群組或建立新的放置群組。
7. 完成精靈以啟動 Outpost 子網路中的執行個體。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的下列內容：
   - Linux — 使用新啟動執行個體精靈啟動執行個體
   - Windows — 使用新的啟動執行個體精靈啟動執行個體

> **Note**
>
> 如果您要建立 Amazon EBS 磁碟區，則必須使用 gp2 磁碟區類型，否則精靈將會失敗。

步驟 6：測試連線

您可以透過使用適當的使用案例來測試連線。

測試從您本機網路到 Outpost 的連線

從區域網路中的電腦，將ping命令執行到 Outpost 執行個體的私有 IP 位址。

```
ping 10.0.3.128
```

下列為範例輸出。

```
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
```

測試從 Outpost 執行個體到您本機網路的連線

視您的作業系統而定，使用 ssh 或 rdp 連線到您 Outpost 執行個體的私有 IP 地址。如需連線至 Linux 執行個體的相關資訊，請參閱 Amazon EC2 使用者指南中的 Connect 到 Linux 執行個體。如需連線至 Windows 執行個體的相關資訊，請參閱 Amazon EC2 使用者指南中的 Connect 到 Windows 執行個體。

在執行個體執行之後，請對您本機網路中電腦的 IP 地址執行 ping 命令。在下列範例中，IP 地址為 172.16.0.130。

```
ping 172.16.0.130
```

下列為範例輸出。

```
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
```

測試 AWS 區域和前哨站之間的連接

在 AWS 區域中的子網路中啟動執行個體。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
```

在執行個體執行之後，請執行下列操作：

1. 取得 AWS 區域中執行個體的私有 IP 位址。此資訊可在 Amazon EC2 主控台的執行個體詳細資訊頁面上找到。
2. 視您的作業系統而定，使用 ssh 或 rdp 連線到您 Outpost 執行個體的私有 IP 地址。
3. 從 Outpost 執行個體執行ping命令，指定 AWS 區域中執行個體的 IP 位址。

   ```
   ping 10.0.1.5
   ```

   下列為範例輸出。

   ```
   Pinging 10.0.1.5

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

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

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

客戶擁有的 IP 地址連線範例

測試從您本機網路到 Outpost 的連線

從您本機網路中的電腦，對 Outpost 執行個體的客戶擁有 IP 地址執行 ping 命令。

```
ping 172.16.0.128
```

下列為範例輸出。

```
Pinging 172.16.0.128

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

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

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

測試從 Outpost 執行個體到您本機網路的連線

視您的作業系統而定，使用 ssh 或 rdp 連線到您 Outpost 執行個體的私有 IP 地址。如需連線至 Linux 執行個體的相關資訊，請參閱 Amazon EC2 使用者指南中的 Connect 到 Linux 執行個體。如需連線至 Windows 執行個體的相關資訊，請參閱 Amazon EC2 使用者指南中的 Connect 到 Windows 執行個體。

在 Outpost 執行個體執行之後，請對您本機網路中電腦的 IP 地址執行 ping 命令。

```
ping 172.16.0.130
```

下列為範例輸出。

```
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
```

測試 AWS 區域和前哨站之間的連接

在 AWS 區域中的子網路中啟動執行個體。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
```

在執行個體執行之後，請執行下列操作：

1. 取得 AWS 區域執行個體私有 IP 位址，例如 10.0.0.5。此資訊可在 Amazon EC2 主控台的執行個體詳細資訊頁面上找到。
2. 視您的作業系統而定，使用 ssh 或 rdp 連線到您 Outpost 執行個體的私有 IP 地址。
3. 將命ping令從 Outpost 執行個體執行到 AWS 區域執行個體 IP 位址。

   ```
   ping 10.0.0.5
   ```

   下列為範例輸出。

   ```
   Pinging 10.0.0.5

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

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

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

AWS Outposts 連線至 AWS 區域

AWS Outposts 通過服務鏈路連接支持廣域網絡（WAN）連接。

目錄

透過服務連結進行連線

服務鏈接是您的 Outposts 和您選擇的 AWS 地區（或所在地區）之間的必要連接，並允許對 Outposts 進行管理以及進出該地區的流量交換。 AWS 服務連結利用一組加密的 VPN 連線來與主要區域進行通訊。

若要設定服務連結連線，您或 AWS 必須在 Outpost 佈建期間設定服務連結實體、虛擬 LAN (VLAN) 以及與本機網路裝置的網路層連線。如需詳細資訊，請參閱《機架的本機網路連線》和《Outpost 機架的站點要求》。

對於與該地區的廣域網絡（WAN）連接， AWS Outposts 可以通過該 AWS 地區的公共連接建立服務鏈接 VPN 連接。 AWS 這需要 Outposts 能夠訪問該地區的公共 IP 範圍，這些 IP 範圍可以通過公共互聯網或公 AWS Direct Connect 共虛擬界面。如需目前的 IP 地址範圍，請參閱《Amazon VPC 使用者指南》中的《AWS IP 地址範圍》。此連線可透過在服務連結網路層路徑中設定特定或預設 (0.0.0.0/0) 路由來啟用。如需詳細資訊，請參閱《服務連結 BGP 連線》和《服務連結基礎設施子網路公告和 IP 範圍》。

或者，您可以為 Outpost 選取私有連線選項。如需詳細資訊，請參閱《使用 VPC 進行服務連結私有連線》。

建立服務連結連線後，您的 Outpost 就會開始運作，並由 AWS其管理。服務連結用於下列流量：

- Outpost 與任何相關聯 VPC 之間的客戶 VPC 流量。
- Outpost 管理流量，例如資源管理、資源監控，以及韌體和軟體更新。

服務連結最大傳輸單位 (MTU) 要求

網路連線的最大傳輸單位 (MTU) 係允許通過該連線的最大封包大小 (以位元組為單位)。網路必須在父區域中的 Outpost 和服務連結端點之間支援 1500 位元組的 MTU。 AWS 如需 Outpost 中的執行個體與 AWS 區域中透過服務連結的執行個體之間所需 MTU 的相關資訊，請參閱 Amazon EC2 使用者指南中的 Amazon EC2 執行個體的網路最大傳輸單位 (MTU)。

服務連結頻寬建議

為了獲得最佳體驗和恢復能力， AWS 建議您使用至少 500 Mbps 的備援連線 (1 Gbps 更好) 來連接至區域的服務連線。 AWS 您可以使用 AWS Direct Connect 或互聯網連接的服務鏈接。至少 500 Mbps 的服務連結連線可讓您啟動 Amazon EC2 執行個體、連接 Amazon EBS 磁碟區，以及存取 AWS 服務，例如 Amazon EKS、Amazon EMR 和指標。 CloudWatch

您的 Outpost 服務連結頻寬要求會因下列特性而有所不同：

- AWS Outposts 機架數量和容量配置
- 工作負載特性，例如 AMI 大小、應用程式彈性、爆量速度需求和區域的 Amazon VPC 流量

若要收到有關您需求所需服務連結頻寬的自訂建議，請聯絡您的 AWS 銷售代表或 APN 合作夥伴。

防火牆和服務連結

本節討論防火牆組態和服務連結連線。

在下圖中，組態將 Amazon VPC 從該 AWS 區域延伸到前哨基地。公 AWS Direct Connect 共虛擬界面是服務鏈接連接。下列流量會通過服務連結和 AWS Direct Connect 連線：

- 透過服務連結傳送至 Outpost 的管理流量
- Outpost 與任何相關聯 VPC 之間的流量

如果您搭配網際網路連線使用具狀態的防火牆來限制從公有網際網路到服務連結 VLAN 的連線，則可以封鎖所有從網際網路起始的傳入連線。這是因為服務連結 VPN 只會從 Outpost 起始到區域，不會從區域起始到 Outpost。

如果您使用防火牆來限制來自服務連結 VLAN 的連線，則可以封鎖所有傳入連線。根據下表，您必須允許從 AWS 區域返回前哨的輸出連線。如果防火牆具狀態，則會允許來自 Outpost 的傳出連線，這表示其是從 Outpost 起始，應允許反向傳入。

通訊協定	來源連接埠	來源地址	目標連接埠	目的地地址
UDP	443	AWS Outposts 服務鏈接 /26	443	AWS Outposts 地區的公共路線
TCP	1025-65535	AWS Outposts 服務鏈接 /26	443	AWS Outposts 地區的公共路線

> **Note**
>
> Outpost 中的執行個體無法使用服務連結與另一個 Outpost 中的執行個體進行通訊。利用透過本機閘道或本機網路介面的路由在 Outpost 之間進行通訊。
> AWS Outposts 機架也採用備援電源和網路設備設計，包括本機閘道元件。如需詳細資訊，請參閱 AWS Outposts.

使用 VPC 進行服務連結私有連線

當您建立 Outpost 時，可以在主控台中選取私有連線選項。當您這麼做時，就會在使用您指定的 VPC 和子網路安裝 Outpost 之後，建立服務連結 VPN 連線。這允許透過 VPC 進行私有連線，並最大程度地減少公有網際網路暴露。

必要條件

您必須先符合下列先決條件，才能為 Outpost 設定私有連線：

- 您必須設定 IAM 實體 (使用者或角色) 的許可，允許使用者或角色建立服務連結角色以進行私有連線。IAM 實體需要許可才能存取下列動作：
  - `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*` 的 `iam:CreateServiceLinkedRole`
  - `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*` 的 `iam:PutRolePolicy`

- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`

如需詳細資訊，請參閱 以下項目的身分識別與存取管理 (IAM) AWS Outposts 及 使用 AWS Outposts的服務連結角色。

- 在與您的 Outpost 相同的 AWS 帳戶和可用區域中，建立 VPC 的唯一目的是使用 /25 或更大版本的子網路 /25 或更高版本，而該 VPC 不會與 10.1.0.0/16 衝突。例如，您可以使用 10.2.0.0/16。
- 建立 AWS Direct Connect 連線、私有虛擬界面和虛擬私有閘道，以允許內部部署 Outpost 存取 VPC。如果 AWS Direct Connect 連線位於與 VPC 不同的 AWS 帳戶中，請參閱《AWS Direct Connect 使用者指南》中的〈跨帳戶建立虛擬私有閘道關聯〉。
- 向您的內部部署網路公告子網路 CIDR。您可以使 AWS Direct Connect 用這樣做。如需詳細資訊，請參閱《 指南》中的《AWS Direct Connect AWS Direct Connect 虛擬介面》和《使用 AWS Direct Connect 閘道》。

當您在 AWS Outposts 主控台中建立 Outpost 時，可以選取私有連線選項。如需說明，請參閱建立 Outpost 並訂購 Outpost 容量。

> **Note**
>
> 若要在 Outpost 處於 擱置中 狀態時選取私有連線選項，請從主控台選擇 Outpost，然後選取您的 Outpost。選擇 動作、新增私有連線，然後依照步驟進行。

為 Outpost 選取私人連線選項後， AWS Outposts 會自動在您的帳戶中建立服務連結角色，讓其代表您完成下列工作：

- 在您指定的子網路和 VPC 中建立網路介面，並為網路介面建立安全群組。
- 授予 AWS Outposts 服務權限，以將網路介面連結至帳戶中的服務連結端點執行個體。
- 將網路介面連接至帳戶中的服務連結端點執行個體。

如需服務連結角色的詳細資訊，請參閱使用 AWS Outposts的服務連結角色。

> **Important**
>
> 安裝 Outpost 之後，請確認可從 Outpost 連線到子網路中的私有 IP。

備援網際網路連線

當您建立從 Outpost 到 AWS 區域的連線時，我們建議您建立多個連線以獲得更高的可用性和彈性。如需詳細資訊，請參閱 AWS Direct Connect 彈性建議。

如果您需要連線到公有網際網路，您可以使用備援網際網路連線和各種網際網路供應商，就像現有的內部部署工作負載一樣。

Outpost 和站點

管理的 AWS Outposts Outposts 和網站.

您可標記 Outpost 和站點，幫助您根據組織需求予以識別或分類。如需有關標記的詳細資訊，請參閱AWS 一般參考 指南中的標記 AWS 資源。

主題

- 管理 Outpost
- 管理 Outpost 站點

管理 Outpost

AWS Outposts 包括稱為 Outposts 的硬件和虛擬資源。請利用本節建立及管理 Outpost，包括變更名稱，以及新增或檢視詳細資訊或標籤。

建立 Outpost

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 Outpost。
4. 選擇 建立 Outpost。
5. 選擇此 Outpost 的硬體類型。
6. 輸入 Outpost 的名稱和描述。
7. 選擇 Outpost 的可用區域。
8. (選擇性) 選擇 私有連線選項。對於虛擬私人雲端和子網路，請在與前哨站相同的 AWS 帳戶和可用區域中選取 VPC 和子網路。

   > **Note**
   >
   > 如果需要復原您 Outpost 的私有連線，您必須聯絡 AWS Enterprise Support。

9. 從 站點 ID，執行以下其中一項：

   - 若要選取現有站點，請選擇該站點。
   - 若要建立新的站點，請選擇 建立站點，按一下 下一步 並在新視窗中輸入站點的相關資訊。

建立站點之後，請返回此視窗以選取站點。您可能需要重新整理站點清單才能看到新站點。若要重新整理資料，請選擇重新整理圖示 ()。

如需詳細資訊，請參閱 the section called “網站”。

10. 選擇 建立 Outpost。

> **Tip**
>
> 您必須下訂單才能為新的 Outpost 增加容量。

使用下列步驟編輯 Outpost 名稱和描述。

編輯 Outpost 名稱和描述

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 Outpost。
4. 選取 Outpost，然後選擇 動作、編輯 Outpost。
5. 修改名稱和描述。

   針對 名稱，輸入名稱。

   針對 描述，輸入描述。
6. 選擇儲存變更。

使用下列步驟檢視 Outpost 詳細資訊。

檢視 Outpost 詳細資訊

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 Outpost。
4. 選取 Outpost，然後選擇 動作、檢視詳細資訊。

您也可以使用檢視 AWS CLI 前哨詳細資料。

若要檢視前哨詳細資料 AWS CLI

- 使用取得前哨 AWS CLI 指令。

使用下列步驟管理 Outpost 的標籤。

管理 Outpost 標籤

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 Outpost。
4. 選取 Outpost，然後選擇 動作、管理標籤。
5. 新增或移除標籤。

   若要新增標籤，請選擇 新增標籤，然後執行下列動作：

   - 在索引鍵中，輸入索引鍵名稱。
   - 對於 Value (值)，進入金鑰值。

   若要移除標籤，請選擇標籤索引鍵和值右側的 移除。
6. 選擇儲存變更。

管理 Outpost 站點

客戶管理的實體建築物， AWS 將在其中安裝您的前哨。站點必須符合 Outpost 的設施、網路和電源要求。如需詳細資訊，請參閱 Outposts 機架的要求。

建立 Outpost 站點

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 站點。
4. 選擇 Create site (建立網站)。
5. 選擇站點支援的硬體類型。

6. 輸入站點的名稱、描述和營運地址。如果選擇在站點支援機架，請輸入下列資訊：
   - 最大重量 – 指定此站點可承受的最大機架重量。
   - 耗電量 – 指定機架硬體放置位置可提供的耗電量，以 kVA 為單位。
   - 電源選項 – 指定您可為硬體提供的電源選項。
   - 電源連接器 — 指定 AWS 應計劃為連接硬體提供的電源連接器。
   - 供電位置 – 指定從機架上方或下方供電。
   - 上行鏈路速度 – 指定機架連線到區域應支援的上行鏈路速度。
   - 上行鏈路數目 – 指定您要用來將機架連線到網路之每部 Outpost 網路裝置的上行鏈路數目。
   - 光纖類型 – 指定您要用來將 Outpost 連線到網路的光纖類型。
   - 光學標準 – 指定您要用來將 Outpost 連線到網路的光學標準類型。
   - 備註 - 指定有關站點的備註。
7. 閱讀設施要求並選擇 我已閱讀設施要求。
8. 選擇 Create site (建立網站)。

使用下列步驟編輯 Outpost 站點。

編輯站點

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 站點。
4. 選取站點，然後選取 動作、編輯站點。
5. 您可以修改名稱、描述、營運地址和站點詳細資訊。

   如果變更營運地址，請注意此類變更不會傳播到現有訂單。
6. 選擇儲存變更。

使用下列步驟檢視 Outpost 站點的詳細資訊。

檢視站點詳細資訊

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。

3. 在導覽窗格中，選擇 站點。
4. 選取站點，然後選擇 動作、檢視詳細資訊。

使用下列步驟管理 Outpost 站點的標籤。

管理站點標籤

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 站點。
4. 選取站點，然後選擇 動作、管理標籤。
5. 新增或移除標籤。

   若要新增標籤，請選擇 新增標籤，然後執行下列動作：

   - 在索引鍵中，輸入索引鍵名稱。
   - 對於 Value (值)，進入金鑰值。

   若要移除標籤，請選擇標籤索引鍵和值右側的 移除。
6. 選擇儲存變更。

本機閘道

本機閘道是 Outpost 架構的核心元件。本機閘道可讓您在 Outpost 子網路與內部部署網路之間進行連線。如果內部部署基礎設施提供網際網路存取，則在 Outpost 上執行的工作負載也可以利用本機閘道與區域服務或區域工作負載進行通訊。這種連線可透過使用公有連線 (網際網路) 或使用 Direct Connect 來實現。如需詳細資訊，請參閱 AWS Outposts 連線至 AWS 區域。

目錄

本機閘道基本概念

每個 Outpost 都支援單一本機閘道。本機閘道具有下列元件：

- 路由表 – 可用來建立本機閘道路由表。如需詳細資訊，請參閱 the section called “本機閘道路由表”。
- CoIP 集區 – (選擇性) 您可以使用自己擁有的 IP 地址範圍，在內部部署網路與 VPC 中的執行個體之間進行通訊。如需詳細資訊，請參閱 the section called “客戶擁有的 IP 地址”。
- 虛擬介面 (VIF) — 為每個 LAG AWS 建立一個 VIF，並將兩個 VIF 新增至 VIF 群組。本機閘道路由表必須具有一個連到兩個 VIF 的預設路由，才能進行本機網路連線。如需詳細資訊，請參閱 本機網路連線。
- VIF 群組關聯 — AWS 將其建立的 VIF 新增至 VIF 群組。VIF 群組是 VIF 的邏輯分組。如需詳細資訊，請參閱 the section called “VIF 群組關聯”。
- VPC 關聯 – 可用來建立 VPC 與本機閘道路由表之間的 VPC 關聯。與位於 Outpost 上的子網路相關聯的 VPC 路由表可以使用本機閘道作為路由目標。如需詳細資訊，請參閱 the section called “VPC 關聯”。

當 AWS 佈建您的前哨機架時，我們會創建一些組件，您需要負責創建其他組件。

AWS 責任

- 提供硬體。

- 建立本機閘道。
- 建立虛擬介面 (VIF) 和 VIF 群組。

您的責任

- 建立本機閘道路由表。
- 將 VPC 與本機閘道路由表建立關聯。
- 將 VIF 群組與本機閘道路由表建立關聯。

路由

Outpost 子網路中的執行個體可以使用下列其中一個選項，透過本機閘道與您的內部部署網路進行通訊：

- 私有 IP 地址 – 本機閘道會使用 Outpost 子網路中執行個體的私有 IP 地址與您的內部部署網路進行通訊。此為預設值。
- 客戶擁有的 IP 地址 – 本機閘道會針對您指派給 Outpost 子網路中執行個體的客戶擁有 IP 地址執行網路位址轉譯 (NAT)。此選項支援重疊的 CIDR 範圍和其他網路拓撲。

如需詳細資訊，請參閱 the section called “本機閘道路由表”。

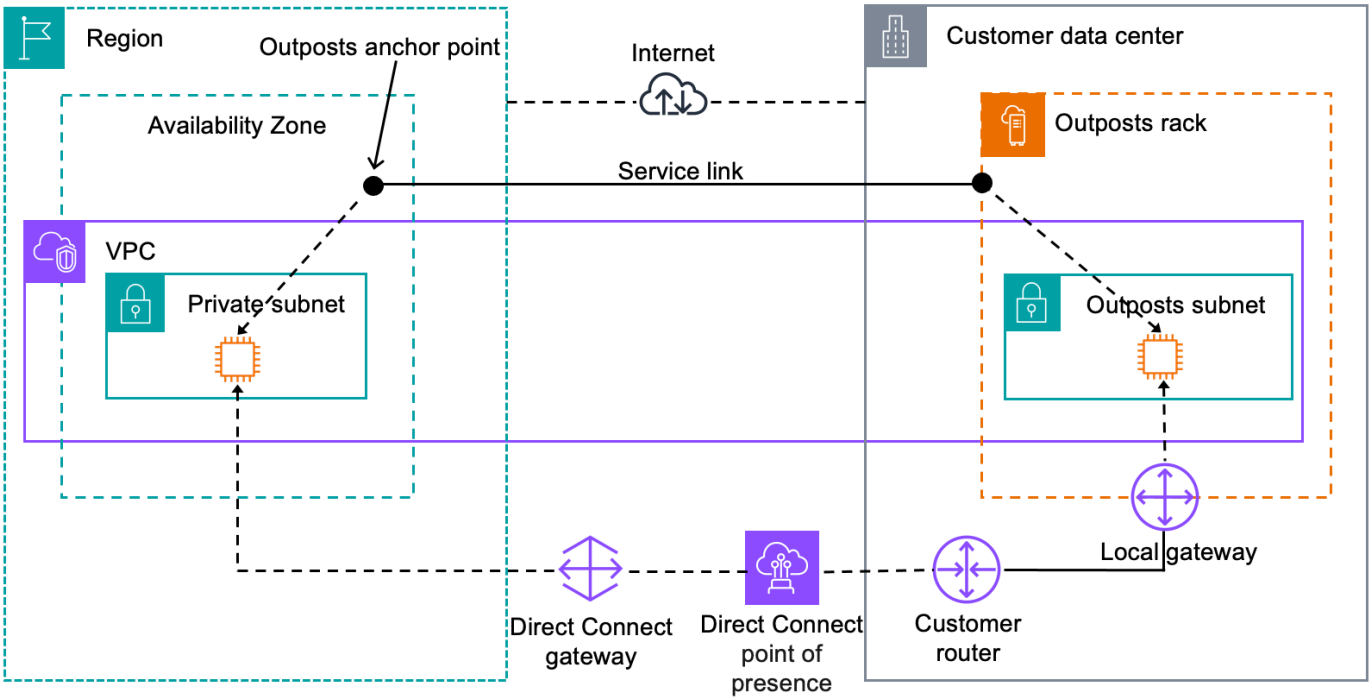
透過本機閘道進行連線

本機閘道的主要角色是提供從 Outpost 到本機內部部署網路的連線。其也可讓您透過內部部署網路連線到網際網路。如需範例，請參閱 the section called “直接 VPC 路由” 和 the section called “客戶擁有的 IP 地址”。

本機閘道也可以提供回到「 AWS 區域」的資料平面路徑。本機閘道的資料平面路徑會透過本機閘道，從 Outpost 周遊到您的私有本機閘道 LAN 區段。然後會遵循私有路徑返回該區域中的 AWS 服務端點。請注意，無論您使用的資料平面路徑為何，控制平面路徑一律會使用服務連結連線。

您可以將內部部署 Outposts 基礎架構連接到 AWS 服務 該地區私下。 AWS Direct Connect如需詳細資訊，請參閱《AWS Outposts 私有連線》。

下圖顯示如何透過本機閘道進行連線：



本機閘道路由表

機架上的 Outpost 子網路路由表可包含連至內部部署網路的路由。本機閘道會將此流量路由至內部部署網路，以提供低延遲路由。

根據預設，Outpost 會使用 Outpost 上執行個體的私有 IP 地址與您的內部部署網路進行通訊。這稱為「 AWS Outposts的直接 VPC 路由」(或直接 VPC 路由)。不過，您可以提供地址範圍 (稱為「客戶擁有的 IP 地址集區」(CoIP))，讓網路上的執行個體使用這些地址與您的內部部署網路進行通訊。直接 VPC 路由和 CoIP 是互斥的選項，路由的運作方式會根據您的選擇而有所不同。

目錄

直接 VPC 路由

直接 VPC 路由會使用 VPC 中執行個體的私有 IP 地址與您的內部部署網路進行通訊。這些地址會透過 BGP 公告到您的內部部署網路。BGP 公告僅適用於屬於 Outpost 機架上子網路的私有 IP 地址。這種

類型的路由是 Outpost 的預設模式。在此模式下，本機閘道不會針對執行個體執行 NAT，而且您不需要將彈性 IP 地址指派給 EC2 執行個體。您可以選擇使用自己的地址空間，而不是使用直接 VPC 路由模式。如需詳細資訊，請參閱 客戶擁有的 IP 地址。

直接 VPC 路由僅支援執行個體網路介面。使用代表您 AWS 建立的網路介面 (稱為請求者管理的網路介面)，其私有 IP 位址無法從您的內部部署網路存取。例如，無法從您的內部部署網路直接連線到 VPC 端點。

下列範例說明直接 VPC 路由。

範例

- 範例：透過 VPC 進行網際網路連線
- 範例：透過內部部署網路進行網際網路連線

範例：透過 VPC 進行網際網路連線

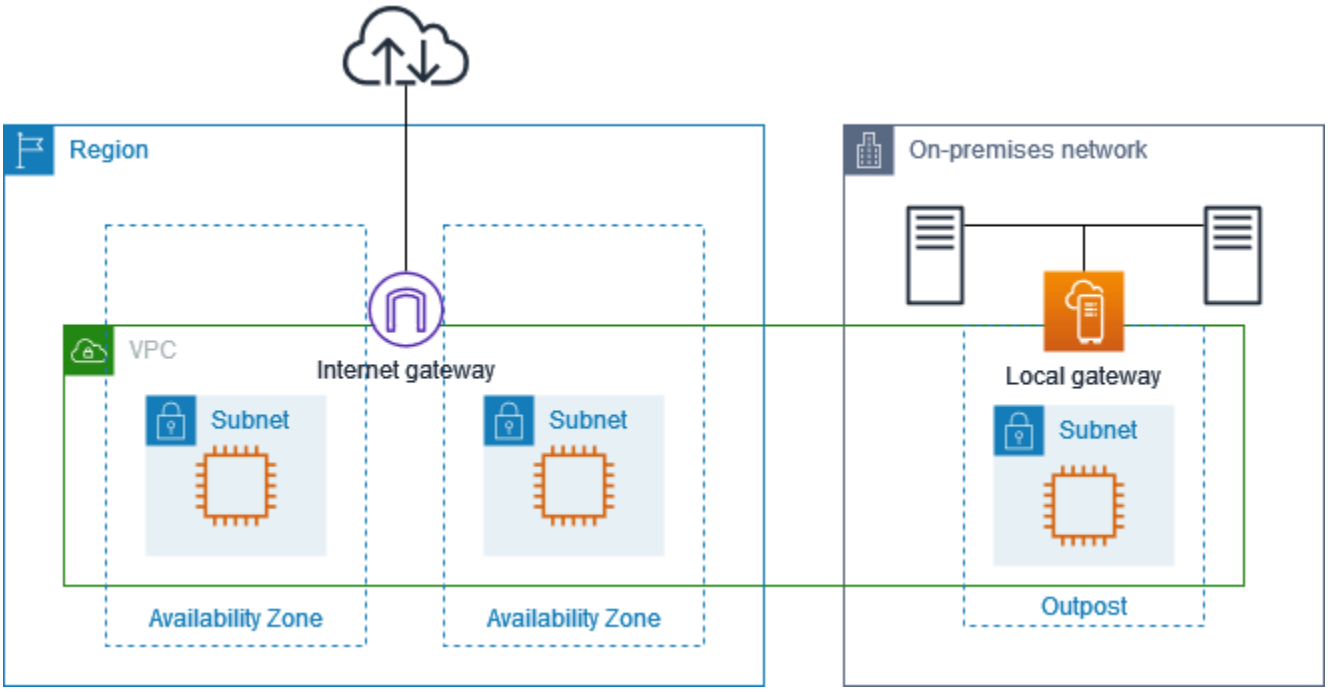
Outpost 子網路中的執行個體可以透過連接至 VPC 的網際網路閘道存取網際網路。

請考慮下列組態：

- 父 VPC 跨越兩個可用區域，每個可用區域都有一個子網路。
- Outpost 有一個子網路。
- 每個子網路都有一個 EC2 執行個體。
- 本機閘道會使用 BGP 公告，將 Outpost 子網路的私人 IP 地址公告到內部部署網路。

> **Note**
>
> 只有 Outpost 上具有以本機閘道為目的地之路由的子網路，才支援 BGP 公告。任何其他子網路都不會透過 BGP 公告。

在下圖中，來自 Outpost 子網路中執行個體的流量可以使用網際網路閘道，讓 VPC 存取網際網路。



若要透過父區域實現網際網路連線，Outpost 子網路的路由表必須具有下列路由。

目的地	目標	說明
VPC CIDR	區域	提供 VPC 中子網路之間的連線。
0.0.0.0	*internet-gateway-id*	將目的地為網際網路的流量傳送至網際網路閘道。
###### CIDR	*local-gateway-id*	將目的地為內部部署網路的流量傳送至本機閘道。

範例：透過內部部署網路進行網際網路連線

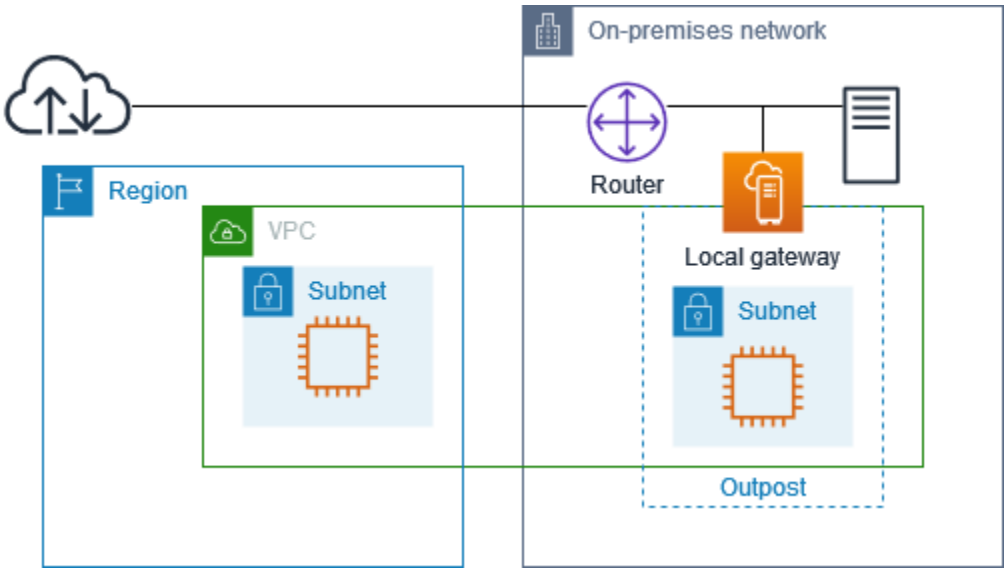
Outpost 子網路中的執行個體可以透過內部部署網路存取網際網路。Outpost 子網路中的執行個體不需要公有 IP 地址或彈性 IP 地址。

請考慮下列組態：

- Outpost 子網路有一個 EC2 執行個體。
- 內部部署網路中的路由器會執行網路位址轉譯 (NAT)。
- 本機閘道會使用 BGP 公告，將 Outpost 子網路的私人 IP 地址公告到內部部署網路。

> **Note**
>
> 只有 Outpost 上具有以本機閘道為目的地之路由的子網路，才支援 BGP 公告。任何其他子網路都不會透過 BGP 公告。

在下圖中，來自 Outpost 子網路中執行個體的流量可以使用本機閘道存取網際網路或內部部署網路。來自內部部署網路的流量會使用本機閘道來存取 Outpost 子網路中的執行個體。



若要透過內部部署網路實現網際網路連線，Outpost 子網路的路由表必須具有下列路由。

目的地	目標	說明
VPC CIDR	區域	提供 VPC 中子網路之間的連線。
0.0.0.0/0	*local-gateway-id*	將目的地為網際網路的流量傳送至本機閘道。

對網際網路的傳出存取

起始自 Outpost 子網路中執行個體且目的地為網際網路的流量會使用 0.0.0.0/0 的路由，將流量路由至本機閘道。本機閘道會將流量傳送至路由器。路由器會使用 NAT 將私有 IP 地址轉譯為路由器上的公有 IP 地址，然後將流量傳送至目的地。

對內部部署網路的傳出存取

起始自 Outpost 子網路中執行個體且目的地為內部部署網路的流量會使用 0.0.0.0/0 的路由，將流量路由至本機閘道。本機閘道會將流量傳送至內部部署網路中的目的地。

來自內部部署網路的傳入存取

來自內部部署網路且目的地為 Outpost 子網路中執行個體的流量會使用執行個體的私有 IP 地址。當流量到達本機閘道時，本機閘道會將流量傳送至 VPC 中的目的地。

客戶擁有的 IP 地址

根據預設，本機閘道會使用 VPC 中執行個體的私有 IP 地址與您的內部部署網路進行通訊。不過，您可以提供地址範圍 (稱為「客戶擁有的 IP 地址集區」(CoIP))，以支援重疊的 CIDR 範圍和其他網路拓撲。

如果選擇 CoIP，則必須建立地址集區、將其指派給本機閘道路由表，並透過 BGP 將這些地址公告回您的客戶網路。任何與本機閘道路由表相關聯的客戶擁有 IP 地址，都會在路由表中顯示為傳播路由。

客戶擁有的 IP 地址可讓您對內部部署網路中的資源進行本機或外部連線。您可以透過從客戶擁有的 IP 集區配置新的彈性 IP 地址，然後將其指派給您的資源，將這些 IP 地址指派給 Outpost 上的資源 (例如 EC2 執行個體)。如需詳細資訊，請參閱 the section called “3f：(選擇性) 指派客戶擁有的 IP 位址給執行個體”。

客戶擁有的 IP 地址集區適用下列要求：

- 您必須能夠路由網路中的地址
- CIDR 區塊必須至少為 /26

當您從客戶擁有的 IP 地址集區配置彈性 IP 地址時，您會繼續擁有客戶擁有 IP 地址集區中的 IP 地址。您有責任視需要在內部網路或 WAN 上公告這些地址。

您可以選擇性地使用與組織 AWS 帳戶 中的多個人共用 AWS Resource Access Manager客戶擁有的集區。共用集區之後，參與者就可以從客戶擁有的 IP 地址集區配置彈性 IP 地址，然後將其指派給 Outpost 上的 EC2 執行個體。如需詳細資訊，請參閱 AWS RAM 使用者指南中的共用 AWS 資源。

範例

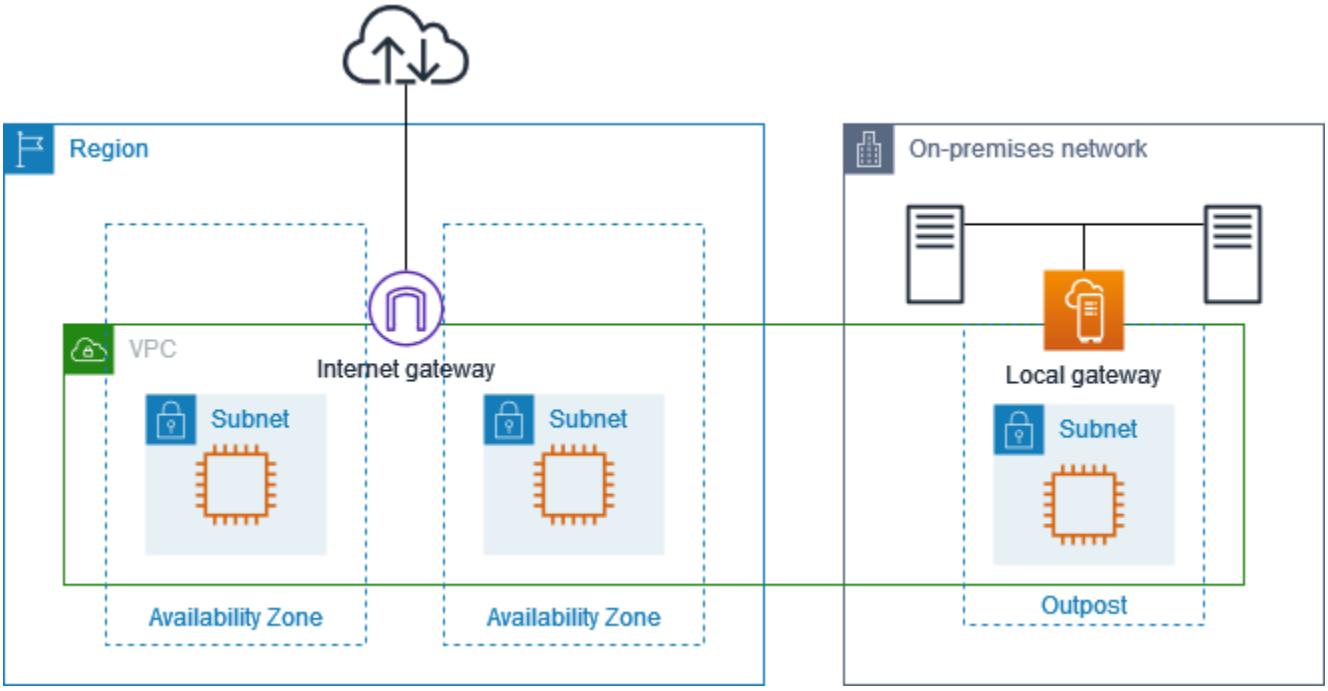
- 範例：透過 VPC 進行網際網路連線
- 範例：透過內部部署網路進行網際網路連線

範例：透過 VPC 進行網際網路連線

Outpost 子網路中的執行個體可以透過連接至 VPC 的網際網路閘道存取網際網路。

請考慮下列組態：

- 父 VPC 跨越兩個可用區域，每個可用區域都有一個子網路。
- Outpost 有一個子網路。
- 每個子網路都有一個 EC2 執行個體。
- 有一個客戶擁有的 IP 地址集區。
- Outpost 子網路中的執行個體具有來自客戶擁有 IP 地址集區的彈性 IP 地址。
- 本機閘道會使用 BGP 公告，將客戶擁有的 IP 地址集區公告到內部部署網路。



若要透過區域實現網際網路連線，Outpost 子網路的路由表必須具有下列路由。

目的地	目標	說明
VPC CIDR	區域	提供 VPC 中子網路之間的連線。
0.0.0.0	*internet-gateway-id*	將目的地為公有網際網路的流量傳送至網際網路閘道。

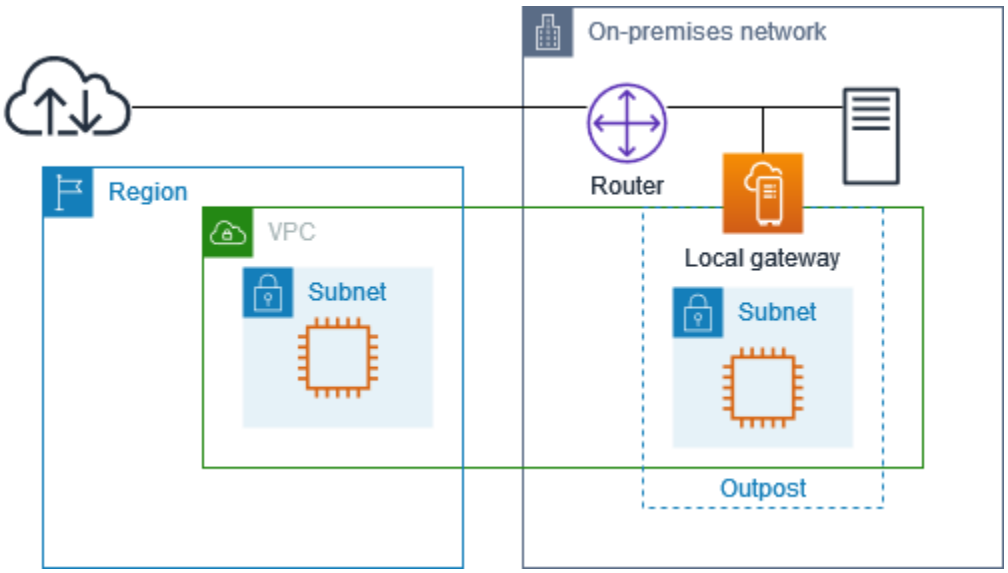
目的地	目標	說明
###### CIDR	*local-gateway-id*	將目的地為內部部署網路的流量傳送至本機閘道。

範例：透過內部部署網路進行網際網路連線

Outpost 子網路中的執行個體可以透過內部部署網路存取網際網路。

請考慮下列組態：

- Outpost 子網路有一個 EC2 執行個體。
- 有一個客戶擁有的 IP 地址集區。
- 本機閘道會使用 BGP 公告，將客戶擁有的 IP 地址集區公告到內部部署網路。
- 將 10.0.3.112 映射至 10.1.0.2 的彈性 IP 地址關聯。
- 客戶內部部署網路中的路由器會執行 NAT。



若要透過本機閘道實現網際網路連線，Outpost 子網路的路由表必須具有下列路由。

目的地	目標	說明
VPC CIDR	區域	提供 VPC 中子網路之間的連線。

目的地	目標	說明
0.0.0.0/0	*local-gateway-id*	將目的地為網際網路的流量傳送至本機閘道。

對網際網路的傳出存取

起始自 Outpost 子網路中 EC2 執行個體且目的地為網際網路的流量會使用 0.0.0.0/0 的路由，將流量路由至本機閘道。本機閘道會將執行個體的私有 IP 地址映射至客戶擁有的 IP 地址，然後將流量傳送至路由器。路由器會使用 NAT 將客戶擁有的 IP 地址轉譯為路由器上的公有 IP 地址，然後將流量傳送至目的地。

對內部部署網路的傳出存取

起始自 Outpost 子網路中 EC2 執行個體且目的地為內部部署網路的流量會使用 0.0.0.0/0 的路由，將流量路由至本機閘道。本機閘道會將 EC2 執行個體的 IP 地址轉譯為客戶擁有的 IP 地址 (彈性 IP 地址)，然後將流量傳送至目的地。

來自內部部署網路的傳入存取

來自內部部署網路且目的地為 Outpost 子網路中執行個體的流量會使用執行個體的客戶擁有 IP 地址 (彈性 IP 地址)。當流量到達本機閘道時，本機閘道會將客戶擁有的 IP 地址 (彈性 IP 地址) 映射至執行個體 IP 地址，然後將流量傳送至 VPC 中的目的地。此外，本機閘道路由表會評估任何以彈性網路介面為目標的路由。如果目的地地址符合任何靜態路由的目的地 CIDR，流量就會傳送至該彈性網路介面。當流量遵循彈性網路介面的靜態路由時，則會保留目的地地址，而不會將其轉譯為網路介面的私有 IP 地址。

使用本機閘道路由表

做為機架安裝的一部分， AWS 建立本機閘道、設定 VIF 和 VIF 群組。您可以建立本機閘道路由表。本機閘道路由表必須與 VIF 群組和 VPC 有關聯。您可以建立和管理 VIF 群組和 VPC 的關聯。請考慮以下有關本機閘道路由表的資訊：

- VIF 群組和本機閘道路由表必須有 one-to-one關係。
- 本機閘道由與 Outpost 相關聯的 AWS 帳戶所擁有，只有擁有者可以修改本機閘道路由表。
- 您可以使用與其他 AWS 帳戶或組織單位共用本機閘道路由表 AWS Resource Access Manager。如需詳細資訊，請參閱《使用共用的 AWS Outpost 資源》。

- 本機閘道路由表的模式可決定是使用執行個體的私有 IP 地址與您的內部部署網路進行通訊 (直接 VPC 路由)，還是使用客戶擁有的 IP 地址集區 (CoIP) 進行通訊。直接 VPC 路由和 CoIP 是互斥的選項，路由的運作方式會根據您的選擇而有所不同。如需詳細資訊，請參閱 ???。
- 直接 VPC 路由模式不支援重疊的 CIDR 範圍。

任務

- 檢視本機閘道路由表詳細資訊
- 建立自訂本機閘道路由表
- 管理本機閘道路由表路由
- 管理本機閘道路由表標籤
- 切換本機閘道路由表模式或刪除本機閘道路由表
- 管理 CoIP 集區
- VIF 群組關聯
- VPC 關聯

檢視本機閘道路由表詳細資訊

您可以使用主控台或 AWS CLI來檢視本機閘道路由表的詳細資訊。

AWS Outposts console

檢視本機閘道路由表詳細資訊

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選取本機閘道路由表，然後選擇 動作、檢視詳細資訊。

AWS CLI

檢視本機閘道路由表詳細資訊

使用描述本機閘道路由表命令 AWS CLI 。

範例

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

輸出

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

> **Note**
>
> 如果您正在檢視的預設本機閘道路由表使用 CoIP 模式，則本機閘道路由表會設定為具有一個連至每個 VIF 的預設路由，以及一個連至 CoIP 集區中每個相關聯客戶擁有 IP 地址的傳播路由。

建立自訂本機閘道路由表

您可以使用 AWS Outposts 主控台建立本機閘道的自訂路由表。

使用主控台建立自訂本機閘道路由表

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選擇 建立本機閘道路由表。
5. (選擇性) 針對 名稱，輸入您的本機閘道路由表名稱。
6. 針對 本機閘道，選擇您的本機閘道。
7. (選擇性) 選擇 關聯 VIF 群組，然後選擇您的 VIF 群組。

8. 針對 模式，選擇與您內部部署網路通訊的模式。

   - 選擇 直接 VPC 路由 以使用執行個體的私有 IP 地址。
   - 選擇 CoIP 以使用客戶擁有的 IP 地址。
     - (選擇性) 新增或移除 CoIP 集區和其他 CIDR 區塊

       [新增 CoIP 集區] 選擇 新增集區，然後執行下列動作：
       - 針對 名稱，輸入您的 CoIP 集區名稱。
       - 針對 CIDR，輸入客戶擁有 IP 地址的 CIDR 區塊。
     - [新增 CIDR 區塊] 選擇 新增 CIDR，然後輸入客戶擁有的 IP 地址範圍。
     - [移除 CoIP 集區或其他 CIDR 區塊] 選擇 CIDR 區塊右側或 CoIP 集區下方的 移除。

       您最多可以指定 10 個 CoIP 集區和 100 個 CIDR 區塊。
9. (選用) 新增或移除標籤。

   [新增標籤] 選擇新增標籤，並執行下列動作：

   - 對於 Key (金鑰)，輸入金鑰名稱。
   - 對於 Value (值)，進入金鑰值。

   [移除標籤] 選擇標籤金鑰和值右側的 移除。
10. 選擇 建立本機閘道路由表。

管理本機閘道路由表路由

您可以建立本機閘道路由表以及對 Outpost 上彈性網路介面的傳入路由。您也可以修改現有的本機閘道傳入路由來變更目標彈性網路介面。

只有當路由的目標彈性網路介面連接至執行中的執行個體時，路由才會處於作用中狀態。如果執行個體已停止或介面已分離，則路由會從作用中狀態變為黑洞狀態。

本機閘道適用下列要求和限制：

- 目標彈性網路介面必須屬於您 Outpost 上的子網路，而且必須連接至該 Outpost 中的執行個體。本機閘道路由無法以不同 Outpost 上或父 AWS 區域中的 Amazon EC2 執行個體為目標。
- 子網路必須屬於與本機閘道路由表相關聯的 VPC。
- 同一個路由表中的彈性網路介面路由數量不得超過 100 個。

- AWS 優先考慮最具體的路由，如果路由匹配，我們將靜態路由優先於傳播的路由。
- 不支援介面 VPC 端點。
- BGP 公告僅適用於 Outpost 上具有路由表中以本機閘道為目標之路由的子網路。如果子網路在路由表中沒有以本機閘道為目標的路由，則不會透過 BGP 公告這些子網路。
- 只有連接至 Outpost 執行個體的 ENI 才能透過該 Outpost 的本機閘道進行通訊。屬於 Outpost 子網路但連接至區域中執行個體的 ENI 無法透過該 Outpost 的本機閘道進行通訊。
- 無法透過本機閘道從內部部署連線到受管介面 (例如 VPCE 端點或介面)。只能從 Outpost 內的執行個體連線到這些介面。

適用下列 NAT 考量。

- 本機閘道不會在符合彈性網路介面路由的流量上執行 NAT，而是會保留目的地 IP 地址。
- 關閉目標彈性網路介面的來源/目的地檢查。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的網路界面基本概念。
- 將作業系統設定為允許在網路介面上接受來自目的地 CIDR 的流量。

AWS Outposts console

編輯本機閘道路由表路由

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選取本機閘道路由表，然後選擇 動作、編輯路由。
5. 若要新增路由，請選擇 Add route (新增路由)。針對 目的地，輸入目的地 CIDR 區塊、單一 IP 地址或字首清單的 ID。
6. 若要修改現有路由，請針對 Destination (目的地)，取代目的地 CIDR 區塊或單一 IP 地址。針對 Target (目標)，選擇一個目標。
7. 選擇 Save routes (儲存路由)。

AWS CLI

建立本機閘道路由表路由

- 使用「建立-本機閘道-路 AWS CLI 由」指令。

範例

```
aws ec2 create-local-gateway-route \
    --local-gateway-route-table-id lgw-rtb-059615ef7dEXAMPLE \
    --network-interface-id eni-03e612f0a1EXAMPLE \
    --destination-cidr-block 192.0.2.0/24
```

輸出

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

修改本機閘道路由表路由

您可以修改現有路由的目標彈性網路介面。若要進行修改操作，路由表必須已有具指定目的地 CIDR 區塊的路由。

- 使用「修改-局部-閘道-佈 AWS CLI 線」指令。

範例

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

輸出

```
{
    "Route": {
```

```
        "DestinationCidrBlock": "192.0.2.0/24",
        "NetworkInterfaceId": "eni-12a345b6c7EXAMPLE",
        "Type": "static",
        "State": "active",
        "LocalGatewayRouteTableId": "lgw-rtb-059615ef7dEXAMPLE",
        "LocalGatewayRouteTableArn": "arn:aws:ec2:us-west-2:111122223333:local-
gateway-route-table/lgw-rtb-059615ef7dEXAMPLE",
        "OwnerId": "111122223333"
    }
}
```

管理本機閘道路由表標籤

您可為本機閘道路由表新增標籤，以便根據組織需求進行識別或分類。

管理本機閘道路由表標籤

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選取本機閘道路由表，然後選擇 動作、管理標籤。
5. 新增或移除標籤。

   若要新增標籤，請選擇 新增標籤，然後執行下列動作：

   - 在索引鍵中，輸入索引鍵名稱。
   - 對於 Value (值)，進入金鑰值。

   若要移除標籤，請選擇標籤索引鍵和值右側的 移除。
6. 選擇儲存變更。

切換本機閘道路由表模式或刪除本機閘道路由表

您必須刪除並重建本機閘道路由表，才能切換模式。刪除本機閘道路由表會導致網路流量中斷。

切換模式或刪除本機閘道路由表

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/

2. 請確認您是否正確無誤 AWS 區域。

   若要變更「地區」，請使用頁面右上角的「地區」選擇器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 確認本機閘道路由表是否與 VIF 群組相關聯。如果已關聯，則必須移除本機閘道路由表與 VIF 群組之間的關聯。

   a. 選擇本機閘道路由表的 ID。
   b. 選擇 VIF 群組關聯索引標籤。
   c. 如果一或多個 VIF 群組與本機閘道路由表相關聯，請選擇 「編輯 VIF 群組關聯」。
   d. 清除「關聯 VIF 群組」核取方塊。
   e. 選擇儲存變更。
5. 選擇 [刪除本機閘道路由表]。
6. 在確認對話方塊中輸入 **delete**，然後選擇 刪除。
7. (選擇性) 使用新模式建立本機閘道路由表。

   a. 在導覽窗格中，選擇 本機閘道路由表。
   b. 選擇 建立本機閘道路由表。
   c. 使用新模式設定本機閘道路由表。如需詳細資訊，請參閱《建立自訂本機閘道路由表》。

管理 CoIP 集區

您可以提供 IP 地址範圍，在內部部署網路與 VPC 中的執行個體之間進行通訊。如需詳細資訊，請參閱《客戶擁有的 IP 地址》。

客戶擁有的 IP 集區適用於 CoIP 模式的本機閘道路由表。若要在本機閘道路由表模式之間切換，請參閱《切換本機閘道路由表模式》。

使用下列程序建立 CoIP 集區。

建立 CoIP 集區

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選擇路由表。

5. 在詳細資訊窗格中選擇 CoIP 集區 標籤，然後選擇 建立 CoIP 集區。
6. (選擇性) 針對 名稱，輸入您的 CoIP 集區名稱。
7. 選擇 新增 CIDR，然後輸入客戶擁有的 IP 地址範圍。
8. (選擇性) 新增或移除 CIDR 區塊

   [新增 CIDR 區塊] 選擇 新增 CIDR，然後輸入客戶擁有的 IP 地址範圍。

   [移除 CIDR 區塊] 選擇 CIDR 區塊右側的 移除。
9. 選擇 建立 CoIP 集區。

使用下列程序編輯 CoIP 集區。

編輯 CoIP 集區

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選擇路由表。
5. 在詳細資訊窗格中選擇 CoIP 集區 標籤，然後選擇 CoIP 集區。
6. 選擇 動作、編輯 CoIP 集區。
7. 選擇 新增 CIDR，然後輸入客戶擁有的 IP 地址範圍。
8. (選擇性) 新增或移除 CIDR 區塊

   [新增 CIDR 區塊] 選擇 新增 CIDR，然後輸入客戶擁有的 IP 地址範圍。

   [移除 CIDR 區塊] 選擇 CIDR 區塊右側的 移除。
9. 選擇儲存變更。

使用下列程序管理標籤或將名稱標籤新增至 CoIP 集區。

管理 CoIP 集區上的標籤

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。

4. 選擇路由表。
5. 在詳細資訊窗格中選擇 CoIP 集區 標籤，然後選擇 CoIP 集區。
6. 選擇 動作、管理標籤。
7. 新增或移除標籤。

   若要新增標籤，請選擇 新增標籤，然後執行下列動作：

   - 在索引鍵中，輸入索引鍵名稱。
   - 對於 Value (值)，進入金鑰值。

   若要移除標籤，請選擇標籤索引鍵和值右側的 移除。
8. 選擇儲存變更。

使用下列程序刪除 CoIP 集區。

刪除 CoIP 集區

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選擇路由表。
5. 在詳細資訊窗格中選擇 CoIP 集區 標籤，然後選擇 CoIP 集區。
6. 選擇 動作、刪除 CoIP 集區。
7. 在確認對話方塊中輸入 **`delete`**，然後選擇 刪除。

VIF 群組關聯

VIF 群組是虛擬介面 (VIF) 的邏輯分組。您可以變更與 VIF 群組相關聯的本機閘道路由表。取消 VIF 群組與本機閘道路由表的關聯時，會刪除路由表中的所有路由並中斷網路流量。

變更 VIF 群組的關聯

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。

4. 選擇路由表。
5. 在詳細資訊窗格中選擇 VIF 群組關聯 標籤，然後選擇 編輯 VIF 群組關聯。
6. 針對 VIF 群組設定，執行下列其中一個動作：

   - 若要將 VIF 群組與本機閘道路由表建立關聯，請選擇 關聯 VIF 群組，然後選擇 VIF 群組。
   - 若要取消 VIF 群組與本機閘道路由表的關聯，請清除 關聯 VIF 群組。

   > **Important**
   >
   > 取消 VIF 群組與本機閘道路由表的關聯時，會自動刪除所有路由並中斷網路流量。

7. 選擇儲存變更。

VPC 關聯

您必須將 VPC 與本機閘道路由表建立關聯。這兩者預設沒有關聯。

建立 VPC 關聯

使用下列程序將 VPC 與本機閘道路由表建立關聯。

您可選擇性地為關聯新增標籤，以便根據組織需求進行識別或分類。

AWS Outposts console

建立 VPC 的關聯

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選取路由表，然後選擇 動作、關聯 VPC。
5. 針對 VPC ID，選取要與本機閘道路由表建立關聯的 VPC。
6. (選用) 新增或移除標籤。

   若要新增標籤，請選擇 新增標籤，然後執行下列動作：

   - 在索引鍵中，輸入索引鍵名稱。
   - 對於 Value (值)，進入金鑰值。

若要移除標籤，請選擇標籤索引鍵和值右側的 移除。

7. 選擇 Associate VPC (關聯 VPC)。

AWS CLI

建立 VPC 的關聯

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

範例

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

輸出

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

刪除 VPC 關聯

使用下列程序取消 VPC 與本機閘道路由表的關聯。

AWS Outposts console

取消 VPC 的關聯

1. 請在以下位置開啟 AWS Outposts 主控台。 https://console.aws.amazon.com/outposts/
2. 若要變更 AWS 區域，請使用頁面右上角的「地區」選取器。
3. 在導覽窗格中，選擇 本機閘道路由表。

4. 選取路由表，然後選擇 動作、檢視詳細資訊。
5. 在 VPC 關聯 中，選取要取消關聯的 VPC，然後選擇 取消關聯。
6. 選擇取消關聯。

AWS CLI

取消 VPC 的關聯

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

範例

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

輸出

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

機架的本機網路連線

您需要下列元件才能將 Outpost 機架連線到內部部署網路：

- 從 Outpost 配線面板到客戶本機網路裝置的實體連線。
- 連結彙總控制通訊協定 (LACP)，以建立兩個連至 Outpost 網路裝置和本機網路裝置的連結彙總群組 (LAG) 連線。
- Outpost 與客戶本機網路裝置之間的虛擬 LAN (VLAN) 連線。
- 每個 VLAN 的第 3 層 point-to-point 連線能力。
- Outpost 與內部部署服務連結之間路由公告的邊界閘道協定 (BGP)。
- Outpost 與內部部署本機網路裝置之間路由公告的 BGP，以連線到本機閘道。

目錄

實體連線

Outpost 機架有兩部連接至您本機網路的實體網路裝置。

Outpost 在這些 Outpost 網路裝置與您的本機網路裝置之間至少需要兩個實體連結。Outpost 針對每個 Outpost 網路裝置支援下列上行鏈路速度和數量。

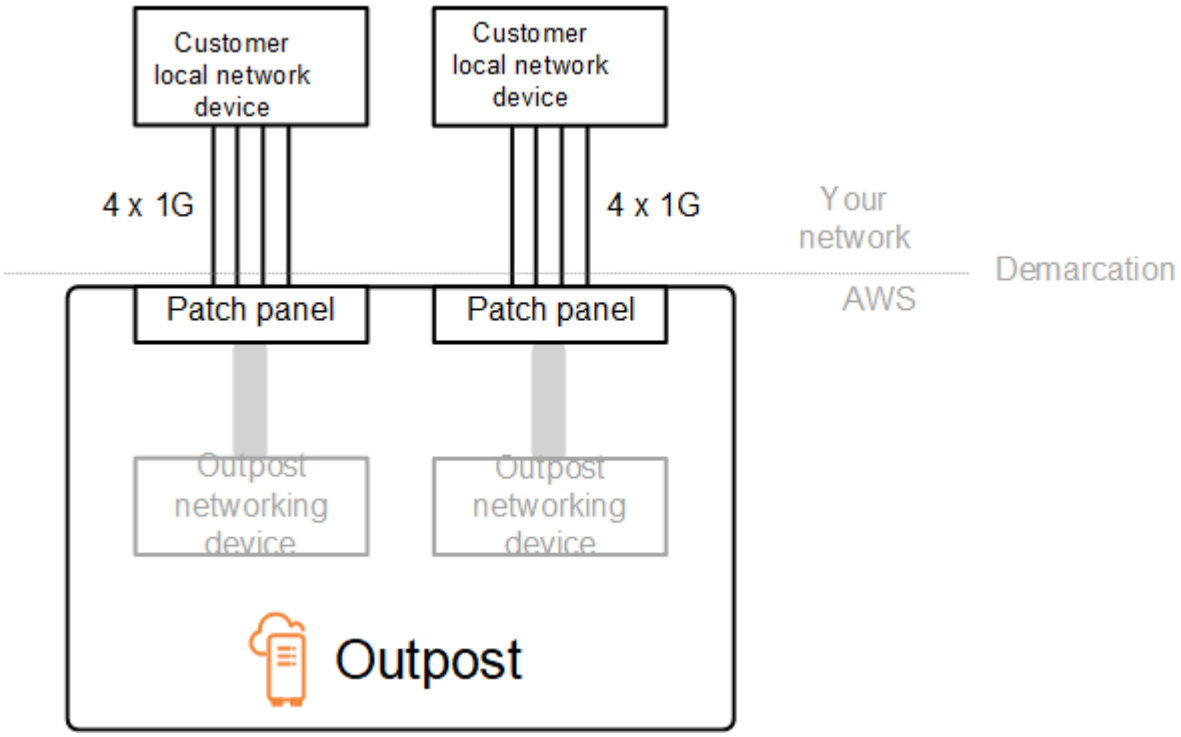
上行鏈路速度	上行鏈路數目
1 Gbps	1、2、4、6 或 8

上行鏈路速度	上行鏈路數目
10 Gbps	1、2、4、8、12 或 16
40 Gbps 或 100 Gbps	1、2 或 4

上行鏈路速度和數量在每部 Outpost 網路裝置上都是對稱的。如果您使用 100 Gbps 的上行鏈路速度，則必須設定正向錯誤修正 (FEC CL91) 的連結。

前哨機架可支援單模光纖 (SMF)，搭配朗訊連接器 (LC)、多模光纖 (MMF) 或含 LC 的 MMF OM4。AWS 提供與您在機架位置提供的光纖相容的光學元件。

在下圖中，實體分界是每個 Outpost 中的光纖配線面板。您必須提供將 Outpost 連線到配線面板所需的光纖纜線。



連結彙總

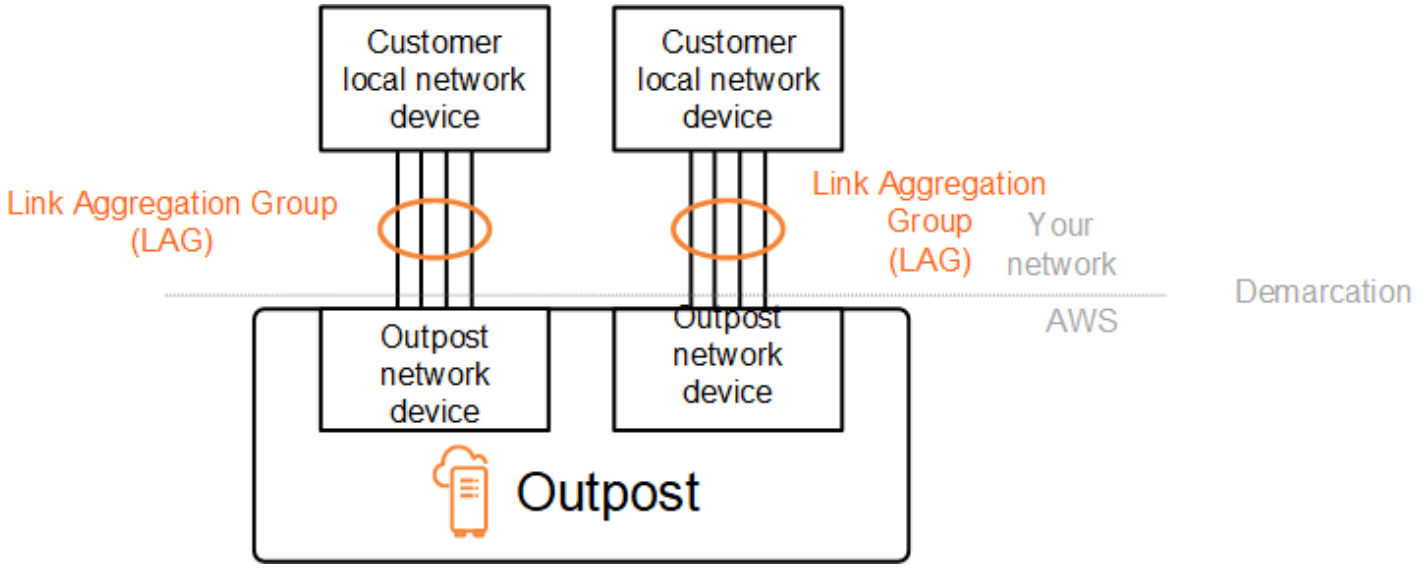
AWS Outposts 使用「連結彙總控制通訊協定」(LACP) 來建立兩個連結彙總群組 (LAG) 連線，每個 Outpost 網路裝置各一個連線到每個區域網路裝置。來自每部 Outpost 網路裝置的連結會彙總為乙太網路 LAG，以代表單一網路連線。這些 LAG 使用 LACP 搭配標準快速計時器。您無法將 LAG 設定為使用慢速計時器。

若要在站點安裝 Outpost，您必須在網路裝置上設定 LAG 連線端。

從邏輯的角度來看，請略過以 Outpost 配線面板作為分界點，並使用 Outpost 網路裝置。

對於具有多個機架的部署，Outpost 網路裝置的彙總層與您的本機網路裝置之間必須有四個 LAG。

下圖顯示每個 Outpost 網路裝置與其連線的本機網路裝置之間的四個實體連線。我們使用乙太網路 LAG 來彙總連線 Outpost 網路裝置和客戶本機網路裝置的實體連結。



虛擬 LAN

Outpost 網路裝置與本機網路裝置之間的每個 LAG 都必須設定為 IEEE 802.1q 乙太網路主幹。這可讓您使用多個 VLAN 來隔離資料路徑之間的網路。

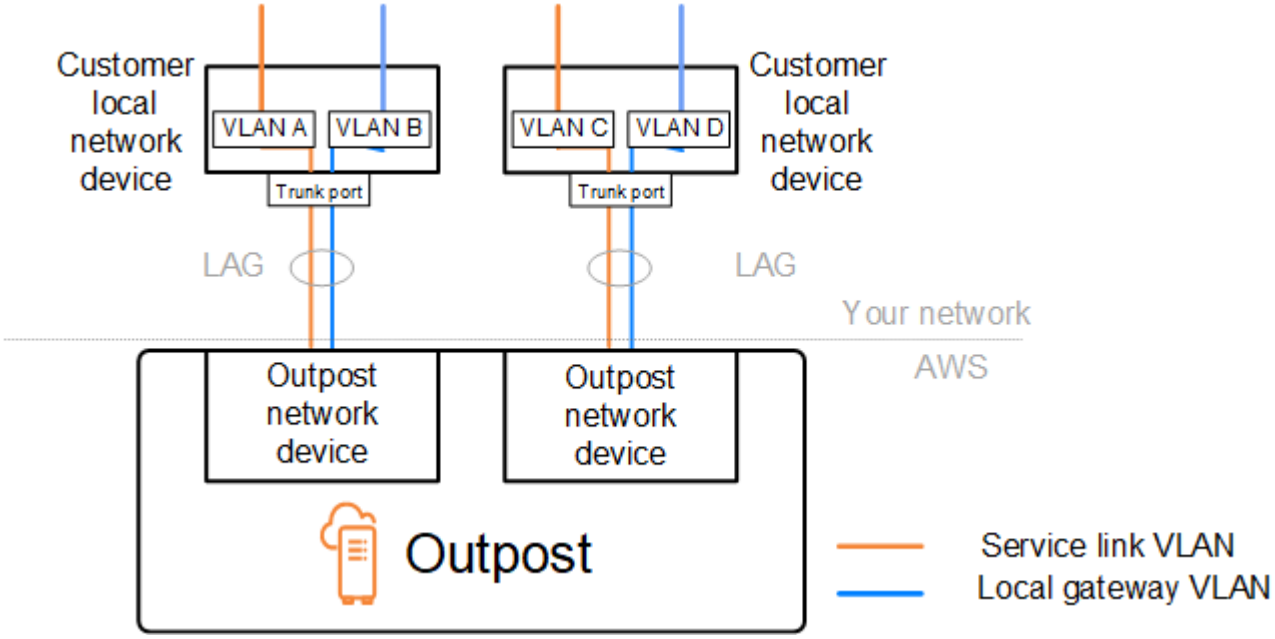
每個 Outpost 都有下列 VLAN，可與您的本機網路裝置通訊：

- 服務連結 VLAN – 可讓您在 Outpost 與本機網路裝置之間進行通訊，以便建立服務連結路徑進行服務連結連線。如需詳細資訊，請參閱《AWS 區域的AWS Outposts 連線》。
- 本機閘道 VLAN – 可讓您在 Outpost 與本機網路裝置之間進行通訊，以便建立本機閘道路徑來連線 Outpost 子網路和本機區域網路。Outpost 本機閘道利用此 VLAN 為您的執行個體提供內部部署網路連線，其中可能包括透過您的網路存取網際網路。如需詳細資訊，請參閱《本機閘道》。

您只能在 Outpost 與客戶本機網路裝置之間設定服務連結 VLAN 和本機閘道 VLAN。

Outpost 旨在將服務連結與本機閘道資料路徑分隔為兩個隔離的網路。這可讓您選擇哪些網路能夠與 Outpost 上執行的服務通訊。其也可讓您透過使用客戶本機網路裝置上的多個路由表 (通常稱為虛擬路

由和轉送執行個體 (VRF))，將服務連結設為與本機閘道網路隔離的網路。分界線存在於 Outpost 網路裝置的連接埠。 AWS 管理連線 AWS 側面的任何基礎架構，並且您可以管理生產線上的任何基礎架構。



若要在安裝和持續操作期間將 Outpost 與內部部署網路整合，您必須配置在 Outpost 網路裝置與客戶本機網路裝置之間使用的 VLAN。您必須在安裝 AWS 之前向其提供此資訊。如需詳細資訊，請參閱 the section called “網路整備檢查清單”。

網路層連線

為了建立網路層連線，每部 Outpost 網路裝置都設定了虛擬介面 (VIF)，其中包括每個 VLAN 的 IP 地址。透過這些 VIF， AWS Outposts 網路裝置就可以設定本機網路設備的 IP 連線和 BGP 工作階段。

我們建議下列作法：

- 使用具有 /30 或 /31 CIDR 的專用子網路來代表此邏輯連線。 point-to-point
- 請勿橋接本機網路裝置之間的 VLAN。

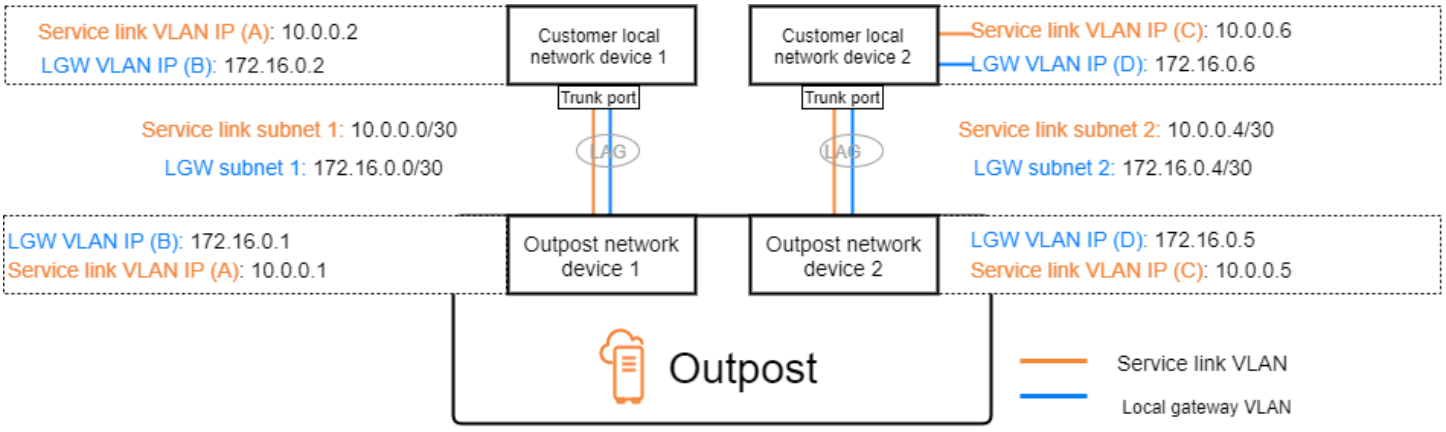
對於網路層連線，您必須建立兩個路徑：

- 服務連結路徑 - 若要建立此路徑，請為 AWS Outposts 網路裝置上的每個服務連結 VLAN 指定具有 /30 或 /31 範圍和一個 IP 地址的 VLAN 子網路。針對此路徑使用服務連結虛擬介面 (VIF)，在您的 Outpost 與本機網路裝置之間建立 IP 連線和 BGP 工作階段，以進行服務連結連線。如需詳細資訊，請參閱《AWS 區域的AWS Outposts 連線》。

- 本機閘道路徑 - 若要建立此路徑，請為 AWS Outposts 網路裝置上的本機閘道 VLAN 指定具有 /30 或 /31 範圍和一個 IP 地址的 VLAN 子網路。在此路徑上使用本機閘道 VIF，在您的 Outpost 與本機網路裝置之間建立 IP 連線和 BGP 工作階段，以進行本機資源連線。

下圖顯示從每部 Outpost 網路裝置到客戶本機網路裝置之連線的服務連結路徑和本機閘道路徑。此範例包含四個 VLAN：

- VLAN A 是連線 Outpost 網路裝置 1 與客戶本機網路裝置 1 的服務連結路徑。
- VLAN B 是連線 Outpost 網路裝置 1 與客戶本機網路裝置 1 的本機閘道路徑。
- VLAN C 是連線 Outpost 網路裝置 2 與客戶本機網路裝置 2 的服務連結路徑。
- VLAN D 是連線 Outpost 網路裝置 2 與客戶本機網路裝置 2 的本機閘道路徑。



下表顯示連線 Outpost 網路裝置 1 與客戶本機網路裝置 1 的子網路值範例。

VLAN	子網路	客戶裝置 1 IP	AWS 上 1 IP 地址
A	10.0.0.0/30	10.0.0.2	10.0.0.1
B	172.16.0.0/30	172.16.0.2	172.16.0.1

下表顯示連線 Outpost 網路裝置 2 與客戶本機網路裝置 2 的子網路值範例。

VLAN	子網路	客戶裝置 2 IP	AWS 上 2 IP 地址
C	10.0.0.4/30	10.0.0.6	10.0.0.5

VLAN	子網路	客戶裝置 2 IP	AWS 上 2 IP 地址
D	172.16.0.4/30	172.16.0.6	172.16.0.5

ACE 機架連線能力

> **Note**
>
> 如果您不需要 ACE 機架，請略過本節。

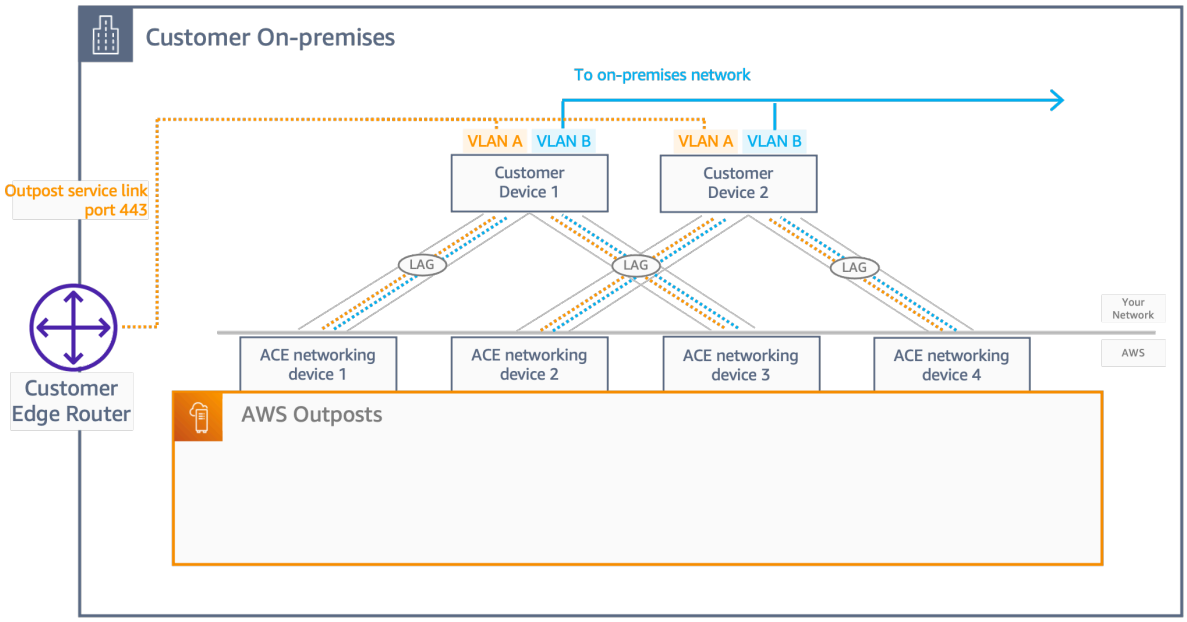
聚合、核心、邊緣 (ACE) 機架可作為多機架 Outpost 部署的網路聚合點。如果您有五個以上的運算機架，則必須使用 ACE 機架。如果您的運算機架少於五個，但計劃 future 擴充至五個以上的機架，我們建議您最早安裝 ACE 機架。

使用 ACE 機架時，Outposts 網路裝置不再直接連接到您的內部部署網路裝置。相反地，它們會連接至 ACE 機架，提供前哨機架的連線能力。在此拓撲中， AWS 擁有 Outposts 網路裝置與 ACE 網路裝置之間的 VLAN 介面配置和組態。

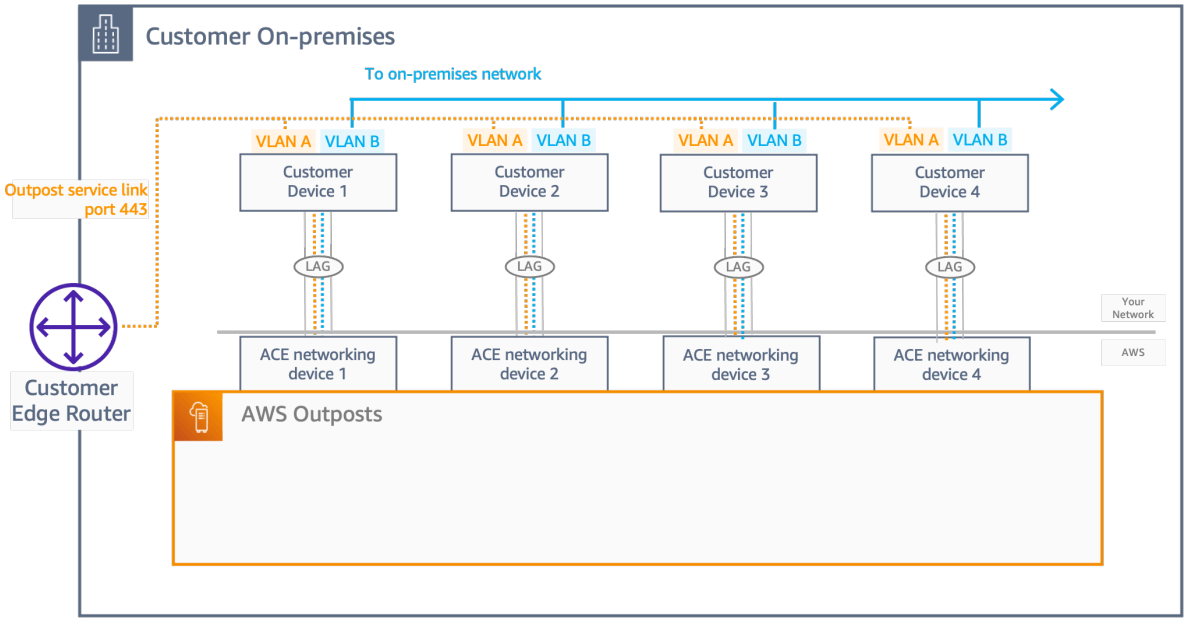
ACE 機架包含四個網路裝置，可連接至客戶內部部署網路中的兩個上游客戶裝置，或四個上游客戶裝置，以獲得最大的復原能力。

下列影像顯示兩個網路拓撲。

下圖顯示連接到兩個上游客戶裝置的 ACE 機架的四個 ACE 網路裝置：



下圖顯示連接至四個上游客戶裝置的 ACE 機架上的四個 ACE 網路裝置：

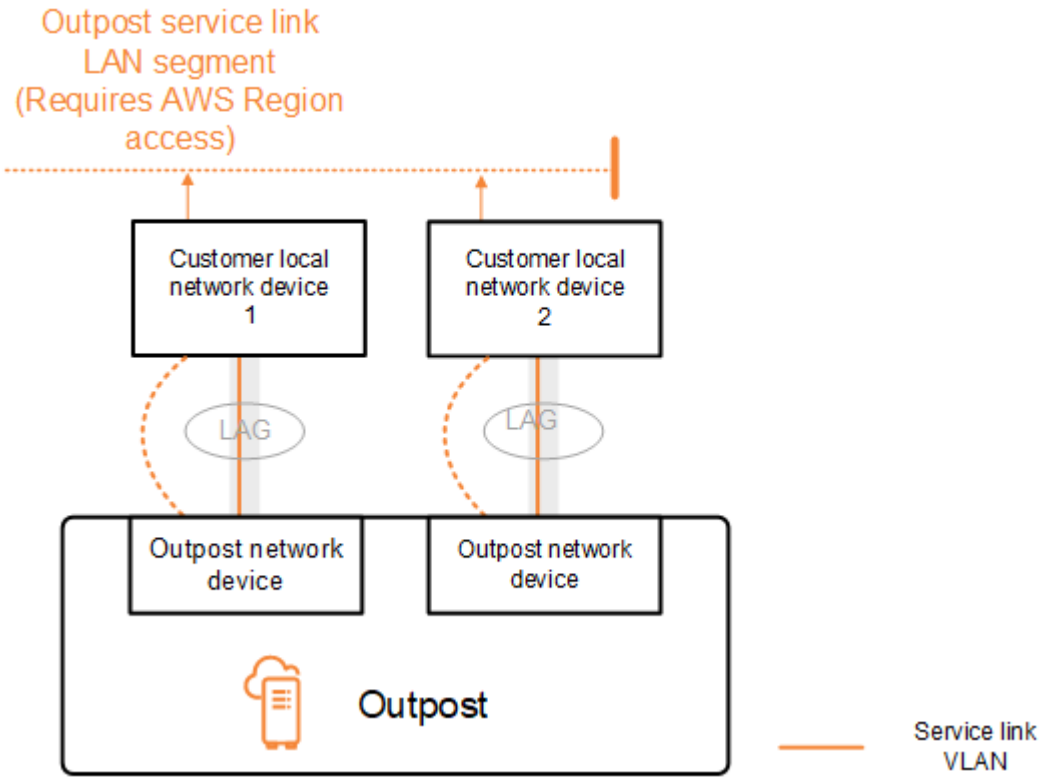


服務連結 BGP 連線

Outpost 會在每部 Outpost 網路裝置與客戶本機網路裝置之間建立外部 BGP 對等互連工作階段，以透過服務連結 VLAN 進行服務連結連線。BGP 對等工作階段會在為 VLAN 提供的 /30 或 /31 IP 位址之間建立。 point-to-point 每個 BGP 對等互連工作階段都會使用 Outpost 網路裝置上的私用自治系統編號 (ASN)，以及您為客戶本機網路裝置選擇的 ASN。 AWS 會在安裝過程中提供這些屬性。

考量以下情境：您有一個 Outpost，其中兩部 Outpost 網路裝置透過服務連結 VLAN 連線到兩部客戶本機網路裝置。您可以為每個服務連結設定下列基礎設施及客戶本機網路裝置 BGP ASN 屬性：

- 服務連結 BGP ASN。2 個位元組 (16 位元) 或 4 個位元組 (32 位元)。有效值為 64512-65535 或 4200000000-4294967294。
- 基礎設施 CIDR。這必須是每個機架一個 /26 CIDR。
- 客戶本機網路裝置 1 服務連結 BGP 對等 IP 地址。
- 客戶本機網路裝置 1 服務連結 BGP 對等 ASN。有效值為 1-4294967294。
- 客戶本機網路裝置 2 服務連結 BGP 對等 IP 地址。
- 客戶本機網路裝置 2 服務連結 BGP 對等 ASN。有效值為 1-4294967294。如需詳細資訊，請參閱《RFC4893》。



Outpost 使用下列程序透過服務連結 VLAN 建立外部 BGP 對等互連工作階段：

1. 每部 Outpost 網路裝置都會使用 ASN 與其所連線的本機網路裝置建立 BGP 對等互連工作階段。
2. Outpost 網路裝置將 /26 CIDR 範圍公告為兩個 /27 CIDR 範圍，以支援連結和裝置故障。每個 OND 都會公告自己的 /27 字首 (其 AS-Path 長度為 1)，加上所有其他 OND 的 /27 字首 (其 AS-Path 長度為 4) 作為備份。

3. 子網路用於從前哨到 AWS 區域的連線。

建議您將客戶網路設備設定為接收來自 Outpost 的 BGP 公告，而不變更 BGP 屬性。客戶網路應優先使用 Outpost 中 AS-Path 長度為 1 的路由，而不是 AS-Path 長度為 4 的路由。

客戶網路應向所有 OND 公告具有相同屬性的等量 BGP 字首。Outpost 網路負載預設會平衡所有上行鏈路之間的傳出流量。Outpost 端使用了路由政策，可在需要維護時從 OND 轉移流量。此流量轉移需要所有 OND 上的客戶端都有等量 BGP 字首。如果客戶網路需要維護，建議您在前面加上 AS-Path 以暫時從特定上行鏈路轉移流量。

服務連結基礎設施子網路公告和 IP 範圍

安裝之前，請為「服務連結基礎設施子網路」提供 /26 CIDR 範圍。Outpost 基礎設施使用此範圍，透過服務連結建立與區域的連線。服務連結子網路是起始連線的 Outpost 來源。

Outpost 網路裝置將 /26 CIDR 範圍公告為兩個 /27 CIDR 區塊，以支援連結和裝置故障。

您必須為 Outpost 提供服務連結 BGP ASN 和基礎設施子網路 CIDR (/26)。對於每部 Outpost 網路裝置，提供本機網路裝置 VLAN 上的 BGP 對等互連 IP 地址，以及本機網路裝置的 BGP ASN。

如果您有多個機架部署，則每個機架必須有一個 /26 子網路。

本機閘道 BGP 連線

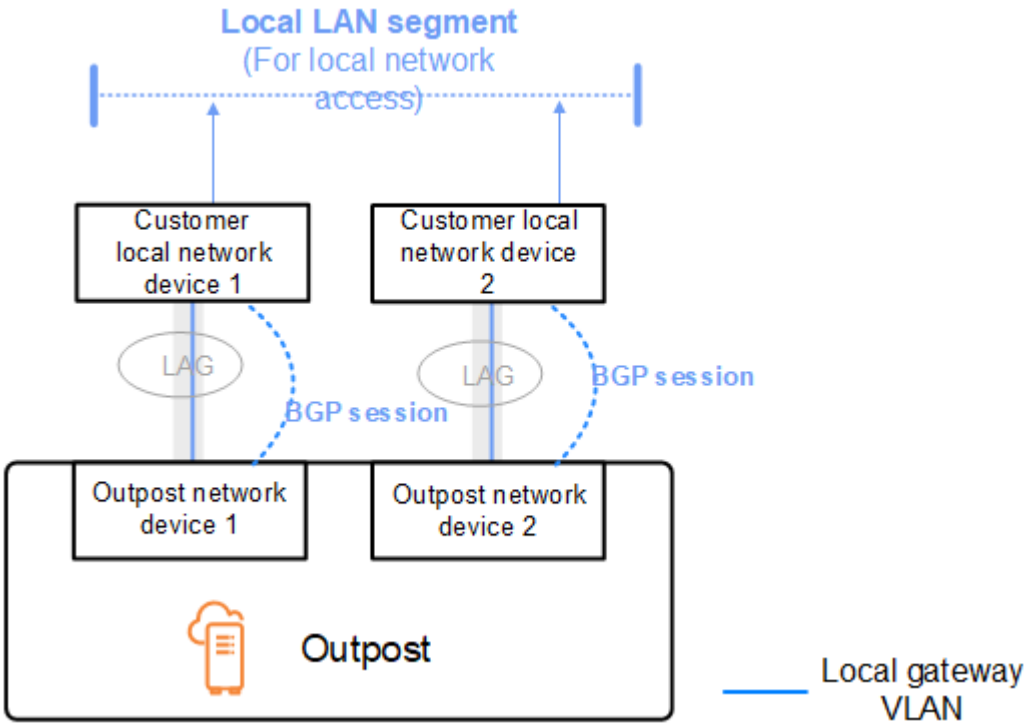
Outpost 會建立從每部 Outpost 網路裝置到本機網路裝置的外部 BGP 對等互連，以連線到本機閘道。其使用您指派的私有自治系統編號 (ASN)，以便建立外部 BGP 工作階段。每部 Outpost 網路裝置都有單一外部 BGP 對等互連，使用其本機閘道 VLAN 連至一部本機網路裝置。

Outpost 會在每部 Outpost 網路裝置與其連線的客戶本機網路裝置之間，透過本機閘道 VLAN 建立外部 BGP 對等互連工作階段。當您設定網路連線，並使 point-to-point 用 Outpost 網路裝置與客戶區域網路裝置之間的連線時，會在 /30 或 /31 IP 之間建立對等工作階段。如需詳細資訊，請參閱 the section called “網路層連線”。

每個 BGP 工作階段都使用 Outpost 網路裝置端的私有 ASN，以及您在客戶區域網路裝置端選擇的 ASN。 AWS 提供屬性做為安裝前程序的一部分。

考量以下情境：您有一個 Outpost，其中兩部 Outpost 網路裝置透過服務連結 VLAN 連線到兩部客戶本機網路裝置。您可以為每個服務連結設定下列本機閘道及客戶本機網路裝置 BGP ASN 屬性：

- AWS 提供本機閘道 BGP ASN。2 位元組 (16 位元) 或 4 位元組 (32 位元)。有效值為 64512-65535 或 4200000000-4294967294。
- (選擇性) 提供客戶擁有的 CIDR 進行公告 (公有或私有且至少為 /26)。
- 提供客戶本機網路裝置 1 本機閘道 BGP 對等 IP 地址。
- 提供客戶本機網路裝置 1 本機閘道 BGP 對等 ASN。有效值為 1-4294967294。如需詳細資訊，請參閱《RFC4893》。
- 提供客戶本機網路裝置 2 本機閘道 BGP 對等 IP 地址。
- 提供客戶本機網路裝置 2 本機閘道 BGP 對等 ASN。有效值為 1-4294967294。如需詳細資訊，請參閱《RFC4893》。



建議您將客戶網路設備設定為接收來自 Outpost 的 BGP 公告，而不變更 BGP 屬性，並啟用 BGP 多路徑/負載平衡以獲得最佳傳入流量。在本機閘道字首前面加上 AS-Path，以在需要維護時從 OND 轉移流量。客戶網路應優先使用 Outpost 中 AS-Path 長度為 1 的路由，而不是 AS-Path 長度為 4 的路由。

客戶網路應向所有 OND 公告具有相同屬性的等量 BGP 字首。Outpost 網路負載預設會平衡所有上行鏈路之間的傳出流量。Outpost 端使用了路由政策，可在需要維護時從 OND 轉移流量。此流量轉移需要所有 OND 上的客戶端都有等量 BGP 字首。如果客戶網路需要維護，建議您在前面加上 AS-Path 以暫時從特定上行鏈路轉移流量。

本機閘道客戶擁有的 IP 子網路公告

根據預設，本機閘道會使用 VPC 中執行個體的私有 IP 地址與您的內部部署網路進行通訊。不過，您可以提供客戶擁有的 IP 地址集區 (CoIP)。

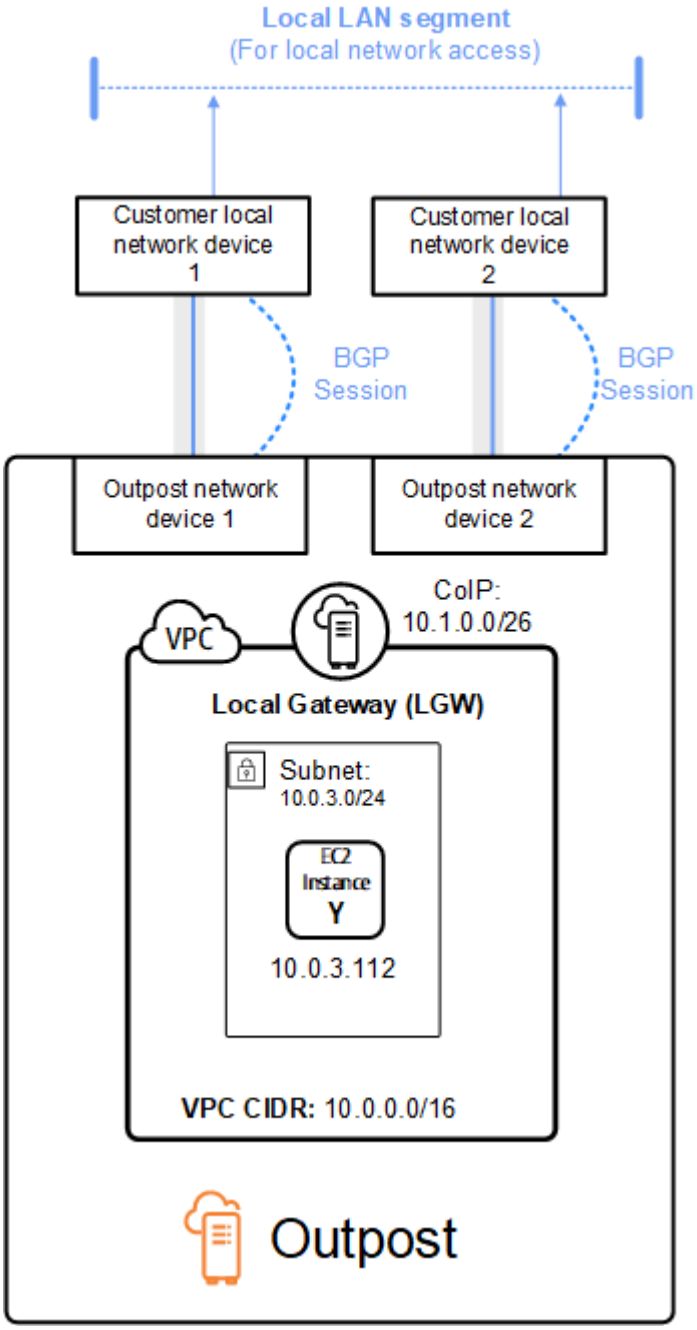
如果您選擇 CoIP，則 AWS 會根據您在安裝程序期間提供的資訊建立集區。您可以從此集區建立彈性 IP 地址，然後將地址指派給 Outpost 上的資源 (例如 EC2 執行個體)。

本機閘道會將彈性 IP 地址轉譯為客戶擁有集區中的地址。本機閘道會向您的內部部署網路，以及與 Outpost 通訊的任何其他網路，公告轉譯後的地址。這些地址會在兩個本機閘道 BGP 工作階段上向本機網路裝置公告。

> **Tip**
>
> 如果您不使用 CoIP，則 BGP 會公告 Outpost 上具有路由表中以本機閘道為目標之路由的子網路私有 IP 地址。

考量以下情境：您有一個 Outpost，其中兩部 Outpost 網路裝置透過服務連結 VLAN 連線到兩部客戶本機網路裝置。設定了下列項目：

- 具有 CIDR 區塊 10.0.0.0/16 的 VPC。
- VPC 中具有 CIDR 區塊 10.0.3.0/24 的子網路。
- 子網路中具有私有 IP 地址 10.0.3.112 的 EC2 執行個體。
- 客戶擁有的 IP 集區 (10.1.0.0/26)。
- 將 10.0.3.112 關聯到 10.1.0.2 的彈性 IP 地址關聯。
- 使用 BGP 透過本機裝置向內部部署網路公告 10.1.0.0/26 的本機閘道。
- Outpost 與內部部署網路之間的通訊將使用 CoIP 彈性 IP 來定址 Outpost 中的執行個體，而不是使用 VPC CIDR 範圍。


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

使用共用AWS Outposts資源

透過前哨共用，Outpost 擁有者可以與同一組織下的其他帳戶共用其 AWS Outposts 和 Outpost 資源，包括前哨網站和子網路。AWS身為 Outpost 擁有者，您可以集中建立和管理 Outpost 資源，並在組織內的多個AWS帳戶共用資源。AWS這可讓其他消費者使用 Outpost 網站、設定 VPC，以及在共用 Outpost 上啟動和執行執行個體。

在此模型中，擁有 Outpost 資源 (擁有者) 的帳AWS戶會與同一組織中的其他AWS帳戶 (用戶) 共用資源。消費者可以在 Outposts 上創建資源，這些資源與他們共享的方式與他們在 Outposts 上創建資源的方式相同，他們在自己的帳戶中創建。所有者負責管理前哨和他們在其中創建的資源。擁有者可以隨時變更或撤銷共享的存取權。除了消耗容量保留的執行個體外，擁有者還可以檢視、修改和刪除取用者在共用 Outposts 上建立的資源。擁有者在他們共用的 容量預留中無法修改消費者啟動的執行個體。

消費者負責管理他們在與其共用的 Outposts 上建立的資源，包括消耗容量保留的任何資源。消費者無法檢視或修改其他消費者或 Outpost 擁有者所擁有的資源。他們也無法修改與他們共享的 Outposts。

前哨所有者可以與以下方式共享前哨資源：

- 在其組織內部的特定AWS帳戶AWS Organizations。
- 其組織內部的組織單位AWS Organizations。
- 它的整個組織在AWS Organizations.

目錄

可共用的前哨資源

Outpost 擁有者可以與消費者共用本節中列出的 Outpost 資源。

這些是前哨機架器可用的資源。 如需伺服器資源，請參閱 Outposts 伺服器AWS Outposts使用指南中的使用共用AWS Outposts資源。

- 配置的專用主機 — 具有此資源存取權的用戶可以：
  - 在專用主機上啟動和執行 EC2 執行個體。
- 容量保留 — 具有此資源存取權的消費者可以：
  - 識別與其共用的容量保留。
  - 啟動和管理消耗容量保留的執行個體。
- 客戶擁有的 IP 位址 (CoIP) 集區 — 擁有此資源存取權的取用者可以：
  - 配置客戶擁有的 IP 位址並將其關聯至執行個體。
- 本機閘道路由表 — 具有此資源存取權的用戶可以：
  - 建立和管理與本機閘道的 VPC 關聯。
  - 檢視本機閘道路由表和虛擬介面的組態。
- Outposts — 具有此資源存取權的消費者可以：
  - 在前哨上創建和管理子網。
  - 在前哨上建立和管理 EBS 磁碟區。
  - 使用 AWS Outposts API 查看有關前哨的信息。
- Outposts 上的 S3 — 可以存取此資源的消費者可以：
  - 在 Outpost 上建立和管理 S3 儲存貯體、存取點和端點。
- 網站 — 具有此資源存取權的消費者可以：
  - 創建，管理和控制站點的前哨。
- 子網路 — 具有此資源存取權的取用者可以：
  - 檢視有關子網路的資訊。
  - 在子網路中啟動並執行 EC2 執行個體。

  使用 Amazon VPC 主控台共用前哨子網路。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的共用子網路。

共用 Outposts 資源的先決條件

- 若要與中的組織或組織單位共用 Outpost 資源AWS Organizations，您必須啟用與AWS Organizations共用。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的透過 AWS Organizations 啟用共用。
- 若要共用 Outpost 資源，您必須在AWS帳戶中擁有該資源。您無法共用已與您共用的 Outpost 資源。
- 若要共用 Outpost 資源，您必須與組織內的帳號共用該資源。

相關服務

前哨資源共享與集成AWS Resource Access Manager（AWS RAM）。 AWS RAM是一項服務，可讓您與任何AWS帳戶或透過其他帳戶共用AWS資源AWS Organizations。您可以透過 AWS RAM 建立資源共享，以分享您擁有的資源。資源共享指定要分享的資源，以及共用它們的消費者。消費者可以是中的個人AWS帳戶、組織單位或整個組織AWS Organizations。

如需 AWS RAM 的詳細資訊，請參閱《AWS RAM 使用者指南》。

跨可用區域共用

為確保資源分配至區域中的所有可用區域，可用區域會獨立對應至各個帳戶的名稱。這可能導致帳戶之間的可用區域命名出現差異。例如，您 AWS 帳戶的可用區域 `us-east-1a` 與其他 AWS 帳戶的 `us-east-1a` 可能不在同一位置。

若要識別與帳戶相關的 Outpost 資源位置，您必須使用可用區域 ID (AZ ID)。AZ ID 是可用區域在所有 AWS 帳戶之間唯一且一致的識別符。例如，`use1-az1` 是 `us-east-1` 區域的 AZ ID，它在每一個 AWS 帳戶的位置都相同。

檢視您帳戶中可用區域的 AZ ID

1. 在 AWS RAMhttps://console.aws.amazon.com/ram 開啟 主控台。
2. 畫面右側的 Your AZ ID (您的 AZ ID) 面板中會顯示目前區域的 AZ ID。

> **Note**
>
> 本機閘道路由表與其 Outpost 位於相同的 AZ 中，因此您不需要為路由表指定 AZ ID。

共用前哨資源

當所有者與消費者共享前哨時，消費者可以在 Outpost 上創建資源，就像他們在自己的帳戶中創建的 Outposts 上創建資源相同。具有共用本機閘道路由表存取權的取用者可以建立和管理 VPC 關聯。如需詳細資訊，請參閱可共用的前哨資源。

若要共用 Outpost 資源，您必須將其新增至資源共用。資源共享是可讓您在 AWS 帳戶之間分享資源的一種 AWS RAM 資源。資源共享指定要分享的資源，以及共用它們的消費者。當您使用AWS Outposts主控台共用 Outpost 資源時，您可以將其新增至現有的資源共用。若要將 Outpost 資源新增至新的資源共用，您必須先使用AWS RAM主控台建立資源共用。

如果您是組織的一員，AWS Organizations並且已啟用組織內的共用功能，您可以將組織中的用戶從AWS RAM主控台授與共用 Outpost 資源的存取權。否則，取用者會收到加入資源共用的邀請，並在接受邀請後授予對共用 Outpost 資源的存取權。

您可以使用AWS Outposts主控台、AWS RAM主控台或共用您擁有的 Outpost 資源。AWS CLI

使用主控台分享您擁有的AWS Outposts前哨

1. 於 AWS Outpostshttps://console.aws.amazon.com/outposts/ 開啟 主控台。
2. 在導覽窗格中，選擇「Outposts」。
3. 選取「前哨」，然後選擇「作業」，「檢視明細」。
4. 在「前哨」摘要頁面上，選擇「資源共用」。
5. 選擇 Create resource share (建立資源共用)。

系統會使用下列程序將您重新導向至AWS RAM主控台，以完成 Outpost 的共用程序。若要共用您擁有的本機閘道路由表，請同時使用下列程序。

共用您使用主控台擁有的 Outpost 或本機閘道路由表 AWS RAM

請參閱《AWS RAM 使用者指南》中的建立資源共享。

若要共用您使用 AWS CLI

使用 create-resource-share 命令。

取消共用的前哨資源

取消共用的 Outpost 時，取用者無法再在主控台中檢視 Outpost。AWS Outposts他們無法在 Outpost 上建立新的子網路、在 Outpost 上建立新的 EBS 磁碟區，或使用主控台或檢視 Outpost 詳細資料和執行個體類型。AWS Outposts AWS CLI不會刪除取用者建立的現有子網路、磁碟區或執行個體。在 Outpost 上建立的任何現有子網路用戶仍然可以用來啟動新的執行個體。

取消共用本機閘道路由表時，取用者無法再建立新的 VPC 關聯。建立的任何現有 VPC 關聯用戶都會與路由表保持關聯。這些 VPC 中的資源可以繼續將流量路由到本機閘道。

若要取消共用您擁有的共用 Outpost 資源，您必須將其從資源共用中移除。您可以使用 AWS RAM 主控台或 AWS CLI 執行這項作業。

若要取消共用您使用主控台擁有的共用 Outpost 資源 AWS RAM

請參閱《AWS RAM 使用者指南》中的更新資源共享。

若要取消共用您擁有的共用 Outpost 資源，請使用 AWS CLI

使用 disassociate-resource-share 命令。

識別共用的前哨資源

所有者和消費者可以使用AWS Outposts控制台和AWS CLI識別共享的 Outposts。他們可以使用識別共用本機閘道路由表AWS CLI。

使用主控台識別共用的AWS Outposts前哨

1. 於 AWS Outpostshttps://console.aws.amazon.com/outposts/ 開啟 主控台。
2. 在導覽窗格中，選擇「Outposts」。
3. 選取「前哨」，然後選擇「作業」，「檢視明細」。
4. 在前哨摘要頁面上，檢視擁有者 ID 以識別前哨擁有者的AWS帳戶 ID。

若要使用識別共用的前哨資源 AWS CLI

使用列表前哨和 describe-local-gateway-route-表命令。這些命令會傳回您擁有的 Outpost 資源，以及與您共用的 Outpost 資源。 `OwnerId`顯示前哨資源擁有者的AWS帳號 ID。

共用的前哨資源權限

擁有者的許可

所有者負責管理前哨和他們在其中創建的資源。擁有者可以隨時變更或撤銷共享的存取權。他們可以用AWS Organizations來檢視、修改和刪除取用者在共用 Outposts 上建立的資源。

消費者的許可

消費者可以在 Outposts 上創建資源，這些資源與他們共享的方式與他們在 Outposts 上創建資源的方式相同，他們在自己的帳戶中創建。消費者負責管理他們在 Outposts 上啟動的資源，這些資源與他們共享。消費者無法查看或修改其他消費者或 Outpost 所有者擁有的資源，也無法修改與他們共享的 Outposts。

計費和計量

擁有者需支付他們共用的 Outposts 和前哨資源的費用。他們還需支付與來自該AWS地區的 Outpost 服務鏈接 VPN 流量相關的任何數據傳輸費用。

共用本機閘道路由表不會產生額外費用。對於共用子網路，VPC 擁有者需支付虛擬私人雲端層級資源 (例如 VPN 連線、NAT 閘道AWS Direct Connect和私人連結連線) 的費用。

消費者需支付在共用 Outposts 上建立的應用程式資源 (例如負載平衡器和 Amazon RDS 資料庫) 的費用。消費者也需要支付從該AWS地區傳輸的可收費資料費用。

限制

下列限制適用於使用AWS Outposts共用：

- 共用子網路的限制適用於使用AWS Outposts共用。如需 VPC 共用限制的詳細資訊，請參閱 Amazon Virtual Private Cloud 使用者指南中的限制。
- Service Quotas 適用於個別帳戶。

中的安全性 AWS Outposts

安全性 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 — AWS 負責保護在 AWS 雲端中執行 AWS 服務的基礎架構。 AWS 還為您提供可以安全使用的服務。若要深入瞭解適用於的規範遵循計劃 AWS Outposts，請參閱合規計劃的AWS 服務範圍範圍)。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

如需有關安全性與合規性的詳細資訊 AWS Outposts，請參閱AWS Outposts 機架常見問答集AWS Outposts

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Outposts。其中說明如何達成您的安全與合規目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護您的資源。

目錄

資料保護 AWS Outposts

AWS 共用責任模型適用於中的資料保護 AWS Outposts。如此模型中所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。此內容包括您使用的安全性組態和管理工作。 AWS 服務

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。

如需有關資料隱私權的更多相關資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

靜態加密

使用時 AWS Outposts，所有資料都會在靜態時加密。金鑰材料會包裝到外部金鑰，儲存在抽取式裝置中，也就是 Nitro 安全金鑰 (NSK)。需要 NSK 才能解密 Outpost 機架上的資料。

您可以對 EBS 磁碟區和快照使用 Amazon EBS 加密。Amazon EBS 加密使用 AWS Key Management Service (AWS KMS) 和 KMS 金鑰。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 Amazon EBS 加密。

傳輸中加密

AWS 加密您的前哨站和其區域之間的傳輸中資料。 AWS 如需詳細資訊，請參閱 透過服務連結進行連線。

您可以使用 Transport Layer Security (TLS) 等加密通訊協定，對透過本機閘道傳輸到您本機區域網路的敏感資料進行加密。

資料刪除

當您停止或終止 EC2 執行個體時，Hypervisor 會先清除配置到該執行個體的記憶體 (設定為零)，再將其配置到新的執行個體，而且會重設儲存體的每個區塊。

銷毀 Nitro 安全金鑰會以密碼編譯方式銷毀 Outpost 上的資料。

以下項目的身分識別與存取管理 (IAM) AWS Outposts

AWS Identity and Access Management (IAM) 是協助管理員安全地控制 AWS 資源存取的 AWS 服務。IAM 管理員控制哪些人可以通過身份驗證 (登入) 和授權 (具有權限) 來使用 AWS Outposts 資源。您可以免費使用 IAM。

目錄

- AWS 受管理的政策 AWS Outposts

AWS Outposts 如何與 IAM 搭配使用

在您使用 IAM 管理前 AWS 哨的存取權限之前，請先了解哪些 IAM 功能可用於 AWS Outposts。

您可以搭配 AWS Outposts 使用的 IAM 功能

IAM 功能	AWS Outposts 支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	是

前哨基於身份的政策 AWS

支援身分型政策	是

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

Outposts 哨基於身份的政策示例 AWS

若要檢視 AWS Outposts 身分型原則的範例，請參閱。AWS Outposts 政策示例

Outposts 基於資源的政策 AWS

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

若要啟用跨帳戶存取，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 角色與資源型政策有何差異。

AWS Outposts 的政策行動

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 AWS Outposts 動作清單，請參閱服務授權參考 AWS Outposts中定義的動作。

AWS Outposts 中的策略動作在動作之前使用以下前綴：

```
outposts
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

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

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 `List` 文字的所有動作，請包含以下動作：

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

AWS Outposts 的政策資源

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

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

一些 AWS Outposts API 操作支持多種資源。若要在單一陳述式中指定多項資源，請使用逗號分隔 ARN。

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

```
]
```

若要查看 AWS Outposts 資源類型及其 ARN 的清單，請參閱服務授權參考 AWS Outposts中所定義的資源類型。若要了解您可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Outposts定義的動作。

AWS Outposts 的政策條件鍵

支援服務特定政策條件金鑰	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 AWS Outposts 條件金鑰清單，請參閱服務授權參考 AWS Outposts中的條件金鑰。若要瞭解您可以使用條件索引鍵的動作和資源，請參閱定義的動作 AWS Outposts。

若要檢視 AWS Outposts 身分型原則的範例，請參閱。AWS Outposts 政策示例

Outposts 中的 AWS ACL

支援 ACL	否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

與 AWS Outposts 的 ABAC

支援 ABAC (政策中的標籤)	是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

使用 AWS Outposts 的臨時憑據

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

Outposts 的 AWS 跨服務主體權限

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

AWS Outpost 的服務角色

支援服務角色	否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

Outposts 的 AWS 服務連結角色

支援服務連結角色	是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需有關建立或管理 AWS Outposts 服務連結角色的詳細資訊，請參閱。使用 AWS Outposts的服務連結角色

AWS Outposts 政策示例

默認情況下，用戶和角色沒有創建或修改 AWS Outposts 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

有關 AWS Outposts 定義的動作和資源類型的詳細資訊，包括每個資源類型的 ARN 格式，請參閱服務授權參考 AWS Outposts中的動作、資源和條件索引鍵。

目錄

- 範例：使用資源層級許可

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以在您的帳戶中建立、存取或刪除 AWS Outposts 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

範例：使用資源層級許可

下列範例使用資源層級許可來授予許可，以便取得指定 Outpost 的相關資訊。

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

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

下列範例使用資源層級許可來授予許可，以便取得指定站點的相關資訊。

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

使用 AWS Outposts的服務連結角色

AWS Outposts 使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結到 AWS Outposts的唯一 IAM 角色類型。服務連結角色由預先定義， AWS Outposts 並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您 AWS Outposts 更有效率地設定，因為您不需要手動新增必要的權限。 AWS Outposts 定義其服務連結角色的權限，除非另有定義，否則只 AWS Outposts 能擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除相關的資源，才能刪除服務連結角色。這樣可以保護您的 AWS Outposts 資源，因為您無法不小心移除存取資源的權限。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (是) 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

AWS Outposts的服務連結角色許可

AWS Outposts 使用名為 AWSServiceRoleForOutposts_ ***OutPostId*** 的服務連結角色 — 允許 Outposts 代表您存取 AWS 資源以進行私人連線。此服務連結角色會允許私有連線組態、建立網路介面，並將其連接至服務連結端點執行個體。

AWSServiceRoleForOutposts_ *OutposId* 服務連結角色會信任下列服務擔任該角色：

- outposts.amazonaws.com

AWSServiceRoleForOutposts_ 輸***# ID*** 服務連結角色包含下列原則：

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_ ***##***

此AWSOutpostsServiceRolePolicy原則是一項服務連結角色原則，可讓您存取由 AWS Outposts管理的 AWS 資源。

此原則允許 AWS Outposts 對指定的資源完成下列動作：

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

AWSOutpostsPrivateConnectivityPolicy_ ***OutPostId*** 策略允許 AWS Outposts 對指定的資源完成以下操作：

- 動作：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" }}
```

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

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

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

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

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

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

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱《IAM 使用者指南》中的服務連結角色許可。

為 AWS Outposts建立服務連結角色

您不需要手動建立一個服務連結角色。當您在中設定 Outpost 的私人連線時 AWS Management Console，會為您 AWS Outposts 建立服務連結角色。

如需詳細資訊，請參閱 使用 VPC 進行服務連結私有連線。

為 AWS Outposts編輯服務連結角色

AWS Outposts 不允許您編輯 AWSServiceRoleForOutposts _ *## ID* 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

為 AWS Outposts刪除服務連結角色

如果您不再需要使用服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，就不會有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

> **Note**
>
> 當您嘗試刪除資源時，如果 AWS Outposts 服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘後並再次嘗試操作。

> **Warning**
>
> 您必須先刪除前哨，才能刪除 AWSServiceRoleForOutposts _ *OutPostId* 服務連結角色。下列程序會刪除您的 Outpost。

在開始之前，請確保您的前哨沒有使用 AWS Resource Access Manager （ AWS RAM ）共享。如需詳細資訊，請參閱 取消共用的前哨資源。

若要刪除 AWSServiceRoleForOutposts _ ## ID 所使用的 AWS Outposts 資源

- 請聯絡 AWS 企業 Support 以刪除您的前哨。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除 AWSServiceRoleForOutposts _ #########。 AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

AWS Outposts 服務連結角色的支援區域

AWS Outposts 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS Outposts 端點和配額。

AWS 受管理的政策 AWS Outposts

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理策略： AWSOutpostsServiceRolePolicy

此原則附加至服務連結角色，可 AWS Outposts 代表您執行動作。如需詳細資訊，請參閱 使用服務連結角色。

AWS 受管理策略： AWSOutpostsPrivateConnectivityPolicy

此原則附加至服務連結角色，可 AWS Outposts 代表您執行動作。如需詳細資訊，請參閱 使用服務連結角色。

AWS OutpostsAWS 受管理策略的更新

檢視 AWS Outposts 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。

變更	描述	日期
AWS Outposts 開始追蹤變更	AWS Outposts 開始追蹤其 AWS 受管理策略的變更。	2019 年 12 月 3 日

基礎結構安全 AWS Outposts

作為託管服務， AWS Outposts 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎結構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發布的 API 調用通過網絡訪問 AWS Outposts。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

如需為 Outpost 上所執行 EC2 執行個體和 EBS 磁碟區提供之基礎設施安全的詳細資訊，請參閱《Amazon EC2 中的基礎設施安全》。

VPC 流程記錄的功能與在 AWS 區域中的運作方式相同。這意味著它們可以發佈到 CloudWatch 日誌、Amazon S3 或 Amazon 進 GuardDuty 行分析。數據需要被發送回地區以發布到這些服務，因此當前哨處於斷開連接狀態時，從 CloudWatch 或其他服務中看不到數據。

設 AWS Outposts 備上的竄改監控

確保沒有人修改，改變，逆向工程師或篡改設備。 AWS Outposts AWS Outposts 設備可能會配備篡改監測，以確保遵守AWS 服務條款。

韌性在 AWS Outposts

AWS Outposts 被設計為具有高可用性。Outpost 機架經過設計，具有備援電源和網路設備。為了提高恢復能力，建議您為 Outpost 提供雙電源和備援網路連線。

為了獲得高可用性，您可以在 Outpost 機架上佈建額外的內建且永遠處於作用中的容量。Outpost 容量組態是專為在生產環境中運作所設計，當您佈建容量時，可支援每個執行個體系列 N+1 個執行個體。AWS 建議您為任務關鍵型應用程式配置足夠的額外容量，以便在發生基礎主機問題時進行復原和容錯移轉。您可以使用 Amazon CloudWatch 容量可用性指標並設定警示來監控應用程式的運作狀態、建立動 CloudWatch 作以設定自動復原選項，以及監控 Outposts 隨時間變化的容量使用率。

建立前哨時，您可以從區域選取可用區 AWS 域。此可用區域支援控制平面操作，例如回應 API 呼叫、監控 Outpost 及更新 Outpost。若要利用可用區域提供的恢復能力，您可以在多個 Outpost 上部署應用程式，並將每個應用程式連接至不同的可用區域。這可讓您提高應用程式恢復能力，避免依賴單一可用區域。如需區域與可用區域的詳細資訊，請參閱《AWS 全球基礎設施》。

您可以使用具有分散策略的放置群組，確保將執行個體放在不同的 Outpost 機架上。這樣做可協助減少相互關聯的故障。如需詳細資訊，請參閱 Outpost 中的放置群組。

您可以使用 Amazon EC2 Auto Scaling 在 Outpost 中啟動執行個體，並建立 Application Load Balancer 在執行個體之間分配流量。如需詳細資訊，請參閱《在 AWS Outposts上設定 Application Load Balancer》。

符合性驗證 AWS Outposts

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求，例如 PCI DSS，滿足特定合規性架構所規定的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

AWS Outposts 工作負載上網

本節說明 AWS Outposts 工作負載如何透過下列方式存取網際網路：

- 通過父 AWS 區域
- 透過您當地的資料中心網路

透過父 AWS 區域存取網際網路

在此選項中，Outposts 中的工作負載會透過服務連結存取網際網路，然後透過父 AWS 區域中的網際網路閘道 (IGW) 存取網際網路。網際網路的輸出流量可透過 VPC 中具現化的 NAT 閘道。為了提高入

口和出口流量的安全性，您可以使用區 CloudFront 域中的 AWS 安全服務 AWS WAF AWS Shield，例如、和 Amazon。 AWS

如需 Outposts 子網路上的路由表設定，請參閱本機閘道路由表。

考量事項

- 在以下情況使用此選項：
  - 您需要靈活地使用該 AWS 地區的多種 AWS 服務來保護互聯網流量。
  - 您的資料中心或主機代管設施中沒有網際網路連線點。
- 在此選項中，流量必須遍歷父 AWS 區域，這會導致延遲。
- 與區 AWS 域中的資料傳輸費用類似，從上層可用區域傳出至 Outpost 的資料會產生費用。若要進一步了解資料傳輸，請參閱 Amazon EC2 隨需定價。
- 服務連結頻寬的使用率會增加。

下圖顯示 Outposts 執行個體中的工作負載與經過父 AWS 區域的網際網路之間的流量。

透過您當地資料中心的網路存取網際網路

在此選項中，駐留在 Outposts 的工作負載會透過本機資料中心存取網際網路。存取網際網路的工作負載流量會遍歷您本機的網際網路連線點，並在本機輸出。本機資料中心網路的安全層負責保護 Outposts 工作負載流量的安全性。

如需 Outposts 子網路上的路由表設定，請參閱本機閘道路由表。

考量事項

- 在以下情況使用此選項：
  - 您的工作負載需要低延遲存取網際網路服務。
  - 您希望避免產生資料傳出 (DTO) 費用。
  - 您想要保留控制平面流量的服務連結頻寬。
- 您的安全層負責保護 Outposts 工作負載流量的安全。
- 如果您選擇直接 VPC 路由 (DVR)，則必須確保 Outposts CIDR 不會與內部部署 CIDR 衝突。
- 如果預設路由 (0/0) 是透過本機閘道 (LGW) 傳播的，則執行個體可能無法進入服務端點。或者，您可以選擇 VPC 端點以連接所需的服務。

下圖顯示 Outposts 執行個體中的工作負載與通過本機資料中心的網際網路之間的流量。

監控 Outpost

AWS Outposts 與以下提供監控和記錄功能的服務整合：

CloudWatch 度量

使用 Amazon CloudWatch 來擷取有關 Outposts 資料點的統計資料，做為一組排序的時間序列資料 (稱為指標)。您可以使用這些指標來確認您的系統是否依照預期執行。如需詳細資訊，請參閱 CloudWatch 度量 AWS Outposts。

CloudTrail 日誌

使用 AWS CloudTrail 來擷取有關對 AWS API 進行之呼叫的詳細資訊。您可以將這些呼叫儲存為 Amazon S3 中的日誌檔案。您可以使用這些 CloudTrail 記錄來判斷這類資訊，例如撥打哪個呼叫、來源 IP 位址、撥打電話的人員，以及撥打電話的時間。

記 CloudTrail 錄檔包含的 API 動作呼叫的相關資訊AWS Outposts。也包含來自 Outpost 服務 (例如 Amazon EC2 和 Amazon EBS) 的 API 動作呼叫資訊。如需詳細資訊，請參閱 AWS Outposts中的資訊 CloudTrail。

VPC 流量日誌

使用 VPC Flow Logs 來擷取有關進出 Outpost 以及 Outpost 內部之流量的詳細資訊。如需詳細資訊，請參閱 《Amazon VPC 使用者指南》中的 VPC 流量日誌。

流量鏡射

使用流量鏡像將網路流量從 Outpost 複製並轉送到 Outpost 中的 out-of-band安全性和監控應用裝置。您可以使用鏡像流量進行內容檢查、威脅監控或疑難排解。如需詳細資訊，請參閱 Amazon Virtual Private Cloud 的《流量鏡像指南》。

AWS Health Dashboard

AWS Health Dashboard 會顯示資訊，以及由於 AWS 資源運作狀態變更所發出的通知。該資訊以兩種方式呈現：儀表板 (依類別顯示最近和近期事件) 和完整的事件日誌 (顯示過去 90 天內的所有事件)。例如，服務連結連線問題所引發的事件會出現在儀表板和事件日誌中，並在事件日誌中保留 90 天。AWS Health Dashboard是 AWS Health 服務的一部分，不需要設定，而且您帳戶中經過驗證的任何使用者皆可檢視。如需詳細資訊，請參閱 AWS Health Dashboard 入門。

CloudWatch 度量 AWS Outposts

AWS Outposts將數據點發佈到 Amazon CloudWatch 為您的 Outposts。 CloudWatch 可讓您擷取有關這些資料點的統計資料，做為一組排序的時間序列資料 (稱為指標)。您可以將指標視為要監控的變數，且資料點是該變數在不同時間點的值。例如，您可以監控 Outpost 在指定期間內可用的執行個體容量。每個資料點都有相關聯的時間戳記和可選的測量單位。

您可以使用指標來確認系統的運作符合預期。例如，您可以建立 CloudWatch 警示來監視指ConnectedStatus標。如果平均度量小於1，則 CloudWatch 可以啟動動作，例如將通知傳送至電子郵件地址。然後，您可以調查可能會影響 Outpost 操作的潛在內部部署或上行鏈路網路問題。常見問題包括最近對防火牆和 NAT 規則的內部部署網路組態變更，或網際網路連線問題。對於 ConnectedStatus 問題，建議您確認從內部部署網路到 AWS 區域的連線；如果問題仍存在，請聯絡 AWS Support。

如需有關建立 CloudWatch 警示的詳細資訊，請參閱 Amazon 使用 CloudWatch 者指南中的使用 Amazon CloudWatch 警示。如需有關的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南。

目錄

Outpost 指標

AWS/Outposts 命名空間包含下列指標。

ConnectedStatus

Outpost 服務連結連線的狀態。如果平均統計值小於 1，則連線已受損。

單位：計數

最大解析度：1 分鐘

統計資訊：最實用的統計資訊是 Average。

尺寸: OutpostId

`CapacityExceptions`

執行個體啟動時的容量不足錯誤數目。

單位：計數

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 `Maximum` 與 `Minimum`。

維度：`InstanceType` 和 `OutpostId`

`IfTrafficIn`

Outpost 虛擬介面 (VIF) 從已連線本機網路裝置接收的資料位元速率。

單位：位元/秒

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 `Max` 與 `Min`。

本機閘道 VIF (lgw-vif) 的維度：`OutpostsId`、`VirtualInterfaceGroupId` 和 `VirtualInterfaceId`

服務連結 VIF (sl-vif) 的維度：`OutpostsId` 和 `VirtualInterfaceId`

`IfTrafficOut`

Outpost 虛擬介面 (VIF) 傳輸至已連線本機網路裝置的資料位元速率。

單位：位元/秒

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 `Max` 與 `Min`。

本機閘道 VIF (lgw-vif) 的維度：`OutpostsId`、`VirtualInterfaceGroupId` 和 `VirtualInterfaceId`

服務連結 VIF (sl-vif) 的維度：`OutpostsId` 和 `VirtualInterfaceId`

`InstanceFamilyCapacityAvailability`

可用的執行個體容量百分比。此指標不包含在 Outpost 上設定之任何專用執行個體的容量。

單位：百分比

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。

維度：InstanceFamily 和 OutpostId

InstanceFamilyCapacityUtilization

使用中的執行個體容量百分比。此指標不包含在 Outpost 上設定之任何專用執行個體的容量。

單位：百分比

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。

維度：Account、InstanceFamily 和 OutpostId

InstanceTypeCapacityAvailability

可用的執行個體容量百分比。此指標不包含在 Outpost 上設定之任何專用執行個體的容量。

單位：百分比

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。

維度：InstanceType 和 OutpostId

InstanceTypeCapacityUtilization

使用中的執行個體容量百分比。此指標不包含在 Outpost 上設定之任何專用執行個體的容量。

單位：百分比

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。

維度：Account、InstanceType 和 OutpostId

UsedInstanceType_Count

目前使用中的執行個體類型數量，包括 Amazon Relational Database Service (Amazon RDS) 或 Application Load Balancer 等受管服務使用的任何執行個體類型。此指標不包含在 Outpost 上設定之任何專用執行個體的容量。

單位：計數

最大解析度：5 分鐘

維度：Account、InstanceType 和 OutpostId

AvailableInstanceType_Count

可用的執行個體類型數量。此指標不包含在 Outpost 上設定之任何專用執行個體的容量。

單位：計數

最大解析度：5 分鐘

維度：InstanceType 和 OutpostId

AvailableReservedInstances

Outpost 上可用於隨需容量保留 (ODCR) 的執行個體數量。此指標不會測量 Amazon EC2 預留執行個體。

單位：計數

最大解析度：5 分鐘

維度：InstanceType 和 OutpostId

UsedReservedInstances

Outpost 上可用於隨需容量保留 (ODCR) 的執行個體數量。此指標不會測量 Amazon EC2 預留執行個體。

單位：計數

最大解析度：5 分鐘

維度：InstanceType 和 OutpostId

TotalReservedInstances

Outpost 上可用於隨需容量保留 (ODCR) 的執行個體數量。此指標不會測量 Amazon EC2 預留執行個體。

單位：計數

最大解析度：5 分鐘

維度：InstanceType 和 OutpostId

EBSVolumeTypeCapacityUtilization

使用中的 EBS 磁碟區類型容量百分比。

單位：百分比

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。

維度：VolumeType 和 OutpostId

EBSVolumeTypeCapacityAvailability

可用的 EBS 磁碟區類型容量百分比。

單位：百分比

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。

維度：VolumeType 和 OutpostId

EBSVolumeTypeCapacityUtilizationGB

EBS 磁碟區類型的使用中 GB 數。

單位：千兆位元組 (GB)

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。

維度：VolumeType 和 OutpostId

EBSVolumeTypeCapacityAvailabilityGB

EBS 磁碟區類型的可用容量 GB 數。

單位：千兆位元組 (GB)

最大解析度：5 分鐘

統計資訊：最實用的統計資訊是 `Average` 與 `pNN.NN` (百分位數)。

維度：`VolumeType` 和 `OutpostId`

Outpost 指標維度

若要篩選 Outpost 的指標，請使用下列維度。

維度	描述
`Account`	使用容量的帳戶或服務。
`InstanceFamily`	執行個體系列。
`InstanceType`	執行個體類型。
`OutpostId`	Outpost 的 ID。
`VolumeType`	EBS 磁碟區類型。
`VirtualInterfaceId`	本機閘道或服務連結虛擬介面 (VIF) 的 ID。
`VirtualInterfaceGroupId`	本機閘道虛擬介面 (VIF) 的虛擬介面群組 ID。

查看前哨站的 CloudWatch 指標

您可以使用 CloudWatch 主控台檢視負載平衡器的 CloudWatch 指標。

使用 CloudWatch 主控台檢視指標

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽窗格中，選擇 指標。
3. 選取 Outpost 命名空間。
4. (選擇性) 若要檢視所有維度的指標，請在搜尋方塊位中輸入其名稱。

若要使用 AWS CLI 來檢視指標

使用下列 list-metrics 命令列出可用指標。

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

使用 AWS CLI 取得指標的統計資料

使用下列get-metric-statistics命令取得指定之測量結果和維度的統計資料。 CloudWatch 將每個唯一維度組合視為單獨的量度。您無法使用未具體發佈的維度組合來擷取統計資料。您必須指定建立指標時所使用的相同維度。

```
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 的日誌 AWS Outposts API 呼叫

AWS Outposts與 (提供中的使用者AWS CloudTrail、角色或服務所採取的動作記錄) 的AWS服務整合 AWS Outposts。 CloudTrail 擷取AWS Outposts作為事件的所有 API 呼叫。擷取的呼叫包括從 AWS Outposts 主控台進行的呼叫，以及針對 AWS Outposts API 操作的程式碼呼叫。如果您建立追蹤，您可以啟用 CloudTrail 事件持續傳遞至 S3 儲存貯體，包括AWS Outposts. 如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷提出的要求AWS Outposts、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。

若要取得有關的更多資訊 CloudTrail，請參閱AWS CloudTrail使用者指南。

AWS Outposts中的資訊 CloudTrail

CloudTrail 在您創建AWS帳戶時，您的帳戶已啟用。當活動發生在中時AWS Outposts，該活動會與事件歷史記錄中的其他AWS服務 CloudTrail 事件一起記錄在事件中。您可以檢視、搜尋和下載 AWS 帳戶的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需您 AWS 帳戶中正在進行事件的記錄 (包含 AWS Outposts 的事件)，請建立線索。追蹤可 CloudTrail 將日誌檔傳遞至父項中的 S3 儲存貯體AWS 區域。根據預設，當您在主控台建立追蹤記錄時，追蹤記錄會套用到所有 AWS 區域。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 S3 儲存貯體。此外，您還可以設定其他AWS服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件和從多個帳戶接收 CloudTrail日誌文件

所有AWS Outposts動作皆由記錄 CloudTrail。其會記載於《AWS Outposts API 參考》中。例如，呼叫`CreateOutpost`、`GetOutpostInstanceTypes`、和`ListSites`動作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌項目都會包含產生請求者的資訊。身分資訊可協助您判斷提出請求的身分是：

- 使用根或使用者憑證。
- 使用某個角色的暫時安全憑證登入資料或聯合身分使用者。
- 透過另一項 AWS 服務。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

了解 AWS Outposts 日誌檔案項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞至您指定的 S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求。它包括請求的動作、動作的日期和時間、請求參數等相關資訊。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範`CreateOutpost`動作的 CloudTrail 記錄項目。

```
{
    "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 維護

在共同責任模式下， AWS 負責運行 AWS 服務的硬件和軟件。這適用於 AWS Outposts，就像它對一個 AWS 區域一樣。例如， AWS 管理安全性修補程式、更新韌體，以及維護 Outpost 設備。 AWS 也會監控 Outpost 的效能、健全狀況和指標，並判斷是否需要進行任何維護。

> **Warning**
>
> 如果底層的磁碟機故障，或者如果執行個體停止、休眠或終止，執行個體儲存體磁碟區上的資料就會遺失。為了防止資料遺失，建議您將執行個體儲存體磁碟區上的長期資料備份到持久性儲存，例如 Amazon S3 儲存貯體、Amazon EBS 磁碟區或內部部署網路中的網路儲存裝置。

目錄

硬體維護

如果 AWS 偵測到在 Outpost 上執行的硬體託管 Amazon EC2 執行個體存在無法彌補的問題，我們會通知 Outpost 的擁有者和執行個體的擁有者，告知受影響的執行個體排定停用。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的《執行個體淘汰》。

Outpost 擁有者和執行個體擁有者可以共同解決問題。執行個體擁有者可以停止並啟動受影響的執行個體，將其移轉至可用的容量。執行個體擁有者可以在方便時停止並啟動受影響的執行個體。否則， AWS 會在執行個體淘汰日期停止並啟動受影響的執行個體。如果 Outpost 上沒有額外的容量，執行個體會繼續處於已停止狀態。Outpost 擁有者可以嘗試釋放已使用的容量或要求 Outpost 的額外容量，以便完成移轉。

如果需要維護硬件， AWS 將與 Outpost 站點的經理聯繫，以確認 AWS 安裝團隊訪問的日期和時間。最快可在站點經理與 AWS 團隊交談當日的兩個工作天內安排到訪。

當 AWS 安裝團隊抵達現場時，他們會取代運作狀況不佳的主機、交換器或機架元件，並將新容量上線。他們不會在現場執行任何硬體診斷或維修。如果他們更換了主機，就會移除並銷毀 NIST 相容的實體安全金鑰，進而有效地銷毀任何可能保留在硬體上的資料。如此即可確保不會有任何資料離開您的站點。如果他們更換了 Outpost 網路裝置，當該裝置從站點移除時，網路組態資訊可能會出現在裝置上。此資訊可能包括 IP 地址和 ASN，這些項目是用來建立虛擬介面，以設定本機網路徑或返回區域的路徑。

韌體更新

更新 Outpost 韌體通常不會影響 Outpost 上的執行個體。在極少數情況下，我們需要重新啟動 Outpost 設備才能安裝更新，您會收到在該容量上執行之任何執行個體的執行個體淘汰通知。

網路設備維護

在不影響正常 Outpost 操作和流量的情況下，執行 Outpost 網路裝置 (OND) 的維護。如果需要進行維護，則會從 OND 轉移流量。您可能會注意到 BGP 公告中的暫時變更 (例如在前面加上 AS-Path)，以及 Outpost 上行鏈路之流量模式中的相應變更。在 OND 韌體更新時，您可能會注意到 BGP 震盪。

建議您將客戶網路設備設定為接收來自 Outpost 的 BGP 公告，而不變更 BGP 屬性，並啟用 BGP 多路徑/負載平衡以獲得最佳傳入流量。在本機閘道字首前面加上 AS-Path，以在需要維護時從 OND 轉移流量。客戶網路應優先使用 Outpost 中 AS-Path 長度為 1 的路由，而不是 AS-Path 長度為 4 的路由。

客戶網路應向所有 OND 公告具有相同屬性的等量 BGP 字首。Outpost 網路負載預設會平衡所有上行鏈路之間的傳出流量。Outpost 端使用了路由政策，可在需要維護時從 OND 轉移流量。此流量轉移需要所有 OND 上的客戶端都有等量 BGP 字首。如果客戶網路需要維護，建議您在前面加上 AS-Path 以暫時從特定上行鏈路轉移流量。

AWS Outposts 電源和網路事件的最佳做法

正如 AWS Outposts 客戶AWS 服務條款中所述，Outposts 設備所在的設施必須滿足最低功率和網絡要求，以支持 Outposts 設備的安裝，維護和使用。只有在電源和網路連線不中斷時，Outposts 機架式才能正常運作。

電源事件

在完全停電的情況下，存在 AWS Outposts 資源可能無法自動返回服務的固有風險。除了部署備援電源和備用電源解決方案之外，建議您事先執行下列動作，以減輕某些最壞情況的影響：

- 使用 DNS 架構或機架外負載平衡變更，以受控方式將您的服務和應用程式從 Outpost 設備移出。
- 以循序增量方式停止容器、執行個體和資料庫，並在還原時使用相反的順序。
- 測試服務的受控移動或停止計畫。
- 備份關鍵資料和組態，並將其儲存在 Outpost 之外。
- 將停電的停機時間降至最低。
- 避免在維護期間重複切換電源供應 (關開關開)。
- 在維護時段內允許額外的時間來處理意外情況。
- 透過傳達比一般所需更寬的維護時段時間範圍來管理使用者和客戶的期望。

網路連線事件

您的 Outpost 與 AWS 區域或 Outposts 所在地區之間的服務連結連線通常會在網路維護完成後，自動從上游公司網路裝置或任何第三方連線供應商網路中可能發生的網路中斷或問題中復原。在服務連結連線中斷期間，您的 Outpost 操作僅限於本機網路活動。

如需詳細資訊，請參閱《AWS Outposts 機架常見問答集》頁面上的《當我的設施網路連線中斷，會發生什麼情況》問題。

如果服務連結因為現場電源問題或網路連線中斷，會 AWS Health Dashboard 傳送通知給擁有 Outposts 的帳戶。您也不 AWS 能禁止服務鏈接中斷的通知，即使預期中斷也是如此。如需詳細資訊，請參閱《 指南》中的《AWS Health AWS Health Dashboard入門》。

如果計畫的服務維護會影響網路連線，請採取下列主動步驟來限制潛在問題情況的影響：

- 如果您的 Outposts 機架通過互聯網或公共 Direct Connect 連接到父 AWS 區域，那麼在計劃的維護之前，捕獲跟踪路線。具備有效 (網路維護前) 的網路徑和有問題 (網路維護後) 的網路徑來識別差異將有助於進行疑難排解。如果您將維護後的問題升級到 AWS 或您的 ISP，則可以包含此資訊。

  擷取下列項目之間的 trace-route：

  - 位於 Outpost 位置的公有 IP 地址，以及 `outposts.region.amazonaws.com` 傳回的 IP 地址。將`##`替換為父 AWS 區域的名稱。
  - 父區域中任何具有公有網際網路連線的執行個體，以及位於 Outpost 位置的公有 IP 地址。
- 如果網路維護在您的控制下，請限制服務連結的停機時間。在維護程序中加入驗證網路是否已復原的步驟。
- 如果網路維護不在您的控制下，請監控與宣布維護時段相關的服務連結停機時間，如果服務連結未在宣布的維護時段結束時恢復上線，請及早向負責計畫網路維護的一方呈報。

資源

以下是一些監控相關資源，這些資源可確保 Outpost 在計畫或意外的電源或網路事件發生之後正常運作：

- AWS 博客監控最佳實踐 AWS Outposts涵蓋了 Outposts 特定的可觀察性和事件管理最佳實踐。
- Amazon VPC 網路連線的 AWS 部落格偵錯工具說明了 AWSSupport-Setu MonitoringFrom Pip VPC 工具。此工具是一份 AWS Systems Manager 文件 (SSM 文件)，可在您指定的子網路中建立 Amazon EC2 監視器執行個體並監控目標 IP 地址。此文件會執行 ping、MTR、TCP 追蹤路由和追蹤路徑診斷測試，並將結果儲存在 Amazon CloudWatch Logs 中，並可在 CloudWatch 儀表板中視覺化 (例如延遲、封包遺失)。對於 Outposts 監控，監控執行個體應位於父 AWS 區域的一個子網路中，並設定為使用其私有 IP 監視一或多個 Outpost 執行個體-這將提供和父 AWS 區域之間的封包遺失圖形 AWS Outposts 和延遲。
- 部署自動化 Amazon CloudWatch 儀表板以供 AWS Outposts 使用的部 AWS落格 AWS CDK說明部署自動化儀表板所涉及的步驟。
- 如果您有疑問或需要更多資訊，請參閱《AWS Support 使用者指南》中的《建立支援案例》。

優化 Amazon EC2 AWS Outposts

與此相反 AWS 區域，前哨 Amazon Elastic Compute Cloud (Amazon EC2) 容量是有限的。您會受到訂購之運算容量的總數量所限制。本主題提供最佳實務和最佳化策略，以協助您充分利用 AWS Outposts中的 Amazon EC2 容量。

目錄

Outpost 上的專用執行個體

Amazon EC2 專用執行個體是具有專供您使用之 EC2 執行個體容量的實體伺服器。Outpost 已提供專用硬體，但專用執行個體可讓您使用現有軟體授權，對單一主機進行個別通訊端、個別核心或個別 VM 授權的限制。如需詳細資訊，請參閱 Amazon EC2 使用者指南 AWS Outposts中的專用主機。對於視窗，請參閱 Amazon EC2 使用者指南 AWS Outposts中的專用主機。

除了授權之外，Outpost 擁有者還可以使用專用執行個體，透過兩種方式將 Outpost 部署中的伺服器最佳化：

- 更改伺服器的容量配置
- 控制硬體層級的執行個體配置

更改伺服器的容量配置

專用主機讓您無需聯絡 AWS Support即可變更 Outpost 部署中伺服器配置的功能。當您為 Outpost 購買容量時，您可以指定每個伺服器提供的 EC2 容量配置。每部伺服器都支援單一系列的執行個體類型。一個配置可以提供單一執行個體類型或多個執行個體類型。專用執行個體可讓您更改為該初始配置選擇的任何內容。如果您配置主機來支援整個容量的單一執行個體類型，則只能從該主機啟動單一執行個體類型。下圖顯示具有同質配置的 m5.24xlarge 伺服器：

您可以為多種執行個體類型配置相同的容量。當您配置主機來支援多種執行個體類型時，就會獲得不需要明確容量配置的異質配置。下圖顯示具有異質配置的完整容量 m5.24xlarge 伺服器：

如需詳細資訊，請參閱 Amazon EC2 使用者指南中的分配專用主機或分配專用主機 Amazon EC2 使用者指南。

控制硬體層級的執行個體配置

您可以使用專用執行個體來控制硬體層級的執行個體配置。使用專用執行個體的自動配置可管理您所啟動的執行個體要在特定主機上啟動，還是在任何具有相符組態的可用主機上啟動。使用主機親和性可建立執行個體與專用執行個體之間的關係。如果您有 Outpost 機架，則可以使用這些專用執行個體功能，將相關硬體故障的影響降到最低。如需執行個體復原的詳細資訊，請參閱 Amazon EC2 使用者指南中的了解自動放置和親和性或了解自動放置和親和性 Amazon EC2 使用者指南。

您可以使用共用專用主機 AWS Resource Access Manager。共用專用執行個體可讓您將 Outpost 部署中的主機分配到各 AWS 帳戶。如需詳細資訊，請參閱 使用共用資源。

設定執行個體復原

Outpost 上由於硬體故障而進入不良狀態的執行個體，必須移轉至狀態良好的主機。您可以設定自動復原，根據執行個體狀態檢查來自動完成這項移轉。如需詳細資訊，請參閱《復原您的 Linux 執行個體》或《復原您的 Windows 執行個體》。

Outpost 中的放置群組

AWS Outposts 支援放置群組。使用放置群組來影響 Amazon EC2 應嘗試將您所啟動相互依存的執行個體群組放在基礎硬體上的方式。您可以使用不同的策略 (叢集、分區或分散) 來滿足不同工作負載的需求。如果您有單機架 Outpost，則可以使用分散策略跨主機 (而非機架) 放置執行個體。

分散放置群組

使用分散放置群組，將單一執行個體分散到不同的硬體。透過分散放置群組來啟動執行個體，可降低同時發生故障的風險，這種情況可能會在執行個體共用相同設備時發生。放置群組可以跨機架或主機分散放置執行個體。您只能搭配使用主機層級分攤放置群組 AWS Outposts。

機架層級分散放置群組

您的機架分散層級放置群組可容納與 Outpost 部署中機架相同數量的執行個體。下圖顯示在機架分散層級放置群組中執行三個執行個體的三機架 Outpost 部署。

主機分散層級放置群組

您的主機分散層級放置群組可容納與 Outpost 部署中主機相同數量的執行個體。下圖顯示在主機分散層級放置群組中執行三個執行個體的單機架 Outpost 部署。

分區放置群組

使用分區放置群組，將多個執行個體分散到具有分割區的機架。每個分區可容納多個執行個體。您可以使用自動分散將執行個體分散到不同的分割區，或將執行個體部署到目標分割區 下圖顯示使用自動分散的分區放置群組。

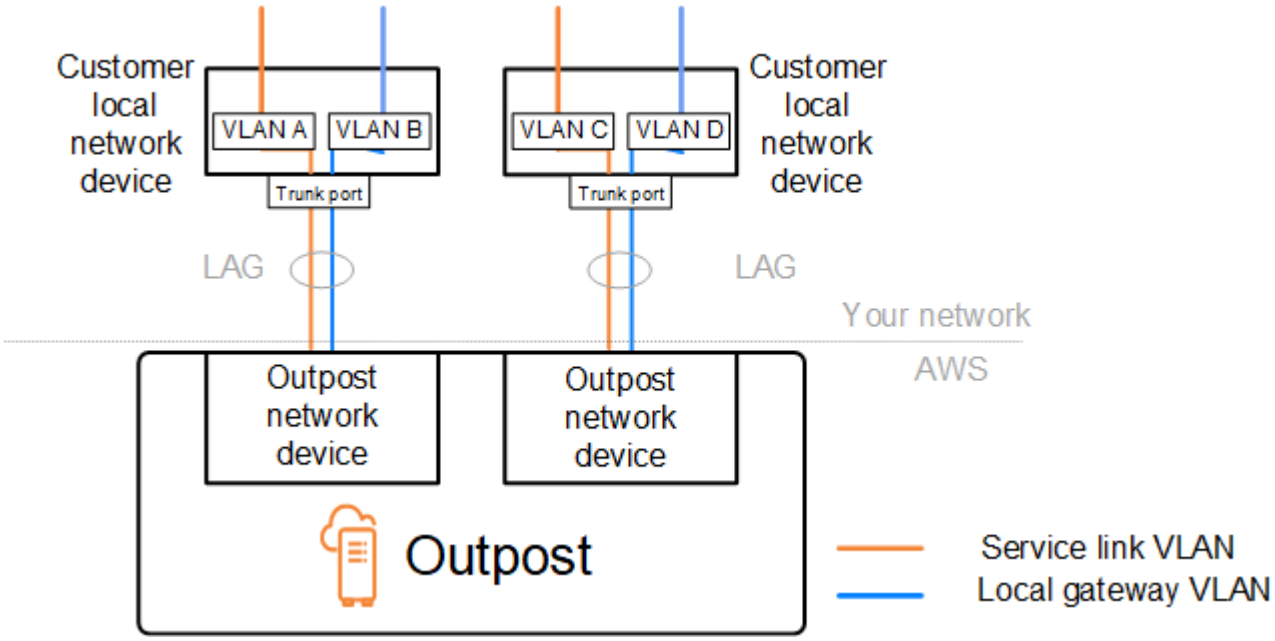
您也可以將執行個體部署到目標分割區。下圖顯示使用目標分散的分區放置群組。

如需使用置放群組的詳細資訊，請參閱 Amazon EC2 使用者指南 AWS Outposts中的放置群組和放置群組。對於視窗，請參閱 Amazon EC2 使用者指南 AWS Outposts中的放置群組和放置群組。

如需 AWS Outposts 高可用性的詳細資訊，請參閱AWS Outposts 高可用性設計與架構考量。

AWS Outposts 機架式網路疑難排解

使用此檢查清單來協助針對狀態為 DOWN 的服務連結進行疑難排解。



與 Outpost 網路裝置的連線

檢查連線到 Outpost 網路裝置之客戶本機網路裝置上的 BGP 對等互連狀態。如果 BGP 對等互連狀態為 DOWN，請依照下列步驟進行：

1. 從客戶裝置 ping Outpost 網路裝置上的遠端對等 IP 地址。您可以在裝置的 BGP 組態中找到對等 IP 地址。您也可以參考安裝時提供給您的《網路整備檢查清單》。
2. 如果 ping 失敗，請檢查實體連線，並確定連線狀態為 UP。
   a. 確認客戶本機網路裝置的 LACP 狀態。
   b. 檢查裝置上的介面狀態。如果狀態為 UP，請跳至步驟 3。
   c. 檢查客戶本機網路裝置，並確認光學模組正常運作。
   d. 更換有缺陷的光纖，並確保指示燈 (Tx/Rx) 在可接受的範圍內。
3. 如果 ping 成功，請檢查客戶本機網路裝置，並確定下列 BGP 組態正確。
   a. 確認已正確設定本機自治系統編號 (客戶 ASN)。
   b. 確認已正確設定遠端自治系統編號 (Outpost ASN)。
   c. 確認已正確設定介面 IP 和遠端對等 IP 地址。
   d. 確認公告和接收的路由正確。
4. 如果您的 BGP 工作階段在作用中和連線狀態之間震盪，請確認客戶本機網路裝置上未封鎖 TCP 連接埠 179 和其他相關暫時性連接埠。
5. 如果您需要進一步疑難排解，請在客戶本機網路裝置上檢查下列各項：

a. BGP 和偵錯日誌

b. BGP 日誌

c. 封包擷取

6. 如果問題仍存在，請從您的 Outpost 連線路由器對 Outpost 網路裝置對等 IP 地址執行 MTR/traceroute/封包擷取。使用您的企業 AWS 支援方案，與 Support 人員共用測試結果。

如果客戶本機網路裝置與 Outpost 網路裝置之間的 BGP 對等互連狀態為 UP，但服務連結仍為 DOWN，您可以透過檢查客戶本機網路裝置上的下列裝置來進一步疑難排解。根據您服務連結連線的佈建方式，使用下列其中一份檢查清單。

- 連線的邊緣路由器 AWS Direct Connect — 用於服務連結連線的公用虛擬介面。如需詳細資訊，請參閱 AWS Direct Connect 與 AWS 區域的公共虛擬界面連接。
- 連接的邊緣路由器 AWS Direct Connect — 用於服務鏈路連接的私有虛擬界面。如需詳細資訊，請參閱 AWS Direct Connect 與 AWS 區域的私有虛擬界面連接。
- 使用網際網路服務供應商 (ISP) 連線的邊緣路由器 – 用於服務連結連線的公有網際網路。如需詳細資訊，請參閱 AWS 區域的 ISP 公有網際網路連線。

AWS Direct Connect 與 AWS 區域的公共虛擬界面連接

當使用公用虛擬介面進行服務連結連線 AWS Direct Connect 時，請使用下列檢查清單對連線的 Edge 路由器進行疑難排解。

1. 確認直接與 Outpost 網路裝置連線的裝置正在透過 BGP 接收服務連結 IP 地址範圍。

   a. 確認正在從您的裝置透過 BGP 接收路由。

   b. 檢查服務連結虛擬路由和轉送執行個體 (VRF) 的路由表。其中應該顯示正在使用 IP 地址範圍。

2. 若要確保區域連線，請檢查服務連結 VRF 的路由表。它應該包括 AWS 公用 IP 地址範圍或默認路由。

3. 如果您沒有在服務鏈接 VRF 中收到 AWS 公共 IP 地址範圍，請檢查以下項目。

   a. 從邊緣路由器或檢查 AWS Direct Connect 連結狀態 AWS Management Console。

   b. 如果實體連結為 UP，請從邊緣路由器檢查 BGP 對等互連狀態。

   c. 如果 BGP 對等狀態為DOWN，請 ping 對等 AWS IP 位址，並檢查邊緣路由器中的 BGP 組態。如需詳細資訊，請參閱AWS Direct Connect 使用指南 AWS Direct Connect中的疑難排解和AWS 主控台中的「我的虛擬介面 BGP 狀態已關閉」。我該怎麼辦》。

d. 如果已建立 BGP，但您在 VRF 中看不到預設路由或 AWS 公用 IP 位址範圍，請使用您的企業 Sup AWS port 方案聯絡支援部門。

4. 如果您有內部部署防火牆，請檢查下列項目。

   a. 確認網路防火牆中允許服務連結連線所需的連接埠。在連接埠 443 上使用 traceroute，或是使用任何其他網路疑難排解工具，確認連線通過防火牆和您的網路裝置。需要在防火牆政策中設定下列連接埠，才能進行服務連結連線。

      - TCP 通訊協定 – 來源連接埠：TCP 1025-65535，目的地連接埠：443。
      - UDP 通訊協定 – 來源連接埠：TCP 1025-65535，目的地連接埠：443。

   b. 如果防火牆是可設定狀態的，請確定輸出規則允許 Outpost 的服務連結 IP 位址範圍到 AWS 公用 IP 位址範圍。如需詳細資訊，請參閱 AWS Outposts 連線至 AWS 區域。

   c. 如果防火牆不可設定狀態，請確保也允許輸入流程（從 AWS 公用 IP 位址範圍到服務連結 IP 位址範圍）。

   d. 如果您已在防火牆中設定虛擬路由器，請確定已針對 Outpost 與 AWS 區域之間的流量設定適當的路由。

5. 如果您已在內部部署網路中設定 NAT，將 Outpost 的服務連結 IP 地址範圍轉譯為您自己的公有 IP 地址，請檢查下列項目。

   a. 確認 NAT 裝置未超載，且具有可用的連接埠以便配置新的工作階段。

   b. 確認 NAT 裝置已正確設定為執行地址轉譯。

6. 如果問題仍然存在，請從邊緣路由器執行 MTR/ 跟踪路由器/數據包捕獲到 AWS Direct Connect 對等 IP 地址。使用您的企業 AWS 支援方案，與 Support 人員共用測試結果。

AWS Direct Connect 與 AWS 區域的私有虛擬界面連接

使用下列檢查清單，針對使用私有虛擬介面進行服務連結連線 AWS Direct Connect 時所連線的邊緣路由器進行疑難排解。

1. 如果 Outpost 機架與 AWS 區域之間的連線正在使用 AWS Outposts 私人連線功能，請檢查下列項目。

   a. 從邊緣路由器 Ping 遠端對等 AWS IP 位址，並確認 BGP 對等狀態。

   b. 請確定您的服務連結端點 VPC 與內部部署上安裝的 Outpost 之間透過 AWS Direct Connect 私有虛擬介面進行 BGP 對等互連。UP如需詳細資訊，請參閱AWS Direct Connect 使用者指南 AWS Direct Connect中的「我的虛擬介面 BGP 狀態已關閉」中的「 AWS疑難排解」。我該怎麼辦》和《如何針對透過 Direct Connect 的 BGP 對等互連問題進行疑難排解》。

c. AWS Direct Connect 私有虛擬界面是與您所選 AWS Direct Connect 位置的邊緣路由器的私人連接，它使用 BGP 交換路由。您的虛擬私有雲端 (VPC) CIDR 範圍會透過此 BGP 工作階段向您的邊緣路由器公告。同樣地，Outpost 服務連結的 IP 地址範圍也會透過 BGP 從您的邊緣伺服器向區域公告。

d. 確認與 VPC 中服務連結私有端點相關聯的網路 ACL 允許相關流量。如需詳細資訊，請參閱 網路整備檢查清單。

e. 如果您有內部部署防火牆，請確定防火牆具有傳出規則，允許服務連結 IP 地址範圍以及位於 VPC 或 VPC CIDR 中的 Outpost 服務端點 (網路介面 IP 地址)。請確定未封鎖 TCP 1025-65535 和 UDP 443 連接埠。如需詳細資訊，請參閱介紹 AWS Outposts 私人連線。

f. 如果防火牆不具狀態，請確定防火牆具有規則和政策，允許從 VPC 中 Outpost 服務端點到 Outpost 的傳入流量。

2. 如果您的內部部署網路中有 100 個以上的網路，您可以透過 BGP 工作階段在私人虛擬介面 AWS 上公告預設路由。如果您不想公告預設路由，請彙總路由，以便公告路由的數量小於 100。
3. 如果問題仍然存在，請從邊緣路由器執行 MTR/ 跟踪路由器/數據包捕獲到 AWS Direct Connect 對等 IP 地址。使用您的企業 AWS 支援方案，與 Support 人員共用測試結果。

AWS 區域的 ISP 公有網際網路連線

使用公有網際網路進行服務連結連線時，請使用下列檢查清單對透過 ISP 連線的邊緣路由器進行疑難排解。

- 確認網際網路連結已啟動。
- 確認可從透過 ISP 連線的邊緣裝置存取公有伺服器。

如果無法透過 ISP 連結存取網際網路或公有伺服器，請完成下列步驟。

1. 檢查 ISP 路由器的 BGP 對等互連狀態是否為「已建立」。
   a. 確認 BGP 沒有震盪。
   b. 確認 BGP 正在從 ISP 接收和公告所需的路由。
2. 在靜態路由組態的情況下，請確認已在邊緣裝置上正確設定預設路由。
3. 確認您是否可以使用其他 ISP 連線來連線到網際網路。
4. 如果問題仍存在，請在您的邊緣路由器上執行 MTR/traceroute/封包擷取。與 ISP 的技術支援團隊共用結果，以進一步疑難排解。

如果可透過 ISP 連結存取網際網路和公有伺服器，請完成下列步驟。

1. 確認是否可從您的邊緣裝置存取 Outpost 主要區域中任何可公開存取的 EC2 執行個體或負載平衡器。您可以使用 ping 或 telnet 來確認連線，然後使用 traceroute 來確認網路徑。
2. 如果您使用 VRF 來分隔網路中的流量，請確認服務連結 VRF 具有引導流量進出 ISP (網際網路) 和 VRF 的路由或政策。請參閱下列檢查點。
   a. 與 ISP 連線的邊緣路由器。檢查邊緣路由器的 ISP VRF 路由表，以確認服務連結 IP 地址範圍存在。
   b. 與 Outpost 連線的客戶本機網路裝置。檢查 VRF 的組態，並確定已正確設定在服務連結 VRF 與 ISP VRF 之間進行連線所需的路由和政策。通常，預設路由是從 ISP VRF 發送到服務連結 VRF 中，以便將流量路由到網際網路。
   c. 如果您在連線到 Outpost 的路由器中設定了以來源為基礎的路由，請確認設定正確。
3. 請確定內部部署防火牆已設定為允許從前哨服務連結 IP 位址範圍到公用 IP 位址範圍的輸出連線 (TCP 1025-65535 和 UDP 443 連接埠)。 AWS 如果防火牆不具狀態，請確定也設定了 Outpost 的傳入連線。
4. 請確定已在內部部署網路中設定 NAT，將 Outpost 的服務連結 IP 地址範圍轉譯為公有 IP 地址。此外，請確認下列項目。
   a. NAT 裝置未超載，且具有可用的連接埠以便配置新的工作階段。
   b. NAT 裝置已正確設定為執行地址轉譯。

如果問題仍存在，請執行 MTR/traceroute/封包擷取。

- 如果結果顯示封包在內部部署網路中捨棄或遭封鎖，請洽詢您的網路或技術團隊以取得其他指引。
- 如果結果顯示封包在 ISP 的網路中捨棄或遭封鎖，請聯絡 ISP 的技術支援團隊。
- 如果結果未顯示任何問題，請從所有測試（例如 MTR、telnet、追蹤路由、封包擷取和 BGP 記錄）收集結果，並使用您的企業 Support 計劃聯絡 AWS 支援部門。

Outposts 位於兩個防火牆設備後面

如果您已將 Outpost 置於高可用性的同步防火牆對或兩個獨立防火牆後面，則可能會發生服務連結的非對稱路由。這意味著入站流量可以通過防火牆 -1，而出站流量通過防火牆 -2。使用下列檢查清單來識別服務連結的潛在非對稱路由，尤其是在之前運作正常的情況下。

- 確認公司網路的路由設定中是否有任何近期變更或持續維護，可能導致透過防火牆對服務連結進行非對稱路由。

  - 使用防火牆流量圖來檢查與服務連結問題開始相符的流量模式是否有變更。
  - 檢查是否有部分防火牆故障或分離式防火牆配對案例，這些案例可能導致防火牆彼此之間不再同步連線表。
  - 檢查您公司網路中的連結關閉或最近的路由變更 (OSPF/ISISS/EIGRP 指標變更、BGP 路由對應變更)，以符合服務連結問題的開始。
- 如果您使用公用網際網路連線來連至本地區域的服務連結，服務提供者維護可能會導致透過防火牆對服務連結進行非對稱路由。
  - 請查看 ISP 連結的流量圖表，瞭解與服務連結問題開始相符的流量模式變更。
- 如果您使用服務 AWS Direct Connect 連結的連線能力，則 AWS 計劃的維護可能會觸發服務連結的非對稱路由。
  - 檢查您 AWS Direct Connect 服務的計劃維護通知。
  - 請注意，如果您有冗餘 AWS Direct Connect 服務，則可以在維護條件下透過每個可能的網路路徑主動測試 Outposts 服務連結的路由。這可讓您測試其中一個服務中斷是否會導致 AWS Direct Connect 服務連結的非對稱路由。具備彈性工具組的復原能力可以測試 end-to-end 網路連線 AWS Direct Connect 部分的 AWS Direct Connect 彈性。如需詳細資訊，請參閱使用 AWS Direct Connect 彈性工具組測試彈性 — 容錯移轉測試。

在您完成前述檢查清單，並將服務連結的非對稱路由指定為可能的根本原因之後，您可以採取一些進一步的動作：

- 還原任何公司網路變更，或等待提供者計劃的維護完成，以還原對稱路由。
- 登入一個或兩個防火牆，並從命令列清除所有流程的所有流程狀態資訊（如果防火牆廠商支援）。
- 通過其中一個防火牆臨時過濾掉 BGP 公告或關閉一個防火牆上的接口，以強制對稱路由通過另一個防火牆。
- 依次重新啟動每個防火牆，以消除防火牆記憶體中服務連結流量的流程狀態追蹤可能的損毀。
- 請您的防火牆廠商，驗證或放鬆追蹤來自連接埠 443 且目的地連接埠 443 的 UDP 連線的 UDP 流量狀態。

AWS Outposts end-of-term 選項

在 AWS Outposts 任期結束時，您有三種選擇：

- 續訂您的訂閱並保留現有的 Outpost。
- 結束您的訂閱並備妥您的 Outpost 機架以便退回。
- 轉換為 month-to-month 訂閱並保留您現有的前哨。

主題

續訂訂閱

續訂您的訂閱並保留現有的 Outpost：

請在 Outpost 使用期限結束前至少 30 天內，完成以下步驟：

1. 登入 AWS Support 中心主控台。
2. 選擇建立案例。
3. 選擇 帳戶和帳單。
4. 針對服務，選擇帳單。
5. 針對類別，選擇其他帳單問題。
6. 針對嚴重性，選擇重要問題。
7. 選擇 Next step: Additional information (下一步：其他資訊)。
8. 在其他資訊頁面上，針對主旨輸入您的續約請求，例如 **`Renew my Outpost subscription`**。
9. 針對描述，輸入下列一種付款選項：
    - 不預付
    - 部分預付
    - 全額預付

如需定價，請參閱《AWS Outposts 機架定價》。您也可以請求報價。

10. 選擇下一步驟：立即解決或聯絡我們。
11. 在 Contact us (聯絡我們) 頁面中，選擇您偏好的語言。
12. 選擇您偏好的聯絡方式。
13. 檢閱您的案例詳細資訊，然後選擇 Submit (提交)。您的案例 ID 編號和摘要隨即出現。

AWS 客戶 Support 將啟動訂閱續訂程序。您的新訂閱將在您目前訂閱結束後的隔天開始生效。

如果您沒有指示要續訂或退回 Outpost 機架，您將自動轉換為 month-to-month 訂閱。您的前哨將按照與您的配置相對應的不預付款選項的費率每月續訂。 AWS Outposts 您的新按月訂閱將在您目前訂閱結束後的隔天開始生效。

結束您的訂閱並備妥機架以便退回

> **Important**
>
> AWS 在您完成下列程序之前，無法開始退貨程序。在您開立結束訂閱的支援案例後，我們就無法停止退回流程。

結束您的訂閱：

請在 Outpost 使用期限結束前至少 30 天內，完成以下步驟：

1. 登入 AWS Support 中心主控台。
2. 選擇建立案例。
3. 選擇 帳戶和帳單。
4. 針對服務，選擇帳單。
5. 針對類別，選擇其他帳單問題。
6. 針對嚴重性，選擇重要問題。
7. 選擇 Next step: Additional information (下一步：其他資訊)。
8. 在 其他資訊 頁面上，針對 主旨，輸入明確的請求，例如 **`End my Outpost subscription`**。
9. 針對描述，輸入您偏好回收 Outpost 的日期。
10. 選擇下一步驟：立即解決或聯絡我們。

11. 在 Contact us (聯絡我們) 頁面中，選擇您偏好的語言。
12. 選擇您偏好的聯絡方式。
13. 檢閱您的案例詳細資訊，然後選擇 Submit (提交)。您的案例 ID 編號和摘要隨即出現。

AWS 「客戶 Support」將與您聯絡以協調擷取作業。

若要準備退貨的 AWS Outposts 機架：

> **Important**
> 請勿關閉前哨機架的電源，直到 AWS 現場進行排定的擷取作業。

1. 如果 Outpost 的資源是共用的，您必須取消共用這些資源。

   您可以透過以下其中一種方式將共用的 Outpost 資源取消共用：

   - 使用控 AWS RAM 制台。如需詳細資訊，請參閱《 指南》中的《AWS RAM 更新資源共用》。
   - 使用執行 AWS CLI 取消關聯資源共用命令。

   如需可共用的 Outpost 資源清單，請參閱《可共用的 Outpost 資源》。
2. 終止與 Outpost 上子網路相關聯的作用中執行個體。若要終止執行個體，請按照 Amazon EC2 使用者指南中的終止執行個體中的指示執行。

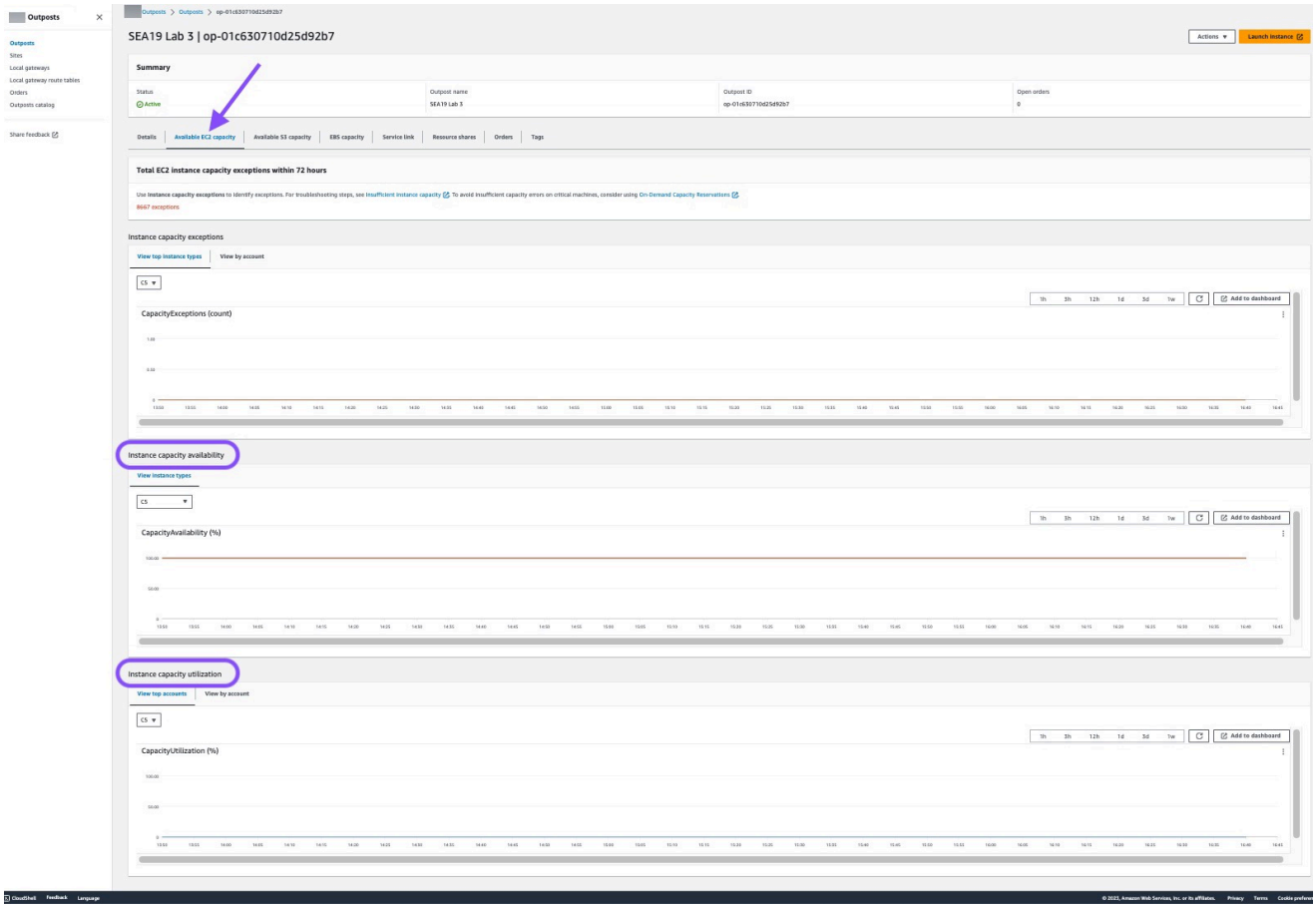
   > **Note**
   > 在 Outpost 上執行的某些 AWS受管服務 (例如應用程式負載平衡器或 Amazon Relational Database Service (RDS) 會消耗 EC2 容量。但是，它們的關聯執行個體在 Amazon EC2 儀表板上不會顯示。您必須終止與這些服務相關聯的資源，才能釋放容量。如需詳細資訊，請參閱為什麼我的 Outpost 缺少某些 EC2 執行個體容量？ 。
3. 驗證您 AWS 帳戶中 instance-capacity-availability 的 Amazon EC2 執行個體。

   a. 開啟主 AWS Outposts 控台，網址為 https://console.aws.amazon.com/outposts/。
   b. 選擇 Outpost。
   c. 選擇您要退回的特定 Outpost。
   d. 在 Outpost 的頁面上，選擇 可用的 EC2 容量 標籤。

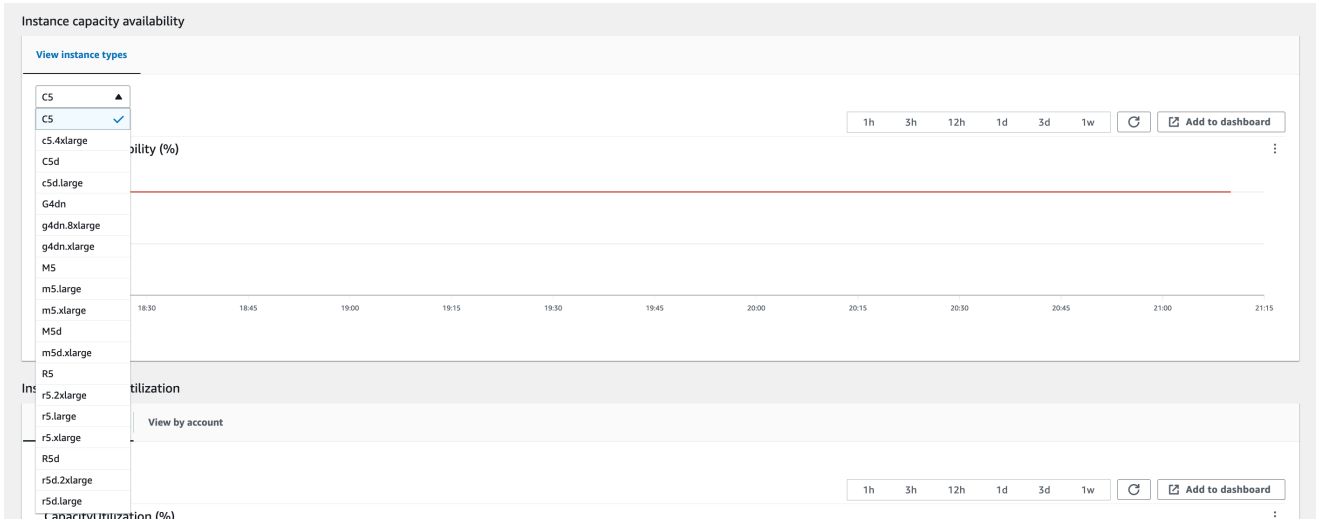
e. 確保每個執行個體系列的 執行個體容量可用性 為 100%。

f. 確保每個執行個體系列的 執行個體容量使用率 為 0%。

下圖顯示 可用的 EC2 容量 標籤上的 執行個體容量可用性 和 執行個體容量使用率 圖表。



下圖顯示執行個體類型清單。



4. 建立 Amazon EC2 執行個體和伺服器磁碟區的備份。若要建立備份，請依照《AWS 方案指引》指南中《備份和復原具有 EBS 磁碟區的 Amazon EC2》的說明進行。
5. 刪除與 Outpost 相關聯的 Amazon EBS 磁碟區。
   a. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
   b. 從導覽窗格，選擇 磁碟區。
   c. 選擇 動作 和 刪除磁碟區。
   d. 在確認對話方塊中，選擇 Delete (刪除)。
6. 如果您有 Amazon S3 on Outpost，請刪除 Outpost 上的任何本機快照。
   a. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
   b. 在導覽窗格中，選擇 Snapshots (快照)。
   c. 選取具有 Outpost ARN 的快照。
   d. 選擇 動作 和 刪除快照。
   e. 在確認對話方塊中，選擇 Delete (刪除)。
7. 刪除與 Outpost 相關聯的任何 Amazon S3 儲存貯體。若要刪除儲存貯體，請依照《Amazon Simple Storage Service 使用者指南》中《刪除 Amazon S3 on Outpost 儲存貯體》的說明進行。
8. 刪除與 Outpost 相關聯之任何 VPC 關聯和客戶擁有的 IP 地址集區 (CoIP) CIDR。

AWS 擷取團隊將關閉機架的電源。關閉電源後，您可以銷毀 AWS Nitro 安全密鑰，或者 AWS 檢索團隊可以代表您這樣做。

轉換為 month-to-month 訂閱

若要轉換為 month-to-month 訂閱並保留現有的 Outpost，不需要採取任何動作。如有任何問題，請開立帳單支援案例。

您的前哨將按照與您的配置相對應的不預付款選項的費率每月續訂。 AWS Outposts 您的新按月訂閱將在您目前訂閱結束後的隔天開始生效。

AWS Outposts 的配額

對於每個配額，您的AWS 帳戶有預設配額，先前稱為限制AWS 服務。除非另有說明，否則每個配額都是區域特定規定。您可以要求提高某些配額，而所有配額無法提高。

若要檢視的配額AWS Outposts，請開啟 Ser vice Quotas 主控台。在導覽窗格中 AWS 服務，選擇並選取AWS Outposts。

若要請求提升配額，請參閱《Service Quotas 使用者指南》中的請求提升配額。

您的 AWS 帳戶 具有下列與 AWS Outposts 相關的配額。

資源	預設	可調整	說明
前哨站點	100	是	前哨站點是客戶管理的實體建築，您可以在其中為 Outpost 設備供電並將其連接到網路。 您可以在AWS帳戶的每個區域中擁有 100 個 Outposts 點。
每個網站的 Outposts	10	是	AWS Outposts包括硬件和虛擬資源，稱為 Outposts。此配額會限制您的 Outpost 虛擬資源。 您可以在每個 Outposts 點中擁有 10 個前哨站。

AWS Outposts以及其他服務的配額

AWS Outposts依賴於其他服務的資源，這些服務可能有自己的默認配額。例如，您的本機網路界面配額來自網路界面的 Amazon VPC 配額。

文件歷史紀錄

下表說明 AWS Outposts 使用者指南的重要變更。

變更	描述	日期
容量管理	您可以修改新 Outposts 訂單的預設容量組態。	2024年4月16日
AWS Outposts 機架支援服務連結介面輸送量指標	您現在可以利IfTraffic In 用和指標來監控 Outpost 機架服務連結虛擬界面 (VIF) 和本機網路裝置之間的輸送量使用情況。IfTrafficOut Amazon CloudWatch	2023 年 11 月 17 日
與本機閘道之間的 VPC 人雲端 AWS Outposts 內通訊	您可以透過本機閘道，在不同 Outpost 的相同 VPC 中的子網路之間建立通訊。	2023 年 8 月 30 日
AWS Outposts 機架的 E nd-of-term 選項	在 AWS Outposts 期限結束時，您可以續訂、結束或轉換訂閱。	2023 年 8 月 1 日
Outposts 上的 Amazon 路線 53 可在 AWS Outposts 機架上使用。	Amazon Route 53 on Outpost 包括一個解析程式，用於快取源自 AWS Outposts的所有 DNS 查詢。您也可以在部署傳入和傳出端點時，在 Outpost 和內部部署 DNS 解析程式之間設定混合式連線。	2023 年 7 月 20 日
本機閘道傳入路由	您可以建立和修改目的地為 Outpost 上彈性網路介面的本機閘道傳入路由。	2022 年 9 月 15 日

介紹下列項目的直接 VPC 路由 AWS Outposts	使用 VPC 中執行個體的私有 IP 地址與內部部署網路進行通訊。	2022 年 9 月 14 日
創建的 Outposts 機架 AWS Outposts 用戶指南	AWS Outposts 用戶指南分為機架和服務器的單獨指南。	2022 年 9 月 14 日
建立和管理本機閘道路由表	建立和修改本機閘道路由表和 CoIP 集區。管理 VIF 群組關聯。	2022 年 9 月 14 日
放置群組 AWS Outposts	使用分散策略的放置群組可跨主機分配執行個體。	2022 年 6 月 30 日
專用主機 AWS Outposts	您現在可以在 Outpost 上使用專用執行個體。	2022 年 5 月 31 日
共用 Outpost 站點	建立和管理 Outpost 網站，並與組織中的其他 AWS 帳戶共用。	2021 年 10 月 18 日
新 CloudWatch 維度	AWS Outposts 命名空間中 CloudWatch 度量的新維度。	2021 年 10 月 13 日
共用 S3 儲存貯體	在您的 Outpost 上共用和管理 S3 儲存貯體。	2021 年 8 月 5 日
支援某些放置群組	您可以像在區域中一樣使用叢集、分區或分散放置策略。	2021 年 7 月 28 日
其他 CloudWatch 指標	預留執行個體可使用其他 CloudWatch 指標。	2021 年 5 月 24 日
網路故障診斷檢查清單	提供網路故障診斷檢查清單。	2021 年 2 月 22 日
其他 CloudWatch 指標	提供 EBS 磁碟區的其他 CloudWatch 指標。	2021 年 2 月 2 日
主控台訂購更新	主控台訂購程序已更新。	2021 年 1 月 14 日

私有連線	當您在 AWS Outposts 主控台中建立 Outpost 時，可以為 Outpost 設定私有連線。	2020 年 12 月 21 日
網路整備檢查清單	當您收集 Outpost 組態的資訊時，請使用網路整備檢查清單。	2020 年 10 月 28 日
共享 AWS Outposts 資源	透過 Outpost 共用，Outpost 擁有者可以與同一組織下的其他 AWS 帳戶共用其 Outposts 和 Outpost 資源，包括本機閘道路由表。 AWS	2020 年 10 月 15 日
其他 CloudWatch 指標	還提供執行個體類型計數的其他 CloudWatch 指標。	2020 年 9 月 21 日
其他 CloudWatch 量度	可使用服務連結連線狀態的其他 CloudWatch 測量結果。	2020 年 9 月 11 日
支援共用客戶擁有的 IPv4 地址	用 AWS Resource Access Manager 於共用客戶擁有的 IPv4 位址。	2020 年 4 月 20 日
其他 CloudWatch 指標	提供 EBS 磁碟區的其他 CloudWatch 指標。	2020 年 4 月 4 日
初始版本	這是的初始版本 AWS Outposts。	2019 年 12 月 3 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。