伺服器使用者指南

AWS Outposts

AWS Outposts: 伺服器使用者指南

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 執行個體和子網路等 AWS 資源時指定子網路。Outpost 子網中的執行個體使用私有 IP 地址與 AWS 區域中的其他執行個體通訊，且都在同一 VPC 內執行。

> **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。
- 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。

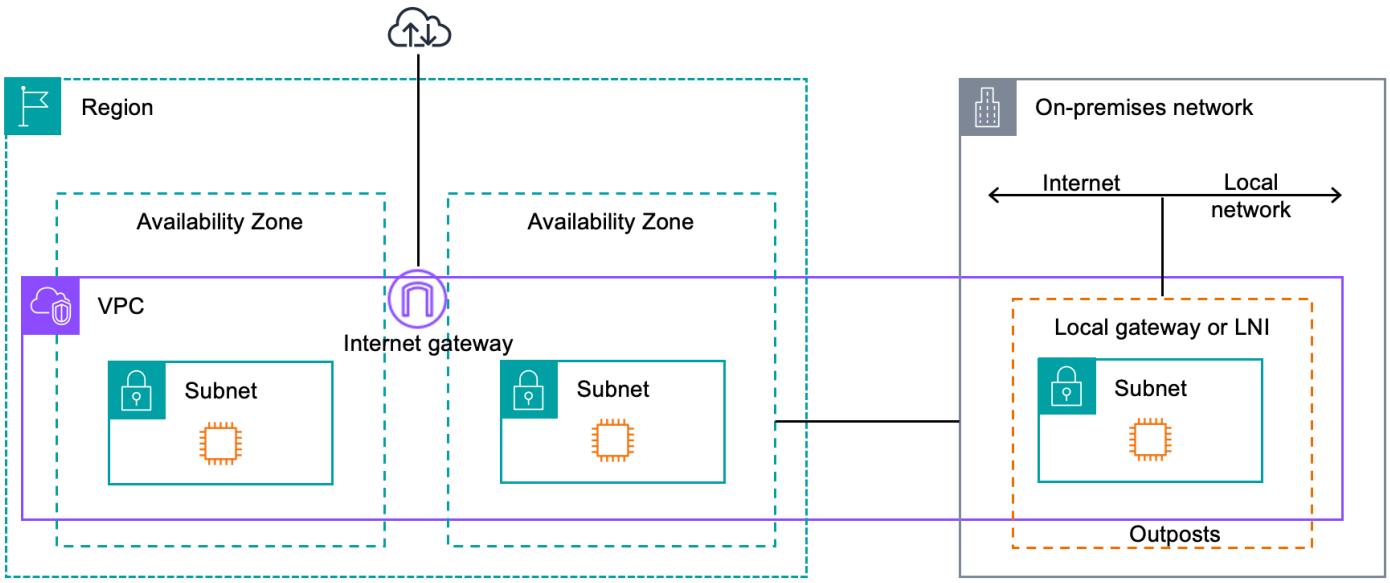
目錄

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。

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。如需更多詳細資訊，請參閱 本機網路介面。

Outposts 服器的站台需求

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 伺服器常見問答集》。請參閱《在哪些國家和地區提供 Outpost 伺服器》問題。

本頁面涵蓋 Outpost 伺服器的要求。如需 Outpost 機架的要求，請參閱《AWS Outposts Outpost 機架使用者指南》中的《Outpost 機架的站點要求》。

設施

以下是伺服器的設施要求。

> **Note**
>
> 這些規格適用於正常操作條件下的伺服器。例如，在初始安裝過程中，聲音可能比較大，但安裝完成後則會按額定聲功率操作。

- 溫度 - 環境溫度必須介於華氏 41-95 度 (攝氏 5-35 度) 之間。

  如果溫度在此範圍外，伺服器會關閉，並在溫度回到範圍內時重新啟動。
- 濕度 - 相對濕度必須介於 8% 和 80% 之間，且無冷凝。
- 空氣品質 - 空氣必須使用 MERV8 (或更高階的) 過濾器過濾。
- 通風 - 伺服器所在位置必須確保與前後牆壁間隔至少 6 英吋 (15 公分)，留有足夠的間隙供氣流流通。
- 重量 - 1U 伺服器重 26 磅，2U 伺服器重 36 磅。確認預計放置伺服器的位置，符合伺服器的承重要求。

  若要查看不同 Outposts 資源的重量需求，請在 AWS Outposts 主控台中選擇「瀏覽目錄」，網址為 https://console.aws.amazon.com/outposts/。
- 導軌套件相容性 - 託運包裹中隨附的導軌套件與符合 EIA-310-D 標準之 19 吋機架的標準 L 形安裝支架相容。

  > **Important**
  >
  > 導軌套件與 U 形安裝支架不相容，如下圖所示。

- 放置機架 - 建議使用深度至少為 36 英吋 (914 公釐) 的標準 19 吋 EIA-310D 機架。
  - Outposts 2U 伺服器需要具備下列尺寸的空間：3.5 英吋高度 (88.9 公釐)、17.5 英吋寬度 (447 公釐)、深度 30 英吋 (762 公釐)
  - Outposts 1U 伺服器需要具有以下尺寸的空間：1.75 英寸高度（44.45 毫米），17.5 英寸寬度（447 毫米），24 英寸深度（610 毫米）

  > **Note**
  > - 不支援垂直掛載 AWS Outposts 伺服器。
  > - 前哨 1U 服務器的寬度與 Outposts 2U 服務器的寬度相同，但高度的一半和更小的深度

  AWS 為伺服器的機架安裝提供導軌套件。如需詳細資訊，請參閱 步驟 3：機架安裝。

  如果伺服器不放在機架中，您仍然必須達到本節列出的其他需求。
- 可維修性 - Outpost 伺服器可從前通道維修。
- 聲音 - 在華氏 80 度 (攝氏 27 度) 的溫度下，額定低於 78 dBA 的聲功率，符合 GR-63 CORE NEBS 規範。
- 抗震支撐 – 在法規要求範圍內，您必須在設施中為伺服器安裝和維護適當的抗震錨固和支撐。
- 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)。
- 清潔 - 請使用含核准之除靜電清潔化學用品的濕巾擦拭表面。

聯網

每個 Outposts 伺服器都包含個非備援實體上行連接埠。連接埠有自己的速度和連接器需求，詳細資訊如下。

連接埠標籤	速度	上游聯網裝置的連接器	流量
連接埠 3	10Gbe	SFP+	服務和 LNI 連接流量皆可使用 - QSFP+ 分接線 (10 英尺/3 公尺) 將流量分段。如需詳

連接埠標籤	速度	上游聯網裝置的連接器	流量
			細資訊，請參閱 設定 QSFP 網路。

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	1024-65535	服務連結 IP	53	DHCP 提供的 DNS 伺服器
UDP	443, 1024-65535	服務連結 IP	443	Outposts 服務連結端點
TCP	1024-65535	服務連結 IP	443	Outposts 註冊端點

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 Outposts 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。

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 的備援連線來連線至區域的服務連線。 AWS 每部 Outpost 伺服器的最大使用率為 500 Mbps。若要提高連線速度，請使用多部 Outpost 伺服器。例如，如果您有三部 AWS Outposts 伺服器，則最大連線速度會提高到 1.5 Gbps (1,500 Mbps)。如需詳細資訊，請參閱 伺服器的服務連結流量。

您的 AWS Outposts 服務連結頻寬需求會根據工作負載特性而有所不同，例如 AMI 大小、應用程式彈性、突發速度需求以及該區域的 Amazon VPC 流量。請注意， AWS Outposts 伺服器不會快取 AMI。每次啟動執行個體都會從區域下載 AMI。

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。

服務連結需要 DHCP 回應

服務連結需要 IPv4 DHCP 回應來設定網路設定。

服務連結最長延遲

服務連結可支援之伺服器及其可用區域的最長網路延遲為 250 毫秒。

電源

這些是 Outpost 伺服器的電源要求。

要求

- 電源支援
- 耗電量
- 電源線
- 備用電源

電源支援

伺服器額定值最高可達 1600W 90-264 VaC 47/63 Hz 交流電源。

耗電量

若要查看不同 Outposts 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」。

電源線

伺服器隨附 IEC C14-C13 電源線。

從伺服器到機架的電源線

使用隨附的 IEC C14-C13 電源線將伺服器連接至機架。

從伺服器到牆上插座的電源線

若要將伺服器連接到標準的牆壁插座，您必須使用 C14 插座轉接器或特定國家/地區的電源線。

請務必使用所在地區的正確轉接器或電源線，以節省伺服器的安裝時間。

- 在美國，您需要 IEC C13 轉 NEMA 5-15P 的電源線。
- 歐洲有些地區可能需要使用 IEC C13 轉 CEE 7/7 的電源線。
- 印度需要 IEC C13 轉 IS1293 的電源線。

備用電源

伺服器有多個電源接口，並隨附多條纜線可供您使用備用電源。建議準備備用電源，但非必要。

伺服器不含不斷電系統 (UPS)。

訂單履行

為了完成訂單， AWS 將運送 Outposts 伺服器設備，包括軌道支架和所需的電源和網絡電纜，到您提供的地址。運送伺服器的包裝盒尺寸如下：

- 2U 伺服器的包裝盒：
  - 長度：約 44 英寸
  - 高：26.5 英吋 / 67.3 公分
  - 寬：17 英吋 / 43.2 公分
- 1U 伺服器的包裝盒：
  - 長：34.5 英吋 / 87.6 公分
  - 高：24 英吋 / 61 公分
  - 寬：9 英吋 / 22.9 公分

您的團隊或第三方供應商必須安裝設備。如需詳細資訊，請參閱 Outpost 伺服器安裝。

當您確認 Outposts 伺服器的 Amazon EC2 容量可從您的 AWS 帳戶取得時，即表示安裝完成。

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
- Outpost 伺服器安裝
- 在 Outpost 伺服器上啟動執行個體

建立 Outpost 並訂購 Outpost 容量

要開始使用 AWS Outposts，請使用擁有前哨的 AWS 帳戶登錄。建立站點和 Outpost。然後，為您需要的 Outpost 伺服器下訂單。

必要條件

- 檢閱 Outpost 伺服器的可用配置。
- 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 Outposts 服器的站台需求。
- 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。操作地址是您將安裝和執行 Outpost 伺服器的位置。建立網站後，為您的網站 AWS Outposts 指派 ID。您必須在建立 Outpost 時指定此站點。

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 僅限伺服器。
7. 輸入站點的名稱、描述和營運地址。
8. (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。
9. 選擇 Create site (建立網站)。

步驟 2：建立 Outpost

為每部伺服器建立一個 Outpost。一個 Outpost 只能與一部伺服器建立關聯。您將在下訂單時指定此 Outpost。

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 Servers (伺服器)。
4. 輸入 Outpost 的名稱和描述。

5. 選擇 Outpost 的可用區域。
6. 針對 站點 ID，選擇您的站點。
7. 選擇 建立 Outpost。

步驟 3：下訂單

為您需要的 Outposts 服務器下訂單。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。如果您選擇預付部分費用或不預付任何費用的付款選項，您將分三年期每月支付費用。

  定價包括運輸、基礎設施服務維護，以及軟體修補和升級。
- 確定運送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 伺服器。
4. 若要新增容量，請選擇一種配置。
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

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。

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。

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，請聯絡 Sup AWS port 部門。

為了履行訂單， AWS 將安排交貨日期。

您必須負責所有安裝任務，包括實體安裝和網路組態。您可以將這些任務交由第三方承包執行。無論您是自行執行安裝還是交由第三方承包，安裝都需要包含 Outpost 之 中的 IAM 憑證，以驗證新裝置的身分。 AWS 帳戶 您必須負責提供和管理此存取權。如需詳細資訊，請參閱 the section called “Outpost 伺服器安裝”。

當您可從 AWS 帳戶使用 Outpost 的 Amazon EC2 容量時，安裝即完成。容量可供使用之後，您就可以在 Outpost 伺服器上啟動 Amazon EC2 執行個體。如需詳細資訊，請參閱 the section called “啟動執行個體”。

Outpost 伺服器安裝

當您訂購 Outpost 伺服器時，您必須負責安裝 (無論是自行完成還是交由第三方承包)。安裝方需要特定許可才能驗證新裝置的身分。如需詳細資訊，請參閱《授予許可》。

先決條件

您的站點必須具備 Outpost 伺服器形式規格。如需詳細資訊，請參閱 建立 Outpost 並訂購 Outpost 容量。

> **Note**
>
> 我們建議您在安裝程序之前和期間檢視安裝 AWS Outposts 伺服器訓練影片。若要存取培訓，您必須在 AWS Skill Builder 上進行登入或建立帳戶。

任務

- 步驟 1：授予許可
- 步驟 2：檢查
- 步驟 3：機架安裝
- 步驟 4：開啟電源
- 步驟 5：連線網路
- 步驟 6：授權伺服器
- Outpost 組態工具命令參考

步驟 1：授予許可

為了驗證新裝置的身分，您必須具有包含 Outpost 之 AWS 帳戶 中的 IAM 憑證。AWSOutpostsAuthorizeServerPolicy 政策會授予安裝 Outpost 伺服器所需之許可。如需詳細資訊，請參閱 the section called “身分與存取管理”。

考量事項

- 如果您使用的第三方無法訪問您的 AWS 帳戶，則必須提供臨時訪問權限。
- AWS Outposts 支援使用臨時認證。您可以設定最多持續 36 小時的臨時憑證。確保提供安裝人員足夠的時間來執行伺服器安裝的所有步驟。如需詳細資訊，請參閱 the section called “臨時憑證”。

步驟 2：檢查

若要完成 Outpost 設備的檢查，您應該檢查運送包裝是否有損壞、打開運送包裝，並找到 Nitro 安全金鑰 (NSK)。請考慮下列有關檢查伺服器的資訊：

- 運送包裝箱的最大兩側有震動感應器。

- 運送包裝箱蓋內側包含有關如何取出伺服器及尋找 NSK 的說明。
- NSK 是一個加密模組。若要完成檢查，請「找到」NSK。您會在稍後的步驟中將 NSK 安裝到伺服器。

檢查運送包裝

檢查運送包裝

- 打開運送包裝之前，請觀察兩個震動感應器，並注意其是否已啟動。如果震動感應器已啟動，裝置可能已損壞。請繼續進行安裝，並花時間注意伺服器或配件是否有任何其他損壞。如果系統的任何部分明顯損壞或安裝無法如預期繼續，請聯絡 Sup AWS port 部門以取得更換 Outposts 伺服器的指導。

如果感應器中間的橫條呈現紅色，則表示感應器已啟動。

打開運送包裝

打開運送包裝

- 打開包裝，並確定其包含下列項目：
  - Server
  - Nitro 安全金鑰 (加密模組) – 以紅色標示 "NSK" 的包裝。如需詳細資訊，請參閱以下有關從運送包裝尋找 NSK 的程序。
  - 機架安裝工具套組 (2 個內側導軌、2 個外側導軌以及螺絲)
  - 安裝手冊
  - 配件套組
    - 一對 C13/14 電源線 - 10 英呎 (3 公尺)
    - QSFP 分接線 - 10 英呎 (3 公尺)
    - USB 纜線 (micro-USB 轉 USB-C) - 10 英呎 (3 公尺)
    - 護刷

尋找 NSK

NSK 位於標示為 A、內含伺服器配件的盒內。

> **Important**
>
> 請勿在安裝期間使用 NSK 銷毀伺服器上的資料。

啟動伺服器需要 NSK。當您將伺服器送回時，也會使用此 NSK 來銷毀伺服器上的資料。在此安裝步驟中，請忽略 NSK 主體上的說明，因為這些說明是用於銷毀資料。

步驟 3：機架安裝

若要完成此步驟，您必須將內側導軌安裝到伺服器、將外側導軌安裝到機架，然後將伺服器安裝在機架上。您需要十字螺絲起子，才能完成這些步驟。

機架安裝替代方案

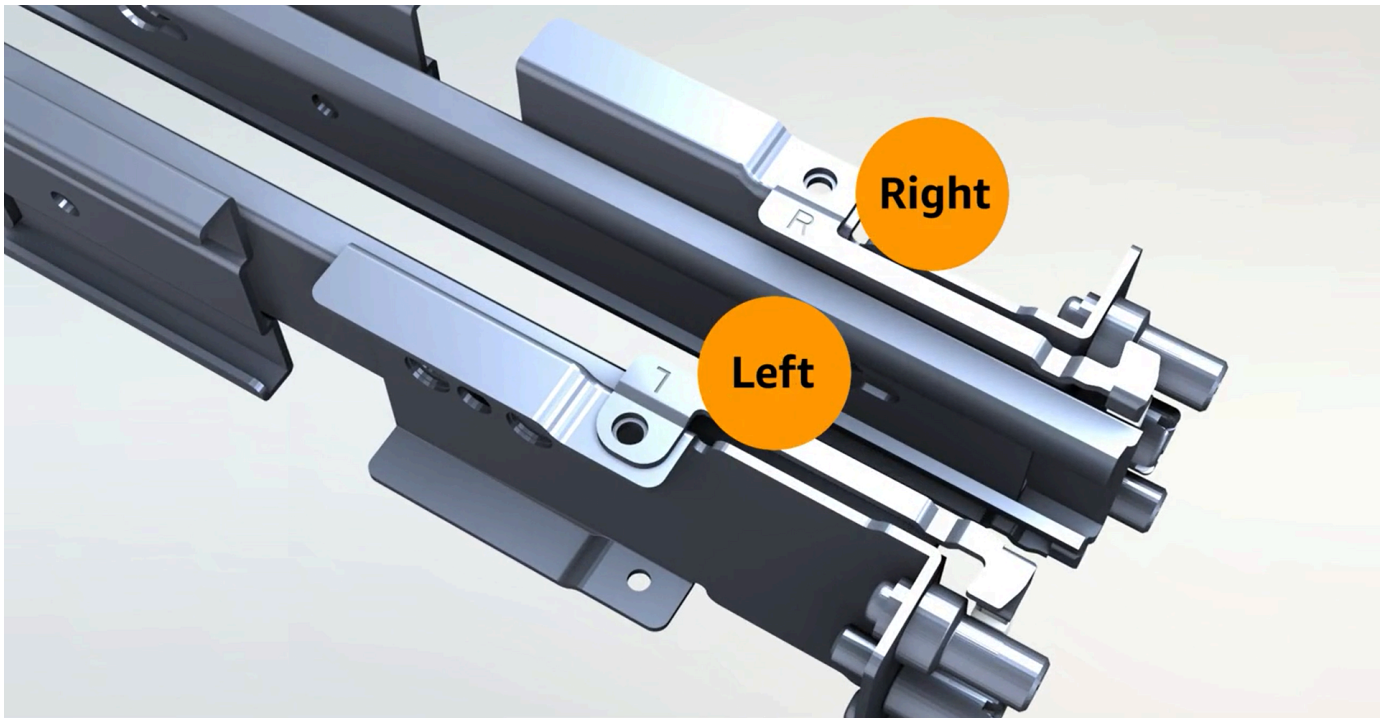
您不需要將伺服器安裝在機架中。如果您未將伺服器安裝在機架中，請考慮下列資訊：

- 確保伺服器與伺服器前後方的牆壁之間至少有 6 英吋 (15 公分) 的間隙，以便讓熱空氣流通。
- 將伺服器放在穩固的表面上，避免潮濕或掉落物體等機械危害。
- 若要使用伺服器隨附的網路線，您必須將伺服器放在距離上游網路裝置 10 英呎 (3 公尺) 的範圍內。
- 遵循當地的抗震支撐和焊接指引。

確定兩側和前後端

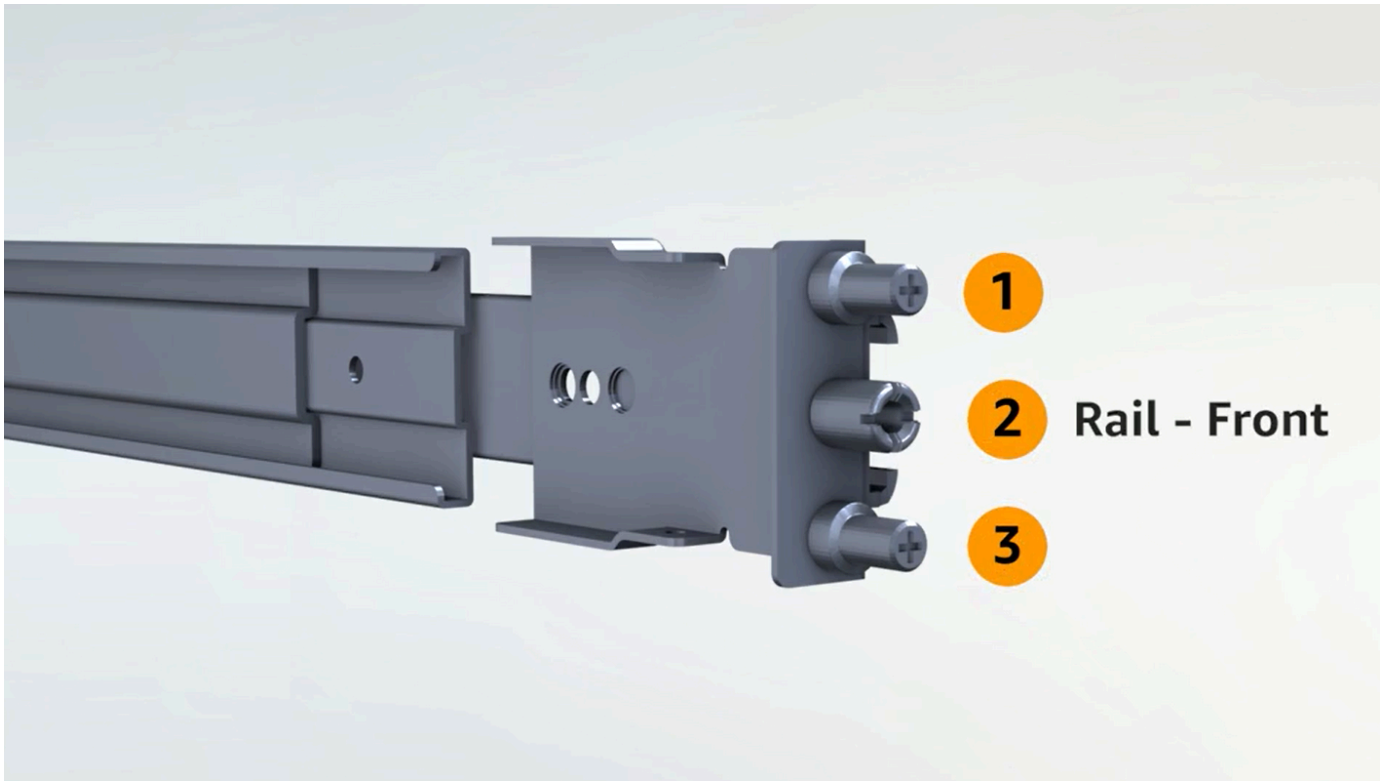
確定左右和前後

1. 找到裝有伺服器隨附機架導軌的盒子，並打開盒子。
2. 查看導軌上的標記以判斷左右。這些標記會決定每個導軌要安裝到伺服器的哪一側。

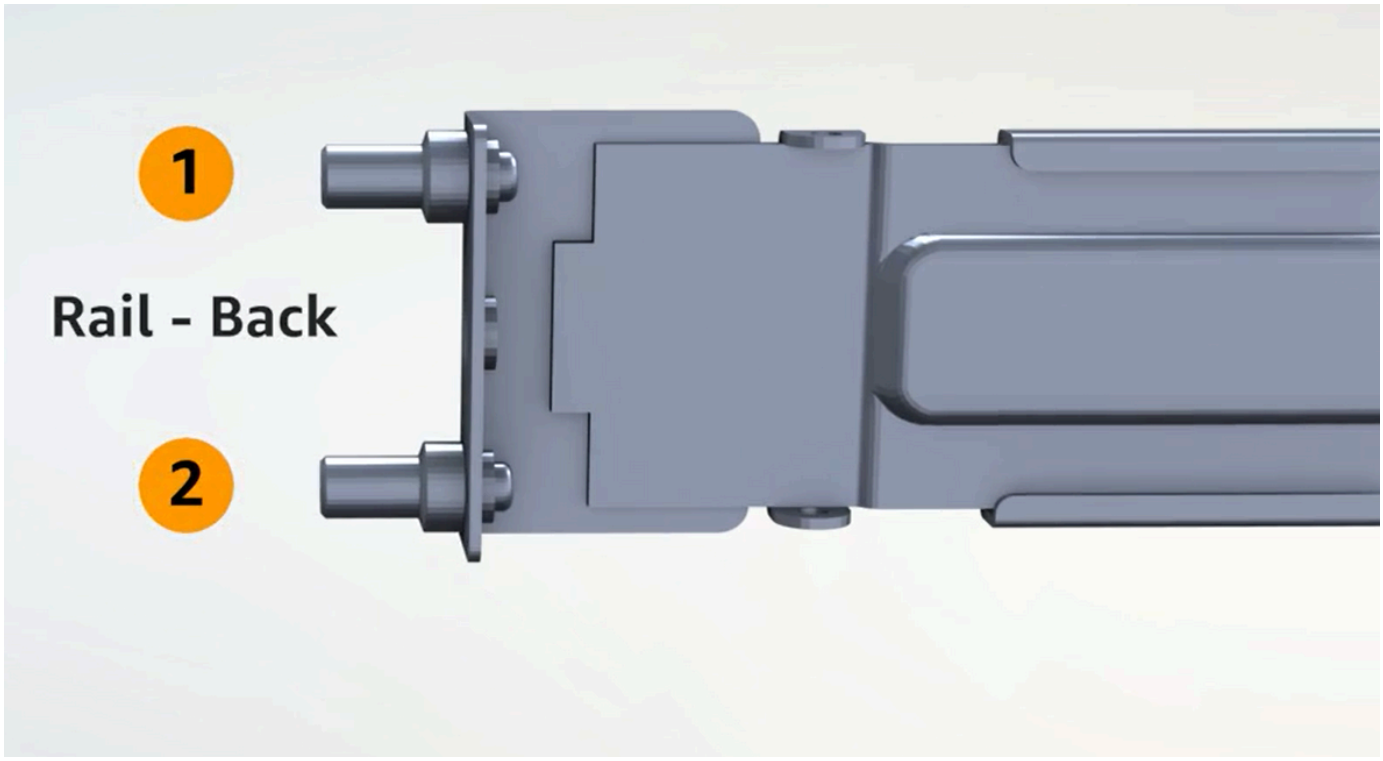


3. 查看導軌兩端的接桿以判斷前後。

   前端有三個接桿。



後端有兩個接桿。



安裝內側導軌

將內側導軌安裝到伺服器

1. 將兩個導軌的內側導軌與外側導軌分離。您應該有四個導軌。
2. 將右內側導軌安裝到伺服器的右側，然後用螺絲固定導軌。確定導軌依正確方向安裝到伺服器。將導軌的前部指向伺服器的前側。
3. 將左內側導軌安裝到伺服器的左側，然後用螺絲固定導軌。

安裝外側導軌

將外側導軌安裝到機架

1. 面對機架，並使用機架右側標示為 R 的導軌。先將導軌後端安裝到機架，再延伸導軌以將其固定到機架前側。

   > **Tip**
   >
   > 請注意導軌的方向。如有必要，請使用隨附的針腳接頭。

2. 重複步驟，將左導軌安裝到左側。

安裝伺服器

將伺服器安裝在機架中

- 將伺服器滑入在上一個步驟中安裝在機架上的外側導軌，並用兩顆隨附的螺絲固定伺服器前側。

  > **Tip**
  >
  > 需要兩個人將伺服器滑入機架。

步驟 4：開啟電源

若要完成開啟電源，請安裝 NSK、將伺服器連接到電源，然後確認伺服器已開啟電源。請考慮下列有關開啟伺服器電源的資訊：

- 伺服器使用一個電源，但 AWS 建議您使用兩個電源來進行備援。

- 請先連接電源線，再連接網路線。
- 使用 C13 插座/C14 插座電源線組，將伺服器連接到機架上的電源供應器。如果您未使用 C14 插座電源線，將伺服器連接到機架上的電源供應器，則必須為連接到電源的 C14 插座提供整流器。

安裝 NSK

您必須將 NSK 安裝到伺服器，以便在操作期間解密伺服器上的資料。

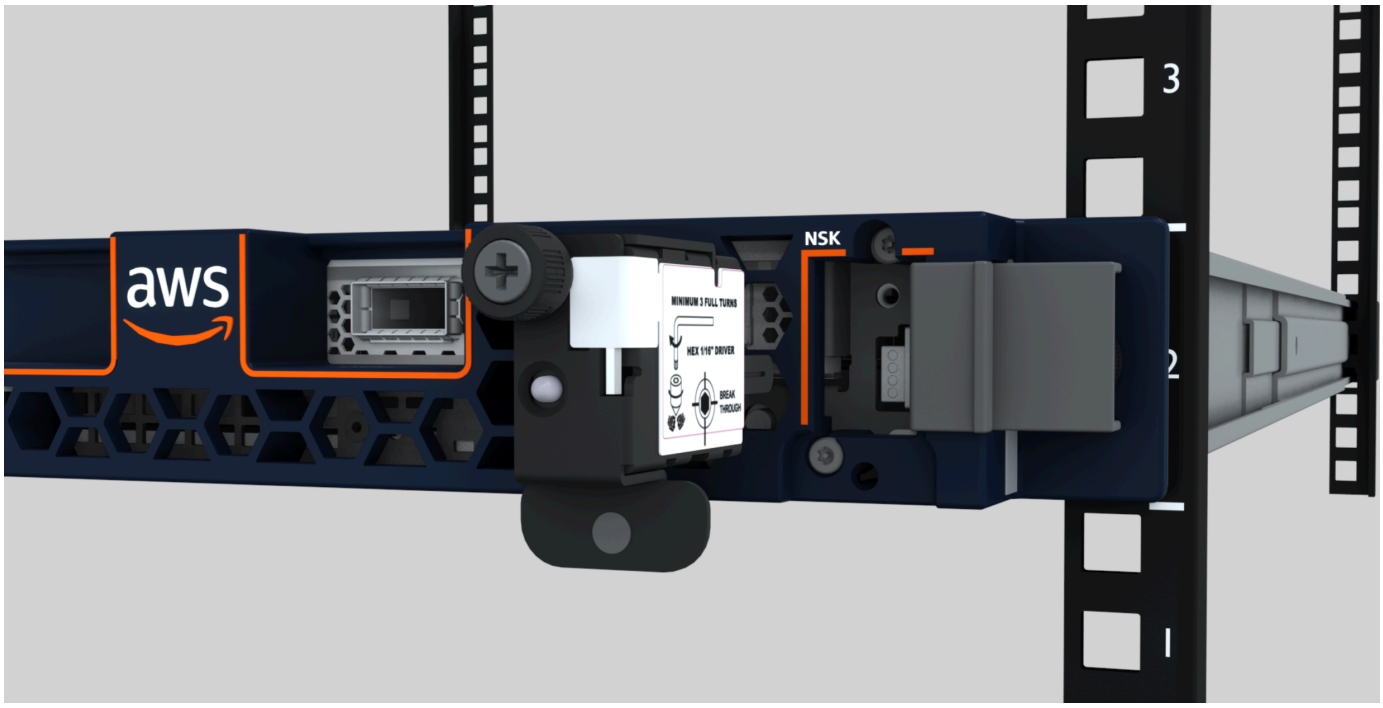
> **Important**
>
> - NSK 的一側有關於如何銷毀 NSK 的說明。目前不用遵循這些說明。只有在將伺服器退回 AWS時，才需要遵循這些說明以密碼編譯方式銷毀伺服器上的資料。
> - 如果您要同時安裝多部伺服器，請確定不要混淆 NSK。您必須將 NSK 安裝到隨附 NSK 的伺服器。如果您使用不同的 NSK，伺服器將無法啟動。

安裝 NSK

1. 在伺服器的右前側，打開 NSK 插槽。

   下圖顯示安裝到 2U 伺服器的 NSK。

下圖顯示安裝到 1U 伺服器的 NSK。

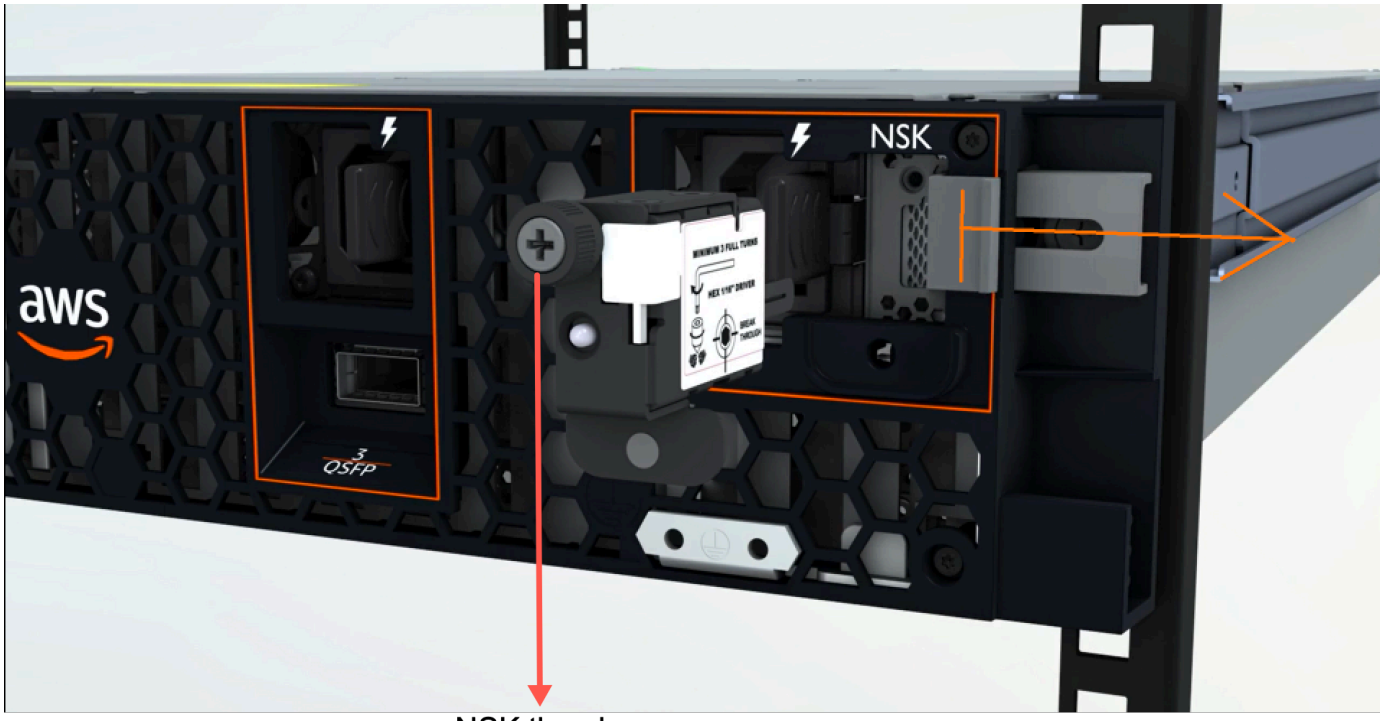


2. 確認 NSK 上的序號 (SN) 與伺服器 NSK 插槽擋板拉出式卡片上的 SN 相符。

   下圖顯示 NSK 和擋板拉出式卡片上的 SN 號碼：

3. 將 NSK 裝入插槽。
4. 使用指旋螺絲徒手栓緊，或使用螺絲起子 (0.7 Nm/0.52 lb-ft) 拴緊到緊貼程度。請勿使用電動工具，因為這可能會過度扭緊而損壞 NSK。

   下圖顯示指旋螺絲的位置。



NSK thumbscrew

下圖顯示可用來將 NSK 安裝到伺服器的螺絲起子類型。

開啟電源

將伺服器連接到電源

1. 找到伺服器隨附的一對 C13/C14 電源線。

2. 將兩條纜線的 C14 端連接到電源。
3. 將兩條纜線的 C13 端連接到伺服器前方的連接埠。

驗證伺服器電源

確認伺服器是否有電源

1. 確認您可以聽到伺服器的運轉聲。

> **Tip**
>
> 在伺服器自行佈建之後，噪音程度就會降低。

2. 確認電源連接埠上方的 LED 電源指示燈亮起。

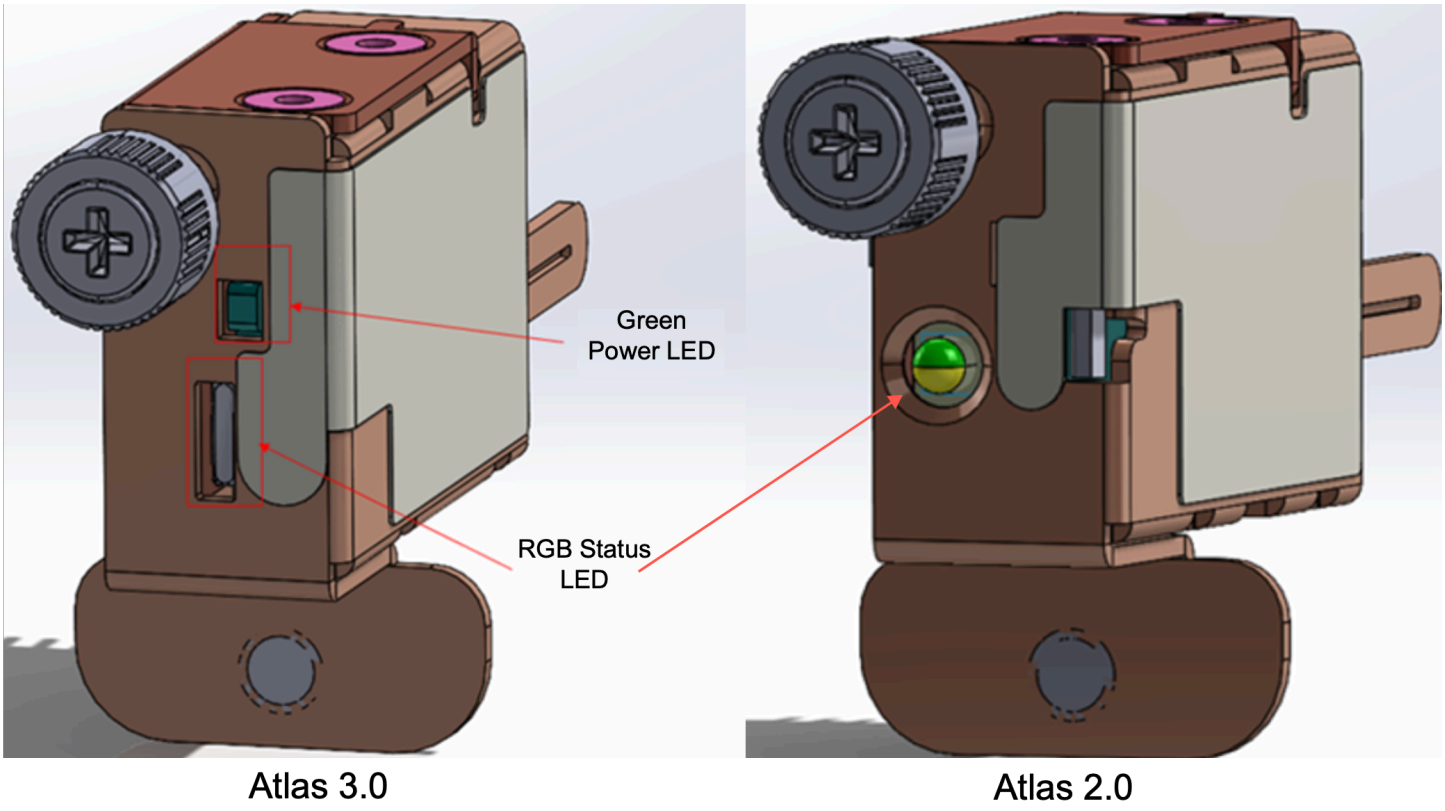
下圖顯示 2U 伺服器上的 LED 電源指示燈

下圖顯示 1U 伺服器上的 LED 電源指示燈

檢查阿特拉斯 3.0 上的電源指示燈。NSK

AWS Outposts 支持兩個版本的 NSK：阿特拉斯 2.0 和阿特拉斯 3.0。兩種 NSK 版本都有一個 RGB 狀態指示燈。此外，阿特拉斯 3.0 有一個綠色的電源 LED。這一步僅適用於阿特拉斯 3.0 NSK.

下圖顯示了阿特拉斯 2.0 和阿特拉斯 3.0 NSK 的 LED 的位置：



如果您有 Atlas 2.0 NSK，請跳至下一個步驟，步驟 5：連線網路因為此版本的 NSK 只有 RGB 狀態 LED，您必須在前哨伺服器佈建並啟動後檢查這個指示燈。

如果你有阿特拉斯 3.0 NSK，檢查綠色電源指示燈：

- 如果綠燈亮起，則表示 NSK 已正確連接到主機並具有電源。您可以繼續進行下一步。
- 如果綠燈熄滅，表示 NSK 未正確連接到主機或/且沒有電源。聯繫 AWS Support。

步驟 5：連線網路

若要完成網路設定，請使用網路線將伺服器連接到上游網路裝置。

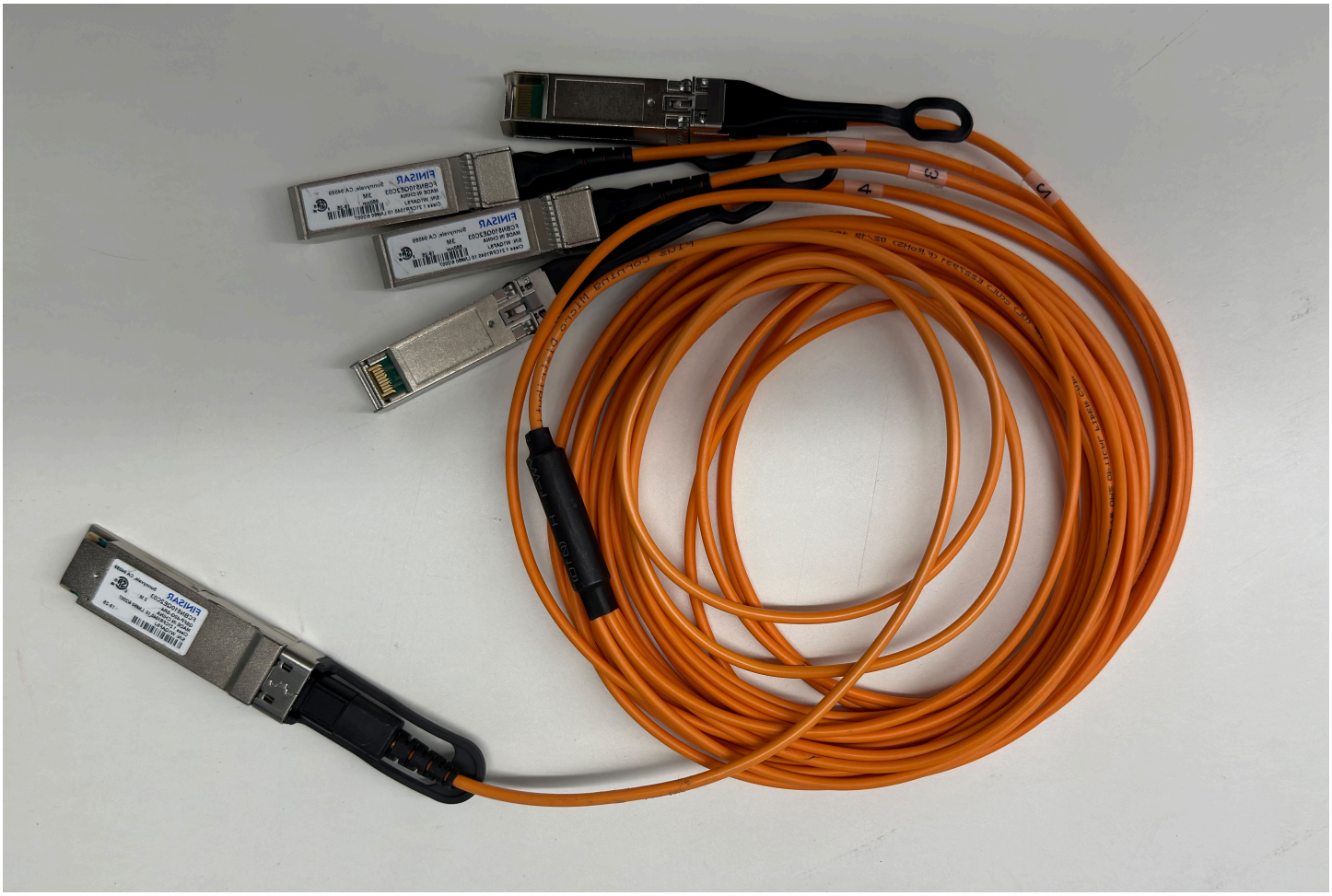
請考慮下列有關連線到網路的資訊：

- 伺服器需要連線兩種類型的流量：服務連結流量和本機網路介面 (LNI) 連結流量。下節中的指示說明要在伺服器上使用哪些連接埠來分段流量。請向您的 IT 群組諮詢，以確定每種類型的流量應由上游網路裝置上的哪個連接埠承載。
- 確保伺服器已連接到您的上游網路裝置，並已獲指派 IP 地址。如需詳細資訊，請參閱 伺服器 IP 地址指派。
- AWS Outposts 伺服器上的光纖連線僅支援 10 Gb，不支援連接埠速度的自動交涉。如果主機連接埠嘗試交涉連接埠速度 (例如介於 10 到 25 Gbits 之間)，您可能會遇到問題。在此情況下，建議您執行下列動作：
  - 將交換器連接埠上的連接埠速度設定為 10 Gbits。
  - 請與您的交換器廠商合作以支援靜態組態。

設定 QSFP 網路

透過 QSFP 分接線，您可以利用分接來分段流量。

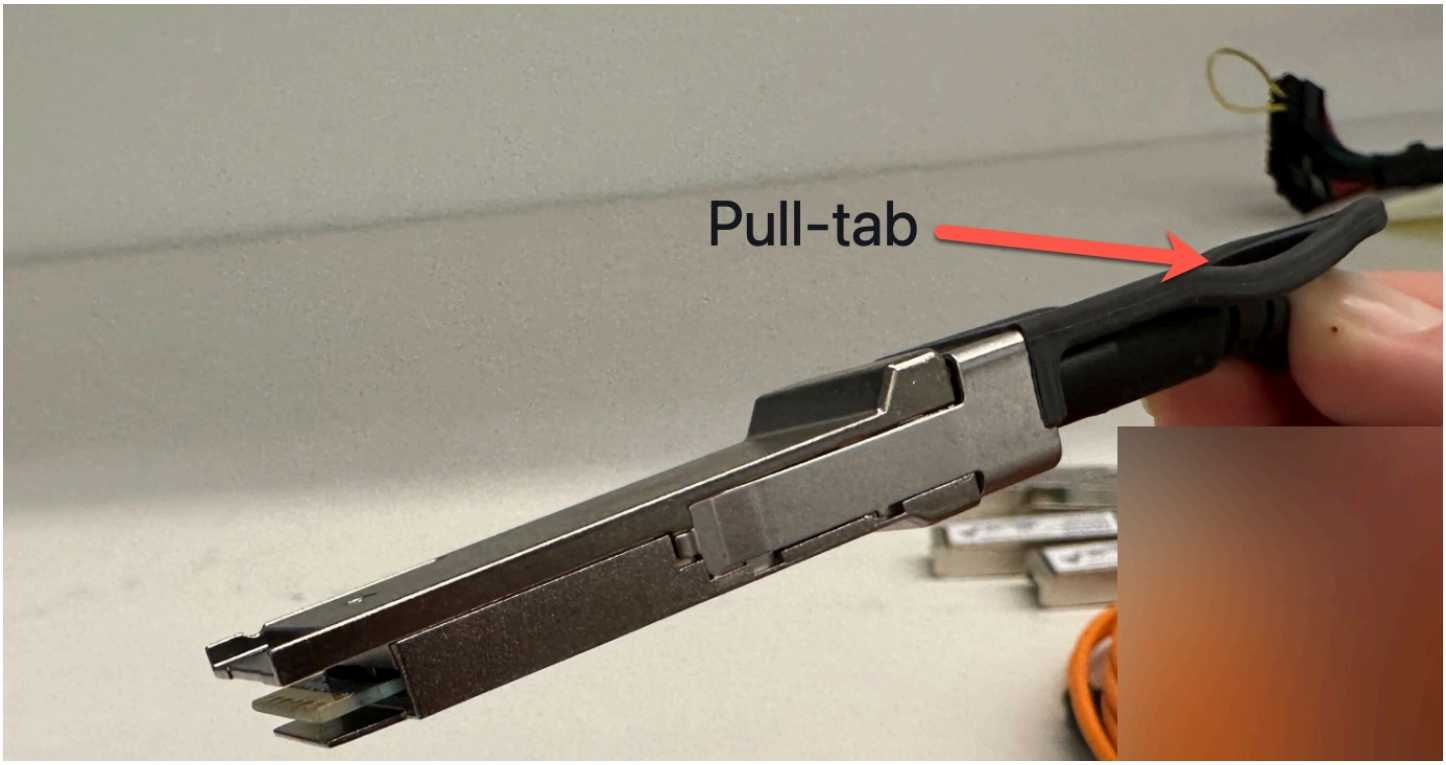
下圖顯示 QSFP 分接線：



> **Note**
>
> AWS Outposts 伺服器在 QSFP 連接埠旁邊有一個實體 RJ45 連接埠。但是，此 RJ45 連接埠並未啟用供任何客戶使用。如果您需要 RJ45 1GbE 連線能力，請使用隨附的 QSFP 纜線將 10 GBASE-X SFP 連接至 1GBe RJ45 媒體轉換器。

QSFP 纜線的一端具有單一接頭。將此端連接到伺服器。

下圖顯示具有單一接頭的纜線端：



QSFP 纜線的另一端具有 4 條分接線，標示為 1 到 4。將標示為 1 的纜線用於 LNI 連結流量，並將標示為 2 的纜線用於服務連結流量。

下圖顯示具有 4 條分接線的纜線端：

使用 QSFP 分接線將伺服器連線到網路

1. 找到伺服器隨附的 QSFP 分接線。
2. 將 QSFP 分接線的一端連接到伺服器上的 QSFP 連接埠。

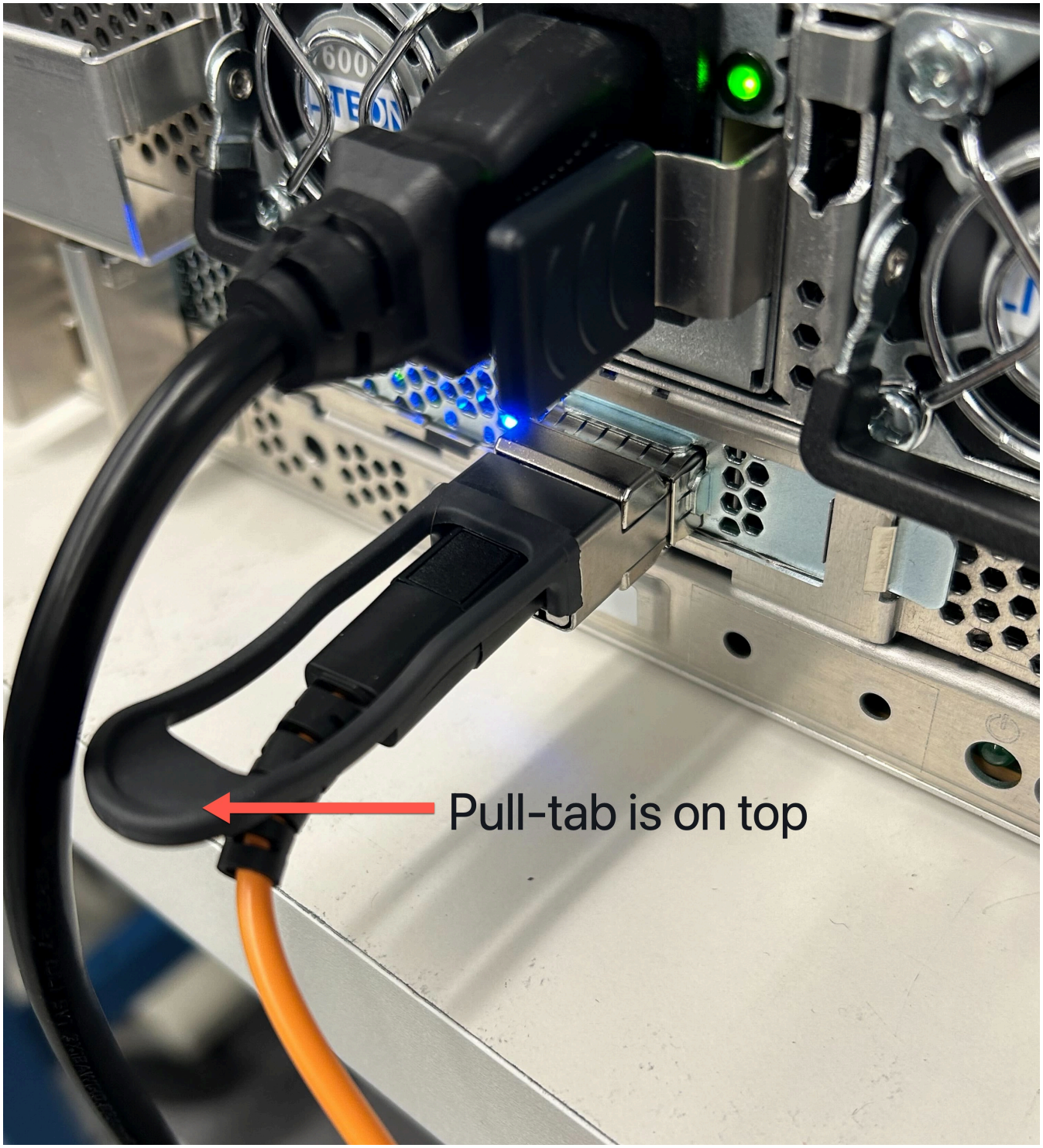
    1. 找到 QSFP 連接埠。

        下圖顯示 2U 伺服器上 QSFP 連接埠的位置。

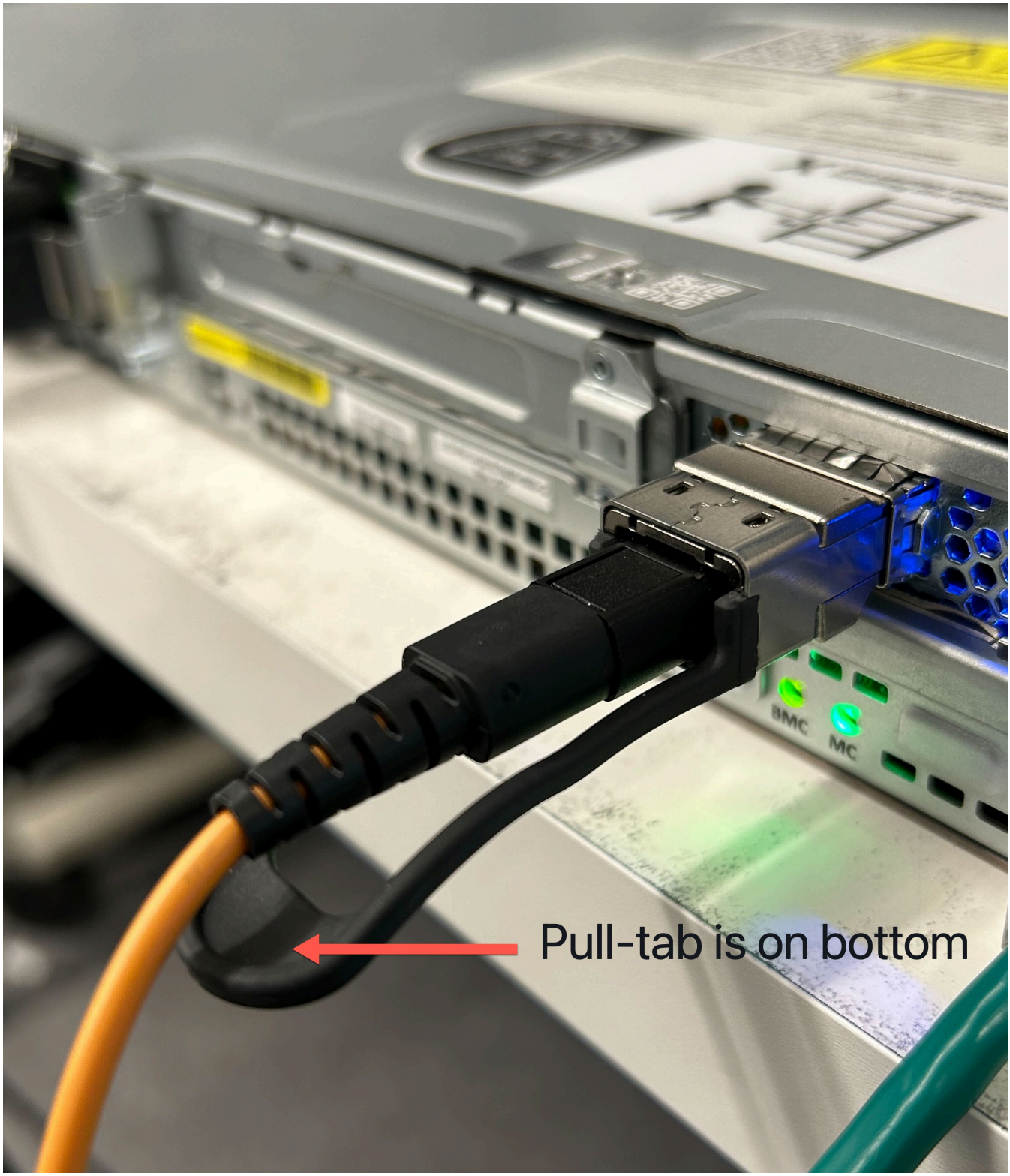
下圖顯示 1U 伺服器上 QSFP 連接埠的位置。

2. 將拉片朝正確方向插入 QSFP。

   若是 2U 伺服器，請將拉片朝上插入 QSFP，如下圖所示。



若是 1U 伺服器，請將拉片朝下插入 QSFP，如下圖所示。



3. 確保您在插入纜線時感覺到或聽到喀噠聲。這表示您已正確插入纜線。

3. 將 QSFP 纜線的分接線 1 和 2 連接到上游網路裝置。

> **Important**
>
> Outpost 伺服器需要有下列兩條纜線才能運作。
>
> - 將標示為 1 的纜線用於 LNI 連結流量。
> - 將標示為 2 的纜線用於服務連結流量。

步驟 6：授權伺服器

若要授權伺服器，您必須使用 USB 纜線將筆記型電腦連接到伺服器，然後使用命令型序列協定來測試連線並授權伺服器。除了 IAM 憑證之外，您還需要 USB 纜線、筆記型電腦和序列終端軟體 (例如 PuTTY 或 screen)，才能完成這些步驟。

或者，如果您的 Android 手機或平板電腦具有支援 USB On The Go (OTG) 的 USB-C 或 micro-USB 接頭，也可以使用 Outpost Server Activator 應用程式來逐步引導您完成伺服器授權程序。您可以從谷歌播放下載該應用

請考慮下列有關授權伺服器的資訊：

- 若要授權伺服器，您或安裝伺服器的一方需要包含 Outpost AWS 帳戶 的 IAM 登入資料。如需詳細資訊，請參閱 the section called “步驟 1：授予許可”。
- 您不需要使用 IAM 憑證進行驗證即可測試連線。
- 在使用匯出命令將 IAM 憑證設定為環境變數之前，請考慮測試連線。
- 為了保護您的帳戶，Outpost 組態工具永遠不會儲存您的 IAM 憑證。
- 若要將筆記型電腦連接到伺服器，請一律將 USB 纜線先插入您的筆記型電腦，再插入伺服器。

任務

- 將您的筆記型電腦連接到伺服器
- 建立與伺服器的序列連線
- 測試連線
- 授權伺服器
- 驗證 NSK 指示燈

將您的筆記型電腦連接到伺服器

將 USB 纜線先連接到您的筆記型電腦，再連接到伺服器。伺服器內含 USB 晶片，可在筆記型電腦上建立虛擬序列埠供您使用。您可以使用此虛擬序列埠來連線到具有序列終端模擬軟體的伺服器。您只能使用此虛擬序列埠來執行 Outpost 組態工具命令。

將筆記型電腦連接到伺服器

將 USB 纜線先插入您的筆記型電腦，再插入伺服器。

> **Note**
>
> USB 晶片需要驅動程式才能建立虛擬序列埠。您的作業系統應該會自動安裝所需的驅動程式 (若尚未存在)。若要下載並安裝驅動程式，請參閱 FTDI 的 Installation Guides。

建立與伺服器的序列連線

本節包含使用常見序列終端程式的說明，但您不需要使用這些程式。請使用具有 `115200` 傳輸速率連線速度的偏好序列終端程式。

範例

- Windows 序列連線
- Mac 序列連線

Windows 序列連線

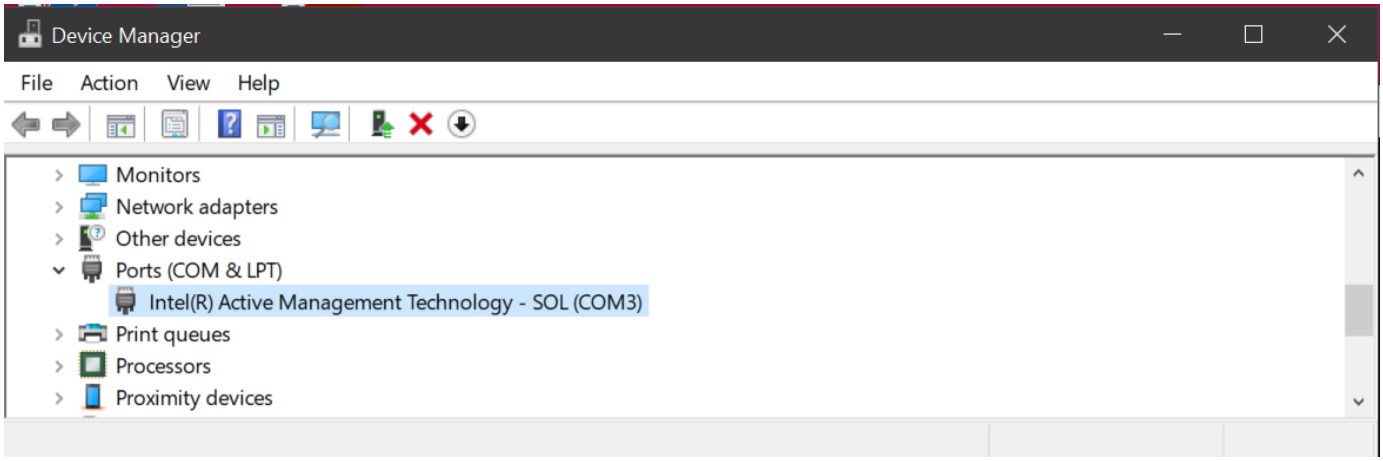
下列說明適用於 Windows 上的 PuTTY。PuTTY 是免費的，但您可能必須自行下載。

下載 PuTTY

從 PuTTY 下載頁面下載並安裝 PuTTY。

使用 PuTTY 在 Windows 上建立序列終端

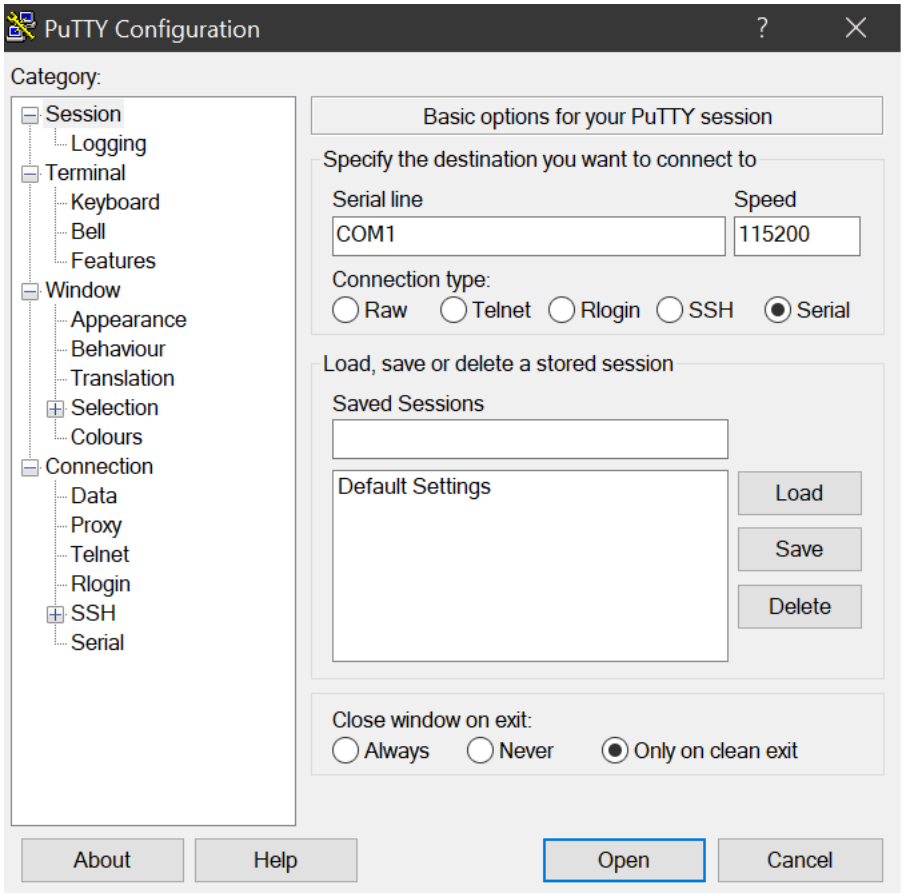
1. 將 USB 纜線先插入您的 Windows 筆記型電腦，再插入伺服器。
2. 從桌面，以滑鼠右鍵按一下 開始，然後選擇 裝置管理員。
3. 在 裝置管理員 中，展開 連接埠 (COM 和 LPT) 以確定 USB 序列連線的 COM 連接埠。您將看到一個名為 USB 序列埠 (COM#) 的節點。COM 連接埠的值取決於您的硬體。



4. 在 PuTTY 中，從 工作階段 選擇 序列 作為 連線類型，然後輸入下列資訊：

   - 在 序列線路 下，輸入裝置管理員中的 COM# 連接埠。
   - 在 速度 下，輸入：115200

   下圖顯示 PuTTY 設定 頁面上的範例：



5. 選擇 Open (開啟)。

空白主控台視窗隨即出現。可能需要 1 到 2 分鐘才會顯示下列其中一項：

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

Mac 序列連線

下列說明適用於 macOS 上的 screen。您可以找到作業系統隨附的 screen。

使用 screen 在 macOS 上建立序列終端

1. 將 USB 纜線先插入您的 Mac 筆記型電腦，再插入伺服器。
2. 在終端中，對輸出使用 `*usb*` 篩選列出 `/dev` 以尋找虛擬序列埠。

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

序列裝置會顯示為 `tty`。例如，考慮以下來自上一個列出命令的範例輸出：

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

3. 在終端中，使用 screen 搭配序列裝置和序列連線的傳輸速率來設定序列連線。在下列命令中，將 *EXAMPLE1* 更換為您筆記型電腦中的值。

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

空白主控台視窗隨即出現。可能需要 1 到 2 分鐘才會顯示下列其中一項：

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

測試連線

本節說明如何使用 Outpost 組態工具來測試連線。您不需要 IAM 憑證即可測試連線。您的連線必須能夠解析 DNS 才能存取 AWS 區域。

1. 測試連結並收集連線的相關資訊
2. 測試 DNS 解析程式
3. 測試訪問 AWS 區域

測試連結

1. 將 USB 纜線先插入您的筆記型電腦，再插入伺服器。
2. 使用序列終端程式 (例如 PuTTY 或 screen) 連線到伺服器。如需詳細資訊，請參閱 the section called “建立與伺服器的序列連線”。
3. 按下 Enter 以存取 Outpost 組態工具命令提示。

```
Outpost>
```

> **Note**
>
> 如果在開啟電源之後於伺服器左側機箱內看到紅燈持續亮著，且無法連線到 Outpost 組態工具，您可能需要關閉電源並耗盡伺服器電力才能繼續。若要耗盡伺服器電力，請拔除所有網路線和電源線，等待五分鐘，然後開啟電源並重新連線網路。

4. 使用 describe-links 傳回伺服器上網路連結的相關資訊。Outpost 伺服器必須有一個服務連結和一個本機網路介面 (LNI) 連結。

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

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

如果有任一連結收到 `connected: False`，請針對硬體上的網路連線進行疑難排解。

5. 使用 describe-ip 傳回服務連結的 IP 指派狀態和組態。

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

NTP 值可能會遺失，因為 NTP 在 DHCP 選項組中是選擇性的。您應該沒有其他遺失值。

測試 DNS

1. 將 USB 纜線先插入您的筆記型電腦，再插入伺服器。
2. 使用序列終端程式 (例如 PuTTY 或 screen) 連線到伺服器。如需詳細資訊，請參閱 the section called “建立與伺服器的序列連線”。
3. 按下 Enter 以存取 Outpost 組態工具命令提示。

```
Outpost>
```

> **Note**
>
> 如果在開啟電源之後於伺服器左側機箱內看到紅燈持續亮著，且無法連線到 Outpost 組態工具，您可能需要關閉電源並耗盡伺服器電力才能繼續。若要耗盡伺服器電力，請拔除所有網路線和電源線，等待五分鐘，然後開啟電源並重新連線網路。

4. 使用 export 輸入 Outpost 伺服器的父區域作為 `AWS_DEFAULT_REGION` 的值。

AWS_DEFAULT_REGION=##

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

result: OK
checksum: 0xB2A945RE
```

- 等號 (=) 前後請勿加上空格。
- 不會儲存任何環境值。 AWS 區域 每次執行 Outpost 設定工具時，都必須匯出。
- 如果您使用第三方安裝伺服器，則必須向第三方提供父區域。

5. 使用 describe-resolve 確定 Outpost 伺服器是否可以連線到 DNS 解析程式，並解析區域中 Outpost 組態端點的 IP 地址。至少需要一個 IP 組態的連結。

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

若要測試存取權 AWS 區域

1. 將 USB 纜線先插入您的筆記型電腦，再插入伺服器。
2. 使用序列終端程式 (例如 PuTTY 或 screen) 連線到伺服器。如需詳細資訊，請參閱 the section called “建立與伺服器的序列連線”。
3. 按下 Enter 以存取 Outpost 組態工具命令提示。

```
Outpost>
```

> **Note**
>
> 如果在開啟電源之後於伺服器左側機箱內看到紅燈持續亮著，且無法連線到 Outpost 組態工具，您可能需要關閉電源並耗盡伺服器電力才能繼續。若要耗盡伺服器電力，請拔除所有網路線和電源線，等待五分鐘，然後開啟電源並重新連線網路。

4. 使用 export 輸入 Outpost 伺服器的父區域作為 AWS_DEFAULT_REGION 的值。

   AWS_DEFAULT_REGION=##

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

   result: OK
   checksum: 0xB2A945RE
   ```

   - 等號 (=) 前後請勿加上空格。
   - 不會儲存任何環境值。 AWS 區域 每次執行 Outpost 設定工具時，都必須匯出。
   - 如果您使用第三方安裝伺服器，則必須向第三方提供父區域。

5. 使用 describe-reachability 確定 Outpost 伺服器是否可以連線到區域中的 Outpost 組態端點。需要正常運作的 DNS 組態，您可以使用 describe-resolve 來確定。

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

   - is_reachable 表示測試的結果
   - src_ip 是伺服器的 IP 地址
   - dst_ip 是區域中 Outpost 組態端點的 IP 地址
   - dst_port 是伺服器用來連線到 dst_ip 的連接埠。

授權伺服器

本節說明如何使用 Outpost 組態工具以及包含 Outpost 之 AWS 帳戶中的 IAM 憑證來授權伺服器。

授權伺服器

1. 將 USB 纜線先插入您的筆記型電腦，再插入伺服器。
2. 使用序列終端程式 (例如 PuTTY 或 screen) 連線到伺服器。如需詳細資訊，請參閱 the section called “建立與伺服器的序列連線”。

3. 按下 Enter 以存取 Outpost 組態工具命令提示。

```
Outpost>
```

> **Note**
>
> 如果在開啟電源之後於伺服器左側機箱內看到紅燈持續亮著，且無法連線到 Outpost 組態工具，您可能需要關閉電源並耗盡伺服器電力才能繼續。若要耗盡伺服器電力，請拔除所有網路線和電源線，等待五分鐘，然後開啟電源並重新連線網路。

4. 使用 export 在 Outpost 組態工具中輸入您的 IAM 憑證。如果您使用第三方安裝伺服器，則必須向第三方提供 IAM 憑證。

   若要進行驗證，您必須匯出以下四個變數。請一次匯出一個變數。等號 (=) 前後請勿加上空格。

   - AWS_ACCESS_KEY_ID=*access-key-id*
   - AWS_SECRET_ACCESS_KEY=*secret-access-key*
   - AWS_SESSION_TOKEN=*session-token*
     - 使用 AWS CLI GetSessionToken命令來取得AWS_SESSION_TOKEN. 如需詳細資訊，請參閱《AWS CLI 命令參考》中的《get-session-token》。

       > **Note**
       >
       > 您必須將AWSOutpostsAuthorizeServerPolicy附加到 IAM 角色才能取得AWS_SESSION_TOKEN.

     - 若要安裝 AWS CLI，請參閱《Verrsion 2 AWS CLI 使用者指南》中的 < 安裝或更新最新版本的 AWS CLI > 。
   - AWS_DEFAULT_REGION=*##*

     使用 Outpost 伺服器的父區域作為 AWS_DEFAULT_REGION 的值。如果您使用第三方安裝伺服器，則必須向第三方提供父區域。

   下列範例中的輸出顯示成功匯出。

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
```

```
result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

5. 使用 start-connection 建立區域的安全連線。

   下列範例中的輸出顯示連線已成功啟動。

```
Outpost>start-connection

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

```
checksum: example-checksum
```

6. 等待約 5 分鐘。
7. 使用 get-connection 檢查是否已建立區域的連線。

   下列範例中的輸出顯示成功連線。

```
Outpost>get-connection


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

   在 keys_exchanged 和 connection_established 變更為 True 之後，Outpost 伺服器會自動佈建並更新為最新的軟體和組態。

> **Note**
>
> 請注意佈建程序的下列相關資訊：
>
> - 啟動完成之後，最多可能需要 10 小時才能使用 Outpost 伺服器。
> - 在此過程中，您必須保持 Outpost 伺服器的電源和網路處於連接且穩定的狀態。
> - 在此過程中，服務連結波動是正常的。

- 如果 `exchange_active` 為 `True`，則連線仍在建立中。請在 5 分鐘後重試。
- 如果 `keys_exchanged` 或 `connection_established` 為 `False`，且 `exchange_active` 為 `True`，則連線仍在建立中。請在 5 分鐘後重試。
- 如果 `keys_exchanged` 或 `connection_established` 在 1 小時後仍為 `False`，請聯絡 AWS Support 中心。
- 如果出`primary_status: No such asset id found.`現訊息，請確認下列事項：
  - 您指定了正確的區域。
  - 您使用的帳戶與用於訂購 Outpost 伺服器的帳戶相同。

  如果該地區正確，而且您使用的帳戶與訂購 Outpost 伺服器時所使用的帳戶相同，請聯絡AWS Support 中心。
- Outpost 的 `LifeCycleStatus` 屬性將從 `Provisioning` 轉換為 `Active`。然後，您將收到一封電子郵件，通知您已佈建和並啟動 Outpost 伺服器。
- 啟動 Outpost 伺服器之後，您不需要重新授權 Outpost 伺服器。

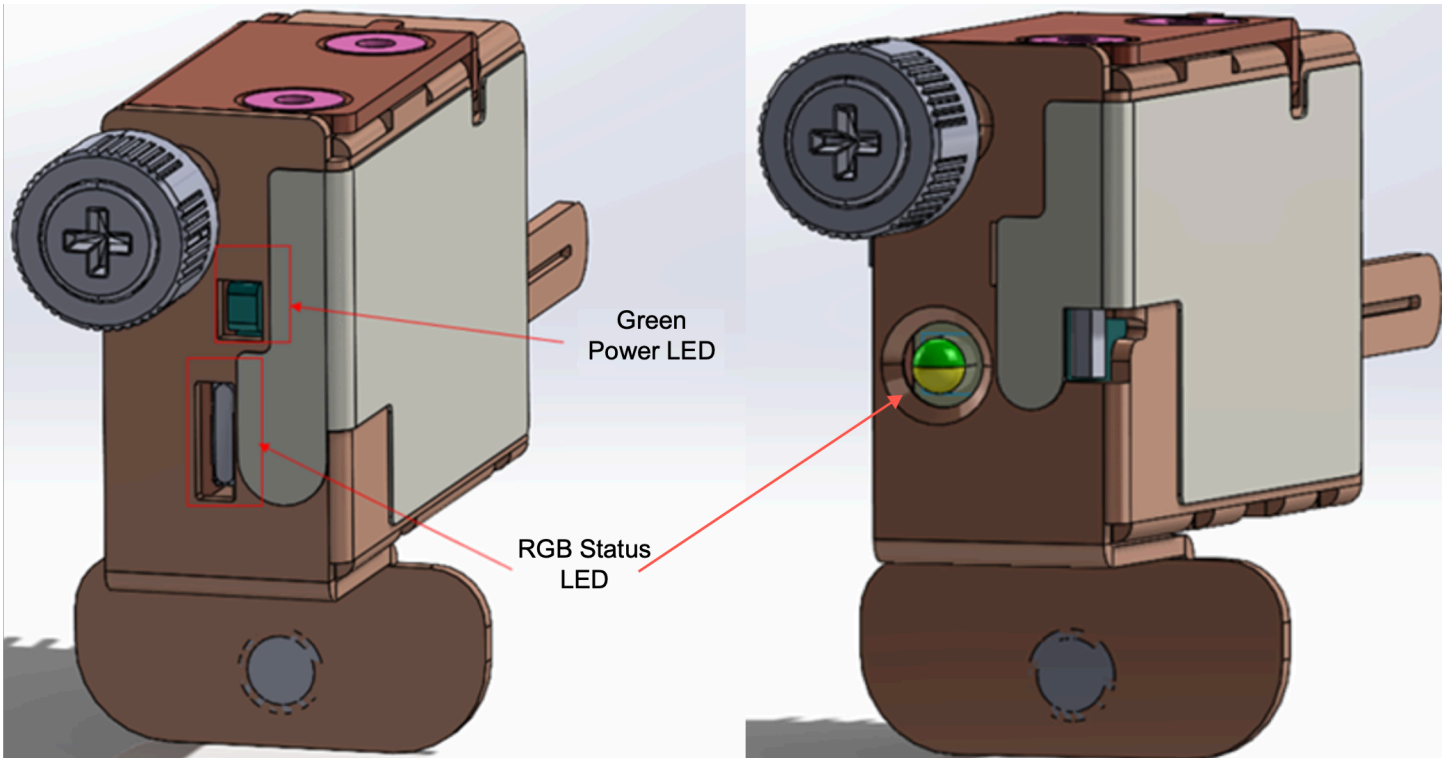
8. 成功連線之後，您可以中斷筆記型電腦和伺服器的連線。

驗證 NSK 指示燈

佈建程序完成後，請檢查 NSK LED。

AWS Outposts 支持兩個版本的 NSK：阿特拉斯 2.0 和阿特拉斯 3.0。兩種 NSK 版本都有一個 RGB 狀態指示燈。此外，阿特拉斯 3.0 有一個綠色的電源 LED。

下圖顯示了阿特拉斯 2.0 和阿特拉斯 3.0 的 LED 的位置：



Atlas 3.0 Atlas 2.0

驗證 NSK 上的狀態和電源指示燈

1. 檢查 RGB 狀態指示燈的顏色。如果顏色為綠色，則 NSK 是健康的。如果顏色不是綠色，請聯繫 AWS Support。
2. 如果你有一個阿特拉斯 3.0 NSK，檢查綠色電源指示燈。如果綠燈亮起，則表示 NSK 已正確連接到主機並具有電源。如果綠燈未亮起，請聯絡 AWS Support。

Outpost 組態工具命令參考

Outpost 組態工具提供下列命令。

命令

- 匯出
- 回應
- 描述連結
- 描述 IP
- 描述解析

- 描述可達性
- 啟動連線
- 取得連線

匯出

匯出

使用 export 將 IAM 憑證設定為環境變數。

語法

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

export 需要變數指派陳述式。

必須使用下列格式：*variable*=*value*

若要進行驗證，您必須匯出以下四個變數。請一次匯出一個變數。等號 (=) 前後請勿加上空格。

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

  使用 Outpost 伺服器的父區域作為 AWS_DEFAULT_REGION 的值。

Example ：成功的憑證匯入

```
Outpost>export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

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

result: OK
checksum: example-checksum
```

回應

回應

使用 echo 顯示您使用 export 命令為變數設定的值。

語法

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

variable-name 可為下列其中之一：

- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_SESSION_TOKEN
- AWS_DEFAULT_REGION

Example ：成功

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

result: OK
checksum: example-checksum

---

Outpost>echo $AWS_DEFAULT_REGION

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

Example ：因為未使用 export 命令設定變數值而失敗

```
Outpost> echo $AWS_ACCESS_KEY_ID

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

Example ：因為變數名稱無效而失敗

```
Oupost>echo $foo

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

Example ：因為語法問題而失敗

```
Outpost>echo AWS_SECRET_ACCESS_KEY

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

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

描述連結

describe-links

使用 describe-links 傳回伺服器上網路連結的相關資訊。Outpost 伺服器必須有一個服務連結和一個本機網路介面 (LNI) 連結。

語法

```
Outpost>describe-links
```

describe-links 不需要任何引數。

描述 IP

describe-ip

使用 describe-ip 傳回每個連線連結的 IP 指派狀態和組態。

語法

```
Outpost>describe-ip
```

describe-ip 不需要任何引數。

描述解析

describe-resolve

使用 describe-resolve 確定 Outpost 伺服器是否可以連線到 DNS 解析程式，並解析區域中 Outpost 組態端點的 IP 地址。至少需要一個 IP 組態的連結。

語法

```
Outpost>describe-resolve
```

describe-resolve 不需要任何引數。

描述可達性

describe-reachability

使用 describe-reachability 確定 Outpost 伺服器是否可以連線到區域中的 Outpost 組態端點。需要正常運作的 DNS 組態，您可以使用 describe-resolve 來確定。

語法

```
Outpost>describe-reachability
```

describe-reachability 不需要任何引數。

啟動連線

start-connection

使用 start-connection 起始與區域中 Outpost 服務的連線。此命令會從您使用 export 載入的環境變數中取得第 4 版簽署程序 (SigV4) 憑證。連線會以非同步方式執行，並立即傳回。若要檢查連線狀態，請使用 get-connection。

語法

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

start-connection 需要一個選用連線索引來起始另一個連線。只有值 `0` 和 `1` 才有效。

Example ：連線已啟動

```
Outpost>start-connection

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

取得連線

get-connection

使用 get-connection 傳回連線狀態。

語法

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

get-connection 需要一個選用連線索引來傳回另一個連線的狀態。只有值 0 和 1 才有效。

Example ：成功連線

```
Outpost>get-connection


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

請注意：

- 如果 exchange_active 為 True，則連線仍在建立中。請在 5 分鐘後重試。

- 如果 `keys_exchanged` 或 `connection_established` 為 `False`，且 `exchange_active` 為 `True`，則連線仍在建立中。請在 5 分鐘後重試。

如果問題在 1 小時後仍然存在，請聯絡 AWS Support 中心。

在 Outpost 伺服器上啟動執行個體

安裝 Outpost 並可使用運算和儲存容量之後，即可開始建立資源。例如，您可以啟動 Amazon EC2 執行個體。

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：建立子網路
- 步驟 2：在 Outpost 上啟動執行個體
- 步驟 3：設定連線
- 步驟 4：測試連線

步驟 1：建立子網路

您可以將 Outpost 子網路新增至「前哨」 AWS 區域中的任何 VPC。當您這樣做時，VPC 也會跨越 Outpost。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 2：在 Outpost 上啟動執行個體。

建立 Outpost 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 並指定子網路的 IP 地址範圍。
5. 選擇建立。
6. 建立子網路之後，請為本機網路介面啟用子網路。

步驟 2：在 Outpost 上啟動執行個體

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

- Outpost 伺服器上的執行個體包括執行個體儲存體磁碟區，但不包括 EBS 磁碟區。選擇具有足夠執行個體儲存空間以符合應用程式需求的執行個體大小。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的《執行個體儲存體磁碟區》。
- 您必須指定僅具有單一快照的 AMI。不支援具有多個快照的 AMI。
- 執行個體儲存體磁碟區上的資料會在執行個體重新啟動之後持續存在，但在執行個體終止之後不會持續存在。若要將執行個體儲存體磁碟區上的長期資料保留超過執行個體的生命週期，請務必將資料備份到持久性儲存，例如 Amazon S3 儲存貯體或內部部署網路中的網路儲存裝置。
- 若要將 Outpost 子網路中的執行個體連線到內部部署網路，您必須新增本機網路介面，如下列程序中所述。

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 伺服器支援的執行個體類型。
5. 選擇 Outposts 伺服器支援的執行個體類型。
6. (選擇性) 您可以立即或在建立執行個體之後新增本機網路介面。若要立即新增，請展開 進階網路組態，然後選擇 新增網路介面。選擇 Outpost 子網路。這會使用裝置索引 1 為執行個體建立網路

介面。如果您將 1 指定為 Outpost 子網路的 LNI 裝置索引，則此網路介面將會是執行個體的本機網路介面。

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

步驟 3：設定連線

如果您未在執行個體啟動期間將本機網路介面新增至執行個體，您現在必須這麼做。如需詳細資訊，請參閱《在啟動之後新增 LNI》。

您必須將執行個體的本機網路介面設定為使用本機網路中的 IP 地址。通常，您可以使用 DHCP 來執行此動作。如需相關資訊，請參閱執行個體上執行的作業系統文件。搜尋有關設定額外網路介面和次要 IP 地址的資訊。

步驟 4：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 執行個體的本機網路介面 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
```

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。

> **Note**
>
> 您無法將 Outpost 伺服器連線至您的 AWS 地區或 AWS Outposts 本地區域的服務連結使用私人連線。

目錄

透過服務連結進行連線

在 AWS Outposts 佈建期間，您或 AWS 建立服務連結連線，將 Outpost 連線回您選擇的 AWS 區域或本 AWS Outposts 地區域。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

Outpost 能夠建立透過公有區域連線連回 AWS 區域的服務連結 VPN。為此，Outpost 需要通過公共互聯網或公共虛擬界面連接到該 AWS 地區的公 AWS Direct Connect 共 IP 範圍。此連線可透過服務連結 VLAN 中的特定路由，或透過預設路由 0.0.0.0/0。如需 AWS公有範圍的詳細資訊，請參閱《AWS IP 地址範圍》。

建立服務連結之後，前哨就在服務中並由 AWS其管理。服務連結用於下列流量：

- 透過服務連結傳送至 Outpost 的管理流量，包括內部控制平面流量、內部資源監控，以及韌體和軟體的更新。
- Outpost 與任何相關聯 VPC 之間的流量，包括客戶資料平面流量。

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 的備援連線來連線至區域的服務連線。 AWS 每部 Outpost 伺服器的最大使用率為 500 Mbps。若要提高連線速度，請使用多部 Outpost 伺服器。例如，如果您有三部 AWS Outposts 伺服器，則最大連線速度會提高到 1.5 Gbps (1,500 Mbps)。如需詳細資訊，請參閱 伺服器的服務連結流量。

您的 AWS Outposts 服務連結頻寬需求會根據工作負載特性而有所不同，例如 AMI 大小、應用程式彈性、突發速度需求以及該區域的 Amazon VPC 流量。請注意， AWS Outposts 伺服器不會快取 AMI。每次啟動執行個體都會從區域下載 AMI。

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	1024-65535	服務連結 IP	53	DHCP 提供的 DNS 伺服器
UDP	443, 1024-65535	服務連結 IP	443	AWS Outposts 服務連結端點
TCP	1024-65535	服務連結 IP	443	AWS Outposts 註冊端點

> **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。

更新和服務連結

AWS 在 Outpost 伺服器與其父 AWS 區域之間維護安全的網路連線。這種網路連線稱為服務連結，對於管理前哨站和地區之間提供 VPC 內部流量至關重要。 AWS AWS Well-Architected 的最佳實務建議使用主動-主動式設計，在父母為不同可用區域的 Outposts 之間部署應用程式。如需詳細資訊，請參閱AWS Outposts 高可用性設計與架構考量。

我們會定期更新服務連結，以維持營運品質和表現。在維護期間，您可能會發現此網路短暫的延遲時間和封包遺失，進而影響依賴 VPC 連線至區域內託管資源的工作負載。不過，穿越區域網路介面 (LNI) 的流量不會受到影響。您可以遵循 AWS Well-Architected 最佳做法，並確保應用程式能夠回復影響單一 Outpost 伺服器的故障或維護活動，以避免對應用程式造成影響。

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 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。

返回 AWS Outposts 服務器

如果 AWS Outposts 檢測到服務器中的缺陷，我們將通知您，開始更換過程以向您發送新的服務器，並通過 AWS Outposts 控制台為您提供運輸標籤。

如果您因為伺服器達到合約期限或任何其他原因，而想要歸還伺服器，請聯絡 AWS Support 中心。

主題

下列步驟將說明如何將伺服器歸還至 AWS。

1. 準備要歸還的伺服器

如要讓伺服器為歸還做好準備，請取消共用資源、備份資料；刪除本機網路介面，並且終止作用中的執行個體。

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. 建立儲存在 AWS Outposts 伺服器上執行之 Amazon EC2 執行個體執行個體儲存體中的資料備份。
3. 刪除與伺服器上執行之執行個體關聯的本機網路介面。
4. 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，請遵循 Amazon EC2 使用者指南中終止執行個體中的指示。

2. 取得歸還運送標籤

> **Important**
>
> 您只能使用 AWS 提供的運送標籤。請勿建立自製的運送標籤。

根據歸還原因取得您的運送標籤。

Shipping label for a server that is being replaced

1. 開啟主 AWS Outposts 控台，網址為 https://console.aws.amazon.com/outposts/。
2. 在導覽窗格上，選擇 訂單。
3. 在 替換訂單摘要 下，選擇 列印歸還標籤 並選擇您要歸還之伺服器的組態 ID。

Shipping label for a server that is not being replaced

1. 聯絡 AWS Support 中心。
2. 針對您要歸還的伺服器要求運送標籤。

3. 包裝伺服器

為了包裝您的伺服器，請使用伺服器一開始隨附的箱子和包裝材料。您也可以使用替換伺服器送來的箱子。或者，聯絡 AWS Support 中心要求一個箱子。包裝伺服器後，請貼上 AWS 提供的託運標籤。

4. 透過貨運業者歸還伺服器

您必須透過您所在國家/地區的指定貨運業者歸還伺服器。您可以將伺服器託付給貨運業者，也可以安排想要的日期和時間讓貨運業者前來收取伺服器。 AWS 提供的運送標籤包含退回伺服器的正確地址。

下表顯示您要寄件國家/地區的聯絡人：

Country	聯絡
阿根廷	聯絡 AWS Support 中心。請在您的請求中包含下列資訊：
巴林	

Country	聯絡
巴西	• AWS提供的運送標籤上的追蹤號碼 • 您希望貨運業者前來收取伺服器的日期和時間 • 聯絡人名稱 • 電話號碼 • 電子郵件地址
汶萊	
加拿大	
智利	
哥倫比亞	
香港	
印度	
印尼	
日本	
馬來西亞	
奈及利亞	
阿曼	
巴拿馬	
秘魯	
菲律賓	
塞爾維亞	
新加坡	
南非	
南韓	
臺灣	

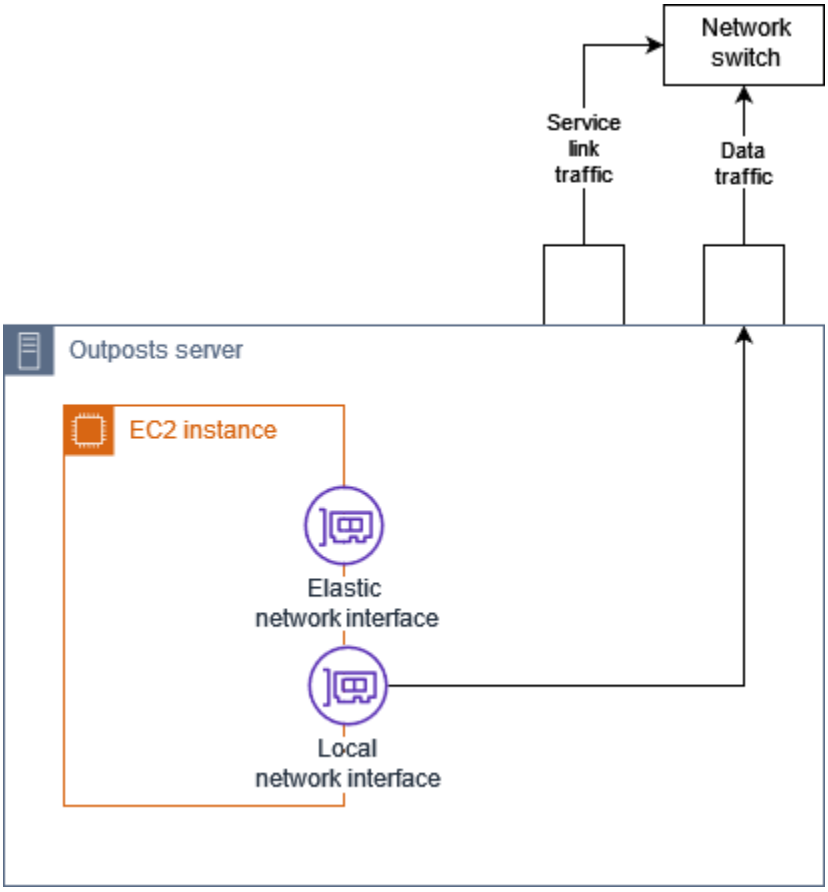
Country	聯絡
泰國	
阿拉伯聯合大公國	
越南	
美國	聯絡 UPS。 您可用下列方式歸還伺服器： • 在您現場進行的例行 UPS 收件期間歸還伺服器。 • 將伺服器放到 UPS 地點。 • 安排您偏好的日期和時間收件。從 AWS提供的運輸標籤中輸入跟踪號碼以免費送貨。
所有其他國家/地區	聯絡 DHL。 您可用下列方式歸還伺服器： • 將伺服器放到 DHL 地點。 • 安排您偏好的日期和時間收件。從 AWS提供的運輸標籤中輸入 DHL 運單號碼以獲得免費送貨。 如果您收到以下錯誤：`Courier pickup cannot be scheduled for an import shipment`，通常是代表您所選取的收件國家/地區與歸還運輸標籤上的收件國家/地區不相符。請選取運輸來源國家/地區，然後再試一次。

本機網路介面

使用 AWS Outposts 伺服器時，本機網路界面 (LNI) 是一種邏輯聯網元件，可將 Outposts 子網路中的 Amazon EC2 執行個體連接到現場部署網路。

本機網路介面會直接在您的區域網路中執行。使用這種類型的本機連線，不需要路由器或閘道即可與內部部署設備通訊。本機網路介面的命名方式與網路介面或彈性網路介面類似。當我們指稱本機網路介面時，一律使用本機 來區分這兩個介面。

在 Outpost 子網路上啟用本機網路介面後，您還可以設定 Outpost 子網路中的 EC2 執行個體，除彈性網路介面之外，另包含本機網路介面。當網路介面連線到 VPC 時，本機網路介面會連線到內部部署網路。下圖顯示 Outpost 伺服器中，同時具有彈性網路介面和本機網路介面的 EC2 執行個體。



您必須將作業系統設定為啟用本機網路介面，才能在區域網路中通訊，就像設定任何其他內部部署設備一樣。您無法在 VPC 中使用 DHCP 選項集來設定本機網路介面，因為本機網路介面會在您的區域網路中執行。

彈性網路介面的作用，與其對可用區域子網路中之執行個體的作用一般無二。例如，您可以使用虛擬私人雲端網路連線來存取的公用區域端點 AWS 服務，或者您可以使用介面 VPC 端點來存取 AWS 服務使用。 AWS PrivateLink如需詳細資訊，請參閱 AWS Outposts 連線至 AWS 區域。

目錄

本機網路介面基本概念

本地網路介面能讓您存取實體第二層網路。VPC 則是虛擬化的第三層網路。本機網路介面不支援 VPC 聯網元件。這些元件包括安全群組、網路存取控制清單、虛擬路由器或路由表以及流程日誌。本機網路介面無法提供可看見 VPC 第三層流程的 Outpost 伺服器。執行個體的主機作業系統確實可以看見完整的實體網路框架。您可以將標準的防火牆邏輯套用至這些框架內的資訊。不過，這種通訊會發生在執行個體內部，但在虛擬建構模組的範圍之外。

考量事項

- 本機網路介面支援 ARP 和 DHCP 協定。但不支援一般的 L2 廣播訊息。
- 本機網路介面的配額來自您網路介面的配額。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的《網路介面》。
- 每個 EC2 執行個體都會有一個本機網路介面。
- 本機網路界面無法使用執行個體的主要網路介面 (eth0)。
- Outpost 伺服器可以託管多個 EC2 執行個體，而每個執行個體都有本機網路介面。

> **Note**
>
> 同一伺服器內的 EC2 執行個體可以直接通訊，無需在 Outpost 伺服器外傳送資料。此通訊包括透過本機網路介面或彈性網路介面的流量。

- 本機網路介面僅供在 Outpost 伺服器之 Outpost 子網路中執行的執行個體使用。
- 本機網路介面不支援混亂模式或 MAC 位址詐騙。

效能

每個執行個體大小的 LNI 都會提供實體 10 GbE LNI 可用頻寬的一部分。下表列出每種執行個體類型的 LNI 網路效能：

執行個體類型	基準頻寬 (Gbps)	高載頻寬 (Gbps)
c6id.large	0.15625	2.5
c6id.large	0.15625	2.5
c6id.xlarge	0.3125	2.5
c6id.2xlarge	0.625	2.5
c6id.4xlarge	1.25	2.5
c6id.8xlarge	2.5	2.5
c6id.12xlarge	3.75	3.75
c6id.16xlarge	5	5
c6id.24xlarge	7.5	7.5
c6id.32xlarge	10	10
c6gd.medium	0.15625	4
c6gd.large	0.3125	4
c6gd.xlarge	0.625	4
c6gd.2xlarge	1.25	4
c6gd.4xlarge	2.5	4
c6gd.8xlarge	4.8	4.8
c6gd.12xlarge	7.5	7.5
c6gd.16xlarge	10	10

安全群組

根據設計，本機網路介面不會在 VPC 中使用安全群組。安全群組可控制輸入和輸出 VPC 流量。本機網路界面未連接到 VPC。本機網路界面連接到本機網路。若要控制本機網路介面的輸入和輸出流量，請使用防火牆或類似策略，就像使用其他內部部署設備一樣。

監控

CloudWatch 指標是為每個本地網絡接口生成的，就像它們用於彈性網絡接口一樣。如需 Linux 執行個體的詳細資訊，請參閱 Amazon EC2 使用者指南中的監控 EC2 執行個體的網路效能。對於 Windows 執行個體，請參閱 Amazon EC2 使用者指南中的監控 EC2 執行個體的網路效能。

MAC 地址

AWS 提供本機網路介面的 MAC 位址。本機網路介面會使用本機管理位址 (LAA) 做為其 MAC 位址。本機網路介面會使用相同的 MAC 位址，直到您刪除介面為止。刪除本機網路介面後，請從本機組態中移除 MAC 位址。 AWS 可以重複使用不再使用的 MAC 地址。

為本機網路介面啟用 Outpost 伺服器的子網路

使用中的修改子網路屬性命令，為本機網路介面啟 AWS CLI 用 Outpost 子網路。您必須在裝置索引上指定網路介面的位置。在啟用的 Outpost 子網路中啟動的所有執行個體都會為本機網路介面使用此裝置位置。例如，值 1 表示 Outpost 子網路中執行個體的次要網路介面 (eth1) 是本機網路介面。

為本機網路介面啟用 Outpost 子網路

在命令提示中，使用下列指令指定本機網路界面的裝置位置。

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

使用本機網路界面

請參閱本節以了解如何使用本機網路介面。

任務

- 新增本機網路介面
- 檢視本機網路介面

- 設定作業系統

新增本機網路介面

您可以在啟動期間或啟動後，將本機網路界面 (LNI) 新增至 Outpost 子網路的 Amazon EC2 執行個體。您可以使用為本機網路介面啟用 Outpost 子網路時所指定的裝置索引，將次要網路介面新增至執行個體，以執行此操作。

考量事項

當您使用主控台指定次要網路介面時，會使用裝置索引 1 建立網路介面。如果這不是您在為區域網路介面啟用 Outpost 子網路時指定的裝置索引，您可以改用 AWS CLI 或 AWS SDK 來指定正確的裝置索引。例如，使用下列指令 AWS CLI：建立網路介面和附加網路介面。

在執行個體啟動期間新增 LNI

1. 在啟動執行個體精靈中，選擇 網路設定 旁的 編輯。
2. 展開 進階網路組態。
3. 選擇 Add network interface (新增網路介面)。這會使用裝置索引 1 建立網路介面。如果您將 1 指定為 Outpost 子網路的 LNI 裝置索引，則此網路介面將會是執行個體的本機網路介面。
4. 選擇 Outpost 子網路，並視需要更新網路介面的組態。
5. 完成精靈後啟動執行個體。

在執行個體啟動後新增 LNI

1. 在導覽窗格中，選擇 網路與安全 和 網路介面。
2. 建立網路介面
   a. 選擇 Create network interface (建立網路介面)。
   b. 選取與執行個體相同的 Outpost 子網路。
   c. 確認 私有 IPv4 地址 設定為 自動指派。
   d. 選取任一安全群組。安全群組不適用於 LNI，所以您選取的安全群組不相關。
   e. 選擇 Create network interface (建立網路介面)。
3. 將網路介面連接到執行個體
   a. 選取新建的網路介面核取方塊。

b. 選擇 Actions (動作)、Attach (連接)。

c. 選擇執行個體。

d. 選擇 Attach (連接)。網路介面連接到裝置索引 1。如果您將 1 指定為 Outpost 子網路的 LNI 裝置索引，則此網路介面會是執行個體的本機網路介面。

檢視本機網路介面

當執行個體為執行中狀態時，您可以使用 Amazon EC2 主控台同時檢視彈性網路介面和本機網路介面，尋找 Outpost 子網路中的執行個體。選取執行個體，然後選擇 聯網 索引標籤。

主控台會顯示來自子網路 CIDR 之 LNI 的私有 IPv4 地址。此位址不是 LNI 的 IP 地址，且無法使用。但是，此地址是從子網路 CIDR 配置，所以您必須在子網路規模調整中就其加以說明。您必須在客機作業系統中以靜態方式或透過 DHCP 伺服器設定 LNI 的 IP 地址。

設定作業系統

啟用本機網路介面後，Amazon EC2 執行個體將會有兩個網路介面，其中一個是本機網路介面。請務必設定您啟動之 Amazon EC2 執行個體的作業系統，以支援多重主目錄聯網組態。

伺服器的本機網路連線

使用本主題以了解裝載 Outpost 伺服器的網路纜線和拓撲需求。如需詳細資訊，請參閱 本機網路介面。

目錄

網路中的伺服器拓撲

Outpost 伺服器需要有兩條不同的網路設備連線。每條連線會使用不同的纜線，並承載不同類型的流量。多條纜線僅供隔離流量類別，不適用於備援。這兩條纜線不需要連接到一般網路。

下表說明 Outpost 伺服器流量類型和標籤。

流量標籤	描述
2	服務連結流量 — 此流量可啟用前哨站和 AWS 區域之間的通訊，以便管理區域和前哨之間的前哨站和 VPC 內部流量。 AWS 服務連結流量包括從 Outpost 到區域的服務連結連線。服務連結是從 Outpost 到地區的一或多個自訂 VPN。Outpost 會連接到您在購買時所選區域的可用區域。
1	本機網路介面 (LNI) 連結流量 - 此流量可讓您透過本機網路介面從 VPC 往本機 LAN 通訊。本機連結流量包括在 Outpost 上執行，可與內部部署網路通訊的執行個體。本機連結流量也會包括透過內部部署網路與網際網路通訊的執行個體。

伺服器實體連線

每部 Outpost 伺服器都有個非備援實體上行鏈路連接埠。連接埠有自己的速度和連接器需求，如下所示：

- 10Gbe – 連接器類型 QSFP+

QSFP+ 纜線

QSFP+ 纜線有一個連接器，可以連接到 Outpost 伺服器的連接埠 3。QSFP+ 纜線的另一端有四個 SFP+ 介面，可以連接到交換器。兩個交換器端介面會標示為 1 和 2。Outpost 伺服器需要有這兩個介面才能運作。2 介面用於處理服務連結流量，1 介面用於 LNI 連結流量。不使用剩餘的介面。

伺服器的服務連結流量

將交換器上的服務連結連接埠設定為具有閘道的 VLAN 未標記存取連接埠，以及下列區域端點的路由：

- 服務連結端點
- Outpost 註冊端點

服務連結連線必須具有可供 Outpost 使用的公用 DNS，才能在 AWS 區域中探索其註冊端點。連線在 Outpost 伺服器和註冊端點之間可有 NAT 裝置。如需有關的公用地址範圍的詳細資訊 AWS，請參閱 Amazon VPC 使用者指南中的 AWS IP 地址範圍和.AWS Outposts AWS 一般參考

若要註冊伺服器，請開啟下列網路連接埠：

- TCP 443
- UDP 443
- UDP 53

上行鏈路速度

每部 Outpost 伺服器都需要 AWS 區域的最低上行鏈路速度 20 Mbps。

您可能需要更快的上行鏈路，視您的 LNI 連結和服務連結使用率而定。如需詳細資訊，請參閱《服務連結的頻寬建議》。

本機網路介面 (LNI) 連結流量

將上游網路裝置的 LNI 連結連接埠設定為本機網路的 VLAN 標準存取連接埠。如果您有多個 VLAN，請將上游網路裝置的所有連接埠設定為幹線連接埠。將上游網路裝置上的連接埠設定為預期有多個 MAC 位址。在伺服器上啟動的每個執行個體都會使用 MAC 位址。有些網路裝置會提供連接埠安全功能，可關閉報告多個 MAC 位址的連接埠。

> **Note**
>
> AWS Outposts 伺服器不會標記 VLAN 流量。如果您將 LNI 設定為幹線，即必須確定作業系統標記 VLAN 流量。

下例示範如何在 Amazon Linux 2023 上為 LNI 設定 VLAN 標籤。如果您使用的是其他 Linux 發行版本，請參閱設定 VLAN 標籤的 Linux 發行版本文件。

範例：在 Amazon Linux 2023 和 Amazon Linux 2 上為 LNI 設定 VLAN 標籤

1. 確定 8021q 模組已載入核心。如果沒有，請使用 `modprobe` 命令載入。

```
modinfo 8021q
```

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

2. 建立 VLAN 裝置。在此範例中：

   - LNI 的介面名稱是 ens6。
   - VLAN ID 是 59
   - 指派給 VLAN 裝置的名稱是 ens6.59

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

3. 選用。如果您要手動指派 IP，請完成此步驟。在本例中，我們要指派 IP 192.168.59.205，其中子網路 CIDR 是 192.168.59.0/24。

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

4. 啟用連結。

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

若要在作業系統層級設定網路介面，並持久性變更 VLAN 標籤，請參閱下列資源：

- 如果您使用的是 Amazon Linux 2，請參閱 Amazon EC2 用戶指南中的使用 ec2 網絡實用程序配置您的網絡界面。
- 如果使用 Amazon Linux 2023，請參閱《Amazon Linux 2023 使用者指南》中的《聯網服務》。

伺服器 IP 地址指派

您不需要為 Outpost 伺服器指派公有 IP 地址。

動態主機控制協定 (DHCP) 是一種網路管理協定，用於自動化 IP 網路上的裝置設定流程。在 Outpost 伺服器環境中，您有兩種方式使用 DHCP：

- 伺服器的網路卡
- 執行個體的本機網路介面

針對服務連接，Outpost 伺服器會使用 DHCP 連接到本地網絡。DHCP 必須傳回 DNS 名稱伺服器和預設閘道。Outpost 伺服器不支援指派服務連結的靜態 IP。

至於 LNI 連結，請使用 DHCP 設定要連接到本機網路的執行個體。如需詳細資訊，請參閱《the section called “設定作業系統”》。

> **Note**
>
> 請務必為 Outpost 伺服器使用穩定的 IP 地址。IP 地址變更會造成 Outpost 子網路暫時服務中斷。

伺服器註冊

Outpost 伺服器在本機網路上建立連線時，會使用服務連結連線來連線到 Outpost 註冊端點並自行註冊。註冊需要公有 DNS。伺服器註冊時，會建立連接至區域中服務連結端點的安全通道。Outpost 伺服器會使用 TCP 連接埠 443 透過公有網際網路促進與地區的通訊。目前， AWS Outposts 伺服器不支援透過 VPC 進行私人連線。如需更多詳細資訊，請參閱 the section called “步驟 6：授權伺服器”。

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。

這些是前哨伺服器可用的資源。如需機架資源，請參閱 Outposts 機架AWS Outposts使用者指南中的使用共用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。
- 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。
  - 使用 AWS Outposts API 查看有關前哨的信息。
- 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，請參閱伺服器常見問

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 伺服器上的資料。

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。

資料刪除

當您終止 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。如需詳細資訊，請參閱以密碼編譯方式銷毀伺服器資料。

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 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，哪個主體在什麼条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

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。

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 受管理策略： AWSOutpostsAuthorizeServerPolicy

使用此政策可授予授權內部部署網路中 Outpost 伺服器硬體時所需之許可。如需詳細資訊，請參閱《授予許可》。

此政策包含以下許可。

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

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
AWSOutpostsAuthorizeServerPolicy – 新政策	AWS Outposts 已新增原則，授與授權內部部署網路中 Outpost 伺服器硬體的權限。	2023 年 1 月 4 日
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。

韌性在 AWS Outposts

為了獲得高可用性，您可以訂購額外的 Outpost 伺服器。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》。

Outpost 伺服器包含執行個體儲存體磁碟區，但不支援 Amazon EBS 磁碟區。執行個體儲存體磁碟區上的資料會在執行個體重新啟動之後持續存在，但在執行個體終止之後不會持續存在。若要將執行個體儲存體磁碟區上的長期資料保留超過執行個體的生命週期，請務必將資料備份到持久性儲存，例如 Amazon S3 儲存貯體或內部部署網路中的網路儲存裝置。

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。

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

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

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。

維度	描述
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》。

AWS 會在執行處分日期終止受影響的執行個體。執行個體儲存體磁碟區上的資料在執行個體終止之後不會持續存在。因此，請務必在執行個體淘汰日期之前採取行動。首先，將您的長期資料從每個受影響執行個體的執行個體儲存體磁碟區傳輸到持久性儲存，例如 Amazon S3 儲存貯體或網路中的網路儲存裝置。

替換伺服器將運送到 Outpost 站點。然後，執行下列動作：

- 從無法修復的伺服器拔下網路線和電源線，並從機架移出伺服器 (如有必要)。
- 將替換伺服器安裝在相同的位置。請依照《Outpost 伺服器安裝》中的安裝說明進行。
- 將無法修復的伺服器封裝到與替換伺服器抵達的相同封裝 AWS 中。
- 使用主控台中附加至訂單組態詳細資訊或替換伺服器訂單的預付退貨運送標籤。

- 將伺服器返回到 AWS。如需詳細資訊，請參閱《退回 AWS Outposts 伺服器》。

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。

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 伺服器才能正常運作。

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：

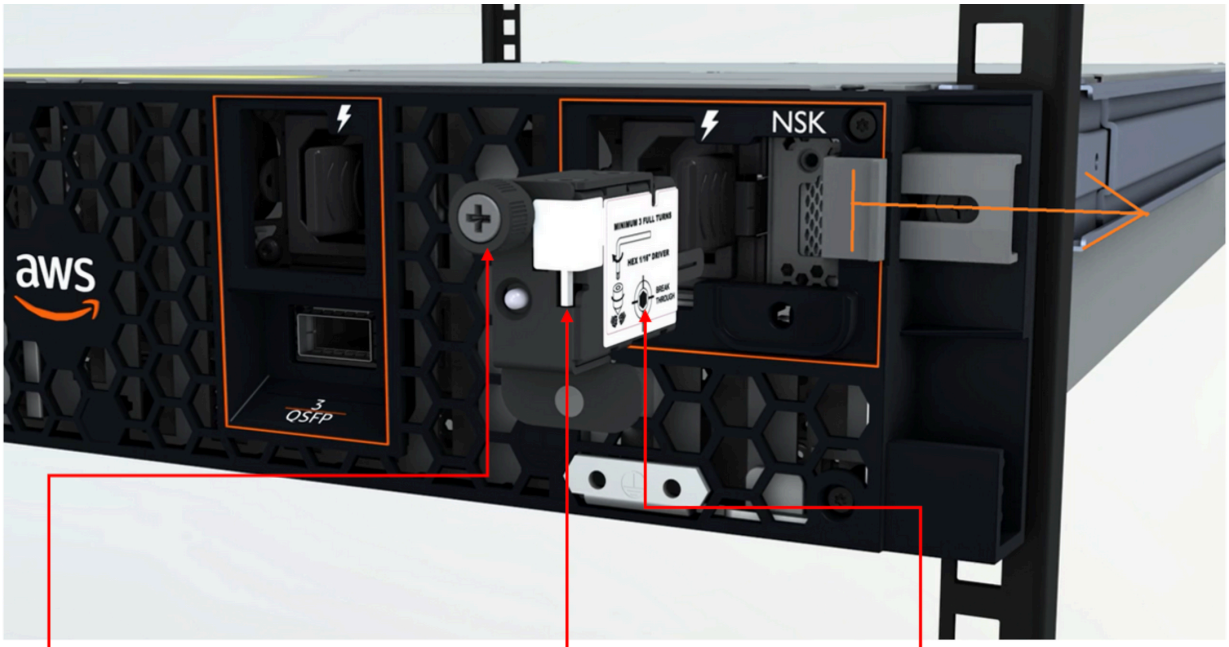
- AWS 博客監控最佳實踐 AWS Outposts涵蓋了 Outposts 特定的可觀察性和事件管理最佳實踐。
- Amazon VPC 網路連線的 AWS 部落格偵錯工具說明了 AWSSupport-Setu MonitoringFrom Pip VPC 工具。此工具是一份 AWS Systems Manager 文件 (SSM 文件)，可在您指定的子網路中建立 Amazon EC2 監視器執行個體並監控目標 IP 地址。此文件會執行 ping、MTR、TCP 追蹤路由和追蹤路徑診斷測試，並將結果儲存在 Amazon CloudWatch Logs 中，並可在 CloudWatch 儀表板中視覺化 (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》。

以密碼編譯方式銷毀伺服器資料

解密伺服器上的資料需要 Nitro 安全金鑰 (NSK)。當您將伺服器返回時 AWS，可能是因為您正在更換伺服器或中斷服務，您可以銷毀 NSK 以加密方式切碎伺服器上的資料。

以密碼編譯方式銷毀伺服器上的資料

1. 將 AWS伺服器寄回目標之前，請先從伺服器移除 NSK。
2. 請確定您有伺服器隨附的正確 NSK。
3. 取出貼紙下的小型六角扳手/內六角扳手。
4. 使用六角扳手將貼紙下的小螺絲旋轉三圈。此動作會銷毀 NSK，並以密碼編譯方式銷毀伺服器上的所有資料。



NSK thumbscrew

HEX tool included with NSK

Use hex tool to crush IC behind the label to destroy data by turning crush screw at least 3 turns

AWS Outposts end-of-term 選項

在您的 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。
- 結束您的訂閱並退回您的 Outpost 伺服器。
- 轉換為 month-to-month 訂閱並保留現有的 Outpost 伺服器。

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 伺服器定價》。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。

如果您沒有指出要續訂或退回 Outpost 伺服器，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。

結束您的訂閱並退回伺服器

> **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. 在說明中，輸入您希望結束訂閱的日期。

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. 如有必要，請備份伺服器上存在的任何執行個體和執行個體資料。
14. 終止在伺服器上啟動的執行個體。
15. 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。
16. 在支援案例中指示之前，請勿關閉伺服器電源或中斷網路連線。

要返回 AWS Outposts 服務器，請按照返回服務 AWS Outposts 器上的程序進行操作。

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 伺服器，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
E AWS Outposts 伺服器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
為 Outposts 服務器創建的 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
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
推出 Outpost 伺服器	增加了 Outposts 服務器，一個新的外 AWS Outposts 形規格。	2021 年 11 月 30 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。