Outposts 伺服器使用者指南

AWS Outposts

AWS Outposts: Outposts 伺服器使用者指南

Table of Contents

什麼是 AWS Outposts？

AWS Outposts 是一項完全受管的服務，可將 AWS 基礎設施、服務APIs、 和工具擴展到客戶內部部署。透過提供 AWS 受管基礎設施的本機存取權， AWS Outposts 可讓客戶使用與 AWS 區域相同的程式設計介面在內部部署中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 是部署在客戶站台的 AWS 運算和儲存容量集區。作為 AWS 區域的一部分 AWS 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 子網路中的執行個體會使用私有 IP 地址與 AWS 區域中的其他執行個體通訊，全部都在相同的 內VPC。

> **Note**
>
> 您無法將 Outpost 連接至相同 內的另一個 Outpost 或本機區域VPC。

如需詳細資訊，請參閱 AWS Outposts 產品頁面。

重要概念

這些是 的關鍵概念 AWS Outposts。

- Outpost 網站 – 客戶管理的實體建築， AWS 其中將安裝您的 Outpost。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。
- Outpost 設備 – 提供 AWS Outposts 服務存取權的實體硬體。硬體包括 擁有和管理的機架、伺服器、交換器和佈線 AWS。
- Outpost 機架 – 業界標準 42U 機架的 Outpost 形式規格。Outposts 機架包括機架安裝式伺服器、交換器、網路修補程式面板、電源架和空白面板。
- Outposts 伺服器 – Outpost 規格尺寸，是業界標準的 1U 或 2U 伺服器，可安裝在標準 EIA-310D 19 相容 4 柱機架中。Outposts 伺服器為空間有限或容量需求較小的站台提供本機運算和聯網服務。
- Outpost 擁有者 – 下 AWS Outposts 訂單之帳戶的帳戶擁有者。與客戶 AWS 互動後，擁有者可能包含其他聯絡點。 AWS 將與聯絡人通訊，以釐清訂單、安裝預約，以及硬體維護和替換。如果聯絡資訊變更，請聯絡 AWS Support 中心。

- 服務連結 – 啟用 Outpost 與其相關聯 AWS 區域之間通訊的網路路由。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，可啟用 Outposts 機架與內部部署網路之間的通訊。
- 本機網路介面 – 啟用 Outposts 伺服器和內部部署網路通訊的網路介面。

AWS Outposts 上的資源

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 叢集、Memcached 叢集）	 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 Edge Manager	是	是

定價

定價是以您的訂單詳細資訊為基礎。當您下訂單時，您可以從各種 Outpost 組態中進行選擇，每個組態都提供 Amazon EC2執行個體類型和儲存選項的組合。您也可以選擇合約條款和付款選項。定價包括下列項目：

- Outposts 機架 - 交付、安裝、基礎設施服務維護、軟體修補程式和升級，以及機架移除。
- Outposts 伺服器 - 交付、基礎設施服務維護，以及軟體修補程式和升級。您要負責安裝和包裝伺服器以進行傳回。

您需支付共用資源的費用，以及從 AWS 區域到 Outpost 的任何資料傳輸費用。您還需要支付 AWS 執行 以維持可用性和安全性的資料傳輸費用。

如需根據位置、組態和付款選項定價，請參閱：

- Outposts 機架定價
- 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廣域網路 (WAN) 存取回區域和網際網路。它還必須提供LAN或WAN存取內部部署工作負載或應用程式所在的區域網路。

下圖說明兩種 Outpost 形式規格。

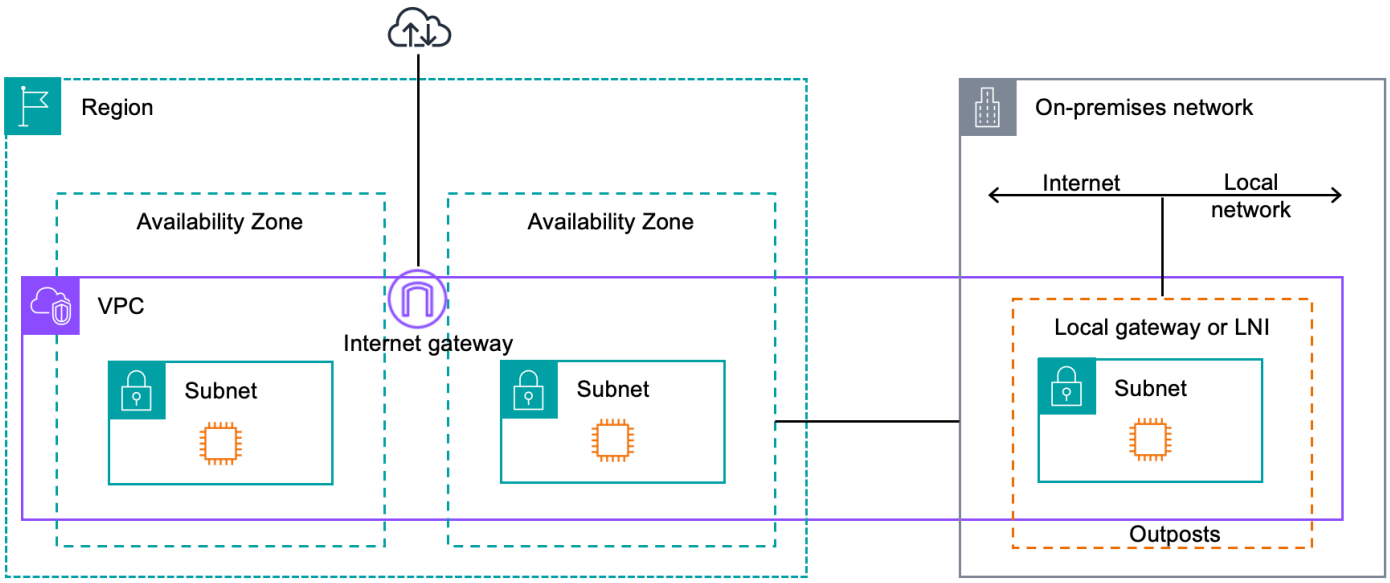
目錄

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 Transit 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VPC具有多個子網路的 A
- 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



VPCs和子網路

虛擬私有雲 (VPC) 橫跨其 AWS 區域中的所有可用區域。您可以透過新增 Outpost 子網路，將該地區VPC中的任何內容擴展到您的前哨站。若要將 Outpost 子網路新增至VPC，請在建立子網路時指定 Outpost 的 Amazon 資源名稱 (ARN)。

Outpost 支援多個子網路。您可以在 Outpost 中啟動EC2執行個體時指定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。

每個前哨可以支持多個可VPCs以有一個或多個 Outpost 子網。如需VPC配額的相關資訊，請參閱 Amazon VPC使用者指南中的 Amazon VPC 配額。

您可以從建立前哨的VPC位置VPCCIDR範圍建立 Outpost 子網路。您可以將 Outpost 位址範圍用於資源，例如駐留在 Outpost 子網路中的EC2執行個體。

路由

預設情況下，每個 Outpost 子網路都會從其繼承主路由表。VPC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 (透過繼承的主路由資料表或自訂資料表) 都會繼承VPC本機路由。這表示中的所有流量 (包括位於目的地的 Outpost 子網路) 都會在中路由VPCCIDR保持路由。VPC VPC

Outpost 子網路路由表可以包含下列目的地：

- VPCCIDRrange — 在安裝時 AWS 定義此項目。這是本機路由，適用於所有VPC路由，包括相同VPC的 Outpost 執行個體之間的流量。
- AWS 區域目的地 — 這包括 Amazon 簡易儲存服務 (Amazon S3)、Amazon DynamoDB 閘道端點、虛擬私有閘道、 AWS Transit Gateway網際網路閘道和VPC對等互連的前置詞清單。

  如果您在同一個 Outpost VPCs 上有多個對等連線，則兩者之間的流量會VPCs保留在 Outpost 中，且不會使用返回該地區的服務連結。

DNS

對於連接到一個的網路界面VPC，Outposts 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，例如在 Outpost 中執行的執行個體的網域註冊、DNS路由和健康狀態檢查。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 回到 AWS 區域的服務連結連線，這些DNS功能才能運作。

Route 53 可能會遇到更長的DNS解決時間，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，您可以使用本機安裝在內部部署環境中的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選項集，並將它們與VPC. 您還必須確保這些DNS服務器具有 IP 連接。您可能還需要將路由添加到本地網關路由表中以實現可達性，但這僅適用於具有本地網關的 Outposts 機架的選項。由於DHCP選項集具有VPC範圍，所以 Outpost 子網路和可用區域子網路中的執行個體都VPC會嘗試使用指定的DNS伺服器進行名稱解析。DNS

查詢記錄不支援來自前哨的查DNS詢。

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。服務鏈接是一組加密的VPN連接，每當前哨站與您選擇的家區域進行通信時使用。您可以使用 virtual LAN (VLAN) 來區段服務連結上的流量。服務連結VLAN可讓前哨站和 AWS 區域之間的通訊，以便管理「前哨站」和「前哨」之間的內 AWS 部VPC流量。

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

Outposts 伺服器包含本機網路介面，可提供內部部署網路的連線能力。本機網路介面僅供在 Outpost 子網路上執行的 Outpost 伺服器使用。您無法使用 Outposts 機架或 AWS 區域中EC2執行個體的本機網路介面。本機網路介面僅適用於內部部署位置。如需詳細資訊，請參閱您的 Outposts 服務器的本地網絡接口。

Outposts 伺服器的網站需求

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FAQs。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。有關 Outposts 機架的要求，請參閱 Outposts 機架AWS Outposts 使用者指南中的 Outposts 機架的站點需求。

目錄

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。
- 空氣質量 — 必須使用MERV8（或更高）過濾器過濾空氣。
- 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]。https://console.aws.amazon.com/outposts/

- 軌道套件相容性 — 託運包裹中隨附的導軌套件與符合 EIA -310-D 標準 19 吋機架的標準 L 形安裝支架相容。導軌套件與 U 形安裝支架不相容，如下圖所示。

- 機架放置 — 我們建議使用深度至少為 36 英吋 (914 公釐) 的標準 19 吋 EIA -310D 機架。 AWS 提供用於伺服器機架安裝的導軌套件。
  - 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）
  - 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

  如果您未將伺服器放在機架中，您仍然必須符合其他站台需求。
- 可維修性 - Outpost 伺服器可從前通道維修。
- 聲學 — 在 80° F（27° C）的溫度下，額定為低於 78 dBA 的聲功率，並符合 GR-63 CORE NEBS 的合規性。
- 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鏈路流量 — QSFP + 突破電纜（10 英尺/3 米）分段流量。

服務連結防火牆

UDP和 TCP 443 必須在防火牆中以狀態方式列出。

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DNS服務器
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 服務鏈接連接，您可以PAT在防火牆NAT或邊緣路由器上使用或。一律會從 Outpost 起始建立服務連結。

服務鏈路最大傳輸單元 (MTU)

網路在父區域中的 Outpost 和服務連結端點MTU之間必須支援 1500 個位元組。 AWS 如需有關服務AWS Outposts 連結的詳細資訊，請參閱伺服器AWS Outposts 使用指南中的「 AWS 區域連線」。

服務連結頻寬建議

為了獲得最佳體驗和恢復能力，您 AWS 必須使用至少 500 Mbps 的備援連線，以及至少 175 毫秒的往返延遲來回服務連線至區域。 AWS 每個 Outposts 伺服器的最大使用率為 500 Mbps。要提高連接速度，請使用多個 Outposts 服務器。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AWS Outposts 使用指南中的伺服器服務連結流量。

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、突發速度需求以及區域的 Amazon VPC 流量。請注意， AWS Outposts 伺服器不會快取 AMIs。AMIs每次啟動執行個體時，都會從區域下載。

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。

服務鏈接需要DHCP響應

服務連結需要IPv4DHCP回應才能設定網路設定。

服務連結最長延遲

服務連結可支援伺服器及其可用區域之間的最大網路延遲 175 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 [瀏覽目錄]。https://console.aws.amazon.com/outposts/

電源線

伺服器隨附一條 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，您需要使用 IEC C13 至 NEMA 5-15P 的電源線。
- 在歐洲部分地區，您可能需要 IEC C13 至 CEE 7/7 電源線。
- 在印度，您需要使用 IEC C13 來IS1293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。

伺服器不包括不斷電供應系統 () 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，請參閱伺服器AWS Outposts 使用指南中的伺服器服務連結流量。

當您確認 Outposts 伺服器的 Amazon EC2 容量可從您 AWS 帳戶的.

Outposts 伺服器入門

訂購 Outposts 伺服器以開始使用。安裝 Outpost 設備後，請啟動 Amazon EC2執行個體並設定與內部部署網路的連線。

任務

- 建立 Outpost 並訂購 Outpost 容量
- 在 Outposts 伺服器上啟動執行個體

建立 Outpost 並訂購 Outpost 容量

若要開始使用 AWS Outposts，請使用 AWS 您的帳戶登入。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 伺服器的網站需求。
- 您必須擁有 AWS Enterprise Support 計畫或 AWS Enterprise On-Ramp Support 計畫。
- 決定 AWS 帳戶 您要使用哪個來建立 Outposts 網站、建立 Outpost，然後下訂單。監控與此帳戶相關聯的電子郵件，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。建立網站之後， 會將 ID AWS Outposts 指派給您的網站。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. 登入 AWS。
2. 在 開啟 AWS Outposts 主控台https://console.aws.amazon.com/outposts/。
3. 若要選取父系 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. （選用）對於網站備註 ，輸入任何其他可能對 有用的資訊 AWS ，以便了解網站。
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

- 確定要與您的網站建立關聯的 AWS 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 伺服器下訂單。

> **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 AWS Support Center 。

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。如果您選擇部分預付或無預付付款選項，您將支付期間內的每月費用。

  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 Next (下一步)。
6. 選擇 使用現有的 Outpost，然後選取您的 Outpost。
7. 選擇 Next (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的運送地址，請聯絡您的 AWS 客戶經理。
10. 選擇 Next (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 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來建立各種執行個體，以滿足業務需求。若要這麼做，您可以建立容量任務、指定執行個體大小和數量，並執行容量任務以實作變更。

> **Note**
>
> - 您可以在為 Outposts 下訂單後變更執行個體大小的數量。
> - 執行個體大小和數量是在 Outpost 層級定義。
> - 執行個體會根據最佳實務自動放置。

若要修改執行個體容量

1. 從AWS Outposts 主控台的AWS Outposts 左側導覽窗格中，選擇容量任務 。
2. 在容量任務頁面上，選擇建立容量任務 。
3. 在入門頁面上，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 Outpost 容量組態 。
2. 選擇 Next (下一步)。
3. 在設定執行個體容量頁面上，每個執行個體類型會顯示一個執行個體大小，其中包含預先選取的數量上限。若要新增更多執行個體大小，請選擇新增執行個體大小 。
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. 檢視每個執行個體類型區段結尾的訊息，告知您容量是否超過或不足。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 請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. 選擇相關執行個體類型區段結尾的自動平衡。

7. 針對每個執行個體類型，請確定至少為一個執行個體大小指定執行個體數量。
8. 選擇 Next (下一步)。
9. 在檢閱和建立頁面上，驗證您正在請求的更新。
10. 選擇建立 . AWS Outposts 建立容量任務。
11. 在容量任務頁面上，監控任務的狀態。

> **Note**
>
> AWS Outposts 可能會要求您停止一或多個執行中的執行個體，以啟用執行容量任務。停止這些執行個體後， AWS Outposts 將執行任務。

Upload JSON file

1. 選擇上傳容量組態 。
2. 選擇 Next (下一步)。
3. 在上傳容量組態計劃頁面上，上傳指定執行個體類型、大小和數量JSON的檔案。

   Example

   範例JSON檔案：

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

4. 在容量組態計劃區段中檢閱JSON檔案的內容。
5. 選擇 Next (下一步)。

6. 在檢閱和建立頁面上，驗證您正在請求的更新。
7. 選擇建立 . AWS Outposts 建立容量任務。
8. 在容量任務頁面上，監控任務的狀態。

> **Note**
>
> AWS Outposts 可能會要求您停止一或多個執行中的執行個體，以啟用執行容量任務。停止這些執行個體後， AWS Outposts 將執行任務。

後續步驟

您可以使用 AWS Outposts 主控台檢視訂單的狀態。訂單的初始狀態為 訂單已收到。如果您對訂單有任何疑問，請聯絡 AWS Support Center 。

若要履行訂單， AWS 將排定交付日期。

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。無論您是執行安裝還是與第三方簽訂合約，安裝都需要 中的IAM憑證 AWS 帳戶 ，其中包含 Outpost，以驗證新裝置的身分。您必須負責提供和管理此存取權。如需詳細資訊，請參閱伺服器安裝指南 。

當 Outpost 的 Amazon EC2容量可從 取得時，安裝即完成 AWS 帳戶。容量可用後，您可以在 Outposts 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”。

在 Outposts 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 Outpost VPC AWS 區域中的任何 。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**
>
> 如果您要在另一個 與您共用的 Outpost 子網路中啟動執行個體 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. 在 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 Create (建立)。
6. 建立子網路後，您必須啟用本機網路介面的子網路。透過 AWS CLI使用 modify-subnet-attribute 命令。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。下列範例使用值 1 來指定次要網路介面。

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

步驟 2：在 Outpost 上啟動執行個體

您可以在您建立的 Outpost 子網路中，或在您共用的 Outpost 子網路中啟動EC2執行個體。安全群組控制 Outpost 子網路中執行個體的傳入和傳出VPC流量，就像對可用區域子網路中的執行個體一樣。若要連線至 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，就像您在可用區域子網路中對執行個體所做的一樣。

考量事項

- Outposts 伺服器上的執行個體包括執行個體存放區磁碟區，但不包括磁碟EBS區。選擇具有足夠執行個體儲存空間的執行個體大小，以滿足應用程式的需求。如需詳細資訊，請參閱 Amazon EC2使用者指南 中的執行個體存放區磁碟區和建立執行個體存放區後端AMI。
- 您必須使用僅AMI具有單一EBS快照的 Amazon EBS後端。AMIs 不支援具有多個EBS快照的 。
- 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. 在 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 子網路的本機網路介面裝置索引，則此網路介面是執行個體的本機網路介面。或者，若要稍後新增，請參閱 新增本機網路介面。
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使用者指南中的啟動EC2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，請參閱新增本機網路介面。

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 來執行此操作 DHCP。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

從本機網路中的電腦，執行 ping命令至 Outpost 執行個體的本機網路介面 IP 地址。

```
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EC2執行個體的相關資訊，請參閱 Amazon EC2使用者指南 中的連線至EC2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 區域與 Outpost 之間的連線

在 AWS 區域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 地址。此資訊可在執行個體詳細資訊頁面上的 Amazon EC2主控台中取得。
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 地址。

   ```
   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 OutpostsAWS 區域連線

AWS Outposts 透過服務連結連線支援廣域網路 （ WAN ） 連線。

> **Note**
>
> 您無法針對將 Outposts 伺服器連線至 AWS 區域或 AWS Outposts 主區域的服務連結連線使用私有連線。

目錄

透過服務連結的連線

在 AWS Outposts 佈建期間，您 或 會 AWS 建立服務連結連線，將 Outposts 伺服器連線至您選擇的 AWS 區域或主區域。服務連結是一組加密的VPN連線，每當 Outpost 與您選擇的主區域通訊時都會使用。您可以使用虛擬 LAN （ VLAN ） 來分割服務連結上的流量。服務連結VLAN可啟用 Outpost 與 AWS 區域之間的通訊，以管理 Outpost 和 AWS 區域與 Outpost 之間的內部VPC流量。

Outpost 能夠透過公有區域連線建立服務 AWS 連結VPN回 區域。若要這麼做，Outpost 需要透過公有網際網路或 AWS Direct Connect 公有虛擬介面連線至 AWS 區域的公有 IP 範圍。此連線可以透過服務連結 中的特定路由VLAN，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》。

建立服務連結後，Outpost 即處於服務狀態，並由 管理 AWS。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 和任何相關聯 之間的流量VPCs，包括客戶資料平面流量。

服務連結最大傳輸單元（MTU）需求

網路連線的最大傳輸單位（MTU）是以位元組為單位的大小，是可通過連線的最大允許封包。網路必須支援 Outpost 和父 AWS 區域中的服務連結端點MTU之間的 1500 位元組。如需 Outpost 中執行個體與 AWS 區域中執行個體MTU之間透過服務連結所需的資訊，請參閱 Amazon 使用者指南 中的 Amazon EC2執行個體的網路最大傳輸單位（MTU）。 EC2

服務連結頻寬建議

為了獲得最佳體驗和恢復能力， AWS 需要您使用至少 500 Mbps 的備援連線，以及最多 175 ms 的往返延遲，才能將服務連結連線至 AWS 區域。每個 Outposts 伺服器的最大使用率為 500 Mbps。若要提高連線速度，請使用多個 Outposts 伺服器。例如，如果您有三個 AWS Outposts 伺服器，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、爆量速度需求，以及 Amazon VPC流量到 區域。請注意， AWS Outposts 伺服器不會快取 AMIs。AMIs 會在每次執行個體啟動時從 區域下載。

若要收到符合您需求的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，組態會將 Amazon VPC 從 AWS 區域延伸至 Outpost。 AWS Direct Connect 公有虛擬介面是服務連結連線。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 和任何相關聯 之間的流量 VPCs

如果您將具狀態防火牆與網際網路連線搭配使用，以限制從公有網際網路到服務連結 的連線VLAN，則可以封鎖從網際網路啟動的所有傳入連線。這是因為服務連結只會從 Outpost VPN啟動至 區域，而不是從 區域啟動至 Outpost。

如果您使用防火牆來限制來自服務連結 的連線VLAN，則可以封鎖所有傳入連線。您必須依照下表，允許傳出連線從 AWS 區域返回 Outpost。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 Service Link 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 會在 Outposts 伺服器與其父 AWS 區域之間維持安全網路連線。此網路連線稱為服務連結，對於透過在 Outpost 和 AWS 區域之間提供內部VPC流量來管理 Outpost 至關重要。AWS 精心建構的最佳實務建議在兩個 Outpost 之間部署應用程式，這些 Outpost 以主動主動設計傳遞至不同的可用區域。如需詳細資訊，請參閱AWS Outposts 高可用性設計和架構考量 。

服務連結會定期更新，以維持操作品質和效能。在維護期間，您可能會在此網路上觀察到短暫的延遲和封包遺失，進而影響依賴於區域內託管資源VPC連線的工作負載。不過，周遊本機網路介面 （LNI） 的流量不會受到影響。您可以遵循 AWS Well-Architected 最佳實務，並確保您的應用程式對影響單一 Outposts 伺服器的故障或維護活動具有彈性，以避免影響您的應用程式。

備援網際網路連線

當您從 Outpost 建置連線至 AWS 區域時，我們建議您建立多個連線，以提高可用性和彈性。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。

傳回 Outposts 伺服器

如果 AWS Outposts 偵測到伺服器中有瑕疵，我們會通知您，啟動替換程序以傳送新的伺服器給您，並透過主控台提供寄件標籤 AWS Outposts 。若要開始使用，請完成下列步驟。

任務

- 步驟 1：準備伺服器以供傳回
- 步驟 2：取得退件寄件標籤
- 步驟 3：封裝伺服器
- 步驟 4：透過快遞傳回伺服器

若要傳回伺服器，因為伺服器已達到合約期限的結尾，或基於其他原因，請聯絡 AWS Support Center 。

步驟 1：準備伺服器以供傳回

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 AWS RAM 主控台。如需詳細資訊，請參閱《 指南》中的《AWS RAM 更新資源共用》。
   - 使用 AWS CLI 執行 disassociate-resource-share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執行個體的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 中的終止執行個體的指示。

步驟 2：取得退件寄件標籤

> **Important**
>
> 您只能使用 AWS 提供的寄件標籤，因為它包含有關您要傳回之伺服器的特定資訊，例如資產 ID。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. 在 開啟 AWS Outposts 主控台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。

步驟 3：封裝伺服器

若要包裝伺服器，請使用 提供的包裝盒和包裝材料 AWS。

1. 將伺服器包裝在下列其中一個方塊中：
   - 伺服器最初進來的盒子和包裝材料。
   - 替換伺服器的盒子和包裝材料。

   或者，聯絡 AWS Support 中心要求一個箱子。
2. 將 AWS 提供的寄件標籤貼在包裝盒的外部。

> **Important**
>
> 確認寄件標籤上的資產 ID 與您傳回的伺服器上的資產 ID 相符。

資產 ID 位於伺服器正面的退出索引標籤上。範例： 1203779889 或 9305589922

3. 安全地密封盒子。

步驟 4：透過快遞傳回伺服器

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 提供的寄件標籤包含傳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： • 位於 AWS提供的寄件標籤上的追蹤號碼 • 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
巴林	
巴西	
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	

Country	聯絡
巴拿馬	
秘魯	
菲律賓	
塞爾維亞	
新加坡	
南非	
南韓	
臺灣	
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： • 在您站點的例行UPS取件期間傳回伺服器。 • 將伺服器投遞至 UPS位置。 • 安排您偏好的日期和時間收件。輸入 AWS所提供運輸標籤上的追蹤編號以利用免費運輸。

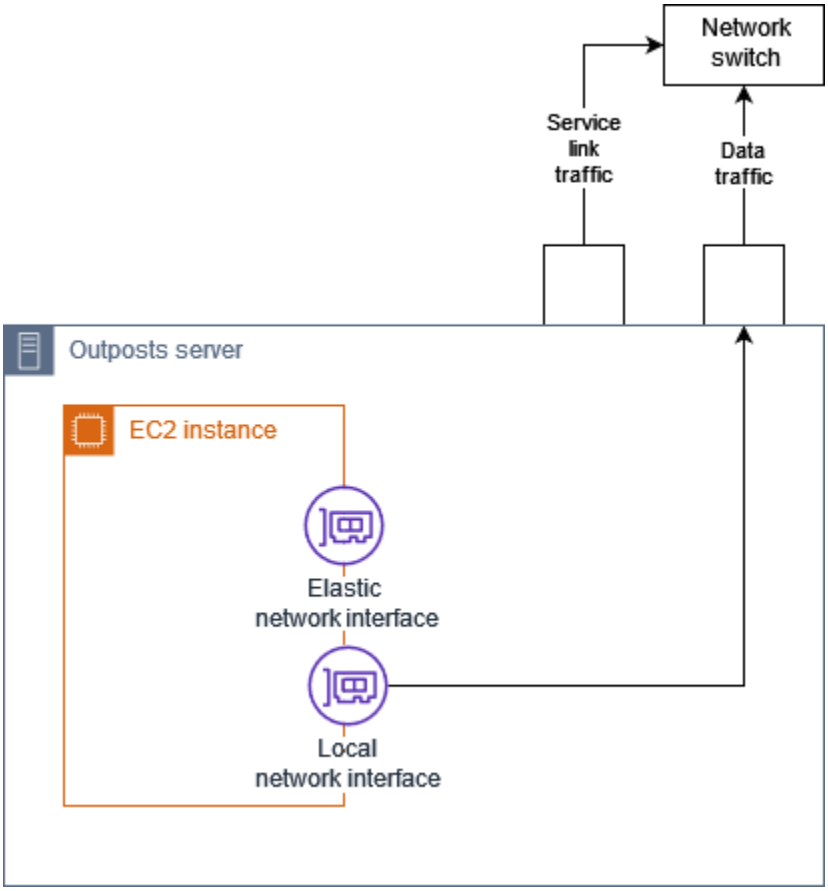
Country	聯絡
所有其他國家/地區	聯絡 DHL。 您可用下列方式歸還伺服器： • 在DHL位置 下架伺服器。 • 安排您偏好的日期和時間收件。輸入 AWS提供的寄件標籤中的DHL提單號碼，即可免費寄件。 如果您收到以下錯誤：`Courier pickup can't be scheduled for an import shipment`，通常是代表您所選取的收件國家/地區與歸還運輸標籤上的收件國家/地區不相符。請選取運輸來源國家/地區，然後再試一次。

您的 Outposts 服務器的本地網絡接口

使用 Outposts 伺服器時，本機網路界面是邏輯聯網元件，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 子網路上啟用區域網路介面後，除了 elastic network interface 之外，您還可以將 Outpost 子網路中的EC2執行個體設定為包含區域網路介面。本機網路介面會在網路介面連線至內部部署網路時連線至VPC. 下圖顯示 Outposts 伺服器上具有 elastic network interface 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。您無法使用中的DHCP選項集VPC來設定區域網路介面，因為區域網路介面會在區域網路上執行。

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VPC網路連線來存取的公用區域端點 AWS 服務，或者您可以 AWS 服務 使用介面VPC端點來存取 AWS PrivateLink。如需詳細資訊，請參閱AWS OutpostsAWS 區域連線。

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。A VPC 是虛擬化的第三層網路。本機網路介面不支援網VPC路元件。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。本機網路介面不會為 Outposts 伺服器提供第三VPC層流程的可見性。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

- 本地網絡接口支持ARP和DHCP協議。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界面配額。
- 每個EC2執行個體都可以有一個區域網路介面。
- 本機網路介面無法使用執行個體的主要網路介面。
- Outposts 服務器可以託管多個EC2實例，每個實例都具有本地網絡接口。

> **Note**
>
> EC2相同伺服器內的執行個體可以直接通訊，而無需在 Outposts 伺服器之外傳送資料。此通訊包括透過本機網路介面或彈性網路介面的流量。

- 本機網路介面僅適用於 Outposts 伺服器上 Outposts 子網路中執行的執行個體。
- 本機網路介面不支援混合模式或MAC位址詐騙。

效能

每個執行個體大小的區域網路介面都會提供實體 10 GbE 可用頻寬的一部分。下表列出每個執行個體類型的網路效能：

執行個體類型	基準頻寬 (Gbps)	高載頻寬 (Gbps)
c6id.large	0.15625	2.5
c6id.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您的VPC. 安全群組控制輸入和輸出VPC流量。本機網路介面未附加至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。如需詳細資訊，請參閱 Amazon EC2 使用者指南中的監控EC2執行個體ENA設定的網路效能。

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的位址 (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該MAC位址。 AWS 可以重複使用不再使用的MAC位址。

將本地網絡接口添加到 Outposts 子網中的EC2實例

您可以在啟動期間或之後將本機網路界面新增至 Outposts 子網路上的 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 AWS SDK改用 AWS CLI 或指定正確的裝置索引。例如，使用下列來自 AWS CLI:create-network-interface和的指令attach-network-interface。

啟動執行個體後，請遵循下列程序來新增區域網路介面。如需在執行個體啟動期間新增執行個體的詳細資訊，請參閱在 Outpost 上啟動執行個體。

新增區域網路介面至EC2執行個體

1. 在打開 Amazon EC2 控制台https://console.aws.amazon.com/ec2/。
2. 在導覽窗格中，選擇 網路與安全 和 網路介面。
3. 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 [私人IPv4位址] 已設定為 [自動指派]。

d. 選取任一安全群組。安全性群組不會套用至區域網路介面，因此您選取的安全性群組不相關。

e. 選擇 Create network interface (建立網路介面)。

4. 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。如果您指定 1 作為 Outpost 子網路之區域網路介面的裝置索引，則此網路介面就是執行個體的區域網路介面。

檢視本機網路介面

執行個體處於執行中狀態時，您可以使用 Amazon EC2 主控台同時檢視 Outpost 子網路中執行個體的彈性網路界面和本機網路界面。選取執行個體，然後選擇 聯網 索引標籤。

主控台會顯示子網路中區域網路介面的私人IPv4位址CIDR。此位址不是本機網路介面的 IP 位址，也無法使用。但是，此位址是從子網路配置的CIDR，因此您必須在子網路大小中對其進行說明。您必須在客體作業系統中，以靜態方式或透過DHCP伺服器設定區域網路介面的 IP 位址。

設定作業系統

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

Outposts 服務器的本地網絡連接

使用本主題可瞭解託管 Outposts 伺服器的網路纜線和拓撲需求。如需詳細資訊，請參閱您的 Outposts 服務器的本地網絡接口。

目錄

- 伺服器註冊

網路中的伺服器拓撲

Outposts 服務器需要兩個不同的連接到您的網絡設備。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 Outposts 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，以便管理前哨站和前哨站之間的內部VPC AWS 流量。服務連結流量包括從 Outpost 到區域的服務連結連線。服務鏈接是自定義VPN或VPNs從前哨到該地區。Outpost 會連接到您在購買時所選區域的可用區域。
1	區域網路介面連結流量 — 此流量可讓您VPC透LAN過區域網路介面與本機的通訊。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，如下所示：

- 10 千兆-連接器類型 + QSFP

QSFP+ 電纜

QSFP+ 電纜有一個連接器，您可以連接到 Outposts 服務器上的端口 3。QSFP+ 纜線的另一端有四個以SFP上的介面，您可以連接到交換器。兩個交換器端介面會標示為 1 和 2。這兩個接口都需要一個 Outposts 服務器的功能。使用2介面處理服務連結流量，以及本機網路1介面連結流量的介面。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埠設定為VLAN具有閘道的未標記存取連接埠，以及前往下列區域端點的路由：

- 服務連結端點
- Outpost 註冊端點

服務連結連線必須有公開DNS可供 Outpost 使用，才能在 AWS 區域中探索其註冊端點。該連接可以在 Outposts 服務器和註冊端點之間具有NAT設備。有關的公共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 一般參考.AWS Outposts

若要註冊伺服器，請開啟下列網路連接埠：

- TCP443
- UDP443
- UDP53

上行鏈路速度

每個 Outposts 伺服器需要到該地區的最低上行鏈路速度為 20 Mbps。 AWS

根據您的區域網路介面連結和服務連結使用率，您可能需要更快的上行鏈路。如需詳細資訊，請參閱《服務連結的頻寬建議》。

區域網路介面連結流量

將上游網路裝置上的區域網路介面連結埠設定為區域網路VLAN上的標準存取連接埠。如果您有多個連接埠VLAN，請將上游網路裝置上的所有連接埠設定為主幹連接埠。將上游網路裝置上的連接埠設定為預期多個MAC位址。在伺服器上啟動的每個執行個體都會使用一個MAC位址。某些網路裝置提供連接埠安全性功能，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。如果您將本機網路介面設定為主幹，則必須確定作業系統已標記VLAN流量。

以下範例說明如何在 Amazon Linux 2023 上為您的本機網路界面設定VLAN標記。如果您正在使用其他 Linux 發行版本，請參閱 Linux 發行版有關設定VLAN標記的文件。

範例：在 Amazon 2023 和 Amazon Linux 2 上為您的本地網路界面設定VLAN標記

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. 建立裝VLAN置。在此範例中：

   - 區域網路介面的介面名稱為 ens6
   - 該VLAN識別碼是 59
   - 指派給VLAN裝置的名稱為 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。在這個例子中，我們分配的 IP 192.168.59.205，其中子網是 192.168.59.0/24。CIDR

```
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，並使標VLAN記變更持續，請參閱下列資源：

- 如果您使用的是 Amazon Linux 2，請參閱 Amazon 用戶指南中的使用 ec2 網絡實用程序配置您的網絡界面。EC2
- 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 Outposts 伺服器指派公用 IP 位址。

動態主機控制通訊協定 (DHCP) 是一種網路管理通訊協定，用於自動化 IP 網路上設定裝置的程序。在 Outposts 服務器的上下文中，您可以使用DHCP兩種方式：

- 伺服器的網路卡

- 執行個體的本機網路介面

對於服務鏈接，Outposts 服務器用於附加DHCP到本地網絡。DHCP必須傳回DNS名稱伺服器和預設閘道。Outposts 服務器不支持服務鏈接的靜態 IP 分配。

若為區域網路介面連結，請使用設定DHCP要連接至區域網路的執行個體。若要取得更多資訊，請參閱the section called “設定作業系統”。

> **Note**
>
> 確保您為 Outposts 服務器使用穩定的 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

Outposts 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。註冊需要公開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。Outposts 服務器使用TCP端口 443 來促進通過公共互聯網與該地區的通信。Outposts 服務器不支持通過VPC私人連接。

分享您的 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 這可讓其他消費者在共用 Outpost 網站上使用 Outpost 網站 VPCs、設定以及啟動和執行執行個體。

在此模型中，擁有 Outpost 資源 (擁有者) 的 AWS 帳戶會與同一組織中的其他 AWS 帳戶 (消費者) 共用資源。取用者可以在與其共用的 Outpost 上建立資源，就像在自己的帳戶中建立的 Outpost 上建立資源一樣。擁有者會負責管理 Outpost 以及在其中建立的資源。擁有者可以隨時變更或撤銷共享的存取權。擁有者也可以檢視、修改和刪除取用者在共用的 Outpost 上建立的資源，但使用容量保留的執行個體則除外。擁有者無法修改取用者啟動到他們已共用的容量保留中的執行個體。

取用者會負責管理在與其共用的 Outpost 上建立的資源，包括使用容量保留的任何資源。取用者無法檢視或修改其他取用者或 Outpost 擁有者所擁有的資源，也無法修改與其共用的 Outpost。

Outpost 擁有者可以與下列對象共用 Outpost 資源：

- 在其組織內部的特定 AWS 帳戶 AWS Organizations。
- AWS Organizations中組織內的組織單位。
- AWS Organizations中的整個組織。

目錄

可共用的 Outpost 資源

Outpost 擁有者可以與取用者共用本節中列出的 Outpost 資源。

這些是 Outposts 服務器可用的資源。有關 Outposts 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。

- 已配置的專用執行個體 – 具有此資源存取權的取用者可以：
  - 在專用主機上啟動和EC2執行執行個體。
- Outpost – 具有此資源存取權的取用者可以：
  - 在 Outpost 上建立和管理子網路。
  - 使用檢 AWS Outposts API視有關前哨的資訊。
- 站點 – 具有此資源存取權的取用者可以：
  - 建立、管理和控制站點的 Outpost。
- 子網路 – 具有此資源存取權的取用者可以：
  - 檢視子網路的相關資訊。
  - 在子網路中啟動並EC2執行執行個體。

  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 Outpost 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戶共用。

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您的 AWS 資源 AWS Organizations。您可以透過 AWS

RAM建立資源共享，以共用您擁有的資源。資源共享指定要共用的資源，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。

若要取得有關的更多資訊 AWS RAM，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us-east-1a用區域可能與其他 AWS 帳戶us-east-1a的位置不同。

若要基於您的帳戶來識別 Outpost 資源的相對位置，您必須使用「可用區域 ID」(AZ ID)。AZ ID 是所有 AWS 帳戶中可用區域的唯一且一致的識別碼。例如，use1-az1是us-east-1區域的 AZ ID，每個 AWS 帳戶中的位置都相同。

若要檢視您帳IDs戶中可用區域的 AZ

1. 請在 https://console.aws.amazon.com/ram 開啟 AWS RAM 主控台。
2. 目前區域IDs的 AZ 會顯示在畫面右側的「您的 AZ ID」面板中。

> **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 Outpost 資源

當擁有者與取用者共用 Outpost 時，取用者可以在 Outpost 上建立資源，就像在自己的帳戶中建立的 Outpost 上建立資源一樣。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 Outpost 資源。

若要共用 Outpost 資源，您必須將其新增至資源共用。資源共用是一 AWS RAM 種可讓您跨 AWS 帳號共用資源的資源。資源共享指定要共用的資源，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，請將其新增至現有的資源共用。若要將 Outpost 資源加入新的資源共用，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，則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，並且在接受邀請後便能存取共用的 Outpost 資源。

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. 在開啟 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 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，也請使用下列程序。

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

使用指create-resource-share令。

將共用的 Outpost 資源取消共用

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不會刪除取用者所建立的現有子網路、磁碟區或執行個體。仍可使用取用者在 Outpost 上建立的任何現有子網路來啟動新的執行個體。

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

若要將您擁有的共用 Outpost 資源取消共用，您必須將其從資源共用中移除。您可以使用控 AWS RAM 制台或 AWS CLI.

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

使用指disassociate-resource-share令。

識別共用的 Outpost 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 AWS CLI來識別共用的本機閘道路由表。

使用主控台識別共用的 AWS Outposts 前哨

1. 在開啟 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` 會顯示 Outpost 擁有者的 AWS 帳戶 ID。

共用的 Outpost 資源許可

擁有者的許可

擁有者會負責管理 Outpost 以及在其中建立的資源。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

取用者可以在與其共用的 Outpost 上建立資源，就像在自己的帳戶中建立的 Outpost 上建立資源一樣。取用者會負責管理在與其共用的 Outpost 上啟動的資源。取用者無法檢視或修改其他取用者或 Outpost 擁有者所擁有的資源，也無法修改與其共用的 Outpost。

計費和計量

擁有者除了須針對其所共用的 Outpost 和 Outpost 資源支付費用之外，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無須額外付費。對於共用子網路，VPC擁有者需支付VPC層級資源 (例如 AWS Direct Connect 和VPN連線、NAT閘道和私人連結連線) 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

安全為 AWS 是最高優先順序。作為 AWS 客戶，您可以從資料中心和網路架構中受益，該架構旨在滿足最安全敏感組織的需求。

安全性是 AWS 和 之間的共同責任。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 Cloud 中執行 AWS 服務的基礎設施。 AWS 也提供您可以安全使用的服務。第三方稽核人員會定期測試和驗證我們安全的有效性，這是AWS 合規計畫 的一部分。若要了解適用於 的合規計劃 AWS Outposts，請參閱合規計劃 AWS 範圍內的合規計劃。
- 雲端安全 – 您的責任取決於您使用 AWS 的服務。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 安全和合規的詳細資訊 AWS Outposts，請參閱AWS Outposts 伺服器 FAQ。

本文件可協助您了解如何在使用 時套用共同的責任模型 AWS Outposts。其中說明如何達成您的安全與合規目標。您也會了解如何使用 AWS 其他服務來協助您監控和保護資源。

目錄

中的資料保護 AWS Outposts

AWS 共同責任模型適用於 中的資料保護 AWS Outposts。如此模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。此內容包含 AWS 服務 您使用之 的安全組態和管理任務。

為了資料保護目的，我們建議您保護 AWS 帳戶 憑證，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management （ ） 設定個別使用者IAM。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。

如需資料隱私權的詳細資訊，請參閱資料隱私權。 FAQ如需歐洲資料保護的相關資訊，請參閱AWS 安全部落格 上的AWS 共同責任模型和GDPR部落格文章。

靜態加密

使用 AWS Outposts時，所有資料都會靜態加密。金鑰材料會包裝在存放在可移除裝置的外部金鑰上，即 Nitro 安全金鑰 （ NSK ）。NSK 需要 才能解密 Outposts 伺服器上的資料。

傳輸中加密

AWS 加密 Outpost 與其 AWS 區域之間的傳輸中資料。如需詳細資訊，請參閱透過服務連結的連線。

資料刪除

當您或終止EC2執行個體時，Hypervisor 會先清除 （ 設定為零 ） 分配給該執行個體的記憶體，然後再將其分配給新執行個體，並且會重設每個儲存區塊。

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。

的身分和存取管理 （ IAM ） AWS Outposts

AWS Identity and Access Management （ IAM ） 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員控制誰可以驗證 （ 登入 ） 和授權 （ 具有許可 ） 使用 AWS Outposts 資源。您可以使用 IAM 而無需額外付費。

目錄

AWS Outposts 如何使用 IAM

在您使用 IAM 管理 AWS Outposts 的存取權之前，請先了解哪些IAM功能可與 AWS Outposts 搭配使用。

IAM 您可以搭配 AWS Outposts 使用的功能

IAM 功能	AWS Outposts 支援
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
ACLs	否
ABAC （政策中的標籤）	是
暫時性憑證	是
主體許可	是
服務角色	否
服務連結角色	是

AWS Outposts 的身分型政策

支援身分型政策：是

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。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型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

透過身分IAM型政策，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。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。若要了解您可以在JSON政策中使用的所有元素，請參閱 IAM 使用者指南 中的IAMJSON政策元素參考。

AWS Outposts 的身分型政策範例

若要檢視 AWS Outposts 身分型政策的範例，請參閱 AWS Outposts 政策範例。

AWS Outposts 中的資源型政策

支援資源型政策：否

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括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。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

若要啟用跨帳戶存取，您可以將另一個帳戶中的整個帳戶或IAM實體指定為資源型政策中的主體。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的 時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授予主體實體（使用者或角色）存取資源的許可。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 中的跨帳戶資源存取權IAM。

AWS Outposts 的政策動作

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什麼。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`元素說明您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API操作相同的名稱。有一些例外狀況，例如沒有相符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 中的 定義的動作 AWS Outposts。

AWS Outposts 中的政策動作在動作之前使用下列字首：

```
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什麼。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 政策元素會指定動作套用的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name （ ARN ） 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": "*"
```

有些 AWS Outposts API動作支援多個資源。若要在單一陳述式中指定多個資源，ARNs請以逗號分隔 。

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

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

AWS Outposts 的政策條件索引鍵

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什麼。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， 會使用邏輯OR操作 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，只有在使用者使用其IAM使用者名稱加上標籤時，您才能授予IAM使用者存取資源的許可。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM政策元素：變數和標籤。

AWS 支援全域條件索引鍵和服務特定條件索引鍵。若要查看所有 AWS 全域條件索引鍵，請參閱 IAM 使用者指南 中的AWS 全域條件內容索引鍵。

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

若要檢視 AWS Outposts 身分型政策的範例，請參閱 AWS Outposts 政策範例。

ACLs 在 AWS Outposts 中

支援ACLs：否

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

ABAC 使用 AWS Outposts

支援 ABAC（政策中的標籤）：是

屬性型存取控制 （ ABAC ） 是一種根據屬性定義許可的授權策略。在 中 AWS，這些屬性稱為標籤。您可以將標籤連接至IAM實體 （ 使用者或角色 ） 和許多 AWS 資源。標記實體和資源是 的第一步 ABAC。然後，您可以設計ABAC政策，以便在主體的標籤與其嘗試存取的資源上的標籤相符時允許操作。

ABAC 有助於快速成長的環境，並有助於處理政策管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 條件索引鍵，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 的詳細資訊ABAC，請參閱 使用者指南 中的什麼是 ABAC？。 IAM 若要檢視包含設定 之步驟的教學課程ABAC，請參閱 IAM 使用者指南 中的使用屬性型存取控制 （ABAC）。

搭配 AWS Outposts 使用臨時憑證

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括 AWS 服務 使用哪些臨時憑證，請參閱 使用者指南 中的 AWS 服務 使用 IAM 。 IAM

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則表示您正在使用臨時憑證。例如，當您 AWS 使用公司的單一登入 （SSO） 連結存取 時，該程序會自動建立臨時憑證。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 中的切換到角色 （主控台）。

您可以使用 AWS CLI 或 手動建立臨時憑證 AWS API。然後，您可以使用這些臨時憑證來存取 AWS. AWS recommends，讓您動態產生臨時憑證，而不是使用長期存取金鑰。如需詳細資訊，請參閱 中的臨時安全憑證IAM。

AWS Outposts 的跨服務主體許可

支援轉送存取工作階段 （FAS）：是

當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為委託人。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 使用呼叫 的委託人許可 AWS 服務，並結合 AWS 服務 請求向下游服務提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。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請求的政策詳細資訊，請參閱轉送存取工作階段 。

AWS Outpost 的服務角色

支援服務角色：否

服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM

AWS Outposts 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的服務角色類型 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 ，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

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

AWS Outposts 政策範例

根據預設，使用者和角色沒有建立或修改 AWS Outposts 資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface （ AWS CLI ） 或 來執行任務 AWS API。若要授予使用者對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，使用者可以擔任角色。

若要了解如何使用這些範例政策文件來建立身分IAM型JSON政策，請參閱 IAM 使用者指南 中的建立IAM政策。

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

目錄

政策最佳實務

身分型政策會決定某人是否可以在帳戶中建立、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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用 AWS 受管政策，將許可授予許多常見使用案例。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 AWS 受管政策或 AWS 受管政策。
- 套用最低權限許可 – 當您使用IAM政策設定許可時， 只會授予執行任務所需的許可。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 套用許可的詳細資訊，請參閱 IAM 使用者指南 中的政策和許可IAM。
- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，例

如 AWS 服務，您也可以使用 條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南 中的IAMJSON政策元素：條件。

- 使用 IAM Access Analyzer 驗證您的IAM政策以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，讓政策遵循IAM政策語言 （JSON） 和IAM最佳實務。IAM Access Analyzer 提供超過 100 個政策檢查和可操作的建議，協助您撰寫安全且實用的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM存取分析器政策驗證。
- 需要多重要素身分驗證 （MFA） – 如果您有需要IAM使用者或 根使用者的案例 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求 ，請將MFA條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的設定 MFA受保護的API存取。

如需 中最佳實務的詳細資訊IAM，請參閱 IAM 使用者指南 中的安全最佳實務IAM。

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"
    }
  ]
}
```

的服務連結角色 AWS Outposts

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至 的服務角色類型 AWS Outposts。 AWS Outposts 定義服務連結角色，並包含 AWS 代表您呼叫其他服務所需的所有許可。

服務連結角色可讓您設定 AWS Outposts 更有效率，因為您不必手動新增必要的許可。 AWS Outposts 會定義其服務連結角色的許可，除非另有定義，否則 AWS Outposts 只能擔任其角色。定義的許可包括信任政策和許可政策，該許可政策無法連接到任何其他IAM實體。

您必須先刪除相關的 資源，才能刪除服務連結角色。這可保護您的 AWS Outposts 資源，因為您不會不小心移除存取資源的許可。

的服務連結角色許可 AWS Outposts

AWS Outposts 使用名為 AWSServiceRoleForOutposts_ 的服務連結角色***OutpostID*** – 允許 Outposts 代表您存取私有連線 AWS 的資源。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_*OutpostID* 服務連結角色信任下列 服務擔任該角色：

- `outposts.amazonaws.com`

AWSServiceRoleForOutposts_***OutpostID*** 服務連結角色包含下列政策：

- AWSOutpostsServiceRolePolicy
- AWSOutpostsPrivateConnectivityPolicy_***OutpostID***

此AWSOutpostsServiceRolePolicy政策是服務連結角色政策，用於啟用 管理 AWS 的資源存取權 AWS Outposts。

此政策允許 AWS Outposts 在指定的資源上完成下列動作：

- 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* 政策允許 AWS Outposts 在指定的資源上完成下列動作：

- 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，以允許IAM實體（例如使用者、群組或角色）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 建立服務連結角色 AWS Outposts

您不需要手動建立一個服務連結角色。當您在 中為 Outpost 設定私有連線時 AWS Management Console， AWS Outposts 會為您建立服務連結角色。

編輯 的服務連結角色 AWS Outposts

AWS Outposts 不允許您編輯 AWSServiceRoleForOutposts_*OutpostID* 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。不過，您可以使用 編輯角色的描述IAM。如需詳細資訊，請參閱 IAM 使用者指南 中的更新服務連結角色。

刪除 的服務連結角色 AWS Outposts

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。

如果您嘗試刪除資源時 AWS Outposts ，服務正在使用角色，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。

您必須先刪除 Outpost，才能刪除 AWSServiceRoleForOutposts_*OutpostID* 服務連結角色。

開始之前，請確定您的 Outpost 並未使用 AWS Resource Access Manager （ ） 共用AWS RAM。如需詳細資訊，請參閱將共用的 Outpost 資源取消共用。

若要刪除 AWSServiceRoleForOutposts_ 使用 AWS Outposts 的資源***OutpostID***

請聯絡 AWS 企業支援部門以刪除您的 Outpost。

使用 手動刪除服務連結角色 IAM

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 支援在提供服務的所有 區域中使用服務連結角色。如需詳細資訊，請參閱 FAQs for Outposts 機架和 Outposts 伺服器 。

AWSAWS Outposts 的 受管政策

AWS 受管政策是由 AWS AWS .managed 政策建立和管理的獨立政策旨在為許多常見使用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 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 AWS 受管政策中定義的許可。如果 AWS 更新受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分 （使用者、群組和角色）。 AWS 當新的 AWS 服務 啟動或新的API操作可用於現有 服務時， 很有可能更新受 AWS 管政策。

如需詳細資訊，請參閱 IAM 使用者指南 中的 AWS 受管政策。

AWS 受管政策： AWSOutpostsServiceRolePolicy

此政策會連接至服務連結角色，允許 AWS Outposts 代表您執行動作。如需詳細資訊，請參閱服務連結角色。

AWS 受管政策： AWSOutpostsPrivateConnectivityPolicy

此政策會連接至服務連結角色，允許 AWS Outposts 代表您執行動作。如需詳細資訊，請參閱服務連結角色。

AWS 受管政策： AWSOutpostsAuthorizeServerPolicy

使用此政策授予在內部部署網路中授權 Outposts 伺服器硬體所需的許可。

此政策包含以下許可。

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

AWS Outpost 對 AWS 受管政策的更新

檢視自此服務開始追蹤這些變更以來， AWS Outposts 受 AWS 管政策更新的詳細資訊。

變更	描述	日期
AWSOutpostsAuthorizeServerPolicy – 新政策	AWS Outposts 新增了政策，授予許可，以授權內部部署網路中的 Outposts 伺服器硬體。	2023 年 1 月 4 日

變更	描述	日期
AWS Outposts 已開始追蹤變更	AWS Outposts 開始追蹤其 AWS 受管政策的變更。	2019 年 12 月 3 日

中的基礎設施安全 AWS Outposts

作為受管服務， AWS Outposts 受到 AWS 全球網路安全的保護。如需有關 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱 AWS Cloud Security 。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱 Security Pillar AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 已發佈的API呼叫，透過網路存取 AWS Outpost。使用者端必須支援下列專案：

- Transport Layer Security （ TLS ）。我們需要 TLS 1.2 和 建議 TLS 1.3。
- 具有完美前向秘密 （ PFS ） 的加密套件，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，必須使用與IAM委託人相關聯的存取金鑰 ID 和秘密存取金鑰來簽署請求。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。

如需有關在 Outpost 上執行之EC2執行個體和EBS磁碟區所提供基礎設施安全的詳細資訊，請參閱 Amazon 中的基礎設施安全。 EC2

VPC 流程日誌的運作方式與在 AWS 區域中相同。這表示它們可以發佈到 CloudWatch Logs、Amazon S3 或 Amazon GuardDuty 進行分析。資料需要傳回區域，才能發佈至這些服務，因此當 Outpost 處於中斷連線狀態時，就無法從 CloudWatch 或其他 服務看見。

中的復原能力 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 CloudWatch 動作來設定自動復原選項，以及監控 Outpost 隨時間的容量使用率。

當您建立 Outpost 時，請從 AWS 區域選取可用區域。此可用區域支援控制平面操作，例如回應API呼叫、監控 Outpost 和更新 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》。

Outposts 伺服器包含執行個體存放區磁碟區，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。

的合規驗證 AWS Outposts

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 依合規計劃範圍然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs 。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 下載報告 AWS Artifact。

使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源以協助合規：

- 安全與合規快速入門指南 – 這些部署指南討論架構考量，並提供以 AWS 安全與合規為重心的基準環境部署步驟。
- Amazon Web Services 上HIPAA安全與合規架構 – 本白皮書說明公司如何使用 AWS 來建立HIPAA符合 資格的應用程式。

> **Note**
>
> 並非所有 AWS 服務 都HIPAA符合資格。如需詳細資訊，請參閱HIPAA合格服務參考 。

- AWS 合規資源 – 此工作手冊和指南集可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同的責任模型。本指南摘要說明跨多個架構 （ 包括國家標準和技術研究所 （ ）NIST、支付卡產業安全標準委員會 （ PCI ） 和國際標準化組織 （ ISO ） ） 保護 AWS 服務 指南並映射至安全控制的最佳實務。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 服務會評估資源組態是否符合內部實務、產業準則和法規。
- AWS Security Hub – 這 AWS 服務 可讓您全面檢視 內的安全狀態 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 – 透過監控您的環境是否有可疑和惡意活動，藉此 AWS 服務 偵測 AWS 帳戶、工作負載、容器和資料的潛在威脅。 GuardDuty 可以協助您滿足特定合規架構強制要求的入侵偵測需求DSS，以解決各種合規要求，例如 PCI 。
- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，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。

監控您的 Outposts 伺服器

AWS Outposts 與下列 服務整合，提供監控和記錄功能：

CloudWatch 指標

使用 Amazon CloudWatch 擷取 Outposts 伺服器資料點的統計資料，作為一組有序的時間序列資料，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 Outposts 伺服器的指標。

CloudTrail 日誌

使用 AWS CloudTrail 擷取對 進行呼叫的詳細資訊 AWS APIs。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 日誌來判斷該資訊，例如進行何種呼叫、呼叫來源 IP 地址、進行呼叫的人員，以及進行呼叫的時間。

CloudTrail 日誌包含 API動作呼叫的相關資訊 AWS Outposts。它們也包含來自 Outpost 上 服務API之動作的呼叫資訊，例如 Amazon EC2和 Amazon EBS。如需詳細資訊，請參閱使用 記錄API呼叫 CloudTrail。

VPC 流程日誌

使用VPC流程日誌來擷取進出 Outpost 和 Outpost 內流量的詳細資訊。如需詳細資訊，請參閱 Amazon VPC使用者指南 中的VPC流程日誌。

流量鏡射

使用流量鏡射，將網路流量從 Outposts 伺服器複製和轉送至 out-of-band安全和監控設備。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 VPC 流量鏡射指南 。

AWS Health Dashboard

AWS Health Dashboard 會顯示 AWS 資源運作狀態變更所啟動的資訊和通知。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 服務的一部分 AWS Health Dashboard 不需要設定，而且可在您的帳戶中驗證的任何使用者檢視。如需詳細資訊，請參閱 AWS Health Dashboard入門。

CloudWatch Outposts 伺服器的指標

AWS Outposts 會將資料點發佈至 Amazon CloudWatch for您的 Outposts。 CloudWatch 可讓您擷取有關這些資料點的統計資料，作為一組有序的時間序列資料，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 警示來監控ConnectedStatus指標。如果平均指標小於 1， 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。常見問題包括最近內部部署網路組態對防火牆和NAT規則的變更，或網際網路連線問題。對於ConnectedStatus問題，我們建議您在內部部署網路中驗證 AWS 與區域的連線，如果問題持續存在，請聯絡 AWS 支援。

如需建立 CloudWatch 警示的詳細資訊，請參閱 Amazon CloudWatch 使用者指南 中的使用 Amazon 警示。 CloudWatch 如需 的詳細資訊 CloudWatch，請參閱 Amazon CloudWatch 使用者指南 。

目錄

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

最長解析時間：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

最長解析時間：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

最長解析時間：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

最長解析時間：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

最長解析時間：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

最長解析時間：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

目前使用的執行個體類型數目，包括受管服務所使用的任何執行個體類型，例如 Amazon Relational Database Service （Amazon RDS） 或 Application Load Balancer 。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

最長解析時間：5 分鐘

維度：Account、InstanceType 和 OutpostId

AvailableInstanceType_Count

可用的執行個體類型數量。此指標包含AvailableReservedInstances計數。

若要判斷您可以保留的執行個體數量，請從AvailableReservedInstances計數中減去AvailableInstanceType_Count計數。

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

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

最長解析時間：5 分鐘

維度：InstanceType 和 OutpostId

AvailableReservedInstances

可使用容量預留 啟動運算容量的執行個體數目https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/capacity-reservations-outposts.html。

此指標不包含 Amazon EC2 Reserved Instances。

此指標不包含您可以預留的執行個體數量。若要判斷您可以保留的執行個體數量，請從AvailableReservedInstances計數中減去AvailableInstanceType_Count計數。

```
Number of instances that you can reserve = AvailableInstanceType_Count
 - AvailableReservedInstances
```

單位：計數

最長解析時間：5 分鐘

維度：InstanceType 和 OutpostId

UsedReservedInstances

使用容量預留 保留的運算容量中執行的執行個體數目。此指標不包含 Amazon EC2 預留執行個體。

單位：計數

最長解析時間：5 分鐘

維度：InstanceType 和 OutpostId

TotalReservedInstances

由使用容量預留 預留的運算容量所提供，執行中且可啟動的執行個體總數https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/capacity-reservations-outposts.html。此指標不包含 Amazon EC2 預留執行個體。

單位：計數

最長解析時間：5 分鐘

維度：InstanceType 和 OutpostId

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。

維度	描述
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的 ID （ VIF ）。
VirtualInterfaceGroupId	本機閘道虛擬介面 （ ） 的虛擬介面群組 IDVIF。

檢視 Outposts 伺服器的 CloudWatch 指標

您可以使用主控台檢視 Outposts 伺服器的 CloudWatch CloudWatch指標。

使用 CloudWatch 主控台檢視指標

1. 在 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. (選用) 若要檢視所有維度的指標，請在搜尋欄位中輸入其名稱。

若要使用 檢視指標 AWS CLI

使用下列 list-metrics 命令列出可用指標。

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

使用 取得指標的統計資料 AWS CLI

使用以下get-metric-statistics命令取得指定指標和維度的統計資料。 CloudWatch 將維度的每個唯一組合視為個別指標。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 記錄 AWS Outposts API呼叫 AWS CloudTrail

AWS Outposts 已與 整合 AWS CloudTrail，此服務提供使用者、角色或 AWS service. CloudTrail captures API呼叫 AWS Outposts 作為事件所採取動作的記錄。擷取的呼叫包括從 AWS Outposts 主控台呼叫，以及對 操作的 AWS Outposts API程式碼呼叫。使用 所收集的資訊 CloudTrail，您可以判斷對 提出的請求 AWS Outposts、提出請求的 IP 地址、提出的時間，以及其他詳細資訊。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 該請求是使用根使用者還是使用者憑證提出。
- 是否代表 IAM Identity Center 使用者提出請求。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務服務提出。

CloudTrail 當您建立 AWS 帳戶時， 會在您的帳戶中處於作用中狀態，而且您會自動存取 CloudTrail 事件歷史記錄 。 CloudTrail 事件歷史記錄提供過去 90 天內記錄的管理事件的可檢視、可搜尋、可下載和不可變記錄 AWS 區域。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南 中的使用 CloudTrail 事件歷史記錄。檢視事件歷史記錄 不收取任何 CloudTrail 費用。

如需 AWS 帳戶 過去 90 天內持續記錄的事件，請建立追蹤或 CloudTrail Lake 事件資料存放區。

CloudTrail 追蹤

追蹤可讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。使用 建立的所有追蹤 AWS Management Console 都是多區域。您可以使用 建立單一區域或多區域追蹤 AWS CLI。建議您建立多區域追蹤，因為您擷取帳戶中所有 AWS 區域 中的活動。如果您建立單一區域追蹤，您只能檢視記錄於追蹤 的事件 AWS 區域。如需追蹤的詳細資訊，請參閱 AWS CloudTrail 使用者指南 中的為您的 建立追蹤 AWS 帳戶和為組織建立追蹤。

您可以透過建立追蹤 CloudTrail ，免費將一份正在進行的管理事件副本交付至 Amazon S3 儲存貯體，但需要支付 Amazon S3 儲存費用。如需 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。 如需 Amazon S3 定價的相關資訊，請參閱 Amazon S3 定價。

CloudTrail Lake 事件資料存放區

CloudTrail Lake 可讓您在事件上執行SQL以 為基礎的查詢。 CloudTrail Lake 會以資料列為基礎的JSON格式將現有事件轉換為 Apache ORC 格式。ORC 是一種欄式儲存格式，已針對快速擷取資料進行最佳化。系統會將事件彙總到事件資料存放區中，事件資料存放區是事件的不可變集合，其依據為您透過套用進階事件選取器選取的條件。套用於事件資料存放區的選取器控制哪些事件持續存在並可供您查詢。如需 CloudTrail Lake 的詳細資訊，請參閱 AWS CloudTrail 使用者指南 中的使用 AWS CloudTrail Lake。

CloudTrail Lake 事件資料存放區和查詢會產生成本。建立事件資料存放區時，您可以選擇要用於事件資料存放區的定價選項。此定價選項將決定擷取和儲存事件的成本，以及事件資料存放區的預設和最長保留期。如需 CloudTrail 定價的詳細資訊，請參閱AWS CloudTrail 定價。

AWS Outposts 中的管理事件 CloudTrail

管理事件提供有關在 中資源上執行的管理操作的資訊 AWS 帳戶。這些也稱為控制平面操作。根據預設， 會 CloudTrail 記錄管理事件。

AWS Outposts 會將所有 AWS Outposts 控制平面操作記錄為管理事件。如需 AWS Outposts 記錄到的 AWS Outposts 控制平面操作清單 CloudTrail，請參閱 AWS Outposts API參考 。

AWS Outposts 事件範例

下列範例顯示示範 `SetSiteAddress`操作 CloudTrail 的事件。

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

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

Outposts 伺服器維護

在共同責任模型 ， AWS 負責執行 AWS 服務的硬體和軟體。這適用於 AWS Outposts，就像它對 AWS 區域一樣。例如， AWS 管理安全修補程式、更新韌體和維護 Outpost 設備。 AWS 也會監控 Outposts 伺服器的效能、運作狀態和指標，並判斷是否需要任何維護。

> **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，我們建議您將執行個體儲存磁碟區的長期資料備份至持久性儲存體，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

更新聯絡詳細資訊

如果 Outpost 擁有者變更，請使用新擁有者的名稱和聯絡資訊聯絡 AWS Support Center。

硬體維護

如果在伺服器佈建程序期間或在 Outposts 伺服器上託管執行的 Amazon EC2執行個體時 AWS 偵測到硬體發生無法修復的問題，我們將通知 Outpost 擁有者和執行個體擁有者受影響的執行個體已排定淘汰。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 會在執行個體淘汰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。請遵循 Outposts 伺服器安裝 中的安裝指示。
- 將無法修復的伺服器包裝在替換伺服器抵達的相同包裝 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。
- 將伺服器傳回 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。

電源和網路事件的最佳實務

如 AWS Outposts 客戶AWS 服務條款中所述，Outposts 設備所在的設施必須符合最低電力和網路需求，以支援 Outposts 設備的安裝、維護和使用。Outposts 伺服器只有在未中斷電源和網路連線時才能正確運作。

電源事件

在完全停電的情況下， AWS Outposts 資源有可能無法自動恢復服務的固有風險。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型或機架外負載平衡變更，以受控方式將服務和應用程式移出 Outposts 設備。
- 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 （ off-on-off-on ）。
- 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。
- 電源還原後，在 AWS Support Center 建立案例，以請求驗證 AWS Outposts 和相關服務正在執行。

網路連線事件

您的 Outpost 與 AWS 區域或 Outposts 主區域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提供者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。

Outposts 伺服器上的 Amazon EC2執行個體、LNI網路和執行個體儲存磁碟區將繼續正常運作，並且可以透過本機網路和 本機存取LNI。同樣地，諸如 Amazon ECS工作者節點之類的 AWS 服務資源會繼續在本機執行。不過，API可用性會降低。例如，執行、啟動、停止和終止APIs可能無法運作。執行個體指標和日誌將繼續在本機快取數小時，並在連線恢復時推送至 AWS 區域。不過，中斷連線超過數小時可能會導致指標和日誌遺失。

如果服務連結因現場電源問題或網路連線中斷而中斷， AWS Health Dashboard 會傳送通知給擁有 Outposts 的帳戶。您和 都 AWS 無法隱藏服務連結中斷的通知，即使預期會中斷。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：

- 的 AWS 部落格監控最佳實務涵蓋 Outposts 特有的可觀測性和事件管理最佳實務。 AWS Outposts
- Amazon 網路連線的 AWS 部落格偵錯工具說明 AWSSupport-S etupIPMonitoringFromVPC 工具。 VPC此工具是一種 AWS Systems Manager 文件（SSM 文件），可在您指定的子網路中建立 Amazon EC2 Monitor 執行個體，並監控目標 IP 地址。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，這些日誌可在 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 監控一個或多個 Outpost 執行個體 （這將提供封包遺失圖和 AWS Outposts 父 AWS 區域之間的延遲。
- AWS 部落格部署 AWS Outposts 使用 的自動化 Amazon CloudWatch 儀表板 AWS CDK，說明部署自動化儀表板所涉及的步驟。

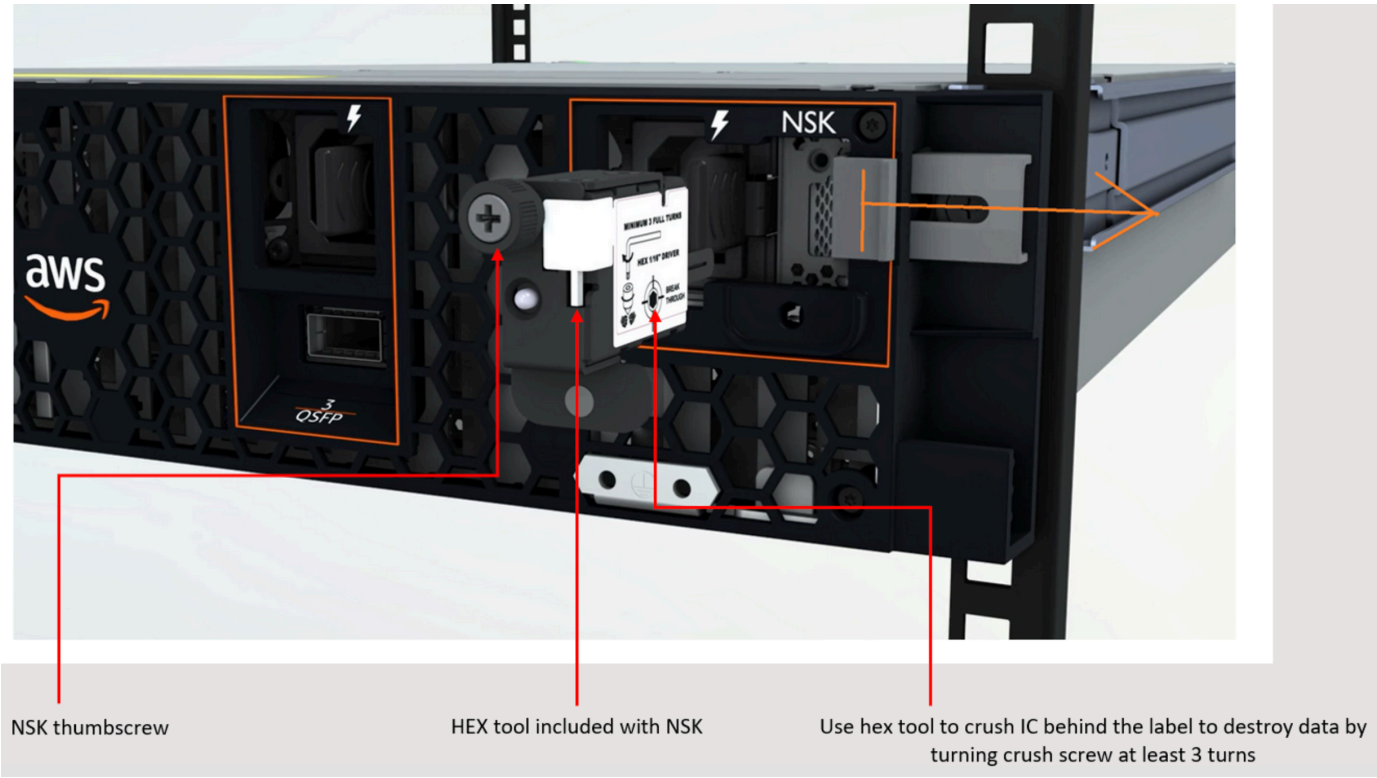
- 如果您有疑問或需要更多資訊，請參閱《AWS Support 使用者指南》中的《建立支援案例》。

以密碼編譯方式銷毀伺服器資料

需要 Nitro 安全金鑰 （NSK） 才能解密伺服器上的資料。當您將伺服器還原至 時 AWS，因為您要取代伺服器或停止服務，您可以銷毀 NSK以密碼編譯方式分割伺服器上的資料。

以密碼編譯方式銷毀伺服器上的資料

1. 將伺服器送回 之前，NSK請先從伺服器移除 AWS。
2. 確保您擁有伺服器NSK隨附的正確 。
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和 以密碼編譯方式分割伺服器上的所有資料。



Outposts 服務器 end-of-term 選項

在 AWS Outposts 學期結束時，您必須選擇以下選項：

- 續訂您的訂閱並保留您現有的 Outposts 伺服器。
- 結束您的訂閱並返回您的 Outposts 伺服器。
- 轉換為 month-to-month 訂閱並保留您現有的 Outposts 伺服器。

續訂訂閱

您必須在 Outposts 伺服器的目前訂閱結束前至少 30 天完成以下步驟。

續訂您的訂閱並保留現有的 Outposts 伺服器

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。

如果您沒有表示要續訂或返回 Outposts 服務器，則會自動將您轉換為 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

您必須在 Outposts 伺服器的目前訂閱結束前至少 30 天完成以下步驟。 AWS 除非您這樣做，否則無法啟動退貨過程。

> **Important**
>
> AWS 在您開啟支援案例以結束訂閱之後，就無法停止退貨程序。

結束您的訂閱

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. 請將伺服器關閉NOT電源或中斷網路連線，直到在支援案例中指示這樣做為止。

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 Outposts 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 新的每月訂購授權會在目前的訂閱結束後的第二天開始計算。

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。

Outposts 伺服器的文件歷史記錄

下表說明 Outposts 伺服器的文件更新。

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
Outposts 服務器介紹	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。