



Outposts 伺服器的使用者指南

# AWS Outposts



# AWS Outposts: Outposts 伺服器的使用者指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

# Table of Contents

什麼是 AWS Outposts ? .....	1
重要概念 .....	1
AWS Outposts 上的 資源 .....	2
定價 .....	4
AWS Outposts 運作方式 .....	6
網路元件 .....	6
VPC 和子網路 .....	7
路由 .....	7
DNS .....	8
服務連結 .....	8
本機網路介面 .....	9
網站需求 .....	10
設施 .....	10
聯網 .....	11
服務連結防火牆 .....	12
服務連結最大傳輸單位 (MTU) .....	12
服務連結頻寬建議 .....	12
電源 .....	13
電源支援 .....	13
耗電量 .....	13
電源線 .....	13
備用電源 .....	14
訂單履行 .....	14
開始使用 .....	15
建立 Outpost 並訂購容量 .....	15
步驟 1：建立站點 .....	15
步驟 2：建立 Outpost .....	16
步驟 3：下訂單 .....	17
步驟 4：修改執行個體容量 .....	18
後續步驟 .....	20
啟動執行個體 .....	20
步驟 1：建立子網路 .....	21
步驟 2：在 Outpost 上啟動執行個體 .....	22
步驟 3：設定連線 .....	23

步驟 4：測試連線 .....	23
服務連結 .....	26
連線能力 .....	26
最大傳輸單位 (MTU) 需求 .....	27
頻寬建議 .....	12
備援網際網路連線 .....	27
更新和服務連結 .....	27
防火牆和服務連結 .....	28
網路故障診斷 .....	29
初始評估 .....	29
步驟 1. 檢查實體連線 .....	30
步驟 2. 測試與的 Outposts 伺服器連線 AWS .....	30
步驟 3. 重新建立連線 .....	31
歸還伺服器 .....	32
步驟 1：準備伺服器以供傳回 .....	32
步驟 2：列印傳回標籤 .....	33
步驟 3：封裝伺服器 .....	33
步驟 4：透過貨運業者傳回伺服器 .....	34
本機網路介面 .....	37
本機網路介面基本概念 .....	38
效能 .....	39
Security groups (安全群組) .....	40
監控 .....	40
MAC 地址 .....	40
新增本機網路介面 .....	40
檢視本機網路介面 .....	41
設定作業系統 .....	41
本機連線 .....	41
網路中的伺服器拓撲 .....	42
伺服器實體連線 .....	42
伺服器的服務連結流量 .....	43
本機網路介面連結流量 .....	43
伺服器 IP 地址指派 .....	44
伺服器註冊 .....	45
容量管理 .....	46
檢視容量 .....	46

修改執行個體容量 .....	18
考量事項 .....	47
故障診斷容量任務問題 .....	50
訂單 <i>oo-xxxxxx</i> 與 Outpost ID <i>op-xxxxx</i> 沒有關聯 .....	50
容量計劃包含不支援的執行個體類型 .....	50
沒有 Outpost ID 為 <i>op-xxxxx</i> 的 Outpost .....	51
Outpost <i>op-XXXX</i> 已找到 Active CapacityTask <i>cap-XXXX</i> .....	51
Outpost <i>op-XXXX</i> 上的資產 <i>XXXX</i> 已找到作用中的 CapacityTask <i>cap-XXXX</i> .....	52
AssetId= <i>XXXX</i> 對 Outpost= <i>op-XXXX</i> 無效 .....	53
共用 資源 .....	55
可共用的 Outpost 資源 .....	56
共用 Outpost 資源的先決條件 .....	56
相關服務 .....	57
跨可用區域共用 .....	57
共用 Outpost 資源 .....	57
將共用的 Outpost 資源取消共用 .....	58
識別共用的 Outpost 資源 .....	59
共用的 Outpost 資源許可 .....	60
擁有者的許可 .....	60
消費者的許可 .....	60
計費和計量 .....	60
限制 .....	60
第三方區塊儲存 .....	61
外部區塊資料磁碟區 .....	61
外部區塊開機磁碟區 .....	62
安全 .....	63
資料保護 .....	63
靜態加密 .....	64
傳輸中加密 .....	64
資料刪除 .....	64
身分與存取管理 .....	64
AWS Outposts 如何與 IAM 搭配使用 .....	64
政策範例 .....	68
服務連結角色 .....	70
AWS 受管政策 .....	73
基礎設施安全性 .....	74

恢復能力 .....	75
法規遵循驗證 .....	75
監控 .....	76
CloudWatch 指標 .....	77
指標 .....	77
指標維度 .....	83
檢視 Outposts 伺服器的 CloudWatch 指標 .....	83
使用 CloudTrail 記錄 API 呼叫 .....	84
AWS Outposts CloudTrail 中的 管理事件 .....	85
AWS Outposts 事件範例 .....	85
Maintenance (維護) .....	87
更新聯絡詳細資訊 .....	87
硬體維護 .....	87
韌體更新 .....	88
電源和網路事件 .....	88
電源事件 .....	88
網路連線事件 .....	89
Resources .....	89
以密碼編譯方式銷毀伺服器資料 .....	90
使用期限結束時的選項 .....	91
續訂訂閱 .....	91
傳回伺服器 .....	92
步驟 1：準備要傳回的伺服器 .....	32
步驟 2：停用伺服器 .....	93
步驟 3：取得送回運送標籤 .....	33
步驟 4：封裝伺服器 .....	33
步驟 5：透過貨運業者傳回伺服器 .....	34
轉換訂閱 .....	97
配額 .....	98
AWS Outposts 和其他服務的配額 .....	98
文件歷史紀錄 .....	99
.....	ci

# 什麼是 AWS Outposts ？

AWS Outposts 是一種全受管服務，可將 AWS 基礎設施、服務、APIs 和工具延伸到客戶內部部署。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](#) 相同的程式設計界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 是在客戶網站部署的 AWS 運算和儲存容量集區。會 AWS 操作、監控和管理此容量，做為 AWS 區域的一部分。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 連接到相同 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

這些是的重要概念 AWS Outposts。

- Outpost 網站 – AWS 將安裝 Outpost 的客戶受管實體建築物。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。AWS Outposts 支援自助式容量管理，您可以在 Outpost 層級定義，以重新設定 Outpost 中的所有資產，或專門為每個個別資產進行設定。Outpost 資產可以是 Outposts 機架或 Outposts 伺服器內的單一伺服器。
- Outpost 設備 – 提供存取 AWS Outposts 服務的實體硬體。硬體包括擁有和管理的機架、伺服器、交換器和纜線 AWS。
- Outpost 機架 – 業界標準 42U 機架的 Outpost 形式規格。Outpost 機架包括機架掛載伺服器、交換器、網路修補程式面板、電源架和空白面板。
- 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。Outposts 伺服器為空間有限或容量需求較小的網站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 支援中心](#)。
- **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。
- **本機網路界面** – 一種網路界面，可啟用來自 Outposts 伺服器 and 內部部署網路的通訊。

## 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



Resource Type (資源類型)	機架	伺服器
<a href="#">Amazon EC2 執行個體</a>	 是	 是
<a href="#">Amazon ECS 叢集</a>	 是	 是
<a href="#">Amazon EKS 節點</a>	 是	 否

## 資料庫與分析

Resource Type (資源類型)	機架	伺服器	
<a href="#">Amazon ElastiCache 節點</a> (Redis 叢集、Memcached 叢集)	 是		否
<a href="#">Amazon EMR 叢集</a>	 是		否
<a href="#">Amazon RDS 資料庫執行個體</a>	 是		否

## 聯網



Resource Type (資源類型)	機架	伺服器	
<a href="#">App Mesh Envoy 代理</a>	 是	 是	
<a href="#">Application Load Balancer</a>	 是		否
<a href="#">Amazon VPC 子網路</a>	 是	 是	

Resource Type (資源類型)	機架	伺服器	
<a href="#">Amazon Route 53</a>	 是		否

## 儲存

Resource Type (資源類型)	機架	伺服器	
<a href="#">Amazon EBS 磁碟區</a>	 是		否
<a href="#">Amazon S3 儲存貯體</a>	 是		否

## 其他 AWS 服務

服務	機架	伺服器
AWS IoT Greengrass	 是	 是

## 定價

定價是以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。您也可以選擇合約期限和付款選項。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。您要負責安裝和封裝伺服器以進行傳回。

您需要支付共用資源以及從 AWS 區域到 Outpost 的任何資料傳輸的費用。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](#)

# AWS Outposts 運作方式

AWS Outposts 旨在您的 Outpost 和 AWS 區域之間以一致且一致的連線運作。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區域的廣域網路 (WAN) 存取權。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

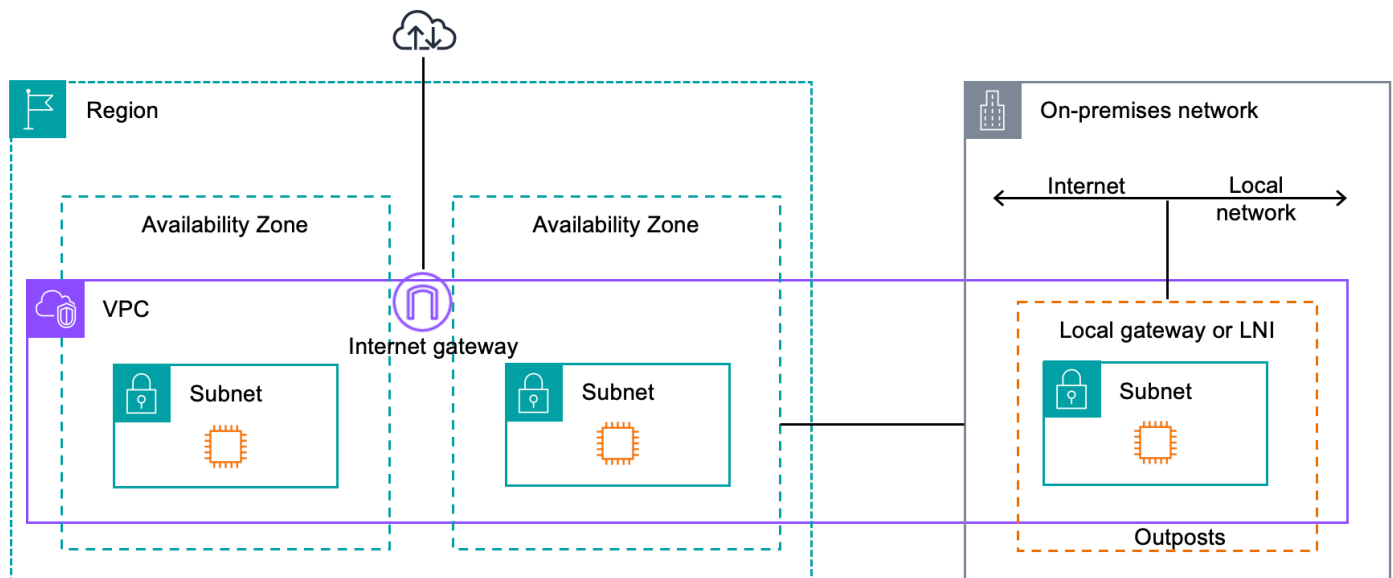
- [網路元件](#)
- [VPC 和子網路](#)
- [路由](#)
- [DNS](#)
- [服務連結](#)
- [本機網路介面](#)

## 網路元件

AWS Outposts 使用區域中可存取的 VPC 元件，包括網際網路閘道、虛擬私有閘道、Amazon VPC Transit Gateways 和 VPC 端點，將 Amazon VPC 從區域擴展 AWS 到 Outpost。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 與提供的本機網路之間的連線：
  - 對於 Outpost 機架：本機閘道
  - 對於 Outpost 伺服器：本機網路介面 (LNI)



## VPC 和子網路

虛擬私有雲端 (VPC) 跨越其區域中的所有可用區域 AWS。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 定義此項目。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 Simple Storage Service (Amazon S3)、Amazon DynamoDB 閘道端點、AWS Transit Gateway、虛擬私有閘道、網際網路閘道和 VPC 對等互連的字首清單。

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。Route 53 解析程式託管在 AWS 區域中。因此，從 Outpost 返回 AWS 區域的服務連結連線必須啟動並執行，這些 DNS 功能才能運作。

Route 53 可能會遇到較長的 DNS 解析時間，具體取決於 Outpost 與 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。您可能需要將路由新增至本機閘道路由表，才能連線，但這只是具有本機閘道的 Outposts 機架選項。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

服務連結是從您的 Outpost 返回所選 AWS 區域或 Outposts 主區域的連線。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 VPC 內流量。

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，會 AWS 建立服務連結。如需詳細資訊，請參閱：

-

- AWS Outposts 高可用性設計和架構考量 AWS 白皮書中的 [應用程式/工作負載路由](#)

## 本機網路介面

Outpost 伺服器包含本機網路介面，可讓您連線至內部部署網路。本機網路介面僅供在 Outpost 子網路上執行的 Outpost 伺服器使用。您無法從 Outposts 機架或 AWS 區域中的 EC2 執行個體使用本機網路介面。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 [Outposts 伺服器的本機網路介面](#)。

# 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 Outposts 機架的需求，請參閱 [《Outposts 機架使用者指南》](#) 中的 [Outposts 機架的站點需求](#)。AWS Outposts

## 目錄

- [設施](#)
- [聯網](#)
- [電源](#)
- [訂單履行](#)

## 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 資源的權重需求，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。導軌套件與 U 形安裝支架不相容，如下圖所示。
- 機架置放 – 建議使用深度至少為 36 英吋 (914 公釐) 的標準 19 英吋 EIA-310D 機架。AWS 提供機架掛載伺服器的導軌套件。
  - Outposts 2U 伺服器需要具有下列維度的空間：高度 3.5 英吋 (88.9 公釐)、寬度 17.5 英吋 (447 公釐)、深度 30 英吋 (762 公釐)
  - Outposts 1U 伺服器需要具有下列維度的空間：高度 1.75 英吋 (44.45 公釐)、寬度 17.5 英吋 (447 公釐)、深度 24 英吋 (610 公釐)
  - 不支援垂直掛載 AWS Outposts 伺服器。
  - Outposts 1U 伺服器寬度與 Outposts 2U 伺服器相同，但高度的一半，深度更小

如果您未將伺服器放在機架中，您仍然必須符合其他網站需求。

- 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 伺服器都包含非備援的實體上行連接埠。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。

## 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	DNS 伺服器
UDP	443、1024-65535	服務連結 IP	443	Outposts Service Link 端點
TCP	1024-65535	服務連結 IP	443	Outposts 註冊端點

您可以使用 Direct Connect 連線或公有網際網路連線，將 Outpost 連線至 AWS 區域。對於 Outposts 服務連結連線，您可以在防火牆或邊緣路由器使用 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 Outpost 和父 AWS 區域中的服務連結端點之間支援 1500 位元組的 MTU。如需服務連結的詳細資訊，請參閱《AWS Outposts 伺服器使用者指南》中的[AWS Outposts AWS 區域連線](#)。

## 服務連結頻寬建議

為了獲得最佳體驗和彈性，AWS 需要您使用至少 500 Mbps 的備援連線，以及最多 175 毫秒的往返延遲，才能連線至 AWS 區域。每個 Outposts 伺服器的使用率上限為 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《[伺服器使用者指南](#)》中的[伺服器的服務連結流量](#)。

### AWS Outposts

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、高載速度需求，以及通往區域的 Amazon VPC 流量。請注意，AWS Outposts 伺服器不會快取 AMIs。每次啟動執行個體都會從區域下載 AMI。

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。

# 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/>。

## 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确轉接器或電源線，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

為了履行訂單，AWS 會將 Outposts 伺服器設備，包括軌道掛載和所需的電源和網路纜線，運送到您提供的地址。運送伺服器的包裝盒尺寸如下：

- 2U 伺服器的包裝盒：
  - 長度：44 英吋 / 111.8 公分
  - 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《[伺服器使用者指南](#)》中的[伺服器的服務連結流量](#)。AWS Outposts

當您確認 Outposts 伺服器的 Amazon EC2 容量可從取得時，安裝即完成 AWS 帳戶。

# 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 帳戶登入。建立站點和 Outpost。然後，為您需要的 Outpost 伺服器下訂單。

### 先決條件

- 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 計劃或 AWS Enterprise On-Ramp Support 計劃。
- 決定 AWS 帳戶 您將使用哪個 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。

## 先決條件

- 確定操作地址。

## 建立網站

1. 登入 AWS。
2. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
3. 若要選取父項 AWS 區域，請使用頁面右上角的區域選擇器。
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，輸入任何其他可能有助於 AWS 了解網站的資訊。
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。

### 先決條件

- 決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。

**Note**

完成訂單後，您將無法修改 Outpost 的 AZ 錨點或實體位置。

## 步驟 3：下訂單

訂購您需要的 Outposts 伺服器。

**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 支援中心](#)。

### 先決條件

- 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 Outpost 訂單的容量都會以預設容量組態設定。您可以轉換預設組態來建立各種執行個體，以符合您的業務需求。若要這樣做，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 Outpost 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。


### 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已預先選取數量上限的一個執行個體大小。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，通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. 您也可以請求 AWS Outposts 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，請確定已為至少一個執行個體大小指定執行個體數量。
8. 選擇下一步。
9. 在檢閱和建立頁面上，驗證您要請求的更新。
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。停止這些執行個體之後，AWS Outposts 會執行任務。

## Upload JSON file


1. 選擇上傳容量組態。
2. 選擇下一步。
3. 在上傳容量組態計劃頁面上，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. 在容量組態計劃區段中檢閱 JSON 檔案的內容。
5. 選擇下一步。
6. 在檢閱和建立頁面上，驗證您要請求的更新。
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。停止這些執行個體之後，AWS Outposts 會執行任務。


## 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 支援中心](#)。

為了履行訂單，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 [伺服器安裝指南](#)。

當您可從 AWS 帳戶使用 Outpost 的 Amazon EC2 容量時，安裝即完成。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”](#)。

 Note

完成訂單後，您將無法修改服務連結組態。

## 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 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

如果您要在由另一個與您共用的 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 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
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，您必須為本機網路介面啟用于網路。使用來自的 [modify-subnet-attribute](#) 命令 AWS CLI。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的執行個體尺寸，以滿足您的應用程式需求。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](#)。
- 您必須使用僅具有單一 EBS 快照的 Amazon EBS 後端 AMI。不支援具有多個 EBS 快照 AMIs。
- 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。
- 若要使用相容第三方儲存體支援的區塊資料或開機磁碟區，您必須佈建和設定這些磁碟區，以與 Outposts 上的 EC2 執行個體搭配使用。如需詳細資訊，請參閱[第三方區塊儲存](#)。
- 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 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
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 主控台內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。請注意，顯示為灰色的執行個體無法使用。
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. (選用) 您可以新增 [第三方資料磁碟區](#)。

- a. 展開設定儲存。在外部儲存磁碟區旁，選擇編輯。
  - b. 針對儲存網路通訊協定，選擇 iSCSI。
  - c. 輸入啟動器 IQN，然後新增目標 IP 地址、連接埠和外部儲存陣列的 IQN。
8. 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](#)：Amazon EC2

## 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。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

從本機網路的電腦，對 Outpost 執行個體的本機網路介面 IP 地址執行 ping 命令。

```
ping 10.0.3.128
```

以下為範例輸出。

```
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。如需有關連線至 EC2 執行個體的資訊，請參閱《Amazon [EC2 使用者指南](#)》中的[連線至 EC2 執行個體](#)。Amazon EC2

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
```

以下為範例輸出。

```
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 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，在 AWS 區域中指定執行個體的 IP 地址。

```
ping 10.0.1.5
```

以下為範例輸出。

```
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 AWS 區域連線

AWS Outposts 透過服務連結連線支援廣域網路 (WAN) 連線。

## Note

您無法針對將您的 Outpost 伺服器連線至 AWS 區域或 AWS Outposts 主要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](#)
- [更新和服務連結](#)
- [防火牆和服務連結](#)
- [Outposts 伺服器網路疑難排解](#)

## 透過服務連結的連線

在 AWS Outposts 佈建期間，您或 AWS 會建立服務連結連線，將您的 Outpost 伺服器連線到您選擇的 AWS 區域或主要區域。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 VPC 內流量。

Outpost 能夠建立透過公有區域連線連回 AWS 區域的服務連結 VPN。若要這樣做，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。如需公有範圍的詳細資訊 AWS，請參閱《Amazon VPC 使用者指南》中的 [AWS IP 地址範圍](#)。

建立服務連結後，Outpost 會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 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)。

注意下列事項：

- 網路必須在 Outpost 和父 AWS 區域中的服務連結端點之間支援 1500 位元組的 MTU。
- 從 Outposts 中的執行個體到區域中執行個體的流量具有 1300 個位元組的 MTU，由於封包額外負荷，因此低於 1500 個位元組的必要 MTU。

## 服務連結頻寬建議

為了獲得最佳體驗和彈性，AWS 需要您使用至少 500 Mbps 的備援連線，以及最多 175 毫秒的往返延遲，才能連線至 AWS 區域。每個 Outposts 伺服器的使用率上限為 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、高載速度需求，以及通往區域的 Amazon VPC 流量。請注意，AWS Outposts 伺服器不會快取 AMIs。每次啟動執行個體都會從區域下載 AMI。

我們強烈建議諮詢您的 AWS 銷售代表或 APN 合作夥伴，以評估您地理位置中可用的主區域選項，並針對工作負載的服務連結頻寬和延遲需求尋求自訂建議。

## 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 [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。

## 更新和服務連結

AWS 會維護 Outposts 伺服器與其父 AWS 區域之間的安全網路連線。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 VPC 內流量來管理 Outpost 至關重要。[AWS Well-Architected](#) 最佳實務建議透過主動-主動設計，將應用程式部署到父系至不同可用區域的兩個 Outpost。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，以維持營運品質和效能。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 VPC 連線至區域內託管資源的工作負載。不過，周遊[本機網路界面 \(LNI\)](#) 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。

## 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 區域延伸到 Outpost。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 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。

如果您使用同時具備 UDP 和 TCP 感知的狀態防火牆來限制與服務連結 VLAN 相關的連線，則可以拒絕所有傳入連線。如果防火牆以有狀態的方式運作，允許來自 Outposts 服務連結的傳出連線應該會自動允許回傳的回覆流量，而無需明確規則組態。只有從 Outpost 服務連結啟動的傳出連線需要設定為允許。

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	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

如果您使用非狀態防火牆來限制與服務連結 VLAN 相關的連線，則必須允許從 Outposts 服務連結啟動到區域的公有 AWS Outposts 網路的傳出連線。您還必須明確允許來自 Outposts 區域的公有網路傳入服務連結 VLAN 的中的回覆流量。連線一律會從 Outposts 服務連結開始傳出，但必須允許回覆流量回到服務連結 VLAN。

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	DNS 伺服器
UDP	443、1024-65535	服務連結 IP	443	AWS Outposts Service Link 端點
TCP	1025-65535	服務連結 IP	443	AWS Outposts Service Link 端點
UDP	53	DNS 伺服器	1025-65535	服務連結 IP
UDP	443	AWS Outposts Service Link 端點	443、1024-65535	服務連結 IP
TCP	443	AWS Outposts Service Link 端點	1025-65535	服務連結 IP

### 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。

## Outposts 伺服器網路疑難排解

使用此檢查清單來協助針對狀態為 DOWN 的服務連結進行疑難排解。

### 初始評估

透過 Amazon CloudWatch 指標驗證服務連結的狀態：

1. 在命名空間中 AWS Outposts 監控 ConnectedStatus 指標。
2. 如果平均值小於 1，這可確認服務連結受損。
3. 如果服務連結受損，請完成下列各節中的步驟來解析並重新建立連線。

## 步驟 1. 檢查實體連線

1. 確認您使用的是提供的 QSFP 分線。如果問題仍然存在，如果有的話，請使用不同的 QSFP 分線進行測試。
2. 確認 Outposts 伺服器中的 QSFP 分線是否穩固就位。
3. 確認纜線 1 (LNI) 已穩固地放置在交換器中。
4. 確認纜線 2 (服務連結) 已穩固地放置在交換器中。
5. 完成一般開關狀態檢查，例如檢查連結燈。

## 步驟 2. 測試與的 Outposts 伺服器連線 AWS

[建立與 Outposts 伺服器的序列連線](#)，並執行下列測試：

1. [測試連結](#)。
  - a. 如果成功，請繼續下一個測試。
  - b. 如果失敗，則為 [驗證網路組態](#)。
2. [測試 DNS 解析](#)。
  - a. 如果成功，請繼續下一個測試。
  - b. 如果失敗，則為 [檢查防火牆規則](#)。
3. [測試 AWS 區域的存取權](#)。
  - a. 如果成功，請繼續重新建立連線。
  - b. 如果失敗，則為 [驗證 MTU](#)。

### 驗證網路組態

請確定您的交換器符合下列規格：

- 基本組態 — 服務連結連接埠必須是具有閘道的 VLAN 的未標記存取連接埠，以及 AWS 端點的路由。
- 連結速度 — 交換器連接埠必須將連結速度設定為 10 Gb，且必須關閉自動交涉。

## 驗證 MTU

網路必須在 Outpost 和父 AWS 區域中的服務連結端點之間支援 1500 位元組的 MTU。如需服務連結的詳細資訊，請參閱[AWS Outposts AWS 區域連線](#)。

## 檢查防火牆規則

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。您必須允許從 AWS 區域返回 Outpost 的傳出連線，如下表所示。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	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

## 步驟 3。重新建立連線

如果先前的檢查通過，但服務連結仍然存在 DOWN(ConnectedStatus 在 CloudWatch 中小於 1)，則請依照[使用 Outpost 組態工具授權 Outposts 伺服器](#)中的步驟重新建立連線。

### Note

如果服務連結仍然關閉，請在 [AWS 支援中心](#) 建立案例。

# 傳回 Outposts 伺服器

## Note

如果您收到的伺服器在運送時受損，請參閱伺服器AWS Outposts 安裝指南中的[步驟 2：檢查 Outposts 伺服器設備](#)。

若要傳回使用中且您想要取代 或訂閱已結束的伺服器，請檢閱本節。

如果 AWS Outposts 偵測到伺服器中有瑕疵，我們會通知您，開始替換程序以傳送新的伺服器給您，並透過主控台提供您傳回標籤 AWS Outposts。當您傳回 Outposts 伺服器時，不會向您收取運送費用。不過，如果您傳回損壞的伺服器，可能會產生費用。

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：列印傳回標籤](#)
- [步驟 3：封裝伺服器](#)
- [步驟 4：透過貨運業者傳回伺服器](#)

## 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所存放資料的備份。

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](#)中的指示。
5. 銷毀 Nitro 安全金鑰 (NSK)，以密碼編譯方式銷毀伺服器上的資料。若要銷毀 NSK，請遵循[密碼編譯碎片伺服器資料](#)中的指示。

## 步驟 2：列印傳回標籤

### Important

您只能使用 AWS 提供的傳回標籤，因為它包含您要傳回之伺服器的特定資訊，例如資產 ID。請勿建立您自己的傳回標籤。

若要取得您的傳回標籤：

1. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
2. 在導覽窗格上，選擇 訂單。
3. 選擇您要傳回之伺服器的順序。
4. 在訂單詳細資訊頁面的訂單狀態區段中，選擇列印傳回標籤。

### Note

在目前的訂閱結束之前傳回 Outpost 伺服器，不會終止與此 Outpost 相關的任何未結費用。

## 步驟 3：封裝伺服器

若要封裝您的伺服器，請使用提供的方塊和封裝材料 AWS。

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

或者，聯絡 [AWS 支援中心](#) 要求一個箱子。

2. 將 AWS 提供的傳回標籤貼到方塊外部。

### Important

確認傳回標籤上的資產 ID 與您傳回的伺服器上的資產 ID 相符。

資產 ID 位於伺服器正面的提取標籤上。範例：1203779889 或 9305589922

3. 安全地密封箱子。

## 步驟 4：透過貨運業者傳回伺服器

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 提供的傳回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 <a href="#">AWS 支援中心</a> 。請在您的請求中包含下列資訊： <ul style="list-style-type: none"> <li>• AWS 所提供傳回標籤上的追蹤號碼</li> <li>• 您希望貨運業者前來收取伺服器的日期和時間</li> <li>• 聯絡人名稱</li> <li>• 電話號碼</li> <li>• 電子郵件地址</li> </ul>
巴林	
巴西	
汶萊	
加拿大	
智利	
哥倫比亞	
香港	
印度	
印尼	

Country	聯絡
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	
泰國	
阿拉伯聯合大公國	
越南	
墨西哥	AWS 聯絡 <a href="#">資料庫 Schenker</a> 並請求從您的位置取件。資料庫 Schenker 接著會與您聯絡，以排定收件의日期和時間。

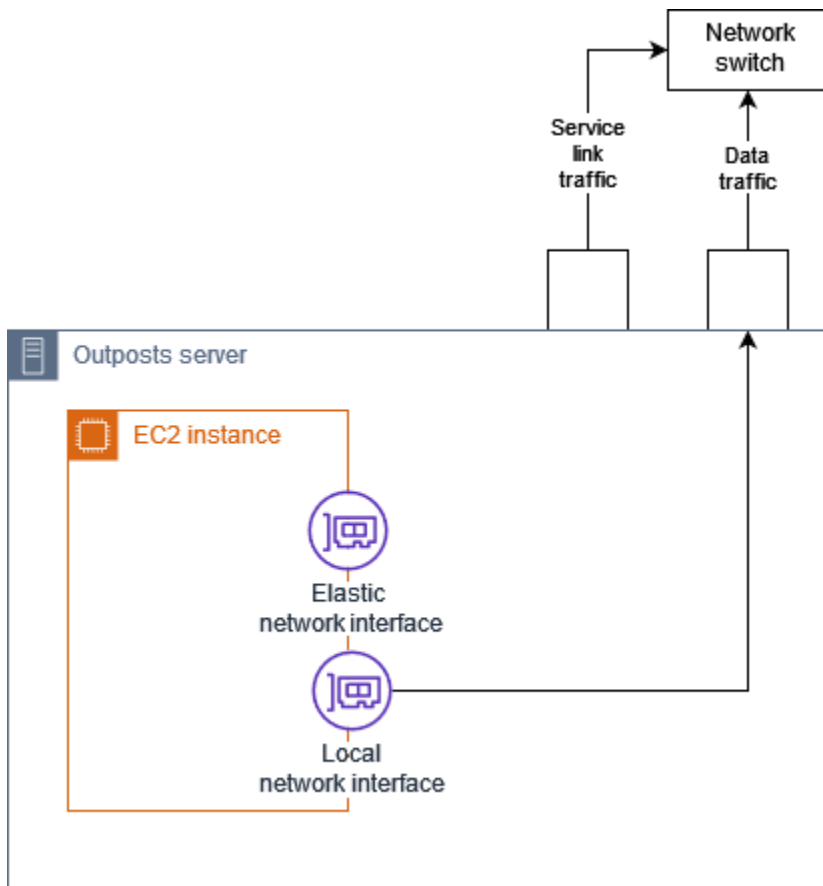
Country	聯絡
美國	<p>聯絡 <a href="#">UPS</a>。</p> <p>您可用下列方式歸還伺服器：</p> <ul style="list-style-type: none"><li>• 在您現場進行的例行 UPS 收件期間歸還伺服器。</li><li>• 將伺服器放到 <a href="#">UPS 地點</a>。</li><li>• 安排您偏好的日期和時間<a href="#">收件</a>。輸入 AWS 提供的免費運送回郵標籤中的追蹤號碼。</li></ul>
所有其他國家/地區	<p>聯絡 <a href="#">DHL</a>。</p> <p>您可用下列方式歸還伺服器：</p> <ul style="list-style-type: none"><li>• 將伺服器放到 <a href="#">DHL 地點</a>。</li><li>• 安排您偏好的日期和時間<a href="#">收件</a>。輸入 AWS 所提供歸還標籤中的 DHL Waybill 號碼，即可免費運送。</li></ul> <p>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。</p>

## Outposts 伺服器的本機網路介面

使用 Outposts 伺服器時，本機網路介面是一種邏輯聯網元件，可將 Outposts 子網路中的 Amazon EC2 執行個體連線至您的內部部署網路。

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 VPC 網路連線來存取 的公有區域端點 AWS 服務，也可以使用界面 VPC 端點來存取 AWS 服務 AWS PrivateLink。如需詳細資訊，請參閱[AWS Outposts AWS 區域連線](#)。

## 目錄

- [本機網路介面基本概念](#)
- [將本機網路界面新增至 Outposts 子網路中的 EC2 執行個體](#)
- [Outposts 伺服器的本機網路連線](#)

## 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。本機網路界面不會為 Outposts 伺服器提供對 VPC layer-3 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[網路介面配額](#)。
- 每個 EC2 執行個體都會有一個本機網路介面。
- 本機網路介面無法使用執行個體的主要網路介面。
- 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亂模式或 MAC 位址詐騙。

## 效能

每個執行個體大小的本機網路界面提供一部分的實體 10 GbE 可用頻寬。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

## Security groups (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。本機網路介面未連接到 VPC。本機網路介面連接到本機網路。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 指標是針對每個本機網路介面所產生，就像為彈性網路介面產生一樣。如需詳細資訊，請參閱《Amazon [EC2 使用者指南](#)》中的[監控 EC2 執行個體上 ENA 設定的網路效能](#)。Amazon EC2

## MAC 地址

AWS 提供本機網路介面的 MAC 地址。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 地址。AWS 可以重複使用不再使用的 MAC 地址。

## 將本機網路介面新增至 Outposts 子網路中的 EC2 執行個體

您可以在啟動期間或之後，將本機網路介面新增至 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。如果這不是您在為本機網路介面啟用 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，從使用以下命令 AWS CLI：[create-network-interface](#) 和 [attach-network-interface](#)。

啟動執行個體後，請使用下列程序來新增本機網路介面。如需有關在執行個體啟動期間新增執行個體的資訊，請參閱在 [Outpost 上啟動執行個體](#)。

將本機網路介面新增至 EC2 執行個體

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
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。安全群組不適用於本機網路介面，因此您選擇的安全群組不相關。
  - 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。如果您將 1 指定為 Outpost 子網路本機網路界面的裝置索引，則此網路界面是執行個體的本機網路界面。

## 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 之本機網路界面的私有 IPv4 地址。此地址不是本機網路介面的 IP 地址，而且無法使用。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。您必須為訪客作業系統內的本機網路界面設定 IP 地址，無論是靜態或透過 DHCP 伺服器。

## 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。

## Outposts 伺服器的本機網路連線

使用此主題來了解託管 Outposts 伺服器的網路佈線和拓撲需求。如需詳細資訊，請參閱[Outposts 伺服器的本機網路界面](#)。

### 目錄

- [網路中的伺服器拓撲](#)
- [伺服器實體連線](#)
- [伺服器的服務連結流量](#)
- [本機網路介面連結流量](#)
- [伺服器 IP 地址指派](#)

- [伺服器註冊](#)

## 網路中的伺服器拓撲

Outposts 伺服器需要您聯網設備的兩個不同連線。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 Outposts 伺服器流量類型和標籤。

流量標籤	Description
2	服務連結流量 – 此流量可讓 Outpost 和 AWS 區域之間的通訊，以管理 Outpost 和 AWS 區域和 Outpost 之間的 VPC 內流量。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	本機網路介面連結流量 – 此流量可讓您透過本機網路介面，從 VPC 與本機 LAN 進行通訊。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 伺服器都包含非備援的實體上行連接埠。連接埠有自己的速度和連接器需求，如下所示：

- 10Gbe – 連接器類型 QSFP+

### QSFP+ 纜線

QSFP+ 纜線具有您連接至 Outposts 伺服器上連接埠 3 的連接器。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。Outposts 伺服器需要這兩個介面才能運作。將 2 介面用於服務連結流量，將 1 介面用於本機網路介面連結流量。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

服務連結連線必須有公有 DNS 可供 Outpost 在 AWS 區域中探索其註冊端點。連線可以在 Outposts 伺服器和註冊端點之間具有 NAT 裝置。如需公有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《》中的[AWS Outposts 端點和配額](#)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

## 本機網路介面連結流量

將上游網路裝置上的本機網路介面連結連接埠設定為本機網路上 VLAN 的標準存取連接埠。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。如果您將本機網路介面設定為幹線，則必須確保您的作業系統標記 VLAN 流量。

下列範例顯示如何在 Amazon Linux 2023 上設定本機網路介面的 VLAN 標記。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 上設定本機網路介面的 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 VLAN 裝置。在此範例中：

- 本機網路界面的界面名稱為 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 Linux 2 使用者指南》中的[使用 ec2-net-utils for AL2 設定網路介面](#)。
- 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

執行個體上的 AWS Outposts 伺服器服務連結和本機網路介面不需要公有 IP 地址指派。對於服務連結，您可以手動指派 IP 地址或使用動態主機控制通訊協定 (DHCP)。若要設定服務連結連線，請參閱 AWS Outposts 伺服器安裝指南中的[設定和測試連線](#)。

若要設定本機網路介面連結，請參閱 [the section called “設定作業系統”](#)。

**Note**

請確定您使用 Outposts 伺服器的穩定 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

當 Outpost 伺服器在本機網路上建立連線時，他們會使用服務連結連線來連線至 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。Outposts 伺服器使用 TCP 連接埠 443 來促進透過公有網際網路與區域的通訊。Outpost 伺服器不支援透過 VPC 的私有連線。

# 的容量管理 AWS Outposts

Outpost 會在您的站點提供 AWS 運算和儲存容量集區，做為 AWS 區域中可用區域的私有延伸。由於 Outpost 中可用的運算和儲存容量有限，且取決於您站點 AWS 安裝的資產大小和數量，因此您可以決定執行初始工作負載所需的 AWS Outposts 容量為多少 Amazon EC2、Amazon EBS 和 Amazon S3、適應未來成長，並提供額外的容量來緩解伺服器故障和維護事件。

## 主題

- [檢視 AWS Outposts 容量](#)
- [修改 AWS Outposts 執行個體容量](#)
- [故障診斷容量任務問題](#)

## 檢視 AWS Outposts 容量

您可以在執行個體或 Outpost 層級檢視容量組態。

使用主控台檢視 Outpost 的容量組態

1. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
2. 從左側導覽窗格中，選擇 Outpost。
3. 選擇 Outpost。
4. 在 Outpost 詳細資訊頁面上，選取執行個體檢視或機架檢視。
  - 執行個體檢視 - 提供 Outposts 上設定的執行個體，以及依大小和系列分佈執行個體的相關資訊。
  - 機架檢視 - 提供每個 Outpost 內每個資產上執行個體的視覺化，並可讓您選取修改執行個體容量以變更執行個體容量。

## 修改 AWS Outposts 執行個體容量

每個新 Outpost 訂單的容量都會以預設容量組態設定。您可以轉換預設組態來建立各種執行個體，以符合您的業務需求。若要這樣做，您可以建立容量任務、選擇 Outpost 或單一資產、指定執行個體大小和數量，以及執行容量任務以實作變更。

## 考量事項

在修改執行個體容量之前，請考慮下列事項：

- 容量任務只能由擁有 Outpost 資源（擁有者）AWS 的帳戶執行。消費者無法執行容量任務。如需擁有者和消費者的詳細資訊，請參閱[共用您的 AWS Outposts 資源](#)。
- 執行個體大小和數量可以在 Outpost 層級或個別資產層級定義。
- 容量會根據可能的組態和最佳實務，在 Outpost 中的資產或所有資產之間自動設定。
- 容量任務執行時，可能會隔離與所選前哨站相關聯的資產。因此，我們建議您只在不預期在 Outpost 上啟動新執行個體時，才建立容量任務。
- 您可以選擇立即執行容量任務，或在接下來的 48 小時內持續定期嘗試。選擇立即執行需要較少的資產隔離時間，但如果執行個體需要停止才能執行任務，任務可能會失敗。選擇定期執行可讓更多時間在任務失敗之前停止執行個體，但資產可能會隔離更長的時間。
- 有效容量組態可能無法在資產上利用所有可用的 vCPU。在這種情況下，執行個體類型區段結尾的訊息會通知您容量不足，但允許根據請求套用組態。
- 當您在主控台中修改 Outpost 時，並非所有支援的執行個體都會顯示，因為在主控台中並未完全支援混合磁碟後端執行個體與 non-disk-backed 執行個體。若要存取所有可能的執行個體，請利用 [StartCapacityTask](#) API。
- 您只能修改現有的 Outposts 容量組態，以從個別資產模型支援的執行個體系列中使用有效的 Amazon EC2 執行個體大小。
- 如果您的 Outpost 上執行了您不想停止執行容量任務的執行個體，請在執行個體區段下選取其個別的執行個體 ID 以保持原狀 – 選用，並確保在更新後的容量組態中保留此執行個體大小的必要數量。這將保留用於在容量任務執行時支援生產工作負載的執行個體。
- 在執行個體系列中設定具有多個執行個體大小的資產時，請使用 Auto-balance 來確保您不會嘗試過度佈建或佈建不足。不支援過度佈建，且會導致容量任務失敗。
- 只要套用到互斥的 AssetIDs 集，就可以平行執行數個容量任務。例如，您可以同時為不同的 AssetIDs 建立多個資產層級容量任務。不過，如果有正在執行的 Outpost 層級任務，您就無法同時建立另一個 Outpost 或資產層級任務。同樣地，如果有執行中的資產層級任務，您就無法在相同的 AssetID 上同時建立 Outpost 層級任務或資產層級任務。

使用主控台修改 Outpost 的容量組態

1. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
2. 從左側導覽窗格中，選擇容量任務。

3. 在容量任務頁面上，選擇建立容量任務。
4. 在入門頁面上，選擇要設定的順序、Outpost 或資產。
5. 若要修改容量，請指定修改方法的選項：主控台中的 e 步驟或上傳 JSON 檔案。
  - 修改容量組態計劃以使用 主控台 中的步驟
  - 上傳容量組態計劃以上傳 JSON 檔案

### Note

- 若要防止容量管理建議特定執行個體停止，請指定不應停止的執行個體。這些執行個體將從要停止的執行個體清單中排除。

### Console steps

1. 選擇執行個體檢視或機架檢視。
2. 選擇修改 Outpost 容量組態或對單一資產進行修改。
3. 如果與目前的選擇不同，請選擇 Outpost 或資產。
4. 選擇立即執行此容量任務，或在 48 小時內定期執行。
5. 選擇下一步。
6. 在設定執行個體容量頁面上，每個執行個體類型會顯示已預先選取數量上限的一個執行個體大小。若要新增更多執行個體大小，請選擇新增執行個體大小。
7. 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。
8. 檢視每個執行個體類型區段結尾的訊息，通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。
9. 您也可以請求 AWS Outposts 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。
10. 針對每個執行個體類型，請確定已為至少一個執行個體大小指定執行個體數量。
11. 或者，選擇執行個體以保持原狀。
12. 選擇下一步。
13. 在檢閱和建立頁面上，驗證您要請求的更新。

14. 選擇建立。AWS Outposts 建立容量任務。
15. 在容量任務頁面上，監控任務的狀態。

### Upload a JSON file

1. 選擇上傳容量組態。
2. 選擇下一步。
3. 在上傳容量組態計劃頁面上，上傳指定執行個體類型、大小和數量的 JSON 檔案。或者，您可以在 JSON 檔案中指定 [InstancesToExclude](#) 和 [TaskActionOnBlockingInstances](#) 參數。

### Example

範例 JSON 檔案：

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

4. 在容量組態計劃區段中檢閱 JSON 檔案的內容。
5. 選擇下一步。

6. 在檢閱和建立頁面上，驗證您要請求的更新。
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。

## 故障診斷容量任務問題

檢閱下列已知問題，以新順序解決與容量管理相關的問題。如果您沒有看到您的問題，請聯絡 支援。

### 訂單 **oo-xxxxxx** 與 Outpost ID **op-xxxxx** 沒有關聯

當您使用 AWS CLI 或 API 執行 `StartCapacityTask` 且請求中的 Outpost ID 不符合 Outpost ID 順序時，就會發生此問題。

若要解決此問題：

1. 登入 AWS。
2. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
3. 從導覽窗格中，選擇訂單。
4. 選取訂單，並確認訂單狀態為下列其中一項：PREPARING、IN\_PROGRESS 或 ACTIVE。
5. 依序記下 Outpost ID。
6. 在 StartCapacityTask API 請求中輸入正確的 Outpost ID。

### 容量計劃包含不支援的執行個體類型

當您使用 AWS CLI 或 API 來建立或修改容量任務，且請求包含不支援的執行個體類型時，就會發生此問題。

若要解決此問題，請使用 主控台 或 CLI。

使用主控台

1. 登入 AWS。
2. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
3. 從導覽窗格中，選擇容量任務。
4. 使用上傳容量組態選項，上傳具有相同執行個體類型的 JSON。
5. 主控台會顯示錯誤訊息，其中包含支援的執行個體類型清單。

6. 更正移除不支援執行個體類型的請求。
7. 使用更正的 JSON 在主控台上建立或修改容量任務，或使用 CLI 或 API 搭配此更正的執行個體類型清單。

### 使用 CLI

1. 使用 [GetOutpostSupportedInstanceTypes](#) 命令查看支援的執行個體類型清單。
2. 使用正確的執行個體類型清單建立或修改容量任務。

## 沒有 Outpost ID 為 **op-xxxxx** 的 Outpost

當您使用 AWS CLI 或 API 執行 [StartCapacityTask](#) 且請求包含因下列其中一個原因而無效的 Outpost ID 時，就會發生此問題：

- Outpost 位於不同的 AWS 區域。
- 您沒有此 Outpost 的許可。
- Outpost ID 不正確。

若要解決此問題：

1. 請注意您在 StartCapacityTask API 請求中使用的 AWS 區域。
2. 使用 [ListOutposts](#) API 動作來取得您在 區域中擁有的 Outposts 清單 AWS。
3. 檢查是否已列出 Outpost ID。
4. 在 StartCapacityTask 請求中輸入正確的 Outpost ID。
5. 如果您找不到 Outpost ID，請再次使用 ListOutposts API 動作來檢查 Outpost 是否存在於其他 AWS 區域。

## Outpost **op-XXXX** 已找到 Active CapacityTask **cap-XXXX**

當您使用 AWS Outposts 主控台或 API 在 Outpost 上執行 [StartCapacityTask](#)，且 Outpost 已有執行中的容量任務時，就會發生此問題。如果容量任務具有下列任何狀態，則視為正在執行：REQUESTED、WAITING\_FOR\_EVACUATION、IN\_PROGRESS 或 CANCELLATION\_IN\_PROGRESS。

若要解決此問題，請使用 AWS Outposts 主控台或 CLI。

## 使用主控台

1. 登入 AWS。
2. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
3. 從導覽窗格中，選擇容量任務。
4. 確保 OutpostId 沒有執行中的容量任務。
5. 如果 OutpostId 有執行中的容量任務，請等待它們終止，或視需要將其取消。
6. 當請求的 OutpostId 沒有執行中的容量任務時，請重試您的請求以建立容量任務。

## 使用 CLI

1. 使用 [ListCapacityTasks](#) 命令尋找 Outpost 的執行中容量任務。
2. 等待所有執行中的容量任務終止，或視需要將其取消。
3. 當請求的 OutpostId 沒有執行中的容量任務時，請重試您的請求以建立容量任務。

## Outpost op-XXXX 上的資產 XXXX 已找到作用中的 CapacityTask cap-XXXX

當您使用 AWS Outposts 主控台或 API 在資產上執行 [StartCapacityTask](#)，且資產已有執行中的容量任務時，就會發生此問題。如果容量任務具有下列任何狀態，則視為正在執行：REQUESTED、WAITING\_FOR\_EVACUATION、IN\_PROGRESS 或 CANCELLATION\_IN\_PROGRESS。

若要解決此問題，請使用 AWS Outposts 主控台或 CLI。

## 使用主控台

1. 登入 AWS。
2. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
3. 從導覽窗格中，選擇容量任務。
4. 確保 OutpostId 沒有執行中的容量任務，且 AssetId 沒有執行中的資產層級容量任務。
5. 如果有執行中的容量任務，請等待它們終止，或視需要將其取消。
6. 當沒有執行中的容量任務時，請重試您的請求以建立容量任務。

## 使用 CLI

1. 使用 [ListCapacityTasks](#) 命令尋找 OutpostID 和 AssetID 的執行中容量任務。
2. 確保 OutpostId 沒有執行中的 Outpost 層級容量任務，且 AssetId 沒有執行中的資產層級容量任務。
3. 如果有執行中的容量任務，請等待它們終止，或視需要將其取消。
4. 重試您的請求以建立容量任務。

## AssetId=XXXX 對 Outpost=op-XXXX 無效

當您使用 AWS Outposts 主控台或 API 在資產上執行 [StartCapacityTask](#)，且 AssetID 因下列其中一個原因而無效時，就會發生此問題：

- 資產未與 Outpost 建立關聯。
- 資產已隔離。

若要解決此問題，請使用 AWS Outposts 主控台或 CLI。

### 使用主控台

1. 登入 AWS。
2. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
3. 選擇 Outpost 的機架檢視。
4. 確認請求的 AssetId 與 Outpost 相關聯，且未標示為隔離的主機。
  - a. 如果資產已隔離，這可能是因為容量任務正在其上執行。您可以導覽至容量任務面板，並檢查是否有任何執行中的 Outpost 或 OutpostId 和 AssetId 的資產層級任務。如果有的話，請等待任務終止，讓資產再次可用。
  - b. 如果隔離資產沒有執行中的容量任務，則資產可能會降級。
5. 在您確認資產存在且處於有效狀態後，請重試您的請求以建立容量任務。

## 使用 CLI

1. 使用 [ListAssets](#) 命令來尋找與 OutpostID 相關聯的資產。
2. 確認請求的 AssetId 與 Outpost 相關聯，且其狀態為 ACTIVE。

- a. 如果資產狀態不是 ACTIVE，這可能是因為容量任務正在其上執行。使用 [ListCapacityTasks](#) 命令來判斷 OutpostId 和 AssetId 是否有正在執行的 Outpost 或 AssetId 層級任務。如果有的話，請等待任務終止，並再次讓資產變成作用中。
  - b. 如果隔離資產沒有執行中的容量任務，則資產可能會降級。
3. 在您確認資產存在且處於有效狀態後，請重試您的請求以建立容量任務。

# 共用您的 AWS Outposts 資源

透過 Outpost 共用，Outpost 擁有者可以與同一 AWS 組織下的其他 AWS 帳戶共用其 Outpost 和 Outpost 資源，包括 Outpost 網站和子網路。身為 Outpost 擁有者，您可以集中建立和管理 Outpost 資源，並跨 AWS 組織內的多個 AWS 帳戶共用資源。這可讓其他取用者使用 Outpost 站點、設定 VPC，以及在共用的 Outpost 上啟動並對執行個體進行執行。

在此模型中，擁有 Outpost 資源 (擁有者) AWS 的帳戶會與相同組織中的其他 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。擁有者無法修改消費者在他們共用的容量保留中啟動的執行個體。

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：

- 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](#)
- [共用 Outpost 資源的先決條件](#)
- [相關服務](#)
- [跨可用區域共用](#)
- [共用 Outpost 資源](#)
- [將共用的 Outpost 資源取消共用](#)
- [識別共用的 Outpost 資源](#)
- [共用的 Outpost 資源許可](#)
- [計費和計量](#)
- [限制](#)

## 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。

對於 Outpost 伺服器資源，請參閱[使用共用 AWS Outposts 資源](#)。

這些是 Outposts 伺服器可用的資源。對於 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：
  - 在專用執行個體上啟動並執行 EC2 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 AWS Outposts API 來檢視 Outpost 的相關資訊。
- 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。
  - 在子網路中啟動並執行 EC2 執行個體。

使用 Amazon VPC 主控台來共用 Outpost 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 AWS Organizations 中的組織或任一組織單位共用 Outpost 資源，您必須透過 AWS Organizations 啟用共用功能。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

Outpost 資源共用與 AWS Resource Access Manager (AWS RAM) 整合。AWS RAM 是一項服務，可讓您與任何 AWS 帳戶或透過 共用 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 中的個別 AWS 帳戶、組織單位或整個組織 AWS Organizations。

如需的詳細資訊 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，us-east-1a 您 AWS 帳戶的可用區域可能沒有與 us-east-1a 另一個 AWS 帳戶相同的位置。

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符。例如，use1-az1 是 us-east-1 區域的 AZ ID，而且在每個 AWS 帳戶中的位置都相同。

檢視您帳戶中可用區域的 IDs

1. 在 [AWS RAM 主控台](#) 中導覽至 AWS RAM 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 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。資源共用是一種 AWS RAM 資源，可讓您跨 AWS 帳戶共用資源。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，您可以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 中組織的一部分，AWS Organizations 且已啟用組織內的共用，則可以將組織中的取用者從 AWS RAM 主控台存取共用的 Outpost 資源。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 AWS Outposts 主控台共用您擁有的 Outpost

1. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
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)。

系統會將您重新導向至 AWS RAM 主控台，以使用下列程序完成共用 Outpost。若要共用您擁有的本機關道路由表，也請使用下列程序。

使用 AWS RAM 主控台共用您擁有的 Outpost 或本機關道路由表

請參閱《AWS RAM 使用者指南》中的 [建立資源共享](#)。

使用 共享您擁有的 Outpost 或本機關道路由表 AWS CLI

使用 [create-resource-share](#) 命令。

## 將共用的 Outpost 資源取消共用

當您取消與消費者共用 Outpost 時，消費者將無法再執行下列動作：

- 在 AWS Outposts 主控台中檢視 Outpost。
- 在 Outpost 上建立新的子網路。
- 在 Outpost 上建立新的 Amazon EBS 磁碟區。
- 使用 AWS Outposts 主控台或 檢視 Outpost 詳細資訊和執行個體類型 AWS CLI。

不會刪除取用者在共用期間建立的子網路、磁碟區或執行個體，而且取用者可以繼續執行下列動作：

- 存取和修改這些資源。
- 在消費者建立的現有子網路上啟動新執行個體。

若要防止消費者存取其資源並在 Outpost 上啟動新執行個體，請要求消費者刪除其資源。

當共用的本機閘道路由表未共用時，消費者就無法再與其建立新的 VPC 關聯。消費者建立的任何現有 VPC 關聯都會保持與路由表的關聯。這些 VPC 中的資源可以繼續將流量路由至本機閘道。若要避免這種情況，請要求消費者刪除 VPC 關聯。

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 AWS RAM 主控台或來執行此操作 AWS CLI。

使用 AWS RAM 主控台取消共用您擁有的共用 Outpost 資源

請參閱《AWS RAM 使用者指南》中的[更新資源共享](#)。

使用 取消共用您擁有的共用 Outpost 資源 AWS CLI

使用 [disassociate-resource-share](#) 命令。

## 識別共用的 Outpost 資源

擁有者和消費者可以使用 AWS Outposts 主控台和來識別共用 Outpost AWS CLI。他們可以使用 AWS CLI來識別共用的本機閘道路由表。

使用 AWS Outposts 主控台識別共用 Outpost

1. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
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，檢視擁有者 ID 以識別 Outpost 擁有者 AWS 的帳戶 ID。

使用 識別共用 Outpost 資源 AWS CLI

使用 [list-Outpost](#) 和 [describe-local-gateway-route-tables](#) 命令。這些命令會傳回您擁有的 Outpost 資源和與您共用的 Outpost 資源。OwnerId會顯示 Outpost 資源擁有者 AWS 的帳戶 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。他們可以使用 AWS Organizations 來檢視、修改和刪除消費者在共用 Outpost 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，他們也會支付與其 Outpost 服務連結 VPN 來自 AWS 區域流量相關聯的任何資料傳輸費用。

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 層級資源的費用，例如 Direct Connect 和 VPN 連線、NAT 閘道和 Private Link 連線。

取用者須針對在共用的 Outpost 上建立的應用程式資源 (例如負載平衡器和 Amazon RDS 資料庫) 支付費用。消費者也會收到來自 AWS 區域的付費資料傳輸費用。

## 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。

# Outposts 伺服器上的第三方區塊儲存

使用 Outposts 伺服器，您可以利用存放在第三方儲存陣列上的現有資料。您可以在 Outpost 上為 EC2 執行個體指定外部區塊資料磁碟區和外部區塊開機磁碟區。使用此整合，您可以使用由第三方廠商支援的外部區塊資料和開機磁碟區，例如 Dell PowerStore、HPE Alletra Storage MP B10000、NetApp 內部部署企業儲存陣列，以及 Pure Storage FlashArray 儲存系統。

## 考量事項

- 適用於 Outposts 機架和 Outposts 2U 伺服器。不適用於 Outposts 1U 伺服器。
- 適用於支援 Outposts 2U 伺服器的所有 AWS 區域。
- 免費提供。
- 您要負責儲存陣列的組態和 day-to-day 管理。您也可以在此儲存陣列上建立和管理外部區塊磁碟區。如果您對於儲存陣列的硬體、軟體或連線有問題，請聯絡第三方儲存廠商。

### Note

存放在外部儲存陣列上的區塊磁碟區包含作業系統，該作業系統將開機至 Outposts 上的 EC2 執行個體。不支援啟動由外部儲存陣列支援的 AMI。若要啟動 AMI，會使用 Outposts 伺服器上的執行個體儲存體。

## 外部區塊資料磁碟區

在佈建和設定相容第三方儲存系統支援的區塊資料磁碟區之後，您可以在啟動磁碟區時將磁碟區連接到 EC2 執行個體。如果您為儲存陣列上的多連接設定磁碟區，您可以將磁碟區連接至多個 EC2 執行個體。

## 關鍵步驟

- 您有責任透過本機網路界面，在 [Outpost 子網路與本機網路](#) 之間建立連線。
- 您可以使用外部儲存陣列的管理界面來建立磁碟區。然後，您將透過建立新的啟動器群組，並將目標 EC2 執行個體的 iSCSI 合格名稱 (IQN) 新增至此群組來設定啟動器映射。這會將外部區塊資料磁碟區與 EC2 執行個體建立關聯。
- 您可以在啟動執行個體時新增外部資料磁碟區。您需要外部儲存陣列的啟動器 IQN、目標 IP 地址、連接埠和 IQN。如需詳細資訊，請參閱在 [Outpost 上啟動執行個體](#)。

如需詳細資訊，請參閱[簡化搭配 使用第三方區塊儲存 AWS Outposts](#)。

## 外部區塊開機磁碟區

從外部儲存陣列在 Outposts 上啟動 EC2 執行個體，可為依賴第三方儲存的現場部署工作負載提供集中、經濟實惠且高效率的解決方案。您可以選擇使用以下模式之一：

### iSCSI SAN 開機

提供從外部儲存陣列直接開機。使用 AWS 提供的 iPXE 協助程式 AMI，讓執行個體可以從網路位置開機。當 iPXE 與 iSCSI 結合時，EC2 執行個體會將遠端 iSCSI 目標（儲存陣列）視為本機磁碟。所有來自作業系統的讀取和寫入操作都會在外部儲存陣列上執行。

### iSCSI 或 NVMe-over-TCP LocalBoot

使用從儲存陣列擷取的開機磁碟區副本啟動 EC2 執行個體，使原始來源映像保持不變。我們會使用 LocalBoot AMI 啟動協助程式執行個體。此協助程式執行個體會將開機磁碟區從儲存陣列複製到 EC2 執行個體的執行個體存放區，並充當 iSCSI 啟動器或 NVMe-over-TCP 主機。最後，EC2 執行個體會使用本機執行個體存放區磁碟區重新啟動。

由於執行個體存放區是暫時儲存體，因此會在 EC2 執行個體終止時刪除開機磁碟區。因此，此選項適用於唯讀開機磁碟區，例如虛擬桌面基礎設施 (VDI) 中使用的磁碟區。

您無法使用 NVMe-over-TCP LocalBoot 啟動 EC2 Windows 執行個體。僅支援使用 EC2 Linux 執行個體。

如需詳細資訊，請參閱[部署外部開機磁碟區以搭配 使用 AWS Outposts](#)。

## 中的安全性 AWS Outposts

的安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，該架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[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 也為您提供可安全使用的服務。在[AWS 合規計畫](#)中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用的合規計畫 AWS Outposts，請參閱[AWS 合規計畫的服務範圍](#)。
- 雲端的安全性 – 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。

如需安全與合規的詳細資訊 AWS Outposts，請參閱[AWS Outposts 伺服器常見問答集](#)。

本文件可協助您了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。您也會了解如何使用其他 AWS 服務來協助您監控和保護資源。

### 目錄

- [中的資料保護 AWS Outposts](#)
- [的身分和存取管理 \(IAM\) AWS Outposts](#)
- [中的基礎設施安全 AWS Outposts](#)
- [中的彈性 AWS Outposts](#)
- [的合規驗證 AWS Outposts](#)

## 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球基礎設施 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。

基於資料保護目的，我們建議您保護 AWS 帳戶登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 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，所有資料都會進行靜態加密。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 Outposts 伺服器上的資料。

## 傳輸中加密

AWS 會加密 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](#)。

## 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 管理員可控制誰可以進行驗證 (登入) 和授權 (具有許可) 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](#)
- [AWS Outposts 政策範例](#)
- [的服務連結角色 AWS Outposts](#)
- [AWS AWS Outposts 的 受管政策](#)

## AWS Outposts 如何與 IAM 搭配使用

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

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

## AWS Outposts 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

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。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](#)。

## 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 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內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。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 動作的清單，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以下字首：

```
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。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (\*) 表示該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項資源，請使用逗號分隔 ARN。

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

若要查看 AWS Outpost 資源類型及其 ARNs 的清單，請參閱《服務授權參考》中的 [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的 ARN，請參閱 [AWS Outposts 定義的動作](#)。

## 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 元素會根據定義的條件，指定陳述式的執行時機。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 身分型政策的範例，請參閱 [AWS Outposts 政策範例](#)。

## ABAC 與 AWS Outpost

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，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

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 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的[使用 ABAC 授權定義許可](#)。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 \(ABAC\)](#)。

## 搭配 AWS Outposts 使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時，會自動建立。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 使用者指南》中的[IAM 中的臨時安全憑證與可與 IAM 搭配運作的 AWS 服務](#)。

## AWS Outposts 的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫的委託人許可 AWS 服務，結合 AWS 服務請求向下游服務提出請求。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 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一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 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 Outpost 資源的許可。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。

如需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 \(主控台\)](#)。

如需 AWS Outposts 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 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](#)
- [範例：使用資源層級許可](#)

## 政策最佳實務

身分型政策會判斷您帳戶中的某人是否可以建立、存取或刪除 AWS Outpost 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，請使用將許可授予許多常見使用案例的 AWS 受管政策。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](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅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。如果透過特定 等使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，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 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，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 [透過 MFA 的安全 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。

### JSON

```
{
```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": "outposts:GetOutpost",
    "Resource": "arn:aws:outposts:us-east-1:111122223333: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。

## JSON

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

## 的服務連結角色 AWS Outposts

AWS Outposts use AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是一種直接連結至的服務角色類型 AWS Outposts。AWS Outposts 會定義服務連結角色，並包含代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您的設定 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，否則只能 AWS Outposts 擔任其角色。定義的許可包括信任政策和許可政策，並且該許可政策不能連接到任何其他 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_`***OutpostID*** 的服務連結角色。此角色授予 Outpost 管理聯網資源的許可，以代表您啟用私有連線。此角色也允許 Outposts 建立和設定網路介面、管理安全群組，以及將介面連接到服務連結端點執行個體。這些許可是建立和維護內部部署 Outpost AWS 和服務之間安全、私有連線的必要許可，可確保 Outpost 部署的可靠操作。

`AWSServiceRoleForOutpost_`***OutpostID*** 服務連結角色信任下列服務可擔任該角色：

- `outposts.amazonaws.com`

### 服務連結角色政策

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

- [AWSOutpostServiceRolePolicy](#)
- `AWSOutpostsPrivateConnectivityPolicy_`***OutpostID***

### `AWSOutpostServiceRolePolicy`

此 `AWSOutpostsServiceRolePolicy` 政策可讓您存取 管理 AWS 的資源 AWS Outposts。

此政策允許 對指定的資源 AWS Outposts 完成下列動作：

- 動作：在所有 AWS 資源 `ec2:DescribeNetworkInterfaces` 上
- 動作：在所有 AWS 資源 `ec2:DescribeSecurityGroups` 上
- 動作：在所有 AWS 資源 `ec2:CreateSecurityGroup` 上
- 動作：在所有 AWS 資源 `ec2:CreateNetworkInterface` 上

### `AWSOutpostPrivateConnectivityPolicy_`***OutpostID***

此 `AWSOutpostsPrivateConnectivityPolicy_`***OutpostID*** 政策允許 對指定的資源 AWS Outposts 完成下列動作：

- 動作：在符合下列條件的所有 AWS 資源 `ec2:AuthorizeSecurityGroupIngress` 上：

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

- 動作：在符合下列條件的所有 AWS 資源 `ec2:AuthorizeSecurityGroupEgress` 上：

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

- 動作：在符合下列條件的所有 AWS 資源 `ec2:CreateNetworkInterfacePermission` 上：

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

- 動作：在符合下列條件的所有 AWS 資源 `ec2:CreateTags` 上：

```
{ "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](#)。

## 建立的服務連結角色 AWS Outposts

您不需要手動建立服務連結角色，當您在 中為 Outpost 設定私有連線時 AWS 管理主控台，會為您 AWS Outposts 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。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 AWS Outposts 服務在您嘗試刪除資源時使用角色，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 `AWSServiceRoleForOutpost_`*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 [取消共用共用的 Outpost 資源](#)。

刪除 `AWSServiceRoleForOutposts_`***OutpostID*** 使用 AWS Outposts 的資源

請聯絡 AWS 企業支援以刪除您的 Outpost。

使用 IAM 手動刪除服務連結角色

如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

## AWS Outposts 服務連結角色支援的區域

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 [Outposts 伺服器的FAQs](#)。

## AWS AWS Outposts 的 受管政策

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，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。我們建議您定義特定於使用案例的[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 更新受管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。AWS 服務當新的啟動或新的 API 操作可用於現有服務時，AWS 最有可能更新 AWS 受管政策。

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

此政策會連接到服務連結角色，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。

JSON

```
{
```

```

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

```

## AWS Outpost 更新 AWS 受管政策

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

變更	描述	Date
<a href="#">AWSOutpostAuthorizeServerPolicy</a> – 新政策	AWS Outposts 新增了政策，授予許可來授權內部部署網路中的 Outposts 伺服器硬體。	2023 年 1 月 4 日
AWS Outpost 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 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 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 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。

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 流程日誌的運作方式與 AWS 區域中的運作方式相同。這表示可將其發佈至 CloudWatch Logs、Amazon S3 或 Amazon GuardDuty 進行分析。需要將資料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，CloudWatch 或其他服務將無法看到資料。

## 中的彈性 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 在一段時間內的容量使用率。

當您建立 Outpost 時，您可以從 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 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。

## 的合規驗證 AWS Outposts

若要了解 AWS 服務 是否在特定合規計劃範圍內，請參閱 [AWS 服務 合規計劃範圍內](#) 然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 [AWS 合規計劃](#)。

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 [下載報告 in AWS Artifact](#)

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 [AWS 安全文件](#)。

# 監控 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 server 資料點的統計資料，做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 [Outposts 伺服器的 CloudWatch 指標](#)。

## CloudTrail 日誌

使用 AWS CloudTrail 擷取對 AWS APIs 進行呼叫的詳細資訊。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 日誌來判斷進行了哪些呼叫、呼叫的來源 IP 地址、進行呼叫的人員以及進行呼叫的時間等資訊。

CloudTrail 日誌包含呼叫 API 動作的相關資訊 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 [使用 CloudTrail 記錄 API 呼叫](#)。

## 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 伺服器複製到 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 儀板表

Health 儀板表 會顯示由 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 Health 儀板表 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 儀板表入門](#)。

# Outposts 伺服器的 CloudWatch 指標

AWS Outposts 會將資料點發佈至 Outposts 的 Amazon CloudWatch。CloudWatch 可讓使用一組時間序列資料的形式來擷取這些資料點的相關統計資料，也就是指標。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 可能會起始動作，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，我們建議您在內部部署網路中驗證與 AWS 區域的連線，如果問題仍然存在，請聯絡 AWS Support。

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 CloudWatch 警示](#)》。如需有關 CloudWatch 的詳細資訊，請參閱《[Amazon CloudWatch 使用者指南](#)》。

## 目錄

- [指標](#)
- [指標維度](#)
- [檢視 Outposts 伺服器的 CloudWatch 指標](#)

## 指標

AWS/Outposts 命名空間包含下列類別的指標。

### 目錄

- [執行個體指標](#)
- [Outposts 指標](#)

## 執行個體指標

下列指標適用於 Amazon EC2 執行個體。

指標	維度	Description
InstanceFamilyCapacityAvailability	InstanceFamily 和 OutpostId	<p>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。</p> <p>單位：百分比</p> <p>最長解析時間：5 分鐘</p> <p>統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。</p>
InstanceFamilyCapacityUtilization	Account、InstanceFamily 與 OutpostId	<p>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。</p> <p>單位：百分比</p> <p>最長解析時間：5 分鐘</p> <p>統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。</p>
InstanceTypeCapacityAvailability	InstanceType 和 OutpostId	<p>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。</p> <p>單位：百分比</p> <p>最長解析時間：5 分鐘</p>

指標	維度	Description
		統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。
InstanceTypeCapacityUtilization	Account、InstanceType 與 OutpostId	<p>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。</p> <p>單位：百分比</p> <p>最長解析時間：5 分鐘</p> <p>統計資訊：最實用的統計資訊是 Average 與 pNN.NN (百分位數)。</p>
UsedInstanceType_Count	Account、InstanceType 與 OutpostId	<p>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。</p> <p>單位：計數</p> <p>最長解析時間：5 分鐘</p>

指標	維度	Description
AvailableInstanceType_Count	InstanceType 和 OutpostId	<p>可用的執行個體類型數量。此指標包含 Available ReservedInstances 計數。</p> <p>若要判斷您可以保留的執行個體數量，請從 Available ReservedInstances 計數中減去 Available InstanceType_Count 計數。</p> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <math display="block">\text{Number of instances that you can reserve} = \text{AvailableInstanceType\_Count} - \text{Available ReservedInstances}</math> </div> <p>此指標不包含在 Outpost 上設定之任何專用執行個體的容量。</p> <p>單位：計數</p> <p>最長解析時間：5 分鐘</p>

指標	維度	Description
AvailableReservedInstances	InstanceType 和 OutpostId	<p>可使用容量保留啟動至預留運算容量的執行個體數量<a href="https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/capacity-reservations-outposts.html">https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/capacity-reservations-outposts.html</a>。</p> <p>此指標不包含 Amazon EC2 預留執行個體。</p> <p>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多少執行個體，請從AvailableReservedInstances 計數中減去AvailableInstanceType_Count 計數。</p> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <math display="block">\text{Number of instances that you can reserve} = \text{AvailableInstanceType\_Count} - \text{AvailableReservedInstances}</math> </div> <p>單位：計數</p> <p>最長解析時間：5 分鐘</p>

指標	維度	Description
UsedReservedInstances	InstanceType 和 OutpostId	<p>使用容量預留在運算容量中執行的執行個體數量<a href="https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/capacity-reservations-outposts.html">https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/capacity-reservations-outposts.html</a>。此指標不包含 Amazon EC2 預留執行個體。</p> <p>單位：計數</p> <p>最長解析時間：5 分鐘</p>
TotalReservedInstances	InstanceType 和 OutpostId	<p>執行中且可供啟動的執行個體總數，由使用<a href="#">容量</a>保留保留的運算容量提供。此指標不包含 Amazon EC2 預留執行個體。</p> <p>單位：計數</p> <p>最長解析時間：5 分鐘</p>

## Outposts 指標

下列指標適用於您的 Outpost。

指標	維度	Description
ConnectedStatus	OutpostId	<p>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。</p> <p>單位：計數</p> <p>最長解析時間：1 分鐘</p>

指標	維度	Description
		統計資訊：最實用的統計資訊是 Average。
CapacityExceptions	InstanceType 和 OutpostId	<p>執行個體啟動時的容量不足錯誤數目。</p> <p>單位：計數</p> <p>最長解析時間：5 分鐘</p> <p>統計資訊：最實用的統計資訊是 Maximum 與 Minimum。</p>

## 指標維度

若要篩選 Outpost 的指標，請使用下列維度。

維度	Description
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。

## 檢視 Outposts 伺服器的 CloudWatch 指標

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

使用 CloudWatch 主控台檢視指標

1. 在 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
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。

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

使用下列 `get-metric-statistics` 命令取得指定指標和維度的統計資料。<https://docs.aws.amazon.com/cli/latest/reference/cloudwatch/get-metric-statistics.html> CloudWatch 會將不同的維度組合視為不同指標。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 服務整合 AWS CloudTrail，此服務可提供使用者、角色或服務所採取動作的記錄 AWS。CloudTrail 會將的 API 呼叫擷取 AWS Outposts 為事件。擷取的呼叫包括來自 AWS Outposts 主控台的呼叫，以及對 AWS Outposts API 操作的程式碼呼叫。您可以使用 CloudTrail 所收集的資訊來判斷提出的請求 AWS Outposts、提出請求的 IP 地址、提出請求的時間，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：

- 該請求是否使用根使用者還是使用者憑證提出。
- 請求是否代表 IAM Identity Center 使用者提出。
- 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。

當您建立 AWS 帳戶時，CloudTrail 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 事件歷史記錄為 AWS 區域中過去 90 天記錄的管理事件，提供可檢視、

可搜尋、可下載且不可變的記錄。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會產生 CloudTrail 費用。

如需 AWS 帳戶 過去 90 天內持續記錄的事件，請建立線索或 [CloudTrail Lake](#) 事件資料存放區。

## CloudTrail 追蹤

線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。使用 建立的所有線索 AWS 管理主控台 都是多區域。您可以使用 AWS CLI 建立單一或多區域追蹤。建議您建立多區域追蹤，因為您擷取 AWS 區域 帳戶中所有的活動。如果您建立單一區域追蹤，您只能檢視追蹤 AWS 區域中記錄的事件。如需追蹤的詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的[為您的 AWS 帳戶建立追蹤](#)和[為組織建立追蹤](#)。

您可以透過建立追蹤，免費將持續管理事件的一個複本從 CloudTrail 傳遞至您的 Amazon S3 儲存貯體，但這樣做會產生 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 讓您能夠對事件執行 SQL 型查詢。CloudTrail Lake 會將分列式 JSON 格式的現有事件轉換為 [Apache ORC](#) 格式。ORC 是一種單欄式儲存格式，針對快速擷取資料進行了最佳化。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費用。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 CloudTrail 中的 管理事件

[管理事件](#)提供有關在 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，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 CloudTrail 的 AWS Outposts 控制平面操作清單，請參閱 [AWS Outposts API 參考](#)。

## AWS Outposts 事件範例

以下範例顯示的 CloudTrail 事件會示範 SetSiteAddress 操作。

```
{
  "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[共同的責任模型](#)下，AWS 負責執行 AWS 服務的硬體和軟體。這適用於 AWS Outposts，就像對 AWS 區域一樣。例如，AWS 會管理安全修補程式、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

如果基礎磁碟機故障或執行個體終止，執行個體存放磁碟區上的資料會遺失。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至持久性儲存，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

- [更新聯絡詳細資訊](#)
- [硬體維護](#)
- [韌體更新](#)
- [電源和網路事件的最佳實務](#)
- [以密碼編譯方式銷毀伺服器資料](#)

## 更新聯絡詳細資訊

如果 Outpost 擁有者變更，請聯絡具有新擁有者名稱和聯絡資訊的 [AWS 支援中心](#)。

## 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，我們會通知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。遵循 [Outposts 伺服器安裝中的安裝說明](#)。
- 將無法修復的伺服器封裝至 AWS，與替換伺服器送達的封裝相同。
- 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。
- 將伺服器傳回至 AWS。如需詳細資訊，請參閱 [《返回 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。只有在電源和網路連線不中斷時，Outposts 伺服器才能正確運作。

### 電源事件

完全停電時，AWS Outposts 存在資源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 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 (關閉關閉)。
- 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 支援 Center](#) 建立案例，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，自動從上游企業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 LNI 在本機存取。同樣地，Amazon ECS 工作者節點等 AWS 服務資源會繼續在本機執行。不過，API 可用性將會降低。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在本機繼續快取長達 7 天，並在連線傳回時推送至 AWS 區域。超過 7 天的中斷連線可能會導致指標和日誌遺失。

如果服務連結因為現場電源問題或網路連線中斷而關閉，Health 儀板表 會傳送通知給擁有 Outpost 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 [Health 儀板表入門](#)》。

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。

## Resources

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 部落格 [監控的最佳實務 AWS Outposts](#) 涵蓋 Outposts 特有的可觀測性和事件管理最佳實務。
- AWS 適用於 [Amazon VPC 網路連線的部落格偵錯工具](#) 說明 AWSSupport-SetupIPMonitoringFromVPC 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。該文件會執行 Ping、MTR、TCP 路由追蹤和路徑追蹤診斷測試，並將結果儲存在 Amazon CloudWatch Logs 中，以便在 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 監控一或多個 Outpost 執行個體 (這將提供封包遺失圖表和 AWS Outposts 父 AWS 區域之間的延遲)。
- AWS 部落格 [部署 AWS Outposts 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。

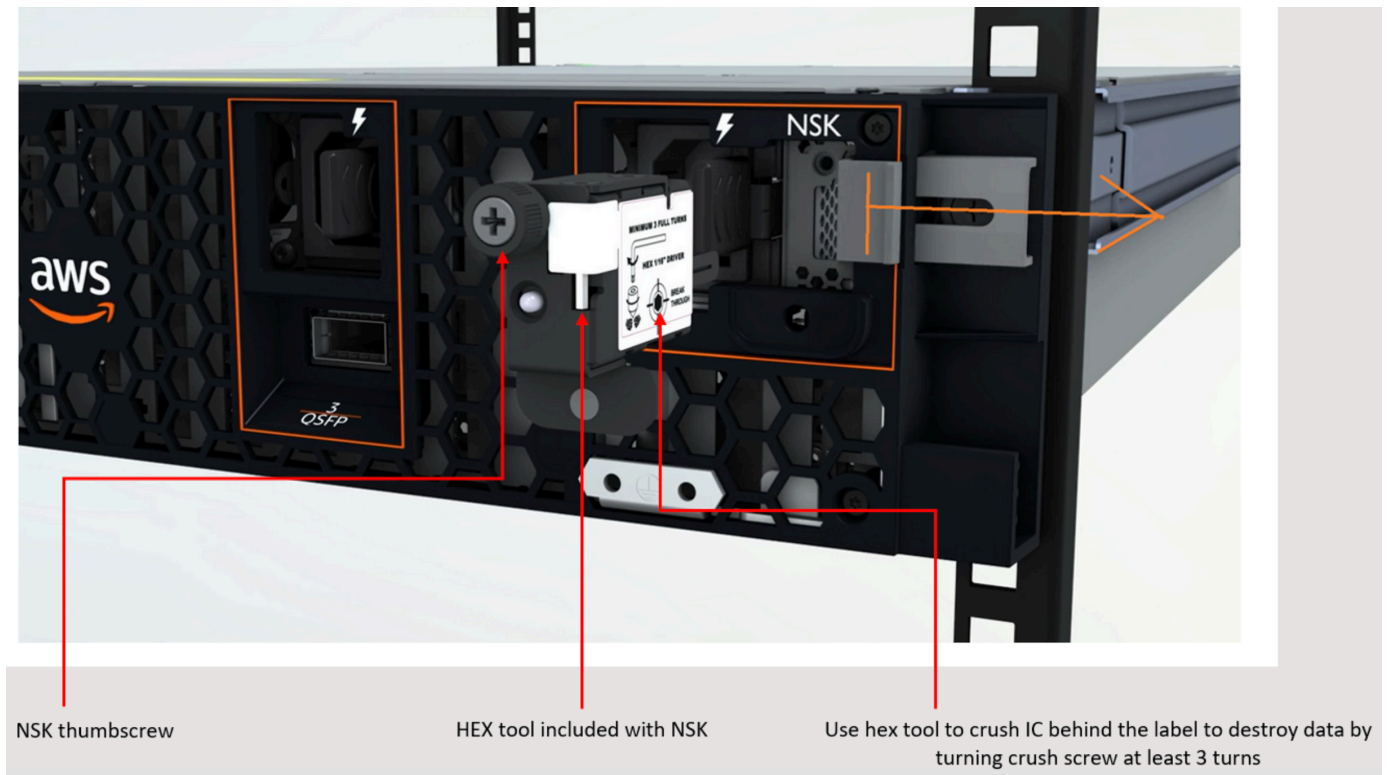
- 如果您有疑問或需要更多資訊，請參閱《AWS Support 使用者指南》中的《[建立支援案例](#)》。

## 以密碼編譯方式銷毀伺服器資料

解密伺服器上的資料需要 Nitro 安全金鑰 (NSK)。當您因為要取代伺服器或終止服務 AWS 而將伺服器傳回時，您可以銷毀 NSK，以密碼編譯方式將伺服器上的資料分割。

以密碼編譯方式銷毀伺服器上的資料

1. 將伺服器運回目的地之前，請從伺服器移除 NSK AWS。
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。



# Outposts 伺服器end-of-term選項

在 AWS Outposts 期限結束時，您必須在下列選項之間進行選擇：

- [續約您的訂閱](#)並保留現有的 Outposts 伺服器。
- [傳回您的 Outpost 伺服器](#)。
- [轉換為month-to-month訂閱](#)並保留現有的 Outposts 伺服器。

## 續訂訂閱

您必須在 Outposts 伺服器目前的訂閱結束前至少 5 個工作天完成下列步驟。如果無法在目前的訂閱結束前至少 5 個工作天完成這些步驟，可能會導致非預期的費用。

續約您的訂閱並保留現有的 Outposts 伺服器

1. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
2. 在導覽窗格中，選擇 Outposts。
3. 選擇動作。
4. 選擇 Renew Outpost。
5. 選擇訂閱期限長度和付款選項。

如需定價，請參閱《[AWS Outposts 伺服器定價](#)》。您也可以請求報價。

6. 選擇提交支援票證。

### Note

如果在 Outposts 伺服器的目前訂閱結束前續約，將會立即向您收取任何預付費用。

您的新訂閱將在您目前訂閱結束後的隔天開始生效。

如果您不表示想要續約訂閱或傳回 Outposts 伺服器，您會自動轉換為month-to-month訂閱。您的 Outpost 將按與您的 AWS Outposts 組態對應的無預付款選項費率每月續約。您的新按月訂閱將在您目前訂閱結束後的隔天開始生效。

## 傳回 Outposts 伺服器

若要因為伺服器已達到合約期限結束而傳回伺服器，您必須先在 Outposts 伺服器目前的訂閱結束前至少 5 個工作天完成停用程序。除非您這麼做，否則 AWS 無法啟動傳回程序。如果無法在目前的訂閱結束前至少 5 個工作日完成除役程序，可能會導致除役和意外費用延遲。

完成停用程序後，您必須準備伺服器以供傳回、取得運送標籤，以及封裝和傳回伺服器 AWS。

當您傳回 Outposts 伺服器時，不會向您收取運送費用。不過，如果您傳回損壞的伺服器，可能會產生費用。

### 任務

- [步驟 1：準備要傳回的伺服器](#)
- [步驟 2：停用伺服器](#)
- [步驟 3：取得送回運送標籤](#)
- [步驟 4：封裝伺服器](#)
- [步驟 5：透過貨運業者傳回伺服器](#)

### 步驟 1：準備要傳回的伺服器

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 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所存放資料的備份。
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](#)中的指示。

5. 銷毀 Nitro 安全金鑰 (NSK)，以密碼編譯方式銷毀伺服器上的資料。若要銷毀 NSK，請遵循[密碼編譯碎片伺服器資料](#)中的指示。

## 步驟 2：停用伺服器

在 Outpost 伺服器的目前訂閱結束前至少 5 個工作天完成下列步驟。

### Important

AWS 在您提交停用請求後，無法停止傳回程序。

1. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
2. 在導覽窗格中，選擇 Outposts。
3. 選擇動作。
4. 選擇停用 Outpost，然後依照工作流程刪除資源。
5. 選擇 Submit request (提交請求)。

### Note

在目前的訂閱結束之前傳回 Outpost 伺服器，不會終止與此 Outpost 相關的任何未結費用。

## 步驟 3：取得送回運送標籤

### Important

您只能使用 AWS 提供的運送標籤，因為它包含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。

若要取得您的運送標籤：

1. 在 <https://console.aws.amazon.com/outposts/> 開啟 AWS Outposts 主控台。
2. 在導覽窗格上，選擇 訂單。
3. 選擇您要傳回之伺服器的順序。

- 在訂單詳細資訊頁面的訂單狀態區段中，選擇列印傳回標籤。

#### Note

在目前的訂閱結束之前傳回 Outpost 伺服器，不會終止與此 Outpost 相關的任何未結費用。

## 步驟 4：封裝伺服器

若要封裝您的伺服器，請使用提供的方塊和封裝材料 AWS。

- 將伺服器封裝在下列其中一個方塊中：

- 伺服器最初進來的盒子和封裝材料。
- 替換伺服器的盒子和封裝材料。

或者，聯絡 [AWS 支援中心](#) 要求一個箱子。

- 將 AWS 提供的運送標籤貼到箱子外部。

#### Important

確認運送標籤上的資產 ID 與您傳回的伺服器上的資產 ID 相符。

資產 ID 位於伺服器正面的提取標籤上。範例：1203779889 或 9305589922

- 安全地密封盒子。

## 步驟 5：透過貨運業者傳回伺服器

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 提供的運送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 <a href="#">AWS 支援中心</a> 。請在您的請求中包含下列資訊：

Country	聯絡
巴林	<ul style="list-style-type: none"><li>• AWS所提供運送標籤上的追蹤號碼</li><li>• 您希望貨運業者前來收取伺服器的日期和時間</li><li>• 聯絡人名稱</li><li>• 電話號碼</li><li>• 電子郵件地址</li></ul>
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	
巴拿馬	
秘魯	
菲律賓	
塞爾維亞	
新加坡	
南非	
南韓	

Country	聯絡
臺灣	
泰國	
阿拉伯聯合大公國	
越南	
美國	<p>聯絡 <a href="#">UPS</a>。</p> <p>您可用下列方式歸還伺服器：</p> <ul style="list-style-type: none"> <li>• 在您現場進行的例行 UPS 收件期間歸還伺服器。</li> <li>• 將伺服器放到 <a href="#">UPS 地點</a>。</li> <li>• 安排您偏好的日期和時間<a href="#">收件</a>。輸入 AWS 所提供運輸標籤上的追蹤編號以利用免費運輸。</li> </ul>
所有其他國家/地區	<p>聯絡 <a href="#">DHL</a>。</p> <p>您可用下列方式歸還伺服器：</p> <ul style="list-style-type: none"> <li>• 將伺服器放到 <a href="#">DHL 地點</a>。</li> <li>• 安排您偏好的日期和時間<a href="#">收件</a>。輸入 AWS 所提供運送標籤中的 DHL Waybill 號碼，即可免費運送。</li> </ul> <p>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。</p>

## 轉換為按月訂閱

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 Outpost 將按與您的 AWS Outposts 組態對應的無預付款選項費率每月續約。您的新每月訂閱會在目前訂閱結束後的那天開始。

## 的配額 AWS Outposts

您的 AWS 帳戶 具有每個預設配額，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，但並非所有配額都能提高。

若要檢視 的配額 AWS Outposts，請開啟 [Service Quotas 主控台](#)。在導覽窗格中，選擇 AWS 服務，然後選取 AWS Outposts。

若要請求提高配額，請參閱 [《Service Quotas 使用者指南》](#) 中的請求提高配額。

您的 AWS 帳戶 具有下列與 相關的配額 AWS Outposts。

資源	預設	可調整	說明
Outpost 站點	100	<a href="#">是</a>	<p>Outpost 站點是客戶管理的實體建築物，您可以在此為 Outpost 設備供電並將其連接至網路。</p> <p>您可以在 AWS 帳戶的每個區域中擁有 100 個 Outposts 網站。</p>
每個站點的 Outpost	10	<a href="#">是</a>	<p>AWS Outposts 包含硬體和虛擬資源，稱為 Outposts。此配額會限制您的 Outpost 虛擬資源。</p> <p>您可以在每個 Outpost 站點中擁有 10 個 Outpost。</p>

## AWS Outposts 和其他服務的配額

AWS Outposts 依賴其他 服務的資源，這些服務可能有自己的預設配額。例如，您的本機網路介面配額來自 Amazon VPC 的網路介面配額。

# 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
<a href="#">AWS Outposts 支援來自 Dell 和 HPE 儲存陣列的外部區塊磁碟區</a>	您可以使用第三方廠商支援的外部區塊資料和開機磁碟區，例如 Dell PowerStore 和 HPE Alletra Storage MP B10000。	2025 年 9 月 30 日
<a href="#">續約您的訂閱並準備伺服器以供傳回</a>	若要續約訂閱或傳回伺服器，您必須在目前的訂閱結束前至少 10 個工作天完成程序。	2025 年 7 月 16 日
<a href="#">對服務連結連線進行故障診斷</a>	如果您的 Outposts 伺服器與 AWS 區域之間的連線中斷，請依照下列步驟進行疑難排解和解決。	2025 年 5 月 5 日
<a href="#">靜態穩定性的更新</a>	如果您的網路中斷，執行個體指標和日誌會在本機快取最多 7 天。之前，Outposts 可以快取日誌幾個小時。	2025 年 5 月 1 日
<a href="#">資產層級的容量管理</a>	您可以在資產層級修改容量組態。	2025 年 3 月 31 日
<a href="#">第三方儲存體支援的外部區塊磁碟區</a>	您現在可以在 Outpost 上的執行個體啟動程序期間，連接相容第三方區塊儲存系統支援的區塊資料磁碟區。	2024 年 12 月 1 日
<a href="#">容量管理</a>	您可以修改新 Outposts 訂單的預設容量組態。	2024 年 4 月 16 日

---

<a href="#">AWS Outposts 伺服器End-of-term選項</a>	在 AWS Outposts 期限結束時，您可以續約、結束或轉換您的訂閱。	2023 年 8 月 1 日
<a href="#">Outposts 伺服器的建立 AWS Outposts 使用者指南</a>	AWS Outposts 使用者指南分為機架和伺服器的個別指南。	2022 年 9 月 14 日
<a href="#">上的置放群組 AWS Outposts</a>	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
<a href="#">Outposts 伺服器簡介</a>	新增 Outposts 伺服器，這是新的 AWS Outposts 規格尺寸。	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。