第一代 Outposts 機架的使用者指南

AWS Outposts

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

AWS Outposts: 第一代 Outposts 機架的使用者指南

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
支援 AWS 服務 者 AWS 區域 3
北美洲 4
非洲 6
亞太區域 6
歐洲 8
中東 10
南美洲 11
AWS Outposts 支援區域的 Amazon RDS 12
定價 13
如何 AWS Outposts 運作 14
網路元件 15
VPC 和子網路 15
路由 16
DNS 16
服務連結 17
本機閘道 17
本機網路介面 18
Outposts 機架的需求 19
設施 19
聯網 20
網路整備檢查清單 21
電源 25
訂單履行 27
ACE 機架的需求 28
ACE 機架容量和擴展 28
設施 28
聯網 29
電源 30
開始使用 31
下訂單 31
步驟 1：建立站點 31

步驟 2：建立 Outpost 32
步驟 3：建立引號 33
步驟 4：下訂單 35
步驟 5：修改執行個體容量 37
後續步驟 27
啟動執行個體 40
步驟 1：建立 VPC 41
步驟 2：建立子網路和自訂路由表 41
步驟 3：設定本機閘道連線 43
步驟 4：設定內部部署網路 46
步驟 5：在 Outpost 上啟動執行個體 48
步驟 6：測試連線能力 49
最佳化 53
Outpost 上的專用執行個體 53
設定執行個體復原 54
Outpost 中的放置群組 54
服務連結 56
連線能力 56
最大傳輸單位 (MTU) 需求 56
頻寬建議 56
備援網際網路連線 57
設定您的服務連結 57
公有連線選項 58
選項 1。透過網際網路的公有連線 58
選項 2。透過公有 VIFs Direct Connect 公有連線 58
私有連線選項 58
先決條件 58
選項 1。透過私有 VIFs Direct Connect 私有連線 62
選項 2。透過 Direct Connect 傳輸 VIFs私有連線 63
防火牆和服務連結 63
網路故障診斷 65
與 Outpost 網路裝置的連線 65
Direct Connect 區域公有虛擬介面連線 AWS 66
Direct Connect 區域私有虛擬介面連線 AWS 67
ISP 公有網際網路連線至 AWS 區域 68
Outpost 位於兩個防火牆裝置後方 69

本機閘道 71
基本概念 71
路由 72
連線能力 73
路由表 74
直接 VPC 路由 74
客戶擁有的 IP 地址 78
自訂路由表 81
路由表路由 81
要求與限制 81
建立自訂本機閘道路由表 82
切換本機閘道路由表模式或刪除本機閘道路由表 83
CoIP 集區 84
監控連線能力 87
本機網路連線 89
實體連線 89
連結彙總 90
虛擬 LAN 91
網路層連線 92
ACE 機架連線 94
服務連結 BGP 連線 95
服務連結基礎設施子網路公告和 IP 範圍 96
本機閘道 BGP 連線 97
本機閘道客戶擁有的 IP 子網路公告 98
容量管理 101
檢視容量 101
修改執行個體容量 37
考量事項 102
故障診斷容量任務問題 105
訂單 *oo-xxxxxx* 與 Outpost ID *op-xxxxx* 沒有關聯 105
容量計劃包含不支援的執行個體類型 105
沒有 Outpost ID 為 *op-xxxxx* 的 Outpost 106
Outpost op-*XXXX* 已找到 Active CapacityTask cap-*XXXX* 107
Outpost op-*XXXX* 上的資產 *XXXX* 已找到作用中的 CapacityTask cap-XXXX 107
AssetId=*XXXX* 對 Outpost=op-*XXXX* 無效 108
共用 資源 110

可共用的 Outpost 資源 111
共用 Outpost 資源的先決條件 112
相關服務 112
跨可用區域共用 112
共用 Outpost 資源 113
將共用的 Outpost 資源取消共用 113
識別共用的 Outpost 資源 114
共用的 Outpost 資源許可 115
擁有者的許可 115
消費者的許可 115
計費和計量 115
限制 115
第三方區塊儲存 116
外部區塊資料磁碟區 116
外部區塊開機磁碟區 117
安全 118
資料保護 118
靜態加密 119
傳輸中加密 119
資料刪除 119
身分與存取管理 119
AWS Outpost 如何與 IAM 搭配使用 120
政策範例 123
服務連結角色 125
AWS 受管政策 129
基礎設施安全性 130
竄改監控 130
恢復能力 131
法規遵循驗證 131
網際網路存取 131
透過父 AWS 區域存取網際網路 132
透過本機資料中心的網路進行網際網路存取 132
監控 134
CloudWatch 指標 135
指標 135
指標維度 146

檢視 Outposts 機架 CloudWatch 指標 147
使用 CloudTrail 記錄 API 呼叫 148
AWS Outposts CloudTrail 中的 管理事件 149
AWS Outposts 事件範例 149
Maintenance (維護) 151
更新聯絡詳細資訊 151
硬體維護 151
韌體更新 152
網路設備維護 152
電源和網路事件 152
電源事件 153
網路連線事件 153
Resources 154
使用期限結束時的選項 155
續訂訂閱 155
傳回機架 155
轉換訂閱 159
配額 160
AWS Outposts 和其他服務的配額 160
文件歷史紀錄 161
..... clxvi

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 AWS 資源時指定子網路，例如 EC2 執行個體、EBS 磁碟區、ECS 叢集和 RDS 執行個體。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 VPC 內。

> **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。
- Outposts ACE 機架 – Aggregation、Core、Edge (ACE) 機架可做為多機架 Outpost 部署的網路彙總點。ACE 機架透過在邏輯 Outposts 和內部部署網路中的多個 Outpost 運算機架之間提供連線，以減少實體聯網連接埠和邏輯界面需求的數目。

如果您有四個或更多運算機架，則必須安裝 ACE 機架。如果您有少於四個運算機架，但計劃在未來擴展到四個或多個機架，我們建議您儘早安裝 ACE 機架。

如需 ACE 機架的其他資訊，請參閱使用 ACE AWS Outposts 機架擴展機架部署。

- Outpost 伺服器：業界標準 1U 或 2U 伺服器的 Outpost 形式規格，可安裝在符合 EIA-310D 19 標準的 4 支桿機架中。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 伺服器和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
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

Resource Type (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

Resource Type (資源類型)	機架	伺服器
Amazon RDS 資料庫執行個體	✓ 是	✗ 否

聯網

Resource Type (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
Amazon Route 53	✓ 是	✗ 否

儲存

Resource Type (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

支援 AWS 服務 者 AWS 區域

AWS Outposts AWS 服務 根據 Outpost 操作 AWS 區域 所在的 來支援 。若要判斷支援的服務，請在個別地理區域中檢視您的 區域：

區域

- 北美洲

- 非洲
- 亞太區域
- 歐洲
- 中東
- 南美洲

北美洲

下表指出在北美區域 AWS Outposts AWS 服務 支援 。

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
美國東部(維吉尼亞北部)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
美國東部(俄亥俄)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
美國西部(加利佛尼亞北部)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
美國西部(奧勒岡)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
加拿大(中部)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是

非洲

下表指出 AWS 服務 在非洲區域的 AWS Outposts 支援。

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
非洲 (開普敦)	是	是	是	是	是	是	是	否	是	是	是	是	是	是	是

亞太區域

下表指出在亞太區域 AWS Outposts AWS 服務 支援 。

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
亞太地區 (雅	是	是	是	是	否	是	是	否	是	是	是	是	是	是	是

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
加達)															
亞太地區(孟買)	是	是	是	是	是	是	是	否	是	是	是	是	是	是	是
亞太地區(大阪)	是	是	是	是	否	是	是	否	是	是	是	是	是	是	是
亞太地區(首爾)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
亞太地區(新加坡)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
亞太地區(悉尼)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
亞太地區(東京)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是

歐洲

下表指出 AWS 服務 歐洲區域中對 的 AWS Outposts 支援。

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
歐洲 (法蘭克福)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
歐洲 (愛爾蘭)	是	是	是	是	是	是	是	否	是	是	是	是	是	是	是
歐洲 (倫敦)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
歐洲 (米蘭)	是	是	是	是	是	是	是	否	是	是	是	是	是	是	是
歐洲 (西班牙)	是	是	否	否	否	是	是	否	是	是	是	是	是	是	是

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
Euro (Paris	是	是	是	是	是	是	是	否	是	是	是	是	是	是	是
歐洲 (斯德哥爾摩)	是	是	是	是	是	是	是	否	是	是	是	是	是	是	是

中東

下表指出 AWS 服務 中東區域的 AWS Outposts 支援。

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
以色列 (特拉	是	是	是	是	是	是	是	否	是	是	是	是	是	是	是

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
維夫)															
Midd East (Bah	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
中東 (阿拉伯聯合大公國)	是	是	否	否	否	是	是	否	是	是	是	否	是	是	是

南美洲

下表指出在南美洲區域 AWS Outposts AWS 服務 支援 。

AWS 區域	Amaz EC2	Amaz EBS	Amaz EBS 快照	Amaz S3	Amaz RDS SQL、、Po QL 和 Orac	Amaz ECS	Amaz EKS	Amaz EKS-LC	Amaz EMR	Amaz Elast he	彈性災難復原	Appli on Load Balar	Direc Conr	Amaz VPC	本機閘道
南美洲 (聖保羅)	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是

AWS Outposts 支援區域的 Amazon RDS

Amazon RDS on AWS Outposts 可在下列位置使用 AWS 區域：

- 非洲 (開普敦)
- 亞太地區 (香港)
- 亞太地區 (東京)
- 亞太地區 (首爾)
- 亞太地區 (大阪)
- 亞太地區 (孟買)
- 亞太地區 (新加坡)
- 亞太地區 (雪梨)
- 加拿大 (中部)
- 歐洲 (法蘭克福)
- 歐洲 (斯德哥爾摩)
- 歐洲 (米蘭)
- 歐洲 (愛爾蘭)
- 歐洲 (倫敦)

- Europe (Paris)
- 以色列 (特拉維夫)
- 中東 (阿拉伯聯合大公國)
- Middle East (Bahrain)
- 南美洲 (聖保羅)
- 美國東部 (維吉尼亞北部)
- 美國東部 (俄亥俄)
- 美國西部 (加利佛尼亞北部)
- 美國西部 (奧勒岡)

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。

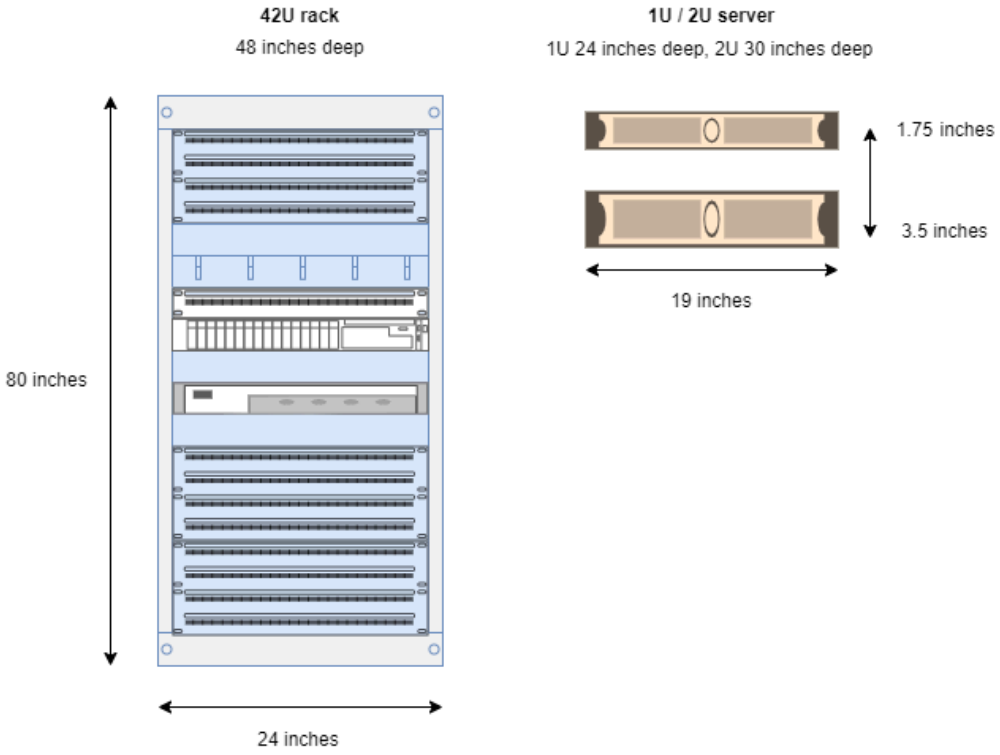
如需根據位置、組態和付款選項定價，請參閱：

- Outposts 機架定價
- Outposts 伺服器定價

如何 AWS Outposts 運作

AWS Outposts 旨在在您的 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

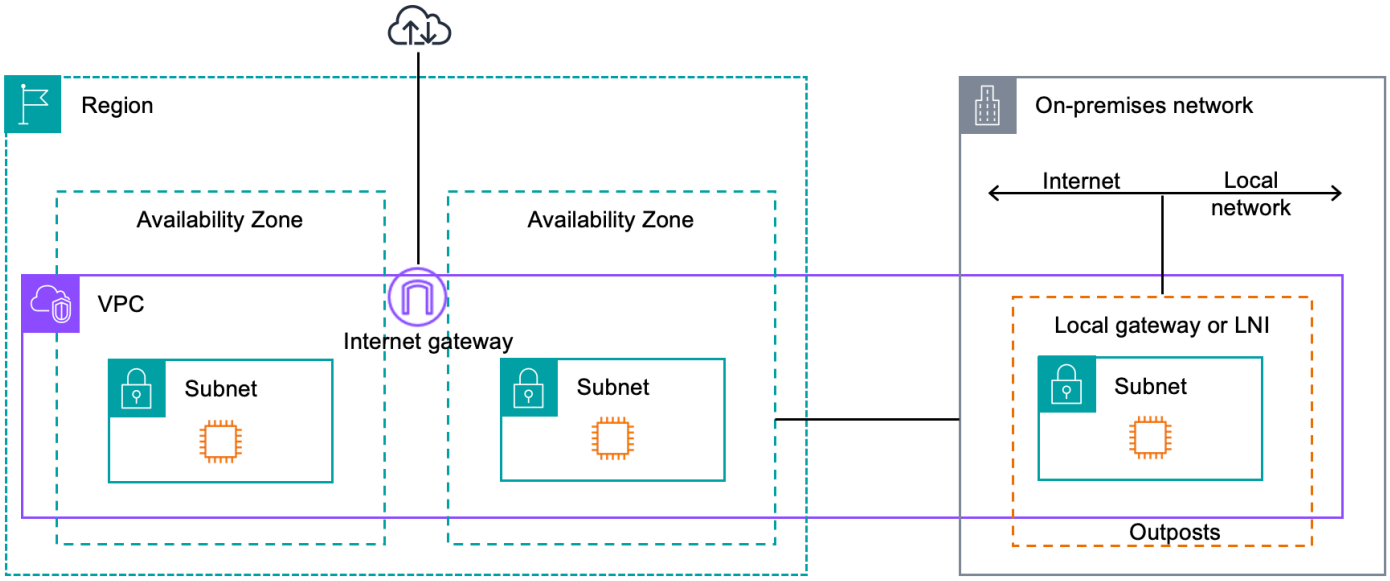
- 網路元件
- VPC 和子網路
- 路由
- DNS
- 服務連結
- 本機閘道
- 本機網路介面

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：本機網路界面 (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。
- 透過本機閘道跨 Outpost 進行 VPC 內部通訊 – 您可以使用直接 VPC 路由，在不同 Outpost 的相同 VPC 中的子網路之間建立通訊。如需詳細資訊，請參閱：
  - 直接 VPC 路由
  - 路由至 AWS Outposts 本機閘道

DNS

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

域。Route 53 解析程式託管在 AWS 區域中。因此，從 Outpost 到 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，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 與 的連線 AWS 區域
- 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

> **IPv6 支援**
>
> 您可以在 Outpost 上建立雙堆疊 (IPv6) 子網路。 僅 AWS Outposts 支援相同 Outpost 中子網路之間的 IPv6 流量。服務連結不支援 Outpost 和 之間的 IPv6 AWS 區域。此外， AWS Outposts 無法透過網際網路閘道使用 IPv6。

本機閘道

Outpost 機架包含本機閘道，可讓您連線至內部部署網路。如果您有 Outposts 機架，您可以包含本機閘道做為目標，其中目的地是您的內部部署網路。本機閘道僅適用於 Outposts 機架，並且只能在與 Outposts 機架相關聯的 VPC 和子網路路由表中使用。如需詳細資訊，請參閱：

- Outposts 機架的本機閘道
- 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

> **IPv6 支援**
>
> 本機閘道僅支援 IPv4 流量。它不支援 IPv6。

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

Outposts 機架的站點需求

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

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

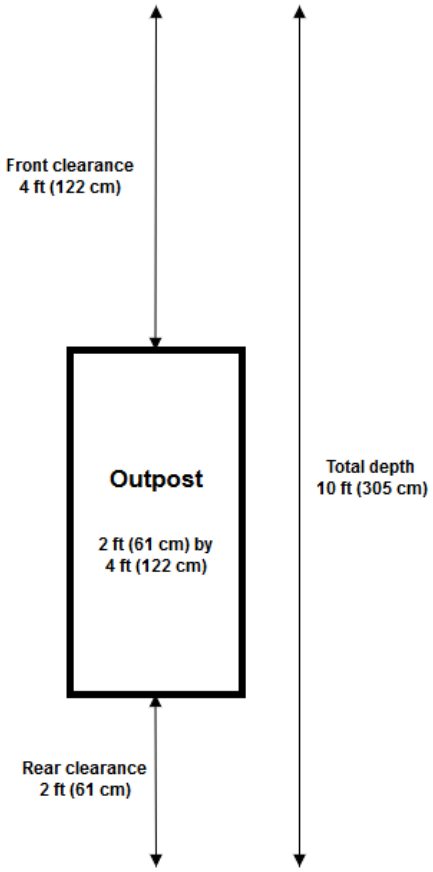
如需 Outpost 伺服器的要求，請參閱《AWS Outposts Outpost 伺服器使用者指南》中的《Outpost 伺服器的站點要求》。

設施

以下是機架的設施要求。

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

  下圖顯示 Outpost 所需的最小總面積 (包括間隙)。



- 地震波紋 – 在法規或程式碼要求的範圍內，當機架位於您的設施時，您將為機架安裝和維護適當的地震波紋和波紋。 AWS 提供地面波紋，可為所有 Outposts 機架提供高達 2.0G 的地震活動提供保護。
- 聯結點 – 建議您在機架位置提供聯結線/點，讓您的電工可以在安裝期間聯結機架，由 AWS經過認證的技術人員驗證。
- 設施存取 – 您不會以負面影響 AWS 存取、服務或移除 Outpost 的能力的方式變更設施。
- 海拔高度 – 安裝機架的機房海拔高度必須低於 10,005 英呎 (3,050 公尺)。

聯網

以下是機架的網路要求。

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

  如需服務連結連線的頻寬建議，請參閱《頻寬建議》。

- 提供單模光纖 (SMF) 搭配 Lucent 連接器 (LC)、多模光纖 (MMF) 或 MMF OM4 搭配 LC。
- 提供一或兩部上游裝置，可以是交換器或路由器。建議使用兩部裝置以提供高可用性。

網路整備檢查清單

當您收集 Outpost 組態的資訊時，請使用此檢查清單。這包括 LAN、WAN，以及 Outpost 與本機流量目的地之間的任何裝置，以及 AWS 區域中的目的地。

上行鏈路速度、連接埠和光纖

上行鏈路速度和連接埠

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

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

1 Gbps

1、2、4、6 或 8 個上行鏈路

10 Gbps

1、2、4、8、12 或 16 個上行鏈路

40 Gbps 或 100 Gbps

1、2 或 4 個上行鏈路

光纖

AWS Outposts 需要具有 Lucent Connectors (LC) 的光纖。

下表列出支援的光學標準和所需的對應光纖類型。如果光纖標準使用多光纖推送 (MPO) 連接器，您將需要 MPO 到 4 x LC Type-B 分線，其中 4 x LC 連接器連接到 Outpost 以建立一個連結。

上行鏈路速度	光學標準	光纖類型
1 Gbps	– 1000Base-LX	SMF (LC)
1 Gbps	– 1000Base-SX	MMF (LC)
10 Gbps	– 10GBASE-IR	SMF (LC)

上行鏈路速度	光學標準	光纖類型
	– 10GBASE-LR	
10 Gbps	– 10GBASE-SR	MMF (LC)
40Gbps	– 40GBASE-IR4 (LR4L) – 40GBASE-LR4	SMF (LC)
40Gbps	– 40GBASE-ESR4 – 40GBASE-SR4	MMF (MPO 到 4 x LC Type-B 分組)
100 Gbps	– 100GBASE-CWDM4 – 100GBASE-LR4	SMF (LC)
100 Gbps	– 100G PSM4 MSA	SMF (MPO 到 4 x LC Type-B 分組)
100 Gbps	– 100GBASE-SR4	MMF (MPO 到 4 x LC Type-B 分組)

Outpost 連結彙總和 VLAN

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

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

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

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

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

Outpost 網路裝置 IP 連線

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

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

服務連結最大傳輸單位 (MTU)

網路必須在 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》。

服務連結邊界閘道協定

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

Outpost	服務連結 BGP 要求
您的 Outpost	– Outpost BGP 自治系統編號 (ASN)。2 個位元組 (16 位元) 或 4 個位元組 (32 位元)。來自您的私有 ASN 範圍 (64512-65534 或 4200000000-4294967294)。 – 基礎設施 CIDR (需要 /26，已公告為兩個連續 /27)。

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

服務連結防火牆

必須在防火牆中以具狀態方式列出 UDP 和 TCP 443。

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

您可以使用 Direct Connect 連線或公有網際網路連線，將 Outpost 連線至 AWS 區域。對於 Outpost 服務連結連線，您可以在防火牆或邊緣路由器上使用 NAT 或 PAT。一律會從 Outpost 起始建立服務連結。

如需服務連結需求的詳細資訊，例如 MTU 和 175 毫秒延遲，請參閱透過服務連結的連線。

本機閘道邊界閘道協定

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

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

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

電源

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

若要查看不同 Outpost 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：//https://console.aws.amazon.com/outposts/。

需求	規格
AC 電源線電壓	單相 208 到 277 VAC；50 或 60 Hz 三階段：

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

電源機箱具有兩個輸入 S1 和 S2，可依照下列方式配置。

	備援、單相	備援、三相	單相	三相
5 kVA	2 x L6-30P 或 IEC309；1 降至 S1，1 降至 S2	2 x AH530P7W, AH532P6W或 CS8365C；1 降至 S1，1 降至 S2	未提供	1 x AH530P7W, AH532P6W或 CS8365C；1 捨棄至 S1
10 kVA	4 個 L6-30P 或 IEC309；2 個降至 S1，2 個降至 S2		2 x L6-30P 或 IEC309；2 捨棄至 S1	
15 kVA	6 x L6-30P 或 IEC309；3 滴至 S1，3 滴至 S2		3 x L6-30P 或 IEC309；3 捨棄至 S1	

如果 AWS 提供的 AC 低音必須安裝替代電源插頭，請考慮下列事項：

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

訂單履行

為了履行訂單， AWS 會為您安排日期和時間。您也會收到安裝之前要確認或提供的項目檢查清單。

AWS 安裝團隊將在排定的日期和時間抵達您的站點。他們會將機架放在識別的位置。您和您的電工必須負責執行機架的電氣連接和安裝。

您必須確保電氣裝置以及這些裝置的任何變更，均由經認證的電工根據所有適用法律、法規和最佳實務來執行。在對 Outpost 硬體或電氣安裝進行任何變更之前，您必須先取得 AWS 的書面同意。您同意 AWS 提供文件，以驗證任何變更的合規性和安全性。對於 Outpost 電氣安裝或設施電氣線路或任何變更所產生的任何風險 AWS ， 概不負責。您不得對 Outpost 硬體進行任何其他變更。

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

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

Outpost ACE 機架的站點需求

> **Note**
>
> 只有在您需要 ACE 機架時才適用。

彙總、核心、邊緣 (ACE) 機架可做為多機架 Outpost 部署的網路彙總點。

若要安裝 ACE 機架，除了 中列出的要求之外，您還必須符合本節中的要求Outposts 機架的站點需求。

ACE 機架容量和擴展

單一 ACE 機架最多支援 15 個運算機架。對於需要超過 15 個運算機架的部署，可以部署額外的網路基礎設施，以擴展超過此限制的容量。

如果您預期部署成長超過 4 個運算機架，建議您預先安裝 ACE 機架以支援未來的擴展。對於具有 1-4 個運算機架的部署，不需要專用網路機架。請聯絡您的 AWS 客戶團隊，討論超過 15 個運算機架的部署擴展選項。

> **Note**
>
> ACE 機架並非完全封閉，也不包含前門或後門。

設施

這些是 ACE 機架的設施需求。

- 電源 – 所有 ACE 機架都隨附 10kVA 單相 (AA+BB；IEC60309 或 L6-30P Whip 連接器類型）。
- 重量支援 – ACE 機架重 705 磅 (320 公斤）。
- 間隙/大小維度 – ACE 機架為 80 英吋 (203 公分） 高、24 英吋 (61 公分） 寬和 42 英吋 (107 公分） 深。

  如果 ACE 機架具有纜線管理臂，則機架的寬度為 36 英吋 (91.5 公分）。

聯網

這些是 ACE 機架的聯網需求。若要了解 ACE 機架如何連接 Outposts 網路裝置、內部部署網路裝置和 Outposts 機架，請參閱 ACE 機架連線。

- 機架網路需求 – 請確定您符合 網路整備檢查清單和 Outposts 機架的本機網路連線區段中列出的需求，但下列變更除外：
  - ACE 機架有四個連接到上游裝置的聯網裝置，而不是兩個，就像單一 Outposts 機架一樣。
  - ACE 機架不支援 1 Gbps 上行鏈路。
- 上行速度 – 提供速度為 10 Gbps、40 Gbps 或 100 Gbps 的上行速度。如需服務連結連線的頻寬建議，請參閱服務連結頻寬建議。

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

- 光纖 – 使用 Lucent Connector (LC) 提供單模光纖 (SMF)，或使用 Lucent Connector (LC) 提供多模光纖 (MMF)。如需支援光纖類型和光學標準的完整清單，請參閱 上行鏈路速度、連接埠和光纖。
- 上游裝置 – 提供兩個或四個上游裝置，可以是交換器或路由器。
- 服務 VLAN 和本機閘道 VLAN – 對於四個 ACE 網路裝置，您必須提供服務 VLAN 和不同的本機閘道 VLAN。您可以選擇僅提供兩個不同的 VLANs，一個用於服務 VLAN，另一個用於本機閘道 VLAN，或每個 ACE 網路裝置中都有不同的 VLANs 用於服務 VLAN 和 LGW VLAN，總共 8 個不同的 VLANs。如需如何使用連結彙總群組 (LAGs) 和 VLAN 的詳細資訊，請參閱 連結彙總和 虛擬 LAN。
- 服務連結和本機閘道 VLANs 的 CIDR 和 IP 地址 – 我們建議為每個 ACE 網路裝置配置專用子網路，並使用 /30 或 /31 CIDR。或者，您可以在每個服務和本機閘道 VLAN 中配置單一 /29 子網路。在這兩種情況下，您必須指定要使用的 ACE 網路裝置的 IP 地址。如需詳細資訊，請參閱網路層連線。
- 服務連結 VLAN 和本機閘道 VLAN 的客戶和 Outpost BGP 自治系統編號 (ASN) – Outpost 會在每個 ACE 機架裝置和本機網路裝置之間建立外部 BGP (eBGP) 對等工作階段，以便透過服務連結 VLAN 進行服務連結連線。此外，它會建立從每個 ACE 網路裝置到本機網路裝置的 eBGP 對等互連工作階段，以便從本機網路連線至本機閘道。如需詳細資訊，請參閱服務連結 BGP 連線及本機閘道 BGP 連線。

> **Important**
>
> 服務連結基礎設施子網路 – Outposts 安裝中包含的每個運算機架都需要服務連結基礎設施子網路 （ 必須是 /26)。

電源

這些是 ACE 機架的電源需求。

需求	規格
AC 電源線電壓	單相 200 到 240 VAC；50 或 60 Hz
耗電量	10 kVA 單相 (AA+BB)
AC 保護裝置 (上游斷路器)	僅限 2N 輸入 (備援)：C 曲線、D 曲線或 K 曲線斷路器。 不支援 B 曲線或更低規格。
AC 電源插座類型 (插座)	IEC60309 或 L6-30P 鞭形連接器類型。

Outposts 機架入門

訂購 Outposts 機架以開始使用。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 Outposts 機架的訂單
- 在 Outposts 機架上啟動執行個體
- 最佳化適用於 的 Amazon EC2 AWS Outposts

建立 Outposts 機架的訂單

若要開始使用 AWS Outposts，您必須建立網站、建立 Outpost、取得引號，然後下單。

先決條件

- 檢閱 Outpost 機架的可用配置。
- Outpost 站點是 Outpost 設備的實體位置。訂購容量之前，請確認您的站點是否符合要求。如需詳細資訊，請參閱Outposts 機架的站點需求。
- 您必須擁有AWS 企業支援計劃或AWS 統一營運計劃。
- 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：建立引號
- 步驟 4：下訂單
- 步驟 5：修改執行個體容量
- 後續步驟

步驟 1：建立站點

建立站點以指定操作地址。操作地址是 Outpost 機架的實體位置。

先決條件

- 確定操作地址。

建立網站

1. 登入 AWS。
2. 在 https：//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 機架和伺服器。
7. 輸入站點的名稱、描述和營運地址。
8. 針對 站點詳細資訊，提供要求的站點資訊。
   - 最大重量 – 此站點可支撐的最大機架重量，以 lbs 為單位。向您的設施團隊或結構工程師檢查您樓層的負載評分，並將其乘以機架足跡 (42U 機架約為 6 平方英尺）。
   - 耗電量 – 機架硬體放置位置可用的耗電量，以 kVA 為單位。檢查機架可用的斷路器或電源分配單元 (PDUs容量。
   - 電源選項 – 您可以為硬體提供的電源選項。
   - 電源接頭 – AWS 應計畫提供以連接到硬體的電源接頭。
   - 供電位置 – 指出是從機架上方或下方供電。
   - 上行鏈路速度 – 機架連線到區域時應支援的上行鏈路速度，以 Gbps 為單位。
   - 上行鏈路數目 – 您要用來將機架連線到網路之每部 Outpost 網路裝置的上行鏈路數目。
   - 光纖類型 – 您要用來將機架連線到網路的光纖類型。
   - 光學標準 – 您要用來將機架連線到網路的光學標準類型。
9. （選用）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。
10. 閱讀設施要求，然後選取 我已閱讀設施要求。
11. 選擇 Create site (建立網站)。

步驟 2：建立 Outpost

為您的機架建立 Outpost。當您建立引號並下單時，您將指定此 Outpost。

先決條件

- 決定要與您的網站建立關聯的 AWS 可用區域。

> **不支援的可用區域**
>
> AWS Outposts 不支援下列可用區域：use1-az3、usw1-az2、euw1-az2 和 apne1-az3。若要在這些 AWS Outposts 區域中使用 AWS 區域，請選取不同的可用區域。

建立 Outpost

1. 在導覽窗格中，選擇 Outposts。
2. 選擇 建立 Outpost。
3. 選擇 機架。
4. 輸入 Outpost 的名稱和描述。
5. 選擇 Outpost 的可用區域。
6. (選擇性) 若要設定私有連線，請選取 使用私有連線。選擇與 Outpost 位於相同 和可用區域中的 VPC AWS 帳戶 和子網路。如需詳細資訊，請參閱the section called “先決條件”。

   > **Note**
   >
   > 如果您需要移除 Outpost 的私有連線，您必須聯絡 AWS 支援 中心。

7. 針對 站點 ID，選擇您的站點。
8. 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：建立引號

引號會根據您的 Outpost 組態提供成本估算。它包含機架組態，顯示下訂單時您的設定會是什麼樣子。引號會在幾秒內產生，有效期為 30 天。

建立引號

1. 從導覽窗格中，選擇引號。
2. 選擇建立引號。
3. 如需一般資訊，請提供下列項目：

   - 描述（選用）– 輸入描述以協助區分引號。例如，包含 Outpost 的目的、組態或特定需求。
   - Outpost 類型 – 如果您要建立新的 Outpost，請選取新增 Outpost；如果您要擴展已部署 Outpost 的容量，請選取現有 Outpost。

   > **Note**
   >
   > 每月訂閱的 Outpost month-to-month 無法擴展。若要擴展，您必須先續約您的期限。

4. 國家/地區（新的 Outpost) – 選取將安裝 Outpost 的國家/地區。並非所有 Outpost 組態都適用於所有國家/地區。

   Outpost ID（現有的 Outpost) – 選取您要新增容量之 Outpost 的 Outpost ID。
5. 針對選取容量，選擇 Outpost 的運算容量。您可以透過兩種方式選取容量：

   - 依容量類型：選取所需 Amazon EC2 執行個體類型和大小的數量。
   - 依組態 – 從專為常見使用案例設計的預先定義組態中選取，或從您的帳戶歷史記錄中選取先前使用的組態。

   > **Note**
   >
   > 您只能選取所選 Outpost 產生和形式因素支援的執行個體容量。

6. 針對儲存類型，選取 Outpost 的儲存容量：

   - EBS 儲存 (TB) – 選取 Amazon EBS 儲存容量層，為您的 Amazon EC2 執行個體提供持久性區塊儲存。
   - S3 儲存 (TB)（選用）– 新增本機物件儲存的 Amazon S3 on Outposts 容量。

> **Note**
>
> 您的輸入將四捨五入至最接近支援的儲存層。並非所有區域都提供 Amazon S3 on Outposts 儲存。

7. （選用）如需網站詳細資訊，請提供網站的力量、空間和權重限制。雖然對於引號為選用，但提供網站詳細資訊有助於確保建議的組態適合您的設施，並可能影響您的預估引號。

> **Note**
>
> 下訂單需要完整的網站資訊，包括操作地址、運送地址和機架實體屬性。

8. 選擇取得引號。

產生引號後，您可以檢閱建議的 Outpost 組態和定價選項。您可以下載 PDF 格式的引號來共用或保留記錄。

編輯引號

- 導覽至引號頁面，選取您要修改的引號，選擇動作，然後選取編輯引號。這可讓您更新需求並接收修訂後的預估值。

> **Note**
>
> 您可以使用重新整理按鈕來更新定價，而不變更您的組態，以重新整理現有的引號。引號會在 30 天後過期。您可以使用重新建立引號按鈕重新建立過期的引號，該按鈕會將過期引號中的相同詳細資訊填入新的引號表單。

步驟 4：下訂單

檢閱您的引號後，您就可以下訂單。每個引號只能用於單一訂單。

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

先決條件

- 作用中的企業支援或統一操作計劃。
- 使用相關聯網站建立的 Outpost。
- 完整的網站詳細資訊，包括操作地址、運送地址和機架實體屬性。
- 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不預付，您將支付合約期間內的每月費用。

下訂單

1. 從導覽窗格中，選擇引號。
2. 選取您要從中訂購的引號，然後選擇下訂單。
3. 如果您的引號建立時只選取了國家/地區，則必須先選取 Outpost 才能繼續。
4. 針對付款條件，選取您的合約期限和付款選項：

   期限長度 – 選擇 Outpost 合約的長度：

   - 1 年合約 – 承諾較短，整體成本較高。
   - 3 年合約 – 承諾時間較長，整體成本較低。

   付款選項 – 選取您想要的付款方式：

   - 無預付 – 在整個合約期間內無需預付任何費用和更高的每月費用。
   - 部分預付 – 支付部分預付，減少合約剩餘部分的每月費用。
   - 全部預付 – 預付整個合約金額，無需每月費用。

> **Note**
>
> 如果您要將容量新增至現有的 Outpost，訂單將按比例分配，以符合現有的 Outpost 合約結束日期。

5. 選擇下一步。
6. 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。
7. 選擇 下訂單。

下訂單後，您將透過電子郵件收到訂單確認，其中包含後續步驟。

下訂單後

團隊 AWS 將與您合作：

- 完成現場準備需求。
- 排程網站評估以驗證網站準備程度。
- 協調安裝排程。
- 完成您區域的任何其他合規或法規要求。

驗證整備程度後，您的 Outpost 將會製造並交付。 AWS 技術人員將抵達現場開始安裝，這涉及啟動機架、執行基本組態，以及驗證 Outpost 網路裝置是否可以建立與 的加密連線 AWS 區域。

> **Note**
>
> 在合約期限結束時，您必須在目前訂閱結束前至少 5 個工作日選擇下列選項：續約訂閱、準備 Outpost 進行傳回，或轉換為month-to-month。如果您不採取任何動作，您的合約將以無預付費率自動轉換為month-to-month訂閱。

步驟 5：修改執行個體容量

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 安裝的機架大小和數量，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。

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 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。停止這些執行個體後， AWS Outposts 會執行任務。
> - 如果您在完成訂單後需要變更容量，請聯絡 AWS 支援 中心進行變更。

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。

   Example

   範例 JSON 檔案：

```
{
    "InstancePools": [
        {
            "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。停止這些執行個體後， AWS Outposts 會執行任務。
> - 如果您在完成訂單後需要變更容量，請聯絡 AWS 支援 中心進行變更。
> - 若要疑難排解問題，請參閱疑難排解容量任務問題。

後續步驟

您可以使用 AWS Outposts 主控台檢視訂單的狀態。訂單的初始狀態為已建立。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 會為您安排日期和時間。

您也會收到安裝之前要確認或提供的項目檢查清單。 AWS 安裝團隊將在排定的日期和時間抵達您的站點。團隊會將機架移至指定的位置，而您的電工可以為機架供電。團隊會透過您提供的上行鏈路為機架建立網路連線，並設定機架的容量。當您確認 Outpost 的 Amazon EC2 和 Amazon EBS 容量可從 AWS 您的帳戶取得時，安裝即完成。

在 Outposts 機架上啟動執行個體

安裝 Outpost 並可使用運算和儲存容量之後，即可開始建立資源。使用 Outpost 子網路在 Outpost 上啟動 Amazon EC2 執行個體，並建立 Amazon EBS 磁碟區。您也可以在 Outpost 上建立 Amazon EBS 磁碟區的快照。如需詳細資訊，請參閱《Amazon EBS 使用者指南》中的 上的 Amazon EBS 本機快照 AWS Outposts。

先決條件

您的站點必須安裝 Outpost。如需詳細資訊，請參閱建立 Outposts 機架的訂單。

任務

- 步驟 1：建立 VPC
- 步驟 2：建立子網路和自訂路由表
- 步驟 3：設定本機閘道連線
- 步驟 4：設定內部部署網路

- 步驟 5：在 Outpost 上啟動執行個體
- 步驟 6：測試連線能力

步驟 1：建立 VPC

您可以將 AWS 區域中的任何 VPC 擴展到 Outpost。如果您已經有可使用的 VPC，請略過此步驟。

為您的 Outpost 建立 VPC

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 選擇與 Outposts 機架相同的區域。
3. 在導覽窗格中，選擇您的 VPCs，然後選擇建立 VPC。
4. 僅選擇 VPC。
5. （選用）針對名稱標籤輸入 VPC 的名稱。
6. 對於 IPv4 CIDR 區塊，選擇 IPv4 CIDR 手動輸入，然後在 IPv4 CIDR 文字方塊中輸入 VPC 的 IPv4 地址範圍。

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

7. 針對 IPv6 CIDR 區塊，選擇無 IPv6 CIDR 區塊。
8. 針對租用，選擇預設。
9. （選用）若要將標籤新增至 VPC，請選擇新增標籤，然後輸入索引鍵和值。
10. 選擇建立 VPC。

步驟 2：建立子網路和自訂路由表

您可以建立 Outpost 子網路，並將其新增至 Outpost 所在 AWS 區域中的任何 VPC。當您這樣做時，VPC 會包含 Outpost。如需詳細資訊，請參閱網路元件。

> **Note**
>
> 如果您要在另一個已與您共用的 Outpost 子網路中啟動執行個體 AWS 帳戶，請跳至步驟 5：在 Outpost 上啟動執行個體。

2a：建立 Outpost 子網路

建立 Outpost 子網路

1. 在 https：//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。
5. 在子網路設定中，選擇性地為您的子網路命名，並指定子網路的 IP 地址範圍。
6. 選擇 Create subnet (建立子網路)。
7. （選用）若要更輕鬆地識別 Outpost 子網路，請啟用子網路頁面上的 Outpost ID 欄。若要啟用資料欄，請選擇偏好設定圖示，選取 Outpost ID，然後選擇確認。

2b：建立自訂路由表

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

建立自訂路由表

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

2c：關聯 Outpost 子網路和自訂路由表

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

建立 Outpost 子網路和自訂路由表的關聯

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

步驟 3：設定本機閘道連線

本機閘道 (LGW) 可啟用 Outpost 子網路與內部部署網路之間的連線。

如需 LGW 的詳細資訊，請參閱本機閘道。

若要在 Outposts 子網路中的執行個體與本機網路之間提供連線，您必須完成下列任務。

3a. 建立自訂本機閘道路由表

使用下列程序為本機閘道建立自訂路由表。

建立自訂本機閘道路由表

1. 在 https：//https://console.aws.amazon.com/outposts/ 開啟 AWS Outposts 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選擇 建立本機閘道路由表。
5. (選用) 針對 Name (名稱)，輸入路由表的名稱。
6. 針對 本機閘道，選擇您的本機閘道。
7. 針對 模式，選擇與您內部部署網路通訊的模式。
   - 選擇直接 VPC 路由以使用執行個體的私有 IP 地址。
   - 選擇 CoIP 以使用客戶擁有 IP 地址集區中的地址。如需詳細資訊，請參閱建立 CoIP 集區。

8. (選用) 若要新增標籤，請選擇新增標籤，然後輸入標籤金鑰和標籤值。
9. 選擇 建立本機閘道路由表。

3b：將 VPC 與自訂路由表建立關聯

使用下列程序將 VPC 與本機閘道路由表建立關聯。這兩者預設沒有關聯。

將 VPC 與自訂本機閘道路由表建立關聯

1. 在 https：//https://console.aws.amazon.com/outposts/ 開啟 AWS Outposts 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選取路由表，然後選擇 動作、關聯 VPC。
5. 針對 VPC ID，選取要與本機閘道路由表建立關聯的 VPC。
6. (選用) 若要新增標籤，請選擇新增標籤，然後輸入標籤金鑰和標籤值。
7. 選擇 Associate VPC (關聯 VPC)。

3c：在 Outpost 子網路路由表中新增路由項目

在 Outpost 子網路路由表中新增路由項目，以啟用 Outpost 子網路與本機閘道之間的流量。

VPC 內的 Outpost 子網路與本機閘道路由表相關聯，可以為其路由表具有額外的 Outpost 本機閘道 ID 目標類型。考慮您希望透過本機閘道將目的地地址為 172.16.100.0/24 的流量路由到客戶網路的情況。若要這樣做，請編輯 Outpost 子網路路由表，並使用目的地網路和本機閘道的目標新增下列路由。

目標	Target
172.16.100.0/24	`lgw-id`

將具有本機閘道的路由項目新增為子網路路由表中的目標

1. 在 https://console.aws.amazon.com/vpc/ 開啟 Amazon VPC 主控台。
2. 在導覽窗格中，選擇路由表，然後選取您在 中建立的路由表2b：建立自訂路由表。
3. 選擇動作，然後選擇編輯路由。
4. 若要新增路由，請選擇 Add route (新增路由)。

5. 針對目的地，將目的地 CIDR 區塊輸入至客戶網路。
6. 針對目標，選擇 Outpost 本機閘道 ID。
7. 選擇儲存變更。

3d：將自訂路由表與 VIF 群組建立關聯，以建立本機閘道路由網域

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

將自訂路由表與 VIF 群組建立關聯

1. 在 https：//https://console.aws.amazon.com/outposts/ 開啟 AWS Outposts 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 在導覽窗格中，選擇聯網，然後選擇 LGW 路由網域。
4. 選擇建立 LGW 路由網域。
5. 輸入本機閘道路由網域的名稱。
6. 選擇本機閘道、本機閘道 VIF 群組和本機閘道路由表。
7. 選擇建立 LGW 路由網域。

3e：在路由表中新增路由項目

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

目標	Target
172.16.100.0/24	`VIF-Group-ID`

在 LGW 路由表中新增路由項目

1. 在 https：//https://console.aws.amazon.com/outposts/ 開啟 AWS Outposts 主控台。
2. 在導覽窗格中，選擇 本機閘道路由表。
3. 選取本機閘道路由表，然後選擇動作、編輯路由。
4. 選擇 Add route (新增路由)。
5. 針對 目的地，輸入目的地 CIDR 區塊、單一 IP 地址或字首清單的 ID。

6. 針對 目標，選取本機閘道的 ID。
7. 選擇 Save routes (儲存路由)。

3f：（選用）將客戶擁有的 IP 地址指派給執行個體

如果您在 中3a. 建立自訂本機閘道路由表將 Outposts 設定為使用客戶擁有的 IP (CoIP) 地址集區，則必須從 CoIP 地址集區配置彈性 IP 地址，並將彈性 IP 地址與執行個體建立關聯。如需詳細資訊，請參閱《客戶擁有的 IP 地址》。

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

共用的客戶擁有 IP 地址集區

如果您想要使用共用的客戶擁有 IP 地址集區，則必須先共用該集區，然後才能開始設定。如需如何共用客戶擁有的 IPv4 地址的詳細資訊，請參閱 the section called “共用 Outpost 資源”。

步驟 4：設定內部部署網路

Outpost 會建立從每個 Outpost 網路裝置 (OND) 到客戶本機網路裝置 (CND) 的外部 BGP 對等互連，以將流量從現場部署網路傳送至 Outpost。

如需詳細資訊，請參閱本機閘道 BGP 連線。

若要從您的內部部署網路傳送和接收流量至 Outpost，請確定：

- 在您的客戶網路裝置上，本機閘道 VLAN 上的 BGP 工作階段從您的網路裝置處於 ACTIVE 狀態。
- 對於從內部部署到 Outposts 的流量，請確定您在 CND 中收到來自 Outposts 的 BGP 廣告。這些 BGP 公告包含您的內部部署網路必須用來將流量從內部部署路由到 Outpost 的路由。因此，請確定您的網路在 Outposts 和內部部署資源之間具有正確的路由。
- 對於從 Outposts 到內部部署網路的流量，請確保您的 CNDs將內部部署網路子網路的 BGP 路由公告傳送到 Outposts（或 0.0.0.0/0)。或者，您可以向 Outposts 公告預設路由（例如 0.0.0.0/0)。CNDs公告的內部部署子網路的 CIDR 範圍必須等於或包含在您在 中設定的 CIDR 範圍中3e：在路由表中新增路由項目。

範例：直接 VPC 模式中的 BGP 公告

假設您有一個 Outpost，設定為 Direct VPC 模式，而兩個 Outposts 機架網路裝置透過本機閘道 VLAN 連接到兩個客戶本機網路裝置。設定了下列項目：

- 具有 CIDR 區塊 10.0.0.0/16 的 VPC。
- VPC 中具有 CIDR 區塊 10.0.3.0/24 的 Outpost 子網路。
- 內部部署網路中具有 CIDR 區塊 172.16.100.0/24 的子網路
- Outposts 會使用 Outpost 子網路上執行個體的私有 IP 地址，例如 10.0.3.0/24，與您的內部部署網路通訊。

在此案例中， 公告的路由：

- 您客戶裝置的本機閘道為 10.0.3.0/24。
- Outpost 本機閘道的客戶裝置為 172.16.100.0/24。

因此，本機閘道會將目的地網路 172.16.100.0/24 的傳出流量傳送至您的客戶裝置。請確定您的網路具有正確的路由組態，以將流量傳送到網路中的目的地主機。

如需檢查 BGP 工作階段狀態所需的特定命令和組態，以及這些工作階段中的公告路由，請參閱網路供應商的文件。

如需故障診斷，請參閱AWS Outposts 機架網路故障診斷檢查清單。

範例：CoIP 模式中的 BGP 公告

假設您的 Outpost 有兩個 Outposts 機架網路裝置透過本機閘道 VLAN 連接到兩個客戶本機網路裝置的案例。設定了下列項目：

- 具有 CIDR 區塊 10.0.0.0/16 的 VPC。
- VPC 中具有 CIDR 區塊 10.0.3.0/24 的子網路。
- 客戶擁有的 IP 集區 (10.1.0.0/26)。
- 將 10.0.3.112 關聯到 10.1.0.2 的彈性 IP 地址關聯。
- 內部部署網路中具有 CIDR 區塊 172.16.100.0/24 的子網路
- Outpost 與內部部署網路之間的通訊將使用 CoIP 彈性 IP 來定址 Outpost 中的執行個體，而不是使用 VPC CIDR 範圍。

在此案例中，路由公告者：

- 您客戶裝置的本機閘道為 10.1.0.0/26。
- Outpost 本機閘道的客戶裝置為 172.16.100.0/24。

因此，本機閘道會將目的地網路 172.16.100.0/24 的傳出流量傳送至您的客戶裝置。確保您的網路具有正確的路由組態，以將流量交付至網路中的目的地主機。

如需檢查 BGP 工作階段狀態所需的特定命令和組態，以及這些工作階段中的公告路由，請參閱網路供應商的文件。

如需故障診斷，請參閱AWS Outposts 機架網路故障診斷檢查清單。

如需故障診斷，請參閱AWS Outposts 機架網路故障診斷檢查清單。

步驟 5：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

- 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。
- 您可以建立置放群組，以影響 Amazon EC2 應嘗試在 Outposts 硬體上置放相互依存執行個體群組的方式。您可以選擇符合工作負載需求的放置群組策略。
- 如果您新增 Amazon EBS 磁碟區，則必須使用 gp2 磁碟區類型。
- 如果您的 Outpost 已設定為使用客戶擁有的 IP (CoIP) 地址集區，則必須為您啟動的任何執行個體指派客戶擁有的 IP 地址。

在 Outpost 子網路中啟動執行個體

1. 在 https：//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 主控台中的執行個體啟動精靈。我們會為您選取 Outpost 子網路，並僅顯示 Outposts 機架支援的執行個體類型。
5. 選擇 Outposts 機架支援的執行個體類型。請注意，顯示為灰色的執行個體無法使用。
6. (選擇性) 若要將執行個體啟動到放置群組中，請展開 進階詳細資訊，然後捲動至 放置群組。您可以選取現有的放置群組或建立新的放置群組。

7. （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 6：測試連線能力

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 執行個體的私有 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 Linux 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
```

客戶擁有的 IP 地址連線範例

測試從您本機網路到 Outpost 的連線

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

```
ping 172.16.0.128
```

以下為範例輸出。

```
Pinging 172.16.0.128

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

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

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

測試從 Outpost 執行個體到您本機網路的連線

視您的作業系統而定，使用 ssh 或 rdp 連線到您 Outpost 執行個體的私有 IP 地址。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的連線至 EC2 執行個體。 Amazon EC2

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

```
ping 172.16.0.130
```

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

   ```
   ping 10.0.0.5
   ```

   以下為範例輸出。

   ```
   Pinging 10.0.0.5

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

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

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

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

最佳化適用於 的 Amazon EC2 AWS Outposts

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

目錄

- Outpost 上的專用執行個體
- 設定執行個體復原
- Outpost 中的放置群組

Outpost 上的專用執行個體

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

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

- 更改伺服器的容量配置
- 控制硬體層級的執行個體配置

更改伺服器的容量配置

專用主機可讓您變更 Outpost 部署中的伺服器配置，而無需聯絡 支援。當您為 Outpost 購買容量時，您可以指定每個伺服器提供的 EC2 容量配置。每部伺服器都支援單一系列的執行個體類型。一個配置可以提供單一執行個體類型或多個執行個體類型。專用執行個體可讓您更改為該初始配置選擇的任何內

容。如果您配置主機來支援整個容量的單一執行個體類型，則只能從該主機啟動單一執行個體類型。下圖顯示具有同質配置的 m5.24xlarge 伺服器：

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

如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的配置專用主機。

控制硬體層級的執行個體配置

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

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

設定執行個體復原

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

Outpost 中的放置群組

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

分散放置群組

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

機架層級分散放置群組

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

主機分散層級放置群組

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

分區放置群組

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

您也可以將執行個體部署到目標分割區。下圖顯示使用目標分散的分區放置群組。

如需使用置放群組的詳細資訊，請參閱《Amazon EC2 使用者指南》中的置放群組和置放群組 AWS Outposts。

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

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。

目錄

- 透過服務連結的連線
- 服務連結公有連線選項
- 服務連結私有連線選項
- 防火牆和服務連結
- Outposts 機架網路疑難排解檢查清單

透過服務連結的連線

服務連結是 Outposts 與 AWS 區域 （或主要區域） 之間的必要連線。它允許管理 Outposts 以及往返 AWS 區域的流量交換。服務連結利用一組加密的 VPN 連線來與主要區域進行通訊。

建立服務連結連線後，您的 Outpost 會變成可操作並由 管理 AWS。服務連結可促進下列流量：

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

服務連結最大傳輸單位 (MTU) 要求

網路連線的最大傳輸單位 (MTU) 係允許通過該連線的最大封包大小 (以位元組為單位)。

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 要求每個運算機架使用至少 500 Mbps 的備援連線，以及服務連結連線至 AWS 區域的往返延遲上限為 175 毫秒。您可以使用 AWS Direct Connect 或網際網路連線進行服

務連結。服務連結連線的最低 500 Mbps 和最長往返時間需求可讓您啟動 Amazon EC2 執行個體、連接 Amazon EBS 磁碟區，以及存取 AWS 具有最佳效能的服務，例如 Amazon EKS、Amazon EMR 和 CloudWatch 指標。

您的 Outpost 服務連結頻寬要求會因下列特性而有所不同：

- AWS Outposts 機架和容量組態的數量
- 工作負載特性，例如 AMI 大小、應用程式彈性、爆量速度需求和區域的 Amazon VPC 流量

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

當您建立從 Outpost 到 AWS 區域的連線時，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。

設定您的服務連結

下列步驟說明服務連結設定程序。

1. 選擇 Outposts 和主要 AWS 區域之間的連線選項。您可以選擇公有或私有連線。
2. 訂購 Outposts 機架之後， 會 AWS 與您聯絡，以收集 VLAN、IP、BGP 和基礎設施子網路 IPs。如需詳細資訊，請參閱本機網路連線。
3. 在安裝期間， 會根據您提供的資訊在 Outpost 上 AWS 設定服務連結。
4. 您可以將路由器等本機聯網裝置設定為透過 BGP 連線連接到每個 Outpost 網路裝置。如需服務連結 VLAN、IP 和 BGP 連線的資訊，請參閱 聯網。
5. 您可以設定您的聯網裝置，例如防火牆，讓您的 Outpost 能夠存取 AWS 區域或主要區域。 AWS Outposts 會使用服務連結基礎設施子網路 IPs來設定 VPN 連線，並與區域交換控制和資料流量。一律會從 Outpost 起始建立服務連結。

> **Note**
>
> 完成訂單後，您將無法修改服務連結組態或連線類型。

服務連結公有連線選項

您可以使用公有連線來設定 Outposts 與主要 AWS 區域之間的流量服務連結。您可以選擇使用公有網際網路或 Direct Connect 公VIFs。

如果您計劃在防火牆上只允許列出 AWS 區域公IPs（而不是 0.0.0.0/0），則必須確保您的防火牆規則與目前的 IP 地址範圍保持up-to-date狀態。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的AWS IP 位址範圍。

下圖顯示在您的 Outposts 和 AWS 區域之間建立服務連結公有連線的兩個選項：

選項 1。透過網際網路的公有連線

此選項需要 AWS Outposts 服務連結基礎設施子網路 IPs，才能存取您 AWS 區域或主要區域的公有 IP 範圍。您必須在防火牆等聯網裝置上允許列出 AWS 區域公IPs 或 0.0.0.0/0。

選項 2。透過公有 VIFs Direct Connect 公有連線

此選項需要 AWS Outposts 服務連結基礎設施子網路 IPs，才能透過 DX 服務存取您 AWS 區域或主要區域的公有 IP 範圍。您必須在防火牆等聯網裝置上允許列出 AWS 區域公IPs 或 0.0.0.0/0。

服務連結私有連線選項

您可以使用私有連線為 Outposts 和主要 AWS 區域之間的流量設定服務連結。您可以選擇使用 Direct Connect 私有或傳輸 VIFs。

當您使用主控台、 AWS CLI 或 API 建立 Outpost AWS Outposts 時，請選取私有連線選項。如需說明，請參閱建立 Outpost。

當您選取私有連線選項時，服務連結 VPN 連線會在安裝 Outpost 後，使用您指定的 VPC 和子網路建立。這允許透過 VPC 進行私有連線，並將公有網際網路暴露降至最低。

下圖顯示在您的 Outpost 和 AWS 區域之間建立服務連結 VPN 私有連線的兩個選項：

先決條件

您必須先符合下列先決條件，才能為 Outpost 設定私有連線：

- 您必須設定 IAM 實體（使用者或角色）的許可，以允許使用者或角色建立服務連結角色，以及為私有連線佈建角色。IAM 實體需要許可才能存取下列動作：
  - `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*` 的 `iam:CreateServiceLinkedRole`
  - `arn:aws:iam::*:role/aws-service-role/outposts.amazonaws.com/AWSServiceRoleForOutposts*` 的 `iam:PutRolePolicy`
  - `arn:aws:iam::*:role/service-role/AWSOutpostsProvisioningRole_*` 的 `iam:CreateRole`
  - `arn:aws:iam::*:role/service-role/AWSOutpostsProvisioningRole_*` 的 `iam:PutRolePolicy`
  - `ec2:DescribeVpcs`
  - `ec2:DescribeSubnets`
  - `ec2:DescribeVpcEndpoints`

  如需詳細資訊，請參閱 AWS Identity and Access Management for AWS Outposts
- 在與 Outpost 相同的 AWS 帳戶和可用區域中，建立 VPC，僅用於 Outpost 與子網路 /24 或更高版本的私有連線，而不會與 10.1.0.0/16 衝突。例如，您可以使用 10.3.0.0/16。

  > **Important**
  >
  > 請勿刪除此 VPC，因為它會維護與 Outpost 的連線。

- 使用安全控制政策 (SCP) 保護此 VPC 免於遭到刪除。

  下列範例 SCP 可防止刪除下列項目：
  - 已標記 Outposts 錨點子網路的子網路
  - VPC 標記的 Outposts 錨點 VPC
  - 標記為 Outposts 錨點路由表的路由表
  - 標記為 Outposts Transit Gateway 的傳輸閘道
  - Virtual Private Gateway 標記的 Outposts Virtual Private Gateway
  - 標記為 Outposts Transit Gateway Route Table 的傳輸閘道路由表
  - 任何具有 Outposts Anchor ENI 標籤的 ENI
- 設定連接到網路介面的安全群組，以允許下列傳入流量：
  - 來自您指定來源的 ICMP

- 來自您指定來源的 TCP 連接埠 443
- 來自您指定來源的 UDP 連接埠 443

> **Note**
>
> 連接埠 443 上的 TCP 和 UDP 都需要私有連線才能正常運作。

- 向您的內部部署網路公告子網路 CIDR。您可以使用 AWS Direct Connect 來執行此操作。如需詳細資訊，請參閱《 指南》中的《Direct Connect Direct Connect 虛擬介面》和《使用 Direct Connect 閘道》。
- 在私有連線 VPC 和子網路 AWS Outposts 中為 建立 VPC 端點。設定私有連線時，需要 VPC 端點 ID。

  使用下列 VPC 端點設定：

  - 服務：Outposts (com.amazonaws.*region*.outposts)

    範例：`com.amazonaws.us-west-2.outposts`
  - 端點類型：界面
  - 啟用私有 DNS：設定為 false （停用）
  - VPC：您為私有連線建立的 VPC
  - 子網路：您為私有連線建立的子網路

  使用下列 IAM 政策文件：

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

- 建立端點的安全群組，並授權地址為 且沒有傳出規則的傳入 TCP 連接埠 443 `0.0.0.0/0` 和 ICMP 流量。

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

在您選取 Outpost 的私有連線選項之後， 會在您的帳戶中 AWS Outposts 自動建立服務連結角色，讓它代表您完成下列任務：

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

當您設定私有連線時， AWS Outposts 也會在名為 的帳戶中建立佈建角色`AWSOutpostsProvisioningRole_`*`outpostId`*。 AWS Outposts 服務使用此角色來啟動和監控 Outpost 的私有連線。

角色使用以下 JSON 信任政策。*`accountId`* 將 取代為 AWS 您的帳戶 ID，並將 *`outpostArn`*取代為 Outpost ARN：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OutpostsProvisioningRoleTrustPolicy",
      "Effect": "Allow",
      "Principal": { "Service": "outposts.amazonaws.com" },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "accountId" },
        "ArnEquals": { "aws:SourceArn": "outpostArn" }
      }
    }
  ]
}
```

此角色使用以下 JSON 內嵌許可政策：

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

Important

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

選項 1。透過私有 VIFs Direct Connect 私有連線

建立 AWS Direct Connect 連線、私有虛擬介面和虛擬私有閘道，以允許內部部署 Outpost 存取 VPC。

如需詳細資訊，請參閱Direct Connect 《 使用者指南》中的下列章節：

- 專用和託管連線
- 建立私有虛擬介面
- 虛擬私有閘道關聯

如果 AWS Direct Connect 連線位於與 VPC 不同的 AWS 帳戶中，請參閱Direct Connect 《 使用者指南》中的跨帳戶建立虛擬私有閘道的關聯。

選項 2。透過 Direct Connect 傳輸 VIFs私有連線

建立 AWS Direct Connect 連線、傳輸虛擬介面和傳輸閘道，以允許內部部署 Outpost 存取 VPC。

如需詳細資訊，請參閱Direct Connect 《 使用者指南》中的下列章節：

- 專用和託管連線
- 建立傳輸虛擬介面到 Direct Connect 閘道
- 傳輸閘道關聯

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	443	AWS Outposts 服務連結 /26	443	AWS Outposts 區域的公有網路

通訊協定	來源連接埠	來源地址	目標連接埠	目的地地址
TCP	1025-65535	AWS Outposts 服務連結 /26	443	AWS Outposts 區域的公有網路

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	443	AWS Outposts 服務連結 /26	443	AWS Outposts 區域的公有網路
TCP	1025-65535	AWS Outposts 服務連結 /26	443	AWS Outposts 區域的公有網路
UDP	443	AWS Outposts 區域的公有網路	443	AWS Outposts 服務連結 /26
TCP	443	AWS Outposts 區域的公有網路	1025-65535	AWS Outposts 服務連結 /26

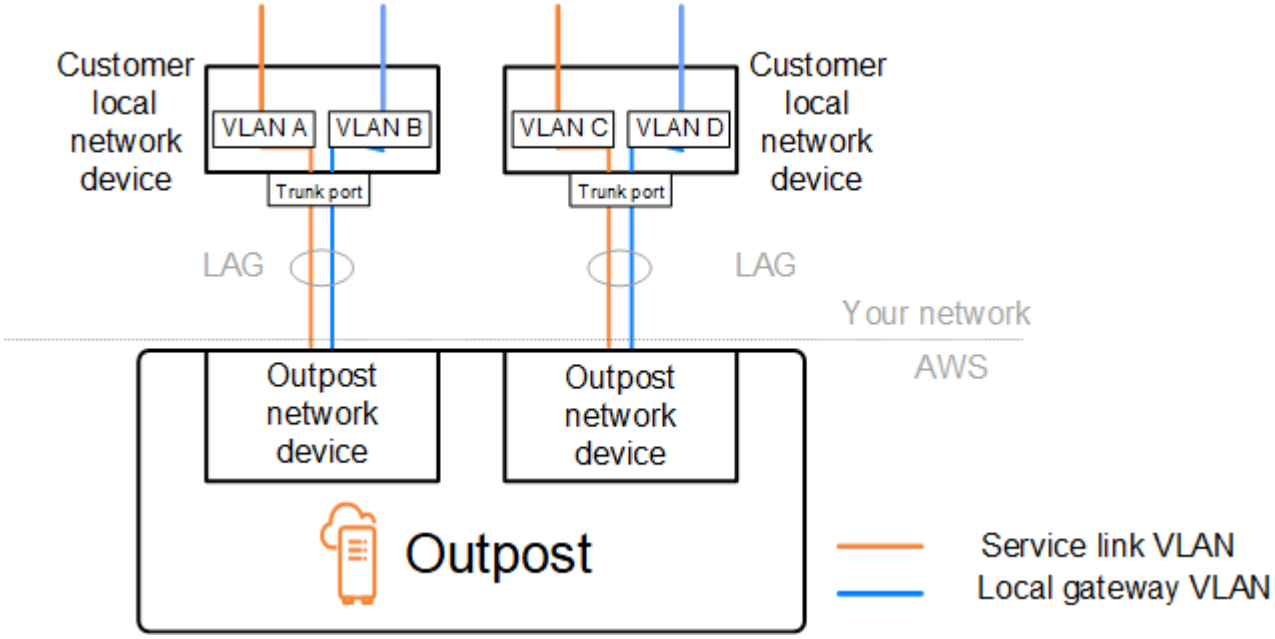
Note

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。

AWS Outposts 機架的設計也包含備援電源和聯網設備，包括本機閘道元件。如需詳細資訊，請參閱 中的彈性 AWS Outposts。

Outposts 機架網路疑難排解檢查清單

使用此檢查清單來協助針對狀態為 DOWN 的服務連結進行疑難排解。



與 Outpost 網路裝置的連線

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

1. 從客戶裝置 ping Outpost 網路裝置上的遠端對等 IP 地址。您可以在裝置的 BGP 組態中找到對等 IP 地址。您也可以參考安裝時提供給您的《網路整備檢查清單》。
2. 如果 ping 失敗，請檢查實體連線，並確定連線狀態為 UP。
   a. 確認客戶本機網路裝置的 LACP 狀態。
   b. 檢查裝置上的介面狀態。如果狀態為 UP，請跳至步驟 3。
   c. 檢查客戶本機網路裝置，並確認光學模組正常運作。
   d. 更換有缺陷的光纖，並確保指示燈 (Tx/Rx) 在可接受的範圍內。
3. 如果 ping 成功，請檢查客戶本機網路裝置，並確定下列 BGP 組態正確。
   a. 確認已正確設定本機自治系統編號 (客戶 ASN)。
   b. 確認已正確設定遠端自治系統編號 (Outpost ASN)。
   c. 確認已正確設定介面 IP 和遠端對等 IP 地址。
   d. 確認公告和接收的路由正確。

4. 如果您的 BGP 工作階段在作用中和連線狀態之間震盪，請確認客戶本機網路裝置上未封鎖 TCP 連接埠 179 和其他相關暫時性連接埠。
5. 如果您需要進一步疑難排解，請在客戶本機網路裝置上檢查下列各項：
   a. BGP 和偵錯日誌
   b. BGP 日誌
   c. 封包擷取
6. 如果問題仍存在，請從您的 Outpost 連線路由器對 Outpost 網路裝置對等 IP 地址執行 MTR/traceroute/封包擷取。使用您的企業支援計劃與 AWS Support 共用測試結果。

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

- 與 連線的邊緣路由器 Direct Connect – 用於服務連結連線的公有虛擬介面。如需詳細資訊，請參閱Direct Connect 區域公有虛擬介面連線 AWS。
- 與 連線的邊緣路由器 Direct Connect – 用於服務連結連線的私有虛擬介面。如需詳細資訊，請參閱Direct Connect 區域私有虛擬介面連線 AWS。
- 使用網際網路服務供應商 (ISP) 連線的邊緣路由器 – 用於服務連結連線的公有網際網路。如需詳細資訊，請參閱ISP 公有網際網路連線至 AWS 區域。

Direct Connect 區域公有虛擬介面連線 AWS

當公有虛擬介面用於服務連結連線 Direct Connect 時，請使用下列檢查清單來疑難排解與 連線的邊緣路由器。

1. 確認直接與 Outpost 網路裝置連線的裝置正在透過 BGP 接收服務連結 IP 地址範圍。
   a. 確認正在從您的裝置透過 BGP 接收路由。
   b. 檢查服務連結虛擬路由和轉送執行個體 (VRF) 的路由表。其中應該顯示正在使用 IP 地址範圍。
2. 若要確保區域連線，請檢查服務連結 VRF 的路由表。它應該包含 AWS 公有 IP 地址範圍或預設路由。
3. 如果您未在服務連結 VRF 中收到 AWS 公有 IP 地址範圍，請檢查下列項目。
   a. 從邊緣路由器或 檢查 Direct Connect 連結狀態 AWS 管理主控台。
   b. 如果實體連結為 UP，請從邊緣路由器檢查 BGP 對等互連狀態。

c. 如果 BGP 對等互連狀態為 DOWN，請 ping 對等 AWS IP 地址，並檢查邊緣路由器中的 BGP 組態。如需詳細資訊，請參閱 Direct Connect 使用者指南中的故障診斷 Direct Connect和 AWS 主控台中的我的虛擬介面 BGP 狀態已關閉。我該怎麼辦》。

d. 如果 BGP 已建立，且您在 VRF 中看不到預設路由或 AWS 公有 IP 地址範圍，請使用您的企業支援計劃聯絡 AWS Support。

4. 如果您有內部部署防火牆，請檢查下列項目。

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

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

b. 如果防火牆具有狀態，請確保傳出規則允許 Outpost 的服務連結 IP 地址範圍到 AWS 公有 IP 地址範圍。如需詳細資訊，請參閱AWS Outposts AWS 區域連線。

c. 如果防火牆不具狀態，請務必同時允許傳入流程（從 AWS 公有 IP 地址範圍到服務連結 IP 地址範圍）。

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

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

a. 確認 NAT 裝置未超載，且具有可用的連接埠以便配置新的工作階段。

b. 確認 NAT 裝置已正確設定為執行地址轉譯。

6. 如果問題仍然存在，請執行從邊緣路由器到 Direct Connect 對等 IP 地址的 MTR/追蹤路由/封包擷取。使用您的企業支援計劃與 AWS Support 共用測試結果。

Direct Connect 區域私有虛擬介面連線 AWS

當私有虛擬介面用於服務連結連線 Direct Connect 時，請使用下列檢查清單來疑難排解與 連線的邊緣路由器。

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

a. 從邊緣路由器 Ping 遠端對等 AWS IP 地址，並確認 BGP 對等互連狀態。

b. 請確定您的服務連結端點 VPC 與 內部部署上安裝的 Outpost 之間的 Direct Connect 私有虛擬介面上的 BGP 對等互連是 UP。如需詳細資訊，請參閱Direct Connect 《 使用者指南》中的故障診

斷 Direct Connect，我的虛擬介面 BGP 狀態在 AWS 主控台中已關閉。我該怎麼辦》和《如何針對透過 Direct Connect 的 BGP 對等互連問題進行疑難排解》。

c. Direct Connect 私有虛擬介面是與所選 Direct Connect 位置中邊緣路由器的私有連線，並使用 BGP 交換路由。您的虛擬私有雲端 (VPC) CIDR 範圍會透過此 BGP 工作階段向您的邊緣路由器公告。同樣地，Outpost 服務連結的 IP 地址範圍也會透過 BGP 從您的邊緣伺服器向區域公告。

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

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

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

2. 如果您的內部部署網路中有超過 100 個網路，您可以透過 BGP 工作階段將預設路由公告至私有虛擬介面 AWS 上的 。如果您不想公告預設路由，請彙總路由，以便公告路由的數量小於 100。
3. 如果問題仍然存在，請執行從邊緣路由器到 Direct Connect 對等 IP 地址的 MTR/追蹤路由/封包擷取。使用您的企業支援計劃與 AWS Support 共用測試結果。

ISP 公有網際網路連線至 AWS 區域

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

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

如果無法透過 ISP 連結存取網際網路或公有伺服器，請完成下列步驟。

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

如果可透過 ISP 連結存取網際網路和公有伺服器，請完成下列步驟。

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

如果問題仍存在，請執行 MTR/traceroute/封包擷取。

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

Outpost 位於兩個防火牆裝置後方

如果您已將 Outpost 放置在高可用性的同步防火牆或兩個獨立防火牆之後，可能會發生服務連結的非對稱路由。這表示傳入流量可以通過防火牆 1，而傳出流量則通過防火牆 2。使用下列檢查清單來識別服務連結的潛在非對稱路由，特別是在之前正常運作時。

- 確認公司網路的路由設定中是否有任何最近變更或持續維護，可能導致服務連結透過防火牆的非對稱路由。

  - 使用防火牆流量圖表來檢查流量模式的變更，以符合服務連結問題的開始。
  - 檢查是否有部分防火牆故障或分裂的防火牆對案例，可能導致您的防火牆不再互相同步其連線資料表。
  - 檢查公司網路中與服務連結問題開始相符的向下或最近路由變更 (OSPF/ISIS/EIGRP 指標變更、BGP 路由對應變更）。
- 如果您使用公有網際網路連線來連接主區域的服務連結，則服務提供者維護可能會透過防火牆導致服務連結的非對稱路由。
  - 檢查流量圖表 (ISP) 的連結是否有與服務連結問題開始相符的流量模式變更。
- 如果您使用服務連結的 Direct Connect 連線，則 AWS 計劃的維護可能會觸發服務連結的非對稱路由。
  - 檢查 （ 您的 ） Direct Connect 服務的計劃維護通知。
  - 請注意，如果您有備援 Direct Connect 服務，您可以在維護條件下，主動測試 Outposts 服務連結在每個可能網路路徑上的路由。這可讓您測試其中一個 Direct Connect 服務的中斷是否會導致服務連結的非對稱路由。end-to-end網路連線 Direct Connect 的部分彈性可由 Direct Connect Resiliency with Resiliency Toolkit 測試。如需詳細資訊，請參閱使用 Direct Connect 彈性測試彈性工具組 – 容錯移轉測試。

在您完成上述檢查清單並將服務連結的非對稱路由定位為可能的根本原因之後，您可以採取一些進一步的動作：

- 透過還原任何公司網路變更或等待供應商規劃的維護完成來還原對稱路由。
- 登入一個或兩個防火牆，並從命令列清除所有流程的所有流程狀態資訊 （ 如果防火牆廠商支援）。
- 透過其中一個防火牆暫時篩選出 BGP 公告，或關閉某個防火牆上的介面，以強制透過另一個防火牆進行對稱路由。
- 輪流重新啟動每個防火牆，以消除防火牆記憶體中服務連結流量的流程狀態追蹤中的潛在損毀。
- 與您的防火牆廠商互動，以驗證或放寬追蹤連接埠 443 上來源且目的地為連接埠 443 之 UDP 連線的 UDP 流程狀態。

Outposts 機架的本機閘道

本機閘道是 Outposts 機架架構的核心元件。本機閘道可啟用 Outpost 子網路與內部部署網路之間的連線。如果內部部署基礎設施提供網際網路存取，在 Outposts 機架上執行的工作負載也可以利用本機閘道與區域服務或區域工作負載通訊。您可以使用公有連線 （網際網路） 或使用 來達成此連線 Direct Connect。如需詳細資訊，請參閱AWS Outposts AWS 區域連線。

目錄

- 本機閘道基本概念
- 本機閘道路由
- 透過本機閘道的連線
- 本機閘道路由表
- 本機閘道路由表路由
- 建立 CoIP 集區
- 監控本機閘道連線

本機閘道基本概念

AWS 會在安裝程序中為每個 Outposts 機架建立本機閘道。Outposts 機架支援單一本機閘道。本機閘道由與 Outposts 機架相關聯的 AWS 帳戶 所擁有。

> **Note**
>
> 若要了解經過本機閘道之流量的執行個體頻寬限制，請參閱《Amazon EC2 使用者指南》中的 Amazon EC2 執行個體網路頻寬。 Amazon EC2

本機閘道具有下列元件：

- 路由表 – 只有本機閘道的擁有者可以建立本機閘道路由表。如需詳細資訊，請參閱the section called “路由表”。
- CoIP 集區 – (選擇性) 您可以使用自己擁有的 IP 地址範圍，在內部部署網路與 VPC 中的執行個體之間進行通訊。如需詳細資訊，請參閱the section called “客戶擁有的 IP 地址”。
- 虛擬介面 VIFs) – 本機閘道 VIFs（虛擬介面） 是 Outposts 機架的邏輯介面元件，可在 Outposts 網路裝置與本機閘道連線的內部部署網路裝置之間設定 VLAN、IP 和 BGP 連線。 會為每個 LAG AWS

建立一個 VIF，並將兩個 VIFs 新增至 VIF 群組。本機閘道路由表必須具有一個連到兩個 VIF 的預設路由，才能進行本機網路連線。如需詳細資訊，請參閱本機網路連線。

- VIF 群組 – 將其建立VIFs AWS 新增至 VIF 群組。VIF 群組是 VIF 的邏輯分組。
- 本機閘道路由表和 VPC 關聯 – 本機閘道路由表和 VPC 關聯可讓您將 VPCs連線至本機閘道路由表。使用此關聯，您可以新增目標為 Outposts 子網路路由表中本機閘道的路由。這可讓您透過本機閘道在 Outposts 子網路資源與內部部署網路之間進行通訊。
- 本機閘道路由網域 – 本機閘道路由網域是本機閘道路由表和本機閘道 VIF 群組的關聯。使用此關聯，您可以新增目標為本機閘道路由表中本機閘道 VIF 群組的路由。這可讓您透過選取的 VIF 群組，在 Outposts 子網路資源與內部部署網路之間進行通訊。

當 AWS 佈建您的 Outposts 機架時，我們會建立一些元件，而您需負責建立其他元件。

AWS 責任

- 提供硬體。
- 建立本機閘道。
- 建立虛擬介面 (VIF) 和 VIF 群組。

您的責任

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

本機閘道路由

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

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

如需詳細資訊，請參閱the section called “路由表”。

透過本機閘道的連線

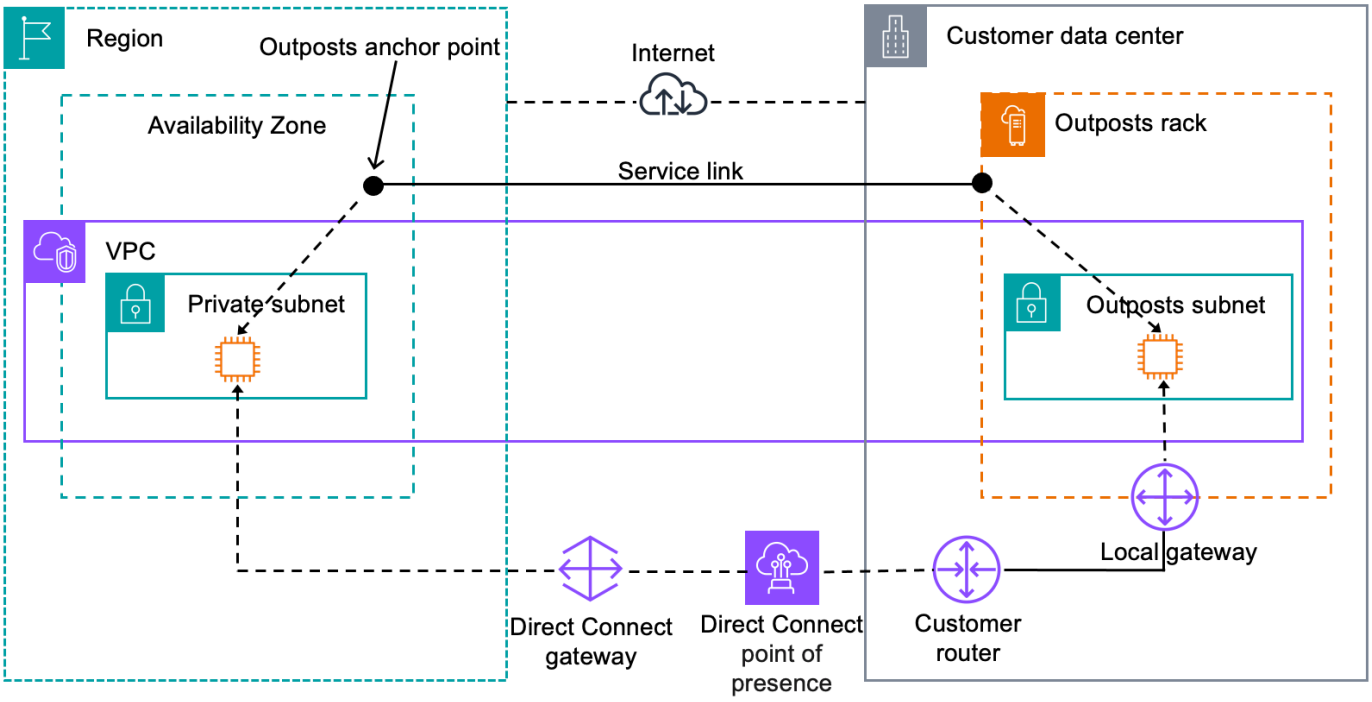
本機閘道的主要角色是提供從 Outpost 到本機內部部署網路的連線。其也可讓您透過內部部署網路連線到網際網路。如需範例，請參閱 the section called “直接 VPC 路由” 和 the section called “客戶擁有的 IP 地址”。

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

您可以將內部部署 Outposts 基礎設施私下連接到 AWS 服務 區域中的 Direct Connect。如需詳細資訊，請參閱《AWS Outposts 私有連線》。

> **IPv6 支援**
>
> 本機閘道僅支援 IPv4 流量。它不支援 IPv6。

下圖顯示如何透過本機閘道進行連線：



本機閘道路由表

在機架安裝過程中， 會 AWS 建立本機閘道、設定 VIFs和 VIF 群組。本機閘道由與 Outpost 相關聯的 AWS 帳戶所擁有。您可以建立本機閘道路由表。本機閘道路由表必須與 VIF 群組和 VPC 有關聯。您可以建立和管理 VIF 群組和 VPC 的關聯。只有本機閘道的擁有者可以修改本機閘道路由表。

Outpost 子網路路由表可以包含本機閘道 VIF 群組的路由，以提供與內部部署網路的連線。

本機閘道路由表的模式決定 Outposts 子網路中的執行個體如何與您的內部部署網路通訊。預設選項是直接 VPC 路由，它使用執行個體的私有 IP 地址。另一個選項是使用您提供的客戶擁有 IP 地址集區 (CoIP) 中的地址。直接 VPC 路由和 CoIP 是互斥選項，可控制路由的運作方式。若要判斷 Outpost 的最佳選項，請參閱如何在 AWS Outposts 機架上選擇 CoIP 和 Direct VPC 路由模式。

您可以使用 與其他 AWS 帳戶或組織單位共用本機閘道路由表 AWS Resource Access Manager。如需詳細資訊，請參閱使用共用 AWS Outposts 資源。

目錄

- 直接 VPC 路由
- 客戶擁有的 IP 地址
- 自訂路由表

直接 VPC 路由

直接 VPC 路由會使用 VPC 中執行個體的私有 IP 地址與您的內部部署網路進行通訊。這些地址會透過 BGP 公告到您的內部部署網路。BGP 的公告僅適用於屬於 Outposts 機架上子網路的私有 IP 地址。這種類型的路由是 Outpost 的預設模式。在此模式下，本機閘道不會針對執行個體執行 NAT，而且您不需要將彈性 IP 地址指派給 EC2 執行個體。您可以選擇使用自己的地址空間，而不是使用直接 VPC 路由模式。如需詳細資訊，請參閱客戶擁有的 IP 地址。

直接 VPC 路由模式不支援重疊的 CIDR 範圍。

直接 VPC 路由僅支援執行個體網路介面。透過代表您 AWS 建立的網路介面 （稱為申請者受管網路介面），無法從您的內部部署網路存取其私有 IP 地址。例如，無法從您的內部部署網路直接連線到 VPC 端點。

下列範例說明直接 VPC 路由。

範例

- 範例：透過 VPC 進行網際網路連線

- 範例：透過內部部署網路進行網際網路連線

範例：透過 VPC 進行網際網路連線

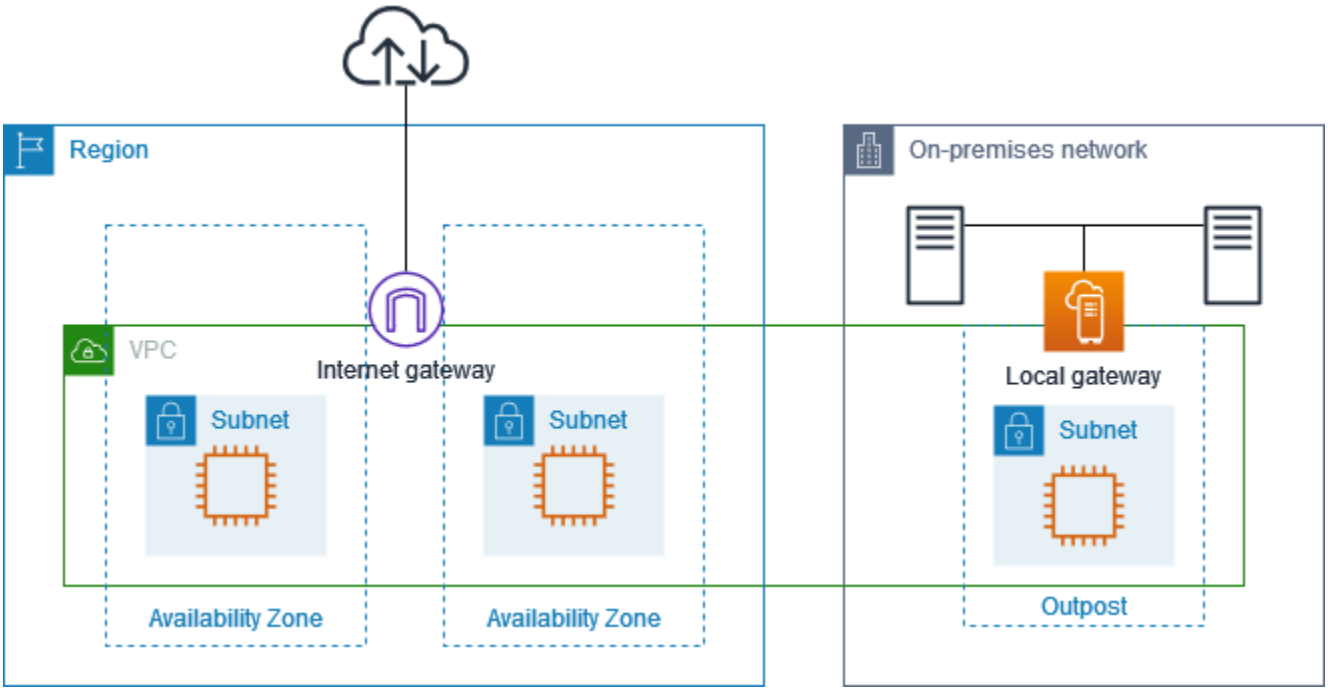
Outpost 子網路中的執行個體可以透過連接至 VPC 的網際網路閘道存取網際網路。

請考慮下列組態：

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

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

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



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

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

範例：透過內部部署網路進行網際網路連線

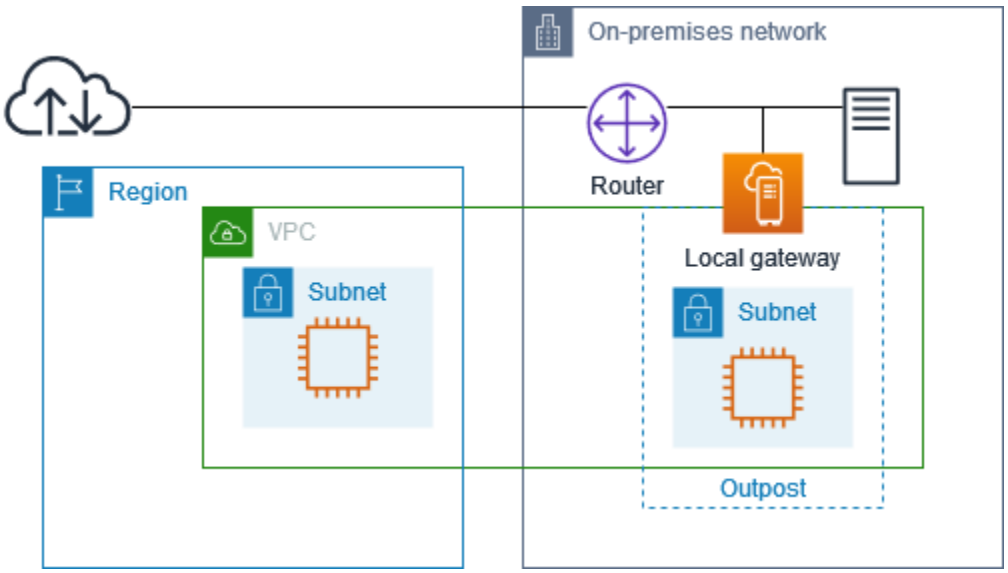
Outpost 子網路中的執行個體可以透過內部部署網路存取網際網路。Outpost 子網路中的執行個體不需要公有 IP 地址或彈性 IP 地址。

請考慮下列組態：

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

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

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



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

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

對網際網路的傳出存取

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

對內部部署網路的傳出存取

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

來自內部部署網路的傳入存取

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

客戶擁有的 IP 地址

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

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

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

> **Note**
>
> 對於客戶擁有的 IP 地址集區，您必須能夠路由網路中的地址。

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

您可以選擇使用 與組織中 AWS 帳戶 的多個 共用客戶擁有的集區 AWS Resource Access Manager。共用集區之後，參與者就可以從客戶擁有的 IP 地址集區配置彈性 IP 地址，然後將其指派給 Outpost 上的 EC2 執行個體。如需詳細資訊，請參閱共用 資源。

範例

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

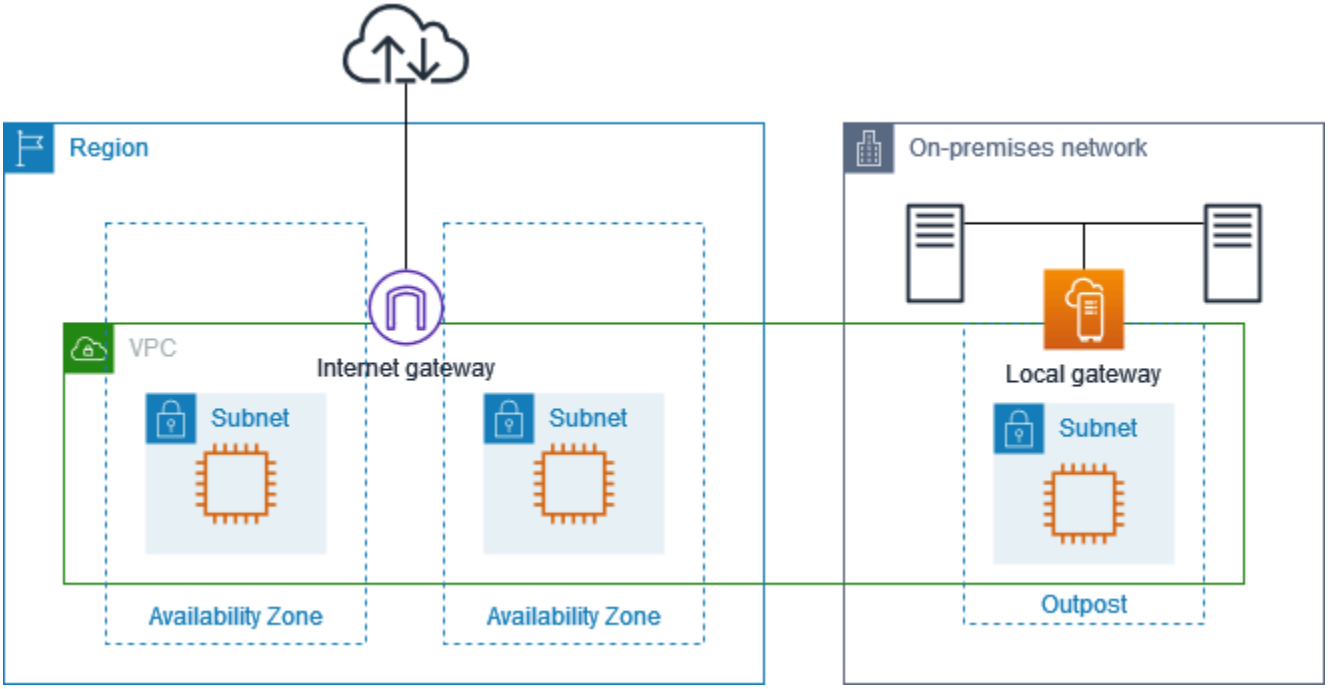
範例：透過 VPC 進行網際網路連線

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

請考慮下列組態：

- 父 VPC 跨越兩個可用區域，每個可用區域都有一個子網路。
- Outpost 有一個子網路。
- 每個子網路都有一個 EC2 執行個體。

- 有一個客戶擁有的 IP 地址集區。
- Outpost 子網路中的執行個體具有來自客戶擁有 IP 地址集區的彈性 IP 地址。
- 本機閘道會使用 BGP 公告，將客戶擁有的 IP 地址集區公告到內部部署網路。



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

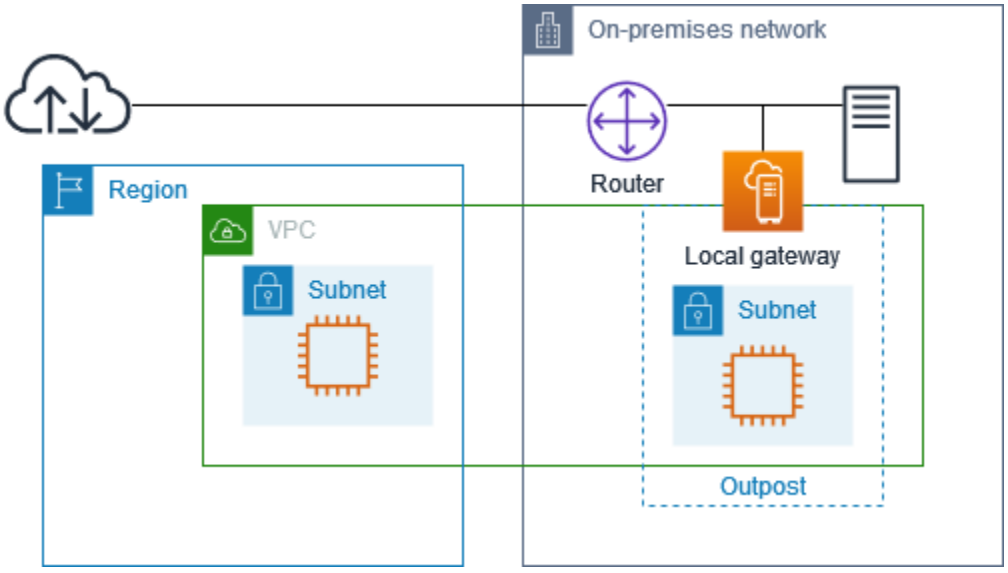
目標	Target	說明
VPC CIDR	區域	提供 VPC 中子網路之間的連線。
0.0.0.0	*internet-gateway-id*	將目的地為公有網際網路的流量傳送至網際網路閘道。
###### CIDR	*local-gateway-id*	將目的地為內部部署網路的流量傳送至本機閘道。

範例：透過內部部署網路進行網際網路連線

Outpost 子網路中的執行個體可以透過內部部署網路存取網際網路。

請考慮下列組態：

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



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

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

對網際網路的傳出存取

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

對內部部署網路的傳出存取

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

來自內部部署網路的傳入存取

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

自訂路由表

您可以為本機閘道建立自訂路由表。本機閘道路由表必須具有與 VIF 群組和 VPC 的關聯。如需step-by-step說明，請參閱設定本機閘道連線。

本機閘道路由表路由

您可以在 Outpost 上建立本機閘道路由表和網路介面的傳入路由。您也可以修改現有的本機閘道傳入路由，以變更目標網路介面。

只有當路由的目標網路介面連接到執行中的執行個體時，路由才會處於作用中狀態。如果執行個體停止或介面分離，路由狀態會從作用中變更為黑洞。

目錄

- 要求與限制
- 建立自訂本機閘道路由表
- 切換本機閘道路由表模式或刪除本機閘道路由表

要求與限制

適用下列要求和限制：

- 目標網路界面必須屬於 Outpost 上的子網路，且必須連接至該 Outpost 中的執行個體。本機閘道路由無法以不同 Outpost 或父系中的 Amazon EC2 執行個體為目標 AWS 區域。

- 子網路必須屬於與本機閘道路由表相關聯的 VPC。
- 相同路由表中的網路介面路由不得超過 100 個。
- AWS 優先考慮最具體的路由，如果路由相符，我們會優先考慮靜態路由而不是傳播的路由。
- 不支援介面 VPC 端點。
- BGP 公告僅適用於 Outpost 上具有路由表中以本機閘道為目標之路由的子網路。如果子網路在路由表中沒有以本機閘道為目標的路由，則不會透過 BGP 公告這些子網路。
- 只有連接至 Outpost 執行個體的網路介面可以透過該 Outpost 的本機閘道進行通訊。屬於 Outpost 子網路但連接至 區域中執行個體的網路介面無法透過該 Outpost 的本機閘道進行通訊。
- 無法透過本機閘道從內部部署網路到達請求者受管界面，例如為 VPC 端點建立的界面。它們只能從 Outpost 子網路中的執行個體進行連接。

適用下列 NAT 考量：

- 本機閘道不會對符合網路介面路由的流量執行 NAT。而是會保留目的地 IP 地址。
- 關閉目標網路界面的來源/目的地檢查。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的網路界面概念。
- 將作業系統設定為允許在網路介面上接受來自目的地 CIDR 的流量。

建立自訂本機閘道路由表

您可以使用 AWS Outposts 主控台建立本機閘道的自訂路由表。

使用主控台建立自訂本機閘道路由表

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

   編輯本機閘道路由表，以新增具有 VIF 群組做為目標的靜態路由。
8. 針對 模式，選擇與您內部部署網路通訊的模式。

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

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

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

9. (選用) 新增或移除標籤。

   [新增標籤] 選擇新增標籤，並執行下列動作：

   - 對於 Key (金鑰)，輸入金鑰名稱。
   - 在值欄位中，輸入金鑰值。

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

切換本機閘道路由表模式或刪除本機閘道路由表

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

切換模式或刪除本機閘道路由表

1. 在 https：//https://console.aws.amazon.com/outposts/ 開啟 AWS Outposts 主控台。
2. 確認您位於正確位置 AWS 區域。

   若要變更區域，請使用頁面右上角的區域選擇器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 驗證本機閘道路由表是否與 VIF 群組相關聯。如果關聯，您必須移除本機閘道路由表與 VIF 群組之間的關聯。

   a. 選擇本機閘道路由表的 ID。

b. 選擇 VIF 群組關聯索引標籤。
c. 如果一或多個 VIF 群組與本機閘道路由表相關聯，請選擇編輯 VIF 群組關聯。
d. 清除關聯 VIF 群組核取方塊。
e. 選擇儲存變更。

5. 選擇刪除本機閘道路由表。
6. 在確認對話方塊中輸入 **delete**，然後選擇 刪除。
7. (選擇性) 使用新模式建立本機閘道路由表。

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

建立 CoIP 集區

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

客戶擁有的 IP 集區適用於 CoIP 模式的本機閘道路由表。

使用下列程序建立 CoIP 集區。

Console

使用主控台建立 CoIP 集區

1. 在 https：//https://console.aws.amazon.com/outposts/ 開啟 AWS Outposts 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 在導覽窗格中，選擇 本機閘道路由表。
4. 選擇路由表。
5. 在詳細資訊窗格中選擇 CoIP 集區 標籤，然後選擇 建立 CoIP 集區。
6. (選擇性) 針對 名稱，輸入您的 CoIP 集區名稱。
7. 選擇 新增 CIDR，然後輸入客戶擁有的 IP 地址範圍。
8. （選用）若要新增 CIDR 區塊，請選擇新增 CIDR，然後輸入客戶擁有的 IP 地址範圍。
9. 選擇 建立 CoIP 集區。

AWS CLI

使用 建立 CoIP 集區 AWS CLI

1. 使用 create-coip-pool 命令，為指定的本機閘道路由表建立 CoIP 地址集區。

```
aws ec2 create-coip-pool --local-gateway-route-table-id lgw-rtb-
abcdefg1234567890
```

以下為範例輸出。

```
{
    "CoipPool": {
        "PoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890",
        "PoolArn": "arn:aws:ec2:us-west-2:123456789012:coip-pool/ipv4pool-
coip-1234567890abcdefg"
    }
}
```

2. 使用 create-coip-cidr 命令，在指定的 CoIP 集區中建立 CoIP 地址範圍。

```
aws ec2 create-coip-cidr --cidr 15.0.0.0/24 --coip-pool-id ipv4pool-
coip-1234567890abcdefg
```

以下為範例輸出。

```
{
    "CoipCidr": {
        "Cidr": "15.0.0.0/24",
        "CoipPoolId": "ipv4pool-coip-1234567890abcdefg",
        "LocalGatewayRouteTableId": "lgw-rtb-abcdefg1234567890"
    }
}
```

建立 CoIP 集區之後，請使用下列程序將地址指派給執行個體。

Console

使用主控台將 CoIP 地址指派給執行個體

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

AWS CLI

使用 將 CoIP 地址指派給執行個體 AWS CLI

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

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

以下為範例輸出。

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

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

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

以下為範例輸出。

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

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

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

以下為範例輸出。

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

監控本機閘道連線

您可以從 AWS Outposts 主控台監控本機閘道虛擬介面的連線狀態和 BGP 工作階段狀態。在 主控台中，導覽至您的 Outpost，然後選擇本機閘道虛擬介面索引標籤。網路狀態欄會顯示每個 VIF 是否啟動並準備好轉送流量。選擇狀態連結以開啟預先建置的 Amazon CloudWatch 圖表，其中顯示該 VIF `VifBgpSessionState` 的 `VifConnectionStatus`和 。這些指標會自動發佈到所有 Outpost VIFs的`AWS/Outposts`命名空間，不需要額外的設定。若要在 VIF 故障或 BGP 工作階段不再處於 `Established` 狀態時接收主動通知，您可以選擇在任一指標上建立 CloudWatch 警示。如需指標值和維度的說明，請參閱 Outposts 機架 CloudWatch 指標。

> **Note**
>
> 如果您直接根據 或 `VifBgpSessionState`指標建置儀表板`VifConnectionStatus`或警示，請注意維度名稱會根據您使用的 CloudWatch Widget 而有所不同：更新的 Widget 使用 `OutpostId`，而舊版 Widget 仍會使用 `OutpostsId`來回溯相容性。確認儀表板或警示定義預期要避免遺失資料的維度名稱。如需詳細資訊，請參閱指標。

Outposts 機架的本機網路連線

您需要下列元件，才能將 Outposts 機架連線至您的內部部署網路：

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

目錄

- 實體連線
- 連結彙總
- 虛擬 LAN
- 網路層連線
- ACE 機架連線
- 服務連結 BGP 連線
- 服務連結基礎設施子網路公告和 IP 範圍
- 本機閘道 BGP 連線
- 本機閘道客戶擁有的 IP 子網路公告

實體連線

Outposts 機架有兩個連接到您本機網路的實體網路裝置。

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

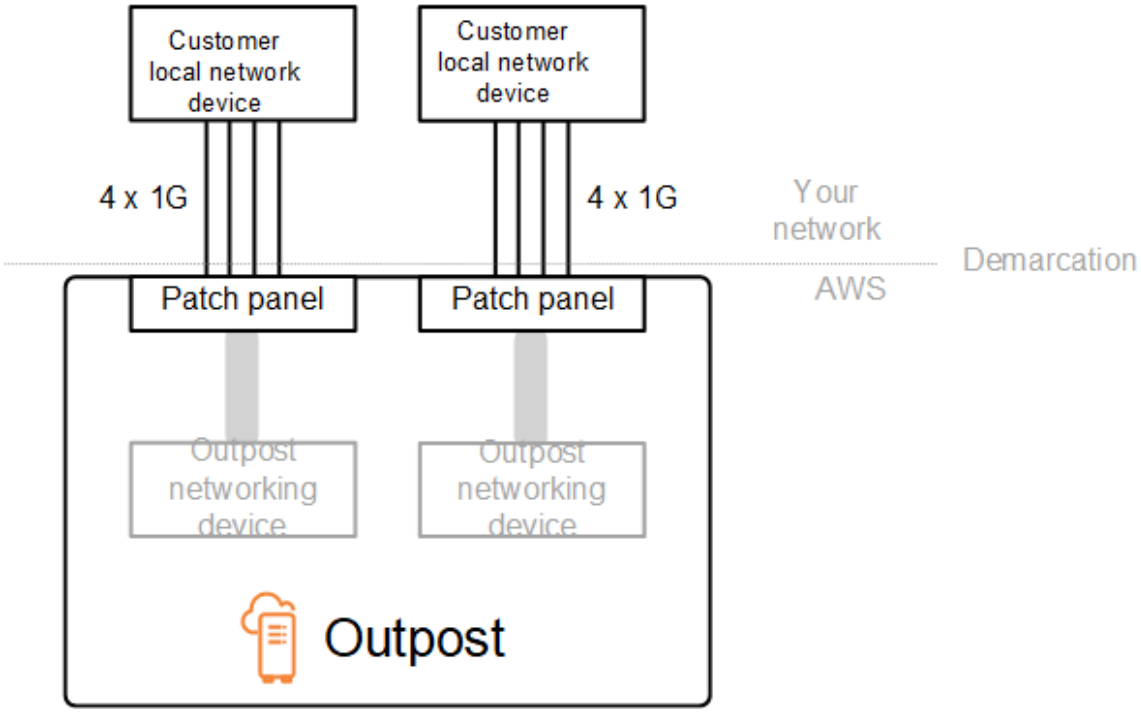
上行鏈路速度	上行鏈路數目
1 Gbps	1、2、4、6 或 8

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

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

Outposts 機架可以支援單模光纖 (SMF) 搭配 Lucent Connector (LC)、多模光纖 (MMF) 或 MMF OM4 搭配 LC。 AWS提供與您在機架位置提供的光纖相容的光纖。

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



連結彙總

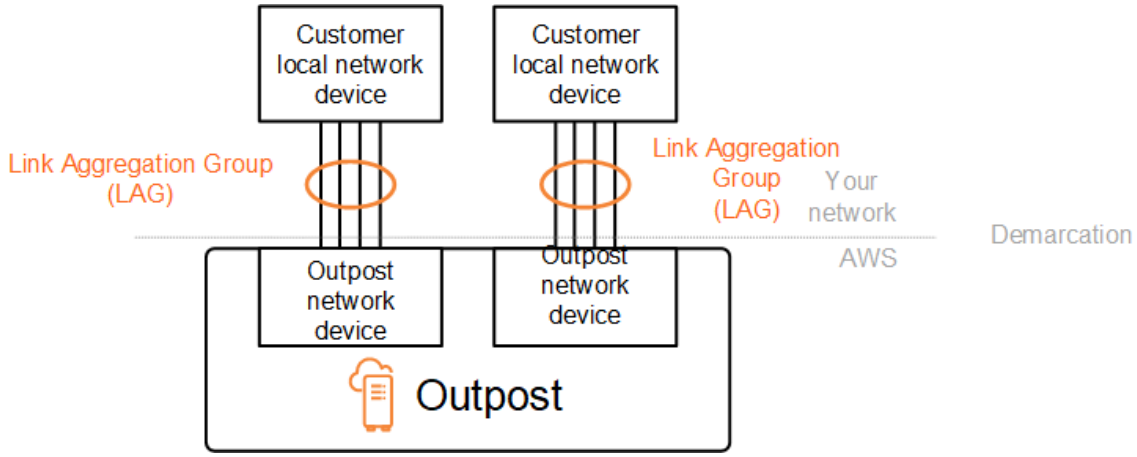
AWS Outposts使用連結彙總控制通訊協定 (LACP) 在 Outpost 網路裝置和本機網路裝置之間建立連結彙總群組 (LAG) 連線。來自每部 Outpost 網路裝置的連結會彙總為乙太網路 LAG，以代表單一網路連線。這些 LAG 使用 LACP 搭配標準快速計時器。您無法將 LAG 設定為使用慢速計時器。

若要在站點安裝 Outpost，您必須在網路裝置上設定 LAG 連線端。

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

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

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



虛擬 LAN

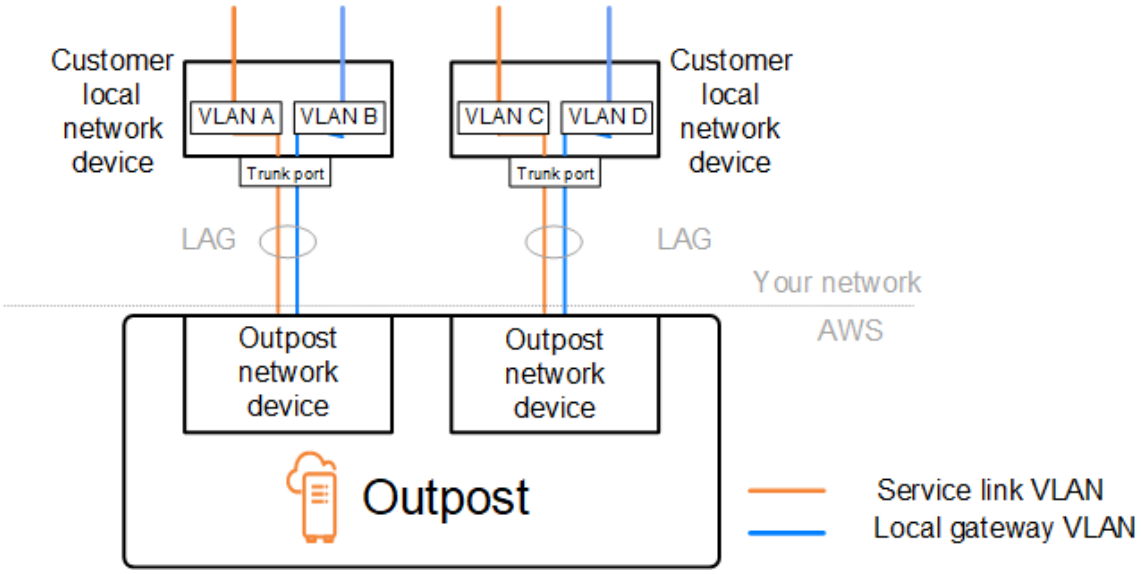
Outpost 網路裝置與本機網路裝置之間的每個 LAG 都必須設定為 IEEE 802.1q 乙太網路主幹。這可讓您使用多個 VLAN 來隔離資料路徑之間的網路。

每個 Outpost 都有下列 VLAN，可與您的本機網路裝置通訊：

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

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

Outpost 旨在將服務連結與本機閘道資料路徑分隔為兩個隔離的網路。這可讓您選擇哪些網路能夠與 Outpost 上執行的服務通訊。其也可讓您透過使用客戶本機網路裝置上的多個路由表 (通常稱為虛擬路由和轉送執行個體 (VRF))，將服務連結設為與本機閘道網路隔離的網路。分界線存在於 Outpost 網路裝置的連接埠。 會AWS管理連線端的任何基礎設施AWS，而您會管理線路端的任何基礎設施。



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

網路層連線

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

我們建議下列作法：

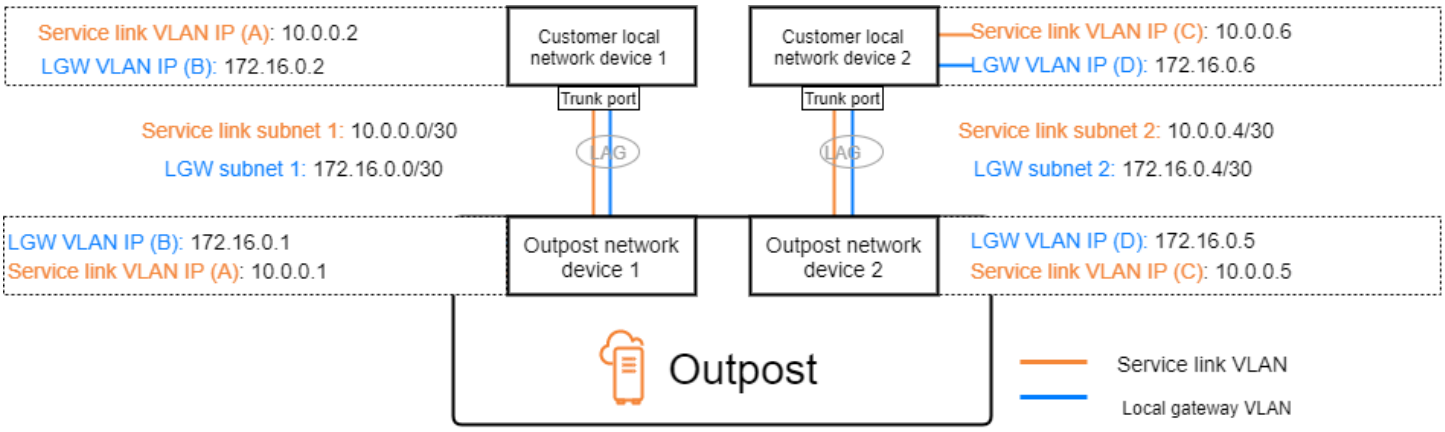
- 使用具有 /30 或 /31 CIDR 的專用子網路來代表此邏輯點對點連線。
- 請勿橋接本機網路裝置之間的 VLAN。

對於網路層連線，您必須建立兩個路徑：

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

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

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



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

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

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

VLAN	子網路	客戶裝置 2 IP	AWSOND 2 IP
C	10.0.0.4/30	10.0.0.6	10.0.0.5
D	172.16.0.4/30	172.16.0.6	172.16.0.5

ACE 機架連線

> **Note**
>
> 如果您不需要 ACE 機架，請略過本節。

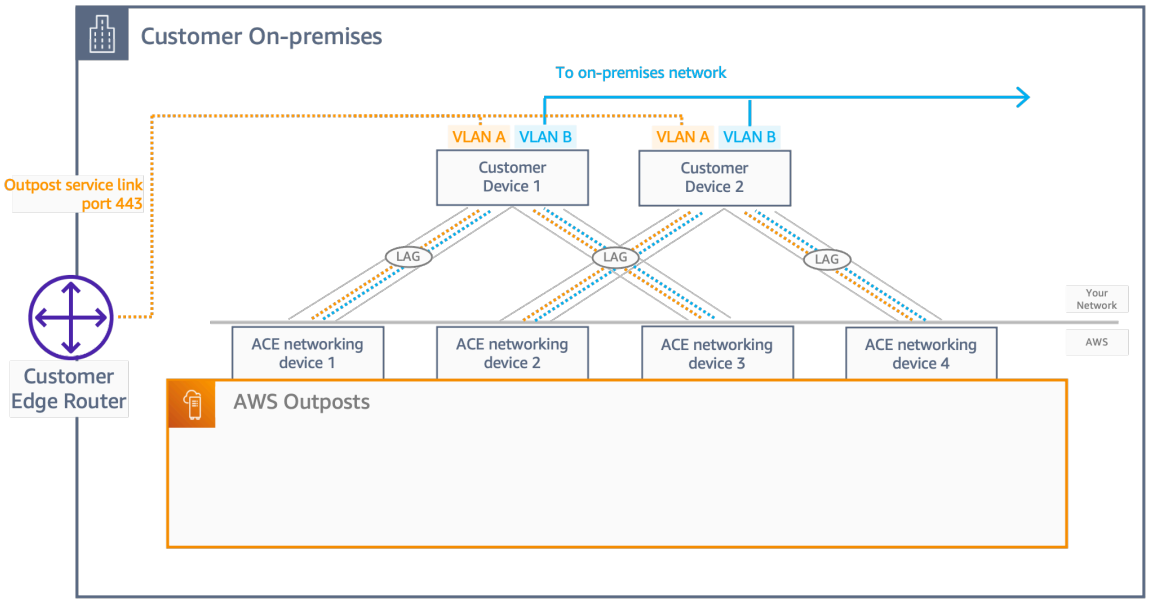
彙總、核心、邊緣 (ACE) 機架可做為多機架 Outpost 部署的網路彙總點。如果您有四個或更多運算機架，則必須使用 ACE 機架。如果您有少於四個運算機架，但計劃在未來擴展到四個或多個機架，我們建議您儘早安裝 ACE 機架。

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

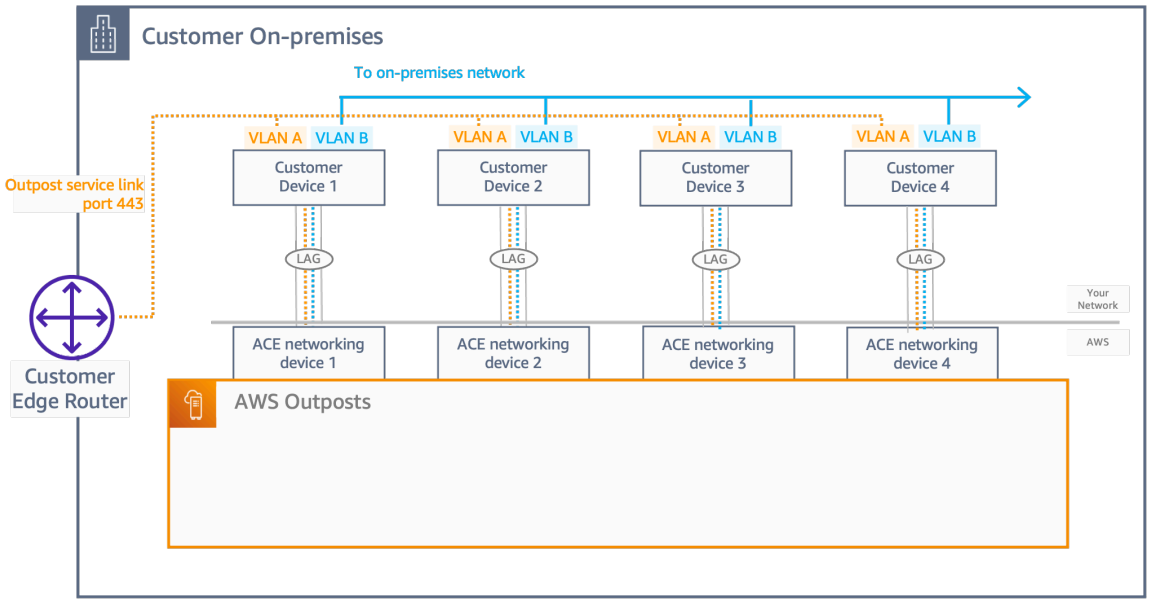
ACE 機架包含四個聯網裝置，可以連接到客戶內部部署網路中的兩個上游客戶裝置，或四個上游客戶裝置，以實現最大的彈性。

下圖顯示兩種聯網拓撲。

下圖顯示連接到兩個上游客戶裝置的 ACE 機架的四個 ACE 網路裝置：



下圖顯示連接到四個上游客戶裝置的 ACE 機架的四個 ACE 網路裝置：

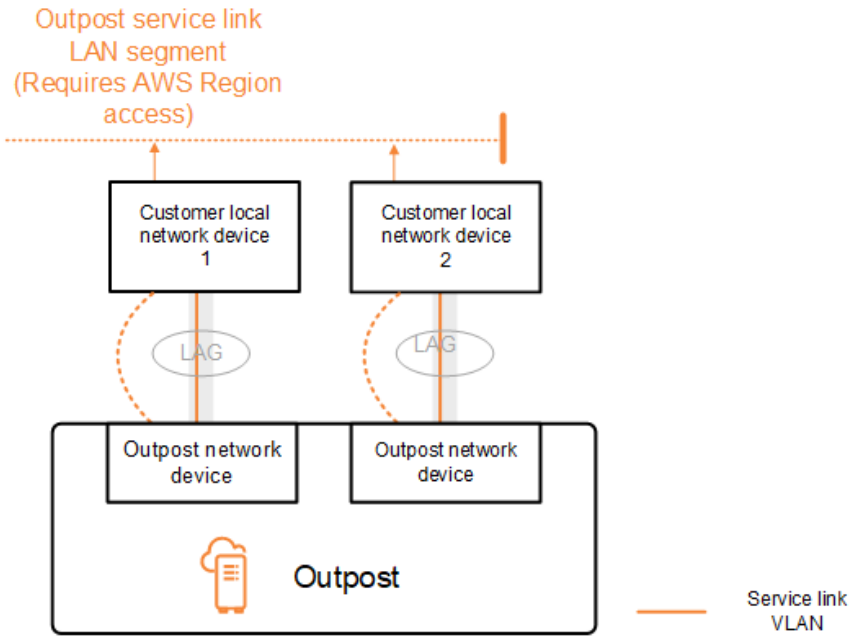


服務連結 BGP 連線

Outpost 會在每部 Outpost 網路裝置與客戶本機網路裝置之間建立外部 BGP 對等互連工作階段，以透過服務連結 VLAN 進行服務連結連線。BGP 對等互連工作階段會在為點對點 VLAN 提供的 /30 或 /31 IP 地址之間建立。每個 BGP 對等工作階段都會在 Outpost 網路裝置上使用私有自治系統編號 (ASN)，以及您為客戶本機網路裝置選擇的 ASN。在安裝過程中， 會AWS設定您提供的屬性。

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

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



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

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

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

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

服務連結基礎設施子網路公告和 IP 範圍

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

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

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

如果您有多個機架部署，則每個機架必須有一個 /26 子網路。

本機閘道 BGP 連線

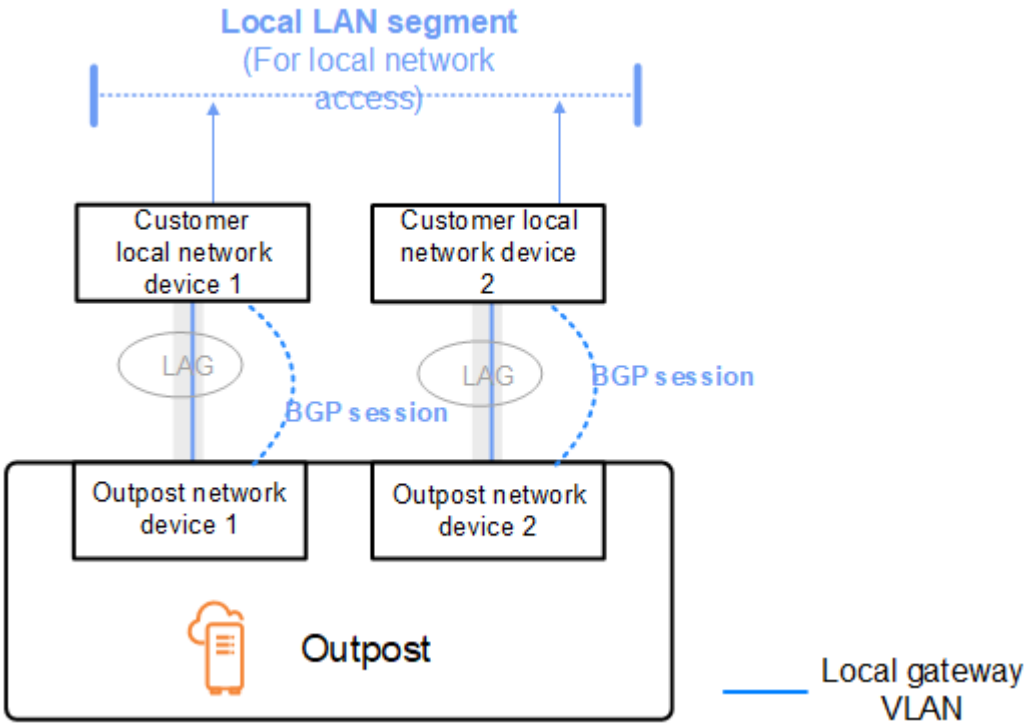
Outpost 會使用您指派的私有自治系統編號 (ASN) 來建立外部 BGP 工作階段。每部 Outpost 網路裝置都有單一外部 BGP 對等互連，使用其本機閘道 VLAN 連至一部本機網路裝置。

Outpost 會在每部 Outpost 網路裝置與其連線的客戶本機網路裝置之間，透過本機閘道 VLAN 建立外部 BGP 對等互連工作階段。此對等互連工作階段會在您設定網路連線時所提供的 /30 或 /31 IP 之間建立，並在 Outpost 網路裝置與客戶本機網路裝置之間使用點對點連線。如需詳細資訊，請參閱the section called “網路層連線”。

每個 BGP 工作階段在 Outpost 網路裝置端使用私有 ASN，並在客戶本機網路裝置端使用您選擇的 ASN。 會在預先安裝程序中AWS設定屬性。

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

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



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

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

本機閘道客戶擁有的 IP 子網路公告

根據預設，本機閘道會使用 VPC 中執行個體的私有 IP 地址（請參閱直接 VPC 路由），以促進與內部部署網路的通訊。不過，您可以提供客戶擁有的 IP 地址集區 (CoIP)。

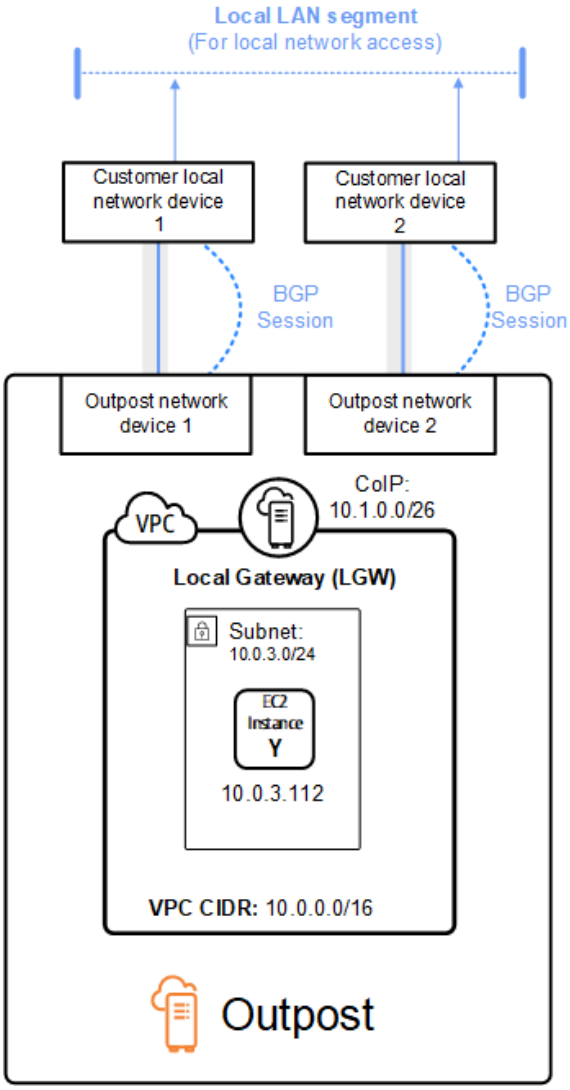
您可以從此集區建立彈性 IP 地址，然後將地址指派給 Outpost 上的資源 (例如 EC2 執行個體)。

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

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

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

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


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

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：//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 內每個資產上的執行個體視覺化，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。
- 您可以使用 主控台中的步驟或上傳 JSON 容量組態計劃來修改容量。使用主控台步驟以互動方式設定單一 Outpost 或資產。使用 JSON 檔案將相同的容量組態套用至多個 Outposts、重複使用組態，而無需直接呼叫 StartCapacityTask API 或每次都透過主控台工作流程，或從失敗的容量任務重新提交輸入。
- 定義 Outpost 的容量時，所有執行個體系列和類型都會包含在重新設定中，除非它們被列為要避免的執行個體。
- 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。
- 如果您想要在 Outpost 上完全重新設定執行個體系列，而不保留原始容量組態中的任何執行個體大小，您必須先停止 Outpost 上該系列的任何執行中執行個體，再執行容量任務。如果執行個體由另一個 帳戶擁有，或由 Outpost 上執行的分層服務使用，您必須使用執行個體擁有者帳戶來停止執行個體或服務執行個體。

- 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：//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：
   - 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. 選擇上傳容量組態計劃。
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：//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：//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. 使用上傳容量組態計劃選項，上傳具有相同執行個體類型清單的 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：//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：//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：//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。

這些是 Outposts 機架可用的資源。

- 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。
- 容量保留 – 具有此資源存取權的取用者可以：
  - 識別與其共用的容量保留。
  - 啟動並管理使用容量保留的執行個體。
- 客戶擁有的 IP 地址 (CoIP) 集區 – 具有此資源存取權的取用者可以：
  - 配置客戶擁有的 IP 地址，並將其與執行個體建立關聯。
- 本機閘道路由表 – 具有此資源存取權的取用者可以：
  - 建立和管理本機閘道的 VPC 關聯。
  - 檢視本機閘道路由表和虛擬介面的組態。
  - 建立目標為本機閘道的 VPC 子網路路由。
- 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。
  - 在 Outpost 上建立和管理 EBS 磁碟區。
  - 使用 AWS Outposts API 來檢視 Outpost 的相關資訊。
- S3 on Outpost – 具有此資源存取權的取用者可以：
  - 在 Outpost 上建立和管理 S3 儲存貯體、存取點和端點。
- 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：//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閘道路由表，也請使用下列程序。

使用 AWS RAM 主控台共用您擁有的 Outpost 或本機閘道路由表

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 或本機閘道路由表 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：//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 機架的第三方區塊儲存

使用 Outposts 機架，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 StorageFlashArray 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。
- 適用於支援第一代 Outpost 機架的所有 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，Outposts 機架需要 EBS 或執行個體儲存體。

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

- AWS 技術人員會設定本機閘道，以確保 Outpost 子網路與本機網路之間的連線。
- 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，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。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 也為您提供可安全使用的服務。作為AWS 合規計畫的一部分，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劃 AWS Outposts，請參閱AWS 合規計劃的 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 機架常見問答集。

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
- AWS Outposts 工作負載的網際網路存取

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。

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 機架的資料。

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

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。

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

資料刪除

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

銷毀 Nitro 安全金鑰會以密碼編譯方式銷毀 Outpost 上的資料。

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

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，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。

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，並結合 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 Outpost 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 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 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 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 受管政策並轉向最低權限許可 – 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:DescribeSubnets`上
- 動作：在所有 AWS 資源`ec2:DescribeVpcEndpoints`上
- 動作：在下列 AWS 資源`ec2:CreateNetworkInterface`上：

```
"arn:*:ec2:*:*:vpc/*",
"arn:*:ec2:*:*:subnet/*",
"arn:*:ec2:*:*:security-group/*"
```

- 動作：在符合下列條件 AWS `"arn:*:ec2:*:*:network-interface/*"`的資源`ec2:CreateNetworkInterface`上：

```
"ForAnyValue:StringEquals" : { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

- 動作：在下列 AWS 資源ec2:CreateSecurityGroup上：

```
"arn:*:ec2:*:*:vpc/*"
```

- 動作：在符合下列條件 AWS "arn:*:ec2:*:*:security-group/*"的資源ec2:CreateSecurityGroup上：

```
"ForAnyValue:StringEquals": { "aws:TagKeys": [ "outposts:private-
connectivity-resourceId" ] }
```

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}}*"}},
"StringEquals": {"ec2:CreateAction" : ["CreateSecurityGroup",
 "CreateNetworkInterface"]}
```

- 動作：在符合下列條件的所有 AWS 資源ec2:RevokeSecurityGroupIngress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:RevokeSecurityGroupEgress`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:DeleteNetworkInterface`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:DeleteSecurityGroup`上：

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

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。

如需詳細資訊，請參閱服務連結私有連線選項。

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 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 Outposts 機架的FAQs。

AWS AWS Outposts 的 受管政策

AWS 受管政策是由 AWS 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 AWS 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 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	日期
AWS Identity and Access Management 服務連結角色 AWSServiceRoleForOutposts_*OutpostID* 的更新	AWSServiceRoleForOutposts_*OutpostID* 服務連結角色許可已更新，以精簡 如何 AWS Outposts 管理私有連線的網路資源，並更精確地控制服務連結端點執行個體所需的網路界面和安全群組操作。	2025 年 4 月 18 日
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 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，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 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 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。

AWS Outposts 設備上的竄改監控

確保沒有人修改、更改、反向工程或竄改 AWS Outposts equipment. AWS Outposts equipment 可能配備竄改監控，以確保符合 AWS 服務條款。

中的彈性 AWS Outposts

AWS Outposts 專為高度可用性而設計。Outposts 機架的設計採用備援電源和聯網設備。為了提高恢復能力，建議您為 Outpost 提供雙電源和備援網路連線。

為了獲得高可用性，您可以在 Outpost 機架上佈建額外的內建且永遠處於作用中的容量。Outpost 容量組態是專為在生產環境中運作所設計，當您佈建容量時，可支援每個執行個體系列 N+1 個執行個體。AWS 建議您為任務關鍵型應用程式配置足夠的額外容量，以便在發生基礎主機問題時進行復原和容錯移轉。您可以使用 Amazon CloudWatch 容量可用性指標並設定警示來監控應用程式的運作狀態、建立 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，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 及更新 Outpost。若要利用可用區域提供的恢復能力，您可以在多個 Outpost 上部署應用程式，並將每個應用程式連接至不同的可用區域。這可讓您提高應用程式恢復能力，避免依賴單一可用區域。如需區域與可用區域的詳細資訊，請參閱《AWS 全球基礎設施》。

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

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

的合規驗證 AWS Outposts

我們的新 AWS 註冊體驗並非針對受管制的工作負載而設計。如果您正在使用我們新的 AWS 註冊體驗，但想要將 AWS 用於受管制的工作負載，您可以註冊 AWS （進階） 或為您的 AWS 環境啟用進階功能。

若要了解 是否 AWS 服務 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。

AWS Outposts 工作負載的網際網路存取

本節說明 AWS Outposts 工作負載如何以下列方式存取網際網路：

- 透過父 AWS 區域
- 透過本機資料中心的網路

透過父 AWS 區域存取網際網路

在此選項中，Outposts 中的工作負載會透過服務連結存取網際網路，然後透過父 AWS 區域中的網際網路閘道 (IGW) 存取網際網路。網際網路的傳出流量可以透過 VPC 中執行個體化的 NAT 閘道。為了提高輸入和輸出流量的安全性，您可以在 AWS 區域中使用 AWS 安全服務 AWS WAF，例如 AWS Shield和 Amazon CloudFront。

如需 Outposts 子網路上的路由表設定，請參閱本機閘道路由表。

考量事項

- 在下列情況下使用此選項：
  - 您需要在 AWS 區域中使用多個 AWS 服務來保護網際網路流量的彈性。
  - 您的資料中心或主機代管設施中沒有網際網路點。
- 在此選項中，流量必須周遊父 AWS 區域，這會引入延遲。
- 與 AWS 區域中的資料傳輸費用類似，從父可用區域到 Outpost 的資料傳輸會產生費用。若要進一步了解資料傳輸，請參閱 Amazon EC2 隨需定價。
- 服務連結頻寬的使用率將會增加。

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

透過本機資料中心的網路進行網際網路存取

在此選項中，位於 Outposts 中的工作負載會透過本機資料中心存取網際網路。存取網際網路的工作負載流量會透過本機網際網路的存在點周遊，並在本機輸出。本機資料中心網路的安全層負責保護 Outposts 工作負載流量。

如需 Outposts 子網路上的路由表設定，請參閱本機閘道路由表。

考量事項

- 在下列情況下使用此選項：
  - 您的工作負載需要低延遲存取網際網路服務。

  - 您偏好避免產生資料傳輸 (DTO) 費用。
  - 您想要保留控制平面流量的服務連結頻寬。
- 您的安全層負責保護 Outposts 工作負載流量。
- 如果您選擇直接 VPC 路由 (DVR)，則必須確保 Outposts CIDRs不會與內部部署 CIDRs衝突。
- 如果預設路由 (0/0) 透過本機閘道 (LGW) 傳播，則執行個體可能無法存取服務端點。或者，您可以選擇 VPC 端點來到達所需的服務。

下圖顯示 Outposts 執行個體中的工作負載與網際網路之間經過您本機資料中心的流量。

監控您的 Outposts 機架

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 rack 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 機架 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 機架複製並轉送到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 機架 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 機架 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
- Amazon EBS 指標
- 虛擬介面指標
- LAG 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	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)。
InstanceFamilyCapacityUtilization	Account、InstanceFamily 與 OutpostId	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)。
InstanceTypeCapacityAvailability	InstanceType 和 OutpostId	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

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	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)。
UsedInstanceType_Count	Account、InstanceType 與 OutpostId	目前使用中的執行個體類型數量，包括 Amazon Relational Database Service (Amazon RDS) 或 Application Load Balancer 等受管服務使用的任何執行個體類型。此指標不包含在 Outpost 上設定之任何專用執行個體的容量。 單位：計數 最長解析時間：5 分鐘

指標	維度	Description
AvailableInstanceType_Count	InstanceType 和 OutpostId	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

指標	維度	Description
AvailableReservedInstances	InstanceType 和 OutpostId	可使用容量保留啟動至預留運算容量的執行個體數量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。 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。 `Number of instances that you can reserve = AvailableInstanceType_Count - AvailableReservedInstances` 單位：計數 最長解析時間：5 分鐘

指標	維度	Description
UsedReservedInstances	InstanceType 和 OutpostId	使用容量預留在運算容量中執行的執行個體數量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
TotalReservedInstances	InstanceType 和 OutpostId	執行中且可供啟動的執行個體總數，由使用容量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。 單位：計數 最長解析時間：5 分鐘

Amazon EBS 指標

下列指標適用於 EBS 磁碟區類型容量。

指標	維度	Description
EBSVolumeTypeCapacityUtilization	VolumeType 和 OutpostId	使用中的 EBS 磁碟區類型容量百分比。 單位：百分比 最長解析時間：5 分鐘

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)。
EBSVolumeTypeCapacityAvailability	VolumeType 和 OutpostId	可用的 EBS 磁碟區類型容量百分比。 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)。
EBSVolumeTypeCapacityUtilizationGB	VolumeType 和 OutpostId	EBS 磁碟區類型的使用中 GB 數。 單位：千兆位元組 (GB) 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)。
EBSVolumeTypeCapacityAvailabilityGB	VolumeType 和 OutpostId	EBS 磁碟區類型的可用容量 GB 數。 單位：千兆位元組 (GB) 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)。

虛擬介面指標

下列指標適用於虛擬界面 (VIF)。

指標	維度	Description
VifBgpSessionState	本機閘道 VIFs 的維度：OutpostId 、LagId、VirtualInterfaceGroupId 、VirtualInterfaceId 。 服務連結 VIFs 的維度：OutpostId 、LagId、VirtualInterfaceGroupId 、VirtualInterfaceId 。服務連結 VIFs VirtualInterfaceGroupId 一律顯示為「-」；CloudWatch 小工具對齊包含。	AWS Outposts 虛擬介面 (VIF) 和內部部署裝置之間的邊界閘道協定 (BGP) 工作階段狀態。 單位：值 1 到 6，其中： • 1 – 閒置。這是 Outposts 機架正在等待啟動事件的初始狀態。 • 2 – 連線。Outposts 機架正在等待 TCP 連線完成。 • 3 – 作用中。Outposts 機架正在嘗試啟動 TCP 連線。 • 4 – OpenSent。路由器已傳送 OPEN 訊息，並正在等待傳回。 • 5 – OpenConfirm。路由器已收到 OPEN 訊息，並正在等待 KEEPALIVE 訊息。 • 6 – 已建立。BGP 連線已完全建立，Outposts 機架和內部部署裝置可以交換路由資訊。 最大解析度：5 分鐘 統計資訊：最實用的統計資訊是 Maximum。
VifConnectionStatus	本機閘道 VIFs 的維度：OutpostId	顯示虛擬介面 (VIFs) 是否已準備好轉送流量。

指標	維度	Description
	、LagId、VirtualInterfaceGroupId 、VirtualInterfaceId 。 服務連結 VIFs 的維度：OutpostId 、LagId、VirtualInterfaceGroupId 、VirtualInterfaceId 。服務連結 VIFs VirtualInterfaceGroupId 一律顯示為「-」；CloudWatch 小工具對齊包含。	單位：1 或 0，其中： • 1 – 表示 Outpost VIF 已成功連接到現場部署裝置、設定好並準備好轉送流量。 • 0 – 表示 Outpost VIF 尚未準備好轉送流量。 最大解析度：5 分鐘 統計資訊：最實用的統計資訊是 Maximum。
IfTrafficIn	本機閘道 VIFs (lgw-vif) 的維度：OutpostId 、VirtualInterfaceGroupId 、 LagId和 VirtualInterfaceId 服務連結 VIFs (sl-vif) 的維度：OutpostId 、VirtualInterfaceGroupId 、 LagId和 VirtualInterfaceId 。服務連結 VIFs VirtualInterfaceGroupId 一律顯示為 "-"；CloudWatch Widget 對齊包含。	Outpost 虛擬介面 (VIF) 從已連線本機網路裝置接收的資料位元速率。 單位：位元/秒 最長解析時間：5 分鐘 統計資訊：最實用的統計資訊是 Max 與 Min。

指標	維度	Description
IfTrafficOut	本機閘道 VIFs (lgw-vif) 的維度：OutpostId 、VirtualInterfaceGroupId 、 LagId和 VirtualInterfaceId 服務連結 VIFs (sl-vif) 的維度：OutpostId 、VirtualInterfaceGroupId 、 LagId和 VirtualInterfaceId 。服務連結 VIFs VirtualInterfaceGroupId 一律顯示為 "-"；CloudWatch Widget 對齊包含。	Outpost 虛擬介面 (VIF) 傳輸至已連線本機網路裝置的資料位元速率。 單位：位元/秒 最長解析時間：5 分鐘 統計資訊：最實用的統計資訊是 Max 與 Min。

維LagId度已新增至 VifBgpSessionState、IfTrafficIn、 VifConnectionStatus和 IfTrafficOut指標。這可讓您將 VIF 層級指標與其對應的 LAG 建立關聯，讓您更輕鬆地識別連線問題是源自 VIF 組態層級還是實體 LAG 層級。新的 CloudWatch 小工具會使用更新的維度名稱 顯示所有指標 （現有的 VIF 指標和新的 LAG 指標）OutpostId。先前的小工具會繼續使用舊版維度名稱繼續顯示，OutpostsId以實現回溯相容性。

LAG 指標

AWS Outposts 會將連結彙總群組 (LAG) 狀態指標發佈至 Amazon CloudWatch。這些指標可讓您了解 Outpost 網路裝置與內部部署網路裝置之間 LAG 連線的操作狀態。將這些指標與 VIF 指標搭配使用，將實體 LAG 運作狀態與虛擬介面和 BGP 工作階段狀態建立關聯，以進行end-to-end連線故障診斷。

指標	維度	Description
LagStatus	OutpostId ，LagId, VirtualInterfaceGroupId ，VirtualInterfaceId	Outpost 網路裝置與內部部署網路裝置之間 LAG 連線的操作狀態。 單位：值，其中：

指標	維度	Description
		• 1 – LAG 可運作（向上） • 0 – LAG 無法運作（向下） 報告條件：有要報告的資料。 最長解析時間：5 分鐘 統計資訊：最實用的統計資訊是 Maximum。

下列維度用於 LagStatus 指標。

維度	Description
OutpostId	Outpost 的 ID（例如 op-1234567890abcdef0)
LagId	連結彙總群組的 ID（例如 op-lag-02343ndswe3190d1)
VirtualInterfaceGroupId	虛擬介面群組的 ID。LAG 指標一律顯示為「-」；CloudWatch Widget 會包含與 VIF 指標的一致性。
VirtualInterfaceId	虛擬界面的 ID。LAG 指標一律顯示為「-」；CloudWatch Widget 會包含與 VIF 指標的一致性。

Important

如果整個 Outpost 失去連線，基礎遙測服務就無法從網路裝置收集資料。在此期間不會發佈指標資料點，CloudWatch 圖形會顯示受影響時間範圍的差距。

Outposts 指標

下列指標適用於您的 Outpost。

指標	維度	Description
ConnectedStatus	OutpostId	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。
CapacityExceptions	InstanceType 和 OutpostId	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。

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。
VolumeType	EBS 磁碟區類型。

維度	Description
LagId	與此 VIF 相關聯的連結彙總群組 ID。
VirtualInterfaceId	本機閘道或服務連結虛擬介面 (VIF) 的 ID。
VirtualInterfaceGroupId	本機閘道虛擬介面 (VIF) 的虛擬介面群組 ID。

檢視 Outposts 機架 CloudWatch 指標

您可以使用 CloudWatch 主控台檢視 Outposts 機架 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.htmlCloudWatch 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 機架維護

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

目錄

- 更新聯絡詳細資訊
- 硬體維護
- 韌體更新
- 網路設備維護
- 電源和網路事件的最佳實務

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 機架託管執行的 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》。

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

如果需要硬體維護， AWS將聯絡 Outpost 擁有者，確認AWS安裝團隊造訪的日期和時間。Outpost 擁有者與AWS團隊交談後，只要兩個工作天就可以排定造訪。

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

韌體更新

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

網路設備維護

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

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

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

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 機架才能正確運作。

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 (關開關開)。
- 在維護時段內允許額外的時間來處理意外情況。
- 透過傳達比一般所需更寬的維護時段時間範圍來管理使用者和客戶的期望。
- 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 上的 Amazon EC2 執行個體、本機閘道和 Amazon EBS 磁碟區將繼續正常運作，並且可以透過本機網路在本機存取。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。

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

如果服務連結因為現場電源問題或網路連線中斷而關閉， 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 HealthHealth 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：

- 如果您的 Outposts 機架透過網際網路或公有 Direct Connect 連線至父AWS區域，則在計劃維護之前擷取追蹤路由。具備有效 (網路維護前) 的網路徑和有問題 (網路維護後) 的網路徑來識別差異將有助於進行疑難排解。如果您將維護後問題呈報至 AWS或 ISP，您可以包含此資訊。

  擷取下列項目之間的 trace-route：

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

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》。

Outposts 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 機架。
- 準備您的 Outposts 機架以供傳回。
- 轉換為month-to-month訂閱並保留現有的 Outposts 機架。

續訂訂閱

您必須在 Outposts 機架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。

若要續約訂閱並保留現有的 Outposts 機架：

1. 在 https：//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 並遵循工作流程。

> **Note**
>
> 如果在 Outposts 機架目前的訂閱結束之前續約，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 機架，則會自動轉換為month-to-month訂閱。您的 Outposts 機架將按與您的 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 AWS Outposts 機架

您必須在 Outposts AWS Outposts 機架目前的訂閱結束前至少 5 個工作日準備您的機架以供傳回並完成除役程序。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 個工作天完成這些步驟，可能會導致解除委任和非預期費用延遲。

當您送回 Outposts 機架時，不會向您收取運送費用。不過，如果您傳回損壞的機架，可能會產生費用。

若要準備您的 AWS Outposts 機架以供送回：

> **Important**
>
> 在 AWS 現場進行排定的擷取之前，請勿關閉 Outposts 機架。

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. 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。

   > **Note**
   >
   > 在 Outpost 上執行的一些 AWS受管服務，例如 Application Load Balancer 或 Amazon Relational Database Service (RDS)，會耗用 EC2 容量。不過，Amazon EC2 儀表板上不會顯示其相關聯的執行個體。您必須終止繫結至這些服務的資源，才能釋放容量。如需詳細資訊，請參閱 Outpost 上為什麼缺少一些 EC2 執行個體容量？。

3. 確認 AWS 帳戶中 Amazon EC2 執行個體的執行個體容量可用性。

   a. 在 https：//https://console.aws.amazon.com/outposts/ 開啟 AWS Outposts 主控台。

   b. 選擇 Outpost。

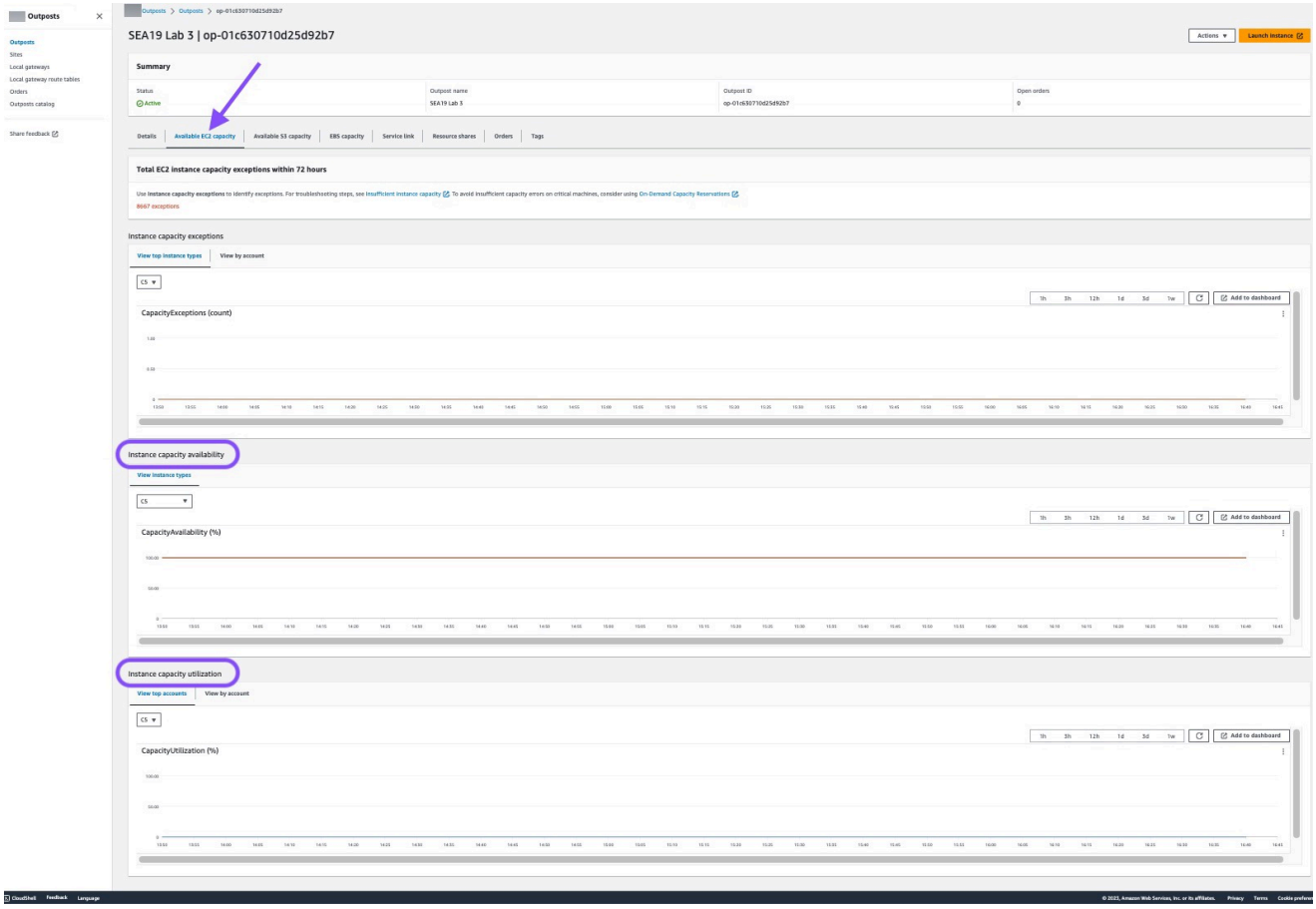
   c. 選擇您要退回的特定 Outpost。

   d. 在 Outpost 的頁面上，選擇 可用的 EC2 容量 標籤。

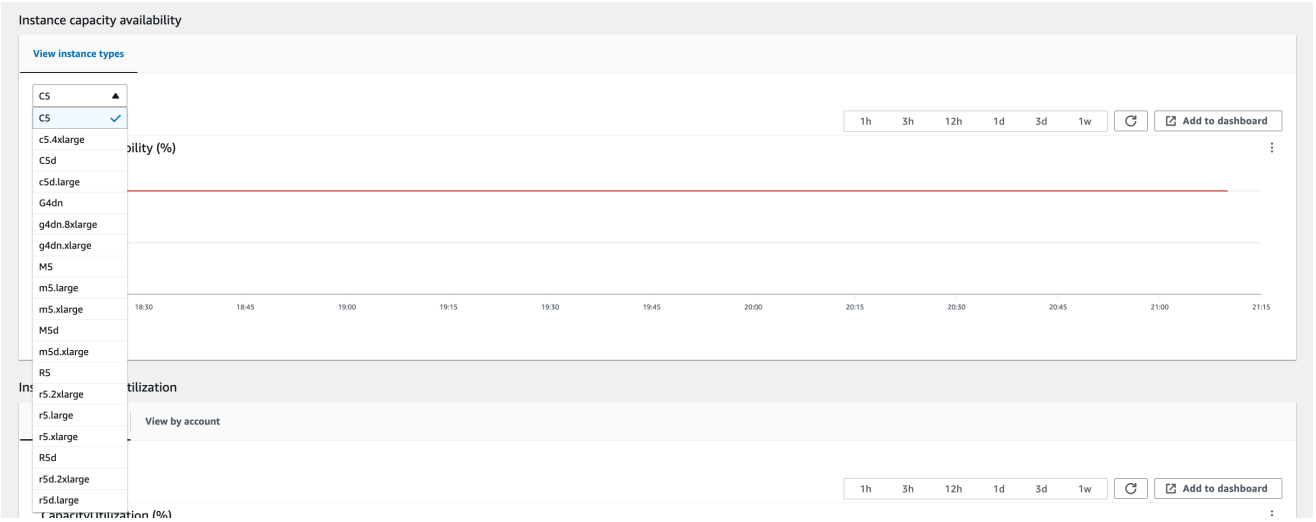
   e. 確保每個執行個體系列的 執行個體容量可用性 為 100%。

   f. 確保每個執行個體系列的 執行個體容量使用率 為 0%。

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



下圖顯示執行個體類型清單。



4. 建立 Amazon EC2 執行個體和伺服器磁碟區的備份。若要建立備份，請依照《AWS 方案指引》指南中《備份和復原具有 EBS 磁碟區的 Amazon EC2》的說明進行。

5. 刪除與 Outpost 相關聯的 Amazon EBS 磁碟區。

   a. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。

   b. 從導覽窗格，選擇 磁碟區。

   c. 選擇 動作 和 刪除磁碟區。

   d. 在確認對話方塊中，選擇 Delete (刪除)。

6. 如果您有 Amazon S3 on Outpost，請刪除 Outpost 上的任何本機快照。

   a. 在 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。

   b. 在導覽窗格中，選擇 Snapshots (快照)。

   c. 選取具有 Outpost ARN 的快照。

   d. 選擇 動作 和 刪除快照。

   e. 在確認對話方塊中，選擇 Delete (刪除)。

7. 刪除與 Outposts 機架相關聯的任何 Amazon S3 儲存貯體。若要刪除儲存貯體，請遵循《Amazon S3 on Outposts 使用者指南》中的刪除 Amazon S3 on Outposts 儲存貯體中的指示。 Amazon S3

8. 刪除與 Outpost 相關聯之任何 VPC 關聯和客戶擁有的 IP 地址集區 (CoIP) CIDR。

AWS 擷取團隊將關閉機架的電源。關閉電源後，您可以銷毀 AWS Nitro 安全金鑰，或者 AWS 擷取團隊可以代表您執行此操作。

傳回您的 AWS Outposts 機架

> **Important**
>
> AWS 在您提交停用請求後， 無法停止傳回程序。

1. 在 https：//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)。

   AWS 代表將與您聯絡，以開始停用程序。

> **Note**
>
> 在 Outposts 機架的目前訂閱結束之前傳回機架，不會終止與此 Outpost 相關的任何未結費用。

AWS 擷取團隊將關閉機架的電源。關閉電源後，您可以銷毀 AWS Nitro 安全金鑰，或者 AWS 擷取團隊可以代表您執行此操作。

轉換為按月訂閱

若要轉換為month-to-month訂閱並保留現有的 Outposts 機架，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 Outposts 機架將按對應於 Outposts 組態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第二天開始。

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	是	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。 您可以在 AWS 帳戶的每個區域中擁有 100 個 Outposts 網站。
每個站點的 Outpost	10	是	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。 您可以在每個 Outpost 站點中擁有 10 個 Outpost。

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 機架的文件歷史記錄

下表說明 Outposts 機架的文件更新。

變更	描述	日期
5 年期不再適用於第一代 Outposts 機架	當您訂購第一代 Outposts 機架時，您可以選擇 1 年或 3 年合約。5 年合約適用於第二代 Outposts 機架。	2026 年 9 月 1 日
AWS Outposts 支援來自 Dell 和 HPE 儲存陣列的外部區塊磁碟區	您可以使用外部區塊資料和第三方供應商支援的開機磁碟區，例如 Dell PowerStore 和 HPE Alletra Storage MP B10000。	2025 年 9 月 30 日
VIF 連線狀態和 BGP 工作階段狀態可用的指標。	您可以使用 ConnectionStatus 和 BGPSessionState 指標，在 CloudWatch 主控台上監控 AWS Outposts VIF 連線和 BGP 工作階段的狀態。	2025 年 7 月 31 日
續約您的訂閱並準備機架以供傳回	若要續約訂閱或傳回機架，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
AWS 服務支援	AWS Outposts 根據 Outpost 操作所在的 AWS 區域支援 AWS 服務。	2025 年 7 月 14 日
靜態穩定性的更新	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
AWS Identity and Access Management 服務連結角	AWSServiceRoleForOutposts_*OutpostID* 服務連	2025 年 4 月 17 日

色 AWSServiceRoleForOutposts_*OutpostID* 的更新	結角色許可已更新，以精簡 如何 AWS Outposts 管理私有連線的網路資源，並更精確地控制服務連結端點執行個體所需的網路界面和安全群組操作。	
資產層級的容量管理	您可以在資產層級修改容量組態。	2025 年 3 月 31 日
使用 Direct Connect 傳輸 VIF 的私有連線	您現在可以將服務連結設定為使用 Direct Connect 傳輸 VIF 來啟用 Outposts 與主要 AWS 區域之間的私有連線。	2024 年 12 月 11 日
第三方儲存體支援的外部區塊磁碟區	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
容量管理	您可以修改執行個體的容量組態。	2024 年 11 月 11 日
容量管理	您可以修改新 Outposts 訂單的預設容量組態。	2024 年 4 月 16 日
AWS Outposts 機架支援服務連結介面輸送量指標	您現在可以利用 `IfTrafficIn` 和 `IfTrafficOut` Amazon CloudWatch 指標，監控 Outposts 機架服務連結虛擬介面 (VIFs) 與本機網路裝置之間的輸送量用量。	2023 年 11 月 17 日
跨 AWS Outposts 與本機閘道的 VPC 內通訊	您可以透過本機閘道，在不同 Outpost 的相同 VPC 中的子網路之間建立通訊。	2023 年 8 月 30 日
AWS Outposts 機架End-of-term選項	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

Outposts 上的 Amazon Route 53 可在 AWS Outposts 機架上使用。	Amazon Route 53 on Outpost 包括一個解析程式，用於快取源自 AWS Outposts的所有 DNS 查詢。您也可以在部署傳入和傳出端點時，在 Outpost 和內部部署 DNS 解析程式之間設定混合式連線。	2023 年 7 月 20 日
本機閘道傳入路由	您可以建立和修改目的地為 Outpost 上彈性網路介面的本機閘道傳入路由。	2022 年 9 月 15 日
介紹 的直接 VPC 路由 AWS Outposts	使用 VPC 中執行個體的私有 IP 地址與內部部署網路進行通訊。	2022 年 9 月 14 日
Outposts 機架的建立 AWS Outposts 使用者指南	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
建立和管理本機閘道路由表	建立和修改本機閘道路由表和 CoIP 集區。管理 VIF 群組關聯。	2022 年 9 月 14 日
上的置放群組 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
上的專用主機 AWS Outposts	您現在可以在 Outpost 上使用專用執行個體。	2022 年 5 月 31 日
共用 Outpost 站點	建立和管理 Outpost 網站，並與組織中的其他 AWS 帳戶共用。	2021 年 10 月 18 日
新的 CloudWatch 維度	AWS Outposts 命名空間中指標的新 CloudWatch 維度。	2021 年 10 月 13 日
共用 S3 儲存貯體	在您的 Outpost 上共用和管理 S3 儲存貯體。	2021 年 8 月 5 日

支援某些放置群組	您可以像在區域中一樣使用叢集、分區或分散放置策略。	2021 年 7 月 28 日
其他 CloudWatch 指標	預留執行個體有其他 CloudWatch 指標可供使用。	2021 年 5 月 24 日
網路故障診斷檢查清單	提供網路故障診斷檢查清單。	2021 年 2 月 22 日
其他 CloudWatch 指標	EBS 磁碟區有其他 CloudWatch 指標可供使用。	2021 年 2 月 2 日
主控台訂購更新	主控台訂購程序已更新。	2021 年 1 月 14 日
私有連線	當您在 AWS Outposts 主控台中建立 Outpost 時，可以為 Outpost 設定私有連線。	2020 年 12 月 21 日
網路整備檢查清單	當您收集 Outpost 組態的資訊時，請使用網路整備檢查清單。	2020 年 10 月 28 日
共用 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，包括本機閘道路由表。	2020 年 10 月 15 日
其他 CloudWatch 指標	執行個體類型計數有其他 CloudWatch 指標可供使用。	2020 年 9 月 21 日
其他 CloudWatch 指標	服務連結連線狀態有其他 CloudWatch 指標可供使用。	2020 年 9 月 11 日
支援共用客戶擁有的 IPv4 地址	使用 AWS Resource Access Manager 共用客戶擁有的 IPv4 地址。	2020 年 4 月 20 日
其他 CloudWatch 指標	EBS 磁碟區有其他 CloudWatch 指標可供使用。	2020 年 4 月 4 日

初始版本	這是 的初始版本 AWS Outposts。	2019 年 12 月 3 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。