使用 建置混合雲端架構的最佳實務 AWS 服務

AWS 方案指引

AWS 方案指引: 使用 建置混合雲端架構的最佳實務 AWS 服務

Table of Contents

使用 建置混合雲端架構的最佳實務 AWS 服務

Amazon Web Services （貢獻者）

2025 年 6 月 (文件歷史記錄)

許多企業和組織已採用雲端運算作為其技術策略的關鍵層面。他們通常會將工作負載遷移到 AWS 雲端 ，以提高敏捷性、節省成本、效能、可用性、彈性和可擴展性。大多數應用程式可以輕鬆遷移，但某些應用程式必須保留在內部部署，以利用內部部署環境的低延遲和本機資料處理，以避免高資料傳輸成本，或符合法規。此外，一部分的應用程式可能需要重新架構或現代化，才能移至雲端。這會導致許多組織尋求混合雲端架構，以整合其內部部署和雲端操作，以支援廣泛的使用案例。這種混合式方法可以同時提供內部部署和雲端運算的優點，對於邊緣運算案例特別有用。

當您使用 建置混合雲端時 AWS，我們建議您決定混合雲端策略和技術策略：

- 混合雲端策略提供指導方針，可管理雲端和內部部署資源的消耗，以支援您的業務目標。本指南說明建置混合雲端的常見使用案例，例如支援持續遷移至雲端、在災難期間確保業務持續性、將雲端基礎設施擴展至內部部署環境以支援低延遲應用程式，或擴展您的國際據點 AWS。定義此策略可協助您識別和定義建置混合雲端的業務目標，並提供在混合雲端上放置工作負載的指導方針。
- 混合雲端的技術策略可識別混合雲端架構的引導原則，並定義實作架構。本指南概述持續部署和受管混合雲端架構的常見需求，以協助您定義規劃混合雲端實作的原則。這些要求包括跨雲端基礎設施進行資源佈建和管理的標準化界面。

本指南說明 操作和管理架構，以協助解決方案架構師和運算子識別建置區塊、最佳實務，以及 AWS 混合雲端和區域內服務，以實作混合雲端 AWS。

許多組織已使用本指南所述的解決方案，成功部署混合雲端環境，以利用 提供的規模、敏捷性、創新和全球足跡 AWS 雲端。（請參閱案例研究。）AWS 混合雲端服務提供從雲端到內部部署和邊緣的一致 AWS 體驗。當您在最終使用者裝置或現有的內部部署資料中心和工作負載伺服器之間需要 低延遲時，例如 AWS Outposts 和 將運算、儲存、資料庫和其他 選取 AWS Local Zones 項目放置在 AWS 服務接近大型人口和產業中心的位置。

在本指南中：

概觀

本指南將混合雲端 AWS 的建議分為五大支柱：聯網、安全性、彈性、容量規劃和基礎設施管理。它提供指導方針，協助您改善準備程度，並使用 AWS Outposts 或 等 AWS 混合邊緣服務來開發遷移策略 AWS Local Zones。我們強烈建議您與 AWS 帳戶 您的團隊合作 AWS Partner ，或確保 AWS 混合雲端專家可在您遵循本指南並開發程序時為您提供協助。

> **Note**
>
> 雖然 AWS Outposts 和 Local Zones 可解決類似的問題，但建議您檢閱使用案例以及可用的服務和功能，以決定哪種方案最適合您的需求。如需詳細資訊，請參閱 AWS 部落格文章AWS Local ZonesAWS Outposts，並為您的邊緣工作負載選擇正確的技術。

混合雲端研討會

在 AWS 混合雲端主題專家 (SME) 的協助下，您可以執行混合雲端研討會，以評估貴公司與本指南中討論的五大支柱相關的成熟度。

研討會著重於組織內的內部領域，例如聯網、安全、合規、DevOps、虛擬化和業務單位。它可協助您設計符合您組織需求的混合雲端架構，並依照本指南混合雲端採用程序一節中的步驟定義實作詳細資訊。

PoCs

如果您有特定要求，您可以使用概念驗證 (PoCs) 來驗證 Local Zones 中的功能，並根據這些要求 AWS Outposts 進行驗證。

AWS 使用 PoCs來協助您測試要移至 Outpost 或 Local Zone 的工作負載，以判斷工作負載是否在測試架構下運作。若要存取 Local Zones 進行測試，請遵循 Local Zones 文件中的指示。若要測試您的工作負載 AWS Outposts，請與您的 AWS 帳戶 團隊合作 AWS Partner 或存取 AWS Outposts 測試實驗室，並從解決方案架構師取得指導 AWS 。在所有情況下，PoC 的開發都需要您產生包含下列項目的測試文件：

- AWS 服務 要使用，例如 Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Block Store (Amazon EBS)、Amazon Virtual Private Cloud (Amazon VPC) 和 Amazon Elastic Kubernetes Service (Amazon EKS)

- 要使用的執行個體大小和數量 （例如， m5.xlarge或 c5.2xlarge)
- 測試架構圖
- 測試成功條件
- 要執行之每個測試的詳細資訊和目標

支柱

下一節涵蓋使用本指南中討論之架構的先決條件和限制。之後的章節涵蓋了每個支柱的詳細資訊，以便您在混合雲端研討會期間建立的建議文件可以反映實作所需的設計詳細資訊。

- 邊緣聯網
- 邊緣的安全性
- 邊緣的彈性
- 邊緣的容量規劃
- 邊緣基礎設施管理

先決條件和限制

遵循本指南之前，請先與 AWS 帳戶 您的團隊或 合作 AWS Partner ，以檢閱使用 和 Local Zones 實作邊緣架構的先決條件 AWS Outposts 和限制。

先決條件

AWS Outposts

- 您現有的資料中心必須符合設施、聯網和電源AWS Outposts 的需求。 AWS Outposts 的設計是為了在具有 5-15 kVA 備援電源輸入的資料中心環境中運作、每分鐘立方英呎 (CFM) 氣流的 145.8 倍，以及介於 41° F (5° C) 和 95° F (35° C) 之間的環境溫度等需求。
- 請參閱AWS Outposts 機架FAQs，確認 AWS Outposts 服務可在您的國家/地區使用。請參閱問題：在哪些國家和地區可使用 Outposts 機架？
- 如果您的組織需要四個以上的AWS Outposts 機架，您的資料中心必須符合彙總、核心、邊緣 (ACE) 機架需求。
- 必須提供並維持至少 500 Mbps (1 Gbps 更好） 的網際網路或 AWS Direct Connect 連結，才能AWS Outposts 連線到 AWS 區域，如果您的使用案例需要，請使用適當的備份連線。從 AWS Outposts 到 區域的往返時間延遲上限為 175 毫秒。
- 您必須擁有 AWS Enterprise Support 或 AWS Unified Operations 計畫的作用中合約。

AWS Local Zones

- AWS 本機區域必須靠近您的資料中心或使用者。請參閱AWS Local Zones 位置。
- 確認您具有從現場部署基礎設施到 Local Zone 的網路連線能力：
  - 選項 1：從資料中心到最接近本機區域的Direct Connect 存在點 (PoP) Direct Connect 的連結。如需詳細資訊，請參閱 Local Zones 文件中的 Direct Connect。
  - 選項 2：內部部署虛擬私有網路 (VPN) 設備以外的網際網路連結，以及在 Local Zone 的 Amazon EC2 上啟動軟體型 VPN 設備所需的授權。如需詳細資訊，請參閱 Local Zones 文件中的 VPN 連線。

如需其他連線選項，請參閱 Local Zones 文件。

限制

AWS Outposts

- AWS Outposts 多可用區域部署上的 Amazon Relational Database Service (Amazon RDS) 需要客戶擁有的 IP (CoIP) 地址集區。如需詳細資訊，請參閱 Amazon RDS on 的客戶擁有 IP 地址 AWS Outposts。
- 上的異地同步備份 AWS Outposts 可用於 Amazon RDS on 上所有支援的 MySQL 和 PostgreSQL 版本 AWS Outposts。如需詳細資訊，請參閱 AWS Outposts 上的 Amazon RDS 支援 Amazon RDS 功能。上的 AWS Outposts Amazon RDS 支援 SQL Server、Amazon RDS for MySQL 和 Amazon RDS for PostgreSQL 資料庫。
- AWS Outposts 並非設計用於在中斷與 的連線時運作 AWS 區域。如需詳細資訊，請參閱白皮書AWS Outposts 高可用性設計和架構考量中的 AWS 關於故障模式的思考一節。
- 上的 Amazon Simple Storage Service (Amazon S3) AWS Outposts 有一些限制。Amazon S3 on Outposts 與 Amazon S3 有何不同之處中有相關討論？ Amazon S3 on Outposts 使用者指南的 部分。
- 上的 Application Load Balancer AWS Outposts 不支援交互 TLS (mTLS) 或黏性工作階段。
- ACE 機架並非完全封閉，也不包含前門或後門。
- 執行個體容量工具僅適用於新訂單。

AWS Local Zones

- 本機區域沒有 AWS Site-to-Site VPN 端點。反之，請在 Amazon EC2 上使用軟體型 VPN。
- Local Zones 不支援 AWS Transit Gateway。反之，請使用 Direct Connect 私有虛擬界面 (VIF) 連線到 Local Zone。
- 並非所有 Local Zones 都支援 Amazon RDS、Amazon FSx、Amazon EMR 或 Amazon ElastiCache 或 NAT 閘道等服務。如需詳細資訊，請參閱 AWS Local Zones 功能。
- Local Zones 中的 Application Load Balancer 不支援 mTLS 或黏性工作階段。

混合雲端採用程序

下列各節討論 AWS 混合雲端每個支柱的架構和設計詳細資訊：

在邊緣聯網

當您設計使用 AWS 邊緣基礎設施的解決方案時，例如 AWS Outposts 或 Local Zones，您必須仔細考慮網路設計。網路是連線能力的基礎，可到達部署在這些節點的工作負載，對於確保低延遲至關重要。本節概述混合邊緣連線的各個層面。

VPC 架構

虛擬私有雲端 (VPC) 跨越其 中的所有可用區域 AWS 區域。您可以使用 AWS 主控台或 AWS Command Line Interface (AWS CLI) 新增 Outpost 或 Local Zone 子網路，將區域中的任何 VPC 無縫擴展至 Outpost 或 Local Zones。下列範例示範如何使用 在 AWS Outposts 和 Local Zones 中建立子網路 AWS CLI：

- AWS Outposts：若要將 Outpost 子網路新增至 VPC，請指定 Outpost 的 Amazon Resource Name (ARN)。

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.0.0/24 \
--outpost-arn arn:aws:outposts:us-west-2:11111111111:outpost/op-0e32example1 \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

  如需詳細資訊，請參閱 AWS Outposts 文件。

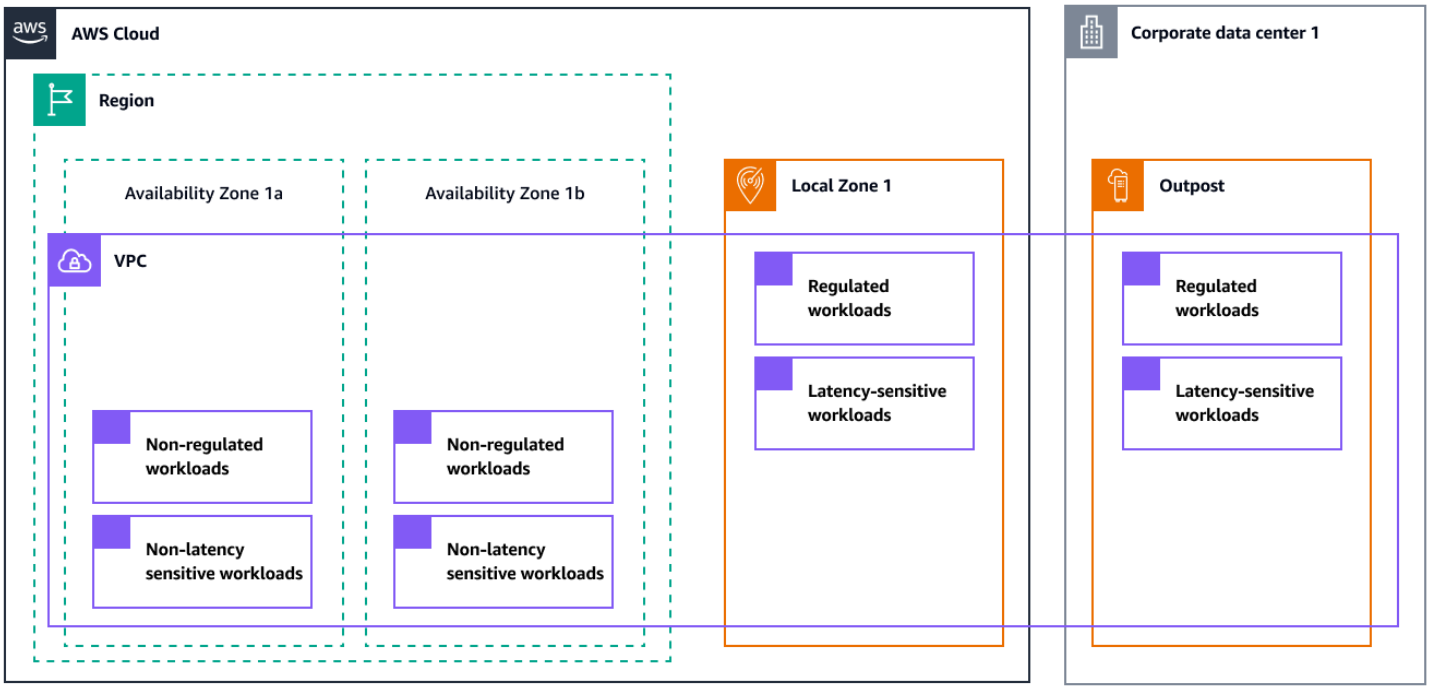
- Local Zones：若要將 Local Zone 子網路新增至 VPC，請遵循與可用區域搭配使用的相同程序，但指定 Local Zone ID (<local-zone-name>在下列範例中）。

```
aws ec2 create-subnet --vpc-id vpc-081ec835f3EXAMPLE \
--cidr-block 10.0.1.0/24 \
```

```
--availability-zone <local-zone-name> \
--tag-specifications ResourceType=subnet,Tags=[{Key=Name,Value=my-ipv4-only-subnet}]
```

如需詳細資訊，請參閱 Local Zones 文件。

下圖顯示包含 Outpost 和 Local Zone 子網路的 AWS 架構。



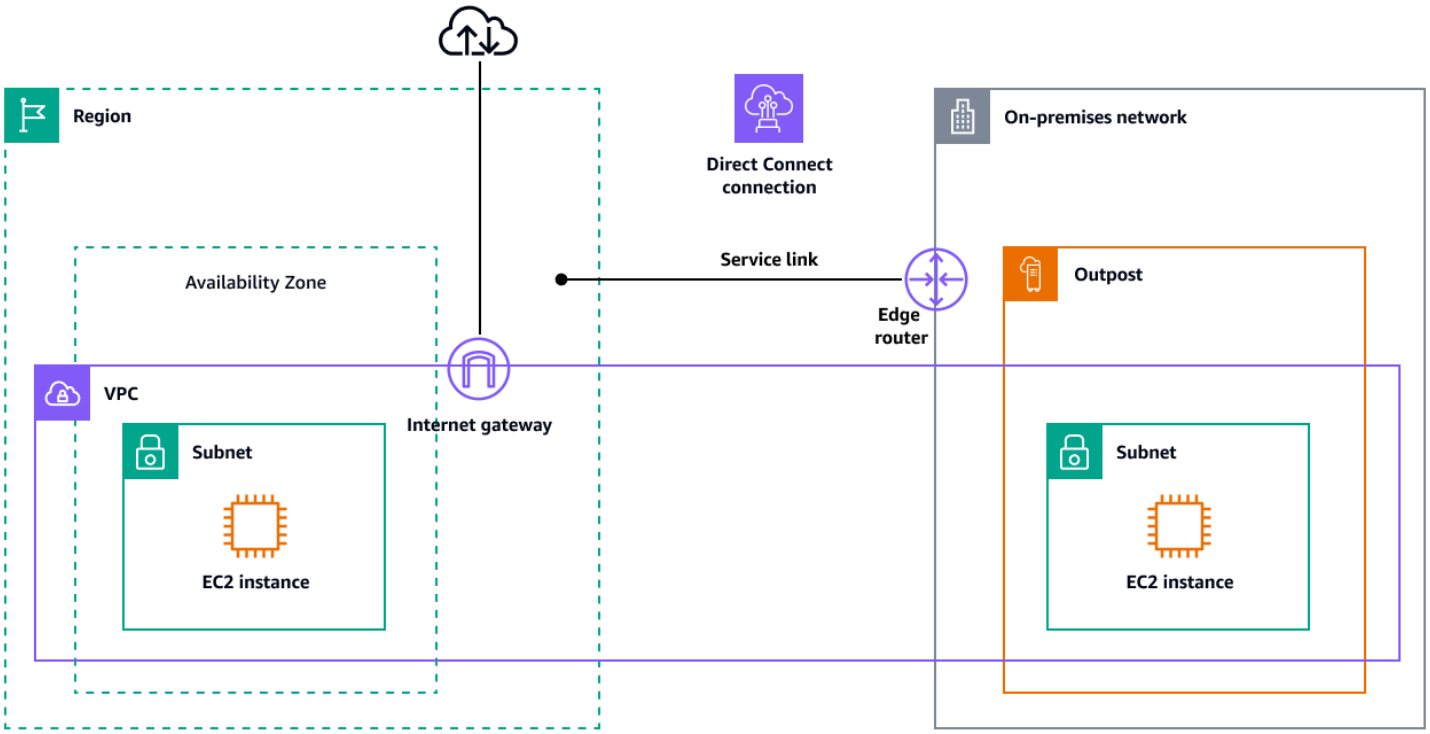
邊緣到區域流量

當您使用 Local Zones 和 等服務設計混合架構時 AWS Outposts，請考慮控制流程和邊緣基礎設施與之間的資料流量 AWS 區域。根據邊緣基礎設施的類型，您的責任可能有所不同：有些基礎設施要求您管理與父區域的連線，而其他基礎設施則透過 AWS 全球基礎設施處理。本節探索 Local Zones 和 的控制平面和資料平面連線影響 AWS Outposts。

AWS Outposts 控制平面

AWS Outposts 提供稱為服務連結的聯網建構。服務連結是 AWS Outposts 與所選 AWS 區域 或父區域 （ 也稱為主區域) 之間的必要連線。它可以管理 Outpost，以及在 Outpost 和 之間交換流量 AWS 區域。服務連結使用一組加密的 VPN 連線來與主要區域通訊。您必須 AWS 區域 透過網際網路連結或 Direct Connect 公有虛擬界面 （ 公有 VIF)，或透過 Direct Connect 私有虛擬界面 （ 私有 VIF)，在 AWS Outposts 和 之間提供連線。為了獲得最佳體驗和彈性， AWS 建議您使用至少 500 Mbps (1 Gbps 更好 ） 的備援連線來連接 的服務連結 AWS 區域。最低 500 Mbps 的服務連結連線可讓您啟動 Amazon EC2 執行個體、連接 Amazon EBS 磁碟區，以及存取 AWS 服務 Amazon EKS、Amazon

EMR 和 Amazon CloudWatch 指標。網路必須支援 Outpost 與服務連結端點之間 1，500 個位元組的最大傳輸單位 (MTU) AWS 區域。如需詳細資訊，請參閱 Outposts 文件中的AWS Outposts 連線至 AWS 區域 。



如需有關為使用 Direct Connect 和公有網際網路的服務連結建立彈性架構的資訊，請參閱 AWS 白皮書AWS Outposts 高可用性設計和架構考量中的錨點連線一節。

AWS Outposts 資料平面

AWS Outposts 與 之間的資料平面由控制平面所使用的相同服務連結架構 AWS 區域 支援。 AWS Outposts 與 之間的資料平面服務連結頻寬 AWS 區域 應與必須交換的資料量相關：資料相依性越高，連結頻寬就越大。

頻寬需求會根據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、應用程式彈性和高載速度需求
- 通往區域的 VPC 流量

中的 EC2 執行個體 AWS Outposts 與 中的 EC2 AWS 區域 執行個體之間的流量具有 1，300 個位元組的 MTU。建議您先與 AWS 混合雲端專家討論這些需求，再提議在 區域與 之間具有共同相依性的架構 AWS Outposts。

Local Zones 資料平面

全球基礎設施 AWS 區域 支援 AWS Local Zones 與 之間的資料平面。資料平面會透過 VPC 從 擴展 AWS 區域 到 Local Zone。Local Zones 也提供與 的高頻寬、安全連線 AWS 區域，並可讓您透過相同的 APIs 和工具集無縫連線至完整的區域服務。

下表顯示連線選項和相關聯的 MTUs。

從	至	MTU
區域中的 Amazon EC2	Local Zones 中的 Amazon EC2	1，300 個位元組
Direct Connect	本機區域	1，468 個位元組
網際網路閘道	本機區域	1，500 個位元組
Local Zones 中的 Amazon EC2	Local Zones 中的 Amazon EC2	9，001 個位元組

Local Zones 使用 AWS 全域基礎設施進行連線 AWS 區域。基礎設施由 完全管理 AWS，因此您不需要設定此連線。建議您先與 AWS 混合雲端專家討論 Local Zones 的需求和考量，再設計任何在區域和 Local Zones 之間具有共同相依性的架構。

邊緣到內部部署流量

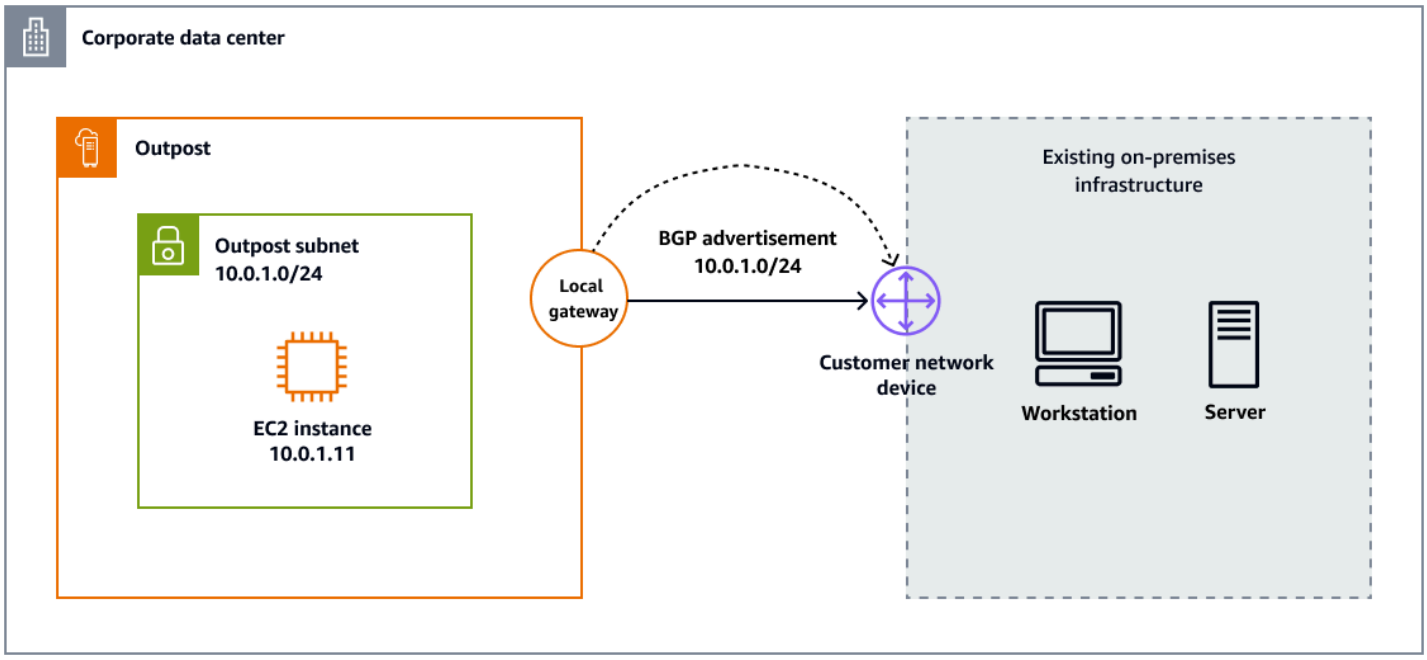
AWS 混合雲端服務旨在解決需要低延遲、本機資料處理或資料駐留合規的使用案例。存取此資料的網路架構很重要，取決於您的工作負載是在 AWS Outposts 或 Local Zones 中執行。本機連線也需要定義明確的範圍，如以下章節所述。

AWS Outposts 本機閘道

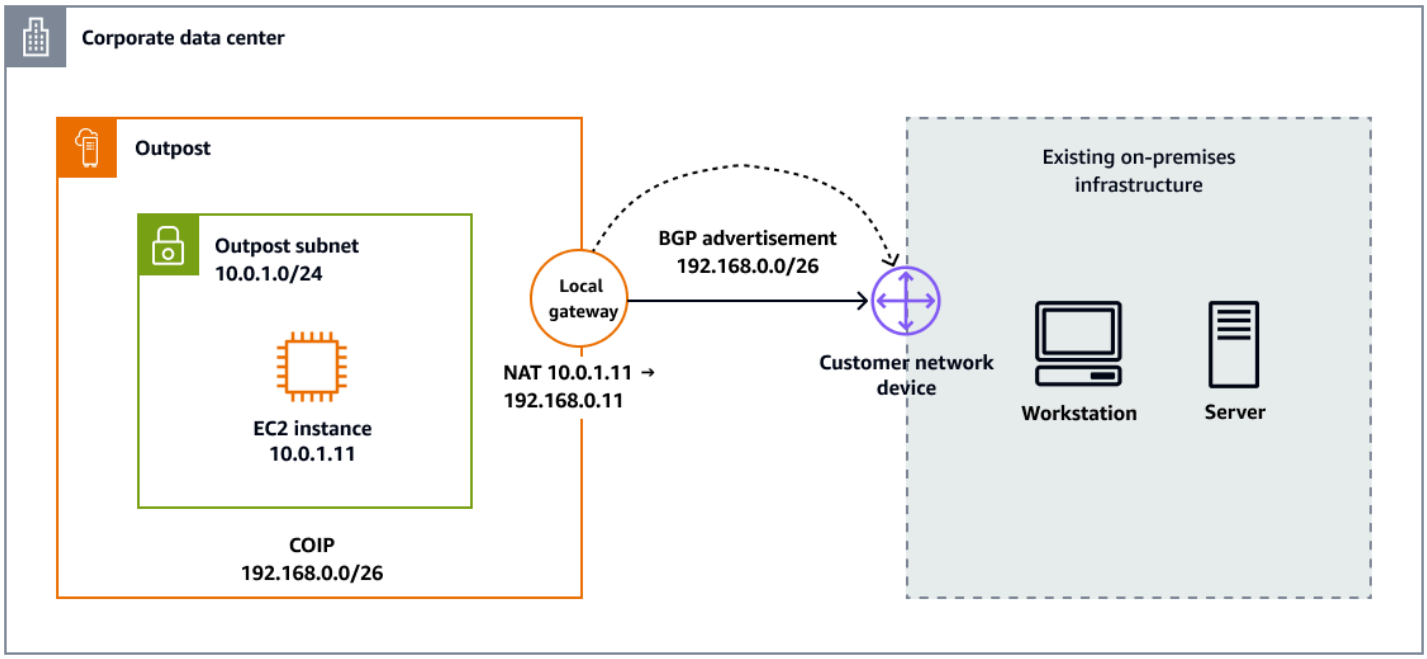
本機閘道 (LGW) 是 AWS Outposts 架構的核心元件。本機閘道可讓您在 Outpost 子網路與內部部署網路之間進行連線。LGW 的主要角色是提供從 Outpost 到本機內部部署網路的連線。它還透過直接 VPC 路由或客戶擁有的 IP 地址，透過內部部署網路提供網際網路連線。

- 直接 VPC 路由使用 VPC 中執行個體的私有 IP 地址，以促進與內部部署網路的通訊。這些地址會使用邊界閘道協定 (BGP) 公告到您的內部部署網路。BGP 公告僅適用於屬於 Outpost 機架上子網路的私有 IP 地址。這種類型的路由是 的預設模式 AWS Outposts。在此模式中，本機閘道不會為執行個

體執行 NAT，而且您不需要將彈性 IP 地址指派給 EC2 執行個體。下圖顯示使用直接 VPC 路由的 AWS Outposts 本機閘道。



- 使用客戶擁有的 IP 地址，您可以提供地址範圍，稱為客戶擁有的 IP (CoIP) 地址集區，支援重疊的 CIDR 範圍和其他網路拓撲。選擇 CoIP 時，您必須建立地址集區，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網路。CoIP 地址可為內部部署網路中的資源提供本機或外部連線。您可以將這些 IP 地址指派給 Outpost 上的資源，例如 EC2 執行個體，方法是從 CoIP 配置新的彈性 IP 地址，然後將其指派給您的資源。下圖顯示使用 CoIP 模式的 AWS Outposts 本機閘道。



從 AWS Outposts 到本機網路的本機連線需要一些參數組態，例如在 BGP 對等之間啟用 BGP 路由通訊協定和公告字首。Outpost 和本機閘道之間可支援的 MTU 為 1，500 個位元組。如需詳細資訊，請聯絡 AWS 混合雲端專家或檢閱 AWS Outposts 文件。

Local Zones 和網際網路

需要低延遲或本機資料駐留的產業（範例包括遊戲、即時串流、金融服務和政府），可以使用 Local Zones 透過網際網路部署和提供其應用程式給最終使用者。在部署 Local Zone 期間，您必須配置要在 Local Zone 中使用的公有 IP 地址。當您配置彈性 IP 地址時，您可以指定 IP 地址的公告位置。此位置稱為網路邊界群組。網路邊界群組是可用區域、本機區域或 AWS Wavelength 區域的集合，可從中 AWS 公告公有 IP 地址。這有助於確保 AWS 網路與存取這些區域中資源的使用者之間的最小延遲或實體距離。若要查看 Local Zones 的所有網路邊界群組，請參閱 Local Zones 文件中的可用 Local Zones。

若要將本機區域中的 Amazon EC2 託管工作負載公開至網際網路，您可以在啟動 EC2 執行個體時啟用自動指派公有 IP 選項。如果您使用 Application Load Balancer，您可以將它定義為面向網際網路，以便指派給 Local Zone 的公有 IP 地址可以由與 Local Zone 相關聯的邊界網路傳播。此外，當您使用彈性 IP 地址時，您可以在其中一個資源啟動後將其與 EC2 執行個體建立關聯。當您透過 Local Zones 中的網際網路閘道傳送流量時，會套用區域使用的相同執行個體頻寬規格。本機區域網路流量會直接流向網際網路或存在點 (PoPs)，而不周遊本機區域的父區域，以啟用低延遲運算的存取。

Local Zones 透過網際網路提供下列連線選項：

- 公開存取：透過網際網路閘道使用彈性 IP 地址，將工作負載或虛擬設備連線至網際網路。

- 傳出網際網路存取：讓資源透過網路位址轉譯 (NAT) 執行個體或具有相關聯彈性 IP 地址的虛擬設備到達公有端點，而無需直接網際網路暴露。
- VPN 連線：透過具有相關聯彈性 IP 地址的虛擬設備，使用網際網路通訊協定安全 (IPsec) VPN 建立私有連線。

如需詳細資訊，請參閱 Local Zones 文件中的 Local Zones 連線選項。

本機區域和 Direct Connect

Local Zones 也支援 Direct Connect，可讓您透過私有網路連線路由流量。如需詳細資訊，請參閱 Local Zones 文件中 Local Zones 中的 Direct Connect。

本機區域和傳輸閘道

AWS Transit Gateway 不支援將 VPC 直接連接至 Local Zone 子網路。不過，您可以在相同 VPC 的父可用區域子網路中建立 Transit Gateway 附件，以連線至 Local Zone 工作負載。此組態可在多個 VPCs和您的 Local Zone 工作負載之間進行互連。如需詳細資訊，請參閱 Local Zones 文件中的 Local Zones 之間的傳輸閘道連線。

本機區域和 VPC 對等互連

您可以透過建立新的子網路並將其指派給 Local Zone，將父區域的任何 VPC 延伸到 Local Zone。可以在延伸到 Local Zones VPCs 之間建立 VPC 對等互連。當對等 VPCs位於相同的 Local Zone 時，流量會保持在 Local Zone 內，而不會透過父區域髮夾。

邊緣的安全性

在 中 AWS 雲端，安全是首要任務。隨著組織採用雲端的可擴展性和靈活性， 會 AWS 協助他們採用安全性、身分和合規性作為關鍵業務因素。 將安全性 AWS 整合到其核心基礎設施，並提供 服務來協助您滿足獨特的雲端安全需求。當您將架構的範圍擴展到 時 AWS 雲端，您可以從本機區域和 Outpost 等基礎設施的整合中獲益 AWS 區域。此整合可讓 AWS 將一組選取的 核心安全服務擴展到邊緣。

安全性是 AWS 與您之間的共同責任。AWS 共同責任模型區分雲端安全性和雲端安全性：

- 雲端的安全性 – AWS 負責保護在 AWS 服務 中執行的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在AWS 合規計畫中，第三方稽核人員會定期測試和驗證 AWS 安全性的有效性。
- 雲端的安全性 – 您的責任取決於您使用 AWS 服務 的 。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。

資料保護

AWS 共同責任模型適用於 AWS Outposts 和 中的資料保護 AWS Local Zones。如此模型所述， AWS 負責保護執行 AWS 雲端 (雲端安全性) 的 全球基礎設施。您有責任控制在此基礎設施 (雲端中的安全) 上託管的內容。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 Identity and Access Management (IAM) 或 設定個別使用者AWS IAM Identity Center。這只會為每個使用者提供完成其工作職責所需的許可。

靜態加密

EBS 磁碟區中的加密

使用 時 AWS Outposts，所有資料都會進行靜態加密。金鑰材料是以外部金鑰 Nitro 安全金鑰 (NSK) 包裝，存放在可移除的裝置中。需要 NSK 才能解密 Outpost 機架上的資料。您可以對 EBS 磁碟區和快照使用 Amazon EBS 加密。Amazon EBS 加密使用 AWS Key Management Service (AWS KMS) 和 KMS 金鑰。

在 Local Zones 中， 除非為帳戶啟用加密，否則所有 EBS 磁碟區都會預設在所有 Local Zones 中加密，除了 AWS Local Zones 常見問答集中記錄的清單 （請參閱問題：Local Zones 中 EBS 磁碟區的預設加密行為是什麼？)。

Amazon S3 on Outposts 中的加密

依預設，所有存放在 Amazon S3 on Outposts 中的資料均會使用伺服器端加密與 Amazon S3 受管加密金鑰 (SSE-S3) 進行加密。您可以選擇性以客戶提供的加密金鑰 (SSE-C) 使用伺服器端加密。若要使用 SSE-C，請指定加密金鑰做為物件 API 請求的一部分。伺服器端加密只會加密物件資料，非物件中繼資料。

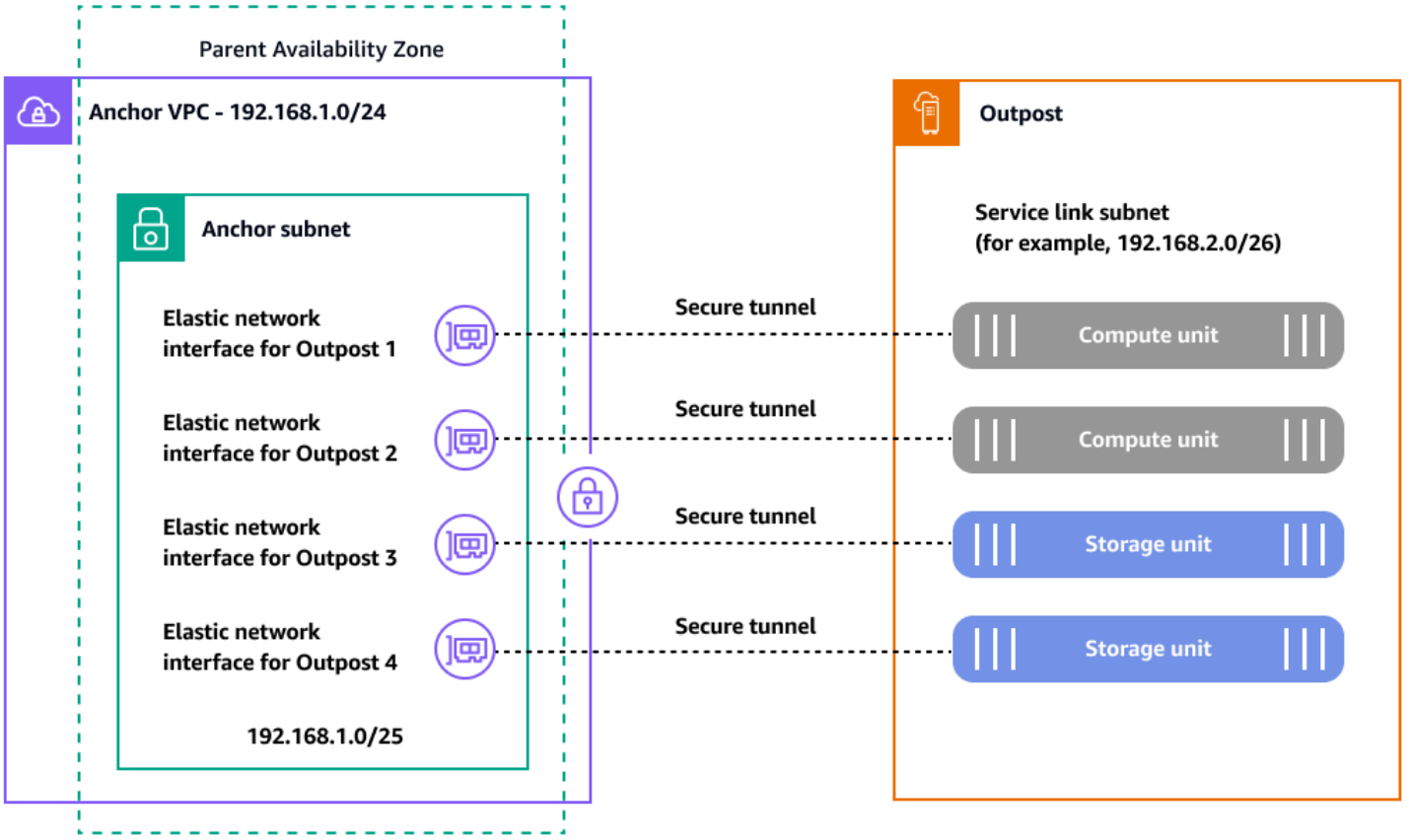
> **Note**
>
> Amazon S3 on Outposts 不支援使用 KMS 金鑰 (SSE-KMS) 的伺服器端加密。

傳輸中加密

對於 AWS Outposts，服務連結是 Outposts 伺服器與所選 AWS 區域 （或主要區域） 之間的必要連線，並允許管理 Outpost 和往返 的流量交換 AWS 區域。服務連結使用 AWS 受管 VPN 與主要區域通訊。內部的每個主機 AWS Outposts 都會建立一組 VPN 通道，以分割控制平面流量和 VPC 流量。根據 的服務連結連線 （網際網路或 Direct Connect) AWS Outposts，這些通道需要開啟防火牆連接埠，

服務連結才能在上面建立浮水印。如需 和服務連結安全性 AWS Outposts 的詳細資訊，請參閱 AWS Outposts 文件中的透過服務連結的連線和 中的基礎設施安全性 AWS Outposts。

AWS Outposts 服務連結會建立加密通道，以建立與父系的控制平面和資料平面連線 AWS 區域，如下圖所示。



每個 AWS Outposts 主機（運算和儲存）都需要透過已知的 TCP 和 UDP 連接埠使用這些加密通道，才能與其父區域通訊。下表顯示 UDP 和 TCP 通訊協定的來源和目的地連接埠和地址。

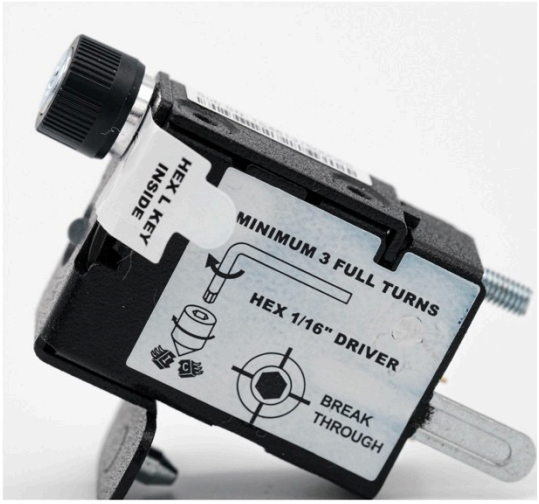
通訊協定	來源連接埠	來源地址	目的地連接埠	目的地地址
UDP	443	AWS Outposts 服務連結 /26	443	AWS Outposts 區域的公有路由或錨點 VPC CIDR

通訊協定	來源連接埠	來源地址	目的地連接埠	目的地地址
TCP	1025-65535	AWS Outposts 服務連結 /26	443	AWS Outposts 區域的公有路由或錨點 VPC CIDR

Local Zones 也會透過備援且高頻寬的 Amazon 全域私有骨幹連接到父區域。此連線可讓在 Local Zones 中執行的應用程式快速、安全且無縫地存取其他 AWS 服務。只要 Local Zones 是 AWS 全球基礎設施的一部分，在離開 AWS 安全設施之前，所有流經 AWS 全球網路的資料都會在實體層自動加密。如果您對於加密內部部署位置和 Direct Connect PoPs 之間傳輸中的資料以存取 Local Zone 有特定需求，您可以在內部部署路由器或交換器與 Direct Connect 端點之間啟用 MAC Security (MACsec)。如需詳細資訊，請參閱 AWS 部落格文章將 MACsec 安全性新增至 Direct Connect 連線。

資料刪除

當您在 中停止或終止 EC2 執行個體時 AWS Outposts，Hypervisor 會先清除 （設定為零） 分配給新執行個體的記憶體，並重設每個儲存區塊。從 Outpost 硬體刪除資料涉及使用專用硬體。NSK 是一種小型裝置，如下圖所示，連接至 Outpost 中每個運算或儲存單元的正面。它旨在提供一個機制，以防止您的資料從資料中心或主機代管網站公開。Outpost 裝置上的資料會受到保護，方法是包裝用來加密裝置的金鑰資料，並將包裝的資料存放在 NSK 上。當您傳回 Outpost 主機時，您可以旋轉晶片上的小型螺絲來銷毀 NSK，這樣會破碎 NSK 並實際銷毀晶片。銷毀 NSK 會在 Outpost 上以密碼編譯方式分割資料。



身分與存取管理

AWS Identity and Access Management (IAM) 是 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。如果您有 AWS 帳戶，則可以免費使用 IAM。

下表列出您可以使用的 IAM 功能 AWS Outposts。

IAM 功能	AWS Outposts 支援
身分型政策	是
資源型政策	是*
政策動作	是
政策資源	是
政策條件索引鍵 (服務特定)	是
存取控制清單 (ACL)	否
以屬性為基礎的存取控制 (ABAC)	是
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	是

* 除了 IAM 身分型政策之外，Amazon S3 on Outposts 還支援儲存貯體和存取點政策。這些是連接至 Amazon S3 on Outposts 資源的資源型政策。

如需 中如何支援這些功能的詳細資訊 AWS Outposts，請參閱 AWS Outposts 使用者指南。

基礎設施安全性

基礎設施保護是資訊安全計畫的關鍵部分。它可確保工作負載系統和服務受到保護，免於意外和未經授權的存取，以及潛在的漏洞。例如，您可以定義信任界限 （例如網路和帳戶界限）、系統安全組態和

維護（例如強化、最小化和修補）、作業系統身分驗證和授權（例如使用者、金鑰和存取層級），以及其他適當的政策強制執行點（例如 Web 應用程式防火牆或 API 閘道）。

AWS 提供多種基礎設施保護方法，如以下各節所述。

保護網路

您的使用者可能是人力資源或客戶的一部分，而且可以位於任何地方。因此，您無法信任有權存取您網路的每個人。當您遵循在所有層套用安全性的原則時，您會採用零信任方法。在零信任安全模型中，應用程式元件或微服務被視為分散的，而且沒有元件或微服務信任任何其他元件或微服務。若要實現零信任安全性，請遵循下列建議：

- 建立網路層。分層網路有助於在邏輯上將類似的聯網元件分組。它們也會縮小未經授權的網路存取的潛在影響範圍。
- 控制流量層。針對傳入和傳出流量，使用defense-in-depth方法套用多個控制項。這包括使用安全群組（狀態檢查防火牆）、網路 ACLs、子網路和路由表。
- 實作檢查和保護。檢查和篩選每個 layer 的流量。您可以使用 Network Access Analyzer 來檢查 VPC 組態是否有潛在的意外存取。您可以指定網路存取需求，並識別不符合這些要求的潛在網路路徑。

保護運算資源

運算資源包括 EC2 執行個體、容器、 AWS Lambda 函數、資料庫服務、IoT 裝置等。每種運算資源類型都需要不同的安全方法。不過，這些資源確實會共用您需要考慮的常見策略：深度防禦、漏洞管理、減少攻擊面、組態和操作的自動化，以及遠端執行動作。

以下是保護關鍵服務運算資源的一般指引：

- 建立和維護漏洞管理計劃。定期掃描和修補資源，例如 EC2 執行個體、Amazon Elastic Container Service (Amazon ECS) 容器和 Amazon Elastic Kubernetes Service (Amazon EKS) 工作負載。
- 自動化運算保護。自動化您的保護性運算機制，包括漏洞管理、減少攻擊面，以及管理 資源。此自動化可釋放時間，讓您用來保護工作負載的其他層面，並協助降低人為錯誤的風險。
- 減少攻擊面。透過強化您的作業系統，並將您使用的元件、程式庫和外部消耗服務降至最低，以減少意外存取的風險。

此外，針對 AWS 服務 您使用的每個 ，請檢查服務文件中的特定安全建議。

網際網路存取

AWS Outposts 和 Local Zones 都提供架構模式，讓您的工作負載能夠存取和存取網際網路。當您使用這些模式時，只有當您將其用於修補、更新、存取外部的 Git 儲存庫，以及類似案例時 AWS，才考慮從 區域使用網際網路是可行的選項。對於此架構模式，會套用集中式傳入檢查和集中式網際網路輸出的概念。這些存取模式使用 AWS Transit Gateway NAT 閘道、網路防火牆和其他位於 中的元件 AWS 區域，但透過區域和邊緣之間的資料路徑連接到 AWS Outposts 或 Local Zones。

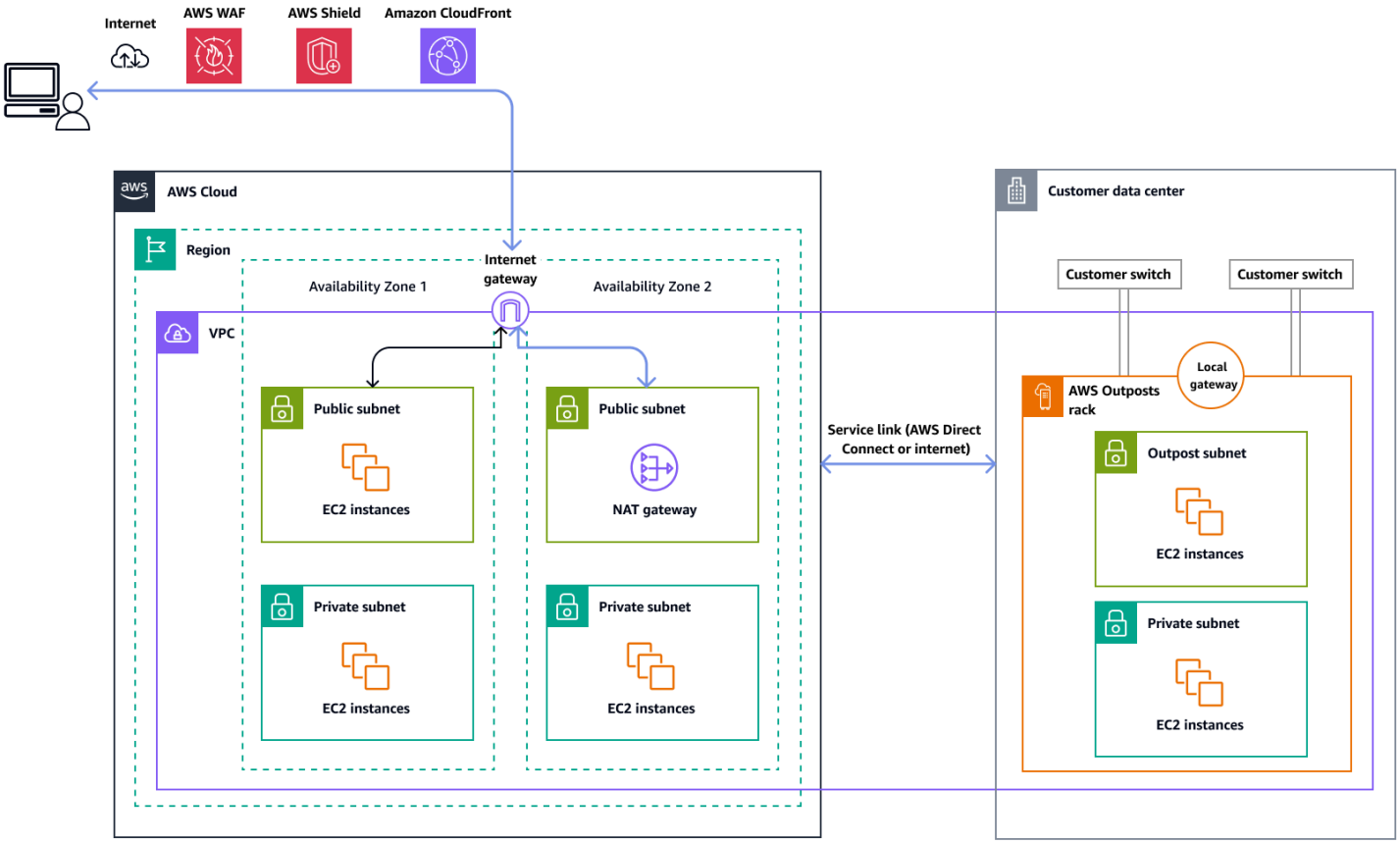
Local Zones 採用稱為網路邊界群組的網路建構，在 中使用 AWS 區域。 AWS 公告來自這些唯一群組的公有 IP 地址。網路邊界群組包含可用區域、本機區域或 Wavelength 區域。您可以明確配置公有 IP 地址集區，以用於網路邊界群組。您可以使用網路邊界群組，允許從群組提供彈性 IP 地址，將網際網路閘道延伸到 Local Zones。此選項要求您部署其他元件，以補充 Local Zones 中提供的核心服務。這些元件可能來自 ISVs並協助您在 Local Zone 中建置檢查層，如 AWS 部落格文章所述。 AWS Local Zones

在 中 AWS Outposts，如果您想要使用本機閘道 (LGW) 從網路連線到網際網路，則必須修改與 AWS Outposts 子網路相關聯的自訂路由表。路由表必須具有使用 LGW 做為下一個躍點的預設路由項目 (0.0.0.0/0)。您有責任在本機網路中實作 剩餘的安全控制，包括周邊防禦，例如防火牆和入侵預防系統或入侵偵測系統 (IPS/IDS)。這符合共同的責任模型，這會劃分您與雲端提供者之間的安全責任。

透過父系存取網際網路 AWS 區域

在此選項中，Outpost 中的工作負載會透過服務連結和父系中的網際網路閘道存取網際網路 AWS 區域。網際網路的傳出流量可以透過 VPC 中執行個體化的 NAT 閘道路由。為了提高輸入和輸出流量的安全性，您可以在 中使用 AWS 安全服務 AWS WAF，例如 AWS Shield和 Amazon CloudFront AWS 區域。

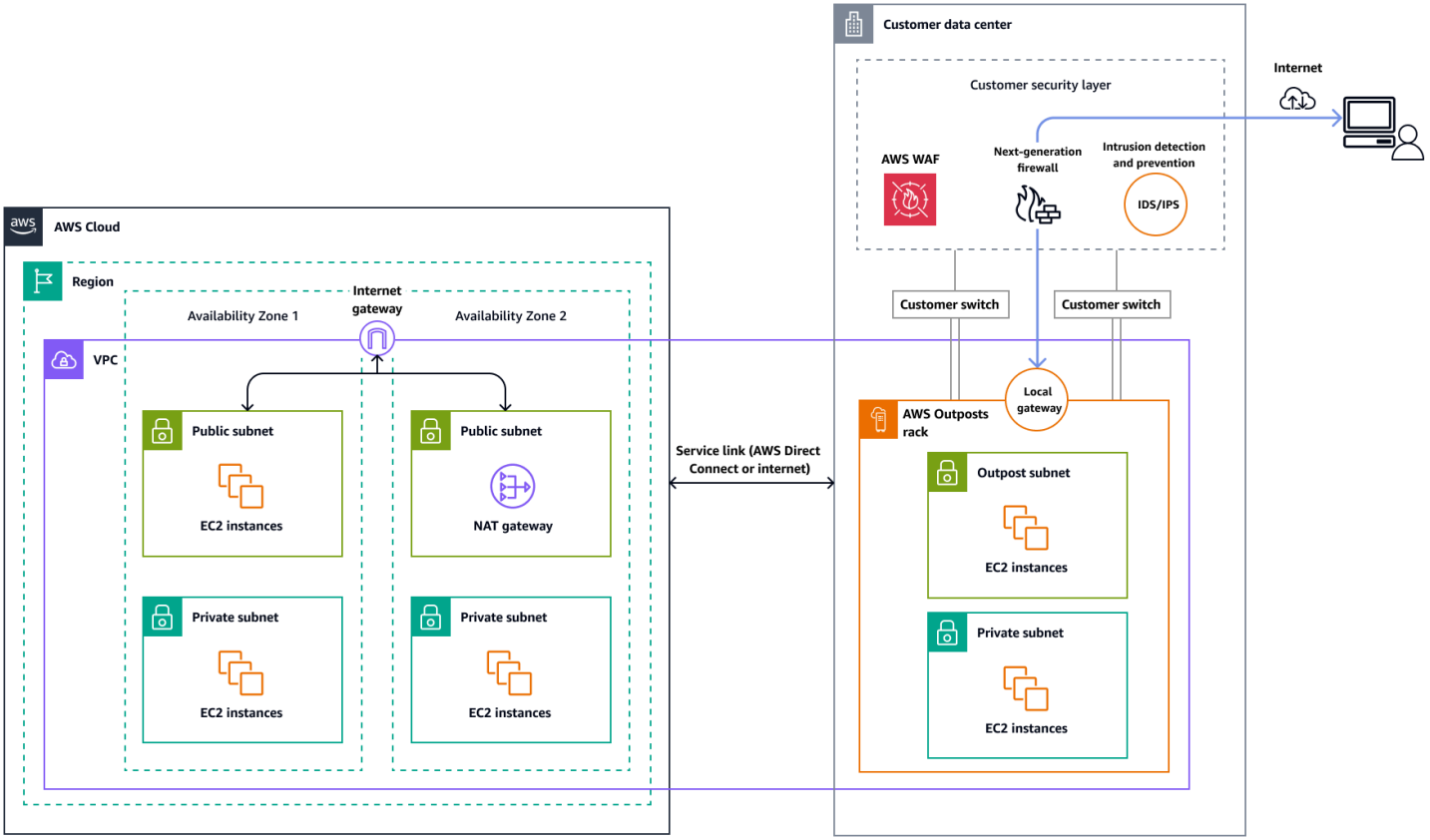
下圖顯示 AWS Outposts 執行個體中的工作負載與透過父系的網際網路之間的流量 AWS 區域。



透過您本機資料中心的網路進行網際網路存取

在此選項中，Outpost 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您本機網際網路的存在點周遊，並在本機輸出。在這種情況下，您本機資料中心的網路安全基礎設施負責保護 AWS Outposts 工作負載流量。

下圖顯示 AWS Outposts 子網路中的工作負載與網際網路之間經過資料中心的流量。



基礎設施控管

無論您的工作負載部署在 AWS 區域、Local Zone 或 Outpost 中，您都可以使用 AWS Control Tower 進行基礎設施控管。 AWS Control Tower 提供簡單的方法來設定和管理 AWS 多帳戶環境，遵循規範最佳實務。 AWS Control Tower 會協調數個其他 的功能 AWS Organizations， AWS 服務包括 和 IAM Identity Center （請參閱所有整合服務) AWS Service Catalog，以在不到一小時的時間內建置登陸區域。資源會代表您設定和管理。

AWS Control Tower 提供跨所有 AWS 環境的統一控管，包括區域、本地區域 （低延遲延伸） 和 Outposts （內部部署基礎設施）。這有助於確保整個混合雲端架構的安全性和合規性一致。如需詳細資訊，請參閱 AWS Control Tower 文件。

您可以設定 AWS Control Tower 和 功能，例如護欄，以符合政府和金融服務機構 (FSIs) 等受監管產業的資料駐留要求。若要了解如何在邊緣部署資料駐留的護欄，請參閱以下內容：

- AWS Local Zones 使用登陸區域控制在 中管理資料駐留的最佳實務 (AWS 部落格文章）
- 使用 AWS Outposts 機架和登陸區域護欄建立資料駐留的架構 (AWS 部落格文章）
- Hybrid Cloud Services Lens 的資料常駐性 (AWS Well-Architected Framework 文件）

共用 Outpost 資源

由於 Outpost 是位於資料中心或主機代管空間中的有限基礎設施，為了集中管理 AWS Outposts，您需要集中控制要共用哪些帳戶 AWS Outposts 資源。

透過 Outpost 共用，Outpost 擁有者可以與同一組織中 AWS 帳戶 的其他 共用其 Outpost 和 Outpost 資源，包括 Outpost 網站和子網路 AWS Organizations。身為 Outpost 擁有者，您可以從中央位置建立和管理 Outpost 資源，並在 AWS 帳戶 AWS 組織內的多個 之間共用資源。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。

中的可共用資源 AWS Outposts 包括：

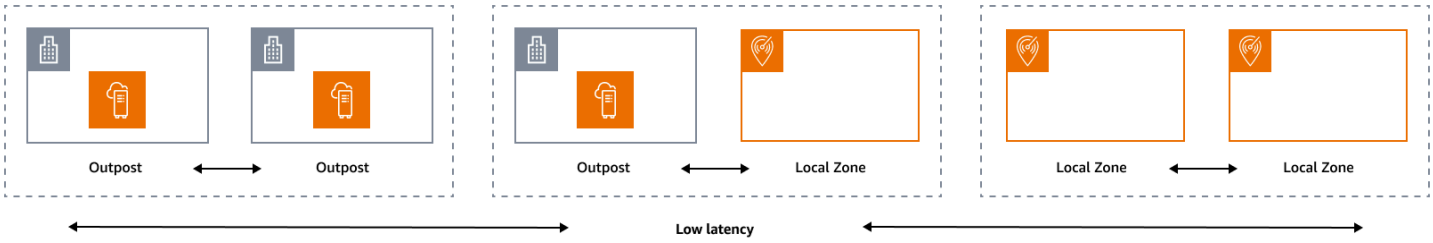
- 配置的專用主機
- 容量保留
- 客戶擁有的 IP (CoIP) 地址集區
- 本機閘道路由表
- Outpost
- Amazon S3 on Outposts
- 網站
- 子網路

若要遵循在多帳戶環境中共用 Outposts 資源的最佳實務，請參閱下列 AWS 部落格文章：

- AWS Outposts 在多帳戶 AWS 環境中共用：第 1 部分
- AWS Outposts 在多帳戶 AWS 環境中共用：第 2 部分

邊緣的彈性

可靠性支柱包含工作負載在預期情況下正確且一致地執行其預期功能的能力。這包括在整個工作負載生命週期中操作和測試工作負載的能力。在此意義上，當您在邊緣設計彈性架構時，您必須先考慮要使用哪些基礎設施來部署該架構。使用 AWS Local Zones 和 實作三種可能的組合 AWS Outposts：Outpost 到 Outpost、Outpost 到 Local Zone 和 Local Zone 到 Local Zone，如下圖所示。雖然彈性架構還有其他可能性，例如將 AWS 邊緣服務與傳統的現場部署基礎設施或 結合 AWS 區域，但本指南著重於這三種適用於混合式雲端服務設計的組合



基礎架構考量因素

在 AWS，服務設計的核心原則之一是避免基礎實體基礎設施中的單點故障。由於此原則， AWS 軟體和系統使用多個可用區域，並對單一區域的故障具有彈性。在邊緣， AWS 提供以 Local Zones 和 Outposts 為基礎的基礎設施。因此，確保基礎設施設計彈性的關鍵因素是定義應用程式資源的部署位置。

本機區域

Local Zones 的作用類似於其內的可用區域 AWS 區域，因為它們可以選取為區域 AWS 資源的置放位置，例如子網路和 EC2 執行個體。不過，它們不位於目前 AWS 區域 不存在的 AWS 區域，但接近大型人口、工業和 IT 中心。儘管如此，它們仍會保留本機區域中本機工作負載與在 中執行之工作負載之間的高頻寬、安全連線 AWS 區域。因此，您應該使用 Local Zones 來部署更接近使用者的工作負載，以滿足低延遲需求。

Outpost

AWS Outposts 是一種全受管服務，可將 AWS 基礎設施、 AWS 服務、APIs 和工具擴展到您的資料中心。用於 的相同硬體基礎設施 AWS 雲端 會安裝在您的資料中心。Outpost 接著會連接到最近的 AWS 區域。您可以使用 Outposts 來支援低延遲或本機資料處理需求的工作負載。

父可用區域

每個 Local Zone 或 Outpost 都有一個父區域 （ 也稱為主區域)。父區域是 AWS 節點基礎設施 (Outpost 或 Local Zone) 的控制平面錨定位置。如果是 Local Zones，父區域是 Local Zone 的基本架構元件，客戶無法修改。 會將 AWS Outposts 延伸 AWS 雲端 到您的內部部署環境，因此您必須在訂購程序期間選取特定區域和可用區域。此選項會將 Outpost 部署的控制平面錨定至所選的 AWS 基礎設施。

當您在邊緣開發高可用性架構時，這些基礎設施的父區域，例如 Outpost 或 Local Zones，必須相同，以便在它們之間延伸 VPC。此延伸 VPC 是建立這些高可用性架構的基礎。當您定義高彈性架構時，這就是為什麼您必須驗證服務將錨定 （ 或已錨定 ） 的父區域和可用區域。如下圖所示，如果您想要在兩

個 Outpost 之間部署高可用性解決方案，您必須選擇兩個不同的可用區域來錨定 Outpost。這允許從控制平面角度進行異地同步備份架構。如果您想要部署包含一或多個 Local Zones 的高可用性解決方案，您必須先驗證基礎設施錨定所在的父可用區域。為此，請使用下列 AWS CLI 命令：

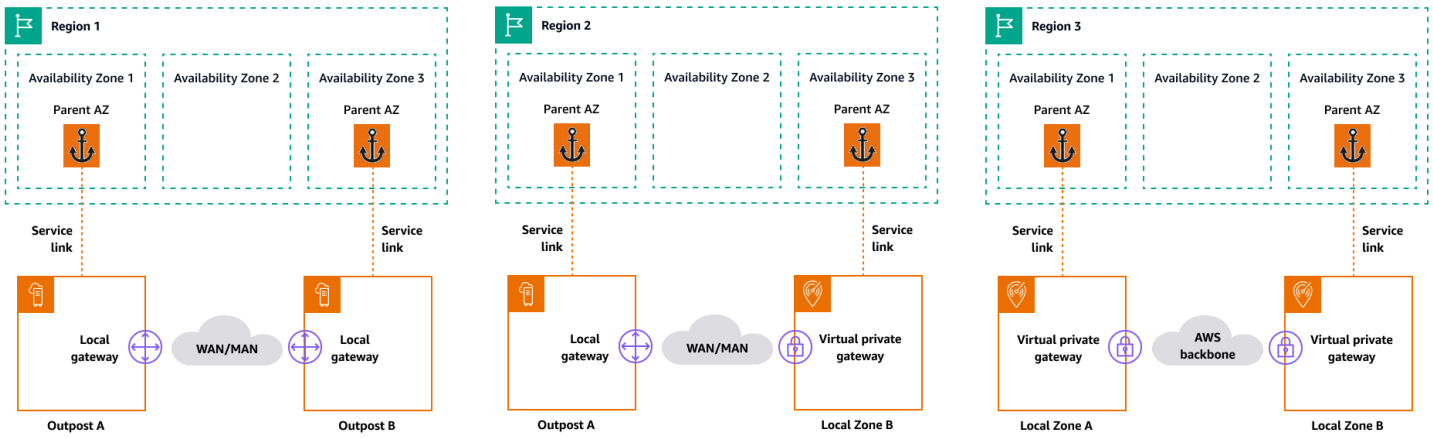
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

上一個命令的輸出：

```
{     "AvailabilityZones": [
          {
              "State": "available",
              "OptInStatus": "opted-in",
              "Messages": [],
              "RegionName": "us-east-1",
              "ZoneName": "us-east-1-mia-1a",
              "ZoneId": "use1-mia1-az1",
              "GroupName": "us-east-1-mia-1",
              "NetworkBorderGroup": "us-east-1-mia-1",
              "ZoneType": "local-zone",
              "ParentZoneName": "us-east-1d",
              "ParentZoneId": "use1-az2"
          }
      ]
 }
```

在此範例中，邁阿密本地區域 (us-east-1d-mia-1a1) 錨定在us-east-1d-az2 可用區域中。因此，如果您需要在邊緣建立彈性架構，您必須確保次要基礎設施 (Outpost 或 Local Zones) 錨定至 以外的可用區域us-east-1d-az2。例如， us-east-1d-az1是有效的。

下圖提供高可用性邊緣基礎設施的範例。



網路考量事項

本節討論在邊緣聯網的初始考量，主要用於存取邊緣基礎設施的連線。它會檢閱為服務連結提供彈性網路的有效架構。

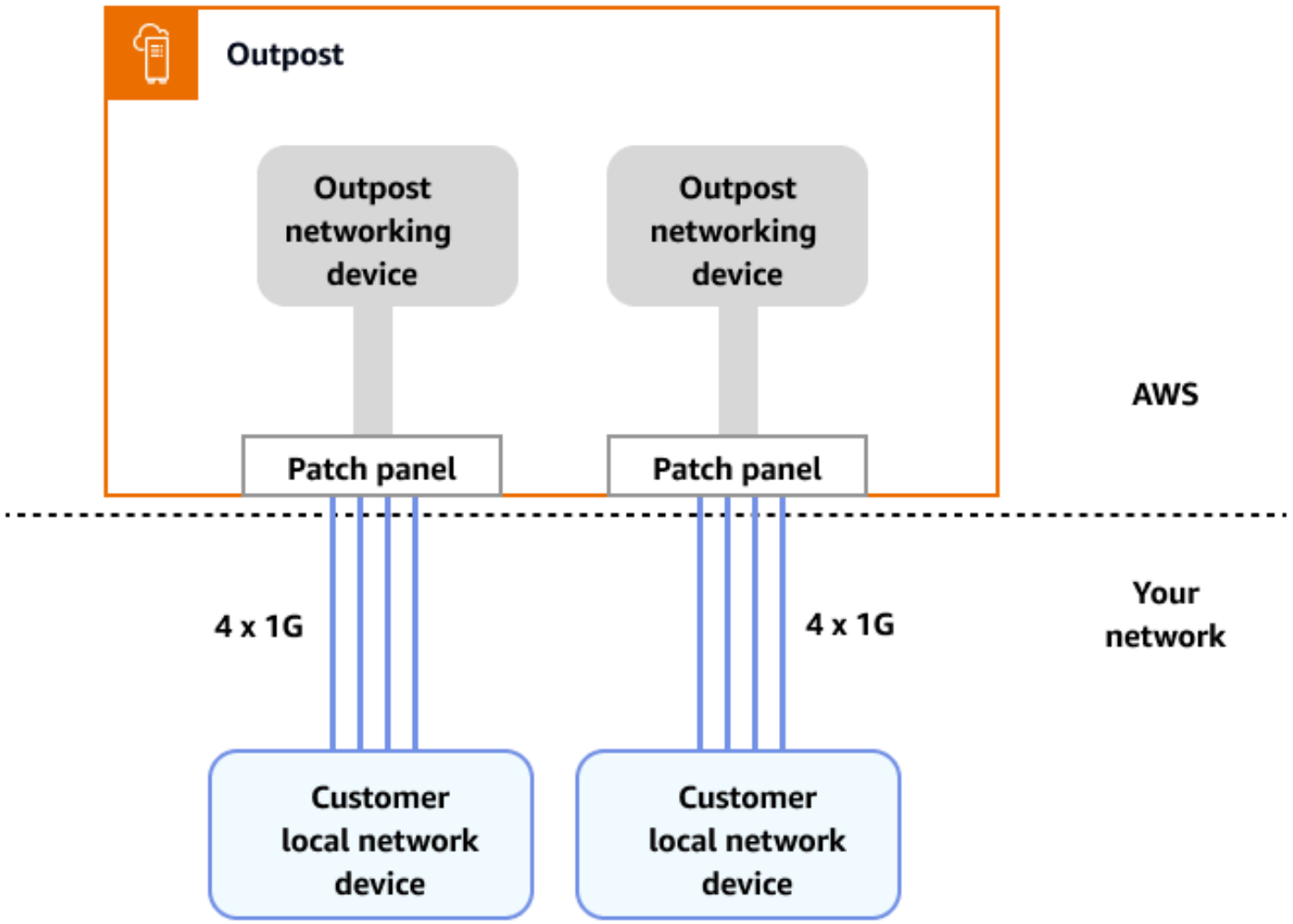
Local Zones 的彈性聯網

本機區域透過多個備援、安全、高速的連結連接到父區域，可讓您順暢地使用任何區域服務，例如 Amazon S3 和 Amazon RDS。您有責任提供從現場部署環境或使用者到 Local Zone 的連線。無論您選擇何種連線架構 （ 例如 VPN 或 Direct Connect)，都必須透過網路連結達到的延遲必須相等，以避免主要連結發生故障時對應用程式效能造成任何影響。如果您使用的是 Direct Connect，則適用的彈性架構與存取 的架構相同 AWS 區域，如Direct Connect 彈性建議中所述。不過，有些案例主要適用於國際本地區域。在啟用 Local Zone 的國家/地區中，只有單一 Direct Connect PoP 就無法建立建議 Direct Connect 用於恢復能力的架構。如果您只能存取單一 Direct Connect 位置，或需要單一連線以外的彈性，您可以在 Amazon EC2 上建立 VPN 設備 Direct Connect，如 AWS 部落格文章所述和討論啟用從內部部署到 的高可用性連線 AWS Local Zones。

Outposts 的彈性聯網

與 Local Zones 不同，Outposts 具有備援連線，可從本機網路存取 Outposts 中部署的工作負載。此備援是透過兩個 Outposts 網路裝置 (ONDs) 達成。每個 OND 至少需要兩個與本機網路 1 Gbps、10 Gbps、40 Gbps 或 100 Gbps 的光纖連線。這些連線必須設定為連結彙總群組 (LAG)，以允許可擴展性新增更多連結。

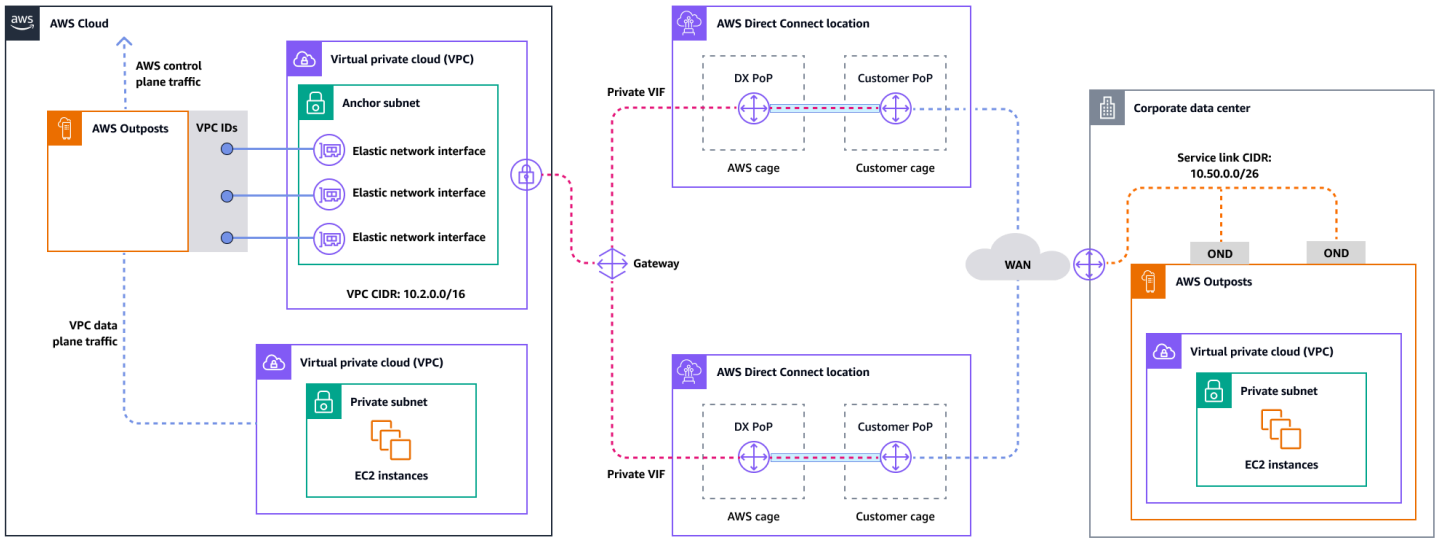
上行鏈路速度	上行鏈路數目
1 Gbps	1、2、4、6 或 8
10 Gbps	1、2、4、8、12 或 16
40 或 100 Gbps	1、2 或 4



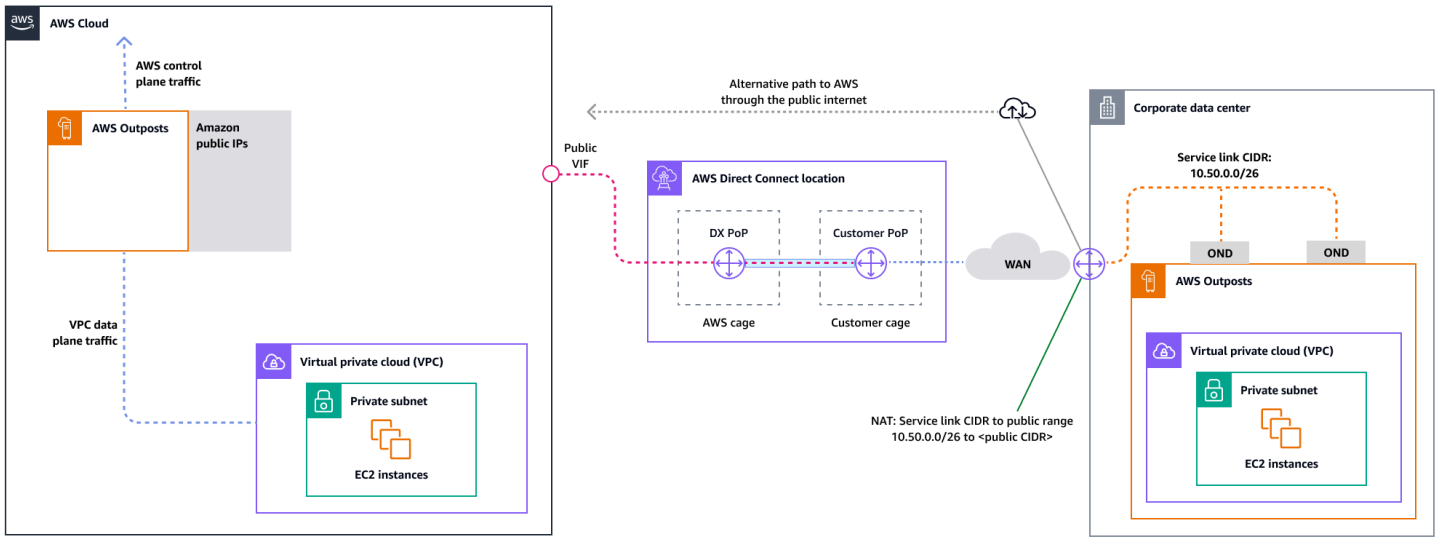
如需此連線的詳細資訊，請參閱 AWS Outposts 文件中的 Outposts 機架的本機網路連線。

為了獲得最佳體驗和彈性， AWS建議您使用至少 500 Mbps (1 Gbps 更好） 的備援連線來連接 的服務連結 AWS 區域。您可以使用 Direct Connect 或 服務連結的網際網路連線。此最小值可讓您啟動 EC2 執行個體、連接 EBS 磁碟區和存取 AWS 服務，例如 Amazon EKS、Amazon EMR 和 CloudWatch 指標。

下圖說明高可用私有連線的此架構。



下圖說明高可用公有連線的此架構。

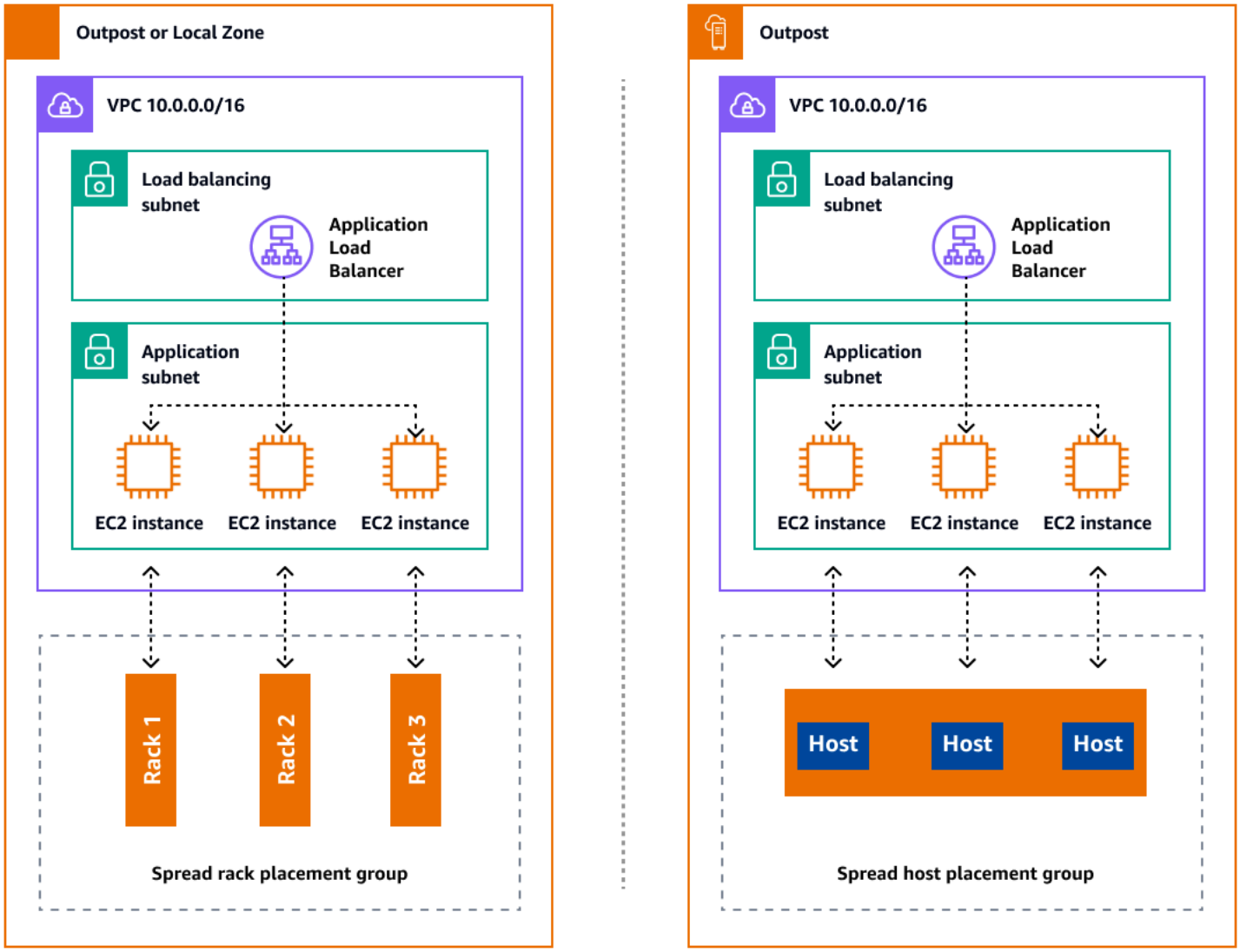


使用 ACE 機架擴展 Outposts 機架部署

彙總、核心、邊緣 (ACE) 機架是 AWS Outposts 多機架部署的關鍵彙總點，主要建議用於超過三個機架的安裝或規劃未來擴展。每個 ACE 機架都有四個路由器，支援 10 Gbps、40 Gbps 和 100 Gbps 連線 (100 Gbps 為最佳）。每個機架最多可以連接到四個上游客戶裝置，以實現最大備援。ACE 機架會耗用高達 10 kVA 的電力，且重量高達 705 磅。主要優點包括降低實體聯網需求、減少光纖纜線上行連結，以及減少 VLAN 虛擬介面。 透過 VPN 通道的遙測資料 AWS 監控這些機架，並在安裝期間與客戶緊密合作，以確保適當的電源可用性、網路組態和最佳配置。隨著部署的擴展，ACE 機架架構提供更高的價值，並有效簡化連線，同時降低大型安裝的複雜性和實體連接埠需求。 如需詳細資訊，請參閱 AWS 部落格文章使用 ACE AWS Outposts 機架擴展機架部署。

將執行個體分散到 Outpost 和本機區域

Outpost 和 Local Zones 的運算伺服器數量有限。如果您的應用程式部署多個相關執行個體，這些執行個體可能會在相同伺服器或相同機架的伺服器上部署，除非設定不同。除了預設選項之外，您還可以跨伺服器分配執行個體 ，以降低在相同基礎設施上執行相關執行個體的風險。您也可以使用分割區置放群組，將執行個體分散到多個機架。這稱為分散機架分佈模型。使用自動分佈將執行個體分散到群組中的分割區，或將執行個體部署到選取的目標分割區。透過將執行個體部署到目標分割區，您可以將選取的資源部署到相同的機架，同時將其他資源分散到機架。Outposts 也提供另一個稱為分散主機的選項，可讓您在主機層級分配工作負載。下圖顯示分散機架和分散主機分佈選項。



中的 Amazon RDS 多可用區 AWS Outposts

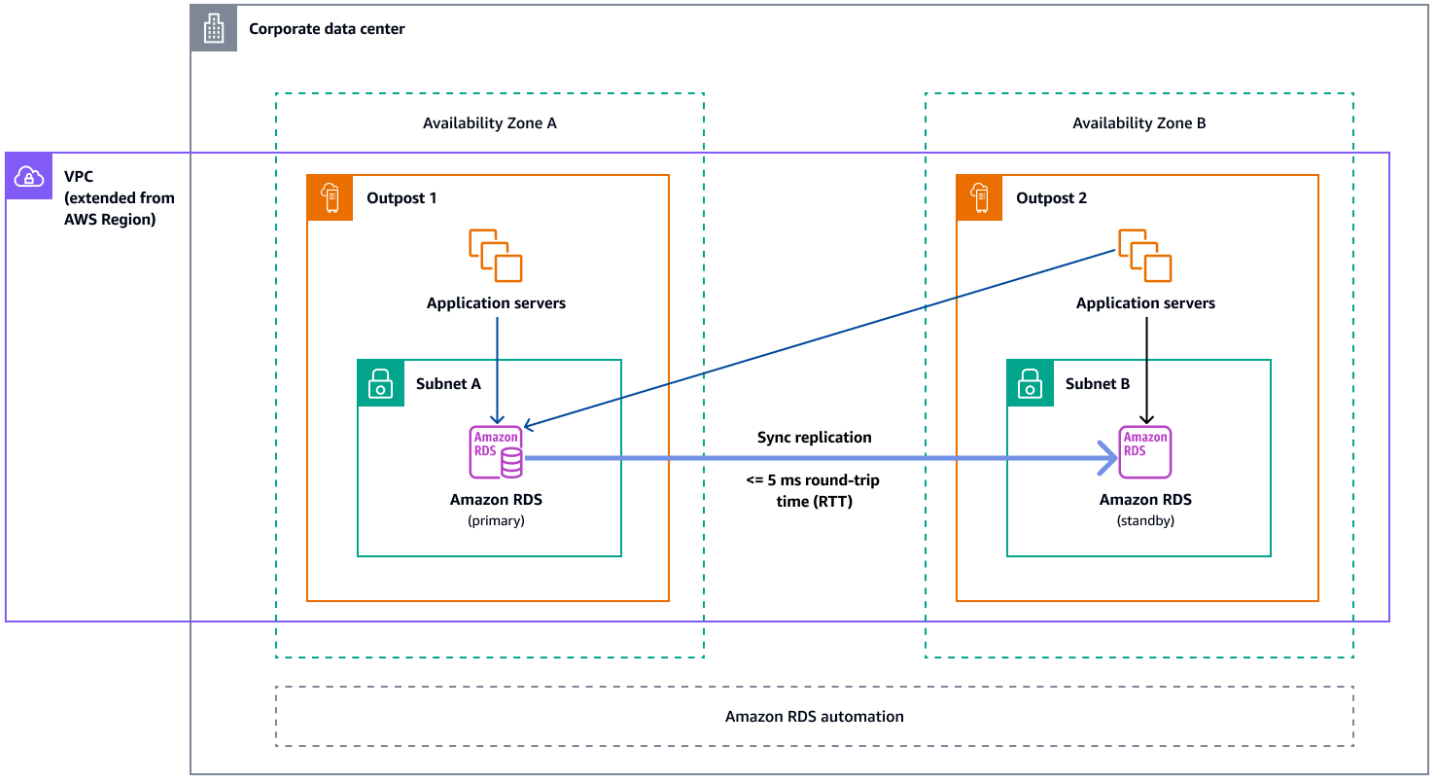
當您在 Outposts 上使用異地同步備份執行個體部署時，Amazon RDS 會跨兩個 Outposts 建立兩個資料庫執行個體。每個 Outpost 都會在自己的實體基礎設施上執行，並連線到區域中的不同可用區域，

以獲得高可用性。當透過客戶管理的本機連線連接兩個 Outpost 時，Amazon RDS 會管理主要和待命資料庫執行個體之間的同步複寫。如果發生軟體或基礎設施故障，Amazon RDS 會自動將待命執行個體提升為主要角色，並更新 DNS 記錄以指向新的主要執行個體。若為異地同步備份部署，Amazon RDS 會在一個 Outpost上建立主要資料庫執行個體，並將資料同步複製至不同 Outpost 上的備用資料庫執行個體。Outposts 上的異地同步備份部署的運作方式與 中的異地同步備份部署類似 AWS 區域，但有以下差異：

- 其需要在兩個或多個 Outpost 之間建立本機連線。
- 它們需要客戶擁有的 IP (CoIP) 地址集區。如需詳細資訊，請參閱 Amazon RDS 文件中的 上的 Amazon RDS 客戶擁有 IP 地址 AWS Outposts。
- 在您的本機網路上執行複寫。

異地同步備份部署適用於所有支援的 MySQL 和 PostgreSQL on Amazon RDS on Outposts 版本。異地同步備份部署不支援本機備份。

下圖顯示 Amazon RDS on Outposts 異地同步備份組態的架構。

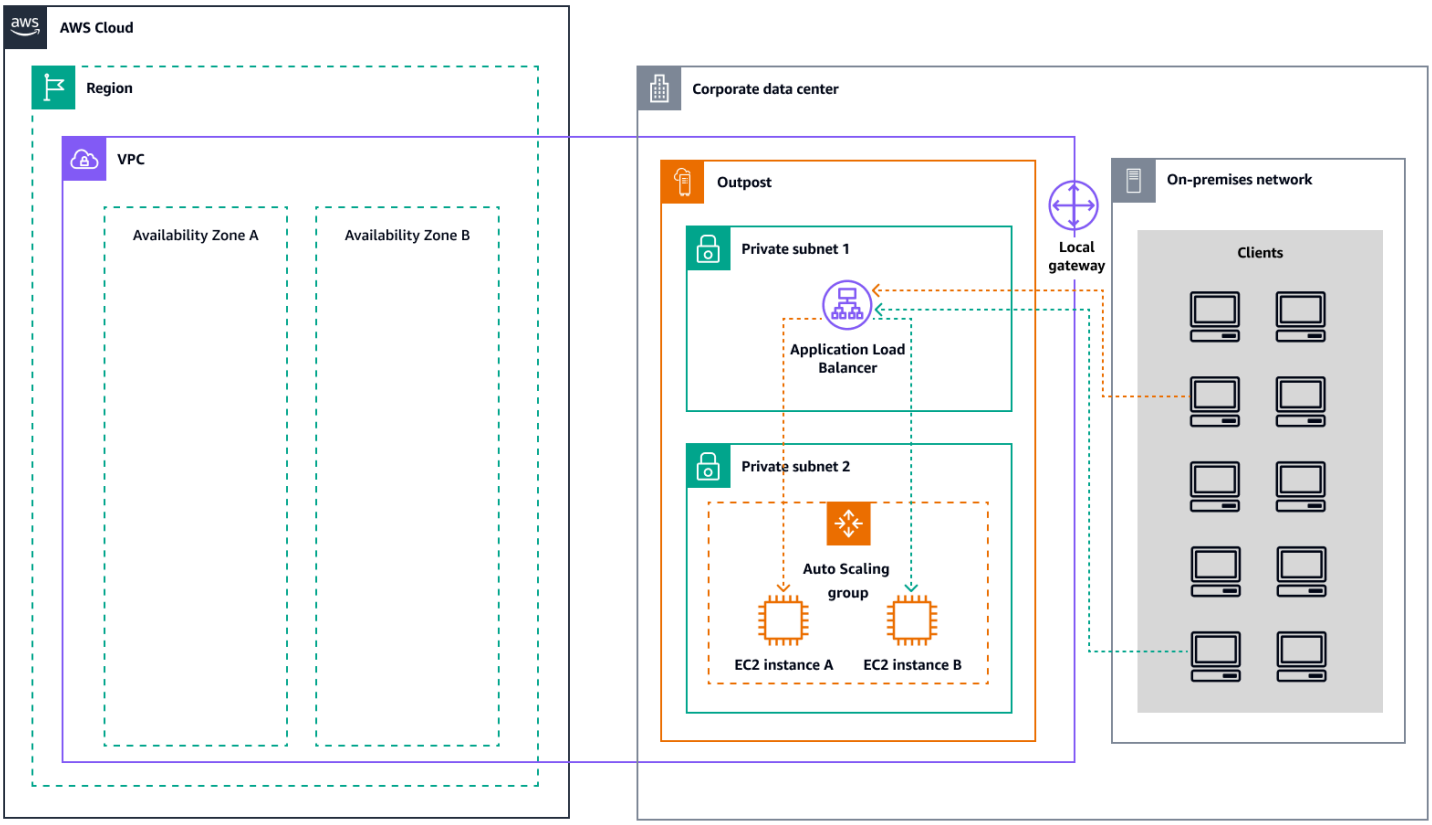


容錯移轉機制

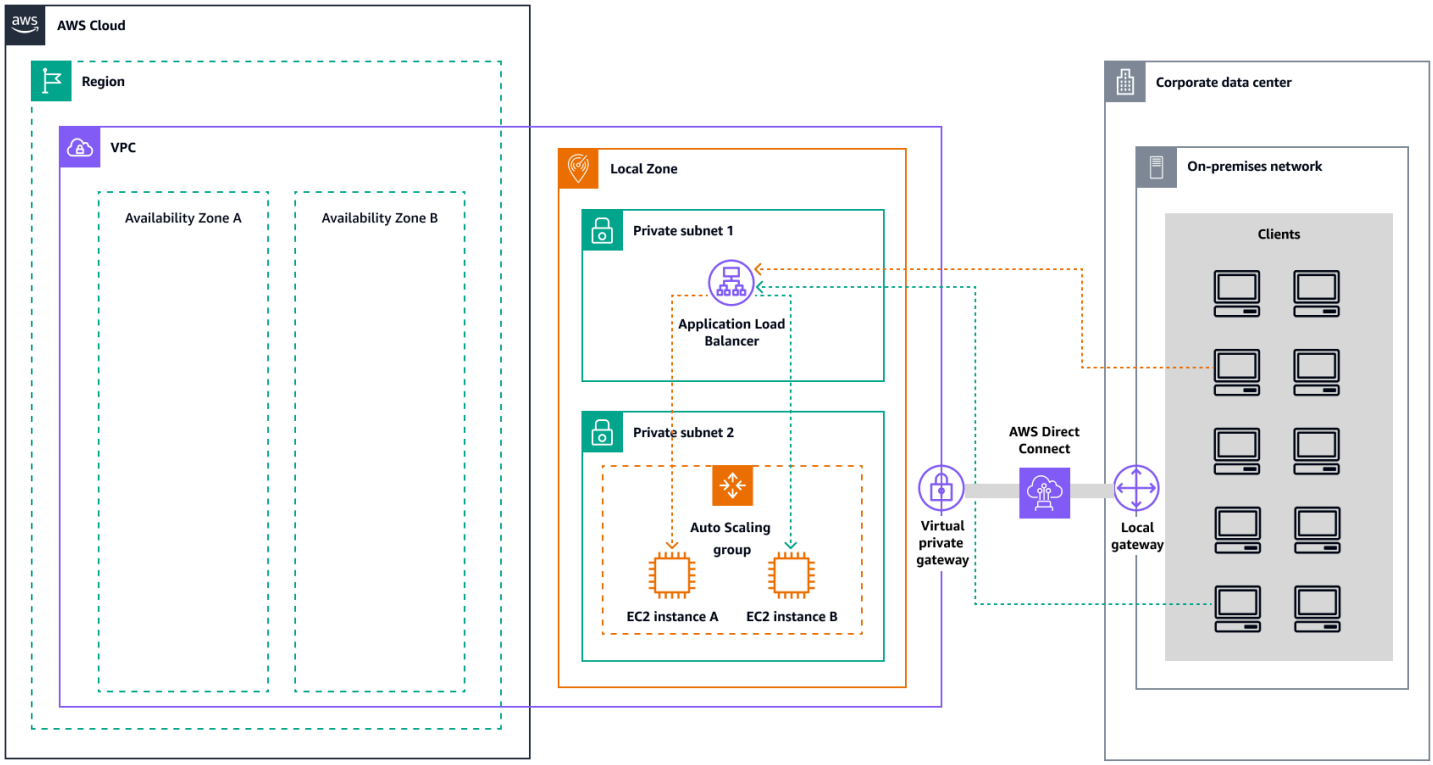
負載平衡和自動擴展

Elastic Load Balancing (ELB) 會自動將傳入的應用程式流量分配到您正在執行的所有 EC2 執行個體。ELB 透過最佳路由流量來協助管理傳入請求，讓單一執行個體不會不堪負荷。若要搭配 Amazon EC2 Auto Scaling 群組使用 ELB，請將負載平衡器連接至 Auto Scaling 群組。這樣會將群組註冊到負載平衡器，該負載平衡器會作為 群組所有 Web 流量的單一聯絡點。當您搭配 Auto Scaling 群組使用 ELB 時，不需要向負載平衡器註冊個別 EC2 執行個體。由 Auto Scaling 群組啟動的執行個體會自動註冊到負載平衡器。同樣地，由 Auto Scaling 群組終止的執行個體會自動從負載平衡器取消註冊。將負載平衡器連接到 Auto Scaling 群組之後，您可以將群組設定為使用 ELB 指標 （例如每個目標的 Application Load Balancer 請求計數），以隨著需求波動擴展群組中的執行個體數量。或者，您可以將 ELB 運作狀態檢查新增至 Auto Scaling 群組，以便 Amazon EC2 Auto Scaling 可以根據這些運作狀態檢查來識別和取代運作狀態不佳的執行個體。您也可以建立 Amazon CloudWatch 警示，在目標群組的運作狀態良好主機計數低於允許值時通知您。

下圖說明 Application Load Balancer 如何在 中管理 Amazon EC2 上的工作負載 AWS Outposts。



下圖說明 Amazon EC2 在 Local Zones 中的類似架構。

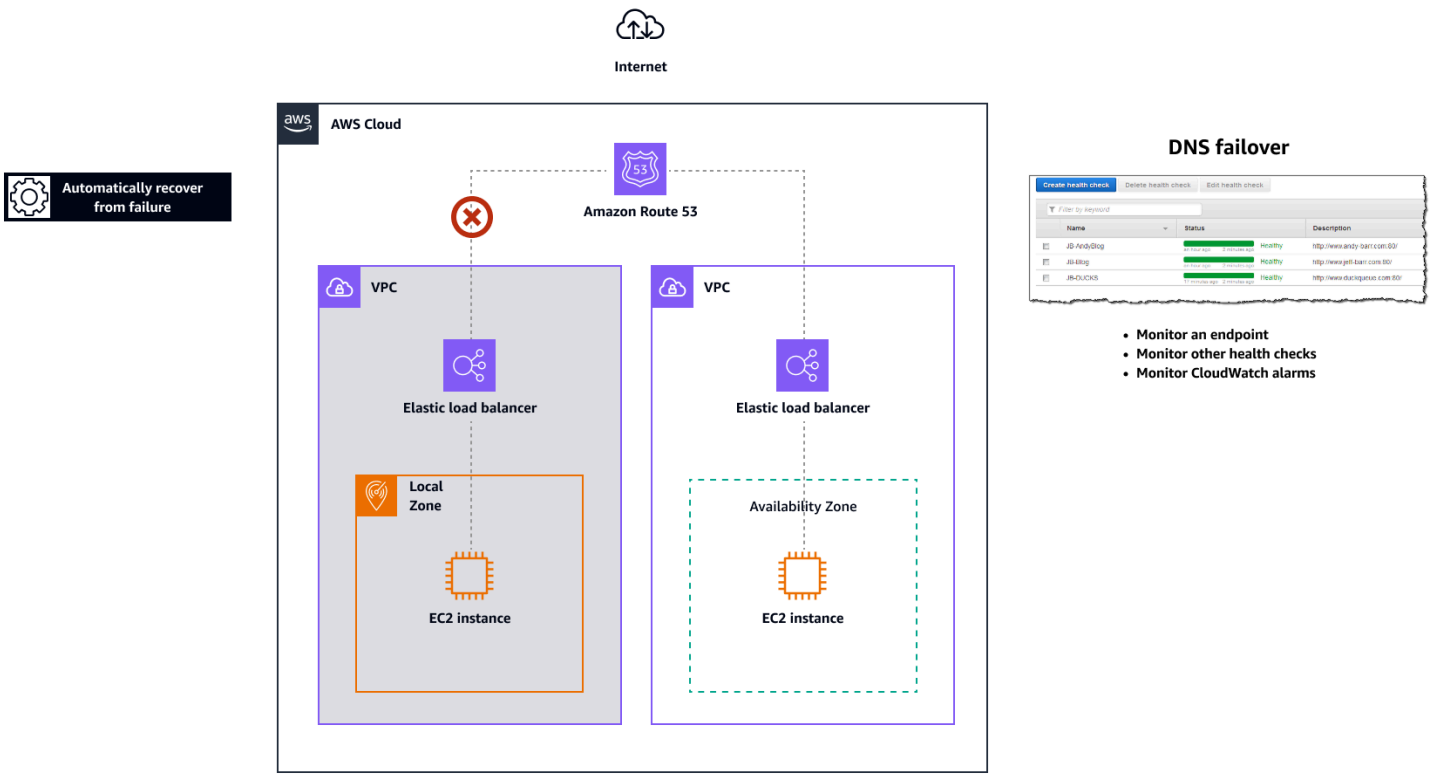


> **Note**
>
> Application Load Balancer 可在 AWS Outposts 和 Local Zones 中使用。不過，若要在 中使用 Application Load Balancer AWS Outposts，您需要調整 Amazon EC2 容量的大小，以提供負載平衡器所需的可擴展性。如需在 中調整負載平衡器大小的詳細資訊 AWS Outposts，請參閱 AWS 部落格文章在 上設定 Application Load Balancer AWS Outposts。

DNS 容錯移轉的 Amazon Route 53

當您有一個以上的資源執行相同的函數時，例如多個 HTTP 或郵件伺服器，您可以設定 Amazon Route 53 來檢查資源的運作狀態，並僅使用運作狀態良好的資源來回應 DNS 查詢。例如，假設您的網站 `example.com`託管在兩個伺服器上。一個伺服器位於 Local Zone，另一個伺服器位於 Outpost。您可以設定 Route 53 來檢查這些伺服器的運作狀態，並`example.com`僅使用目前運作狀態良好的伺服器來回應 的 DNS 查詢。如果您使用別名記錄將流量路由到選取的 AWS 資源，例如 ELB 負載平衡器，您可以設定 Route 53 來評估資源的運作狀態，並僅將流量路由到運作狀態良好的資源。當您設定別名記錄以評估資源的運作狀態時，您不需要為該資源建立運作狀態檢查。

下圖說明 Route 53 容錯移轉機制。



備註

- 如果您要在私有託管區域中建立容錯移轉記錄，您可以建立 CloudWatch 指標、將警示與指標建立關聯，然後建立以警示資料串流為基礎的運作狀態檢查。
- 若要 AWS Outposts 使用 Application Load Balancer 在 中公開存取應用程式，請設定聯網組態，讓目的地網路位址轉譯 (DNAT) 從公有 IPs 轉換為負載平衡器的完整網域名稱 (FQDN)，並建立 Route 53 容錯移轉規則，其中包含指向公開公有 IP 的運作狀態檢查。此組合可確保對 Outposts 託管應用程式的可靠公開存取。

Amazon Route 53 Resolver 上的 AWS Outposts

Amazon Route 53 Resolver 可在 Outposts 機架上使用。它直接從 Outposts 為您的內部部署服務和應用程式提供本機 DNS 解析。Local Route 53 Resolver 端點也啟用 Outposts 與內部部署 DNS 伺服器之間的 DNS 解析。Route 53 Resolver on Outposts 有助於改善現場部署應用程式的可用性和效能。

Outposts 的典型使用案例之一是部署需要低延遲存取內部部署系統的應用程式，例如工廠設備、高頻率交易應用程式和醫療診斷系統。

當您選擇在 Outposts 上使用本機 Route 53 解析程式時，應用程式和服務將繼續受益於本機 DNS 解析，以探索其他服務，即使與父系的連線 AWS 區域 中斷。本機解析程式也有助於減少 DNS 解析的延遲，因為查詢結果會從 Outposts 在本機快取和提供，這樣可消除對父系不必要的往返 AWS 區域。使用私有 DNS 的 Outposts VPCs中應用程式的所有 DNS 解析都會在本機提供。 https://docs.aws.amazon.com/managedservices/latest/userguide/set-dns.html

除了啟用本機解析程式之外，此啟動也會啟用本機解析程式端點。Route 53 Resolver 傳出端點可讓 Route 53 Resolvers 將 DNS 查詢轉送至您管理的 DNS 解析程式，例如，在內部部署網路上。相反地，Route 53 Resolver 傳入端點會將他們從 VPC 外部收到的 DNS 查詢轉送到在 Outposts 上執行的 Resolver。它可讓您從該 VPC 外部，針對部署在私有 Outposts VPC 上的服務傳送 DNS 查詢。如需傳入和傳出端點的詳細資訊，請參閱 Route 53 文件中的解決 VPCs 與網路之間的 DNS 查詢。

邊緣的容量規劃

容量規劃階段涉及收集 vCPU、記憶體和儲存需求，以部署您的架構。在 AWS Well-Architected Framework 的成本最佳化支柱中，適當調整規模是從規劃開始的持續程序。您可以使用 AWS 工具，根據其中的資源使用量來定義最佳化 AWS。

Local Zones 中的邊緣容量規劃與 中的相同 AWS 區域。您應該檢查以確定您的執行個體在每個 Local Zone 中可用，因為某些執行個體類型可能與 中的類型不同 AWS 區域。對於 Outpost，您應該根據您的工作負載需求來規劃容量。Outpost 具有每個主機固定數量的執行個體，可視需要重新繪製。如果您的工作負載需要備用容量，請在規劃容量需求時將其納入考量。

Outpost 上的容量規劃

AWS Outposts 容量規劃需要區域適當大小的特定輸入，以及會影響應用程式可用性、效能和成長的邊緣特定因素。如需詳細指引，請參閱白皮書AWS Outposts 高可用性設計和架構考量中的 AWS 容量規劃。

本機區域的容量規劃

Local Zone 是 的延伸 AWS 區域 ，地理位置接近您的使用者。在 Local Zone 中建立的資源可以為本機使用者提供極低延遲的通訊。若要在您的 中啟用本機區域 AWS 帳戶，請檢閱 AWS 文件中的 入門 AWS Local Zones。每個 Local Zone 都有不同的插槽可供 EC2 執行個體系列使用。在使用前，驗證每個 Local Zone 中可用的執行個體。若要確認可用的 EC2 執行個體，請執行下列 AWS CLI 命令：

```
aws ec2 describe-instance-type-offerings \
--location-type "availability-zone" \
```

```
--filters Name=location,Values=<local-zone-name>
```

預期的輸出結果：

```
{
  "InstanceTypeOfferings": [
      {
          "InstanceType": "m5.2xlarge",
          "LocationType": "availability-zone",
          "Location": "<local-zone-name>"
      },
      {
          "InstanceType": "t3.micro",
          "LocationType": "availability-zone",
          "Location": "local.zone-name"
      },
      ...
  ]
}
```

邊緣基礎設施管理

AWS 提供全受管服務，可將 AWS 基礎設施、服務、APIs和工具延伸到更接近最終使用者和資料中心的位置。Outpost 和 Local Zones 中可用的服務與 中可用的服務相同 AWS 區域，因此您可以使用相同的 AWS 主控台 AWS CLI或 AWS APIs來管理這些服務。如需支援的服務，請參閱AWS Outposts 功能比較表和AWS Local Zones 功能。

在邊緣部署服務

您可以在 Local Zones 和 Outposts 中設定可用的服務，方法與在 中設定服務的方式相同 AWS 區域：使用 AWS 主控台 AWS CLI或 AWS APIs。區域和邊緣部署的主要差異是佈建資源的子網路。節點的聯網部分描述了如何在 Outposts 和 Local Zones 中部署子網路。識別邊緣子網路之後，您可以使用邊緣子網路 ID 做為參數，在 Outposts 或 Local Zones 中部署服務。下列各節提供部署邊緣服務的範例。

邊緣的 Amazon EC2

下列`run-instances`範例會在目前區域的邊緣子網路`m5.2xlarge`中啟動 類型的單一執行個體。如果您不打算使用 Linux 上的 SSH 或 Windows 上的遠端桌面通訊協定 (RDP) 連線到執行個體，則金鑰對是選用的。

```
aws ec2 run-instances \
    --image-id ami-id \
    --instance-type m5.2xlarge \
    --subnet-id <subnet-edge-id> \
    --key-name MyKeyPair
```

邊緣的 Application Load Balancer

下列`create-load-balancer`範例會建立內部 Application Load Balancer，並啟用指定子網路的 Local Zones 或 Outposts。

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internal \
    --subnets <subnet-edge-id>
```

若要將面向網際網路的 Application Load Balancer 部署到 Outpost 上的子網路，請在 `--scheme`選項中設定 `internet-facing`旗標並提供 CoIP 集區 ID，如本範例所示：

```
aws elbv2 create-load-balancer \
    --name my-internal-load-balancer \
    --scheme internet-facing \
    --customer-owned-ipv4-pool <coip-pool-id>
    --subnets <subnet-edge-id>
```

如需有關在邊緣部署其他 服務的資訊，請遵循下列連結：

服務	AWS Outposts	AWS Local Zones
Amazon EKS	使用 部署 Amazon EKS 內部部署 AWS Outposts	使用 啟動低延遲 EKS 叢集 AWS Local Zones
Amazon ECS	上的 Amazon ECS AWS Outposts	共用子網路、本機區域和 Wavelength 區域中的 Amazon ECS 應用程式
Amazon RDS	上的 Amazon RDS AWS Outposts	選取本機區域子網路

服務	AWS Outposts	AWS Local Zones
Amazon S3	Amazon S3 on Outposts 入門	無
Amazon ElastiCache	搭配 ElastiCache 使用 Outpost	搭配 ElastiCache 使用本機區域
Amazon EMR	上的 EMR 叢集 AWS Outposts	上的 EMR 叢集 AWS Local Zones
Amazon FSx	無	選取本機區域子網路
AWS 彈性災難復原	使用 AWS 彈性災難復原 和 AWS Outposts	不適用
AWS Transform MGN	不適用	選取 Local Zone 子網路做為預備子網路

Outposts 特定的 CLI 和 SDK

AWS Outposts 有兩個命令和 APIs 群組，用於建立服務訂單或操作本機閘道和本機網路之間的路由表。

Outposts 訂購程序

您可以使用 AWS CLI或 Outposts APIs 來建立 Outposts 網站、建立 Outpost，以及建立 Outposts 訂單。我們建議您在 AWS Outposts 訂購過程中與混合雲端專家合作，以確保為您的實作需求適當選擇資源 IDs 和最佳組態。如需完整的資源 ID 清單，請參閱AWS Outposts 機架定價頁面。

本機閘道管理

Outposts 中本機閘道 (LGW) 的管理和操作需要了解適用於此任務的 AWS CLI 和 SDK 命令。您可以使用 AWS CLI 和 AWS SDKs 來建立和修改 LGW 路由，以及其他任務。如需管理 LGW 的詳細資訊，請參閱下列資源：

- AWS CLI 適用於 Amazon EC2 的
- 中的 EC2.Client 適用於 Python (Boto) 的 AWS SDK
- 中的 Ec2Client 適用於 Java 的 AWS SDK

CloudWatch 指標和日誌

對於可在 Outpost 和 Local Zones 中使用的 AWS 服務 ，指標和日誌的管理方式與區域相同。Amazon CloudWatch 提供指標，專用於監控下列維度的 Outpost：

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

如需詳細資訊，請參閱 Outposts 文件中的 Outposts 機架的 CloudWatch 指標。

資源

AWS 參考

- 使用 的混合雲端 AWS
- AWS Outposts Outposts 機架使用者指南
- AWS Local Zones 使用者指南
- AWS Outposts 系列
- AWS Local Zones
- 將 VPC 擴展至本機區域、Wavelength 區域或 Outpost (Amazon VPC 文件）
- Local Zones 中的 Linux 執行個體 (Amazon EC2 文件）
- Outposts 中的 Linux 執行個體 (Amazon EC2 文件）
- 開始使用 部署低延遲應用程式 AWS Local Zones（教學課程）

AWS 部落格文章

- 使用 Amazon EC2 在內部部署上執行 AWS 基礎設施
- 在 Amazon EC2 上使用 Amazon EKS 建置現代應用程式
- 如何在 Amazon EC2 機架上選擇 CoIP 和直接 VPC 路由模式
- 為您的 Amazon EC2 選取網路交換器
- 在 中維護資料的本機副本 AWS Local Zones
- Amazon EC2 上的 Amazon ECS
- 使用適用於 的 Amazon EKS 管理邊緣感知服務網格 AWS Local Zones
- 在 Amazon EC2 上部署本機閘道傳入路由
- 在 中自動化工作負載部署 AWS Local Zones
- 在多帳戶 AWS 環境中共用 Amazon EC2：第 1 部分
- 在多帳戶 AWS 環境中共用 Amazon EC2：第 2 部分
- AWS Direct Connect 和 AWS Local Zones 互通性模式
- 以多可用區域高可用性在 Amazon EC2 上部署 Amazon RDS

貢獻者

下列個人對本指南有所貢獻。

編寫

- Leonardo Solano，首席混合雲端解決方案架構師， AWS
- Len Gomes，合作夥伴解決方案架構師 AWS
- Matt Price，資深企業支援工程師， AWS
- Tom Gadomski，解決方案架構師 AWS
- Obed Gutierrez，解決方案架構師 AWS
- Dionysios Kakaletris，技術客戶經理 AWS
- Vamsi Krishna，首席 Outposts 專家， AWS

檢閱

- David Filiatrault， 交付顧問 AWS

技術寫入

- Handan Selamoglu，資深文件經理， AWS

文件歷史紀錄

下表描述了本指南的重大變更。如果您想收到有關未來更新的通知，可以訂閱 RSS 摘要。

變更	描述	日期
初次出版	—	2025 年 6 月 10 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。