AWS 白皮書

AWS Outposts 高可用性設計和架構考量

AWS Outposts 高可用性設計和架構考量: AWS 白皮書

Table of Contents

AWS Outposts 高可用性設計和架構考量

發佈日期：2021 年 8 月 12 日 (文件歷史紀錄)

本白皮書討論架構考量事項和建議實務，IT 管理員和系統架構師可以運用這些考量事項和建議實務來建置高可用性的內部部署應用程式環境 AWS Outposts。

您是 Well-Architected 嗎？

AWS Well-Architected Framework 可協助您了解在雲端建置系統時所做決策的優缺點。架構的六個支柱可讓您了解架構最佳實務，以設計和操作可靠、安全、高效、經濟實惠且永續的系統。使用 AWS Well-Architected Tool免費提供的 AWS Management Console，您可以透過回答每個支柱的一組問題，根據這些最佳實務來檢閱工作負載。

如需雲端架構的更多專家指導和最佳實務，請參閱AWS 架構中心，參考架構部署、圖表和白皮書。

簡介

此白皮書適用於希望使用 AWS 雲端平台部署、遷移和操作應用程式，並在具有AWS Outposts 機架的現場部署上執行這些應用程式，即 42U 機架形式因素的 IT 管理員和系統架構師AWS Outposts。

它介紹了架構模式、反模式和建議的實務，用於建置包含 AWS Outposts 機架的高可用性系統。您將了解如何管理您的 AWS Outposts 機架容量，並使用聯網和資料中心設施服務來設定高可用性的 AWS Outposts 機架基礎設施解決方案。

AWS Outposts 機架是一種全受管服務，可提供雲端運算、儲存和聯網功能的邏輯集區。使用 Outposts 機架，客戶可以在其內部部署環境中使用支援的 AWS 受管服務，包括：Amazon Elastic Compute Cloud (Amazon EC2)、Amazon Elastic Block Store (Amazon EBS)、Amazon S3 on Outposts、Amazon Elastic Kubernetes Service (Amazon EKS)、Amazon Elastic Container Service (Amazon ECS)、Amazon Relational Database Service (Amazon RDS) 和 AWS Outposts 上的其他服務。Outposts 上的服務會在 中使用的相同 AWS Nitro 系統上交付 AWS 區域。

透過利用 AWS Outposts 機架，您可以使用熟悉的 AWS 雲端服務和工具來建置、管理和擴展高可用性的現場部署應用程式。 AWS Outposts rack 非常適合需要低延遲存取現場部署系統、本機資料處理、資料駐留和遷移具有本機系統依存性的應用程式的工作負載。

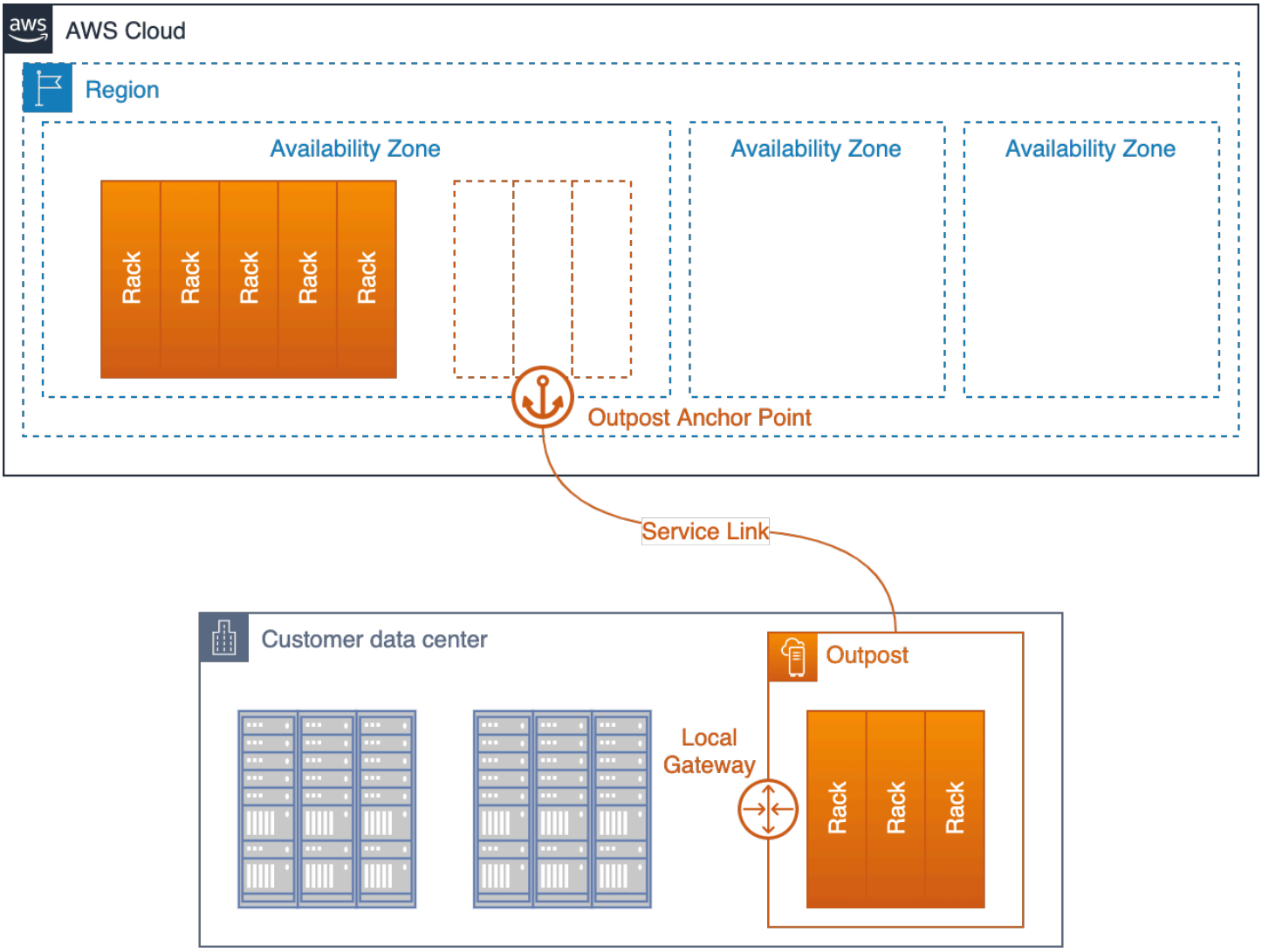
將 AWS 基礎設施和服務擴展到內部部署位置

AWS Outposts 此服務將 AWS 基礎設施和服務交付至 50 多個國家和地區的現場部署據點，讓客戶能夠將相同的 AWS 基礎設施、 AWS 服務、APIs 和工具部署到幾乎任何資料中心、共同位置空間或現場部署設施，以獲得真正一致的混合體驗。若要了解如何使用 Outposts 設計，您應該了解組成 AWS 雲端的不同層。

AWS 區域 是世界的地理區域。每個 AWS 區域 都是資料中心的集合，以邏輯方式分組為可用區域 (AZs)。 AWS 區域 提供多個 （至少兩個） 實體分隔和隔離的可用區域，這些區域以低延遲、高輸送量和備援網路連線。每個 AZ 由一或多個實體資料中心組成。

邏輯 Outpost （以下稱為 Outpost) 是一個或多個實體連線 AWS Outposts 機架的部署，以單一實體管理。Outpost 會在其中一個站點提供 AWS 運算和儲存容量集區，做為 中 AZ 的私有延伸 AWS 區域。

的最佳概念模型可能是 AWS Outposts 考慮從 的 AZ 中的資料中心拔除一或多個機架 AWS 區域，並將其安裝在您自己的資料中心或主機代管設施中。您可以將機架從 AZ 資料中心滾動到資料中心。然後，您可以使用 （極長） 長纜線將機架插入 AZ 資料中心的錨點，讓機架繼續做為 的一部分運作 AWS 區域。您也可以將它們插入您的本機網路，以便在內部部署網路和在這些機架上執行的工作負載之間提供低延遲連線。這可提供 的操作和 API 一致性 AWS 雲端，同時保持工作負載在本機。



部署在客戶資料中心並連接到其錨點可用區域和父區域的 Outpost

Outpost 可做為 AZ 的延伸，在其中錨點。 會作為 的一部分 AWS 操作、監控和管理 AWS Outposts 基礎設施 AWS 區域。Outpost 會透過一組稱為 Service Link 的加密 VPN 通道，來連接其父區域，而不是非常長的實體纜線。

Service Link 會在 Outpost 父區域中可用區域 (AZ) 中的一組錨點上終止。

您可以選擇內容的存放位置。您可以將內容複寫和備份到 AWS 區域 或其他位置。未經您同意，您的內容將不會移動或複製到您選擇的位置之外，除非是為了遵守法律或政府機構的約束命令而需要。如需更多資訊，請參閱 AWS 資料隱私權常見問答集。

您在這些機架上部署的工作負載會在本機執行。此外，雖然這些機架中可用的運算和儲存容量有限，且無法容納執行 的雲端規模服務 AWS 區域，但部署在機架上的資源 （您的執行個體及其本機儲存體） 會獲得在本機執行的優勢，而管理平面會繼續在 中操作 AWS 區域。

若要在 Outpost 上部署工作負載，請將子網路新增至虛擬私有雲端 (VPC) 環境，並將 Outpost 指定為子網路的位置。然後，當您透過 AWS Management Console、CLI、APIs、CDK 或基礎設施做為程式碼 (IaC) 工具部署支援 AWS 的資源時，請選取所需的子網路。Outpost 子網路中的執行個體會透過 VPC 網路與 Outpost 或 區域中的其他執行個體通訊。

Outpost Service Link 同時承載 Outpost 管理流量和客戶 VPC 流量 (Outpost 上的子網路與 區域中的子網路之間的 VPC 流量）。

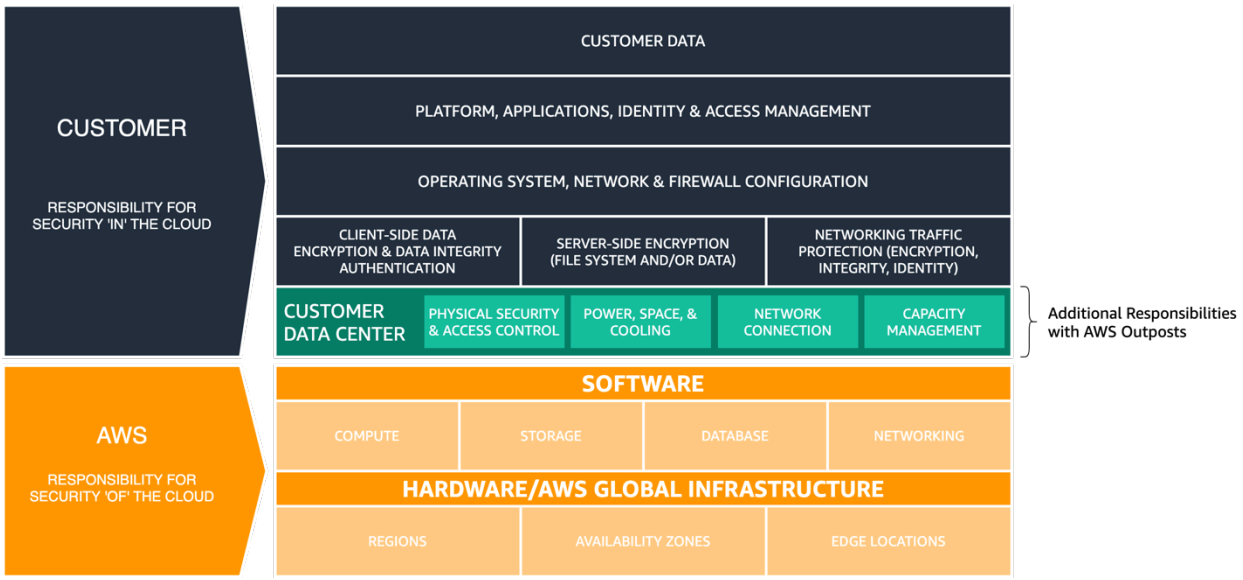
重要術語：

- AWS Outposts – 是一項全受管服務， AWS 可為幾乎任何資料中心、主機代管空間或內部部署設施提供相同的 AWS 基礎設施、服務、APIs 和工具，以獲得真正一致的混合體驗。
- Outpost – 是一或多個實體連線 AWS Outposts 機架的部署，以單一邏輯實體和部署在客戶站點的 AWS 運算、儲存和聯網集區的形式進行管理。
- 父區域 – AWS 區域 提供 Outpost 部署的管理、控制平面服務和區域 AWS 服務。
- 錨點可用區域 （錨點可用區域） – 父區域中託管 Outpost 錨點的可用區域。Outpost 可做為其錨點 AZ 的延伸。錨點 AZ 是由客戶在下單時選擇。選擇錨點 AZ 後，無法在 AWS Outposts 訂閱期間變更。
- 錨點 – 錨點 AZ 中的端點，接收來自遠端部署 Outposts 的連線。
- Service Link – 一組加密的 VPN 通道，可將 Outpost 連接到其父區域中的錨點可用區域。
- Local Gateway (LGW) – 邏輯互連虛擬路由器，可啟用 Outpost 與內部部署網路之間的通訊。

了解 AWS Outposts 共同責任模型

當您將 AWS Outposts 基礎設施部署到資料中心或共同位置設施時，您會在AWS 共同責任模型中承擔其他責任。例如，在 區域中， AWS 提供多樣化的電源、備援的核心聯網和彈性廣域網路 (WAN) 連線，以確保在一或多個元件故障時提供服務。

使用 Outposts，您有責任為 Outpost 機架提供彈性電力和網路連線，以滿足您在 Outposts 上執行工作負載的可用性需求。



AWS 已更新 的共同責任模型 AWS Outposts

使用 時 AWS Outposts，您必須負責資料中心環境的實體安全和存取控制。您必須提供足夠的電力、空間和冷卻，以保持 Outpost 操作和網路連線，將 Outpost 連接到 區域。

由於 Outpost 容量有限，且取決於您站點安裝的 AWS 機架大小和數量，因此您必須決定執行初始工作負載、適應未來成長所需的 EC2、EBS 和 S3 on Outposts 容量，並提供額外容量來緩解伺服器故障和維護事件。

AWS 負責 Outposts 基礎設施的可用性，包括 AWS Outposts 機架內的電源、伺服器和聯網設備。AWS 也會管理虛擬化 Hypervisor、儲存系統和在 Outposts 上執行 AWS 的服務。

每個 Outposts 機架中的中央電源架會從 AC 轉換為 DC 電源，並透過匯流排架構為機架中的伺服器提供電源。使用匯流排架構時，機架中一半的電源可能會失敗，且所有伺服器都會繼續執行不中斷。

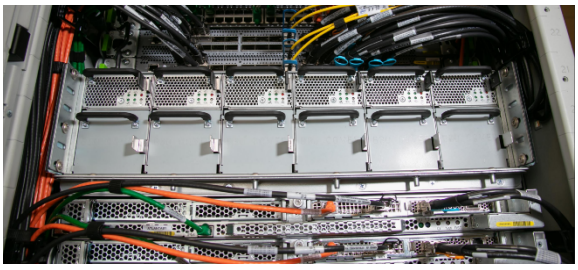


圖 3 - AWS Outposts AC-to-DC電源和匯流排電源分佈

Outposts 機架內和之間的網路切換和佈線也是完全冗餘的。光纖修補程式面板提供 Outpost 機架與內部部署網路之間的連線，並做為客戶受管資料中心環境與受管 AWS Outposts 環境之間的分界點。

如同在 區域中， AWS 負責 Outposts 提供的雲端服務，並在您選取和部署更高層級的受管服務時承擔其他責任，例如 Amazon RDS on Outposts。您應該檢閱個別服務的AWS 共同責任模型和常見問答集 (FAQ) 頁面，如同您考慮的一樣，並選取要在 Outposts 上部署的服務。這些資源提供您與 之間責任劃分的其他詳細資訊 AWS。

考慮失敗模式

設計高可用性應用程式或系統時，您必須考量哪些元件可能失敗、元件故障對系統的影響，以及應用程式 RPO/RTO 目標，以及您可以實作哪些機制來緩解或消除元件故障的影響。您的應用程式是在單一伺服器、單一機架或單一資料中心執行？ 當伺服器、機架或資料中心發生暫時性或永久故障時，會發生什麼情況？ 當聯網等關鍵子系統或應用程式本身發生故障時，會發生什麼情況？ 這些是失敗模式。

規劃 Outpost 和應用程式部署時，您應該考慮本節中的失敗模式。以下各節將說明如何緩解這些失敗模式，為您的應用程式環境提供更高水準的高可用性。

失敗模式 1：網路

Outpost 部署取決於與其父區域的彈性連線，以進行管理和監控。網路中斷可能由各種故障造成，例如操作員錯誤、設備故障和服務提供者中斷。當 Outpost 無法透過 Service Link 與區域通訊時，可能包含在網站中連接在一起的一或多個機架。

備援網路路徑有助於降低中斷連線事件的風險。您應該映射應用程式相依性和網路流量，以了解中斷連線事件對工作負載操作的影響。規劃足夠的網路備援，以符合您的應用程式可用性需求。

在中斷連線事件期間，在 Outpost 上執行的執行個體會繼續執行，並可透過 Outpost Local Gateway (LGW) 從內部部署網路存取。如果本機工作負載和服務依賴 區域中的服務，可能會受損或失敗。將請求（例如在 Outpost 上啟動或停止執行個體）、控制平面操作和服務遙測（例如，CloudWatch 指標）在 Outpost 與區域中斷連線時將會失敗。CloudWatch 指標會在您的 Outpost 上於本機進行多工緩衝處理，短暫中斷網路連線，並在重新建立服務連結連線時，傳送至 區域以供檢閱。

失敗模式 2：執行個體

如果 Amazon EC2 執行個體執行的伺服器發生問題，或執行個體遇到作業系統或應用程式故障，則 Amazon EC2 執行個體可能會受損或失敗。應用程式如何處理這些類型的故障取決於應用程式架構。單體應用程式通常會使用應用程式或系統功能進行復原，而模組化服務導向或微服務架構通常會取代失敗的元件，以維持服務的可用性。

您可以使用 Amazon EC2 Auto Scaling 群組等自動化機制，將失敗的執行個體取代為新的執行個體。執行個體自動復原可以重新啟動因伺服器故障而失敗的執行個體，前提是剩餘伺服器上有足夠的備用容量，而且服務連結仍然連線。

失敗模式 3：運算

伺服器可能會失敗或受損，而且可能需要因各種原因而停止運作（暫時或永久），例如元件故障和排程維護操作。Outposts 機架上的服務如何處理伺服器故障和損害，會有所不同，並且取決於客戶如何設定高可用性選項。

您應該訂購足夠的運算容量來支援N+M可用性模型，其中 N 是必要的容量，而 M 是佈建來因應伺服器故障的備用容量。

故障伺服器的硬體替換是全受管 AWS Outposts 機架服務的一部分。 AWS 主動監控 Outpost 部署中所有伺服器和聯網裝置的運作狀態。如果需要執行實體維護， AWS 會安排時間造訪您的網站，以取代失敗的元件。佈建備用容量可讓您在運作狀態不佳的伺服器停止服務並取代時，保持工作負載彈性，避免主機故障。

失敗模式 4：機架或資料中心

機架故障可能是因為機架的電力完全耗盡，或環境故障，例如因洪水或地震對資料中心造成冷卻或實體損壞。在標準資料中心電源維護期間，資料中心電源分佈架構的不足或錯誤可能會導致一個或多個機架或整個資料中心的電源中斷。

這些案例可以透過將基礎設施部署到同一個校園或都會區中彼此獨立的多個資料中心樓層或位置來緩解。

採用此方法搭配 AWS Outposts 機架時，需要仔細考慮應用程式如何建構和分佈，以跨多個不同的邏輯 Outpost 執行，以維持應用程式的可用性。

失敗模式 5： AWS 可用區域或區域

每個 Outpost 錨定到 內的特定可用區域 (AZ) AWS 區域。錨點 AZ 或父區域中的故障可能會導致 Outpost 管理和可變性遺失，並可能中斷 Outpost 和 區域之間的網路通訊。

與網路故障類似，AZ 或區域故障可能會導致 Outpost 與區域中斷連線。在 Outpost 上執行的執行個體會繼續執行，並可透過 Outpost Local Gateway (LGW) 從內部部署網路存取，如果它們依賴 區域中的服務，則可能會受損或失敗，如前所述。

若要減輕 AZ AWS 和區域故障的影響，您可以將多個 Outpost 分別部署到不同的 AZ 或區域。然後，您可以使用許多類似的機制和架構模式，設計工作負載以在分散式多點部署模型中操作，這些機制和架構模式是您目前用來設計和部署的 AWS 。

在 上執行的服務控制平面 AWS Outposts 位於其錨定的區域中，在 Amazon EC2 和 Amazon EBS 等區域服務以及 Amazon RDS、Elastic Load Balancing 和 Amazon EKS 等區域服務上產生相依性。在 Outposts 中，應用程式可以在靜態穩定性的概念下部署，以協助改善彈性以控制平面受損。

使用 AWS Outposts 機架建置 HA 應用程式和基礎設施解決方案

透過 AWS Outposts 機架，您可以使用熟悉的 AWS 雲端服務和工具來建置、管理和擴展高可用性的內部部署應用程式。請務必了解雲端 HA 架構和方法通常與您目前在資料中心中執行的傳統內部部署 HA 架構不同。

透過傳統的內部部署 HA 應用程式部署，應用程式會部署在虛擬機器 VMs) 中。部署和維護複雜的 IT 系統和基礎設施，以保持這些虛擬機器的運作狀態良好。VMs 通常具有特定的身分，而且每個 VM 可能在整體應用程式架構中扮演關鍵角色。

架構角色與 VM 身分緊密結合。系統架構師利用 IT 基礎設施功能提供高可用性的 VM 執行期環境，讓每個 VM 能夠可靠地存取運算容量、儲存磁碟區和網路服務。如果 VM 失敗，則會執行自動或手動復原程序，將失敗的 VM 還原至運作狀態良好，通常是在其他基礎設施或另一個資料中心。

雲端 HA 架構採用不同的方法。 AWS 雲端服務提供可靠的運算、儲存和聯網功能。應用程式元件會部署到 EC2 執行個體、容器、無伺服器函數或其他受管服務。

執行個體是應用程式元件的實例化，可能是執行該角色的其中之一。應用程式元件彼此鬆散地耦合，並與其在整體應用程式架構中扮演的角色耦合。執行個體的個別身分通常並不重要。可以建立或銷毀其他執行個體，以擴展或縮減規模，以因應需求。失敗的執行個體或運作狀態不佳的執行個體，只會以運作狀態良好的新執行個體取代。

AWS Outposts 機架是一種全受管服務，可將 AWS 運算、儲存、聯網、資料庫和其他雲端服務延伸至內部部署位置，以提供真正一致的混合體驗。您不應將 Outposts 機架服務視為具有傳統內部部署 HA 機制的 IT 基礎設施系統的插入式替代。嘗試使用 AWS 服務和 Outposts 支援傳統的內部部署 HA 架構是一種反模式。

在 AWS Outposts 機架上執行的工作負載會使用雲端 HA 機制，例如 Amazon EC2 Auto Scaling（水平擴展以滿足工作負載需求）、EC2 運作狀態檢查（偵測和移除運作狀態不佳的執行個體） 和 Application Load Balancer（將傳入工作負載流量重新導向至擴展或取代的執行個體）。將應用程式遷移至雲端時，無論是 AWS 區域 或 AWS Outposts 機架，您都應該更新您的 HA 應用程式架構，以開始利用受管雲端服務和雲端 HA 機制。

下列各節介紹架構模式、反模式和建議實務，用於在內部部署環境中部署 AWS Outposts 機架，以執行具有高可用性需求的工作負載。這些章節介紹模式和實務；但不提供組態和實作詳細資訊。您應該閱讀並熟悉AWS Outposts 機架FAQs和使用者指南，以及針對 Outposts 機架上執行之服務的FAQs和服務文件，同時為 Outposts 機架和應用程式準備環境以遷移至 AWS 服務。

主題

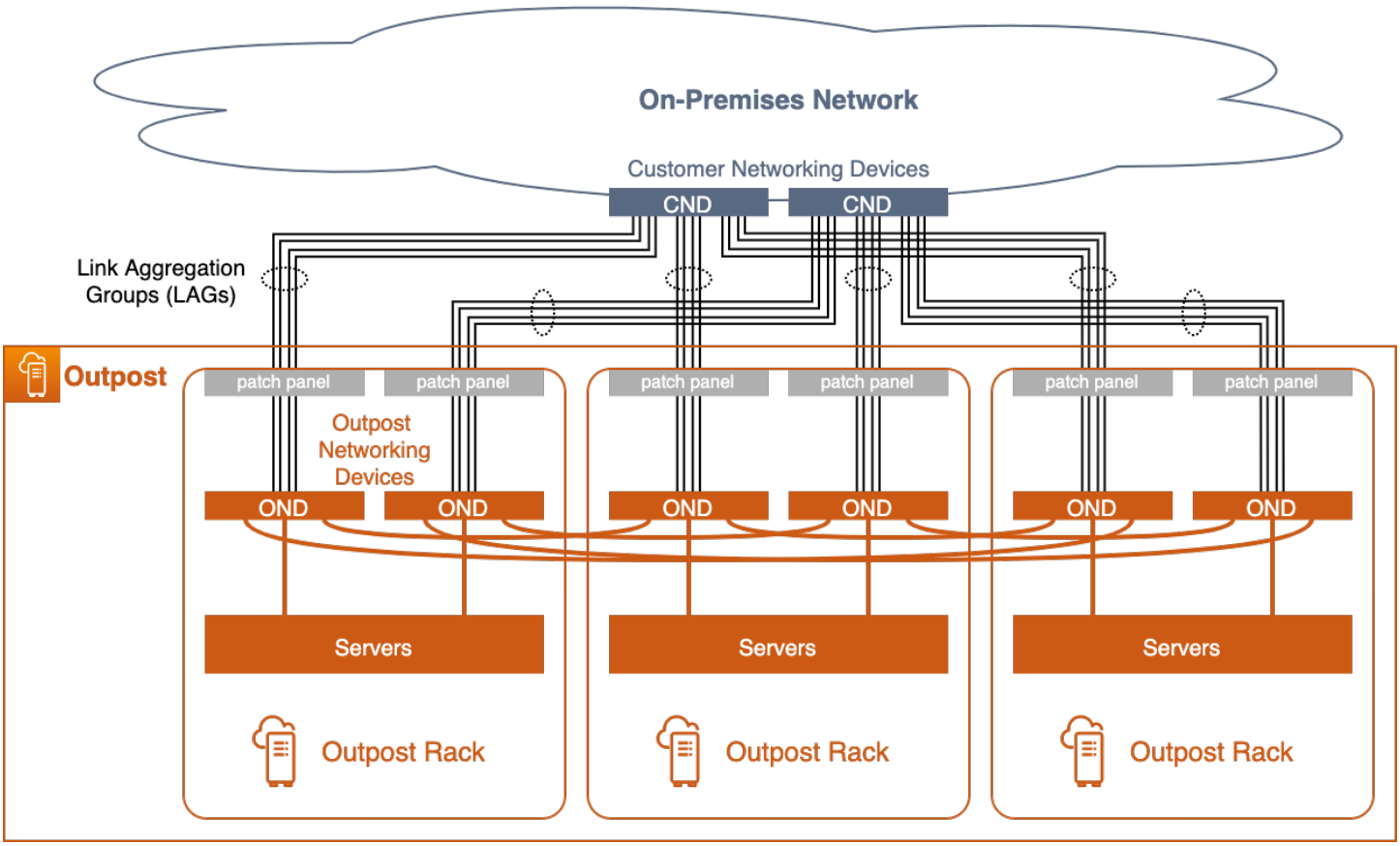
聯網

Outpost 部署取決於其錨點可用區域彈性連線，以便管理、監控和服務操作正常運作。您應該佈建內部部署網路，為每個 Outpost 機架提供備援網路連線，並將可靠連線傳回 AWS 雲端的錨點。同時考慮在 Outpost 上執行的應用程式工作負載與其通訊的其他內部部署和雲端系統之間的網路路徑，您將如何在網路中路由此流量？

主題

網路連接

每個 AWS Outposts 機架都設定了稱為 Outpost Networking Devices (ONDs備援top-of-rack切換。每個機架中的運算和儲存伺服器都會同時連線到 ONDs。您應該將每個 OND 連接到資料中心稱為客戶聯網裝置 (CND) 的個別交換器，為每個 Outpost 機架提供不同的實體和邏輯路徑。ONDs使用光纖纜線和光學收發器，透過一或多個實體連線連接到 CNDs。實體連線是在邏輯連結彙總群組 (LAG) 連結中設定。



具有備援網路附件的多機架 Outpost

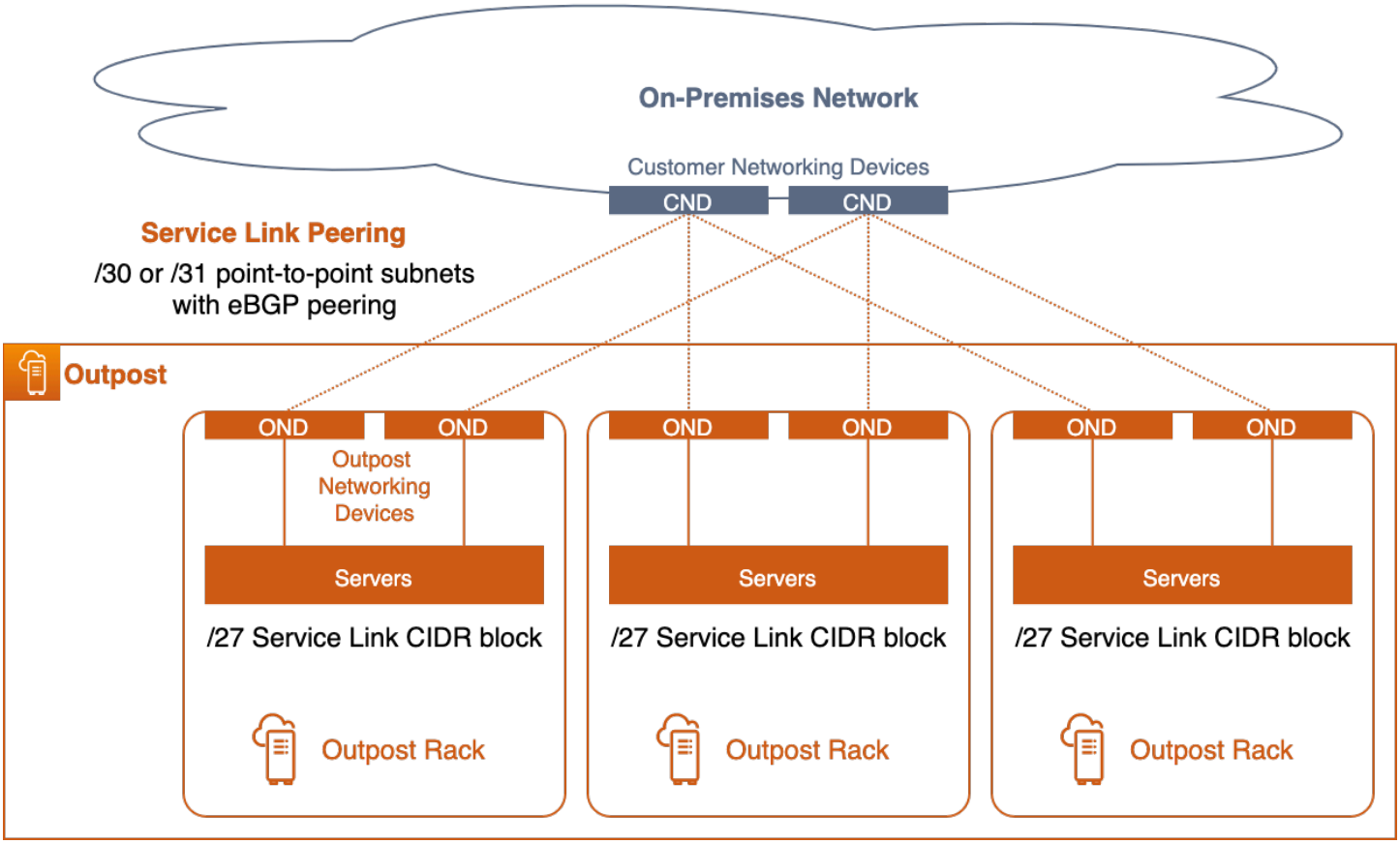
OND 到 CND 連結一律在 LAG 中設定，即使實體連線是單一光纖纜線也是一樣。將連結設定為 LAG 群組可讓您新增其他實體連線至邏輯群組，以增加連結頻寬。LAG 連結設定為 IEEE 802.1q 乙太網路幹線，以啟用 Outpost 和內部部署網路之間的隔離聯網。

每個 Outpost 至少有兩個邏輯隔離的網路，需要與客戶網路通訊或跨客戶網路通訊：

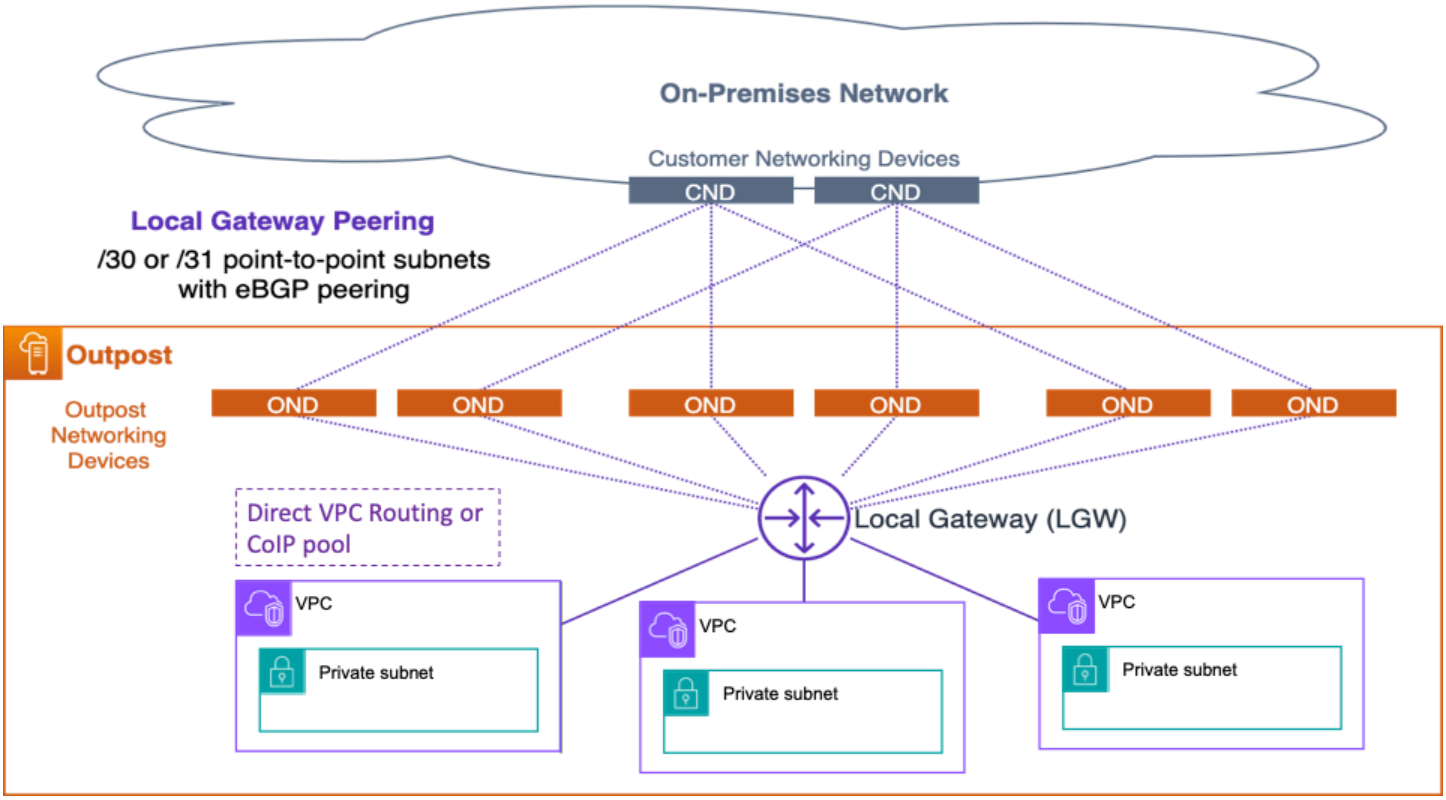
- 服務連結網路 – 將服務連結 IP 地址配置到 Outpost 伺服器，並促進與內部部署網路的通訊，以允許伺服器連接到區域中的 Outpost 錨點。當您在單一邏輯 Outpost 中有多個機架實作時，您需要為每個機架指派 Service Link /26 CIDR。
- 本機閘道網路 – 透過 Outpost 本機閘道 (LGW) 啟用 Outpost 上的 VPC 子網路與內部部署網路之間的通訊。

這些隔離的網路會透過 LAG 連結，透過一組point-to-point IP 連線連接到內部部署網路。每個 OND 到 CND LAG 連結都使用 VLAN IDs、point-to-point(/30 或 /31) IP 子網路，以及每個隔離網路的 eBGP 對等互連（服務連結和 LGW) 進行設定。您應該將 LAG 連結及其point-to-point和子網路視為第 2 層分割

的路由第 3 層連線。 VLANs 路由 IP 連線提供備援邏輯路徑，有助於 Outpost 上隔離網路與內部部署網路之間的通訊。



服務連結對等



本機閘道對等互連

您應該終止直接連接之 CND 交換器上的 layer-2 LAG 連結（及其 VLANs），並在 CND 交換器上設定 IP 介面和 BGP 對等互連。您不應該在資料中心切換之間橋接 LAG VLANs。如需詳細資訊，請參閱AWS Outposts 《使用者指南》中的網路層連線。

在邏輯多機架 Outpost 內，ONDs 會以備援方式互連，在機架與伺服器上執行的工作負載之間提供高可用性的網路連線。 AWS 負責 Outpost 內的網路可用性。

不使用 ACE 的高可用性網路連接的建議實務

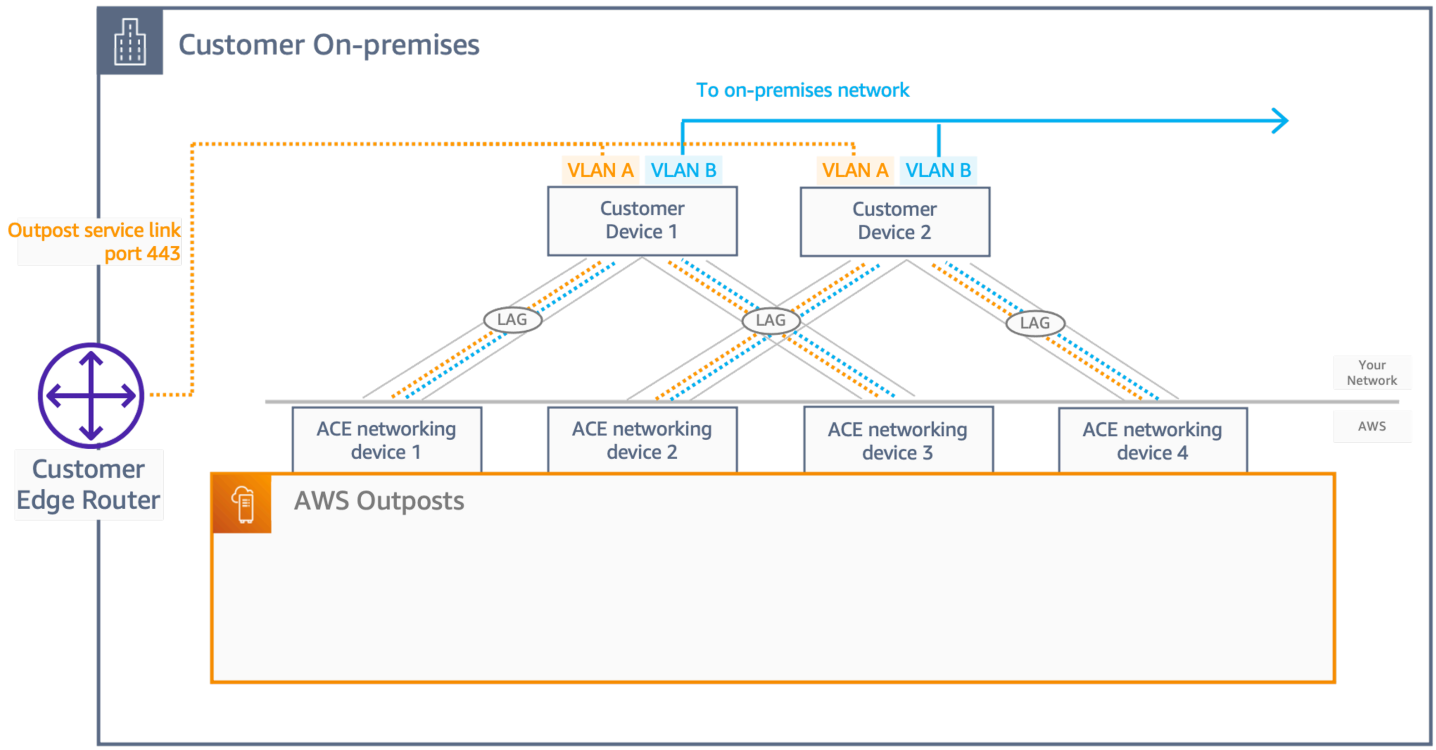
- 將 Outpost 機架中的每個 Outpost 網路裝置 (OND) 連接到資料中心中的個別客戶網路裝置 (CND)。
- 在直接連接的客戶聯網裝置 (CND) 交換器上終止 layer-2 連結、VLANs、 layer-3 IP 子網路和 BGP 對等互連。請勿在 CND 之間或跨內部部署網路橋接 OND 至 CNDs VLANs。
- 新增連結彙總群組 (LAGs) 的連結，以增加 Outpost 和資料中心之間的可用頻寬。請勿透過這兩個 ONDs 依賴不同路徑的彙總頻寬。
- 透過備援 ONDs 使用各種路徑，在 Outpost 網路和內部部署網路之間提供彈性連線。
- 為了實現最佳備援並允許不中斷的 OND 維護，我們建議客戶設定 BGP 公告和政策，如下所示：

- 客戶網路設備應從 Outpost 接收 BGP 公告，而不變更 BGP 屬性，並啟用 BGP 多路徑/負載平衡，以實現最佳的傳入流量（從客戶到 Outpost)。AS-Path 前綴用於 Outpost BGP 字首，以便在需要維護時將流量移離特定 OND/上行連結。客戶網路應該偏好從 AS-Path 長度為 1 的 Outpost 路由，而不是 AS-Path 長度為 4 的路由，也就是說，對 AS-Path 前置做出反應。
- 客戶網路應該向 Outpost 中的所有 ONDs 公告具有相同屬性的同等 BGP 字首。根據預設，Outpost 網路負載會平衡所有上行連結之間的傳出流量（朝向客戶）。在 Outpost 端使用路由政策，以在需要維護時將流量移離特定 OND。所有 ONDs 上客戶端的相同 BGP 字首需要執行此流量轉移，並以不中斷的方式執行維護。當客戶網路上需要維護時，我們建議您使用 AS-Path 前置，暫時移離特定上行連結或裝置的流量。

使用 ACE 進行高可用性網路連接的建議實務

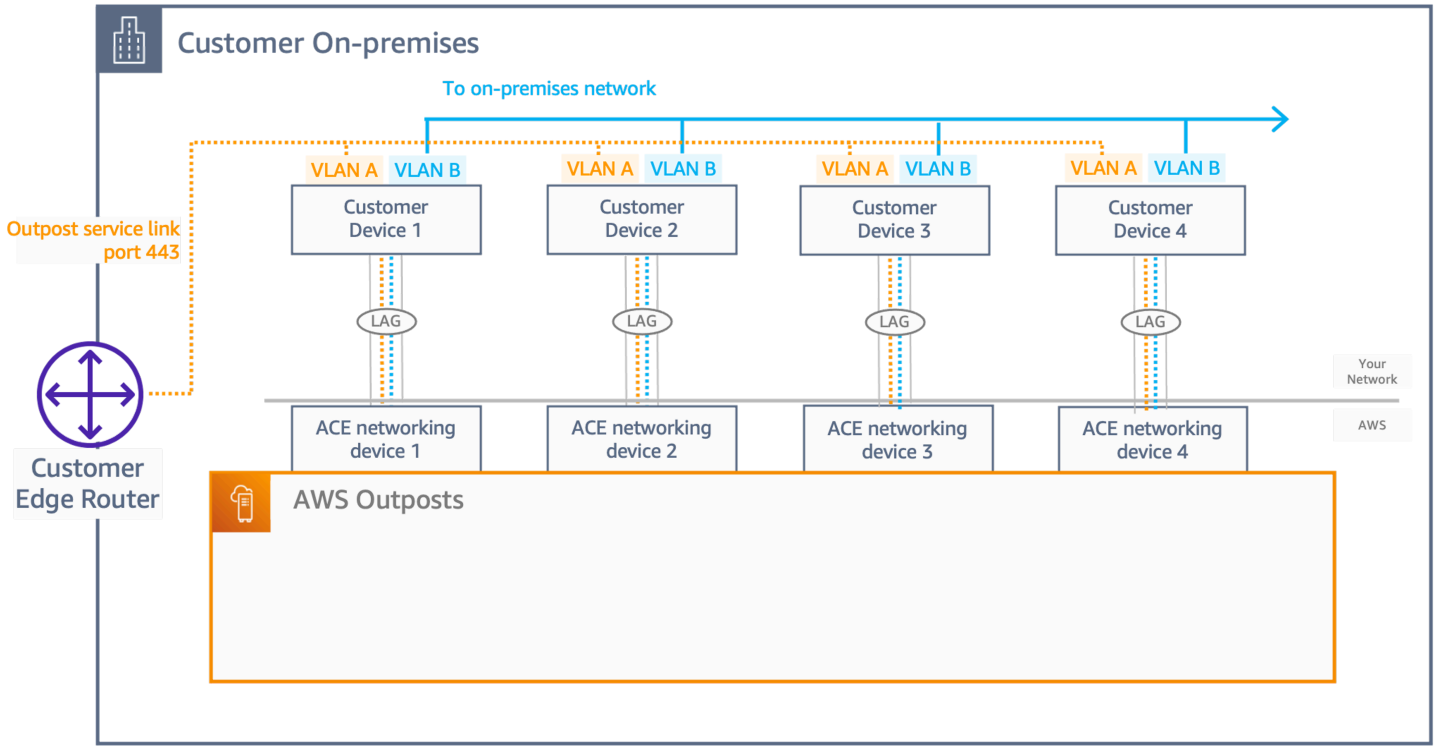
對於具有四個或更多運算機架的多機架部署，您必須使用彙總、核心、邊緣 (ACE) 機架，這將作為網路彙總點，以減少內部部署聯網裝置的光纖連結數量。ACE 機架提供每個 Outposts 機架中 ONDs 的連線能力，因此 AWS 將擁有 ONDs和 ACE 網路裝置之間的 VLAN 介面配置和組態。

無論是否使用 ACE 機架，Service Link 和 Local Gateway 網路的隔離網路層仍然是必要的，其目標是具有 VLAN point-to-point (/30 或 /31) IP 子網路，以及每個隔離網路的 eBGP 對等互連組態。提議的架構應遵循下列兩種架構中的任何一種：



兩個客戶網路裝置

- 透過此架構，客戶應有兩個聯網裝置 (CND) 來互連 ACE 網路裝置，以提供備援。
- 對於每個實體連線，您必須啟用 LAG （以增加 Outpost 和資料中心之間的可用頻寬），即使它是單一實體連接埠，它也會攜帶兩個網路區段，具有 2 個point-to-point VLANs(/30 或 /31)，以及 ACEs 和 CNDs 之間的 eBGP 組態。
- 在穩定狀態中，流量會依照等成本多路徑 (ECMP) 模式，從 ACE 層往返客戶網路進行負載平衡，在 ACE 之間向客戶分配 25% 的流量。為了允許此行為，ACEs 和 CNDs 之間的 eBGP 對等互連必須啟用 BGP 多路徑/負載平衡，並在 4 個 eBGP 對等互連連線上宣告具有相同 BGP 指標的客戶字首。
- 為了實現最佳備援並允許不中斷的 OND 維護，我們建議客戶遵循下列建議：
  - 客戶聯網裝置應該向 Outpost 中的所有 ONDs 公告具有相同屬性的同等 BGP 字首。
  - 客戶聯網裝置應從 Outpost 接收 BGP 公告，而不變更 BGP 屬性，並啟用 BGP 多路徑/負載平衡。



四客戶網路裝置

透過此架構，客戶將擁有四個聯網裝置 (CND) 來互連 ACE 網路裝置，提供備援和相同的聯網邏輯，包括適用於 2 CND 架構VLANs、eBGP 和 ECMP。

錨點連線

Outpost 服務連結會連線至 Outpost 父區域中特定可用區域 (AZ) 中的公有或私有錨點（非兩者）。Outpost 伺服器會啟動傳出服務連結 VPN 從其服務連結 IP 地址到錨點 AZ 中的錨點。這些連線使用 UDP 和 TCP 連接埠 443。 AWS 負責區域中錨點的可用性。

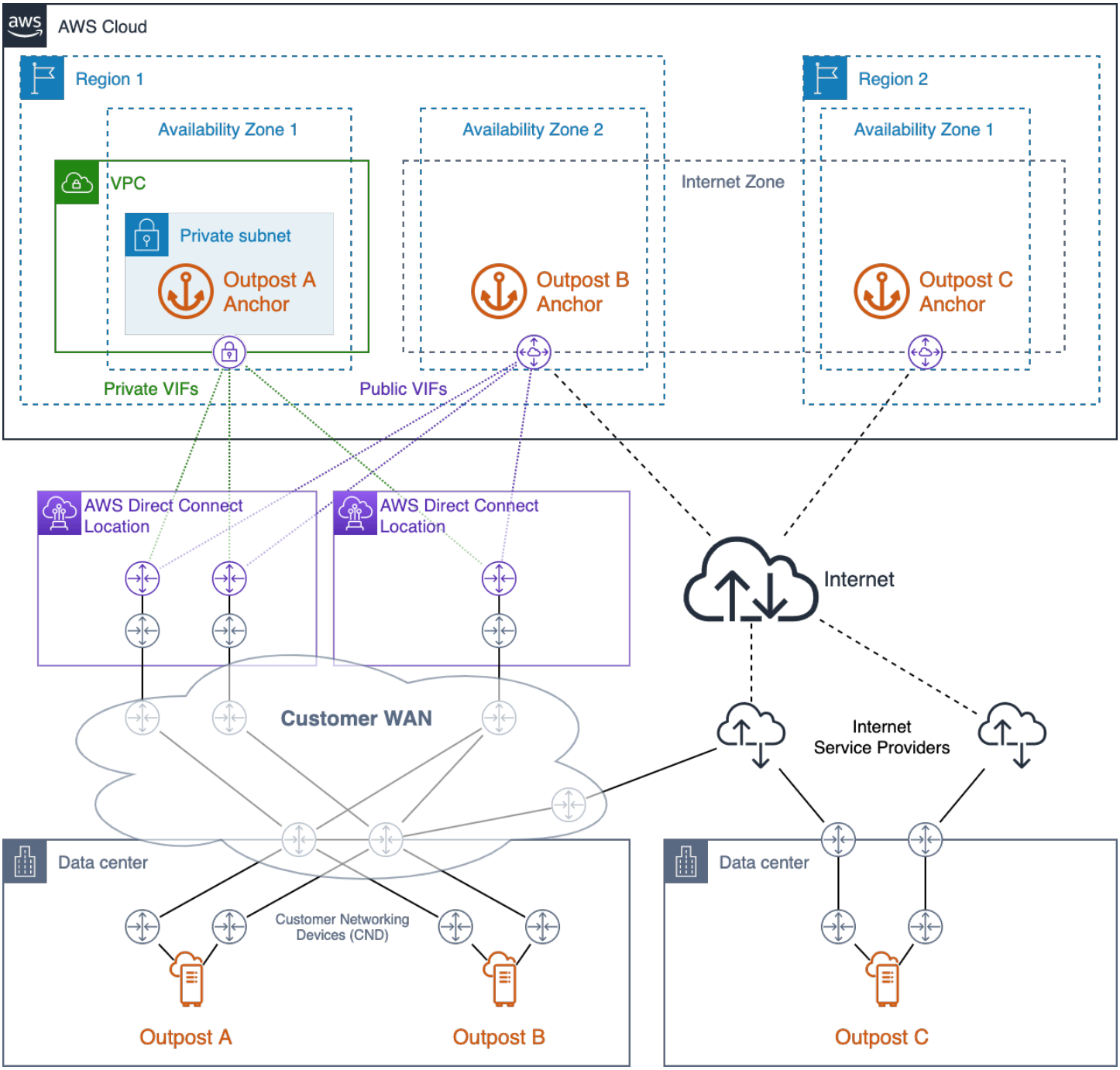
您必須確保 Outpost 服務連結 IP 地址可以透過您的網路連接到錨點 AZ 中的錨點。服務連結 IP 地址不需要與內部部署網路上的其他主機通訊。

公有錨點位於區域的公有 IP 範圍（在 EC2 服務 CIDR 區塊中），可透過網際網路或 AWS Direct Connect(DX) 公有虛擬介面 VIFs) 存取。使用公有錨點可讓選擇更靈活的路徑，因為服務連結流量可以透過任何可成功到達公有網際網路上錨點的可用路徑路由。

私有錨點可讓您使用 IP 地址範圍進行錨點連線。使用客戶指派的 IP 地址，在專用 VPC 內的私有子網路中建立私有錨點。VPC 是在擁有 Outpost 資源的 中建立 AWS 帳戶 的，而您有責任確保 VPC 可用且設定正確。使用 AWSOrigamiServiceGateway Organizations 中的安全控制政策 (SCP)，以防止使用者刪除該虛擬私有雲端 (VPC)。必須使用 Direct Connect 私有 VIFs存取私有錨點。

您應該在 Outpost 和 區域中的錨點之間佈建備援網路路徑，並在多個位置的個別裝置上終止連線。動態路由應設定為在連線或聯網裝置失敗時，自動將流量重新路由至替代路徑。您應該佈建足夠的網路容量，以確保一個 WAN 路徑的失敗不會超過剩餘的路徑。

下圖顯示三個 Outpost，其具有使用 的錨定 AZs 的備援網路路徑， AWS Direct Connect 以及公有網際網路連線。Outpost A 和 Outpost B 錨定到相同區域中的不同可用區域。Outpost A 連接到區域 1 AZ 1 中的私有錨點。Outpost B 連接到區域 1 AZ 2 中的公有錨點。Outpost C 連接到區域 2 AZ 1 中的公有錨點。



與 AWS Direct Connect 和公有網際網路存取的高可用性錨點連線

Outpost A 有三個備援網路路徑，可到達其私有錨點。兩個路徑可透過單一 Direct Connect 位置的備援 Direct Connect 電路使用。第三個路徑可透過第二個 Direct Connect 位置的 Direct Connect 電路使用。此設計會保留 Outpost A 在私有網路上的服務連結流量，並提供路徑備援，允許任何一個 Direct Connect 電路故障或整個 Direct Connect 位置故障。

Outpost B 有四個備援網路路徑，可到達其公有錨點。三個路徑可透過佈建在 Direct Connect 電路和 Outpost A 使用位置上的公有 VIFs 取得。第四個路徑可透過客戶 WAN 和公有網際網路取得。Outpost B 的服務連結流量可以透過任何可成功到達公有網際網路上錨點的可用路徑路由。使用 Direct Connect 路徑可提供更一致的延遲和更高的頻寬可用性，而公有網際網路路徑可用於災難復原 (DR) 或頻寬增強案例。

Outpost C 有兩個備援網路路徑，可到達其公有錨點。Outpost C 部署在與 Outposts A 和 B 不同的資料中心。Outpost C 的資料中心沒有連接到客戶 WAN 的專用電路。相反地，資料中心具有兩個不同的網際網路服務供應商 (ISPs) 提供的備援網際網路連線。Outpost C 的服務連結流量可以透過任一 ISP 網路路由，以到達公有網際網路上的錨點。此設計可讓任何可用的公有網際網路連線靈活路由服務連結流量。不過，end-to-end路徑取決於頻寬可用性和網路延遲波動的公有第三方網路。

Outpost 及其服務連結錨點之間的網路路徑必須符合下列頻寬規格：

- 每個 Outpost 機架 500 Mbps - 1 Gbps 的可用頻寬（例如，3 個機架：1.5 – 3 Gbps 的可用頻寬）

高可用性錨點連線的建議實務

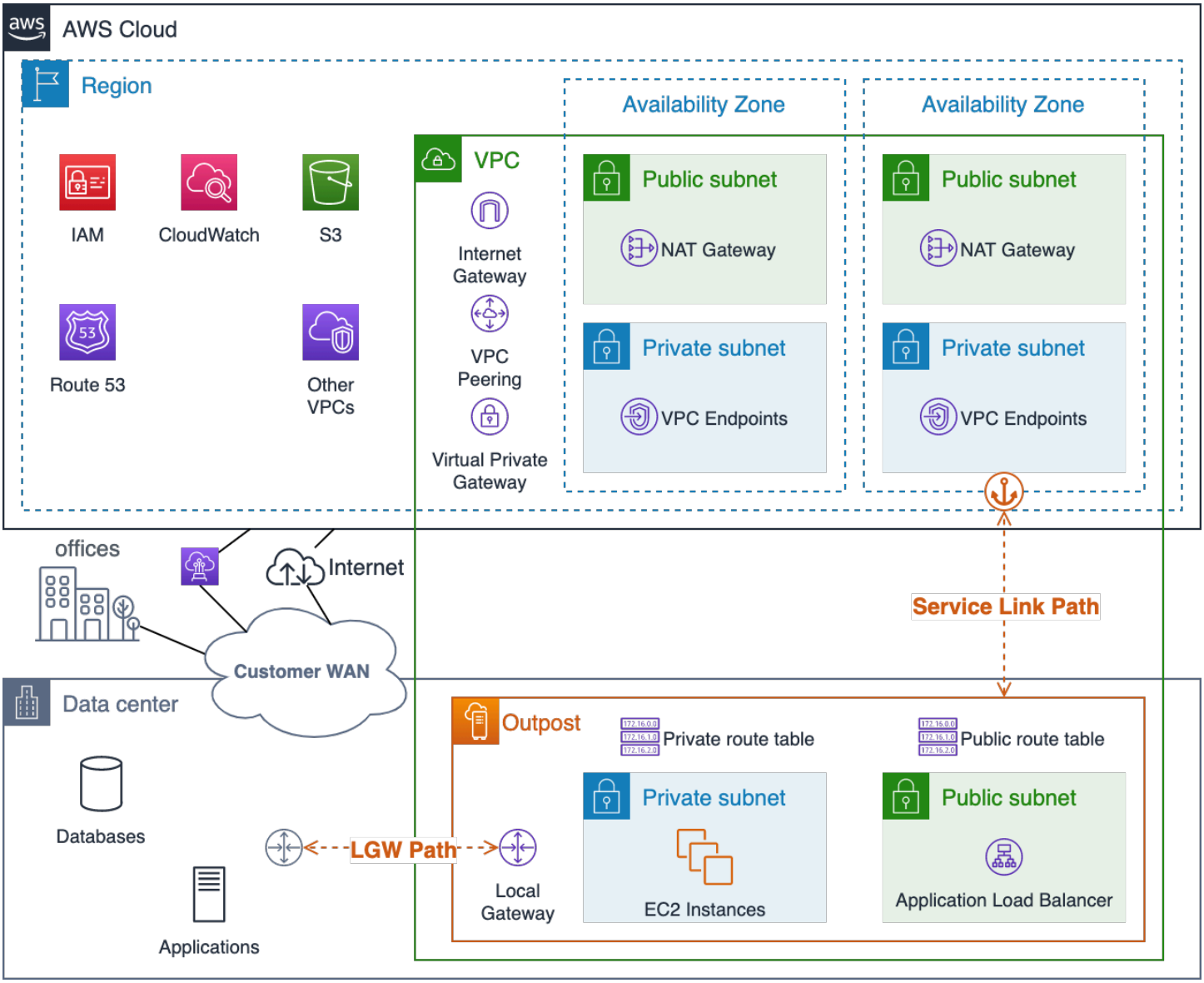
- 在區域中的每個 Outpost 及其錨點之間佈建備援網路路徑。
- 使用 Direct Connect (DX) 路徑來控制延遲和頻寬可用性。
- 確定 TCP 和 UDP 連接埠 443 已從 Outpost Service Link CIDR 區塊開啟（傳出），到達父區域中的 EC2 IP 地址範圍。確定所有網路路徑上的連接埠都已開啟。
- 如果您使用區域 CIDR 範圍的子集，請追蹤防火牆上的 Amazon EC2 IP 地址範圍。
- 確保每個路徑都符合頻寬可用性和延遲要求。
- 使用動態路由來自動化網路故障的流量重新導向。
- 測試將服務連結流量路由到每個計劃的網路路徑，以確保路徑功能如預期。

應用程式/工作負載路由

Outpost 應用程式工作負載有兩個路徑：

- 服務連結路徑：考量應用程式流量除了將 MTU 限制為 1300 個位元組之外，還會與 Outposts 控制平面流量競爭。
- 本機閘道 (LGW) 路徑：考慮客戶的本機網路允許存取內部部署和 中的應用程式 AWS 區域。

您可以設定 Outpost 子網路路由表，以控制要採取哪些路徑才能到達目的地網路。指向 LGW 的路由會將流量導向本機閘道和內部部署網路。指向 區域的服務和資源的路由，例如網際網路閘道、NAT 閘道、虛擬私有閘道和 TGW，將使用服務連結來達到這些目標。如果您在相同的 Outpost 上具有與多個 VPCs的 VPCs 對等互連，VPC 之間的流量會保留在 Outpost 上，而且不會使用返回 區域的服務連結。如需 VPC 對等互連的相關資訊，請參閱《Amazon VPCs 使用者指南》中的使用 VPC 對等互連 VPC。



Outpost 服務連結和 LGW 網路路徑的視覺化

在規劃應用程式路由時，您應該謹慎考慮正常操作和網路故障期間有限的路由和服務可用性。當 Outpost 從 區域中斷連線時，無法使用 Service Link 路徑。

您應該佈建各種路徑，並設定 Outpost LGW 與關鍵現場部署應用程式、系統和使用者之間的動態路由。備援網路路徑可讓網路繞過故障的流量，並確保內部部署資源能夠在部分網路故障期間與在 Outpost 上執行的工作負載進行通訊。

Outpost VPC 路由組態是靜態的。您可以透過 AWS Management Console、CLI、APIs 和其他基礎設施做為程式碼 (IaC) 工具來設定子網路路由表；不過，在中斷連線事件期間，您將無法修改子網路路由表。您必須重新建立 Outpost 與 區域之間的連線，才能更新路由表。針對您計劃在中斷連線事件期間使用的正常操作，使用相同的路由。

Outpost 上的資源可以透過服務連結和 區域中的網際網路閘道 (IGW) 或透過本機閘道 (LGW) 路徑來連接網際網路。透過 LGW 路徑和內部部署網路路由網際網路流量，可讓您使用現有的內部部署網際網路輸入/輸出點，相較於使用服務連結路徑到 區域中的 IGW，可提供更低的延遲、更高的 MTUs 和更低 AWS 的資料輸出費用。

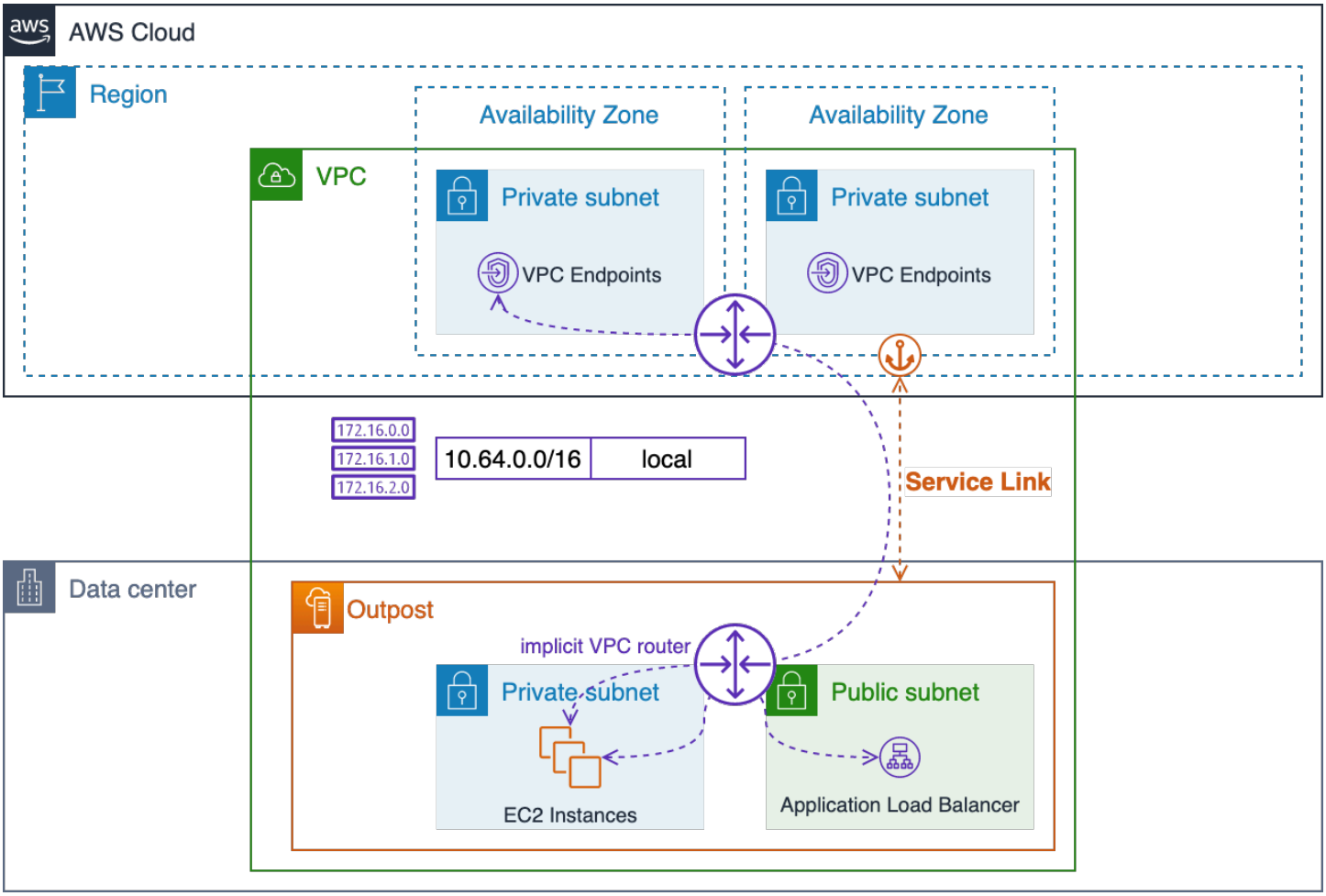
如果您的應用程式必須執行內部部署，且需要從公有網際網路存取，您應該透過內部部署網際網路連線將應用程式流量路由至 LGW 以連接 Outpost 上的資源。

雖然您可以在 Outpost 上設定子網路，例如區域中的公有子網路，但對於大多數使用案例來說，這可能是不理想的做法。傳入網際網路流量將透過 傳入， AWS 區域 並透過服務連結路由至 Outpost 上執行的資源。

回應流量將接著透過服務連結路由，並透過 AWS 區域網際網路連線傳回。此流量模式可能會增加延遲，並會在流量離開區域前往 Outpost 時產生資料輸出費用，而傳回流量透過區域傳回，而輸出進入網際網路時產生資料輸出費用。如果您的應用程式可以在 區域中執行，則 區域是執行它的最佳位置。

VPC 資源之間的流量 （在相同 VPC 中） 將一律遵循本機 VPC CIDR 路由，並由隱含 VPC 路由器在子網路之間路由。

例如，在 Outpost 上執行的 EC2 執行個體與 區域中的 VPC 端點之間的流量一律會透過服務連結路由。



透過隱含路由器的本機 VPC 路由

應用程式/工作負載路由的建議實務

- 盡可能使用 Local Gateway (LGW) 路徑，而非服務連結路徑。
- 透過 LGW 路徑路由網際網路流量。
- 使用一組標準路由設定 Outpost 子網路路由表 – 它們將用於正常操作和中斷連線事件期間。
- 在 Outpost LGW 和關鍵現場部署應用程式資源之間佈建備援網路路徑。使用動態路由來自動化內部部署網路故障周圍的流量重新導向。

運算

雖然 中的 Amazon EC2 容量 AWS 區域 似乎無限，但 Outposts 上的容量有限。您負責規劃和管理 Outposts 部署的運算容量。

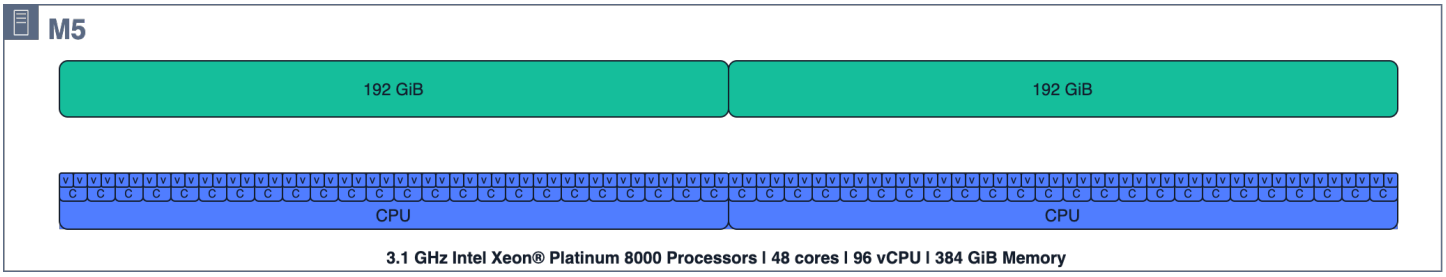
主題

容量規劃

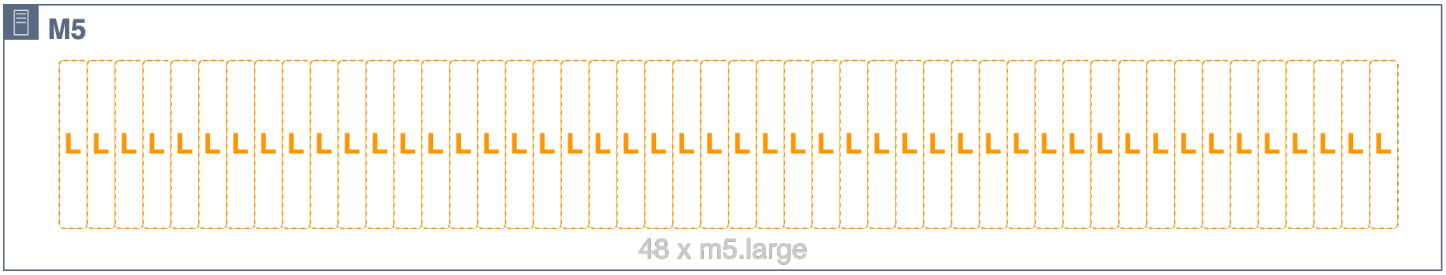
雖然 中的 Amazon EC2 容量 AWS 區域 似乎是無限的，但 Outposts 上的容量是無限的 – 受限於所訂購運算容量的總容量。您負責規劃和管理 Outposts 部署的運算容量。您應該訂購足夠的運算容量來支援 N+M 可用性模型，其中 N 是必要的伺服器數量，M 是佈建以適應伺服器故障的備用伺服器數量。N+1 和 N+2 是最常見的可用性層級。

每個主機 (C5、R5、 等） M5都支援單一系列的 EC2 執行個體。在 EC2 運算伺服器上啟動執行個體之前，您必須提供槽配置，指定您希望每個伺服器提供的 EC2 執行個體大小。使用請求的槽配置來 AWS 設定每個伺服器。

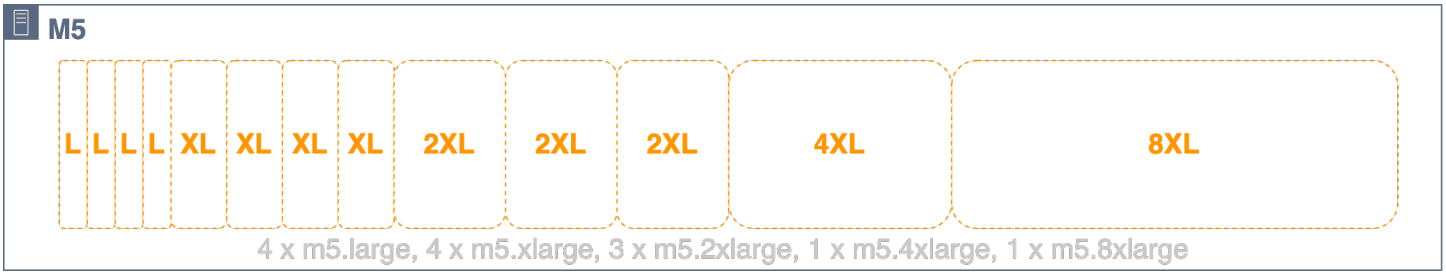
主機可以是同質槽，其中所有槽都是相同的執行個體大小（例如 48 m5.large 個槽），或是與執行個體類型（例如 4m5.large、4m5.xlarge、3m5.2xlarge、1 m5.4xlarge和 1m5.8xlarge) 混合的異質槽 – 請參閱以下三個圖表，了解這些槽組態的視覺化效果。



m5.24xlarge 主機運算資源



m5.24xlarge 主機以同質方式槽入 48 個*m5.large*插槽



m5.24xlarge 主機以異質方式插入 4*m5.large*、4*m5.xlarge*、3*m5.2xlarge*、1 *m5.4xlarge*和 1 個*m5.8xlarge*插槽

完全的主機容量不需要槽化。插槽可以新增至具有可用未配置容量的主機。您可以使用 的容量管理 APIs或 UIs 來修改槽配置， AWS Outposts 並建立新的容量任務。如需詳細資訊，請參閱 AWS Outposts 機架使用者指南中的 的容量管理 AWS Outposts。如果執行中的執行個體佔用了某些插槽，但無法套用新的槽配置，您可能需要關閉或重新啟動特定執行個體以完成新的容量任務。CreateCapacityTask API 可讓您表達應出現在指示 Outpost ID 上的每個執行個體大小數目，如果任務因執行中的執行個體而無法完成， 會傳回必須停止的執行個體，以滿足請求。此時，您可以選擇性地指示您希望在不希望停止傳回其中一個執行個體的情況下看到「N」其他選項，也可以指示不應建議做為執行個體關閉的 EC2 執行個體 ID、EC2 執行個體標籤、帳戶或服務，以滿足容量任務請求。選擇您要使用的選項後，建議您使用 Dry Run 參數來驗證提議的變更，並了解實作之前的潛在影響。

所有主機都會將其佈建的插槽貢獻至 Outpost 上的 EC2 容量集區，而指定執行個體類型和大小的所有插槽都會以單一 EC2 容量集區的形式管理。例如，先前具有 m5.large、m5.xlarge、m5.2xlarge、 m5.4xlarge和 m5.8xlarge 插槽的異質槽式主機會將這些插槽貢獻到五個 EC2 容量集區 – 每個執行個體類型和大小都有一個集區。這些集區可能會分散到多個主機，而執行個體置放應該是實現工作負載高可用性的考量因素。

在規劃 N+M 主機可用性的備用容量時，請務必考慮主機槽和 EC2 容量集區。 會 AWS 偵測主機故障或降級，並排定網站造訪以取代故障的主機。您應該設計 EC2 容量集區，以容忍 Outpost 中每個執行個體系列 (N+1) 中至少一個伺服器發生故障。使用此最低層級的主機可用性，當主機故障或需要停止服務時，您可以在相同系列的其餘主機的備用插槽上重新啟動故障或降級的執行個體。

當您擁有同質槽式主機或具有相同槽式配置的異質槽式主機群組時，規劃 N+M 可用性非常簡單。您只需計算執行所有工作負載所需的主機 (N) 數量，然後新增 (M) 其他主機，以滿足您在故障和維護事件期間對伺服器可用性的需求。

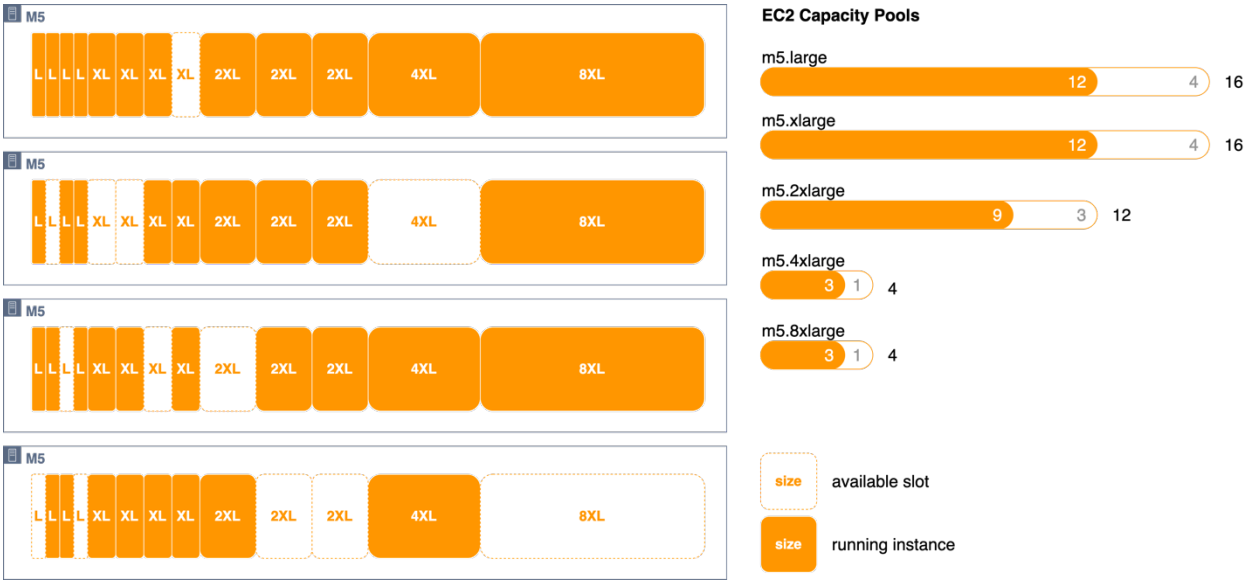
由於 NUMA 界限，下列槽組態無法使用：

- 3 m5.8xlarge

- 1 m5.16xlarge和 1 m5.8xlarge

請洽詢 AWS 帳戶 您的團隊以驗證您規劃的 AWS Outposts 機架槽組態。

在下圖中，四個m5.24xlarge主機以異質槽化方式搭配相同的槽式配置。四個主機會建立五個 EC2 容量集區。每個集區都以最大使用率 (75%) 執行，以維持在這四個主機上執行之執行個體的 N+1 可用性。如果有任何主機失敗，有足夠的空間來重新啟動其餘主機上失敗的執行個體。



EC2 主機插槽、執行中的執行個體和插槽集區的視覺化

對於較複雜的槽式配置，其中主機的槽式不同，您將需要計算每個 EC2 容量集區的 N+M 可用性。您可以使用下列公式來計算有多少個主機 （對指定的 EC2 容量集區貢獻插槽） 會失敗，但仍允許剩餘的主機攜帶執行中的執行個體：

$$M = \left\lceil \frac{poolSlots_{available}}{serverSlots_{max}} \right\rceil$$

其中：

- $poolSlots_{available}$ 是指定 EC2 容量集區中的可用插槽數量 （集區中的插槽總數減去執行中的執行個體數量）
- $serverSlots_{max}$ 是任何主機對指定 EC2 容量集區貢獻的插槽數量上限
- M 是可能失敗的主機數量，但仍允許剩餘的主機攜帶執行中的執行個體

範例：Outpost 有三個主機，可將插槽貢獻至`m5.2xlarge`容量集區。第一個貢獻 4 個插槽，第二個貢獻 3 個插槽，第三個主機貢獻 2 個插槽。Outpost 上的`m5.2xlarge`執行個體集區總容量為 9 個插槽 (4 + 3 + 2)。Outpost 有 4 個執行中的`m5.2xlarge`執行個體。有多少個主機可能失敗，但仍允許剩餘的主機攜帶執行中的執行個體？

$$poolSlots_{available} = total\ capacity - running\ instances = 9 - 4 = 5$$

$$serverSlots_{max} = \max([4, 3, 2]) = 4$$

$$M = \left[\frac{poolSlots_{available}}{serverSlots_{max}}\right] = \left[\frac{5}{4}\right] = [1.25] = 1$$

答案：您可能會遺失任何一個主機，但仍在剩餘的主機上攜帶執行中的執行個體。

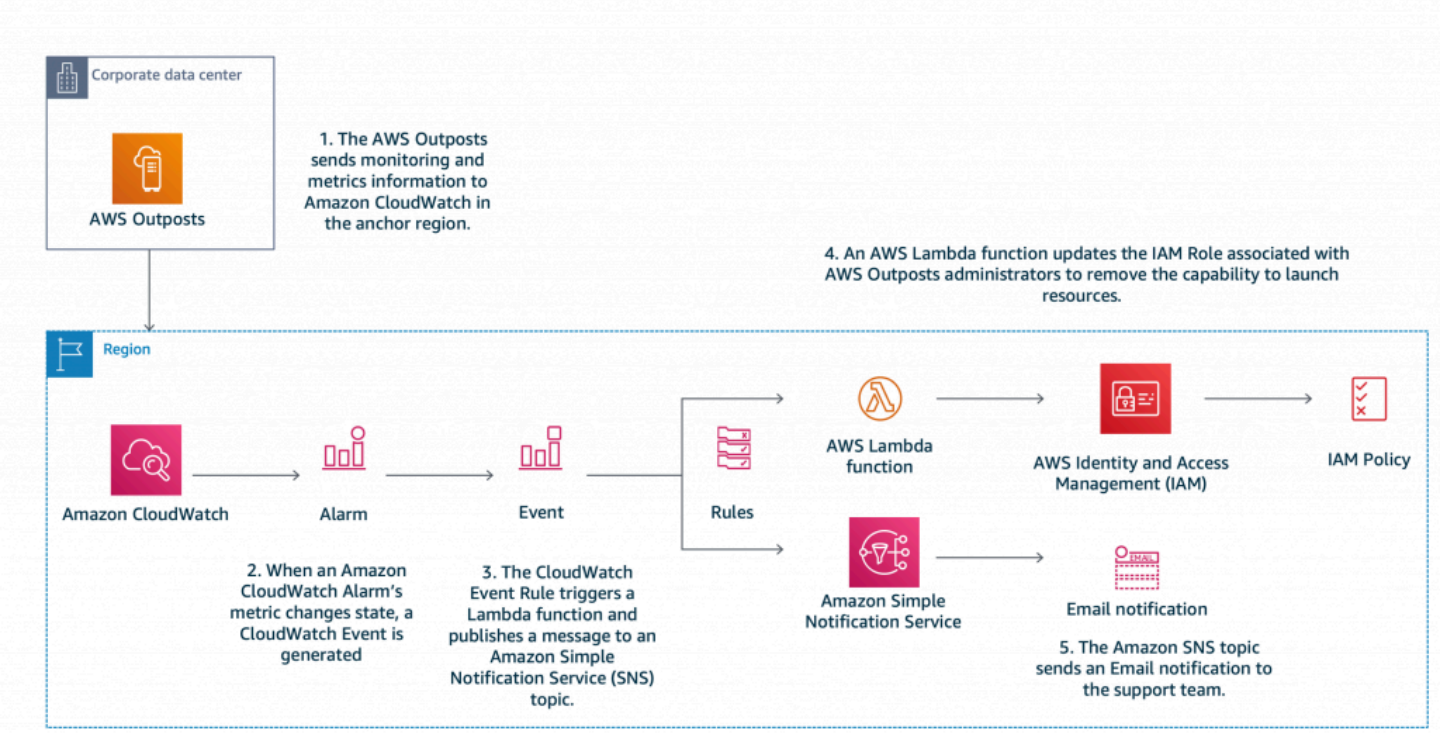
運算容量規劃的建議實務

- 調整運算容量的大小，為 Outpost 上的每個 EC2 容量集區提供 N+M 備援。
  - 為同質或相同的異質槽式伺服器部署 N+M 伺服器。
  - 計算每個 EC2 容量集區的 N+M 可用性，並確保每個集區符合您可用性需求。

容量管理

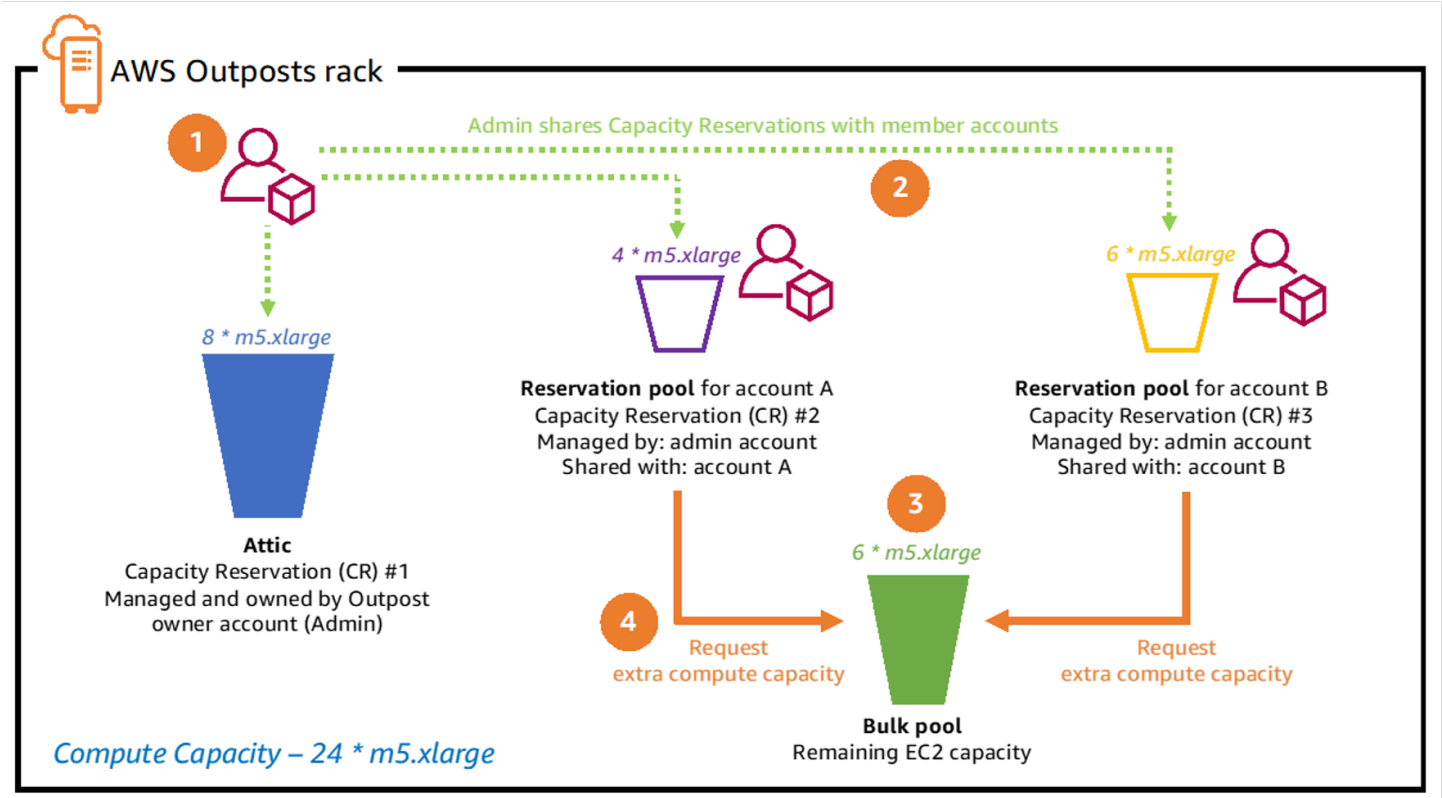
您可以透過 AWS Management Console 和 Amazon CloudWatch 指標來監控 Outpost EC2 執行個體集區使用率。請聯絡企業支援，以擷取或變更 Outpost 的槽配置。

您可以使用相同的執行個體自動復原和 EC2 Auto Scaling 機制來復原或取代受伺服器故障和維護事件影響的執行個體。您必須監控和管理 Outpost 容量，以確保隨時有足夠的備用容量，以適應伺服器故障。使用 Amazon CloudWatch 和部落格文章管理您的 AWS Outposts 容量 AWS Lambda提供實作教學課程，示範如何結合 AWS CloudWatch AWS Lambda 並管理您的 Outpost 容量以維持執行個體可用性。

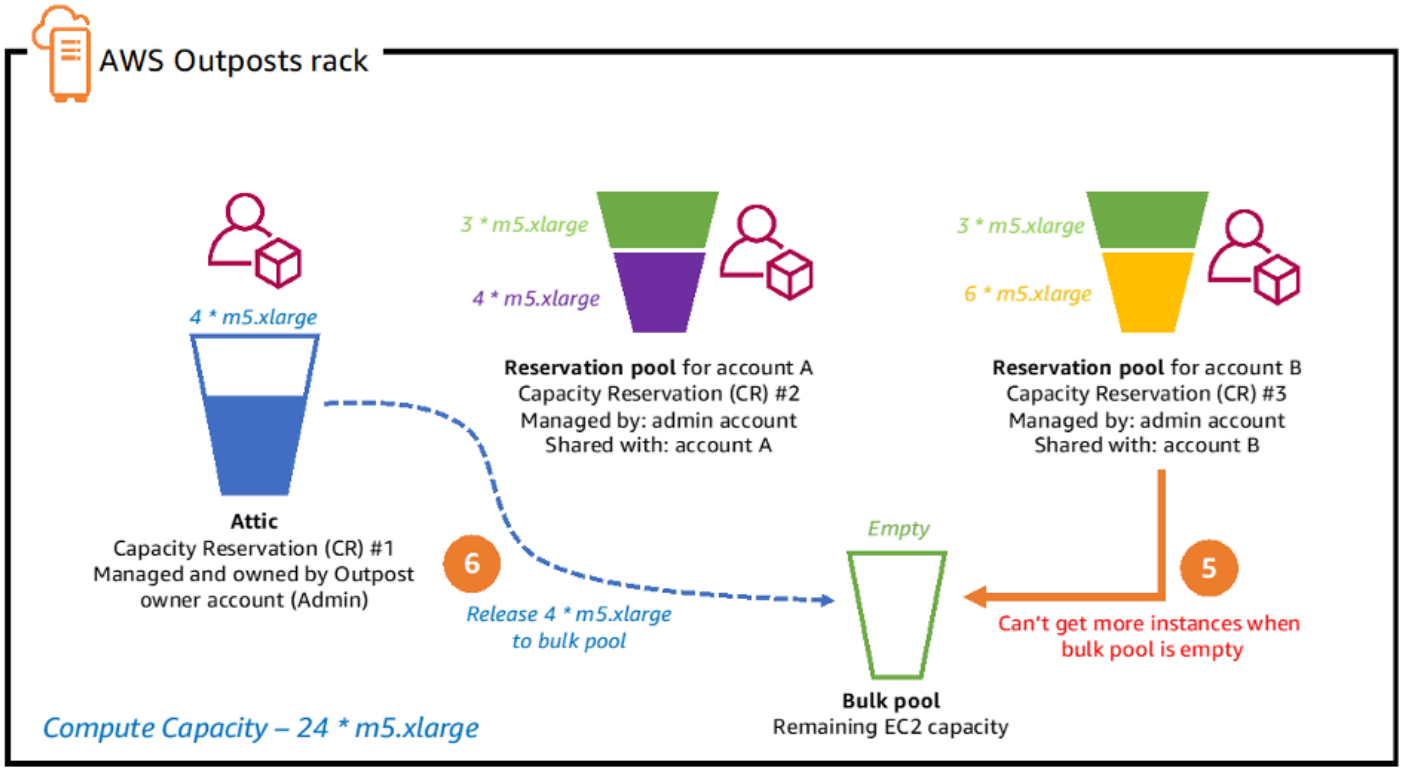


使用 Amazon CloudWatch 和 管理 AWS Outposts 容量 AWS Lambda

容量保留可用於多帳戶環境中，以控制單一帳戶或包含多個帳戶 AWS 的組織單位 (OU) 使用多少 Outpost 運算容量。您可以為 Amazon EC2 on Outposts 以及支援的 Outposts 建立容量保留， AWS 服務 例如 Amazon Elastic Kubernetes Service (EKS、Amazon Elastic Container Service (ECS) 和 Amazon Elastic Map Reduce (EMR)。 容量保留是透過 Outpost 擁有者帳戶中的 AWS Resource Access Manager (AWS RAM) 建立和共用給帳戶。使用 EC2 容量保留共享在 AWS Outposts 機架上建立運算配額提供實作教學，以及使用 Outpost 實作容量保留的額外指引，以管理容量。



Capacity Reservation sharing process steps 1-4



Capacity Reservation sharing process steps 5-6

運算容量管理的建議實務

- 在 Auto Scaling 群組中設定 EC2 執行個體，或使用執行個體自動復原重新啟動失敗的執行個體。
- 自動化 Outpost 部署的容量監控，並設定容量警示的通知和（選擇性）自動化回應。
- 使用容量保留，以精細控制與您 AWS 組織內其他帳戶共用的運算容量。

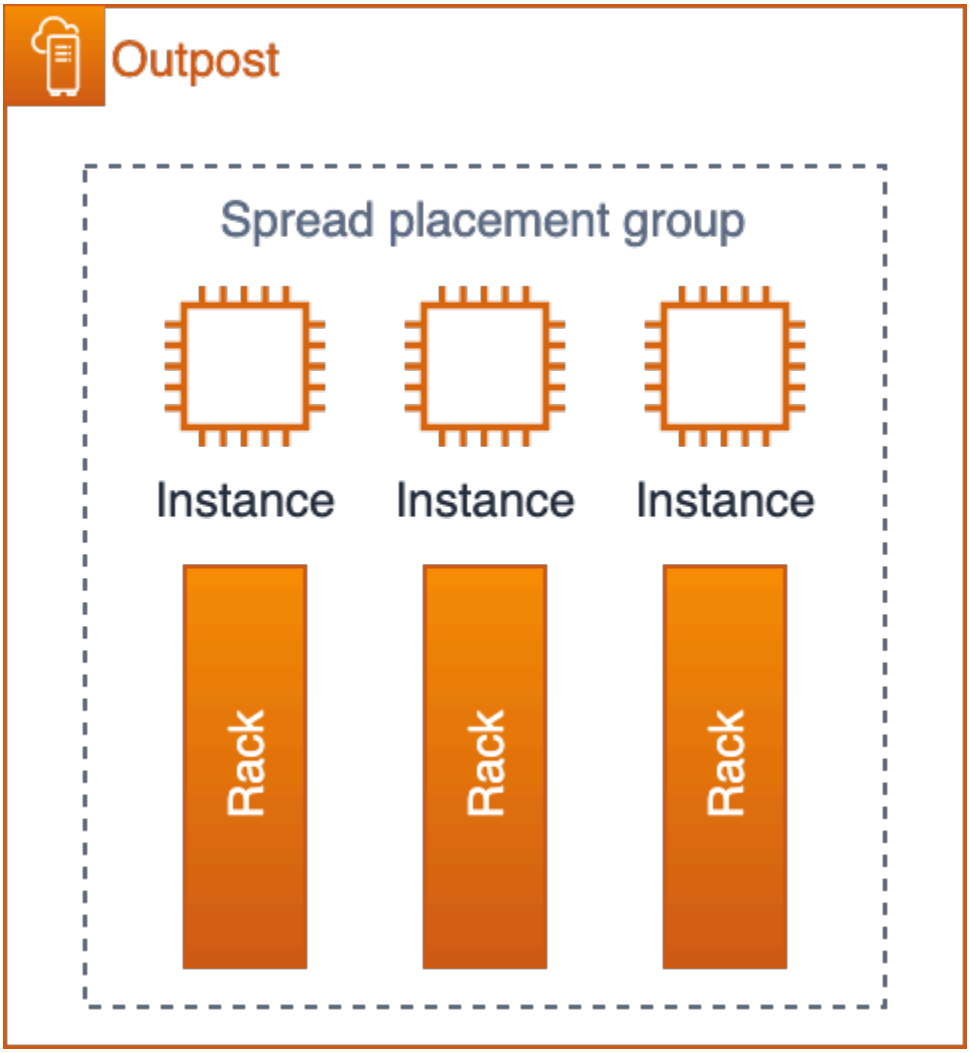
執行個體置放

Outpost 運算主機的數量有限。如果您的應用程式在 Outposts 上部署多個相關執行個體；無需其他組態，執行個體可以部署在相同主機或相同機架的主機上。目前，您可以使用三種機制來分發執行個體，以降低在相同基礎設施上執行相關執行個體的風險：

Multi-Outpost 部署 – 類似於 區域中的多可用區域策略，您可以部署 Outpost 來分隔資料中心，並將應用程式資源部署到特定的 Outpost。這可讓您在所需的 Outpost（一組邏輯機架）上執行執行個體。使用直接 VPC 路由跨多個 Outpost 進行內部 VPC 通訊是另一種策略，可用於使用 Outpost 本機閘道 (LGW) 在 Outpost 上的子網路之間建立路由，將工作負載分散到相同 VPC 內的多個 Outpost。可以使用多 Outpost 策略來防止機架和資料中心故障模式，如果 Outpost 錨定到不同的 AZs 或區域， 也可以提供對 AZ 或區域故障模式的保護。如需多輸出站架構的詳細資訊，請參閱較大的故障模式。

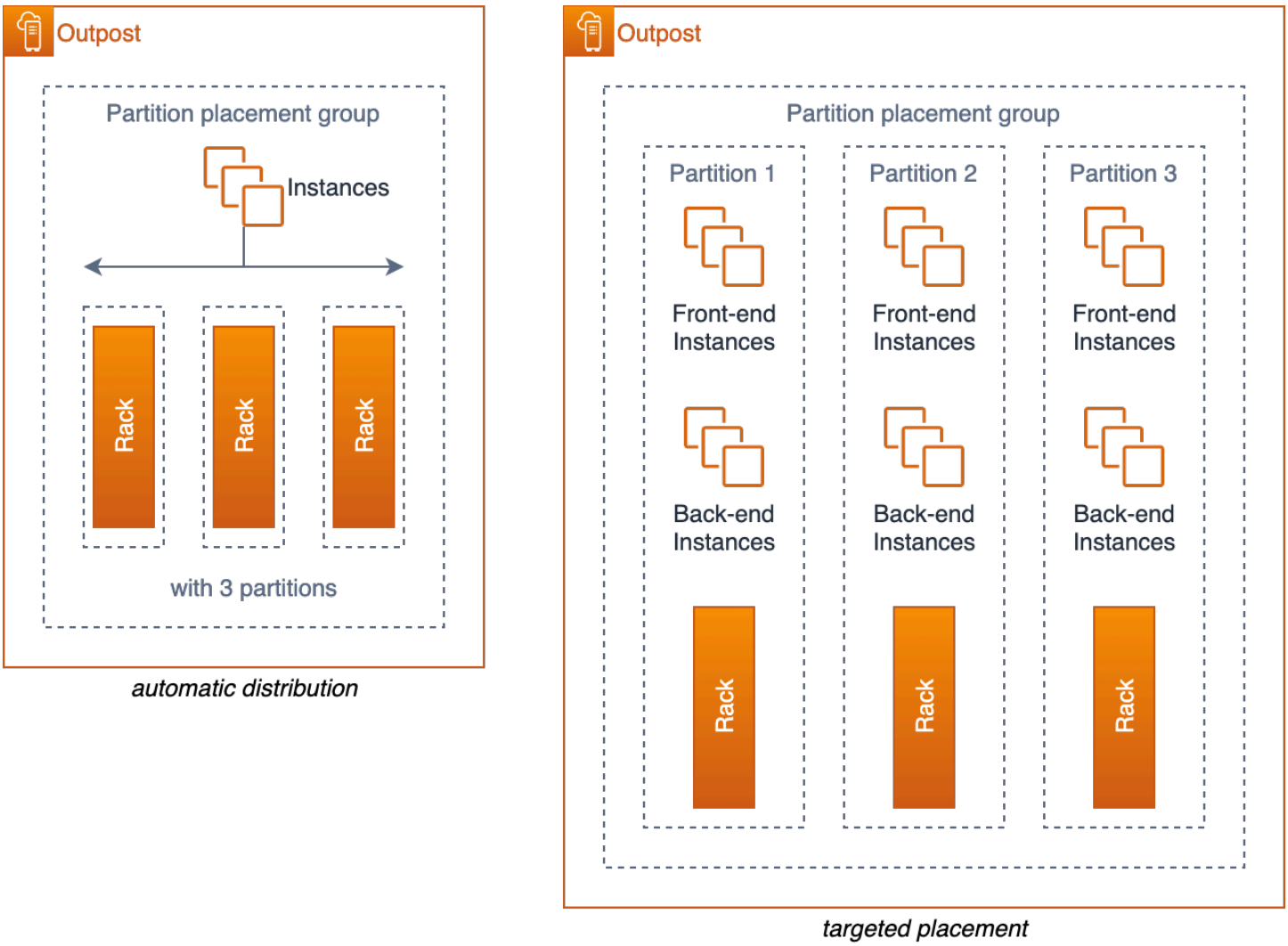
Outposts 上的 Amazon EC2 置放群組（單一-Outpost 多機架執行個體置放）– 您可以在帳戶中建立的 Outpost 置放群組。這樣，您就可以在站點上的 Outpost 中跨基礎硬體分散執行個體。在 Outpost 中建立具有分散策略的置放群組時，可以選擇讓置放群組在主機層級或是機架層級分散執行個體。

分散置放群組提供一種簡單的方式，將單一執行個體分散到機架或主機，以減少相關故障的可能性。您只能將與 Outpost 中主機數量相同的執行個體部署到 群組。



具有三個機架的 Outpost 上的 EC2 分散置放群組

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。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。將執行個體部署到目標分割區可讓您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。例如，如果您有邏輯 Outpost 具有三個機架，則建立具有三個分割區的分割區置放群組可讓您將資源分散到整個機架。



Outpost 上具有三個機架的 EC2 分割區置放群組

創意伺服器槽 – 如果您有單一機架 Outpost 或您在 Outposts 上使用的服務不支援置放群組，則您可以使用創意槽，以確保執行個體不會部署在相同的實體伺服器上。如果相關執行個體是相同的 EC2 執行個體大小，則您可能可以槽化伺服器，以限制每個伺服器上設定的該大小的槽數 – 將槽分散到伺服器上。伺服器槽化會限制可在單一伺服器上執行的執行個體數量 （該大小）。

例如，請考慮先前圖 13 中顯示的槽配置。如果您的應用程式需要部署三個`m5.4xlarge`執行個體到使用此槽配置設定的 Outpost，EC2 會將每個執行個體放在個別的伺服器上，而且這些執行個體不可能在相同的伺服器上執行，只要槽組態不會變更為在伺服器上開啟其他`m5.4xlarge`插槽。

運算執行個體置放的建議實務

- 在 Outpost 上使用 Amazon EC2 置放群組，以控制執行個體在單一邏輯 Outpost 中跨機架置放。

- 與其訂購具有單一中型或大型 Outpost 機架的 Outpost，請考慮將容量分割為兩個小型或中型機架，以讓您利用 EC2 置放群組在機架之間分配執行個體的能力。
- Outposts 上的 Amazon EC2 Placement 群組可用來影響 EKS 節點群組、EKS Local Cluster 控制平面節點和 ECS 任務的位置。
- 使用內部 VPC 通訊將工作負載分散到相同 VPC 內的多個 Outpost。

儲存

AWS Outposts 機架服務提供三種儲存類型：

- 支援的 EC2 執行個體類型上的執行個體儲存體
- 適用於持久性區塊儲存的 Amazon Elastic Block Store (EBS) gp2 磁碟區
- 適用於本機物件儲存的 Amazon Simple Storage Service on Outposts (S3 on Outposts)

執行個體儲存是在支援的伺服器 (C5d、M5d、G4dn、 R5d和 I3en) 上提供。如同 區域，執行個體存放區中的資料只會在執行個體的 （ 執行中 ） 生命週期內持續存在。

Outposts EBS 磁碟區和 S3 on Outposts 物件儲存作為 AWS Outposts 機架受管服務的一部分提供。客戶負責管理 Outpost 儲存集區的容量。客戶在訂購 Outpost 時指定其 EBS 和 S3 儲存體的儲存需求。使用提供請求儲存容量所需的儲存伺服器數量 AWS 來設定 Outpost。 AWS 負責 EBS 和 S3 on Outposts 儲存服務的可用性。佈建足夠的儲存伺服器，以提供 Outpost 高度可用的儲存服務。失去單一儲存伺服器不應中斷服務，也不應導致資料遺失。

您可以使用 AWS Management Console 和 CloudWatch 指標來監控 Outpost EBS 和 S3 on Outposts 容量使用率。

資料保護

對於 EBS 磁碟區： AWS Outposts rack 支援 EBS 磁碟區快照，以提供簡單且安全的資料保護機制，以保護區塊儲存資料。快照是 EBS 磁碟區的point-in-time增量備份。根據預設，Outpost 上的 Amazon EBS 磁碟區的快照會存放在 區域的 Amazon S3 上。如果您的 Outposts 已設定 S3 on Outposts 容量，您可以使用 Outposts 上的 EBS 本機快照，使用 S3 on Outposts 儲存將快照儲存在 Outposts 本機上。

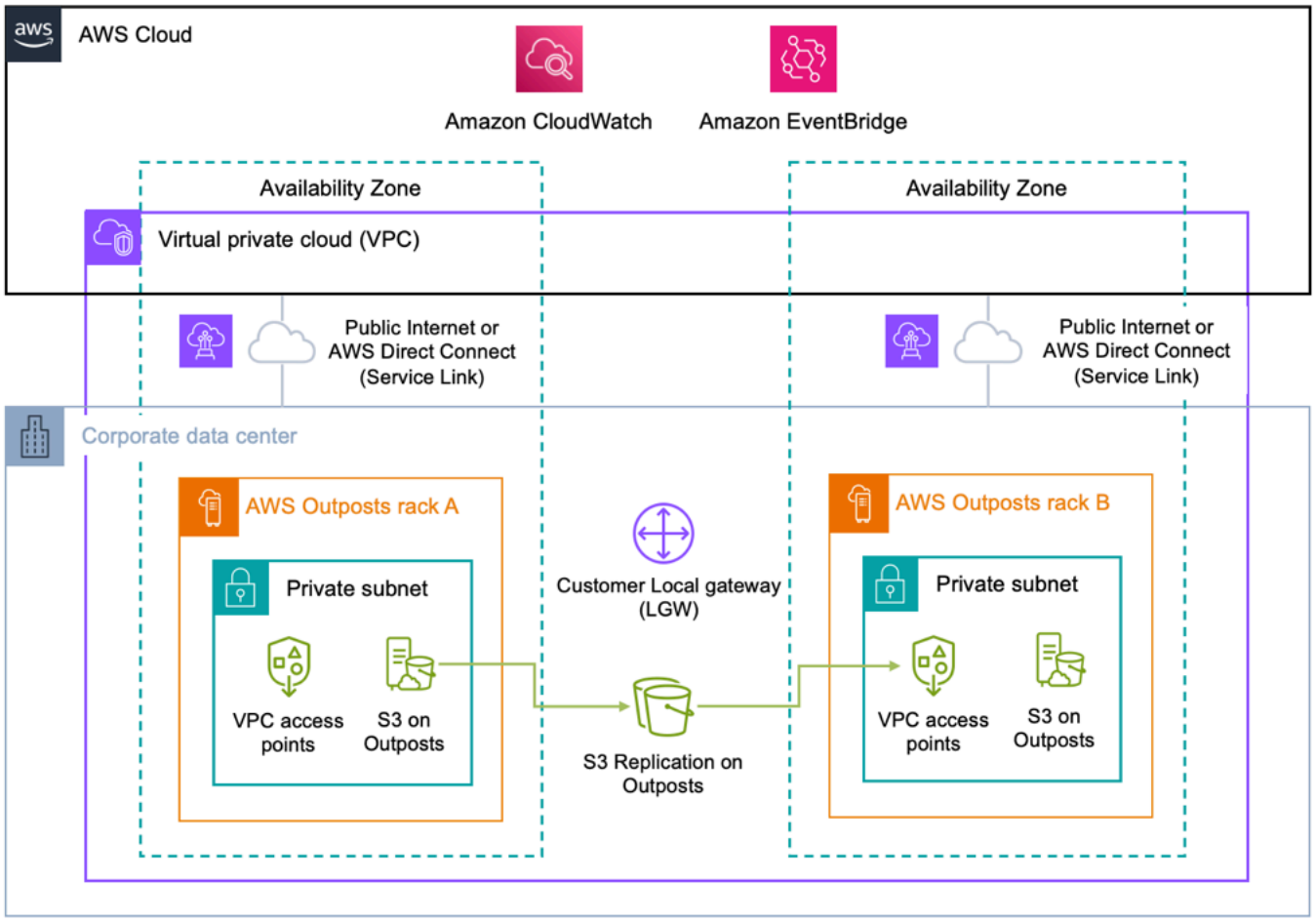
對於 S3 on Outposts 儲存貯體 （ 資料駐留使用案例 ）：

- 您可以在 Outpost 上使用 S3 版本控制，以儲存物件的所有變更和歷史記錄。啟用時，S3 版本控制會在相同的儲存貯體中儲存物件的多個不同複本。您可以使用 S3 版本控制，保留、擷取和還原在

Outposts 儲存貯體中所存放每個物件的各個版本。S3 版本控制可協助您從意外的使用者動作和應用程式失敗中復原。

- 您可以使用 S3 Replication on Outposts 來建立和設定複寫規則，以自動將 S3 物件複寫到另一個 Outpost，或相同 Outpost 上的另一個儲存貯體。在複寫期間，S3 on Outposts 物件會透過客戶的本機閘道 (LGW) 傳送，而物件不會傳回 AWS 區域。S3 Replication on Outposts 提供簡單且彈性的方式，可自動複寫特定資料周邊內的資料，以解決資料備援和合規需求。

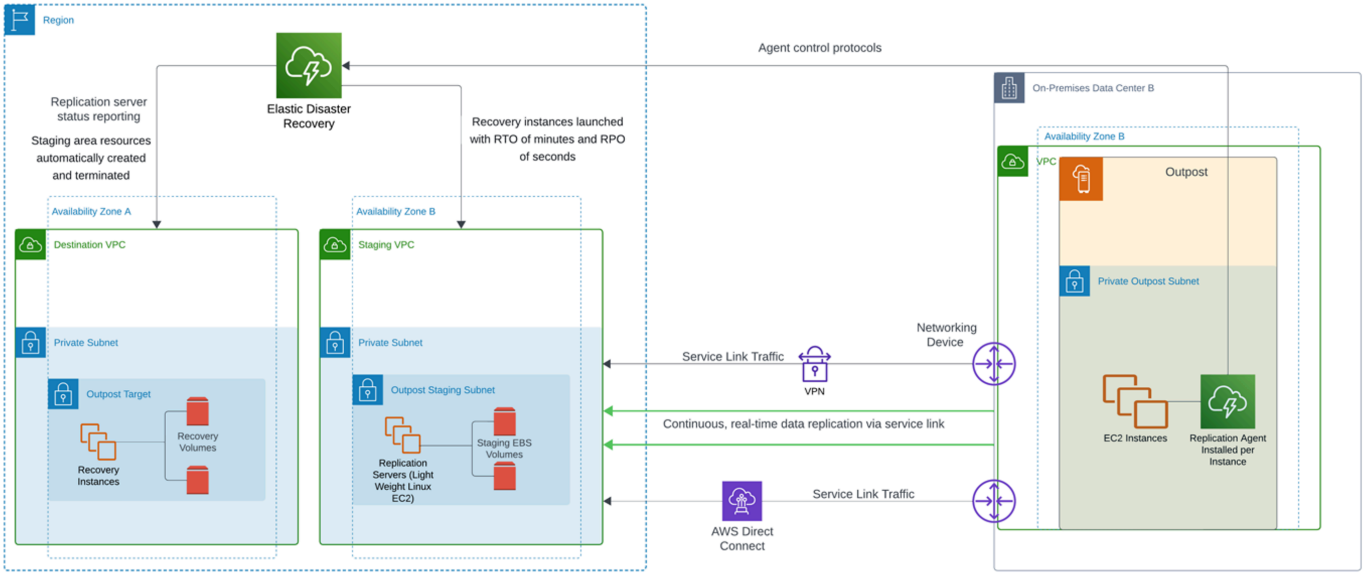
  S3 Replication on Outposts 也提供詳細的指標和通知，以監控物件複寫的狀態。您可以使用 Amazon CloudWatch 追蹤來源和目的地 Outposts 儲存貯體之間的待定位元組、待定操作和複寫延遲，藉此監控複寫進度。您也可以設定 Amazon EventBridge 規則來接收複寫失敗事件，以快速診斷和修正組態問題。如需如何設定的其他詳細資訊，請參閱 Amazon S3 Replication on Outposts YouTube 影片。



對於 S3 on Outposts 儲存貯體（非資料駐留使用案例）到 AWS 區域：您可以使用 AWS DataSync 來自動化 Outpost 與 區域之間的 Amazon S3 on Outposts 資料傳輸。DataSync 可讓您選擇要傳輸的內容、何時傳輸，以及要使用多少頻寬。將內部部署 S3 on Outposts 儲存貯體備份到 中的 S3 儲存貯

體， AWS 區域 可讓您利用 99.999999999% (11 個 9) 的資料耐用性和其他儲存層 （ 標準、不常存取和 Glacier)，以最佳化區域 S3 服務提供的成本。

執行個體複寫：您可以使用 AWS Elastic Disaster Recovery (AWS DRS) 將個別執行個體和連接的區塊儲存，從現場部署系統複寫到 Outpost、從 Outpost 到 區域、從 區域複寫到 Outpost，或從一個 Outpost 複寫到另一個 Outpost。使用 AWS Elastic Disaster Recovery 的 AWS Outposts 機架上的災難復原架構部落格文章說明了這些案例，以及如何使用 AWS DRS 設計解決方案。



從 Outpost 到 區域的災難復原 (DR)

使用 AWS Outposts 機架做為 AWS DRS 目的地 （ 複寫目標 ） 需要 S3 on Outposts 儲存體，用於儲存複寫的 Amazon EBS 快照。來源 Outposts 上也需要 S3 on Outposts 儲存以進行容錯回復。Outposts 機架必須使用直接 VPC 路由 (DVR) 來使用 AWS DRS。 AWS DRS 無法用於保護 Outposts 上的受管服務執行個體，它僅支援 EC2 執行個體及其連接的 EBS 磁碟區的災難復原。

資料保護的建議實務：

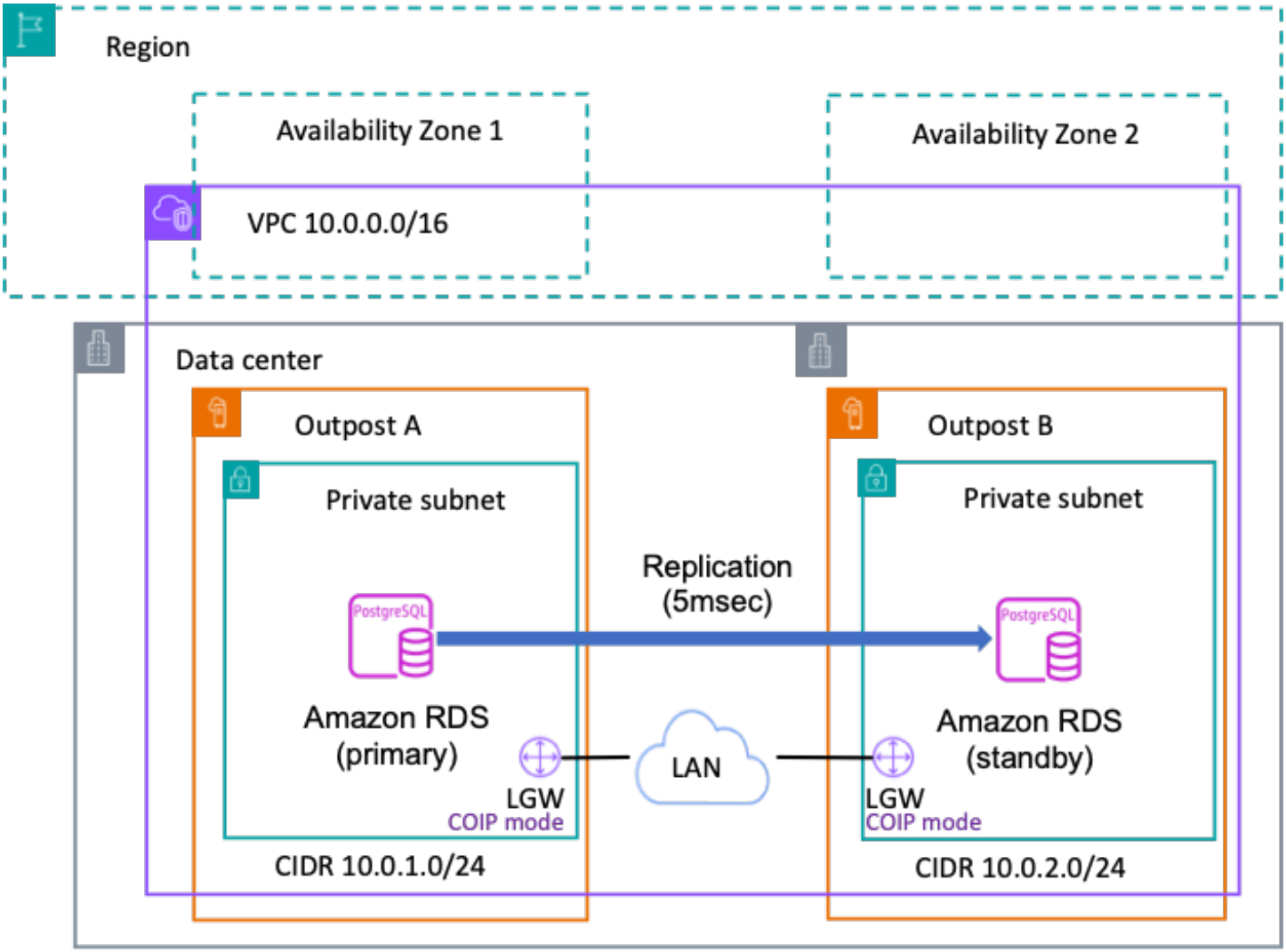
- 使用 EBS 快照建立區塊儲存磁碟區的point-in-time備份至區域或 Amazon S3 S3。
- 使用 S3 on Outposts 物件版本控制來維護物件的多個版本和歷史記錄。
- 在 Outposts 上使用 S3 Replication，自動將您的物件資料複寫到另一個 Outpost。
- 對於非資料駐留使用案例，請使用 AWS DataSync 將存放在 S3 on Outpost 中的物件備份至 區域中的 Amazon S3。
- 使用 AWS DRS 複寫現場部署系統、邏輯 Outpost 和 區域之間的執行個體。

資料庫

上的 Amazon Relational Database Service (RDS) AWS Outposts 將 RDS for SQL Server、RDS for MySQL 和 RDS for PostgreSQL 資料庫擴展到 AWS Outposts 部署。對於必須提供高可用性架構的部署，Amazon RDS 支援 PostgreSQL 和 MySQL 的多可用區域執行個體部署 AWS Outposts。

Amazon RDS on Outposts 搭配異地同步備份

在多可用區域部署中，Amazon RDS 會在一個 上建立主要資料庫執行個體， AWS Outposts 而 RDS 會同步複寫資料至不同 Outpost 上的待命資料庫執行個體。為了提供彈性架構，兩者 AWS Outposts 必須錨定到指定區域中的不同可用區域，並且必須在客戶擁有的 IP (CoIP) 模型上操作。為了允許主要執行個體和待命之間的複寫，兩個 Outpost 之間必須有一個網路連結，且往返時間 (RTT) 延遲為單一位數毫秒。我們建議不超過 5 毫秒。另請考慮調整 Outposts 之間的複寫連結大小，以有足夠的頻寬來避免佇列複寫任務。



Amazon RDS on Outpost 搭配多可用區域

Amazon RDS on Outposts 搭配多可用區域時的考量事項

在異地同步備份中檢閱 Amazon RDS on Outposts 部署的下列考量事項：

- 至少有兩個 Outposts 部署錨定到相同 中的不同可用區域 AWS 區域。
- 主要執行個體和待命執行個體都需要每個 Outpost 部署一個 VPC 和一個子網路。
- 將資料庫執行個體的 VPC 與所有本機閘道路由表建立關聯。
- 確保您的 Outposts 使用客戶擁有的 IP 路由。
- 您的本機網路必須允許 Outposts for Internet Security Association 和金鑰管理通訊協定 (ISAKAMP) 之間的傳出和相關傳入流量，這些通訊協定使用 UPD 連接埠 500 和 IPsec Network Address Translation Traversal (NAT-T) 使用 UDP 連接埠 4500。
- 多可用區域部署不支援本機 RDS 備份。
- 如果您的工作負載必須遵守產業或地理位置的資料駐留法規，請洽詢監管機構，以判斷多可用區域 RDS 是否符合您的需求。

如需詳細資訊，請參閱在 AWS Outposts 上使用 Amazon RDS 的異地同步備份部署。

Amazon RDS on AWS Outposts Read 複本

Amazon RDS 僅供讀取複本為 Amazon RDS 資料庫 (DB) 執行個體提供增強的效能和耐用性。它們可讓您輕鬆彈性擴展，超越單一資料庫執行個體的容量限制，適用於讀取密集型資料庫工作負載。Amazon RDS on AWS Outposts 使用 MySQL 和 PostgreSQL 資料庫引擎的內建複寫功能，從來源資料庫執行個體建立僅供讀取複本。來源資料庫執行個體會成為主要資料庫執行個體。對主要資料庫執行個體所做的更新，會以非同步方式複製到僅供讀取複本。僅供讀取複本使用客戶擁有的 IP (CoIP) 模型，複寫會在您的本機網路上執行。

Amazon RDS on Outposts 僅供讀取複本的考量

檢閱讀取複本的 Amazon RDS on Outposts 部署的下列考量事項：

- 您無法在 RDS on Outposts 資料庫執行個體上建立 RDS for SQL Server 的僅供讀取複本。
- RDS on Outposts 上不支援跨區域僅供讀取複本。
- RDS on Outposts 上不支援階層式僅供讀取複本。

- 來源 RDS on Outposts 資料庫執行個體不能具有本機備份。來源資料庫執行個體的備份目標必須是您的 AWS 區域。請確定您的備援服務連結連線至少為 500 mbps，以將 RDS 備份傳送至經常變更資料或繁重寫入流量的 AWS 區域 資料庫。
- 僅供讀取複本需要客戶擁有的 IP (CoIP) 集區。
- RDS on Outposts 上的僅供讀取複本只能在與來源資料庫執行個體相同的虛擬私有雲端 (VPC) 中建立。
- RDS on Outposts 上的僅供讀取複本可以位於與來源資料庫執行個體相同的 Outpost 或另一個 Outpost 上。
- 您無法為使用 AWS KMS 外部金鑰存放區 (XKS) 加密的資料庫執行個體建立僅供讀取複本。
- 建立您的僅供讀取複本做為異地同步備份部署資料庫執行個體，與來源資料庫是否為異地同步備份部署資料庫執行個體無關。

上的 Amazon RDS 儲存體自動擴展 AWS Outposts

如果您的工作負載是不可預測，您可啟用 Amazon RDS 資料庫執行個體的儲存體自動擴展。上的 Amazon Relational Database Service (Amazon RDS) AWS Outposts 支援手動和自動儲存擴展。啟用儲存體自動擴展功能後，當 Amazon RDS 偵測到資料庫執行個體耗盡可用資料庫空間時，會根據 Outposts 部署的大小 EBS 容量自動擴展您的儲存體。此功能提供與 區域相同的功能，其中有一些特定因素適用於自動調整規模，可在 Amazon RDS Autoscaling 指南中找到。請務必謹慎管理 Outposts 上 RDS 執行個體配置的最大儲存體，因為 EBS 資源僅限於 Outpost 中佈建的容量。Amazon RDS 儲存體自動擴展可讓您設定最大儲存限制，確保您的部署保持在可用的 EBS 容量內。如需管理 Outposts 容量的詳細資訊，請參閱本白皮書的容量管理一節。

AWS Outposts 本機備份上的 Amazon RDS

上的 Amazon RDS 本機備份 AWS Outposts可讓您直接從儲存在 Outposts 本機的 S3 復原 RDS 資料庫執行個體。這可讓您符合資料駐留需求，並相較於從 復原，減少延遲 AWS 區域。開啟 Amazon RDS 後 AWS Outposts，您有下列還原選項：

- 從存放在父區域中或 Outposts 本機的手動資料庫快照。
- 自動化備份 point-in-time復原 ）：
  - 如果從父系還原 AWS 區域，您可以將備份存放在 或 Outposts AWS 區域 上。
  - 如果從 Outpost 還原，備份必須儲存在具有 S3 支援的 Outposts 上本機。

上的 Amazon RDS 本機備份考量事項 AWS Outposts

請參閱下列考量事項，以利用 上的 Amazon RDS 本機備份 AWS Outposts：

- 您需要 S3 on Outposts 容量才能將備份存放在本機。
- MySQL 和 PostgreSQL 資料庫執行個體支援本機備份。
- 多可用區域執行個體部署或僅供讀取複本不支援本機備份。

上的 RDS 匯出和還原快照 AWS Outposts

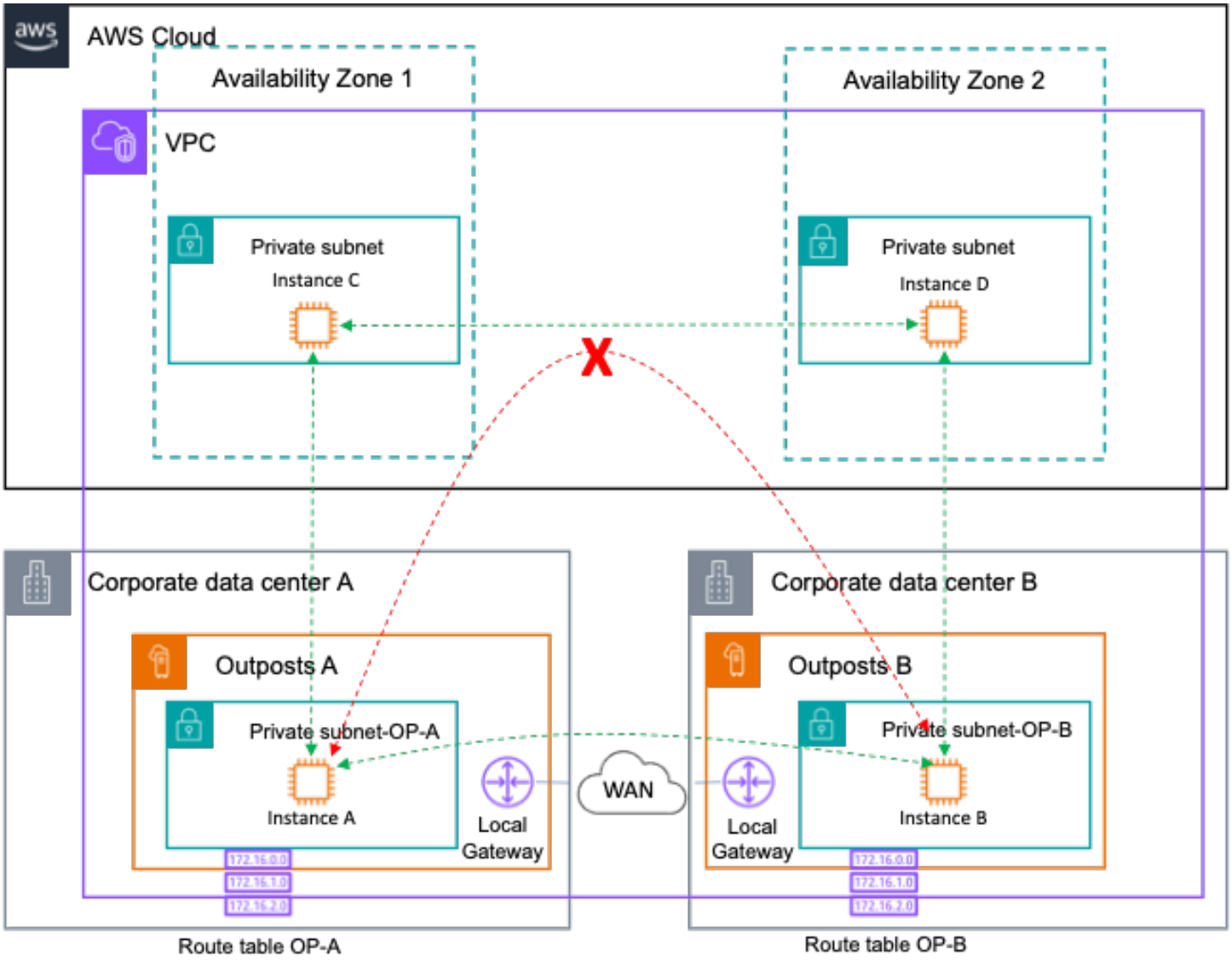
將快照匯出至 S3 並從 Amazon S3 還原資料庫執行個體：雖然 RDS 快照可以直接從 中的 Amazon S3 匯出或還原 AWS 區域，但在 AWS Outposts 環境中不支援此動作。

較大的失敗模式

若要設計 HA 架構來緩解更大的故障模式，例如機架、資料中心、可用區域 (AZ) 或區域故障，您應該在具有獨立電源和 WAN 連線能力的個別資料中心部署具有足夠基礎設施容量的多個 Outpost。您可以將 Outposts 錨定到 內的不同可用區域 (AZs) AWS 區域 或跨多個區域。您也應該在位置之間佈建彈性且足夠的site-to-site連線，以支援同步或非同步資料複寫和工作負載流量重新導向。根據您的應用程式架構，您可以使用全球可用的 Amazon Route 53 DNS 和 Outposts 上的 Amazon Route 53，將流量導向所需的位置，並在發生大規模故障時自動將流量重新導向至存活位置。

Outposts 機架內部 VPC 路由

AWS Outposts 機架支援跨多個 Outpost 進行 VPC 內通訊。兩個不同邏輯 Outpost 上的資源可以透過使用 Outpost 本機閘道 (LGW)，在跨越它們的相同 VPC 內路由子網路之間的流量，彼此通訊。透過跨多個 Outposts 的 VPC 內通訊，您可以使用本機 LGW 作為下一躍點，將更具體的路由新增至其他 Outposts 子網路，以覆寫 Outposts 子網路關聯路由表中的 Local Route。它可以為需要將兩個邏輯 Outpost 之間的 VPC 架構為跨兩個 Outposts 機架或跨 Amazon EKS 叢集的 Amazon ECS 的應用程式提供優勢。 AWS Outposts

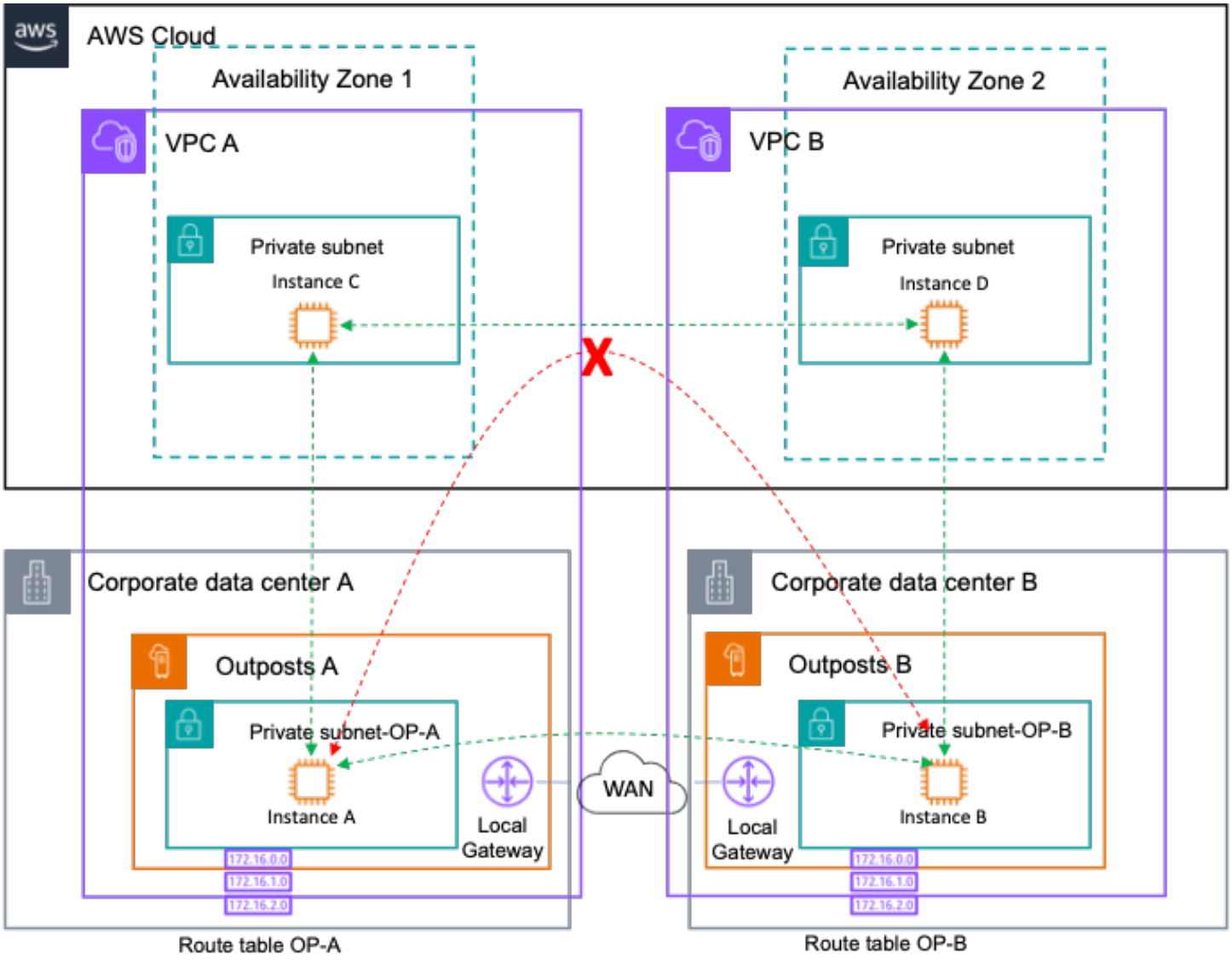


具有多個邏輯 Outpost 的單一 VPC 的網路路徑

Outposts-to-Outposts 透過 區域的流量路由遭到封鎖，因為這是反模式。此類流量會產生雙向的輸出費用，而且相較於透過客戶 WAN 路由流量，延遲會明顯較高。

Outposts Rack Inter-VPC 路由

部署在不同 VPCs 中的兩個不同 Outpost 上的資源可以跨客戶網路互相通訊。部署此架構可讓您透過本機內部部署和 WAN 網路，將流量 Outposts-to-Outposts路由至對應 Outposts/VPC 子網路。



具有多個邏輯 Outpost 的多個 VPC 的網路路徑

防止較大故障模式的建議實務：

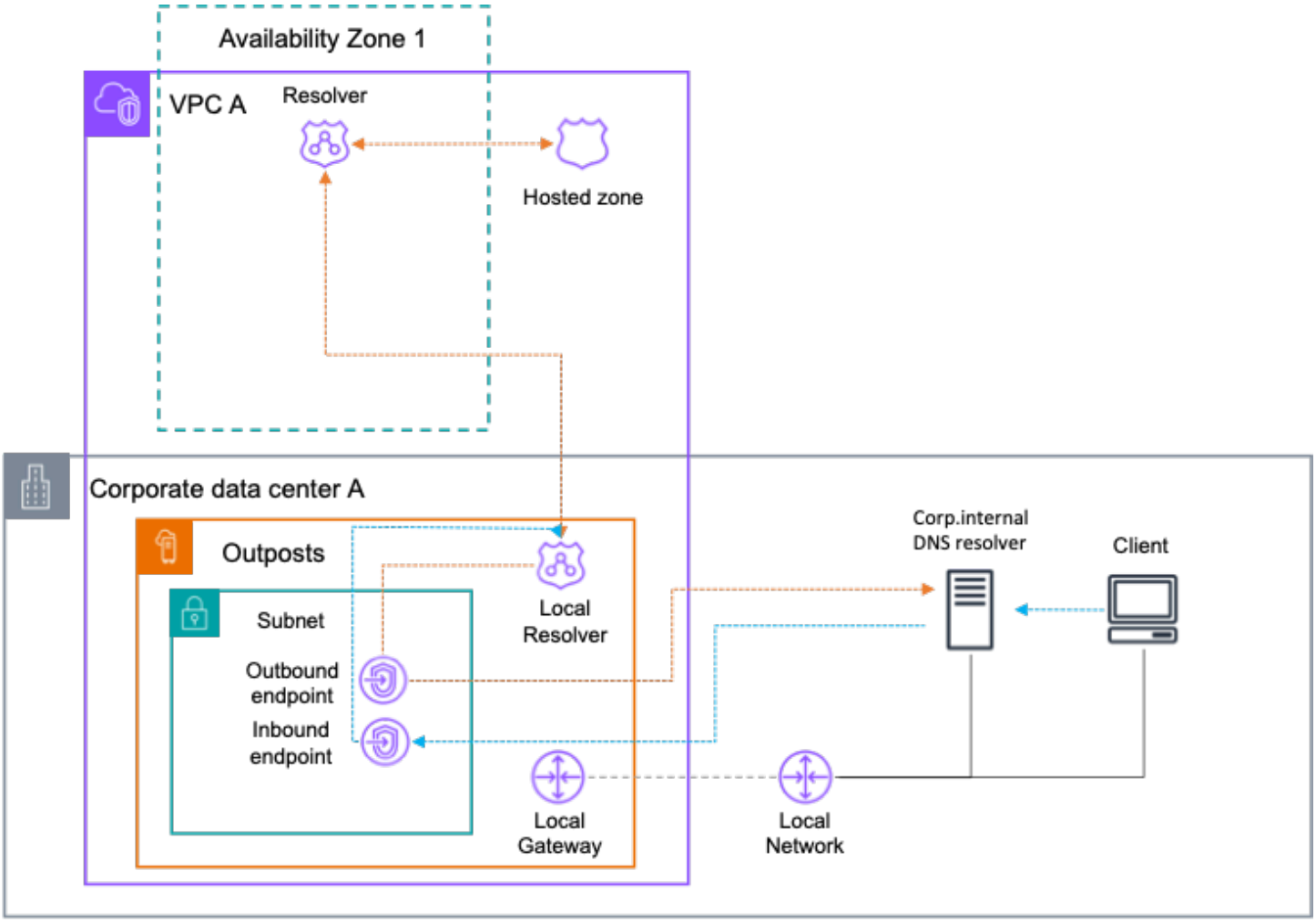
- 部署錨定到多個AZs和區域的多個 Outpost。
- 對多 Outpost 部署中的每個 Outpost 使用不同的 VPCs。

Outpost 上的 Route 53 本機解析程式

當 AWS Outposts 服務連結受到暫時中斷連線的影響時，本機 DNS 解析會失敗，導致應用程式和服務很難探索其他服務，即使它們在相同的 Outposts 機架上執行也一樣。不過，在 Route 53 Resolver 開啟的情況下 AWS Outposts，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，即使父

的連線中斷 AWS 區域。同時，針對內部部署主機名稱的 DNS 解析，Route 53 Resolver on Outposts 有助於減少延遲，因為查詢結果會在本機快取和提供，同時與 Route 53 Resolver 端點完全整合。

Route 53 解析程式傳入端點會將從 VPC 外部收到的 DNS 查詢轉送到在 Outposts 中執行的解析程式。相反地，Route 53 Resolver Outbound 可讓 Route 53 Resolvers 將 DNS 查詢轉送至您在內部部署網路上管理的 DNS 解析程式，如下圖所示。



Outposts 上的 Route 53 解析程式

Route 53 Resolver on Outposts 考量事項

考慮下列各項：

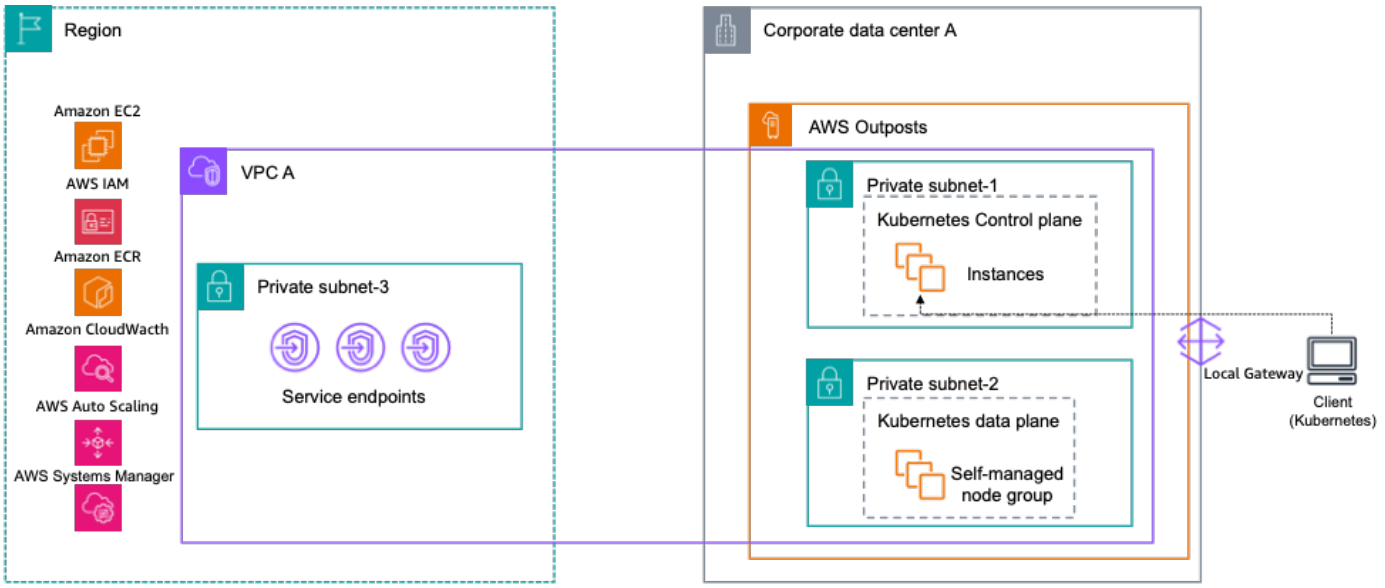
- 您必須啟用 Route 53 Resolver on Outposts，並且適用於整個 Outposts 部署，即使這涉及單一 Outposts ID 下的多個運算機架。
- 若要啟用此功能，您的 Outposts 必須有足夠的運算容量，以任何 c5.xlarge、m5.large 或 m5.xlarge 至少 4 個 EC2 執行個體的形式部署本機解析程式。

- 如果您使用的是私有 DNS，則必須與必要的 Outposts VPCs共用私有託管區域，以便在 Route 53 Resolver on Outposts 中本機快取記錄。
- 為了啟用與內部部署 DNS 與傳入和傳出端點的整合，您的 Outposts 必須有足夠的運算容量，才能為每個 Route53 端點部署兩個 EC2 執行個體。

Outpost 上的 EKS 本機叢集

當 Outposts 服務連結與父區域中斷連線時，做為 EKS 延伸叢集的服務可能會有挑戰，其中控制平面位於該區域。其中的挑戰是 EKS 控制平面與工作者節點和 PODs 之間的通訊中斷。雖然工作者節點和 PODs 都可以繼續在本機操作 和服務駐留在 Outposts 上的應用程式，但 Kubernetes 控制平面可能會認為它們運作狀態不佳，並在控制平面的連線復原時安排其替換。這可能會導致恢復連線時應用程式停機。

為了簡化此作業，您可以選擇在 Outposts 上託管整個 EKS 叢集。在此組態中，Kubernetes 控制平面和您的工作者節點都會在 Outposts 運算容量的本機內部部署上執行。如此一來，您的叢集即使在服務連結連線暫時中斷的情況下，以及還原後，仍會繼續運作。



Outposts 上的 Amazon EKS 本機叢集

Outposts 上的 EKS 本機叢集考量事項

在 Outposts 中部署 EKS 本機叢集時，有一些考量：

- 在中斷連線期間，沒有選項來執行任何需要新增工作者節點的叢集本身變更，或自動擴展節點群組，只要它取決於 EC2 和 ASG API 對 AWS 父區域的呼叫。

- • 在 eksctl AWS Outposts 支援上列出的本機叢集上，有一組不支援的功能。

結論

透過 AWS Outposts 機架，您可以使用熟悉的 AWS 工具和服務來建置、管理和擴展高可用性的內部部署應用程式，例如 Amazon EC2、Amazon EBS、Amazon S3 on Outposts、Amazon ECS、Amazon EKS 和 Amazon RDS。工作負載可以在本機執行、為用戶端提供服務、存取內部部署網路中的應用程式和系統，以及存取 中的完整服務集 AWS 區域。Outposts 機架非常適合需要低延遲存取內部部署系統、本機資料處理、資料駐留，以及具有本機系統相互依存性的應用程式遷移的工作負載。

當您為 Outpost 部署提供足夠的電力、空間，以及與 的冷卻和彈性連線時 AWS 區域，您可以建置高可用性的單一資料中心服務。此外，為了提高可用性和彈性，您可以部署多個 Outpost，並將應用程式分散到邏輯和地理邊界。

Outposts 機架可消除建置內部部署運算、儲存和應用程式聯網集區的無差異繁重負載，並可讓您將 AWS 全球基礎設施的範圍擴展到資料中心和主機代管設施。現在，您可以將時間和精力集中在現代化應用程式、簡化應用程式部署，以及增加 IT 服務的業務影響。

貢獻者

本文件的貢獻者包括：

- Jesus Federico，首席解決方案架構師，Telco，Amazon Web Services
- Mallory Gershenfeld、S3 on Outposts、Amazon Web Services
- Rob Goodwin，Amazon Web Services 混合雲端資深解決方案架構師
- Amazon Web Services 資深專家解決方案架構師 AWS Outposts Chris Lunsford
- Rohan Mathews | AWS Outposts Amazon Web Services 首席架構師
- Brianna Rosentrater，Amazon Web Services 混合邊緣專家解決方案架構師
- Amazon Web Services 首席混合邊緣專家解決方案架構師 Leonardo Solano
-

文件歷史記錄

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
主要更新	新增了有關聯網、DRS 支援、Amazon EKS 本機叢集、置放群組和 Amazon RDS on 的更新 AWS Outposts	2024 年 11 月 24 日
次要更新	在容量規劃中新增了額外的槽化指導。	2024 年 2 月 9 日
次要更新	更新以反映自初次發佈以來的功能啟動。	2023 年 7 月 19 日
次要更新	更新高可用性網路連接的建議實務。	2023 年 6 月 29 日
初次出版	白皮書已首次發佈。	2021 年 8 月 12 日

> **Note**
>
> 若要訂閱 RSS 更新，您必須為正在使用的瀏覽器啟用 RSS 外掛程式。

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品產品和實務，這些產品和實務可能隨時變更，恕不另行通知，且 (c) 不會從 AWS 及其附屬公司、供應商或授權方提供「原樣」的任何承諾或保證。 AWS 產品或服務不提供任何明示或暗示的保證、陳述或條件。 AWS 對其客戶的責任和責任受 AWS 協議控制，本文件不屬於 AWS 與其客戶之間的任何協議，也不會修改。

AWS 詞彙表

如需最新的 AWS 術語，請參閱 AWS 詞彙表 參考中的AWS 詞彙表。

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。