AWS 白皮书

AWS Outposts 高可用性設計與架構考量

AWS Outposts 高可用性設計與架構考量: AWS 白皮书

Table of Contents

AWS Outposts 高可用性設計與架構考量

出版日期：二零二一年八月十二文件歷史紀錄日

本白皮書討論 IT 管理員和系統架構設計人員可以應用的架構考量和建議做法，以建置高可用性的內部部署應用程式環境。 AWS Outposts

你是否 Well-Architected？

AWS Well-Architected 的架構可協助您瞭解在雲端中建置系統時所做決策的優缺點。Framework 的六大支柱可讓您學習如何設計和操作可靠、安全、高效、符合成本效益且可持續發展的系統的架構最佳實務。使用中免費提供的 AWS Well-Architected ToolAWS Management Console，您可以針對每個支柱回答一組問題，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 (參考架構部署、圖表和白皮書)，請參閱架構中心。AWS

簡介

本 paper 適用於希望使用 AWS 雲端平台部署、遷移和操作應用程式的 IT 經理和系統架構師，以及在具有 42U 機架式規格的AWS Outposts 機架內部部署執行這些應用程式。AWS Outposts

本文介紹架構模式、反模式，以及建立包含 AWS Outposts 機架之高可用性系統的建議作法。您將學習如何管理 AWS Outposts 機架容量，並使用網路和資料中心設施服務來設定高可用性 AWS Outposts 機架基礎架構解決方案。

AWS Outposts rack 是一項全受管服務，提供雲端運算、儲存和網路功能的邏輯集區。透過 Outposts 機架，客戶可以在其現場部署環境中使用 AWS 受支援的受管服務，包括：Amazon 彈性運算雲端(Amazon EC2)、Amazon S3 彈性區塊商店(Amazon EBS)、Amazon 彈性區塊商店 (Amazon EBS)、Amazon Relational Database Service 服務 (Amazon RDS)，以及 Outposts 上的其他服務。AWS在 Outposts 服務交付在相同的AWS 硝基系統中使用. AWS 區域

利用 AWS Outposts rack，您可以使用熟悉的 AWS 雲端服務和工具來建置、管理和擴充高可用性的內部部署應用程式。 AWS Outposts rack 非常適合需要低延遲存取內部部署系統、本機資料處理、資料存放區，以及移轉具有本機系統相互依存性之應用程式的工作負載。

將 AWS 基礎架構和服務延伸至內部部署

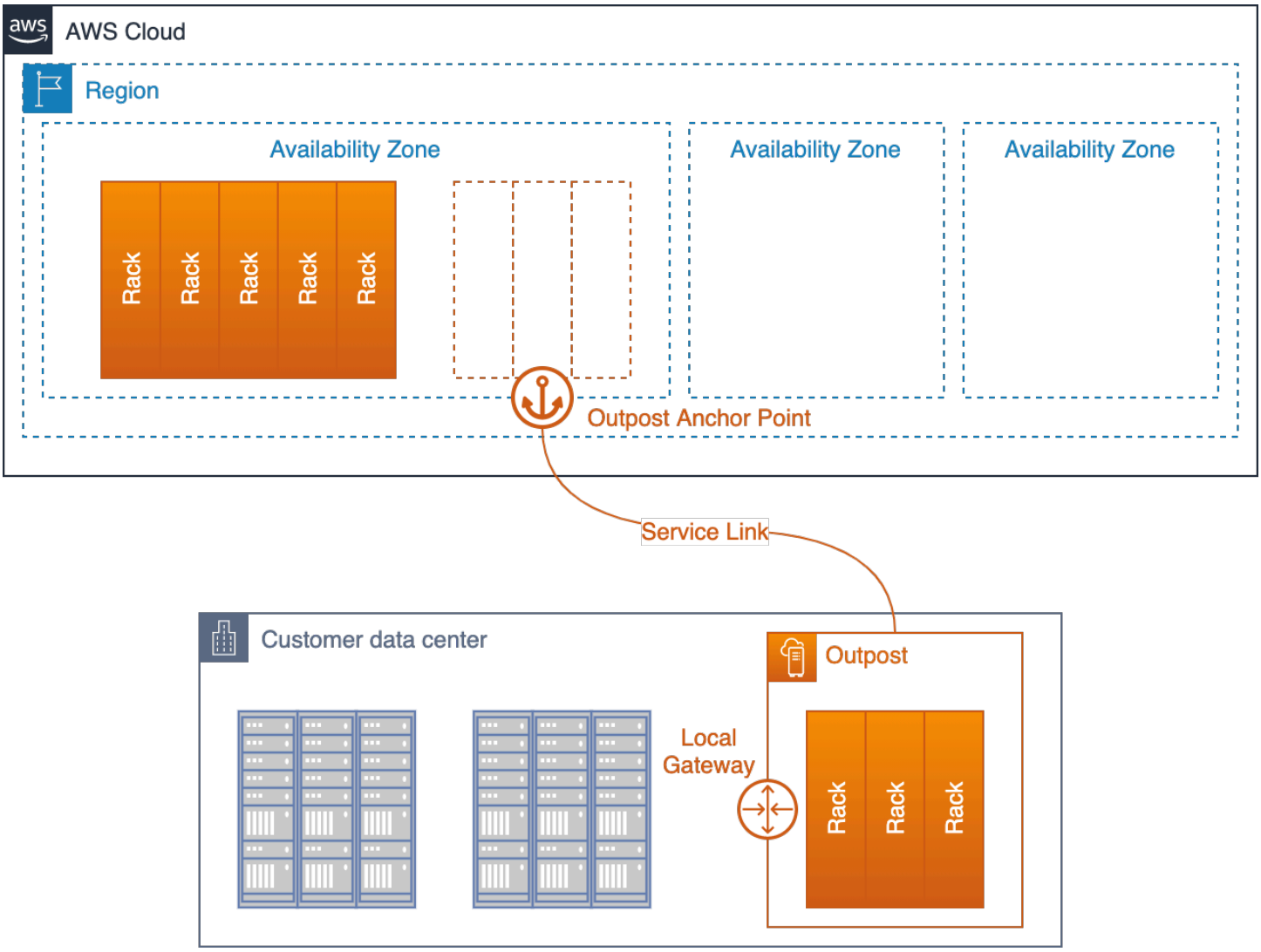
此 AWS Outposts 服務可為 50 多個國家和地區的內部部署位置提供 AWS 基礎架構和服務，讓客戶能夠將相同的 AWS 基礎結構、 AWS 服務、API 和工具部署到幾乎任何資料中心、主機代管空間或內部

部署設施，以獲得真正一致的混合體驗。要了解如何使用 Outposts 進行設計，您應該了解構成 AWS 雲的不同層級。

一個AWS 區域是世界的地理區域。每個都 AWS 區域 是資料中心的集合，這些資料中心按邏輯分組到可用區域 (AZ) 中。 AWS 區域 提供多個（至少兩個）物理分離和隔離的可用區域，這些可用區域以低延遲，高輸送量和冗餘網絡連接進行連接。每個 AZ 由一或多個實體資料中心組成。

邏輯前哨（以下稱為 Outpost）是一個或多個實體連接的 AWS Outposts 機架的部署，作為單一實體進行管理。Outpost 在您的其中一個站台上提供 AWS 運算和儲存容量集區，作為 AZ 的私有擴充功能。AWS 區域

也許最好的概念模型 AWS Outposts 是考慮從 AZ 的數據中心拔出一個或多個機架的插頭。 AWS 區域 您可以將機架從 AZ 資料中心捲到資料中心。然後，您可以使用（非常）長的纜線將機架插入 AZ 資料中心的錨點，以便機架繼續作為其中的一部分運作 AWS 區域。您也可以將它們插入區域網路，以便在內部部署網路與在這些機架上執行的工作負載之間提供低延遲的連線能力。



部署於客戶資料中心的前哨基地，並連接至其主要 AZ 和上層區域

前哨功能作為其錨定 AZ 的擴展。 AWS 操作、監控和管理 AWS Outposts 基礎設施作為 AWS 區域. 前哨站不是很長的實體纜線，而是透過一組稱為「服務連結」的加密 VPN 通道連線回其父區域。

服務連結終止於前哨站上層區域中可用區域 (AZ) 中的一組錨點。

您可以選擇儲存內容的位置。您可以將內容複製並備份到 AWS 區域 或其他位置。您的內容不會在未經您同意的情況下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具有約束力的命令而有必要。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。而且，雖然這些機架中可用的運算和儲存容量是有限的，而且無法容納執行的雲端規模服務 AWS 區域，但是機架上部署的資源 (您的執行個體及其本機儲存) 可在管理平面繼續在中運作時獲得本機執行的好處。 AWS 區域

若要在 Outpost 上部署工作負載，請將子網路新增至 Virtual Private Cloud (VPC) 環境，並指定 Outpost 做為子網路的位置。然後，透過 CLI、API、CDK 或基礎結構即程式碼 (IaC) 工具部署支援的 AWS 資源時，您可以選取所需的子網路。 AWS Management Console Outpost 子網路中的執行個體透過 VPC 網路與 Outpost 或區域中的其他執行個體進行通訊。

Outpost 服務連結承載前哨管理流量和客戶 VPC 流量 (Outpost 上子網路與區域中子網路之間的 VPC 流量)。

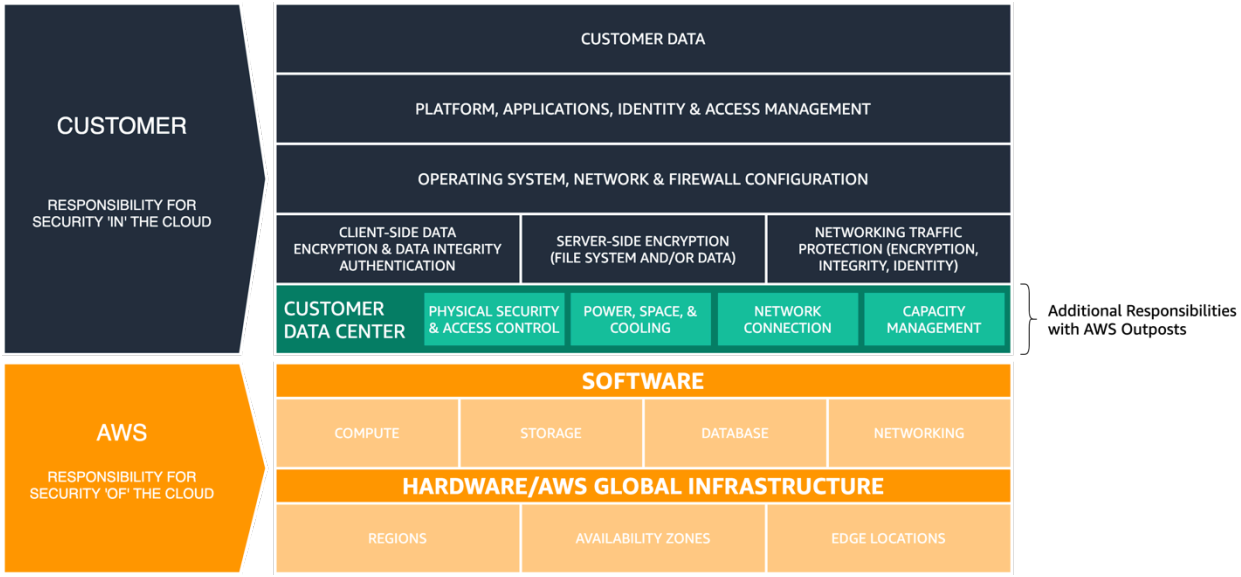
重要條款：

- AWS Outposts— 是一項完全受控的服務，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 基礎結構、 AWS 服務、API 和工具，以獲得真正一致的混合體驗。
- Outpost — 是一個或多個實體連接 AWS Outposts 機架的部署，這些機架是以單一邏輯實體的形式管理，以及部署於客戶站點的 AWS 運算、儲存和網路集區。
- 父區域 — AWS 區域 為 Outpost 部署提供管理、控制平面服 AWS 務和區域服務。
- 錨點可用區域 (錨點 AZ) — 上層區域中的可用區域，裝載前哨的錨點。前哨功能作為其錨可用區域的擴展。
- 錨點 — 錨定 AZ 中的端點，可從遠程部署的 Outposts 接收連接。
- 服務連結 — 一組加密的 VPN 通道，可將前哨站連接到其父區域中的錨定可用區域。
- 本機閘道 (LGW) — 邏輯互連虛擬路由器，可在 Outpost 與內部部署網路之間進行通訊。

瞭解更新的共同責任模式

當您將 AWS Outposts 基礎結構部署到資料中心或主機代管設施時，您需要承擔AWS 共同責任模型中的其他責任。例如，在區域中， AWS 提供多樣化的電源、備援核心網路和彈性的廣域網路 (WAN) 連線能力，以確保在發生一或多個元件故障時提供服務。

透過 Outposts，您有責任為 Outpost 機架提供彈性的電源和網路連線能力，以滿足在 Outposts 上執行的工作負載的可用性需求。



AWS 共同責任模型已更新 AWS Outposts

您必須對資料中心環境的實體安全性和存取控制負責。 AWS Outposts您必須提供足夠的電力、空間和冷卻裝置，以保持 Outpost 的運作和網路連線，才能將 Outpost 連接回該地區。

由於 Outpost 容量是有限的，並且取決於您站點上 AWS 安裝的機架大小和數量，因此您必須決定在 Outposts 容量上執行初始工作負載、因應 future 成長，並提供額外容量以減輕伺服器故障和維護事件所需的 EC2、EBS 和 S3。

AWS 負責 Outposts 基礎架構的可用性，包括 AWS Outposts 機架內的電源供應器、伺服器和網路設備。 AWS 還管理虛擬化管理程序，存儲系統和 Outposts 上運行的 AWS 服務。

每個 Outposts 機架中的中央電源架可從交流電轉換為直流電，並透過匯流排架構為機架內的伺服器供電。使用匯流排列架構，機架中一半的電源供應器可能會故障，而且所有伺服器都會持續不間斷地執行。

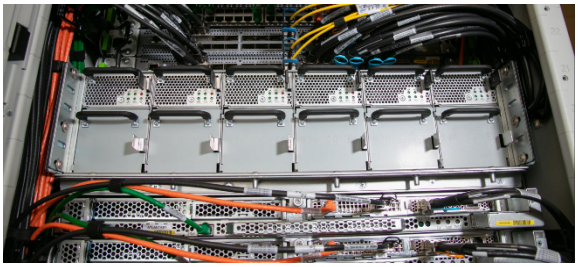


圖 3-交 AWS Outposts 流對直流電源供應器和匯流排條配電

Outposts 機架內部和之間的網路交換器和接線也完全備援。光纖控制面板可在 Outpost 機架與內部部署網路之間提供連線，並做為客戶管理的資料中心環境與受管理環境之間的分界點。 AWS Outposts

就像在該地區一樣， AWS 負責 Outposts 上提供的雲端服務，並在您選擇和部署更高層級的受管服務 (例如 Amazon RDS on Outposts) 時承擔額外的責任。當您考慮並選擇要部署在 Outposts 上的服務時，您應該檢閱個別服務的AWS 共同責任模型和常見問題 (FAQ) 頁面。這些資源提供了有關您和之間責任劃分的其他詳細信息 AWS。

在失敗模式方面思考

在設計高可用性應用程式或系統時，您必須考慮哪些元件可能會失敗、元件故障會對系統造成何種影響，以及您可以實作哪些機制來減輕或消除元件故障所造成的影響。您的應用程式是否在單一伺服器、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或永久性故障時，會發生什麼情況？ 當網路或應用程式本身等關鍵子系統發生故障時，會發生什麼情況？ 這些都是失敗模式。

規劃 Outposts 和應用程式部署時，您應該考慮本節中的失敗模式。以下各節將檢閱如何緩解這些失敗模式，為您的應用程式環境提供更高層級的高可用性。

故障模式 1：網絡

Outpost 部署取決於與其上層區域的彈性連線來進行管理和監控。網路中斷可能是由於各種故障造成的，例如操作員錯誤、設備故障和服務供應商中斷。前哨站可能由一個或多個在站點連接在一起的機架組成，如果無法通過服務鏈接與該地區進行通信，則被視為中斷連接。

備援網路路徑可協助降低中斷連線事件的風險。您應該對應應用程式相依性和網路流量，以瞭解中斷連線事件對工作負載作業的影響。規劃足夠的網路備援，以符合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 本機閘道 (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。當 Outpost 與區域中斷連線時，變更要求 (例如在 Outpost 上啟動或停止執行個體)、控制平面作業和服務遙測 (例如 CloudWatch 指標) 將會失敗。

失敗模式 2：執行個體

如果 EC2 執行個體執行個體所在的伺服器發生問題，或執行個體遇到作業系統或應用程式故障，則 EC2 執行個體可能會受損或失敗。應用程式處理這些失敗類型的方式取決於應用程式架構。整合式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故障的元件以維持服務可用性。

您可以使用 EC2 Auto Scaling 群組等自動化機制，以新執行個體取代失敗的執行個體 如果剩餘伺服器上有足夠的備用容量，則執行個體 auto 復原可以重新啟動因伺服器故障而失敗的執行個體。

故障模式 3：計算

伺服器可能會故障或受損，而且可能因各種原因而需要（暫時或永久）停止運作，例如元件故障和排程的維護作業。Outposts 機架上的服務如何處理伺服器故障和損壞的情況會有所不同，且可能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是所需容量，而且M是佈建用於因應伺服器故障的備用容量。

故障伺服器的硬體更換作為全受管 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網路裝置的健全狀況。如果需要進行物理維護， AWS 將安排一段時間訪問您的站點以更換故障的組件。佈建備用容量可讓您在失敗的伺服器停止服務和更換時保持工作負載的執行。

故障模式 4：機架或資料中心

機架故障可能是由於機架完全喪失電力，或是由於環境故障，例如因洪水或地震造成冷卻損壞或資料中心造成的實體損壞。資料中心配電架構的缺陷或標準資料中心電源維護期間出現錯誤，可能會導致一個或多個機架甚至整個資料中心的電源中斷。

透過將基礎結構部署到多個資料中心樓層，或在相同園區或都會區域內彼此獨立的位置，可以緩解這些情況。

使用 AWS Outposts 機架採用這種方法將需要仔細考慮應用程式的架構和分配方式，以便跨多個獨立的邏輯 Outposts 執行，以維護應用程式的可用性。

故障模式 5： AWS 可用區域或區域

每個前哨都錨定到. AWS 區域錨定 AZ 或父區域內的故障可能會導致前哨管理和可變性的損失，並可能破壞前哨站和區域之間的網絡通信。

與網路故障類似，AZ 或區域故障可能會導致前哨站與區域中斷連線。在 Outpost 上執行的執行個體會繼續執行，並可透過 Outpost 本機閘道 (LGW) 從內部部署網路存取，如果依賴區域中的服務，如先前所述，可能會受損或失敗。

為了減輕 AWS AZ 和區域故障的影響，您可以部署多個 Outposts，每個前哨站都錨定到不同的可用區域或區域。然後，您可以使用許多目前用於設計和部署的類似機制和架構模式，將工作負載設計為在分散式多 Outpost 部署模式中操作。 AWS

使用機架構建置 HA 應用程式和基礎 AWS Outposts 架構

透過 AWS Outposts rack，您可以使用熟悉的 AWS 雲端服務和工具來建置、管理和擴充高可用性的內部部署應用程式。請務必瞭解雲端 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。

使用傳統的內部部署 HA 應用程式部署，應用程式會部署在虛擬機器 (VM) 中。部署和維護複雜的 IT 系統和基礎架構，以保持這些虛擬機器的運作狀態和健康狀態。虛擬機器通常具有特定的身份，並且每個 VM 可能在整個應用程序架構中扮演關鍵角色。

架構角色與 VM 身分緊密結合。系統架構設計人員利用 IT 基礎架構功能來提供高可用性的 VM 執行階段環境，讓每個 VM 都能夠可靠地存取運算容量、儲存磁碟區和網路服務。如果虛擬機器故障，則會執行自動或手動復原程序，將失敗的虛擬機器還原為健康狀態，通常會完全位於其他基礎結構或其他資料中心。

雲端 HA 架構採用不同的方法。 AWS 雲端服務提供可靠的運算、儲存和網路功能。應用程式元件會部署至 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體化，也許是執行該角色的眾多元件之一。應用程式元件彼此鬆散耦合，以及它們在整個應用程式架構中扮演的角色。執行個體的個別識別通常並不重要。可能會建立或銷毀其他執行個體，以因應需求擴展或縮減規模。失敗的執行個體或運作狀態不良的執行個體只會被新的健康狀態良

AWS Outposts rack 是一項全受管服務，可將 AWS 運算、儲存、網路、資料庫和其他雲端服務延伸至內部部署位置，以獲得真正一致的混合體驗。您不應該將 Outposts 機架服務視為具有傳統內部部署 HA 機制的 IT 基礎架構系統的立即替代品。嘗試使用 AWS 服務和 Outposts 來支援傳統的內部部署 HA 架構是一種反模式。

在機 AWS Outposts 架上執行的工作負載使用雲端 HA 機制，例如 Amazon EC2 Auto Scaling (水平擴展以符合工作負載需求)、EC2 運作狀態檢查 (用於偵測和移除運作狀態不良的執行個體) 和應用程式負載平衡器 (將傳入的工作負載流量重新導向到擴展或取代的執行個體)。將應用程式移轉至雲端時，無論是移轉至雲端 AWS 區域 還是機 AWS Outposts 架，都應該更新您的 HA 應用程式架構，以開始利用受管理的雲端服務和雲端 HA 機制。

以下各節將介紹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的架構模式、反模式和建議做法。這些章節介紹了模式和做法；但是，它們不提供配置和實施詳細信息。當您為 Outposts AWS Outposts 機架準備環境和應用程式以移轉至 AWS 服務時，請閱讀並熟悉機架上執行之服務的機架常見問題與使用者指南，以及在 Outposts 機架上執行之服務的常見問題解答和服務文件。

主題

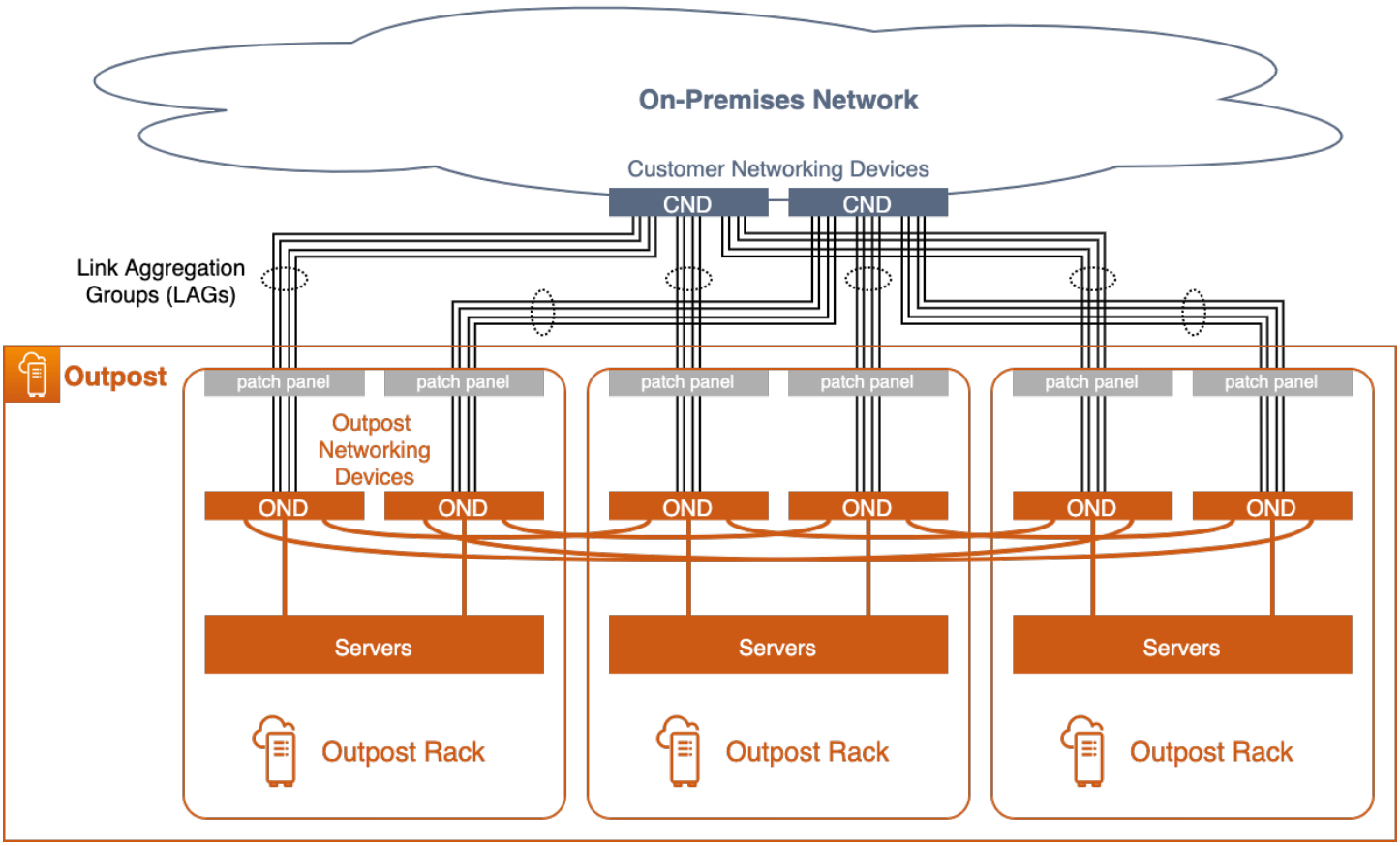
聯網

Outpost 部署取決於與其錨定 AZ 的彈性連線，以便管理、監控和服務作業正常運作。您應該佈建內部部署網路，以便為每個 Outpost 機架提供備援網路連線，並可靠的連線能力回到 AWS 雲端中的錨點。另外，請考慮在 Outpost 上執行的應用程式工作負載與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

網路附件

每個 AWS Outposts 機架都配備備有稱為前哨網路裝置 (OND) 的備援 top-of-rack 交換器。每個機架中的計算和存儲服務器都連接到兩個 OND。您應該將每個 OND 連接到資料中心中稱為客戶網路裝置 (CND) 的個別交換器，以便為每個 Outpost 機架提供多樣化的實體和邏輯路徑。OND 使用光纖電纜和光收發器通過一個或多個物理連接連接到您的 CND。實體連線是在邏輯連結彙總群組 (LAG) 連結中設定的。



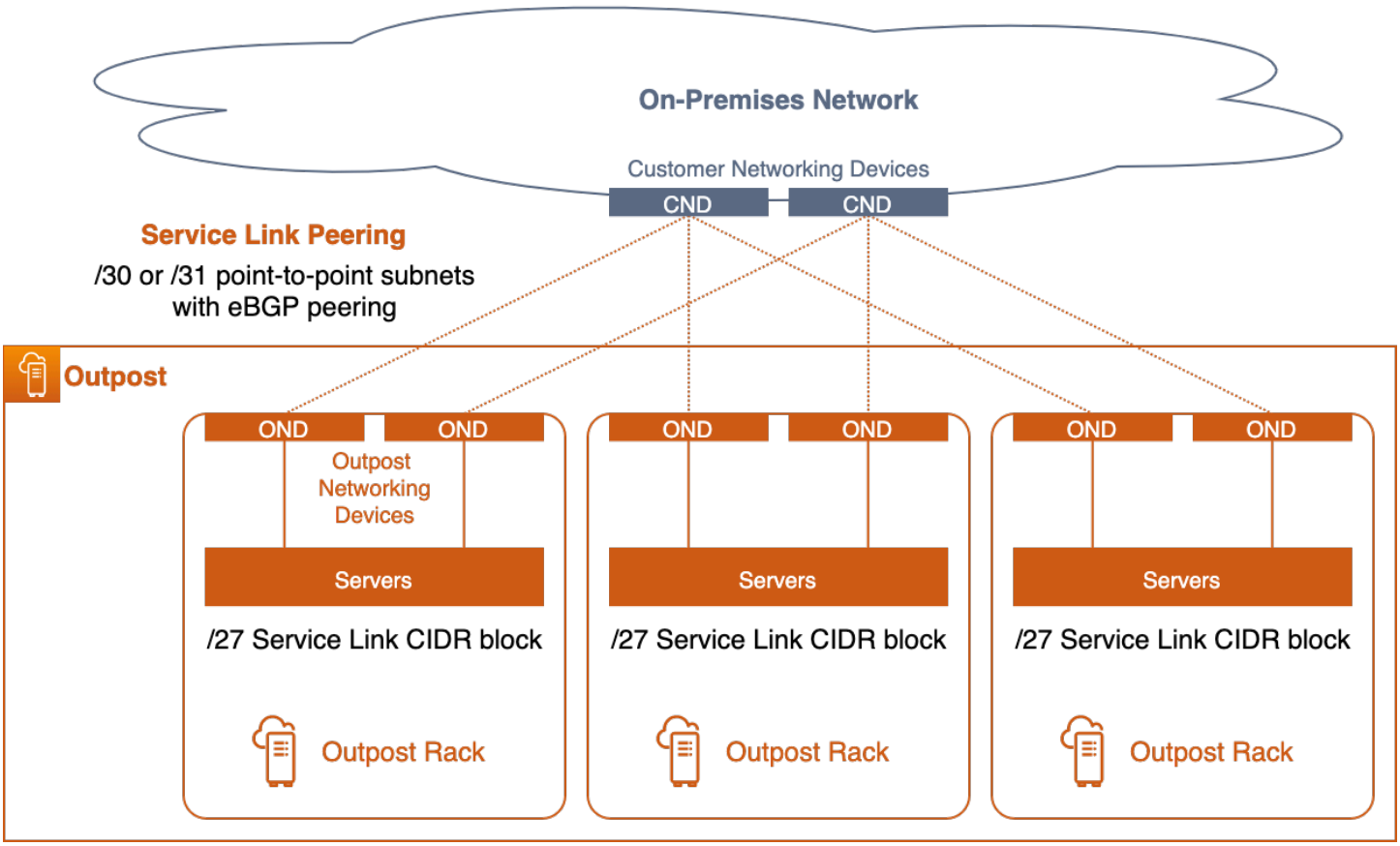
具備備援網路附件的多機架前哨

OND 到 CND 連結始終設定在 LAG 中，即使實體連線是單一光纖纜線也一樣。將連結設定為 LAG 群組可讓您透過向邏輯群組新增其他實體連線來增加連結頻寬。LAG 連結會設定為 IEEE 802.1q 乙太網路主幹線，以啟用前哨與內部部署網路之間的隔離網路。

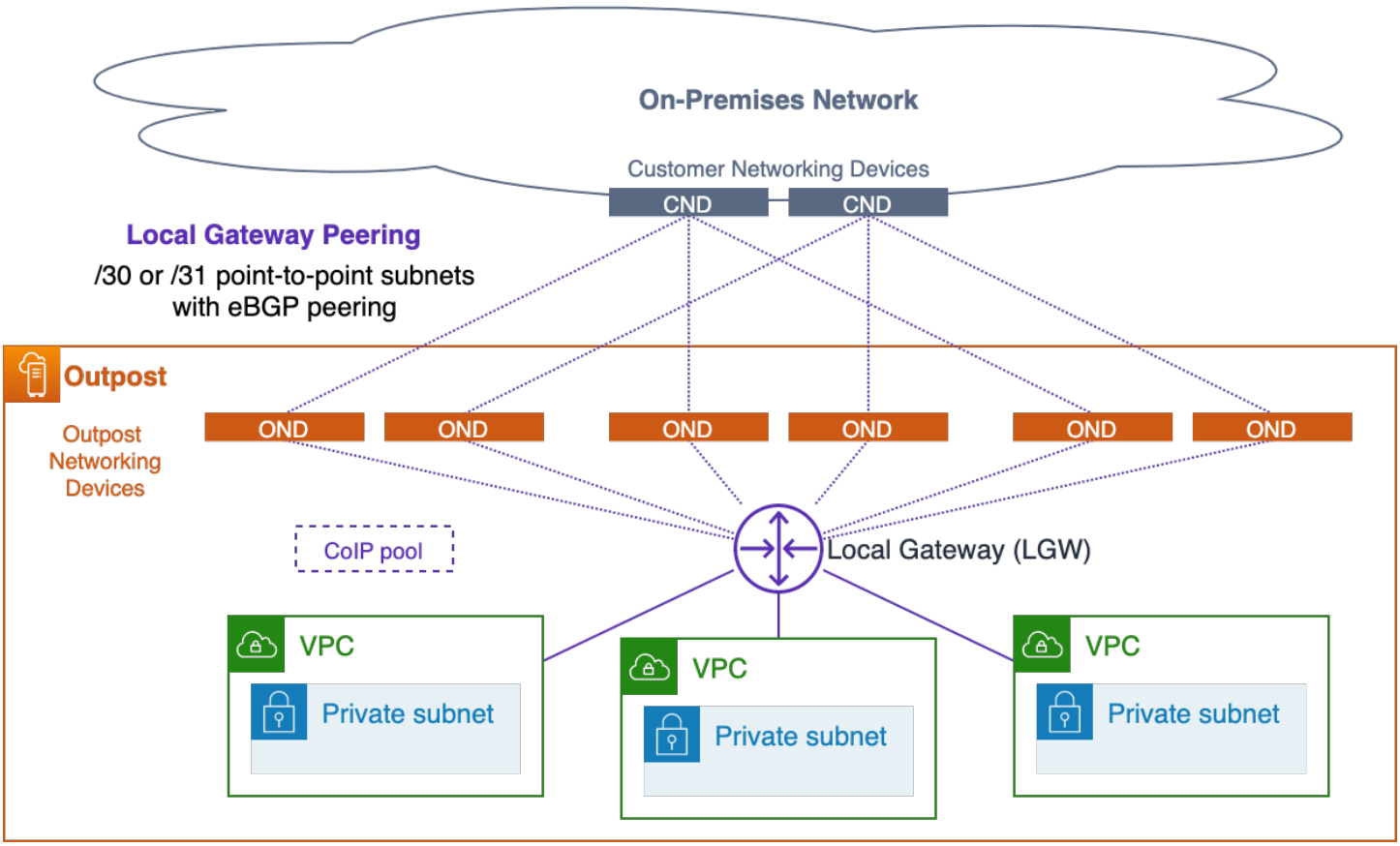
每個前哨都有至少兩個邏輯上隔離的網路，這些網路需要與客戶網路或跨客戶網路通訊：

- 服務連結網路 — 將服務連結 IP 位址分配給 Outpost 伺服器，並促進與內部部署網路的通訊，以允許伺服器連線回區域中的 Outpost 錨點。
- 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。

這些隔離網路會透過 LAG 連結的一組 point-to-point IP 連線，連接至內部部署網路。每個 OND 到 CND LAG 連結都設定了 VLAN 識別碼、 point-to-point (/30 或 /31) IP 子網路，以及每個隔離網路 (服務連結和 LGW) 的 EBGP 對等互連。您應該將 LAG 連結及其 point-to-point VLAN 和子網路視為第 2 層分段路由第 3 層連線。路由的 IP 連線提供備援邏輯路徑，可促進 Outpost 與內部部署網路上隔離的網路之間的通訊。


On-Premises Network
Customer Networking Devices
CND
CND
Service Link Peering
/30 or /31 point-to-point subnets
with eBGP peering
Outpost
OND
OND
Outpost
Networking
Devices
Servers
/27 Service Link CIDR block
Outpost Rack
OND
OND
Servers
/27 Service Link CIDR block
Outpost Rack
OND
OND
Servers
/27 Service Link CIDR block
Outpost Rack

服務連結對等



本機閘道對等互連

您應該在直接連接的 CND 交換器上終止第 2 層 LAG 連結 (及其 VLAN)，並在 CND 交換器上設定 IP 介面和 BGP 對等互連。您不應在資料中心交換器之間橋接 LAG VLAN。若要取得更多資訊，請參閱《使用指南》中的AWS Outposts 〈網路層連線〉

在邏輯多機架 Outpost 內，OND 會以冗餘方式互連，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能力。 AWS 負責前哨內的網絡可用性。

高可用性網路附件的建議作法

- 將 Outpost 機架中的每個前哨網路裝置 (OND) Connect 到資料中心的個別客戶網路裝置 (CND)。
- 在直接連接的客戶網路裝置 (CND) 交換器上終止第 2 層連結、VLAN、第 3 層 IP 子網路和 BGP 對等。請勿將 OND 橋接至 CND 之間或跨內部部署網路的 CND VLAN。
- 新增連結匯總群組 (LAG) 的連結，以增加 Outpost 和資料中心之間的可用頻寬。不要依賴通過兩個 OND 的不同路徑的聚合帶寬。
- 透過備援 OND 使用各種路徑，在 Outpost 網路與內部部署網路之間提供彈性的連線能力。
- 若要達到最佳備援並允許不中斷的 OND 維護，我們建議客戶設定 BGP 通告和原則，如下所示：

- 客戶網路設備應在不變更 BGP 屬性的情況下接收來自 Outpost 的 BGP 廣告，並啟用 BGP 多重路徑/負載平衡，以達到最佳的入站流量流量 (從客戶到前哨)。AS 路徑前置詞用於 Outpost BGP 前綴，以便在需要維護的情況下將流量從特定的開/上行轉移。客戶網絡應該更喜歡從 AS-Path 長度為 1 的前哨路由，而不是 AS 路徑長度為 4 的路由，也就是對 AS 路徑預先處理做出反應。
- 客戶網絡應向前哨中的所有 OND 公告具有相同屬性的相同 BGP 前綴。根據預設，Outpost 網路負載會平衡所有上行之間的輸出流量 (對客戶)。在前哨端使用路由原則，以便在需要維護的情況下將流量從特定 OND 轉移。所有 OND 上的客戶端均需要相同的 BGP 前綴才能執行此流量轉移，並以不中斷的方式執行維護。當客戶的網路需要進行維護時，我們建議您使用預先處理的 AS-Path，以暫時將流量從特定上行或裝置轉移出來。

錨栓連接

Outpost 服務連結會連線到 Outpost 上層區域中特定可用區域 (AZ) 中的公用或私人錨點 (不是兩者皆有)。前哨伺服器會從其服務連結 IP 位址到錨定 AZ 中的錨點，啟動輸出服務連結 VPN 連線。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。

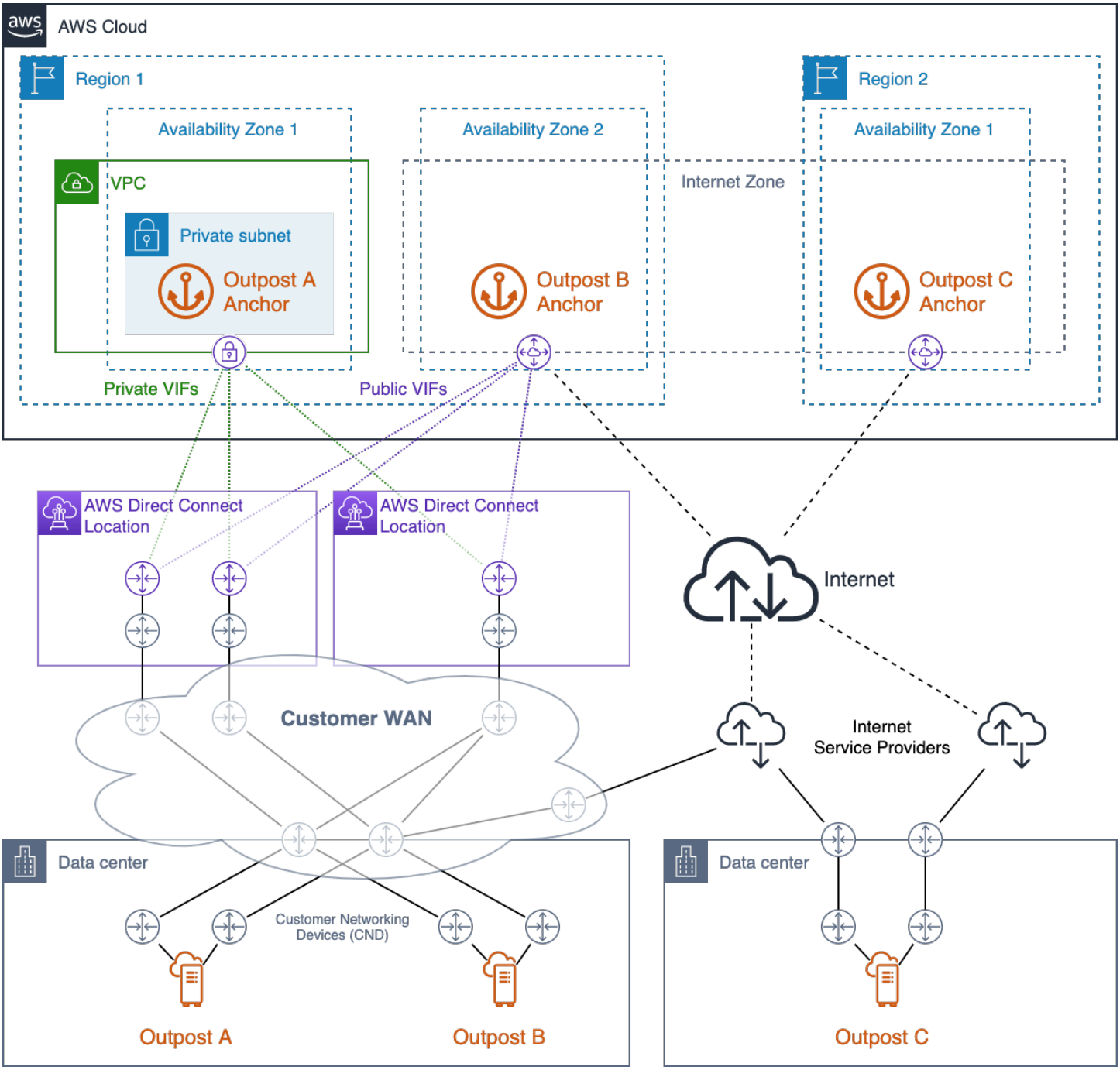
您必須確保前哨服務鏈接 IP 地址可以通過您的網絡連接到錨定 AZ 中的錨點。服務連結 IP 位址不需要與內部部署網路上的其他主機通訊。

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) 公用虛擬界面 (VIF) 存取。使用公共錨點允許更靈活的路徑選擇，因為服務鏈接流量可以通過任何可以成功到達公共互聯網上的錨點的可用路徑進行路由。

私人錨點可讓您使用 IP 位址範圍進行錨點連線。私人錨點是使用客戶指派的 IP 位址，在專用 VPC 內的私有子網路中建立。VPC 是在擁有 Outpost 資源 AWS 帳戶 的中建立的，您必須負責確保 VPC 可用且設定正確 (請勿刪除它！)。必須使用直 Connect 私有 VIF 存取私有錨點。

您應該在 Outpost 和區域中的錨點之間佈建冗餘網路路徑，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網路裝置失敗時，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 路徑的故障不會壓倒剩餘的路徑。

下圖顯示了三個 Outposts，其冗餘網絡路徑到他們的錨定 AZ 使用以 AWS Direct Connect 及公共互聯網連接。前哨 A 和前哨 B 會錨定至相同區域中的不同可用區域。前哨 A 連接到區域 1 的 AZ 1 的私人錨點。前哨 B 連接到區域 1 的 AZ 2 的公共錨點。前哨 C 連接到區域 2 的 AZ 1 的公共錨點。



具有高可用性的錨栓連接 AWS Direct Connect 和公共互聯網訪問

前哨 A 有三個冗餘網絡路徑到達其私有錨點。在單一「直接 Connect」位置透過備援的直接 Connect 電路提供兩條路徑。第三條路徑可透過第二個直接 Connect 位置的直接 Connect 電路取得。此設計可將 Outpost A 的服務連結流量保留在私有網路上，並提供路徑備援，以便讓任何一個直 Connect 電路故障或整個直 Connect 位置失敗。

前哨 B 有四個冗餘網絡路徑到達其公共錨點。透過在直 Connect 電路和 Outpost A 使用的位置上佈建的公用 VIF 可使用三個路徑。第四個路徑可透過客戶 WAN 和公用網際網路取得。Outpost B 的服務鏈接流量可以通過任何可以成功到達公共互聯網上的錨點的可用路徑進行路由。使用 Direct Connect 路徑可提供更一致的延遲和更高的頻寬可用性，而公用網際網路路徑則可用於災難復原 (DR) 或頻寬增強案例。

前哨 C 有兩個冗餘的網絡路徑到達其公共錨點。前哨 C 部署在與前哨 A 和 B. Outposts C 不同的資料中心中，前哨 C 的資料中心沒有連接到客戶廣域網路的專用電路。相反地，資料中心有兩個不同的網際網路服務供應商 (ISP) 所提供的備援網際網路連線。Outpost C 的服務鏈路流量可以通過任一 ISP 網絡進行路由，以到達公共互聯網上的錨點。這種設計允許靈活地通過任何可用的公共互聯網連接路由服務鏈接流量。但是，該 end-to-end 路徑取決於公共第三方網絡，其中帶寬可用性和網絡延遲會波動。

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：

- 500 Mbps-每個前哨機架提供 1 Gbps 的可用頻寬 (例如，3 個機架：1.5 至 3 Gbps 的可用頻寬)

高可用性錨點連接的建議做法：

- 在區域中的每個前哨站及其錨點之間佈建冗餘網路路徑。
- 使用直 Connect (DX) 路徑來控制延遲和頻寬可用性。
- 確定 TCP 和 UDP 連接埠 443 已從前哨服務連結 CIDR 區塊開放 (輸出) 到父區域中的 EC2 IP 位址範圍。確定所有網路路徑上的連接埠均已開啟。
- 確保每個路徑都符合頻寬可用性和延遲需求。
- 使用動態路由自動化圍繞網路故障的流量重新導向。
- 在每個規劃的網路路徑上測試服務連結流量路由，以確保路徑如預期般運作。

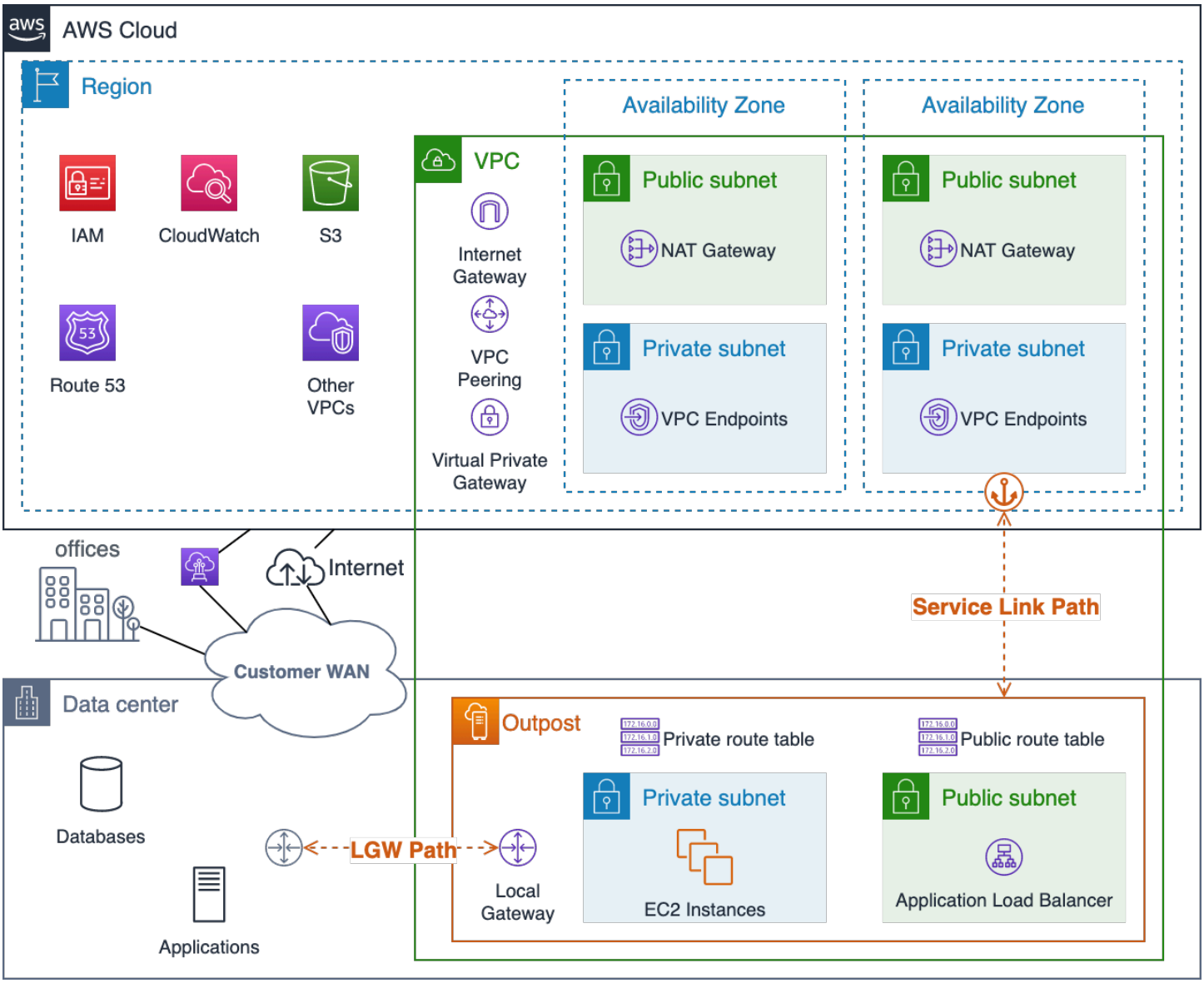
應用程式/工作負載路由

應用程式工作負載的 Outpost 有兩條路徑：

- 服務連結路徑
- 本機閘道 (LGW) 路徑

您可以設定 Outpost 子網路路由表，以控制要使用哪個路徑到達目的地網路。指向 LGW 的路由會將流量引導出本機閘道和內部部署網路。指向區域中的服務和資源的路由，例如 Internet Gateway，NAT 網關，虛擬專用網關和 TGW，將使用服務鏈接到達這些目標。如果您的 VPC 對等連線與同一 Outpost

上的多個 VPC，則 VPC 之間的流量會保留在 Outpost 上，且不會使用返回該區域的服務連結。如需 VPC 對等互連的相關資訊，請參閱 Amazon VPC 使用者指南中的使用 VPC 對等 Connect VPC。



前哨服務鏈路和 LGW 網絡路徑的可視化

在規劃應用模組製程時，您應該小心，以便在網路故障期間同時考慮正常作業與有限的製程與服務可用性。當前哨站與區域中斷連線時，無法使用服務連結路徑。

您應該佈建不同的路徑，並在 Outpost LGW 與重要的內部部署應用程式、系統和使用者之間設定動態路由。備援網路路徑可讓網路繞過故障路由流量，並確保內部部署資源能夠在部分網路故障期間與 Outpost 上執行的工作負載進行通訊。

前哨 VPC 路由配置是靜態的。您可以透過 CLI AWS Management Console、API 和其他基礎結構即程式碼 (IaC) 工具來設定子網路路由表；不過，您將無法在中斷連線事件期間修改子網路路由表。您必須重新建立前哨站和區域之間的連接才能更新路由表。使用與您計劃在中斷連線事件期間使用的一般作業相同的路由。

前哨站上的資源可以通過服務鏈接和該地區的 Internet Gateway（IGW）或通過本地網關（LGW）路徑到達互聯網。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/出口點，與使用區域中 IGW 的服務連結路徑相比，延遲時間更低、更高的 MTU，並降低 AWS 資料輸出費用。

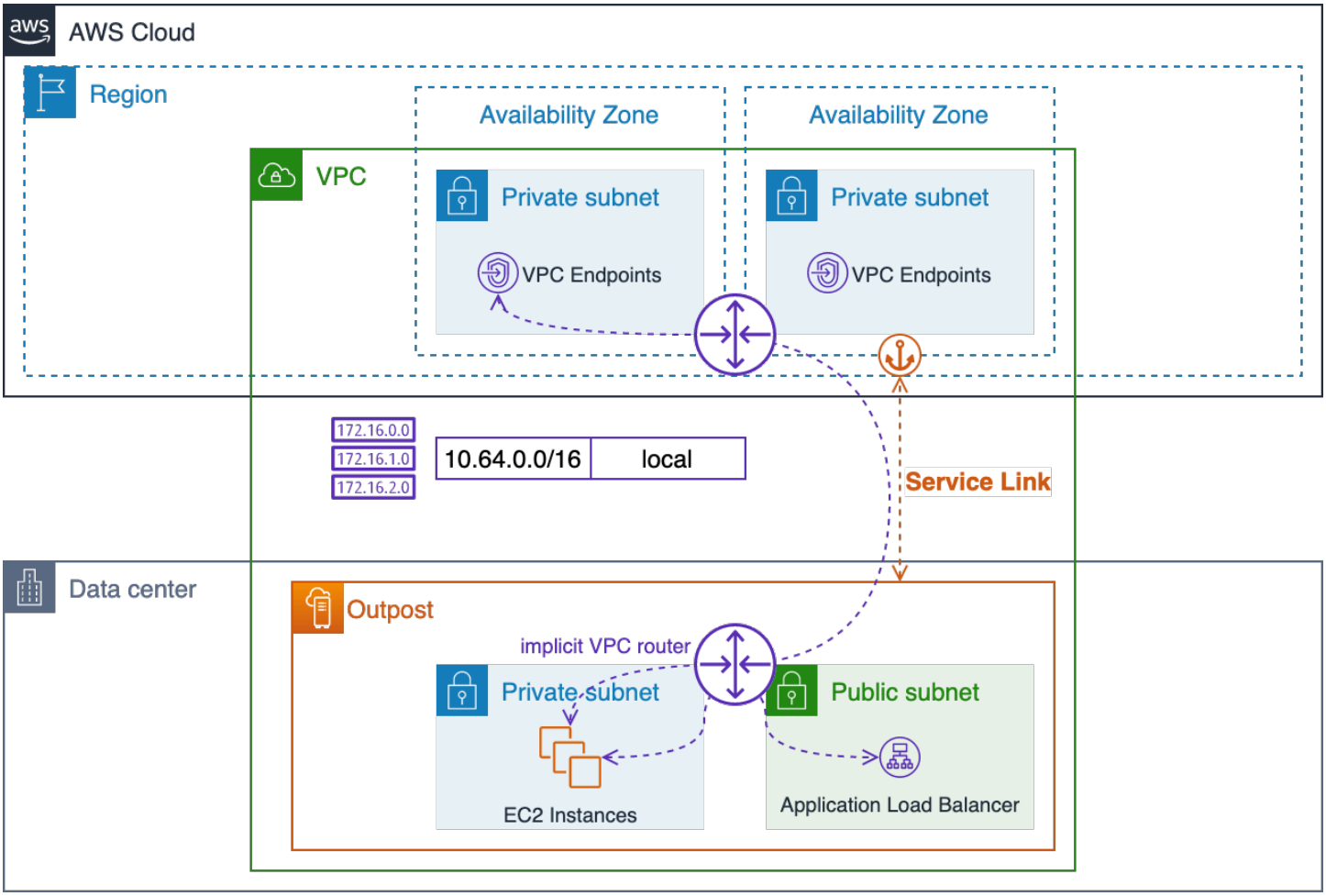
如果您的應用程式必須在內部部署執行，而且需要可從公用網際網路存取，您應該透過內部部署網際網路連線將應用程式流量路由到 LGW，以連線到 Outpost 上的資源。

雖然您可以在 Outpost 上設定子網路，例如區域中的公用子網路，但對於大多數使用案例而言，這可能是不希望的做法。入站網際網路流量將透過服務連結進入， AWS 區域 並透過服務連結路由至 Outpost 上執行的資源。

反過來，響應流量將通過服務鏈接進行路由，然後通過互聯網連接退出。 AWS 區域這種流量模式可能會增加延遲，並在流量離開該地區前往前哨站的路上，並且當返回流量通過該區域返回並輸出到 Internet 時，將產生數據輸出費用。如果您的應用程序可以在該地區運行，則該地區是運行它的最佳場所。

VPC 資源之間的流量（在相同 VPC 中）將始終遵循本機 VPC CIDR 路由，並由隱含的 VPC 路由器在子網路之間進行路由。

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



透過隱含路由器進行本機 VPC 路由

應用程式/工作負載路由的建議做法：

- 盡可能使用本機閘道 (LGW) 路徑，而非服務連結路徑。
- 通過 LGW 路徑路由互聯網流量。
- 使用一組標準的路由設定 Outpost 子網路路由表 — 這些表將用於正常作業和中斷連線事件期間。
- 在 Outpost LGW 與重要的內部部署應用程式資源之間佈建備援網路路徑。使用動態路由自動圍繞內部部署網路故障的流量重新導向

運算

雖然 Amazon EC2 容量似乎 AWS 區域 是無限的，但 Outposts 上的容量是有限的。您負責規劃和管理 Outposts 部署的運算容量。

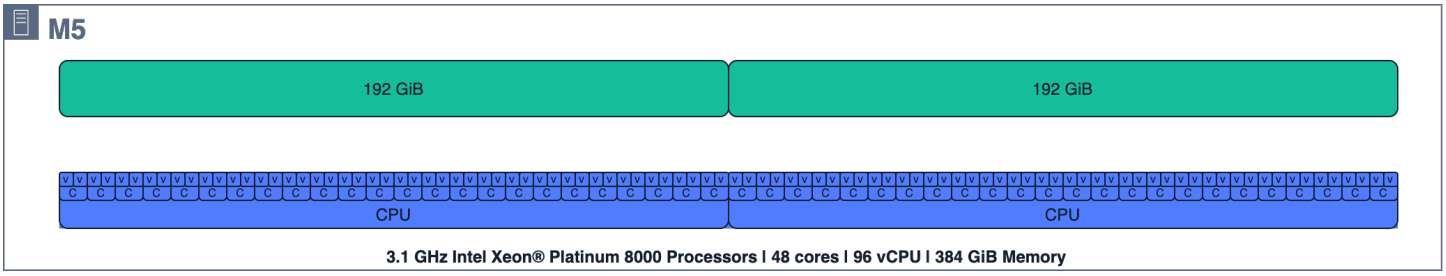
主題

容量規劃

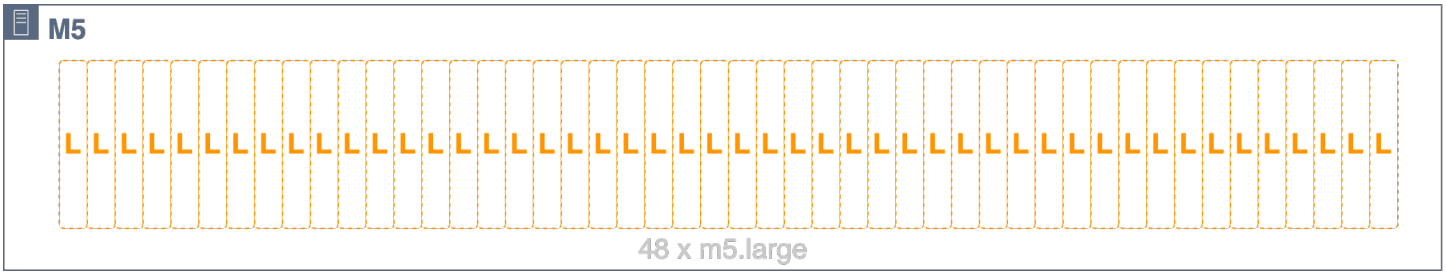
雖然 Amazon EC2 中的容量看似 AWS 區域 無限，但 Outposts 上的容量卻是有限的 — 受訂購的運算容量總容量所限制。您負責規劃和管理 Outposts 部署的運算容量。您應該訂購足夠的運算容量來支援 N+M 可用性模型，其中 N 是所需的伺服器數目，M 是佈建用來因應伺服器故障的備用伺服器數目。N +1 和 N+2 是最常見的可用性等級。

每個伺服器 (C5M5、R5、等) 都支援單一系列 EC2 執行個體。在 EC2 運算伺服器上啟動執行個體之前，您必須提供插槽配置，以指定您希望每個伺服器提供的 EC2 執行個體大小。 AWS 使用要求的開槽配置來設定每個伺服器。

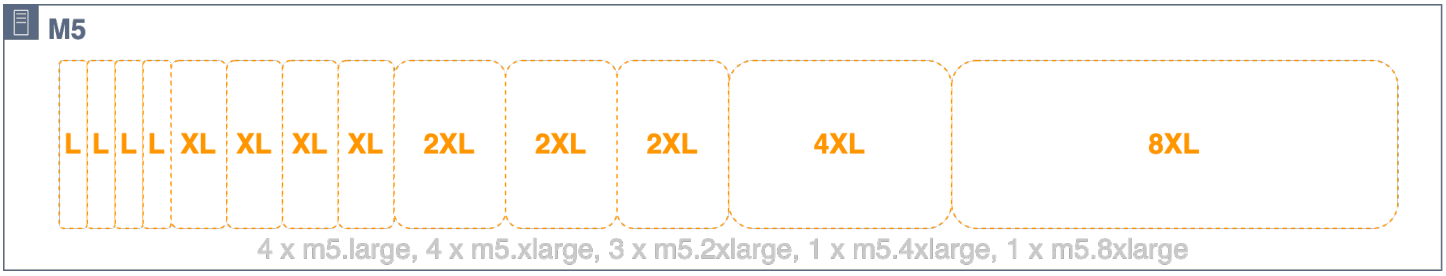
伺服器可以是同質開槽，其中所有插槽都是相同的執行個體大小 (例如 48 個`m5.large`插槽)，或是以混合執行個體類型 (例如 4、4 `m5.large`、3 `m5.2xlarge`、1 和 1 `m5.4xlargem5.8xlarge`) 進行異質開槽 — 請參閱接下來的三個數字`m5.xlarge`，瞭解這些開槽設定的視覺效果。



*`m5.24xlarge`*伺服器計算資源



*`m5.24xlarge`*伺服器均勻插入 48 個插槽 *`m5.large`*



*m5.24xlarge*伺服器異質插入 4 *m5.large*、4、3 *m5.xlarge* *m5.2xlarge* *m5.4xlarge*、1 和 1 插槽 *m5.8xlarge*

完整的伺服器容量不需要插槽。插槽可以新增至具有可用未配置容量的伺服器。您可以通過打開支持票來修改插槽佈局。如果在執行中的執行個體佔用某些插槽時，無法套用新的插槽配置，Enterprise Support 可能會要求您關閉或重新啟動特定執行個體以完成重新輸入要求。

所有伺服器都將其佈建的插槽貢獻給 Outpost 上的 EC2 容量集區，並且指定執行個體類型和大小的所有插槽均以單一 EC2 容量集區的形式進行管理。例如，先前具m5.large有、、和插槽的異質開槽伺服器會將這些m5.8xlarge插槽貢獻給五個 EC2 容量集區m5.4xlarge，每個執行個體類型和大小都有一個集區。m5.xlarge m5.2xlarge

規劃 N+M 伺服器可用性的備用容量時，請務必考慮伺服器插槽和 EC2 容量集區。 AWS 偵測伺服器何時發生故障或效能降級，並排程網站造訪以取代失敗的伺服器。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) 至少一台伺服器的故障。在這個最低層級的伺服器可用性下，當伺服器發生故障或需要停止服務時，您可以在同一系列其餘伺服器的備用插槽上，重新啟動失敗或降級的執行個體。

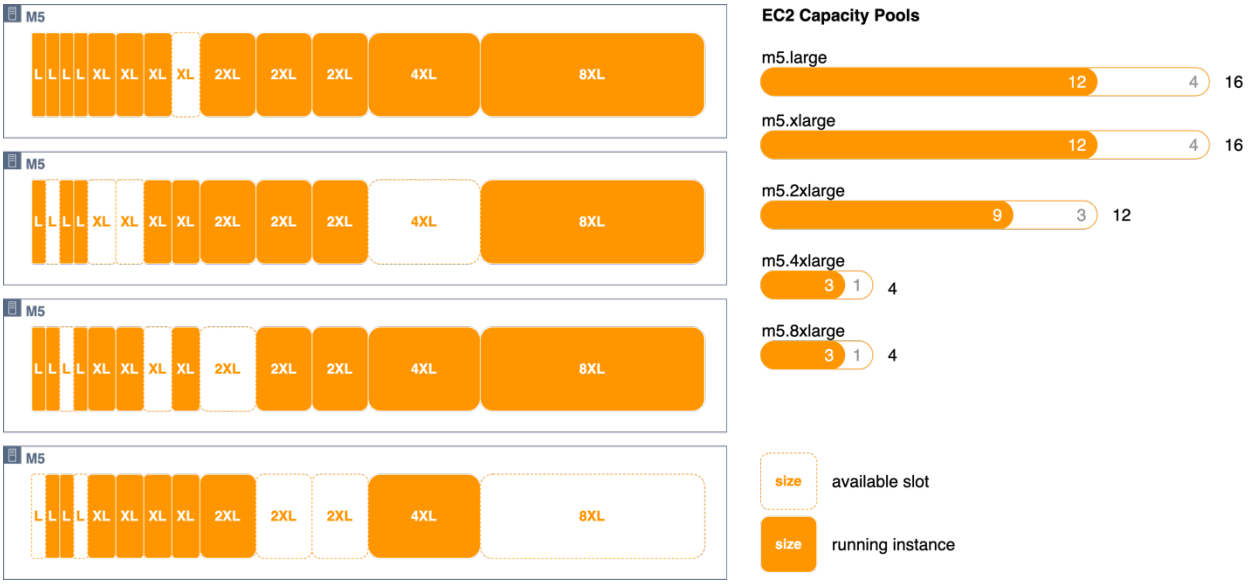
當您擁有均質開槽的伺服器或具有相同開槽配置的異質開槽伺服器群組時，規劃 N+M 可用性非常簡單。您只需計算執行所有工作負載所需的伺服器數量 (N)，然後新增 (M) 額外的伺服器，即可在故障和維護事件期間滿足伺服器可用性的需求。

由於 NUMA 邊界，下列開槽組態無法使用：

- 3 m5.8xlarge
- 一m5.16xlarge和一 m5.8xlarge

請諮詢您的 AWS 帳戶 團隊，以驗證您規劃的 AWS Outposts 機架插槽配置。

在下圖中，四個m5.24xlarge伺服器以異質方式開槽，並具有相同的開槽配置。這四個伺服器會建立五個 EC2 容量集區。每個集區都以最高使用率 (75%) 執行，以維持在這四部伺服器上執行的執行個體 N+1 可用性。如果有任何伺服器故障，則有足夠的空間重新啟動其餘伺服器上的失敗執行個體。



EC2 伺服器插槽、執行中執行個體和插槽集區的視覺化

對於更複雜的插槽配置 (伺服器開槽不相同)，您需要計算每個 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伺服器 (為指定 EC2 容量集區貢獻插槽) 可能會發生故障，而且仍允許剩餘的伺服器攜帶執行中的執行個體：

$$M = \left\lfloor \frac{poolSlots_{available}}{serverSlots_{max}} \right\rfloor$$

其中：

- PoolSlots $_{available}$ 是指定 EC2 容量集區中可用插槽的數量 (集區中的插槽總數減去執行中執行個體的數量)
- 伺服器批次$_{max}$是任何伺服器貢獻給給定 EC2 容量集區的最大插槽數
- M 是可能發生故障的服務器數量，仍然允許其餘服務器攜帶正在運行的實例

範例：Outpost 有三部伺服器，可為`m5.2xlarge`容量集區提供插槽。第一有助於 4 插槽，第二有助於 3 插槽，第三服務器有助於 2 插槽。前哨站上的`m5.2xlarge`執行個體集區總容量為 9 個插槽 (4 + 3 + 2)。前哨有 4 個正在運行的`m5.2xlarge`實例。有多少伺服器可能會失敗，而且仍允許剩餘的伺服器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：您可能會遺失任何一個伺服器，而且仍然會在剩餘的伺服器上攜帶執行中的執行個體。

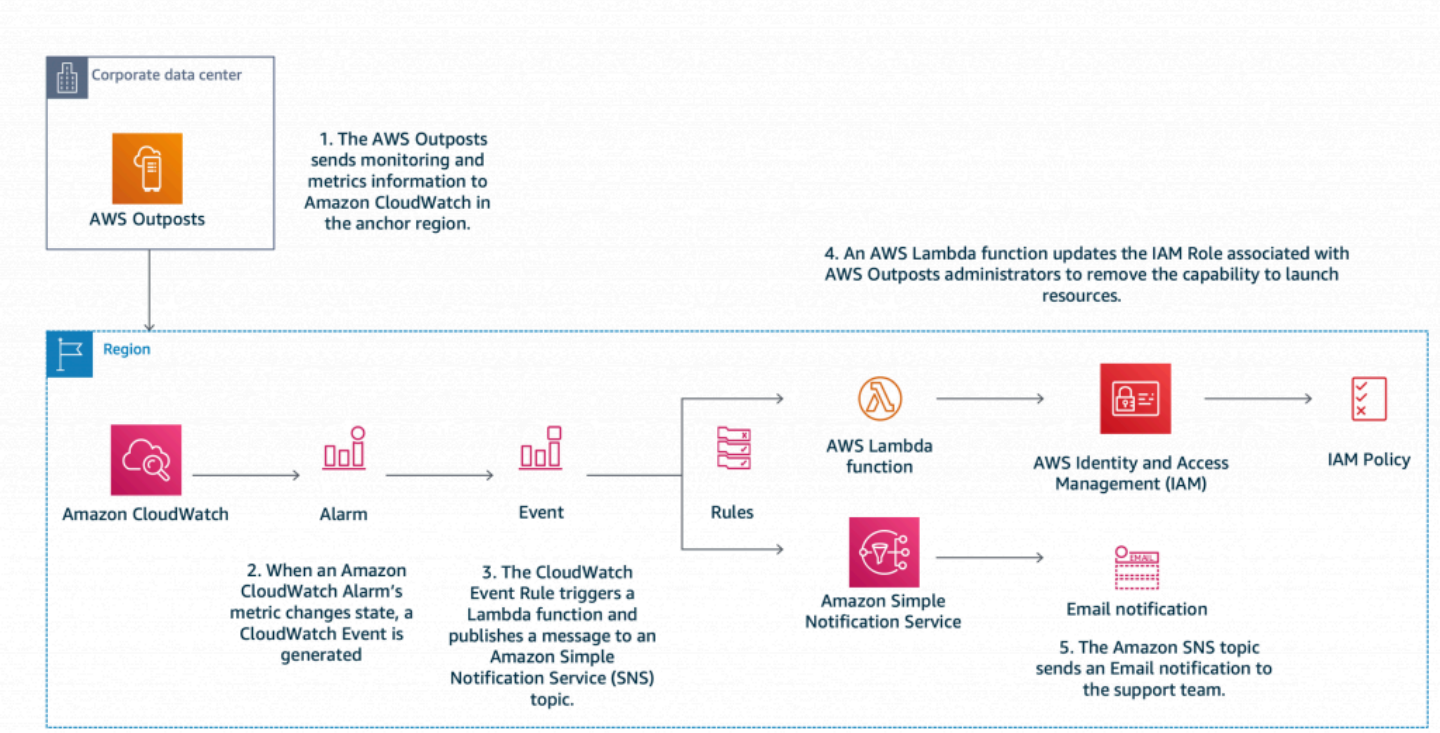
計算容量規劃的建議做法：

- 調整您的運算容量，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開槽伺服器部署 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的可用性需求。

容量管理

您可以在 AWS Management Console 和透過 Amazon CloudWatch 指標監控 Outpost EC2 執行個體集區使用率。請聯絡企業 Support 以擷取或變更 Outposts 的開槽配置。

您可以使用相同的執行個體 auto 復原和 EC2 Auto Scaling 機制來復原或替換受伺服器故障和維護事件影響的執行個體。您必須監視和管理 Outpost 容量，以確保隨時可用足夠的備用容量以因應伺服器故障。使用 Amazon CloudWatch 和 AWS Lambda部落格文章管理 AWS Outposts 容量提供實作教學課程，說明如何合併 AWS CloudWatch 和 AWS Lambda 管理 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

運算容量管理的建議做法：

- 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
- 為 Outpost 部署自動化容量監控，並設定通知，以及 (選擇性) 容量警示的自動回應。

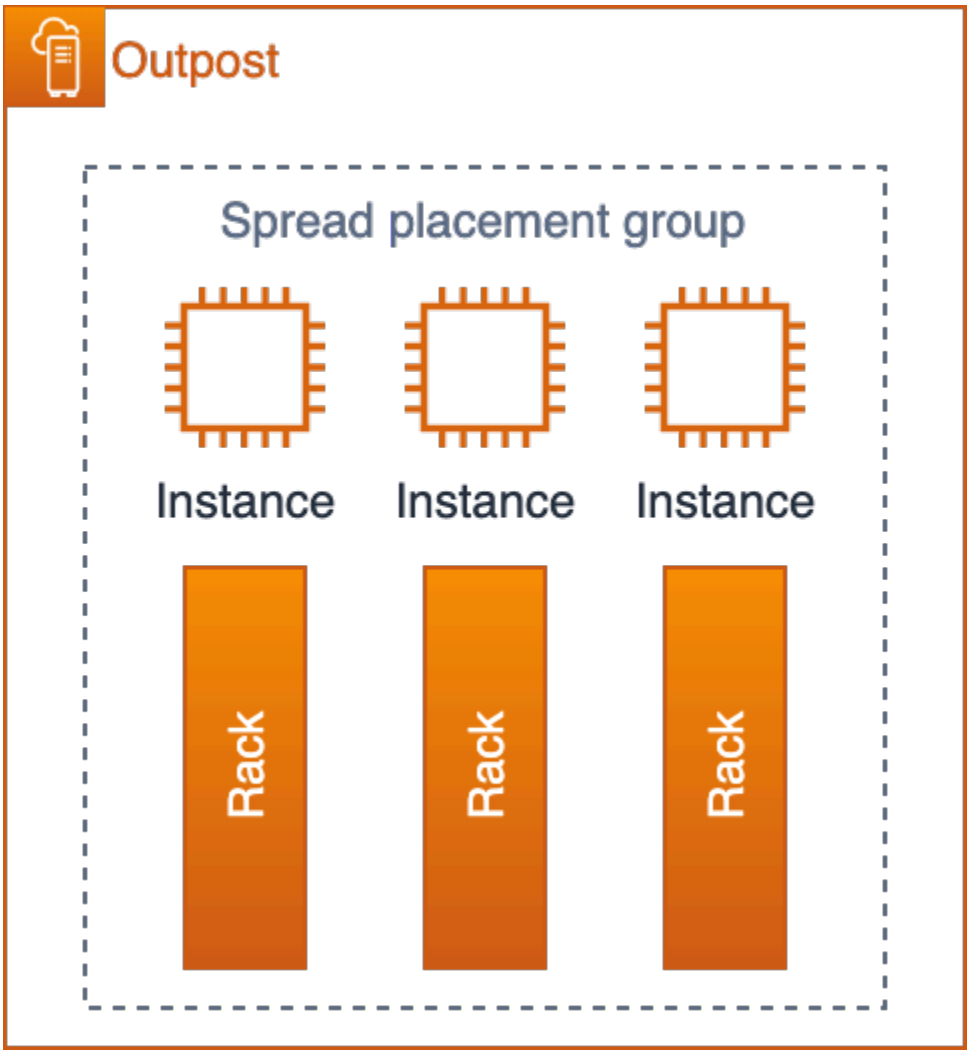
例證放置

Outposts 具有有限數量的計算服務器。如果您的應用程式在 Outposts 上部署了多個相關執行個體；無需額外設定，執行個體可能會部署在相同伺服器或同一機架中的伺服器上。現在，您可以使用三種機制來分配執行個體，以降低在相同基礎結構上執行相關執行個體的風險：

多前哨部署 — 與該地區的異地同步備份策略類似，您可以將 Outposts 部署到不同的資料中心，並將應用程式資源部署到特定的 Outposts。這可讓您在所需的 Outpost (一組邏輯機架) 上執行執行個體。可以採用多出站策略來防止機架和資料中心故障模式，如果 Outposts 錨定到不同的 AZ 或區域，也可以提供針對 AZ 或區域故障模式的保護。如需多前哨架構的詳細資訊，請參閱較大的故障模式。

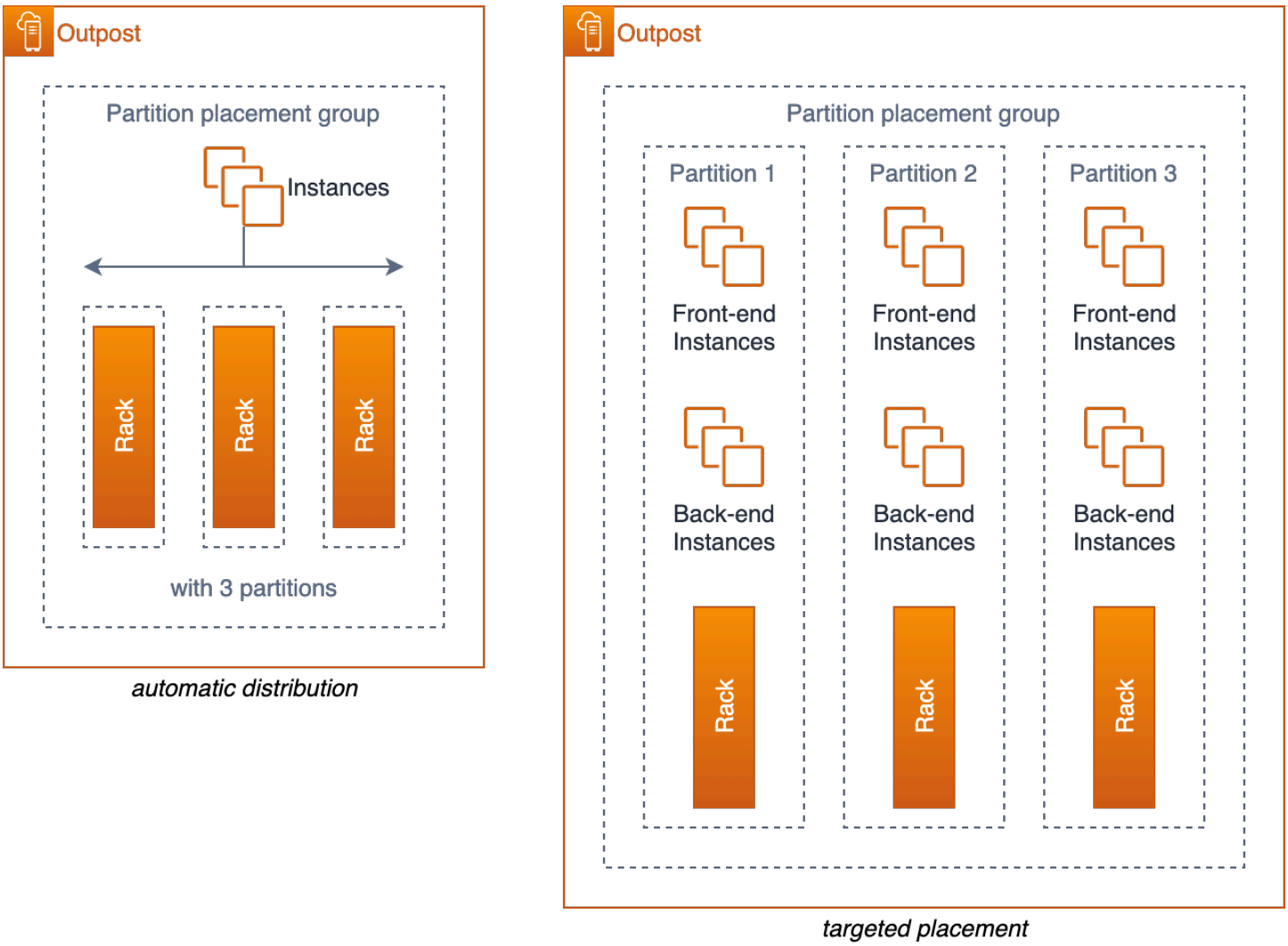
Outposts 上的 Amazon EC2 放置群組 (單一 Outpost 多機架執行個體放置) — 可讓您使用叢集、分攤和分區策略來影響放置。分攤和分區放置策略可讓您在多機架 Outpost 中跨機架分配執行個體。

分攤置放群組提供了一種在機架之間分配單一執行個體的簡單方法，以減少相關故障的可能性。您只能部署到群組中的執行個體，與 Outpost 中的機架數量相同。



具有三個機架的前哨站上的 EC2 分攤放置群組

您也可以使用分割區放置群組，將執行個體分配到多個機架。使用自動分配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同一機架，同時將其他資源分配到機架之間。例如，如果您有一個具有三個機架的邏輯 Outpost，則建立具有三個分割區的分割區放置群組可讓您將資源分配到機架之間。



具有三個機架的前哨站上的 EC2 分區放置群組

創意伺服器插槽 — 如果您有單機架 Outpost，或者您在 Outposts 上使用的服務不支援刊登位置群組，您或許可以使用創意插槽功能來確保您的執行個體不會部署在相同的實體伺服器上。如果相關執行個體的 EC2 執行個體大小相同，您可以插槽伺服器，以限制每部伺服器上設定的該大小插槽數量，並將插槽分散到伺服器上。伺服器插槽會限制可在單一伺服器上執行的執行個體數目 (該大小)。

例如，考慮先前所示的開槽配置圖 13。如果您的應用程式需要在使用此插槽配置的 Outpost 上部署三個`m5.4xlarge`執行個體，EC2 會將每個執行個體放置在單獨的伺服器上，而且這些執行個體不可能在相同的伺服器上執行，只要插槽組態不會變更以在伺服器上開啟其他`m5.4xlarge`插槽。

運算執行個體放置的建議做法：

- 在 Outposts 上使用 Amazon EC2 置放群組來控制單一 Outpost 中跨機架的執行個體放置。

- 與其訂購擁有單一中型或大型 Outpost 機架的 Outpost，不如考慮將容量拆分為兩個中小型機架，以便利用 EC2 置放群組在機架之間分配執行個體的能力。

儲存

AWS Outposts 機架服務提供三種儲存類型：

- 支援 EC2 執行個體類型上的執行個體
- 用於永久性區塊儲存的亞馬遜彈性區塊存放區 (EBS) gp2 磁碟區
- Outposts 上的 Amazon 簡單存儲服務（Outposts 上的 S3），用於本地對象存儲

在支援的伺服器 (C5d、M5d、R5d和I3en) 上提供執行個體儲存體。G4dn就像在區域中一樣，執行個體存放區中的資料只會在執行個體的 (執行中) 生命週期內保留。

Outposts 物件儲存上的前哨 EBS 磁碟區和 S3 是作為 AWS Outposts 機架管理服務的一部分提供。客戶必須負責 Outpost 儲存集區的容量管理。客戶在訂購 Outpost 時，會指定 EBS 和 S3 儲存的儲存需求。 AWS 使用提供要求的儲存容量所需的儲存伺服器數量來設定 Outpost。 AWS 負責 Outposts 儲存服務上 EBS 和 S3 的可用性。已佈建足夠的儲存伺服器，以便為 Outpost 提供高可用性的儲存服務。遺失單一儲存伺服器不應中斷服務，也不會造成資料遺失。

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

資料保護

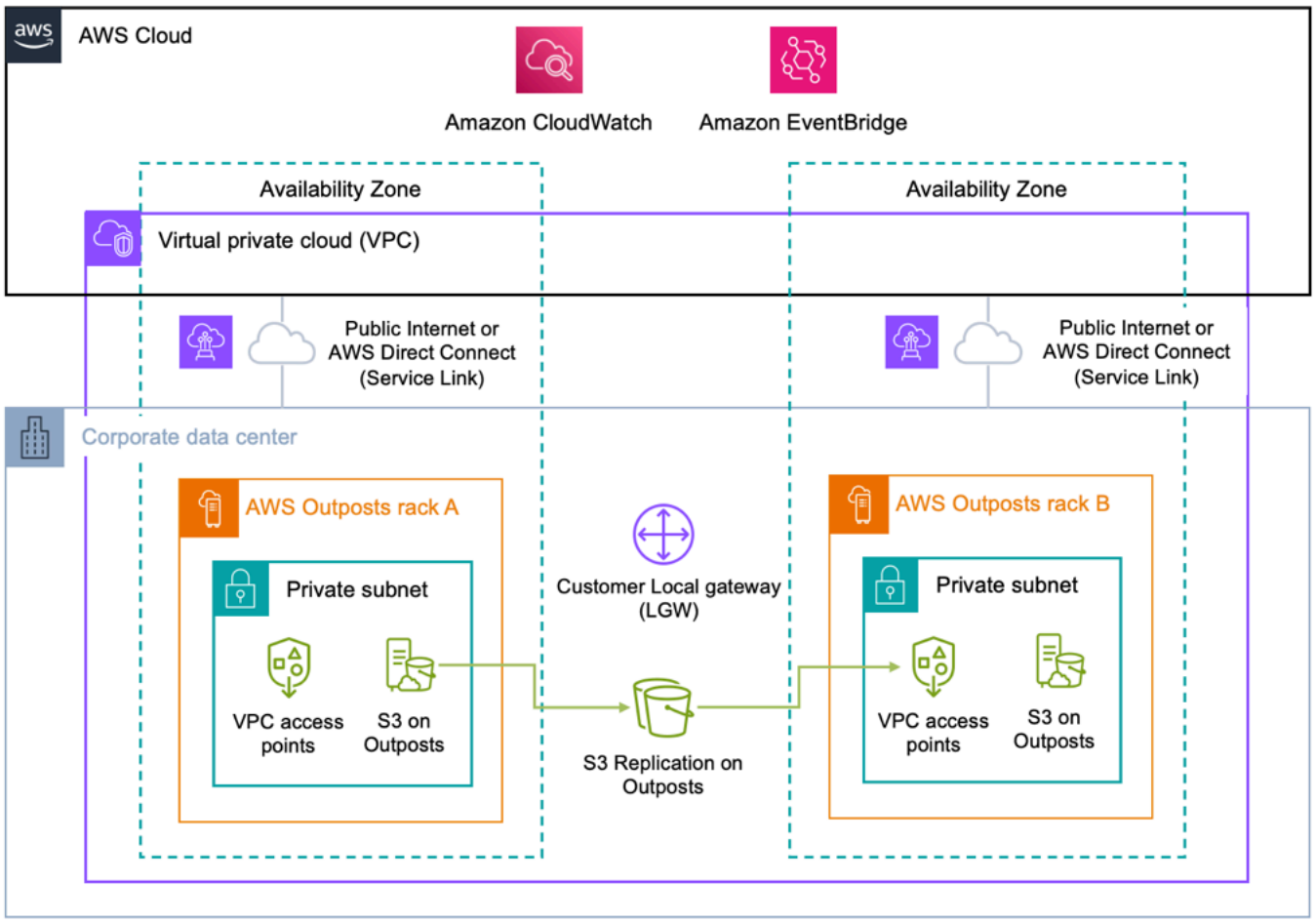
適用於 EBS 磁碟區：機 AWS Outposts 架支援 EBS 磁碟區快照，提供簡單安全的資料保護機制，以保護您的區塊儲存資料。快照是 EBS 磁碟區的 point-in-time 增量備份。根據預設，前哨站上 Amazon EBS 磁碟區的快照會存放在該區域的 Amazon S3 上。如果您的 Outposts 已在 Outposts 容量上設定 S3，您可以使用 Outposts 上的 EBS 本機快照，在 Outposts 儲存體上使用 S3 將快照本地存放在前哨上。

對於 Outposts 儲存貯體上的 S3 (資料駐留使用案例)：

- 您可以在 Outposts 上使用 S3 版本控制，以保存對象的所有更改和歷史記錄。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。

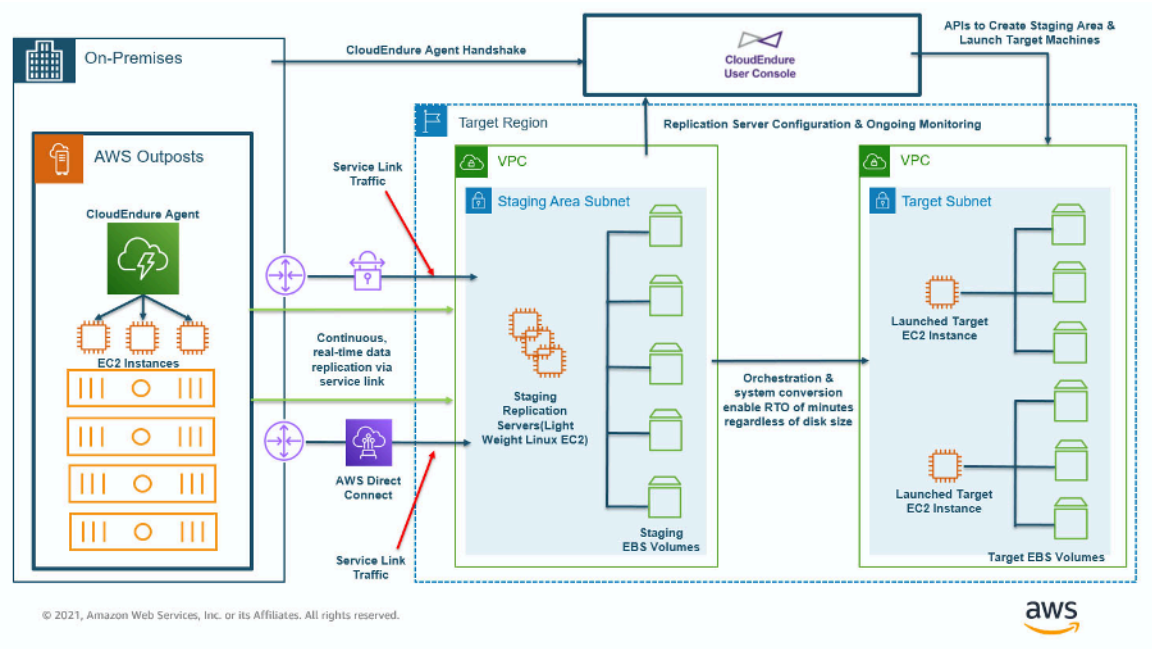
- 您可以在 Outposts 上使用 S3 複寫，建立和設定複寫規則，以自動將 S3 物件複寫到另一個 Outpost，或複寫到相同 Outpost 上的另一個儲存貯體。在複寫期間，Outposts 物件上的 S3 會透過客戶的本機閘道 (LGW) 傳送，且物件不會傳回。 AWS 區域在 Outposts 上進行 S3 複寫提供了一種簡單且靈活的方式，可在特定資料周邊自動複寫資料，以解決資料備援和合規要求。

  Outposts 上的 S3 複寫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 儲存貯體之間的擱置中位元組、擱置中的作業以及複寫延遲來監控複寫進度。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。



對於 Outposts 儲存貯體上的 S3（非資料駐留使用案例） AWS 區域：您可以使用AWS DataSync在 Outpost 和區域之間自動執行 Outposts 資料傳輸的 S3。 DataSync 允許您選擇要傳輸的內容，何時傳輸以及使用多少頻寬。將 Outposts 儲存貯體上的現場部署 S3 備份到中的 S3 儲存貯體，可 AWS 區域讓您利用 99.999999999% (11 個) 的資料耐久性和額外的儲存層 (標準、不常存取和 Glacier)，進行區域 S3 服務所提供的成本最佳化。

執行個體複寫：您可CloudEndure以使用將個別執行個體從內部部署系統複製到 Outpost、從 Outpost 複製到區域、從區域複製到 Outpost，或從一個 Outpost 複製到另一個。AWS Outposts 使用 CloudEndure部落格文章的 DR 架構描述了每個案例，以及如何使用 CloudEndure.



從前哨站到該地區的災難恢復（DR）

使用 AWS Outposts 機架做為 CloudEndure 目的地 (複寫目標) 需要 Outposts 儲存上的 S3。

建議的資料保護做法：

- 使用 EBS 快照建立區塊儲存磁碟區 point-in-time 備份到區域中的 Amazon S3 或 Outposts 上的 S3。
- 在 Outposts 物件版本管理上使用 S3 來維護物件的多個版本和歷程記錄。
- 在 Outposts 上使用 S3 複寫，自動將您的物件資料複寫到另一個前哨站。
- 對於非資料駐留使用案例，請 AWS DataSync 使用將存放在 Outpost 上 S3 中的物件備份到該區域的 Amazon S3。
- 用 CloudEndure 於在內部部署系統、邏輯 Outposts 和區域之間複寫執行個體。

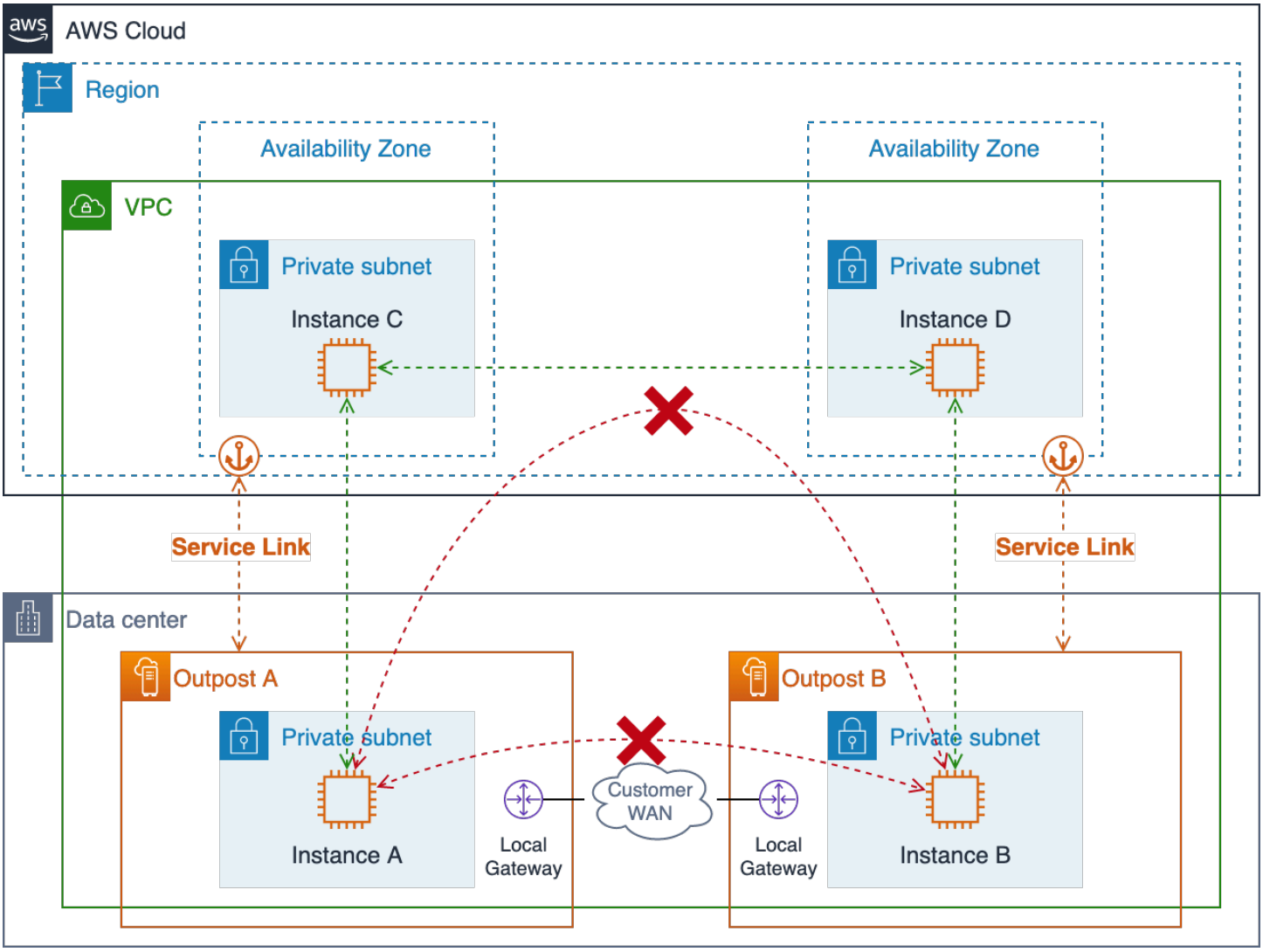
更大的故障模式

若要設計 HA 架構以減輕較大的故障模式，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 連線能力的獨立資料中心部署具有足夠基礎架構容量的多個 Outposts。您可以將 Outposts 錨定在一個 AWS 區域 或跨多個區域的不同可用區域 (AZ)。您還應該在位置之間佈建彈

性和足夠的 site-to-site 連線能力，以支援同步或非同步資料複製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 和區域可用的 E lastic Load Balancing 服務，將流量導向至所需的位置，並在發生大規模故障時自動將流量重新導向至存在的位置。

在多個 Outposts 之間設計和部署應用程式工作負載時，您應該注意一些網路限制。兩個獨立 Outposts 上的資源無法通過通過該地區轉移流量來相互通信。部署在相同 VPC 內的兩個個別 Outposts 上的資源無法透過客戶網路彼此通訊。部署在不同 VPC 中的兩個獨立 Outposts 上的資源可以在客戶網路上彼此通訊。

下列兩個圖表說明封鎖且成功的網路路徑。

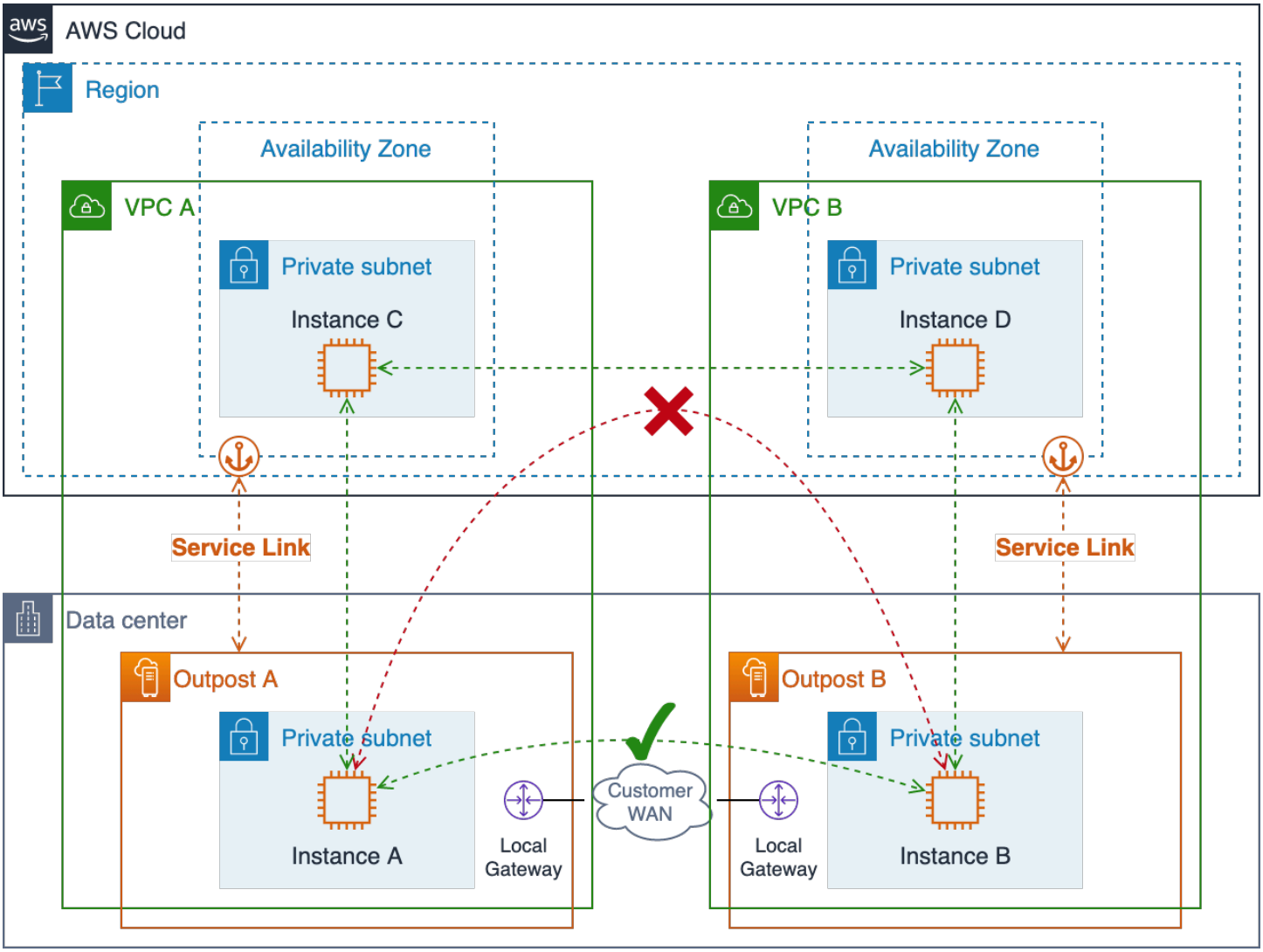


單一 VPC 多重前置網路路徑

由於這是一種反模式，因此會封鎖轉移該地區的前端到前哨流量。這類流量會在兩個方向上產生輸出費用，而且可能比透過客戶 WAN 路由流量的延遲要高得多。

相同 VPC 中多個 Outposts 上的資源無法相互通訊。同一 VPC 中前哨之間的流量將始終遵循本地 VPC CIDR 路由，通過該區域將被阻止的地區。

您應該使用不同的 VPC 在多個 Outposts 上部署資源，以允許您在本機內部部署和 WAN 網路之間路由 Outpost 到 Outpost 流量。



多個 VPC 多重前端網路路徑

防範較大失敗模式的建議做法：

- 部署錨定到多個 AZ 和區域的多個 Outposts。
- 針對多前哨部署中的每個前哨使用不同的 VPC。

結論

透過 AWS Outposts 機架，您可以使用熟悉的工具和服務，如 Outposts、Amazon ECS、Amazon EC2 EKS 和 Amazon RDS 等熟悉的 AWS 工具 Amazon S3 服務，建立、管理和擴展高可用性的現場部署應用程式。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 AWS 區域. Outposts rack 非常適合需要低延遲存取內部部署系統、本機資料處理、資料存放區，以及移轉具有本機系統相互依存性之應用程式的工作負載。

當您為 Outpost 部署提供足夠的電源、空間以及冷卻和彈性連線時 AWS 區域，您可以建置高可用性的單一資料中心服務。此外，為了獲得更高層級的可用性和恢復能力，您可以部署多個 Outposts，並跨越邏輯和地理界限分發您的應用程式。

Outposts 機架消除了建置內部部署運算、儲存和應用程式網路集區的無差別繁重工作，並可讓您將 AWS 全球基礎架構的覆蓋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應用程式現代化、簡化應用程式部署，並增加 IT 服務對業務的影響。

貢獻者

本文件的貢獻者包括：

- 馬洛里·格申費爾德，S3 在 Outposts，Amazon Web Services
- 克里斯·倫斯福德，高級專家解決方案架構師 AWS Outposts，Amazon Web Services
- 羅漢·馬修斯, 首席建築師 AWS Outposts, Amazon Web Services

文件歷史記錄

若要收到有關此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
次要更新	在容量規劃中新增額外的開槽指引。	2024年2月9 日
次要更新	已更新以反映自首次發行以來的功能啟動。	2023 年 7 月 19 日
次要更新	已更新高可用性網路附件的建議作法。	2023 年 6 月 29 日
初次出版	白皮書首次出版。	2021 年 8 月 12 日

> **Note**
>
> 若要訂閱 RSS 更新，您必須啟用所使用瀏覽器的 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 產品供應項目和做法，如有變更，恕不另行通知，且 (c) 不會向其關聯公司、供應商或授權人建立任何承諾或保證。 AWS AWS 產品或服務係依「原狀」提供，不含任何明示或暗示之擔保、陳述或條件。客戶的責任和責任由 AWS 協議控制，本文件不屬於與客戶之間 AWS 的任何協議的一部分，也不會修改。 AWS

AWS 詞彙表

有關最新 AWS 術語，請參閱AWS 詞彙表 參考文獻中的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。