

AWS 白皮書

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 白皮書

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

摘要和介紹	i
你是否 Well-Architected?	1
簡介	1
延伸 AWS 內部部署位置的基礎架構和服	2
瞭解更新的共同責任模式	4
在失敗模式方面思考	7
故障模式 1：網絡	7
失敗模式 2：執行個體	7
故障模式 3：計算	8
故障模式 4：機架或資料中心	8
故障模式 5：AWS 可用區域或地區	8
建置 HA 應用程式和基礎架構解決方 AWS Outposts 架	9
聯網	10
網路附件	10
錨栓連接	14
應用程式/工作負載路由	16
運算	19
容量規劃	20
容量管理	23
例證放置	24
儲存	27
資料保護	27
更大的故障模式	29
結論	32
貢獻者	33
文件歷史紀錄	34
注意	35
AWS 詞彙表	36
.....	xxxvii

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日 [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，以建置具有高可用性內部部署應用程式 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 [AWS Well-Architected Tool](#)，可免費使用 [AWS Management Console](#)，您可以針對每個支柱回答一組問題，根據這些最佳做法來檢閱工作負載。

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Whitepaper)，請參閱 [AWS 建築中心](#)。

簡介

本 paper 適用於希望部署、遷移和操作應用程式的 IT 管理員和系統架構師 AWS 雲平台並在內部部署運行這些應用程式 [AWS Outposts 機架](#)，42U 機架的外形規格 [AWS Outposts](#)。

它介紹了用於構建高可用性系統的架構模式，反模式和建議的實踐，其中包括 AWS Outposts 機架。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

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。使用 Outposts 機架，客戶可以使用支援的 AWS 現場部署環境中的受管服務，包括：[Amazon 彈性運算雲](#) (AmazonEC2)，[Amazon 彈性區塊商店](#) (AmazonEBS)，[Outposts 上的 Amazon S3](#)，[Amazon Elastic Kubernetes Service](#) (AmazonEKS)，Amazon [彈性容器服務](#) (AmazonECS)，Amazon [Relational Database Service](#) (AmazonRDS) 和其他 [AWS Outposts](#) 上的服務。Outposts 上的服務交付在相同 [AWS 硝基系統中](#)使用 AWS 區域。

通過利用 AWS Outposts 機架，您可以使用熟悉的內部部署應用程式來建置、管理和擴充高可用性的 AWS 雲端服務和工具。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。

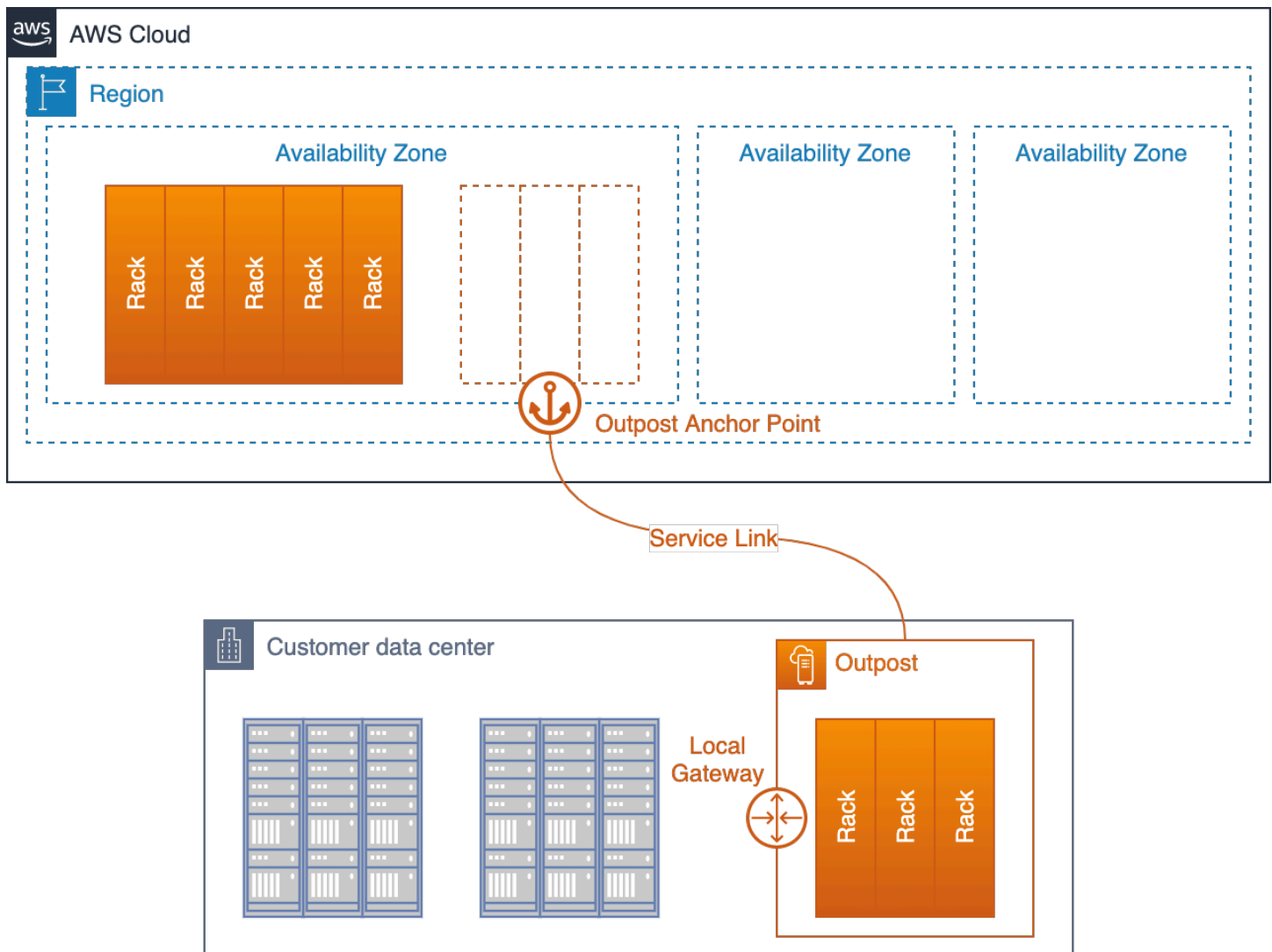
延伸 AWS 內部部署位置的基礎架構和服

所以此 AWS Outposts 服務提供 AWS 為 [50 多個國家和地區的內部部署位置提供基礎架構和服務](#)，讓客戶能夠部署相同的服務 AWS 基礎設施，AWS 適用於幾乎任何資料中心 APIs、主機代管空間或內部部署設施的服務和工具，提供真正一致的混合體驗。要了解如何使用 Outposts 進行設計，您應該了解組成的不同層次 AWS 雲端。

一個 [AWS 區域](#) 是世界上的一個地理區域。每個 AWS 區域 是以邏輯方式分組到 [可用區域](#) (AZs) 中的資料中心集合。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](#) (以下稱為前哨) 是一個或多個物理連接的部署 AWS Outposts 以單一實體的方式管理機架。前哨提供了一個池 AWS 您其中一個站台的運算和儲存容量，做為 AZ 的私有擴充功能 AWS 區域。

也許是最好的概念模型 AWS Outposts 是考慮從 AZ 的數據中心拔出一個或多個機架 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，以便機架繼續作為機架的一部分運作 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 基礎設施的一部分 AWS 區域。Outpost 不是很長的實體纜線，而是透過一組稱為「服務連結」的加密通VPN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 或其他地點。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。如需詳細資訊，請參閱 [AWS 資料隱私權FAQ](#)。

您在這些機架上部署的工作負載會在本機執行。而且，儘管這些機架中可用的計算和存儲容量是有限的，並且無法適應運行的雲端規模服務 AWS 區域，部署在機架上的資源 (您的執行個體及其本機儲存) 可獲得在本機執行的好處，同時管理平台繼續在 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人雲端 (VPC) 環境，並指定 Outpost 做為子網路的位置。然後，您可以在部署支援時選取所需的子網路 AWS 資源通過 AWS Management Console、CLI/APIs/CDK、或基礎架構即程式碼 (IaC) 工具。Outpost 子網路中的執行個體透過網路與 Outpost 或區域中的其他執行個體進行通訊。VPC

Outpost 服務連結承載 Outpost 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)。

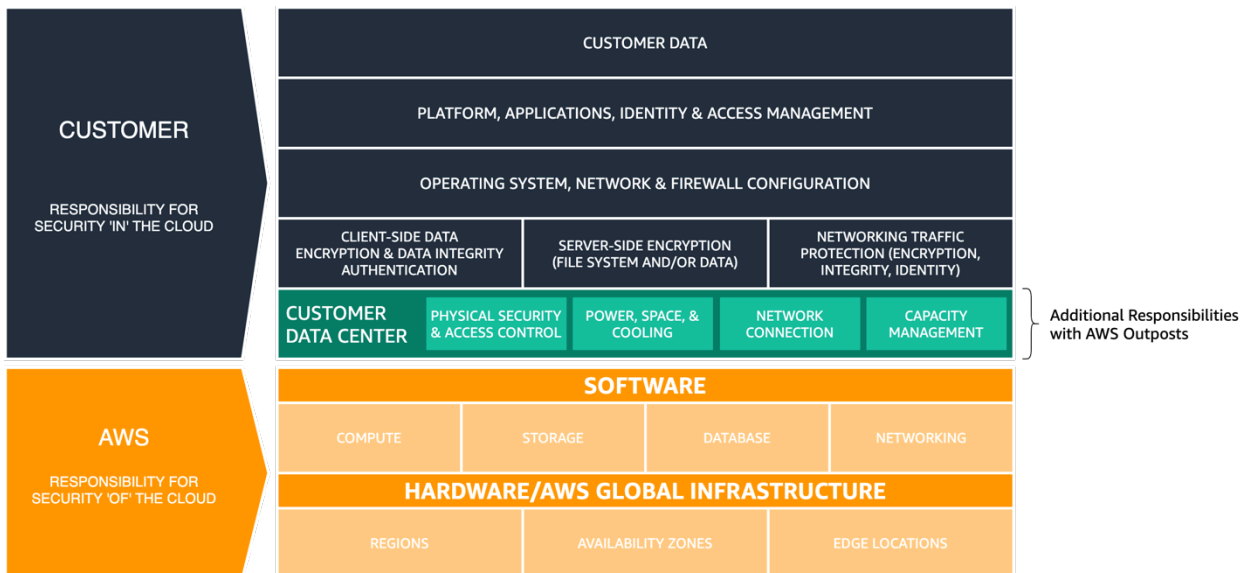
重要條款：

- **AWS Outposts**— 是一個完全託管的服務，提供相同的 AWS 基礎設施，AWS 適用於幾乎任何資料中心 APIs、主機代管空間或內部部署設施的服務和工具，提供真正一致的混合體驗。
- **前哨** — 是一個或多個物理連接的部署 AWS Outposts 以單一邏輯實體和集區的方式管理的機架 AWS 部署於客戶站點的運算、儲存和網路。
- **父區域** — AWS 區域 它提供管理，控制平面服務和區域 AWS 前哨部署的服務。
- **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 VPN 通道，可將 Outpost 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。

瞭解更新的可共同責任模式

當您部署 AWS Outposts 基礎架構到您的資料中心或主機代管設施中，您需要承擔其他責任 [AWS 共同的責任模式](#)。例如，在「區域」中，AWS 提供多樣化的電源、備援核心網路，以及彈性的廣域網路 (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

同 AWS Outposts，您必須負責資料中心環境的實體安全性和存取控制。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。

由於前哨容量是有限的，並通過機架的大小和數量來確定 AWS 在您的網站上安裝，您必須決定執行初始工作負載 EC2/EBS、適應 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 Outposts 容量和 S3 容量。

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

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。



圖三- AWS Outposts 交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。光纖控制面板可提供 Outpost 機架與內部部署網路之間的連線能力，並做為客戶管理的資料中心環境與受管理資料中心之間的分界點 AWS Outposts 環境。

就像在該地區一樣 AWS 負責 Outposts 上提供的雲端服務，並在您在 Outposts 上選擇和部署更高層級的受管服務 (例如 AmazonRDS) 時承擔額外責任。您應該檢閱 [AWS 您考慮](#) 並選擇要在 Outposts 上部署的服務時，個別服務的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您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

EC2 如果執行個體所在的伺服器發生問題，或執行個體發生作業系統或應用程式故障，則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。

故障伺服器的硬體替代作為完全受管理的一部分提供 AWS Outposts 機架服務。AWS 主動監控 Outpost 部署中所有伺服器和網路裝置的健全狀況。如果有需要進行物理維護，AWS 將安排訪問您的網站以替換故障組件的時間。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。

採取這種方法與 AWS Outposts rack 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 可用區域或地區

每個前哨都錨定到特定的可用區域 (AZ) 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路通信。

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。

為了減輕影響 AWS AZ 和區域故障，您可以部署多個 Outposts，每個前哨站都錨定到不同的 AZ 或區域。然後，您可以使用許多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 部署模型中操作 AWS 今天。

建置 HA 應用程式和基礎架構解決方 AWS Outposts 架

同 AWS Outposts 機架，您可以使用熟悉的內部部署應用程式來建置、管理和擴充高可用性的 AWS 雲端服務和工具。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 (VMs) 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。VMs 通常具有特定的身份，並且每個 VM 可能在整個應用程序體系結構中扮演關鍵角色。

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、無伺服器功能或其他受管理服務。

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 機架是可擴充的全受管服務 AWS 運算、儲存、網路、資料庫和其他雲端服務到內部部署位置，提供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 支援傳統內部部署 HA 架構的服務和 Outposts 是一種反模式。

工作負載執行於 AWS Outposts 機架使用 [Amazon EC2 Auto Scaling](#) 等雲端 HA 機制 (水平擴展以符合工作負載需求)、[運作 EC2 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，是否要移轉至 AWS 區域 或 AWS Outposts rack，您應該更新您的 HA 應用程式架構，開始利用受管理的雲端服務和雲 HA 機制。

以下各節介紹架構模式、反模式以及建議的部署作法 AWS Outposts 機架在您的內部部署環境中執行具有高可用性需求的工作負載 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。您應該閱讀並熟悉 [AWS Outposts 機架FAQs](#) 和 [使用者指南](#)，以FAQs及在 Outposts 機架上執行的服務與服務文件，當您準備好 Outposts 機架的環境，以及您的應用程式移轉至 AWS 服務。

主題

- [聯網](#)
- [運算](#)
- [儲存](#)
- [更大的故障模式](#)

聯網

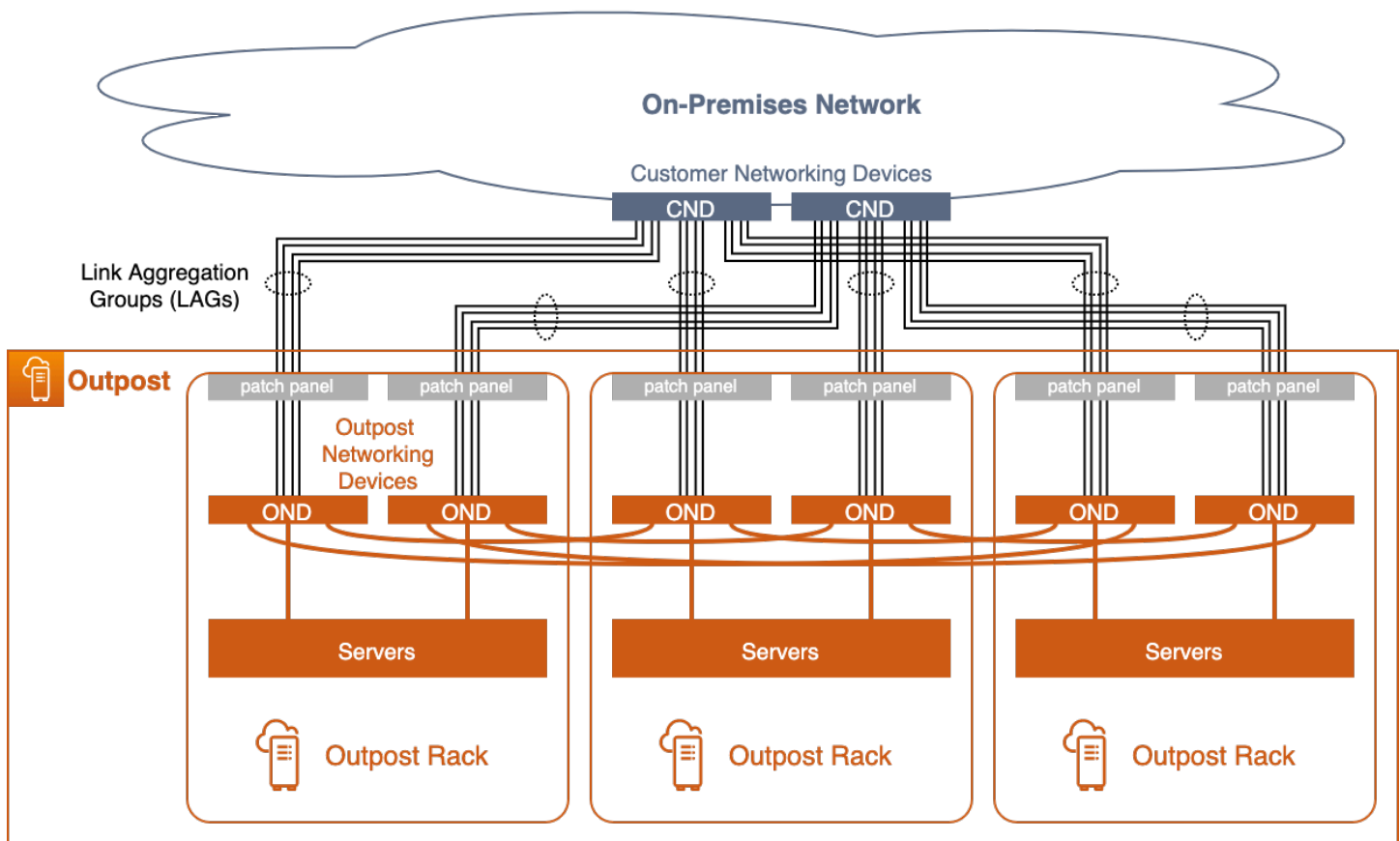
Outpost 部署取決於與其錨定 AZ 的彈性連線，以便管理、監控和服務作業正常運作。您應該佈建您的內部部署網路，以便為每個 Outpost 機架提供備援網路連線，並可靠的連線能力回到 AWS 雲。另外，請考慮在 Outpost 上執行的應用程式工作負載與與其通訊的其他內部部署和雲端系統之間的網路路徑 — 您將如何在網路中路由此流量？

主題

- [網路附件](#)
- [錨柱連接](#)
- [應用程式/工作負載路由](#)

網路附件

每個 AWS Outposts 機架配置備有稱為前哨網路裝置 (ONDs) 的備援 top-of-rack 交換器。每個機架中的運算和儲存伺服器都可連接到兩者 ONDs。您應該將每個交換器連接 OND 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。ONDs 使用光纖電纜和光收發器通 CNDs 過一個或多個物理連接連接到您的。[實體連線](#)會在邏輯連結彙總群組 (LAG) [連結](#)中設定。



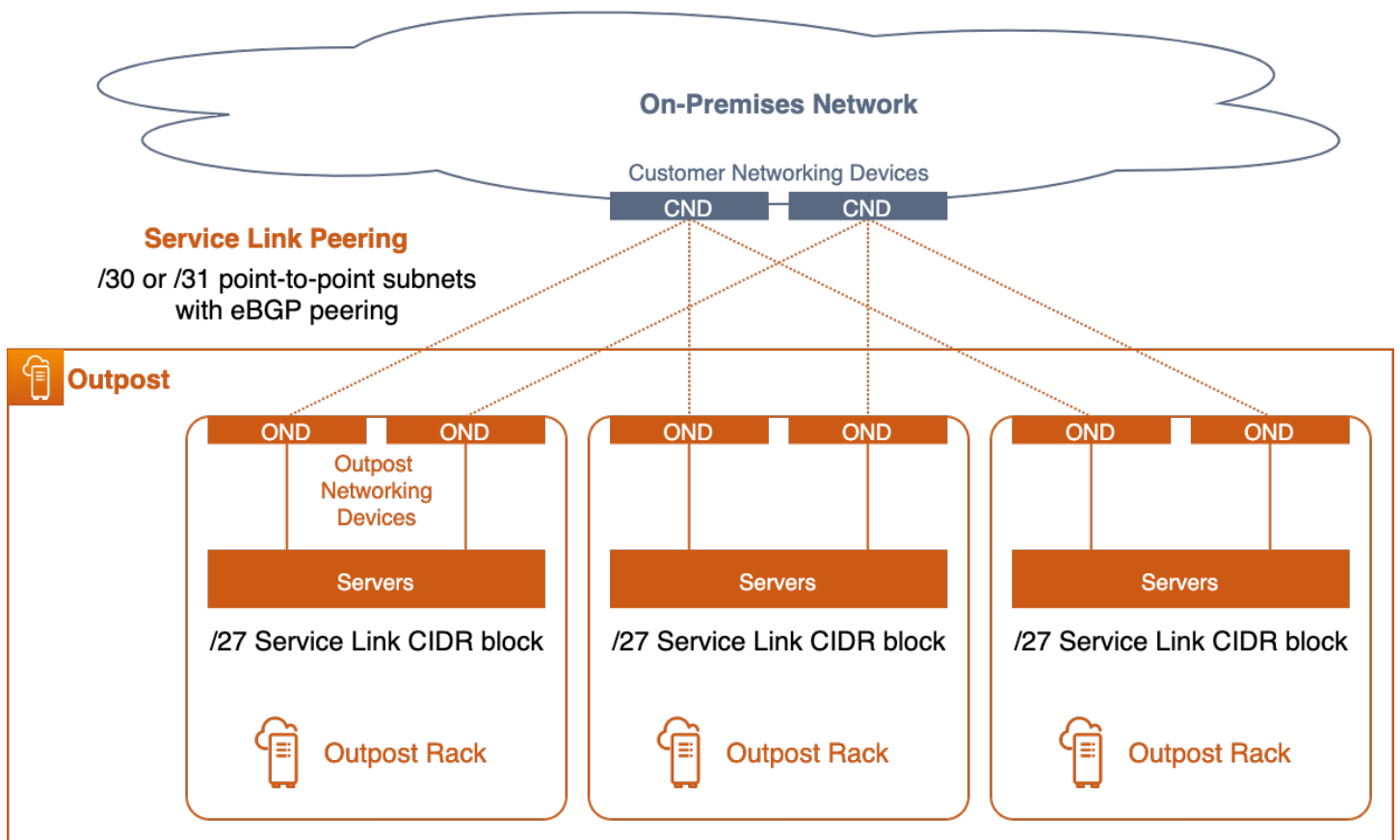
具備備援網路附件的多機架前哨

即使實體連線是單一LAG光纖纜線，「OND到」連CND結始終設定為「」。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。這些LAG連結會設定為 IEEE 802.1q 乙太網路主幹線，以啟用 Outpost 與內部部署網路之間的隔離網路。

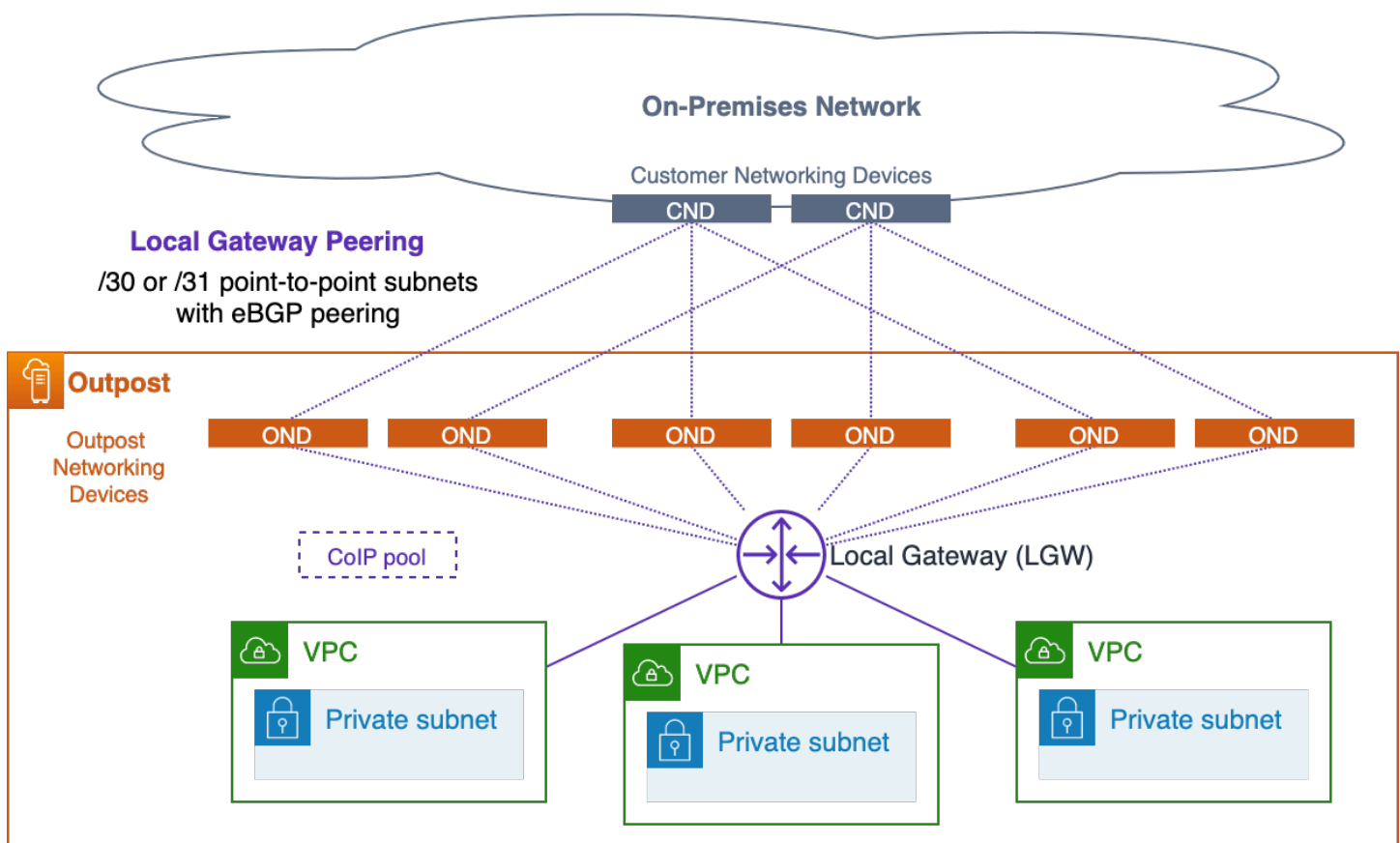
每個前哨都有至少兩個邏輯上隔離的網路，這些網路需要與客戶網路或跨客戶網路通訊：

- 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 () 啟用 Outpost 上的VPC子網路與內部部署網路之間的通訊。LGW

這些隔離網路會透過連結的一組 [point-to-point IP 連線](#)，連接至內部部署網路。LAG每個OND要 CNDLAG連結的VLANIDs設定為 point-to-point (/30 或 /31) IP 子網路，以及每個隔離網路 (服務連結和) 的對BGP等互連。LGW您應該將LAG連結 point-to-point VLANs及其和子網路視為第 2 層分段的路由第 3 層連接。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。



服務連結對等



本機閘道對等互連

您應該終止直接LAG連接的交換器上的第 2 層連結 (及其VLANs)，並在CND交換器上設定 IP 介面和 BGP對等連線。CND您不應在資料中心交換器LAGVLANs之間進行橋接。[如需詳細資訊，請參閱 AWS Outposts 用戶指南。](#)

在邏輯多機架 Outpost 內，備援互連，可在ONDs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 負責前哨內的網路可用性。

高可用性網路附件的建議作法

- 將 Outpost 機架中的每個 Outpost 網路裝置 (OND) Connect 到資料中心的個別客戶網路裝置 (CND)。
- 終止第 2 層連結、第 3 層 IP 子網路VLANs，以及直接連接的客戶網路裝置 () 交換BGP器上的對等互連。CND請勿在內部部OND署網路CNDVLANs之間CNDs或跨越內部部署網路橋接。
- 新增連結匯總群組 (LAGs) 的連結，以增加 Outpost 和資料中心之間的可用頻寬。不要依賴通過兩者的不同路徑的聚合帶寬ONDs。
- 透過備援ONDs使用多種路徑，在 Outpost 網路與內部部署網路之間提供彈性的連線能力。

- 為了達到最佳備援並允許不中斷OND維護，我們建議客戶依下列方式設定BGP廣告和原則：
 - 客戶網絡設備應在不更改BGP屬性的情況下接收來自 Outpost 的BGP廣告，並啟用BGP多路徑/負載平衡以實現最佳的入站流量流量（從客戶到前哨）。AS 路徑前綴用於前哨前BGP綴，以便在需要維護的情況下將流量從特定OND/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。
 - 客戶網絡應該宣傳相同的BGP前綴具有相同的屬性對所有ONDs前哨。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）。在前哨端使用路由策略來將流量從特定的情況下轉移到需要維護OND的情況下。所有客戶端的BGP前綴ONDs都需要相同的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，以暫時移除特定上行或裝置的流量。

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)。Outpost 伺服器會從其服務VPN連結 IP 位址啟動輸出服務連結連線至錨定 AZ 中的錨點。這些連接使UDP用TCP端口 443。AWS 負責區域中錨點的可用性。

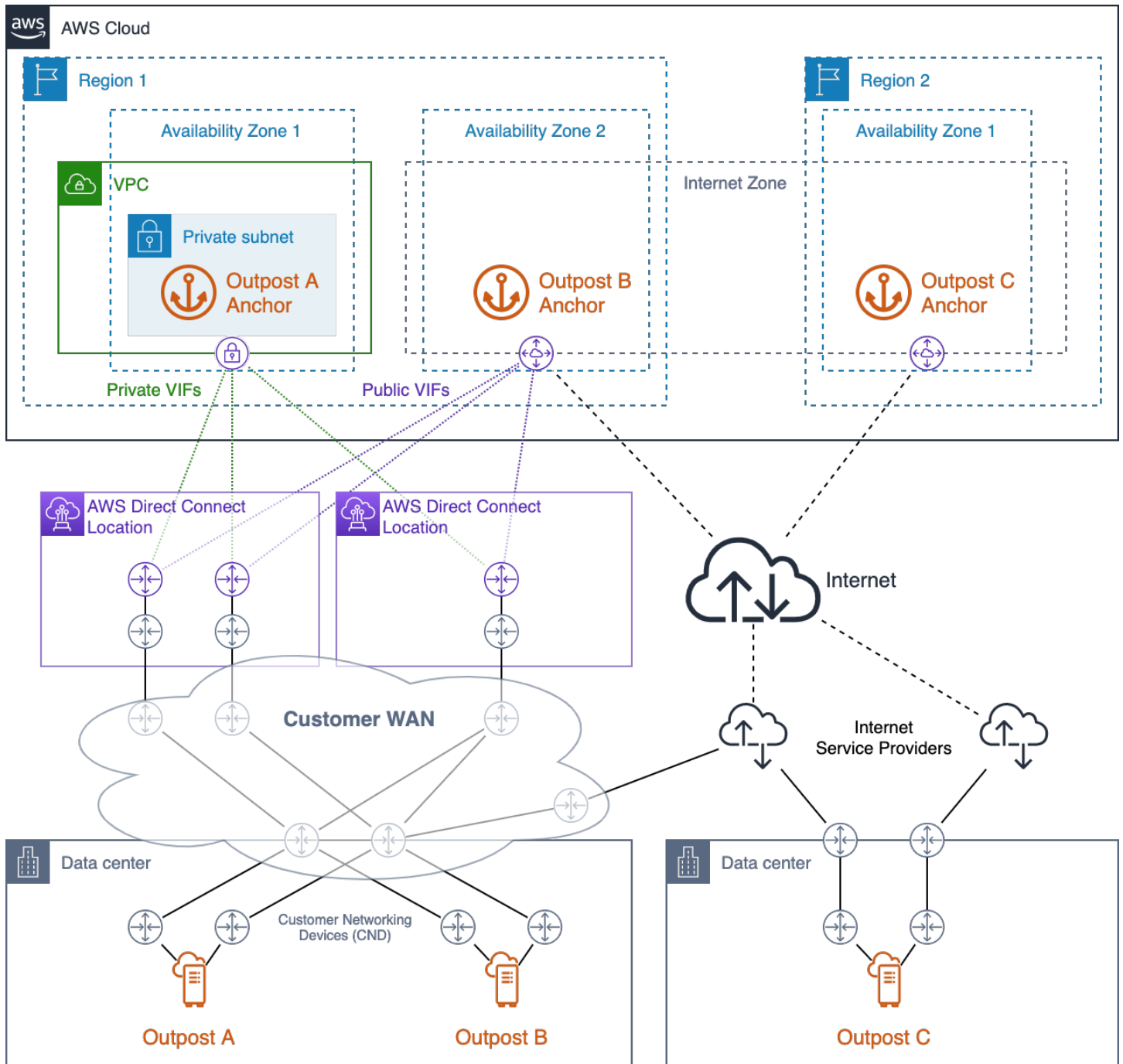
您必須確保 Outpost 服務鏈接 IP 地址可以通過您的網絡連接到錨定 AZ 中的錨點。服務連結 IP 位址不需要與內部部署網路上的其他主機通訊。

公共錨點位於該地區的[公共 IP 範圍](#)（在EC2服務CIDR塊中），並且可以通過互聯網或訪問 [AWS Direct Connect](#)(DX) 公用虛擬介面 (VIFs)。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VPC使用客戶指派的 IP 位址，在[專用的私有子網路](#)中建立。在中建立 VPC AWS 帳戶 擁有 Outpost 資源，並且您負責確保可用VPC且配置正確（不要刪除它！）。私人錨點必須使用[私有直接 Connect](#) 訪問VIFs。

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，以確保其中一個WAN路徑的失敗不會壓倒剩餘的路徑。

下圖顯示了三個 Outposts 與冗餘網路路徑到他們的錨AZs使用 AWS Direct Connect 以及公共互聯網連接。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。



高可用性錨栓連接 AWS Direct Connect 和公共互聯網接入

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 有四個冗餘網路路徑到達其公共錨點。透過在 Outpost A 使用的 Direct Connect 電路 and 位置上的公開 VIFs 佈建，可使用三條路徑。第四條路徑可透過客戶 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 有兩個冗餘的網路路徑到達其公共錨點。前哨 C 部署在與 Outposts A 和 B. Outpost C 不同的資料中心中，其資料中心沒有連接到客戶的專用電路。WAN 相反地，資料中心有兩個不同的網際網路服務供應商所提供的備援網際網路連線 (ISPs)。Outpost C 的服務鏈接流量可以通過任何一個 ISP 網路進行路由，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路，其中帶寬可用性和網路延遲會波動。

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) 路徑控制延遲和頻寬可用性。
- 確保 TCP 定連接 UDP 埠 443 已從 Outpost 服務連結 CIDR 封鎖開啟 (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。

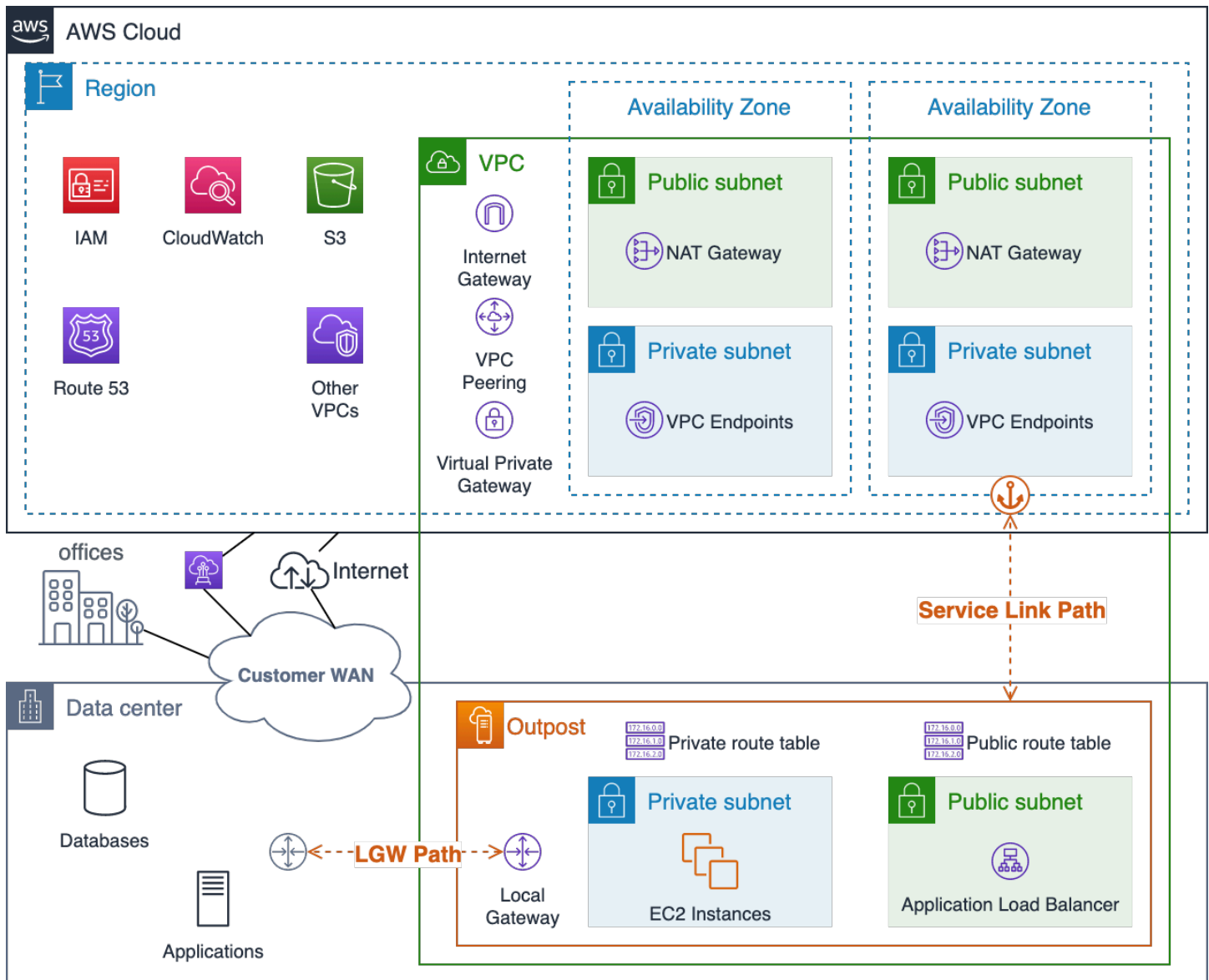
應用程式/工作負載路由

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。指向的路由會 LGW 將流量引導出本機閘道和內部部署網路。指向該地區的服務和資源的路由，例如 Internet Gateway，網 NAT 關，虛擬專用網關 TGW，並將使用 [服務鏈接](#) 到達這些目標。如果您在同一個 Outpost VPCs 上有多個

對VPC等連線，則兩者之間的流量會VPCs保留在 Outpost 上，且不會使用返回該地區的服務連結。
如需對VPC等互 [Connect](#) 的相關資訊，請參閱 [Amazon VPCs 使用VPC者指南](#) 中的使用對VPC等互連線。



前哨服務鏈接和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 和重要的內部部署應用程式、系統LGW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 AWS Management Console、CLI APIs、和其他基礎結構即程式碼 (IaC) 工具；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互 Internet Gateway (IGW) 在該地區或通過本地網關 (LGW) 路徑訪問互聯網。透過LGW路徑和內部部署網路路由傳送網際網路流量，可讓您使用現有的內部部署網際網路入口/出口點，並可提供較低的延遲、提高和減少 MTUs AWS 與使用區域IGW中的服務連結路徑相比，資料輸出會收取費用。

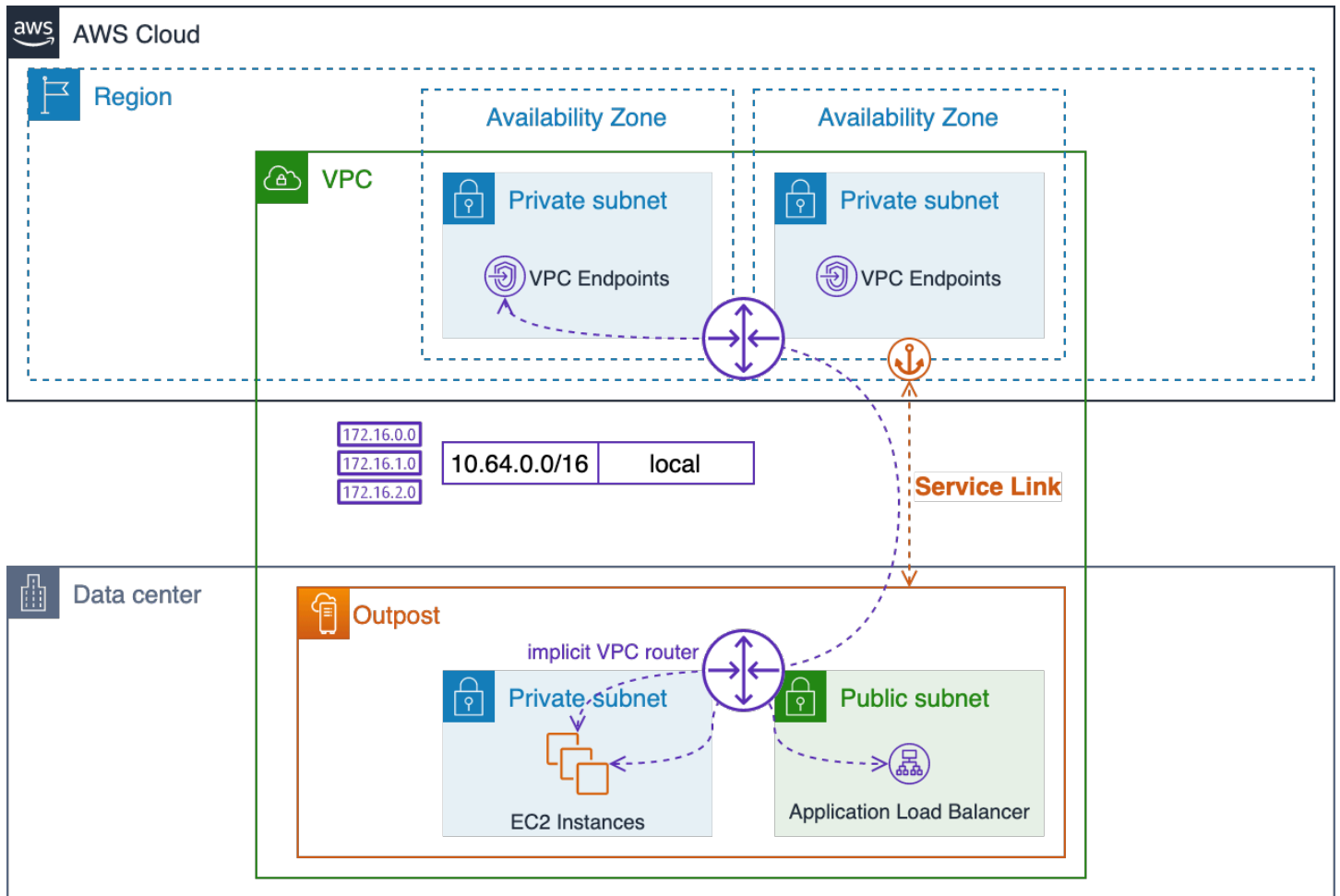
如果您的應用程式必須在內部部署執行，而且需要可從公用網際網路存取，則應透過內部部署網際網路連線將應用程式流量路由LGW至，以連線到 Outpost 上的資源。

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。入站互聯網流量將通過 AWS 區域 並通過服務鏈接路由到前哨上運行的資源。

響應流量將依次通過服務鏈接進行路由，然後通過 AWS 區域的互聯網連接。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。如果您的應用程式可以在該地區運行，則該地區是運行它的最佳場所。

VPC資源之間的流量 (相同VPC) 將始終遵循本地VPCCIDR路由，並VPC由隱式路由器在子網路之間進行路由。

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



通過隱式VPC路由器進行本地路由

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 和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

而 Amazon EC2 容量 AWS 區域 看似是無限的，Outposts 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

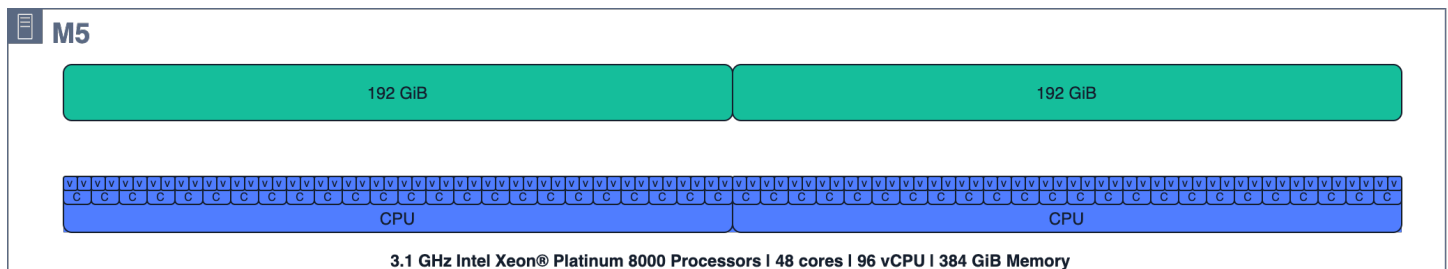
- [容量規劃](#)
- [容量管理](#)
- [例證放置](#)

容量規劃

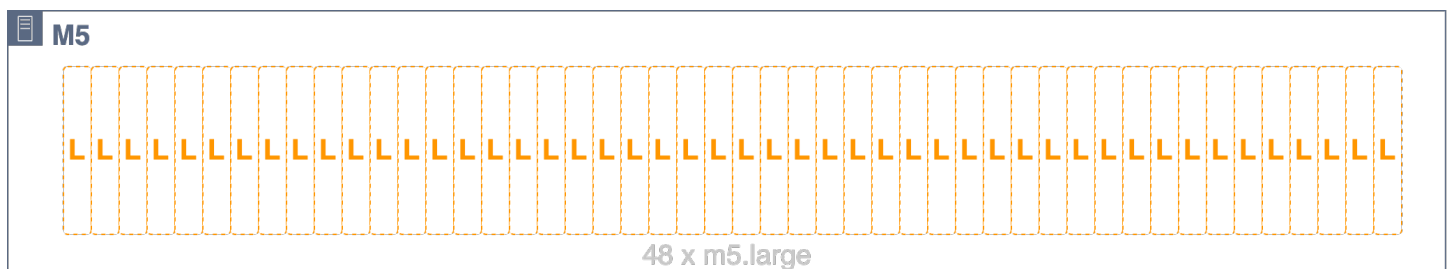
而 Amazon EC2 容量 AWS 區域 看似是無限的，Outposts 上的容量是有限的-受計算容量排序的總體積的限制。您負責規劃和管理 Outposts 部署的運算容量。您應該訂購足夠的運算容量來支援 N+M 可用性模型，其中 N 是所需的伺服器數目，M 是佈建以容納伺服器故障的備用伺服器數目。N+1 和 N+2 是最常見的可用性等級。

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，您必須先提供插槽配置，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。

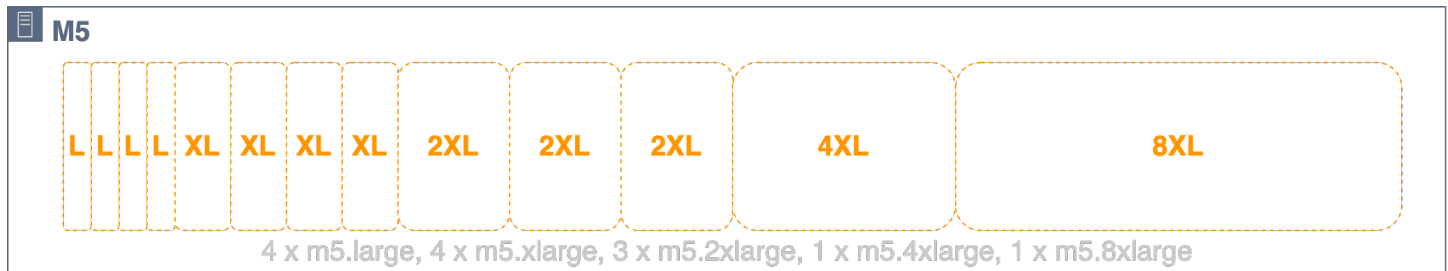
伺服器可以是同質開槽，其中所有插槽都是相同的執行個體大小 (例如 48 個 m5.large 插槽)，或是以混合執行個體類型 (例如 4、4 m5.large、3 m5.2xlarge、1 和 1 m5.4xlarge m5.8xlarge) 進行異質開槽 — 請參閱接下來的三個數字 m5.xlarge，瞭解這些開槽設定的視覺效果。



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*、1 和 1 *m5.4xlarge* 個插槽 *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。

所有伺服器都會將其佈建的插槽貢獻給 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 *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 EC2 容量時，請務必考慮伺服器插槽和容量集區。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) 至少一部伺服器的故障。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*
- $-m5.16xlarge$ 和 $-m5.8xlarge$

諮詢您的 AWS 帳戶 團隊來驗證您的計劃 AWS Outposts 機架開槽配置。

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。



可視化EC2伺服器插槽、執行中執行個體和插槽集區

對於更複雜的開槽配置 (伺服器開槽不相同)，您需要計算每個容量集區的 N+M 可用性。EC2您可以使用下列公式來計算有多少伺服器 (為指定EC2容量集區提供插槽) 可能發生故障，而且仍允許剩餘的伺服器攜帶執行中的執行個體：

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

其中：

- $poolSlots_{available}$ 是指定容量集區中的可用插槽數EC2量 (集區中的插槽總數減去執行中執行個體的數量)
- $serverSlots_{max}$ 是任何伺服器貢獻給指定EC2容量集區的插槽數目上限
- 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？

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

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

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

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。

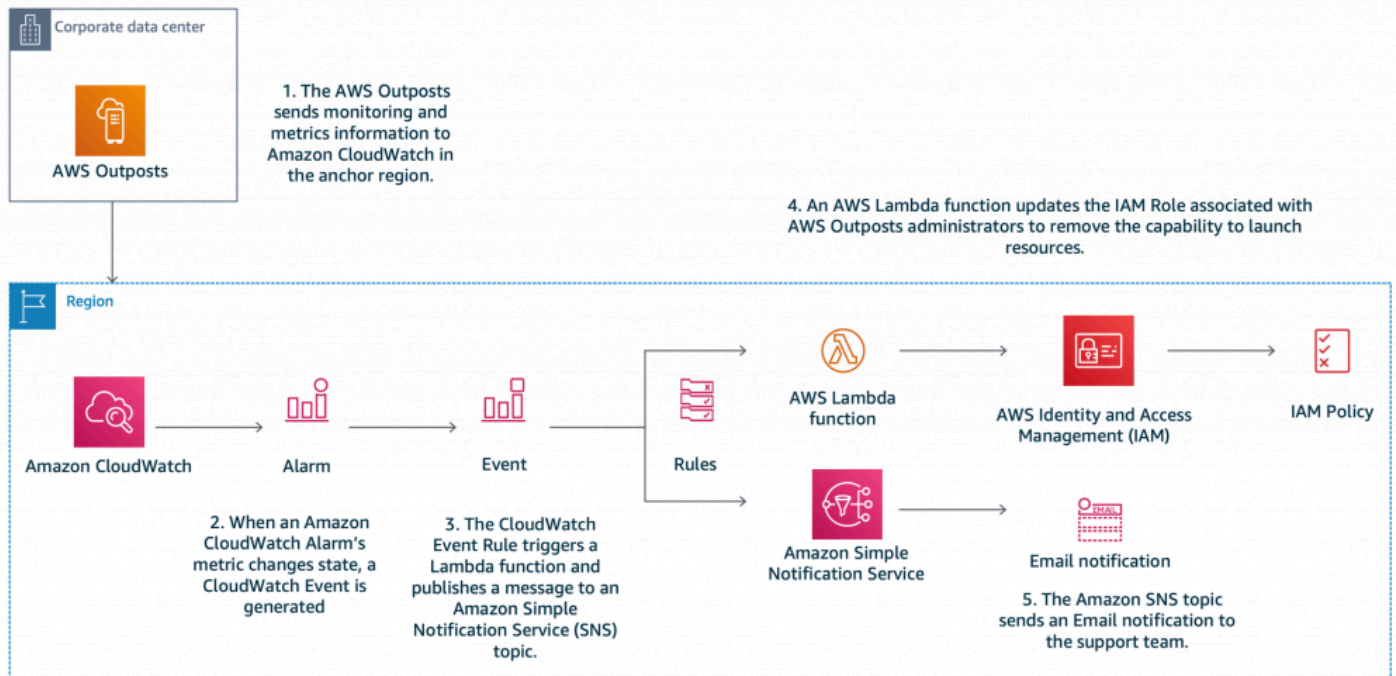
計算容量規劃的建議做法：

- 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

您可以監視 Outpost EC2 執行個體集區使用率 AWS Management Console 並通過 Amazon CloudWatch 指標。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](#) 機制來復原或取代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。在[管理您的 AWS Outposts 使用 Amazon CloudWatch 和容量 AWS Lambda](#) 博客文章提供了一個動手教程，向您展示如何組合 AWS CloudWatch 和 AWS Lambda 管理您的 Outpost 容量以維持執行個體的可用性。



管理 AWS Outposts 能力與 Amazon CloudWatch 和 AWS Lambda

運算容量管理的建議做法：

- 在 Auto Scaling 群組中設定您的 EC2 執行個體，或使用執行個體自動復原重新啟動失敗
- 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。

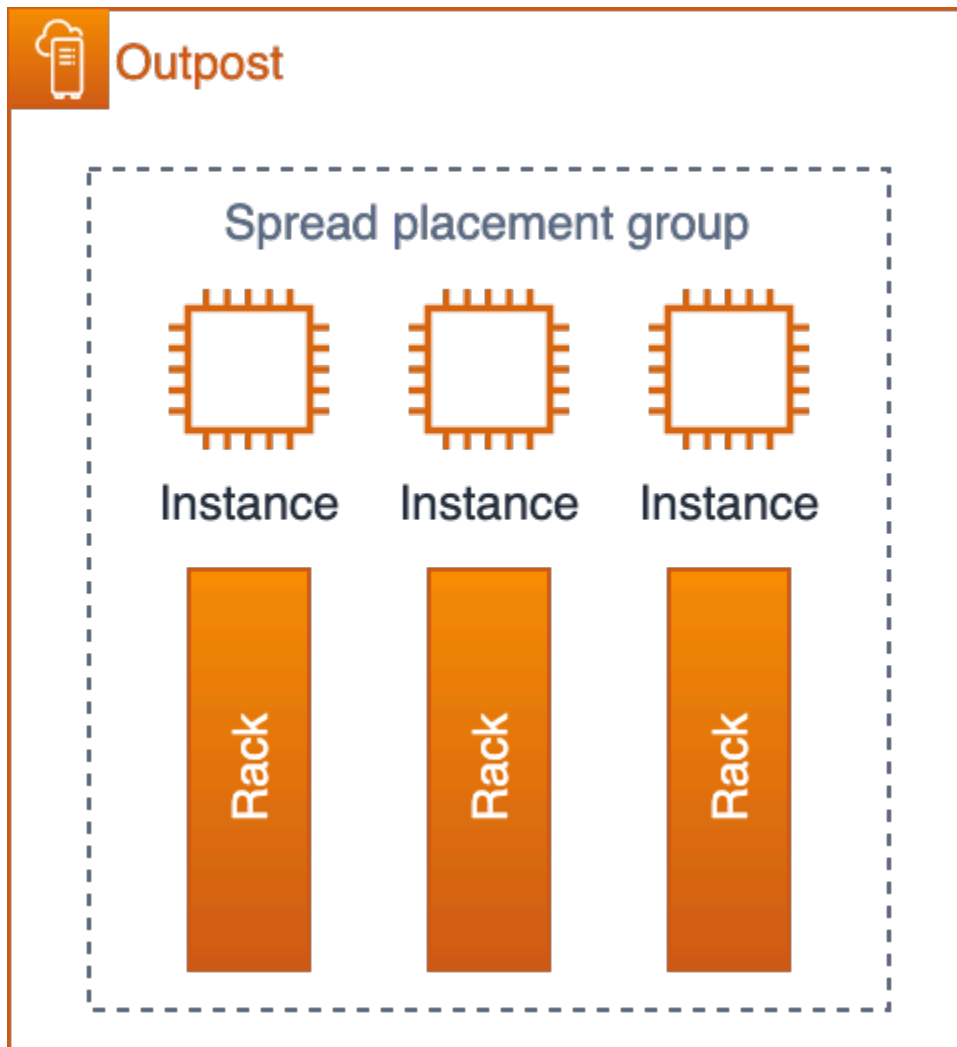
例證放置

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 Outposts 策略來防止機架和資料中心故障模式，如果前哨站固定在單獨 AZs 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](#)。

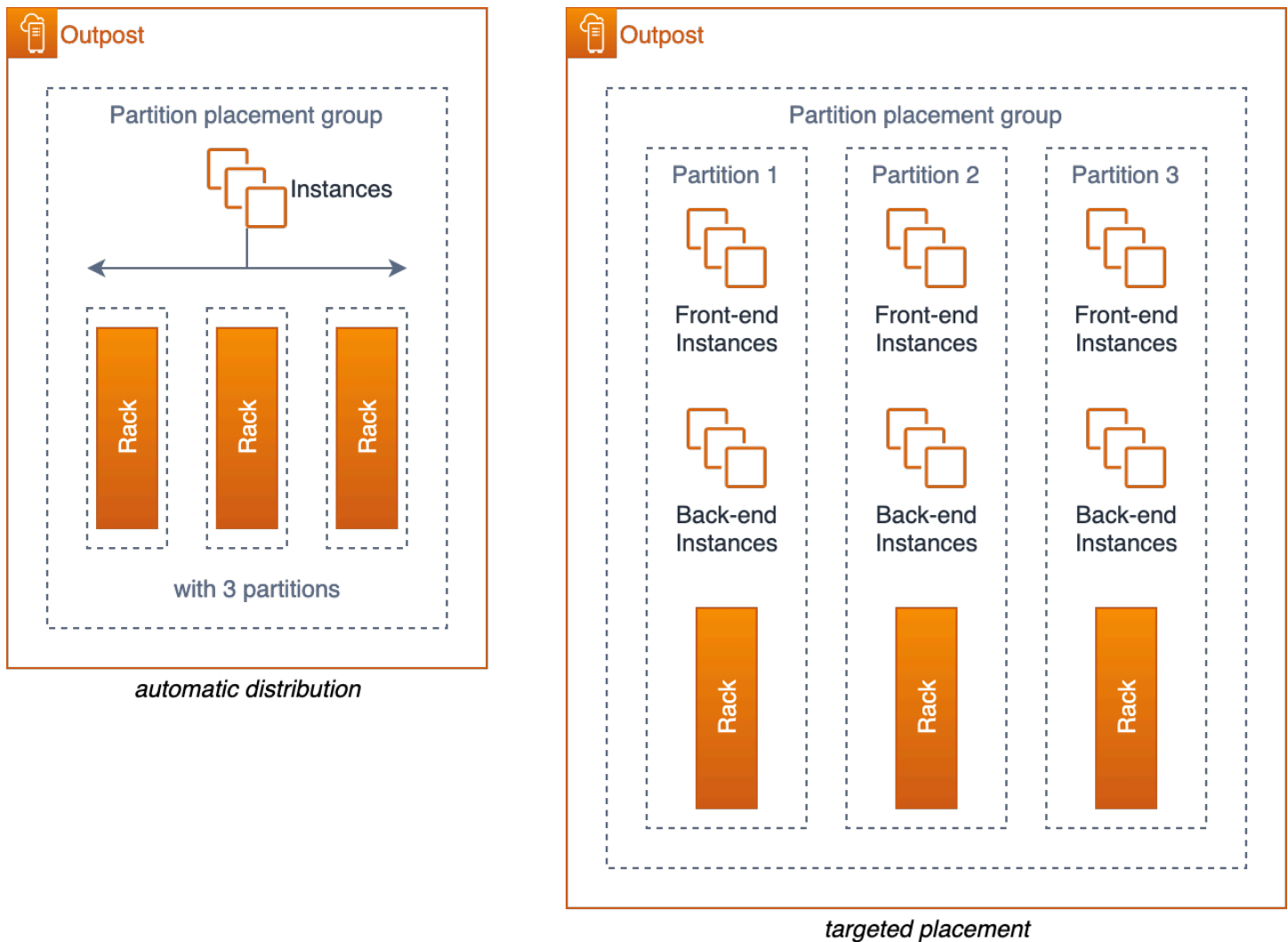
Outposts 上的 Amazon EC2 放置群組 (單一 Outpost 多機架執行個體放置) — 可讓您使用 [叢集](#)、[分攤](#) 和 [分割](#) 策略來影響放置。分攤和分區放置策略可讓您在多機架 Outpost 中跨機架分配執行個體。

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。



EC2在前哨傳播放置組有三個機架

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。



EC2分區放置組在前哨與三個機架

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，您或許可以插入伺服器，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，請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，則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為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 放置群組來控制單一 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，不如考慮將容量分割為兩個中小型機架，讓您能夠利用 EC2 放置群組在機架之間分配執行個體的能力。

儲存

所以此 AWS Outposts 機架服務提供三種儲存類型：

- 支援 [執行個體](#) 類型的 EC2 執行個體
- 用於永久性區塊儲存的 [Amazon 彈性區塊存放區 \(EBS\) gp2 磁碟區](#)
- Outposts [上的 Amazon 簡單儲存服務 \(Outposts 上的 S3 \)](#)，用於本地對象儲存

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 \(執行\) 存留期內](#) 保留。

Outposts 物件儲存裝置上的 Outposts EBS 磁碟區和 S3 是作為 AWS Outposts 機架管理服務。客戶必須負責 Outpost 儲存集區的容量管理。客戶在訂購 Outpost 時，會指定其 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 儲存服務上的 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 以及監控 [Outposts 容量使用率上的前哨站 EBS 和 S3 的 CloudWatch 指標](#)。

資料保護

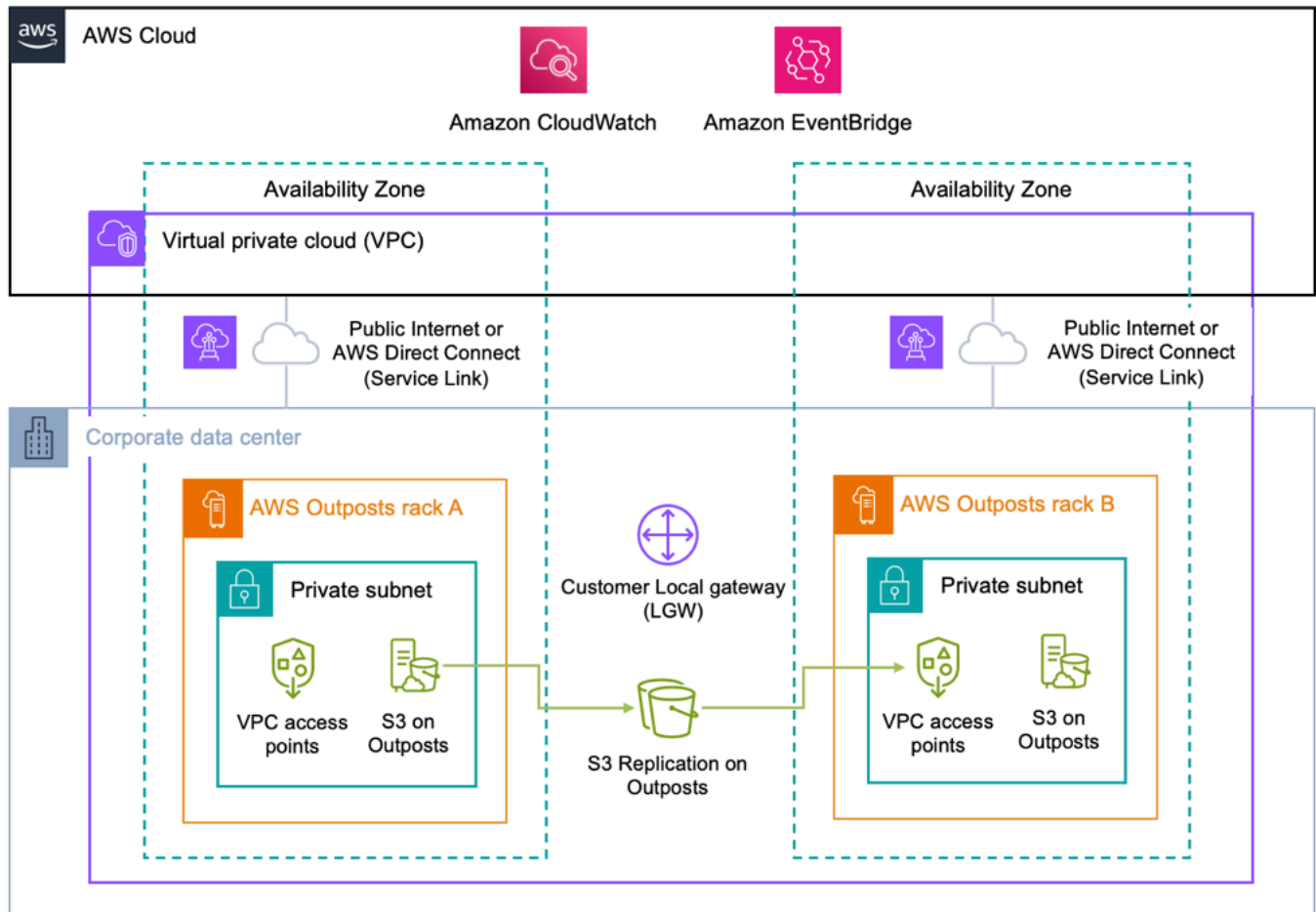
對於 EBS 磁碟區：AWS Outposts rack 支援 EBS 磁碟區快照，提供簡單安全的資料保護機制，以保護您的區塊儲存資料。快照是 EBS 磁碟區的 point-in-time 增量備份。根據預設，前哨站上的 [Amazon EBS 磁碟區快照](#) 會存放在該區域的 Amazon S3 上。如果您的 Outposts 已在 Outposts 容量上設定 S3，您可以使用 Outposts 上的本機 [快照，使用 Outposts 儲存上的 S3 將快照本地](#) 存放在 Outpost 上。

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。

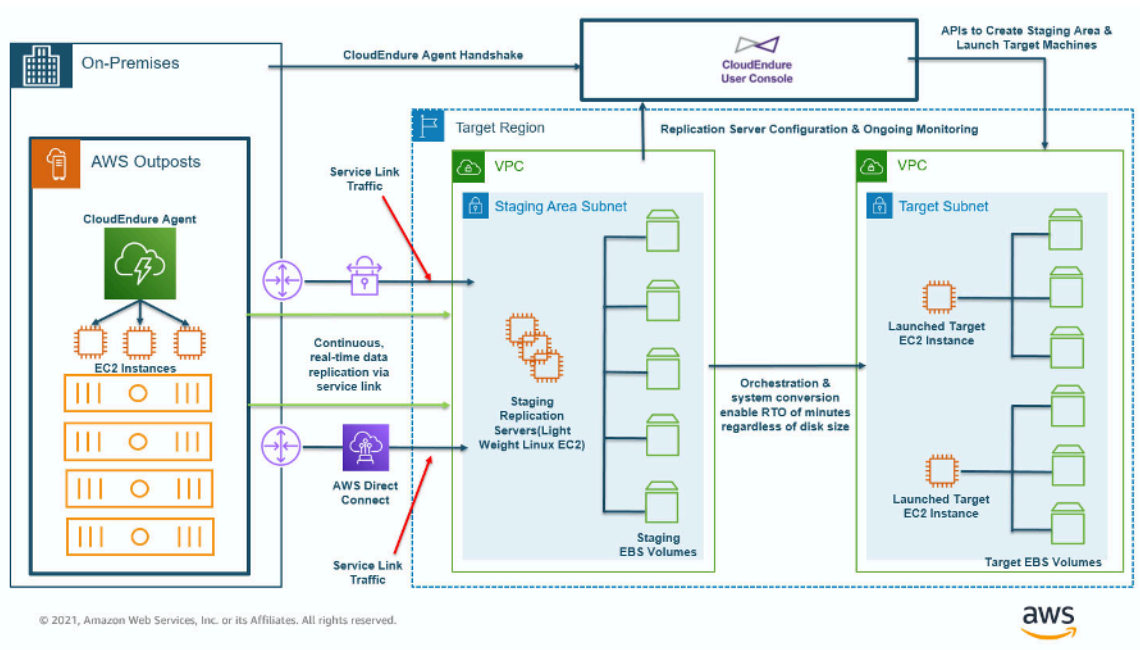
- 您可以在 [Outposts 上使用 S3 複寫](#)，建立和設定複寫規則，以自動將 S3 物件複寫到另一個 Outpost，或複寫到相同 Outpost 上的另一個儲存貯體。在複寫期間，Outposts 物件上的 S3 會透過客戶的本機閘道 (LGW) 傳送，且物件不會傳回 AWS 區域。在 Outposts 上進行 S3 複寫提供了一種簡單且靈活的方式，可在特定資料周邊自動複寫資料，以解決資料備援和合規要求。

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](#) 在您的前哨站和區域之間自動化 S3 的 Outposts 資料傳輸。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 AWS 區域可讓您利用 99.999999999% (11 個 9 年代) 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。DR [的架構 AWS Outposts 與 CloudEndure](#) 博客文章描述了每個這些情況以及如何設計一個解決方案與 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) 需要在 Outposts 儲存上使用 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。
- 對於非資料存放區使用案例，請使用 AWS DataSync 將存放在前哨 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。

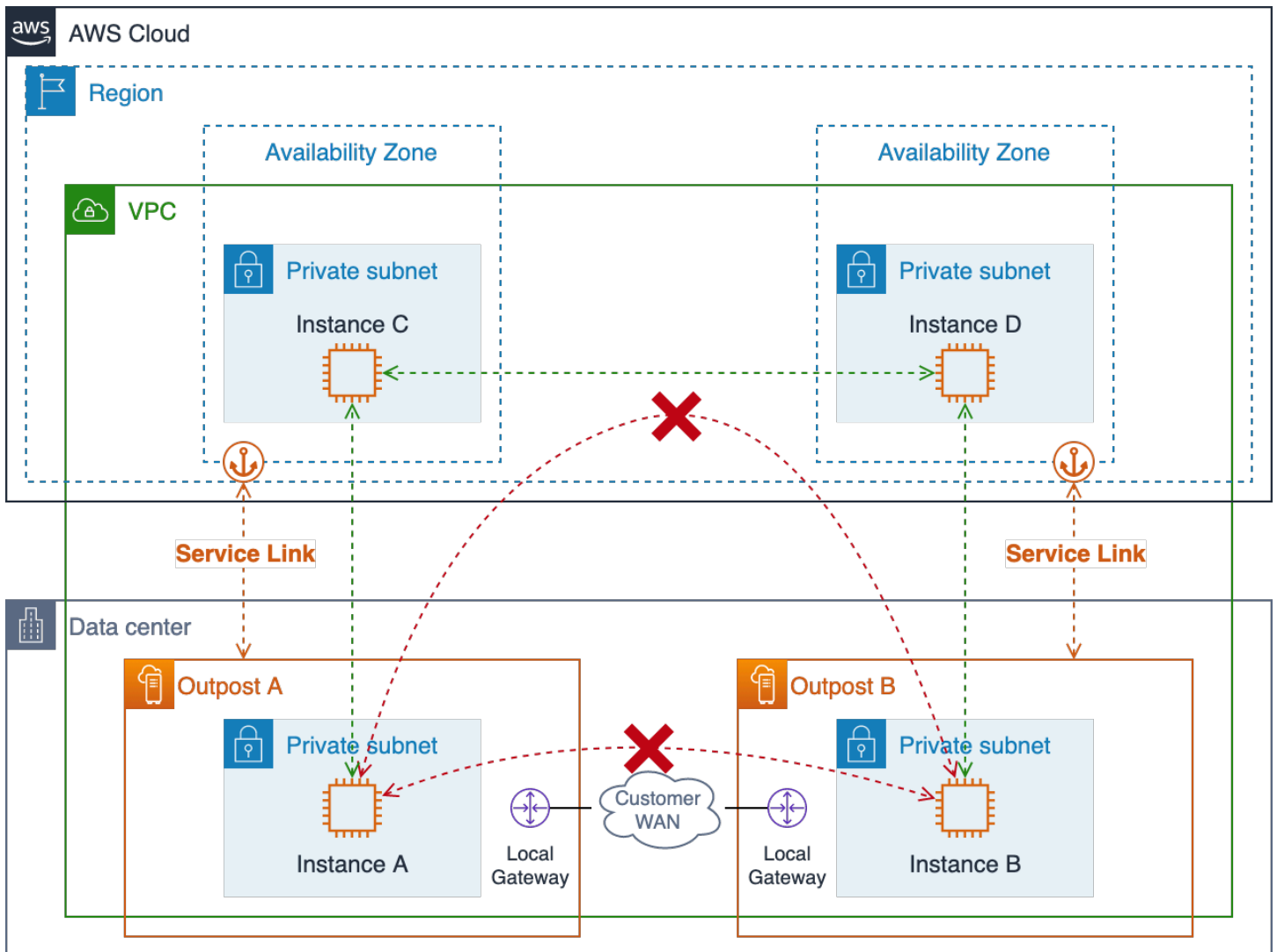
更大的故障模式

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。您將 Outposts 錨定到不同的可用區域 (AZs) AWS 區域 或跨多個區域。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 [Elastic 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。部署在同一個部署的兩個單獨 Outposts 上的資源 VPC 無法在客戶網絡中相互通信。部署在不同部署的兩個獨立 Outposts 上的資源 VPCs 可以在客戶網絡中相互通信。

下列兩個圖表說明封鎖且成功的網路路徑。

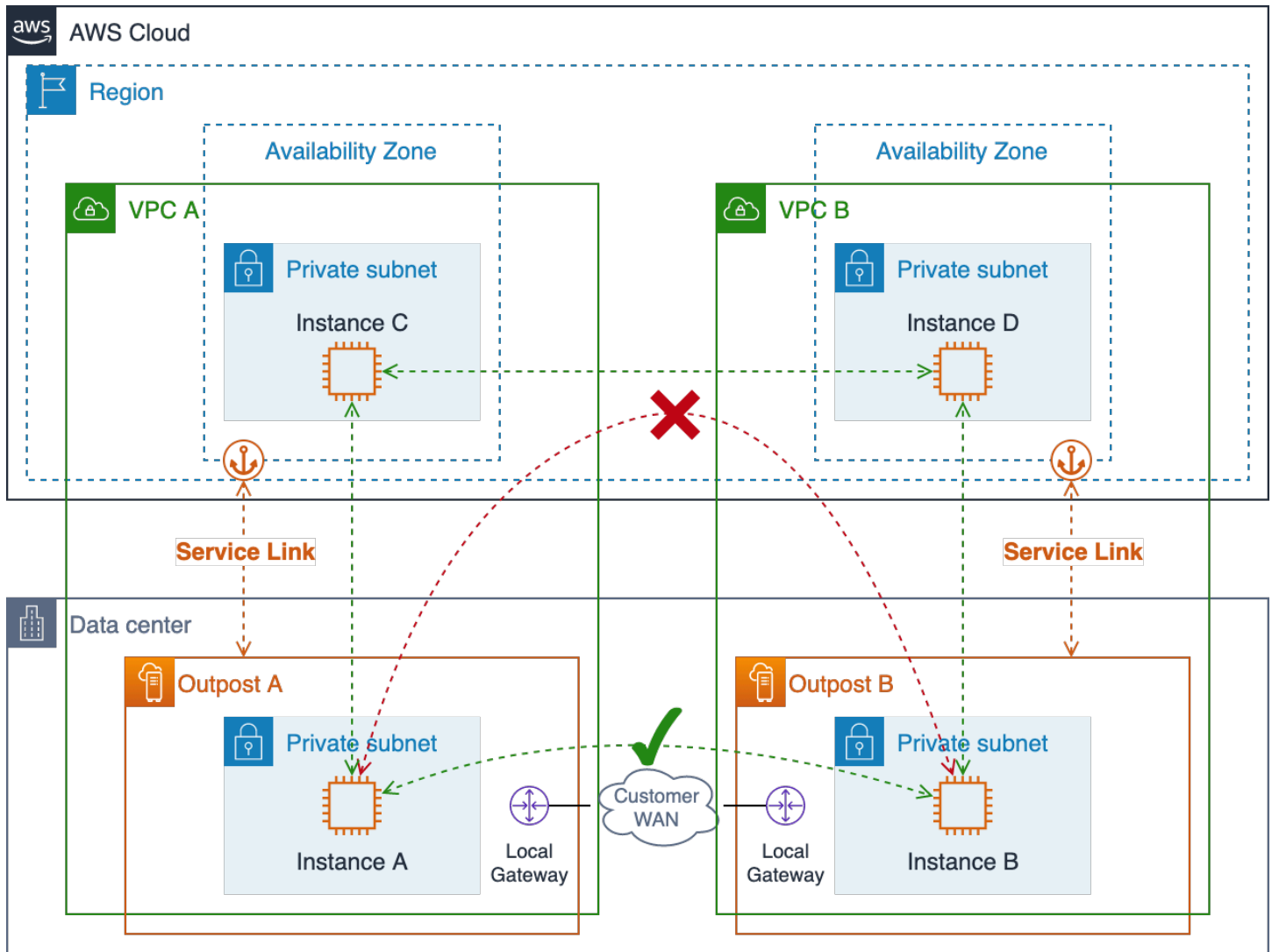


單一VPC多重前端網路路徑

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。此類流量會在兩個方向產生輸出費用，並且可能比將流量路由到客戶WAN的流量高得多。

在同一個多個 Outposts 的資源VPC不能相互通信。前哨站之間的流量VPC將始終遵循當地VPCCIDR路線，通過該地區將被阻止的地區。

您應該使用單獨的VPCs方式在多個 Outposts 上部署資源，以允許您在本地區域內部部署和網路之間路由 Outpost 到 Outpost 流量。WAN



VPC多重前哨網路路徑

防範較大失敗模式的建議做法：

- 部署錨定到多個AZs和區域的多個 Outposts。
- 針VPCs對多前哨部署中的每個前哨使用個別的。

結論

同 AWS Outposts 機架，您可以使用熟悉的內部部署應用程式來建置、管理和擴充高可用性的 AWS 工具和服務 EC2，如 Amazon EBS，Amazon Outposts，Amazon ECS，Amazon 和 Amazon 上的 Amazon EKS S3。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 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。

當您提供具有足夠電源、空間、冷卻和彈性連線的 Outpost 部署時 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 機架消除了構建內部部署運算、儲存和應用程式網路集區的無差別繁重工作，並允許您擴展 AWS 資料中心和主機代管設施的全球基礎架構。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，高級專業解決方案建築師，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) 代表當前文件 AWS 產品供應項目和做法如有變更，恕不另行通知，且 (c) 不會建立任何承諾或保證 AWS 及其關聯公司、供應商或授權人。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。的責任和責任 AWS 它的客戶控制 AWS 協定，且此文件不屬於任何協議的一部分，也不會修改兩者之間的任何協議 AWS 及其客戶。

© 2023 Amazon Web Services, Inc. 或其附屬公司。保留所有權利。

AWS 詞彙表

對於最新 AWS 術語，請參閱 [AWS 詞彙表](#) 中的 AWS 詞彙表 參考。

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。