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至 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：

- 混合雲端策略提供管理雲端和內部部署資源消耗的指導方針，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。這些需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中所述的解決方案，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 選取項目 AWS Local Zones 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
- 先決條件和限制
- 混合雲端採用程序：

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

在遵循本指南之前，請與您的 AWS 帳戶 團隊合作 AWS Partner ，或檢閱使用 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、每分鐘立方英呎 (CFM) 氣流 145.8 倍的資料中心環境中運作，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 Enterprise On-Ramp 的有效合約。

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 Local Zone AWS Direct Connect 的存在點 (PoP) AWS 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 Amazon S3 on Outposts 使用者指南中的 Amazon S3 on Outposts 與 Amazon S3 有何不同？一節會討論這些內容。 Amazon S3
- 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

- Local Zones 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 AWS Direct Connect 私有虛擬介面 (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：

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。網路是連線的基礎，可到達部署在這些節點的工作負載，而且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。

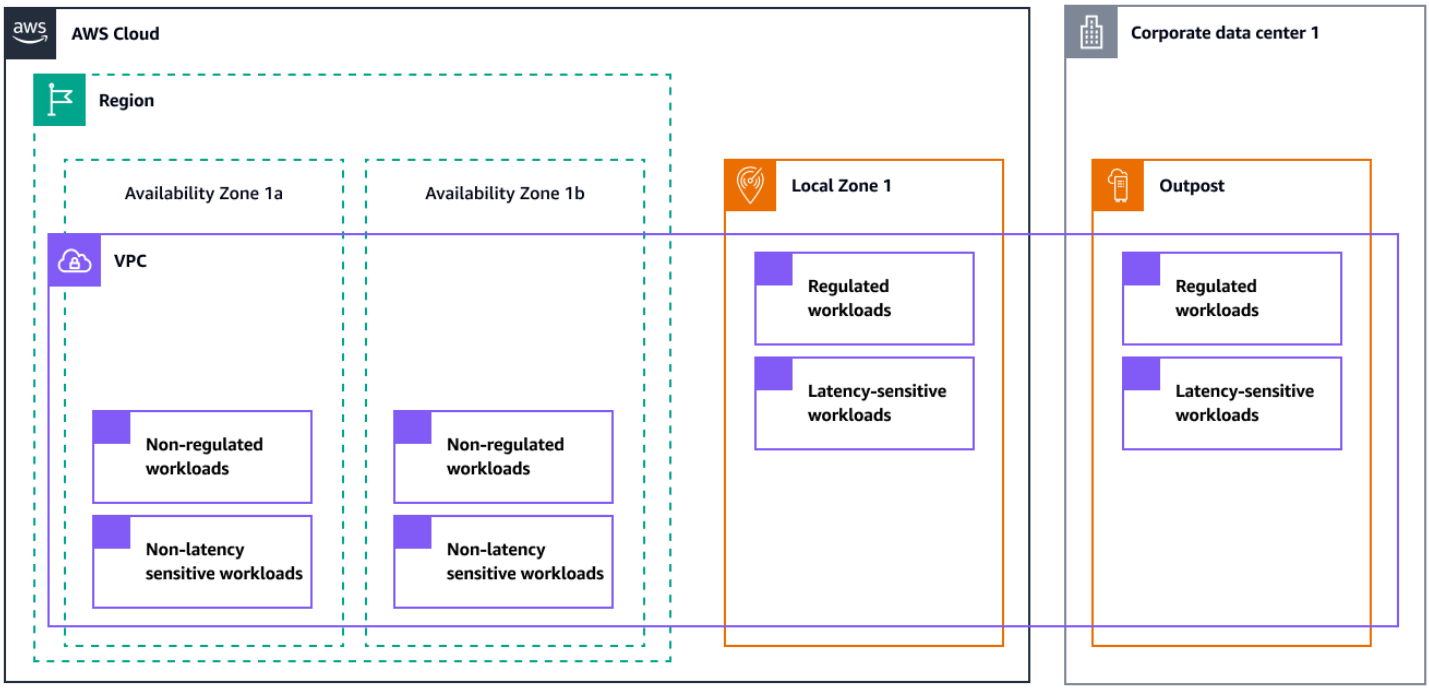
- Local Zones：若要將 Local Zone 子網路新增至 VPC，請遵循與可用區域搭配使用的相同程序，但指定 Local Zone ID (<local-zone-name>在下列範例中）。

```
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。



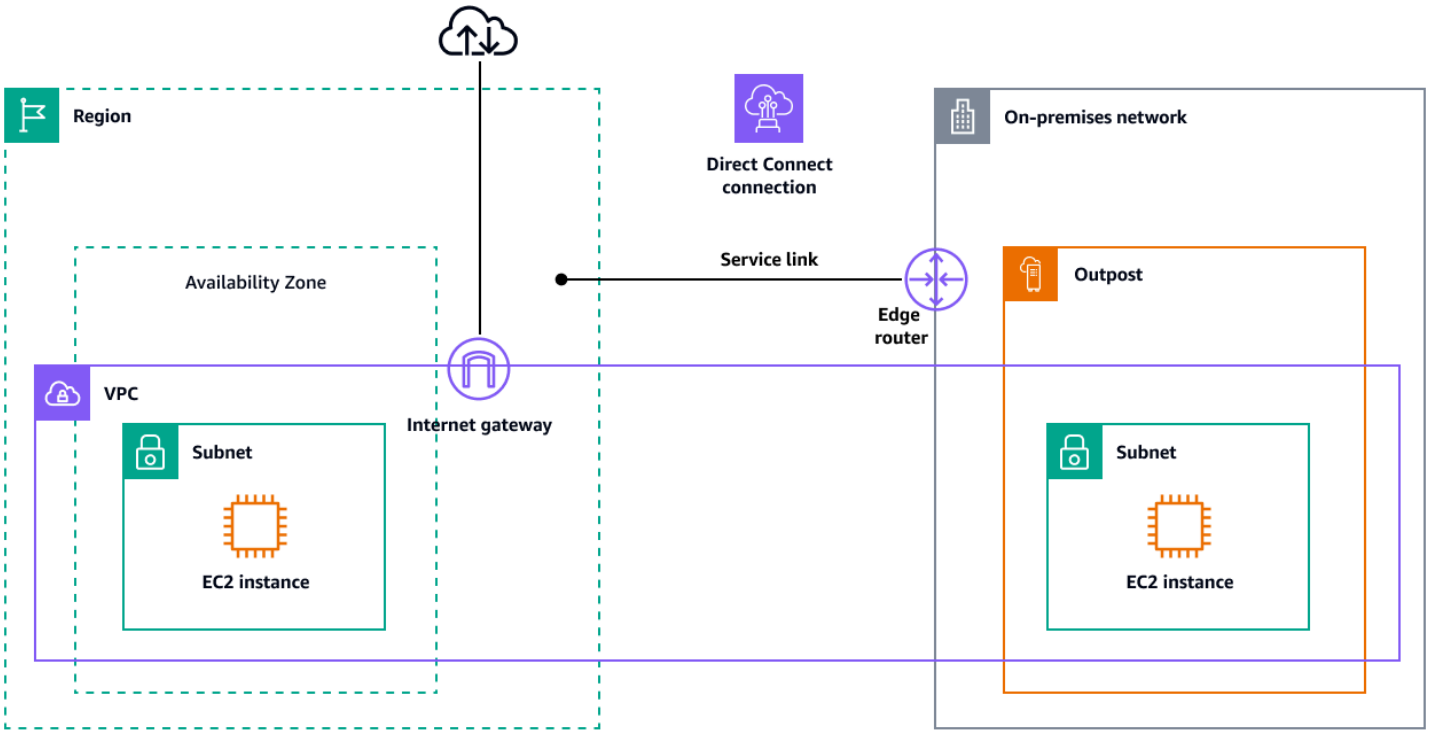
邊緣到區域流量

當您使用 Local Zones 和 等服務來設計混合架構時 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，您的責任可能會有所不同：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，並在 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 AWS Direct Connect 公有虛擬界面 （ 公有 VIF)，或透過 AWS 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 AWS 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 到本機區域。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
AWS 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。基礎設施完全由 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，再設計具有區域與 Local Zones 之間共同相依性的任何架構。

邊緣到內部部署流量

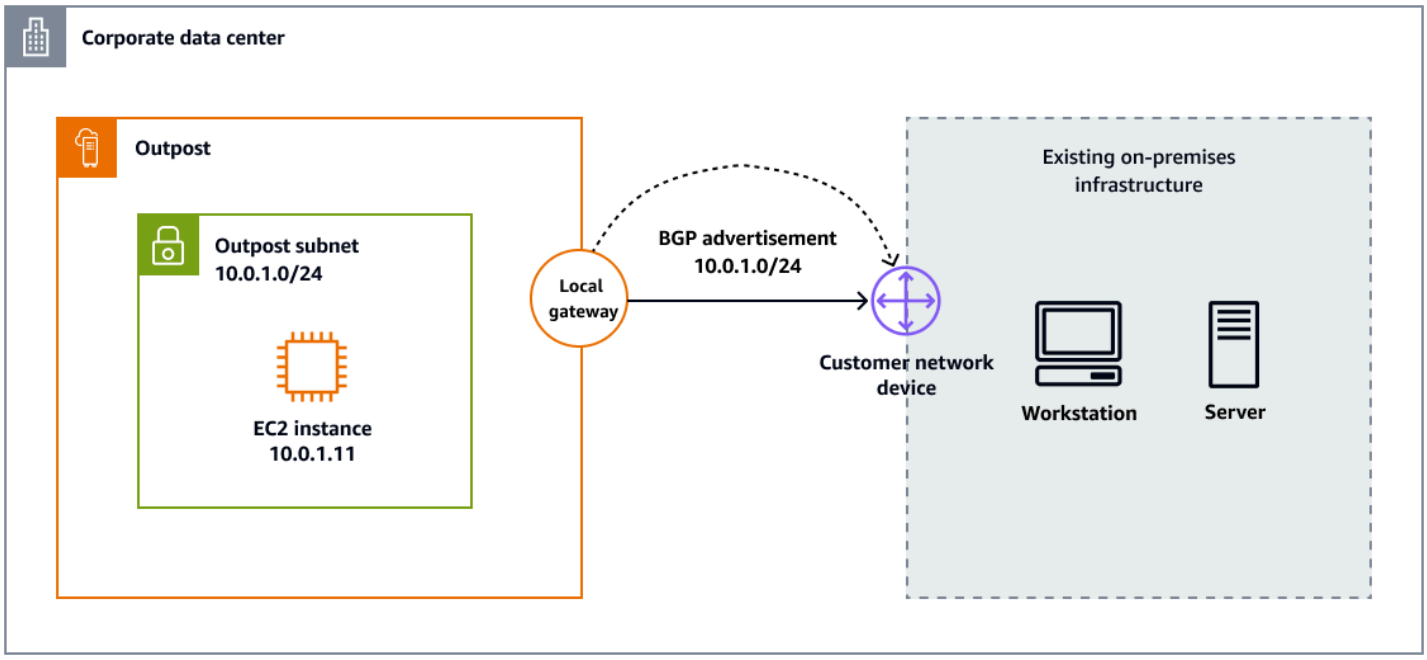
AWS 混合雲端服務旨在解決需要低延遲、本機資料處理或資料駐留合規的使用案例。存取此資料的網路架構很重要，取決於您的工作負載是在 AWS Outposts 或 Local Zones 中執行。本機連線也需要定義明確的範圍，如以下章節所述。

AWS Outposts 本機閘道

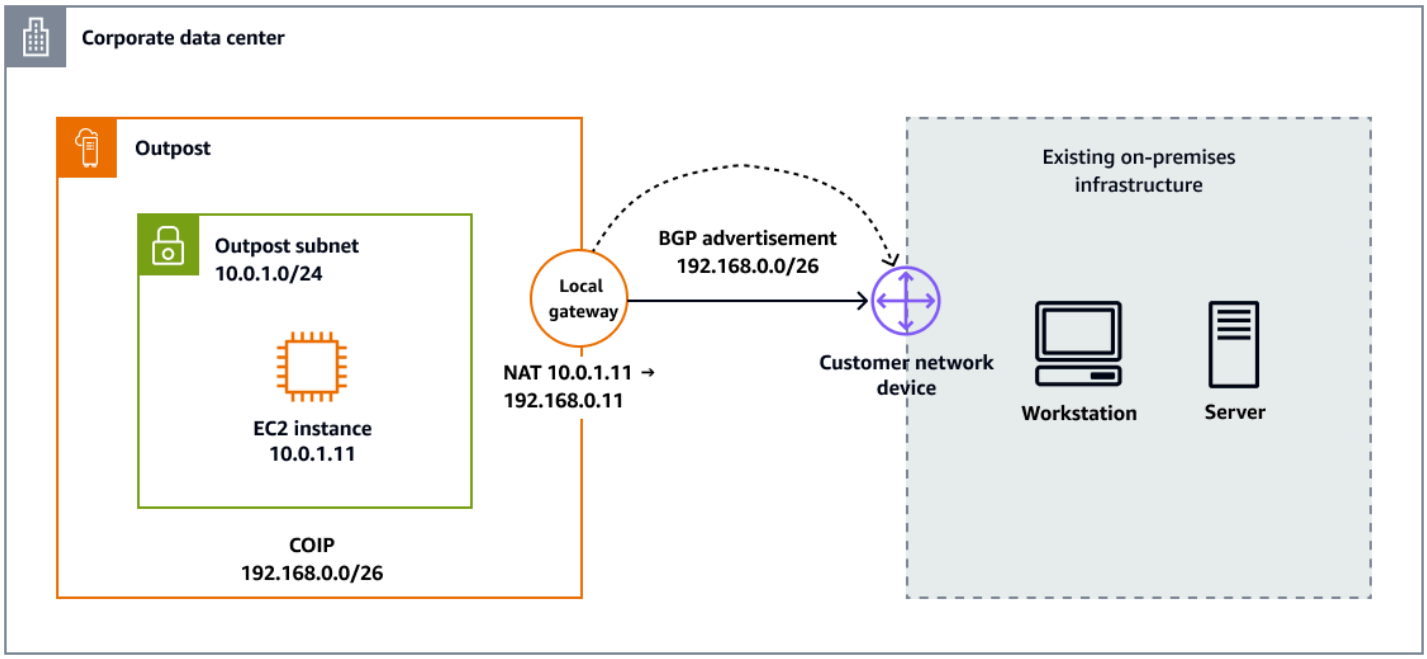
本機閘道 (LGW) 是 AWS Outposts 架構的核心元件。本機閘道可讓您在 Outpost 子網路與內部部署網路之間進行連線。LGW 的主要角色是提供從 Outpost 到本機內部部署網路的連線。它還透過直接 VPC 路由或客戶擁有的 IP 地址，透過內部部署網路提供網際網路連線。

- 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 AWS Direct Connect

Local Zones 也支援 AWS 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 文件中的 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，流量會保留在 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) 的全域基礎設施。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，但 AWS Local Zones FAQ 中記錄的清單除外 （請參閱問題：Local Zones 中 EBS 磁碟區的預設加密行為為何？)。

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。

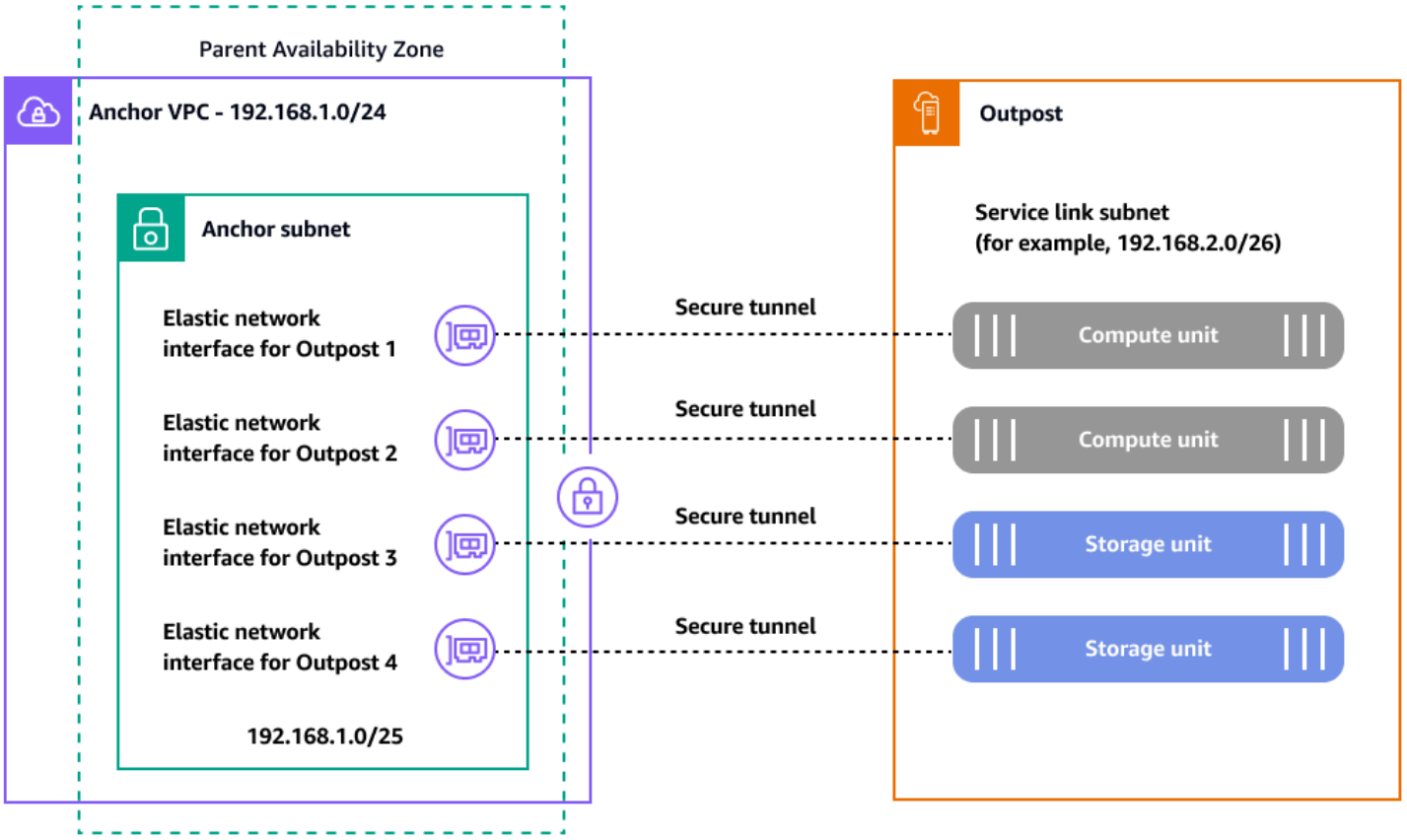
> **Note**
>
> Amazon S3 on Outposts 不支援使用 KMS 金鑰 (SSE-KMS) 的伺服器端加密。

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 AWS 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。

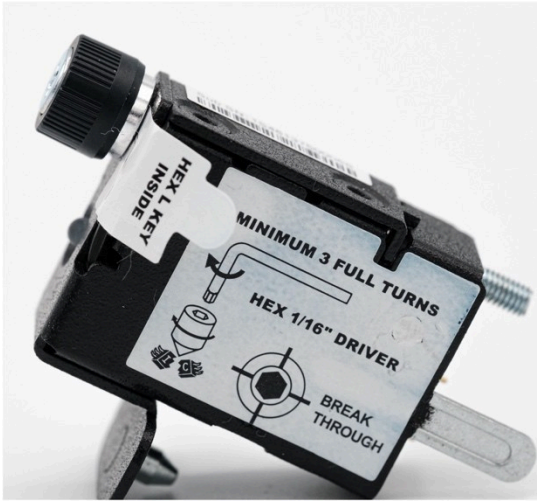
通訊協定	來源連接埠	來源地址	目的地連接埠	目的地地址
UDP	443	AWS Outposts 服務連結 /26	443	AWS Outposts 區域的公有路由或錨點 VPC CIDR

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

本地區域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，所有流經 AWS 全球網路的資料都會在實體層自動加密，再離開 AWS 安全的設施。如果您對於加密內部部署位置和 AWS 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 AWS 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 AWS 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。它旨在提供一種機制，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，該螺絲會摧毀 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) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行驗證 （登入） 和授權 （具有許可） 來使用 AWS Outposts 資源。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。

基礎架構安全

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。分層網路可協助在邏輯上將類似的網路元件分組。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方法來套用多個控制項。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。檢查和篩選每一層的流量。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。每個運算資源類型都需要不同的安全方法。不過，這些資源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畫。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。

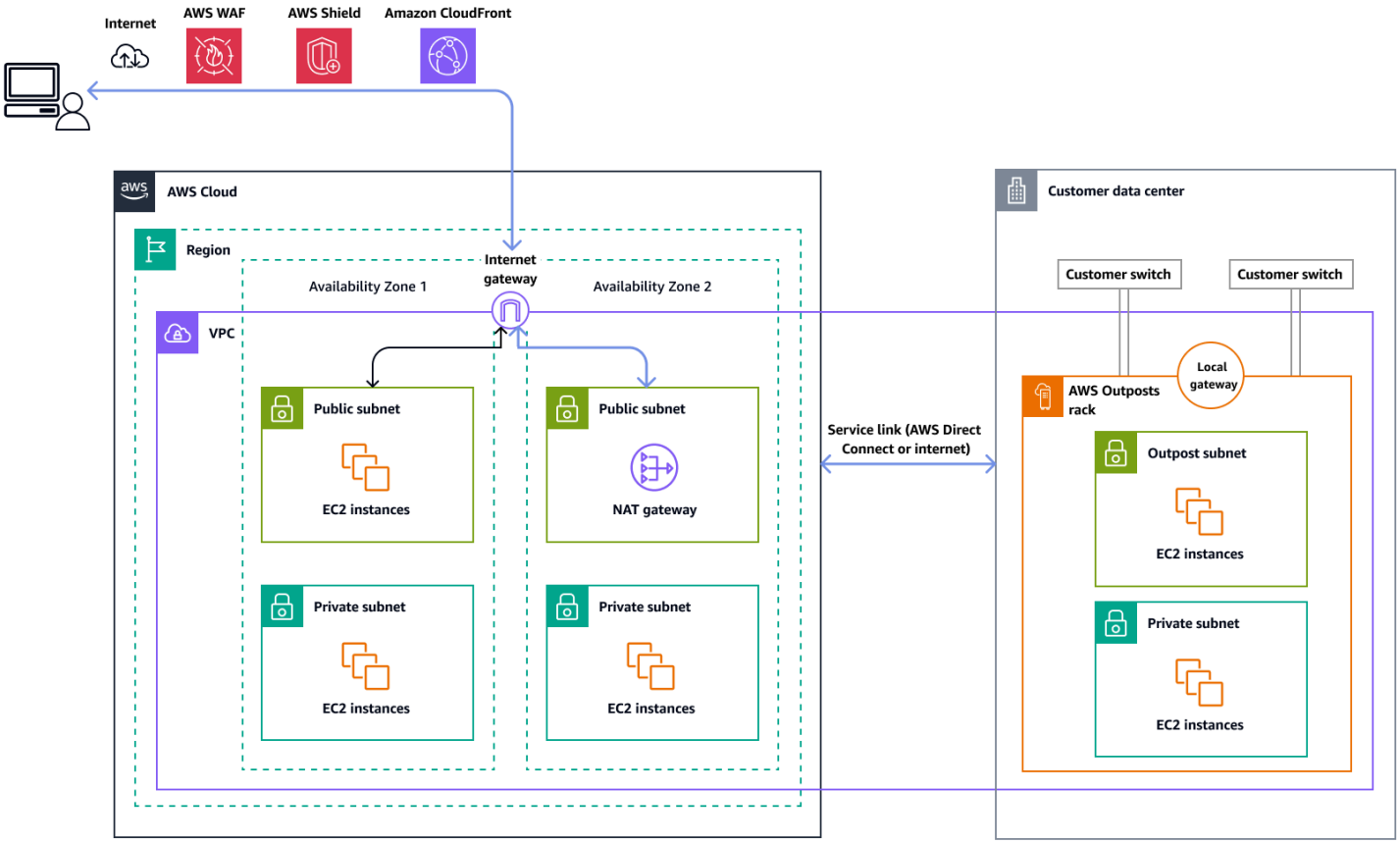
Local Zones 採用稱為網路邊界群組的網路建構，用於 AWS 區域。 會 AWS 公告來自這些唯一群組的公有 IP 地址。網路邊界群組包含可用區域、本機區域或 Wavelength 區域。您可以明確配置公有 IP 地址集區，以用於網路邊界群組。您可以使用網路邊界群組，允許從群組提供彈性 IP 地址，將網際網路閘道延伸到 Local Zones。此選項要求您部署其他元件，以補充 Local Zones 中提供的核心服務。這些元件可能來自 ISVs並協助您在 Local Zone 中建置檢查層，如 AWS 部落格文章所述。 AWS Local Zones

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。

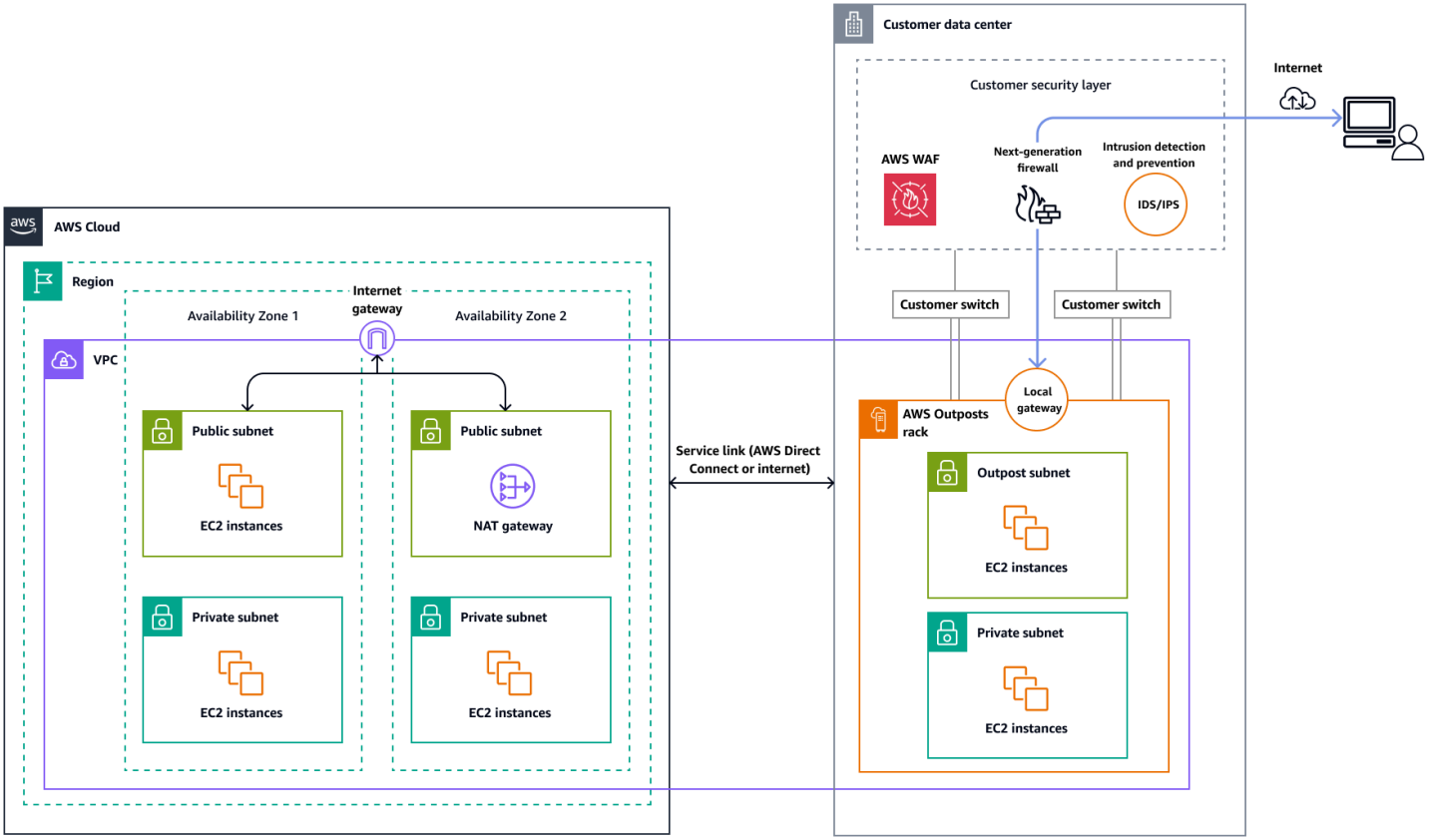
下圖顯示 AWS Outposts 執行個體中的工作負載與透過父系的網際網路之間的流量 AWS 區域。



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

無論您的工作負載是部署在 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，遵循規範的最佳實務。 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 防護機制等功能，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：

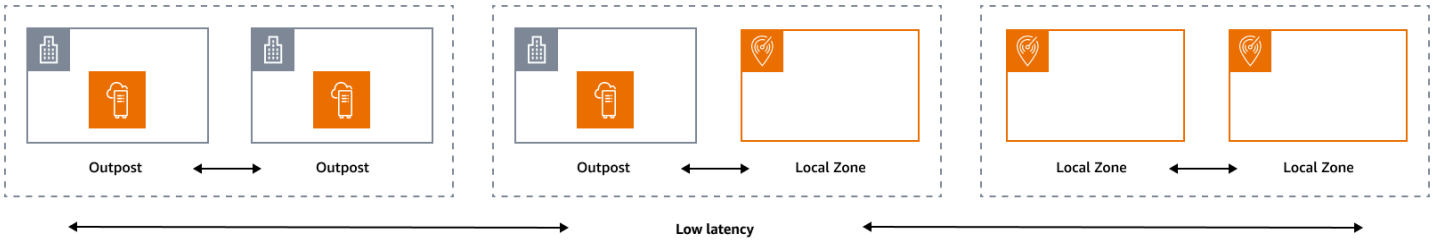
- 配置的專用主機
- 容量保留
- 客戶擁有的 IP (CoIP) 地址集區
- 本機閘道路由表
- Outpost
- Amazon S3 on Outposts
- 網站
- 子網路

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 中執行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。然後 Outpost 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。此選擇會將 Outposts 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：

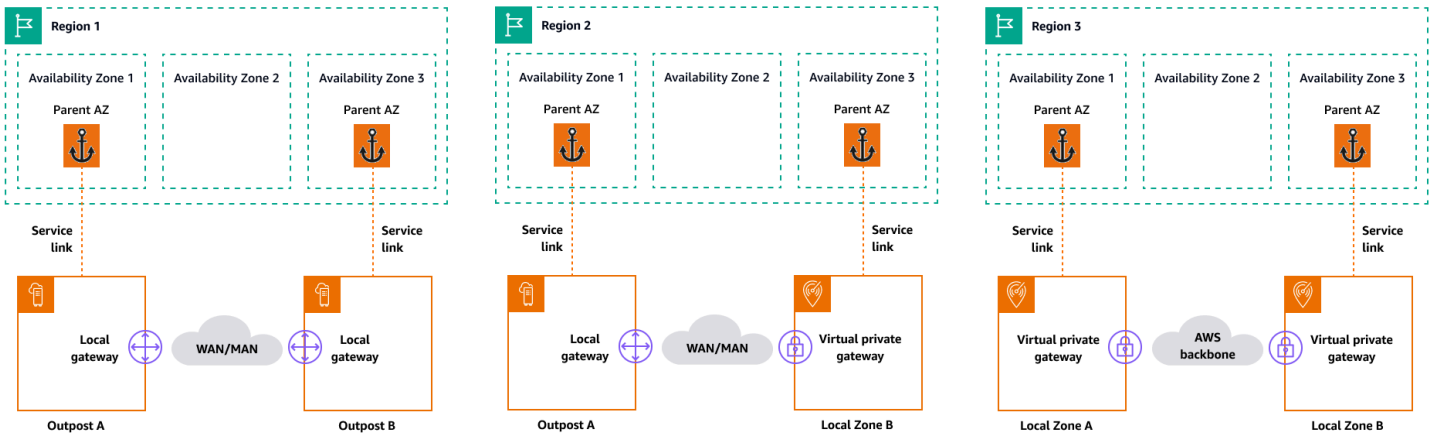
```
aws ec2 describe-availability-zones --zone-ids use1-mia1-az1
```

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) 會錨定在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。

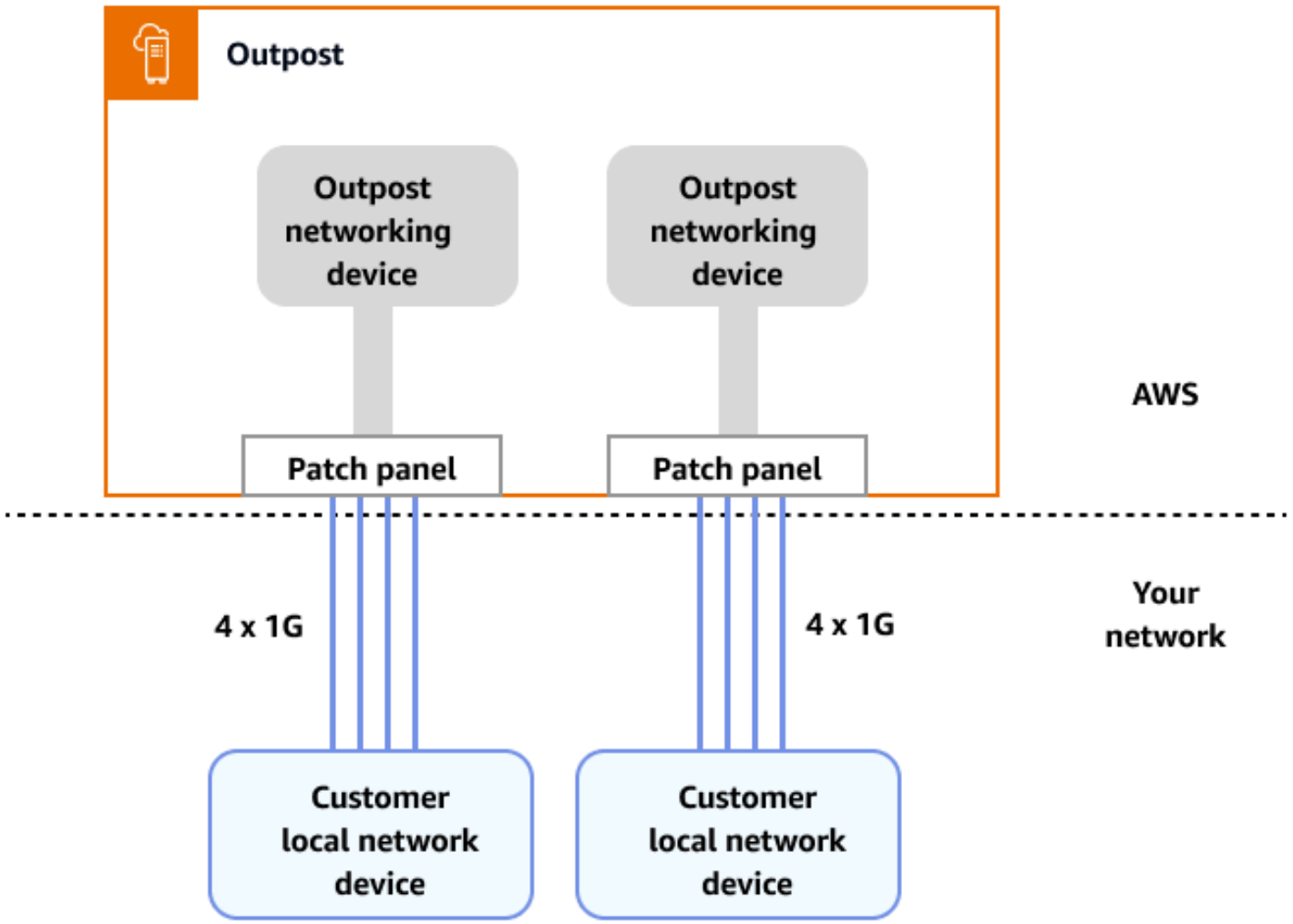
Local Zones 的彈性聯網

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 AWS 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 AWS Direct Connect，則適用的彈性架構與存取 的架構相同 AWS 區域，如AWS 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，只有一個 AWS Direct Connect PoP 就無法建立建議 AWS Direct Connect 用於恢復能力的架構。如果您只能存取單一 AWS 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 AWS Direct Connect，如 AWS 部落格文章所述和討論啟用從現場部署到 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，可從您的本機網路存取 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的 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。

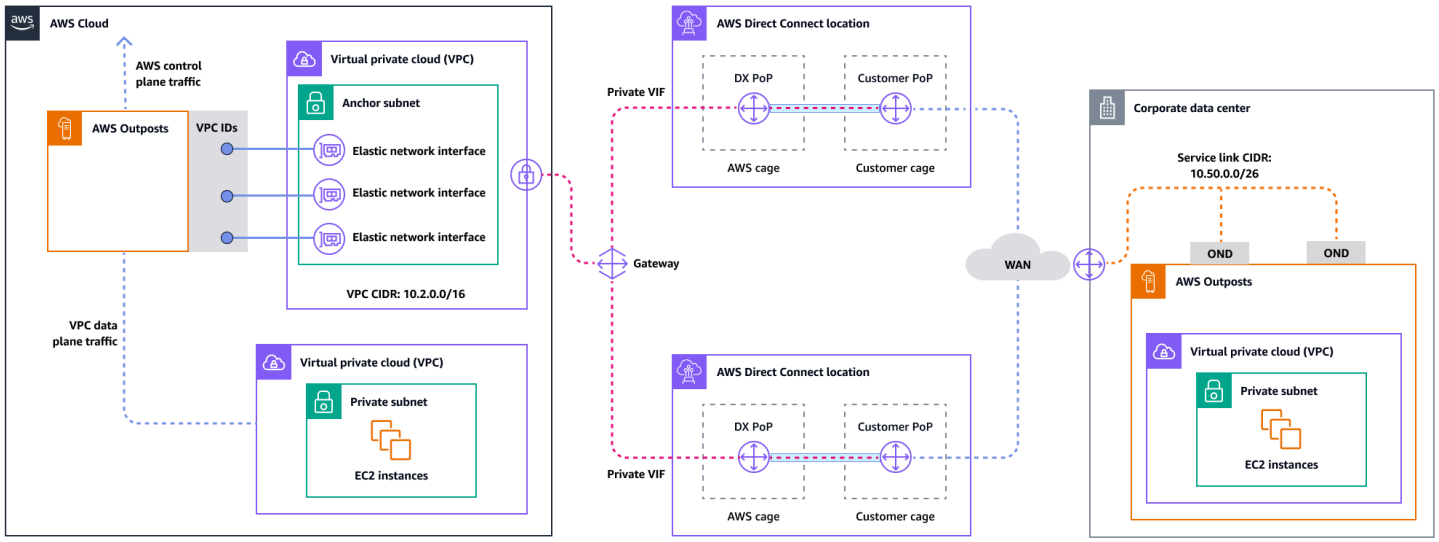
上行鏈路速度	上行鏈路數目
1 Gbps	1、2、4、6 或 8
10 Gbps	1、2、4、8、12 或 16
40 或 100 Gbps	1、2 或 4



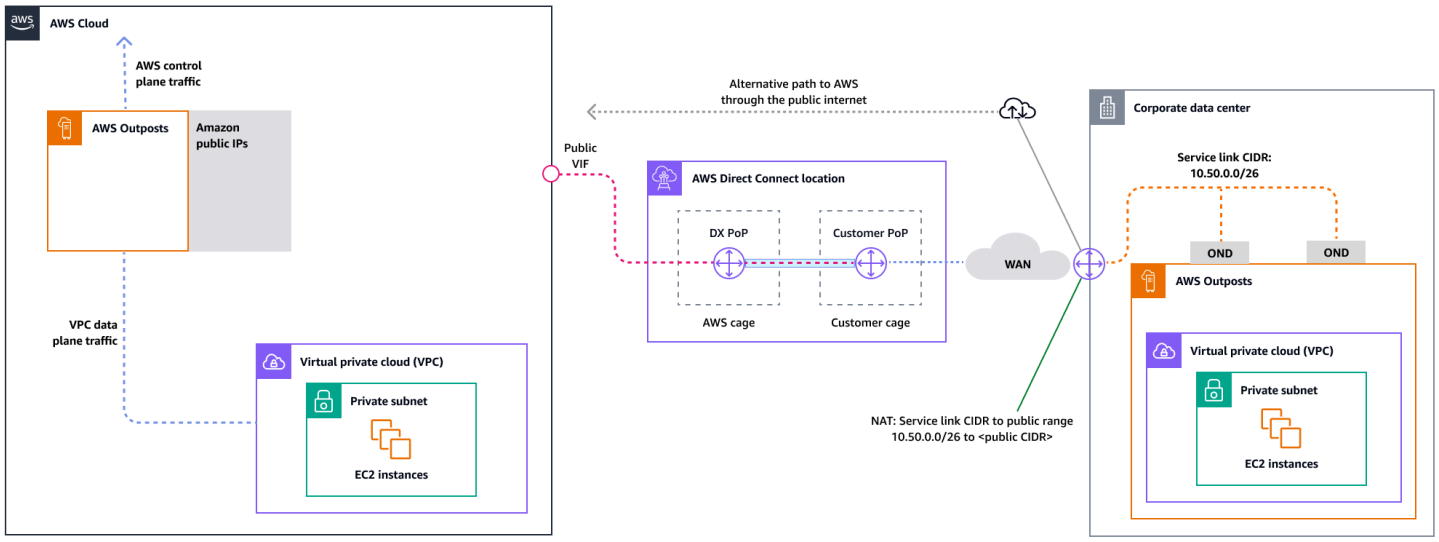
如需此連線的詳細資訊，請參閱 AWS Outposts 文件中的 Outposts 機架的本機網路連線。

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 AWS 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。



下圖說明此架構的高可用性公有連線。

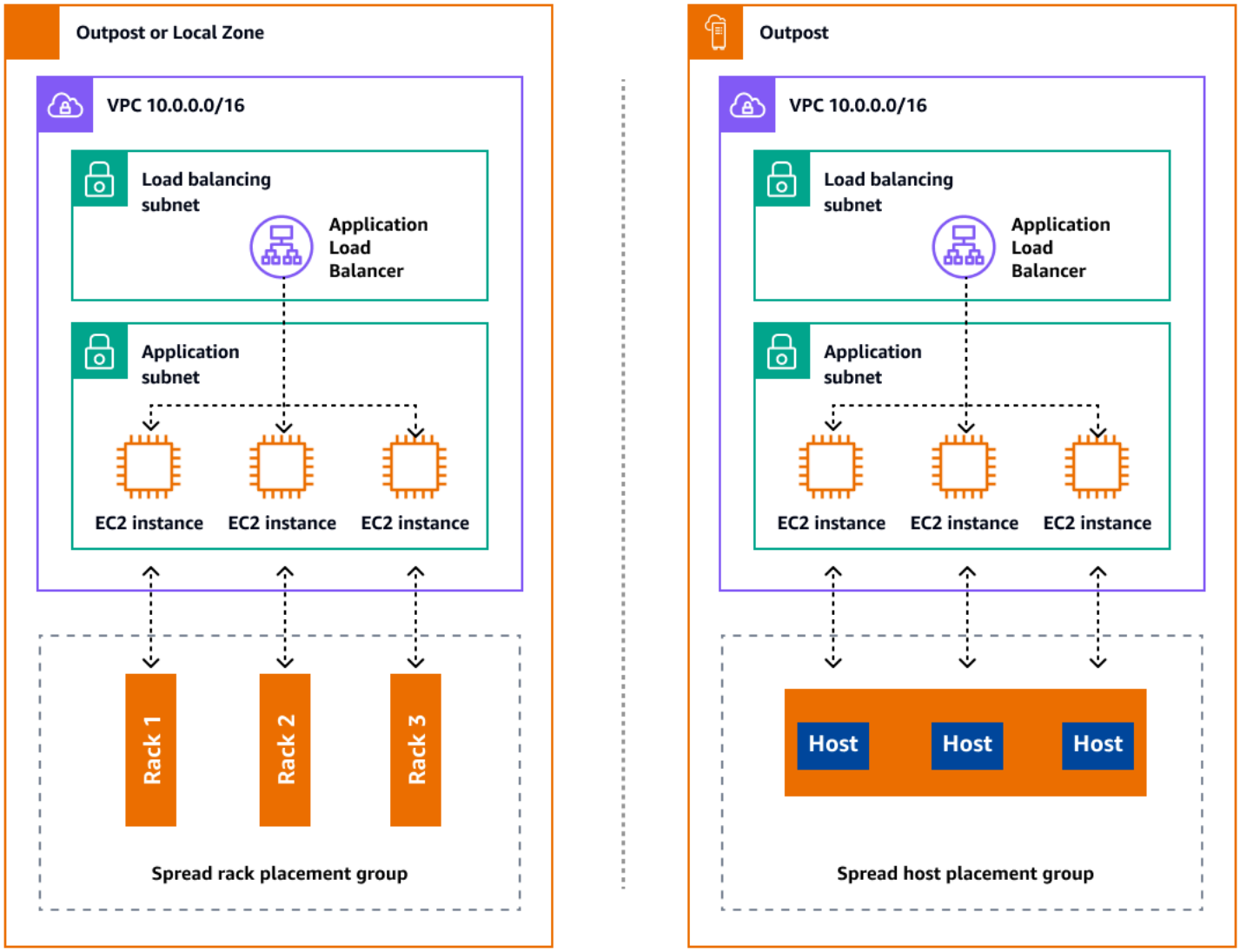


使用 ACE 機架擴展 Outposts 機架部署

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 的功率，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。

跨 Outpost 和本機區域分發執行個體

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

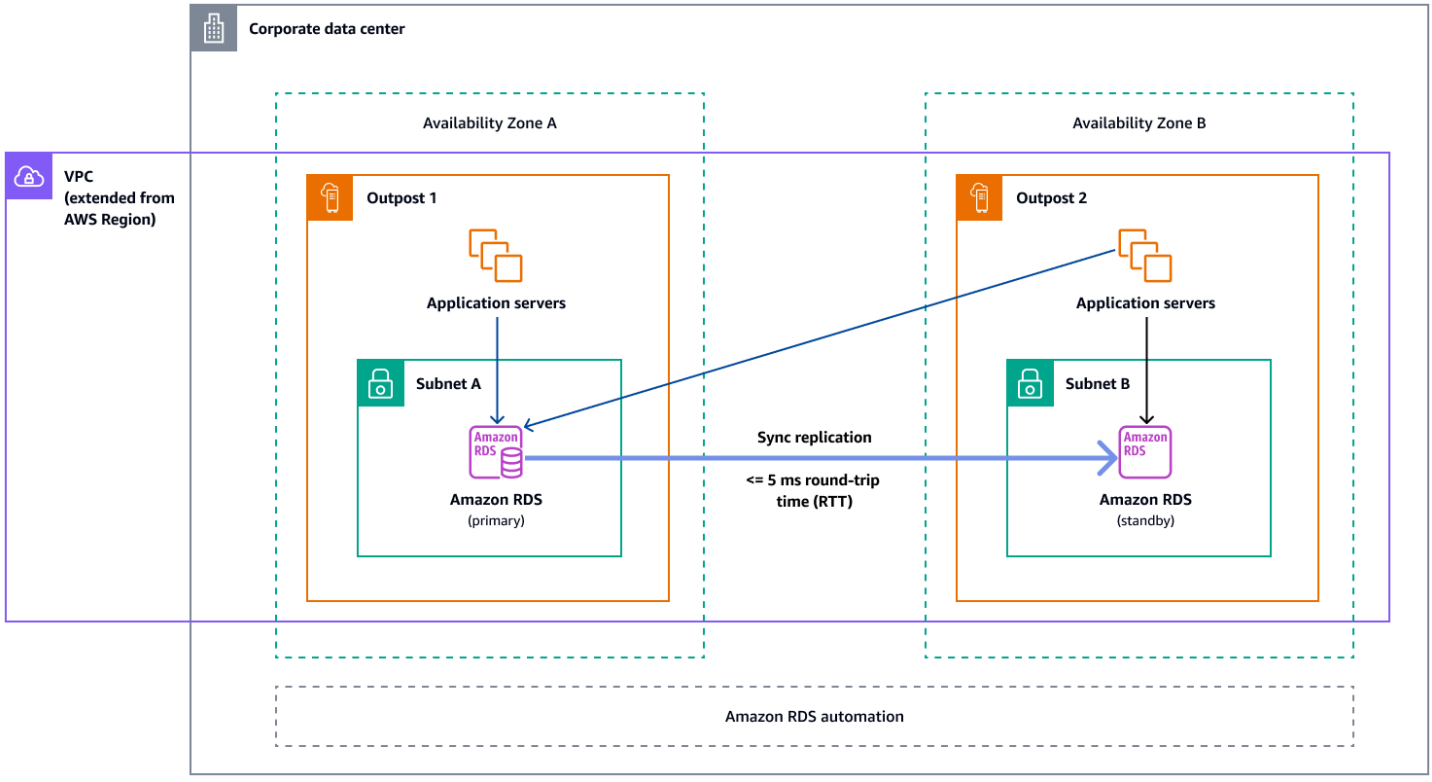
當您在 Outposts 上使用異地同步備份執行個體部署時，Amazon RDS 會跨兩個 Outposts 建立兩個資料庫執行個體。每個 Outpost 都會在自己的實體基礎設施上執行，並連線到區域中的不同可用區域，

以獲得高可用性。當兩個 Outpost 透過客戶管理的本機連線連線時，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 客戶擁有的 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。

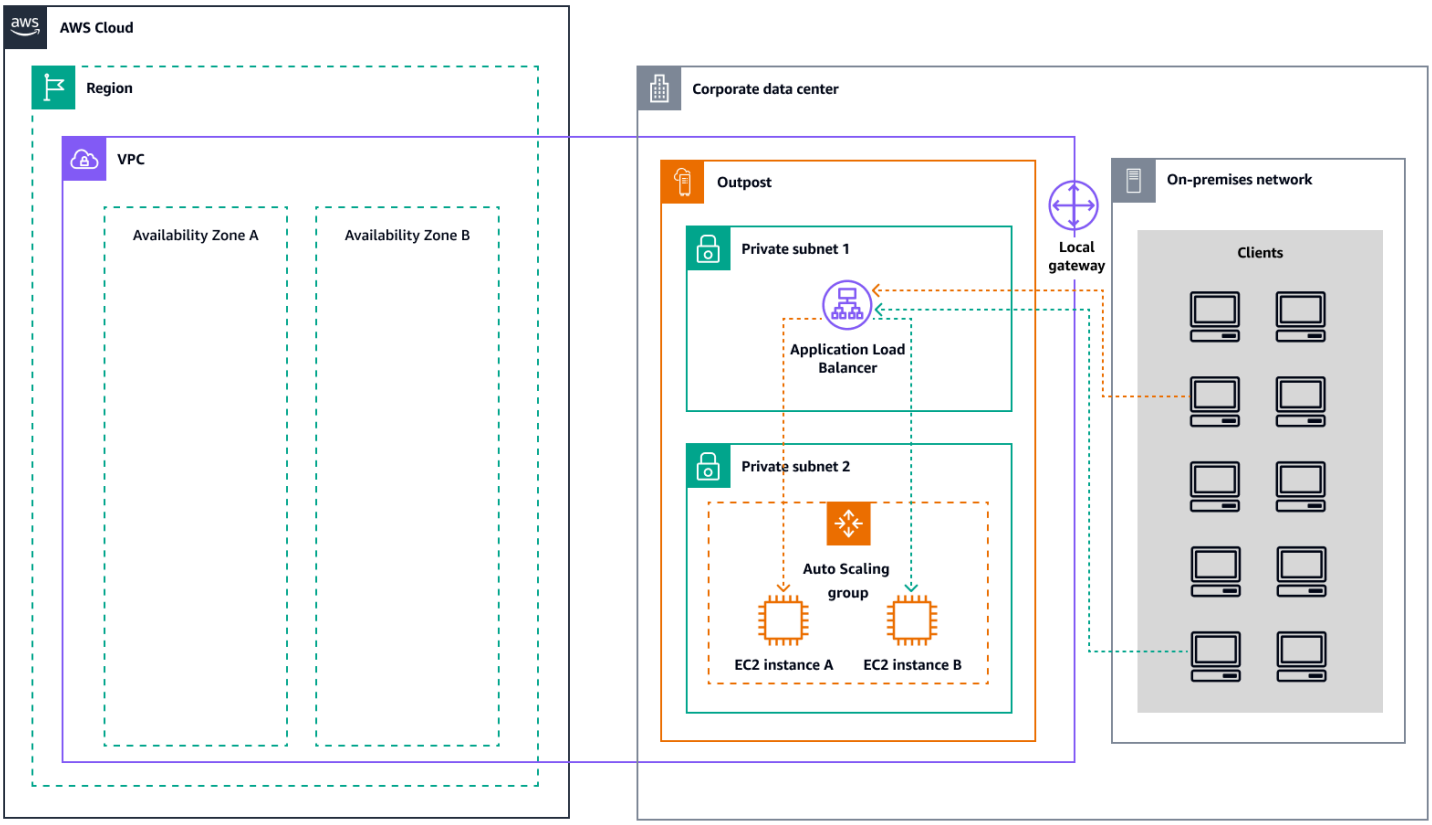


容錯移轉機制

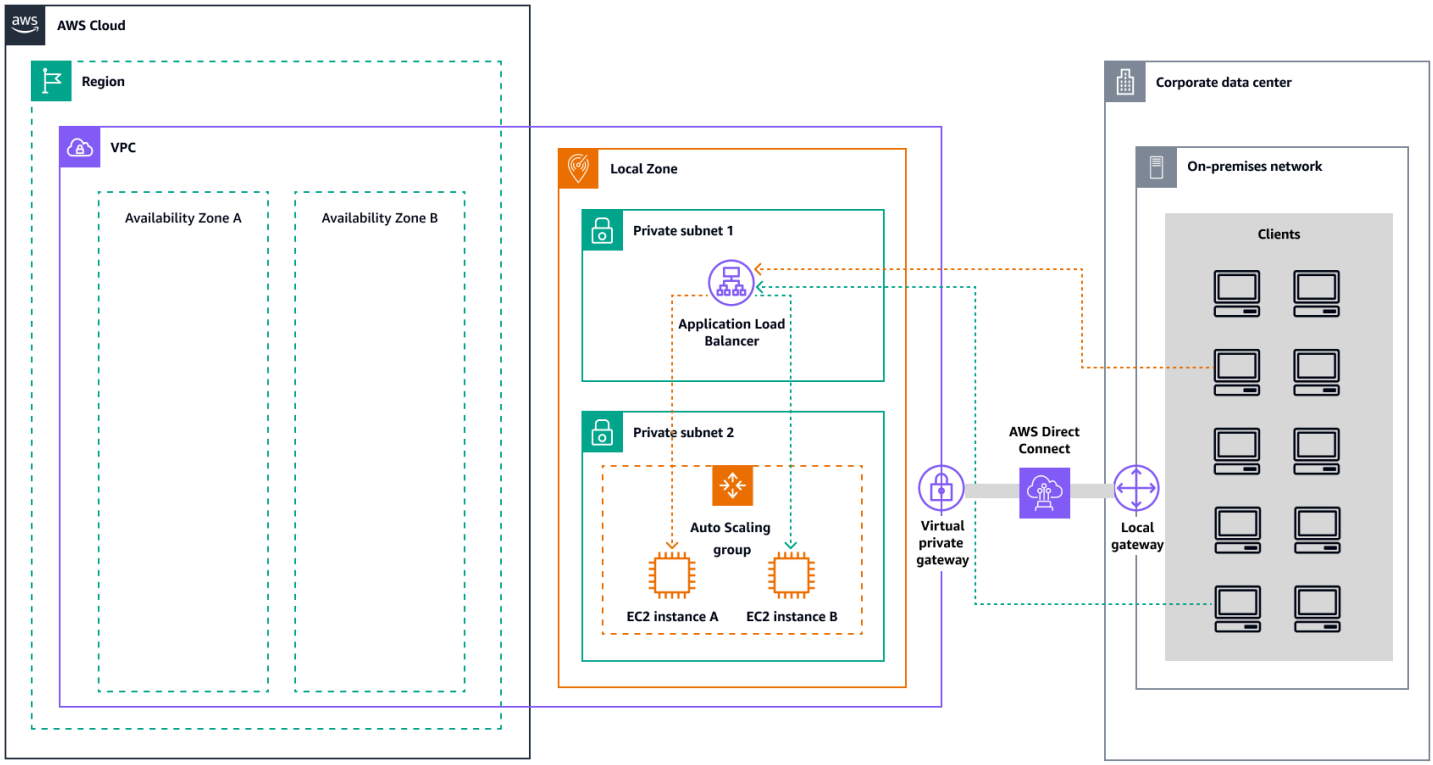
負載平衡和自動擴展

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的主機計數低於允許的主機計數時通知您。

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。

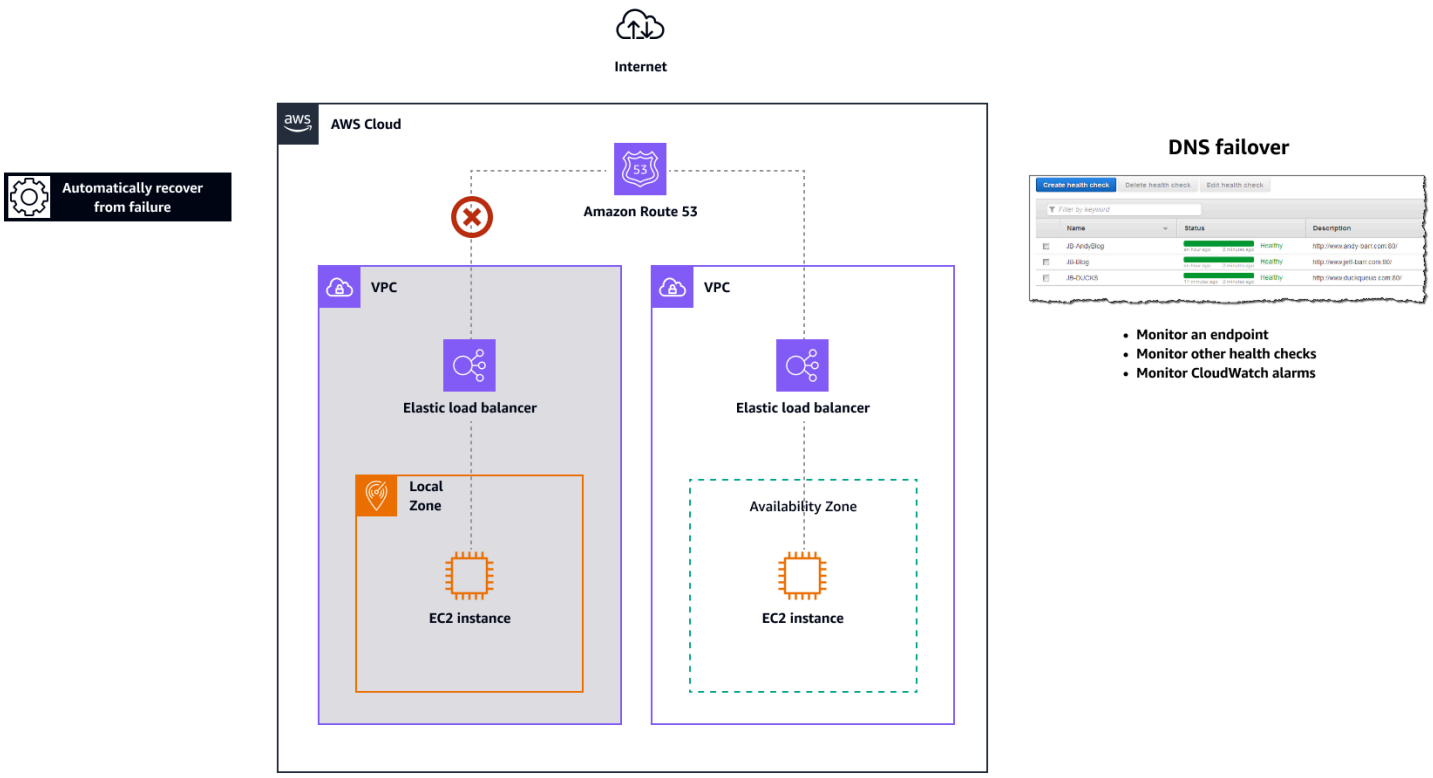


> **Note**
>
> Application Load Balancer 可在 AWS Outposts 和 Local Zones 中使用。不過，若要在 中使用 Application Load Balancer AWS Outposts，您需要調整 Amazon EC2 容量的大小，以提供負載平衡器所需的可擴展性。如需在 中調整負載平衡器大小的詳細資訊 AWS Outposts，請參閱 AWS 部落格文章在 上設定 Application Load Balancer AWS Outposts。

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。當您設定別名記錄來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 到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 Outposts 機架上提供 。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 Outpost 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降低 DNS 解析的延遲，因為查詢結果會從 Outposts 快取並在本機提供，這樣可消除對父系不必要的往返 AWS 區域。Outposts VPCs 中使用私有 DNS 的應用程式的所有 DNS 解析都會在本機提供。

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 傳入端點會將從 VPC 外部收到的 DNS 查詢轉送至在 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
Amazon S3	Amazon S3 on Outposts 入門	無

服務	AWS Outposts	AWS Local Zones
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 Elastic Disaster Recovery	使用 AWS Elastic Disaster Recovery 和 AWS Outposts	不適用
AWS Application Migration Service	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 AWS SDK for Python (Boto)
- 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

AWS 規範性指引詞彙表

以下是 AWS Prescriptive Guidance 提供的策略、指南和模式中常用的術語。若要建議項目，請使用詞彙表末尾的提供意見回饋連結。

數字

7 R

將應用程式移至雲端的七種常見遷移策略。這些策略以 Gartner 在 2011 年確定的 5 R 為基礎，包括以下內容：

- 重構/重新架構 – 充分利用雲端原生功能來移動應用程式並修改其架構，以提高敏捷性、效能和可擴展性。這通常涉及移植作業系統和資料庫。範例：將您的現場部署 Oracle 資料庫遷移至 Amazon Aurora PostgreSQL 相容版本。
- 平台轉換 (隨即重塑) – 將應用程式移至雲端，並引入一定程度的優化以利用雲端功能。範例：將內部部署 Oracle 資料庫遷移至 中的 Amazon Relational Database Service (Amazon RDS) for Oracle AWS 雲端。
- 重新購買 (捨棄再購買) – 切換至不同的產品，通常從傳統授權移至 SaaS 模型。範例：將您的客戶關係管理 (CRM) 系統遷移至 Salesforce.com。
- 主機轉換 (隨即轉移) – 將應用程式移至雲端，而不進行任何變更以利用雲端功能。範例：將您的現場部署 Oracle 資料庫遷移至 中 EC2 執行個體上的 Oracle AWS 雲端。
- 重新放置 (虛擬機器監視器等級隨即轉移) – 將基礎設施移至雲端，無需購買新硬體、重寫應用程式或修改現有操作。您可以將伺服器從內部部署平台遷移到相同平台的雲端服務。範例：將 Microsoft Hyper-V應用程式遷移至 AWS。
- 保留 (重新檢視) – 將應用程式保留在來源環境中。其中可能包括需要重要重構的應用程式，且您希望將該工作延遲到以後，以及您想要保留的舊版應用程式，因為沒有業務理由來進行遷移。
- 淘汰 – 解除委任或移除來源環境中不再需要的應用程式。

A

ABAC

請參閱屬性型存取控制。

抽象服務

請參閱 受管服務。

ACID

請參閱原子性、一致性、隔離性、耐久性。

主動-主動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步 (透過使用雙向複寫工具或雙重寫入操作)，且兩個資料庫都在遷移期間處理來自連接應用程式的交易。此方法支援小型、受控制批次的遷移，而不需要一次性切換。它更靈活，但比主動-被動遷移需要更多的工作。

主動-被動式遷移

一種資料庫遷移方法，其中來源和目標資料庫保持同步，但只有來源資料庫會在資料複寫至目標資料庫時處理來自連線應用程式的交易。目標資料庫在遷移期間不接受任何交易。

彙總函數

在一組資料列上運作的 SQL 函數，會計算群組的單一傳回值。彙總函數的範例包括 SUM和 MAX。

AI

請參閱人工智慧。

AIOps

請參閱人工智慧操作。

匿名化

永久刪除資料集中個人資訊的程序。匿名化有助於保護個人隱私權。匿名資料不再被視為個人資料。

反模式

經常用於經常性問題的解決方案，其中解決方案具有反生產力、無效，或比替代解決方案更有效。

應用程式控制

一種安全方法，僅允許使用核准的應用程式，以協助保護系統免受惡意軟體攻擊。

應用程式組合

有關組織使用的每個應用程式的詳細資訊的集合，包括建置和維護應用程式的成本及其商業價值。此資訊是產品組合探索和分析程序的關鍵，有助於識別要遷移、現代化和優化的應用程式並排定其優先順序。

人工智慧 (AI)

電腦科學領域，致力於使用運算技術來執行通常與人類相關的認知功能，例如學習、解決問題和識別模式。如需詳細資訊，請參閱什麼是人工智慧？

人工智慧操作 (AIOps)

使用機器學習技術解決操作問題、減少操作事件和人工干預以及提高服務品質的程序。如需有關如何在 AWS 遷移策略中使用 AIOps 的詳細資訊，請參閱操作整合指南。

非對稱加密

一種加密演算法，它使用一對金鑰：一個用於加密的公有金鑰和一個用於解密的私有金鑰。您可以共用公有金鑰，因為它不用於解密，但對私有金鑰存取應受到高度限制。

原子性、一致性、隔離性、耐久性 (ACID)

一組軟體屬性，即使在出現錯誤、電源故障或其他問題的情況下，也能確保資料庫的資料有效性和操作可靠性。

屬性型存取控制 (ABAC)

根據使用者屬性 (例如部門、工作職責和團隊名稱) 建立精細許可的實務。如需詳細資訊，請參閱《 AWS Identity and Access Management (IAM) 文件》中的 ABAC for AWS。

授權資料來源

存放主要版本資料的位置，被視為最可靠的資訊來源。您可以將授權資料來源中的資料複製到其他位置，以處理或修改資料，例如匿名、修訂或假名化資料。

可用區域

中的不同位置 AWS 區域 ，可隔離其他可用區域中的故障，並提供相同區域中其他可用區域的低成本、低延遲網路連線能力。

AWS 雲端採用架構 (AWS CAF)

的指導方針和最佳實務架構 AWS ，可協助組織制定高效且有效的計劃，以成功地移至雲端。 AWS CAF 將指導方針組織到六個重點領域：業務、人員、治理、平台、安全和營運。業務、人員和控管層面著重於業務技能和程序；平台、安全和操作層面著重於技術技能和程序。例如，人員層面針對處理人力資源 (HR)、人員配備功能和人員管理的利害關係人。因此， AWS CAF 為人員開發、訓練和通訊提供指引，協助組織做好成功採用雲端的準備。如需詳細資訊，請參閱 AWS CAF 網站和 AWS CAF 白皮書。

AWS 工作負載資格架構 (AWS WQF)

一種工具，可評估資料庫遷移工作負載、建議遷移策略，並提供工作預估值。 AWS WQF 隨附於 AWS Schema Conversion Tool (AWS SCT)。它會分析資料庫結構描述和程式碼物件、應用程式程式碼、相依性和效能特性，並提供評估報告。

B

錯誤的機器人

旨在中斷或傷害個人或組織的機器人。

BCP

請參閱業務持續性規劃。

行為圖

資源行為的統一互動式檢視，以及一段時間後的互動。您可以將行為圖與 Amazon Detective 搭配使用來檢查失敗的登入嘗試、可疑的 API 呼叫和類似動作。如需詳細資訊，請參閱偵測文件中的行為圖中的資料。

大端序系統

首先儲存最高有效位元組的系統。另請參閱 Endianness。

二進制分類

預測二進制結果的過程 (兩個可能的類別之一)。例如，ML 模型可能需要預測諸如「此電子郵件是否是垃圾郵件？」等問題 或「產品是書還是汽車？」

Bloom 篩選條件

一種機率性、記憶體高效的資料結構，用於測試元素是否為集的成員。

藍/綠部署

一種部署策略，您可以在其中建立兩個不同但相同的環境。您可以在一個環境 （藍色） 中執行目前的應用程式版本，並在另一個環境 （綠色） 中執行新的應用程式版本。此策略可協助您快速復原，並將影響降至最低。

機器人

透過網際網路執行自動化任務並模擬人類活動或互動的軟體應用程式。有些機器人有用或有益，例如在網際網路上編製資訊索引的 Web 爬蟲程式。某些其他機器人稱為惡意機器人，旨在中斷或傷害個人或組織。

殭屍網路

受到惡意軟體感染且由單一方控制的機器人網路，稱為機器人繼承器或機器人運算子。殭屍網路是擴展機器人及其影響的最佳已知機制。

分支

程式碼儲存庫包含的區域。儲存庫中建立的第一個分支是主要分支。您可以從現有分支建立新分支，然後在新分支中開發功能或修正錯誤。您建立用來建立功能的分支通常稱為功能分支。當準備好發佈功能時，可以將功能分支合併回主要分支。如需詳細資訊，請參閱關於分支 (GitHub 文件)。

碎片存取

在特殊情況下，以及透過核准的程序，讓使用者能夠快速存取他們通常無權存取 AWS 帳戶 的 。如需詳細資訊，請參閱 Well-Architected 指南中的 AWS 實作碎片程序指標。

棕地策略

環境中的現有基礎設施。對系統架構採用棕地策略時，可以根據目前系統和基礎設施的限制來設計架構。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

緩衝快取

儲存最常存取資料的記憶體區域。

業務能力

業務如何創造價值 (例如，銷售、客戶服務或營銷)。業務能力可驅動微服務架構和開發決策。如需詳細資訊，請參閱在 AWS上執行容器化微服務白皮書的圍繞業務能力進行組織部分。

業務連續性規劃 (BCP)

一種解決破壞性事件 (如大規模遷移) 對營運的潛在影響並使業務能夠快速恢復營運的計畫。

C

CAF

請參閱AWS 雲端採用架構。

Canary 部署

版本對最終使用者的緩慢和增量版本。當您有信心時，您可以部署新版本，並完全取代目前的版本。

CCoE

請參閱 Cloud Center of Excellence。

CDC

請參閱變更資料擷取。

變更資料擷取 (CDC)

追蹤對資料來源 (例如資料庫表格) 的變更並記錄有關變更的中繼資料的程序。您可以將 CDC 用於各種用途，例如稽核或複寫目標系統中的變更以保持同步。

混沌工程

故意引入故障或破壞性事件，以測試系統的彈性。您可以使用 AWS Fault Injection Service (AWS FIS) 執行實驗，為您的 AWS 工作負載帶來壓力，並評估其回應。

CI/CD

請參閱持續整合和持續交付。

分類

有助於產生預測的分類程序。用於分類問題的 ML 模型可預測離散值。離散值永遠彼此不同。例如，模型可能需要評估影像中是否有汽車。

用戶端加密

在目標 AWS 服務 接收資料之前，在本機加密資料。

雲端卓越中心 (CCoE)

一個多學科團隊，可推動整個組織的雲端採用工作，包括開發雲端最佳實務、調動資源、制定遷移時間表以及領導組織進行大規模轉型。如需詳細資訊，請參閱 AWS 雲端 企業策略部落格上的 CCoE 文章。

雲端運算

通常用於遠端資料儲存和 IoT 裝置管理的雲端技術。雲端運算通常連接到邊緣運算技術。

雲端操作模型

在 IT 組織中，用於建置、成熟和最佳化一或多個雲端環境的操作模型。如需詳細資訊，請參閱建置您的雲端操作模型。

採用雲端階段

組織在遷移至 時通常會經歷的四個階段 AWS 雲端：

- 專案 – 執行一些與雲端相關的專案以進行概念驗證和學習用途
- 基礎 – 進行基礎投資以擴展雲端採用 (例如，建立登陸區域、定義 CCoE、建立營運模型)
- 遷移 – 遷移個別應用程式
- 重塑 – 優化產品和服務，並在雲端中創新

這些階段由 Stephen Orban 在部落格文章 The Journey Toward Cloud-First 和 Enterprise Strategy 部落格上的採用階段中定義。 AWS 雲端 如需有關它們如何與 AWS 遷移策略關聯的資訊，請參閱遷移整備指南。

CMDB

請參閱組態管理資料庫。

程式碼儲存庫

透過版本控制程序來儲存及更新原始程式碼和其他資產 (例如文件、範例和指令碼) 的位置。常見的雲端儲存庫包括 GitHub或 Bitbucket Cloud。程式碼的每個版本都稱為分支。在微服務結構中，每個儲存庫都專用於單個功能。單一 CI/CD 管道可以使用多個儲存庫。

冷快取

一種緩衝快取，它是空的、未填充的，或者包含過時或不相關的資料。這會影響效能，因為資料庫執行個體必須從主記憶體或磁碟讀取，這比從緩衝快取讀取更慢。

冷資料

很少存取且通常是歷史資料的資料。查詢這類資料時，通常可接受慢查詢。將此資料移至效能較低且成本較低的儲存層或類別，可以降低成本。

電腦視覺 (CV)

使用機器學習從數位影像和影片等視覺化格式分析和擷取資訊的 AI 欄位。例如，Amazon SageMaker AI 提供 CV 的影像處理演算法。

組態偏離

對於工作負載，組態會從預期狀態變更。這可能會導致工作負載不合規，而且通常是漸進和無意的。

組態管理資料庫 (CMDB)

儲存和管理有關資料庫及其 IT 環境的資訊的儲存庫，同時包括硬體和軟體元件及其組態。您通常在遷移的產品組合探索和分析階段使用 CMDB 中的資料。

一致性套件

您可以組合的 AWS Config 規則和修補動作集合，以自訂您的合規和安全檢查。您可以使用 YAML 範本，將一致性套件部署為 AWS 帳戶 和 區域中或整個組織的單一實體。如需詳細資訊，請參閱 AWS Config 文件中的一致性套件。

持續整合和持續交付 (CI/CD)

自動化軟體發行程序的來源、建置、測試、暫存和生產階段的程序。CI/CD 通常被描述為管道。CI/CD 可協助您將程序自動化、提升生產力、改善程式碼品質以及加快交付速度。如需詳細資訊，請參閱持續交付的優點。CD 也可表示持續部署。如需詳細資訊，請參閱持續交付與持續部署。

CV

請參閱電腦視覺。

D

靜態資料

網路中靜止的資料，例如儲存中的資料。

資料分類

根據重要性和敏感性來識別和分類網路資料的程序。它是所有網路安全風險管理策略的關鍵組成部分，因為它可以協助您確定適當的資料保護和保留控制。資料分類是 AWS Well-Architected Framework 中安全支柱的元件。如需詳細資訊，請參閱資料分類。

資料偏離

生產資料與用於訓練 ML 模型的資料之間有意義的變化，或輸入資料隨時間有意義的變更。資料偏離可以降低 ML 模型預測的整體品質、準確性和公平性。

傳輸中的資料

在您的網路中主動移動的資料，例如在網路資源之間移動。

資料網格

架構架構，提供分散式、分散式資料擁有權與集中式管理。

資料最小化

僅收集和處理嚴格必要資料的原則。在 中實作資料最小化 AWS 雲端 可以降低隱私權風險、成本和分析碳足跡。

資料周邊

AWS 環境中的一組預防性護欄，可協助確保只有信任的身分才能從預期的網路存取信任的資源。如需詳細資訊，請參閱在 上建置資料周邊 AWS。

資料預先處理

將原始資料轉換成 ML 模型可輕鬆剖析的格式。預處理資料可能意味著移除某些欄或列，並解決遺失、不一致或重複的值。

資料來源

在整個生命週期中追蹤資料的原始伺服器和歷史記錄的程序，例如資料的產生、傳輸和儲存方式。

資料主體

正在收集和處理資料的個人。

資料倉儲

支援商業智慧的資料管理系統，例如 分析。資料倉儲通常包含大量歷史資料，通常用於查詢和分析。

資料庫定義語言 (DDL)

用於建立或修改資料庫中資料表和物件之結構的陳述式或命令。

資料庫處理語言 (DML)

用於修改 (插入、更新和刪除) 資料庫中資訊的陳述式或命令。

DDL

請參閱資料庫定義語言。

深度整體

結合多個深度學習模型進行預測。可以使用深度整體來獲得更準確的預測或估計預測中的不確定性。

深度學習

一個機器學習子領域，它使用多層人工神經網路來識別感興趣的輸入資料與目標變數之間的對應關係。

深度防禦

這是一種資訊安全方法，其中一系列的安全機制和控制項會在整個電腦網路中精心分層，以保護網路和其中資料的機密性、完整性和可用性。當您在 上採用此策略時 AWS，您可以在 AWS

Organizations 結構的不同層新增多個控制項，以協助保護資源。例如，defense-in-depth方法可能會結合多重要素驗證、網路分割和加密。

委派的管理員

在 中 AWS Organizations，相容的服務可以註冊 AWS 成員帳戶來管理組織的帳戶，並管理該服務的許可。此帳戶稱為該服務的委派管理員。如需詳細資訊和相容服務清單，請參閱 AWS Organizations 文件中的可搭配 AWS Organizations運作的服務。

部署

在目標環境中提供應用程式、新功能或程式碼修正的程序。部署涉及在程式碼庫中實作變更，然後在應用程式環境中建置和執行該程式碼庫。

開發環境

請參閱 環境。

偵測性控制

一種安全控制，用於在事件發生後偵測、記錄和提醒。這些控制是第二道防線，提醒您注意繞過現有預防性控制的安全事件。如需詳細資訊，請參閱在 AWS上實作安全控制中的偵測性控制。

開發值串流映射 (DVSM)

一種程序，用於識別並優先考慮對軟體開發生命週期中的速度和品質造成負面影響的限制。DVSM 擴展了最初專為精簡製造實務設計的價值串流映射程序。它著重於透過軟體開發程序建立和移動價值所需的步驟和團隊。

數位分身

真實世界系統的虛擬呈現，例如建築物、工廠、工業設備或生產線。數位分身支援預測性維護、遠端監控和生產最佳化。

維度資料表

在星星結構描述中，較小的資料表包含有關事實資料表中量化資料的資料屬性。維度資料表屬性通常是文字欄位或離散數字，其行為類似於文字。這些屬性通常用於查詢限制、篩選和結果集標記。

災難

防止工作負載或系統在其主要部署位置中實現其業務目標的事件。這些事件可能是自然災難、技術故障或人為動作的結果，例如意外設定錯誤或惡意軟體攻擊。

災難復原 (DR)

您用來將災難造成的停機時間和資料遺失降至最低的策略和程序。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的 上工作負載的災難復原 AWS：雲端中的復原。

DML

請參閱資料庫處理語言。

領域驅動的設計

一種開發複雜軟體系統的方法，它會將其元件與每個元件所服務的不斷發展的領域或核心業務目標相關聯。Eric Evans 在其著作 Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003) 中介紹了這一概念。如需有關如何將領域驅動的設計與 strangler fig 模式搭配使用的資訊，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

DR

請參閱災難復原。

偏離偵測

追蹤與基準組態的偏差。例如，您可以使用 AWS CloudFormation 來偵測系統資源中的偏離，也可以使用 AWS Control Tower 來偵測登陸區域中可能影響控管要求合規性的變更。 https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-drift.html

DVSM

請參閱開發值串流映射。

E

EDA

請參閱探索性資料分析。

EDI

請參閱電子資料交換。

邊緣運算

提升 IoT 網路邊緣智慧型裝置運算能力的技術。與雲端運算相比，邊緣運算可以減少通訊延遲並改善回應時間。

電子資料交換 (EDI)

在組織之間自動交換商業文件。如需詳細資訊，請參閱什麼是電子資料交換。

加密

一種運算程序，可將人類可讀取的純文字資料轉換為加密文字。

加密金鑰

由加密演算法產生的隨機位元的加密字串。金鑰長度可能有所不同，每個金鑰的設計都是不可預測且唯一的。

端序

位元組在電腦記憶體中的儲存順序。大端序系統首先儲存最高有效位元組。小端序系統首先儲存最低有效位元組。

端點

請參閱 服務端點。

端點服務

您可以在虛擬私有雲端 (VPC) 中託管以與其他使用者共用的服務。您可以使用 建立端點服務，AWS PrivateLink 並將許可授予其他 AWS 帳戶 或 AWS Identity and Access Management (IAM) 委託人。這些帳戶或主體可以透過建立介面 VPC 端點私下連接至您的端點服務。如需詳細資訊，請參閱 Amazon Virtual Private Cloud (Amazon VPC) 文件中的建立端點服務。

企業資源規劃 (ERP)

一種系統，可自動化和管理企業的關鍵業務流程 （例如會計、MES 和專案管理）。

信封加密

使用另一個加密金鑰對某個加密金鑰進行加密的程序。如需詳細資訊，請參閱 AWS Key Management Service (AWS KMS) 文件中的信封加密。

環境

執行中應用程式的執行個體。以下是雲端運算中常見的環境類型：

- 開發環境 – 執行中應用程式的執行個體，只有負責維護應用程式的核心團隊才能使用。開發環境用來測試變更，然後再將開發環境提升到較高的環境。此類型的環境有時稱為測試環境。
- 較低的環境 – 應用程式的所有開發環境，例如用於初始建置和測試的開發環境。
- 生產環境 – 最終使用者可以存取的執行中應用程式的執行個體。在 CI/CD 管道中，生產環境是最後一個部署環境。
- 較高的環境 – 核心開發團隊以外的使用者可存取的所有環境。這可能包括生產環境、生產前環境以及用於使用者接受度測試的環境。

epic

在敏捷方法中，有助於組織工作並排定工作優先順序的功能類別。epic 提供要求和實作任務的高層級描述。例如， AWS CAF 安全概念包括身分和存取管理、偵測控制、基礎設施安全、資料保護和事件回應。如需有關 AWS 遷移策略中的 Epic 的詳細資訊，請參閱計畫實作指南。

ERP

請參閱企業資源規劃。

探索性資料分析 (EDA)

分析資料集以了解其主要特性的過程。您收集或彙總資料，然後執行初步調查以尋找模式、偵測異常並檢查假設。透過計算摘要統計並建立資料可視化來執行 EDA。

F

事實資料表

星狀結構描述中的中央資料表。它存放有關業務操作的量化資料。一般而言，事實資料表包含兩種類型的資料欄：包含度量的資料，以及包含維度資料表外部索引鍵的資料欄。

快速失敗

一種使用頻繁和增量測試來縮短開發生命週期的理念。這是敏捷方法的關鍵部分。

故障隔離界限

在 中 AWS 雲端，像是可用區域 AWS 區域、控制平面或資料平面等邊界會限制故障的影響，並有助於改善工作負載的彈性。如需詳細資訊，請參閱AWS 故障隔離界限。

功能分支

請參閱分支。

特徵

用來進行預測的輸入資料。例如，在製造環境中，特徵可能是定期從製造生產線擷取的影像。

功能重要性

特徵對於模型的預測有多重要。這通常表示為可以透過各種技術來計算的數值得分，例如 Shapley Additive Explanations (SHAP) 和積分梯度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

特徵轉換

優化 ML 程序的資料，包括使用其他來源豐富資料、調整值、或從單一資料欄位擷取多組資訊。這可讓 ML 模型從資料中受益。例如，如果將「2021-05-27 00:15:37」日期劃分為「2021」、「五月」、「週四」和「15」，則可以協助學習演算法學習與不同資料元件相關聯的細微模式。

少量擷取提示

在要求 LLM 執行類似的任務之前，提供少量示範任務和所需輸出的範例給 LLM。此技術是內容內學習的應用程式，其中模型會從內嵌在提示中的範例 (快照) 中學習。對於需要特定格式、推理或網域知識的任務，少量的提示非常有效。另請參閱零鏡頭提示。

FGAC

請參閱精細存取控制。

精細存取控制 (FGAC)

使用多個條件來允許或拒絕存取請求。

閃切遷移

一種資料庫遷移方法，透過變更資料擷取使用連續資料複寫，以盡可能在最短的時間內遷移資料，而不是使用分階段方法。目標是將停機時間降至最低。

FM

請參閱基礎模型。

基礎模型 (FM)

大型深度學習神經網路，已針對廣義和未標記資料的大量資料集進行訓練。FMs 能夠執行各種一般任務，例如了解語言、產生文字和影像，以及以自然語言交談。如需詳細資訊，請參閱什麼是基礎模型。

G

生成式 AI

已針對大量資料進行訓練的 AI 模型子集，可使用簡單的文字提示建立新的內容和成品，例如影像、影片、文字和音訊。如需詳細資訊，請參閱什麼是生成式 AI。

地理封鎖

請參閱地理限制。

地理限制 (地理封鎖)

Amazon CloudFront 中的選項，可防止特定國家/地區的使用者存取內容分發。您可以使用允許清單或封鎖清單來指定核准和禁止的國家/地區。如需詳細資訊，請參閱 CloudFront 文件中的限制內容的地理分佈。

Gitflow 工作流程

這是一種方法，其中較低和較高環境在原始碼儲存庫中使用不同分支。Gitflow 工作流程被視為舊版，而以幹線為基礎的工作流程是現代、偏好的方法。

黃金影像

系統或軟體的快照，做為部署該系統或軟體新執行個體的範本。例如，在製造中，黃金映像可用於在多個裝置上佈建軟體，並有助於提高裝置製造操作的速度、可擴展性和生產力。

綠地策略

新環境中缺乏現有基礎設施。對系統架構採用綠地策略時，可以選擇所有新技術，而不會限制與現有基礎設施的相容性，也稱為棕地。如果正在擴展現有基礎設施，則可能會混合棕地和綠地策略。

防護機制

有助於跨組織單位 (OU) 來管控資源、政策和合規的高層級規則。預防性防護機制會強制執行政策，以確保符合合規標準。透過使用服務控制政策和 IAM 許可界限來將其實作。偵測性防護機制可偵測政策違規和合規問題，並產生提醒以便修正。它們是透過使用 AWS Config AWS Security Hub、Amazon GuardDuty、、Amazon Inspector AWS Trusted Advisor和自訂 AWS Lambda 檢查來實作。

H

HA

請參閱高可用性。

異質資料庫遷移

將來源資料庫遷移至使用不同資料庫引擎的目標資料庫 (例如，Oracle 至 Amazon Aurora)。異質遷移通常是重新架構工作的一部分，而轉換結構描述可能是一項複雜任務。AWS 提供有助於結構描述轉換的 AWS SCT。

高可用性 (HA)

在遇到挑戰或災難時，工作負載能夠在不介入的情況下持續運作。HA 系統的設計目的是自動容錯移轉、持續提供高品質的效能，以及處理不同的負載和故障，並將效能影響降至最低。

歷史現代化

一種方法，用於現代化和升級操作技術 (OT) 系統，以更好地滿足製造業的需求。歷史資料是一種資料庫，用於從工廠中的各種來源收集和存放資料。

保留資料

從用於訓練機器學習模型的資料集中保留的部分歷史標記資料。您可以使用保留資料，透過比較模型預測與保留資料來評估模型效能。

異質資料庫遷移

將您的來源資料庫遷移至共用相同資料庫引擎的目標資料庫 (例如，Microsoft SQL Server 至 Amazon RDS for SQL Server)。同質遷移通常是主機轉換或平台轉換工作的一部分。您可以使用原生資料庫公用程式來遷移結構描述。

熱資料

經常存取的資料，例如即時資料或最近的轉譯資料。此資料通常需要高效能儲存層或類別，才能提供快速的查詢回應。

修補程序

緊急修正生產環境中的關鍵問題。由於其緊迫性，通常會在典型 DevOps 發行工作流程之外執行修補程式。

超級護理期間

在切換後，遷移團隊在雲端管理和監控遷移的應用程式以解決任何問題的時段。通常，此期間的長度為 1-4 天。在超級護理期間結束時，遷移團隊通常會將應用程式的責任轉移給雲端營運團隊。

I

IaC

將基礎設施視為程式碼。

身分型政策

連接至一或多個 IAM 主體的政策，可定義其在 AWS 雲端 環境中的許可。

閒置應用程式

90 天期間 CPU 和記憶體平均使用率在 5% 至 20% 之間的應用程式。在遷移專案中，通常會淘汰這些應用程式或將其保留在內部部署。

IIoT

請參閱工業物聯網。

不可變的基礎設施

為生產工作負載部署新基礎設施的模型，而不是更新、修補或修改現有的基礎設施。不可變基礎設施本質上比可變基礎設施更一致、可靠且可預測。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的使用不可變基礎設施的部署最佳實務。

傳入 (輸入) VPC

在 AWS 多帳戶架構中，接受、檢查和路由來自應用程式外部之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

增量遷移

一種切換策略，您可以在其中將應用程式分成小部分遷移，而不是執行單一、完整的切換。例如，您最初可能只將一些微服務或使用者移至新系統。確認所有項目都正常運作之後，您可以逐步移動其他微服務或使用者，直到可以解除委任舊式系統。此策略可降低與大型遷移關聯的風險。

工業 4.0

2016 年 Klaus Schwab 推出的術語，透過連線能力、即時資料、自動化、分析和 AI/ML 的進展，指製造程序的現代化。

基礎設施

應用程式環境中包含的所有資源和資產。

基礎設施即程式碼 (IaC)

透過一組組態檔案來佈建和管理應用程式基礎設施的程序。IaC 旨在協助您集中管理基礎設施，標準化資源並快速擴展，以便新環境可重複、可靠且一致。

工業物聯網 (IIoT)

在製造業、能源、汽車、醫療保健、生命科學和農業等產業領域使用網際網路連線的感測器和裝置。如需詳細資訊，請參閱建立工業物聯網 (IIoT) 數位轉型策略。

檢查 VPC

在 AWS 多帳戶架構中，集中式 VPC，可管理 VPCs 之間 （在相同或不同的 中 AWS 區域)、網際網路和內部部署網路之間的網路流量檢查。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

物聯網 (IoT)

具有內嵌式感測器或處理器的相連實體物體網路，其透過網際網路或本地通訊網路與其他裝置和系統進行通訊。如需詳細資訊，請參閱什麼是 IoT？

可解釋性

機器學習模型的一個特徵，描述了人類能夠理解模型的預測如何依賴於其輸入的程度。如需詳細資訊，請參閱 的機器學習模型可解譯性 AWS。

IoT

請參閱物聯網。

IT 資訊庫 (ITIL)

一組用於交付 IT 服務並使這些服務與業務需求保持一致的最佳實務。ITIL 為 ITSM 提供了基礎。

IT 服務管理 (ITSM)

與組織的設計、實作、管理和支援 IT 服務關聯的活動。如需有關將雲端操作與 ITSM 工具整合的資訊，請參閱操作整合指南。

ITIL

請參閱 IT 資訊庫。

ITSM

請參閱 IT 服務管理。

L

標籤型存取控制 (LBAC)

強制存取控制 (MAC) 的實作，其中使用者和資料本身都會獲得明確指派的安全標籤值。使用者安全標籤和資料安全標籤之間的交集會決定使用者可以看到哪些資料列和資料欄。

登陸區域

登陸區域是架構良好的多帳戶 AWS 環境，可擴展且安全。這是一個起點，您的組織可以從此起點快速啟動和部署工作負載與應用程式，並對其安全和基礎設施環境充滿信心。如需有關登陸區域的詳細資訊，請參閱設定安全且可擴展的多帳戶 AWS 環境。

大型語言模型 (LLM)

預先訓練大量資料的深度學習 AI 模型。LLM 可以執行多個任務，例如回答問題、摘要文件、將文字翻譯成其他語言，以及完成句子。如需詳細資訊，請參閱什麼是 LLMs。

大型遷移

遷移 300 部或更多伺服器。

LBAC

請參閱標籤型存取控制。

最低權限

授予執行任務所需之最低許可的安全最佳實務。如需詳細資訊，請參閱 IAM 文件中的套用最低權限許可。

隨即轉移

請參閱 7 個 R。

小端序系統

首先儲存最低有效位元組的系統。另請參閱 Endianness。

LLM

請參閱大型語言模型。

較低的環境

請參閱 環境。

M

機器學習 (ML)

一種使用演算法和技術進行模式識別和學習的人工智慧。機器學習會進行分析並從記錄的資料 (例如物聯網 (IoT) 資料) 中學習，以根據模式產生統計模型。如需詳細資訊，請參閱機器學習。

主要分支

請參閱分支。

惡意軟體

旨在危及電腦安全或隱私權的軟體。惡意軟體可能會中斷電腦系統、洩露敏感資訊，或取得未經授權的存取。惡意軟體的範例包括病毒、蠕蟲、勒索軟體、特洛伊木馬程式、間諜軟體和鍵盤記錄器。

受管服務

AWS 服務 會 AWS 操作基礎設施層、作業系統和平台，而您會存取端點來存放和擷取資料。Amazon Simple Storage Service (Amazon S3) 和 Amazon DynamoDB 是受管服務的範例。這些也稱為抽象服務。

製造執行系統 (MES)

一種軟體系統，用於追蹤、監控、記錄和控制生產程序，將原物料轉換為現場成品。

MAP

請參閱遷移加速計劃。

機制

建立工具、推動工具採用，然後檢查結果以進行調整的完整程序。機制是在操作時強化和改善自身的循環。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的建置機制。

成員帳戶

除了屬於組織一部分的管理帳戶 AWS 帳戶 之外的所有 AWS Organizations。一個帳戶一次只能是一個組織的成員。

製造執行系統

請參閱製造執行系統。

訊息佇列遙測傳輸 (MQTT)

根據發佈/訂閱模式的輕量型machine-to-machine(M2M) 通訊協定，適用於資源受限的 IoT 裝置。

微服務

一種小型的獨立服務，它可透過定義明確的 API 進行通訊，通常由小型獨立團隊擁有。例如，保險系統可能包含對應至業務能力 (例如銷售或行銷) 或子領域 (例如購買、索賠或分析) 的微服務。微服務的優點包括靈活性、彈性擴展、輕鬆部署、可重複使用的程式碼和適應力。如需詳細資訊，請參閱使用無 AWS 伺服器服務整合微服務。

微服務架構

一種使用獨立元件來建置應用程式的方法，這些元件會以微服務形式執行每個應用程式程序。這些微服務會使用輕量型 API，透過明確定義的介面進行通訊。此架構中的每個微服務都可以進行更新、部署和擴展，以滿足應用程式特定功能的需求。如需詳細資訊，請參閱在 上實作微服務 AWS。

Migration Acceleration Program (MAP)

此 AWS 計畫提供諮詢支援、訓練和服務，以協助組織建立強大的營運基礎，以移至雲端，並協助抵銷遷移的初始成本。MAP 包括用於有條不紊地執行舊式遷移的遷移方法以及一組用於自動化和加速常見遷移案例的工具。

大規模遷移

將大部分應用程式組合依波次移至雲端的程序，在每個波次中，都會以更快的速度移動更多應用程式。此階段使用從早期階段學到的最佳實務和經驗教訓來實作團隊、工具和流程的遷移工廠，以透過自動化和敏捷交付簡化工作負載的遷移。這是 AWS 遷移策略的第三階段。

遷移工廠

可透過自動化、敏捷的方法簡化工作負載遷移的跨職能團隊。遷移工廠團隊通常包括營運、業務分析師和擁有者、遷移工程師、開發人員以及從事 Sprint 工作的 DevOps 專業人員。20% 至 50% 之間的企業應用程式組合包含可透過工廠方法優化的重複模式。如需詳細資訊，請參閱此內容集中的遷移工廠的討論和雲端遷移工廠指南。

遷移中繼資料

有關完成遷移所需的應用程式和伺服器的資訊。每種遷移模式都需要一組不同的遷移中繼資料。遷移中繼資料的範例包括目標子網路、安全群組和 AWS 帳戶。

遷移模式

可重複的遷移任務，詳細描述遷移策略、遷移目的地以及所使用的遷移應用程式或服務。範例：使用 AWS Application Migration Service 重新託管遷移至 Amazon EC2。

遷移組合評定 (MPA)

線上工具，提供驗證商業案例以遷移至 的資訊 AWS 雲端。MPA 提供詳細的組合評定 (伺服器適當規模、定價、總體擁有成本比較、遷移成本分析) 以及遷移規劃 (應用程式資料分析和資料收集、應用程式分組、遷移優先順序，以及波次規劃)。MPA 工具 （需要登入） 可供所有 AWS 顧問和 APN 合作夥伴顧問免費使用。

遷移準備程度評定 (MRA)

使用 AWS CAF 取得組織雲端整備狀態的洞見、識別優缺點，以及建立行動計劃以消除已識別差距的程序。如需詳細資訊，請參閱遷移準備程度指南。MRA 是 AWS 遷移策略的第一階段。

遷移策略

用來將工作負載遷移至 的方法 AWS 雲端。如需詳細資訊，請參閱本詞彙表中的 7 個 Rs 項目，並請參閱動員您的組織以加速大規模遷移。

機器學習 (ML)

請參閱機器學習。

現代化

將過時的 (舊版或單一) 應用程式及其基礎架構轉換為雲端中靈活、富有彈性且高度可用的系統，以降低成本、提高效率並充分利用創新。如需詳細資訊，請參閱《》中的現代化應用程式的策略 AWS 雲端。

現代化準備程度評定

這項評估可協助判斷組織應用程式的現代化準備程度；識別優點、風險和相依性；並確定組織能夠在多大程度上支援這些應用程式的未來狀態。評定的結果就是目標架構的藍圖、詳細說明現代化程序的開發階段和里程碑的路線圖、以及解決已發現的差距之行動計畫。如需詳細資訊，請參閱《》中的評估應用程式的現代化準備 AWS 雲端程度。

單一應用程式 (單一)

透過緊密結合的程序作為單一服務執行的應用程式。單一應用程式有幾個缺點。如果一個應用程式功能遇到需求激增，則必須擴展整個架構。當程式碼庫增長時，新增或改進單一應用程式的功能也會變得更加複雜。若要解決這些問題，可以使用微服務架構。如需詳細資訊，請參閱將單一體系分解為微服務。

MPA

請參閱遷移產品組合評估。

MQTT

請參閱訊息佇列遙測傳輸。

多類別分類

一個有助於產生多類別預測的過程 (預測兩個以上的結果之一)。例如，機器學習模型可能會詢問「此產品是書籍、汽車還是電話？」 或者「這個客戶對哪種產品類別最感興趣？」

可變基礎設施

更新和修改生產工作負載現有基礎設施的模型。為了提高一致性、可靠性和可預測性， AWS Well-Architected Framework 建議使用不可變的基礎設施作為最佳實務。

O

OAC

請參閱原始存取控制。

OAI

請參閱原始存取身分。

OCM

請參閱組織變更管理。

離線遷移

一種遷移方法，可在遷移過程中刪除來源工作負載。此方法涉及延長停機時間，通常用於小型非關鍵工作負載。

OI

請參閱 操作整合。

OLA

請參閱操作層級協議。

線上遷移

一種遷移方法，無需離線即可將來源工作負載複製到目標系統。連接至工作負載的應用程式可在遷移期間繼續運作。此方法涉及零至最短停機時間，通常用於關鍵的生產工作負載。

OPC-UA

請參閱開啟程序通訊 - 統一架構。

開放程序通訊 - 統一架構 (OPC-UA)

用於工業自動化的machine-to-machine(M2M) 通訊協定。OPC-UA 提供資料加密、身分驗證和授權機制的互通性標準。

操作水準協議 (OLA)

一份協議，闡明 IT 職能群組承諾向彼此提供的內容，以支援服務水準協議 (SLA)。

操作整備審查 (ORR)

問題和相關最佳實務的檢查清單，可協助您了解、評估、預防或減少事件和可能失敗的範圍。如需詳細資訊，請參閱 AWS Well-Architected Framework 中的操作準備審查 (ORR)。

操作技術 (OT)

使用實體環境控制工業操作、設備和基礎設施的硬體和軟體系統。在製造業中，整合 OT 和資訊技術 (IT) 系統是工業 4.0 轉型的關鍵重點。

操作整合 (OI)

在雲端中將操作現代化的程序，其中包括準備程度規劃、自動化和整合。如需詳細資訊，請參閱操作整合指南。

組織追蹤

由 建立的線索 AWS CloudTrail 會記錄 AWS 帳戶 組織中所有 的所有事件 AWS Organizations。在屬於組織的每個 AWS 帳戶 中建立此追蹤，它會跟蹤每個帳戶中的活動。如需詳細資訊，請參閱 CloudTrail 文件中的建立組織追蹤。

組織變更管理 (OCM)

用於從人員、文化和領導力層面管理重大、顛覆性業務轉型的架構。OCM 透過加速變更採用、解決過渡問題，以及推動文化和組織變更，協助組織為新系統和策略做好準備，並轉移至新系統和策略。在 AWS 遷移策略中，此架構稱為人員加速，因為雲端採用專案所需的變更速度。如需詳細資訊，請參閱 OCM 指南。

原始存取控制 (OAC)

CloudFront 中的增強型選項，用於限制存取以保護 Amazon Simple Storage Service (Amazon S3) 內容。OAC 支援所有 S3 儲存貯體中的所有伺服器端加密 AWS KMS (SSE-KMS) AWS 區域，以及對 S3 儲存貯體的動態PUT和DELETE請求。

原始存取身分 (OAI)

CloudFront 中的一個選項，用於限制存取以保護 Amazon S3 內容。當您使用 OAI 時，CloudFront 會建立一個可供 Amazon S3 進行驗證的主體。經驗證的主體只能透過特定 CloudFront 分發來存取 S3 儲存貯體中的內容。另請參閱 OAC，它可提供更精細且增強的存取控制。

ORR

請參閱操作整備審核。

OT

請參閱操作技術。

傳出 (輸出) VPC

在 AWS 多帳戶架構中，處理從 應用程式內啟動之網路連線的 VPC。AWS 安全參考架構建議您使用傳入、傳出和檢查 VPC 來設定網路帳戶，以保護應用程式與更廣泛的網際網路之間的雙向介面。

P

許可界限

附接至 IAM 主體的 IAM 管理政策，可設定使用者或角色擁有的最大許可。如需詳細資訊，請參閱 IAM 文件中的許可界限。

個人身分識別資訊 (PII)

當直接檢視或與其他相關資料配對時，可用來合理推斷個人身分的資訊。PII 的範例包括名稱、地址和聯絡資訊。

PII

請參閱個人身分識別資訊。

手冊

一組預先定義的步驟，可擷取與遷移關聯的工作，例如在雲端中提供核心操作功能。手冊可以採用指令碼、自動化執行手冊或操作現代化環境所需的程序或步驟摘要的形式。

PLC

請參閱可程式設計邏輯控制器。

PLM

請參閱產品生命週期管理。

政策

可定義許可的物件（請參閱身分型政策）、指定存取條件（請參閱資源型政策），或定義組織中所有帳戶的最大許可 AWS Organizations（請參閱服務控制政策）。

混合持久性

根據資料存取模式和其他需求，獨立選擇微服務的資料儲存技術。如果您的微服務具有相同的資料儲存技術，則其可能會遇到實作挑戰或效能不佳。如果微服務使用最適合其需求的資料儲存，則可以更輕鬆地實作並達到更好的效能和可擴展性。如需詳細資訊，請參閱在微服務中啟用資料持久性。

組合評定

探索、分析應用程式組合並排定其優先順序以規劃遷移的程序。如需詳細資訊，請參閱評估遷移準備程度。

述詞

傳回 `true`或 的查詢條件`false`，通常位於 `WHERE`子句中。

述詞下推

一種資料庫查詢最佳化技術，可在傳輸前篩選查詢中的資料。這可減少必須從關聯式資料庫擷取和處理的資料量，並改善查詢效能。

預防性控制

旨在防止事件發生的安全控制。這些控制是第一道防線，可協助防止對網路的未經授權存取或不必要變更。如需詳細資訊，請參閱在 AWS上實作安全控制中的預防性控制。

委託人

中可執行動作和存取資源 AWS 的實體。此實體通常是 AWS 帳戶、IAM 角色或使用者的根使用者。如需詳細資訊，請參閱 IAM 文件中角色術語和概念中的主體。

設計隱私權

透過整個開發程序將隱私權納入考量的系統工程方法。

私有託管區域

一種容器，它包含有關您希望 Amazon Route 53 如何回應一個或多個 VPC 內的域及其子域之 DNS 查詢的資訊。如需詳細資訊，請參閱 Route 53 文件中的使用私有託管區域。

主動控制

旨在防止部署不合規資源的安全控制。這些控制項會在佈建資源之前對其進行掃描。如果資源不符合控制項，則不會佈建。如需詳細資訊，請參閱 AWS Control Tower 文件中的控制項參考指南，並參閱實作安全控制項中的主動控制項。 AWS

產品生命週期管理 (PLM)

產品整個生命週期的資料和程序管理，從設計、開發和啟動，到成長和成熟，再到拒絕和移除。

生產環境

請參閱 環境。

可程式設計邏輯控制器 (PLC)

在製造中，高度可靠、可調整的電腦，可監控機器並自動化製造程序。

提示鏈結

使用一個 LLM 提示的輸出作為下一個提示的輸入，以產生更好的回應。此技術用於將複雜任務分解為子任務，或反覆精簡或展開初步回應。它有助於提高模型回應的準確性和相關性，並允許更精細、個人化的結果。

擬匿名化

將資料集中的個人識別符取代為預留位置值的程序。假名化有助於保護個人隱私權。假名化資料仍被視為個人資料。

發佈/訂閱 (pub/sub)

一種模式，可啟用微服務之間的非同步通訊，以改善可擴展性和回應能力。例如，在微服務型 MES 中，微服務可以將事件訊息發佈到其他微服務可訂閱的頻道。系統可以新增新的微服務，而無需變更發佈服務。

Q

查詢計劃

一系列步驟，如指示，用於存取 SQL 關聯式資料庫系統中的資料。

查詢計劃迴歸

在資料庫服務優化工具選擇的計畫比對資料庫環境進行指定的變更之前的計畫不太理想時。這可能因為對統計資料、限制條件、環境設定、查詢參數繫結的變更以及資料庫引擎的更新所導致。

R

RACI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RAG

請參閱擷取增強生成。

勒索軟體

一種惡意軟體，旨在阻止對計算機系統或資料的存取，直到付款為止。

RASCI 矩陣

請參閱負責、負責、諮詢、告知 (RACI)。

RCAC

請參閱資料列和資料欄存取控制。

僅供讀取複本

用於唯讀用途的資料庫複本。您可以將查詢路由至僅供讀取複本以減少主資料庫的負載。

重新架構師

請參閱 7 個 R。

復原點目標 (RPO)

自上次資料復原點以來可接受的時間上限。這會決定最後一個復原點與服務中斷之間可接受的資料遺失。

復原時間目標 (RTO)

服務中斷與服務還原之間的可接受延遲上限。

重構

請參閱 7 個 R。

Region

地理區域中的 AWS 資源集合。每個 AWS 區域 都獨立於其他 ，以提供容錯能力、穩定性和彈性。如需詳細資訊，請參閱指定 AWS 區域 您的帳戶可以使用哪些。

迴歸

預測數值的 ML 技術。例如，為了解決「這房子會賣什麼價格？」的問題 ML 模型可以使用線性迴歸模型，根據已知的房屋事實 (例如，平方英尺) 來預測房屋的銷售價格。

重新託管

請參閱 7 個 R。

版本

在部署程序中，它是將變更提升至生產環境的動作。

重新放置

請參閱 7 個 R。

Replatform

請參閱 7 個 R。

回購

請參閱 7 個 R。

彈性

應用程式抵禦中斷或從中斷中復原的能力。在 中規劃彈性時，高可用性和災難復原是常見的考量 AWS 雲端。如需詳細資訊，請參閱AWS 雲端 彈性。

資源型政策

附接至資源的政策，例如 Amazon S3 儲存貯體、端點或加密金鑰。這種類型的政策會指定允許存取哪些主體、支援的動作以及必須滿足的任何其他條件。

負責者、當責者、事先諮詢者和事後告知者 (RACI) 矩陣

矩陣，定義所有參與遷移活動和雲端操作之各方的角色和責任。矩陣名稱衍生自矩陣中定義的責任類型：負責人 (R)、責任 (A)、諮詢 (C) 和知情 (I)。支援 (S) 類型為選用。如果您包含支援，則矩陣稱為 RASCI 矩陣，如果您排除它，則稱為 RACI 矩陣。

回應性控制

一種安全控制，旨在驅動不良事件或偏離安全基準的補救措施。如需詳細資訊，請參閱在 AWS上實作安全控制中的回應性控制。

保留

請參閱 7 個 R。

淘汰

請參閱 7 個 R。

檢索增強生成 (RAG)

一種生成式 AI 技術，其中 LLM 會在產生回應之前參考訓練資料來源以外的授權資料來源。例如，RAG 模型可能會對組織的知識庫或自訂資料執行語意搜尋。如需詳細資訊，請參閱什麼是 RAG。

輪換

定期更新秘密的程序，讓攻擊者更難存取登入資料。

資料列和資料欄存取控制 (RCAC)

使用已定義存取規則的基本、彈性 SQL 表達式。RCAC 包含資料列許可和資料欄遮罩。

RPO

請參閱復原點目標。

RTO

請參閱復原時間目標。

執行手冊

執行特定任務所需的一組手動或自動程序。這些通常是為了簡化重複性操作或錯誤率較高的程序而建置。

S

SAML 2.0

許多身分提供者 (IdP) 使用的開放標準。此功能會啟用聯合單一登入 (SSO)，讓使用者可以登入 AWS Management Console 或呼叫 AWS API 操作，而不必為您組織中的每個人在 IAM 中建立使用者。如需有關以 SAML 2.0 為基礎的聯合詳細資訊，請參閱 IAM 文件中的關於以 SAML 2.0 為基礎的聯合。

SCADA

請參閱監督控制和資料擷取。

SCP

請參閱服務控制政策。

秘密

您以加密形式存放的 AWS Secrets Manager機密或限制資訊，例如密碼或使用者登入資料。它由秘密值及其中繼資料組成。秘密值可以是二進位、單一字串或多個字串。如需詳細資訊，請參閱 Secrets Manager 文件中的 Secrets Manager 秘密中的什麼內容？。

依設計的安全性

透過整個開發程序將安全性納入考量的系統工程方法。

安全控制

一種技術或管理防護機制，它可預防、偵測或降低威脅行為者利用安全漏洞的能力。安全控制有四種主要類型：預防性、偵測性、回應性和主動性。

安全強化

減少受攻擊面以使其更能抵抗攻擊的過程。這可能包括一些動作，例如移除不再需要的資源、實作授予最低權限的安全最佳實務、或停用組態檔案中不必要的功能。

安全資訊與事件管理 (SIEM) 系統

結合安全資訊管理 (SIM) 和安全事件管理 (SEM) 系統的工具與服務。SIEM 系統會收集、監控和分析來自伺服器、網路、裝置和其他來源的資料，以偵測威脅和安全漏洞，並產生提醒。

安全回應自動化

預先定義和程式設計的動作，旨在自動回應或修復安全事件。這些自動化可做為偵測或回應式安全控制，協助您實作 AWS 安全最佳實務。自動化回應動作的範例包括修改 VPC 安全群組、修補 Amazon EC2 執行個體或輪換登入資料。

伺服器端加密

由接收資料的 AWS 服務 在其目的地加密資料。

服務控制政策 (SCP)

為 AWS Organizations中的組織的所有帳戶提供集中控制許可的政策。SCP 會定義防護機制或設定管理員可委派給使用者或角色的動作限制。您可以使用 SCP 作為允許清單或拒絕清單，以指定允許或禁止哪些服務或動作。如需詳細資訊，請參閱 AWS Organizations 文件中的服務控制政策。

服務端點

的進入點 URL AWS 服務。您可以使用端點，透過程式設計方式連接至目標服務。如需詳細資訊，請參閱 AWS 一般參考 中的 AWS 服務 端點。

服務水準協議 (SLA)

一份協議，闡明 IT 團隊承諾向客戶提供的服務，例如服務正常執行時間和效能。

服務層級指標 (SLI)

服務效能方面的測量，例如其錯誤率、可用性或輸送量。

服務層級目標 (SLO)

代表服務運作狀態的目標指標，由服務層級指標測量。

共同責任模式

描述您與 共同 AWS 承擔雲端安全與合規責任的模型。 AWS 負責雲端的安全，而 負責雲端的安全。如需詳細資訊，請參閱共同責任模式。

SIEM

請參閱安全資訊和事件管理系統。

單一故障點 (SPOF)

應用程式的單一關鍵元件故障，可能會中斷系統。

SLA

請參閱服務層級協議。

SLI

請參閱服務層級指標。

SLO

請參閱服務層級目標。

先拆分後播種模型

擴展和加速現代化專案的模式。定義新功能和產品版本時，核心團隊會進行拆分以建立新的產品團隊。這有助於擴展組織的能力和服務，提高開發人員生產力，並支援快速創新。如需詳細資訊，請參閱 中的階段式應用程式現代化方法 AWS 雲端。

SPOF

請參閱單一故障點。

星狀結構描述

使用一個大型事實資料表來存放交易或測量資料的資料庫組織結構，並使用一或多個較小的維度資料表來存放資料屬性。此結構旨在用於資料倉儲或商業智慧用途。

Strangler Fig 模式

一種現代化單一系統的方法，它會逐步重寫和取代系統功能，直到舊式系統停止使用為止。此模式源自無花果藤，它長成一棵馴化樹並最終戰勝且取代了其宿主。該模式由 Martin Fowler 引入，作為重寫單一系統時管理風險的方式。如需有關如何套用此模式的範例，請參閱使用容器和 Amazon API Gateway 逐步現代化舊版 Microsoft ASP.NET (ASMX) Web 服務。

子網

您 VPC 中的 IP 地址範圍。子網必須位於單一可用區域。

監控控制和資料擷取 (SCADA)

在製造中，使用硬體和軟體來監控實體資產和生產操作的系統。

對稱加密

使用相同金鑰來加密及解密資料的加密演算法。

合成測試

以模擬使用者互動的方式測試系統，以偵測潛在問題或監控效能。您可以使用 Amazon CloudWatch Synthetics 來建立這些測試。

系統提示

一種向 LLM 提供內容、指示或指導方針以指示其行為的技術。系統提示有助於設定內容，並建立與使用者互動的規則。

T

標籤

做為中繼資料以組織 AWS 資源的鍵值對。標籤可協助您管理、識別、組織、搜尋及篩選資源。如需詳細資訊，請參閱標記您的 AWS 資源。

目標變數

您嘗試在受監督的 ML 中預測的值。這也被稱為結果變數。例如，在製造設定中，目標變數可能是產品瑕疵。

任務清單

用於透過執行手冊追蹤進度的工具。任務清單包含執行手冊的概觀以及要完成的一般任務清單。對於每個一般任務，它包括所需的預估時間量、擁有者和進度。

測試環境

請參閱 環境。

訓練

為 ML 模型提供資料以供學習。訓練資料必須包含正確答案。學習演算法會在訓練資料中尋找將輸入資料屬性映射至目標的模式 (您想要預測的答案)。它會輸出擷取這些模式的 ML 模型。可以使用 ML 模型，來預測您不知道的目標新資料。

傳輸閘道

可以用於互連 VPC 和內部部署網路的網路傳輸中樞。如需詳細資訊，請參閱 AWS Transit Gateway 文件中的什麼是傳輸閘道。

主幹型工作流程

這是一種方法，開發人員可在功能分支中本地建置和測試功能，然後將這些變更合併到主要分支中。然後，主要分支會依序建置到開發環境、生產前環境和生產環境中。

受信任的存取權

將許可授予您指定的服務，以代表您在組織中 AWS Organizations 及其帳戶中執行任務。受信任的服務會在需要該角色時，在每個帳戶中建立服務連結角色，以便為您執行管理工作。如需詳細資訊，請參閱 文件中的 AWS Organizations 搭配使用 AWS Organizations 與其他 AWS 服務。

調校

變更訓練程序的各個層面，以提高 ML 模型的準確性。例如，可以透過產生標籤集、新增標籤、然後在不同的設定下多次重複這些步驟來訓練 ML 模型，以優化模型。

雙比薩團隊

兩個比薩就能吃飽的小型 DevOps 團隊。雙披薩團隊規模可確保軟體開發中的最佳協作。

U

不確定性

這是一個概念，指的是不精確、不完整或未知的資訊，其可能會破壞預測性 ML 模型的可靠性。有兩種類型的不確定性：認知不確定性是由有限的、不完整的資料引起的，而隨機不確定性是由資料中固有的噪聲和隨機性引起的。如需詳細資訊，請參閱量化深度學習系統的不確定性指南。

未區分的任務

也稱為繁重工作，這是建立和操作應用程式的必要工作，但不為最終使用者提供直接價值或提供競爭優勢。未區分任務的範例包括採購、維護和容量規劃。

較高的環境

請參閱 環境。

V

清空

一種資料庫維護操作，涉及增量更新後的清理工作，以回收儲存並提升效能。

版本控制

追蹤變更的程序和工具，例如儲存庫中原始程式碼的變更。

VPC 對等互連

兩個 VPC 之間的連線，可讓您使用私有 IP 地址路由流量。如需詳細資訊，請參閱 Amazon VPC 文件中的什麼是 VPC 對等互連。

漏洞

危害系統安全性的軟體或硬體瑕疵。

W

暖快取

包含經常存取的目前相關資料的緩衝快取。資料庫執行個體可以從緩衝快取讀取，這比從主記憶體或磁碟讀取更快。

暖資料

不常存取的資料。查詢這類資料時，通常可接受中等速度的查詢。

視窗函數

SQL 函數，對與目前記錄在某種程度上相關的資料列群組執行計算。視窗函數適用於處理任務，例如根據目前資料列的相對位置計算移動平均值或存取資料列的值。

工作負載

提供商業價值的資源和程式碼集合，例如面向客戶的應用程式或後端流程。

工作串流

遷移專案中負責一組特定任務的功能群組。每個工作串流都是獨立的，但支援專案中的其他工作串流。例如，組合工作串流負責排定應用程式、波次規劃和收集遷移中繼資料的優先順序。組合工作串流將這些資產交付至遷移工作串流，然後再遷移伺服器和應用程式。

WORM

請參閱寫入一次，讀取許多。

WQF

請參閱AWS 工作負載資格架構。

寫入一次，讀取許多 (WORM)

儲存模型，可一次性寫入資料，並防止刪除或修改資料。授權使用者可以視需要多次讀取資料，但無法變更資料。此資料儲存基礎設施被視為不可變。

Z

零時差入侵

利用零時差漏洞的攻擊，通常是惡意軟體。

零時差漏洞

生產系統中未緩解的瑕疵或漏洞。威脅行為者可以使用這種類型的漏洞來攻擊系統。開發人員經常因為攻擊而意識到漏洞。

零鏡頭提示

提供 LLM 執行任務的指示，但沒有可協助引導任務的範例 (快照)。LLM 必須使用其預先訓練的知識來處理任務。零鏡頭提示的有效性取決於任務的複雜性和提示的品質。另請參閱少量擷取提示。

殭屍應用程式

CPU 和記憶體平均使用率低於 5% 的應用程式。在遷移專案中，通常會淘汰這些應用程式。

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。