歡迎學習模組 7：連接網路。

模組概覽

aws academy

小節目錄

1. 架構需求
2. 使用 AWS Site-to-Site VPN 連接到遠端網路
3. 使用 AWS Direct Connect 連接到遠端網路
4. 使用 VPC 對等連接在 AWS 中連接 VPC
5. 使用 AWS Transit Gateway 擴展 VPC 網路
6. 將 VPC 連接到受支援的 AWS 服務

活動

- AWS Transit Gateway

實驗

- 指導實驗：創建 VPC 對等連接

知識測驗

本模組包含以下章節：

1. 架構需求
2. 使用 AWS Site-to-Site VPN 連接到遠端網路
3. 使用 AWS Direct Connect 連接到遠端網路
4. 使用 VPC 對等連接在 AWS 中連接 VPC
5. 使用 AWS Transit Gateway 擴展 VPC 網路
6. 將 VPC 連接到受支援的 AWS 服務

本模組還包括：

- 一項活動，您將在此活動中討論如何使用 AWS Transit Gateway 連接三個 Virtual Private Cloud (VPC)
- 一個指導實驗，您將在此實驗中創建 VPC 對等連接

最後，您需要完成一個知識測驗，以測試您對本模組中涵蓋的關鍵概念的理解程度。

模組目標

學完本模組後，您應該能夠：

- 描述如何將本地網路連接到 Amazon Web Services (AWS) 雲
- 描述如何在 AWS 雲中連接 VPC
- 使用 VPC 對等連接在 AWS 雲中連接 VPC
- 描述如何在 AWS 雲中擴展 VPC
- 描述如何將 VPC 連接到受支援的 AWS 服務

學完本模組後，您應該能夠：

- 描述如何將本地網路連接到 Amazon Web Services (AWS) 雲
- 描述如何在 AWS 雲中連接 VPC
- 使用 VPC 對等連接在 AWS 雲中連接 VPC
- 描述如何在 AWS 雲中擴展 VPC
- 描述如何將 VPC 連接到受支援的 AWS 服務

模組 7：連接網路

第 1 節：架構需求

介紹第 1 節：架構需求。

咖啡館業務要求

咖啡館的工作負載越來越複雜。該架構必須支持多個 VPC 之間的連接，
並且具有高可用性和容錯能力。

咖啡館啟動了忠誠度獎勵計畫，客戶在購買 10 件或更多類似商品後可獲得免費飲料或甜點。客戶線上訂購時，他們必須提供一些個人身份資訊 (PII)，例如電子郵寄地址和信用卡號碼。出於合規性原因，咖啡館不能將這些資訊存儲在雲中。因此，Sofía 和 Nikhil 需要使用一種方法將其本地資料庫（存儲敏感客戶資訊）連接到其雲系統（存儲交易資料）。然後，他們必須對兩個系統之間的資料進行映射，以提供客戶獲得的獎勵。

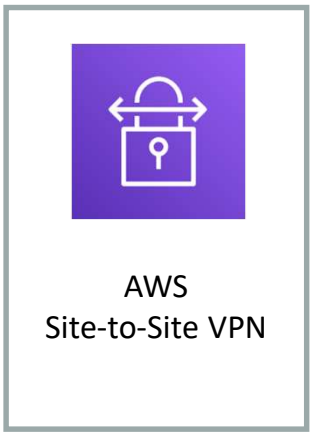
此外，出於安全考慮，Sofía 告訴 Olivia，她希望將開發環境隔離在一個 VPC 中，將生產環境隔離在另一個 VPC 中，但兩者之間仍然互相連接。Olivia 認為這是個好主意，並建議 Sofía 在設計網路環境時使其具有高可用性和容錯能力。

模組 7：連接網路

第 2 節：使用 AWS Site-to-Site VPN 連接到遠端網路

介紹第 2 節：使用 AWS Site-to-Site VPN 連接到遠端網路。

AWS Site-to-Site VPN



AWS Site-to-Site 是一種高度可用的解決方案，可讓您安全地將本地網路或分支機構網站連接到 VPC。

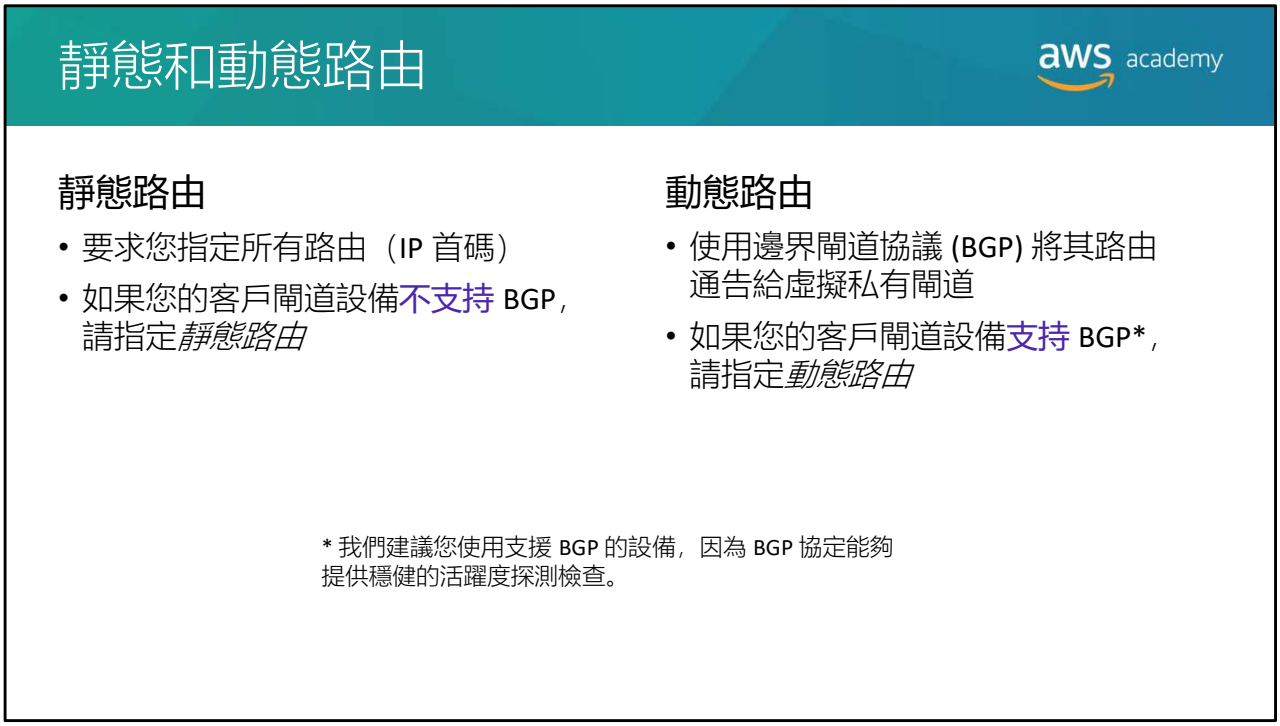
- 使用互聯網協定安全 (IPSec) 通信創建加密的虛擬私有網路 (VPN) 隧道
- 為每個 VPN 連接提供兩個加密隧道
- 按 VPN 連接小時收費

預設情況下，您在 AWS 上的 Virtual Private Cloud (VPC) 中啟動的實例無法與本地網路通信。

您可以使用 AWS Site-to-Site Virtual Private Network (AWS Site-to-Site VPN) 將本地網路或分支機構網站安全地連接到 VPC。每個 AWS Site-to-Site VPN 連接都使用互聯網協定安全 (IPSec) 通信在兩個位置之間創建加密的 VPN 隧道。*VPN 隧道*是用於在客戶網路和 AWS 之間傳輸資料的加密連結。連接的 AWS 端是*虛擬私有閘道*。（請注意，您還可以在中轉閘道上創建 Site-to-Site VPN 連接，而不使用虛擬私有閘道。稍候您將在本模組中瞭解有關 AWS Transit Gateway 的更多資訊。）連接的本地端是*客戶閘道*。

AWS Site-to-Site VPN 提供兩個跨多個可用區的 VPN 隧道，您可以同時使用這兩條 VPN 隧道來實現高可用性。您可以通過第一個隧道資料流主要流量，使用第二個隧道進行冗餘。如果一條隧道發生故障，流量仍會傳輸到 VPC。

如果創建與 VPC 相連的 Site-to-Site VPN 連接，您需要為 VPN 連接已預置且可用的 VPN 連接小時付費。有關定價的更多資訊，請參閱 AWS Site-to-Site VPN 和 Accelerated Site-to-Site VPN 連接定價。



在創建 Site-to-Site VPN 連接時，必須指定計劃使用的路由類型，而且必須更新子網的路由表。

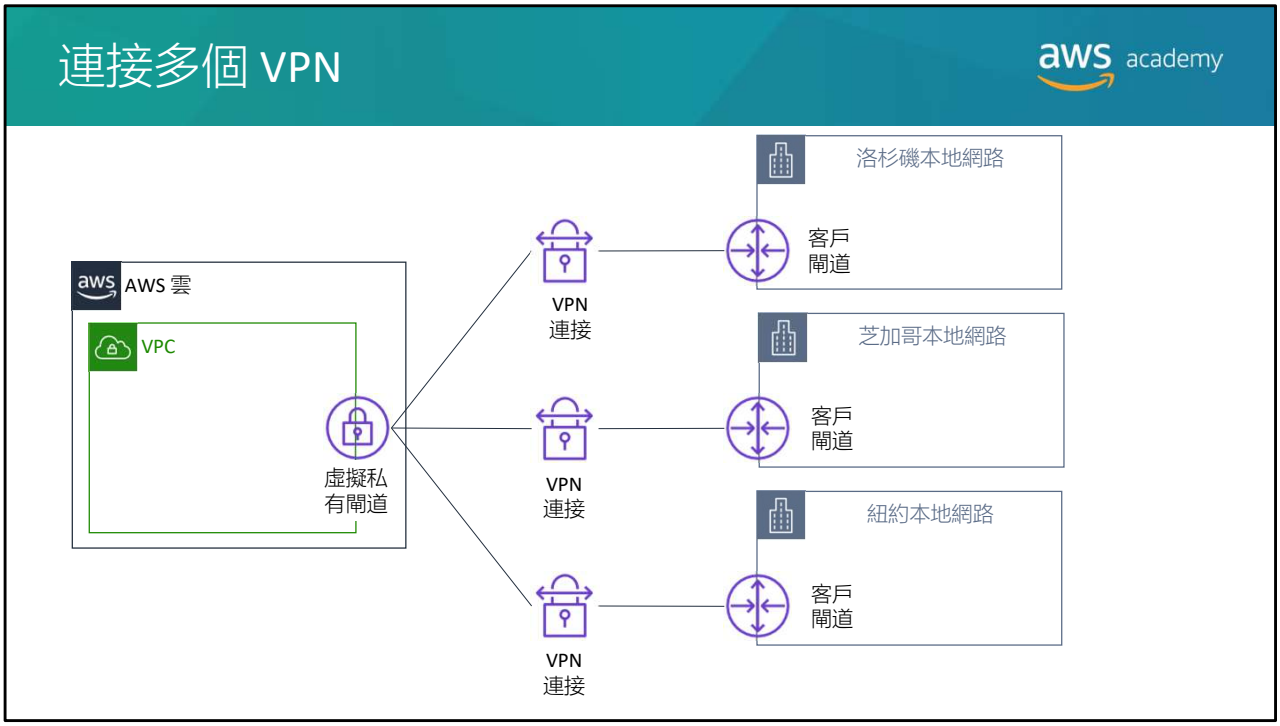
AWS Site-to-Site VPN 支援兩種類型的路由。您選擇的路由類型取決於您的 VPN 設備的品牌和型號：

- 如果您的 VPN 設備支援邊界閘道協定 (BGP)，您可以在配置 Site-to-Site VPN 連接時指定*動態路由*方式。*動態路由*使用 BGP 向虛擬私有閘道通告路由。動態路由每個路由表最多支援 100 個傳播路由。（有關當前限制，請參閱 AWS Site-to-Site VPN 限制。）
- 如果您的 VPN 設備不支援 BGP，請指定*靜態路由*。*靜態路由*要求您為網路指定應與虛擬私有閘道通信的路由（即 IP 首碼）。預設情況下，靜態路由支援每個路由表 50 個非傳播路由，最多可支援 1000 個非傳播路由。（有關當前限制，請參閱 AWS Site-to-Site VPN 限制。）

我們建議您使用支援 BGP 的設備，因為 BGP 協定可提供穩健的活性探測檢查，可以在第一條隧道出現故障時協助容錯移轉到第二條 VPN 隧道。不支援 BGP 的設備也可執行運行狀況檢查，以便在需要時協助容錯移轉到第二條隧道。

有關已使用 Amazon VPC 測試的靜態和動態路由設備的清單，請參閱 *AWS Site-to-Site VPN 網路系統管理員指南*中的我們已測試的客戶閘道設備。

有關 Site-to-Site VPN 路由選項的詳細資訊，請參閱靜態路由和動態路由選項。



為了保持客戶閘道的高可用性，您可以設置冗余客戶閘道設備。如果您有冗余客戶閘道設備，則每個設備都會通告相同的首碼（例如 *0.0.0.0/0*）給虛擬私有閘道。AWS 使用 BGP 路由確定流量的路徑。如果一個客戶閘道設備發生故障，則虛擬私有閘道會將所有流量定向到正常工作的客戶閘道設備。

您可以使用 AWS VPN CloudHub 建立從多個客戶閘道設備到單個虛擬私有閘道的多個 VPN 連接。此配置可在不同的方式中用於在 VPN 連接側實現冗餘和容錯移轉。

AWS VPN CloudHub 以輪輻模式運行，使多個網站能夠訪問您的 VPC 或安全地相互訪問。您可以在包含或不包含 VPC 的情況下使用它。您配置各個客戶閘道設備以通告具體網站相關的首碼（例如 *10.0.0.0/24*、*10.0.1.0/24*）給虛擬私有閘道。虛擬私有閘道將所有流量導向適當的網站，並將該網站的可到達性通告給所有其他網站。

有關使用 AWS Site-to-Site VPN 的更多資訊，請參閱以下資源：

- Site-to-Site VPN 單一連接和多個連接示例
- 使用冗餘 Site-to-Site VPN 連接以提供容錯移轉

第 2 節要點

- AWS Site-to-Site VPN 是一種高度可用的解決方案，可讓您安全地將本地網路或分支機構網站連接到 VPC
- AWS Site-to-Site VPN 支持靜態和動態路由
- 您可以建立從多個客戶閘道設備到單個虛擬私有閘道的多個 VPN 連接

本模組中這節內容的要點包括：

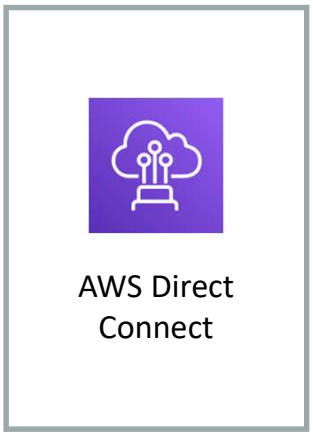
- AWS Site-to-Site VPN 是一種高度可用的解決方案，可讓您安全地將本地網路或分支機構網站連接到 VPC
- AWS Site-to-Site VPN 支援靜態和動態路由
- 您可以建立從多個客戶閘道設備到單個虛擬私有閘道的多個 VPN 連接

模組 7：連接網路

第 3 節：使用 AWS Direct Connect 連接到遠端網路

介紹第 3 節：使用 AWS Direct Connect 連接到遠端網路。

AWS Direct Connect (DX)



AWS Direct Connect（也稱為DX）可為您提供容量為 1Gbps 或10Gbps 的專用私有網路

降低資料傳輸成本

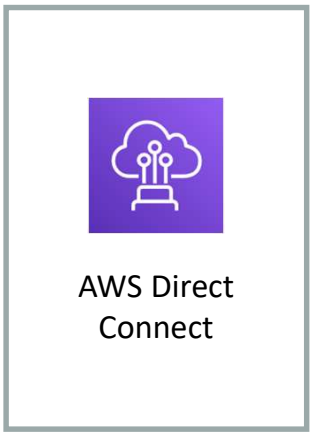
通過可預測的指標提高應用程式性能

如您所知，AWS Site-to-Site VPN 是用於將本地網路連接到 AWS 全球網路的一個選項。使用這個選項，您的資料將經由公共互聯網通過加密的隧道傳輸。

AWS Direct Connect（即 DX）是另一種超越簡單互聯網連接的解決方案。DX 使用開放標準 802.1q 虛擬區域網路 (VLAN)，因此您可以建立從本地到 AWS 的專用私有網路連接。這種私有連接可以降低網路成本，增加頻寬輸送量，同時提供優於互聯網連接的穩定網路體驗。

可提供 1Gbps 和 10Gbps 容量的專用連接。

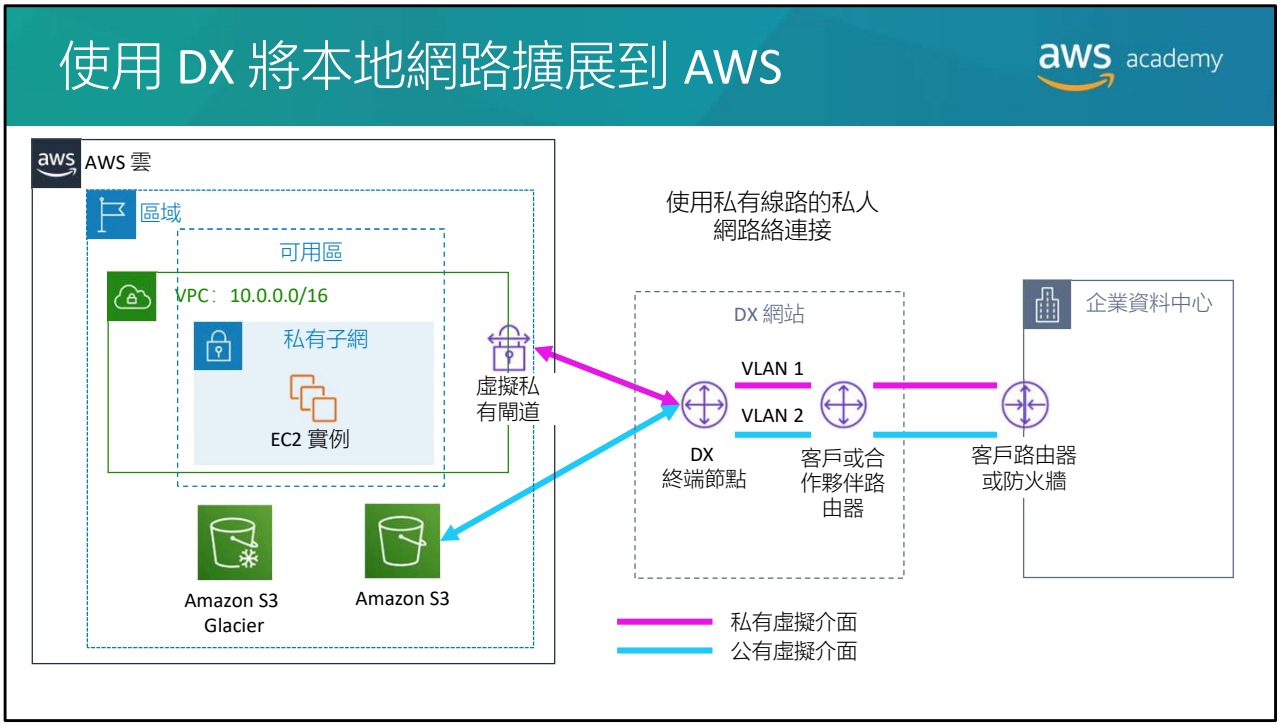
DX 使用案例



- 混合環境
- 傳輸大型資料集
- 可預測的網路性能
- 安全性與合規性

DX 在幾種場景中非常有用，例如：

- *混合環境* – 對於需要訪問現有資料中心設備（例如本地資料庫）的應用程式，DX 使您能夠創建一個混合環境，從而使您能夠利用 AWS 的彈性和經濟效益。
- *傳輸大型資料集* – 對於在大型資料集上運行的應用程式（例如高性能計算 (HPC) 應用程式），通過互聯網在資料中心和 AWS 雲之間傳輸大型資料集既耗時又昂貴。對於此類應用程式，使用 DX 連接到 AWS 雲是個很好的解決方案，其原因在於：
  - 網絡傳輸不會爭用資料中心的互聯網頻寬。
  - 高頻寬鏈路可降低網路擁塞和應用程式性能下降的可能性。
  - 通過限制應用程式使用的互聯網頻寬，您可以減少支付給 Internet 服務提供者 (ISP) 的網路費用，同時避免為增加的互聯網頻寬承諾或新合同付費。此外，通過 DX 傳輸的所有資料會按照降低後的 DX 資料傳輸費率（而非互聯網資料傳輸費率）收費，這可以降低您的網路成本。
- *提升應用程式性能* – DX 對需要可預測的網路性能的應用程式也很有用。其中包括處理即時資料源（如音訊流或視頻流）的應用程式。在這種情況下，私人網路絡連接可以提供一致性比標準互聯網連接更強的網路性能。
- *安全與合規性* – 有時候，企業安全或監管政策要求託管在 AWS 雲上的應用程式只能通過私有網路線路進行訪問。DX 自然而然成為針對此要求的一種解決方案，因為您的資料中心與應用程式之間的流量會流經專用的私有網路連接。

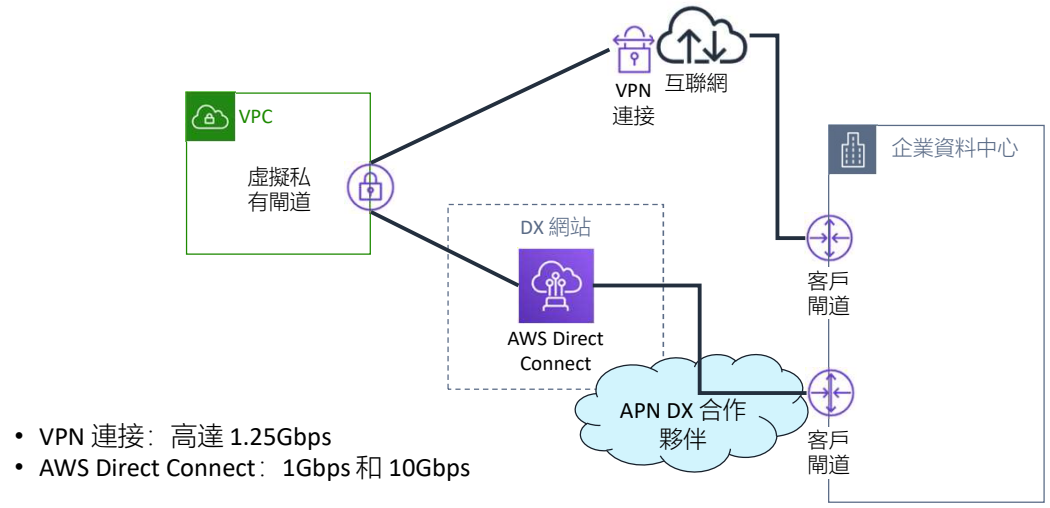


DX 通過標準的乙太網光纖電纜將您的內部網路連結到 DX 網站。纜線的一端連接到您的路由器。另一端連接到 DX 路由器。通過此連接，您可以創建允許直接訪問 AWS 服務的*虛擬接口*。公有虛擬介面允許訪問公有 AWS 服務，例如 Amazon Simple Storage Service (Amazon S3)。私有虛擬介面允許對您的 VPC 進行訪問。

您可以從任何受支援的 DX 位置訪問任何區域（中國除外）的任何 VPC 或公有 AWS 服務。如果您的 DX 網站沒有設備，則可以在 DX AWS 合作夥伴網路 (APN) 合作夥伴的協助下訪問 DX。

有關 DX 的資訊，請參閱什麼是 AWS Direct Connect?

實現高可用性：具有備份 VPN 連接的 DX



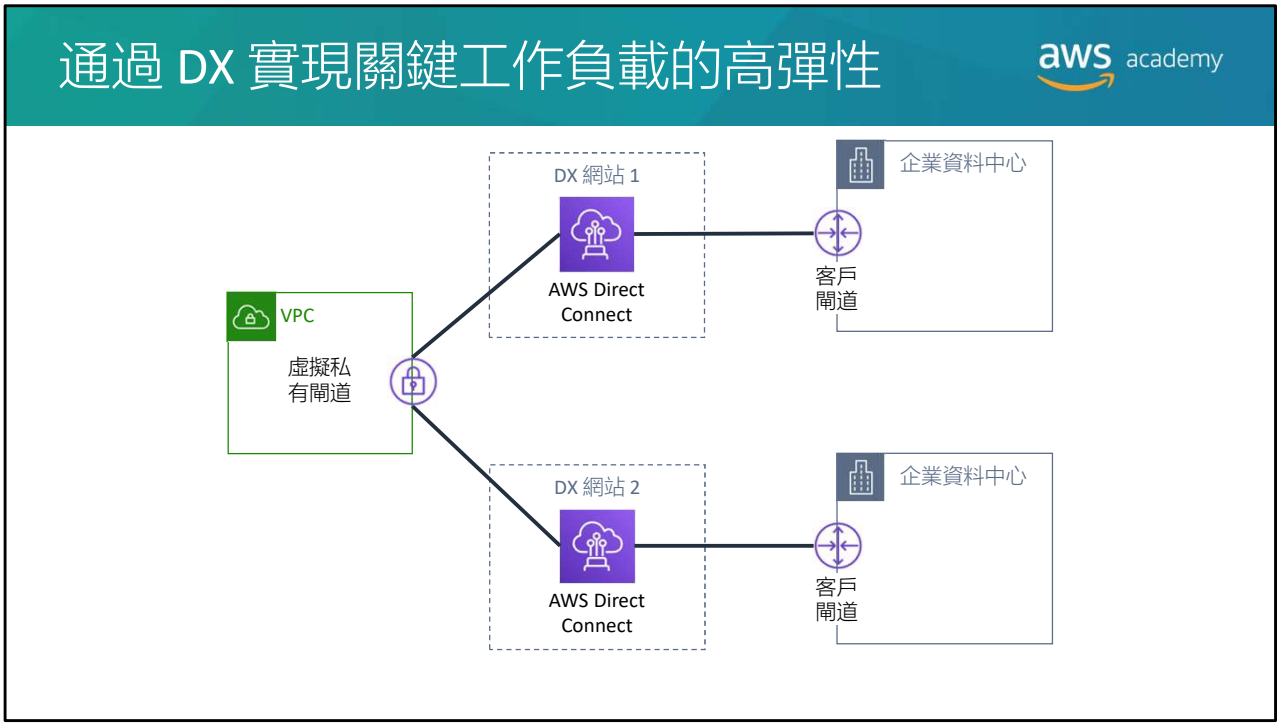
通過將用於主連接的一個或多個 DX 連接與成本較低的備份 VPN 連接相結合，您可以在資料中心和 VPC 之間實現高可用性連接。

在此示例中，配置包含兩個動態路由連接，一個使用 DX，另一個使用兩個來自不同客戶設備的 VPN 連接。AWS 提供了示例路由器配置，說明您建立 DX 連接和動態路由 VPN 連接。預設情況下，AWS 始終優先通過 DX 連接發送流量，因此不需要其他特定於 AWS 的配置來定義主連接和備份連接。但是，您應該配置 DX 和 VPN 特定的內部路由傳播，以確保內部系統選擇適當的路徑。

這種方法讓您可以為 AWS 流量選擇主網路路徑和網路提供商，還讓您可以選擇使用其他提供商來備份 VPN 連接。您應該選擇符合組織風險承受能力、財務預期和資料中心連接策略的網路提供商和 DX 網站。

最後，您可以在分開部署的私有 IP 位址空間之間使用多個 DX 線路和多個 VPN 隧道。您還可以使用多個 DX 網站來實現高可用性。如果您使用多個 AWS 區域，您還需要在至少兩個區域中使用多個 DX 網站。您可能需要考慮使用 AWS Marketplace 設備作為 VPN 的端點。

通過 DX 實現關鍵工作負載的高彈性



高彈性且具備容錯能力的網路連接是構建架構完善的系統的關鍵。AWS 建議從多個資料中心進行連接以實現物理位置冗餘。在設計遠端連接時，可以考慮使用冗餘硬體和電信提供商。

此外，最佳實踐是使用動態路由、主動/主動連接在冗餘網路連接之間實現自動負載均衡和容錯移轉。預置足夠的網路容量，確保在一個網路連接發生故障時，不會使冗餘連接遭到摧毀和性能降低。

對於需要高彈性的關鍵生產工作負載，AWS 建議您在多個位置建立一個連接。如架構圖所示，這種拓撲可確保在因硬體故障或整個位置故障而導致連接故障時具有彈性。您可以使用 Direct Connect Gateway 從任何 DX 網站訪問任何 AWS 區域（中國境內的 AWS 區域除外）。

要詳細瞭解連接到 AWS 時需要牢記的其他拓撲指南，請參閱 AWS Direct Connect 彈性建議。

第 3 節要點

aws academy

- AWS Direct Connect 使用開放標準 802.1q VLAN，使您能夠建立從本地到 AWS 的專用私有網路連接
- 您可以從任何受支援的 DX 網站訪問任何區域（中國除外）的任何 VPC 或公有 AWS 服務
- 通過將用於主連接的一個或多個 DX 連接與成本較低的備份 VPN 連接相結合，您可以在資料中心和 VPC 之間實現高度可用的連接
- 為了實現高彈性且具備容錯能力的架構，請從多個資料中心連接到 AWS 網路，以便實現物理位置冗餘

本模組中這節內容的要點包括：

- AWS Direct Connect 使用開放標準 802.1q VLAN 允許您建立從本地到 AWS 的專用私有網路連接
- 您可以從任何受支援的 DX 網站訪問任何區域（中國除外）的任何 VPC 或公有 AWS 服務
- 通過將用於主連接的一個或多個 DX 連接與成本較低的備份 VPN 連接相結合，您可以在資料中心和 VPC 之間實現高度可用的連接
- 為了實現高彈性且具備容錯能力的架構，請從多個資料中心連接到 AWS 網路，以便實現物理位置冗餘

模組 7：連接網路

第 4 節：使用 VPC 對等連接在 AWS 中連接 VPC

介紹第 4 節：使用 VPC 對等連接在 AWS 中連接 VPC。

連接 VPC

- 隔離一些工作負載通常是一種很好的做法。
- 但是，您可能需要在兩個或更多 VPC 之間傳輸資料

將工作負載隔離在單獨的 VPC 中通常是一種很好的做法。例如，當您的業務或架構規模過大時，您可能需要出於安全性、架構目的或簡單性而將邏輯元素隔開。但是，當需要在 VPC 之間傳輸資料時，最好在 VPC 之間建立連接。

VPC 對等連接

- 兩個 VPC 之間的一對一網路連接
- 無需閘道、VPN 連接和單獨的網路設備
- 高度可用的連接
- 沒有單點故障或頻寬瓶頸
- 流量始終保留在全球 AWS 骨幹網上

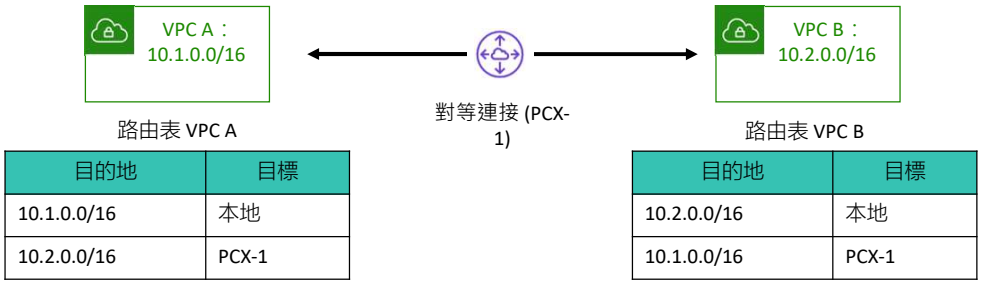
*VPC 對等連接*是兩個 VPC 之間的一對一網路連接，讓您可以私下在它們之間路由流量。這兩個 VPC 中的實例可以彼此通信，就像它們位於同一網路中一樣。您可以在您自己的 VPC 之間創建 VPC 對等連接：可以與其他 AWS 帳戶中的 VPC 建立連接，也可以與其他 AWS 區域中的 VPC 建立連接。

您可以在不同 AWS 區域的 VPC 之間建立對等連接關係。區域間 VPC 對等連接提供了一種簡單經濟的方式，可在區域間共用資源或為實現地理冗餘性而複製資料。通過區域間 VPC 對等連接傳輸的資料將按標準的區域間資料傳輸費率收費。

區域間 VPC 對等連接使 VPC 資源能夠使用私有 IP 位址相互通信，而無需閘道、VPN 連接或獨立的網路設備。VPC 資源的一些示例包括 Amazon Elastic Compute Cloud (Amazon EC2) 實例、Amazon Relational Database Service (Amazon RDS) 資料庫以及在不同區域運行的 AWS Lambda 函數。

流量仍保留在私有 IP 位址空間中。所有區域間流量都經過加密，沒有單點故障或頻寬瓶頸。流量始終保留在全球 AWS 骨幹網上。流量永遠不會經過公共互聯網，這樣可以減少面臨的威脅，例如常見漏洞和分散式拒絕服務 (DDoS) 攻擊。

建立 VPC 對等連接



路由表 VPC A

目的地	目標
10.1.0.0/16	本地
10.2.0.0/16	PCX-1

路由表 VPC B

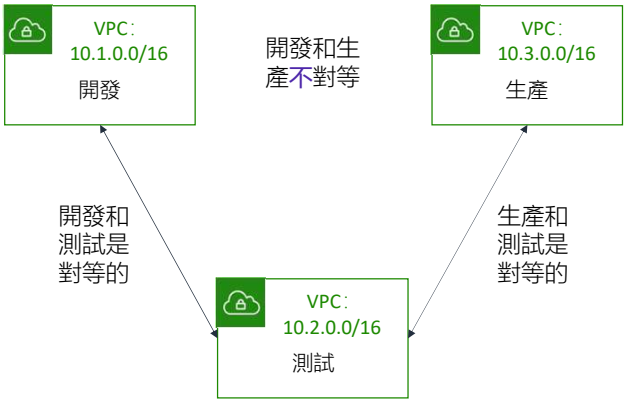
目的地	目標
10.2.0.0/16	本地
10.1.0.0/16	PCX-1

要建立 VPC 對等連接，請求者 VPC（或本地 VPC）的所有者應向對等 VPC 的所有者發送一個請求。要啟動連接，對等 VPC 的所有者必須接受 VPC 對等連接請求。

要通過使用私有 IP 位址啟用對等 VPC 之間的流量流，您必須向 VPC 的一個或多個路由表添加路由。此路由必須指向對等 VPC 的 IP 地址範圍。然後，對等 VPC 的所有者會向其任一 VPC 路由表添加一條指向您的 VPC IP 地址範圍的路由。

您可能還需要更新與您的實例關聯的安全性群組規則，以便進出對等 VPC 的流量不受限制。

VPC 對等連接限制



- 使用私有 IP 地址
- 可以在不同的 AWS 帳戶之間建立
- 不能有重疊的 CIDR 塊
- 任何兩個 VPC 之間只能有一個對等資源
- 不支援傳遞對等關係

在建立 VPC 對等連接時，您應該注意一些限制：

- VPC 對等連接使用私有 IP 位址。
- 可以在不同的 AWS 帳戶之間建立 VPC 對等連接。對等 VPC 的 CIDR 塊不能與請求者的 CIDR 塊重疊。
- 您在任何兩個 VPC 之間只能有一個對等資源。
- 不支援可傳遞對等互連。例如，在圖示中，開發 VPC 和測試 VPC 之間已建立對等連接，生產 VPC 和測試 VPC 之間已建立對等連接。但是，這並不意味著生產 VPC 已連接到開發 VPC。預設情況下，VPC 對等連接不允許生產 VPC 連接到開發 VPC，除非它們*明確建立了對等連接*。因此，您可以控制哪些 VPC 可以相互通信。

要瞭解有關 VPC 對等連接限制的更多資訊，請參閱 VPC 對等連接限制。

有關對等連接多個 VPC 的注意事項

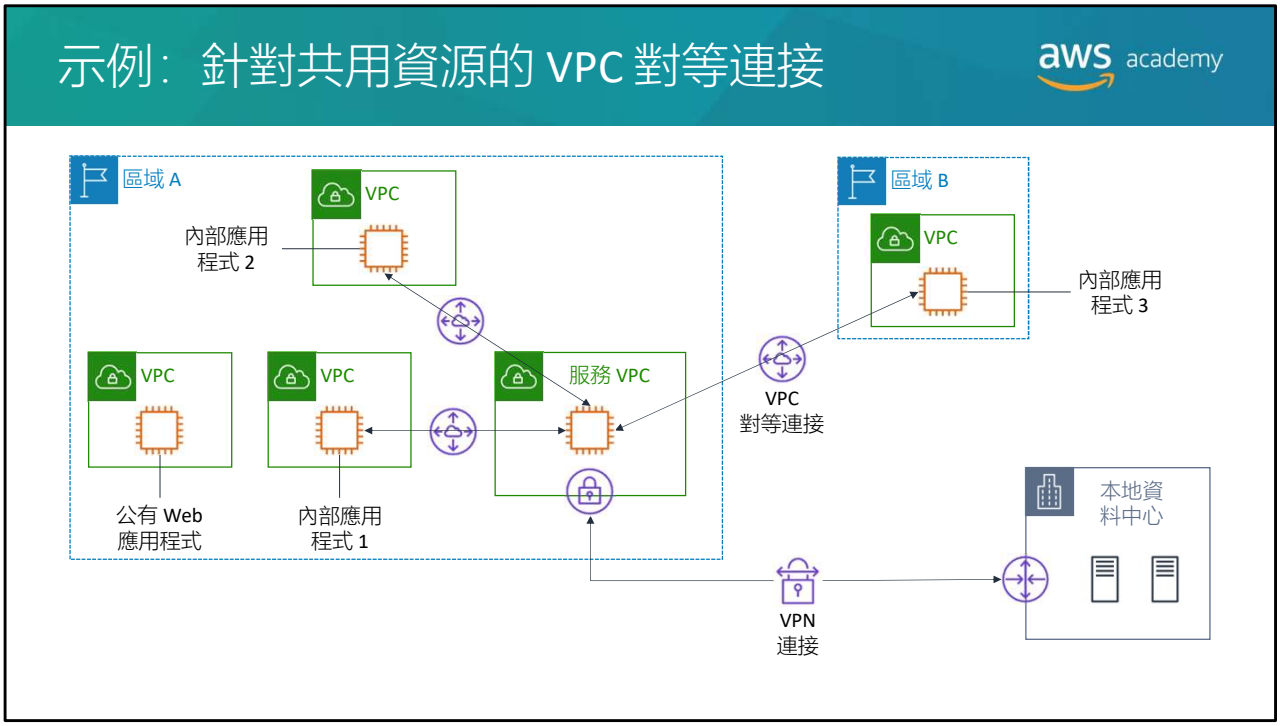
在連接多個 VPC 時，請考慮以下網絡設計原則：

僅連接必要的 VPC

確保解決方案可以擴展

在單個 AWS 區域中連接多個 VPC 時，請考慮以下網路設計原則：

- 僅連接那些真正必須彼此通信的 VPC
- 確保您選擇的解決方案可以根據您當前和未來的 VPC 連接需求進行擴展



本示例展示了如何將 VPC 對等連接用於共用資源。

在本示例中，公司中的每個部門 VPC 都與共用*服務 VPC* 建立了對等連接。此 VPC 包含與 Microsoft Active Directory 的連接、安全掃描工具、監控和日誌記錄工具以及其他各種功能。它還提供了一個代理，通過該代理，部門 VPC 可以訪問一些本地資源。VPC 對等連接使處於不同 VPC 中的公司應用程式能夠訪問共用服務 VPC，但彼此間仍保持隔離。在本示例中，還請注意 VPC 對等連接是在不同區域的 VPC 之間建立的。

第 4 節要點

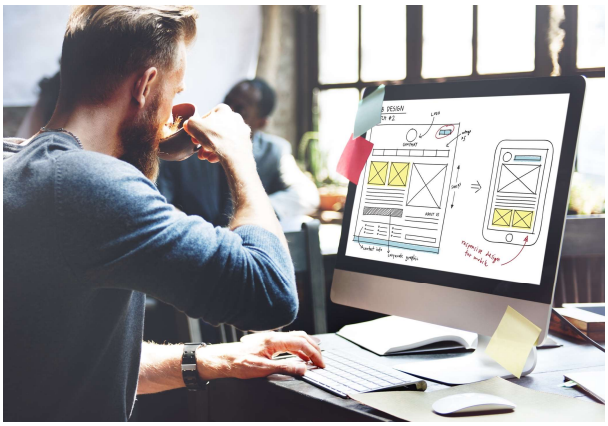
- VPC 對等連接是兩個 VPC 之間的一對一網路連接，使您可以私下在它們之間路由流量
- 您可以在不同 AWS 區域的 VPC 之間建立對等關係
- VPC 對等連接 –
  - 使用私有 IP 地址
  - 可以在不同的 AWS 帳戶之間建立
  - 不能有重疊的 CIDR 塊
  - 任何兩個 VPC 之間只能有一個對等資源
  - 不支持傳遞對等關係

本模組中這節內容的要點包括：

- VPC 對等連接是兩個 VPC 之間的一對一網路連接，使您可以私下在它們之間路由流量
- 您可以在不同 AWS 區域的 VPC 之間建立對等關係
- VPC 對等連接 –
  - 使用私有 IP 地址
  - 可以在不同的 AWS 帳戶之間建立
  - 不能有重疊的 CIDR 塊
  - 任何兩個 VPC 之間只能有一個對等資源
  - 不支持傳遞對等關係

模組 7 – 指導實驗：創建 VPC 對等連接

aws academy



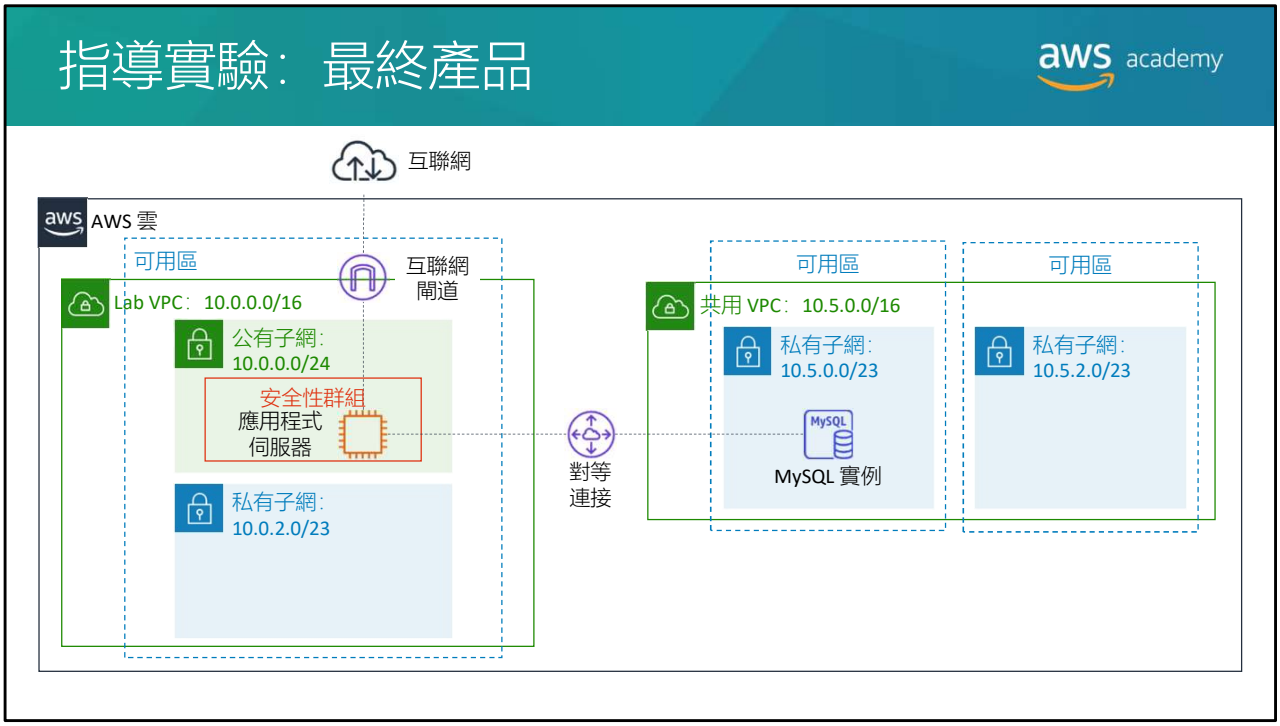
您現在將完成模組 7 – 指導實驗：創建 VPC 對等連接。

指導實驗：任務

1. 在兩個 VPC 之間建立對等連接
2. 配置路由表以將流量發送到對等連接
3. 測試對等連接

在本指導實驗中，您將完成以下任務：

1. 在兩個 VPC 之間建立對等連接
2. 配置路由表以將流量發送到對等連接
3. 測試對等連接



該圖總結了您完成實驗後將會構建的內容。

現在可以開始指導實驗了。

指導實驗總結：要點

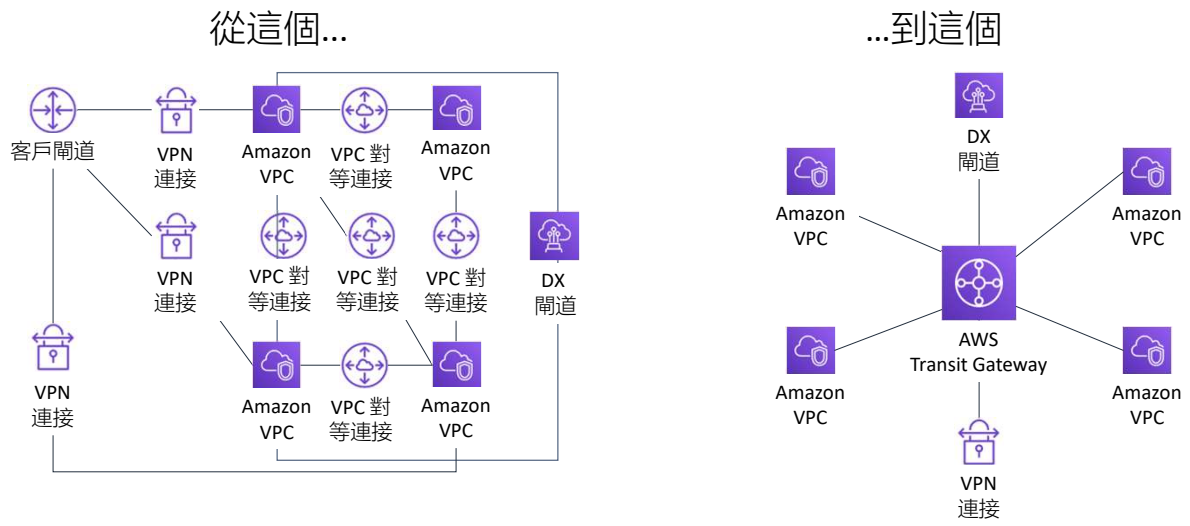
完成這個指導實驗之後，您的講師可能會帶您討論此指導實驗的要點。

模組 7：連接網路

第 5 節：使用 AWS Transit Gateway 擴展 VPC 網路

介紹第 5 節：使用 AWS Transit Gateway 擴展 VPC 網路。

需要跨多個 VPC 擴展網路



隨著 AWS 上運行的工作負載數量增加，您必須能夠跨多個帳戶和 VPC 擴展網路，才能跟上增長速度。您可以使用 VPC 對等連接來連接任意兩個 VPC。但是，如果無法集中管理連接策略，那麼就會造成運營成本高昂，且難於跨多個 VPC 管理點對點連接。對於本地連接，必須將 VPN 連接到每個單獨的 VPC。當 VPC 數量增長到數百個時，此解決方案的構建可能非常耗時，而且難以管理。

思考以下幾個問題非常重要：在經過一段時間後，您的環境會達到多大規模？環境的擴展能力如何？以及您如何管理 VPC？要解決此問題，您可以使用 AWS Transit Gateway 來簡化聯網模型。

AWS Transit Gateway

AWS Transit Gateway

AWS Transit Gateway 是一項服務，使您可以將 VPC 和本地網路連接到單個網關。

- 完全託管、高度可用且靈活的路由服務
- 充當所有流量流經您網路的樞紐
- 使用單個閘道連接多達 5000 個 VPC 和本地環境

借助 AWS Transit Gateway 這項服務，您能夠將 VPC 和本地網路連接到單個閘道（稱為中轉閘道）。借助 AWS Transit Gateway，只需創建和管理從中央閘道到網路中每個 VPC、本地資料中心或遠端辦公室的一條連接。

AWS Transit Gateway 使用輪輻模型。這種模型可以大大簡化管理工作並降低運營成本，因為每個網路只需連接到中轉閘道，而不是連接到所有其他網路。將任何新的 VPC 連接到中轉閘道，然後它就會自動向連接到中轉閘道的所有其他網路開放。這種易連線性使您可以隨著需求的增長更輕鬆地擴展網路。

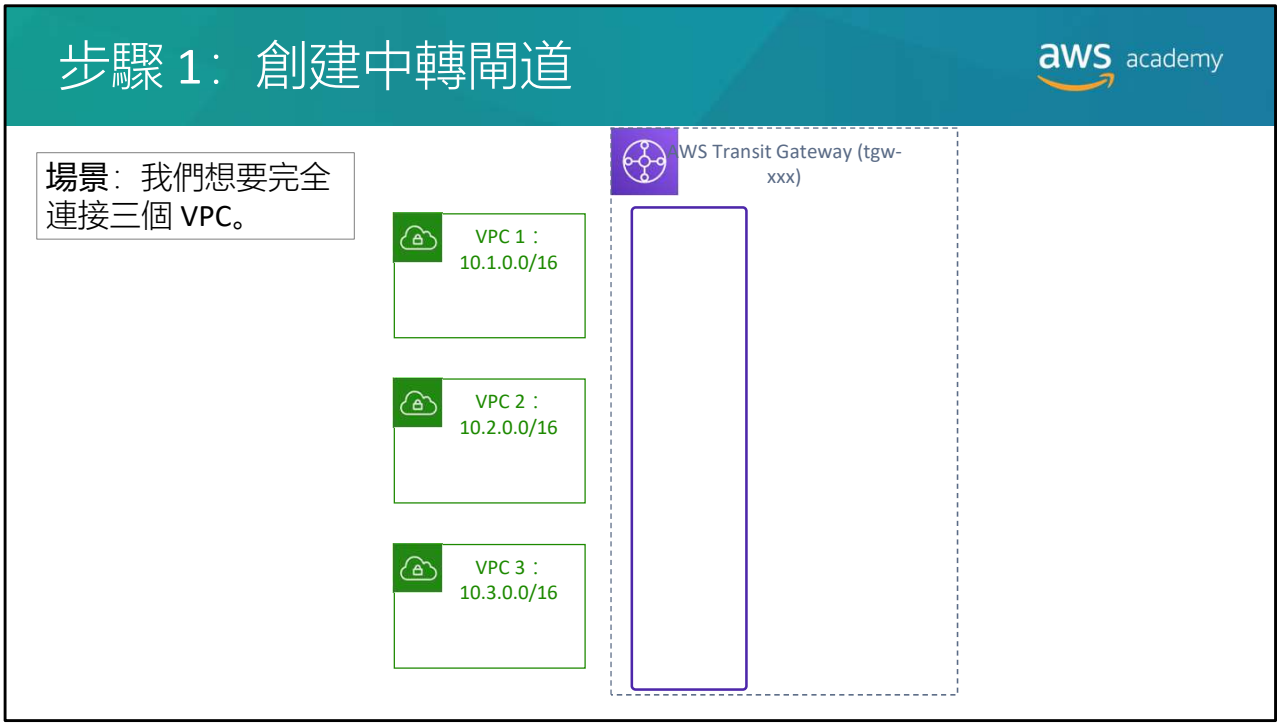
您可以使用 AWS Transit Gateway 連接多達 5000 個 VPC 和本地網路。

連接多個 VPC

場景：我們想要完全連接三個 VPC。

要瞭解如何使用 AWS Transit Gateway 連接多個 VPC，請考慮此場景。您想要完全連接網路中的三個 VPC。在此場景中，您將學習如何在單個區域中部署 AWS Transit Gateway 和三個具有非重疊 IP 位址空間的 VPC。然後，您將中轉閘道連接到這些 VPC。

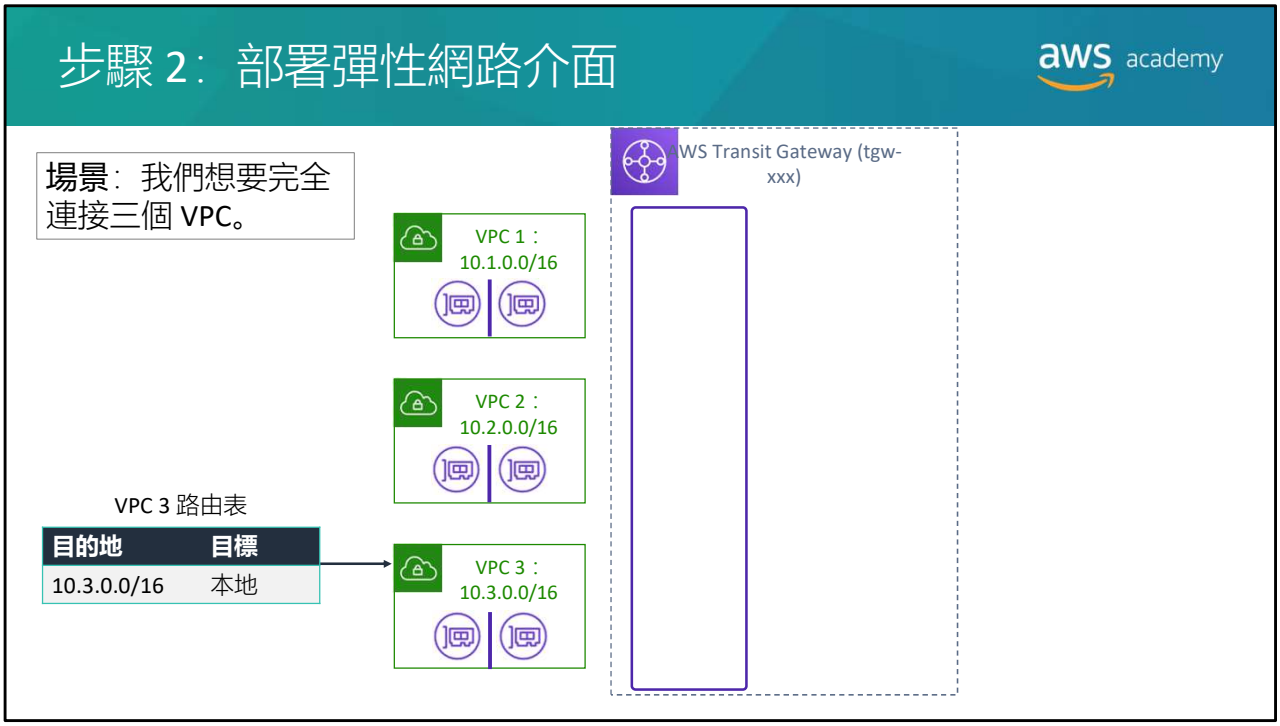
步驟 1：創建中轉閘道



連接多個 VPC 的第一步是創建中轉閘道。*中轉閘道*是中轉中心，您可用它來互連 VPC 和本地網路。它充當區域虛擬路由器，用於路由在您的 VPC 和 VPN 連接之間流動的流量。中轉閘道根據網路流量的規模靈活地進行擴展。

您可以通過 Amazon VPC 控制台設置中轉閘道。使用 AWS Transit Gateway 需要支付各種費用，因此請確保您的架構和預算能夠支援使用中轉閘道。

有關詳細資訊，請參閱什麼是中轉閘道？

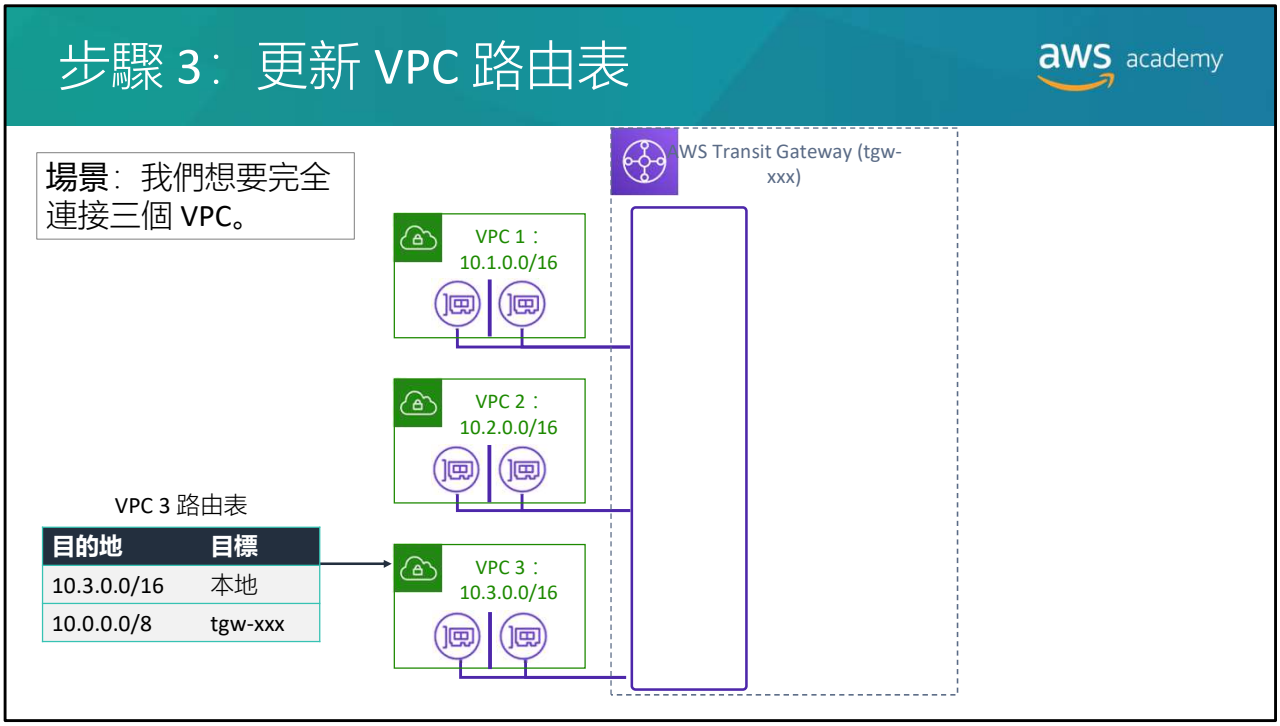


AWS Transit Gateway 通過彈性網路介面（即 ENI）連接到 VPC，這些介面部署到子網中。

您必須確保屬於 VPC 的每個可用區都有一個將 VPC 連接到中轉閘道的 ENI。您可以通過從每個可用區中為 ENI 選擇至少一個子網來實現此目的。

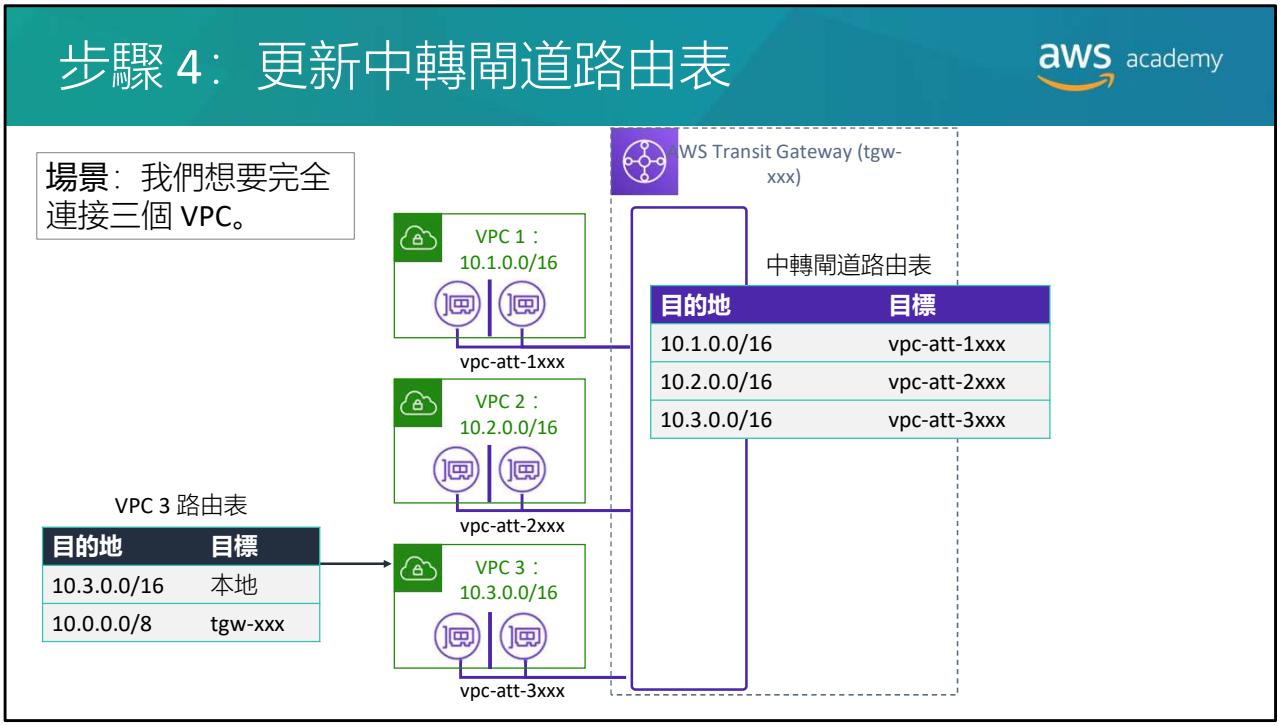
請注意，在此示例中，VPC 3 的路由表具有使用 10.3.0.0/16 網路的 VPC 3 的本地目的地路由。

步驟 3：更新 VPC 路由表



在連接 ENI 後，下一步是在 VPC 路由表中添加一個路由，以將發往網路中其他 VPC 的流量發送到中轉閘道。

在此示例中，VPC 3 路由表的第二行顯示，發往 10.0.0.0/8 網路的流量被發送到中轉閘道。此路由使從 VPC 3 到 VPC 1 或 VPC 2 的任何流量都可以發送到中轉閘道，因為 CIDR 塊 10.0.0.0/8 包括 10.X.0.0/16 CIDR 塊（由單獨 VPC 使用）。

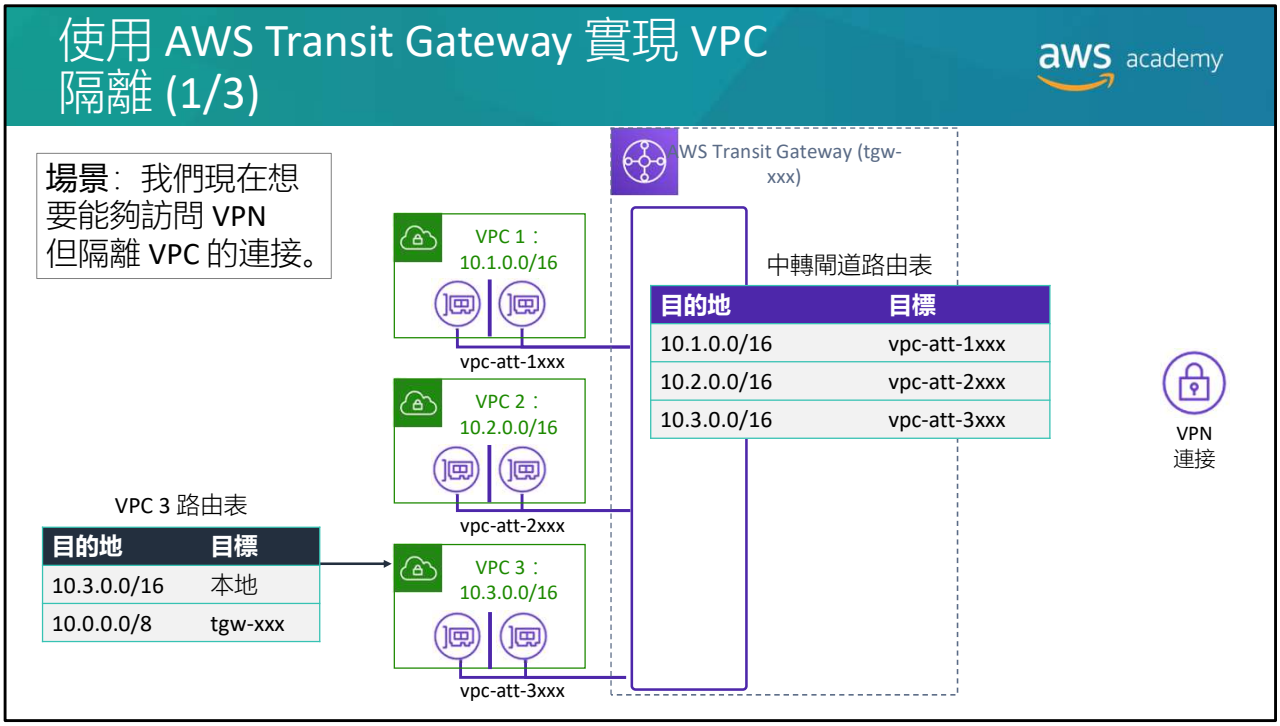


接下來，您必須配置中轉閘道路由表，以將流量路由到所連接的 VPC。

在創建中轉閘道時，將創建默認的中轉閘道路由表。中轉閘道路由表中的每條路由使中轉閘道能夠將發往其中一個 VPC 的流量發送到相應的附件（這是對連接到 VPC 本身的 ENI 的引用）。

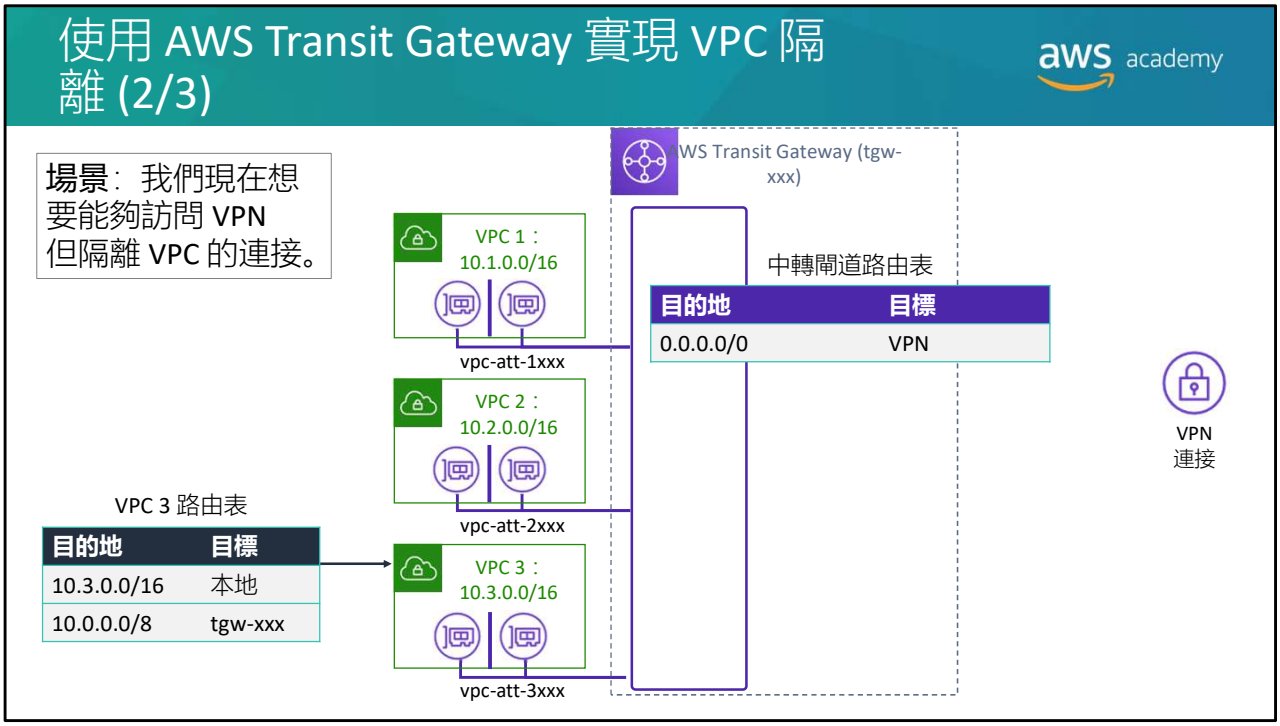
在此示例中，中轉閘道路由表中有一條路由，該路由將任何發往 10.1.0.0/16 網路的流量發送到 vpc-att-1xxx（VPC 1 的附件）。同樣，任何發往其他 VPC 網路的流量都會發送到相應的附件。

有關如何使用 AWS Transit Gateway 創建互連環境的更多資訊，請參閱 Transit Gateways 入門。



儘管可以使用 AWS Transit Gateway 連接多個 VPC，但也可以使用它在 VPC 環境中實現隔離。在這個場景中，您想要將 VPN 源連接到 VPC 環境。您還希望阻止 VPC 直接連接彼此，讓 VPN 來決定是否必須將來自一個 VPC 的流量轉發到另一個 VPC。

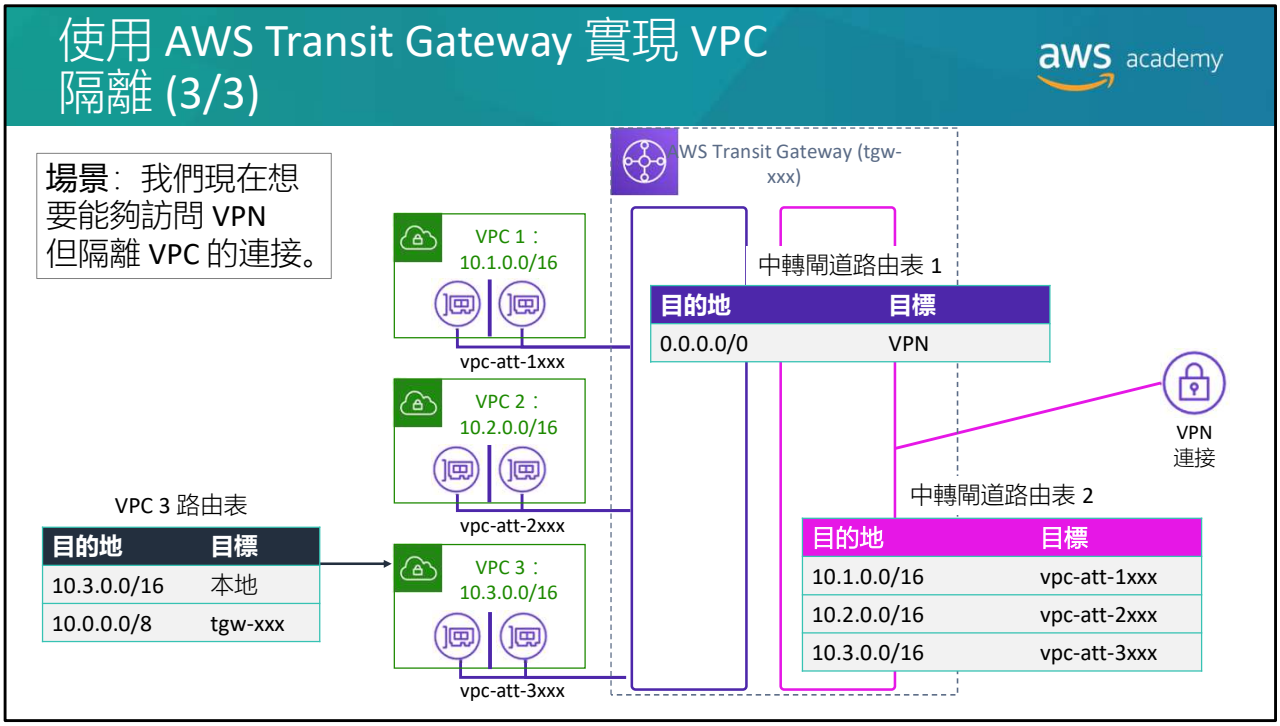
通過適當地為中轉閘道設置路由表，您可以阻止 VPC 之間的資訊共用。



要實施此解決方案，請更新中轉閘道路由表中的路由，以將所有已知流量發送到 VPN 連接。

在此示例中，當 10.0.0.0/8 網路中任何 VPC 的流量從 VPC 3 發送到中轉閘道時，中轉閘道會將流量轉發到 VPN（如幻燈片所示）。中轉閘道不會將流量發送到任何其他 VPC，因為沒有指向任何 VPC 附件的路由。

現在，您具有了對 VPC 環境的隔離且安全的 VPN 訪問，而 VPC 之間沒有交叉通信。

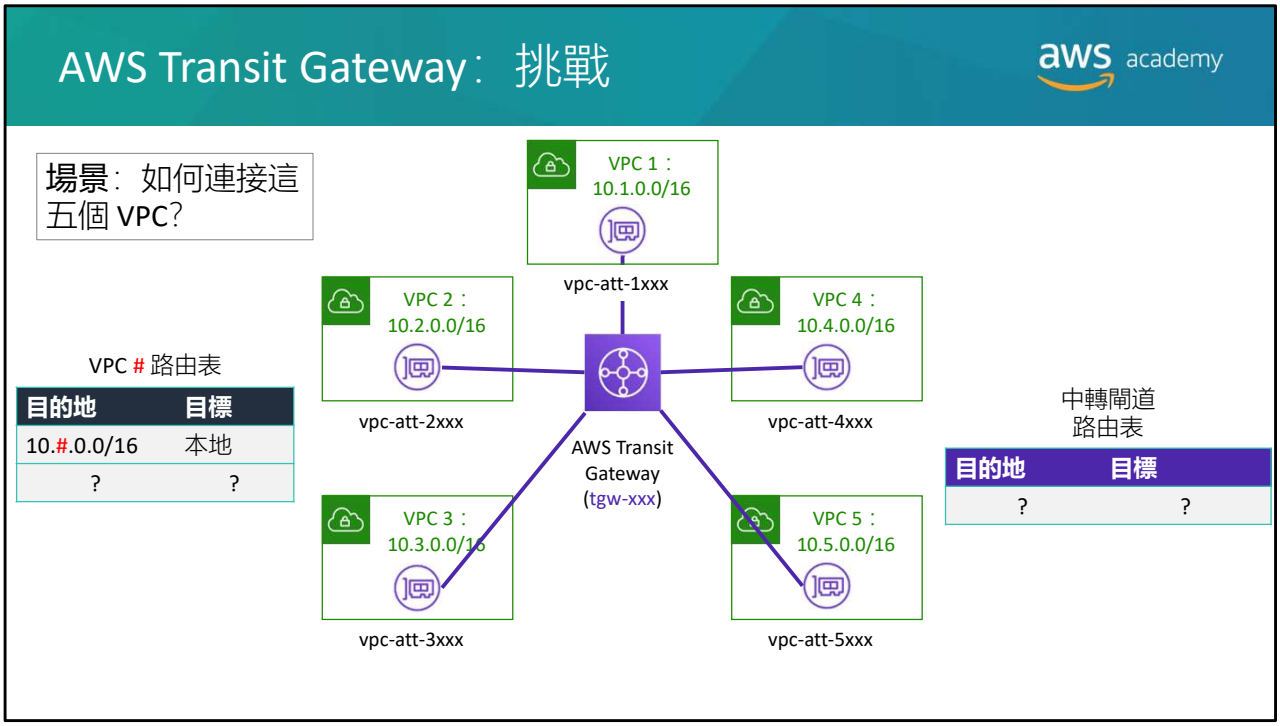


您可以根據需要創建多個針對特定交互的中轉閘道路由表來定向流量。

在此示例中，第二個路由表將來自 VPN 的入站流量定向到連接到中轉閘道的其中一個 VPC。

活動： AWS Transit Gateway

您現在將完成以下活動：AWS Transit Gateway。

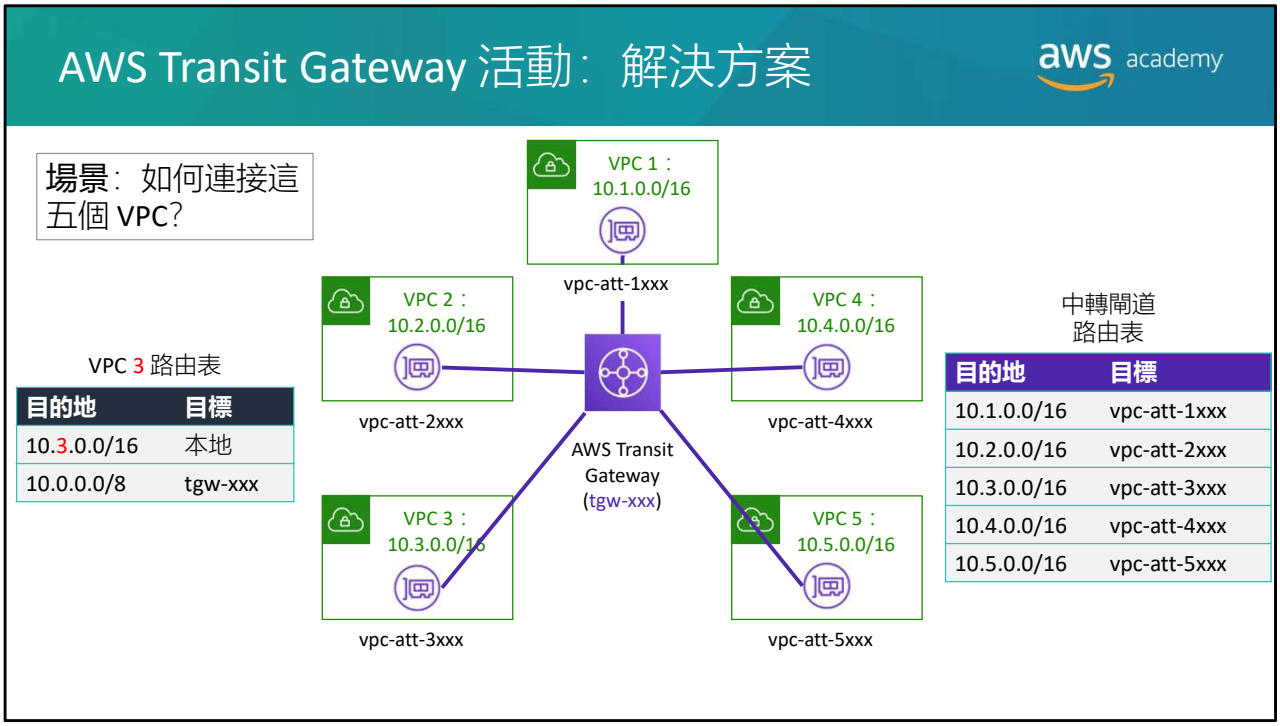


在本活動中，您有五個要通過 AWS Transit Gateway 相互連接的 VPC。

回答以下問題：

- 為了實現完全連接，需要向每個 VPC 路由表添加哪些路由?
- 為了實現完全連接，需要向中轉閘道路由表添加哪些路由?

AWS Transit Gateway 活動：解決方案



為了實現完全連接，必須在每個 VPC 路由表中添加哪些路由？

- 請參閱為 VPC 3 路由表提供的解決方案。您要以類似方式更新其他 VPC 路由表。

為了實現完全連接，必須向中轉閘道路由表添加哪些路由？

- 為每個 VPC 附件添加路由，以將流量定向到每個 VPC。

第 5 節要點

- 借助 AWS Transit Gateway，您能夠將 VPC 和本地網路連接到單個網關（稱為中轉閘道）
- AWS Transit Gateway 使用輪輻模型來簡化 VPC 管理並降低運營成本

本模組中這節內容的要點包括：

- 借助 AWS Transit Gateway，您能夠將 VPC 和本地網路連接到單個閘道（稱為中轉閘道）
- AWS Transit Gateway 使用輪輻模型來簡化 VPC 管理並降低運營成本

模組 7：連接網路

第 6 節：將 VPC 連接到受支援的 AWS 服務

aws academy

介紹第 6 節：將 VPC 連接到受支援的 AWS 服務。

VPC 終端節點

- 讓您能夠將 VPC 以私密方式連接到受支援的 AWS 服務和由 AWS PrivateLink 提供支援的 VPC 終端節點服務
- 支援 VPC 和其他服務之間的流量而不脫離 Amazon 網路
- 無需互聯網閘道、VPN、網路位址轉譯 (NAT) 設備或防火牆代理
- 可水準擴展、冗餘且高度可用

借助 *VPC 終端節點*，您能夠將 VPC 以私密方式連接到受支援的 AWS 服務和由 AWS PrivateLink 提供支援的 VPC 終端節點服務。由 AWS PrivateLink 提供支援的 VPC 終端節點服務包括一些 AWS 服務、由其他 AWS 客戶和 AWS 合作夥伴網路 (APN) 合作夥伴在其自己的 VPC 中託管的服務（稱為*終端節點服務*）以及受支援的 AWS Marketplace APN 合作夥伴服務。

VPC 終端節點不需要互聯網閘道、NAT 設備、VPN 連接或 DX 連接。VPC 中的實例無需公有 IP 位址便可與服務中的資源通信。VPC 和其他服務之間的流量不會脫離 Amazon 網路。

終端節點是虛擬裝置。它們是水準擴展、冗餘且高度可用的 VPC 組件。通過終端節點，VPC 中的實例與服務之間可以進行通信，而不會對網路通信帶來可用性風險或頻寬約束。

有兩種類型的 VPC 終端節點：

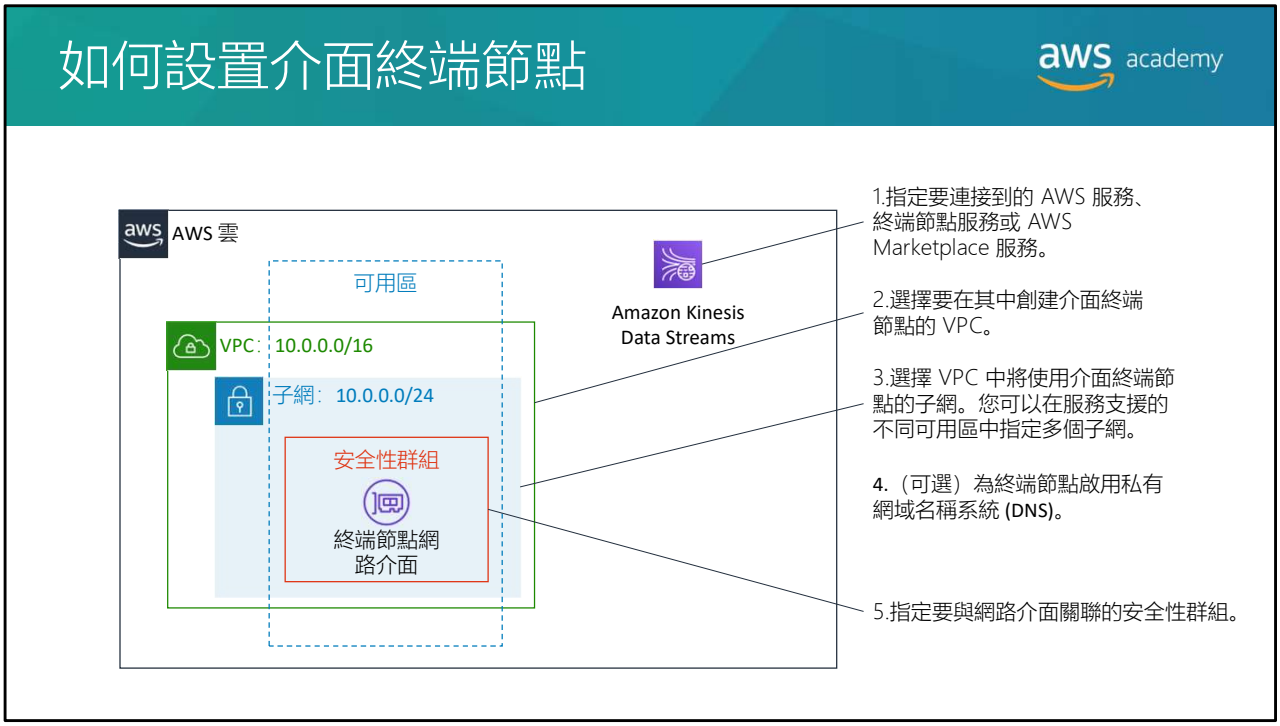
- *介面終端節點*是具有私有 IP 位址的彈性網路介面。此 IP 位址作為發往受支援服務的流量的入口點。介面終端節點使您能夠連接到由 AWS PrivateLink 提供支援的服務。服務的所有者是*服務提供商*。作為創建介面終端節點的委託人，您是*服務使用者*。有關介面終端節點支援的服務的完整清單，請參閱 VPC 終端節點 – 介面終端節點。

- *閘道終端節點*是一個您在路由表中指定為某個路由的目標的閘道。該路由適用於發往受支援的 AWS 服務的流量。閘道終端節點支援 Amazon S3 和 Amazon DynamoDB。

使用閘道 VPC 終端節點不會產生資料處理費用或按小時計算的費用。但是，我們將按照 VPC 終端節點在沒個可用區中保持已預置狀態的小時數收費，無論其與服務的關聯狀態如何。當您刪除 VPC 終端節點時，我們就會停止這種按小時計費。如果終端節點服務擁有者拒絕讓您的 VPC 終端節點與其服務連接，我們也會停止按小時計費。該服務隨後會被刪除。有關介面終端節點定價的更多資訊，請參閱 AWS PrivateLink 定價。

要瞭解有關 VPC 終端節點的更多資訊，請參閱 AWS 文檔中的 VPC 終端節點。

如何設置介面終端節點



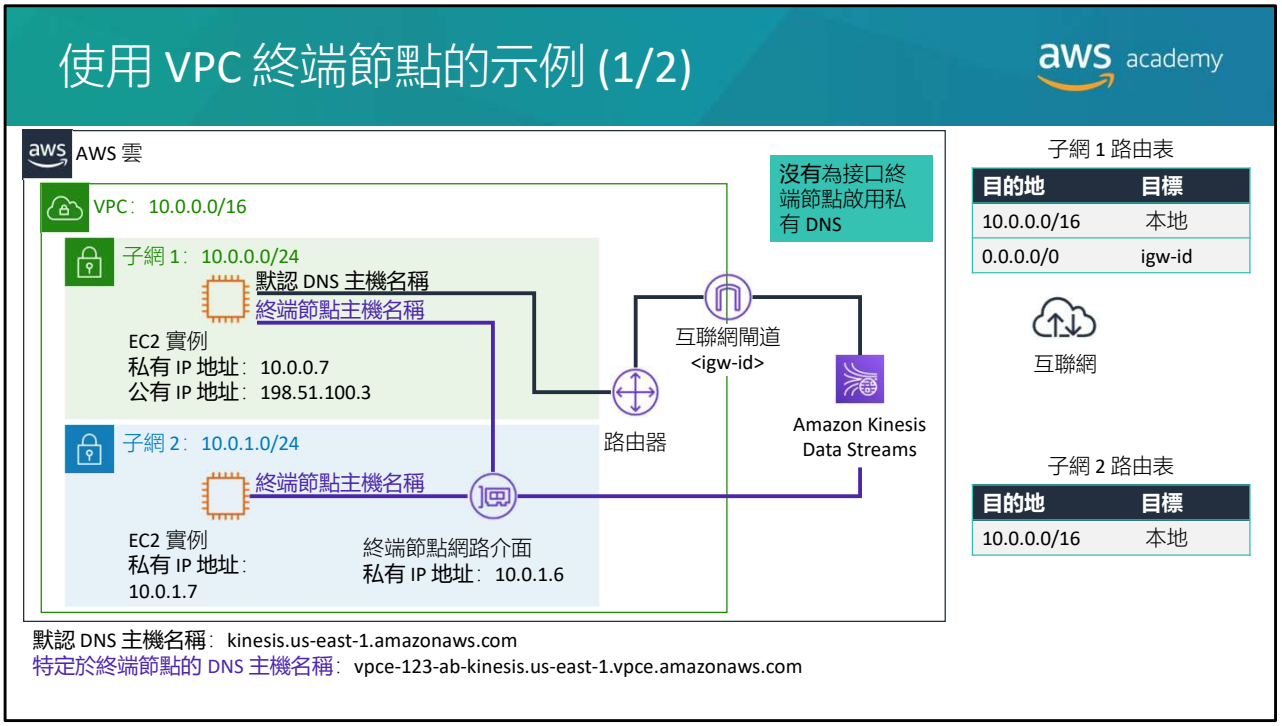
要設置介面終端節點，請從 Amazon VPC 控制台執行以下常規步驟：

1. 指定要連接的 AWS 服務、終端節點服務或 AWS Marketplace 服務的名稱。
2. 選擇要在其中創建介面終端節點的 VPC。您可以在服務支援的不同可用區中指定多個子網。這樣做有助於確保介面終端節點在遇到可用區故障時能夠恢復。在此情況下，將在您指定的每個子網中創建一個終端節點網路介面。
3. 選擇 VPC 中將使用介面終端節點的子網。當您在 VPC 中為某項服務創建介面終端節點時，將在所選子網中創建*終端節點網路介面*。終端節點網路介面具有私有 IP 位址，可用作發往該服務的流量的入口點。
4. （可選）為終端節點啟用私有網域名稱系統 (DNS)。這樣一來，您可以使用它的預設 DNS 主機名稱向服務發出請求（預設情況下，已針對為 AWS 服務和 AWS Marketplace 合作夥伴服務創建的終端節點啟用）。
5. 指定要與網路介面關聯的安全性群組。安全性群組規則將控制從 VPC 中的資源發送到終端節點網路介面的流量。如果您未指定安全性群組，將使用 VPC 的默認安全性群組。

服務無法通過終端節點向您 VPC 中的資源發起請求。終端節點僅針對從您 VPC 中的資源發起的流量返回回應。

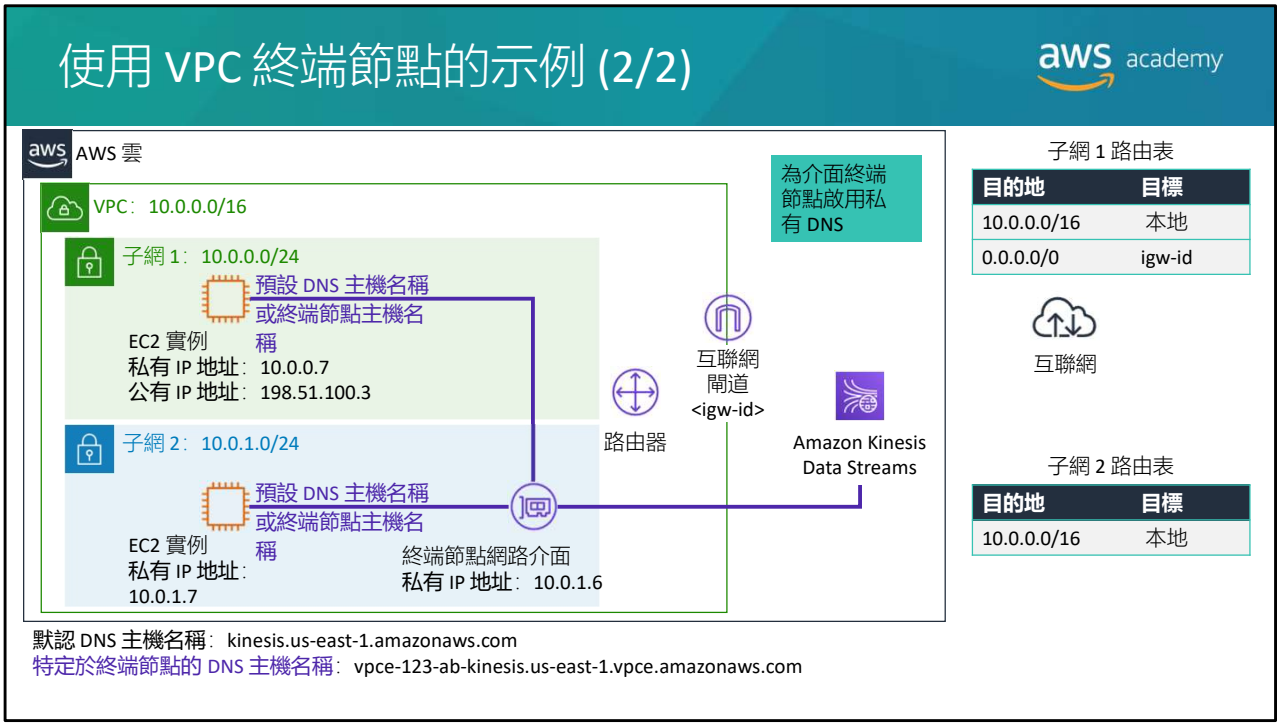
有關如何創建介面終端節點的詳細資訊，請參閱：

- 創建介面終端節點
- 什麼是介面 VPC 終端節點，如何為我的 VPC 創建介面終端節點？



當您創建介面終端節點時，將生成您可用於與服務通信的特定於終端節點的 DNS 主機名稱。對於 AWS 服務和 AWS Marketplace 合作夥伴服務，私有 DNS 選項（預設啟用）會將私有託管區域與您的 VPC 相關聯。託管區域包含用於服務的預設 DNS 名稱的記錄集（例如，kinesis.us-east-1.amazonaws.com），該記錄集解析為您的 VPC 中終端節點網路介面的私有 IP 位址。這樣您的應用程式就能夠使用服務的預設 DNS 主機名稱而不是特定於終端節點的 DNS 主機名稱來向服務發出請求。這允許您的現有應用程式通過介面終端節點向 AWS 服務發出請求，而無需任何配置更改。

在此示例中，子網 2 中有一個針對 Amazon Kinesis Data Streams 的介面終端節點和一個終端節點網路介面。**尚未**為介面終端節點啟用私有 DNS。任一子網中的實例都可以使用特定於終端節點的 DNS 主機名稱通過介面終端節點向 Amazon Kinesis Data Streams 發送請求。子網 1 中的實例可以使用服務的預設 DNS 主機名稱，通過 AWS 區域中的公有 IP 位址空間與 Amazon Kinesis Data Streams 通信。



在此示例中，已為終端節點啟用私有 DNS。任一子網中的實例都可以使用預設的 DNS 主機名稱或特定於終端節點的 DNS 主機名稱，通過介面終端節點向 Amazon Kinesis Data Streams 發送請求。

有關此示例的更多資訊，請參閱接口終端節點的私有 DNS。

第 6 節要點

- VPC 終端節點使您能夠將 VPC 以私密方式連接到受支援的 AWS 服務和由 AWS PrivateLink 提供支援的 VPC 終端節點服務
- VPC 終端節點不需要互聯網閘道、NAT 設備、VPN 連接或 AWS Direct Connect 連接
- VPC 終端節點有兩種類型：接口終端節點和網關終端節點

本模組中這節內容的要點包括：

- VPC 終端節點使您能夠將 VPC 以私密方式連接到受支援的 AWS 服務和由 AWS PrivateLink 提供支援的 VPC 終端節點服務
- VPC 終端節點不需要互聯網閘道、NAT 設備、VPN 連接或 AWS Direct Connect 連接
- VPC 終端節點有兩種類型：介面終端節點和閘道終端節點

模組 7：連接網路

模組總結

現在來回顧下本模組，並對知識測驗和對實踐認證考試問題的討論進行總結。

模組總結

總體來說，您在本模組中學習了如何：

- 描述如何將本地網路連接到 AWS 雲
- 描述如何在 AWS 雲中連接 VPC
- 使用 VPC 對等連接在 AWS 雲中連接 VPC
- 描述如何在 AWS 雲中擴展 VPC
- 描述如何將 VPC 連接到受支援的 AWS 服務

總體來說，您在本模組中學習了如何：

- 描述如何將本地網路連接到 AWS 雲
- 描述如何在 AWS 雲中連接 VPC
- 使用 VPC 對等連接在 AWS 雲中連接 VPC
- 描述如何在 AWS 雲中擴展 VPC
- 描述如何將 VPC 連接到受支援的 AWS 服務

完成知識測驗

現在可以完成本模組的知識測驗。

樣題

aws academy

一個在 Amazon Elastic Compute Cloud (Amazon EC2) 實例上運行的應用程式處理存儲在 Amazon Simple Storage Service (Amazon S3) 上的敏感資訊。此資訊可以通過互聯網訪問。安全團隊擔心 Amazon S3 的互聯網連接會帶來安全風險。

哪種解決方案可以解決這個安全擔心？

A. 通過互聯網閘道訪問資料。
B. 通過 VPN 連接訪問資料。
C. 通過 NAT 閘道訪問資料。
D. 通過 Amazon S3 的 VPC 終端節點訪問資料。

請查看答案選項，並根據之前突出顯示的關鍵字排除錯誤選項。

正確答案是 D： *“通過 Amazon S3 的 VPC 終端節點訪問資料。”* 選項 A（“通過互聯網閘道訪問資料”）可以排除，因為將 Amazon S3 中存儲的資料公開會帶來安全風險。選項 B（“通過 VPN 連接訪問資料”）也可以排除，因為您無法通過 VPN 連接到 Amazon S3。雖然選項 C（“通過 NAT 閘道訪問資料”）也沒錯，但您只能選擇一個正確的答案。選項 D 更合適，因為其無需額外的成本，也沒有性能限制。

其他資源

- AWS re:Invent 2018 視頻：AWS VPN 解決方案
- AWS 知識中心視頻：如何使用 Amazon VPC 創建 VPN？
- 如何通過 AWS Direct Connect 配置 VPN？
- AWS re:Invent 2019 視頻：從一個到多個：Amazon VPC 設計的演進
- 構建可擴展的安全多 VPC AWS 網路基礎設施白皮書
- AWS 知識中心視頻：什麼是 AWS 對等連接？
- AWS re:Invent 2019 視頻：適用於多 VPC 的 AWS Transit Gateway 參考架構
- AWS 知識中心視頻：什麼是介面 VPC 終端節點，如何為我的 VPC 創建介面終端節點？

如果您想瞭解有關本模組所涵蓋主題的更多資訊，下面這些其他資源可能會有所幫助：

- AWS re:Invent 2018 視頻：AWS VPN 解決方案
- AWS 知識中心視頻：如何使用 Amazon VPC 創建 VPN？
- 如何通過 AWS Direct Connect 配置 VPN？
- AWS re:Invent 2019 視頻：從一個到多個：Amazon VPC 設計的演進
- 構建可擴展的安全多 VPC AWS 網路基礎設施白皮書
- AWS 知識中心視頻：什麼是 AWS 對等連接？
- AWS re:Invent 2019 視頻：適用於多 VPC 的 AWS Transit Gateway 參考架構
- AWS 知識中心視頻：什麼是介面 VPC 終端節點，如何

感謝您完成本模組的學習。