AWS 白皮書

建置可擴展且安全的多個 VPC AWS 網路基礎設施

建置可擴展且安全的多個 VPC AWS 網路基礎設施: AWS 白皮書

Table of Contents

摘要 1
摘要 1
簡介 2
VPC 到 VPC 的連線能力 4
VPC 對等互連 4
傳輸 VPC 解決方案 5
轉換閘道 5
Transit Gateway 與傳輸 VPC 的比較 6
Transit Gateway 與 VPC 對等互連的比較 6
AWS PrivateLink 7
Amazon VPC 共享 7
混合連線 9
VPN 9
Direct Connect 10
網際網路的集中式輸出 12
VPC 到 VPC 和內部部署到 VPC 流量的集中式網路安全 15
DNS 17
混合 DNS 17
集中存取 VPC 私有端點 19
介面 VPC 端點 19
結論 21
作者群 22
文件歷史記錄 23
聲明 24

建置可擴展且安全的多個 VPC AWS 網路基礎設施

出版日期：2020 年 6 月 10 日 (文件歷史記錄)

摘要

AWS 客戶通常會依靠數百個帳戶和 VPC 來分割其工作負載並擴大其使用量。這種規模級別往往會在資源共享、VPC 間連線及內部部署到 VPC 連線上帶來挑戰。

本白皮書說明了在大型網路中使用 AWS 服務 (如 Amazon VPC、AWS Transit Gateway、AWS PrivateLink 和 AWS Direct Connect 閘道) 建立可擴展且安全之網路架構的最佳實務。其展現了用於管理不斷增長之基礎設施的解決方案 — 確保可擴展性、高可用性和安全性，同時保持低成本。

簡介

AWS 客戶首先在單一 AWS 帳戶中建置資源，該帳戶代表一個管理邊界，其對許可、成本和服務進行劃分。但是，隨著客戶組織的發展，需要對服務進行更為仔細的劃分，以監控成本、控制存取並提供更輕鬆的環境管理。多帳戶解決方案藉由為組織內的 IT 服務和使用者提供特定帳戶來解決這些問題。AWS 提供多種工具來管理和設定此基礎設施，包括 AWS 登陸區域 和 AWS Control Tower。

圖 1 – 登陸區域帳戶結構

AWS 登陸區域和 AWS Control Tower 會自動設定和整合多個 AWS 服務，以提供基準、高度控制的多帳戶環境，包括身分和存取管理 (IAM)、治理、資料安全、網路設計和日誌記錄。

圖 1 中的 AWS 登陸區域解決方案包括四個帳戶：AWS Organizations 帳戶 (用來管理組態並存取 AWS 登陸區域受管帳戶)、共享服務帳戶 (用來建立基礎設施共享服務，如目錄服務)、日誌封存帳戶 (集中登錄到 S3 儲存貯體)和安全帳戶 (可供公司的安全和合規性團隊在輻射帳戶發生事故時稽核或執行緊急安全作業)。

本白皮書介紹了由管理 AWS 基礎設施的聯網團隊所擁有的網路服務帳戶。帳戶的聯網服務和網路基礎設施為所有帳戶和 VPC 以集中方式共享 (類似於軸輻設計)。此設計可更為完善地管理您的登陸區域，並透過移除在每個輻射 VPC 和帳戶中複製網路服務的需要，協助降低成本。

> **Note**
>
> 於本白皮書中，「登陸區域」是用來部署工作負載的可擴展、安全和高性能的多帳戶/多 VPC 設定的廣義術語。此設定可使用任何工具進行建置。

大多數客戶會從幾個 VPC 開始部署其基礎設施。客戶擁有的 VPC 數量通常與其帳戶數量、使用者和暫存環境 (產品、開發、測試等) 相關。隨着雲端使用量的增長，客戶與之互動的使用者、業務單位、應用程式和區域數量也會增加，從而建立新的 VPC。

隨着 VPC 數量的增長，跨 VPC 管理對於客戶雲端網路的作業變得至關重要。本白皮書含括了跨 VPC 和混合連線中三個特定領域的最佳實務：

- 網路連線 – 大規模互連 VPC 和內部部署網路。
- 網路安全 – 建置用於存取網際網路和端點 (如 NAT 閘道、VPC 端點和 AWS PrivateLink) 的集中式輸出點。

- DNS 管理 – 於登陸區域和混合 DNS 內解析 DNS。

VPC 到 VPC 的連線能力

客户可使用兩種不同的 VPC 流程模式，來設定多個 VPC 環境：多對多環境或軸輻式環境。在多對多方法中，每個 VPC 之間的流量在每個 VPC 之間皆為單獨管理。在軸輻式模型中，所有 VPC 間流量皆流經一個中央資源，該資源會根據既定規則路由傳送流量。

主題

- VPC 對等互連
- 傳輸 VPC 解決方案
- 轉換閘道
- AWS PrivateLink
- Amazon VPC 共享

VPC 對等互連

連接兩個 VPC 的最簡單方法是使用 VPC 對等互連。在此設定中，連線會啟用 VPC 之間的完整雙向連線能力。 此對等連線可用來路由 VPC 之間的流量。 跨帳戶和 AWS 區域的 VPC 亦可對等互連在一起。VPC 對等互連只會在透過連線傳輸流量時產生成本 (此並無每小時的基礎設施費用)。

VPC 對等互連為點對點連線能力，且其不支援傳遞路由。例如，若您在 VPC A 和 VPC B 之間及 VPC A 和 VPC C 之間有 VPC 對等互連，則 VPC B 中的執行個體無法經由 VPC A 傳輸至 VPC C。如要在 VPC B 和 VPC C 之間路由封包，您需要建立一個直接 VPC 對等連線。

在規模上，當您擁有 10 到 100 個 VPC 時，將其與對等互連會產生一個 100 到 1000 個對等連線的網格，此將難以管理和擴展。每個 VPC 的限制上限為 125 個對等連接數。

圖 2 – 使用 VPC 對等互連進行網路設定

若您使用是 VPC 對等互連，則必須與每個 VPC 建立內部部署連線能力 (VPN 和/或 Direct Connect)。VPC 中的資源無法使用對等 VPC 的混合連線能力至內部部署 (圖 2)。

當某個 VPC 中的資源必須與另一個 VPC 中的資源進行通訊、這兩個 VPC 的環境受到控制和保護，且要連接的 VPC 數量少於 10 (可讓每個連線進行單獨管理) 時，最好使用 VPC 對等互連。與 VPC 間連線的其他選項相比，VPC 對等互連提供了最低的總體成本。

傳輸 VPC 解決方案

傳輸 VPC 可透過引入用於 VPC 間連線的軸輻設計來解決 VPC 對等互連的一些缺點。於傳輸 VPC 網路中，一個中央 VPC (軸心 VPC) 經由一個 VPN 連接 (通常利用 IPsec 上的 BGP)，與其他每個 VPC (輻射 VPC) 連線。中央 VPC 包含執行軟體設備的 EC2 執行個體，這些設備使用 VPN 覆蓋將傳入流量路由至其目的地 (圖 3)。傳輸 VPC 對等互連具有下列優點：

- 使用覆蓋 VPN 網路啟用傳遞路由，從而實現更簡單的軸輻設計。
- 在軸心傳輸 VPC 中的 EC2 執行個體上使用第三方廠商軟體時，可利用圍繞進階安全性 (第 7 層防火牆/IPS/ID) 的廠商功能。若客戶在內部部署使用相同的軟體，其將會受益於統一的操作/監控體驗。

圖 3 – 以 Cisco CSR 傳輸 VPC

傳輸 VPC 有其自身的挑戰，例如執行虛擬設備的成本較高、每個 VPC 的輸送量有限 (每個 VPN 通道高達 1.25 Gbps)，及額外的組態和管理開銷 (客戶必須管理 EC2 執行個體的可用性和備援)。

轉換閘道

AWS Transit Gateway 提供了一個軸輻設計，用於連接 VPC 和內部部署網路以作為全受管服務，而無需您佈建如 Cisco CSR 等虛擬設備。無須 VPN 覆蓋，而 AWS 管理高可用性和可擴展性。

Transit Gateway 可使客戶連接數千個 VPC。您可將所有混合連線 (VPN 和 Direct Connect 連線) 連接至單一 Transit Gateway — 可將您組織的整個 AWS 路由組態進行整合並控制於一處 (圖 4)。Transit Gateway 使用路由表控制如何於所有連線輻射網路之間路由流量。此軸輻模型簡化了管理並降低了運營成本，因 VPC 僅能連線至 Transit Gateway，以取得至連線網路的存取權限。

圖 4 — 使用 AWS Transit Gateway 的軸輻設計

Transit Gateway 是一種區域資源，可連接相同 AWS 區域內的數千個 VPC。您可為每個區域建立多個 Transit Gateway，但無法對一個 AWS 區域內的 Transit Gateway 進行對等互連，且您可在單一 Direct Connect 連線上連接至最多三個 Transit Gateway，以實現混合連線。基於這些理由，您應將您的架構限制為，僅使用一個 Transit Gateway 連接指定區域中的所有 VPC，並使用 Transit Gateway 路由表在需要時將其隔離。有個有效案例，可建立多個 Transit Gateway，純粹是為了限制不當組態設定的影響範圍。

將組織的 Transit Gateway 置於其網路服務帳戶中。這使管理網路服務帳戶的網路工程師可進行集中管理。使用 AWS Resource Access Manager (RAM) 共享一個 Transit Gateway，用於連接相同區域內 AWS 組織中多個帳戶間的 VPC。 AWS RAM 可讓您輕鬆安全地與任何 AWS 帳戶或在 AWS 組織內共享 AWS 資源。如需詳細資訊，請參閱將 AWS Transit Gateway 連接自動化為中央帳戶中的 transit gateway 部落格文章。

主題

- Transit Gateway 與傳輸 VPC 的比較
- Transit Gateway 與 VPC 對等互連的比較

Transit Gateway 與傳輸 VPC 的比較

與傳輸 VPC 相比，Transit Gateway 具有許多優勢：

- Transit Gateway 抽離維護與數百個 VPC 的 VPN 連接的複雜性。
- Transit Gateway 無需管理和擴展基於 EC2 的軟體設備。AWS 負責管理路由流量所需的所有資源。
- Transit Gateway 透過提供高可用性和備援的多可用區域基礎設施，無需管理高可用性。
- Transit Gateway 將 VPC 間通訊的頻寬提升至每可用區域 50 Gbps 的爆增速度。
- Transit Gateway 將使用者成本簡化為簡單的每小時每 GB 傳輸模式。
- Transit Gateway 透過刪除 EC2 代理和 VPN 封裝來減少延遲。

Transit Gateway 與 VPC 對等互連的比較

Transit Gateway 解決了大規模建立和管理多個 VPC 對等互連所涉及的複雜性。雖然這使 TGW 成為大多數網路架構的良好預設，但 VPC 對等互連仍是個有效的選擇，因為其比 TGW 具有下列優勢：

- 更低的成本 — 使用 VPC 對等互連，您僅需支付數據傳輸費用。除了資料傳輸費用之外，Transit Gateway 還會收取每個連接的小時費用。
- 無頻寬限制 — 使用 Transit Gateway，每個 VPC 連線的最大頻寬 (爆增) 為 50 Gbps。VPC 對等互連並無彙總頻寬。個別的執行個體網路效能限制和流量限制 (置放群組內為 10 Gbps，否則為 5 Gbps) 適用於這兩個選項。僅 VPC 對等互連支援置放群組。
- 延遲 — 與 VPC 對等互連不同，Transit Gateway 是 VPC 之間的額外跳轉。
- 安全群組兼容性 — 引用的安全群組與區域內 VPC 對等互連搭配使用。其目前不適用於 Transit Gateway。

於您的登陸區域設定中，VPC 對等互連可與 Transit Gateway 啟用的軸輻模型結合使用。

AWS PrivateLink

客戶可能希望以只有消費者 VPC 啟動與服務供應商 VPC 連線的方式，將駐留於一個 VPC (服務供應商) 中的服務/應用程式私下公開給 AWS 區域內的其他消費者 VPC。其顯示的一個範例是您私有應用程式可存取服務供應商 API 的能力。

如要使用 AWS PrivateLink，請在 VPC 中為您的應用程式建立 Network Load Balancer，然後建立指向該負載平衡器的 VPC 端點服務組態。接著，服務消費者會對您的服務建立介面端點。這會在您的子網路中建立包含私有 IP 地址的彈性網路介面，用於指定於服務的流量進入點。消費者和服務不需要位於相同 VPC 中。若 VPC 不同，則消費者和服務供應商 VPC 可能具有重疊的 IP 地址範圍。除了建立介面 VPC 端點來存取其他 VPC 中的服務之外，您還可建立介面 VPC 端點，私下透過 AWS PrivateLink 存取受支援的 AWS 服務 (圖 5)。

圖 5 – AWS PrivateLink

於 Transit Gateway、VPC 對等互連，和 AWS PrivateLink 之間的選擇皆取決於連線能力。

AWS PrivateLink — 當您設定了用戶端/伺服器，並希望可讓一個或多個消費者 VPC 單向存取服務供應商 VPC 中的特定服務或一組執行個體時，請使用 AWS PrivateLink。只有消費者 VPC 中的用戶端才可啟動與服務供應商 VPC 中的服務連線。當兩個 VPC 中的用戶端和伺服器具有重疊的 IP 地址時，這也是個不錯的選項，因為 AWS PrivateLink 利用了用戶端 VPC 內的 ENI，如此便不會與服務供應商產生 IP 衝突。您可透過 VPC 對等互連、VPN 和 AWS Direct Connect 存取 AWS PrivateLink 端點。

VPC 對等互連和 Transit Gateway — 當您希望於 VPC 之間啟用第 3 層 IP 連線能力時，請使用 VPC 對等互連和 Transit Gateway。

您的架構將包含這些技術的組合，以滿足不同的使用案例。所有這些服務皆可相互組合和運作。例如，AWS PrivateLink 處理 API 風格的用戶端-伺服器連線、用於處理直接連線要求的 VPC 對等互連，其中可能仍需要區域內的置放群組或需要區域間連線，和 Transit Gateway 可大規模簡化 VPC 連線，以及用於混合連線的邊緣整合。

Amazon VPC 共享

當團隊之間的網路隔離無需由 VPC 擁有者嚴格管理，但帳戶級別的使用者和許可必須嚴格管理時，共享 VPC 非常有用。使用共享 VPC，多個 AWS 帳戶可於共享、集中管理的 Amazon VPC 中建立其應用程式資源 (如 Amazon EC2 執行個體)。於此模型中，擁有 VPC (擁有者) 的帳戶會和其他帳戶 (參與

者) 共用一個或多個子網路。共用子網路後，參與者可以檢視、建立、修改及刪除與其共用之子網路中的應用程式資源。參與者無法檢視、修改或刪除屬於其他參與者或 VPC 擁有者的資源。共享 VPC 中資源之間的安全性使用安全群組和子網路 ACL 進行管理。

VPC 共享優勢：

- 簡化的設計 — VPC 間連線無復雜性
- 較少的受管 VPC
- 網路團隊和應用程式擁有者之間的職責分工
- 更好的 IPv4 地址利用率
- 更低的成本 — 屬於相同可用區域內不同帳戶的執行個體之間不收取數據傳輸費用

注意：當您與多個帳戶共享一個子網路時，您的參與者應該有一定程度的合作，因為其共享 IP 空間和網路資源。如有必要，您可以選擇為每個參與者帳戶共享不同的子網路。每個參與者一個子網路可讓網路 ACL 提供除安全群組之外的網路隔離。

大多數客户架構將包含多個 VPC，其中許多 VPC 將與兩個或多個帳戶共享。Transit Gateway 和 VPC 對等互連可用來連接共享 VPC。例如，假設您有 10 個應用程式。每個應用程式都需要其自己的 AWS 帳戶。應用程式可分為兩個應用程式組合 (相同組合中的應用程式具有相似的聯網要求，「行銷」中的應用程式 1-5 和「銷售」中的應用程式 6-10)。

每個應用程式組合可具有一個 VPC (總共兩個 VPC)，且 VPC 與該組合內的不同應用程式擁有者帳戶共享。應用程式擁有者將應用程式部署至其各自的共享 VPC 中 (於此情況下，在不同的子網路中使用 NACL 進行網路路由分隔和隔離)。兩個共享 VPC 透過 Transit Gateway 進行連接。利用此設定，您可以從必須連接 10 個 VPC 到僅連接 2 個 (圖 6)。

圖 6 — 範例設定 — 共享 VPC

> **Note**
>
> VPC 共享參與者無法於共享子網路中建立所有的 AWS 資源。如需詳細資訊，請參閱 Amazon VPC 限制。

混合連線

本節著重於雲端資源與內部部署資料中心的安全連接。啟用混合連線的方法有兩種：

1. 一對一連線 — 在此設定中，將為每個 VPC 建立 VPN 連接和/或 Direct Connect 私有 VIF。這是利用虛擬私有閘道 (VGW) 來完成。此選項非常適合少量 VPC，但隨著客戶擴展其 VPC，管理每個 VPC 的混合連線可能會變得困難。
2. 邊緣整合 — 在此設定中，客户在單一端點上為多個 VPC 整合混合 IT 連線。所有 VPC 共享這些混合連線。這是利用 AWS Transit Gateway 和 Direct Connect 閘道來完成的。

主題

- VPN
- Direct Connect

VPN

圖 7 — AWS VPN 終止選項

有三種方法可將 VPN 設定至 AWS：

1. 在 Transit Gateway 上整合 VPN 連線 – 此選項使用 Transit Gateway 上的 Transit Gateway VPN 連接。Transit Gateway 支援 Site-to-Site VPN 的 IPsec 終止。客户可以建立 Transit Gateway 的 VPN 通道，並可存取與其連接的 VPC。Transit Gateway 支援靜態和 BGP 型動態 VPN 連接。Transit Gateway 還支援 VPN 連接上的相等成本多重路徑 (ECMP)。每個 VPN 連接的輸送量最大為 1.25-Gbps，啟用 ECMP 可讓您跨 VPN 連接彙總輸送量。於此選項中，您將為 Transit Gateway 定價和 AWS VPN 定價付費。我們建議使用此選項進行 VPN 連線。如需詳細資訊，請參閱 AWS VPN 概觀。
2. 終止 EC2 執行個體上的 VPN – 當客戶需要特定廠商軟體功能集 (如 Cisco DMVPN 或 GRE)，或其希望跨多種 VPN 部署保持操作一致性時，客戶可於邊緣情況下利用此選項。您可利用傳輸 VPC 設計進行邊緣整合，但務必記住，傳輸 VPC 的 VPC 到 VPC 連線部分的所有關鍵注意事項皆適用於混合 VPN 連線。您負責管理高可用性，並支付 EC2 執行個體成本及任何廠商軟體授權。
3. 終止虛擬私有閘道 (VGW) 上的 VPN — 此選項支援一對一連線設計，您可在其中為每個 VPC 建立一個 VPN 連接 (由一對備援 VPN 通道組成)。這是開始使用 VPN 連線至 AWS 的絕佳方式，但隨著您擴展 VPC 的數量，利用 Transit Gateway 的邊緣整合設計最終將成為更好的選項。至 VPC 的

VPN 輸送量限制為 1.25 Gbps，不支援 ECMP 負載平衡。從定價的角度來看，您僅需支付 AWS VPN 定價，執行 VGW 不收取任何費用。如需詳細資訊，請參閱 AWS VPN 定價和虛擬私有閘道上的 AWS VPN。

Direct Connect

雖然網際網路上的 VPN 是個很好的入門選項，但網際網路連線對於生產流量並不可靠。由於這種不可靠性，許多客戶選擇 AWS Direct Connect，其可於客戶資料中心和 AWS 之間啟用一致、低延遲、高頻寬的專用光纖連線。有四種方法可利用 AWS Direct Connect 來連接 VPC：

圖 8 — 將內部部署資料中心連接至登陸區域的四種方法

- 建立連接至 VPC 之 VGW 的私有虛擬介面 (VIF) — 您可為每個 Direct Connect 連線建立 50 個 VIF，可讓您最多連接至 50 個 VPC (一個 VIF 提供與一個 VPC 的連線)。每個 VPC 有一個 BGP 對等互連。此設定中的連線僅限於 Direct Connect 位置所在的 AWS 區域。VIF 至 VPC 的一對一映射 (及缺乏全域存取權限) 使此成為存取登陸區域中之 VPC 最不受歡迎的方法。
- 為與多個 VGW 相關聯的 Direct Connect 閘道建立私有 VIF (每個 VGW 皆連接至一個 VPC) — 一個 Direct Connect 閘道可於任何 AWS 帳戶中連接全球 (中國除外) 最多 10 個 VGW。若登陸區域包含少量的 VPC (十個或更少的 VPC) 和/或您需要全域存取權限，此為一個很好的選項。每個 Direct Connect 連線的每個 Direct Connect 閘道皆有一個 BGP 對等互連。Direct Connect 閘道僅用於南北流量流，不允許 VPC 到 VPC 的連線。
- 建立至與 Transit Gateway 關聯的 Direct Connect 閘道的傳輸 VIF – 您可在以 1 Gbps 或更高速度執行的專用或託管 Direct Connect 連線上將 Transit Gateway 關聯至 Direct Connect 閘道。此選項可讓您透過一個 VIF 和 BGP 對等互連，將您的內部部署資料中心連線至跨不同 AWS 區域和 AWS 賬戶的最多三個 Transit Gateway (可連接至 1000 個 VPC)。這是用於大規模連接多個 VPC 之四個選項中最簡單的設定，但您應該注意 Transit Gateway 限制。 一個關鍵限制是，您只能透過傳輸 VIF 通知，從 Transit Gateway 至內部部署路由器的 20 個 CIDR 範圍。利用選項 1 和 2，您會支付 Direct Connect 定價。若為選項 3，您還會支付 Transit Gateway 連接和數據傳輸費用。如需詳細資訊，請造訪 Direct Connect 上的 Transit Gateway 關聯文件。
- 透過 Direct Connect 公有 VIF 建立至 Transit Gateway 的 VPN 連接 – 公有虛擬介面可讓您使用公有 IP 地址存取所有 AWS 公共服務和端點。當您在 Transit Gateway 上建立 VPN 連接時，您會在 AWS 端獲得兩個用於 VPN 終止的公有 IP 地址。這些公有 IP 可透過公有 VIF 達成。您可依據需要，透過公有 VIF 與任意數量的 Transit Gateway 建立任意數量的 VPN 連接。當您在公有 VIF 上建立 BGP 對等互連時，AWS 會將整個 AWS 公有 IP 範圍通知您的路由器。為了確保您只允許某些流

量 (例如，僅允許至 VPN 端點的流量)，建議您在內部部署使用防火牆。此選項可用來在網路層加密您的 Direct Connect。

雖然第三個選項 (將 VIF 傳輸至 Direct Connect 閘道) 似乎是最好的選項，因為其可讓您使用每個 Direct Connect 的單一 BGP 工作階段，在單點 (Transit Gateway) 整合給定 AWS 區域的所有內部部署連線，考慮到選項 3 的一些限制和考慮因素，我們希望客戶同時利用選項 2 和選項 3 來滿足其登陸區域要求。圖 9 說明了一個設定範例，其中傳輸 VIF 用來作為連線至 VPC 的預設方法，私有 VIF 用於邊緣使用案例，其中大量資料必須從內部部署 DC 傳輸至媒體 VPC。私有 VIF 用來避免 Transit Gateway 數據傳輸費用。作為最佳實務，您應該在兩個不同的 Direct Connect 位置至少有兩個連線，以獲得最大備援，總共有四個連線。您可為每個連線建立一個 VIF，共四個私有 VIF 和四個傳輸 VIF。您還可建立 VPN 作為 AWS Direct Connect 連線的備份連線。

圖 9 - 混合連線的範例參考架構

使用網路服務帳戶建立 Direct Connect 資源，以便劃分網路管理邊界。 Direct Connect 連線、Direct Connect 閘道和 Transit Gateway 皆可置放於網路服務帳戶中。為了與您的登陸區域共享 AWS Direct Connect 連線，只需透過 RAM 與其他帳戶共享 Transit Gateway 即可。

網際網路的集中式輸出

當您在登陸區域中部署應用程式時，許多應用程式僅需傳出網際網路存取 (例如，下載程式庫/修補程式/作業系統更新)。您可以使用網路地址轉換 (NAT) 閘道或 EC2 執行個體 (配置了來源 NAT(SNAT)) 作為所有輸出網際網路存取的下一個躍點來達成這一點。內部應用程式駐留於私有子網路中，而 NAT 閘道/EC2 NAT 執行個體駐留於公有子網路中。

使用 NAT 閘道

在每個輻射 VPC 中部署 NAT 閘道可能會相當昂貴，因為您部署的每個 NAT 閘道需依小時支付費用 (請參閱 Amazon VPC 定價)，因此將其集中化可能是個可行的選項。如要集中化，我們在網路服務帳戶中建立一個輸出 VPC，並經由位於此 VPC 中的 NAT 閘道利用 Transit Gateway，路由來自輻射 VPC 的所有輸出流量，如圖 10 所示。

注意：當您使用 Transit Gateway 集中化 NAT 閘道時，您需要支付額外的 Transit Gateway 資料處理費用 — 與在每個 VPC 中執行 NAT 閘道的分散方法相比。在某些邊緣情況下，當您透過 NAT 閘道從 VPC 發送大量資料時，將 NAT 保留於 VPC 中的內部部署以避免 Transit Gateway 資料處理費用可能是更具成本效益的選項。

圖 10 - 使用 Transit Gateway 的集中式 NAT 閘道 (概觀)

圖 11 - 使用 Transit Gateway 的集中式 NAT 閘道 (路由表設計)

於此設定中，輻射 VPC 連接與路由表 1 (RT1) 相關聯，並傳播至路由表 2 (RT2)。我們明確地新增了一個 Blackhole (黑洞) 路由，以禁止兩個 VPC 相互通訊。若要允許 VPC 間的通訊，您可從 RT1 中移除「10.0.0.0/8-> 黑洞」路由項目。這可讓他們經由 NAT 閘道進行通訊。您還可將輻射 VPC 連接傳播至 RT1 (或者，您可使用一個路由表並將所有內容關聯/傳播至該路由表)，使 VPC 之間使用 Transit Gateway 直接流量。

我們在 RT1 中新增一個靜態路由，將所有流量指向輸出 VPC。由於這種靜態路由，Transit Gateway 會透過輸出 VPC 中其 ENI 發送所有網際網路流量。進入輸出 VPC 後，流量會遵循存於這些 Transit Gateway ENI 的子網路路由表中所定義的規則。我們在此子網路路由表中新增一個路由，將所有流量指向 NAT 閘道。NAT 閘道子網路路由表將網際網路閘道 (IGW) 作為下一個躍點。為了使流量迴流，您必須在 NAT 閘道子網路路由表中新增一個靜態路由表項目，將所有輻射 VPC 繫結流量指向 Transit Gateway 作為下一個躍點。

高可用性

如要獲得高可用性，您應該使用兩個 NAT 閘道 (每個可用區域內一個)。於可用區域內，NAT 閘道的可用性 SLA 為 99.9%。針對可用區域內元件故障的備援由 AWS 根據 SLA 協議進行處理。當 NAT 閘道在可用區域中可能無法使用時，流量會在 0.1% 的時間內減少。若一個可用區域完全失效，則該可用區域中的 Transit Gateway 端點和 NAT 閘道將出現故障，且所有流量皆將流經另一個可用區域中的 Transit Gateway 和 NAT 閘道端點。

安全性

您依賴來源執行個體上的安全群組、Transit Gateway 路由表中的黑洞路由，及 NAT 閘道所在子網路的網路 ACL。

可擴展性

NAT 閘道最多可支援至每個唯一目的地的 55,000 個同時連線。從輸送量的角度來看，您受限於 NAT 閘道效能的限制。Transit Gateway 不是負載平衡器，不會在多個可用區域的 NAT 閘道之間平均分配流量。如果可能，Transit Gateway 的流量將保留於可用區域內。若啟動流量的 EC2 執行個體在可用區域 1 中，流量將從輸出 VPC 中相同可用區域 1 的 Transit Gateway 彈性網路介面流出，並將根據彈性網路介面所在的子網路路由表流向下一個躍點 .如需規則的完整清單，請參閱 NAT 閘道規則和限制。

如需詳細資訊，請參閱使用 AWS Transit Gateway 從多個 VPC 建立一個單一網際網路退出點部落格文章。

將 EC2 執行個體用於集中式傳出

使用來自 AWS Marketplace 的軟體型防火牆設備 (在 EC2 上) 作為輸出點類似於 NAT 閘道設定。若您想利用各種廠商產品的第 7 層防火牆/入侵防禦/偵測系統 (IPS/IDS) 功能，可以使用此選項。

於圖 12 中，我們將 NAT 閘道替換為 EC2 執行個體 (在 EC2 執行個體上啟用 SNAT)。此選項有幾個關鍵注意事項：

高可用性

於此設定中，您負責監控 EC2 執行個體、偵測故障，並以備份/備用執行個體替換 EC2 執行個體。大多數 AWS 供應商都為此設定中部署的軟體預先建置了自動化。該自動化可控制下列內容：

- 偵測主要 EC2-1 執行個體的故障
- 變更路由表「路由表 Egx 1」，以便在主要執行個體發生故障時將所有流量指向備份 EC2-2 執行個體。還必須對可用區域 2 中的子網路執行此作業。

圖 12 – 使用 EC2 執行個體和 Transit Gateway 的集中式 NAT

可擴展性

Transit Gateway 不是負載平衡器，不會在兩個可用區域中的執行個體間平均分配流量。如果可能，Transit Gateway 的流量將保留於可用區域內。您受到單一 EC2 執行個體的頻寬功能限制。隨著使用量的增加，您可垂直擴展此 EC2 執行個體。

若您為輸出流量檢查選擇的廠商不支援故障檢測自動化，或若您需要水平擴展，則可使用替代設計。於此設計 (圖 13) 中，我們不會在 Transit Gateway 上為輸出 VPC 建立 VPC 連接，而是建立 IPsec VPN 連接，並建立從 Transit Gateway 到 EC2 執行個體的 IPsec VPN，利用 BGP 來交換路由。

優點

- BGP 處理的流量故障檢測和重新進行路由。無需自動化 VPC 子網路路由表。
- BGP ECMP 可用於跨多個 EC2 執行個體對流量進行負載平衡 — 可以進行橫向擴展。

圖 13 – 使用 EC2 執行個體和 Transit Gateway VPN 的集中式 NAT

關鍵考量

- EC2 執行個體上的 VPN 管理開銷
- Transit Gateway 的頻寬限制為每個 VPN 通道 1.25 Gbps。使用 ECMP Transit Gateway 可以支援高達 50 Gbps 的總 VPN 頻寬。廠商設備的 VPN 和封包處理功能可為一個限制因素。
- 此設計假定 FW EC2 執行個體使用相同的彈性網路介面進行傳入和傳出流量作業。
- 若您啟用跨多個 EC2 執行個體之流量的 ECMP 負載平衡，則必須在 EC2 執行個體上對流量進行 SNAT，以保證傳回流對稱，這表示目的地不會知道真實來源。

VPC 到 VPC 和內部部署到 VPC 流量的集中式網路安全

AWS 提供安全群組和子網路 NACLS，於您的登陸區域內實作網路安全。這些是第 4 層防火牆。在某些狀況下，客戶可能希望在其登陸區域內實作第 7 層防火牆/IPS/IDS，以檢查 VPC 之間或內部部署資料中心與 VPC 之間的流量。這可使用 Transit Gateway 和在 EC2 執行個體上執行的第三方軟體設備來達成。使用圖 14 中的架構，我們可以啟用 VPC 到 VPC 和內部部署到 VPC 的流量經由 EC2 執行個體流動。該設定與我們在圖 12 中所討論過的內容相似，但我們另外移除了路由表 1 中的黑洞路由，允許實習 VPC 流量，並將 VPN 連接和/或 Direct Connect GW 連接，連接至路由表 1 以讓混合流量流動。這使得來自輻射的所有流量在發傳送至目的地之前流向輸出 VPC。您需要輸出 VPC 子網路路由表 (防火牆 EC2 設備所在的位置) 中的靜態路由，以在流量檢查後經由 Transit Gateway 傳送流量至輻射 VPC 和內部部署 CIDR。

> **Note**
>
> 路由資訊不會從 Transit Gateway 動態傳播至子網路路由表中，必須以靜態方式輸入。子網路路由表中有 50 個靜態路由的軟限制。

圖 14 – VPC 到 VPC 和 VPC 到內部部署流量控制

對 EC2 執行個體傳送流量以進行內嵌檢查時的關鍵考量：

- 其他 Transit Gateway 資料處理費用
- 流量必須經過兩個額外的躍點 (EC2 執行個體和 Transit Gateway)
- 頻寬和效能瓶頸的潛在性
- 維護、管理和擴展 EC2 執行個體的其他複雜性：
  - 檢測故障和容錯移轉到備用
  - 跟蹤使用情況和橫向/垂直擴展
  - 防火牆組態、修補程式管理
  - 負載平衡保證對稱流量時，流量的來源網路地址轉換 (SNAT)

您應對經由這些 EC2 執行個體通過的流量具有選擇性。繼續處理的一種方法是定義安全區域並檢查不受信任區域之間的流量。不受信任的區域可為由第三方管理的遠端網站、您不控制/信任的廠商 VPC，或沙盒/dev VPC，其與您的其他環境相比，具有更輕鬆的安全架構。圖 15 允許在受信任網路之間直接

流量流動，同時使用內嵌 EC2 執行個體檢查至/來自不受信任網路的流量。我們於此範例中建立了三個區域：

- 不受信任區域 — 此適用於來自「VPN 到遠端不受信任網站」或第三方廠商 VPC 的任何流量。
- 產品區域 — 這包含來自生產 VPC 和內部部署客戶 DC 的流量。
- 開發區域 — 此包含來自兩個開發 VPC 的流量。

下列為我們為跨區域通訊定義的範例規則：

1. 不受信任的區域產品區域 - 不允許通訊
2. 產品區域開發區域 - 允許經由輸出 VPC 中的 EC2 FW 設備進行通訊
3. 不受信任的區域開發區域 - 允許經由輸出 VPC 中的 EC2 FW 設備進行通訊
4. 產品區域產品區域和開發區域開發區域 – 經由 Transit Gateway 的進行直接通訊

這是一個有三個安全區域的設定，但你可能有更多。您可使用多個路由表和黑洞路由來達成安全隔離和最佳流量。選擇合適的區域取決於您整體的登陸區域設計策略 (帳戶結構、VPC 設計)。您可使用區域啟用 BU、應用程式、環境等之間的隔離。

於此範例中，我們會終止 Transit Gateway 上不受信任的遠端 VPN，並將所有流量傳送至 EC2 上的軟體 FW 設備以進行檢查。或者，您可直接在 EC2 執行個體上終止這些 VPN，而非 Transit Gateway。利用此方法，不受信任的 VPN 流量永遠不會與 Transit Gateway 直接互動。流量中的躍點數減少 1，則您可節省 AWS VPN 成本。如要啟用動態路由交換 (使 Transit Gateway 可經由 BGP 瞭解遠端 VPN 的 CIDR)，防火牆執行個體應經由 VPN 連接至 Transit Gateway。在原生 TGW 連接模型中，您必須在 TGW 路由表中為 VPN CIDE 新增靜態路由，並以下一個躍點作為輸出/安全 VPC。在我們的設定 (圖 15) 中，我們有一個所有流量的輸出 VPC 的預設路由，因此我們不必明確地新增任何特定的靜態路由。利用此方法，您可從全受管的 Transit Gateway VPN 終止端點轉移到自我管理的 EC2 執行個體，進而新增 VPN 管理開銷以及 EC2 執行個體在運算和記憶體方面的其他負載。

圖 15 – 使用 Transit Gateway 進行流量隔離並定義安全區域

DNS

當您在非預設 VPC 中啟動執行個體時，AWS 會為該執行個體提供私有 DNS 主機名稱 (可能是公有 DNS 主機名稱)，此依據您為 VPC 指定的 DNS 屬性，以及執行個體是否含公有 IPv4 地址而定。 當 “enableDnsSupport” 屬性設定為 true 時，您會從 Route 53 Resolver 獲得 VPC 內的 DNS 解析 (+2 IP 偏移到 VPC CIDR)。依預設，Route 53 Resolver 會回應 VPC 網域名稱的 DNS 查詢，例如用於 EC2 執行個體或 Elastic Load Balancing 負載平衡器的網域名稱。利用 VPC 對等互連，一個 VPC 中的主機可將公有 DNS 主機名解析為對等 VPC 中執行個體的私有 IP 地址，前提是啟用了如此執行的選項。此同樣適用於經由 AWS Transit Gateway 連接的 VPC。如需詳細資訊，請參閱「啟用 VPC 對等互連連線的 DNS 解析支援」。

若要將執行個體映射至自訂網域名稱，您可使用 Amazon Route 53 建立自訂 DNS 到 IP 映射記錄。Amazon Route 53 託管區域是一個容器，其中包含您希望 Amazon Route 53 如何回應網域及其子網域的 DNS 查詢資訊。公有託管區域包含可透過公共網際網路解析的 DNS 資訊，而私有託管區域是一個特定實作，僅向已連接至特定私有託管區域的 VPC 提供資訊。在您擁有多個 VPC/帳戶的登陸區域設定中，您可將單一私有託管區域與跨 AWS 帳戶和跨區域的多個 VPC 相關聯。VPC 中的終端主機使用其各自的 Route 53 Resolver IP (+2 偏移 VPC CIDR) 作為 DNS 查詢的名稱伺服器。VPC 中的 Route 53 Resolver 僅接受來自 VPC 內部資源的 DNS 查詢。

混合 DNS

在 AWS 登陸區域設定和內部部署資源之間協調 DNS 解析是混合網路中最關鍵的部分之一。實作混合環境的客戶通常已安裝了 DNS 解析系統，他們想要一個與其當前系統協同工作的 DNS 解決方案。當您將 AWS 區域中 VPC 的 DNS 與您網路的 DNS 整合時，您需要一個 Route 53 Resolver 傳入端點 (用於您轉送至 VPC 的 DNS 查詢) 和一個 Route 53 Resolver 傳出端點 (用於從 VPC 轉送至您網路的查詢)。 如圖 16 所示，您可設定傳出 Resolver 端點，將其從您的 VPC 中 EC2 執行個體收到的查詢轉送至您網路上的 DNS 伺服器。若要轉送選取的查詢，從 VPC 至內部部署，建立 Route 53 Resolver 規則，而該規則指定您想要轉送之 DNS 查詢的網域名稱 (如 example.com)，以及您要轉送查詢至網路上哪個 DNS 解析程式的 IP 地址。對於從內部部署到 Route 53 託管區域的傳入查詢，您網路上的 DNS 伺服器可將查詢轉送至指定 VPC 中的傳入 Resolver 端點。

圖 16 – 使用 Route 53 Resolver 進行混合 DNS 解析

這可讓您的內部部署 DNS 解析程式輕鬆解析 AWS 資源的網域名稱，例如，EC2 執行個體或與該 VPC 相關聯之 Route 53 私有託管區域中的記錄。

不建議在登陸區域的每個 VPC 中建立 Route 53 Resolver 端點。將其集中於中央輸出 VPC 中 (在網路服務帳戶中)。這種方法允許更好的管理性，同時保持較低的成本 (您需為您建立的每個傳入/傳出端點依小時支付費用)。您與登陸區域的其餘部分共享集中式傳入和傳出端點。

傳出解析 — 使用網路服務帳戶編寫解析程式規則 (依據要轉送至內部部署 DNS 伺服器的 DNS 查詢)。使用 Resource Access Manager (RAM)，與多個帳戶共享這些 Route 53 Resolver 規則 (並與帳戶中的 VPC 相關聯)。輻射 VPC 中的 EC2 執行個體可將 DNS 查詢傳送至 Route 53 Resolver，Route 53 Resolver 服務會經由輸出 VPC 中的傳出 Route 53 Resolver 端點將這些查詢轉送至內部部署 DNS 伺服器。 您不需要將輻射 VPC 對等互連至輸出 VPC，或經由 Transit Gateway 將其連線。請勿將傳出解析程式端點的 IP 用來作為輻射 VPC 中的主 DNS。輻射 VPC 應於其 VPC 中使用 Route 53 Resolver (偏移 VPC CIDR)。

圖 17 – 集中輸出 VPC 中的 Route 53 Resolver 端點

傳入 DNS 解析 – 於集中式 VPC 中建立 Route 53 Resolver 傳入端點，並將您登陸區域中的所有私有託管區域與此集中式 VPC 相關聯。如需詳細資料，請參閱建立多個 VPC 與一個私有託管區域的關聯。與 VPC 關聯的多個私有託管區域 (PHZ) 不可重疊。如圖 17 所示，PHZ 與集中式 VPC 的這種關聯將使內部部署伺服器使用集中式 VPC 中的傳入端點為任何私有託管區域 (與中央 VPC 相關聯) 中的任何項目解析 DNS。 如需有關混合 DNS 設定的詳細資訊，請參閱使用 Amazon Route 53 和 AWS Transit Gateway 對混合雲端進行集中式 DNS 管理和適用於 Amazon VPC 的混合雲端 DNS 選項。

集中存取 VPC 私有端點

VPC 端點可讓您將 VPC 私下連接到受支援的 AWS 服務，無需網際網路閘道或 NAT 裝置。您 VPC 中的執行個體不需要公有 IP 地址，即可與此介面端點與 AWS 服務端點通訊。VPC 與其他服務之間的流量都會保持在 AWS 網路的骨幹網路內。當前可佈建兩種類型的端點：介面端點 (採用 AWS PrivateLink 技術) 和閘道端點。閘道端點可以自由佈建，且並無強大的集中化使用案例。

介面 VPC 端點

介面端點包含具私有 IP 地址的一或多個彈性網路介面，做為通往受支援 AWS 服務的流量進入點。當您佈建介面端點時，使用者在端點執行的每個小時都會產生費用。依預設，您在要從中存取 AWS 服務的每個 VPC 中建立一個介面端點。在客戶想要跨多個 VPC 與特定 AWS 服務互動的登陸區域設定中，這可能相當昂貴且難以管理。為避免此種情況，您可於一個集中式 VPC 中託管介面端點。所有輻射 VPC 皆將使用這些集中式端點。

當您對 AWS 服務建立 VPC 端點時，您可啟用私有 DNS。啟用後，該設定會建立一個 AWS 受管 Route 53 私有託管區域 (PHZ)，其允許將公有 AWS 服務端點解析為介面端點的私有 IP。受管 PHZ 僅在具有介面端點的 VPC 內運作。在我們的設定中，當我們希望輻射 VPC 可以解析託管於集中式 VPC 中的 VPC 端點 DNS 時，受管 PHZ 將無法正常運作。如要克服這個問題，請於建立介面端點時停用自動建立私有 DNS 的選項。或者，您可手動建立 Route 53 PHZ，並新增別名記錄，其中完整的 AWS 服務端點名稱指向介面端點，如圖 18 所示。

圖 18 – 手動建立的 PHZ

我們將此私有託管區域與登陸區域內的其他 VPC 相關聯。此組態可讓輻射 VPC 將全服務端點名稱解析為集中式 VPC 中的介面端點。

> **Note**
>
> 如要存取共享私有託管區域，輻射 VPC 中的主機應使用其 VPC 的 Route 53 Resolver IP。介面端點還可透過 VPN 和 Direct Connect 從內部部署網路存取。使用條件轉發規則將全服務端點名稱的所有 DNS 流量傳送至 Route 53 Resolver 傳入端點，其將根據私有託管區域解析 DNS 請求。

於圖 19 中，Transit Gateway 啟用從輻射 VPC 至集中式介面端點的流量。在網路服務帳戶中為其建立 VPC 端點和私有託管區域，並與輻射帳戶中的輻射 VPC 共享。如需有關與其他 VPC 共享端點資訊的

更多詳細資訊，請參閱與 AWS PrivateLink 和 Amazon Route 53 Resolver 整合 AWS Transit Gateway 部落格文章。

注意：分散式 VPC 端點方法 (即每個 VPC 一個端點) 可讓您在 VPC 端點上套用最低權限政策。在集中式方法中，您將在單一端點上套用並管理所有輻射 VPC 存取的政策。隨着 VPC 數量的增加，使用單一政策文件維護最低權限的複雜性可能會增加。單一政策文件還會導致較大的影響範圍。您也受到政策文件大小的限制 (20,480 個字元)。

圖 19 – 集中介面 VPC 端點

結論

隨着您擴展 AWS 的使用量並在 AWS 登陸區域中部署應用程式，VPC 和聯網元件的數量也會隨之增加。本白皮書說明我們如何管理此一不斷增長的基礎設施，以確保可擴展性、高可用性和安全性，同時保持低成本。在利用 Transit Gateway、共享 VPC、AWS Direct Connect、VPC 端點和第三方軟體設備等服務時，做出正確的設計決策變得至關重要。了解每種方法的關鍵考量因素，並從您的需求逆向處理，分析哪個選項或選項組合最適合您。這是非常重要的。

作者群

協力完成這份文件的人員如下：

- Sidhartha Chauhan，Amazon Web Services 解決方案架構師
- Amir Abu-akeel，Amazon Web Services 雲端基礎設施架構師
- Sohaib Tahir，Amazon Web Services 解決方案架構師

文件歷史記錄

如要收到此白皮書更新的通知，請訂閱 RSS 摘要。

update-history-change	update-history-description	update-history-date
小幅度更新	更新了 Transit Gateway 與 VPC 對等互連的比較部分。	2021 年 4 月 2 日
白皮書已更新	更正文本符合說明於圖 7 中的選項。	2020 年 6 月 10 日
小幅度更新	更正文本符合說明於圖 7 中的選項。	2020 年 6 月 10 日
初次出版	白皮書已發佈。	2019 年 11 月 15 日

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品供應與實務，如有變更恕不另行通知，以及 (c) 不構成 AWS 及其關係企業、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶之責任與義務，應受 AWS 協議之約束，且本文件並不屬於 AWS 與其客戶間之任何協議的一部分，亦非上述協議之修改。