對本書的讚譽

對於渴望提升 Azure 生態系知識的讀者，本書是極佳資源，它的範疇涵蓋眾多 Azure 服務，能夠滿足初學者和箇中好手的需求。

Jonah 條理分明地介紹 Azure 組件的細節，以架構剖析搭配實作案例的方式，加深讀者對 Azure 的瞭解，透過技能評量，讓讀者不僅汲取資訊，還能積極參與其中。

本書獨特之處在於清晰說明諸多 Azure 服務之間的關聯，揭開複雜而神秘的術語面紗，以及指引有關服務的使用方式。無庸置疑，Jonah 有一股助人成長的熱情，只要你見過 Jonah，在閱讀這本書時都會感受到這份熱情。

本人衷心推薦本書給想要擴展 Azure 技能的人，它不單單是一本書，更是為讀者進軍雲端運算而打造的完整指南。

—*Mathias Olausson*，*Solidify* 首席技術官、微軟 *MVP*

閱讀本書將會感受一趟 Azure 奇妙之旅，它是適合新手入門、也適合高手去追求的雲端寶藏。本書是一套全方位指南，為初學者指引一條康莊大道，也是經驗豐富的專業人士之隨身寶典。

—*Peter T. Lee*，*Capgemini America* 的管理交付架構師

Azure 是一個巨大平台，初學者可能認為只有專家才有辦法瞭解裡頭的各種組件，Jonah Andersson 則透過本書向一般技術人員精闢介紹完整的服務堆疊，書中內容經過精心安排，易於閱讀，有效傳遞 Azure 和雲端運算的重要知識，以及 Azure 的機器學習和人工智慧能力，讓我這樣的資料專家尤為受益，因此，推薦本書給想從 Azure 獲得實用又具技術性雲端運算知識的專業人員。

—*George Mount*，*Stringfest Analytics* 的資料分析師和講師

在我使用微軟 Azure 時，最想擁有像本書這樣的資源，Jonah 具有以淺顯文字描述複雜技術概念的魔力，讓讀者輕鬆理解深奧的內容，無論初學者還是經驗老到的雲端工程師，本書都能帶領讀者充分瞭解和學習 Azure，並能夠有效使用 Azure 的完整特色和功能。

—*Nikolaos Delis*，*Helo AB* 的資深雲端工程師和雲端倡導者

這是 Jonah 提供給雲端運算工程師的一本關於 Azure 全面而易於理解的教材，條理清晰的內容說明，對初學者而言是好的開始，也是專業人士手上極佳的參考資料。本書提供用例的精闢見解和對複雜概念的淺顯闡釋，使讀者易於理解其中涵義，是一本不可多得的技術資產。不論是初跨入雲端或者想追求更高深技術，本書是瞭解 Azure 基礎的寶貴資源。

—*Priyanshu Jimish*，*Virta Technologies* 的技術傳教士

Jonah Andersson 在本書完整地解析 Azure 核心面向，並深入探討整合、DevOps 和治理的細微差異，對於想要全面掌握 Azure 的工程師來說，這是一本不可多得的好書。

—*Milan Milanović* 博士，首席技術長和微軟 *MVP*

為書撰寫評語，向來都不是簡單任務，尤其是一本如此全面又實用的書。本書含括 Azure 雲端服務、Azure DevOps 發行管線、Azure 網路服務、容器化、人工智慧等實用資訊。

經由本書，Jonah Andersson 展現出雲端運算方面的卓越培訓技巧和知識，為讀者提供廣泛、完整又實用的資訊，讓讀者能夠在微軟 Azure 平台上實作自己的解決方案。

—*Reza Salehi*，顧問和《*Azure Cookbook*》的作者

無論是有經驗的老手或是 Azure 初學者，對於想要深入瞭解 Azure 的人，本書將所需的一切統整在一起，並精心安排內容，會讓學習變得更加輕鬆。

—*Lior Yantovski*，*AT&T* 的 *DevOps* 技術主管

對於想學習微軟 Azure 和雲端概念的人來說，本書是極佳的資源，Jonah Andersson 盡可能含括各項主題，以易於理解的方式提供詳細資訊，它的內容包含入門程度到進階技術的各個層面，讀者可藉由本書內容，在真實專案裡實作雲端解決方案。

—*Sagar Rastogi*，印度塔塔諮詢服務公司的技術架構師

Jonah Carrio Andersson 這份著作是一本不同凡響的指南，為錯綜複雜的 Azure 提供一趟全面而深入的學習之旅，Andersson 在雲端運算、Azure 服務、人工智慧、物聯網和 DevSecOps 等方面充分展現出她的專業知識，為讀者提供極具結構且詳盡的內容探討，對於想要成為 Azure 高手的人，本書是不可或缺的寶典。Jonah 提供清晰闡述和務實見解，初學者和有經驗的專業人士都應該閱讀本書，將有助於他們在專案和職涯發展中充分利用 Azure 的強大威力。

—*Amit Dass*，資料架構經理、微軟認證講師、微軟 *Azure* 資料架構師和首席資料工程師，也是谷歌雲端平台、*Azure* 和 *AWS*（多雲）的認證專業資料工程師和架構師

第 4 章

Azure 的雲端網路服務

> 網路服務對於任何公有雲來說都是不可或缺的，有好的網路才能有效地將地端和雲端環境整合在一起，讓我們依需求調整資源規模，同時保護基礎設施，如此才能配合機構或客戶的需要而靈活地變更資源需求。使用 Azure 網路服務可以實現合規性和安全性，還能節省成本和時間，彈性調適和滿足當前及未來需求。
>
> — Ryan O'Connell，IT 解決方案架構師、Azure MVP、MCT、IT 經理及部落格 RockITWorks 的經營著

第 3 章介紹 Azure 計算服務，以及利用此服務在 Azure 上開發應用系統的優勢。本章將深入探討讀者需要知道的概念，實現計算服務與 Azure 網路服務的結合，讀完本章後，就能在合適的網路服務上使用現有應用程式，也有助於規劃 Azure 的網路拓撲和混合解決方案。

Azure 網路服務

Azure 網路服務是一項完全受管理且可擴縮的網路和連接服務的選項，例如在地端資料中心和雲端建立連接，透過 Azure 網路服務，用戶可以建構安全的虛擬網路（*https://oreil.ly/IJudJ*）、管理應用程式的網路流量、並保護應用系統免受 DDoS 攻擊（*https://oreil.ly/7VH2w*）。利用 Azure 的網路資源還可建立對機構內部資源的安全遠端存取，並使用監控和安全功能與全球網路連線。

登入 Azure 入口網站後，在訂閱服務可以查看網路類別裡所有可新增的 Azure 資源，只需點擊「建立資源」，從 Azure Marketplace（市集；*https://oreil.ly/6I5W7*）選擇「網路」類，便可探索微軟及其合作夥伴提供的網路資源。

Azure 網路服務的類型

Azure 裡有許多網路服務可供選擇，它們是依用途分類。

連接服務

在 Azure 的網路類型裡有許多關於網路連線的服務可供選擇，用戶可利用這些服務來建立連線，例如想將 Azure 資源與地端資源連線，就可以使用 Azure 虛擬網路（VNet）、ExpressRoute、虛擬廣域網路（WAN）、虛擬網路 NAT 閘道、VNet 對等服務、VPN 閘道、Azure 堡壘主機和 Azure DNS。

應用系統防禦保護服務

這類網路資源可用來保護 Azure 裡的應用程式或系統，用戶可以選用 Azure 負載平衡、防火牆、VNet 端點、私有連線和 DDoS 防禦等網路服務。

應用內容傳遞服務

當應用情境涉及應用內容傳遞時，就很適合選擇這類網路資源，包括使用 *Azure CDN*（內容傳遞網路）來交付內容、使用 *Azure Front Door*（前端入口）服務來傳遞全球性的 Web 流量、使用 *Azure Traffic Manager*（流量管理員）提供跨 Azure 地區的全球性流量負載平衡，以及如 Application Gateway（應用程式閘道）和 Internet Analyzer（網際網路流量分析儀）等其他資源。

網路監控服務

可以使用 Network Watcher（網路監看員）、ExpressRoute 監視器、Azure 監視器和 VNet 終端機存取點（TAP）等網路服務的一種或多種組合來監視網路資源。

本章其餘部分會更詳細探討各個網路類型，以便清楚瞭解不同網路服務在不同情境的應用方式。

Azure 網路連接服務

Azure 提供了一套強大、完全受管理且動態的網路基礎設施，能夠支援複雜的網路架構，從建立供大眾存取應用服務的安全網路，到地端基礎設施和雲端之間的混合連接等各式各樣解決方案。

Azure 虛擬網路

在 Azure 基礎設施內建置網路時，Azure 虛擬網路（VNet）扮演著重要角色，它是用戶的 Azure 資源維持在私有網路內的基本元件，讓用戶可以在該網路中安全地進行管理，並藉由網際網路連接到其他外部網路（公共網路和地端網路）。

Azure VNet 比一般的地端和傳統網路更強大，除了具有隔離、高可用性和可擴縮性的優點外，還能讓用戶根據自己的偏好來管理、過濾或轉送網路流量，藉以強化 Azure 資源的安全性。

如圖 4-1 所示，Azure VMs 透過虛擬網路介面卡（VNIC）連接 Azure VNet，其中一部 VM 擁有三張 NIC：**預設網卡**、**網卡** *1* 和**網卡** *2*。

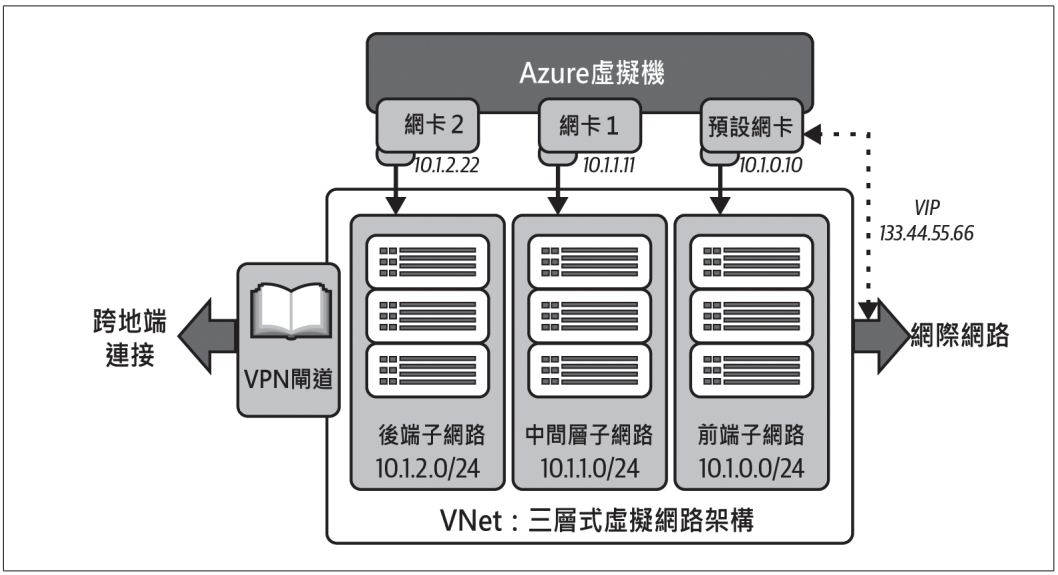

圖 4-1　三層式的 VNet，一部 VM 帶有多張 NIC

Azure 資源必須在內部私有網路、透過網際網路及地端網路之間進行安全通訊，而 Azure VNet 讓這一切成為可能，接著來仔細地看看這些通訊形式。

網際網路通訊

Azure VNet 基本上能夠對外連接網際網路，如果要允許由外對內與 Azure 資源通訊，可以為 Azure 設定公共 IP 位址，或者利用允許外部連線的 Azure 負載平衡器來通訊。

Azure 資源間的通訊

Azure 資源可以透過此虛擬網路與 VNet 對等網路及延伸的虛擬網路之服務端點安全地通訊，例如，可在同一虛擬網路內部署專用的 Azure 資源，如 AKS、Azure Batch、Azure SQL 受控執行個體、微軟 Entra 網域服務、Azure 容器執行個體（ACI）、Azure 函式、Azure App 服務環境和 Azure VM 擴展集。

網路流量轉送和篩選

有許多方式能夠篩選子網路之間的通訊流量，可使用網路安全性群組（NSG；*https://oreil.ly/u98W-*）和應用安全性群組來控制安全規則（入站和出站），以管制和篩選網路流量；另一個不錯的選擇，是使用網路虛擬機（VM），在其中設置防火牆和網路規則，並優化廣域網路連線。在 Azure 市集裡還有一些用於外部服務或在微軟內部的網路設備管理程式（*https://oreil.ly/rPngs*）。

Azure VNet 對等互連

用戶可透過 Azure VNet 對等互連來連接多個**虛擬網路**（VNet），這些對等互連裡的 VMs 會在安全的私有網路裡，透過微軟的基礎設施相互連線及傳送流量，已對等互連的 VNets 可以直接和另一個 VNet 分享資源。

截到目前，Azure 支援 VNet 對等互連和全域 VNet 對等互連，兩者的差別在於全域 VNet 對等互連是橫跨 Azure 地區（region）的虛擬網路，而 VNet 對等互連是同一個 Azure 地區內的虛擬網路。

圖 4-2 呈現兩個虛擬網路 *VNet A* 和 *VNet B* 之間的 VNet 對等互連，兩者裡有多個資源連線。

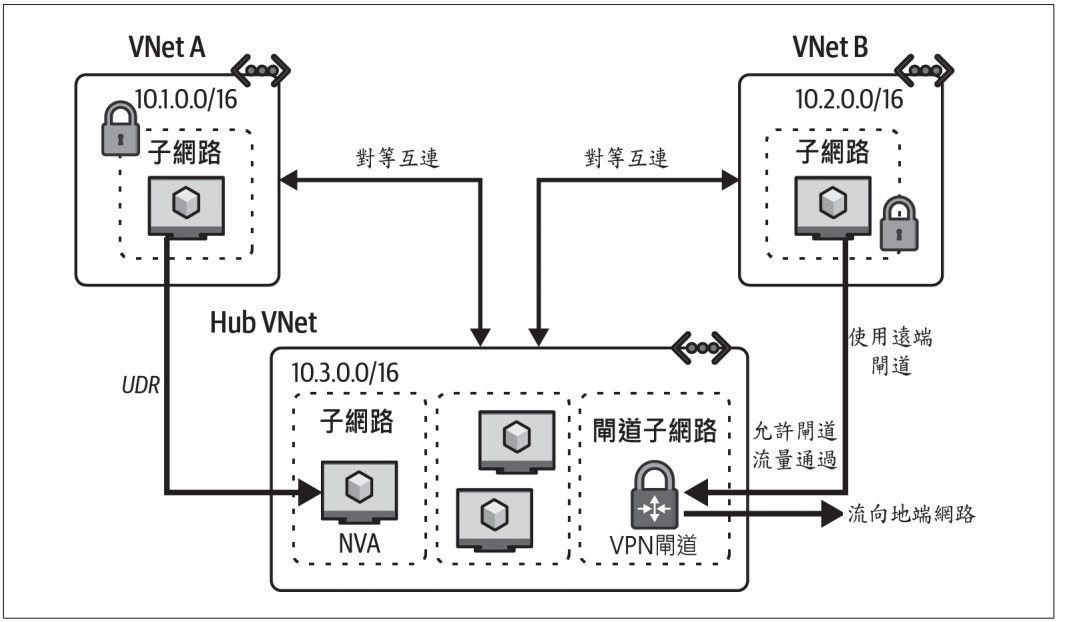

圖 4-2　Azure 的 VNet 對等互連

VNet 對等互連和全域 VNet 對等互連都支援閘道傳輸（gateway transit），這是對等互連網路的一個特性，允許 VNet 利用已建立對等互連的虛擬網路之 *VPN 閘道*進行跨域（cross-premises）連線或 VNet 對 VNet 連線。用戶可以使用 Azure 入口網站、PowerShell，ARM 範本和 Azure CLI 來設定 Azure 閘道，以建立 VPN 閘道傳輸為 VNet 對等網路傳送流量（*https://oreil.ly/XDPmE*）。

VNet 對等互連可能會出現問題，想要排除故障就必須找出問題根因，在進行問題排解時，一般會先考慮虛擬網路是否在同一訂閱中，以及是否位於相同地區或不同地區。想要知道更多有關 VNet 對等互連的問題，請參閱微軟的「針對虛擬網路對等互連問題進行疑難排解」文件（*https://oreil.ly/jjLp_*）。

VNet 對等互連使用 IP 位址，在 Azure 裡有兩種 IP 位址類型：公共 IP 和私有 IP。私有 IP 位址用於同一資源群組內的連接，以及 Azure 資源之間的通訊；公共 IP 位址則能夠讓網際網路上的端點對 Azure 資源進行入站通訊，這類 IP 位址讓 Azure 資源和供公眾使用的 Azure 服務能夠經由網際網路通訊。

微軟文件提供更多關於 IP 服務（*https://oreil.ly/eMMij*）的資訊及 Azure 虛擬網路（*https://oreil.ly/LxZET*）的最佳實作建議。

Azure 虛擬廣域網路

Azure Virtual WAN（虛擬廣域網路）是依靠 Azure 全球網路（*https://oreil.ly/ZW4EO*）的受管網路服務和統一框架，提供網路服務、安全性和路由功能，它的功能包括站對站、點對站的 VPN 連接、ExpressRoute 等。

虛擬 WAN 可協助機構或業務部門連接網際網路和其他 Azure 資源，例如供網路工作者和遠距使用者連線（*https://oreil.ly/xH_E2*），對於喜歡在家工作或遠距工作的人來說，這種網路服務有效又實用，借助 Azure 虛擬廣域網路，還能將地端現有的基礎設施或資料中心搬移到 Azure 上（*https://oreil.ly/BAEQH*）。

Azure 虛擬 WAN 的功能包括：

- 分支連線（透過來自虛擬 WAN 合作夥伴裝置的自動化連線，例如 SD-WAN 或 VPN CPE）。
- 站對站 VPN 連線。
- 供遠距使用者連線的點對站台 VPN。
- 使用 ExpressRoute 的私有連線。
- VNet 的雲端內連線。
- 使用 VPN ExpressRoute 的互連能力。
- 供私有連線使用的路由、Azure 防火牆和加密功能。

Azure 虛擬 WAN 還有其他優點，例如在中樞輪輻（hub-spoke）網路拓撲的整合連接方案、自動設定輪輻（spoke）組態、提供疑難排解和網路監控工具。要設定 Azure 虛擬 WAN，需要有虛擬廣域網路資源，如 Virtual Hub（虛擬中樞）、虛擬網路連接、中樞對中樞連接、中樞路由表和站台資源。

圖 4-3 是 Azure 虛擬廣域網路用在遠距連接的示意圖。

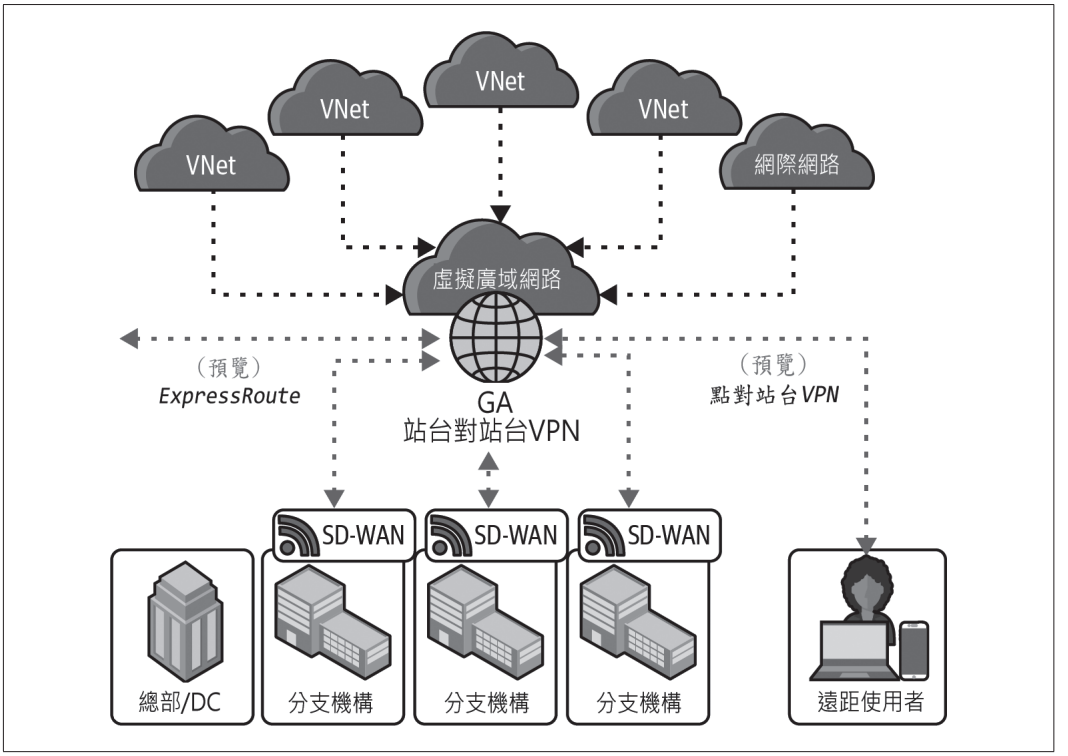

圖 4-3　Azure 虛擬廣域網路（改編自微軟文件裡的圖片；*https://oreil.ly/seNQ5*）

每次遷移都是獨特的作業，請選擇可用資源和項目，以便協助你移轉至 Azure 虛擬 WAN（*https://oreil.ly/KrxWS*）。

Azure 虛擬 WAN 是一項廣泛又複雜的主題，想要更深入瞭解，可參閱微軟的虛擬 WAN 文件（*https://oreil.ly/GfaJh*）。

Azure ExpressRoute

Azure ExpressRoute 可讓用戶在私有連線上，透用連線服務提供者，將地端網路延伸至微軟的雲端基礎設施，基本上，這種網路服務能夠將地端網路與 Azure 連接起來，兩者間的連線可以使用第三層自由連通（any-to-any）的網路（IPVPN）來建立，將 Azure 與用戶自有的地端廣域網路或資料中心連接在一起。

在 Azure ExpressRoute 裡的連線是私密的，連線流量不會經過網際網路，也就是說，利用 ExpressRoute 連線比使用公眾網路連線，具有更快速、更安全、更可靠和更高可用性（*https://oreil.ly/VcCNa*）。

如圖 4-4 所示，透過 ExpressRoute，可以和微軟的其他雲端資源（如 Microsoft 365、Dynamic 365 和 Azure）建立安全連線。

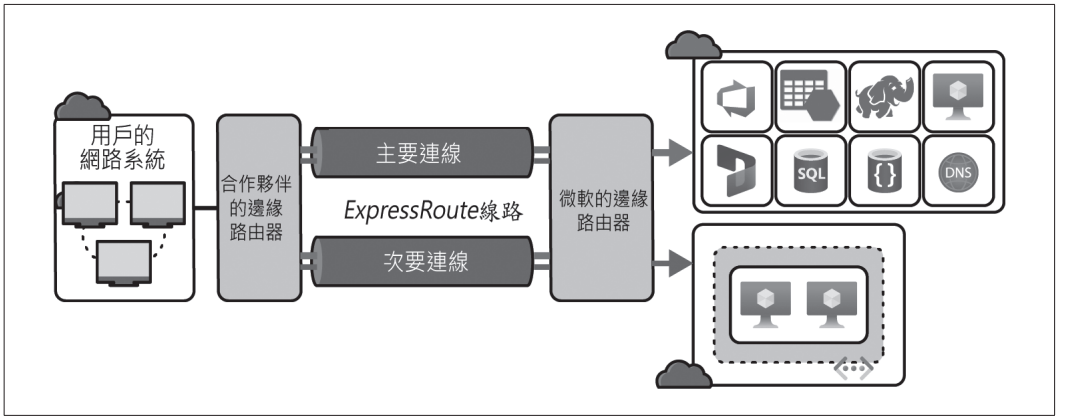

圖 4-4　Azure ExpressRoute 為公有雲和地端網路建立連線（改編自微軟文件的插圖；*https://oreil.ly/05TZx*）

ExpressRoute 具有諸多實用功能，例如支援地端網路和 Azure 之間的不同連線模型（*https://oreil.ly/Ft_eu*），如圖 4-5 所示，這些連接模型可以透過服務提供者或直接連線來實作，服務提供者目前使用三種模型來建立連線：**共置雲端交換**（*cloud exchange co-location*）、**點對點乙太網路連接**和 *IPVPN* **自由連接**（*any-to-any*），也可用 ExpressRoute Direct 直接連接到 Azure。

若想用高達 10 GBps 或 100 GBps 的速度，將自有網路以對等互連方式直接連到微軟的全球網路，*ExpressRoute Direct* 服務是不錯的選擇，可以使用 Azure 入口網站、Azure CLI 和 PowerShell 建立 ExpressRoute Direct 連線（*https://oreil.ly/TS87Q*）。微軟文件有更多關於 ExpressRoute Direct 線路（*https://oreil.ly/aR9fH*）、工作流程、VLAN tagging、**服務水準協議**（SLA）和計價的資訊。如果有資料擷取（ingestion of data）需求，可以將 Azure 儲存服務和 ExpressRoute Direct 整合使用。

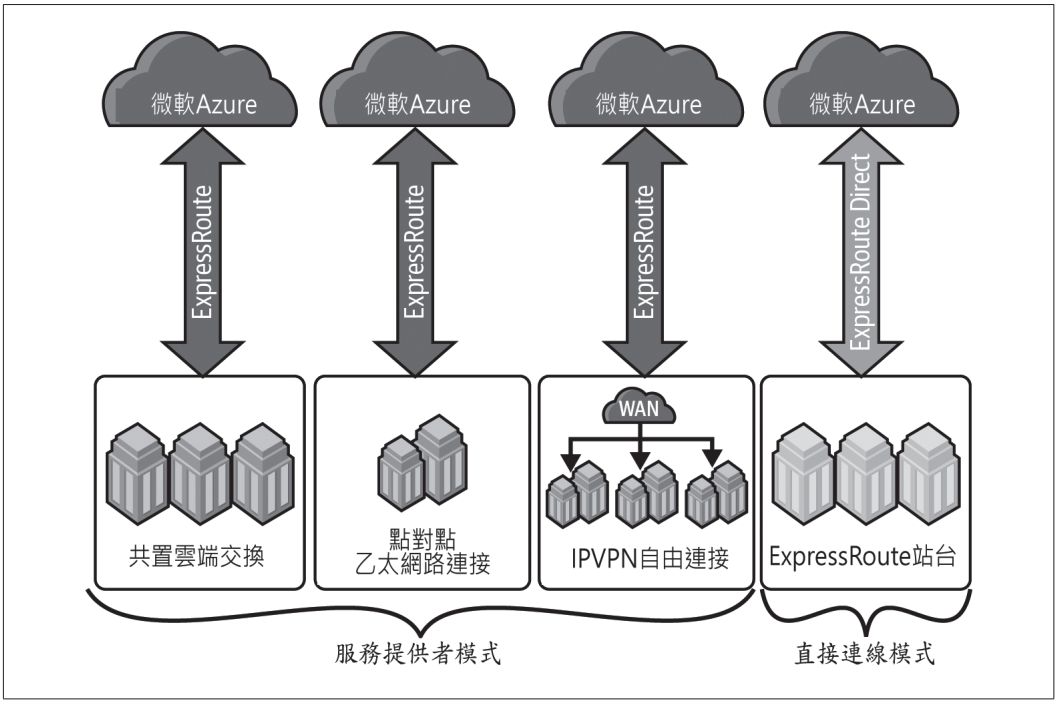

圖 4-5　不同的 Azure ExpressRoute 連接模型

在設定和管理 ExpressRoute 時，想連接到微軟的雲端服務，需要有網路位址轉換（NAT；*https://oreil.ly/u0h8X*），第三方供應者通常以服務模式提供 NAT 管理。此外，微軟的對等互連和 Azure 的公共對等互連（*https://oreil.ly/eb-eD*）也有 NAT 需求。讀者還需要瞭解一些 ExpressRoute 路由（*https://oreil.ly/P7hJk*）需求。

有些選項可讓 Azure ExpressRoute 建立 Azure 資源的私有對等互連，像是 VM 和適用於 Azure 虛擬桌面的 RDP Shortpath（*https://oreil.ly/TDUXH*）。

Azure ExpressRoute 全球可達服務：除了 Azure ExpressRoute 的直接連線和服務提供者的不同連線模型外，還有稱為 ExpressRoute 全球可達的網路服務，專為連結全球各地分支機構之類情境而設計。