VMware NSX Data Center

主要優勢

- 利用工作負載層級微分段和精密安全性保護應用程式。
- 透過自動化將網路佈建時間從數天減少至數秒，並改善營運效率。
- 無論資料中心和原生公有雲內部與彼此之間的實體網路拓撲為何，均能以一致的方式管理網路與安全性原則。
- 取得詳細的應用程式拓撲虛擬化、自動化安全性原則建議與持續的流量監控能力。
- 利用內建的完全分散式威脅防禦引擎，針對東西向流量啟用進階橫向威脅防護。

VMware NSX® Data Center 是實現虛擬雲端網路的網路虛擬化與安全性平台，透過軟體定義的方法，將網路延伸至資料中心、雲端和應用程式架構。無論應用程式是在虛擬機、容器或是裸機等任何環境上運作，NSX Data Center 都能讓網路與安全性更貼近應用程式。如同虛擬機的運作模式，無論底層硬體為何，皆可在其上佈建和管理網路。NSX Data Center 會以軟體重建整個網路模型，並在數秒內建立和佈建任何網路拓撲，從簡單到複雜的多層級網路，都可一手包辦。使用者可建立滿足不同需求的多個虛擬網路，透過 NSX 或廣泛的協力廠商技術整合商業網路 (從新一代防火牆到效能管理解決方案) 所提供的服務組合，建置本質上更敏捷且更安全的環境。這些服務還可延伸至雲端內部以及跨雲端的各個不同端點。

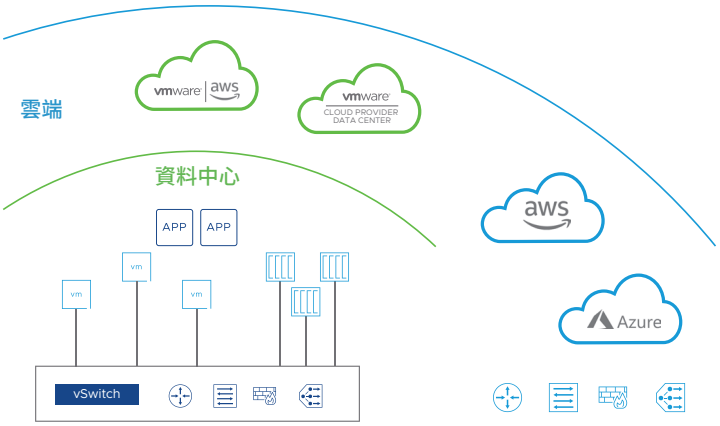

圖 1：NSX DATA CENTER 網路虛擬化與安全性平台。

網路全憑軟體

VMware NSX Data Center 為軟體定義的網路提供全新的作業模式，可為軟體定義的資料中心 (SDDC) 打下深厚基礎，並延伸到虛擬雲端網路。現在，資料中心的作業人員可實現各種層級的靈活性、安全性與經濟效益，徹底擺脫過去資料中心網路完全受限於實體硬體元件的窘境。NSX Data Center 提供一套完整的邏輯網路與安全功能和服務，包含邏輯交換、路由、防火牆保護、負載平衡、虛擬私有網路 (VPN)、服務品質 (QoS) 與監控。運用 NSX Data Center API，即可透過任何雲端管理平台，將這些服務佈建在虛擬網路中。虛擬網路是以不中斷運作的方式部署在任何現有網路硬體上，而且可延伸至資料中心、公有雲和私有雲、容器平台和裸機伺服器。

重要功能

交換	能夠在資料中心界限內部與彼此之間的路由 (第 3 層) 結構上建立第 2 層邏輯層疊延伸。支援 VXLAN 和 GENEVE 網路層疊。
路由	在虛擬化管理程序核心中，以分散形式執行虛擬網路之間的動態路由，透過使用實體路由器的主動-主動式容錯移轉達成水平擴充路由。支援靜態路由與動態路由通訊協定，包括支援 IPv6。
閘道防火牆	涵蓋至第 7 層 (包括應用程式識別和分散式完整網域名稱允許清單) 的具連線狀態防火牆保護，不僅內嵌在 NSX 閘道內，還可透過集中式原則和管理分散至整個環境。
分散式防火牆	涵蓋至第 7 層 (包括應用程式識別和分散式完整網域名稱允許清單) 的具連線狀態防火牆保護，不僅內嵌在虛擬化管理程序核心內，還可透過集中式原則和管理分散至整個環境。此外，NSX 分散式防火牆可直接整合到 Kubernetes 和 Pivotal Cloud Foundry 等雲端原生平台、AWS 和 Azure 等原生公有雲，以及裸機伺服器內。
負載平衡	第 4 層至第 7 層負載平衡器配備 SSL 卸載和直通功能、伺服器運作狀況檢查 (和被動式運作狀況檢查)，以及應用程式規則，可依據這些規則透過 GUI 或 API 編寫程式並操控流量。
VPN	具備站點對站點與遠端存取的 VPN 功能，且可針對雲端閘道服務提供未受管理的 VPN。
NSX 閘道	對於設定在實體網路和 NSX 層疊網路上的 VLAN，提供 VLAN 之間的橋接支援，以便順暢連接虛擬與實體工作負載。
NSX Intelligence™	NSX Intelligence 可針對每個網路流量提供自動化安全性原則建議與持續的監控與虛擬化能力，進而強化能見度，並實現可輕鬆進行高度稽核的安全態勢。NSX Intelligence 與 NSX-T™ Data Center 共用相同的使用者介面，能為網路與安全性團隊提供單一介面。
NSX 分散式威脅防禦 (NSX Distributed IDS/IPS[1])	NSX Distributed IDS/IPS™ 是一款專門打造的先進威脅偵測引擎，可用來偵測東西向流量上的橫向威脅移動。獨特的分散式架構結合精確的應用程式情境，讓安全性團隊在更換離散應用裝置的同時，還能輕鬆符合法規，並建立虛擬安全性區域，而無需實際區隔基礎架構。
聯合掌控	從單一介面對多個位置進行集中式原則設定及強制執行，針對整個網路啟用一致的原則，以簡化作業與災難復原架構。
虛擬路由及轉遞 (VRF)	利用獨立路由表完成租戶間的資料轉發平台隔離，NSX 第 0 層閘道上的每個 VRF 均支援 NAT 與邊緣防火牆。
NSX Data Center API	採用 JSON 技術的 RESTful API，方便與雲端管理平台、開發營運自動化工具和自訂自動化整合。
作業	提供原生作業功能，例如中央指令行介面 (CLI)、traceflow、層疊邏輯 SPAN 與 IPFIX，可進行疑難排解和主動監控虛擬網路基礎架構。與 VMware vRealize® Network Insight™ 等工具整合，以提供進階分析與疑難排解。
情境感知的微分段功能	可依據屬性 (不僅止於 IP 位址、連接埠和通訊協定) 動態建立並自動更新安全性群組和原則，以包含機器名稱與標籤、作業系統類型和第 7 層應用程式資訊等項目，進而實現自調式微分段原則。依據 Active Directory 和其他來源提供之身分識別資訊所建立的原則，能提供使用者層級安全性，深入遠端桌面服務和虛擬桌面基礎架構 (VDI) 環境內的個別使用者工作階段層級。

自動化與雲端管理	能與 vRealize Automation™/vRealize Automation Cloud™、OpenStack 等服務進行原生整合。完整支援的 Ansible 模組、完整支援的 Terraform 供應商及 PowerShell Integration。
協力廠商合作夥伴整合	支援與協力廠商合作夥伴在各種不同類別上的管理、控制平台和資料轉發平台整合，例如新一代防火牆、入侵偵測系統 (IDS)/入侵防禦系統 (IPS)、無代理程式的防毒保護、交換、作業與能見度、進階安全性等等。
多雲網路與安全性	無論底層實體拓撲或雲端平台為何，均能在各個資料中心站點以及跨私有雲和公有雲界限，實現一致的網路與安全性。
容器網路與安全性	針對 Kubernetes 和 Cloud Foundry 平台上的容器 (無論是在虛擬機或裸機伺服器上運作)，支援其負載平衡、微分段 (分散式防火牆保護)、路由和交換。提供容器網路流量能見度 (邏輯連接埠、SPAN/Mi、IPFIX 和 Traceflow)。

使用情境

安全性

透過 NSX Data Center，即可在私有雲和公有雲環境中，有效率地實際運用應用程式的零信任安全性。無論目標是要鎖定關鍵應用程式、在軟體中建立邏輯緩衝區域 (DMZ)，還是縮小虛擬桌面環境中的攻擊範圍，NSX Data Center 都能實現微分段，以定義並強制執行個別工作負載層級的網路安全性原則。

多雲網路

NSX Data Center 提供一套網路虛擬化解決方案，能在各個異質站點實現一致的網路與安全性，進而簡化多雲維運。因此，NSX Data Center 能配合多雲使用情境，從順暢的資料中心延伸到多資料中心集區，再到快速工作負載行動化。

自動化

透過網路與安全服務的虛擬化，NSX Data Center 成功免除手動管理網路與安全服務和原則所面臨的瓶頸，進而加速推動完整堆疊應用程式的佈建與部署作業。NSX Data Center 能原生整合雲端管理平台和其他自動化工具 (例如 vRealize Automation/vRealize Automation Cloud、OpenStack、Terraform、Ansible 等)，協助開發人員和 IT 團隊依據業務需求佈建、部署與管理應用程式。

雲原生應用程式的網路與安全性

NSX Data Center 為容器化的應用程式與微服務提供整合式完整堆疊的網路與安全性，進而在開發新應用程式期間提供以容器為基礎的精密原則。如此一來，傳統與新應用程式皆可享有原生容器對容器第 3 層網路、適用於微服務的微分段，以及網路與安全性原則的端對端能見度。

VMware NSX Data Center 的版本

Standard
適合需要有敏捷且自動化網路的組織。

Professional
適合需要有 Standard 版本功能外加微分段功能，且可能有公有雲端點的組織。

Advanced
適合需要有 Professional 版本功能，外加進階網路與安全服務，並與廣大商業網路整合，且可能有多個站點的組織。

Enterprise Plus
適合需要最進階的 NSX Data Center 功能、vRealize Network Insight 的網路作業、VMware HCX® 的混合雲行動化，以及 NSX Intelligence 的流量能見度與安全性作業的組織。

Remote Office Branch Office (ROBO)
適合需要在遠端辦公室或分公司，將應用程式的網路與安全性虛擬化的組織。

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX DATA CENTER[1]					
分散式交換與路由	•	•	•	•	•[6]
NSX 閘道防火牆 (具狀態)	•	•	•	•	•
NSX 閘道 NAT	•	•	•	•	•
軟體第 2 層橋接到實體環境	•	•	•	•	
透過 ECMP (主動-主動) 的動態路由	•	•	•	•	•
與雲端管理平台整合[3]	•	•	•	•	•
具備靜態路由的 IPv6 及靜態 IPv6 配置	•	•	•	•	
為在裸機上運作的虛擬機和工作負載提供分散式防火牆保護		•	•	•	•
VPN (第 2 層與第 3 層)		•	•	•	•
與 NSX Cloud™[4] 整合，以支援 AWS 和 Azure		•	•	•	•
負載平衡			•	•	•
與分散式防火牆整合 (Active Directory、VMware AirWatch®、端點保護與協力廠商服務增強)			•	•	•
容器網路與安全性			•	•	
多 vCenter® 網路與安全性			•	•	
具備動態路由的 IPv6、動態 IPv6 配置及服務			•	•	
情境感知的微分段技術 (第 7 層應用程式識別、RDSH、通訊協定分析器)			•	•	
分散式完整網域名稱允許清單			•	•	
NSX Distributed IDS[5]			•	•	
VRF (第 0 層閘道 VRF)			•	•	
聯合掌控				•	

	STANDARD	PROFESSIONAL	ADVANCED	ENTERPRISE PLUS	ROBO
NSX INTELLIGENCE					
虛擬機至虛擬機流量分析				•	
防火牆能見度				•	
自動化安全性原則				•	
規則與群組建議分析				•	
vREALIZE NETWORK INSIGHT ADVANCED[2]				•	
VMWARE HCX ADVANCED[2]				•	

1. 如需詳細功能說明，請參閱 NSX Data Center for vSphere® 功能及 NSX-T Data Center 功能的知識庫文章，包括 *NSX-T Data Center 3.0 產品方案*文章，以取得最新資訊。
2. NSX Data Center Enterprise Plus 包含完整版 vRealize Network Insight Advanced 與 VMware HCX Advanced。如需詳細資訊，請參閱 *vRealize Network Insight 規格說明*以及 *HCX 規格說明*。
3. 只與第 2 層、第 3 層和 NSX 閘道整合。不會使用安全性群組。
4. 公有雲工作負載需要有 NSX Cloud 訂閱。
5. NSX Distributed IDS 需另外訂閱。
6. 僅交換，支援 VLAN。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com
11073 台北市信義區松仁路 100 號 38 樓之一台北南山廣場辦公大樓 電話 +886-2-3725-7000 傳真 +886-2-3725-7010 www.vmware.com/tw