VMware NSX Cloud

跨私有雲和原生公有雲的混合雲網路與安全性

概觀

VMware NSX® Cloud 能為在公有雲上原生執行的應用程式提供一致的網路與安全性。NSX Cloud 使用與 NSX Data Center 一樣的管理平台及控制平台，因此只需部署一套網路與安全性解決方案，即可管理從私有資料中心到公有雲之間的所有活動。

主要優點

在 AWS 與 Azure 等公有雲中提供共用的網路與安全性，可大幅提升延展性、控制力和能見度，而且營運成本更低：

- 透過 NSX 架構或原生公有雲架構提供部署彈性
- 為虛擬網路、可用區域、地區，以及公有雲等環境提供簡易的延展性
- 精準的安全性控制能力與網路服務，為應用程式帶來防護能力，同時協助其完成標準化作業
- 端對端的網路與安全性能見度，確保公有雲環境裡的應用程式運作正常並符合相關規範

價格

- 依不同訂閱方式計價，提供 1 年期或 3 年期的限期授權
- 無論虛擬網路數量多少，一律以公有雲裡已開機之工作負載所使用的 vCPU 數量來計算；例如，AWS Virtual Private Clouds (VPC) 與 Azure Virtual Networks (VNet)
- 僅限雲端的使用情境不需要 NSX Data Center 授權

因應雲端原則打造的網路

VMware NSX Cloud 能為在公有雲上原生執行的應用程式提供網路與安全性。VMware NSX Cloud 搭配 VMware NSX 系列一起運作就能組成虛擬雲端網路，並可利用這個軟體定義的網路架構串連起資料中心、雲端環境、各個端點與物件。

圖 1：虛擬雲端網路。

使用情境

跨雲端的一致安全性

NSX Cloud 能夠將原則貫徹到跨多個公有雲和內部部署資料中心運作的工作負載。這些原則只要定義一次，即可套用至任何位置的工作負載，包括雲端虛擬網路、地區、可用區域和多雲供應商。安全性原則是根據應用程式屬性與使用者定義的標籤，動態套用到個別工作負載。針對沒有套用適當微分段安全性原則的異常或遭到入侵的工作負載，甚至會自動加以隔離。NSX Cloud 支援南北向服務增強，能將選定的流量路由到協力廠商安全性應用裝置，以獲得進階安全保護。

精確控制雲端網路

VMware NSX Cloud 適用於原生公有雲環境，例如 Amazon (AWS) 與 Microsoft Azure。NSX Cloud 能與這些公有雲供應商所提供的原生服務相輔相成。有了 NSX Cloud，您可以針對工作負載需要，無限制地繼續使用公有雲供應商的基礎架構和應用程式服務 (例如，AWS ELB/Azure Load Balancer、AWS Route 53/Azure DNS、AWS Direct Connect/Azure ExpressRoute，以及 Amazon RDS/Azure Database)。您可以使用現有的自動化工具，透過 REST API 要求，將佈建與組態設定管理自動化。NSX Cloud 也支援傳輸到 VPC/VNet 的閘道整合，這能實現作業簡化並使用內建服務，例如站點到站點 VPN 以及協力廠商邊緣網段/傳輸服務。

端對端的營運控制與能見度

VMware NSX Cloud 提供標準的介面與通訊協定，可讓您從雲端網路存取網路與安全性資料。流量、封包和事件資訊都可透過 IPFIX、Traceflow、封包側錄和 Syslog 提供。您可以使用現有的內部部署作業工具來取用這些資料，以針對監控、疑難排解和稽核作業提供深入的端對端能見度。這些豐富的作業資料有助於大幅縮短混合雲的整體部署 (包括內部部署與位於公有雲的應用程式) 時，識別和解決網路連線、效能與安全性問題所需的時間。NSX Cloud 提供跨所有 VPC/VNet 上公有雲工作負載的精密能見度，以及有助於簡化管理的多樣搜尋與篩選功能，而且您可以輕鬆挑選要使用 NSX 進行管理的工作負載。

重要功能

NSX 強化模式 – 使用 NSX 工具，即可對內部部署與原生公有雲工作負載施行一致的安全性與網路原則。

原生雲端強化模式 – 使用公有雲供應商的安全性與網路架構，即可對內部部署與原生公有雲工作負載施行一致的安全性與網路原則。

原生公有雲服務端點的探索與保護 – 除了虛擬機 (VM) 與 EC2 執行個體外，還可提供原生公有雲服務端點的探索與保護。

多雲端、多站點網路與安全性 - 能為多雲端端點引進網路與安全功能，並藉由整合 NSX Data Center 之便，實現跨雲端與資料中心站點的網路與安全性管理功能。

微分段 - 可掌控在公有雲中以原生方式運作的應用程式工作負載之間的東西向流量。NSX Cloud 也支援對 VMware Horizon® Cloud on Azure 部署的虛擬桌面進行微分段。

豐富的安全性原則定義抽象化 – 可根據各種豐富的原則結構定義安全性群組和規則，例如執行個體名稱、作業系統類型、AMI ID 和使用者定義的標籤。

動態原則 – 可根據執行個體屬性和使用者定義的標籤，自動套用並施行安全性原則。當執行個體在雲端內部或雲端之間移動時，這些原則會自動隨著執行個體一起移動。

隔離執行個體 - 可在沒有微分段安全性的情況下，隔離在公有雲執行的惡意工作負載和遭入侵的工作負載。遭隔離的執行個體無法在雲端網路上進行通訊，確保多層安全性。

服務增強 - 使用原則式路由將選定的南北向流量路由到協力廠商新一代防火牆合作夥伴應用裝置。

站點至站點 VPN - 利用內建 VPN 支援，將流量回傳到內部部署資料中心。

分散式架構 – 使用 NSX Cloud 分散式防火牆架構免除額外的網路躍點和流量，該架構會在每個執行個體的虛擬網路介面上施行原則，而非路由穿越外部防火牆。

傳輸至 VPC/VNet 的共用閘道 – 可支援傳輸到 VPC/VNet 的閘道整合，這會簡化管理、加快運算 VPC/VNet 上線的速度，而且能夠增強協力廠商服務。

邊緣防火牆 - 使用具連線狀態防火牆篩選虛擬網路執行個體與公用網際網路之間的南北向流量。

RESTful API – 運用 RESTful API 和自動化工具透過程式佈建及設定隨選網路與安全性基礎架構。

若要取得更多資訊或購買 VMWARE 產品

請致電 +886-2-3725-7001、造訪 vmware.com/tw/products/nsx-cloud 或 vmware.com/tw/products，或是線上搜尋授權經銷商。

範本 - 使用現有的自動化與協調作業工具來建立標準化應用程式範本，並且簡化在公有雲佈建及管理網路與安全服務的作業。

東西向流量能見度 - 使用現有的次要作業工具來取得 VPC 內部與彼此之間的東西向流量能見度。

安全性日誌記錄 - 取得允許/拒絕和隔離事件等安全性事件的即時能見度，並加以稽核。可將安全性事件資訊傳送至 Syslog 或 SIEM 伺服器。

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 +886-2-3725-7001 傳真 +886-2-3725-7010 www.vmware.com/tw

文件編號：301621aq-ds-NSX-cloud-a4