VMware NSX-T Data Center 2.4 版本說明

VMware NSX-T Data Center 2.4 | 2019 年 2 月 28 日 | 組建編號 12456646

請定期查看這些版本說明的增補和更新。

版本說明的內容

此版本說明涵蓋下列主題：

新增功能

NSX-T Data Center 2.4 提供了多種新功能，可為私有雲、公有雲和混合雲的虛擬化網路和安全性提供新功能。主要功能包括新的基於意圖的網路使用者介面、內容感知防火牆、客體和網路自我檢查功能、IPv6、高可用性叢集管理、適用於 vSphere 運算叢集之以設定檔為基礎的 NSX 安裝、適用於 NSX for vSphere 運算叢集的無重新開機維護升級模式、適用於 vSphere 運算叢集的新就地升級模式，以及用於從 NSX Data Center for vSphere 移轉至 NSX-T Data Center 的移轉協調器。

NSX-T Data Center 2.4 版本中提供了下列新功能和增強功能。

管理叢集

NSX-T Data Center 2.4 現在支援建立管理程式叢集以獲得使用者介面和 API 高可用性的功能。此叢集化支援外部平衡器和負載分佈或 NSX 提供的虛擬 IP，以實現冗餘。此外，管理平面功能和中央控制平面功能已納入這個新的管理叢集中，以減少必須透過 NSX 管理進行部署和管理的虛擬應用裝置數目。對於不同的部署案例，NSX Manager 應用裝置提供三個不同的大小。小型應用裝置適用於實驗室或概念驗證部署。中型應用裝置適用於 64 台主機的部署，而大型應用裝置適用於部署到大型環境的客戶。如需有關組態上限的詳細資料，請參閱 VMware 組態上限工具，網址為：https://configmax.vmware.com

支援單一叢集設計

使用在單一實體主機中的單一 N-VDS 所提供的摺疊 Edge+Management+Compute 虛擬機器支援單一叢集設計。VCF SP 客戶的一般參考設計指定具有兩個主機交換器的 4x10G pNIC，一個用於 Edge+Management，而另一個則用於計算虛擬機器。這可有效隔離 Edge 虛擬機器和計算虛擬機器之間的通訊，以便流量離開主機並重新返回。但是，由於 25G NIC 的趨勢經濟，VCF SP 客戶逐漸標準化 2x25G NIC 的主機，而這種設計使得他們能夠移到提供具有 2pNIC 主機的單一 N-VDS。在這種設計中，屬於相同子網路的 Edge 虛擬機器和計算虛擬機器能夠通訊，而流量不用離開主機上行並返回。

原則和使用者介面

NSX 管理和自動化

- **宣告式原則管理** - 透過結果導向的原則聲明簡化並自動化網路與安全性組態。這項新的宣告式原則 API 透過允許使用者說明所需的最終目標，同時讓系統確定實現目標的最佳方式來減少設定步驟數目。定義整個網路拓撲，並且以一個與順序無關的規定方式一次性部署該拓撲。

使用者介面增強功能

- **增強型導覽和頁面配置**：改進了導覽列和頁面配置，以減少存取重要資訊的點按次數。
- **國際化**：改進了對地區設定特定項目的處理，例如日期/時間格式、數字格式、時區。

附註：2.3 版中推出的 NSX Policy Manager 網路拓撲視覺化功能在此版本中已過時。

防火牆

分散式防火牆和閘道防火牆將支援從 NSX-T Data Center 2.4 篩選 IPv6 流量。此外，本產品還新增了各種操作功能，如下所示：

發佈/還原按鈕

單一發佈按鈕適用於整個防火牆資料表。此按鈕同時適用於分散式防火牆和閘道防火牆。在 NSX-T Data Center 2.4 之前的版本中，發佈按鈕分別用於每個區段。此按鈕將透過 API 提供。此外，您可以選擇還原變更。您還可以選擇在更新變更時鎖定區段。

規則統計資料

每個規則都具有叫用計數、封包計數、工作階段計數、位元組計數和權數索引。還具有與目前叫用計數相對的最大值。此統計資料可透過按鈕進行重設。

分組增強功能

可以使用基於虛擬機器的作業系統和 Active Directory 群組的其他分組準則。

每個虛擬機器的規則可見度

透過查看每個虛擬機器的邏輯交換器連接埠關聯，可取得特定虛擬機器的防火牆規則清單。

虛擬機器的 IP 探索

除了 ARP 窺探和 DHCP 窺探之外，還將更新預設 IP 探索設定檔以包含基於 VMTools 的 IP 探索。從舊版執行升級的現有客戶必須更新 IP 探索設定檔，才能啟用基於 VMTools 的偵測。此外，NSX-T 2.4 支援建立全域 IP 探索設定檔。另外，還有下列變更：

1. 基於 DHCPv6 和芳鄰探索機制的 IPv6 IP 探索可供使用。
2. IPv6 探索預設為停用狀態。
3. 自動探索的 IP 繫結可以手動加入白名單，也可以放在略過清單中。
4. 依預設，系統將忽略本機連結 IPv4 位址。

身分識別防火牆

NSX-T Data Center 2.4 針對分散式防火牆採用以身分識別 (使用者識別碼) 為基礎的規則。現在，防火牆管理員可以根據以 Active Directory 為基礎的群組在虛擬機器上設定分散式規則。此功能可讓防火牆管理員根據登入虛擬機器的使用者提供防火牆規則。NSX 會自動偵測登入/登出的使用者，然後相應地為使用者啟用特定規則。以身分識別為基礎的防火牆可以為每個虛擬機器的單一使用者偵測並強制執行規則，甚至追蹤相同虛擬機器中具有特定工作階段的多個使用者。防火牆管理員會使用 Active Directory 群組做為準則來建立 NSX-T 群組。NSX-T Manager 會自動從提供的網域控制站擷取 Active Directory 群組清單。防火牆管理員可以控制使用者的東西向存取，特別是在已啟用終端機服務的虛擬桌面環境或遠端桌面工作階段中。

內容感知分散式防火牆的 L7 應用程式簽章

NSX-T Data Center 2.4 提供了分散式防火牆規則中以 L7 為基礎的應用程式簽章的功能。使用者可以組合使用 L3/L4 規則與 L7 應用程式簽章，也可以僅建立以 L7 應用程式簽章為基礎的規則。我們目前僅針對伺服器-伺服器或用戶端-伺服器通訊支援具有各種子屬性的應用程式簽章。在 NSX-T Data Center 2.4 中，這僅適用於以 ESXi 為基礎的傳輸節點。

內容感知分散式防火牆的 FQDN/URL 白名單

NSX-T Data Center 2.4 在分散式防火牆中採用以 URL/FQDN 白名單為基礎的規則。NSX-T Data Center 採用了一項使用分散式 DNS 窺探的創新，可讓每個虛擬機器的每個連線都有其自己的 URL/FQDN 解析。防火牆管理員可以使用預先定義的 URL 網域，並將其套用至分散式防火牆中的規則。存取 SaaS 服務或雲端式服務的應用程式 (本質上為混合) 可以根據存取的 URL 進行微分割。用戶端應用程式或存取 SaaS 應用程式的瀏覽器可以在細微的基礎上被授與存取權。在 NSX-T Data Center 2.4 中，這僅適用於以 ESXi 為基礎的傳輸節點。

服務插入

NSX-T Data Center 2.4 採用了大量原生安全功能，例如，第 7 層應用程式身分識別、FQDN 白名單和身分識別防火牆，這些功能甚至能夠進行更細微的微分割。除了分散式防火牆和閘道防火牆提供的原生安全性控制，NSX 服務插入架構還允許各種類型的合作夥伴服務 (例如，IDS/IPS、NGFW 和網路監控解決方案) 透明地插入到資料路徑中並從 NSX 內使用，而無需在拓撲中進行任何變更。

在 NSX-T Data Center 2.4 中，服務插入現在支援東西向流量 (即資料中心內虛擬機器之間的流量)。資料中心內虛擬機器之間的所有流量都可以重新導向至合作夥伴服務的動態鏈結。

E-W 服務平面提供自己的轉送機制，允許沿著服務鏈結對流量進行以原則為基礎的重新導向。平台完全自動沿著服務平面進行轉送：偵測到故障、視情況重新導向現有/新流量、執行流量固定以支援可設定狀態的服務，並且可以使用多個路徑選取原則來最佳化輸送量/延遲或密度。

Guest Introspection

NSX-T Data Center 2.4 針對 VMware 合作夥伴採用 Guest Introspection 服務平台，針對 vSphere ESXi Hypervisor 上的 Windows 客體虛擬機器工作負載提供以原則為基礎的無代理程式防毒軟體和反惡意程式碼卸載功能。

在 NSX-T Data Center 2.4 中，Guest Introspection 平台提供：

- 透過將 Guest Introspection 部署合併到 NSX 代理程式主機準備安裝，並且不再要求在每個 ESXi Hypervisor 上部署 Guest Introspection 通用服務虛擬機器，簡化了部署和生命週期管理。
- 在多個 vCenter 之間提供一致的以原則為基礎的服務。
- 透過調整合作夥伴 SVM 的大小 (例如「小型」、「中型」和「大型」合作夥伴應用裝置)，增強 VMware 合作夥伴縮放功能。

L2 網路

每台主機多個 N-VDS

除了提供組織整理虛擬機器流量的彈性之外，這項支援每台主機多個 N-VDS 的新功能還有助於符合 PCI 規則，其中虛擬機器流量需要嚴格隔離。

透過新增此功能，現在可以將 ENS 上行與非 ENS 上行分開；這項功能非常有用，因為 ENS 目前沒有與 N-VDS 同位的功能，因此由 ENS 提供支援的工作負載將取得快速路徑，但功能效率卻很低。

N-VDS 視覺化

此功能提供了將 N-VDS 做為獨立物件進行管理的功能，以及向下切入以查看連線的主機等功能。查看特定主機時，可以看到一個使用者介面網格，其中顯示了與 N-VDS 連線的方式。邏輯介面 (例如，虛擬機器核心介面) 也會顯示為 N-VDS 的一部分。這是對主機視圖的顯著改進，顯示了在一個視圖中包含所有實體 NIC、虛擬機器核心介面和所有 OVS 連接埠的介面的清單。

對實體 NIC 的 LLDP 支援

此功能有助於縮小 NSX 在 LLDP 實作中的差距。可以為實體交換器連線提供偵錯能力。解密哪些實體連接埠連線到主機上的哪些介面的功能有助於對佈線問題輕鬆地進行疑難排解。此功能的範圍適用於參與 NSX 數據平面的所有實體主機 (ESXi、KVM、裸機 Linux 主機以及裸機 Edge)。

對 Edge 節點上 Proxy ARP 的支援

當外部用戶端存取具有相同子網路位址的服務 (如 LB、IKE 等) 時，它們會叫用裝置路由。它們會為繫結到回送連接埠的這些位址傳送 ARP 查詢，但是，LR 回送連接埠沒有 MAC 位址，因此無法回應這些 ARP 查詢。這會導致存取問題。

目前，因應措施是在這些用戶端中設定 /32 路由，例如回送 IP/32 → 上行/CSP，以便能夠將流量轉送到上行/CSP 連接埠，然後它可以前往正確的回送連接埠。ARP Proxy 是克服該缺點的正確解決方案。

L3 網路

MTU 組態增強功能

NSX-T 2.4 提供兩個新的 MTU 全域參數：

- 全域實體上行 MTU，可針對 NSX 網域中的所有 N-VDS 執行個體設定 MTU。這可以轉譯為 GENEVE 封裝式框架的最大框架大小或 TEP MTU。
    - 上行設定檔 MTU 可以覆寫特定主機上的全域實體上行參數。
- 全域邏輯介面 MTU，可針對所有邏輯路由器介面設定 MTU。
    - 如果需要，邏輯路由器上行 MTU 和 CSP 連接埠 MTU 可以覆寫特定連接埠上的全域邏輯介面 MTU。

這將允許已設定超過 1500 位元組 MTU 之虛擬機器的端對端通訊用於東西向和南北向流量。

SR 間路由

處於作用中/作用中模式的 Tier0 邏輯路由器現在可以在指定 Tier0 邏輯路由器的所有服務路由器 (SR) 部分之間，自動建立完整網格 iBGP 對等。這可以防止在 SR 設定多個上行並且只有其中一個上行失敗時造成流量捨棄。如果目的地在其自己的上行上不可用，則此失敗案例中的 SR 現在會將流量轉送給另一個 SR。

DNS 轉寄站增強功能

- 現在可以啟用或停用 DNS 轉寄站功能，而不遺失其目前組態。
- DNS 轉寄站功能還可透過 API 和使用者介面公開統計資料、事件和警示。

支援上行之間的 SNAT

NSX-T 2.4 採用了 SNAT (來源位址轉譯) 支援，以便流量透過一個上行進入 Tier0 邏輯路由器，並透過另一個上行離開相同的邏輯路由器。當多個 Tier0 邏輯路由器互連時，此功能非常有用。

Tier0 邏輯路由器上的 Proxy ARP 支援

NSX-T 2.4 採用了 Tier0 邏輯路由器上行上的 Proxy ARP 支援。這將允許在無法在 Tier0 邏輯路由器的北向路由器上設定路由的環境中部署 NSX-T。透過此功能，NAT、LB 或任何可設定狀態的服務均可設有屬於 Tier0 上行網路的 IP 位址。

Edge 節點增強功能

- NSX-T 2.4 採用裸機 Edge 節點上的選項以支援在快速路徑 NIC 上進行管理，而不再需要專用的管理 NIC。

- 裸機 Edge 節點還支援 25 Gbps Intel NIC XXV710。
- Edge 節點支援多個 GENEVE 通道端點 (TEP)。這可讓 Edge 節點無需使用 LAG 即可實現覆疊流量的高可用性。

BGP 增強功能

- 從 NSX-T 2.4 開始，Tier0 邏輯路由器支援 iBGP 與北向實體路由器對等。
- NSX-T 2.4 採用在不同 ASN 中的 eBGP 對等之間啟用 ECMP (as-path multipath relax) 的選項，還採用了 Tier0 邏輯路由器支援，以在 AS 路徑中允許其自己的 ASN (allow-as in)。

IPv6

NSX-T 2.4 採用 IPv6 路由/轉送和安全性。其中包含以下支援：

- IPv6 靜態路由
- IPv6 芳鄰探索
- DHCPv6 轉送
- IPv6 分散式防火牆 (DFW)
- IPv6 Edge 防火牆
- IPv6 位址家族，適用於 MP-BGP 和相關聯的首碼清單/路由對應
- IPv6 交換器安全性
- IPv6 位址探索
- IPv6 作業工具

作業

Traceflow 增強功能

Traceflow 新增了對更多疑難排解和視覺化功能的支援。在 NSX-T 2.4 中，Traceflow 可提供對集中式服務 (例如 Edge 防火牆、負載平衡器、NAT 和路由型 VPN) 的觀察。

安裝增強功能

- NSX 使用針對 vSphere 運算叢集之以設定檔為基礎的新 NSX 元件安裝實現簡化部署。此功能有助於實現更快的部署、促進組態一致性、避免手動錯誤，並提供「定義一次並重複使用多次」的方法。
- 支援從使用者介面自動安裝和叢集化 NSX Manager 節點。
- 支援更多的部署組態，以便建立多個 N-VDS 交換器，並透過設定檔移轉 VMKernel 連接埠和實體介面卡。

升級增強功能

- 增強功能使用預設維護模式 NSX 升級，針對 ESXi 主機提供完整有組織的升級，而不會產生主機重新開機成本。
- 採用新的 NSX 升級模式，稱為「就地」升級。此功能有助於簡化操作，並實現更快的升級。使用此模式時，ESXi 主機上的 NSX 元件將會升級，而無需關閉工作負載的電源或將其移轉到其他 Hypervisor。
- 採用新的架構並提供立即可用的測試，以便在 NSX 升級期間進行預先檢查和後續檢查，進而有助於在開始實際升級之前或升級後立即反白顯示休眠基礎問題。

偵測變更後進行 NSX 備份

NSX 透過提供偵測組態變更並主動將其備份至安全儲存區的功能，增強其災難復原解決方案。此功能使客戶可以獲得更好的 SLA 以進行組態備份，而不會產生將不必要的檔案備份到儲存區伺服器的成本。

NFV

在 EDP 模式中，N-VDS 交換器現在支援下列增強功能。

- 分散式防火牆
- IP 探索
- SpoofGuard
- IPFIX
- IPv6
- 增強了 Edge 虛擬機器的效能，現在在 EDP 模式下的輸送量提高了五倍以上。
- 多宿主應用程式的路徑冗餘。將虛擬機器釘選到特定上行的功能，允許在具有 VTEP 的 NSX 上建構目前的多宿主冗餘路徑。

作業 - AAA/RBAC 和平台安全性

作業

- **主體身分識別增強功能**：可讓主體身分識別使用者登錄和安裝 NSX 元件。新增了使用者介面支援，以建立主體身分識別使用者和角色指派。
- **密碼原則增強功能**：針對預設密碼強制使用至少 12 個字元的密碼長度。採用設定密碼到期時間的功能，當密碼即將到期時會產生警示。依預設，密碼會在 90 天後到期。如需重設密碼和調整密碼到期的指示，請參閱知識庫文章 70691。

- **憑證管理**：新增用於檢查憑證撤銷狀態的功能。

VPN

NSX-T 2.4 為 VPN 服務新增了下列功能：

- 原則 API 和 GUI 同時適用於 L3 VPN 和 L2 VPN 服務。
- L3 VPN 服務支援憑證式驗證，以實現更好的安全性管理。
- 可以使用 L2 VPN 用戶端模式以支援將 L2 從 NSX-T SDDC 延伸至 NSX-T SDDC。
- DH 群組 19、20 和 21 可滿足高安全性需求。

負載平衡

NSX-T 2.4 為負載平衡服務新增了下列功能：

- 原則 API 和新 GUI 可供使用。在 [進階網路與安全性] 索引標籤下仍提供舊的負載平衡器 GUI。
- 獨立 SR 上的 VIP 可能與集中式服務連接埠或 CSP 屬於相同的子網路。在此版本之前，如果要在與 CSP 網路相同的子網上建立 VIP，則必須將 CSP IP 位址用於 VIP。否則，您必須在其他網路上建立 VIP。
- 同一個第 1 層閘道上的負載平衡器流量流程支援 DNAT 和 Edge 防火牆。在此版本之前，負載平衡器流量流程略過了 Edge 防火牆。
- LB 規則支援開頭為「_」的 HTTP 標頭。透過此增強功能，可以針對 vIDM 和 AirWatch 部署 NSX 負載平衡器。
- VIP 可用作 LB SNAT 的來源 IP 位址。
- 最大 HTTP 回應標頭大小可最多設定為 64K 位元組。預設大小與先前版本 (4K 位元組) 保持一致。
- 大型 Edge 虛擬機器支援大型 LB 執行個體。在此版本之前，大型 Edge 虛擬機器最多支援中型 LB 執行個體。

NSX Data Center for vSphere 至 NSX-T Data Center 的移轉

NSX-T 2.4 現在具有移轉協調器，可用來協助從 NSX Data Center for vSphere 移轉至 NSX-T Data Center。此功能旨在移轉現有的主機而不使用 vMotion 移轉。移轉協調器支援移轉第 2 層網路、第 3 層網路、防火牆、負載平衡和 VPN。《NSX-T Data Center 移轉協調器指南》提供了工具詳細資料。

除了部署 NSX-T Manager 和 Edge 節點之外，不需要其他計算資源。移轉完成後，客戶可以解除安裝 NSX for vSphere 以及相關聯的管理程式、控制器和 Edge。請注意，此移轉確實會影響數據平面流量，其設計為在單一變更時段內完成。

Automation、OpenStack 和其他 CMP

NSX-T 2.4 透過其 Neutron 外掛程式針對 OpenStack 耗用採用下列功能：

- Rocky 和 Queens 支援
- 管理平面叢集化支援
  OpenStack Neutron 外掛程式利用具有管理程式叢集的新功能。它可能會耗用不具有外部 VIP 的三個管理程式 REST API 端點，以獲得其他效能及更高的可用性。
- Barbican 支援
  OpenStack Neutron 外掛程式現在支援 Barbican。Barbican 是專為安全儲存、佈建和管理秘密 (例如密碼、加密金鑰和 X.509 憑證) 而設計的 REST API。這樣可以管理負載平衡器即服務的憑證，以便執行 HTTPS 終止。此功能目前僅在 VIO 環境中受支援。

在 NSX-T 2.4 中，NSX-T Terraform 提供者為已有項目新增了以下功能 (建立邏輯交換器、路由器、防火牆規則等)：

- 能夠支援負載平衡器上的 CRUD 以及負載平衡器組態 (監視器、集區等)。
- 能夠支援 DHCP 伺服器上的 CRUD
- 能夠支援 NSX-T IPAM 上的 CRUD (IP 區塊、IP 集區)

NSX Cloud

適用於 NSX Cloud 的 NSX-T 2.4 具有許多新功能，可以為客戶簡化採用/部署，提供更多有關客戶如何進行服務插入、VPN 終止、管理其 VDI 環境的選項，從而管理真正的多區域、多雲端混合部署。
NSX-T 2.4 具有 NSX Cloud 中的一些重要功能：

- 傳送 VPC/VNET 中的共用閘道，可簡化和加速上線與整併
- 用於將流量空載傳輸回內部部署 DC 的 VPN
- 選擇性南北向服務插入與合作夥伴整合
- Horizon Cloud for Azure 上的微分割
- 適用於混合工作負載的基於意圖的原則

簡化的傳送 VPC/VNET 架構：從 2.4 版開始，客戶可以在傳送 VPC/VNET 上安裝單一 NSX Cloud 閘道，並管理最多 10 個運算 VPC/VNET。這可簡化中樞和支點傳送/運算架構，並啟用計算 VPC 之間的轉移路由，即使這些 VPC 沒有對等連線。藉由使用 NSX 覆疊通道，VPC 之間的流量可以在覆疊通道中傳送。轉送原則可直接在虛擬機器層級設定，規定流量是否應為 Geneve 封裝並在覆疊中傳送，或其應該在公有雲提供者的底層網路中傳送。就使用者如何在其公有雲網路內部和外部路由流量而言，這些功能可提供更多彈性。

用於空載傳輸流量的 VPN：NSX Cloud 現在具有內建支援，可讓 VPN 通道將流量從公有雲空載傳輸到內部部署資料中心。現在可以在公有雲的 NSX Cloud 閘道中直接終止內部部署資料中心的 VPN。客戶不需要公有雲廠商所提供的 VGW，這樣可以降低成本。它還可以減少管理費用，因為 NSX Cloud 閘道會自動透過 BGP 傳播路由。從 BW 的觀點來看，NSX Cloud 也在容量方面產生了巨大的衝擊：透過對等 VPC，VPC 間流量可以達到 5Gbps，而透過 VGW 提供的流量僅為 1Gbps。

選擇性南北向服務插入與合作夥伴整合：客戶可以直接從共用服務/傳送架構中的公有雲市集部署合作夥伴服務。可以對傳送 VPC/VNET 中存在的 NSX Cloud 閘道進行程式設計，以根據 NSX 原則有選擇地將流量路由到合作夥伴服務應用裝置。這可以為客戶節省大量成本，因為他們不會被迫透過為公有雲購買的虛擬 L7 防火牆應用裝置來導向所有流量，該公有雲是根據通過它的流量進行計費的。如果這還不夠，使用 NSX Cloud 插入服務不需要透過 VPN 來計算 VPC/VNET。這樣可以節省更多成本，並減少運作。

Horizon Cloud for Azure 上的微分割：NSX Cloud 現在具有與 Horizon Cloud for Azure 結合的解決方案。對於選擇在 Azure 中部署 Horizon VDI 環境的客戶，NSX Cloud 將會提供必要的微分割，並確保 VDI 環境安全。

適用於混合工作負載的基於意圖的原則：Cloud Service Manager (CSM) 現在已與 NSX Manager 合併。客戶現在可以從 Policy Manager 定義單個基於意圖的原則，而無需擔心部署工作負載的位置或將來要移動的位置。NSX Cloud 將在內部部署 DC、Azure 和 AWS 之間以一致的方式實現此原則。

相容性和系統需求

如需相容性和系統需求資訊，請參閱《NSX-T Data Center 安裝指南》。

API 和 CLI 資源

請參閱 code.vmware.com 以使用 NSX-T Data Center API 或 CLI 進行自動化。

API 說明文件可從 API 參考索引標籤取得。CLI 說明文件可從說明文件索引標籤取得。

文件修訂歷程記錄

2019 年 2 月 28 日。第一版。
2019 年 4 月 2 日。第二版。已新增已知問題：2273651、2279326、2281095 和 2296888。已新增已修正的問題：2199785。
2019 年 4 月 10 日。第三版。已新增已知問題：2203863、2248186、2252738、2277543、2276398、2279326、2281537、2287124、2290688、2294178、2295592、2296430、2297157、2297918 以及 2298499。已更新「新增功能」區段，以包含單一叢集設計的支援。
2019 年 6 月 20 日。第四版。已新增已知問題 2261818。已新增已修正的問題 2182745。
2019 年 8 月 23 日。第五版。已新增已知問題 2362688、2395334 和 2392093。

已解決的問題

- 已修正的問題 1842511：Multihop-BFD 不支援靜態路由
  在 NSX-T 2.0 中，可為 (MH-BGP) Multihop BGP 芳鄰啟用 BFD (雙向轉送偵測)。在 NSX-T 2.0 中無法設定使用 BFD 來支援 Multihop 靜態路由的功能，只有 BGP 可以。請注意，如果您已設定由 BFD 支援的 Multihop BGP 芳鄰，並使用與 BGP 芳鄰相同的 Nexthop 來設定對應的 Multihop 靜態路由，則 BFD 工作階段狀態會同時影響 BGP 工作階段和靜態路由。

- 已修正的問題 2279326：建立具有 4 個以上 IP:PORT 組合的 IPFIX L2 收集器時，未顯示錯誤
  IP:PORT 組合允許的上限不會顯示錯誤訊息。若超過上限時，使用者介面會限制標籤建立，所以不會造成傷害。

- 已修正的問題 1931707：自動傳輸點功能要求叢集中的所有主機都具有相同的 pnics 設定
  自動傳輸點功能要求叢集中的所有主機都具有相同的 pnics 設定。範本中的所有 pnics 必須可供傳輸節點組態的所有主機使用，否則 pnics 遺失或遭佔用之主機上的傳輸節點組態可能失敗。

- 已修正的問題 1909703：NSX 管理員可在 OpenStack 直接從後端所建立的路由器中建立新的靜態路由、NAT 規則和連接埠
  在 NSX-T 2.0 提供的 RBAC 功能中，NSX 管理員無法從 NSX UI/API 直接刪除或修改由 OpenStack 外掛程式所建立的交換器、路由器、安全性群組等資源。這些資源只能由透過 OpenStack 外掛程式所傳送的 API 來加以修改/刪除。此功能有些限制。目前，NSX 管理員只是不能刪除/修改 OpenStack 所建立的資源，但管理員可以在 OpenStack 所建立的現有資源中建立新資源，例如靜態路由、NAT 規則。

- 已修正的問題 1989407：具有企業管理員角色的 vIDM 使用者無法覆寫物件保護
  具有企業管理員角色的 vIDM 使用者無法覆寫物件保護，且無法建立或刪除主體身分識別。

- 已修正的問題 2030784：無法使用包含非 ASCII 字元的遠端使用者名稱登入 NSX Manager
  您無法以具有包含非 ASCII 字元之使用者名稱的遠端使用者身分登入 NSX Manager 應用裝置。

- 已修正的問題 2111047：NSX-T 2.2 版中的 VMware vSphere 6.7 主機上不支援 Application Discovery
  在安全群組 (擁有 vSphere 6.7 主機上執行的虛擬機器) 上執行 Application Discovery 會導致探索工作階段失敗。

- 已修正的問題 2157370：設定含截斷的 L3 交換連接埠分析器 (SPAN) 時，特定的實體交換器會捨棄鏡像的封包
  設定含截斷的 GRE/ERSPAN 所屬的 L3 SPAN 時，因為實體交換器原則而會捨棄截斷的鏡像封包。可能的原因是連接埠正在接收封包，其中裝載中的位元組數不等於類型長度欄位。

- 已修正的問題 2174583：在 [入門] 精靈中，[設定傳輸節點] 按鈕無法在 Microsoft Edge 瀏覽器中正常運作
  在 [入門] 精靈中，按一下 [設定傳輸節點] 按鈕後，Microsoft Edge 網頁瀏覽器會失敗並顯示發生 JavaScript 錯誤。

- 已修正的問題 2114756：在某些情況下，從 NSX-T 備妥的叢集中移除主機時不會移除 VIB
  從 NSX-T 備妥的叢集中移除主機時，部分 VIB 可能會保留在主機上。

- 已修正的問題 2059414：由於 python-gevent RPM 的版本較舊，RHEL LCP 服務包安裝會失敗
  如果 RHEL 主機包含較新版本的 python-gevent RPM，RHEL LCP 服務包安裝會失敗，因為 NSX-T Data Center RPM 包含較舊版本的 python-gevent RPM。

- 已修正的問題 2142755：OVS 核心模組無法安裝，視正在執行的次要 RHEL 7.4 核心版本而定
  無法在執行次要核心 17.1 版或更高版本的 RHEL 7.4 主機上安裝 OVS 核心模組。安裝失敗會使核心資料路徑停止運作，這會導致應用裝置管理主控台變得無法使用。

- 已修正的問題 2125725：還原大型拓撲部署後，搜尋資料變得不同步，且數個 NSX Manager 頁面無回應
  還原具有大型拓撲部署的 NSX Manager 後，搜尋資料變得不同步，且數個 NSX Manager 頁面會顯示錯誤訊息：發生無法復原的錯誤。

- 已修正的問題 2187888：從 NSX Manager 使用者介面自動部署的 NSX Edge 會無限期保持登錄擱置中狀態
  從 NSX Manager 使用者介面自動部署的 NSX Edge 會無限期保持登錄擱置中狀態。此狀態會導致 NSX Edge 變得無法用於進一步設定。

- 已修正的問題 2077145：在某些情況下，嘗試強制刪除傳輸節點可能會導致孤立傳輸節點
  使用 API 呼叫嘗試強制刪除傳輸節點造成問題，例如發生硬體故障且主機變得無法擷取、將傳輸節點狀態變更為孤立。

- 已修正的問題 2099530：變更橋接器節點 VTEP IP 位址導致流量中斷
  當橋接器節點 VTEP IP 位址變更時，在遠端 Hypervisor 上未更新從 VLAN 至覆疊的 MAC 資料表，導致流量中斷長達 10 分鐘。

- 已修正的問題 2106176：在安裝的「正在等待登錄」步驟期間，NSX Controller 自動安裝會停止
  使用 NSX Manager API 或 UI 執行 NSX Controller 自動安裝期間，其中一個進行中的 NSX Controller 的狀態會停止，且無限期顯示為 [正在等待登錄]。

- 已修正的問題 2125514：第 2 層橋接器容錯移轉後，某些 NSX Edge 虛擬機器上的邏輯交換器可能會對每個單一封包執行 BUM 複寫，直到重新學習 MAC
  第 2 層橋接器容錯移轉後，某些 NSX Edge 虛擬機器上的邏輯交換器可能會對每個單一封包執行 BUM 複寫將近 10 分鐘，直到為端點重新學習 MAC。端點產生下一個 ARP 後，系統復原本身。

- 已修正的問題 2183549：在編輯集中式服務連接埠時，無法檢視新建立的 VLAN 邏輯交換器

在 Manager UI 中，建立集中式服務連接埠和新的 VLAN 邏輯交換器後，如果您編輯集中式服務連接埠，則無法看到新建立的 VLAN 邏輯交換器。

- 已修正的問題 2186040：如果傳輸節點不在系統中的前 250 個上行設定檔中，則會在使用者介面中停用實體 NIC 的上行下拉式清單
  如果傳輸節點不在系統中的前 250 個上行設定檔中，則會在使用者介面中停用實體 NIC 的上行下拉式清單。儲存傳輸節點導致從傳輸節點移除上行名稱。

- 已修正的問題 2106635：建立靜態路由期間，變更 NULL 路由的管理距離會導致下一個躍點 NULL 設定從使用者介面中消失
  建立靜態路由期間，如果您將下一個躍點設定為 NULL 且變更 NULL 路由的管理距離，下一個躍點 NULL 設定會從使用者介面中消失。

- 已修正的問題 1928376：還原 NSX Manager 後，Controller 叢集成員節點的狀態會降級
  如果將 NSX Manager 還原至從叢集卸離此成員節點之前製作的備份映像，控制器叢集成員節點可能會變得不穩定並回報健全狀況狀態已降級。

- 已修正的問題 2128361：用於將 NSX Manager 的記錄層級設定為偵錯模式的 CLI 命令未正常運作
  使用 CLI 命令 set service manager logging-level debug 將 NSX Manager 的記錄層級設定為偵錯模式時，不會收集偵錯記錄資訊。

- 已修正的問題 1940046：在多個第 1 層邏輯路由器中新增相同的靜態路由並通告時，東-西向流量失效
  在多個第 1 層邏輯路由器中新增相同的靜態路由並通告時，東-西向流量失效。

- 已修正的問題 2160634：變更回送上的 IP 位址可以變更上行上的路由器識別碼的 IP 位址
  如果已變更回送上的 IP 位址，NSX Edge 會選取上行上的 IP 位址做為路由器識別碼。無法變更已指派為路由器識別碼的上行的 IP 位址。

- 已修正的問題 2199785：將健全狀況監控 (不含連接埠號碼) 新增至動態集區 (具有連接埠號碼) 時，發現 NGINX 核心。
  當使用具有動態成員 (具有連接埠號碼) 的伺服器集區設定負載平衡，然後嘗試將其與沒有設定任何監控連接埠的健全狀況監視器相關聯時，nginx 可能會當機。

- 已修正的問題 2182745：重新分配規則中的 le/ge 先前未在管理程式中進行驗證且未正常運作
  重新分配規則支援 prefixlist 中的 le/ge。

已知問題

已知問題分類如下。

- 一般已知問題
- 安裝已知問題
- NSX Manager 已知問題
- NSX Edge 已知問題
- 邏輯網路已知問題
- 安全服務已知問題
- KVM 網路已知問題
- 負載平衡器已知問題
- 解決方案互通性已知問題
- 作業和監控服務已知問題
- 升級已知問題
- API 已知問題
- NSX Policy Manager 已知問題
- NSX Cloud 已知問題

一般已知問題

- 問題 2239365：撤回「未經授權」錯誤
  由於使用者嘗試在同一瀏覽器類型上開啟多個驗證工作階段，可能會導致此錯誤。如此一來，登入將會失敗並顯示上述錯誤，且無法進行驗證。記錄位置：`/var/log/proxy/reverse-proxy.log` `/var/log/syslog`

  因應措施：關閉所有開啟的驗證視窗/索引標籤，然後重試驗證。

- 問題 2287482：[自動探索的繫結] 表中可能包含目前未探索的繫結
  可能不會再探索 [自動探索的繫結] 表中標記為「重複」的繫結。

  因應措施：無。

- 問題 2278142：交換器 IPFIX 全域設定檔無法編輯
  如果全域設定檔在系統中可用，您無法透過介面進行修改或刪除，因為全域設定檔沒有對應的工作流程。

  因應措施：使用 API 刪除此類全域設定檔。

- 問題 2292222：在 [解決錯誤] 畫面上，如果指紋不正確，不會通知使用者
  如果主機準備作業失敗，使用者可以透過按一下 [NSX 安裝失敗] 來解決問題，在此情況下需要提供主機的使用者名稱、密碼和指紋。如果使用者提供的指紋不正確，系統不會通知使用者，此問題仍未解決。

  沒有明確的方法可以知道指紋是不正確的。檢查已記錄此 ThumbPrintValidationFailedException 的記錄。

  因應措施：提供正確的指紋。

- 問題 2252487：同時新增多個 TN 時，不會針對 BM Edge 傳輸節點儲存傳輸節點狀態
  傳輸節點狀態在 MP 使用者介面中未正確顯示。

  因應措施：

  1. 將 proton 重新開機，可以正確更新所有傳輸節點狀態。
  2. 或者，使用 API https://<nsx-manager>/api/v1/transport-nodes/<node-id>/status?source=realtime 查詢傳輸節點狀態。

- 問題 2285117：不支援在 NSX 管理的虛擬機器上進行核心升級
  在某些 Linux Ubuntu 市集映像中，核心會在虛擬機器重新開機時自動升級。因此，nsx-agent 不會按預期運作。雖然 NSX 代理程式可能看起來運作正常，但有部分未實現的網路原則會影響 nsx-agent。代理程式一再重試以實現這些原則，從而導致 CPU 使用率偏高。

  因應措施：如果需要進行核心升級，則必須首先下載適用於較新核心的 Linux 標頭，並且需要重新編譯 openvswitch 資料路徑 dkms 套件。

- 問題 2285544：叫用需要指定 ssh_fingerprint 值的 NSX API 時，不再支援 MD5 雜湊
  NSX-T 2.4 不再支援非 FIPS 加密演算法、雜湊等，其中包括叫用備份/還原、file-store 和支援服務包 NSX API，以及為 ssh_fingerprint 值指定 MD5 雜湊。如此一來，不再支援 MD5 雜湊。

  因應措施：指定使用不同雜湊演算法 (例如 SHA256) 計算的其他雜湊。

- 問題 2256709：在執行 vMotion 期間，即時複製虛擬機器或從快照還原的虛擬機器會暫時失去 AV 保護
  還原虛擬機器的快照，並將虛擬機器移轉到另一台主機。合作夥伴主控台沒有針對已移轉的即時複製虛擬機器顯示 AV 保護。已暫時失去 AV 保護。

  因應措施：無。

- 問題 2261431：根據其他部署參數，需要篩選過的資料存放區清單
  如果選取了不正確的選項，使用者介面上會顯示相應的錯誤。客戶可以刪除此部署並建立新部署，以從錯誤中復原。

因應措施：如果您要建立叢集部署，請選取共用資料存放區。

- 問題 2266553：在 NSX 應用裝置中，服務可能無法在其首次開機時初始化
  已部署的節點無法滿足要求，或無法形成叢集。

  因應措施：請嘗試重新啟動失敗的服務。

- 問題 2267632：GI 保護組態遺失
  在原則使用者介面上發佈的客體保護規則顯示 [成功]。行為的相應變更未反映在客體虛擬機器中。OpsAgent 記錄同時顯示重新啟動。客體虛擬機器保護遺失。

  因應措施：手動重新執行組態變更。

- 問題 2269901：封包擷取 CLI 中不包含 vmk 介面
  無法發出此命令。

  因應措施：使用封包擷取 uw 執行相同動作。

- 問題 2274988：服務鏈結不支援來自同一服務的連續服務設定檔
  流量不會周遊服務鏈結，只要鏈結具有屬於同一服務的兩個連續服務設定檔，它就會遭到捨棄。

  因應措施：從不同的服務中新增服務設定檔，以確保沒有兩個連續服務設定檔屬於同一服務。或者，定義第三個服務設定檔，此設定檔將針對兩個串連的原始設定檔執行相同的作業，然後在服務鏈結中單獨使用第三個設定檔。

- 問題 2275285：在第一個要求完成且叢集穩定之前，節點提出加入同一叢集的第二個要求
  叢集無法正常運作，並且 CLI 命令 get cluster status、get cluster config 可能會傳回錯誤。

  因應措施：在第一個加入要求後，請勿在 10 分鐘內發出任何新的加入命令以加入同一叢集。

- 問題 2275388：在新增篩選器以拒絕路由之前，回送介面/已連線介面路由會進行重新分配
  不必要的路由更新可能會導致流量轉移持續幾秒到幾分鐘的時間。

  因應措施：無。

- 問題 2275708：如果憑證的私密金鑰具有複雜密碼，無法使用此私密金鑰匯入憑證
  傳回的訊息為「針對憑證收到無效的 PEM 資料。(錯誤碼: 2002)」。無法使用私密金鑰匯入新憑證。

  因應措施：

  1. 使用私密金鑰建立憑證。當系統提示時，請勿輸入新的複雜密碼；而是按 Enter。
  2. 選取 [匯入憑證]，然後選取憑證檔案和私密金鑰檔案。

  透過開啟金鑰檔案進行驗證。如果在產生金鑰時輸入了複雜密碼，檔案中的第二行會顯示類似「Proc-Type: 4,ENCRYPTED」的內容。

  如果在產生金鑰檔案時沒有使用複雜密碼，則這一行會遺失。

- 問題 2275985：未連線至邏輯交換器的 vNIC 會列為 NSGroup 直接成員的選項
  未連線至邏輯交換器的 vNIC 會新增做為 NSGroup 的直接成員。作業成功，但該群組上套用的原則不會在 vNIC 上強制執行。

  因應措施：無。

  將 vNIC 新增為 NSGroup 的直接成員之前，確認此 vNIC 是否已連線到邏輯交換器。

- 問題 2277742：如果 NSX-T Manager 應用裝置已設定完整網域名稱 (FQDN) 而不僅僅是主機名稱，則使用將 publish_fqdns 設定為 true 的要求本文叫用 PUT https://<MGR_IP>/api/v1/configs/management 可能會失敗
  如果已設定 FQDN，則無法叫用 PUT https://<MGR_IP>/api/v1/configs/management。

因應措施：使用主機名稱而非 FQDN 來部署 NSX Manager。

- 問題 2279249：在執行 vMotion 期間，即時複製虛擬機器失去 AV 保護
  即時複製虛擬機器已從一台主機移轉到另一台主機。在移轉之後，eicar 檔案隨即遺留在虛擬機器上。暫時失去 AV 保護。

  因應措施：無。

- 問題 2290669：隨著虛擬伺服器數目的增加，每個伺服器的組態時間也會增加
  隨著虛擬伺服器數目的增加，每個伺服器的組態時間會因大量驗證而有所增加。對於前 100 個虛擬伺服器，平均回應時間約為 1 秒。在 250 個虛擬伺服器之後，平均回應時間會增加到 5 至 10 秒。在 450 個虛擬伺服器之後，回應時間會增加到大約 30 秒。

  因應措施：無。您可以根據拓撲將虛擬伺服器設定為多個 LbService，否則，在使用虛擬伺服器進行大規模設定時，預期回應速度會變慢。

- 問題 2292116：透過 IPFIX L2 頁面建立群組時，套用至以 CIDR 為基礎的 IP 位址群組的 IPFIX L2 未在使用者介面上列出
  如果嘗試從 [套用至] 對話方塊建立一組 IP 位址，並且在 [設定成員] 對話方塊中輸入錯誤的 IP 位址或 CIDR，則這些成員不會列在群組下。您必須再次編輯該群組以輸入有效的 IP 位址。

  因應措施：移至群組清單頁面，並在該群組中新增 IP 位址。接著，該群組會開始填入 [套用至] 對話方塊中。

- 問題 2294821：NSX 應用裝置資訊顯示在叢集監控儀表板中，出現「無法刪除節點」錯誤，但沒有可供使用者處理此情況的指引。
  使用者嘗試透過介面刪除自動部署的節點且關閉該節點的電源失敗後，會出現此問題。如果叢集遺失節點，您必須使用以下因應措施手動新增節點並清理組態狀態。

  因應措施：一旦透過 API/UI 刪除應用裝置失敗，請使用 force-delete API 手動刪除該應用裝置，如下所示：
  `POST api/v1/cluster/nodes/deployments/467a102d-472f-4f43-a93c-08b992b9f471?action=delete&force_delete=true`
  之後，從 vCenter 終結虛擬機器。

- 問題 2281095：將部署了 svm 的主機重新新增到同一叢集時，不從 EAM 觸發回撥
  所有客體虛擬機器可能不受保護。NSX UI 始終顯示進行中狀態。

  因應措施：從主機移除 SVM，然後再將其新增至叢集。

- 問題 1957072：橋接器節點的上行設定檔應該一律對多個上行使用 LAG
  使用未構成 LAG 的多個上行時，流量無法達到負載平衡，且可能無法正常運作。

  因應措施：在橋接器節點上針對多個上行使用 LAG。

- 問題 1970750：搭配使用 LACP 與快速計時器的傳輸節點 N-VDS 設定檔不會套用至 vSphere ESXi 主機
  設定採用快速速率的 LACP 上行設定檔並套用至 NSX Manager 上的 vSphere ESXi 傳輸節點時，NSX Manager 顯示已成功套用此設定檔，但 vSphere ESXi 主機使用的是預設 LACP 緩慢計時器。在 vSphere Hypervisor 上，當傳輸節點上使用來自 NSX Manager 的 LACP NSX 受管理分散式交換器 (N-VDS) 設定檔時，您無法查看 LACP 逾時值 (SLOW/FAST) 的效果。

  因應措施：無。

- 問題 2261818：從 eBGP 芳鄰學習的路由會通告回到相同的芳鄰
  啟用 BGP 偵錯記錄會指出正在重新接收的封包以及遭到捨棄的封包，並且顯示錯誤訊息。BGP 程序在捨棄傳送給對等的更新訊息時會耗用額外的 CPU 資源。如果存在大量的路由和對等，這會影響路由聚合。

  因應措施：無。

安裝已知問題

- 問題 2238093：如果 NSX 套件已強制移除，則不支援解析程式
  若要從主機解除安裝 NSX，會強制移除 NSX 套件。這可能會導致 NSX 套件的損毀狀態。如果在解析程式之前強制移除 NSX 套件，則適用於 NSX 套件安裝的解析程式可能無法成功運作。記錄位置：`/var/log/proton/nsxapi.log`

  因應措施：無。

  不要強制移除 NSX 套件。透過 NSX 說明文件中所述的標準步驟來解除安裝 NSX 元件。

- 問題 2288872：安裝狀態顯示為 [節點未就緒]
  Edge 節點並未上線。傳輸節點組態狀態為 [擱置中]，因此無法新增至 Edge 叢集。記錄位置：`/var/log/proton/nsxapi.log`

  因應措施：重試 Edge 節點登錄。或者，關閉 Edge 節點的電源。啟動時，它會建立 MP-MPA 通道。

- 問題 2252776：即使現已解決先前在主機上發生的驗證錯誤，傳輸節點設定檔也無法套用到其中一個叢集成員主機上
  在叢集上套用 TNP。但無法在其中一個叢集成員主機上套用 TNP，因為其中一個驗證可能無法通過 (例如，已在主機上開啟虛擬機器電源)。使用者解決了此問題，但驗證仍顯示在使用者介面上，並且 TNP 不會自動套用於該主機上。

  因應措施：將主機移出叢集，然後再次新增它。這會觸發在主機上套用傳輸節點設定檔的活動。

- 問題 2284683：刪除並再次新增已登錄的計算管理程式時，無法刪除自動部署的應用裝置
  刪除應用裝置失敗，並顯示錯誤「無法關閉電源」指示找不到計算管理程式。

  因應措施：一旦透過 API/UI 刪除應用裝置失敗，請使用 force-delete API 手動刪除該應用裝置，如下所示：POST api/v1/cluster/nodes/deployments/<node-id>?action=delete&force_delete=true。從 VC 終結虛擬機器。

- 問題 1957059：嘗試進行主機取消準備時，如果將包含現有 VIB 的主機新增至叢集，則取消準備會失敗
  將主機新增至叢集之前，如果未完全移除 VIB，則主機取消準備作業會失敗。

  因應措施：請確定主機上的 VIB 已完全移除，並重新啟動主機。

- 問題 2296888：傳輸節點 (TN)/傳輸節點設定檔 (TNP) 組態不能將「僅限 PNIC 的移轉」旗標設為 true，也不能將用於安裝的 VMK 對應填入主機交換器
  在建立期間提供不相符的組態時 (「僅限 PNIC 的移轉」旗標設為 true 以及用於安裝的 VMK 對應填入所有主機交換器)，會出現下列例外狀況：

  主機 b17afc36-bbdc-491a-b944-21f73cf91585 的 VMK 移轉失敗，並顯示錯誤 [com.vmware.nsx.management.switching.common.exceptions.SwitchingException: 將 ESX VMK 介面 NULL 移轉至 [null] 時，無法更新或刪除 TransportNode [TransportNode/b17afc36-bbdc-491a-b944-21f73cf91585]。]。(錯誤碼: 9418)

  在更新期間，提供不相符的組態時，會出現下列例外狀況：
  一般錯誤 (錯誤碼：400)

  套用包含「僅限 PNIC 的移轉」旗標設為 true 以及 VMK 移轉對應的 TN/TNP 組態時，會出現例外狀況。

  因應措施：每個傳送至主機的組態可以將「僅限 PNIC 的移轉」旗標設為 true 或將用於安裝的 VMK 對應填入主機交換器，但不能兩者皆是。

  1. 使用需要將「僅限 PNIC 的移轉」旗標設為 true 的主機交換器傳送 TN 組態。
  2. 將所有「僅限 PNIC 的移轉」旗標都設為 false，並視需要填入用於安裝的 VMK 對應來更新 TN 組態。

換句話說，確保設定傳送到 TN 的組態僅將「僅限 PNIC 的移轉」旗標設為 true，或將用於安裝的 VMK 對應填入所有主機交換器。兩個獨立的組態呼叫必須針對需要這兩者的任何組態進行設定。

- 問題 2273651 - 刪除傳輸節點後，使用者將無法透過 SSH 存取主機。
  在 KVM 實作中觀察到。使用者刪除傳輸節點，並收到刪除成功訊息。但是，之後使用者就無法透過 SSH 存取相同的主機。此問題可能是因為具有不受 NSX-T 管理的 Open vSwitch (OVS)，且可能預先安裝為 KVM 範本的一部分。

  因應措施：刪除傳輸節點前識別有問題的 OVS。

  1. 執行 `ovs vsctl` 以識別 OVS。
  2. 將任何工作負載的虛擬機器介面從 OVS 移轉至 Linux 橋接器。
  3. 刪除傳輸節點，如下所示：
     `DELETE api/v1/transport-nodes/<uuid>`
- 問題 2281537 - 移轉後，具有多 VTEP 的 ESXi 傳輸節點無法啟動 BFD 工作階段。
  將 NSX-V 節點移轉至 NSX-T 後，具有多 VTEP 的 ESXi 傳輸節點無法啟動所有 VTEP 上的 BFD 工作階段至 Edge 節點。

  因應措施：重新啟動 netcpa 服務。

NSX Manager 已知問題

- 問題 2285306：Guest Introspection 服務的服務部署狀態可能會保持「未知」狀態，直到服務虛擬機器開啟電源為止
  建立服務部署並在 [服務部署] 網格中列出之後，狀態可能不會立即顯示為「進行中」並且可能會保持「未知」，直到重新整理網格為止。

  因應措施：無。10 秒後重新整理頁面。狀態應該會更新。

- 問題 2292526：新增主機時，顯示「主機無法連線」訊息
  新增 ESXi 主機時，會顯示「主機無法連線」訊息，但不會指定原因。可能的原因是認證不正確。

  因應措施：檢閱主機組態，重做認證，然後重試新增主機。

- 問題 2292701：使用者無法更新繫結對應中的序號
  使用者無法透過更新序號來變更套用到實體的設定檔的排序或優先順序。

  因應措施：刪除繫結對應並使用新的所需序號重新建立。

- 問題 2294345：在具有 ESXi 主控和 KVM 主控的虛擬機器的群組上執行 Application Discovery 分類可能會失敗
  僅 ESXi Hypervisor 支援 Application Discovery 功能。對於混合主機 (包含不受支援的主機) 上的虛擬機器群組，無法保證 Application Discovery 分類結果。

  因應措施：無。

NSX Edge 已知問題

- 問題 2248345：安裝 NSX-T Edge 後，機器會開機並顯示空白的黑色畫面。
  無法在 HPE ProLiant DL380 Gen9 機器上安裝 NSX-T Edge。

  因應措施：請使用其他機器，或將 NSX-T Edge 部署做為 Hypervisor 上的虛擬機器。

- 問題 2283559：如果 Edge 具有 RIB 的 65k+ 個路由以及 FIB 的 100k+ 個路由，/routing-table 和 /forwarding-table MP API 會傳回錯誤
  如果 Edge 具有 65k+ 個路由用於 RIB 以及 100k+ 個路由用於 FIB，則從 MP 到 Edge 的申請需要超過 10 秒並導致逾時。這是一個唯讀 API，只有當他們需要使用 API/使用者介面下載 RIB 的 65k+ 個路由以及 FIB 的 100k+ 個路由時才會產生影響。

因應措施：有兩個選項可供擷取 RIB/FIB。

- 這些 API 支援根據網路首碼或路由類型篩選選項。請使用這些選項來下載所需路由。
- CLI 支援，以防需要整個 RIB/FIB 資料表並且沒有逾時。

邏輯網路已知問題

- 問題 2243415：客戶無法使用邏輯交換器 (做為管理網路) 來部署 NXGI 服務
  在 NXGI 部署畫面上，使用者無法在網路選擇控制項中查看邏輯交換器。如果 API 直接與提及做為管理網路的邏輯交換器搭配使用，則使用者會看到下列錯誤：「用於服務部署的指定網路無法存取」。

  因應措施：使用本機交換器或分散式交換器等其他類型的交換器進行部署。

- 問題 2264386：即使傳輸節點是 NS 群組的一部分，也會執行傳輸節點刪除
  即使節點是 NS 群組的一部分，也允許刪除傳輸節點。應阻止刪除。如果您遇到此問題，則必須重新建立 NS 群組並重建與其傳輸節點的關係。

  因應措施：若要避免此問題，請手動確認傳輸節點是否已與任何 NS 群組相關聯。在管理平面介面中，導覽至**進階網路與安全性** > **詳細目錄** > **群組**或**系統** > **節點** > **傳輸節點** > **相關** > NSGroup。

- 問題 2292997：可能無法為 Linux 網路堆疊建立某些邏輯路由器介面
  可能無法為 Linux 網路堆疊建立某些邏輯路由器介面，並傳回下列錯誤：`errorCode="EDG0100002"`, **建立子介面作業失敗： 已超過子介面上限**。如此一來，由第 0 層服務路由器 (T0 SR) 轉送的流量可能由於遺失路由而遭到捨棄。

  因應措施：將受影響的 Edge 節點重新開機。

- 問題 228688：如果已透過 VTI 設定 BPG，應首先刪除 BGP 芳鄰，同時刪除 IPsec 路由基礎工作階段
  如果透過 VTI 設定 BGP 並刪除 IPsec 工作階段，則這兩個 SR 將處於關閉狀態，從而封鎖流量。若要恢復流量，應刪除為 VTI 設定的 BGP 芳鄰。在此案例中，僅設定的 BGP 是透過 VTI 的。

  因應措施：請先刪除 BGP 芳鄰，再刪除 IPsec 工作階段。

- 問題 2288509：Tier0/Tier1 服務介面 (中央服務連接埠) 不支援 MTU 內容
  Tier0/Tier1 服務介面 (中央服務連接埠) 不支援 MTU 內容。

  因應措施：即使 CSP 連接埠是透過原則工作流程建立的，也使用管理平面 API 設定 MTU。

- 問題 2288774：由於標籤數超過 30 個 (錯誤地)，區段連接埠出現實現錯誤
  使用者輸入錯誤地嘗試套用 30 個以上的標籤。但是，原則工作流程未正確驗證/拒絕使用者輸入並允許設定。然後，此原則會顯示警示以及相應的錯誤訊息，指示使用者不應使用 30 個以上的標籤。此時，使用者可以更正此問題。

  因應措施：出現錯誤之後，更正組態。

- 問題 2275412：連接埠連線無法在多個 TZ 中運作
  連接埠連線只能用於單一 TZ。

  因應措施：無。

- 問題 2290083：建立基於 VLAN 的區段時缺少驗證
  當您使用 VLAN 識別碼內容指定 VLAN 傳輸區域時，系統無法驗證並找出錯誤。因此，意圖將在實現期間失敗並引發錯誤。

  因應措施：如需修正輸入的指示，請參閱實現警示錯誤詳細資料。

- 問題 2292096：CLI 命令「get service router config route-maps」傳回空白輸出

即使已設定路由對應，CLI 命令「get service router config route-maps」仍傳回空白輸出。這只是一個顯示問題。

因應措施：使用 CLI 命令 `get service router config`，該命令會傳回路由對應組態以做為整個輸出的子集。

- 問題 2994002：Tier1 未列在 [Tier0/Tier1 閘道] 下拉式清單中，以便在 DNS 轉寄站建立時可供選取
  在具有數千條記錄的大型部署中，Tier1 未列在 [Tier0/Tier1 閘道] 下拉式清單中，以便在 DNS 轉寄站建立工作流程中可供選取。因此，您必須使用 API 來設定 DNS 轉寄站建立。

  因應措施：使用 API 執行組態。

- 問題 2298499 - 如果閘道未使用公用 IP 部署，VPN 會在公用雲端閘道和對等主機之間失敗。
  如果在上行中不使用公用 IP 位址部署 PCG，則無法建立公用雲端閘道 (PCG) 與對等主機之間的 VPN 通道。原因是依預設 PCG 會在 VPN 流量中執行 SNAT。

  因應措施：在部署公用雲端閘道時，啟用上行介面的公用 IP。

- 問題 2392093：流量因 RPF 檢查而導致下降
  如果流量透過 T0 下行 Hairpin，而第 0 層和第 1 層路由器位於相同的 Edge 節點上，則 RPF 檢查可能會導致流量下降。

  因應措施：無。

安全服務已知問題

- 問題 2288523：解除載入 NSX Guest Introspection 驅動程式可能會導致安全性問題
  IDFW 依賴於 NSX Guest Introspection 驅動程式中的使用者身分識別資訊。解除載入驅動程式可能會導致從特定客體登入的使用者出現安全性問題。這將顯示為下列症狀：
  - 對於從解除載入 Guest Introspection 驅動程式的某些客體虛擬機器登入的使用者，不強制執行防火牆規則。
  - 對於從解除載入 Guest Introspection 驅動程式的某些客體虛擬機器登入的使用者，沒有在使用者詳細資料中記錄 IDFW 元件。
  - 即使在主機上啟用了 IDFW，MUX 記錄也不會顯示來自這些客體虛擬機器的任何連線。
  - 即使在主機上啟用了 IDFW，MUX 記錄也不會顯示來自這些客體虛擬機器的任何網路事件。

  因此，預設拒絕所有規則可以封鎖從解除載入 Guest Introspection 驅動程式的客體虛擬機器登入的使用者的存取權限。

  因應措施：無。IT 管理員應遵循安全性最佳做法，以確保沒有使用者被授與在客體虛擬機器內解除載入 Guest Introspection 驅動程式的權限。

- 問題 2288773：舊的 TLS 通訊協定 API 仍然可用，將被覆寫
  NSX-T 具有用於設定 NSX TLS 通訊協定版本和加密套件的新 API，可以更新 NSX-T 叢集中的所有節點。但是，舊 API 仍然可用。可以使用這個舊 API，但是新設定將被全域設定覆寫。

  因應措施：請使用新 API。

- 問題 2291872： 在防火牆規則中使用 TFTP 服務時，記錄訊息會顯示一則警告訊息
  在防火牆規則中使用 TFTP 服務時，記錄訊息會顯示不相關的警告訊息。ESXi 節點上的記錄位置：`/var/log/cfgAgent.log`。

  因應措施：建立 TFTP 的新服務做為 L4PortSet 服務，並且在防火牆規則中使用此服務。

- 問題 2203863 - UDP 和 ICMP 流量不支援身分識別防火牆規則。
  身分識別防火牆規則不適用於 Ping 測試。TCP 流量僅支援目前的功能。

因應措施：使用 TCP 來測試身分識別防火牆規則。在設定身分識別防火牆規則時，永遠不要設定 [服務] 資料行中的 ANY/UDP/ICMP

- 問題 2296430 - 憑證產生期間，NSX-T Manager API 不提供主體替代名稱。
  NSX-T Manager API 不會提供主體替代名稱以核發憑證，特別是 CSR 產生期間。

  因應措施：使用支援延伸的外部工具建立 CSR。收到憑證授權機構的已簽署憑證後，使用 CSR 的金鑰將其匯入 NSX-T Manager。

- 問題 2252738 - 對於完整網域名稱 (FQDN) 的規則，允許不符合規則的封包到達目的地。
  建立特定的 FQDN 規則時，與 IP 位址相關聯的網域名稱會新增至符合規則的防火牆資料庫，且允許傳送到該網域名稱的封包連線到伺服器。但是，如果使用者在網域名稱伺服器上變更與該 IP 位址相關聯的網域名稱，網域名稱項目不會更新在防火牆資料庫中 (除非另一個符合新網域名稱的 FQDN 規則已存在)。如此一來，封包會傳送到新網域名稱，即使 FQDN 規則應該將其捨棄。

  因應措施：無。

- 問題 2395334 - (Windows) 封包因無狀態防火牆規則 conntrack 項目而誤遭捨棄。
  Windows 虛擬機器上的無狀態防火牆規則未受到妥善支援。

  因應措施：改為新增可設定狀態的防火牆規則。

- 問題 2458384 - NSX-T Manager 介面頁面載入失敗，並顯示 403 錯誤。
  問題出現在 2.4.0 和 2.4.1 發行版本中。此問題對管理員和 Identity Manager 登入都會造成影響。NSX-T Manager 的 FQDN 使用 *.SLD.TLD 格式。例如：*.co.uk、*.co.il、*.com.au 等。

  因應措施：使用簡短名稱或 IP (而非 FQDN) 存取 NSX-T Manager UI。請參閱 https://kb.vmware.com/s/article/71217。

KVM 網路已知問題

- 問題 2292995：即使已設定的所有規則均在 OVS 中進行程式設計，實現狀態仍設定為錯誤
  即使 DFW 規則在數據平面中進行程式設計，API 也會顯示誤報。

  因應措施：任何 DFW 規則的更新都會清除此錯誤狀況。例如，只切換規則記錄會強制 KVM DFW 模組清除錯誤狀況。

負載平衡器已知問題

- 問題 2290899：IPSec VPN 無法運作，IPSec 的控制平面實現失敗
  如果在同一 Edge 節點上的 Tier-0 上啟用了超過 62 個 LbServer 以及 IPSec 服務，則 IPSec VPN (或 L2VPN) 無法啟動。

  因應措施：將 LbServer 數目減少至少於 62 個。

- 問題 2297157 - 負載平衡 HTTPS 效能受到 FIPS 模式的影響。
  啟用預設 FIPS 模式時，負載平衡的效能可能會受到負面影響。

  因應措施：如需因應措施，請參閱知識庫文章 67400：NSX-T 2.4.0 Load Balance Service may observe low performance on HTTPs (NSX-T 2.4.0 負載平衡服務可能會在 HTTP 上造成效能低落)。

- 問題 2362688：當負載平衡器服務中的某些集區成員「關閉」時，UI 會將整併狀態顯示為「啟動」
  當集區成員關閉時，原則 UI 上不會指出集區處於綠色的「啟動」狀態。

  因應措施：無。

解決方案互通性已知問題

- 問題 2289150：PCM 呼叫 AWS 無法啟動

如果您將 CSM 上的 AWS 帳戶的 PCG 角色從 *old-pcg-role* 更新為 *new-pcg-role*，CSM 會將 AWS 上 PCG 執行個體的角色更新為 *new-pcg-role*。但是，PCM 不知道 PCG 角色已更新，因此，會繼續使用已使用 *old-pcg-role* 建立的舊 AWS 用戶端。這會導致 PCM AWS 雲端詳細目錄掃描及其他 AWS 雲端呼叫失敗。

因應措施：如果您遇到此問題，請至少在變更為新角色 6.5 小時後再修改/刪除舊 PCG 角色。重新啟動 PCG 將使用新角色認證重新初始化所有 AWS 用戶端。

作業和監控服務已知問題

- 問題 2275869：如果 ESXi 主機上的規則標籤長度超過 31 個字元，則該主機上的 cfgAgent 記錄會在 1 分鐘內變換
  頻繁的記錄變換可能會導致 cfgAgent.log 中用於在主機上進行偵錯和疑難排解的有用資訊遺失。ESXi 主機上的記錄位置：`/var/log/cfgAgent.log`

  因應措施：無。

- 問題 2289984：即使 nsx-context-mux 服務在主機上已停止，mux_connectivity_status 仍顯示為已連線
  當 nsx-context-mux 或 nsx-opsagent 未在主機上執行時，系統 (NSX 介面或服務執行個體 API) 會錯誤地將解決方案狀態和 GI 代理程式狀態顯示為在未變更時間戳記的情況下執行。因此，客體虛擬機器可能會失去 AV 保護。

  因應措施：請嘗試在主機上手動啟動 mux 和 opsagent (如果尚未執行)。

  1. 以根使用者身分登入主機，並執行下列命令：
     `/etc/init.d/nsx-opsagent start`
     `/etc/init.d/nsx-context-mux start`
  2. 啟動代理程式後，請等待幾分鐘的時間，並確認使用者介面上的健全狀況狀態時間戳記已更新。

升級已知問題

- 問題 2273737：從 NSX-T 2.3 升級至 2.4 之後，vIDM 伺服器詳細資料遺失
  如果使用 vIDM，即僅在 NSX 原則應用裝置上設定 vIDM 伺服器的情形下，會在升級中移轉 vIDM 伺服器，但 vIDM 伺服器將從聚合式應用裝置中遺失。

  因應措施：提供兩個選項，具體取決於客戶何時遇到此問題：

  - 從 2.3 版升級至 2.4 版之前：
    在 NSX 原則應用裝置和 NSX Manager 虛擬機器上設定相同的 vIDM 伺服器詳細資料。
  - 從 2.3 版升級至 2.4 版之後：
    在聚合式應用裝置上重新設定相同的 vIDM 伺服器詳細資料。

- 問題 2288549：RepoSync 失敗，並顯示資訊清單檔案上的總和檢查碼失敗
  在最近升級至 2.4 的部署中觀察到。在全新部署的管理程式上備份和還原升級後的設定時，資料庫中存在的存放庫資訊清單總和檢查碼與實際資訊清單檔案的總和檢查碼不相符。這會導致 RepoSync 在備份還原後被標記為失敗。

  因應措施：若要從此失敗復原，請執行下列步驟：

  1. 執行 CLI 命令 `get service install-upgrade`
     記下結果中「Enabled on」的 IP。
  2. 登入上述命令的「Enabled on」傳回項中所示的 NSX Manager IP。
  3. 導覽至**系統** > **概觀**，並找到與「Enabled on」傳回項具有相同 IP 的節點。
  4. 在該節點上按一下**解決**。
  5. 當上述解決作業成功後，在同一介面中的所有節點上按一下**解決**。
     所有三個節點會立即顯示 RepoSync 狀態為**完成**。

- 問題 2279973：如果建立了空白群組並繼續進行升級，則在 MP 升級後，該空白群組會顯示為未啟動
  如果建立了空白群組並繼續進行升級，則會發生此問題。

  因應措施：請勿建立空白群組。

  請執行下列其中一項作業以繼續：

  - 刪除空白群組
  - 按一下 [繼續] 按鈕以完成升級
  - 重設計劃
- 問題 2282389：如果在叢集之間移動 ESX，則 UC 升級計劃與 VC 叢集成員資格不同步
  當 ESX 從 VC 中的一個叢集移到另一個叢集時，變更不會反映在 UC 升級計劃中。如果使用者在群組間選取「並行升級」，這可能會導致多台主機同時進入維護模式。

  因應措施：在 [主機升級] 頁面上，按一下 [重設] 選項可重建計劃，以便 UC 升級計劃與 VC 叢集同步。

- 問題 2288921：新增舊版本 Edge 節點時，升級狀態不同步
  如果使用者在升級 Edge 後新增較舊版本的 Edge 節點，則升級狀態將不同步。這會導致繼續升級呼叫時出現問題。

  因應措施：首先，避免新增舊版本 Edge 節點。如果確實遇到此問題，請重新啟動 UC 服務。

- 問題 2291625：升級計劃同步後，PCG 升級狀態從 SUCCESS 變更為 NOT_STARTED
  僅當使用者升級 PCG，然後嘗試升級更多代理程式/PCG 時，才會遇到此問題。
  在建議的工作流程中，當 PCG 升級後，不再需要透過 UC 介面升級跨雲端元件。

  這不會影響任何功能。先前成功完成的 PCG 升級的狀態在升級使用者介面上顯示為「無」。

  因應措施：無。功能應該不會受到影響。

- 問題 2293227：升級至 2.4 後，不會對執行 VMTools 10.3.5 的虛擬機器套用 IDFW 規則
  執行即時 NSX-T 升級後，不會對執行 VMTools 10.3.5 的虛擬機器套用 IDFW 規則，從而可能導致這些虛擬機器失去 AV 保護。

  因應措施：重新啟動受影響的虛擬機器。

- 問題 2295564：從 2.3 升級到 2.4 之後，Edge 節點控制器連線可能會斷開
  此為間歇性問題，將會影響某些南北向流量。

  因應措施：在同一 Edge 節點上啟用和停用維護模式。

- 問題 2294178 - 從 2.3.1 升級至 2.4 期間主機 VIB 更新失敗。
  從 2.3.1 至 2.4 版的升級程序可能會失敗，並顯示錯誤「在主機上安裝離線服務包失敗」。更確切地說，主機 VIB 更新失敗是因為交換器安全性模組無法解除載入。如果在交換設定檔中啟用 IP 探索功能，且使用執行 ESXi-6.7EP06 (組建編號 11675023) 的主機從 NSX-T 2.3.1 執行就地升級至 NSX-T 2.4 時，就會發生此問題。

  因應措施：如需因應措施，請參閱知識庫文章 67445：With IP Discovery enabled, host VIB update may fail when upgrading from NSX-T 2.3.1 to NSX-T 2.4 (若已啟用 IP 探索，則從 NSX-T 2.3.1 升級至 NSX-T 2.4 時主機 VIB 更新可能會失敗)。

- 問題 2277543 - 在就地升級期間主機 VIB 更新失敗，並顯示錯誤「在主機上安裝離線服務包失敗」。
  使用執行 ESXi-6.5P03 (組建編號 10884925) 的主機從 NSX-T 2.3.x 進行就地升級至 2.4 之前，在主機上執行 Storage vMotion 時，可能會發生此錯誤。如果在主機升級之前執行 Storage vMotion，系統不會移除 2.3.x 交換器安全性模組。Storage vMotion 會觸發記憶體流失，導致交換器安全性模組解除載入失敗。

  因應措施：請參閱知識庫文章 67444：Host VIB update may fail when upgrading from NSX-T 2.3.x to NSX-T 2.4.0 if VMs are storage vMotioned before host upgrade (如果在主機升級前虛擬機器已執行 Storage vMotion，則從 NSX-T 2.3.x 升級至 NSX-T 2.4.0 時，主機 VIB 更新可能會失敗)。

- 問題 2276398 - AV 合作夥伴服務虛擬機器使用 NSX 升級時，可能會有最多二十分鐘失去保護。
  當合作夥伴 SVM 升級時，系統會部署新的 SVM 並刪除舊的 SVM。主機 Syslog 可能會顯示 SolutionHandler 連線錯誤。

  因應措施：升級後刪除主機上的 ARP 快取項目，然後在主機上對合作夥伴控制 IP 執行 Ping 動作來解決此問題。

- 問題 2297918 - 從 2.3.1 升級至 2.4 後，無法從叢集中移除 NSX。
  將叢集從 2.3.1 升級至 2.4 後，NSX-T 無法移除，且會顯示下列執行失敗的訊息：「無法移除叢集上的 NSX：此網狀架構範本已存在相關的傳輸節點範本或傳輸節點集合。針對此網狀架構範本執行刪除/停用之前，必須先刪除傳輸節點範本或傳輸節點集合。」

  因應措施：將傳輸節點設定檔從受影響的叢集中斷連結，然後使用「移除 NSX」工作流程。

- 問題 2286030 - 從 NSX-T 2.3.x 和更早版本升級至 2.4.x 時，傳輸節點組態會顯示為失敗狀態。
  從 NSX-T 2.3.x 更早版本升級至 2.4.x 時，傳輸節點組態會因為 Null 指標例外狀況而進入失敗狀態。如果您將具有 VMkernel 介面卡的 ESXi 傳輸節點移轉至 N-VDS VLAN 邏輯交換器，然後從 NSX-T 2.3.x 升級至 NSX-T 2.4.x，則競爭情況可能會導致 ESXi 傳輸節點組態的狀態顯示為失敗。 不過，即使在節點標記為組態狀態失敗之後，與 NSX Manager 和控制器的 ESXi 傳輸節點連線在升級期間仍會保持原狀。

  因應措施：更新或重新傳送傳輸節點，以將組態狀態重設為成功。

  1. 從 NSX Manager 中，編輯顯示為失敗的 ESXi 傳輸節點。
  2. 在 ESXi 傳輸節點組態快顯視窗上，按一下**儲存**。
     此動作會重設狀態。您不需要修改組態。

API 已知問題

NSX Policy Manager 已知問題

- 問題 2291267：PCM 建立的預設閘道原則區段未獲指派序號，因此原則將序號預設為 0
  如果使用者建立閘道原則時未使用序號或 insert_top 選項，則會產生原則衝突。記錄位置：`/var/log/policy/policy.log`

  因應措施：透過始終使用適當的 sequence_numbers 或使用 URL 參數 `action=revise&operation=insert_top` 建立原則，可防止此問題。

- 問題 2289278：原則 API 擲回錯誤，但允許針對具有不同持續性設定檔的相同集區設定多個虛擬服務器
  對於不同的 LbVirtualServer，系統不支援為相同集區設定衝突的持續性類型。但是，原則無法正確驗證/拒絕衝突的輸入並允許設定。之後，原則會顯示警示以及錯誤訊息。

  因應措施：如果您遇到此問題，可以透過變更 LbVirtualServer 上的群組設定來進行更正。

- 問題 2248186 - BGP 路由器使用自己的介面做為下一個躍點從其芳鄰安裝 IPV6 路由。
  如此一來，已安裝路由的 IPV6 轉送可能會失敗，並導致轉送迴圈。

  因應措施：若要避免發生此問題，請在 BGP 更新中設定路由對應來篩選 IPv6 連線位址做為下一個躍點。

NSX Cloud 已知問題

- 問題 2287884：NSX Cloud 不支援某些 Centos 市集映像
  NSX Cloud 僅支援其發行版本與預期次要核心版本相符的 Centos 市集映像。
  例如，發行版版本及其對應的核心版本應如下所示：

  - RHEL 7.5 3.10.0-862
  - RHEL 7.4 3.10.0-693
  - RHEL 7.3 3.10.0-514

  因應措施：根據說明文件中的建議，僅使用建議的 Centos 發行版。

- 問題 2275232：如果 DFW 的 Connectivity_statregy 已從黑名單變更為白名單，DHCP 將不適用於雲端上的虛擬機器
  申請新 DHCP 租用的所有虛擬機器都將遺失 IP。需要在 DFW 中明確允許 DHCP 用於雲端虛擬機器。

  因應措施：在 DFW 中明確允許 DHCP 用於雲端虛擬機器。

- 問題 2277814：具有無效 nsx.network 標籤值的虛擬機器被移至 vm-overlay-sg
  標記有無效 nsx.network 標籤的虛擬機器將被移至 vm-overlay-sg。

  因應措施：移除無效的標籤。

- 問題 2280663：在少數情況下，使多個 VPC 並行離線可能會導致失敗
  將其中一個計算 VPC 離線會失敗。

  因應措施：手動清除 VPC 及原則上對應的群組。

- 已修正的問題 2287124：在 Microsoft Azure VNet 上部署 PCG 後，在 CSM 中 VNet 的動態磚錯誤地報告警告
  在 Microsoft Azure VNet 上部署 PCG 後，在 CSM 中 VNet 報告警告標誌 (帶有驚嘆號的黃色三角形)。如果您將游標暫留在警告圖示上方，CSM 會報告 MP (管理區域) 和 CCP (控制平面) 的狀態為未知。但是，連線可能沒有任何問題，而該警告的顯示有誤。

- 問題 2290688 - 在 AWS 中升級 Windows 2016 虛擬機器會失敗。
  在 AWS 中升級多個 Windows 工作負載虛擬機器會失敗。在 AWS 入口網站中，虛擬機器的升級狀態會顯示為停滯在「1/2 檢查」。重試也會失敗。此問題僅出現在相同的 NSX-T 版本升級中。

  因應措施：若要從此問題復原，請執行下列步驟：

  1. 確保 PCG 在受影響的主機中進行升級，以便虛擬機器可以下載最新的主機元件。
  2. 重新開機虛擬機器以進入良好狀態。
  3. 手動執行解除安裝 cmd。
  4. 手動執行安裝 cmd。